



Rich's lesson module checklist

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

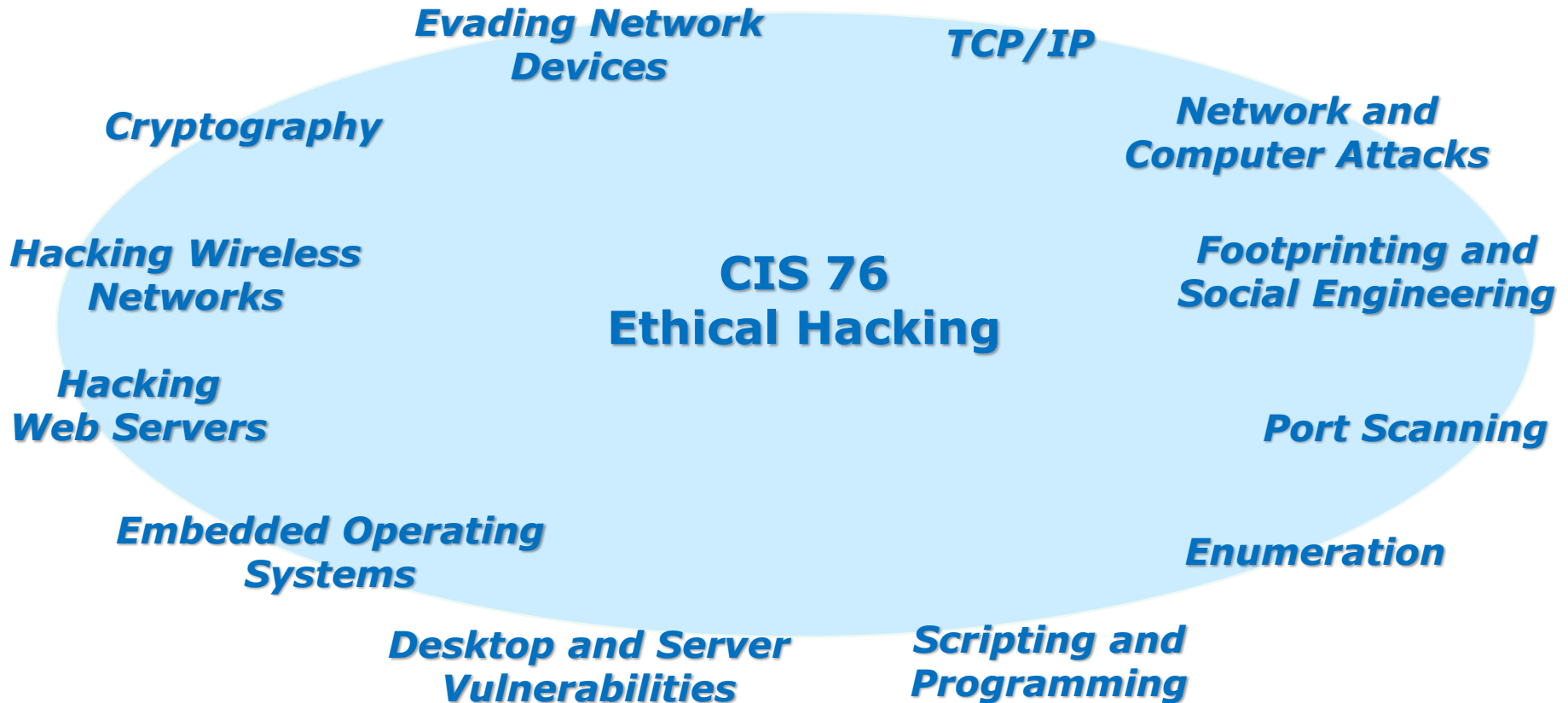
- Flash cards
- Properties
- Page numbers
- 1st minute quiz
- Web Calendar summary
- Web book pages
- Commands

- Practice test on Canvas

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

- Update CCC Confer and 3C Media portals

Last updated 10/24/2017



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. The page title is "Rich's Cabrillo College CIS Classes CIS 90 Calendar". On the left sidebar, there are several course links, with "CIS 76" highlighted in a red box. The main content area shows a table for "CIS 90 (Fall 2014) Calendar" with columns for "Lesson", "Date", "Topics", and "Link". The "Calendar" link is highlighted in a red box. The table content includes:

Lesson	Date	Topics	Link
		<p>Class and Linux Overview</p> <ul style="list-style-type: none"> Understand how the course will work High-level overview of computers, operating systems, and virtual machines Overview of LINUX/Linux market and architecture Using SSH for remote network logs Using terminals and the command line <p>Methods</p> <p>Presentation slides (download)</p> <p>Supplemental</p> <ul style="list-style-type: none"> Howto #148: Logging into Opus (command) <p>Assignments</p> <ul style="list-style-type: none"> Student Survey Lab 1 <p>CCS Center</p> <p>Enter virtual classroom</p>	
	9/2		
		<p>Quiz 1</p> <p>Commands</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-II with Putty or ssh command.

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



Student checklist for suggested screen layout

Google

CCC Confer

Downloaded PDF of Lesson Slides

The screenshot displays a virtual classroom interface. On the left is a Blackboard course page for 'Rich's Cabrillo College CIS 90 Classes'. In the center is a CCC Confer window showing a video of 'Rich Simms' and a chat window with messages. A Google Maps window is open in the foreground, showing a map of the San Francisco Bay Area. On the right is a PDF window titled 'cis90lesson01.pdf - Adobe Acrobat Pro' showing a slide titled 'The CIS 90 System Playground'. Below the PDF is a terminal window showing a login prompt and a password being entered.

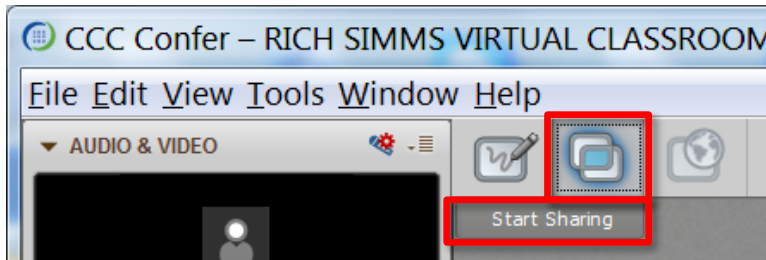
CIS 76 website Calendar page

One or more login sessions to Opus-II

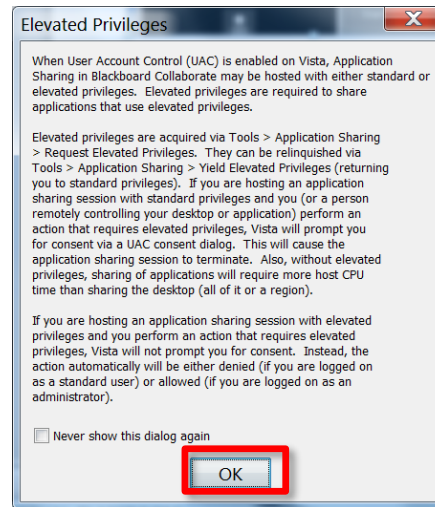


Student checklist for sharing desktop with classmates

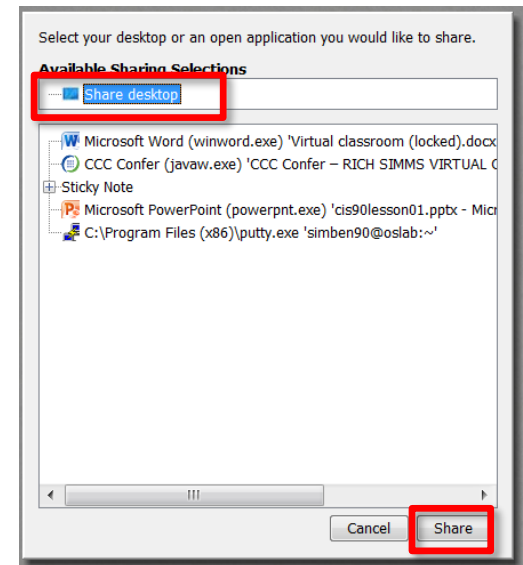
1) Instructor gives you sharing privileges.



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



3) Click OK button.



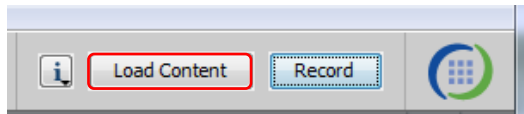
4) Select "Share desktop" and click Share button.



Rich's CCC Confer checklist - setup

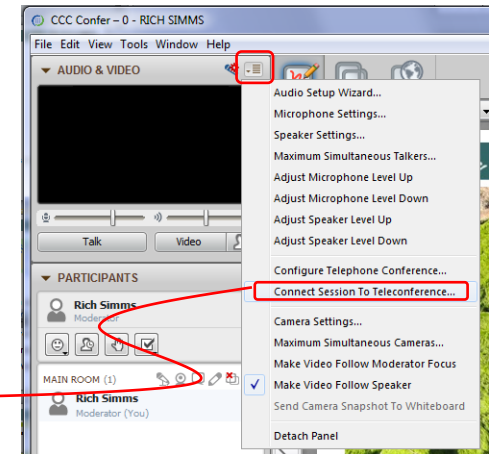
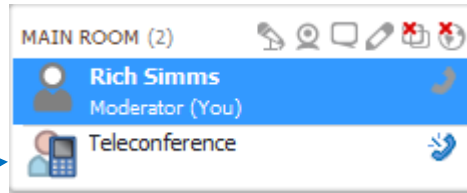


[] Preload White Board



[] Connect session to Teleconference

Session now connected to teleconference



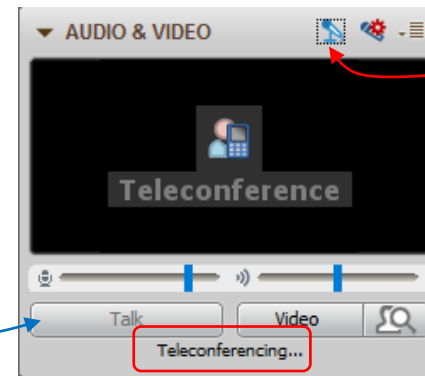
[] Is recording on?



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



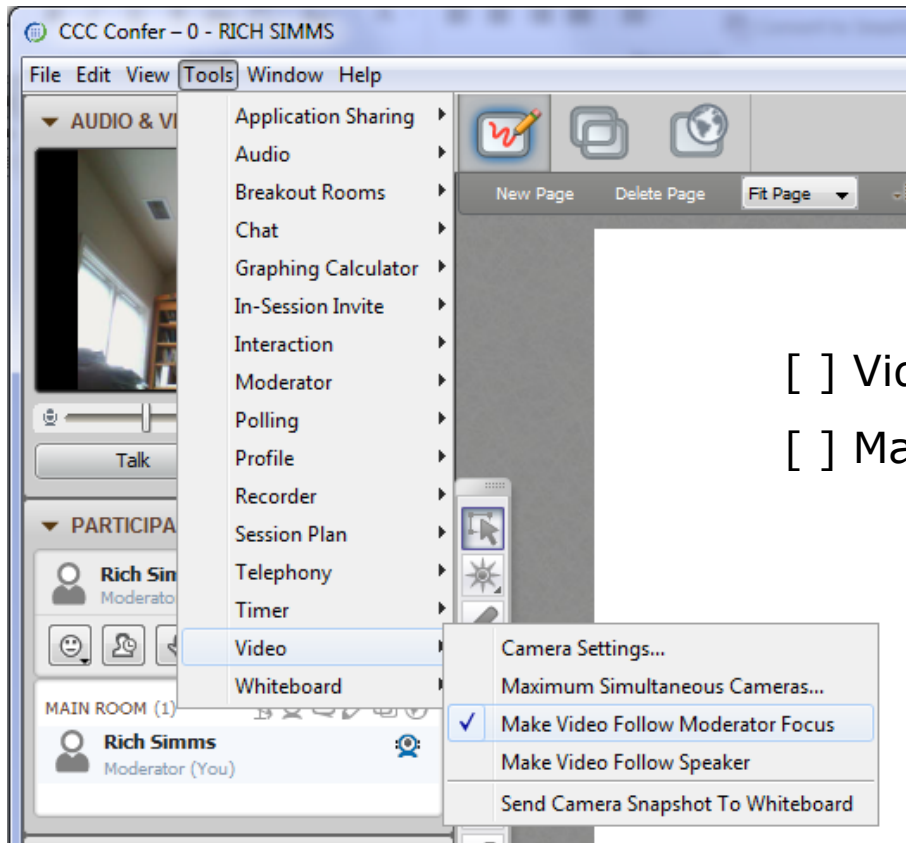
The screenshot displays a Windows desktop with several applications open. On the left, a 'CCC Confer' window shows a video feed of Rich Simms and a list of participants. In the center, a 'Foxit Reader' window displays a PDF document with a file tree on the left. To the right, a 'Chrome' browser window shows a quiz page with questions and answers. In the foreground, a 'Putty' terminal window shows a login attempt for 'simben90@oslab'. In the bottom right, the 'vSphere Client' window shows the vCenter interface. A yellow vertical bar highlights the left side of the desktop. Three red callout boxes with white text label specific elements: '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.

[] layout and share apps





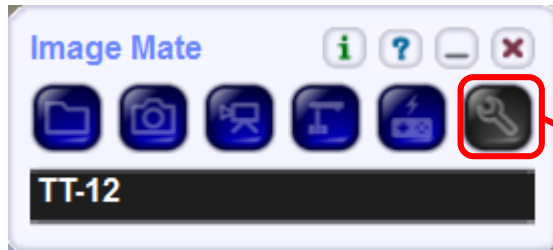
Rich's CCC Confer checklist - webcam setup



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



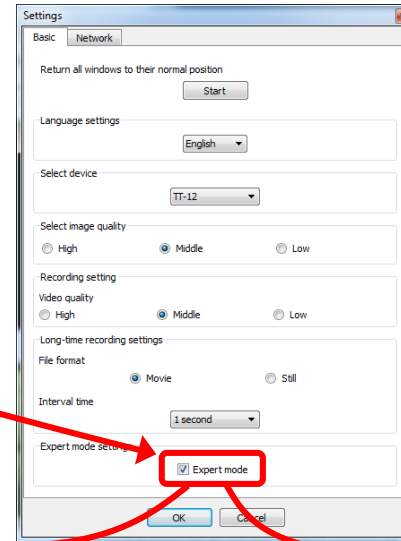
Rich's CCC Confer checklist - Elmo



Elmo rotated down to view side table



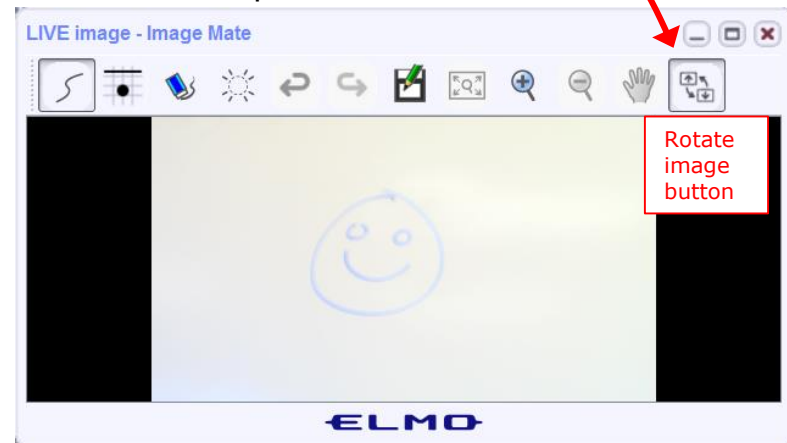
Run and share the Image Mate program just as you would any other app with CCC Confer



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 up to view white board





Rich's CCC Confer checklist - universal fixes

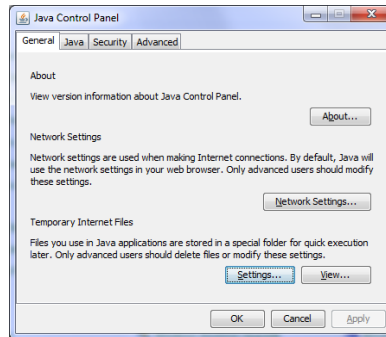
Universal Fix for CCC Confer:

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

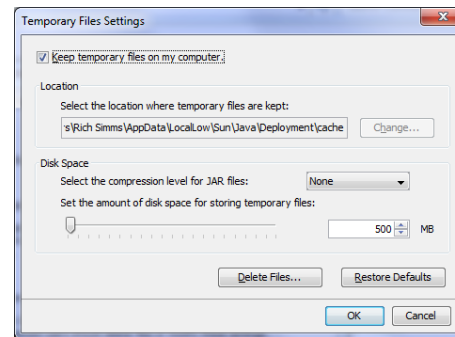
Control Panel (small icons)



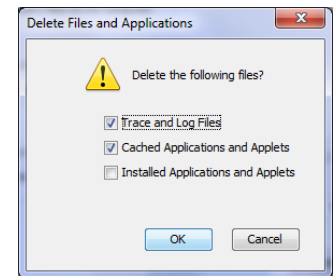
General Tab > Settings...



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.*

Volume

**4 - increase conference volume.*

**7 - decrease conference volume.*

**5 - increase your voice volume.*

**8 - decrease your voice volume.*



Instructor: **Rich Simms**

Dial-in: **888-886-3951**

Passcode: **136690**



Philip



Bruce



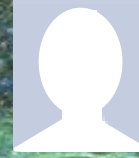
Tre



Sam B.



Sam R.



Miguel



Bobby



Garrett



Ryan A.



Aga



Karina



Chris



Tanner



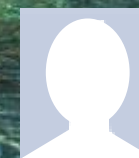
Helen



Xu



Mariano



Cameron



Ryan M.



May



Karl-Heinz



Remy

First Minute Quiz

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

Use CCC Confer White Board

email answers to: risimms@cabrillo.edu

(answers must be emailed within the first few minutes of class for credit)



Review and Gaps

Objectives

- Look at the Mirai Bot
- Get second group attempt on EC-Council mini assessment
- Review material from the NISGTC EH course

Agenda

- Quiz #7
- Questions
- In the news
- Best practices
- Mirai Botnet
- EC-Council mini assessment 1-10
- Housekeeping
- EC-Council mini assessment 11-20
- Red/blue pods
- EC-Council mini assessment 21-30
- NISGTC - Domain 3
- Steganography
- EC-Council mini assessment 31-40
- NISGTC - Domain 4
- More recon websites
- EC-Council mini assessment 41-50
- NISGTC - Domain 10
- Assignment
- Wrap up

Admonition



Unauthorized hacking is a crime.

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

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



Questions

Questions?

Lesson material?

Labs? Tests?

How this course works?

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

Who questions much, shall learn much, and retain much.

- Francis Bacon

If you don't ask, you don't get.

- Mahatma Gandhi

Chinese
Proverb

他問一個問題，五分鐘是個傻子，他不問一個問題仍然是一個傻瓜永遠。

He who asks a question is a fool for five minutes; he who does not ask a question remains a fool forever.

In the news

Recent news

U.S. warns public about attacks on energy, industrial firms
by Jim Finkle Oct 21, 2017

<http://www.reuters.com/article/us-usa-cyber-energy/u-s-warns-public-about-attacks-on-energy-industrial-firms-idUSKBN1CQ0IN>



"The U.S government issued a rare public warning that sophisticated hackers are targeting energy and industrial firms, the latest sign that cyber attacks present an increasing threat to the power industry and other public infrastructure."

Recent news

Google launched a new bug bounty program to root out vulnerabilities in third-party apps on Google Play
by Andrew Liptak Oct 22, 2017

<https://www.theverge.com/2017/10/22/16516670/google-play-security-rewards-program-vulnerabilities-bug-bounty>

THE VERGE



"According to HackerOne, hackers will identify app vulnerabilities and report it to the developer, and both work out a resolution within 90 days. The hacker then requests a reward from the program. Once it's evaluated and found to meet Google's criteria, the finder will be awarded \$1000.

Recent news

Russia's Election Hackers Use D.C. Cyber Warfare Conference as Bait
By Kevin Poulsen Oct 23, 2017

<https://www.thedailybeast.com/russias-election-hackers-use-dc-cyber-warfare-conference-as-bait>



"The Russian hackers' flier for the event is a Microsoft Word document named "Conference_on_Cyber_Conflict.doc". It contains the logos of the conference organizers and a sponsor, and text copied from the conference website touting the 2017 theme, "The Future of Cyber Conflict." But Russia isn't distributing the document to boost attendance. Buried inside is a malicious macro that downloads and installs malware called Seduploader, a Fancy Bear reconnaissance program that lets the hackers take screenshots and gather basic system information to decide if the victim is worth spying on long-term."

Recent news

New Rapidly-Growing IoT Botnet Threatens to Take Down the Internet

By Wang Wei Oct 20, 2017

<https://thehackernews.com/2017/10/iot-botnet-malware-attack.html>



“Just a year after Mirai—biggest IoT-based malware that caused vast Internet outages by launching massive DDoS attacks—completed its first anniversary, security researchers are now warning of a brand new rapidly growing IoT botnet.”

"Dubbed 'IoT_reaper,' first spotted in September by researchers at firm Qihoo 360, the new malware no longer depends on cracking weak passwords; instead, it exploits vulnerabilities in various IoT devices and enslaves them into a botnet network."

Recent news

Multiple Ransomware Infections Reported

Original release date: October 24, 2017

<https://www.us-cert.gov/ncas/current-activity/2017/10/24/Multiple-Ransomware-Infections-Reported>



"US-CERT has received multiple reports of Bad Rabbit ransomware infections in many countries around the world. This suspected variant of Petya ransomware is malicious software that infects a computer and restricts user access to the infected machine until a ransom is paid to unlock it. US-CERT discourages individuals and organizations from paying the ransom, as this does not guarantee that access will be restored. Using unpatched and unsupported software may increase the risk of proliferation of cybersecurity threats, such as ransomware."



Best Practices

Defense Best Practices

Who Makes the IoT Things Under Attack?

<https://krebsonsecurity.com/2016/10/who-makes-the-iot-things-under-attack/>

*"If possible, **reset the device to the factory-default settings**. This should ensure that if any malware has been uploaded to the device that it will be wiped permanently. Most devices have a small, recessed button that needs to be pressed and held down for a several seconds while powered on to reset the thing back to the factory default settings.*

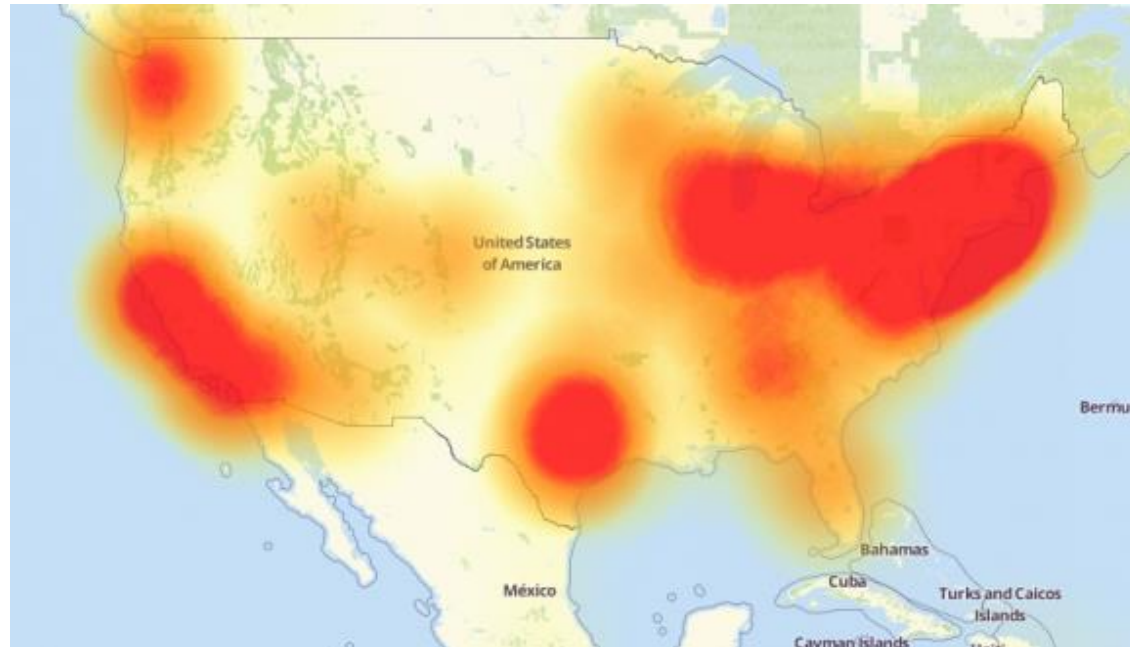
*When the device comes back online, quickly fire up a Web browser, navigate to the administration panel, enter the default credentials, and then **change the default password** to something stronger and more memorable. I hope it goes without saying that any passwords remotely resembling the default passwords noted in the image above are horrible passwords. [Here's some advice](#) on picking better ones."*



Mirai Bot

DDoS attack on Dyn

Friday October 21, 2016



A depiction of the outages caused by today's attacks on Dyn, an Internet infrastructure company. Source: Downtetector.com.

"The attack began creating problems for Internet users reaching an array of sites, including Twitter, Amazon, Tumblr, Reddit, Spotify and Netflix."

<https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/>

DDoS attack on Dyn

Friday October 21, 2016

Drew says the attack consisted mainly of TCP SYN floods aimed directly at against port 53 of Dyn's DNS servers, but also a prepend attack, which is also called a subdomain attack. That's when attackers send DNS requests to a server for a domain for which they know the target is authoritative. But they tack onto the front of the domain name random prepends or subnet designations. The server won't have these in its cache so will have to look them up, sapping computational resources and effectively preventing the server from handling legitimate traffic, he says.

<http://www.networkworld.com/article/3134057/security/how-the-dyn-ddos-attack-unfolded.html>

DDoS attack on Dyn

Friday October 21, 2016

*In an interim report on the attack, Dyn said: “We can confirm, with the help of analysis from **Flashpoint** and **Akamai**, that one source of the traffic for the attacks were devices infected by the **Mirai botnet**. We observed 10s of millions of discrete IP addresses associated with the Mirai botnet that were part of the attack.”*

<https://krebsonsecurity.com/2016/10/iot-device-maker-vows-product-recall-legal-action-against-western-accusers/>

Multiple Mirai botnets now

“While Flashpoint has confirmed that Mirai botnets were used in the October 21, 2016 attack against Dyn, they were separate and distinct botnets from those used to execute the DDoS attacks against ‘Krebs on Security’ and OVH,” Flashpoint said in a statement sent to Salted Hash.

Since the Mirai source code was released earlier this month, copycats have used it to create botnets of their own in order to launch DDoS attacks. Today’s attacks are proof that script kiddies and criminals wasted no time in recycling the Mirai code for their own use.

<http://www.csoonline.com/article/3133992/security/ddos-knocks-down-dns-datacenters-across-the-u-s-affected.html>



Mirai Source Code

Mirai bot source code has been released

The screenshot shows a web browser window with the URL <https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/>. The page features an advertisement for Exabeam at the top, followed by the KrebsOnSecurity logo and a photo of the author. The main article title is "01 Source Code for IoT Botnet 'Mirai' Released" with a date of "OCT 16". The text describes the release of the source code for the Mirai botnet, which was responsible for a large DDoS attack. It mentions that the code is available on GitHub. There is also a sidebar advertisement for ThreatConnect with the slogan "Good by themselves. Better together." and a "DOWNLOAD WHITE PAPER" button.

<https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/>

The screenshot shows a GitHub comment from a user named "tony" dated "October 3, 2016 at 10:43 pm". The comment contains the GitHub repository URL: <https://github.com/jgamblin/Mirai-Source-Code/blob/6a5941be681b839eef8ece1de8b245bcd5ffbo2/mirai/bot/scanner.c#L123>. Below the URL is a "REPLY" button.

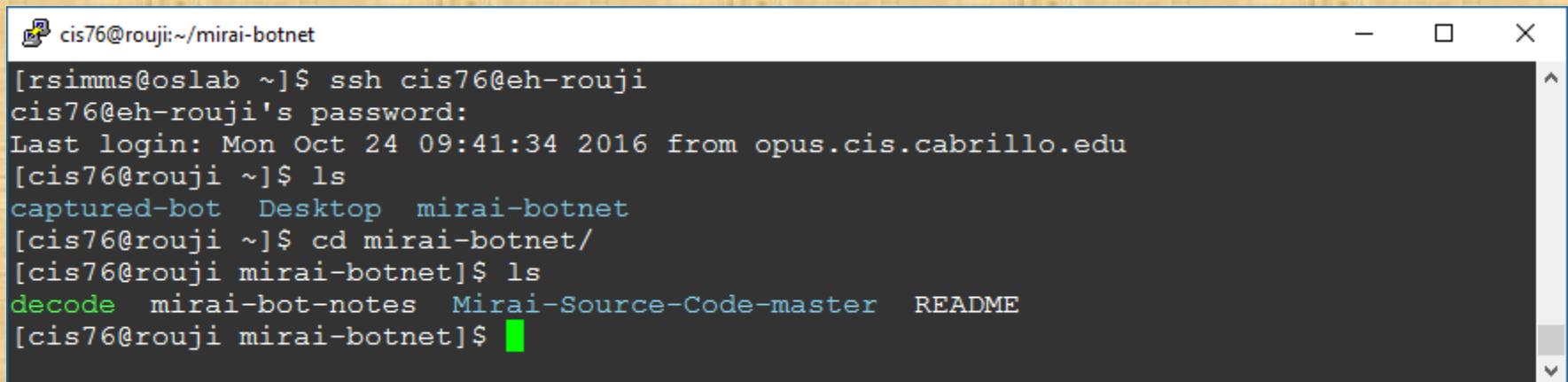
<https://github.com/jgamblin/Mirai-Source-Code>

The source code is available now on EH-Rouji

Activity

Log into eh-rouji and change into the mirai-botnet directory

```
ssh cis76@eh-rouji
cd mirai-botnet
```

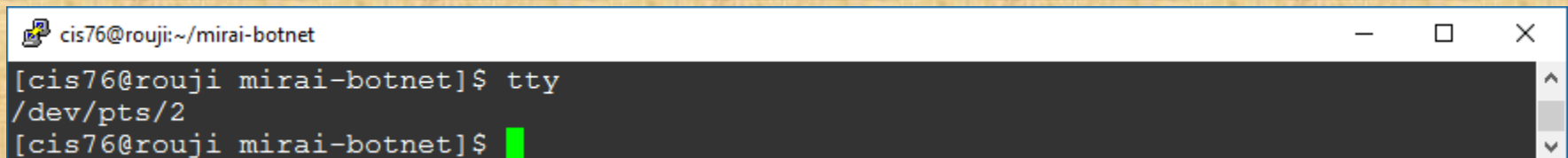


```

cis76@rouji:~/mirai-botnet
[rsimms@oslab ~]$ ssh cis76@eh-rouji
cis76@eh-rouji's password:
Last login: Mon Oct 24 09:41:34 2016 from opus.cis.cabrillo.edu
[cis76@rouji ~]$ ls
captured-bot  Desktop  mirai-botnet
[cis76@rouji ~]$ cd mirai-botnet/
[cis76@rouji mirai-botnet]$ ls
decode  mirai-bot-notes  Mirai-Source-Code-master  README
[cis76@rouji mirai-botnet]$

```

tty



```

cis76@rouji:~/mirai-botnet
[cis76@rouji mirai-botnet]$ tty
/dev/pts/2
[cis76@rouji mirai-botnet]$

```

Use tty and put your terminal device /dev/pts/xx into the chat window

Mirai Default Credentials

Default Credentials

"The purpose of these scans is to locate under-secured IoT devices that could be remotely accessed via easily guessable login credentials—usually factory default usernames and passwords (e.g., admin/admin)."

https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html?utm_source=twitter&utm_medium=organic_emp&utm_campaign=2016_Q4_miraidos

Activity

Change into the bot source code directory and view scanner.c

```
cd mirai-botnet/Mirai-Source-Code-master/mirai/bot/  
vi scanner.c
```

```
cis76@rouji:~/mirai-botnet/Mirai-Source-Code-master/mirai/bot
tcph->source = source_port;
tcph->doff = 0;
tcph->>window = rand_next() & 0xffff;
tcph->syn = TRUE;

// Set up passwords
add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x41\x11\x17\x13\x13", 10); // root xc3511
add_auth_entry("\x50\x4D\x4D\x56", "\x54\x4B\x58\x5A\x54", 9); // root vizxv
add_auth_entry("\x50\x4D\x4D\x56", "\x43\x46\x4F\x4B\x4C", 8); // root admin
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C", 7); // admin admin
add_auth_entry("\x50\x4D\x4D\x56", "\x1A\x1A\x1A\x1A\x1A\x1A", 6); // root 888888
add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x4F\x4A\x46\x4B\x52\x41", 5); // root xmhdipc
add_auth_entry("\x50\x4D\x4D\x56", "\x46\x47\x44\x43\x57\x4E\x56", 5); // root default
add_auth_entry("\x50\x4D\x4D\x56", "\x48\x57\x43\x4C\x56\x47\x41\x4A", 5); // root juantech
add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17\x14", 5); // root 123456
118,1 11%
```

Scroll down to the scanner_init function and find where credentials are being setup. Look for the username "support" and put the corresponding password into the chat window.

Mirai Target IoT Devices

Mirai Target Devices

Username/Password	Manufacturer	Link to supporting evidence
admin/123456	ACTI IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/anko	ANKO Products DVR	http://www.cctvforum.com/viewtopic.php?f=3&t=44250
root/pass	Axis IP Camera, et. al	http://www.cleancss.com/router-default/Axis/0543-001
root/vizxv	Dahua Camera	http://www.cam-it.org/index.php?topic=5192.0
root/888888	Dahua DVR	http://www.cam-it.org/index.php?topic=5035.0
root/666666	Dahua DVR	http://www.cam-it.org/index.php?topic=5035.0
root/7ujMko0vizxv	Dahua IP Camera	http://www.cam-it.org/index.php?topic=9396.0
root/7ujMko0admin	Dahua IP Camera	http://www.cam-it.org/index.php?topic=9396.0
666666/666666	Dahua IP Camera	http://www.cleancss.com/router-default/Dahua/DH-IPC-HDW4300C
root/dreambox	Dreambox TV receiver	https://www.satellites.co.uk/forums/threads/reset-root-password-plugin.101146/
root/zlxx	EV ZLX Two-way Speaker?	?
root/juantech	Guangzhou Juan Optical	https://news.ycombinator.com/item?id=11114012
root/xc3511	H.264 - Chinese DVR	http://www.cctvforum.com/viewtopic.php?f=56&t=34930&start=15
root/hi3518	HiSilicon IP Camera	https://acassis.wordpress.com/2014/08/10/i-got-a-new-hi3518-ip-camera-modules/
root/klv123	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/klv1234	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/jvzbd	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/admin	IPX-DDK Network Camera	http://www.ipxinc.com/products/cameras-and-video-servers/network-cameras/
root/system	IQinVision Cameras, et. al	https://ipvm.com/reports/ip-cameras-default-passwords-directory
admin/meinism	Mobotix Network Camera	http://www.forum.use-ip.co.uk/threads/mobotix-default-password.76/
root/54321	Packet8 VOIP Phone, et. al	http://webcache.googleusercontent.com/search?q=cache:W1phozQZURUJ:community.freepbx.org/t/packet8-atas-phones/4111
root/00000000	Panasonic Printer	https://www.experts-exchange.com/questions/26194395/Default-User-Password-for-Panasonic-DP-C405-Web-Interface.html
root/realtek	RealTek Routers	
admin/1111111	Samsung IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/xmhdipc	Shenzhen Anran Security Camera	https://www.amazon.com/MegaPixel-Wireless-Network-Surveillance-Camera/product-reviews/B00EB6FNDI
admin/smcadmin	SMC Routers	http://www.cleancss.com/router-default/SMC/ROUTER
root/ikwb	Toshiba Network Camera	http://faq.surveillixdvr.support.com/index.php?action=artikel&cat=4&id=8&artlang=en
ubnt/ubnt	Ubiquiti AirOS Router	http://setuprouter.com/router/ubiquiti/airos-airgrid-m5hp/login.htm
supervisor/supervisor	VideoIQ	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/<none>	Vivotek IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
admin/1111	Xerox printers, et. al	https://atyourservice.blogs.xerox.com/2012/08/28/logging-in-as-system-administrator-on-your-xerox-printer/
root/Zte521	ZTE Router	http://www.ironbugs.com/2016/02/hack-and-patch-your-zte-f660-routers.html

Mirai Target Devices

The screenshot shows a web browser window displaying the IPVM website. The page title is "IP Cameras Default Passwords Directory" by Ethan Ace, published on May 28, 2016. The article discusses the difficulty of finding default passwords for IP cameras and provides a list of manufacturers and their default credentials. A sidebar on the right contains the IPVM logo, a description of the site as a leading video surveillance information source, and a "MEMBER LOGIN" form with fields for "Login" and "Password", a "Login" button, and a "Remember me" checkbox.

IPVM About Articles Members Tests Courses Calculator Tools Discussions Login Search

Free 2016 IP Networking Book GET THE FREE BOOK NOW

IP Cameras Default Passwords Directory

Author: Ethan Ace, Published on May 28, 2016

Finding an IP camera's default password can be tedious or aggravating. And keeping up with changes in newer firmwares can be difficult, especially for occasional users.

With that in mind, we have gathered this list of IP camera manufacturers and their default usernames and passwords to help users get started more quickly. After the list, we discuss recent changes by manufacturers as well as password security issues.

[Don't miss [downloading our free IP video surveillance book.](#)]

Manufacturer List

For each manufacturer, we list the username first and password section in the following format: username/password. Where manufacturers have multiple defaults, or differences in newer/older firmwares, we have noted it:

- ACTI: admin/123456 or Admin/123456
- American Dynamics: admin/admin or admin/9999
- Arecont Vision: none
- Avigilon: Previously admin/admin, changed to Administrator/<blank> in later firmware versions
- Axis: Traditionally root/pass, new Axis cameras require password creation during first login (though root/pass may be used for ONVIF access)
- Basler: admin/admin

IPVM
The world's leading video surveillance information source, IPVM provides the best reporting, testing and training for 10,000+ members globally. Dedicated to independent and objective information, we uniquely refuse any and all advertisements, sponsorship and consulting from manufacturers.
About | FAQ | Contact

MEMBER LOGIN

Login

Password

Login

Remember me

An article documenting many of the default usernames and passwords for IP cameras

Mirai Target Devices

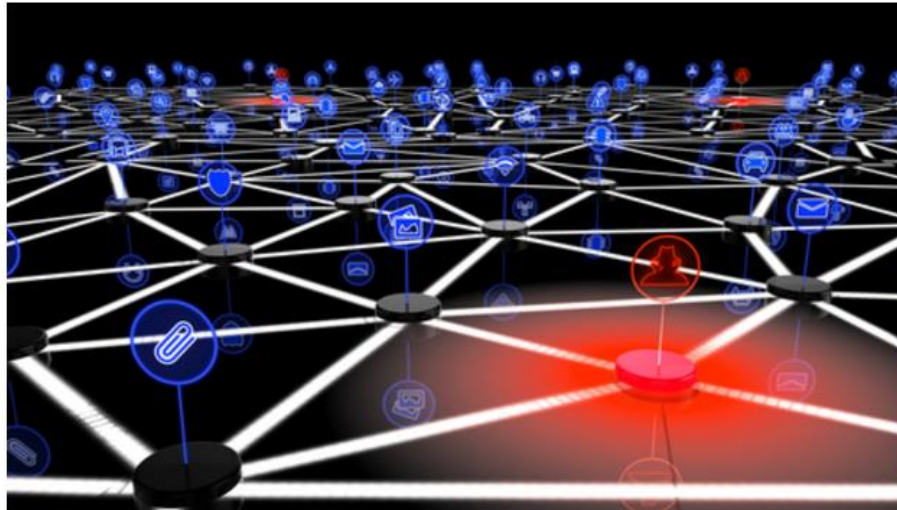


Some of the many IP cameras available today

24 IoT Device Maker Vows Product Recall, Legal Action Against Western Accusers

OCT 16

A Chinese electronics firm pegged by experts as responsible for making many of the components leveraged in **last week's massive attack** that disrupted Twitter and dozens of popular Web sites has vowed to recall some of its vulnerable products, even as it threatened legal action against this publication and others for allegedly tarnishing the company's brand.



Last week's attack on online infrastructure provider **Dyn** was launched at least in part by **Mirai**, a **now open-source** malware strain that scans the Internet for routers, cameras, digital video recorders and other Internet of Things "IoT" devices protected only by the factory-default passwords. Once infected with Mirai, the IoT systems can be used to flood a target with so much junk Web traffic that the target site can no longer accommodate legitimate users or visitors.

<https://krebsonsecurity.com/2016/10/iot-device-maker-vows-product-recall-legal-action-against-western-accusers/>

Mirai IP Address Targets

Mirai avoids attacking specific networks

"One of the most interesting things revealed by the code was a hardcoded list of IPs Mirai bots are programmed to avoid when performing their IP scans."

https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html?utm_source=twitter&utm_medium=organic_emp&utm_campaign=2016_Q4_miraiddos

Activity

Locate the `get_random_ip` function in `scanner.c`

```
cd mirai-botnet/Mirai-Source-Code-master/mirai/bot/
vi scanner.c
```

```

cis76@rouji:~/mirai-botnet/Mirai-Source-Code-master/mirai/bot
static ipv4_t get_random_ip(void)
{
    uint32_t tmp;
    uint8_t o1, o2, o3, o4;

    do
    {
        tmp = rand_next();

        o1 = tmp & 0xFF;
        o2 = (tmp >> 8) & 0xFF;
        o3 = (tmp >> 16) & 0xFF;
        o4 = (tmp >> 24) & 0xFF;
    }
    while (o1 == 127 || // 127.0.0.0/8 - Loopback
           (o1 == 0) || // 0.0.0.0/8 - Invalid address space
           (o1 == 3) || // 3.0.0.0/8 - General Electric Company
           (o1 == 15 || o1 == 16) || // 15.0.0.0/7 - Hewlett-Packard Company
           (o1 == 56) || // 56.0.0.0/8 - US Postal Service
           (o1 == 10) || // 10.0.0.0/8 - Internal network
           (o1 == 192 && o2 == 168) || // 192.168.0.0/16 - Internal network
           (o1 == 172 && o2 >= 16 && o2 < 32) || // 172.16.0.0/14 - Internal network
           (o1 == 100 && o2 >= 64 && o2 < 127) || // 100.64.0.0/10 - IANA NAT reserved
           (o1 == 169 && o2 > 254) || // 169.254.0.0/16 - IANA NAT reserved
           (o1 == 198 && o2 >= 18 && o2 < 20) || // 198.18.0.0/15 - IANA Special use
           (o1 >= 224) || // 224.*.*.*+ - Multicast
           (o1 == 6 || o1 == 7 || o1 == 11 || o1 == 21 || o1 == 22 || o1 == 26 || o1 == 28 || o1 == 29 || o1 == 30 ||
           o1 == 33 || o1 == 55 || o1 == 214 || o1 == 215) // Department of Defense
    );

    return INET_ADDR(o1,o2,o3,o4);
}

```

Remember how to do sub-netting from CIS 81?

The comment for HP is incorrect. What should it be?

Put your answer in the chat window.



Mirai

Obfuscation

Mirai Hex Codes and Obfuscation

Portions of the Mirai source code contain obfuscated hex codes.

```
cd mirai-botnet/Mirai-Source-Code-master/mirai/bot/  
vi table.c
```

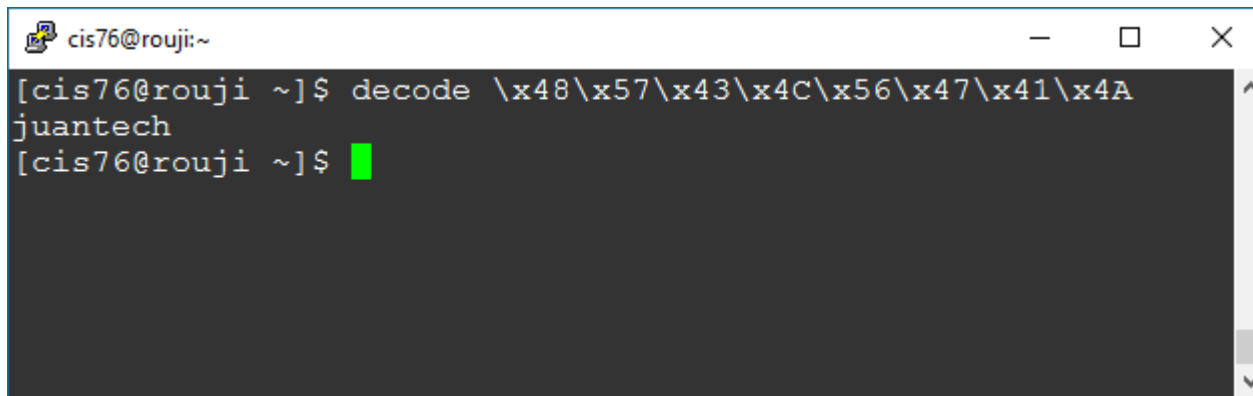
```
add_entry(TABLE_KILLER_PROC, "\x0D\x52\x50\x4D\x41\x0D\x22", 7);  
add_entry(TABLE_KILLER_EXE, "\x0D\x47\x5A\x47\x22", 5);  
add_entry(TABLE_KILLER_DELETED, "\x02\x0A\x46\x47\x4E\x47\x56\x47\x46\x0B\x22", 11);  
add_entry(TABLE_KILLER_FD, "\x0D\x44\x46\x22", 4);  
add_entry(TABLE_KILLER_ANIME, "\x0C\x43\x4C\x4B\x4F\x47\x22", 7);  
add_entry(TABLE_KILLER_STATUS, "\x0D\x51\x56\x43\x56\x57\x51\x22", 8);  
add_entry(TABLE_MEM_QBOT, "\x70\x67\x72\x6D\x70\x76\x02\x07\x51\x18\x07\x51\x22", 13);  
add_entry(TABLE_MEM_QBOT2, "\x6A\x76\x76\x72\x64\x6E\x6D\x6D\x66\x22", 10);  
add_entry(TABLE_MEM_QBOT3, "\x6E\x6D\x6E\x6C\x6D\x65\x76\x64\x6D\x22", 10);
```

The table_init function in table.c

Mirai Hex Codes and Obfuscation

There is a bash decode script in ~/bin (on your path) that will decode the Mirai bot hexcodes

```
decode \x48\x57\x43\x4C\x56\x47\x41\x4A
```



```
cis76@rouji:~  
[cis76@rouji ~]$ decode \x48\x57\x43\x4C\x56\x47\x41\x4A  
juantech  
[cis76@rouji ~]$
```

Use decode then paste the in hex codes as the argument.

Activity

View the table.c code

```
cd mirai-botnet/Mirai-Source-Code-master/mirai/bot/
head -n76 table.c
```

```
add_entry(TABLE_KILLER_PROC, "\x0D\x52\x50\x4D\x41\x0D\x22", 7);
add_entry(TABLE_KILLER_EXE, "\x0D\x47\x5A\x47\x22", 5);
add_entry(TABLE_KILLER_DELETED, "\x02\x0A\x46\x47\x4E\x47\x56\x47\x46\x0B\x22", 11);
add_entry(TABLE_KILLER_FD, "\x0D\x44\x46\x22", 4);
add_entry(TABLE_KILLER_ANIME, "\x0C\x43\x4C\x4B\x4F\x47\x22", 7);
add_entry(TABLE_KILLER_STATUS, "\x0D\x51\x56\x43\x56\x57\x51\x22", 8);
add_entry(TABLE_MEM_QBOT, "\x70\x67\x72\x6D\x70\x76\x02\x07\x51\x18\x07\x51\x22", 13);
add_entry(TABLE_MEM_QBOT2, "\x6A\x76\x76\x72\x64\x6E\x6D\x6D\x66\x22", 10);
add_entry(TABLE_MEM_QBOT3, "\x6E\x6D\x6E\x6C\x6D\x65\x76\x64\x6D\x22", 10);
```

Decode the TABLE_KILLER_SAFE entry to get a URL. Visit the URL in a browser.

What do you see? Put your answer in the chat window.

1. In a terminal, decode a random entry in the table of hex codes in table.c, for example:

```
add_entry(TABLE_ATK_CONTENT_TYPE, "\x61\x4D\x4C\x56\x47\x4C\x56\x0F\x76\x5B\x52\x47\x18\x02\x43\x52\x52\x4E\x4B\x41\x43\x56\x4B\x4D\x4C\x0D\x5A\x0F\x55\x55\x55\x0F\x44\x4D\x50\x4F\x0F\x57\x50\x4E\x47\x4C\x41\x4D\x46\x47\x46\x22", 48);
```

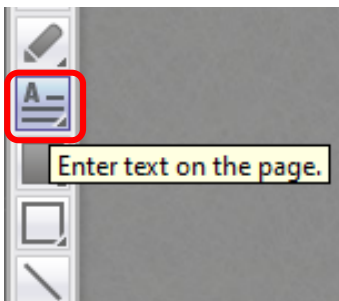
Hex codes

```
[cis76@rouji ~]$ decode \x61\x4D\x4C\x56\x47\x4C\x56\x0F\x76\x5B\x52\x47\x18\x02\x43\x52\x52\x4E\x4B\x41\x43\x56\x4B\x4D\x4C\x0D\x5A\x0F\x55\x55\x55\x0F\x44\x4D\x50\x4F\x0F\x57\x50\x4E\x47\x4C\x41\x4D\x46\x47\x46\x22
```

```
Content-Type: application/x-www-form-urlencoded_22
```

Decoded string

2. Copy the decoded string to the clipboard.
3. In CCC Confer, click the text icon, then paste the decode string into the correct table cell



TABLE_ATK_ACCEPT_LNG	
TABLE_ATK_CONTENT_TYPE	Content-Type: application/x-www-form-urlencoded_22
TABLE_ATK_SET_COOKIE	
TABLE_ATK_REFRESH_HDR	
TABLE_ATK_LOCATION_HDR	

Decode Activity on CCC Confer Whiteboard

TABLE_CNC_DOMAIN	
TABLE_CNC_PORT	
TABLE_SCAN_CB_DOMAIN	
TABLE_SCAN_CB_PORT	
TABLE_EXEC_SUCCESS	
TABLE_KILLER_SAFE	
TABLE_KILLER_PROC	
TABLE_KILLER_EXE	
TABLE_KILLER_DELETED	
TABLE_KILLER_FD	
TABLE_KILLER_ANIME	
TABLE_KILLER_STATUS	
TABLE_MEM_QBOT	
TABLE_MEM_QBOT2	
TABLE_MEM_QBOT3	
TABLE_MEM_UPX	
TABLE_MEM_ZOLLARD	
TABLE_MEM_REMAITEN	
TABLE_SCAN_SHELL	
TABLE_SCAN_ENABLE	
TABLE_SCAN_SYSTEM	
TABLE_SCAN_SH	
TABLE_SCAN_QUERY	
TABLE_SCAN_RESP	
TABLE_SCAN_NCORRECT	

Decode Activity on CCC Confer Whiteboard

TABLE_SCAN_PS	
TABLE_SCAN_KILL_9	
TABLE_ATK_VSE	
TABLE_ATK_RESOLVER	
TABLE_ATK_NSERV	
TABLE_ATK_KEEP_ALIVE	
TABLE_ATK_ACCEPT	
TABLE_ATK_ACCEPT_LNG	
TABLE_ATK_CONTENT_TYPE	
TABLE_ATK_SET_COOKIE	
TABLE_ATK_REFRESH_HDR	
TABLE_ATK_LOCATION_HDR	
TABLE_ATK_SET_COOKIE_HDR	
TABLE_ATK_CONTENT_LENGTH_HDR	
TABLE_ATK_TRANSFER_ENCODING_HDR	
TABLE_ATK_CHUNKED	
TABLE_ATK_KEEP_ALIVE_HDR	
TABLE_ATK_CONNECTION_HDR	
TABLE_ATK_DOSARREST	
TABLE_ATK_CLOUDFLARE_NGINX	
TABLE_HTTP_ONE	
TABLE_HTTP_TWO	
TABLE_HTTP_THREE	
TABLE_HTTP_FOUR	
TABLE_HTTP_FIVE	



EC-Council Mini CEH Assessment (2nd Attempt)

EC-Council

Browser: About - EC-Council
URL: <https://www.eccouncil.org/about/>

Navigation: HOME PROGRAMS FIND TRAINING EVENTS DEGREE OPTIONS RESOURCES ABOUT

Who We Are

International Council of E-Commerce Consultants, also known as EC-Council, is the world's largest cyber security technical certification body. We operate in 140 countries globally and we are the owner and developer of the world-famous Certified Ethical Hacker (CEH), Computer Hacking Forensics Investigator (C|HFI), Certified Security Analyst (ECSA), License Penetration Testing (Practical) programs, among others. We are proud to have trained and certified over 140,000 information security professionals globally that have influenced the cyber security mindset of countless organizations worldwide.

Our certification programs are recognized worldwide and have received endorsements from various government agencies including the US Federal Government via the Montgomery GI Bill, and the US Government National Security Agency (NSA) and the Committee on National Security Systems (CNSS) certifying EC-Council's Certified Ethical Hacking (CEH), Network Security Administrator (ENSA), Computer Hacking Forensics Investigator (CHFI), Disaster Recovery Professional (EDRP), Certified Security Analyst (E|CSA) and Licensed Penetration Tester(LPT) program for meeting the 4011, 4012, 4013A, 4014, 4015 and 4016 training standards for information security professionals and most recently EC-Council has received accreditation from the American National Standards Institute (ANSI).

"Our lives are dedicated to the mitigation and remediation of the cyber plaque that is menacing the world today "

Jay Bavis
President & CEO
EC-Council

EC-Council

Our Mission

The EC-Council mission is “to validate information security professionals who are equipped with the necessary skills and knowledge required in a specialized information security domain that will help them avert a cyber conflict, should the need ever arise.” EC-Council is committed to uphold the highest level of impartiality and objectivity in its practices, decision making, and authority in all matters related to certification.

EC-Council

The screenshot shows a web browser window with the URL <https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/ceh-assessment/>. The page features the EC-Council logo, a navigation menu with items like HOME, PROGRAMS, FIND TRAINING, EVENTS, DEGREE OPTIONS, RESOURCES, and ABOUT, and a 'GET TRAINING!' button. Below the navigation is a banner with the word 'Assessment' and an image of a laptop, tablet, and mouse. The main content area is titled 'CEH ASSESSMENT' and contains a question about penetration testing techniques. A progress indicator shows '4/50'.

Hackers are here. Where are you?

EC-Council GET TRAINING!

HOME PROGRAMS FIND TRAINING EVENTS DEGREE OPTIONS RESOURCES ABOUT

Assessment

CEH ASSESSMENT

4/50

Penetration testing is a method of actively evaluating the security of an information system or network by simulating an attack from a malicious source.

Which of the following technique is used to simulate an attack from someone who is unfamiliar with the system?

EC-Council Mini-Assessment

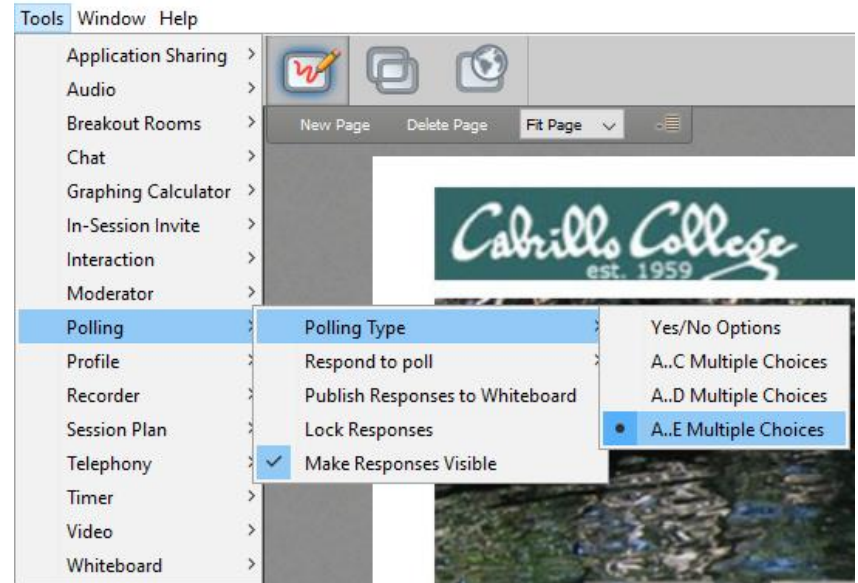
Acceptable. For a muggle. You scored 60%

That was last year. We scored 62% last time we took the test.

Our baseline to beat tonight is 62%

EC-Council Mini-Assessment Q1-10

<https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/ceh-assessment/>



Questions 1-10 (five minutes)

Housekeeping



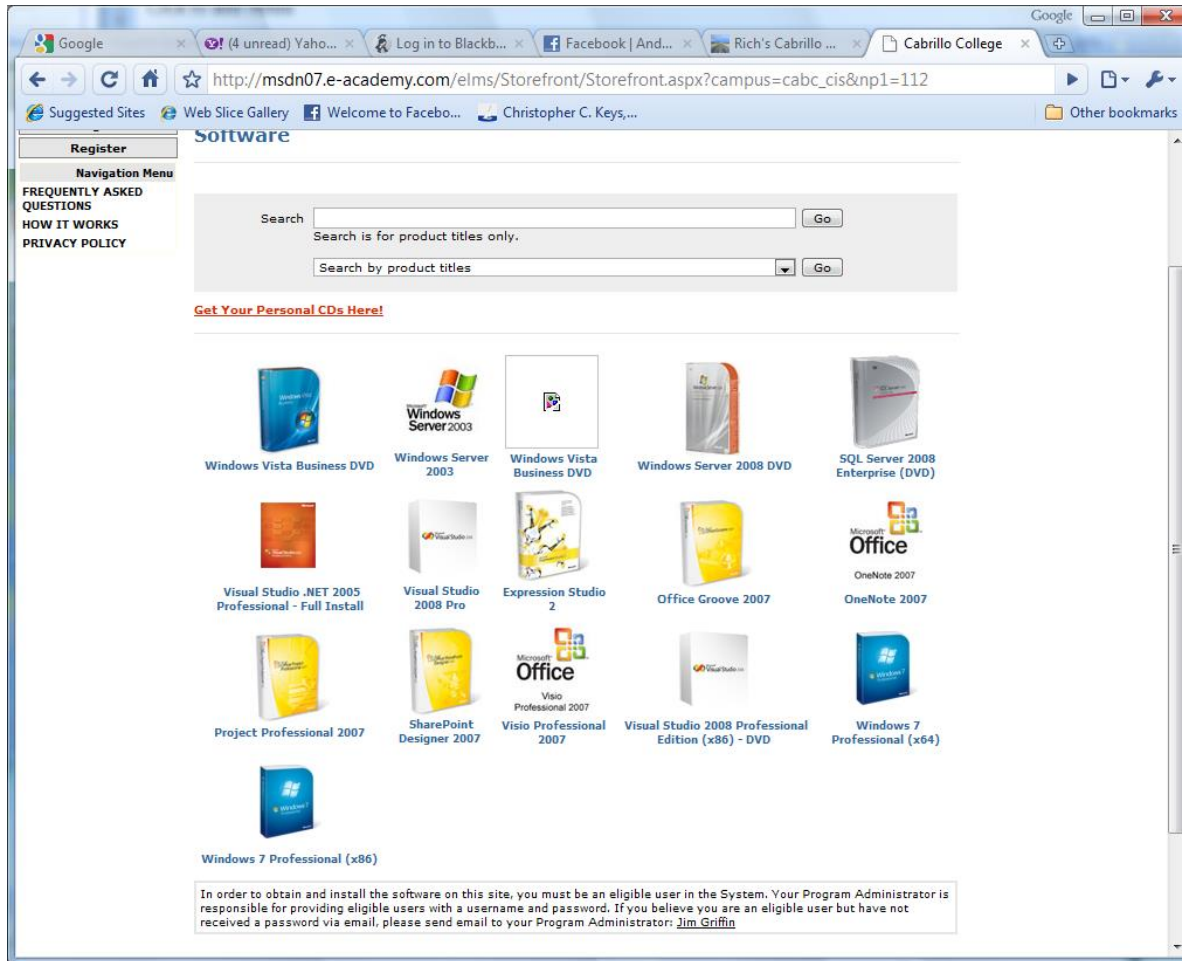
Housekeeping

1. Lab 7 due by 11:59PM (Opus-II time) tonight. PDFs are preferred.
2. Second test next week!
3. Practice test available after class.
4. See some extra credit labs (6 points each) starting to appear on the Calendar page of the website. Not due till the day of the Final Exam.

Test #2

1. Test #2 is **scheduled for our next class!**
2. Same format as before. The 60 minute test will take place during the last hour of class.
3. Alternatively the test can be taken online, outside of class, any time between 4:30 PM and 11:59PM.
4. Practice Test #2 will be available after class on Canvas. It will **no longer be available once the real test period begins.**
5. Work the Practice Test BEFORE the real test begins.

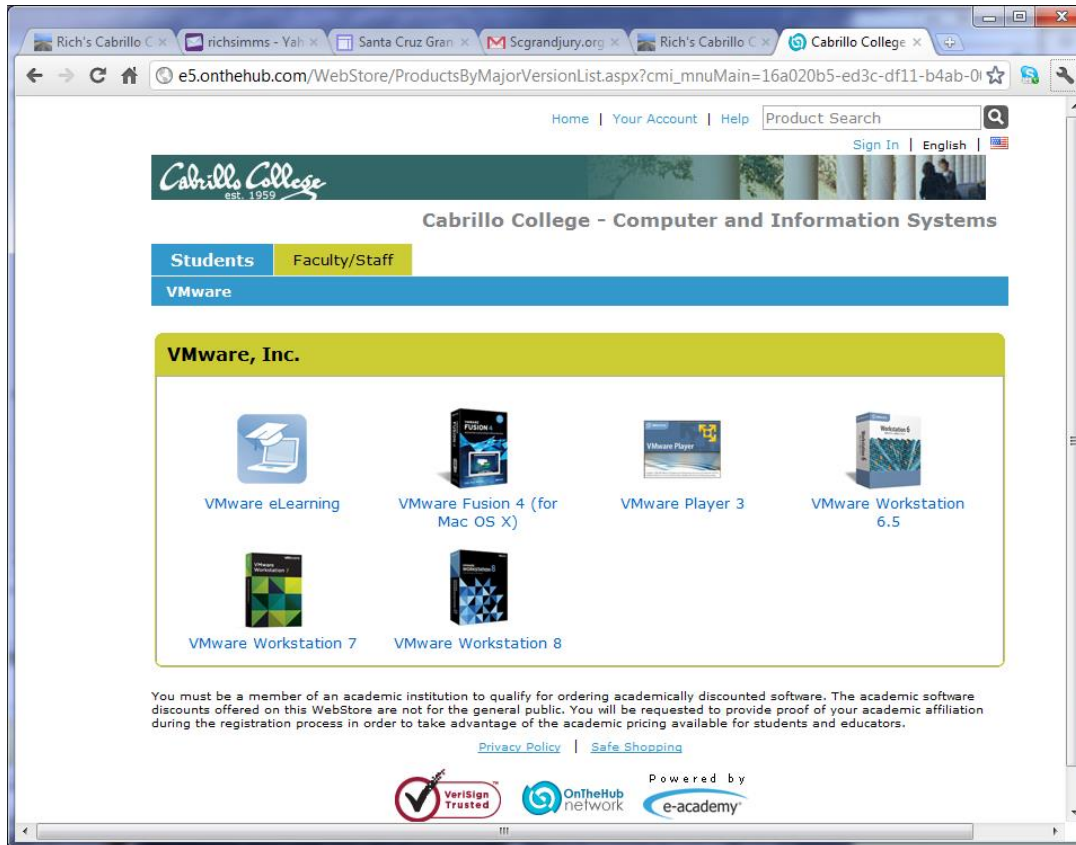
Microsoft Academic Webstore



- Microsoft software for students registered in a CIS or CS class at Cabrillo
- Available after registration is final (two weeks after first class)

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

VMware Academic Webstore



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

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

Heads up on Final Exam

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

Tue	12/12	Test #3 (the final exam)	5 posts Lab X1 Lab X2 Lab X3 Lab X4 Lab X5
		Time <ul style="list-style-type: none"> Tuesday 4:00PM - 6:50PM in Room 828 Materials <ul style="list-style-type: none"> Test (canvas) CCC Confer <ul style="list-style-type: none"> Enter virtual classroom Archives Confer or 3CMedia 	

*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)

FALL 2017 FINAL EXAMINATIONS SCHEDULE DECEMBER 11 TO DECEMBER 16

DAYTIME FINAL SCHEDULE

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

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

CIS 76 Introduction to Cybersecurity: Ethical Hacking

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

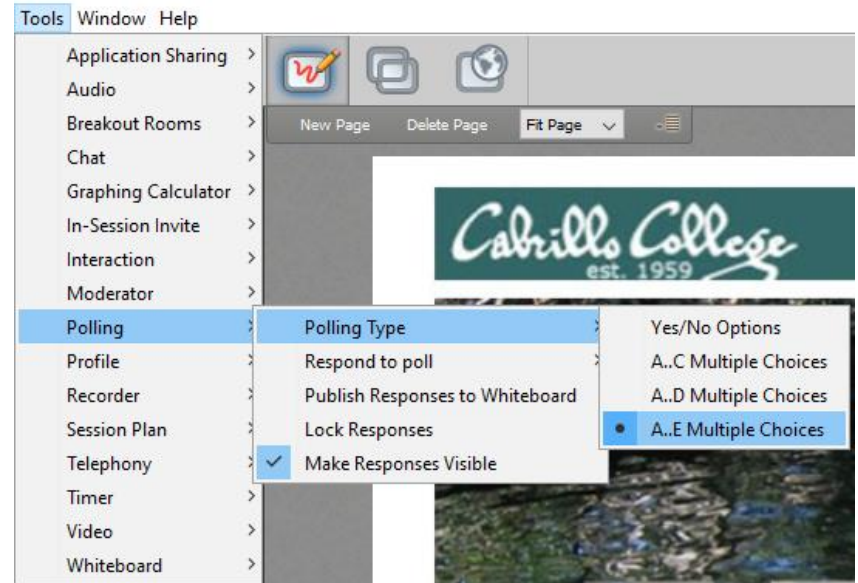
Section	Days	Times	Units	Instructor	Room
98163	T	5:30PM-8:35P	3.00	R.Simms	OL
Section 98163 is an ONLINE course. Meets weekly throughout the semester online by remote technology with an additional 50 min online lab per week. For details, see instructor's web page at go.cabrillo.edu/online .					
98164	T	5:30PM-8:35PM	3.00	R.Simms	828
&	Arr.	Arr.		R.Simms	OL
Section 98164 is a Hybrid ONLINE course. Meets weekly throughout the semester at the scheduled times with an additional 50 min online lab per week. For details, see instructor's web page at go.cabrillo.edu/online .					



EC-Council Mini CEH Assessment (2nd Attempt)

EC-Council Mini-Assessment Q11-20

<https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/ceh-assessment/>



Questions 11-20 (five minutes)

Domain 3



This workforce solution was funded by a grant awarded by the U.S. Department of Labor's Employment and Training Administration. The solution was created by the grantee and does not necessarily reflect the official position of the U.S. Department of Labor. The Department of Labor makes no guarantees, warranties, or assurances of any kind, express or implied, with respect to such information, including any information on linked sites and including, but not limited to, accuracy, continued availability or ownership.

Domain 3

Scanning Networks



Objectives

- Understand the differences between port scanning, network scanning and vulnerability scanning
- Describe the objectives of scanning
- Identify TCP communication flag types
- Identify types of port scans
- Identify scanning countermeasures

Scanning

Port Scanning

- Examine a range of IP addresses
- Identify services running

Network Scanning

- Identify active hosts on a network
- Examine the activity on a network like monitoring data flow and the functioning of network devices

Vulnerability Scanning

- Proactively identify security vulnerabilities of systems on a network to determine where a system can be exploited

Objectives of Scanning

Detect the live systems running on a network

Discover what ports are open

Discover the operating system of the target

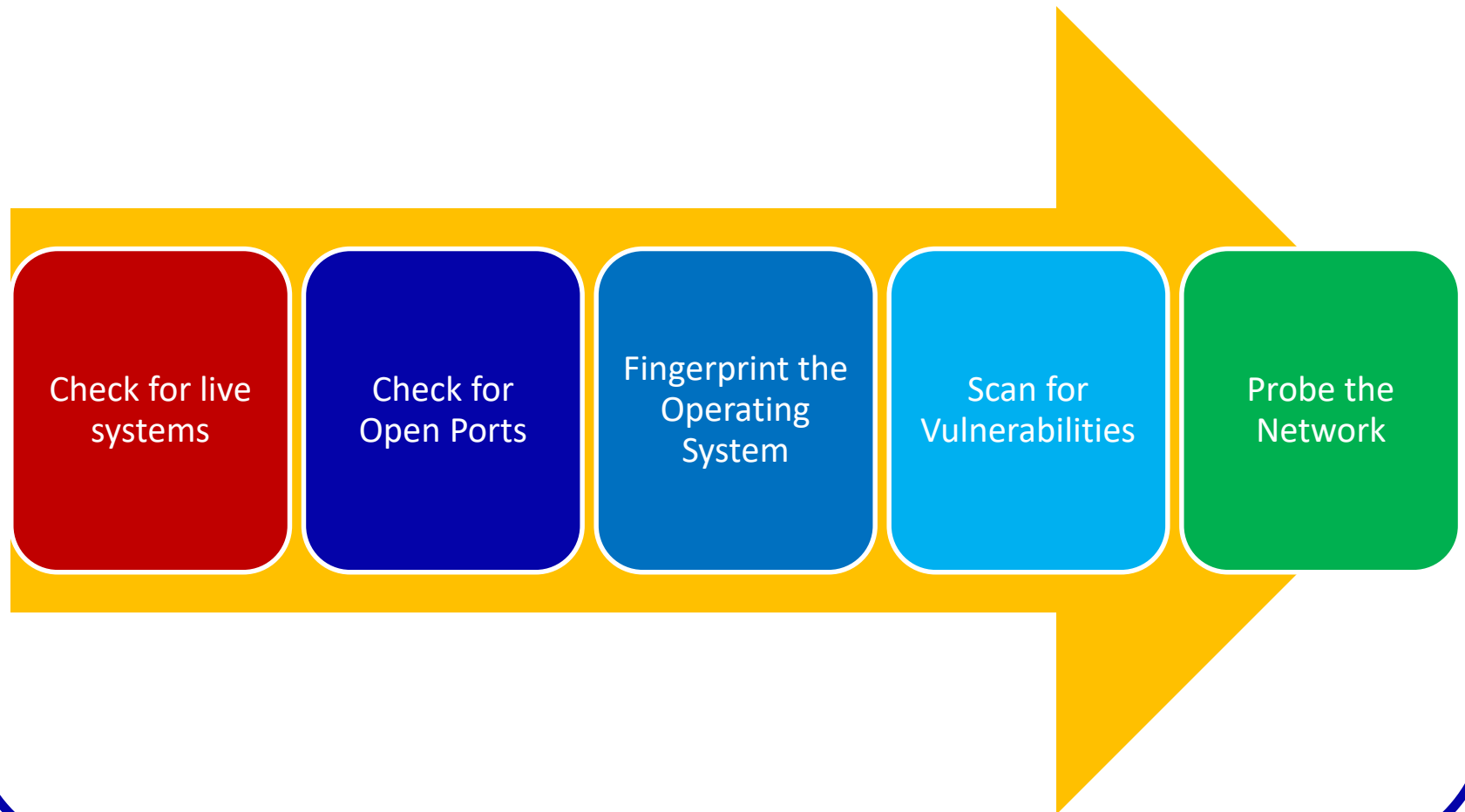
Discover the services running and/or listening

Discover IP addresses

Identify specific applications

Identify vulnerabilities in any of the systems in the network

Scanning Methodology

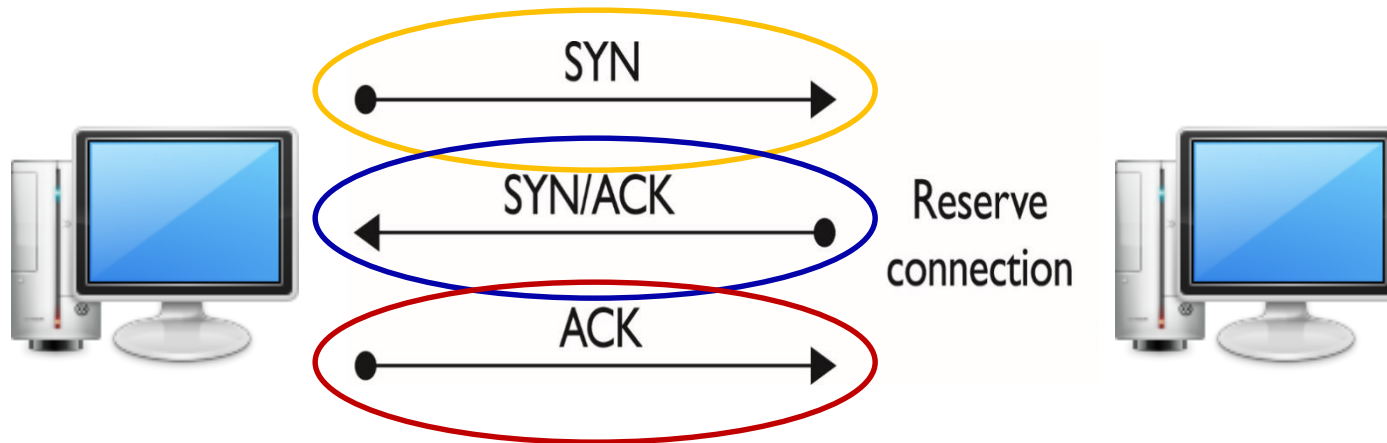


Three Way Handshake

System 1 sends SYN packet to System 2

System 2 responds with SYN/ACK packet

System 1 sends ACK packet to System 2
and communications can then proceed



TCP Flags



URG

- Identifies incoming data as urgent



ACK

- Acknowledges the successful receipt of packets



PUSH

- Ensures that the data is given priority and is processed at the sending or receiving end
- Used at the beginning and the end of a data transfer



RST

- Used when a segment arrives that is not intended for the current connection
- Mean that the remote host has reset the connection



SYN

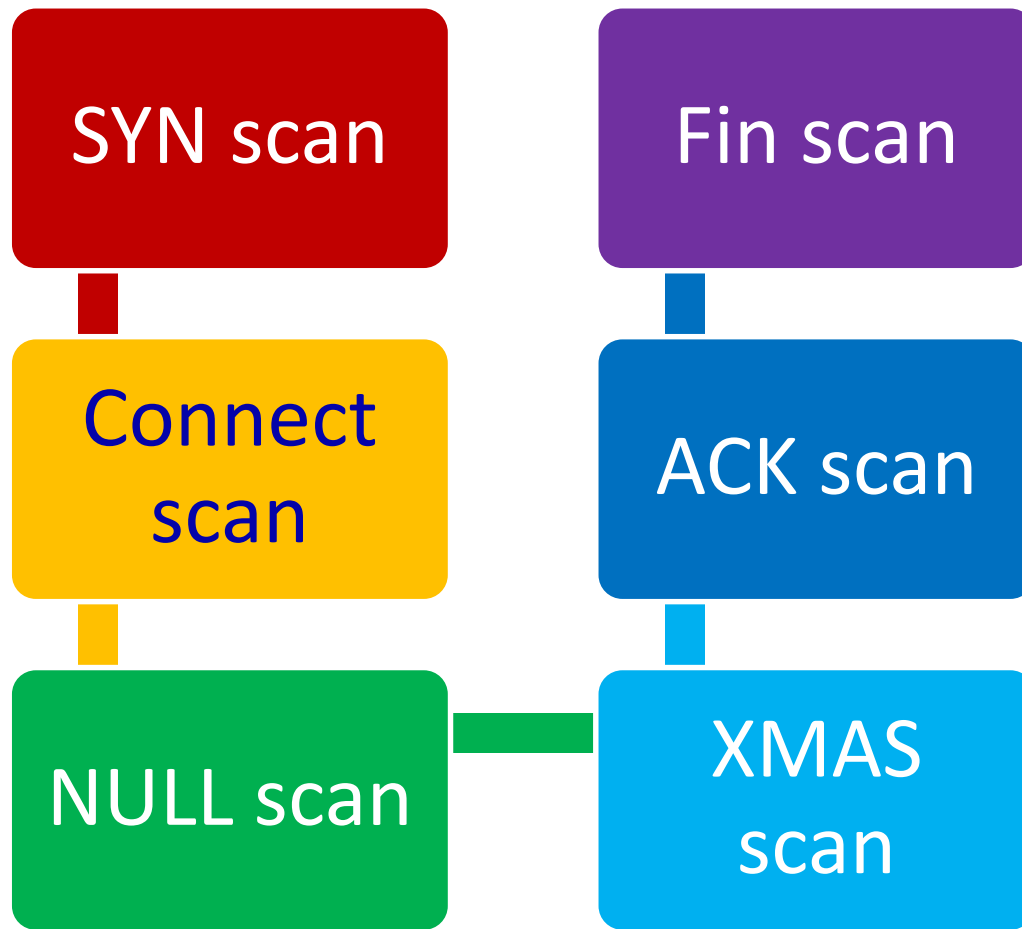
- Starts establishing the 3-way handshake between two hosts



FIN

- Tears down the connection created using the SYN flag

Types of Port Scans



Using Nmap

- Nmap without any switches will be successful against systems blocking ICMP
- A default Nmap scan will scan a large amount of ports, but not all
- When scanning a system on the Internet, you will not see a MAC address

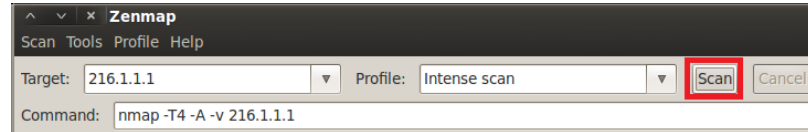
5 ports are open

```
root@bt:~# nmap 216.1.1.1
Starting Nmap 6.01 ( http://nmap.org ) at 2013-02-22 13:32 EST
Nmap scan report for 216.1.1.1
Host is up (0.00045s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
23/tcp    open  telnet
25/tcp    open  smtp
80/tcp    open  http
110/tcp   open  pop3
MAC Address: 00:0C:29:31:57:28 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 25.83 seconds
```

Zenmap

Zenmap is the GUI front end for nmap



	Port	Protocol	State	Service	Version
✓	21	tcp	open	ftp	Microsoft ftpd
✓	23	tcp	open	telnet	Microsoft Windows XP telnetd
✓	25	tcp	open	smtp	Microsoft ESMTP 6.0.3790.0
✓	80	tcp	open	http	Microsoft IIS httpd 6.0
✓	110	tcp	open	pop3	MS Exchange 2003 pop3d 6.5.

Scan Results

```
#Software: Microsoft Internet Information Services 6.0
#Version: 1.0
#Date: 2013-02-22 20:28:25
#Fields: date time s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip cs(User-Agent) sc-status sc
2013-02-22 20:28:25 192.168.1.100 HEAD /Default.htm - 80 - 216.6.1.100 - 200 0 0
2013-02-22 20:28:56 192.168.1.100 GET /default.htm - 80 - 216.6.1.100 - 200 0 0
2013-02-22 20:29:03 192.168.1.100 GET /default.htm - 80 - 216.6.1.100 Mozilla/5.0+(compatible;+Nmap+Scripting+
2013-02-22 20:29:03 192.168.1.100 GET /robots.txt - 80 - 216.6.1.100 Mozilla/5.0+(compatible;+Nmap+Scripting+
2013-02-22 20:29:03 192.168.1.100 GET /default.htm - 80 - 216.6.1.100 Mozilla/5.0+(compatible;+Nmap+Scripting+
2013-02-22 20:29:03 192.168.1.100 GET /favicon.ico - 80 - 216.6.1.100 Mozilla/5.0+(compatible;+Nmap+Scripting+
2013-02-22 20:29:03 192.168.1.100 OPTIONS / - 80 - 216.6.1.100 Mozilla/5.0+(compatible;+Nmap+Scripting+Engine;
2013-02-22 20:29:03 192.168.1.100 OPTIONS / - 80 - 216.6.1.100 Mozilla/5.0+(compatible;+Nmap+Scripting+Engine;
2013-02-22 20:29:03 192.168.1.100 OPTIONS / - 80 - 216.6.1.100 Mozilla/5.0+(compatible;+Nmap+Scripting+Engine;
2013-02-22 20:29:03 192.168.1.100 OPTIONS / - 80 - 216.6.1.100 Mozilla/5.0+(compatible;+Nmap+Scripting+Engine;
2013-02-22 20:29:03 192.168.1.100 OPTIONS / - 80 - 216.6.1.100 Mozilla/5.0+(compatible;+Nmap+Scripting+Engine;
2013-02-22 20:29:03 192.168.1.100 OPTIONS / - 80 - 216.6.1.100 Mozilla/5.0+(compatible;+Nmap+Scripting+Engine;
2013-02-22 20:29:03 192.168.1.100 OPTIONS / - 80 - 216.6.1.100 Mozilla/5.0+(compatible;+Nmap+Scripting+Engine;
2013-02-22 20:29:03 192.168.1.100 OPTIONS / - 80 - 216.6.1.100 Mozilla/5.0+(compatible;+Nmap+Scripting+Engine;
2013-02-22 20:29:03 192.168.1.100 OPTIONS / - 80 - 216.6.1.100 Mozilla/5.0+(compatible;+Nmap+Scripting+Engine;
2013-02-22 20:29:03 192.168.1.100 OPTIONS / - 80 - 216.6.1.100 Mozilla/5.0+(compatible;+Nmap+Scripting+Engine;
```

Web Log File

Crafting Packets

Fping

- Ping multiple IP addresses simultaneously
- Included in BackTrack
- www.fping.com

Hping

- Perform ping sweeps
- Bypass filtering devices
- www.hping.org/download

fping

man fping

```
cis76@eh-kali-05: ~
FPING (8)
NAME
    fping - send ICMP ECHO_REQUEST packets to network hosts

SYNOPSIS
    fping [ options ] [ systems... ] fping6 [ options ] [ systems... ]

DESCRIPTION
    fping is a program like ping which uses the Internet Control Message Protocol (ICMP)
    echo request to determine if a target host is responding. fping differs from ping in
    that you can specify any number of targets on the command line, or specify a file
    containing the lists of targets to ping. Instead of sending to one target until it
    times out or replies, fping will send out a ping packet and move on to the next target
    in a round-robin fashion. In the default mode, if a target replies, it is noted and
    removed from the list of targets to check; if a target does not respond within a
    certain time limit and/or retry limit it is designated as unreachable. fping also
    supports sending a specified number of pings to a target, or looping indefinitely (as
    in ping ). Unlike ping, fping is meant to be used in scripts, so its output is designed
    to be easy to parse.

    The binary named fping6 is the same as fping, except that it uses IPv6 addresses
    instead of IPv4.

Manual page fping(8) line 1 (press h for help or q to quit)
```

fping differs from ping in that it supports multiple targets

fping

fping -h

```

cis76@eh-kali-05: ~
cis76@eh-kali-05:~$ fping -h

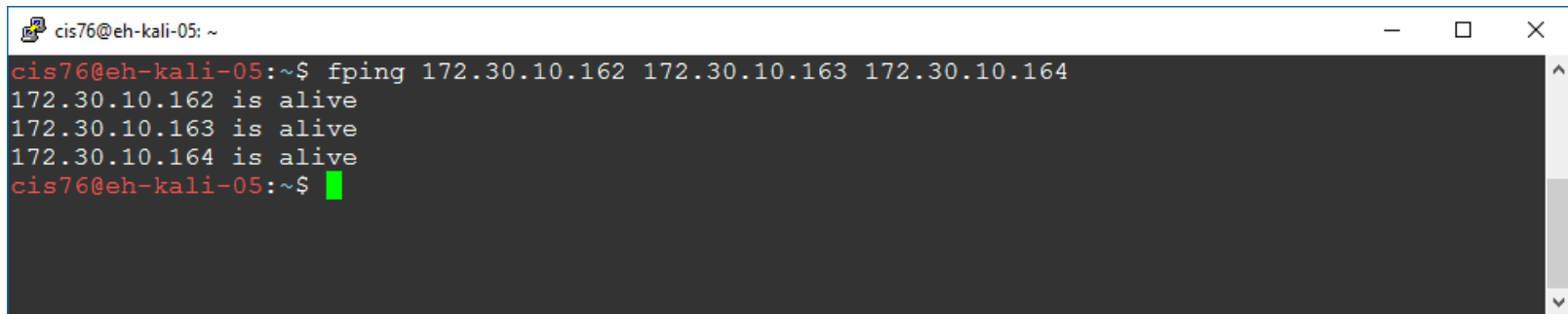
Usage: fping [options] [targets...]
-a          show targets that are alive
-A          show targets by address
-b n       amount of ping data to send, in bytes (default 56)
-B f       set exponential backoff factor to f
-c n       count of pings to send to each target (default 1)
-C n       same as -c, report results in verbose format
-D          print timestamp before each output line
-e          show elapsed time on return packets
-f file    read list of targets from a file ( - means stdin) (only if no -g specified)
-g         generate target list (only if no -f specified)
           (specify the start and end IP in the target list, or supply a IP netmask)
           (ex. fping -g 192.168.1.0 192.168.1.255 or fping -g 192.168.1.0/24)
-H n       Set the IP TTL value (Time To Live hops)
-i n       interval between sending ping packets (in millisec) (default 25)
-I if      bind to a particular interface
-l         loop sending pings forever
-m         ping multiple interfaces on target host
-n         show targets by name (-d is equivalent)
-O n       set the type of service (tos) flag on the ICMP packets
-p n       interval between ping packets to one target (in millisec)
           (in looping and counting modes, default 1000)
-q         quiet (don't show per-target/per-ping results)
-Q n       same as -q, but show summary every n seconds
-r n       number of retries (default 3)
-R         random packet data (to foil link data compression)
-s         print final stats
-S addr    set source address
-t n       individual target initial timeout (in millisec) (default 500)
-T n       ignored (for compatibility with fping 2.4)
-u         show targets that are unreachable
-v         show version
targets   list of targets to check (if no -f specified)

cis76@eh-kali-05:~$ █

```

fping

fping 172.30.10.162 172.30.10.163 172.30.10.164

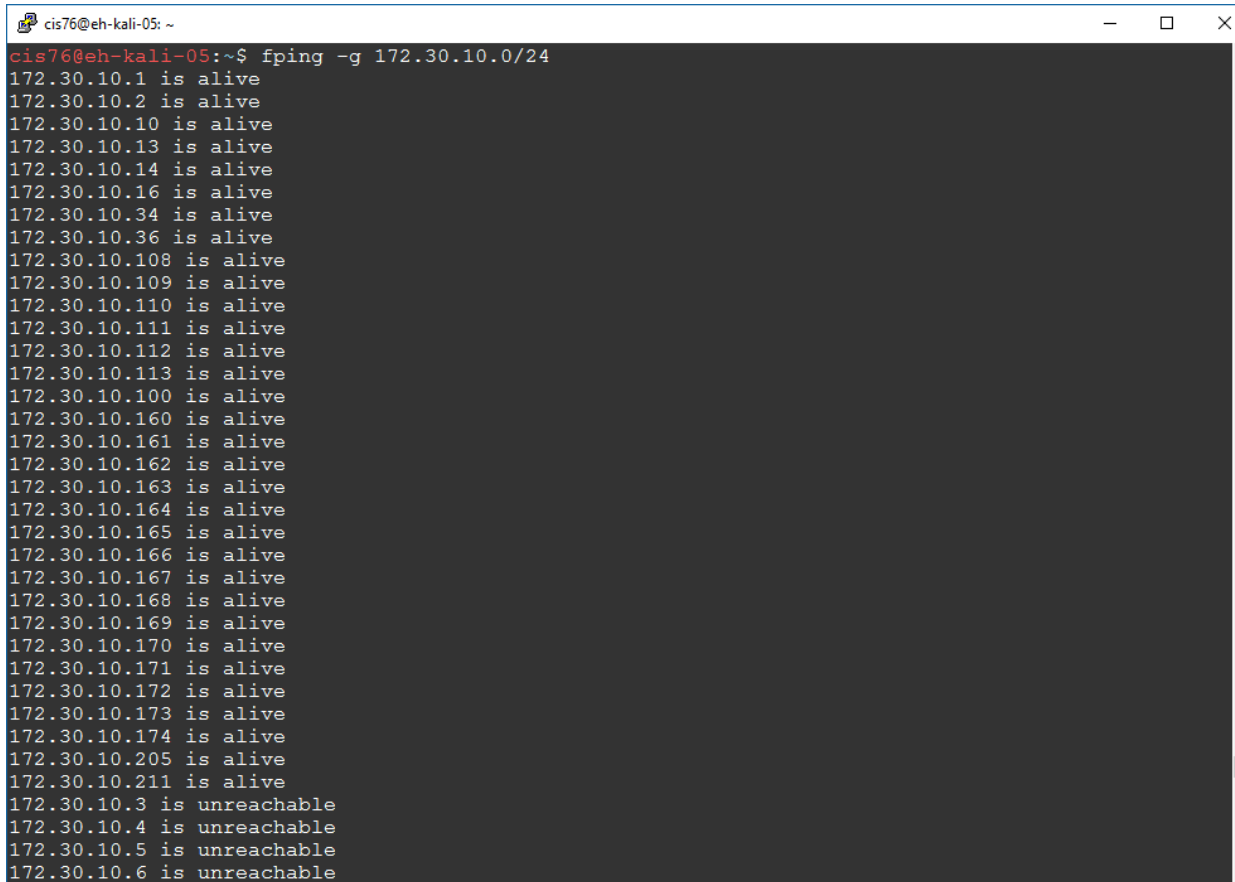


```
cis76@eh-kali-05: ~  
cis76@eh-kali-05:~$ fping 172.30.10.162 172.30.10.163 172.30.10.164  
172.30.10.162 is alive  
172.30.10.163 is alive  
172.30.10.164 is alive  
cis76@eh-kali-05:~$ █
```

Multiple targets

fping

fping -g 172.30.10.0/24



```
cis76@eh-kali-05: ~  
cis76@eh-kali-05:~$ fping -g 172.30.10.0/24  
172.30.10.1 is alive  
172.30.10.2 is alive  
172.30.10.10 is alive  
172.30.10.13 is alive  
172.30.10.14 is alive  
172.30.10.16 is alive  
172.30.10.34 is alive  
172.30.10.36 is alive  
172.30.10.108 is alive  
172.30.10.109 is alive  
172.30.10.110 is alive  
172.30.10.111 is alive  
172.30.10.112 is alive  
172.30.10.113 is alive  
172.30.10.100 is alive  
172.30.10.160 is alive  
172.30.10.161 is alive  
172.30.10.162 is alive  
172.30.10.163 is alive  
172.30.10.164 is alive  
172.30.10.165 is alive  
172.30.10.166 is alive  
172.30.10.167 is alive  
172.30.10.168 is alive  
172.30.10.169 is alive  
172.30.10.170 is alive  
172.30.10.171 is alive  
172.30.10.172 is alive  
172.30.10.173 is alive  
172.30.10.174 is alive  
172.30.10.205 is alive  
172.30.10.211 is alive  
172.30.10.3 is unreachable  
172.30.10.4 is unreachable  
172.30.10.5 is unreachable  
172.30.10.6 is unreachable
```

-g option to generate targets

fping

fping < hostlist

```
cis76@eh-kali-05: ~  
cis76@eh-kali-05:~$ cat hostlist  
172.30.10.162  
172.30.10.163  
172.30.10.164  
172.30.10.165  
172.30.10.166  
172.30.10.167  
172.30.10.168  
172.30.10.169  
172.30.10.170  
172.30.10.171  
172.30.10.172  
cis76@eh-kali-05:~$ fping < hostlist  
172.30.10.162 is alive  
172.30.10.163 is alive  
172.30.10.164 is alive  
172.30.10.165 is alive  
172.30.10.166 is alive  
172.30.10.167 is alive  
172.30.10.168 is alive  
172.30.10.169 is alive  
172.30.10.170 is alive  
172.30.10.171 is alive  
172.30.10.172 is alive  
cis76@eh-kali-05:~$
```

fping also reads from stdin

Activity

Try this command from your EH-Kali VM:

```
echo 172.30.10.{1,2,10,13,162,164} | fmt -1 | fping
```

How many of those devices are up? Put your answer in the chat window.

Scanning Countermeasures

Firewall should detect probes

Network intrusion detection systems should identify the OS detection methods used by various tools

Close any unneeded ports

Deploy tools to detect port scans



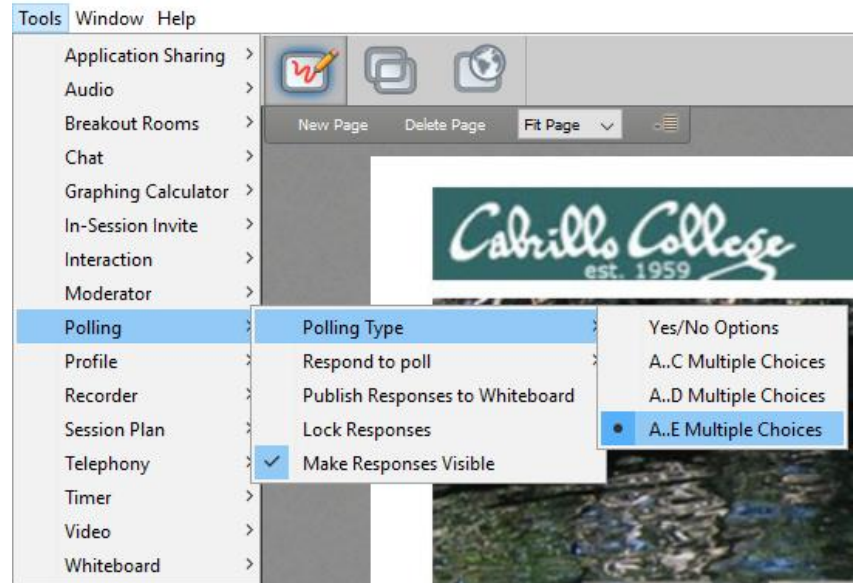
This workforce solution was funded by a grant awarded by the U.S. Department of Labor's Employment and Training Administration. The solution was created by the grantee and does not necessarily reflect the official position of the U.S. Department of Labor. The Department of Labor makes no guarantees, warranties, or assurances of any kind, express or implied, with respect to such information, including any information on linked sites and including, but not limited to, accuracy, continued availability or ownership.



EC-Council Mini CEH Assessment (2nd Attempt)

EC-Council Mini-Assessment Q31-40

<https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/ceh-assessment/>



Questions 31-40 (five minutes)

Domain 4



This workforce solution was funded by a grant awarded by the U.S. Department of Labor's Employment and Training Administration. The solution was created by the grantee and does not necessarily reflect the official position of the U.S. Department of Labor. The Department of Labor makes no guarantees, warranties, or assurances of any kind, express or implied, with respect to such information, including any information on linked sites and including, but not limited to, accuracy, continued availability or ownership.

Domain 4

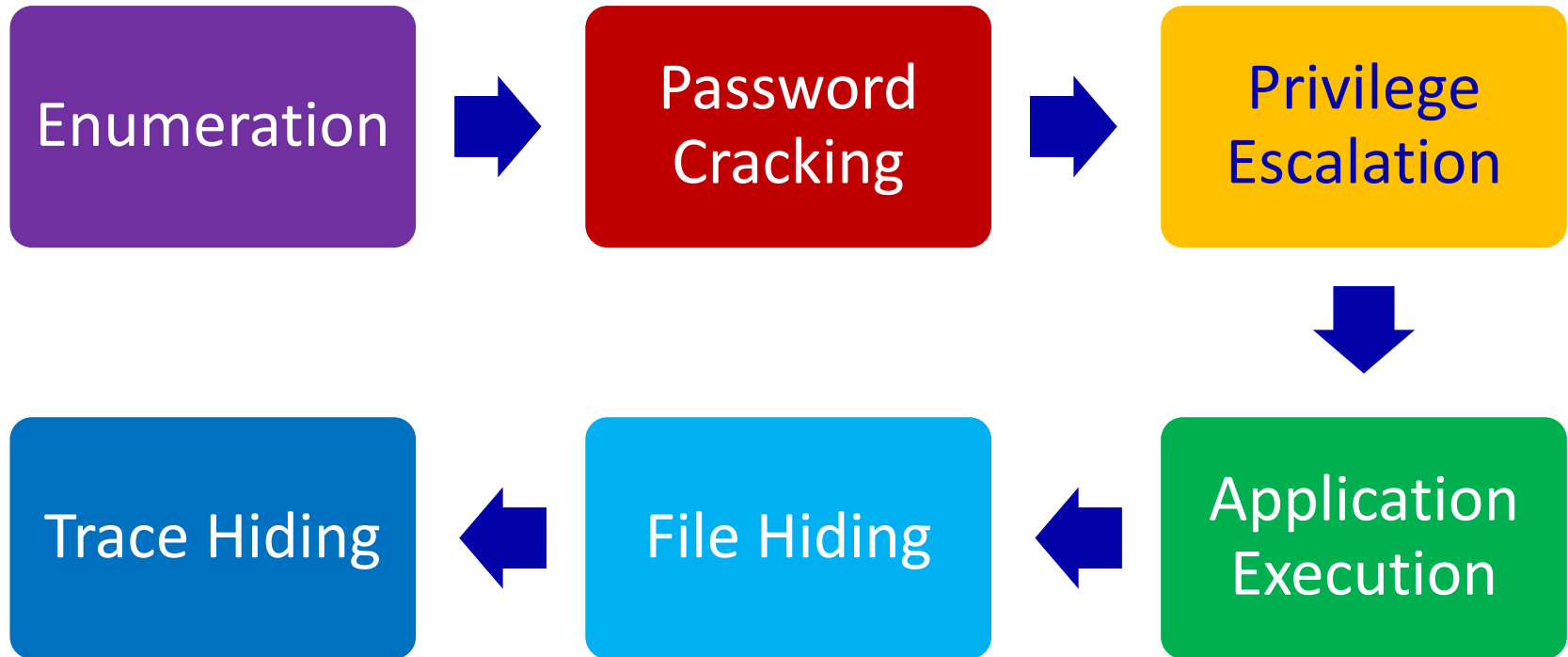
Enumeration



Objectives

- Understand enumeration techniques
- Describe null sessions
- Describe SNMP enumeration
- Identify countermeasures

Steps to Compromise a System



Enumeration

Network resources
and shares

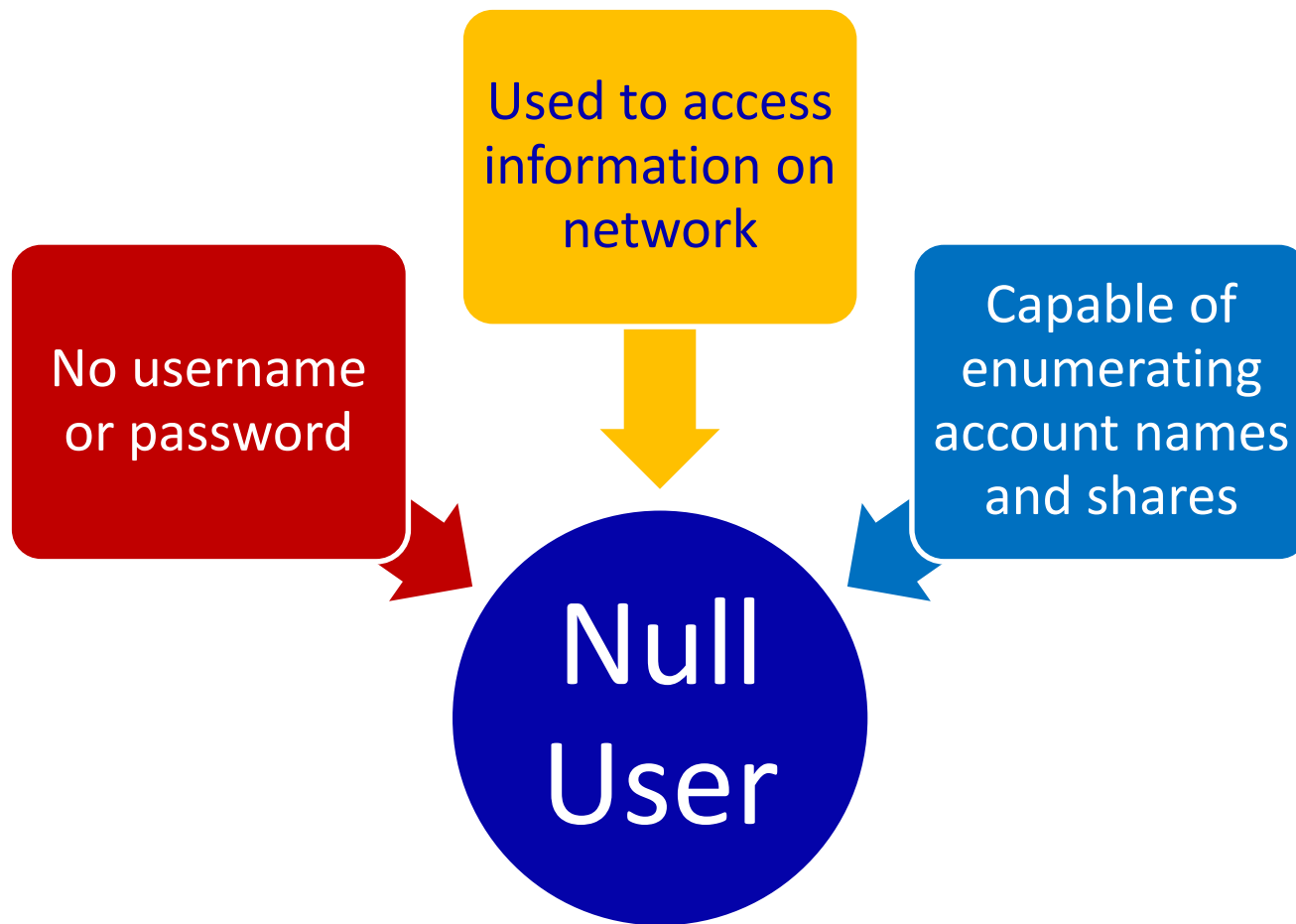
Users and groups

Actively connect
to obtain
information

Auditing settings

Application banners

Null Session Enumeration



Null Sessions

Enumeration Techniques

- Exploit IPC\$ share
- Exploit hard drive
- Enumerate user account

Countermeasures

- Filter ports
- Disable SMB service
- Inspect HKLM
- Configure security policy
- Restrict remote access

```
net use \\192.168.1.101\ipc$ "" /user:""
```

NetBIOS Basics

Windows programming interface that allows computers to communicate across a LAN

Used to share files and printers

Uses UDP ports 137 (Server service), 138 (Datagram service) and TCP port 139 (Session service)

NetBIOS names are the computer names assigned to a system and have a 15-character limit

NetBIOS name must be unique on a network

Command Line Tools

netstat

- Displays network connections, routing tables and network protocol statistics

nbstat

- Diagnostic tool for NetBIOS
- Used to troubleshoot NetBIOS name resolution problems

SNMP Enumeration

Agents deployed onto managed systems and Network Management Stations

Process information collected

A Master Information Base (MIB) is configured with the resources that need to be monitored

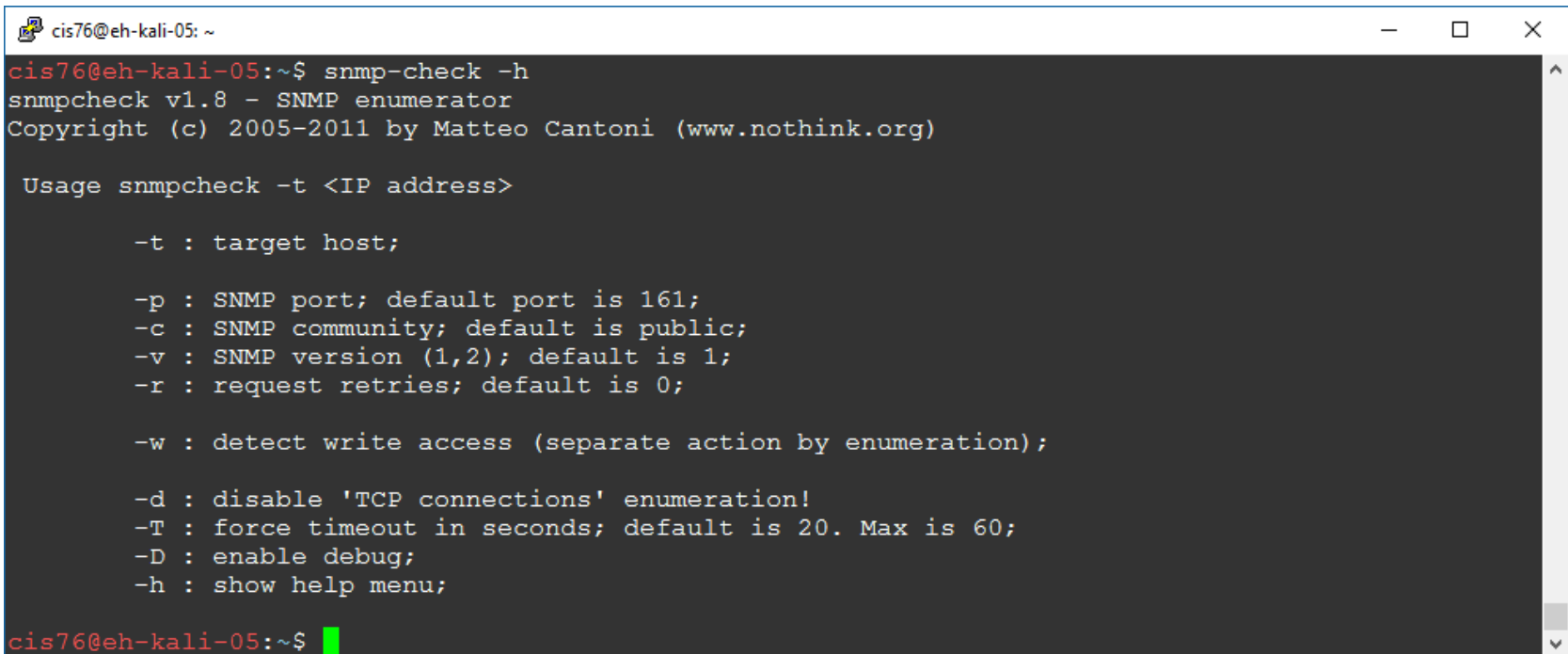
Default community string are the characters PUBLIC

Attacker looks for target host with SNMP enabled and a default community string

Built-in SNMP objects will be visible for enumeration

snmp-check

snmp-check -h



```
cis76@eh-kali-05: ~  
cis76@eh-kali-05:~$ snmp-check -h  
snmpcheck v1.8 - SNMP enumerator  
Copyright (c) 2005-2011 by Matteo Cantoni (www.nothink.org)  
  
Usage snmpcheck -t <IP address>  
  
-t : target host;  
  
-p : SNMP port; default port is 161;  
-c : SNMP community; default is public;  
-v : SNMP version (1,2); default is 1;  
-r : request retries; default is 0;  
  
-w : detect write access (separate action by enumeration);  
  
-d : disable 'TCP connections' enumeration!  
-T : force timeout in seconds; default is 20. Max is 60;  
-D : enable debug;  
-h : show help menu;  
  
cis76@eh-kali-05:~$
```

Used to browse SNMP MIBs

Activity

Try this command from your EH-Kali VM:

```
snmp-check 172.30.10.162
```

Check the "Software components" section of the output.

Is VMware Tools installed?

Write your answer in the chat window.

SNMP Enumeration Countermeasures

Remove the SNMP agent or turn off the SNMP service

Implement the group policy security option

Restrict access to null session shares

Change the community string

Discovering Hosts with Windows Command Line Tools

Here is a list of the commands used during Task 2 to enumerate Windows hosts.

Command	Result
<code>net view</code>	Enumerates the machines within the same workgroup
<code>net view /domain</code>	Enumerates all workgroups and domains
<code>net view /domain:workgroup</code>	Enumerates the machines in the workgroup <u>WORKGROUP</u>
<code>net view /domain:XYZcompany</code>	Enumerates the machines in the workgroup <u>XYZcompany</u>

Discovering Hosts with Metasploit

```
msf auxiliary(arp_sweep) > run

[*] 192.168.1.1 appears to be up (VMware, Inc.).
[*] 192.168.1.100 appears to be up (VMware, Inc.).
[*] 192.168.1.175 appears to be up (VMware, Inc.).
[*] 192.168.1.200 appears to be up (VMware, Inc.).
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
```

```
msf auxiliary(nbname) > run

[*] Sending NetBIOS status requests to 192.168.1.0->192.168.1.255 (256 hosts)
[*] 192.168.1.1 [FW] OS:Windows Names:(FW, WORKGROUP, [??] MSBROWSE [?]) Addresses:(216.1.1.1, 192.168.1.1)
[*] 192.168.1.100 [SERVER] OS:Windows Names:(SERVER, XYZCOMPANY, [??] MSBROWSE [?]) Addresses:(192.168.1.100)
[*] 192.168.1.175 [WINXP] OS:Windows Names:(WINXP, WORKGROUP) Addresses:(192.168.1.175) Mac:00:0c:29:e0:09
[*] 192.168.1.200 [WINFILE] OS:Windows Names:(WINFILE, WORKGROUP) Addresses:(192.168.1.200) Mac:00:0c:29:c4
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
```

Activity

Try these commands on your EH-Kali VM:

```
msfconsole  
msf > use auxiliary/scanner/discovery/arp_sweep  
msf auxiliary(arp_sweep) > show options  
msf auxiliary(arp_sweep) > set RHOSTS 10.76.xx.1-250  
msf auxiliary(arp_sweep) > run
```

 Your pod number


How many VMs in your pod are up and running?

Write your answer in the chat window.

Activity

Try these commands on your EH-Kali VM:

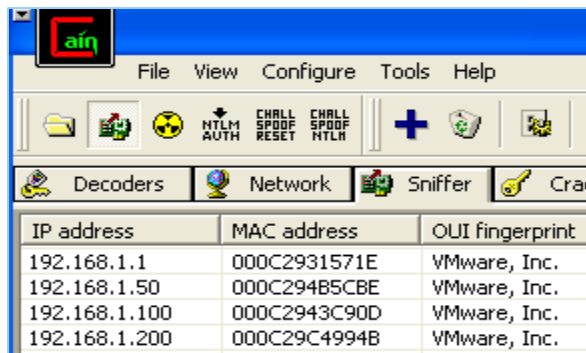
```
msfconsole  
msf > use auxiliary/scanner/netbios/nbname  
msf auxiliary(arp_sweep) > show options  
msf auxiliary(arp_sweep) > set RHOSTS 10.76.xx.1-250  
msf auxiliary(arp_sweep) > run
```

 *Your pod number*

How many NetBIOS supporting VMs in your pod are up and running?

Write your answer in the chat window.

Using Cain



IP address	MAC address	OUI fingerprint	Host name
192.168.1.1	000C2931571E	VMware, Inc.	FW
192.168.1.50	000C294B5CBE	VMware, Inc.	
192.168.1.100	000C2943C90D	VMware, Inc.	server.xyzcompany.com
192.168.1.200	000C29C4994B	VMware, Inc.	WINFILE



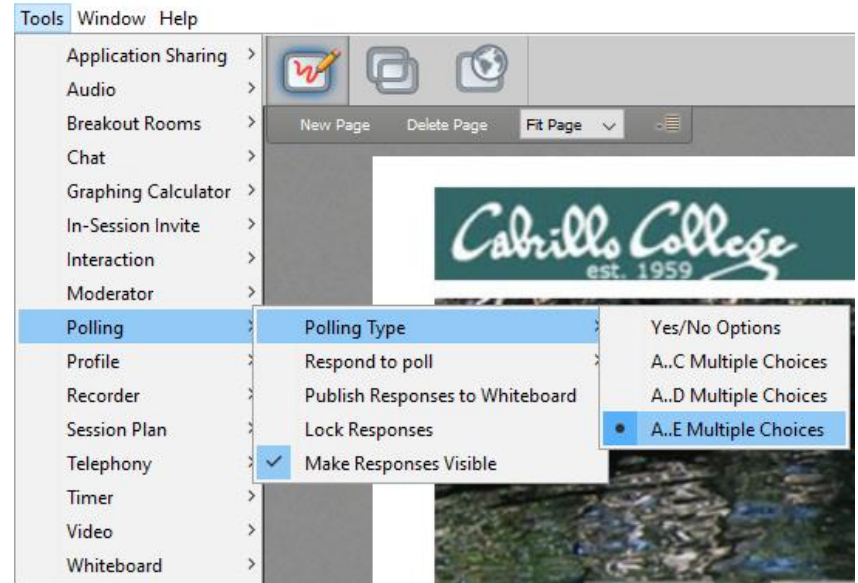
This workforce solution was funded by a grant awarded by the U.S. Department of Labor's Employment and Training Administration. The solution was created by the grantee and does not necessarily reflect the official position of the U.S. Department of Labor. The Department of Labor makes no guarantees, warranties, or assurances of any kind, express or implied, with respect to such information, including any information on linked sites and including, but not limited to, accuracy, continued availability or ownership.



EC-Council Mini CEH Assessment (2nd Attempt)

EC-Council Mini-Assessment Q41-50

<https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/ceh-assessment/>



Questions 41-50 (five minutes)

Domain 10



This workforce solution was funded by a grant awarded by the U.S. Department of Labor's Employment and Training Administration. The solution was created by the grantee and does not necessarily reflect the official position of the U.S. Department of Labor. The Department of Labor makes no guarantees, warranties, or assurances of any kind, express or implied, with respect to such information, including any information on linked sites and including, but not limited to, accuracy, continued availability or ownership.

Domain 10

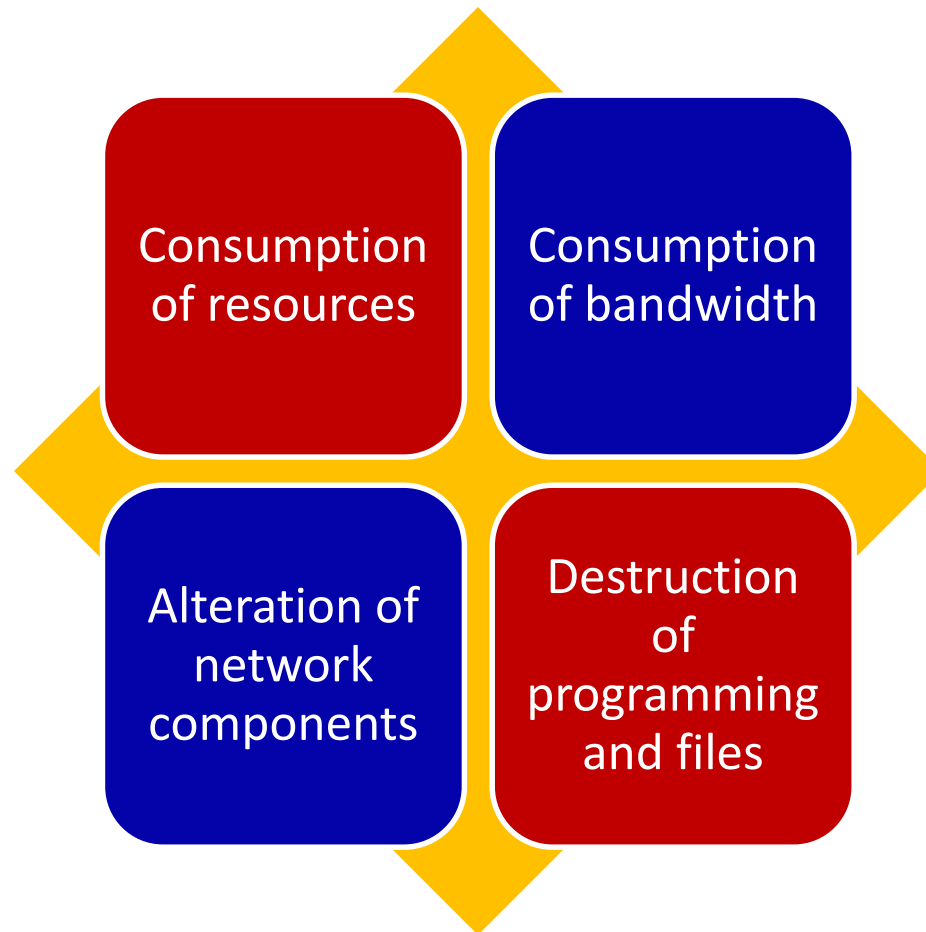
Denial of Service



Objectives

- Define a denial-of-service (DoS) attack
- Analyze symptoms of a DoS attack
- Explain DoS attack techniques
- Describe detection techniques
- Identify countermeasure strategies

Denial-of-Service Attack



Types of Attacks

Smurf

- Attacker sends a lot of ICMP traffic to IP broadcast addresses with a spoofed source IP of the victim

Buffer overflow attack

- Send excessive data to an application to bring down the application and crash the system

Ping of death

- Send an ICMP packet that is larger than the allowed 65,536 bytes

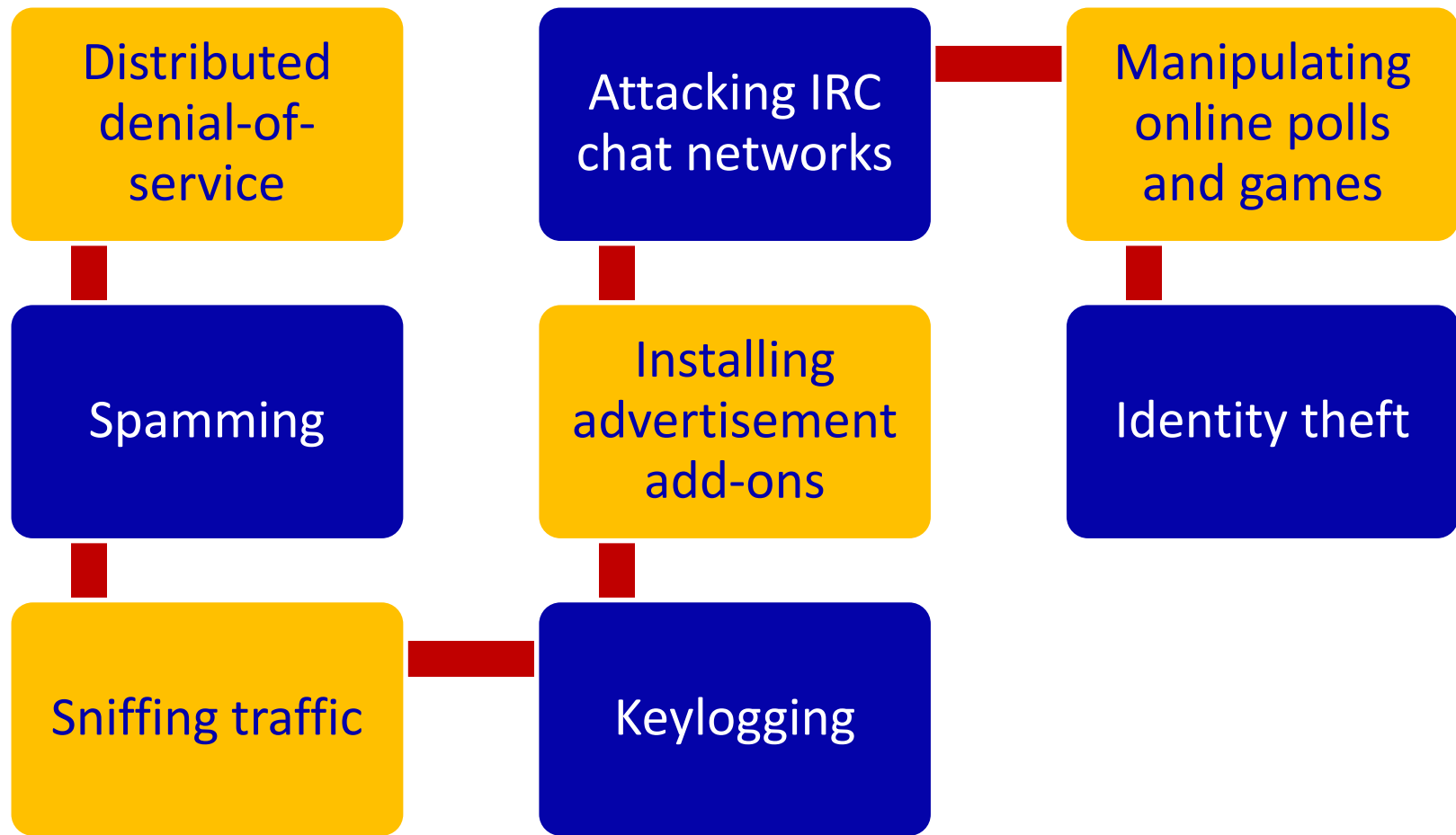
Teardrop

- Manipulate the value of fragments so that they overlap causing the receiving system an issue with reassembling the packet causing it to crash, hang, or reboot

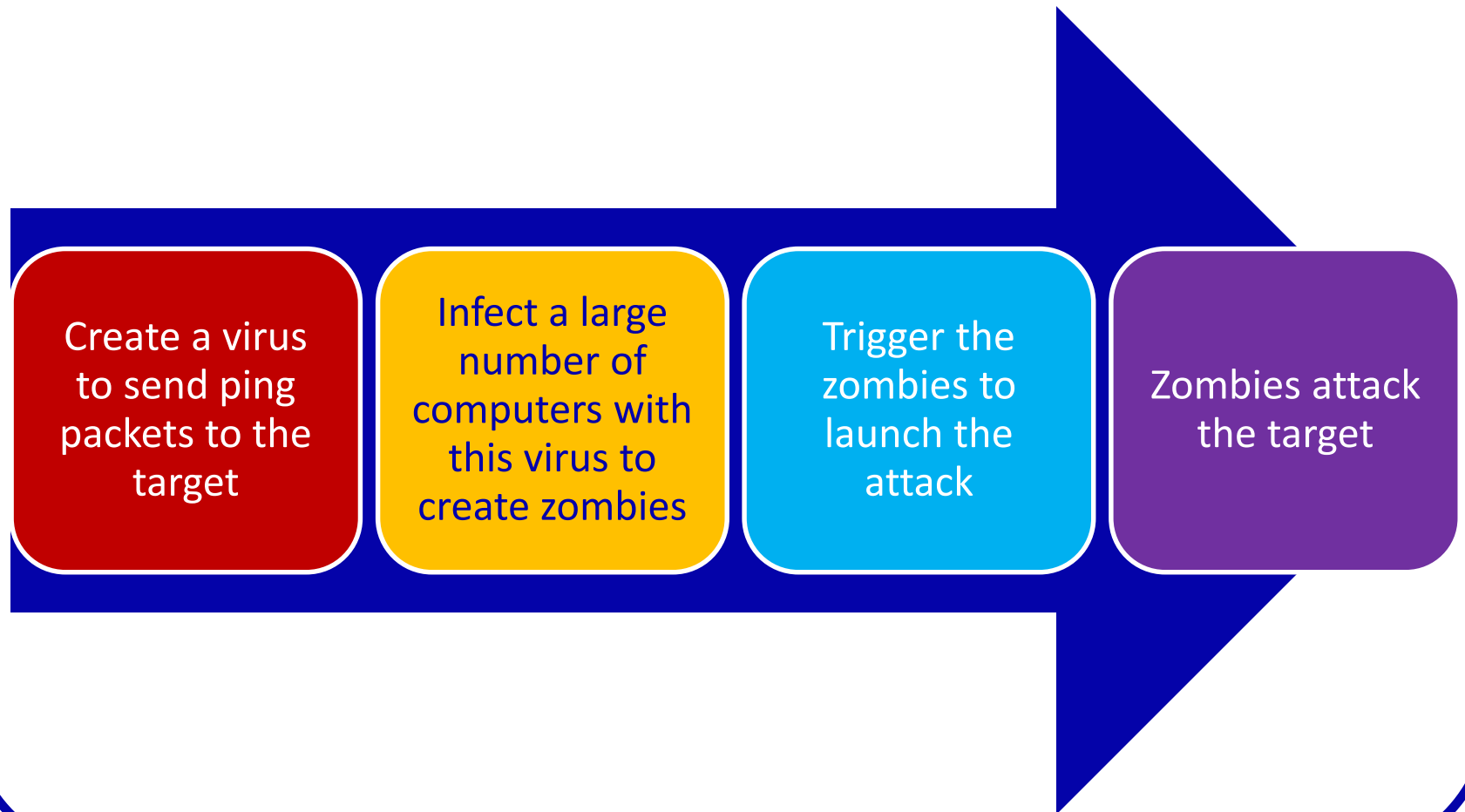
SYN Flood

- Exploits the three-way handshake by never responding to the server's response

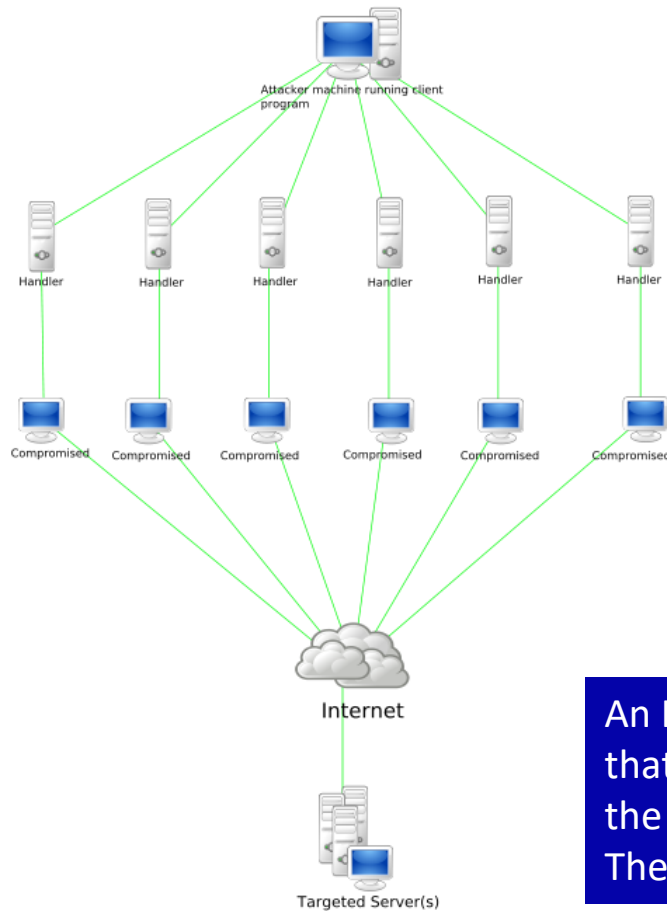
Botnets



Conducting a DDoS Attack



Distributed Denial of Service Attack (DDoS)

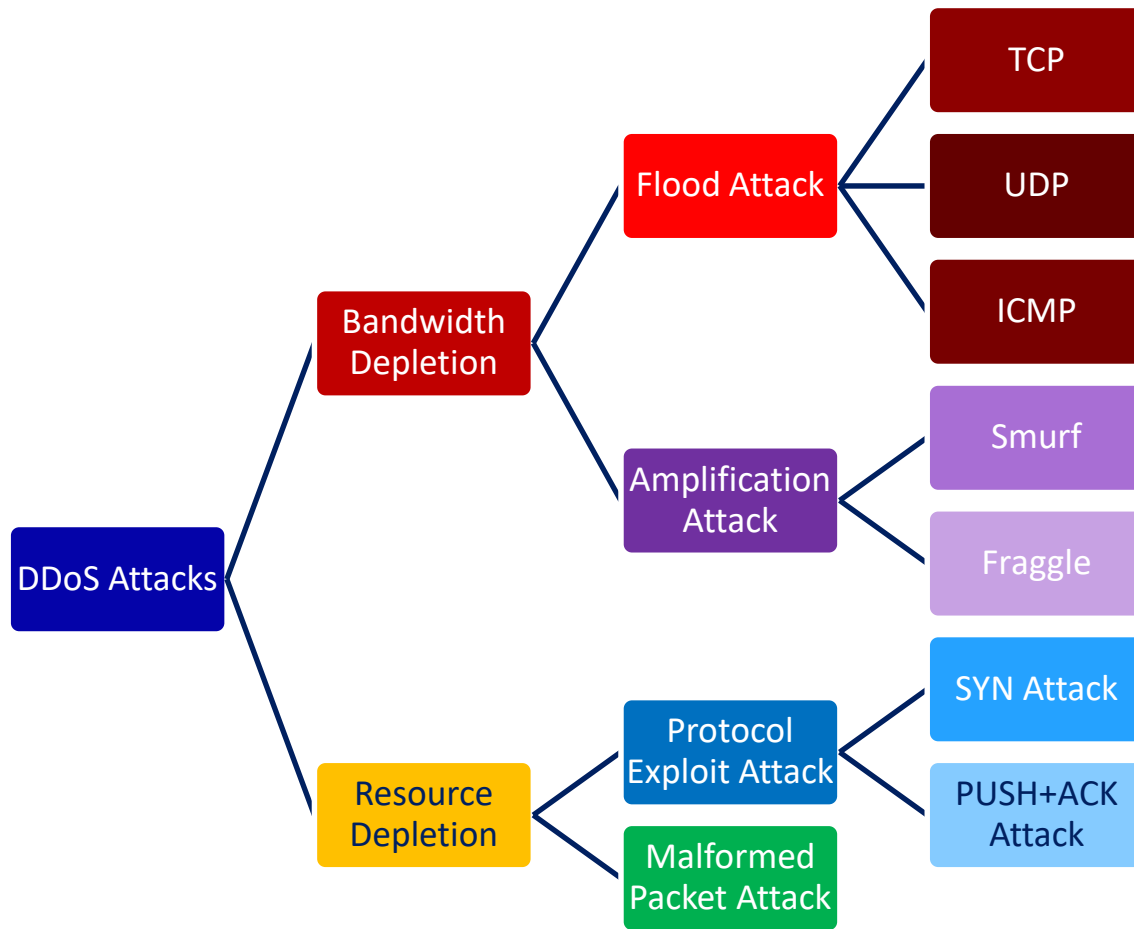


Handler software is placed on a compromised router or network server

Agent software is placed in compromised systems that will carry out the attack

An IRC-based DDoS attack is similar except that it is installed on a network server and uses the IRC communication channel to connect the attacker to the agents

Attack Classes



Amplification Attacks

Smurf Attack

A Smurf Attack (named so as it fits the stereotype of Smurfs with proper visualization) is a denial-of-service (DoS) attack that involves **sending ICMP echo requests (ping) traffic to the broadcast address** of routers and other network devices in large computer networks with a spoofed **source address (the address of the desired DoS target)**. Since the device receiving the original ICMP echo request broadcasts it to every other device it's connected to, each one of these devices sends out an echo reply to the spoofed source address (the DoS target). This will generate a high rate of ICMP traffic and could cause DoS or instability for the target network.

If the original request (to a device in a large network) is broadcast to such a vast number of machines, the resulting attack can be highly effective.

After 1999, however, most routers do not forward packets sent to their broadcast addresses by default, this makes the likelihood of a successful large-scale Smurf Attack fairly low.

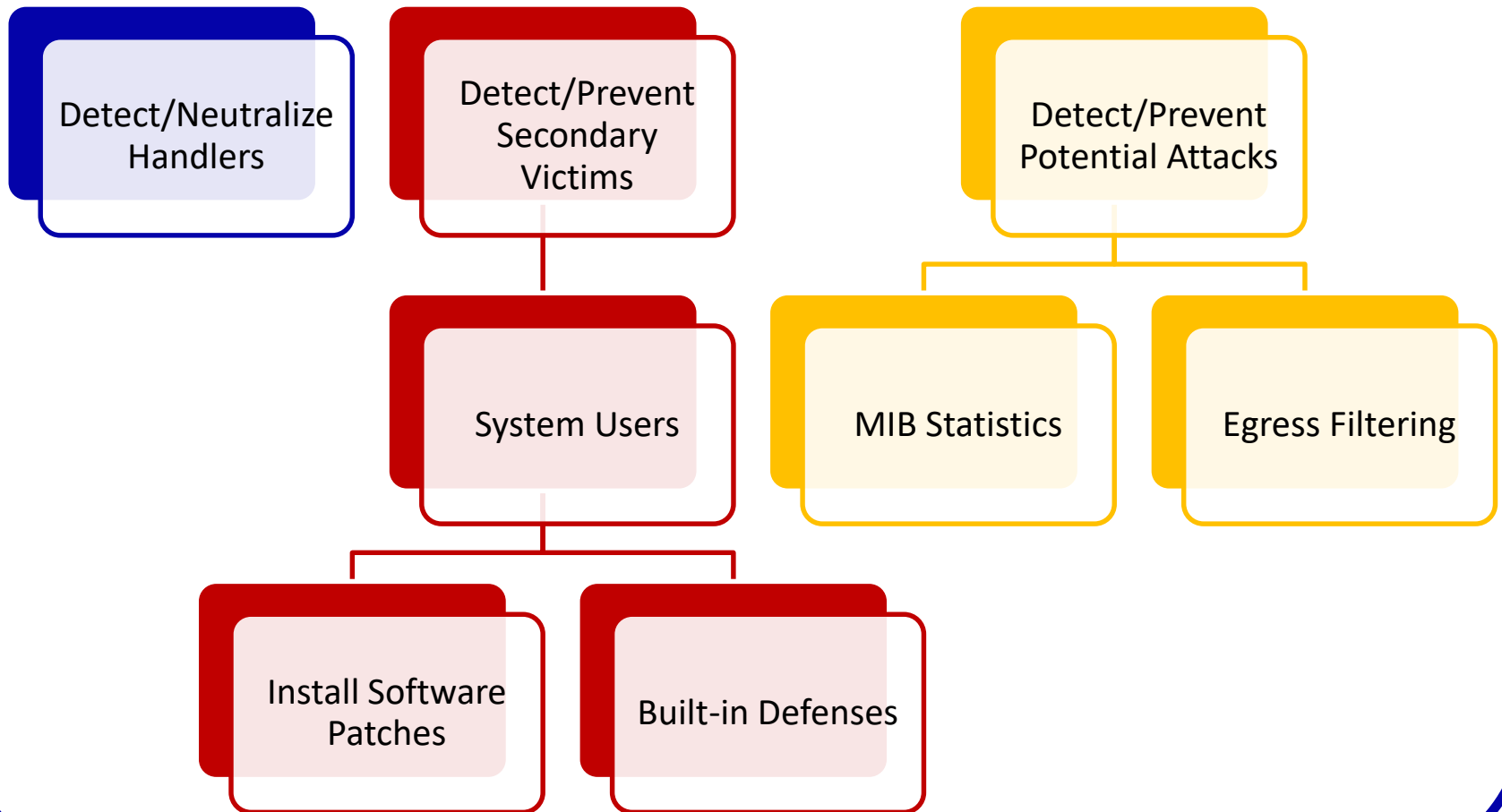
Amplification Attacks

Fraggle Attack

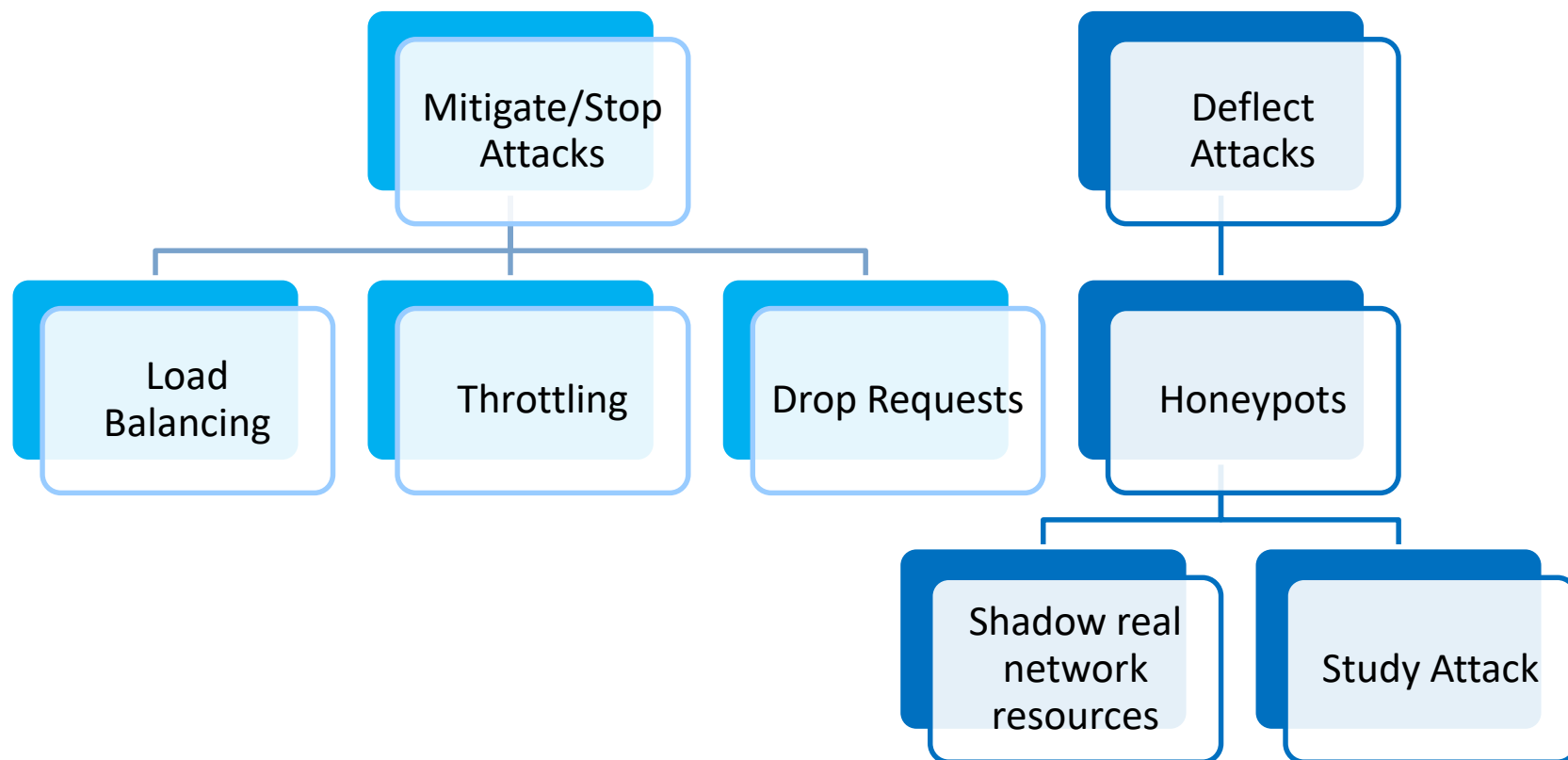
A Fraggle Attack is a denial-of-service (DoS) attack that involves sending a large amount of spoofed UDP traffic to a router's broadcast address within a network. It is very similar to a Smurf Attack, which uses spoofed ICMP traffic rather than UDP traffic to achieve the same goal. Given those routers (as of 1999) no longer forward packets directed at their broadcast addresses, most networks are now immune to Fraggle (and Smurf) attacks.

<https://security.radware.com/ddos-knowledge-center/ddospedia/fraggle-attack/>

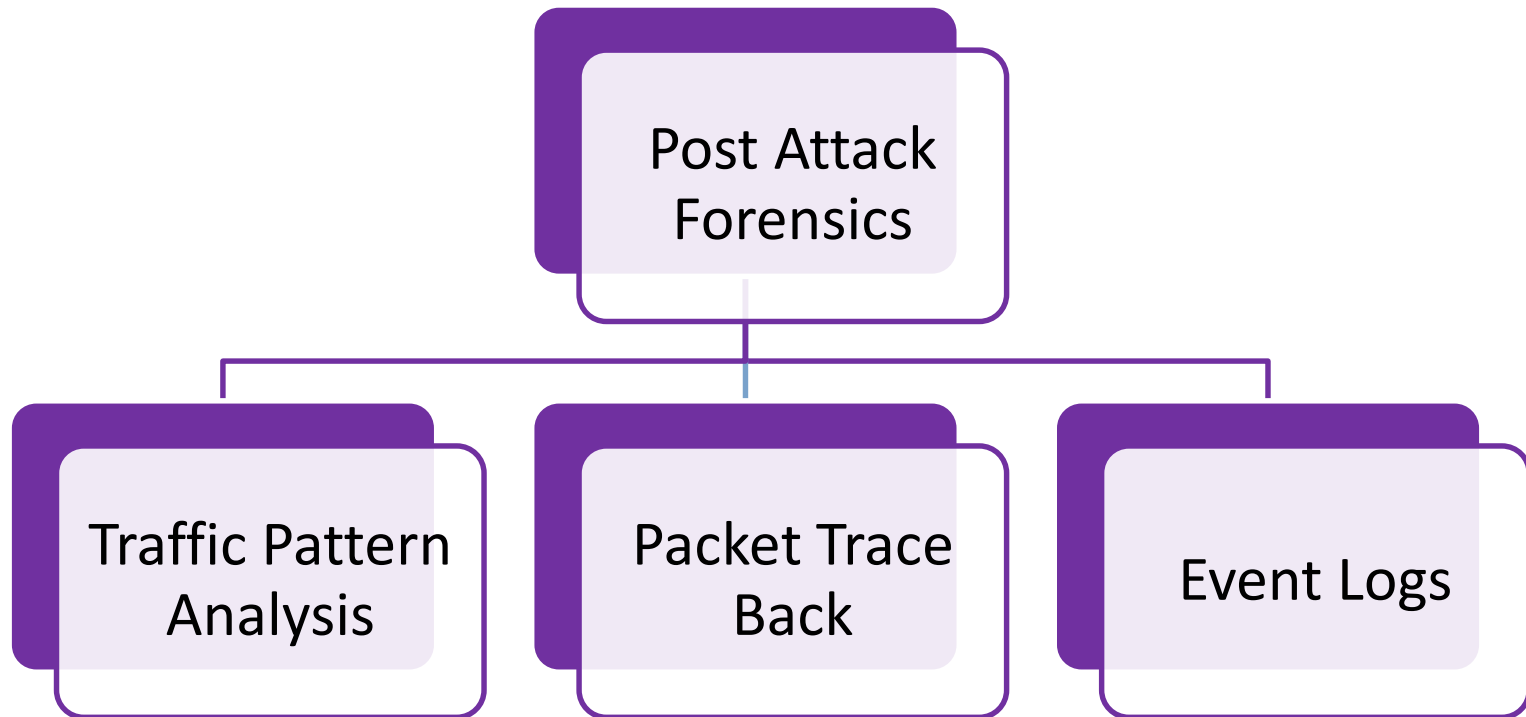
Countermeasures



Countermeasures



Countermeasures



Performing a DoS Attack

```
tcpdump -i eth1 -nntttt -s 0 -w dos.pcap -C 1000
```



Interface format size file name PCAP size

Capture network traffic with Tcpcap

```
root@bt:~# hping3 -S -p 80 --flood 216.1.1.1
HPING 216.1.1.1 (eth0 216.1.1.1): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Command used to start the DoS attack

164125	2013-01-23	14:09:03.324754	216.1.1.1	216.6.1.100	TCP	http > 36013 [RST, ACK]
164126	2013-01-23	14:09:03.324754	216.1.1.1	216.6.1.100	TCP	http > 36014 [RST, ACK]
164127	2013-01-23	14:09:03.324755	216.1.1.1	216.6.1.100	TCP	http > 36015 [RST, ACK]
164128	2013-01-23	14:09:03.324755	216.1.1.1	216.6.1.100	TCP	http > 36016 [RST, ACK]

Sample DoS Packets



This workforce solution was funded by a grant awarded by the U.S. Department of Labor's Employment and Training Administration. The solution was created by the grantee and does not necessarily reflect the official position of the U.S. Department of Labor. The Department of Labor makes no guarantees, warranties, or assurances of any kind, express or implied, with respect to such information, including any information on linked sites and including, but not limited to, accuracy, continued availability or ownership.

Assignment



No Lab assignment this week

Test next week

Practice test available on Canvas



Wrap up

Next Class

Assignment: Check the Calendar Page on the web site to see what is due next week.

No Quiz
No Lab due
Test!



Backup