Rich's lesson module checklist

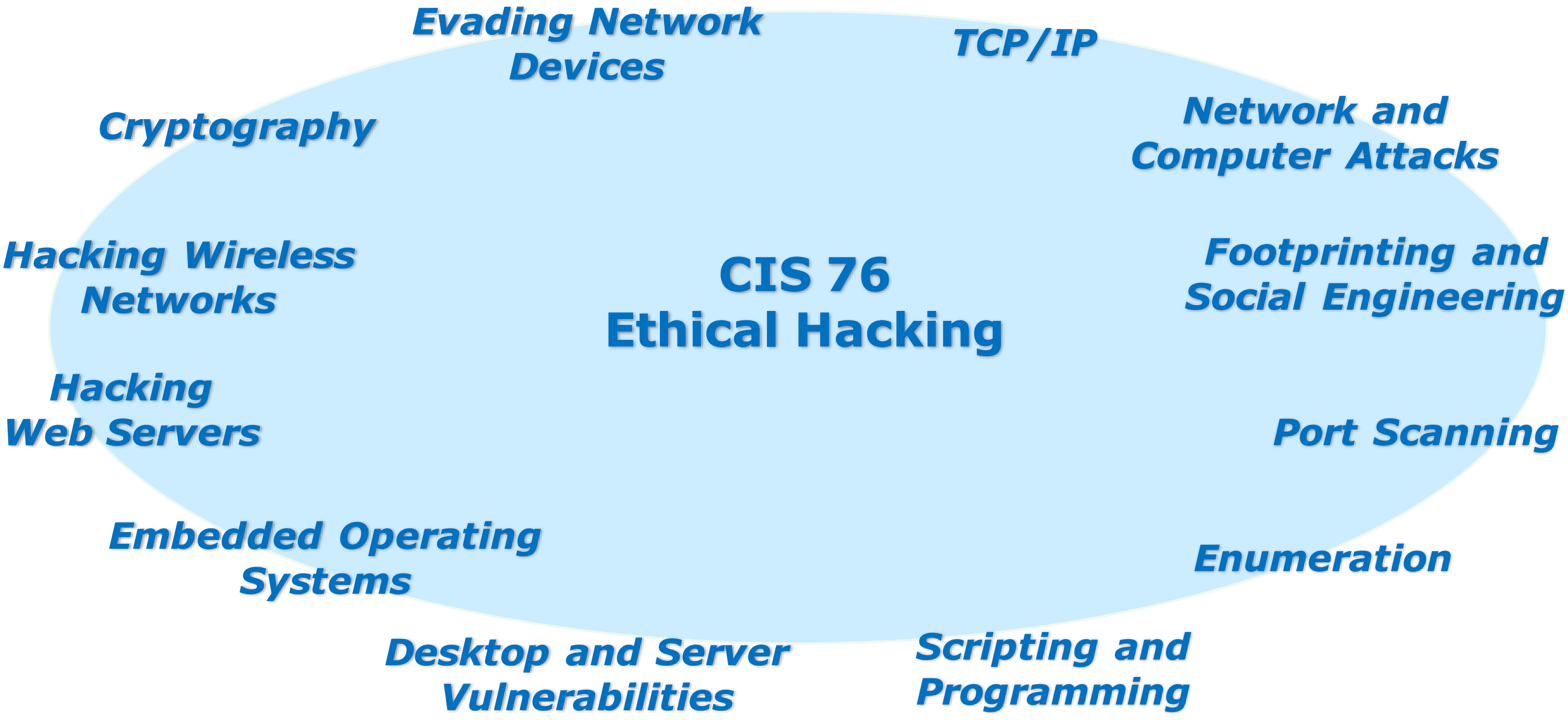
- □ Slides and lab posted
- □ WB converted from PowerPoint
- □ Print out agenda slide and annotate page numbers

- □ 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

Last updated 10/25/2016



CIS 76
Ethical Hacking

Evading Network Devices

TCP/IP

Network and Computer Attacks

Footprinting and Social Engineering

Port Scanning

Enumeration

Scripting and Programming

Desktop and Server Vulnerabilities

Embedded Operating Systems

Hacking Web Servers

Hacking Wireless Networks

Cryptography

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

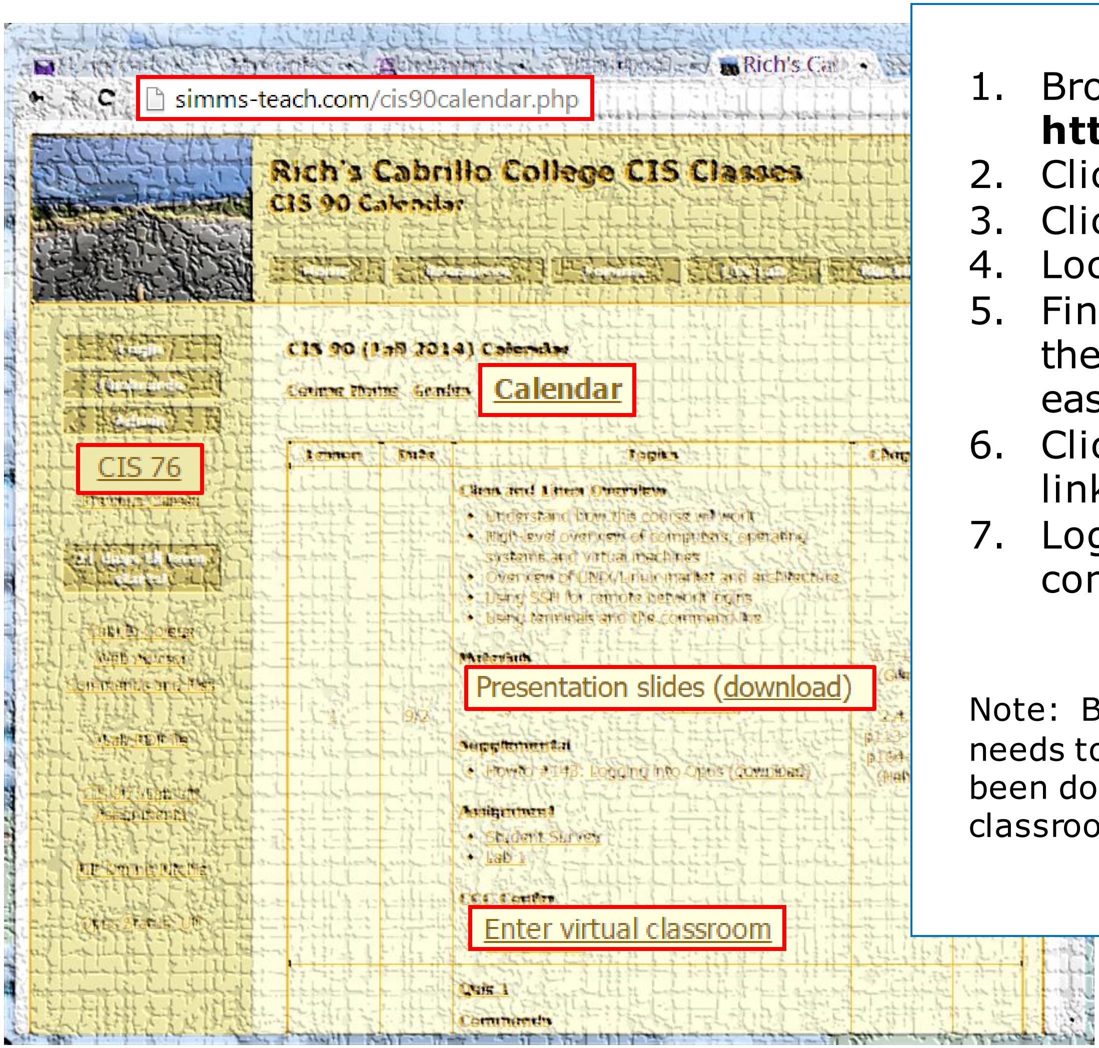
Rich Simms

- 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

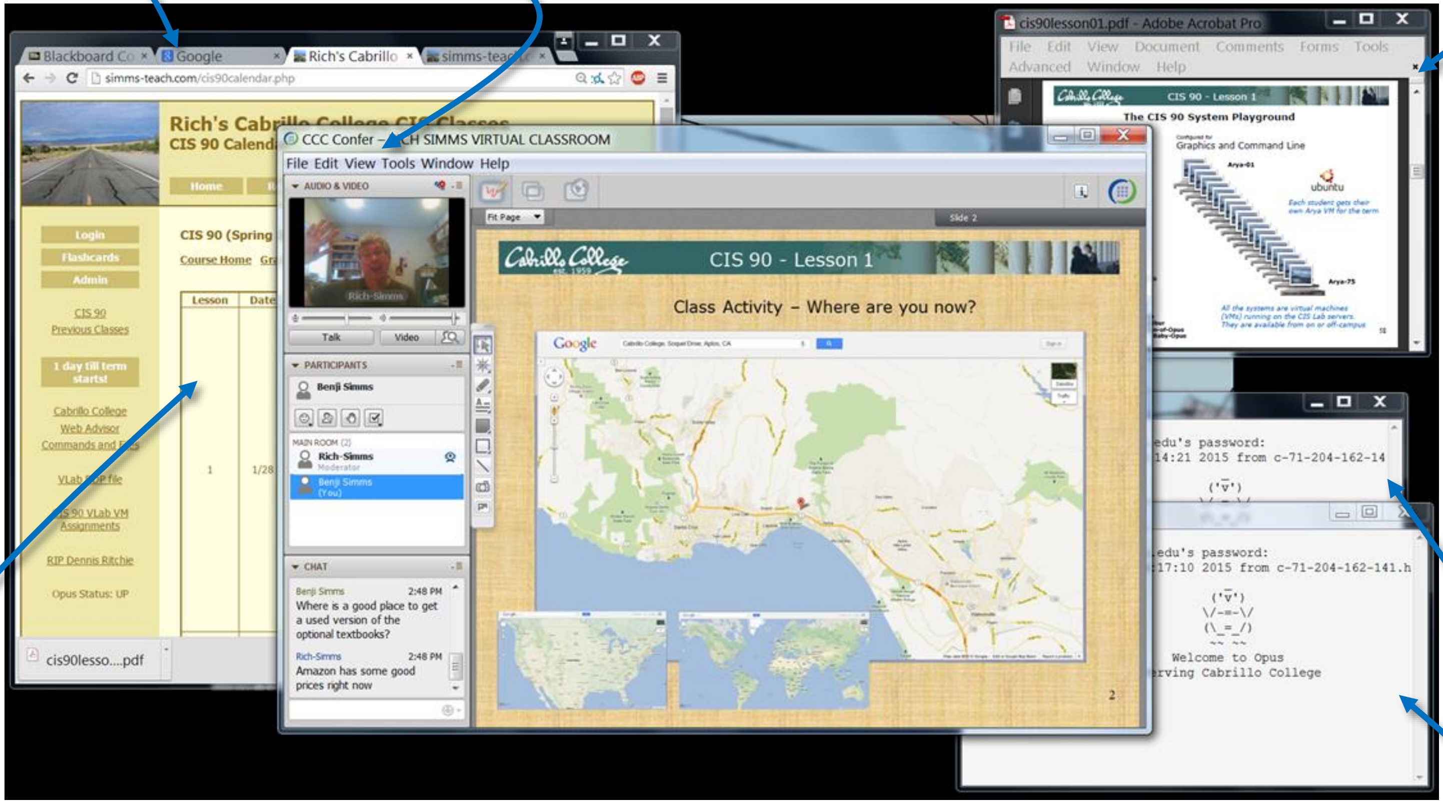

Rich's Cal
simms-teach.com/cis90calendar.php
Rich's Cabrillo College CIS Classes
CIS 90 Calendar
CIS 90 (Fall 2014) Calendar
Calendar
CIS 76
Presentation slides (download)
Enter virtual classroom

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


Blackboard Co
Google
Rich's Cabrillo
simms-teach
simms-teach.com/cis90calendar.php
Rich's Cabrillo College CIS Classes
CIS 90 Calendar
Home
Login
Flashcards
Admin
CIS 90
Previous Classes
1 day till term starts!
Cabrillo College
Web Advisor
Commands and Files
VLab RDP file
CIS 90 VLab VM Assignments
RIP Dennis Ritchie
Opus Status: UP
CIS 90 (Spring
Course Home
Lesson
Date
1
1/28
cis90lesso....pdf
CCC Confer – RICH SIMMS VIRTUAL CLASSROOM
File Edit View Tools Window Help
AUDIO & VIDEO
Rich-Simms
Talk
Video
PARTICIPANTS
Benji Simms
MAIN ROOM (2)
Rich-Simms
Moderator
Benji Simms
(You)
CHAT
Fit Page
Slide 2
CIS 90 - Lesson 1
Class Activity – Where are you now?
Google
Cabrillo College, Soquel Drive, Aptos, CA
2
cis90lesson01.pdf - Adobe Acrobat Pro
File Edit View Document Comments Forms Tools Advanced Window Help
CIS 90 - Lesson 1
The CIS 90 System Playground
Graphics and Command Line
Arya-01
ubuntu
Each student gets their own Arya VM for the term
Arya-75
All the systems are virtual machines (VMs) running on the CIS Lab servers. They are available from on or off-campus

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

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

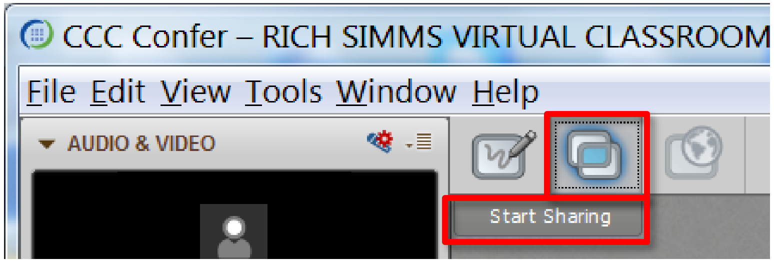
```
edu's password:
14:21 2015 from c-71-204-162-14

         ('v')
```

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

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

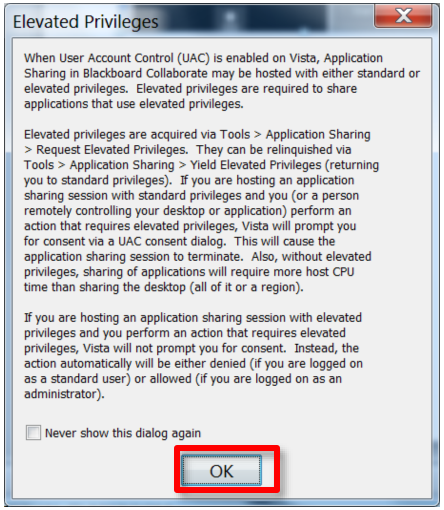
- ❑ *CIS 76 website Calendar page*
- ❑ *One or more login sessions to Opus*

Student checklist for sharing desktop with classmates

1) Instructor gives you sharing privileges.


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

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


Elevated Privileges

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

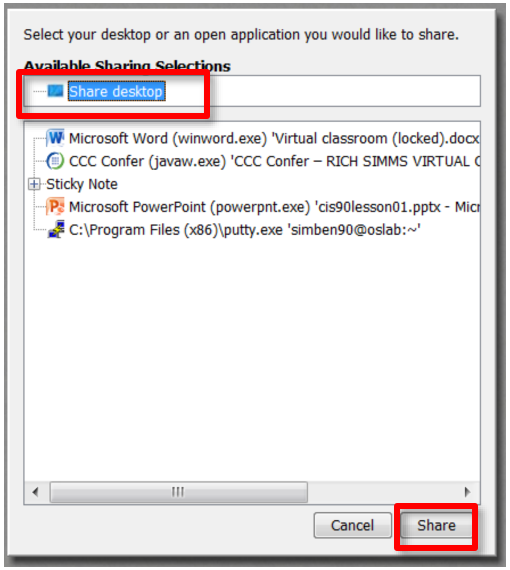
Elevated privileges are acquired via Tools > Application Sharing > Request Elevated Privileges. They can be relinquished via Tools > Application Sharing > Yield Elevated Privileges (returning you to standard privileges). If you are hosting an application sharing session with standard privileges and you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

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

□ Never show this dialog again

OK

3) Click OK button.


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

Available Sharing Selections

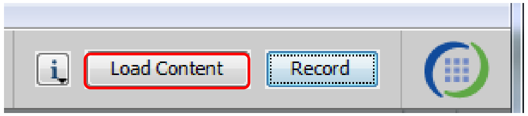
- Share desktop
- Microsoft Word (winword.exe) 'Virtual classroom (locked).docx
- CCC Confer (javaw.exe) 'CCC Confer – RICH SIMMS VIRTUAL C
- Sticky Note
- Microsoft PowerPoint (powerpnt.exe) 'cis90lesson01.pptx - Micr
- C:\Program Files (x86)\putty.exe 'simben90@oslab:~'

Cancel Share

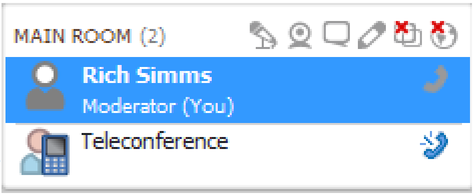
4) Select "Share desktop" and click Share button.

Rich's CCC Confer checklist - setup

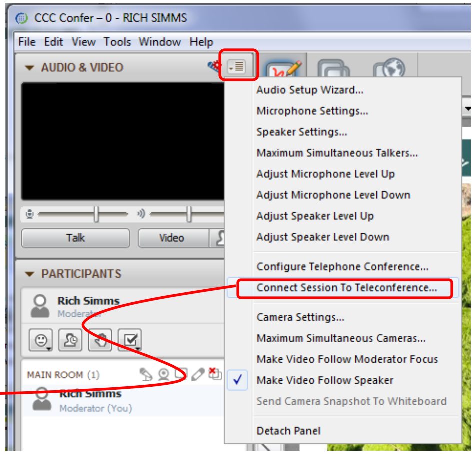
[ ] Preload White Board



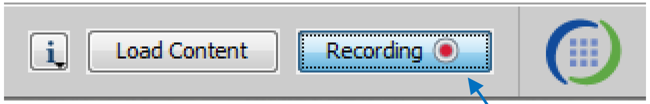
[ ] Connect session to Teleconference



Session now connected to teleconference


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

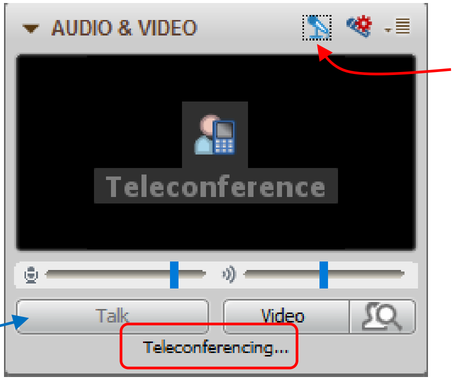
[ ] Is recording on?



Red dot means recording

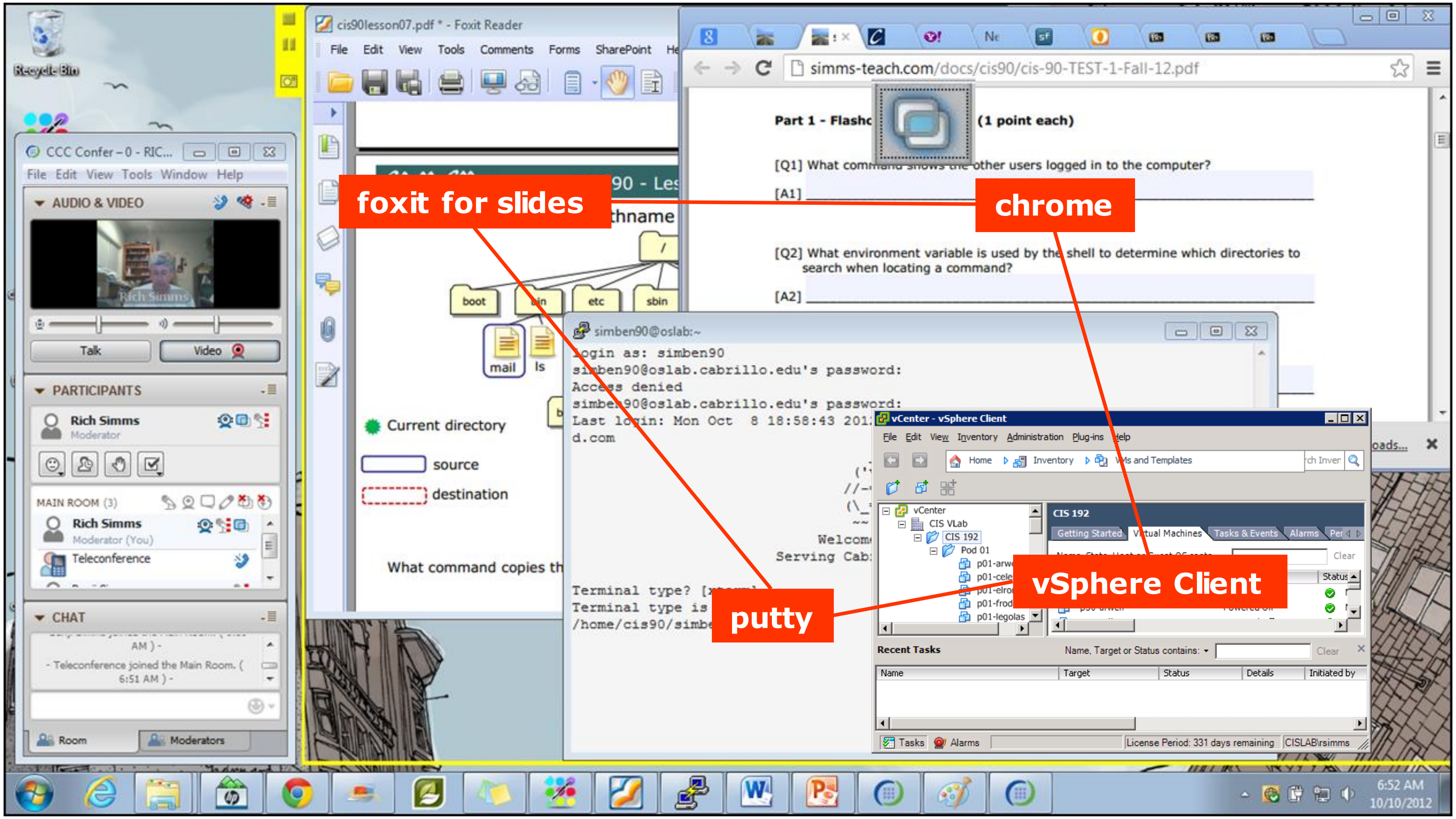
[ ] Use teleconferencing, not mic

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



foxit for slides

chrome

putty

vSphere Client

cis90lesson07.pdf * - Foxit Reader

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

Part 1 - Flashc (1 point each)

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

[A1] ______________________________

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

[A2] ______________________________

Current directory

source

destination

What command copies th

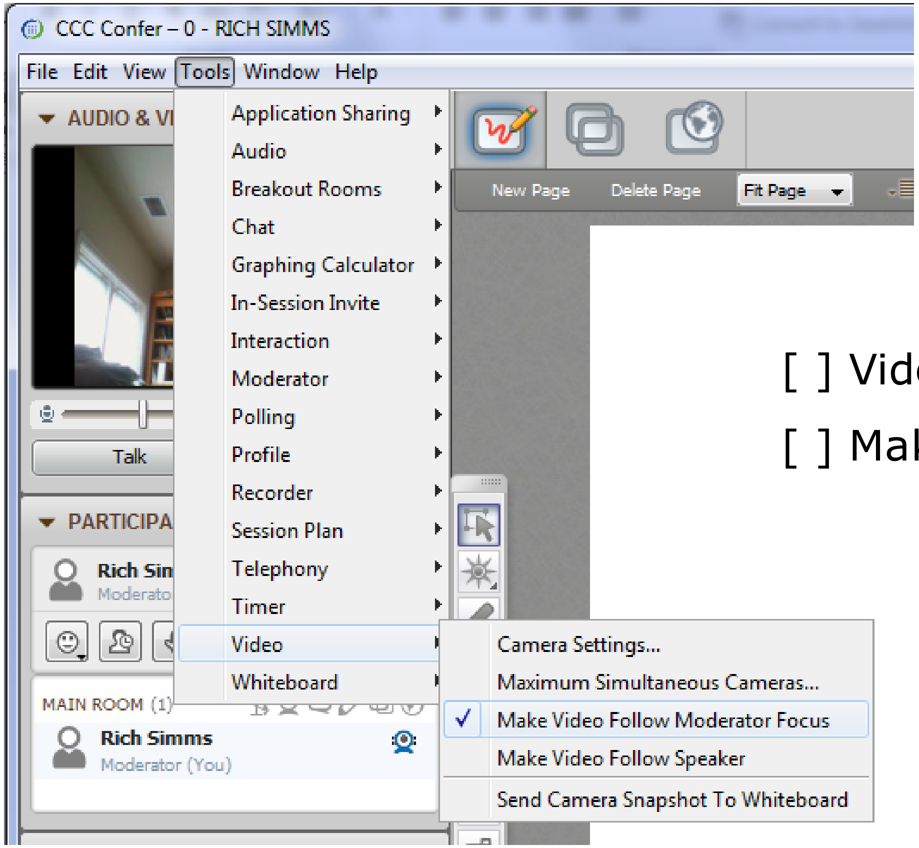
simben90@oslab:~

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

                                        Welcom
                                    Serving Cab

Terminal type? [xterm]
Terminal type is
/home/cis90/simbe
```

vCenter - vSphere Client

[ ] layout and share apps

Rich's CCC Confer checklist - webcam setup



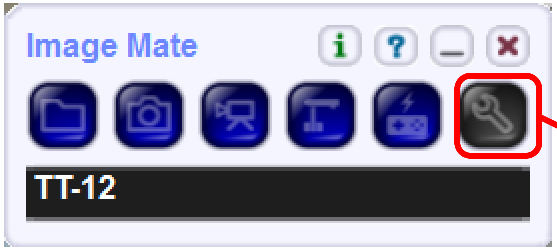
CCC Confer – 0 - RICH SIMMS

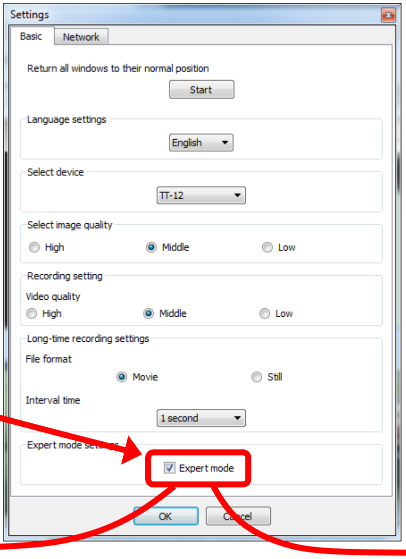
Tools > Video > ✓ Make Video Follow Moderator Focus

[ ] Video (webcam)

[ ] Make Video Follow Moderator Focus

Rich's CCC Confer checklist - Elmo





Settings

Basic | Network

Return all windows to their normal position

Start

Language settings: English

Select device: TT-12

Select image quality: ○ High ● Middle ○ Low

Recording setting

Video quality: ○ High ● Middle ○ Low

Long-time recording settings

File format: ● Movie ○ Still

Interval time: 1 second

Expert mode settings

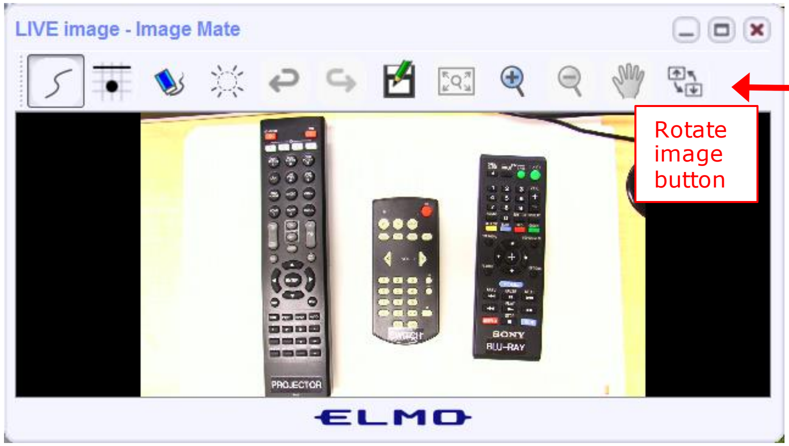
☑ Expert mode

OK | Cancel

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

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

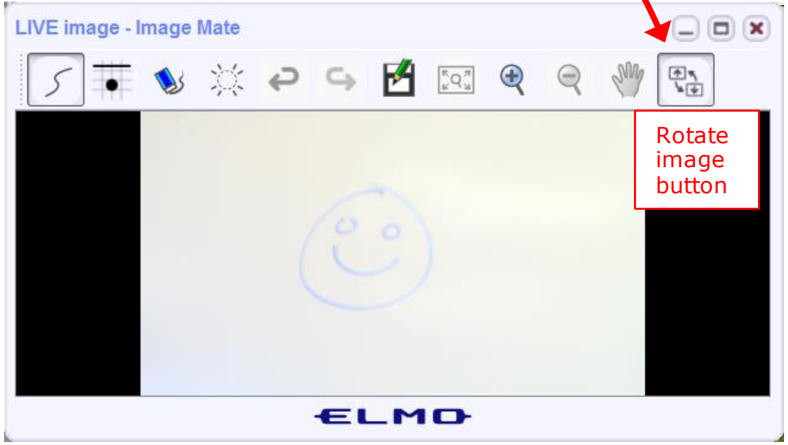
Elmo rotated down to view side table



Rotate image button

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

Elmo rotated up to view white board



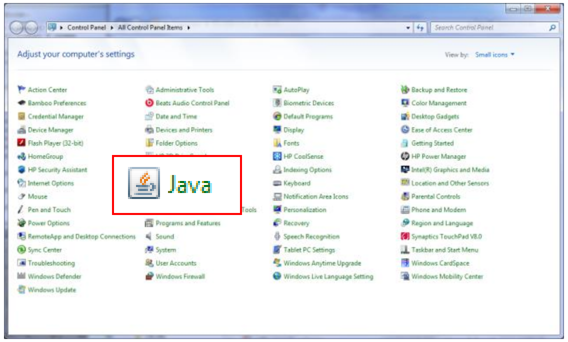
Rotate image button

Rich's CCC Confer checklist - universal fixes

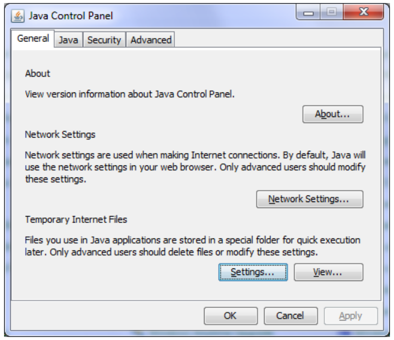
Universal Fix for CCC Confer:

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

Control Panel (small icons)



General Tab > Settings...



About

View version information about Java Control Panel.

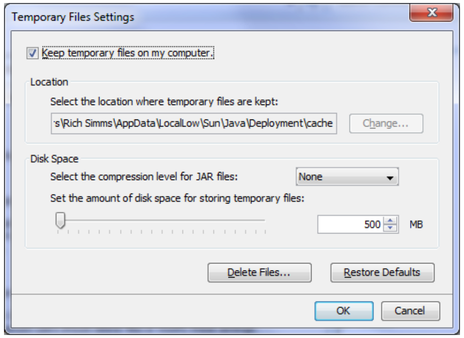
Network Settings

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

Temporary Internet Files

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

500MB cache size



☑ Keep temporary files on my computer.

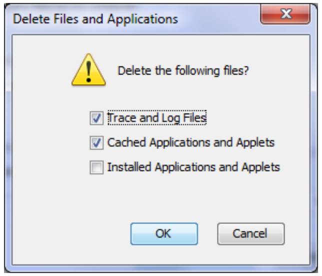
Select the location where temporary files are kept:

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

Select the compression level for JAR files: None

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

Delete these



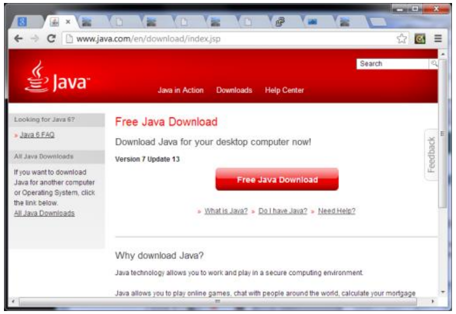
Delete the following files?

☑ Trace and Log Files

☑ Cached Applications and Applets

☐ Installed Applications and Applets

Google Java download



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

Free Java Download

Download Java for your desktop computer now!

Version 7 Update 13

Why download Java?

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

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

Start

Sound Check

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

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

Instructor: **Rich Simms**

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

Passcode: **136690**

Ryan

Jordan

Takashi

Karl-Heinz

Sean

Benji

Joshua

Brian

Tess

Jeremy

David H.

Roberto

Nelli

Mike C.

Deryck

Alex

Michael W.

Carter

Thomas

Wes

Jennifer

Marcos

Tim

Luis

Dave R.

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

First Minute Quiz

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

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

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.*

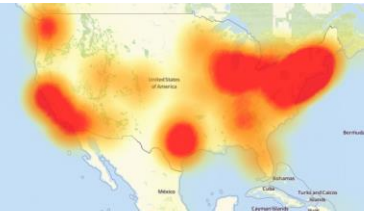
In the news

Recent news

1. This Is Why Half the Internet Shut Down Today

http://gizmodo.com/this-is-probably-why-half-the-internet-shut-down-today-1788062835

Thanks Deryck



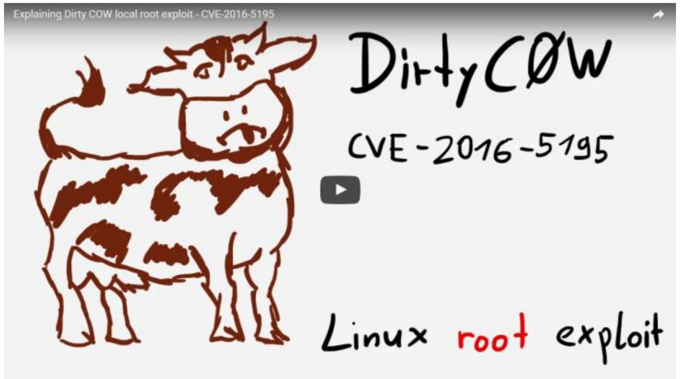
2. American hacker Jester warns Russia to stop interfering with U.S. election

http://www.digitaltrends.com/computing/jester-hacks-russian-ministry/

Recent news

3. Linux exploit ‘Dirty COW’ allows any user to gain root access in mere five seconds

https://thetechportal.com/2016/10/24/linux-vulnerability-serious-hack-easy/



https://youtu.be/kEsshExn7aE

Best Practices

Defense Best Practices

Who Makes the IoT Things Under Attack?

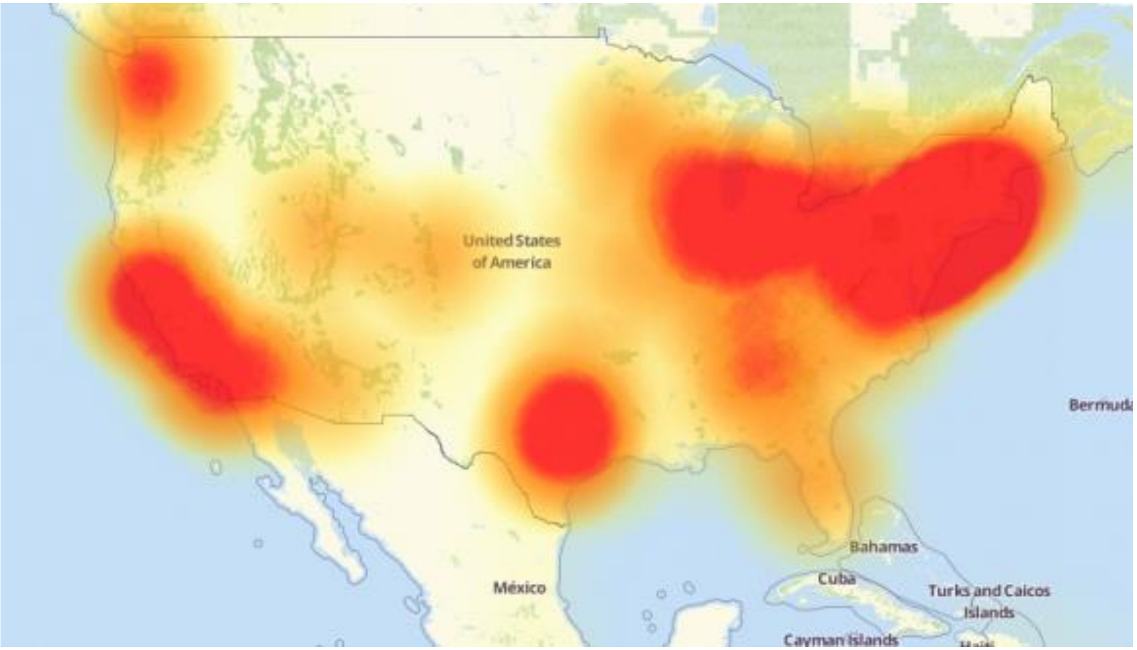
https://krebsonsecurity.com/2016/10/who-makes-the-iot-things-under-attack/

> *"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: Downdetector.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

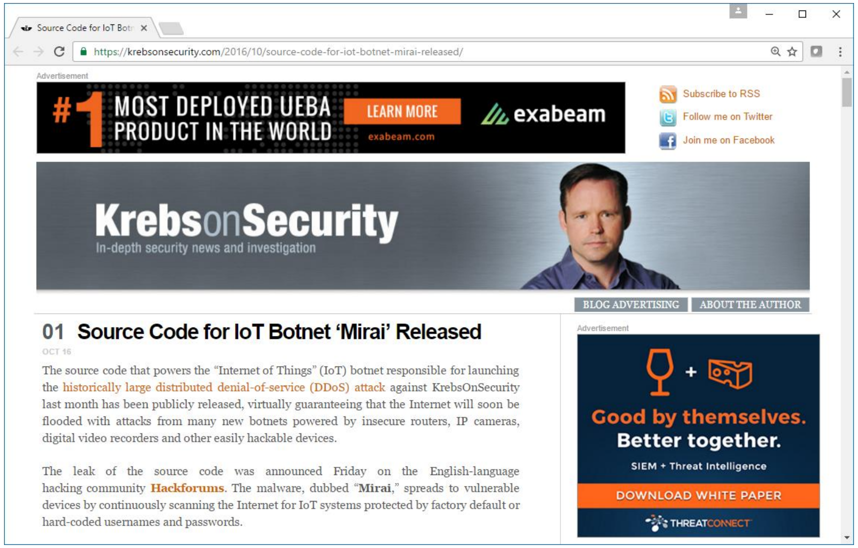
“While Flashpoint has confirmed that Mirai botnets were used in the October 21, 2016 attack against Dyn, they were separate and distinct botnets from those used to execute the DDoS attacks against ‘Krebs on Security’ and OVH,” Flashpoint said in a statement sent to Salted Hash.

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


Source Code for IoT Botn
https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/

Advertisement
#1 MOST DEPLOYED UEBA PRODUCT IN THE WORLD LEARN MORE exabeam.com exabeam

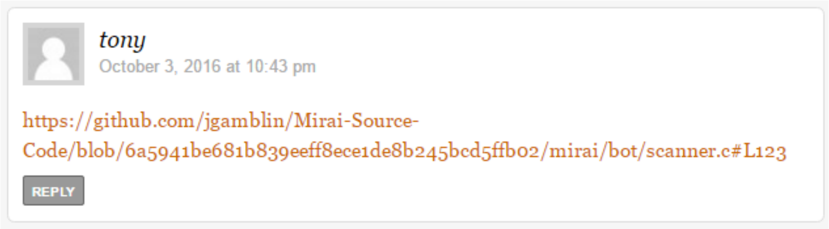
01 Source Code for IoT Botnet 'Mirai' Released

OCT 16

The source code that powers the "Internet of Things" (IoT) botnet responsible for launching the historically large distributed denial-of-service (DDoS) attack against KrebsOnSecurity last month has been publicly released, virtually guaranteeing that the Internet will soon be flooded with attacks from many new botnets powered by insecure routers, IP cameras, digital video recorders and other easily hackable devices.

The leak of the source code was announced Friday on the English-language hacking community **Hackforums**. The malware, dubbed "**Mirai**," spreads to vulnerable devices by continuously scanning the Internet for IoT systems protected by factory default or hard-coded usernames and passwords.

Advertisement
Good by themselves. Better together.
SIEM + Threat Intelligence
DOWNLOAD WHITE PAPER
THREATCONNECT



tony

October 3, 2016 at 10:43 pm

https://github.com/jgamblin/Mirai-Source-Code/blob/6a5941be681b839eeff8ece1de8b245bcd5ffb02/mirai/bot/scanner.c#L123

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

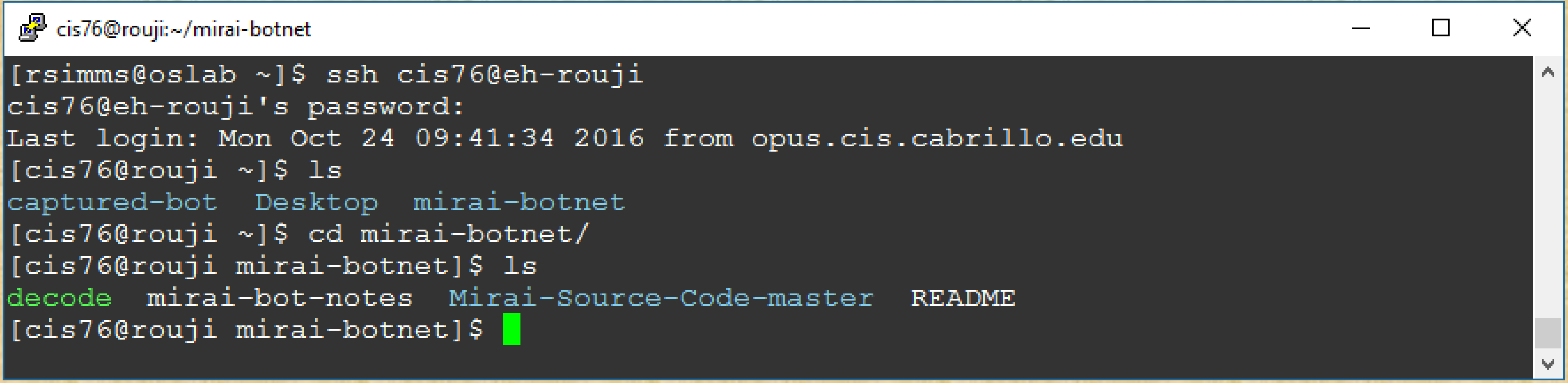
https://github.com/jgamblin/Mirai-Source-Code

The source code is available now on EH-Rouji

Activity

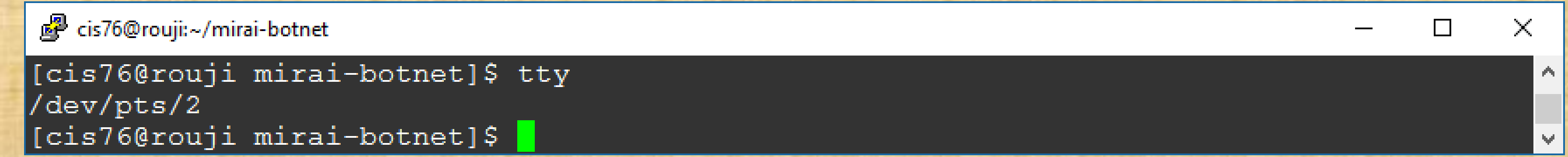
Log into eh-rouji and change into the mirai-botnet directory

ssh cis76@eh-rouji
cd mirai-botnet



```
[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]$ 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

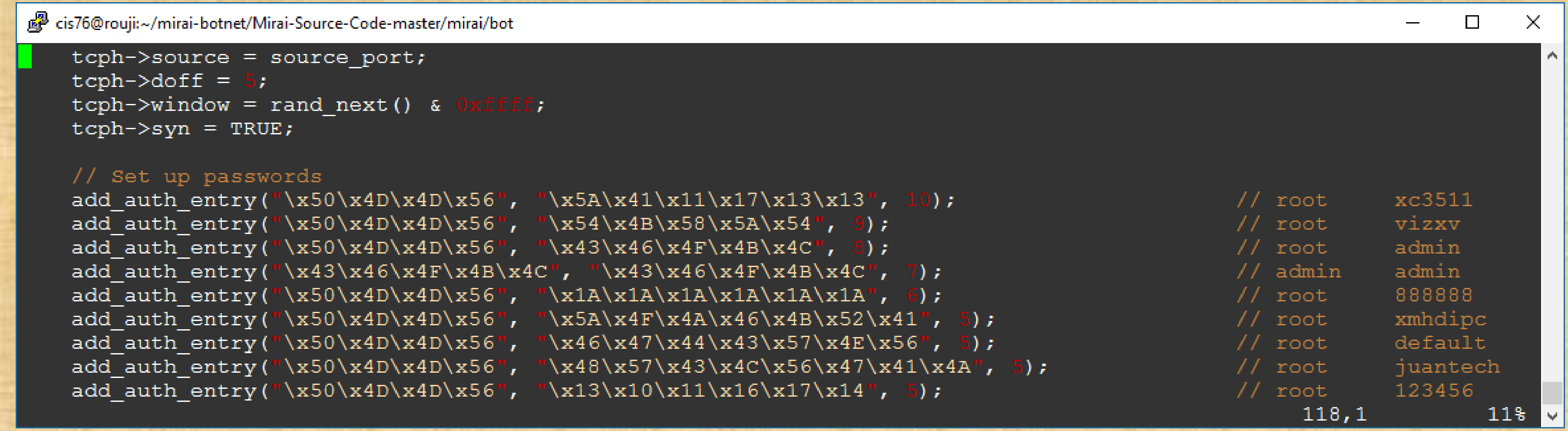
"The purpose of these scans is to locate under-secured IoT devices that could be remotely accessed via easily guessable login credentials—usually factory default usernames and passwords (e.g., admin/admin)."

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

Activity

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

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



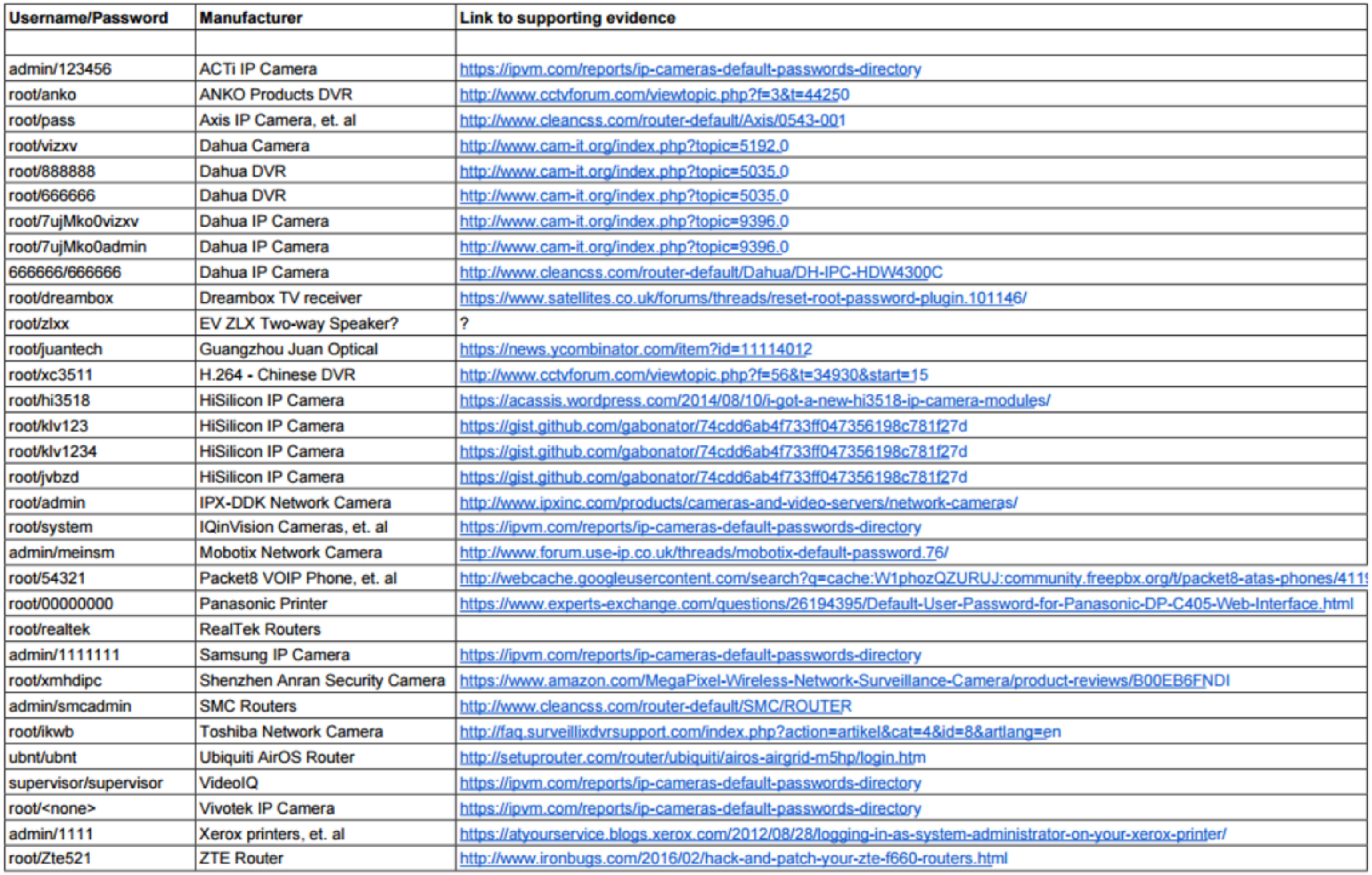
cis76@rouji:~/mirai-botnet/Mirai-Source-Code-master/mirai/bot

```
    tcph->source = source_port;
    tcph->doff = 5;
    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

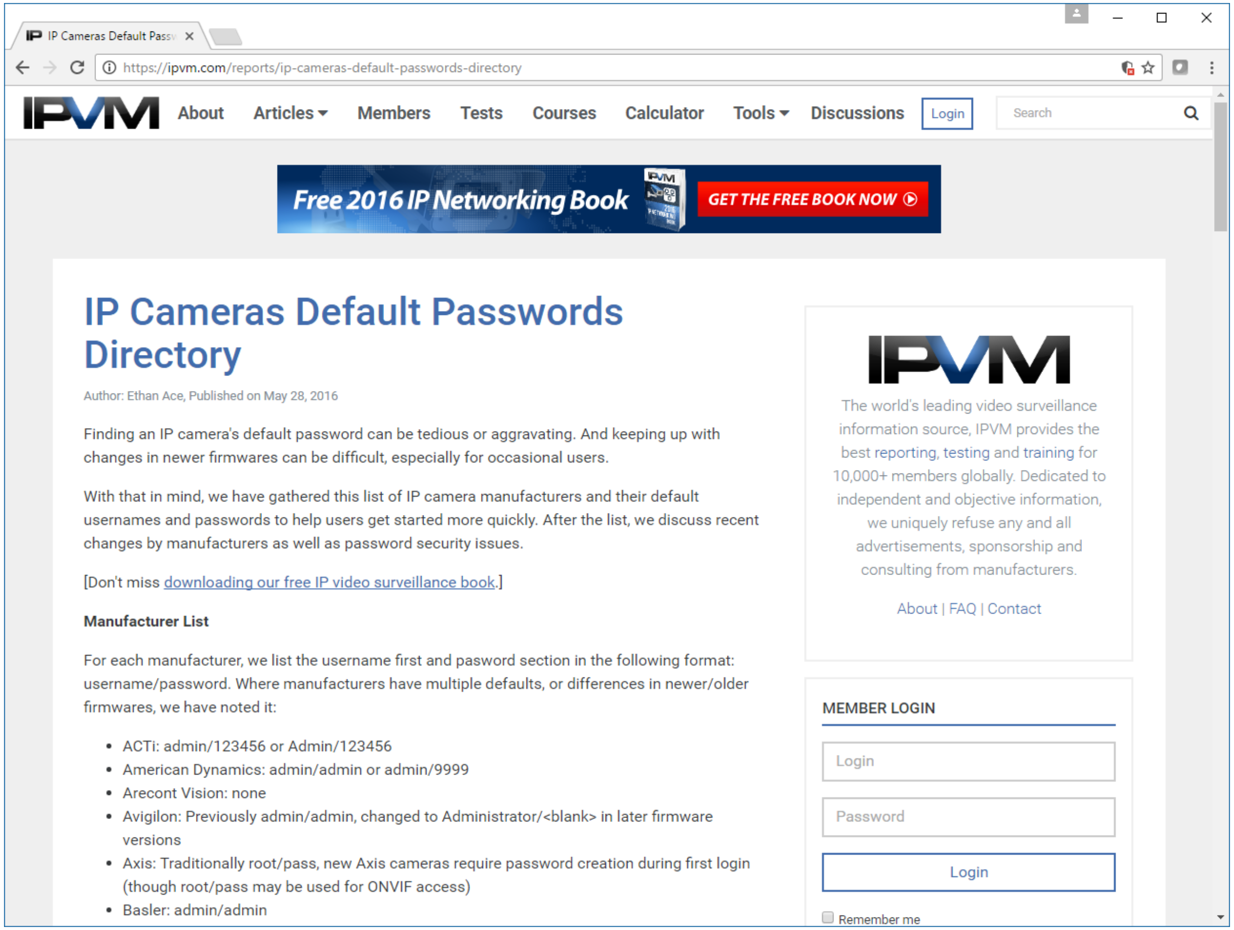
Mirai Target Devices



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/jvbzd	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/meinsm	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/411
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.surveillixdvrsupport.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

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

Mirai Target Devices



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 pasword 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

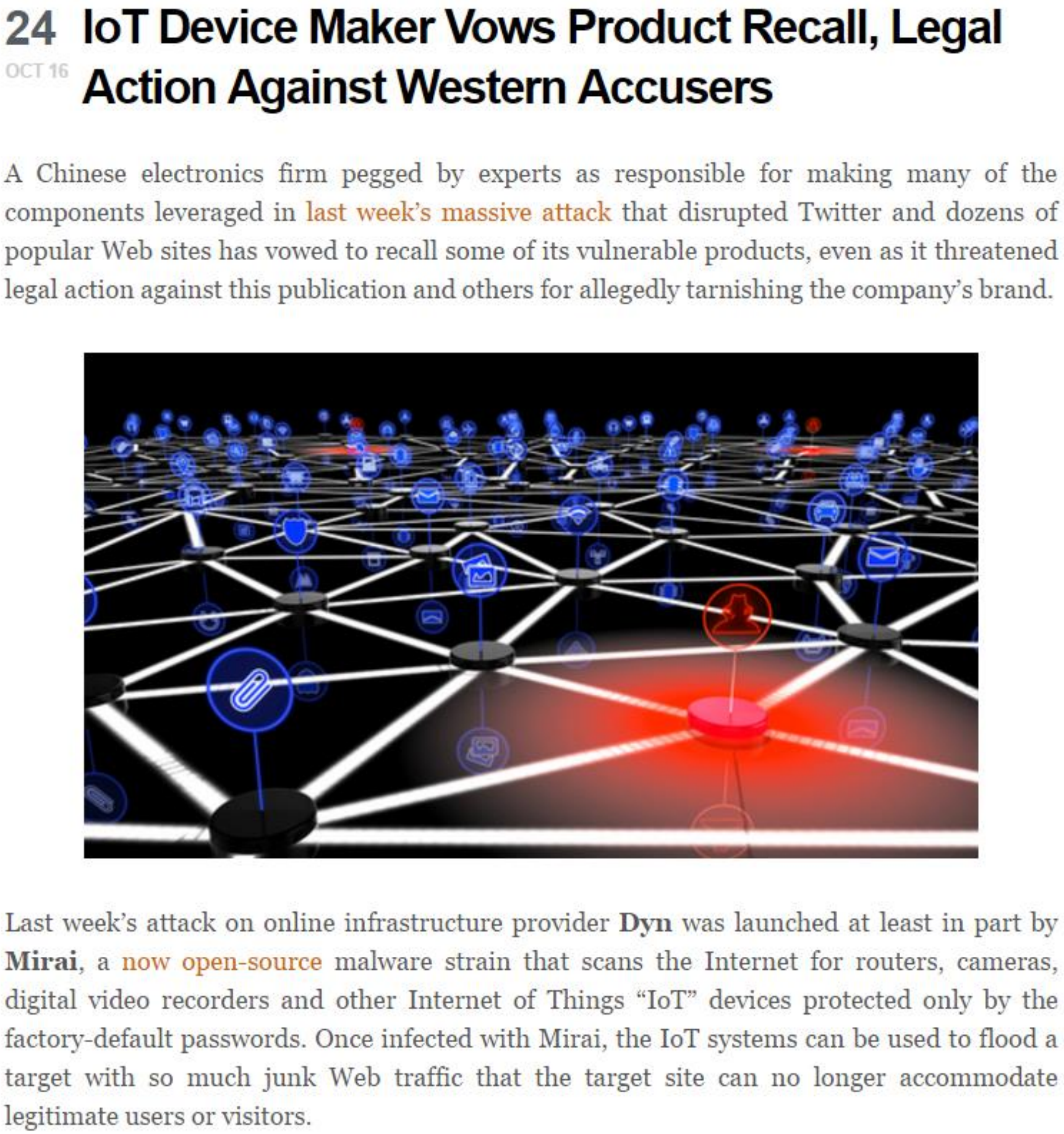
IPVM

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

https://ipvm.com/reports/ip-cameras-default-passwords-directory

Mirai Target Devices



24 OCT 16

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

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

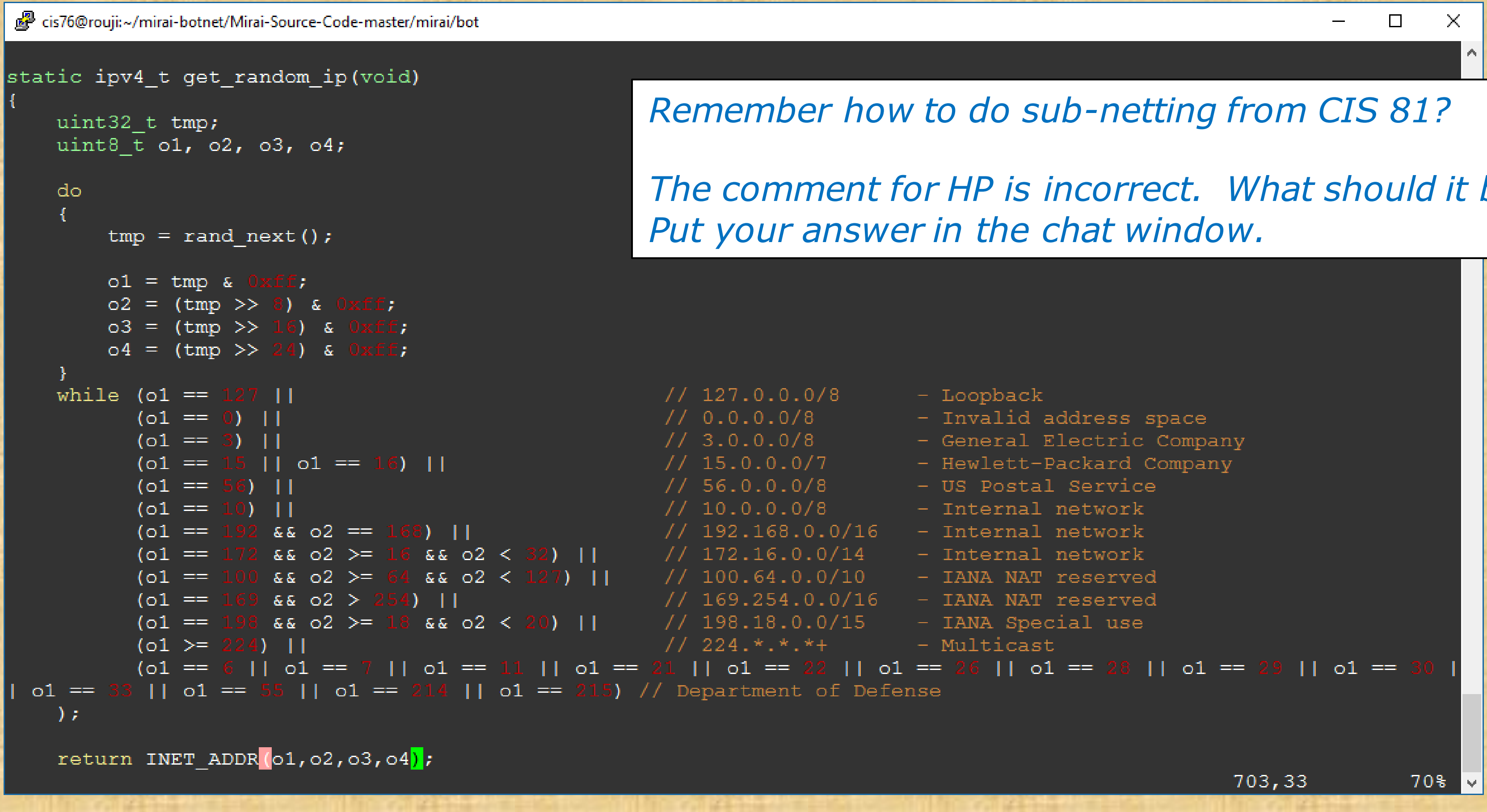
"One of the most interesting things revealed by the code was a hardcoded list of IPs Mirai bots are programmed to avoid when performing their IP scans."

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);
                                                                                                    703,33        70%
```

Remember how to do sub-netting from CIS 81?

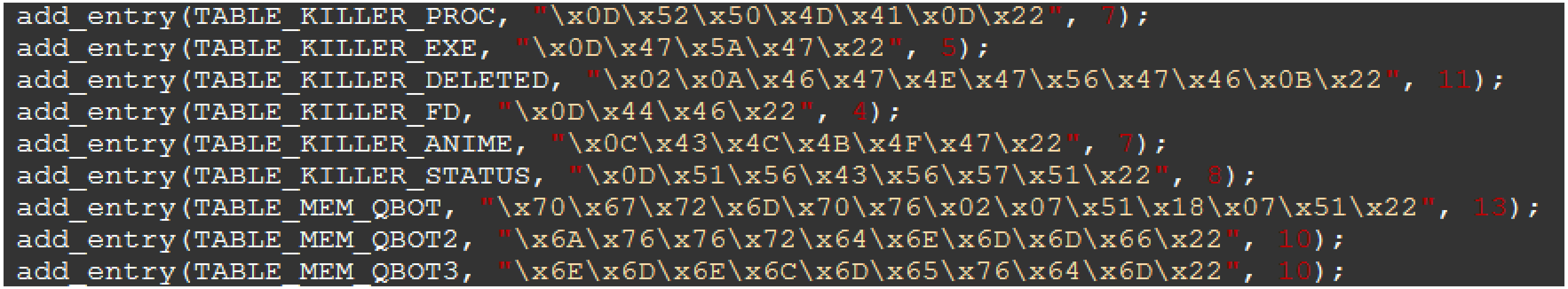
The comment for HP is incorrect. What should it be? Put your answer in the chat window.

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
```



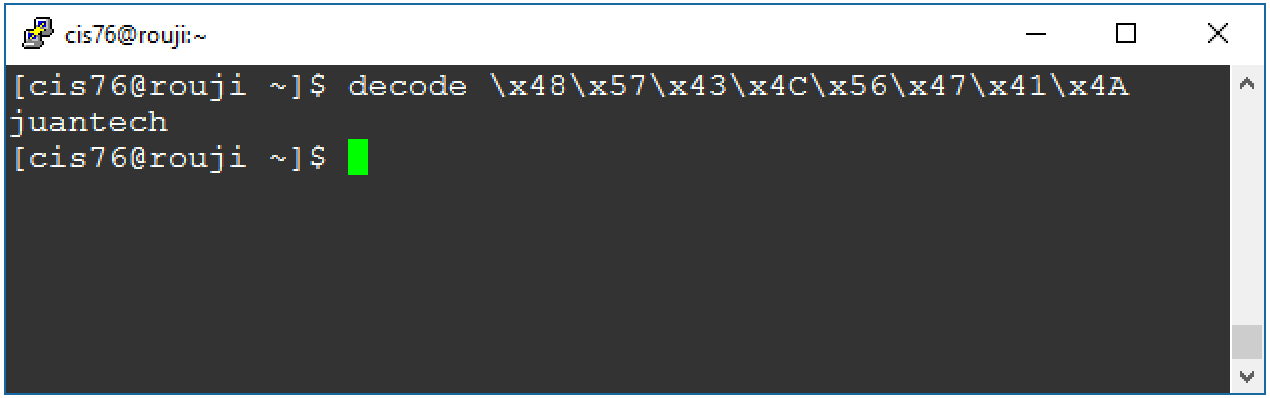
```
add_entry(TABLE_KILLER_PROC, "\x0D\x52\x50\x4D\x41\x0D\x22", 7);
add_entry(TABLE_KILLER_EXE, "\x0D\x47\x5A\x47\x22", 5);
add_entry(TABLE_KILLER_DELETED, "\x02\x0A\x46\x47\x4E\x47\x56\x47\x46\x0B\x22", 11);
add_entry(TABLE_KILLER_FD, "\x0D\x44\x46\x22", 4);
add_entry(TABLE_KILLER_ANIME, "\x0C\x43\x4C\x4B\x4F\x47\x22", 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



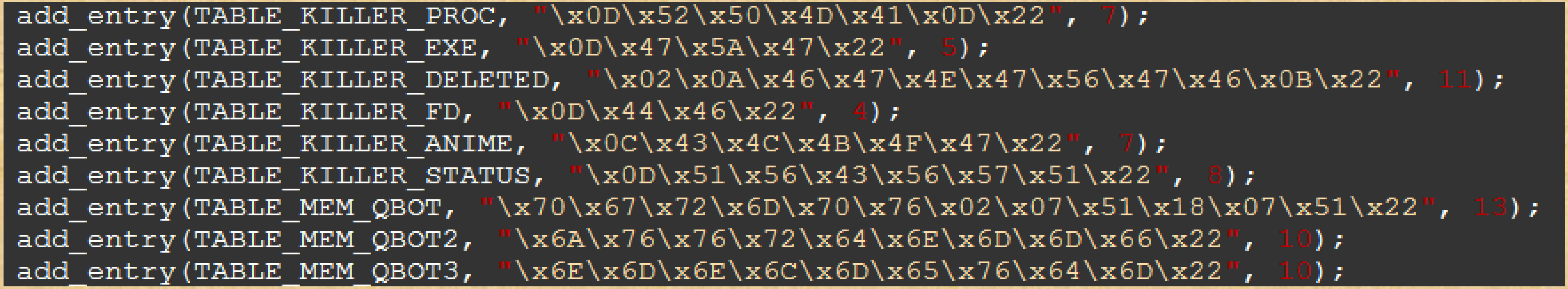
```
[cis76@rouji ~]$ decode \x48\x57\x43\x4C\x56\x47\x41\x4A
juantech
[cis76@rouji ~]$
```

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/
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);
```

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

What do your 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\x7
6\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\x4
D\x46\x47\x46\x22", 48);
```

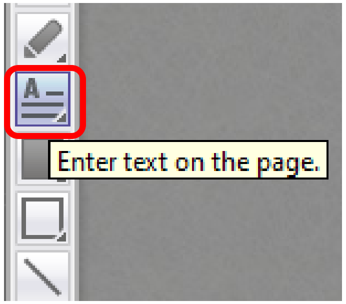
Hex codes

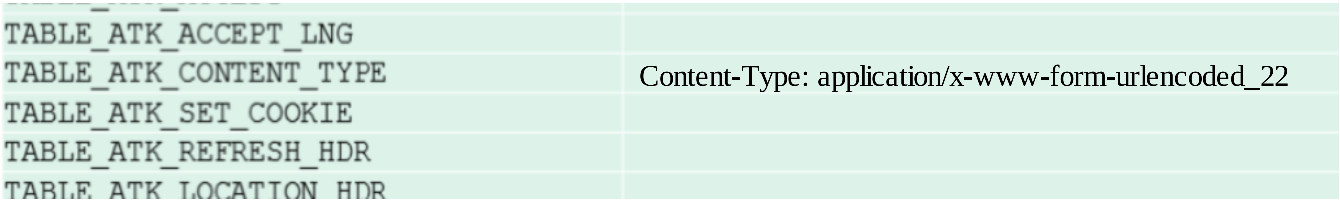
```
[cis76@rouji ~]$ decode \x61\x4D\x4C\x56\x47\x4C\x56\x0F\x76\x5B\x52\x
47\x18\x02\x43\x52\x52\x4E\x4B\x41\x43\x56\x4B\x4D\x4C\x0D\x5A\x0F\x55
\x55\x55\x0F\x44\x4D\x50\x4F\x0F\x57\x50\x4E\x47\x4C\x41\x4D\x46\x47\x
46\x22
Content-Type: application/x-www-form-urlencoded_22
```

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

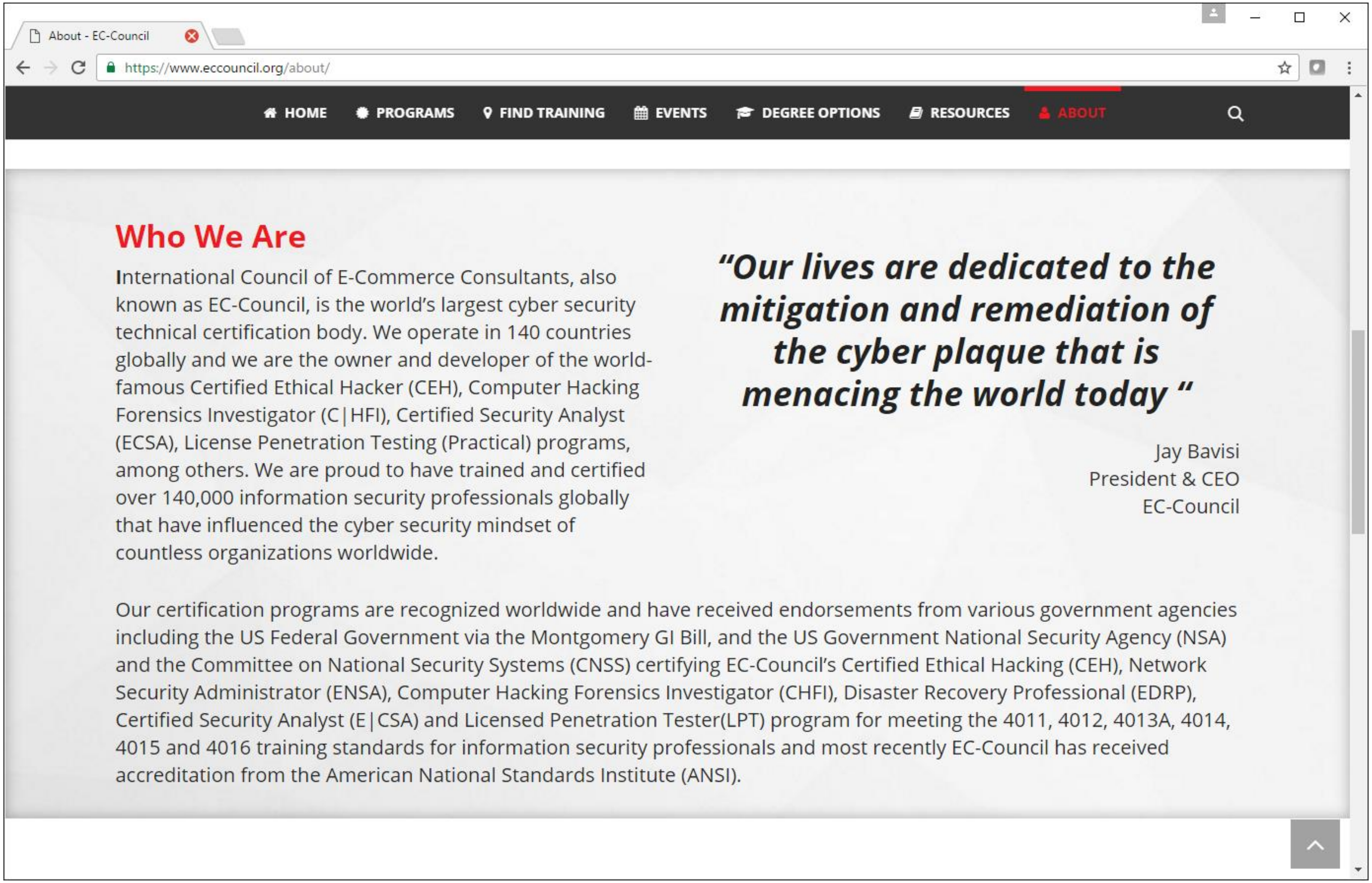
TABLE_CNC_DOMAIN	
TABLE_CNC_PORT	
TABLE_SCAN_CB_DOMAIN	
TABLE_SCAN_CB_PORT	
TABLE_EXEC_SUCCESS	
TABLE_KILLER_SAFE	
TABLE_KILLER_PROC	
TABLE_KILLER_EXE	
TABLE_KILLER_DELETED	
TABLE_KILLER_FD	
TABLE_KILLER_ANIME	
TABLE_KILLER_STATUS	
TABLE_MEM_QBOT	
TABLE_MEM_QBOT2	
TABLE_MEM_QBOT3	
TABLE_MEM_UPX	
TABLE_MEM_ZOLLARD	
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



Who We Are

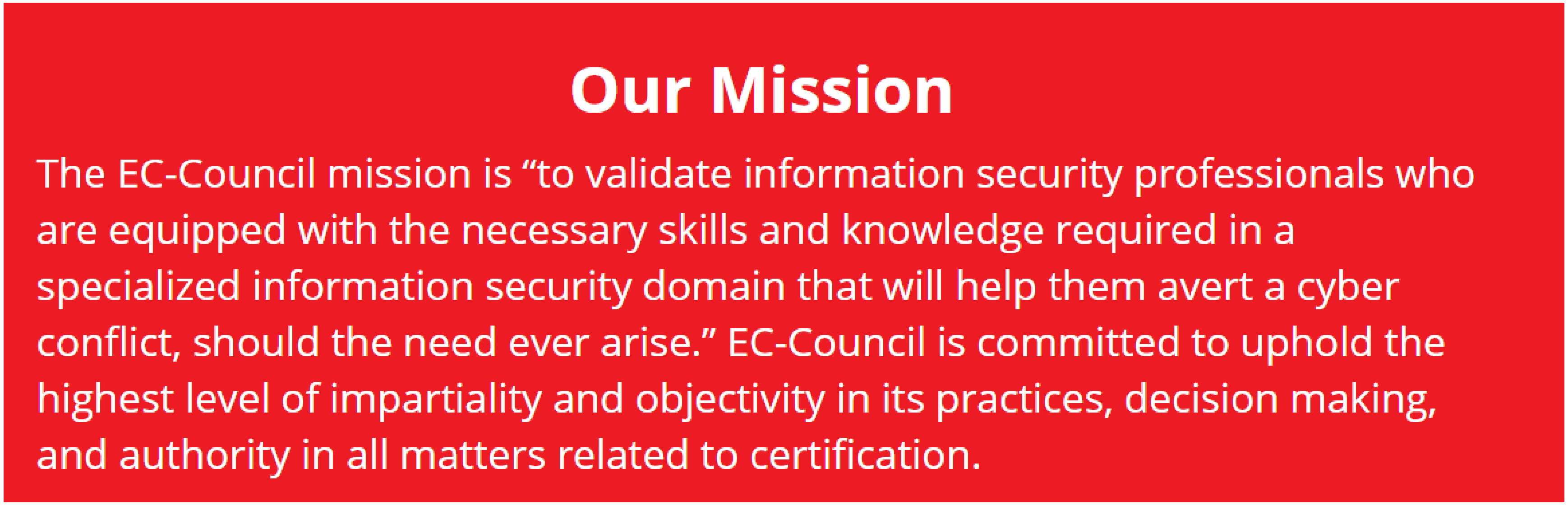
International Council of E-Commerce Consultants, also known as EC-Council, is the world's largest cyber security technical certification body. We operate in 140 countries globally and we are the owner and developer of the world-famous Certified Ethical Hacker (CEH), Computer Hacking Forensics Investigator (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 lives are dedicated to the mitigation and remediation of the cyber plaque that is menacing the world today "***
>
> Jay Bavisi
> President & CEO
> EC-Council

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).

https://www.eccouncil.org/about/

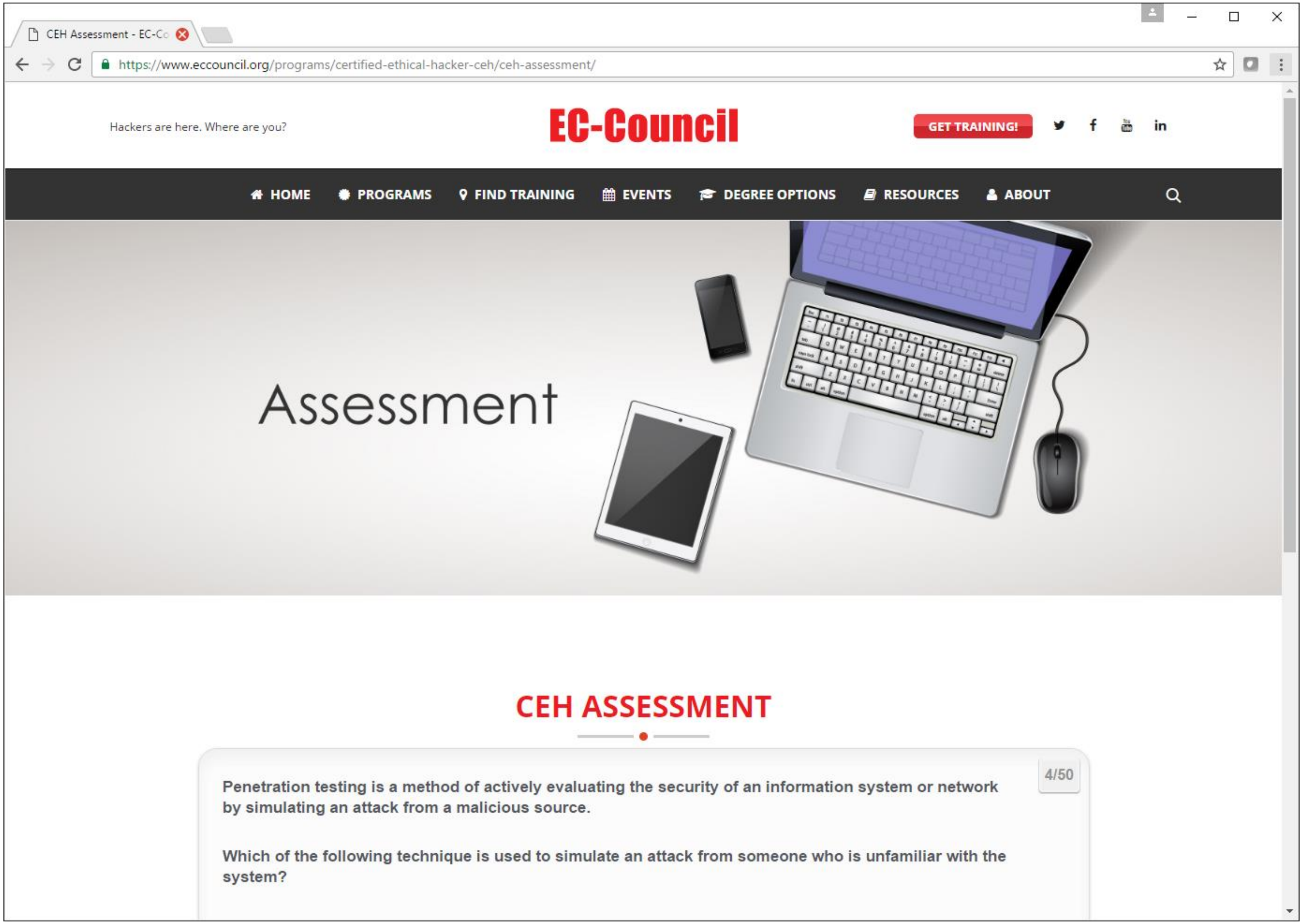
EC-Council



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



CEH ASSESSMENT

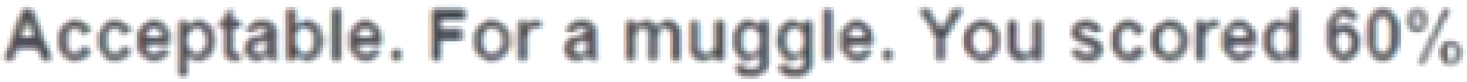
4/50

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?

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

EC-Council Mini-Assessment

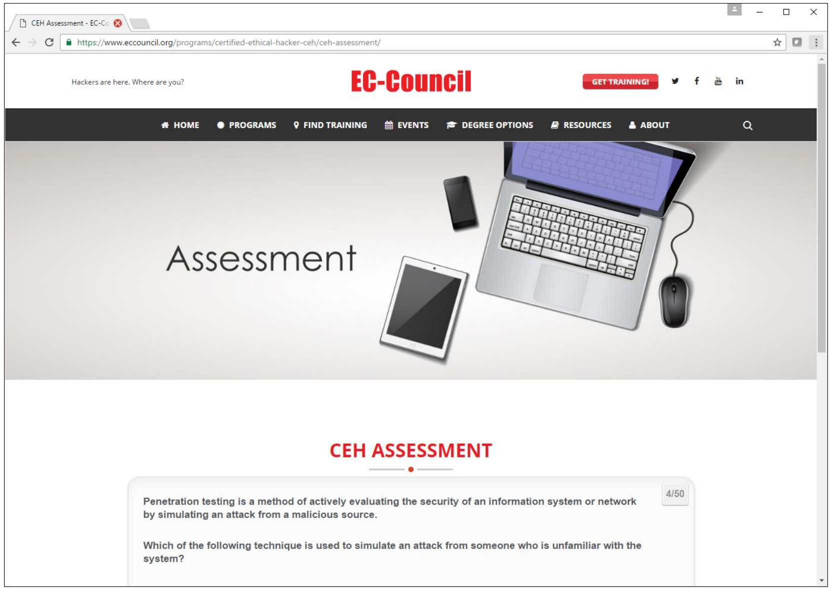


Acceptable. For a muggle. You scored 60%

Our baseline to beat tonight

EC-Council Mini-Assessment Q1-10

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

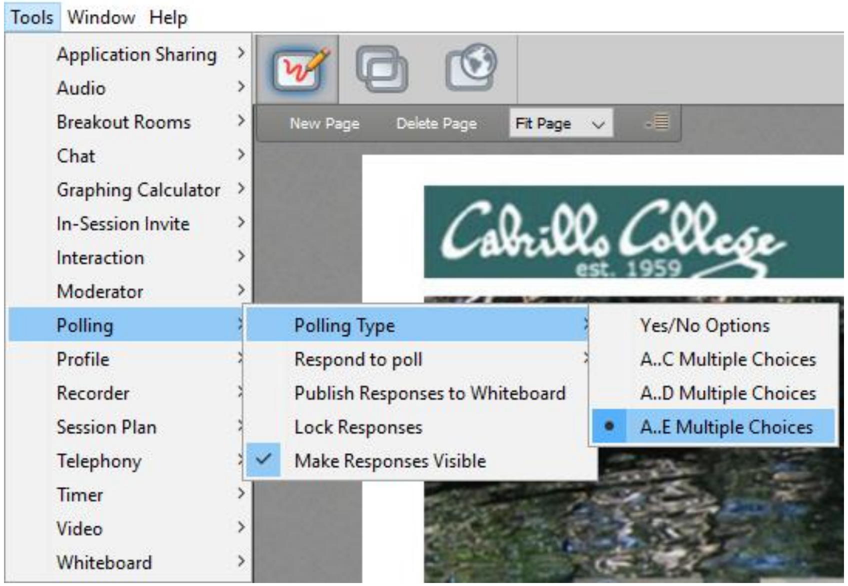


CEH ASSESSMENT

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?



Questions 1-10 (five minutes)

Housekeeping

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

Housekeeping

1. Lab 7 due by 11:59PM (Opus time) tonight. PDFs with full non-cropped screenshots are preferred.

2. Second test next week!

3. Practice test available after class.

Test #2

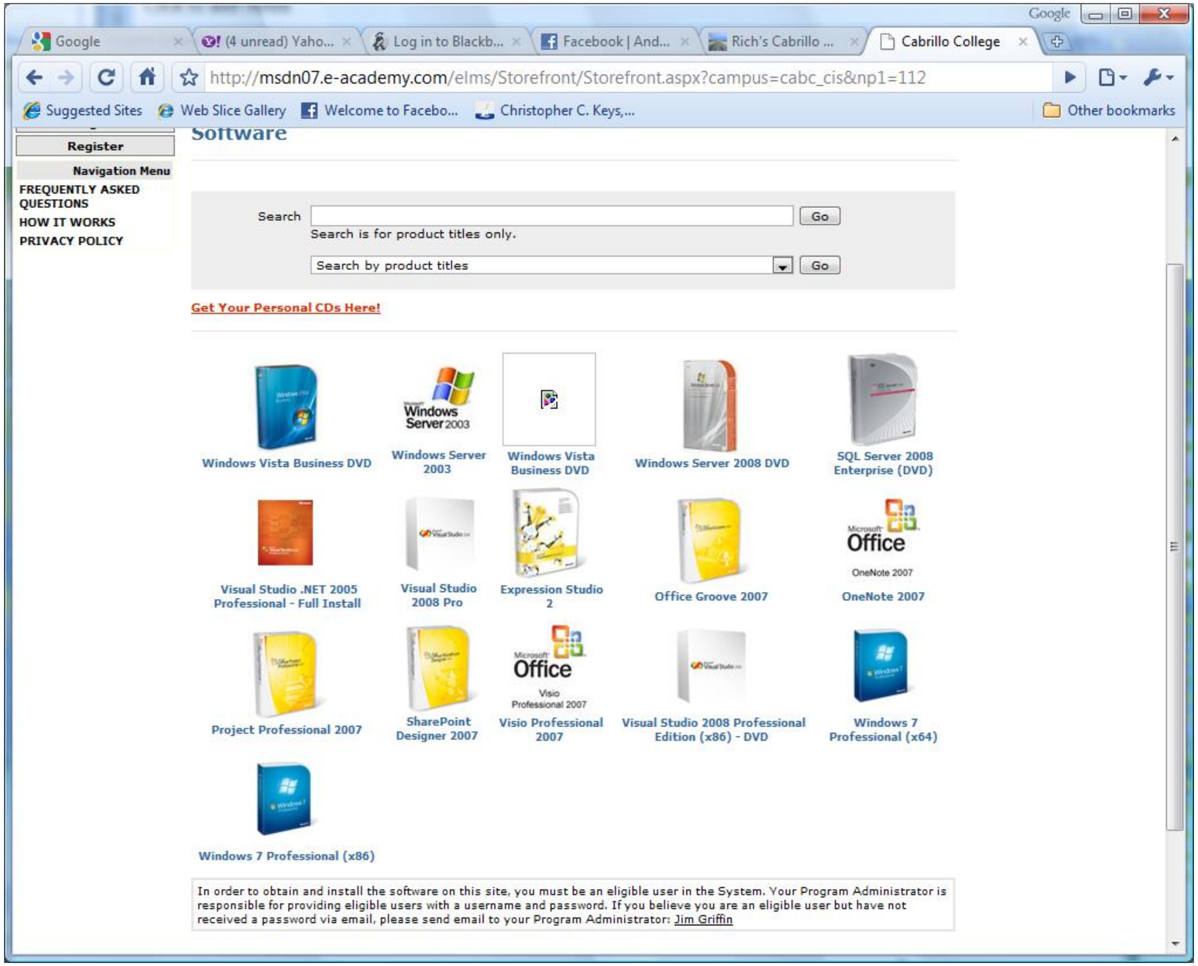
1. Test #2 is **scheduled for our next class!** Same format as before. The test will start during the last hour of class. If you work you can take it later in the day as long as it is completed by 11:59PM.

2. Practice Test #2 will be available after class on Canvas!

3. Work the Practice Test BEFORE the real test begins.

4. The practice test will not be available after the real test starts.

Microsoft Academic Webstore



http://msdn07.e-academy.com/elms/Storefront/Storefront.aspx?campus=cabc_cis&np1=112

Software

Search

Search is for product titles only.

Search by product titles

Get Your Personal CDs Here!

Windows Vista Business DVD | Windows Server 2003 | Windows Vista Business DVD | Windows Server 2008 DVD | SQL Server 2008 Enterprise (DVD)

Visual Studio .NET 2005 Professional - Full Install | Visual Studio 2008 Pro | Expression Studio 2 | Office Groove 2007 | OneNote 2007

Project Professional 2007 | SharePoint Designer 2007 | Visio Professional 2007 | Visual Studio 2008 Professional Edition (x86) - DVD | Windows 7 Professional (x64)

Windows 7 Professional (x86)

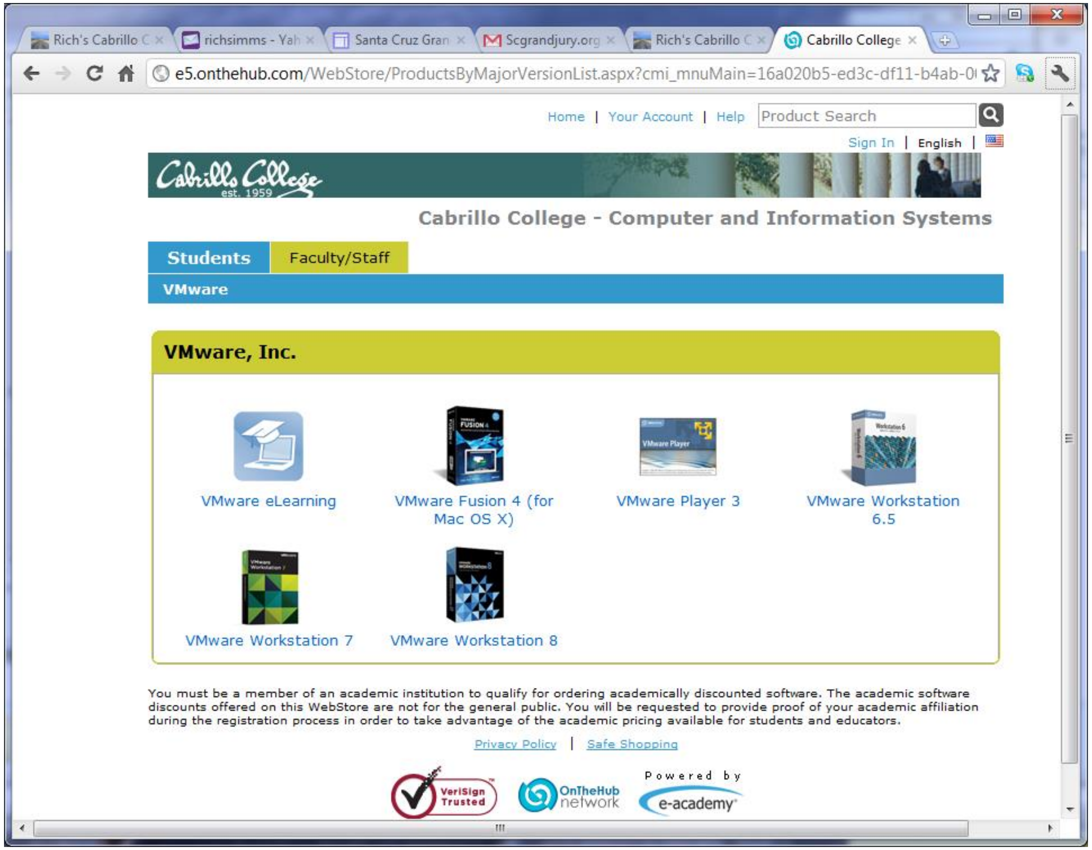
In order to obtain and install the software on this site, you must be an eligible user in the System. Your Program Administrator is responsible for providing eligible users with a username and password. If you believe you are an eligible user but have not received a password via email, please send email to your Program Administrator: Jim Griffin

- 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



e5.onthehub.com/WebStore/ProductsByMajorVersionList.aspx?cmi_mnuMain=16a020b5-ed3c-df11-b4ab-0

Cabrillo College - Computer and Information Systems

VMware, Inc.

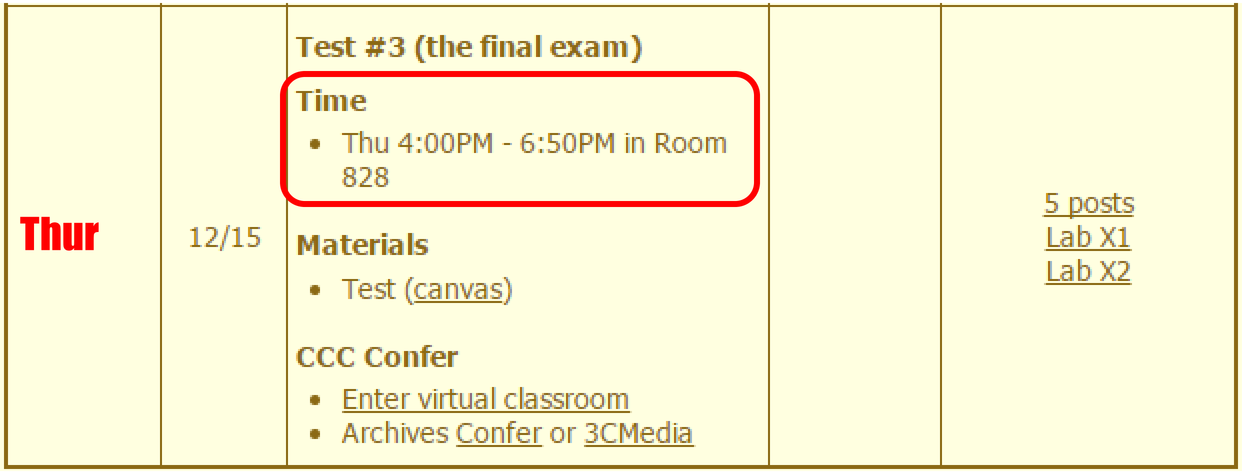
You must be a member of an academic institution to qualify for ordering academically discounted software. The academic software discounts offered on this WebStore are not for the general public. You will be requested to provide proof of your academic affiliation during the registration process in order to take advantage of the academic pricing available for students and educators.

- 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

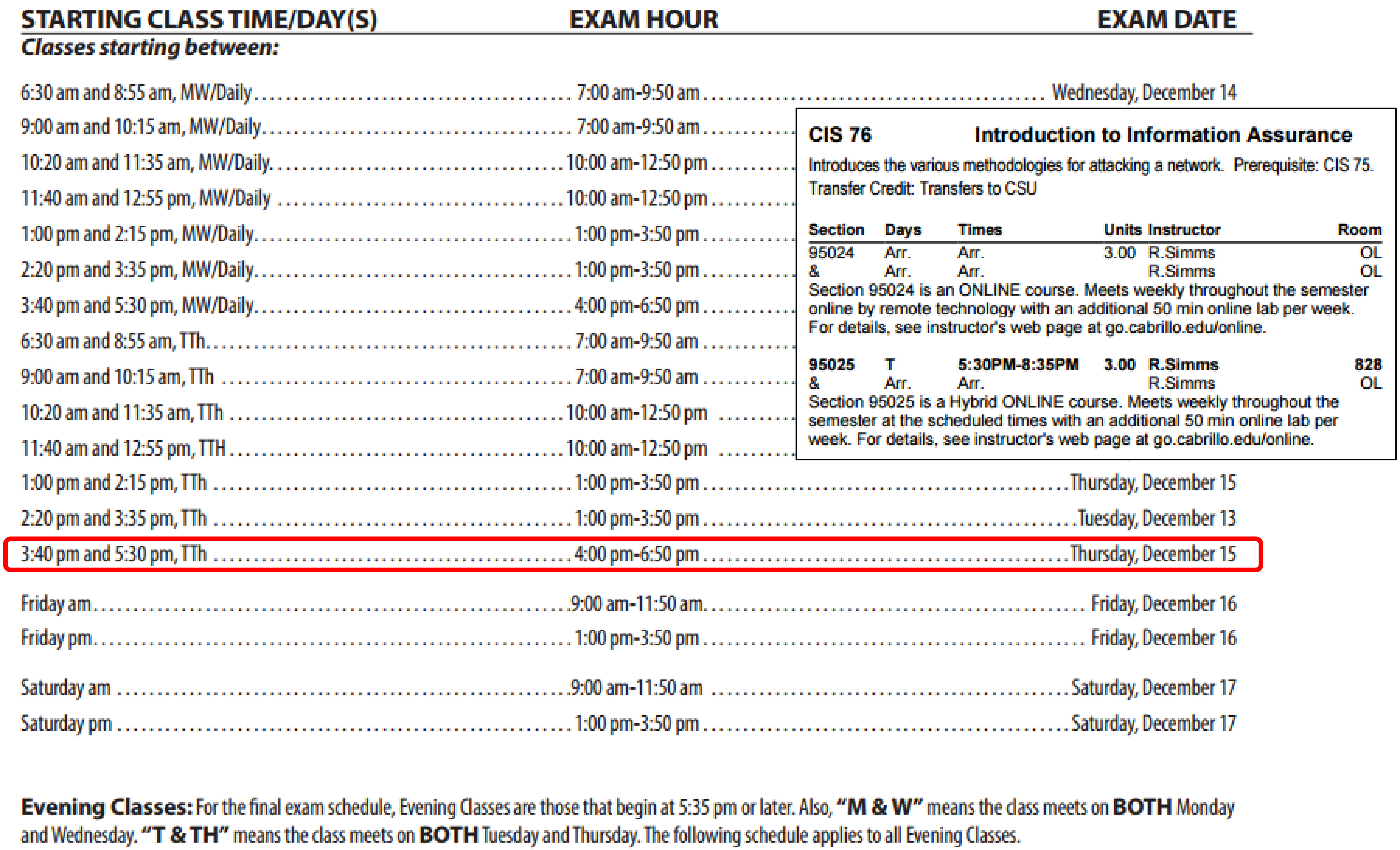
Test #3 (final exam) is THURSDAY Dec 15 4-6:50PM



Thur	12/15	**Test #3 (the final exam)** **Time** • Thu 4:00PM - 6:50PM in Room 828 **Materials** • Test (canvas) **CCC Confer** • Enter virtual classroom • Archives Confer or 3CMedia		5 posts Lab X1 Lab X2

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

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



STARTING CLASS TIME/DAY(S)	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

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.

CIS 76 Introduction to Information Assurance

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

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

Section 95024 is an ONLINE course. Meets weekly throughout the semester online by remote technology with an additional 50 min online lab per week. For details, see instructor's web page at go.cabrillo.edu/online.

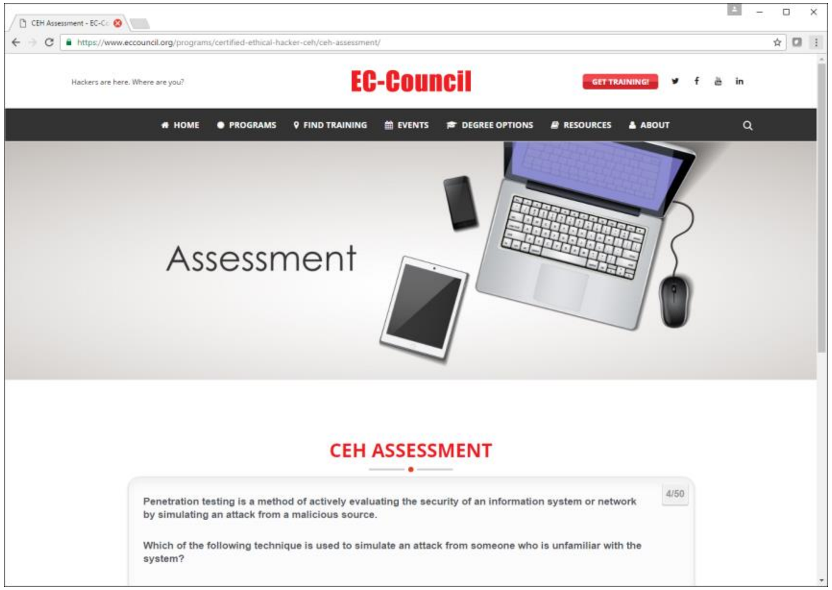
Section	Days	Times	Units	Instructor	Room
95025	**T**	**5:30PM-8:35PM**	**3.00**	**R.Simms**	**828**
&	Arr.	Arr.		R.Simms	OL

Section 95025 is a Hybrid ONLINE course. Meets weekly throughout the semester at the scheduled times with an additional 50 min online lab per week. For details, see instructor's web page at go.cabrillo.edu/online.

EC-Council Mini CEH Assessment (2nd Attempt)

EC-Council Mini-Assessment Q11-20

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

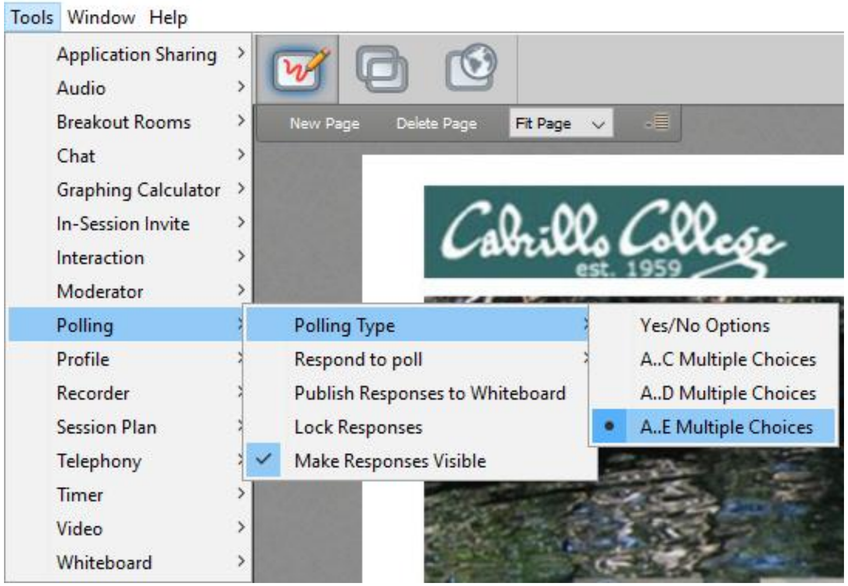


CEH ASSESSMENT

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.

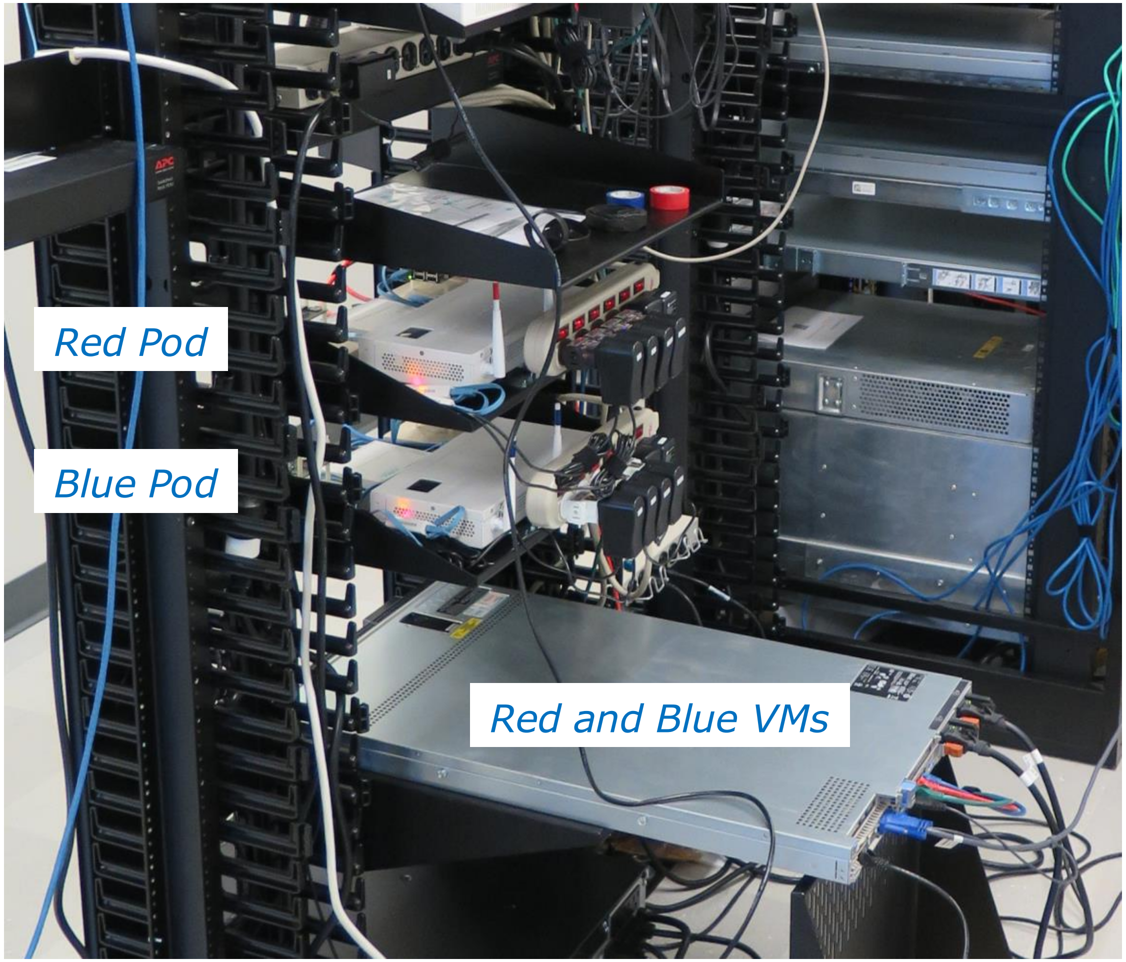
Which of the following technique is used to simulate an attack from someone who is unfamiliar with the system?



Questions 11-20 (five minutes)

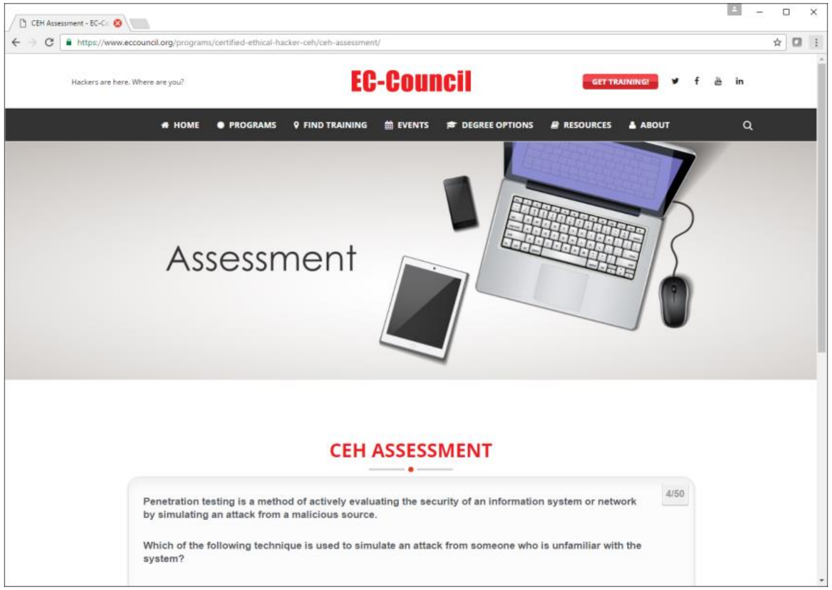
Red and Blue Pods

Red and Blue Pods in Microlab Lab Rack



EC-Council Mini-Assessment Q21-30

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

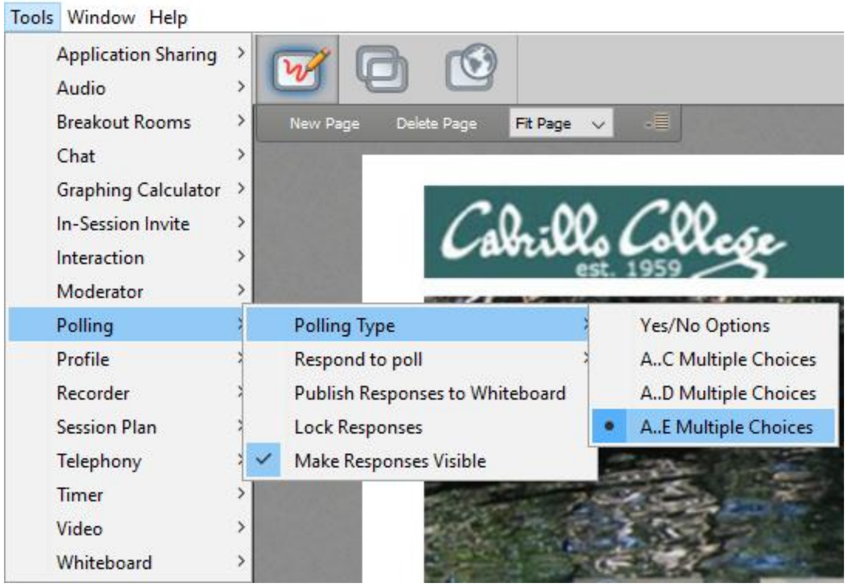


CEH ASSESSMENT

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?



Questions 21-30 (five minutes)

Domain 3

NISGTC

The National Information, Security & Geospatial Technologies Consortium

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

NISGTC

The National Information, Security & Geospatial Technologies Consortium

© 2013 NISGTC

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

© 2013 NISGTC

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

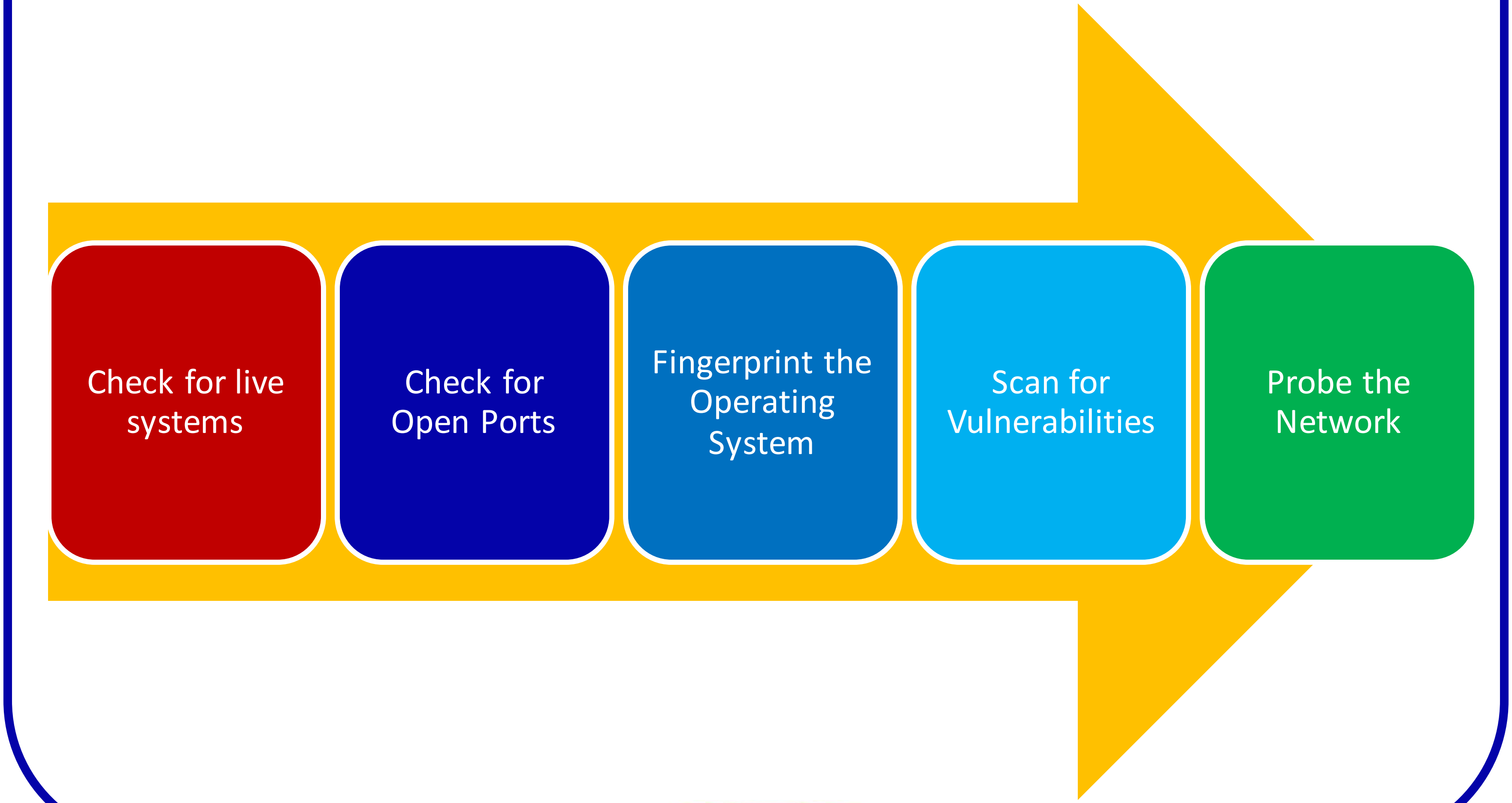
© 2013 NISGTC

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

© 2013 NISGTC

Scanning Methodology


Check for live systems

Check for Open Ports

Fingerprint the Operating System

Scan for Vulnerabilities

Probe the Network

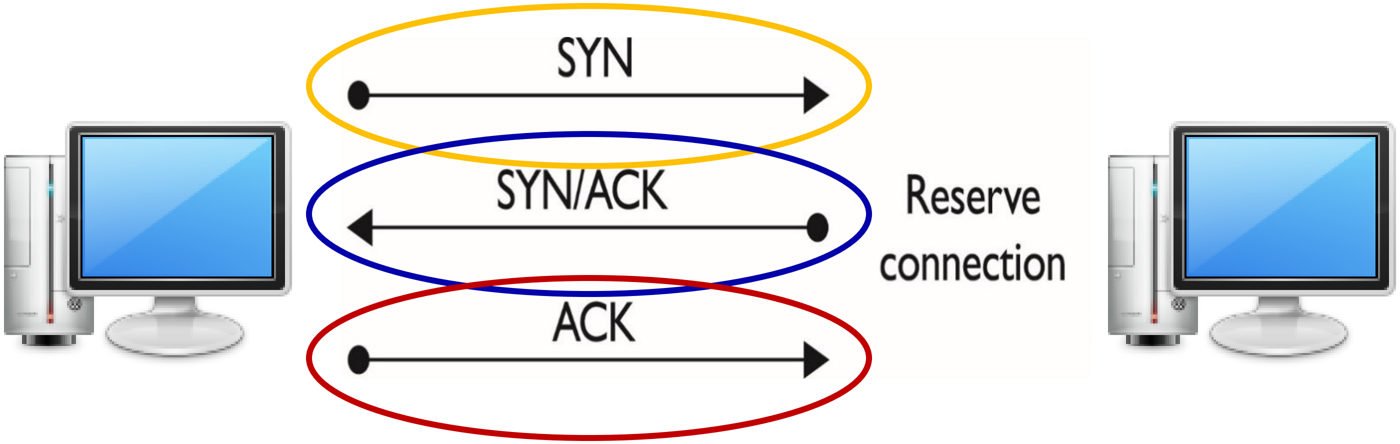
© 2013 NISGTC

Three Way Handshake

System 1 sends SYN packet to System 2

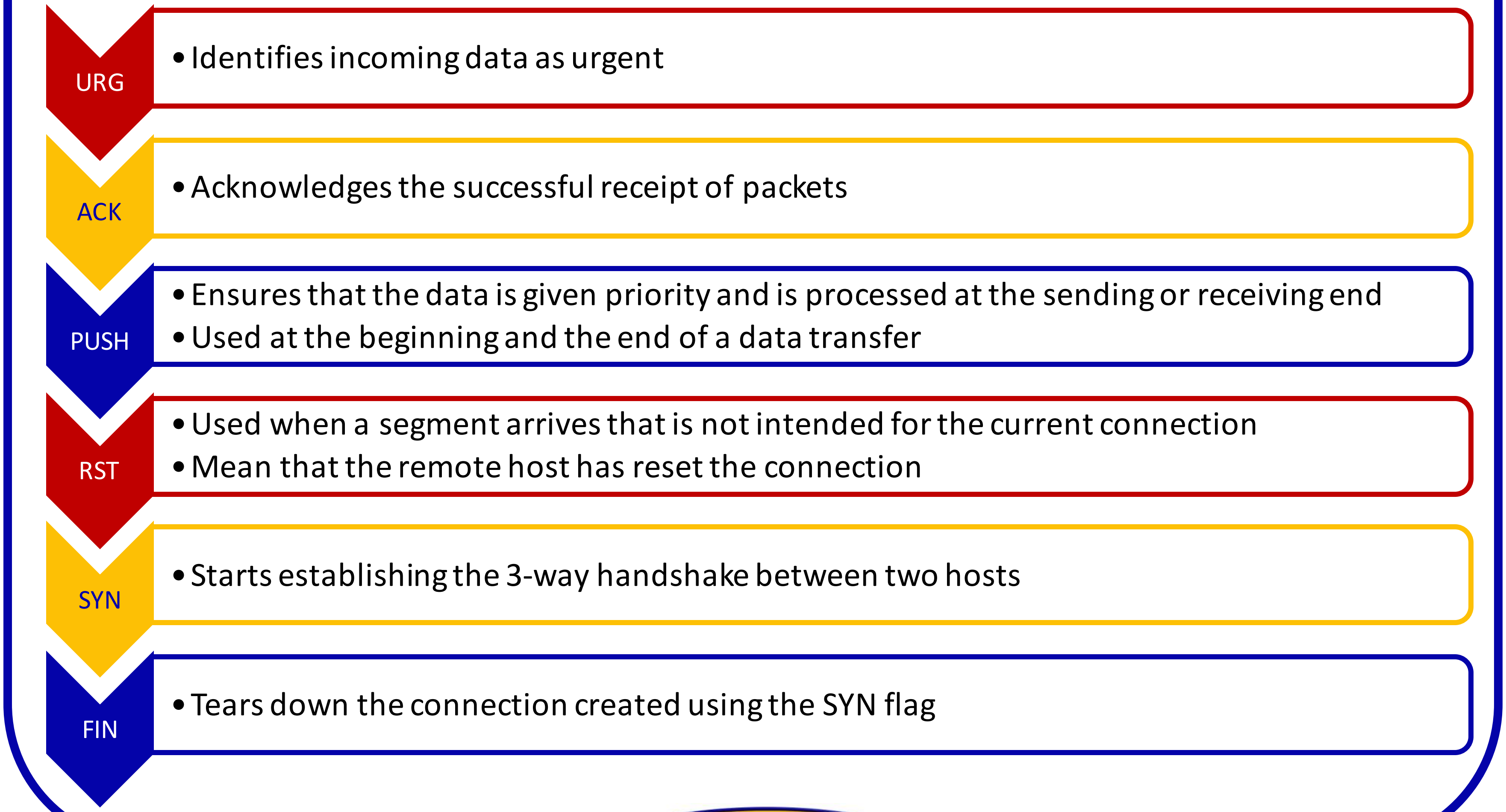
System 2 responds with SYN/ACK packet

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



© 2012 NISGTC

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

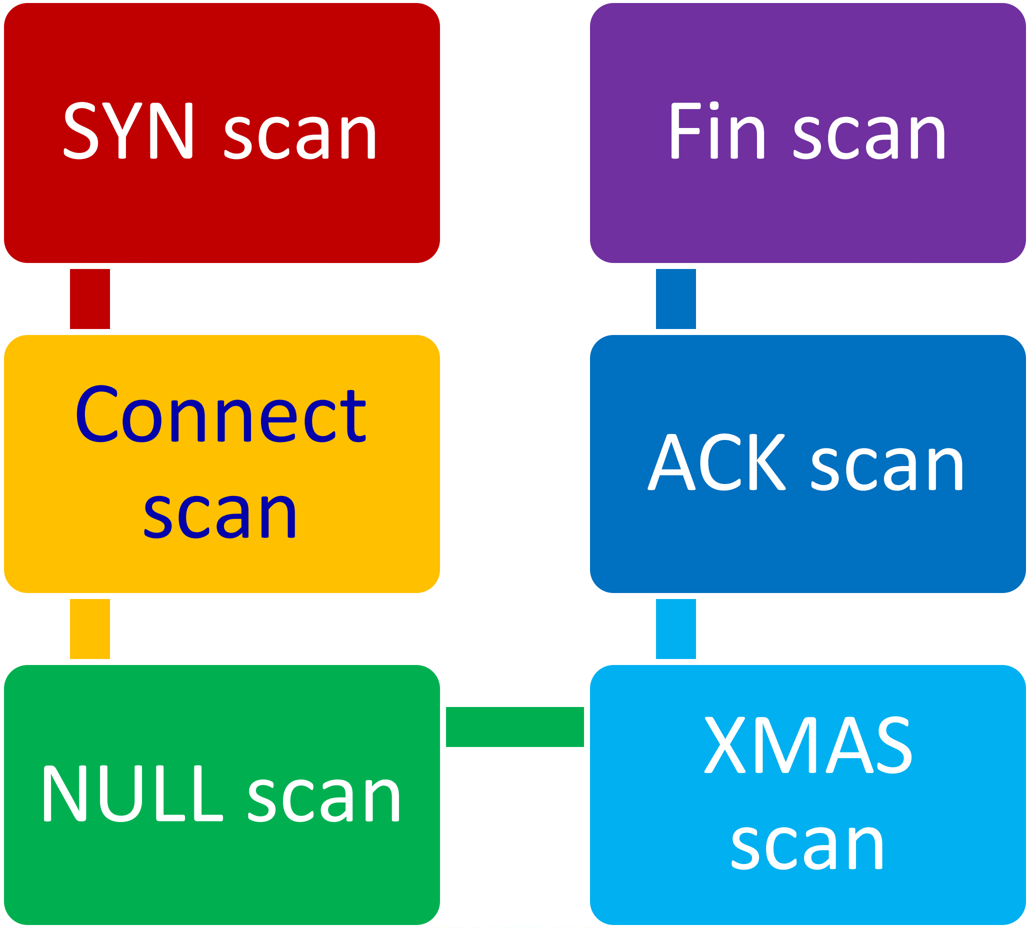
- Starts establishing the 3-way handshake between two hosts

FIN

- Tears down the connection created using the SYN flag

© 2013 NISGTC

Types of Port Scans



SYN scan

Connect scan

NULL scan

Fin scan

ACK scan

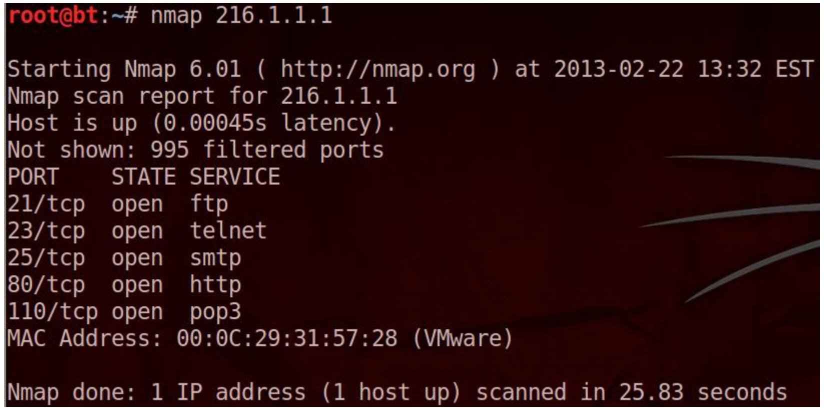
XMAS scan

© 2013 NISGTC

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

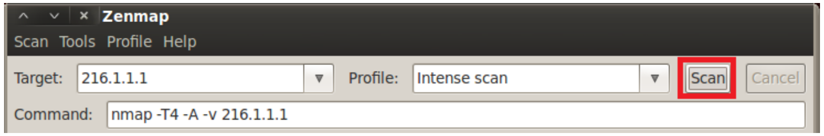


```
root@bt:~# nmap 216.1.1.1

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
```

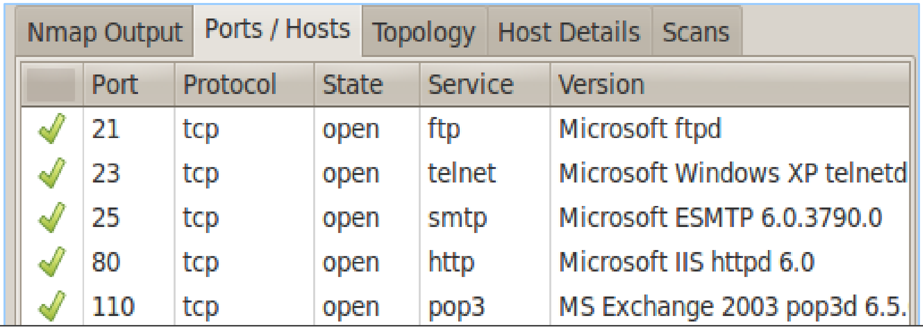
© 2013 NISGTC

Zenmap

Zenmap is the GUI front end for nmap

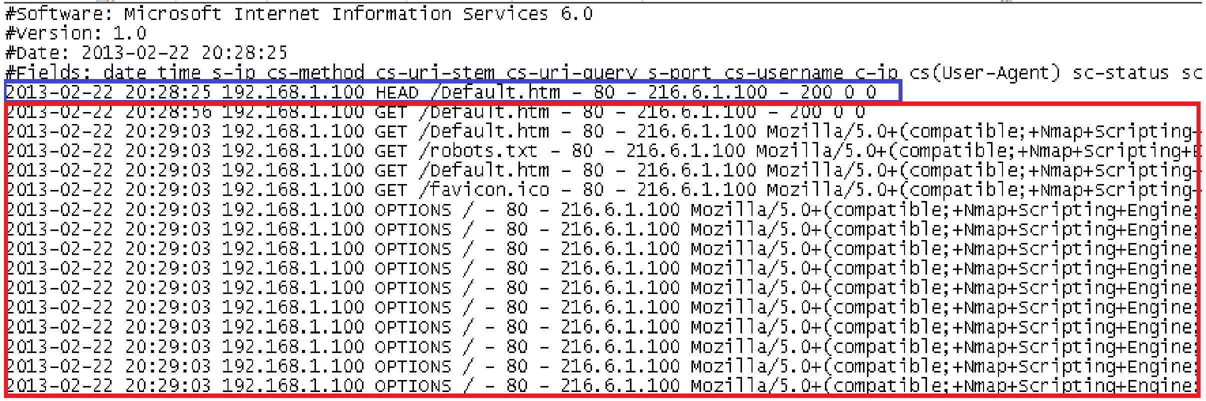


Target: 216.1.1.1
Profile: Intense scan
Command: nmap -T4 -A -v 216.1.1.1



	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+E
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

© 2013 NISGTC

Crafting Packets

Fping

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

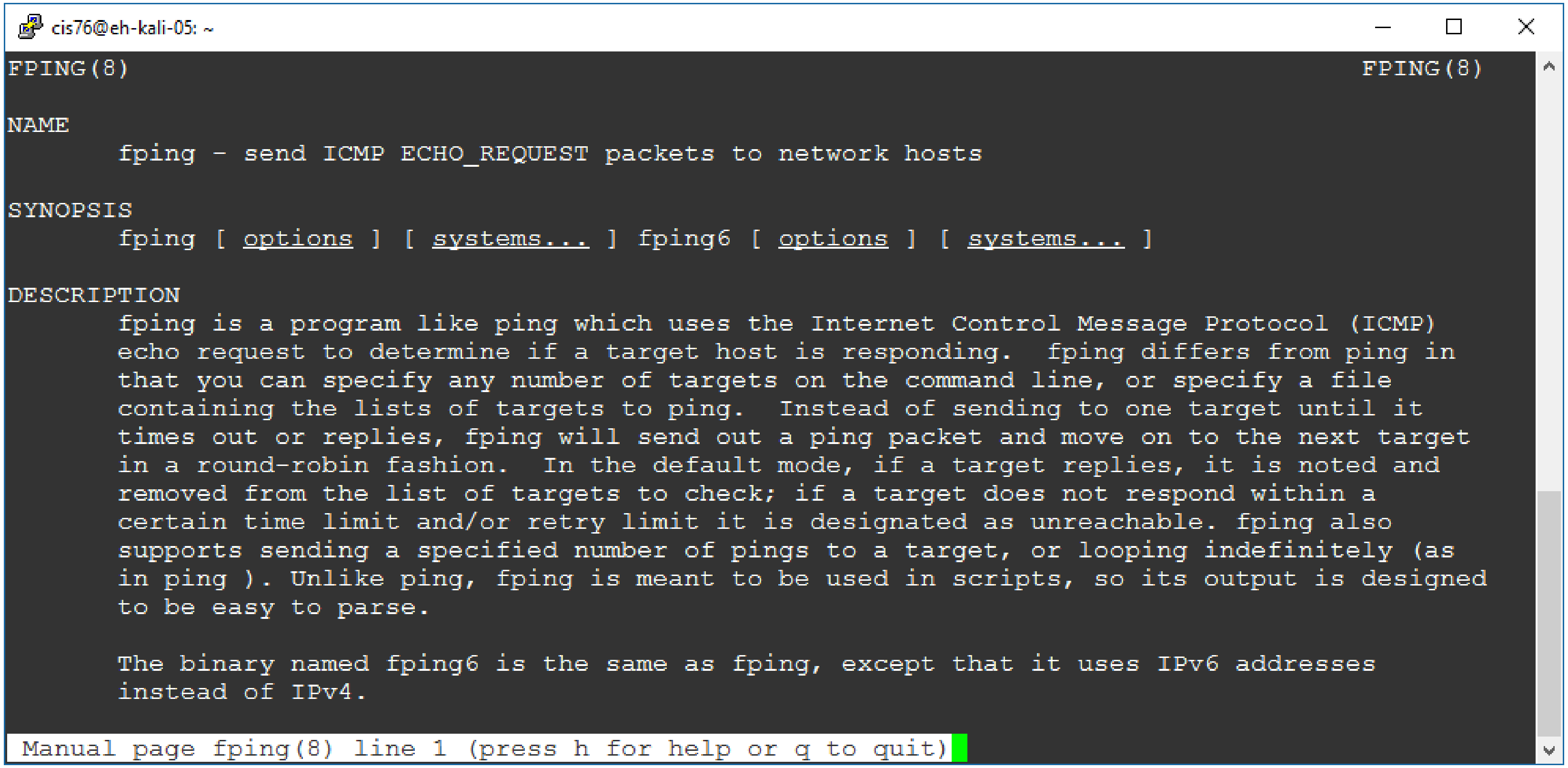
Hping

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

© 2013 NISGTC

fping

man fping

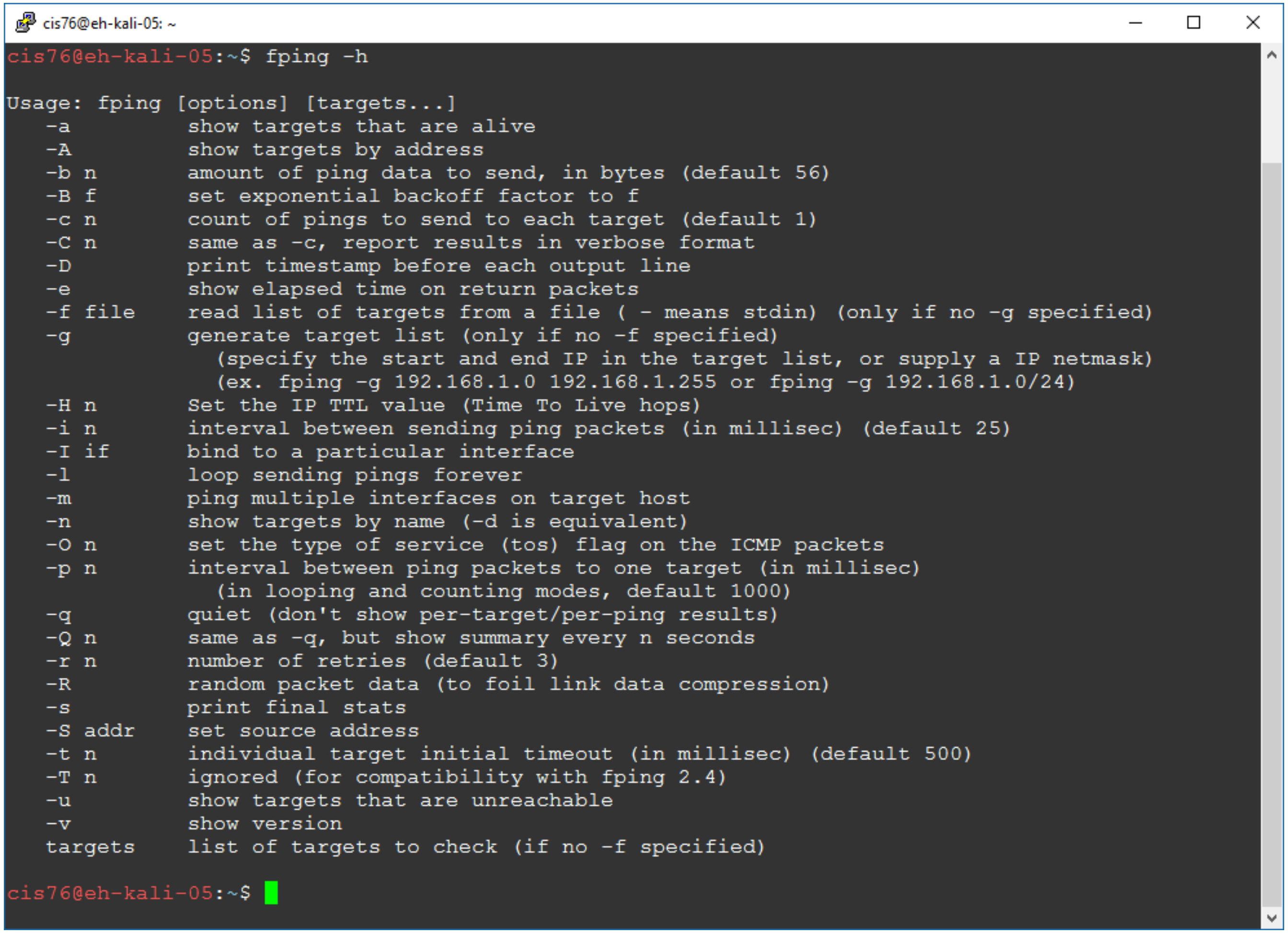


```
FPING(8)                                                                                    FPING(8)

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

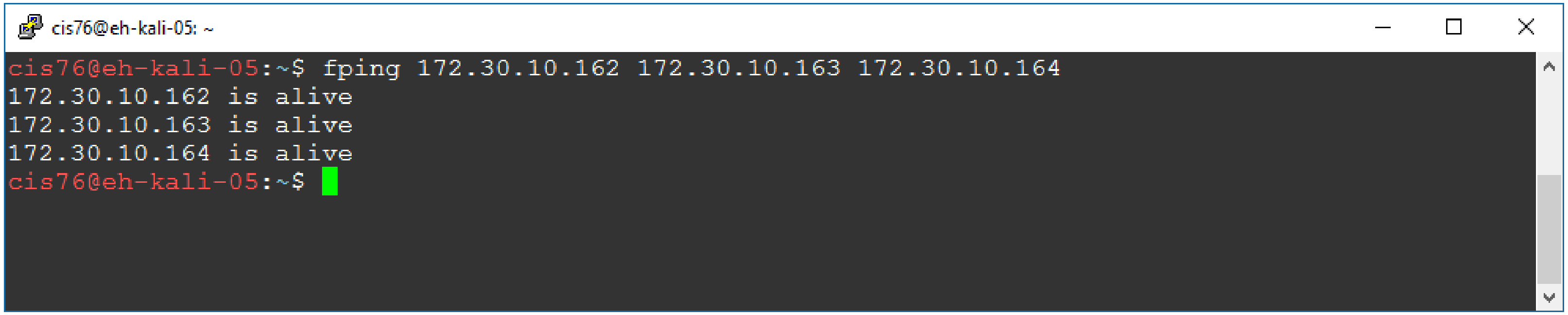
fping -h



```
cis76@eh-kali-05:~$ 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`

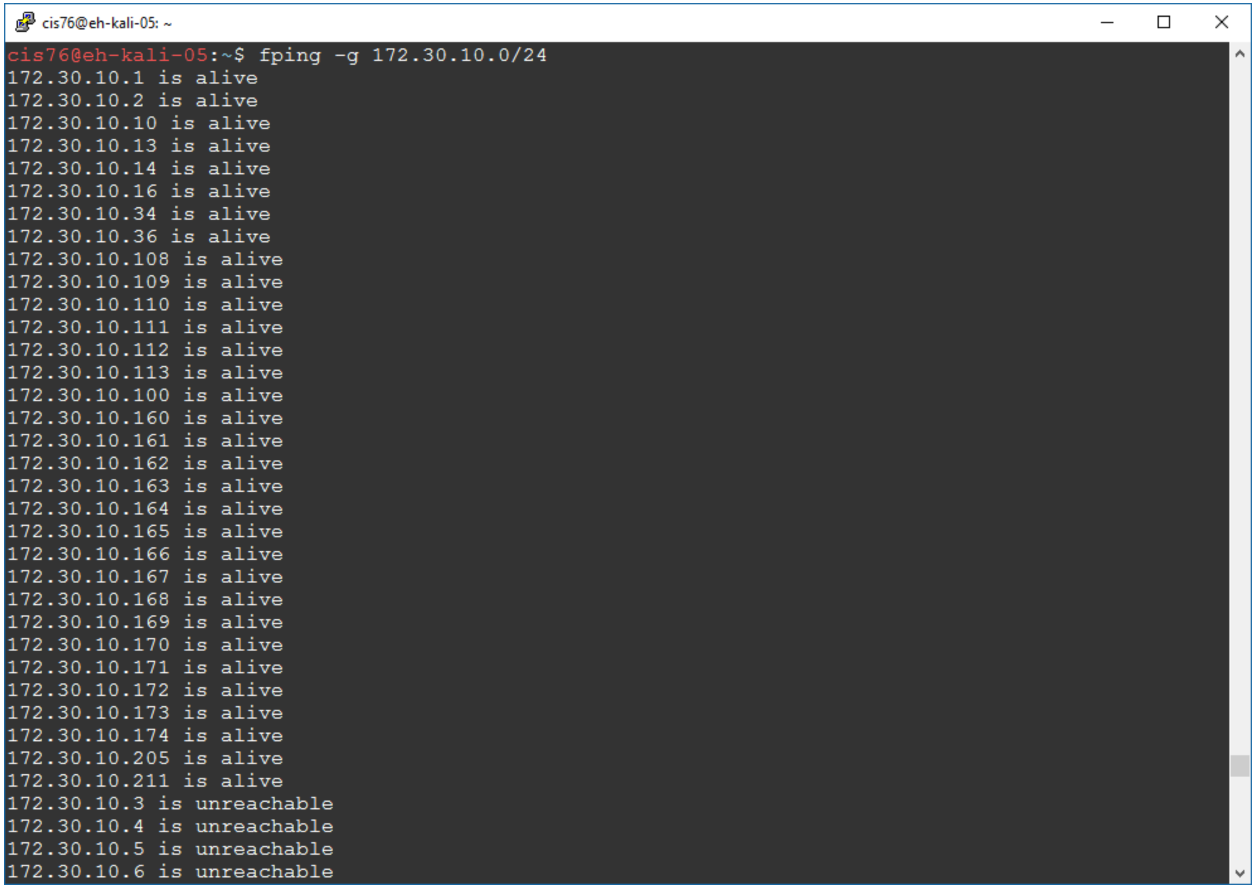


```
cis76@eh-kali-05:~$ fping 172.30.10.162 172.30.10.163 172.30.10.164
172.30.10.162 is alive
172.30.10.163 is alive
172.30.10.164 is alive
cis76@eh-kali-05:~$
```

Multiple targets

fping

`fping -g 172.30.10.0/24`

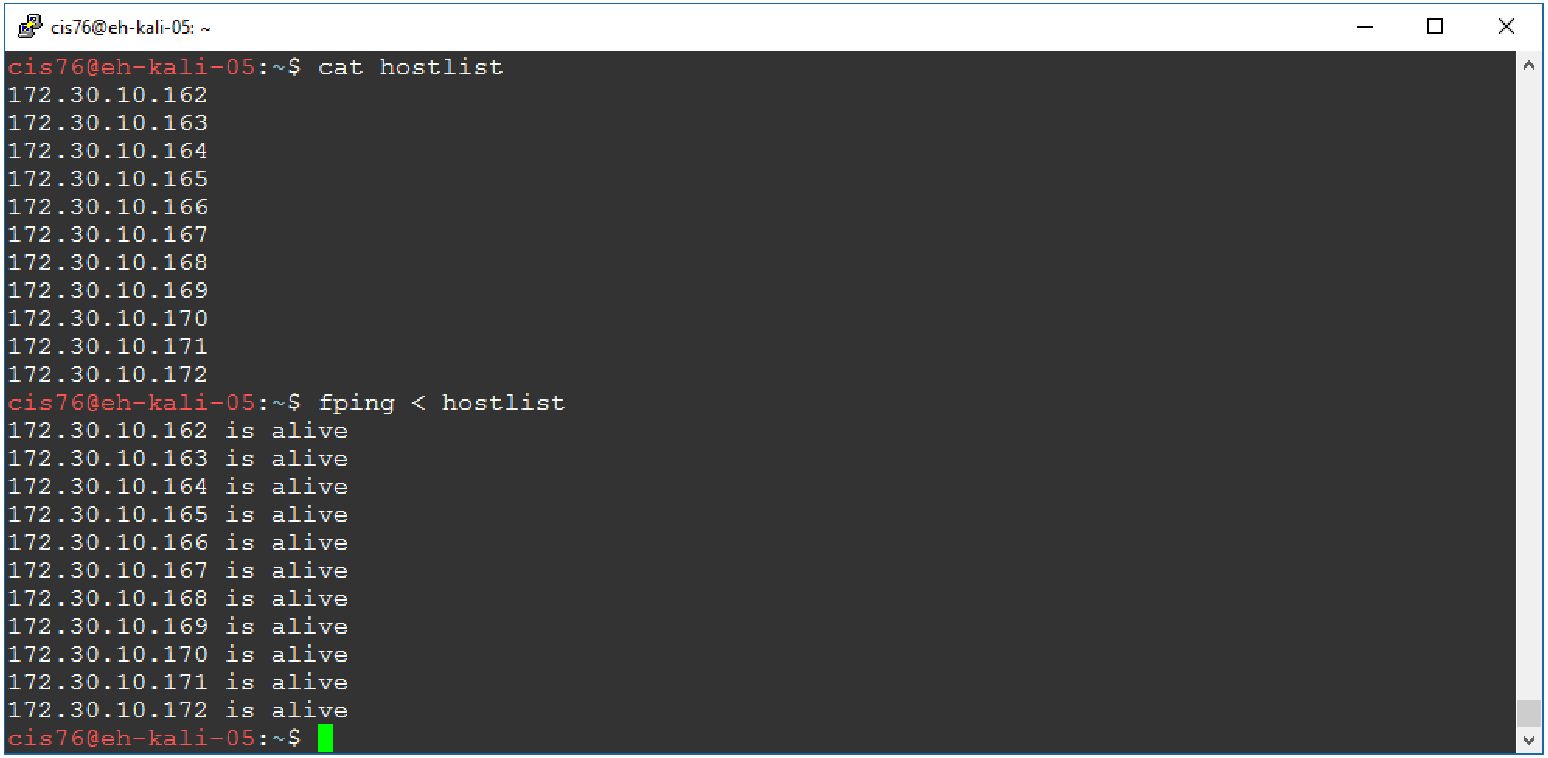


```
cis76@eh-kali-05:~$ fping -g 172.30.10.0/24
172.30.10.1 is alive
172.30.10.2 is alive
172.30.10.10 is alive
172.30.10.13 is alive
172.30.10.14 is alive
172.30.10.16 is alive
172.30.10.34 is alive
172.30.10.36 is alive
172.30.10.108 is alive
172.30.10.109 is alive
172.30.10.110 is alive
172.30.10.111 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:~$ 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

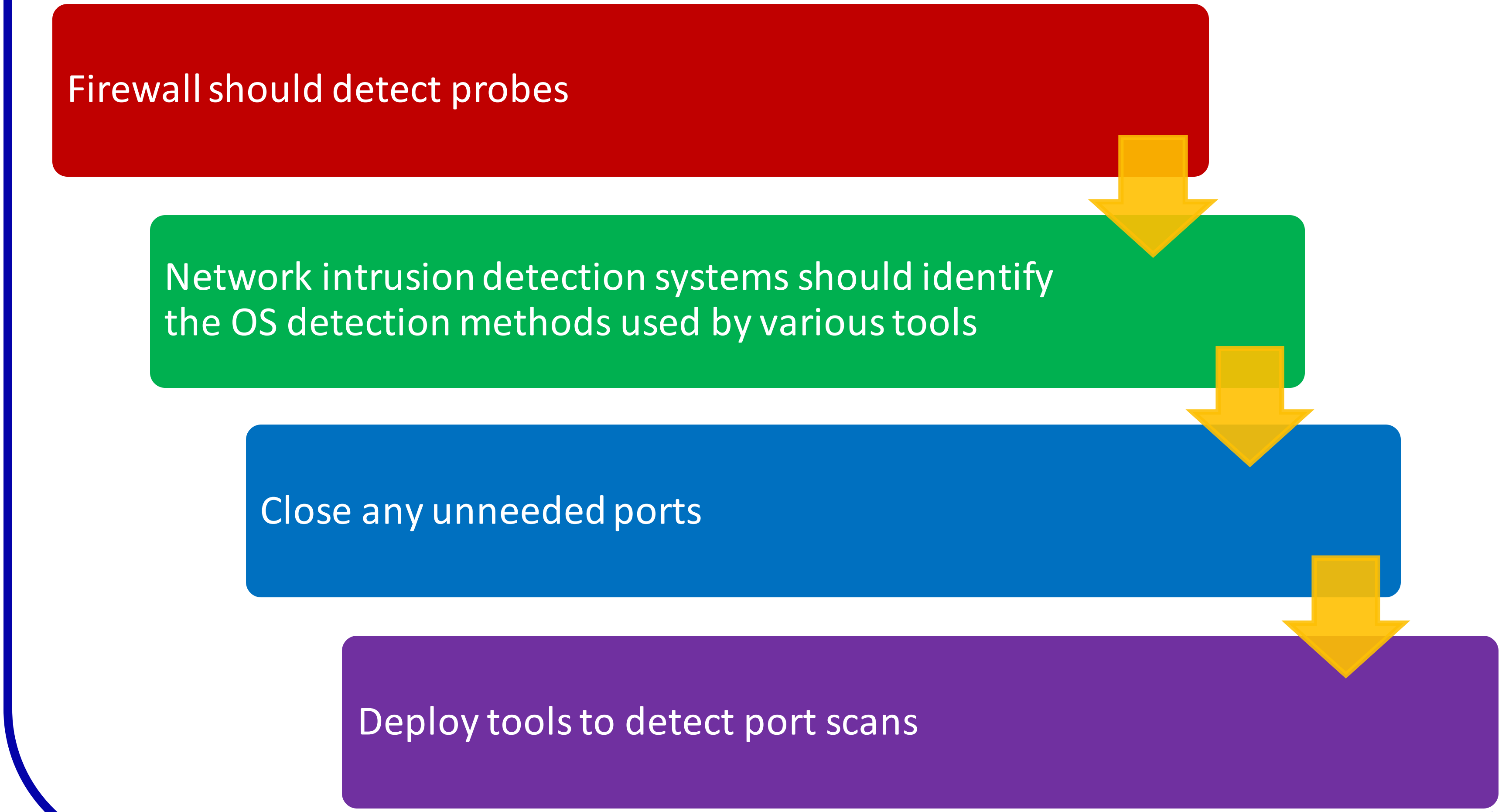
Activty

Try this command from your EH-Kali VM:

```
echo 172.30.10.{1,2,10,13,14} | 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

NISGTC

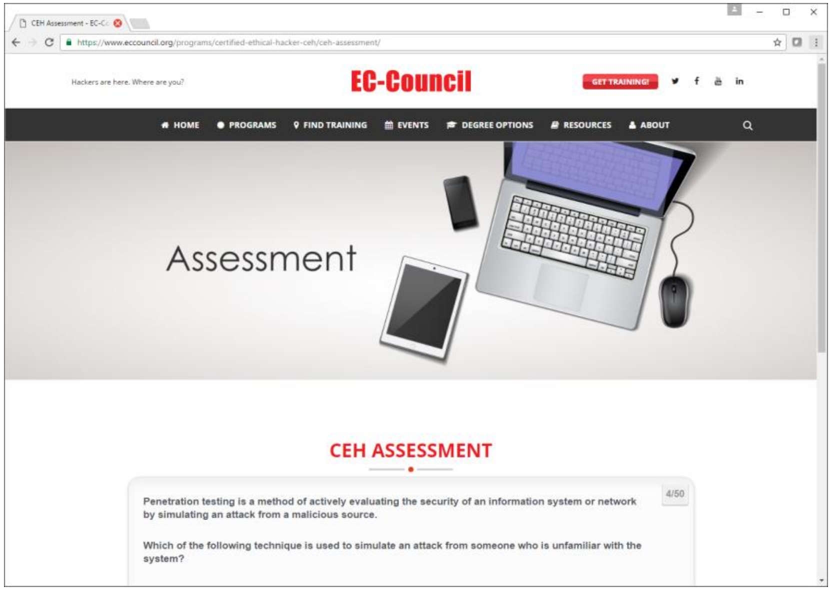
The National Information, Security & Geospatial Technologies Consortium

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)

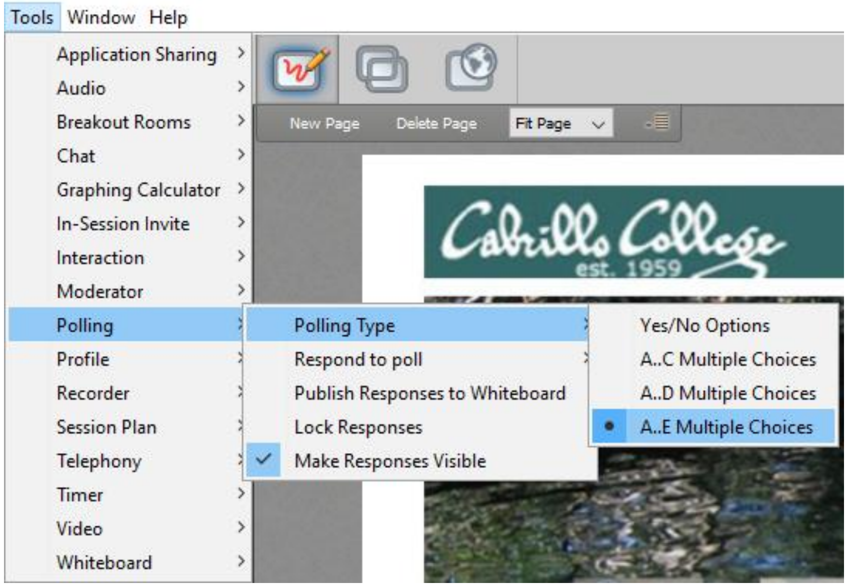
EC-Council Mini-Assessment Q31-40

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



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?



Questions 31-40 (five minutes)

Domain 4

NISGTC

The National Information, Security & Geospatial Technologies Consortium

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

NISGTC

The National Information, Security & Geospatial Technologies Consortium

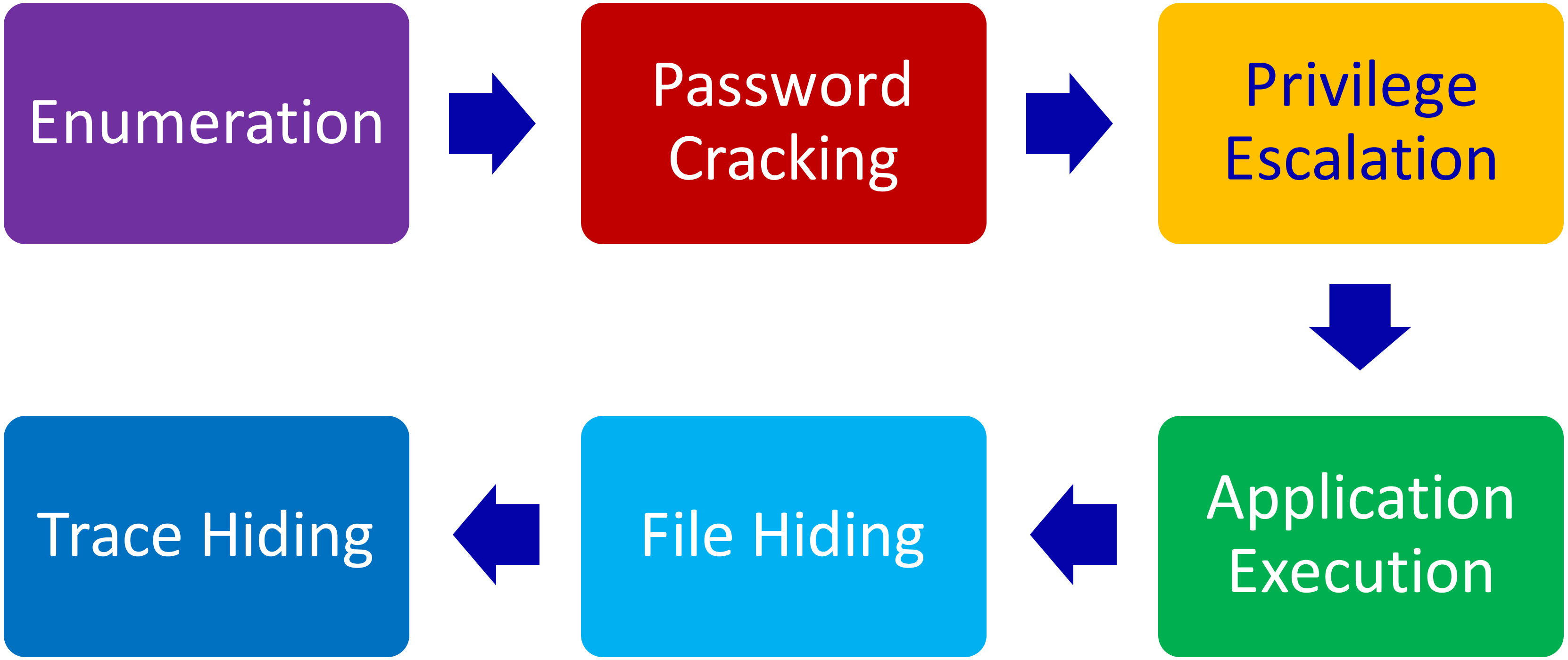
© 2013 NISGTC

Objectives

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

© 2013 NISGTC

Steps to Compromise a System



Enumeration

Password Cracking

Privilege Escalation

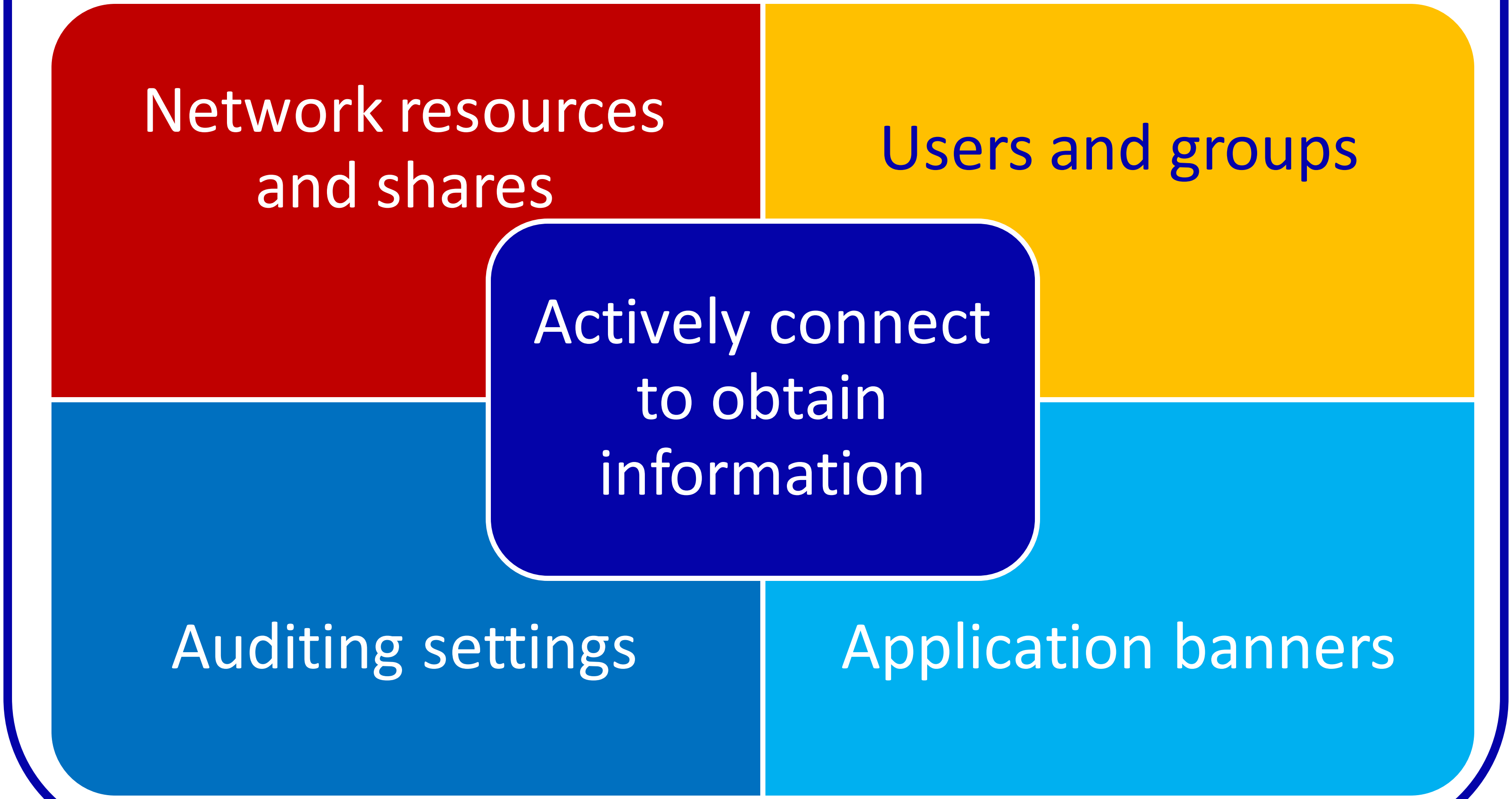
Application Execution

File Hiding

Trace Hiding

© 2013 NISGTC

Enumeration



Actively connect to obtain information

Network resources and shares

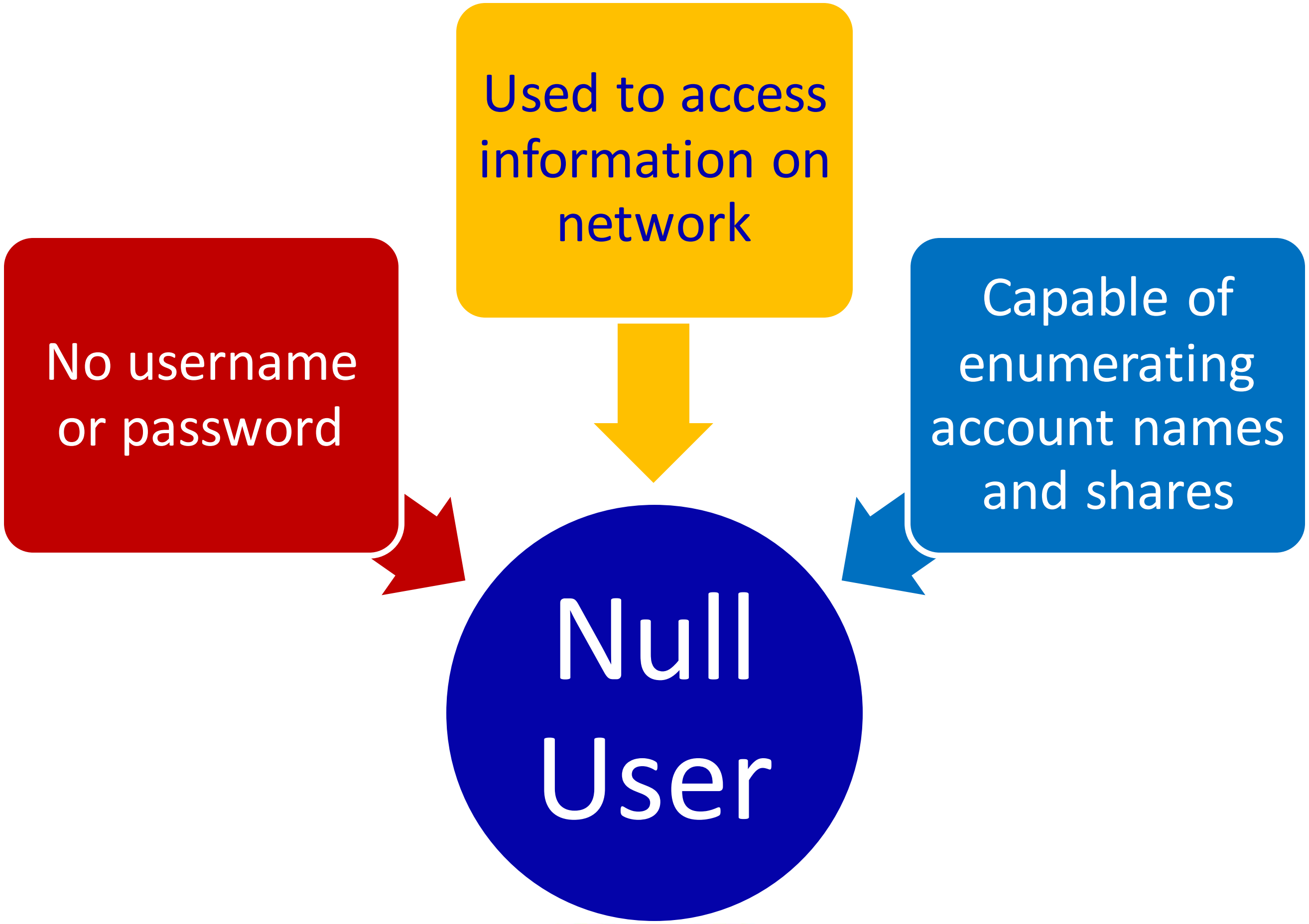
Users and groups

Auditing settings

Application banners

© 2013 NISGTC

Null Session Enumeration



Used to access information on network

No username or password

Capable of enumerating account names and shares

Null User

© 2013 NISGTC

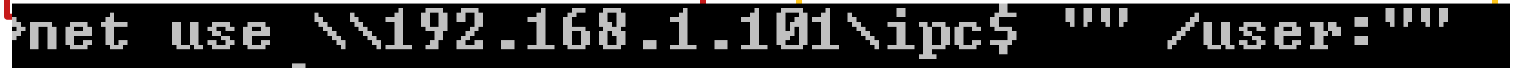
Null Sessions

Enumeration Techniques

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

Countermeasures

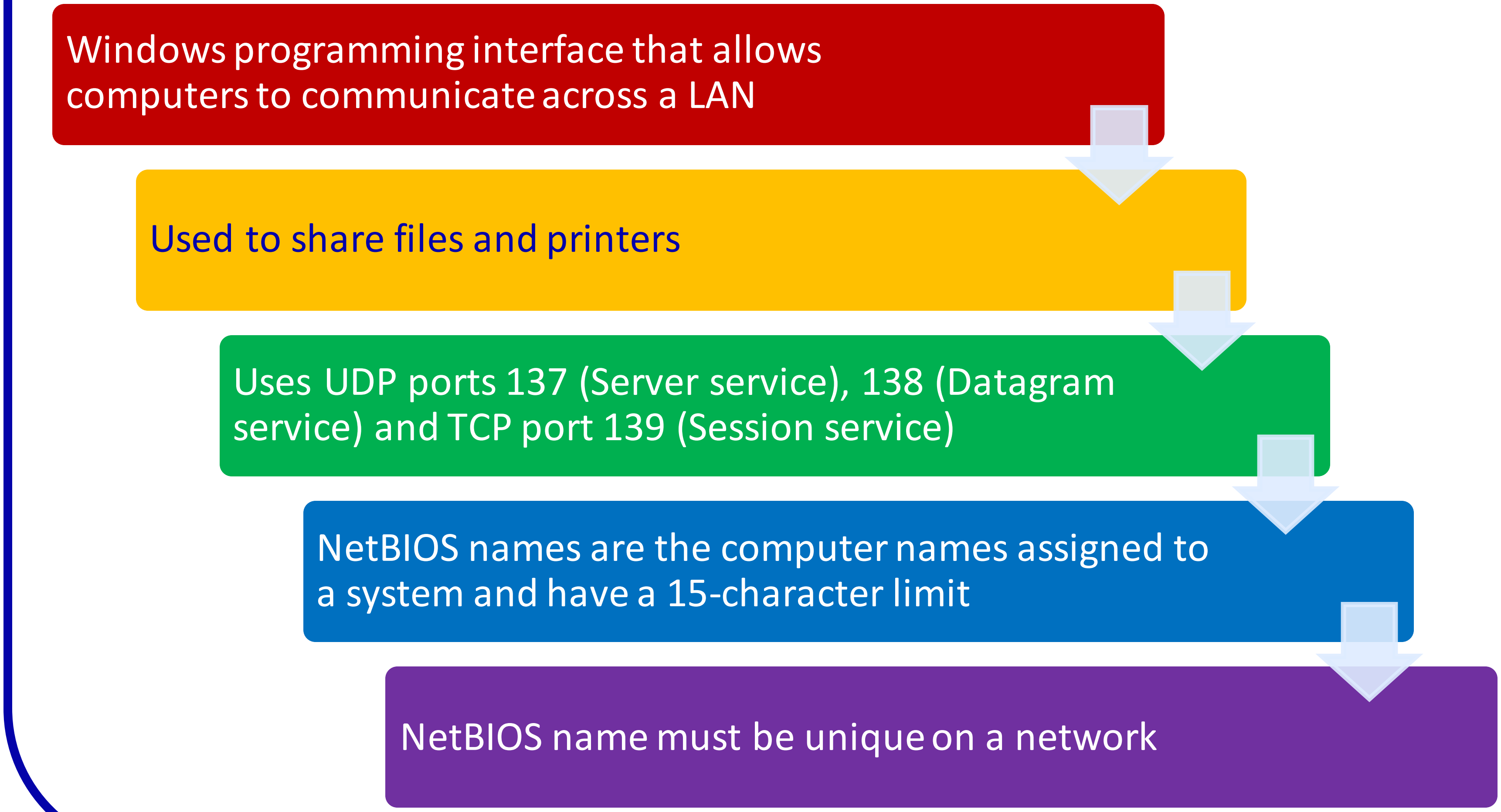
- Filter ports
- Disable SMB service
- Inspect HKLM
- Configure security policy
- Restrict remote access



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

© 2012 NISGTC

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

© 2013 NISGTC

Command Line Tools

netstat

- Displays network connections, routing tables and network protocol statistics

nbstat

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

© 2013 NISGTC

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

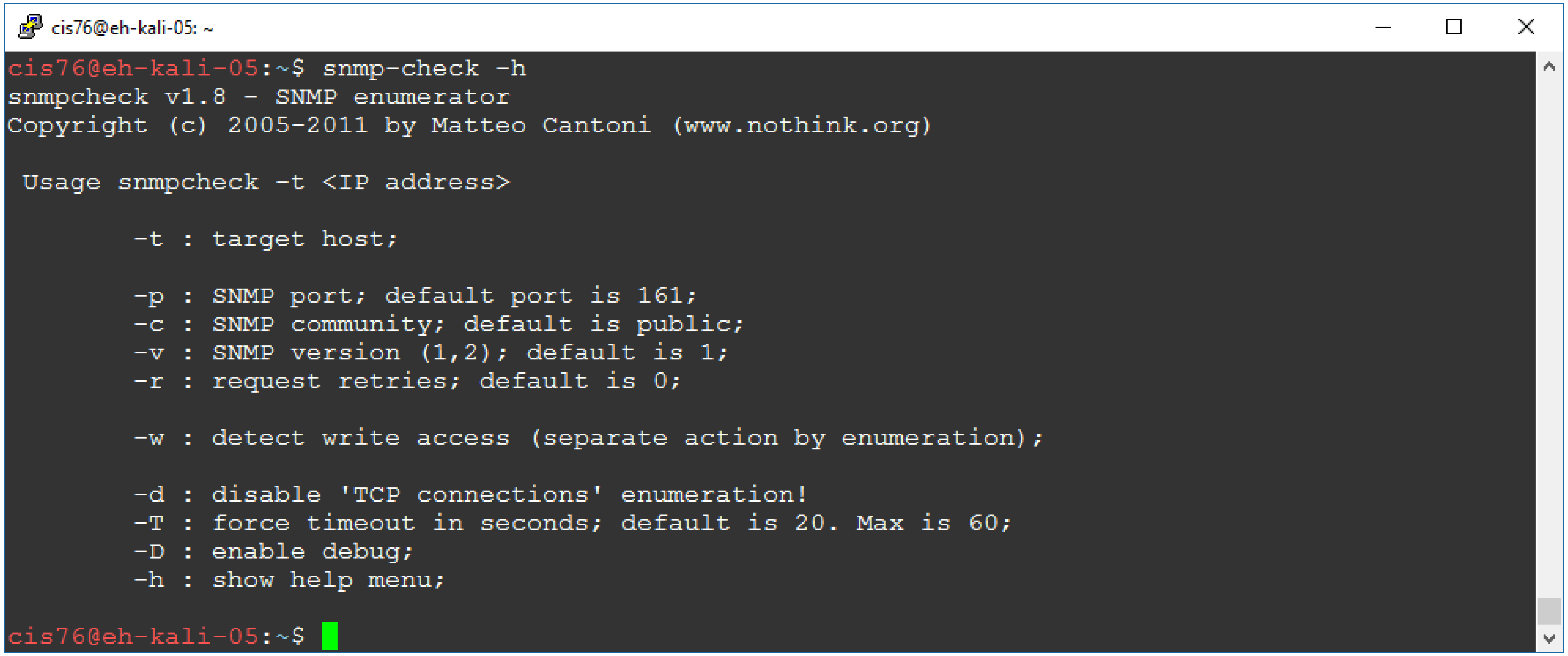
Attacker looks for target host with SNMP enabled and a default community string

Built-in SNMP objects will be visible for enumeration

© 2013 NISGTC

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 -t 172.30.10.162
```

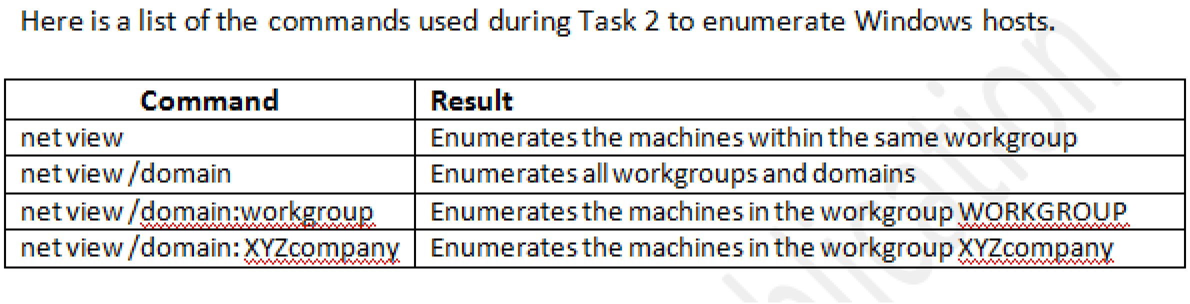
Check the Software Components section of the output. Is VMware Tools installed? Write your answer in the chat window.

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

© 2013 NISGTC

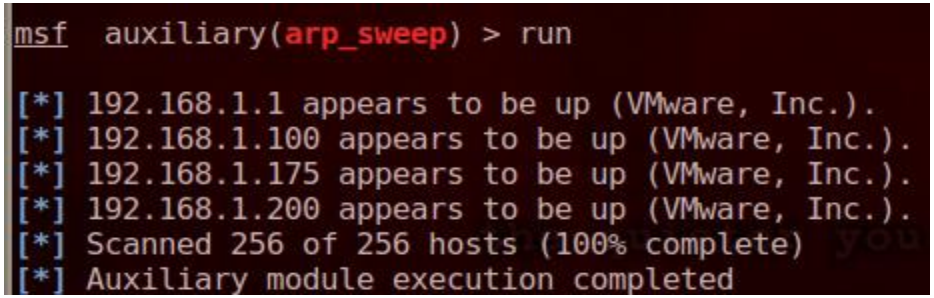
Discovering Hosts with Windows Command Line Tools



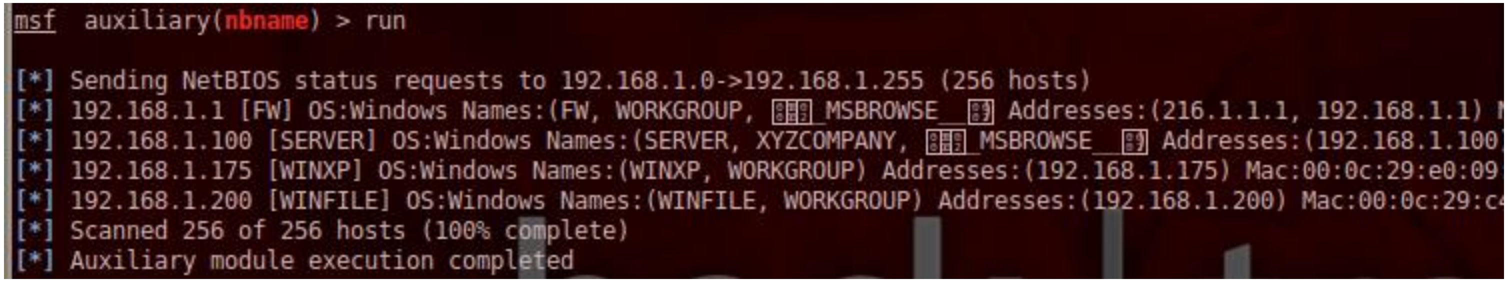
Here is a list of the commands used during Task 2 to enumerate Windows hosts.

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

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
```

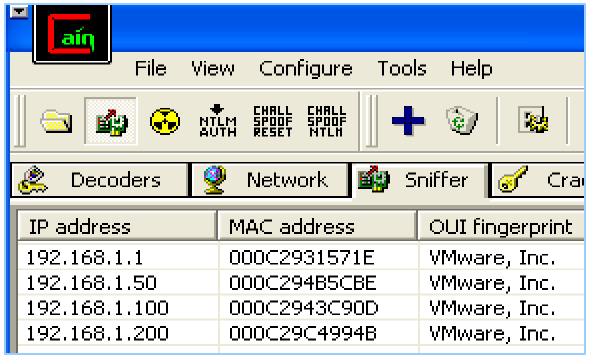


```
msf  auxiliary(nbname) > run

[*] 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:c
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
```

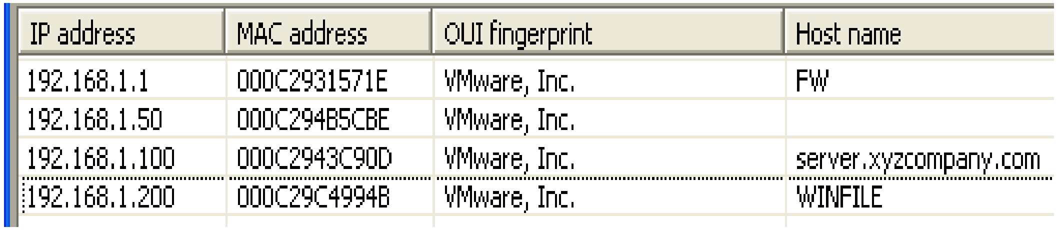
NISGTC
The National Information, Security & Geospatial Technologies Consortium

© 2013 NISGTC

Using Cain



IP address	MAC address	OUI fingerprint
192.168.1.1	000C2931571E	VMware, Inc.
192.168.1.50	000C294B5CBE	VMware, Inc.
192.168.1.100	000C2943C90D	VMware, Inc.
192.168.1.200	000C29C4994B	VMware, Inc.



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

NISGTC

The National Information, Security & Geospatial Technologies Consortium

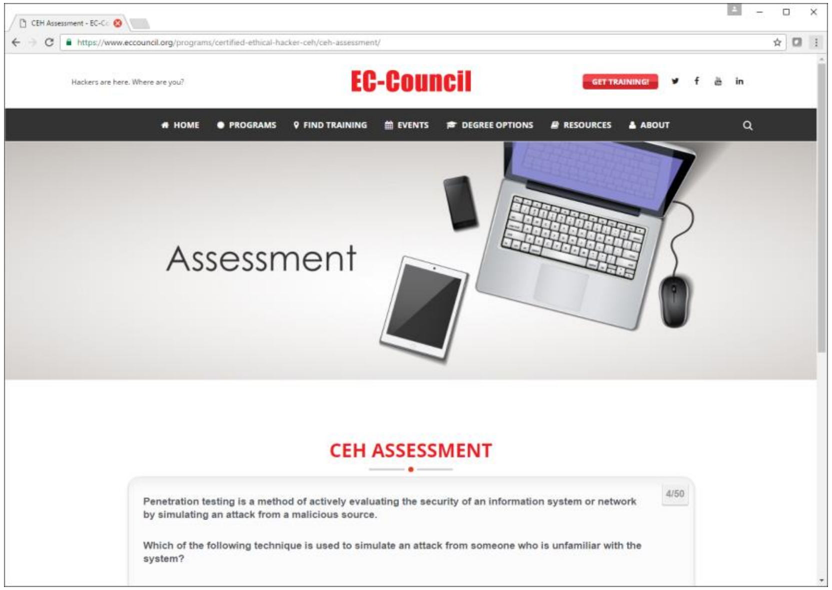
This workforce solution was funded by a grant awarded by the U.S. Department of Labor’s Employment and Training Administration. The solution was created by the grantee and does not necessarily reflect the official position of the U.S. Department of Labor. The Department of Labor makes no guarantees, 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.

© 2013 NISGTC

EC-Council Mini CEH Assessment (2nd Attempt)

EC-Council Mini-Assessment Q41-50

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

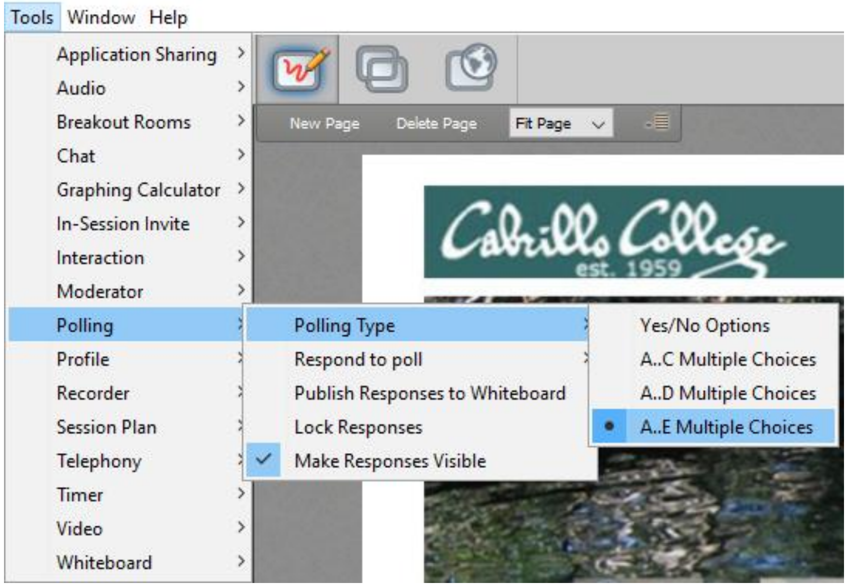


CEH ASSESSMENT

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?



Questions 41-50 (five minutes)

Domain 10

NISGTC

The National Information, Security & Geospatial Technologies Consortium

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

NISGTC

The National Information, Security & Geospatial Technologies Consortium

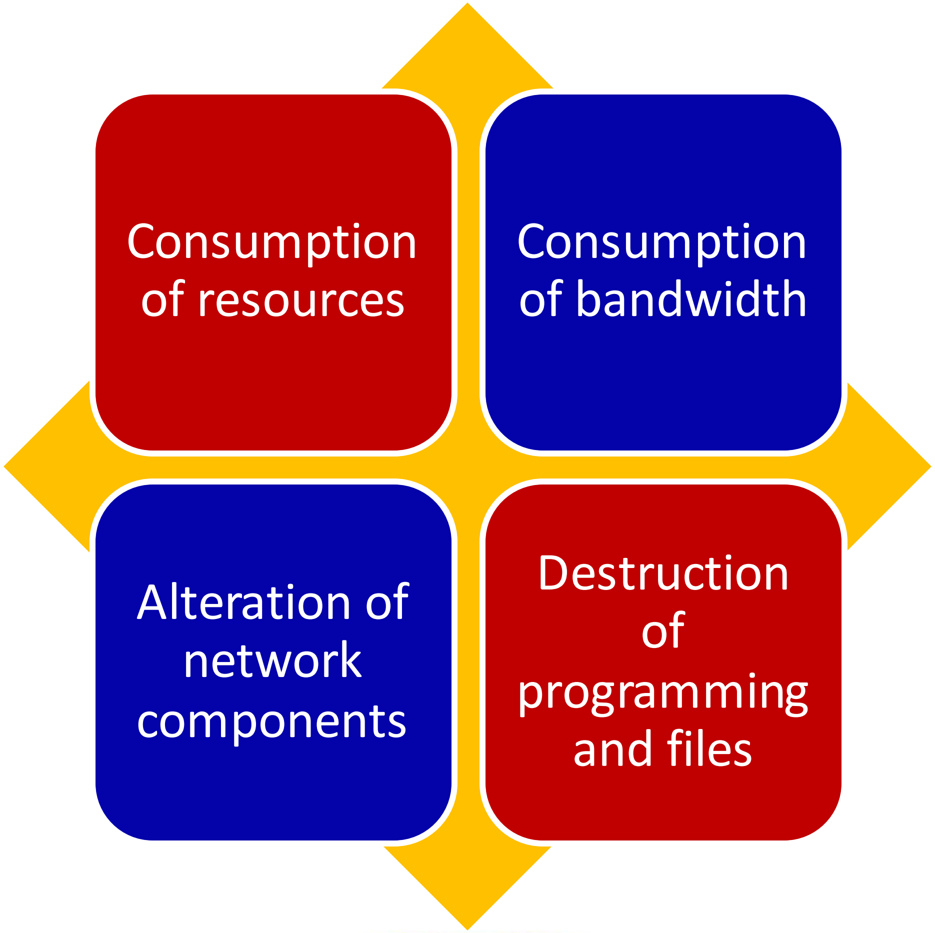
© 2013 NISGTC

Objectives

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

© 2013 NISGTC

Denial-of-Service Attack



Consumption of resources

Consumption of bandwidth

Alteration of network components

Destruction of programming and files

© 2013 NISGTC

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

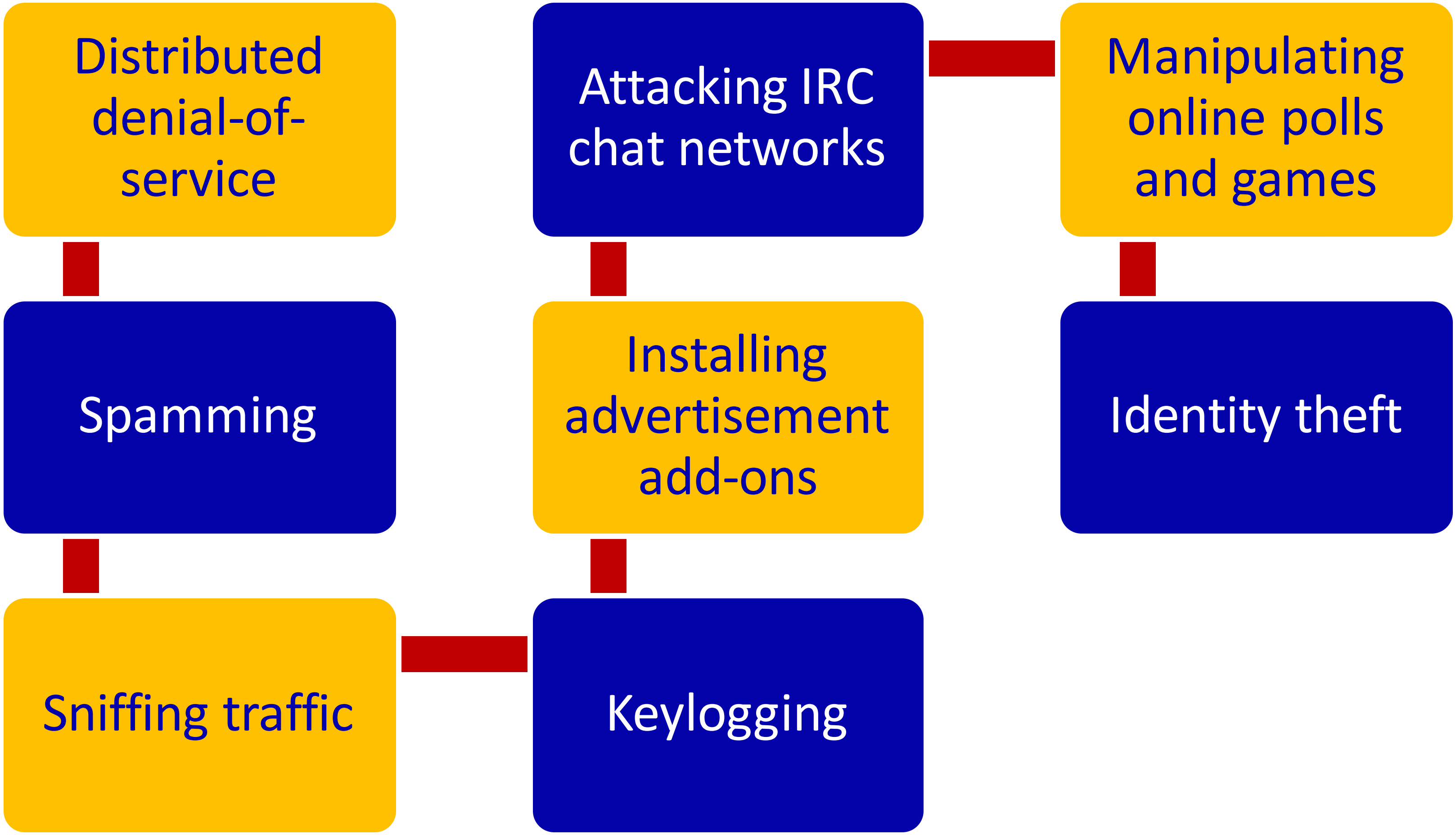
- Manipulate the value of fragments so that they overlap causing the receiving system an issue with reassembling the packet causing it to crash, hang, or reboot

SYN Flood

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

© 2013 NISGTC

Botnets



Distributed denial-of-service

Spamming

Sniffing traffic

Keylogging

Installing advertisement add-ons

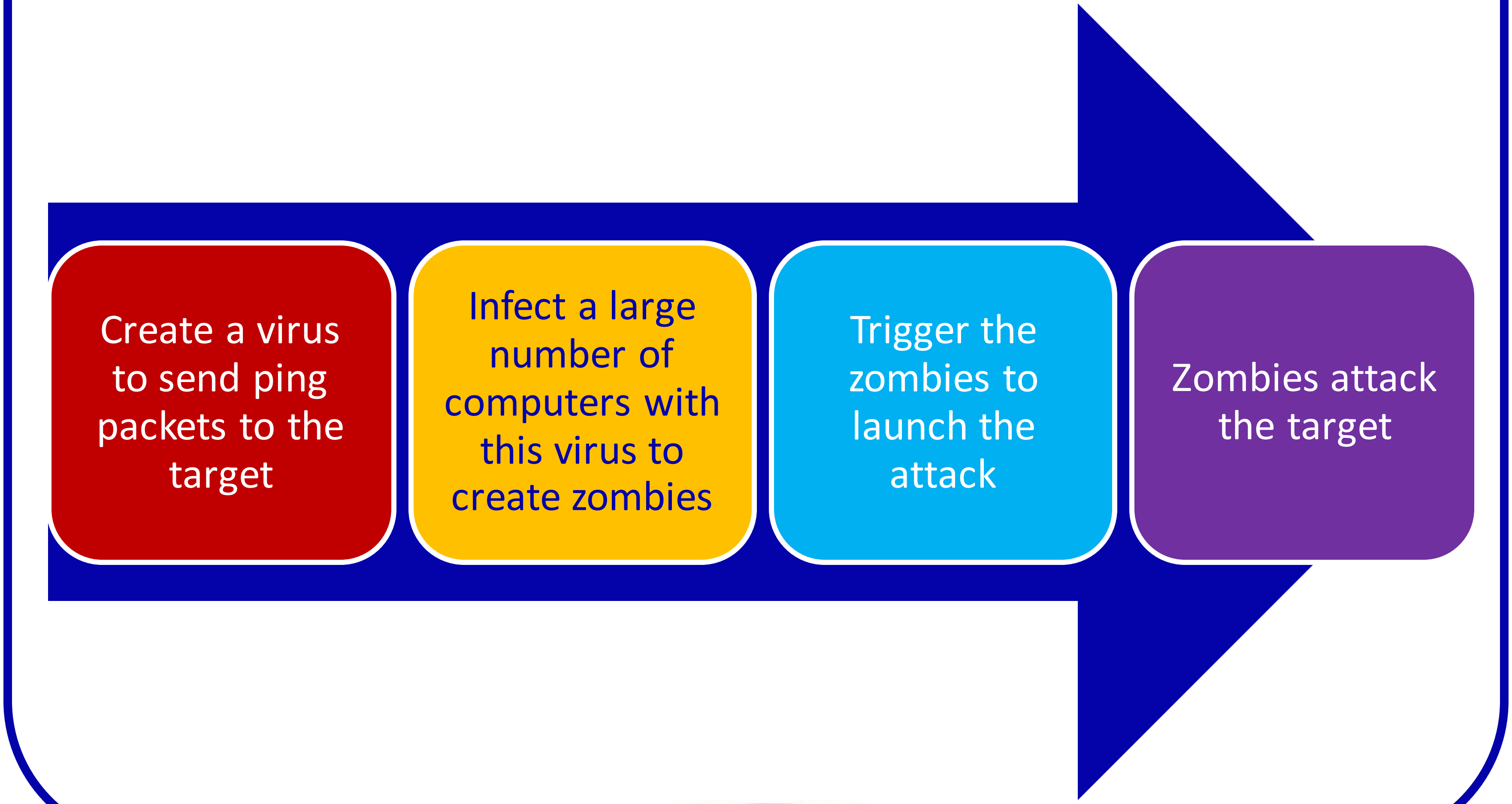
Attacking IRC chat networks

Manipulating online polls and games

Identity theft

© 2013 NISGTC

Conducting a DDoS Attack



Create a virus to send ping packets to the target

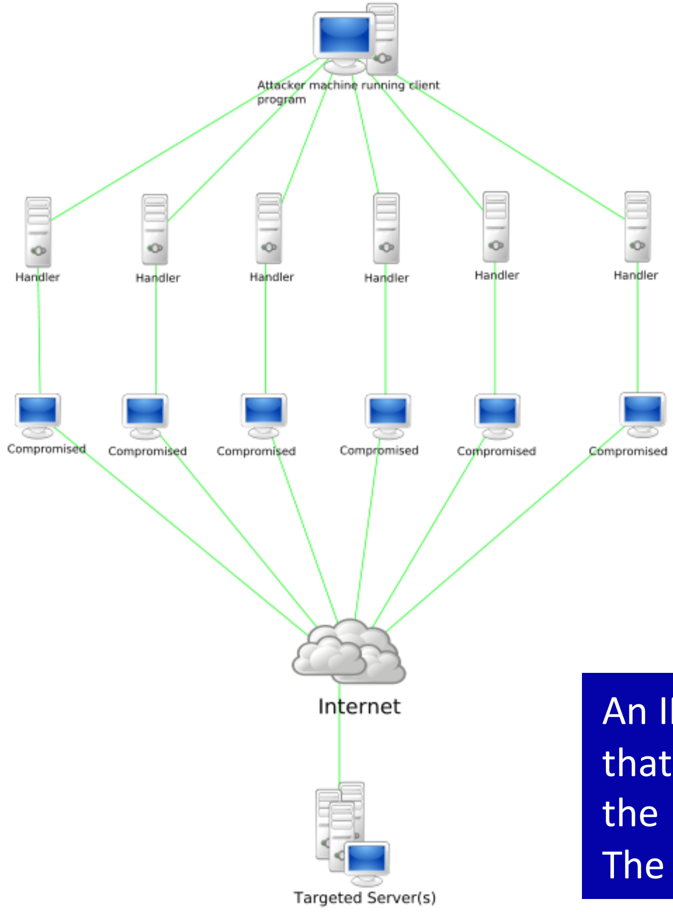
Infect a large number of computers with this virus to create zombies

Trigger the zombies to launch the attack

Zombies attack the target

© 2013 NISGTC

Distributed Denial of Service Attack (DDoS)



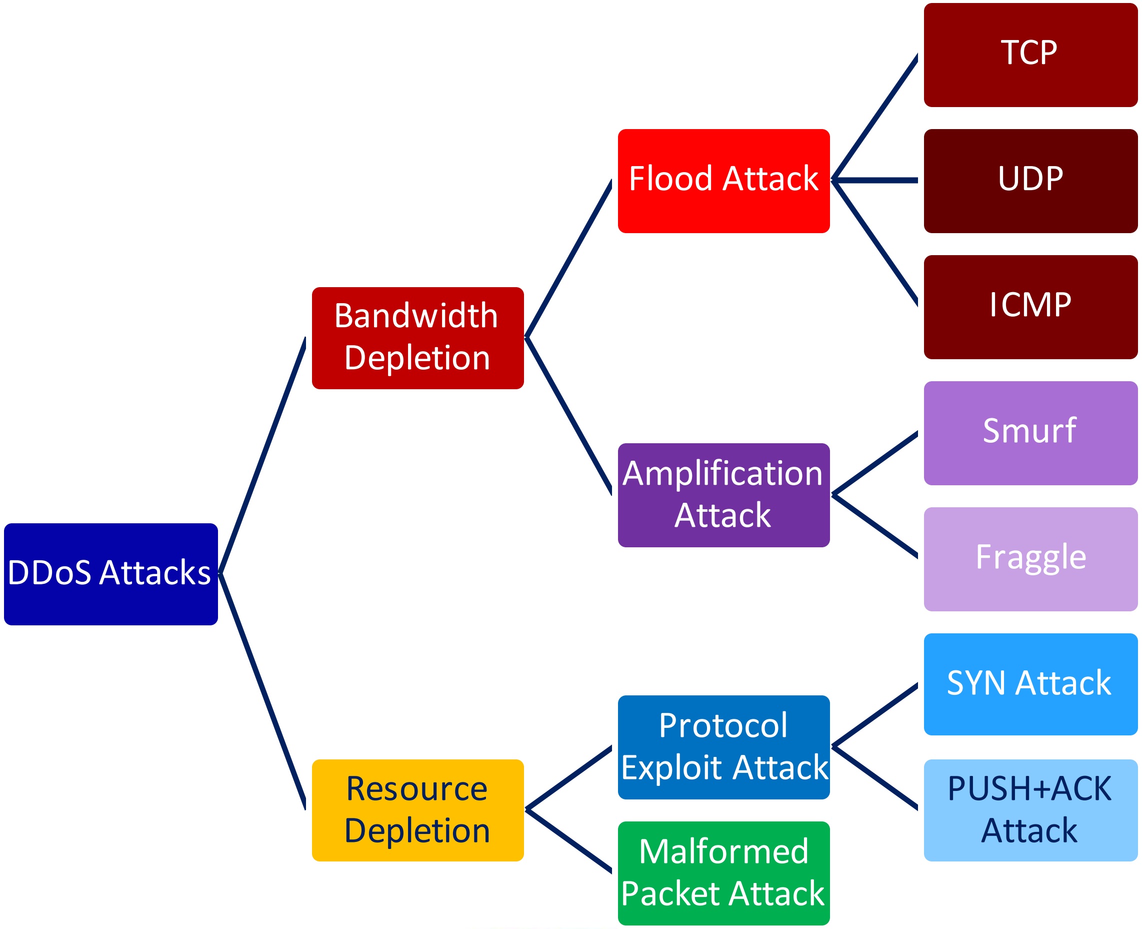
Handler software is placed on a compromised router or network server

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

© 2013 NISGTC

Attack Classes



NISGTC
The National Information, Security & Geospatial Technologies Consortium

© 2013 NISGTC

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.

https://security.radware.com/ddos-knowledge-center/ddospedia/smurf-attack/

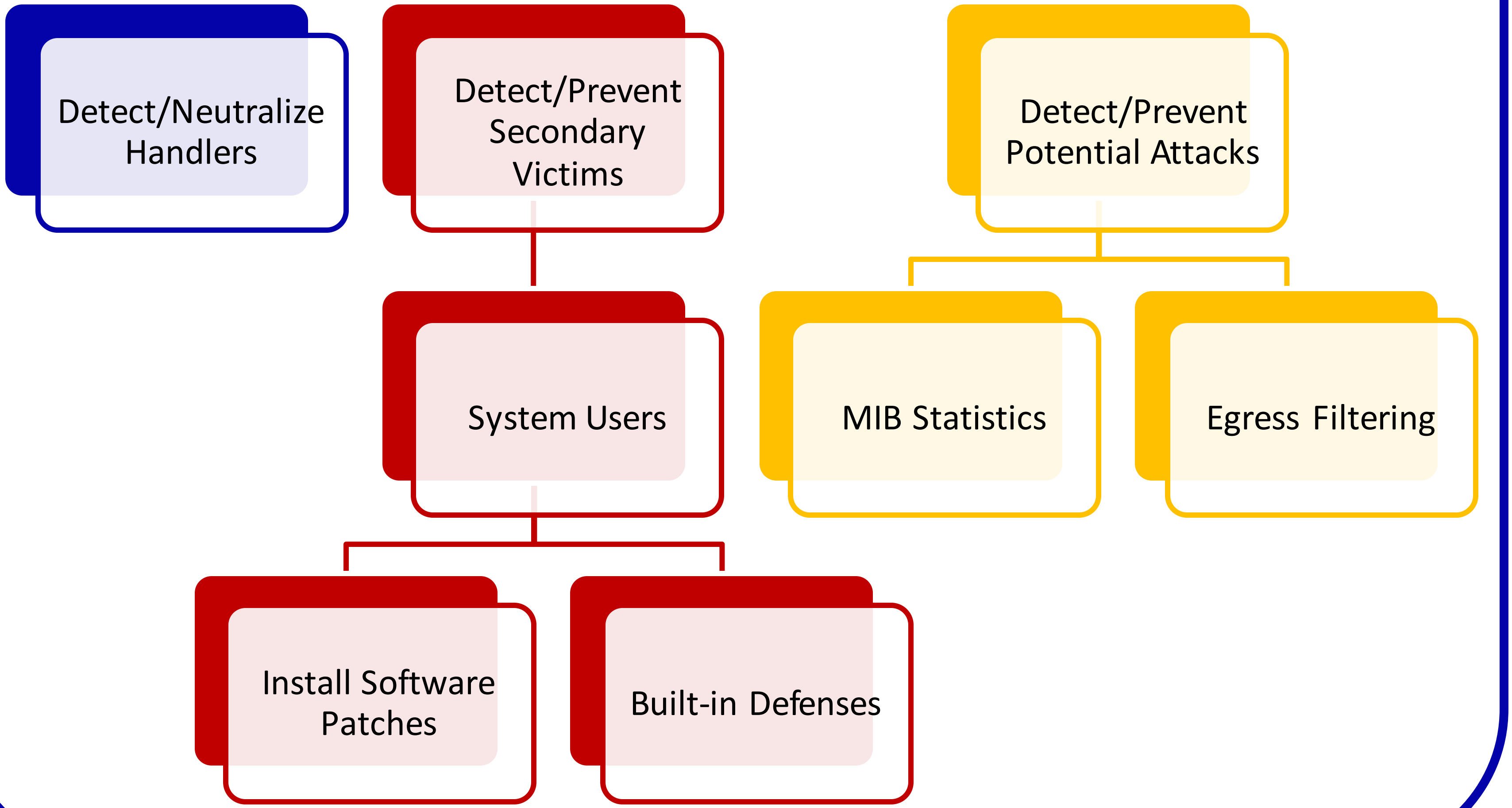
Amplification Attacks

Fragggle 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



Detect/Neutralize Handlers

Detect/Prevent Secondary Victims

System Users

Install Software Patches

Built-in Defenses

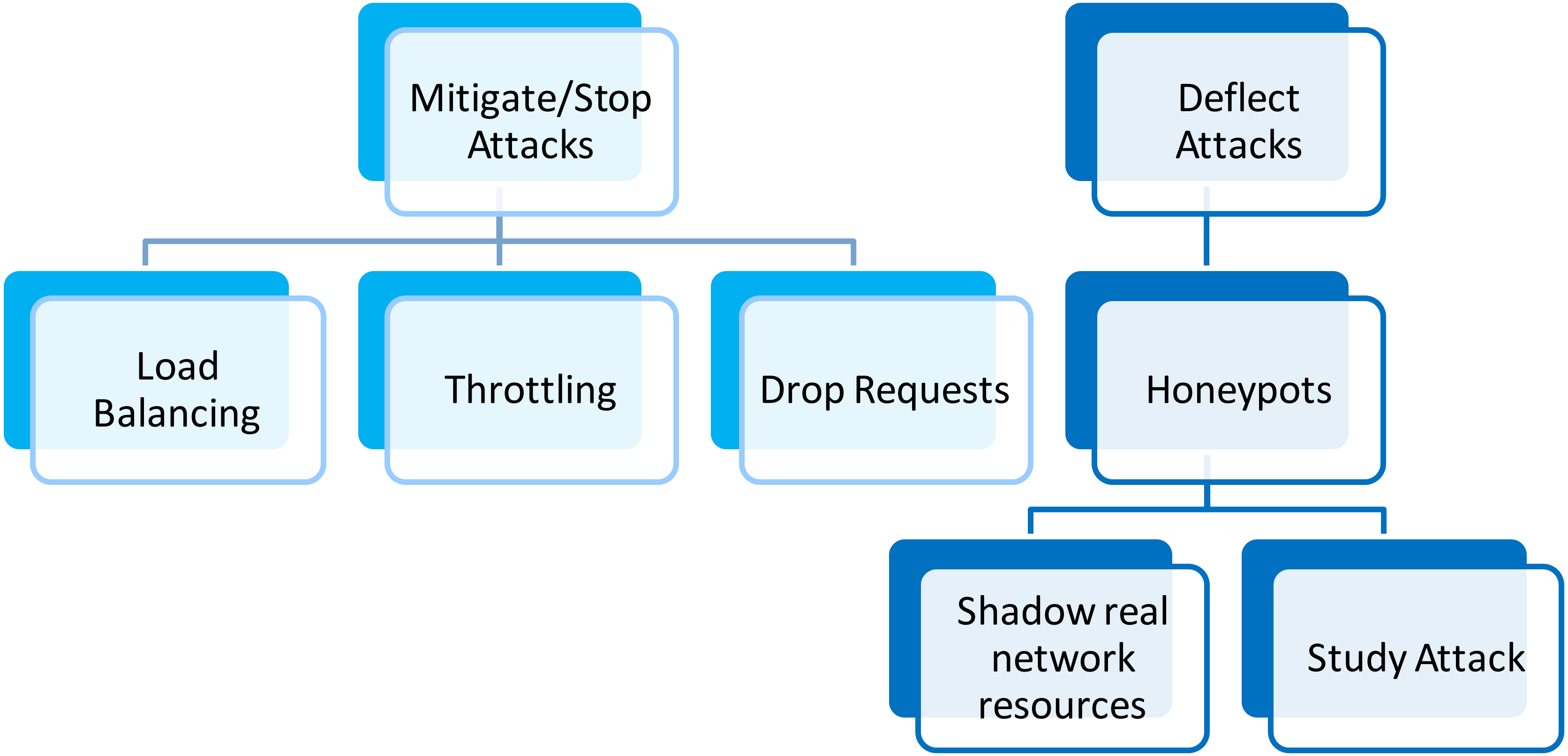
Detect/Prevent Potential Attacks

MIB Statistics

Egress Filtering

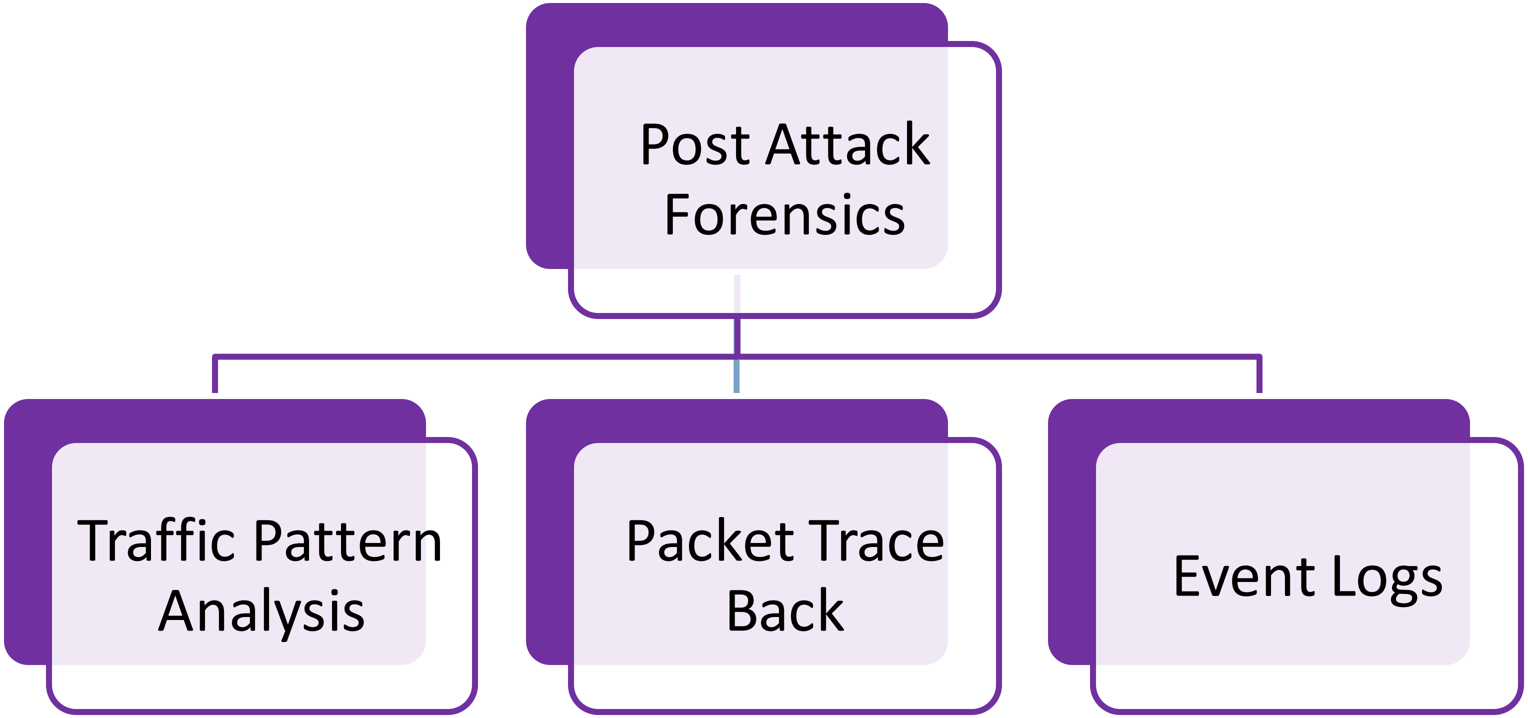
© 2013 NISGTC

Countermeasures



© 2013 NISGTC

Countermeasures



Post Attack Forensics

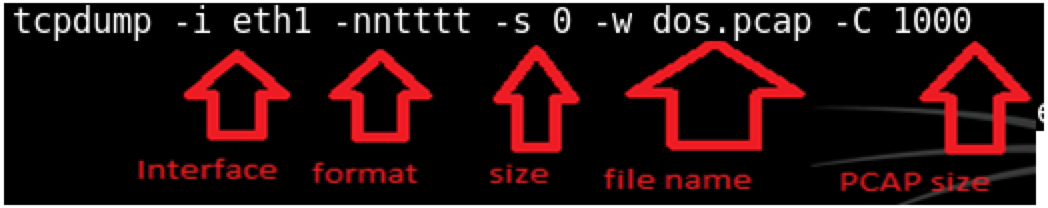
Traffic Pattern Analysis

Packet Trace Back

Event Logs

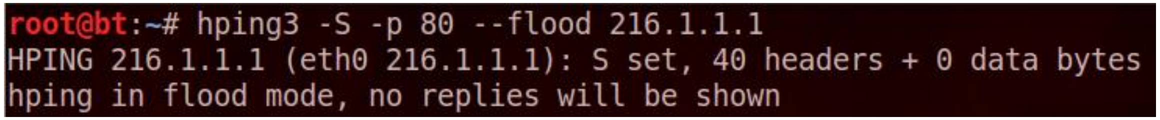
© 2013 NISGTC

Performing a DoS Attack



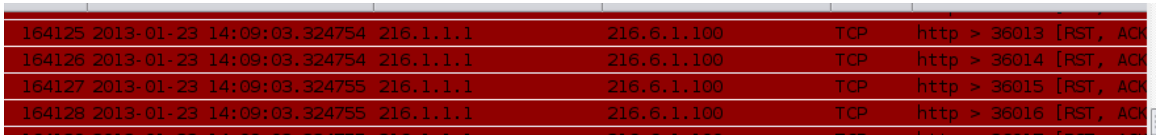
```
tcpdump -i eth1 -nntttt -s 0 -w dos.pcap -C 1000
```

Capture network traffic with Tcpdump



```
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

NISGTC

The National Information, Security & Geospatial Technologies Consortium

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