



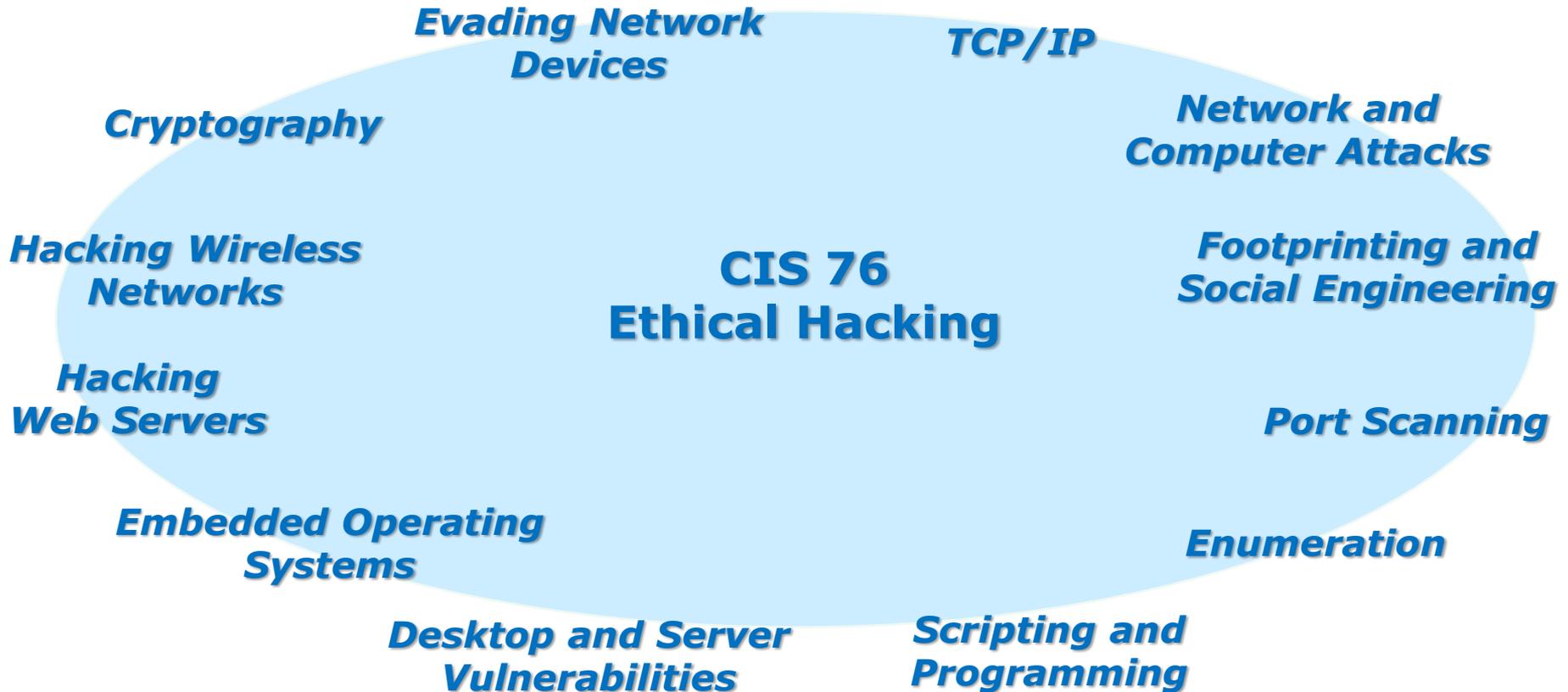
Rich's lesson module checklist

- 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

- Lab 5 posted and tested
- T1 on Canvas for last hour of class
- Copy T1 steganography file to depot directory

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



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". The main content area is titled "CIS 90 (Fall 2014) Calendar" and includes a "Calendar" link. A table lists lessons with columns for "Lesson", "Date", "Topics", and "Link". The "CIS 76" link is highlighted. The "Presentation slides (download)" link is also highlighted. The "Enter virtual classroom" link is highlighted. The "Topics" column for Lesson 6 includes: "Class and Linux Operations", "Understand how the course will work", "High-level overview of computers, operating systems and virtual machines", "Overview of UNIX/Linux market and architecture", "Using SSH for remote network logs", and "Using terminals and the command line". The "Supplemental" section includes "PowerPoint: Logging into Opus (download)". The "Assignments" section includes "Student Survey" and "Lab 1". The "CCC Confer" section includes "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

The screenshot shows a virtual classroom interface. On the left is a sidebar with navigation options like 'Login', 'Flashcards', 'Admin', and 'CIS 90 (Spring)'. The main area contains a video conference window for 'Rich-Simms' with a 'PARTICIPANTS' list and a 'CHAT' window. A central window displays 'CIS 90 - Lesson 1' with a map titled 'Class Activity - Where are you now?'. To the right, a PDF window shows 'The CIS 90 System Playground' with a diagram of server racks. Below the PDF, a terminal window shows a password prompt and system information.

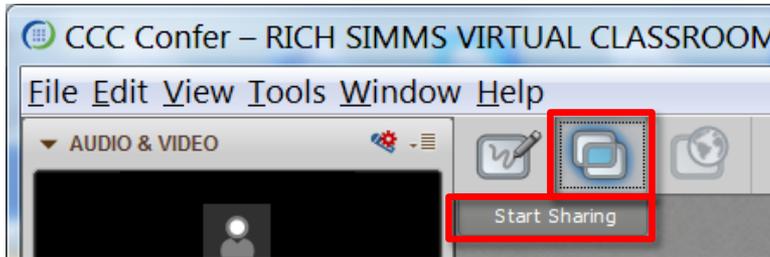
CIS 76 website Calendar page

One or more login sessions to Opus

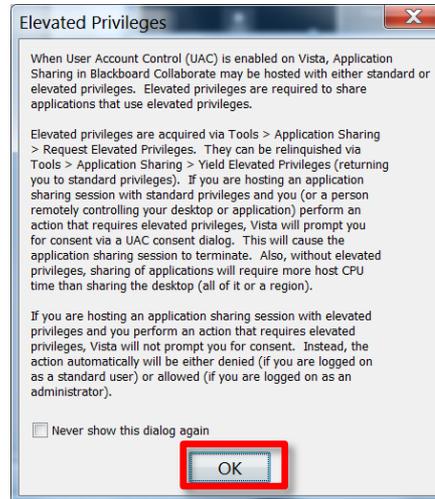


Student checklist for sharing desktop with classmates

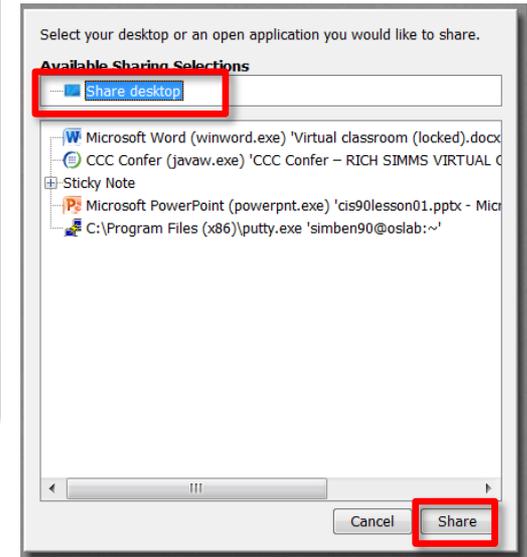
1) Instructor gives you sharing privileges.



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



3) Click OK button.



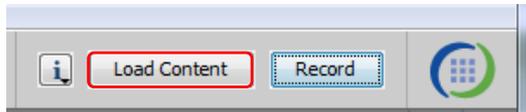
4) Select "Share desktop" and click Share button.



Rich's CCC Confer checklist - setup

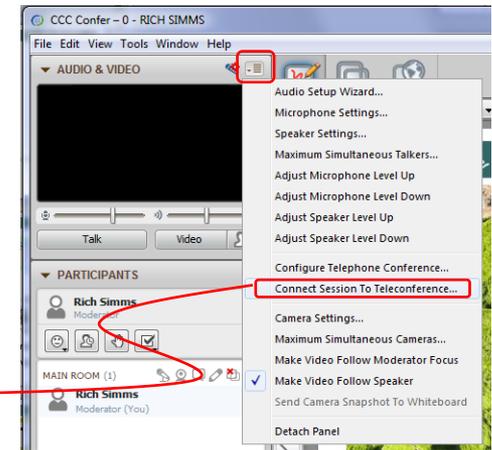
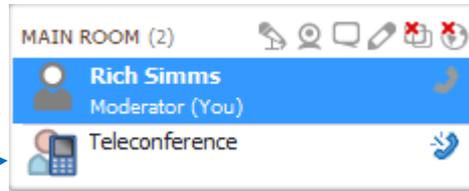


[] Preload White Board



[] Connect session to Teleconference

Session now connected to teleconference



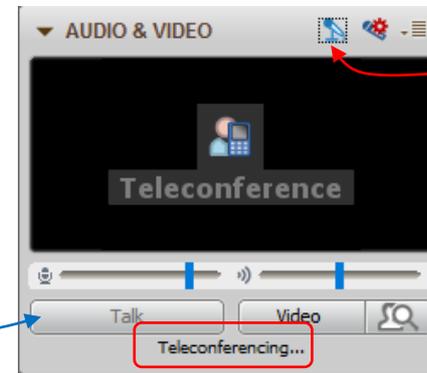
[] Is recording on?



Red dot means recording

[] Use teleconferencing, not mic

Should be grayed out



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



Rich's CCC Confer checklist - screen layout



The screenshot displays a Windows desktop with several applications open:

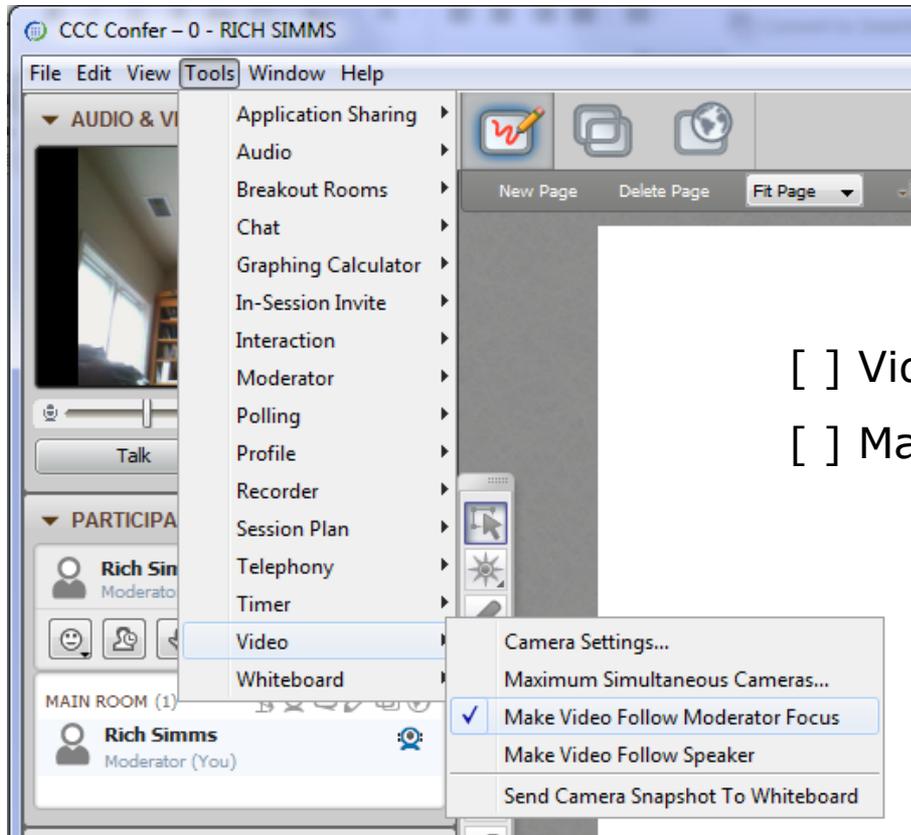
- CCC Confer - 0 - RIC...:** A teleconference window showing a video feed of Rich Simms, a list of participants (Rich Simms as Moderator), and a chat window.
- foxit for slides:** A Foxit Reader window displaying a PDF document titled 'cis90lesson07.pdf' with a directory tree showing folders like 'boot', 'bin', 'etc', and 'sbin'.
- chrome:** A Chrome browser window showing a quiz page from 'simms-teach.com/docs/cis90/cis-90-TEST-1-Fall-12.pdf'. The quiz includes questions like 'What command shows the other users logged in to the computer?' and 'What environment variable is used by the shell to determine which directories to search when locating a command?'.
- putty:** A terminal window showing a login session for 'simben90@oslab:~'. The terminal output includes 'login as: simben90', 'Access denied', and 'Last login: Mon Oct 8 18:58:43 2012'.
- vSphere Client:** A vSphere Client window showing the 'CIS 192' virtual machine and its recent tasks.

[] layout and share apps





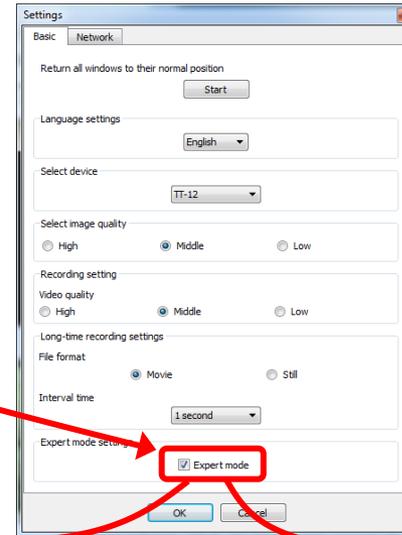
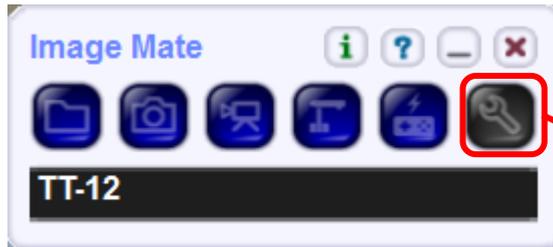
Rich's CCC Confer checklist - webcam setup



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



Rich's CCC Confer checklist - Elmo



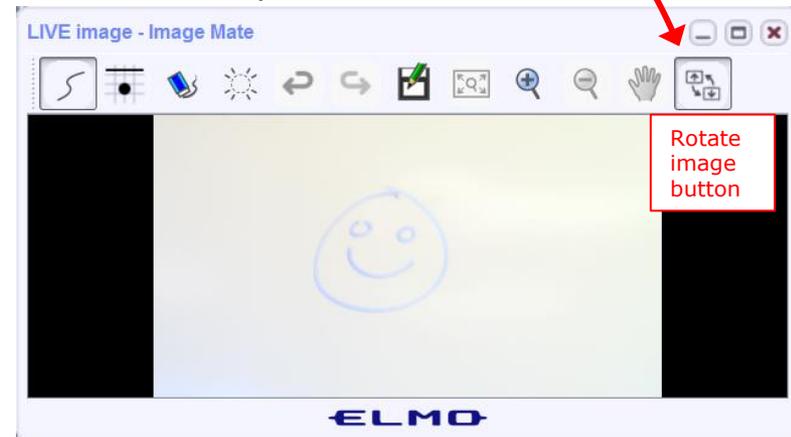
The "rotate image" button is necessary if you use both the side table and the white board.

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

Elmo rotated down to view side table



Elmo rotated up to view white board



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

Rich's CCC Confer checklist - universal fixes

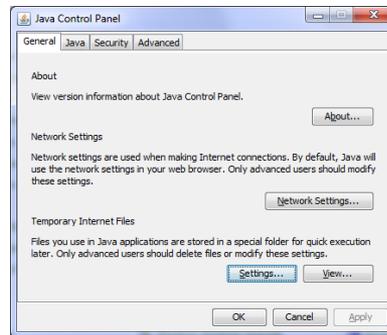
Universal Fix for CCC Confer:

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

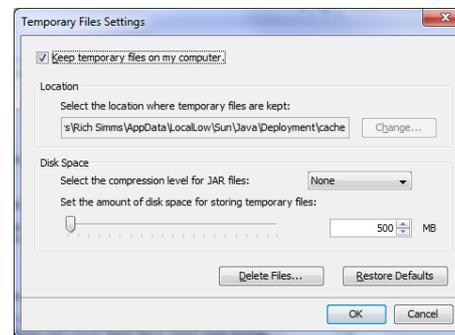
Control Panel (small icons)



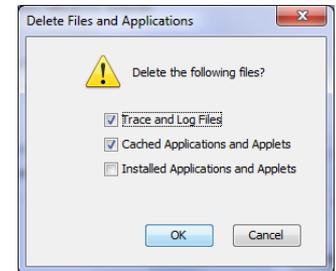
General Tab > Settings...



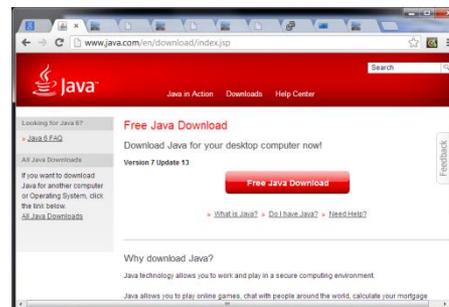
500MB cache size



Delete these



Google Java download





Start



Sound Check

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

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



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



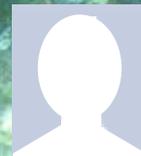
Alex



Michael W.



Carter



Thomas



Wes



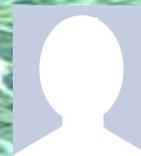
Jennifer



Marcos



Tim



Luis



Dave R.



Scanning

Objectives

- Understand different types of port scans
- Look at port scan tools
- Understand vulnerability scans
- Look at vulnerability scan tools

Agenda

- Questions
- Housekeeping
- Port Scanning
- Vulnerability scanning
- Assignment
- Wrap up
- Test 1

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. Catfishing

<http://www.zdnet.com/article/exclusive-inside-a-million-dollar-amazon-kindle-catfishing-scam/>

Thanks Marcos

Vulnerability Summary for the Week of September 26, 2016

Bulletin (SB16-277) More Bulletins

Vulnerability Summary for the Week of September 26, 2016

Original release date: October 03, 2016

Print Tweet Send Share

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

The vulnerabilities are based on the CVE vulnerability naming standard and are organized according to severity, determined by the Common Vulnerability Scoring System (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

High Vulnerabilities				
Primary Vendor - Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- digital_editions	Use-after-free vulnerability in Adobe Digital Editions before 4.5.2 allows attackers to execute arbitrary code via unspecified vectors, a different	2016-09-26	10.0	CVE-2016-6980 BID@



Best Practices



Defense Best Practices

How to detect a phishing email

<http://blog.inspiredelearning.com/wp-content/uploads/2014/04/phishing-infographic-full.jpg>

Thanks Deryck

Housekeeping



No labs due today

Test 1 will become available at 7:30 PM tonight

- Open book, open notes, open computer.
- You must work alone and not help or receive help from others.
- Online timed 60 minute test using Canvas
- Online "archive watching" students that work can take it later today but it must be completed by 11:59 PM.
- **Practice test ends 30 minutes before real test starts!**

Next week:

- Quiz 5
- Lab 5 is due

Test 1

HONOR CODE:

This test is open book, open notes, and open computer.

HOWEVER, you must work alone. You may not discuss the test questions or answers with others during the test.

You may not ask or receive assistance from anyone other than the instructor when doing this test.

Likewise you may not give any assistance to anyone taking the test.

Perkins/VTEA Survey

phpBB® Cabrillo College: Computer and Information Systems
creating communities
 Forum for students in the Computer Networking and System Administration and/or Computer Support Specialist programs

Search...

Quick links FAQ Register Login

Board index < Cabrillo College Fall 2015 Courses < CIS 90 - Fall 2015

Carl D. Perkins Vocational and Technical Education Act

Post Reply Search this topic...

5 posts • Page 1 of 1

Carl D. Perkins Vocational and Technical Education Act
by Rich Simms • Tue Sep 22, 2015 2:34 pm

The Carl D. Perkins Vocational and Technical Education Act was originally authorized by Congress in 1984. It was reauthorized in 1998 and again in 2006. This act provides federal funding for improving career technical education (CTE) within the United States in order to help the economy.

For Cabrillo College to receive a portion of this funding students in technical classes must fill out a survey. The more surveys completed the more funds the college will receive. The survey only needs to be completed once per term by each student.

This survey can be completed online using web advisor:

Log on to WEBADVISOR at <https://wave.cabrillo.edu>

Select "STUDENTS: Click Here" (navy blue bar)

- Under "Academic Profile" Click on "Student Update Form"
- Use drop down list under "Select the earliest term for which you are registered" and click on the current term.
- Select "SUBMIT"

Scroll down to the "Career Technical Information"

- Answer questions by clicking on the circle to the left of your "Yes" or "No" answers
- You can get details about a question by clicking on blue underlined phrase
- After answering all questions Select "SUBMIT"

Then "LOG OUT"

Thank you for taking a few minutes to help Cabrillo College CS/CIS programs!

- Rich



Rich Simms
Posts: 1793
 Joined: Sat Jan 16, 2010 5:47 pm
 Contact: []

<http://oslab.cis.cabrillo.edu/forum/viewtopic.php?f=121&t=4176>

This is an important source of funding for Cabrillo College.

*Send me an email stating you completed this Perkins/VTEA survey for **three points extra credit!***

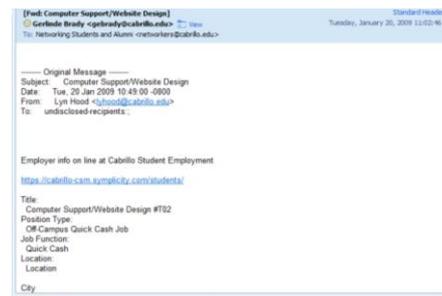
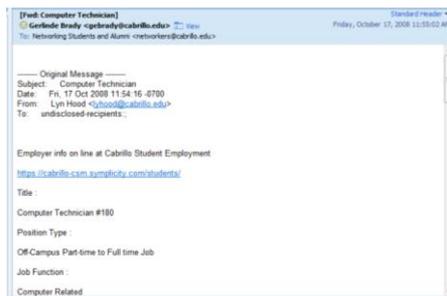
Career Technical Information	
Your answers to these questions will help qualify Cabrillo College for Perkins/VTEA grant funds.	
Are you currently receiving benefits from:	
<input type="radio"/> Yes	TANF/CALWORKS
<input type="radio"/> No	
<input type="radio"/> Yes	SSI (Supplemental Security Income)
<input type="radio"/> No	
<input type="radio"/> Yes	GA (General Assistance)
<input type="radio"/> No	
<input type="radio"/> Yes	Does your income qualify you for a fee waiver?
<input type="radio"/> No	
<input type="radio"/> Yes	Are you a single parent with custody of one or more minor children?
<input type="radio"/> No	
<input type="radio"/> Yes	Are you a displaced homemaker attending Cabrillo to develop job skills?
<input type="radio"/> No	
<input type="radio"/> Yes	Have you moved in the preceding 36 months to obtain, or to accompany parents or spouses to obtain, temporary or seasonal employment in agriculture, dairy, or fishing?
<input type="radio"/> No	

Cabrillo Networking Program Mailing list

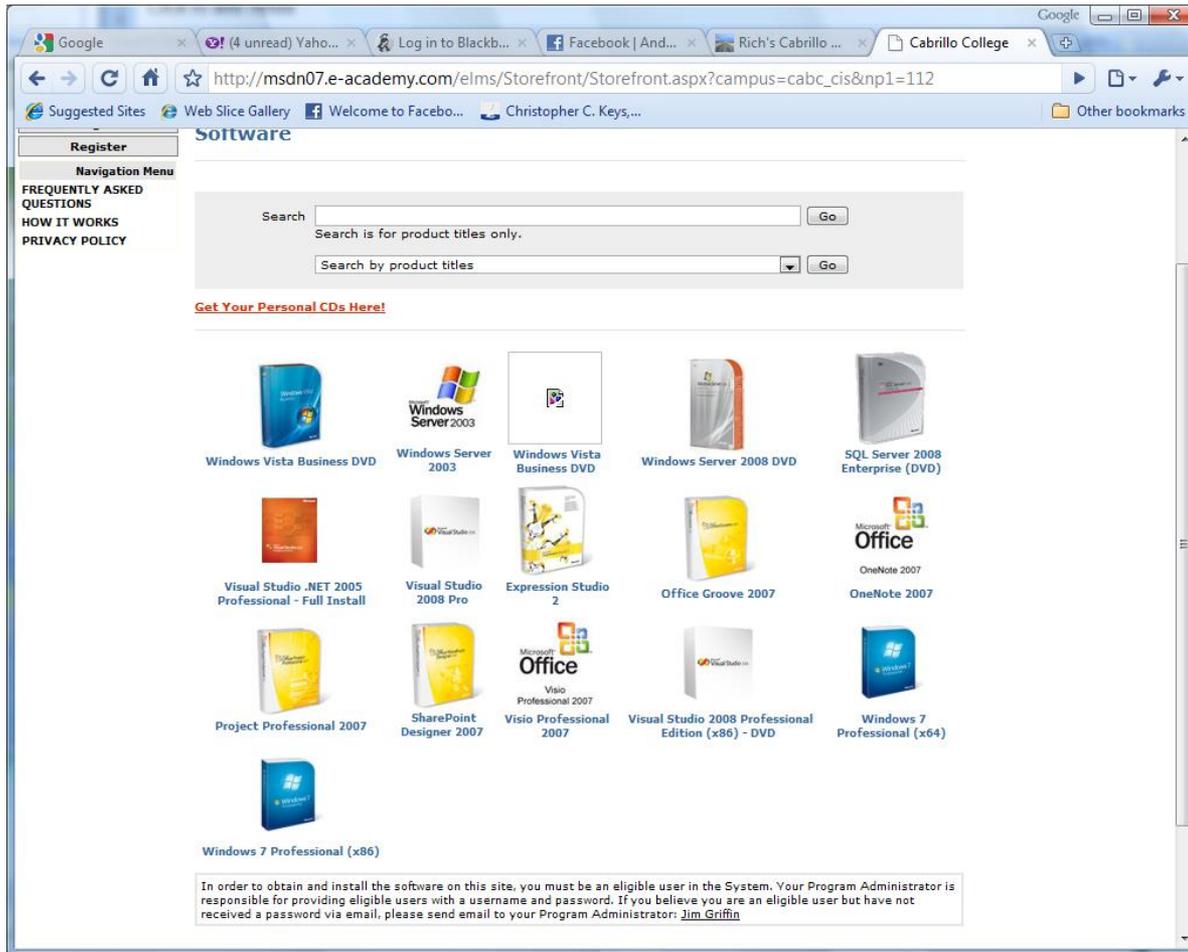
Subscribe by sending an email (no subject or body) to:

networkers-subscribe@cabrillo.edu

- Program information
- Certification information
- Career and job information
- Short-term classes, events, lectures, tours, etc.
- Surveys
- Networking info and links



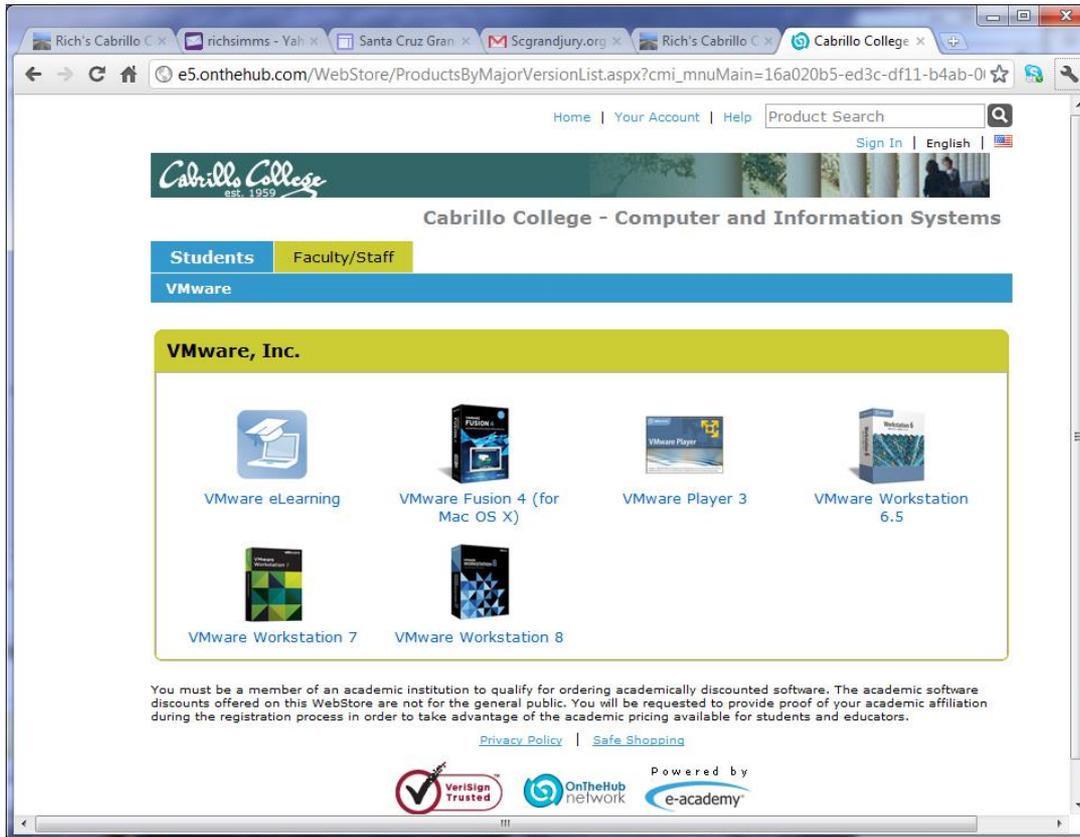
Microsoft Academic Webstore



- 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

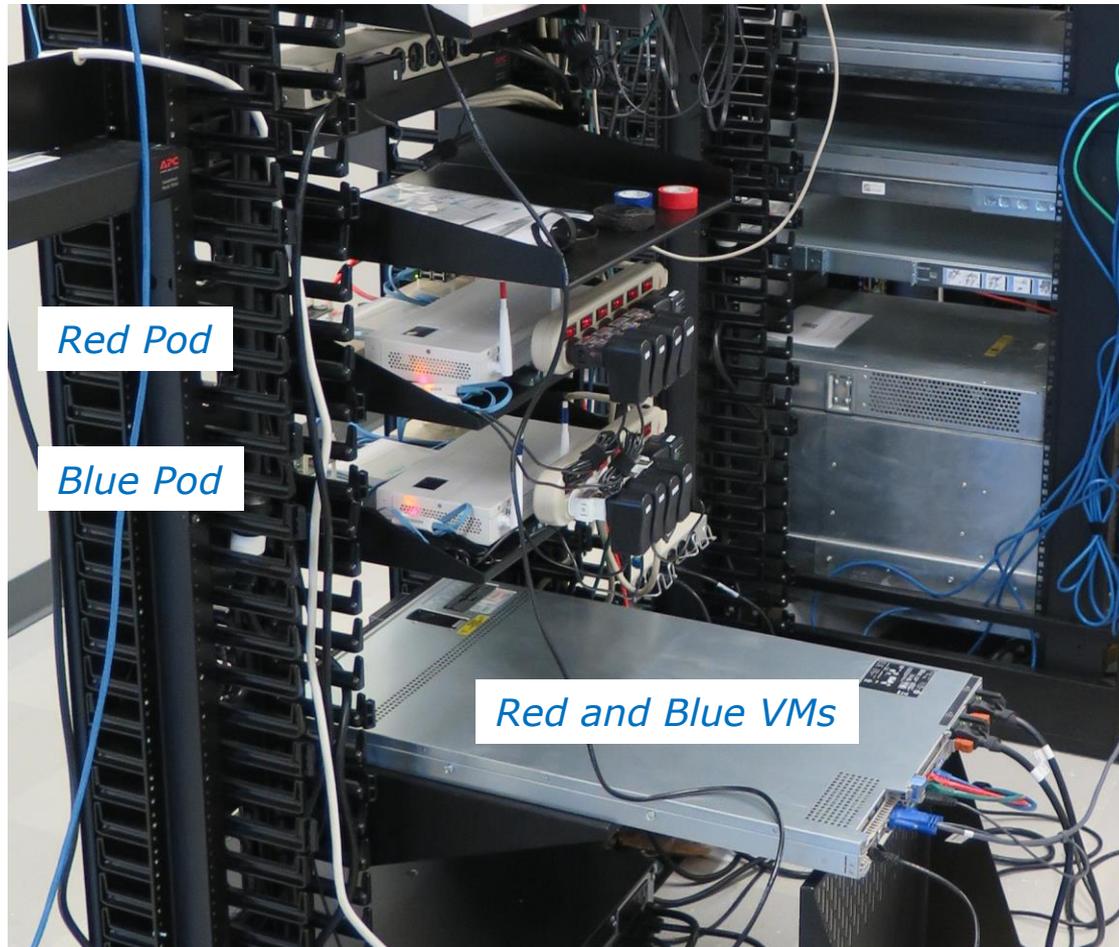
VMware Academic Webstore



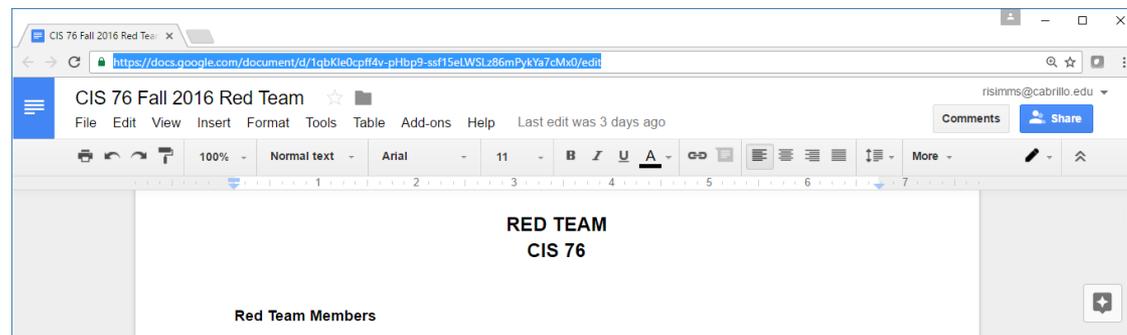
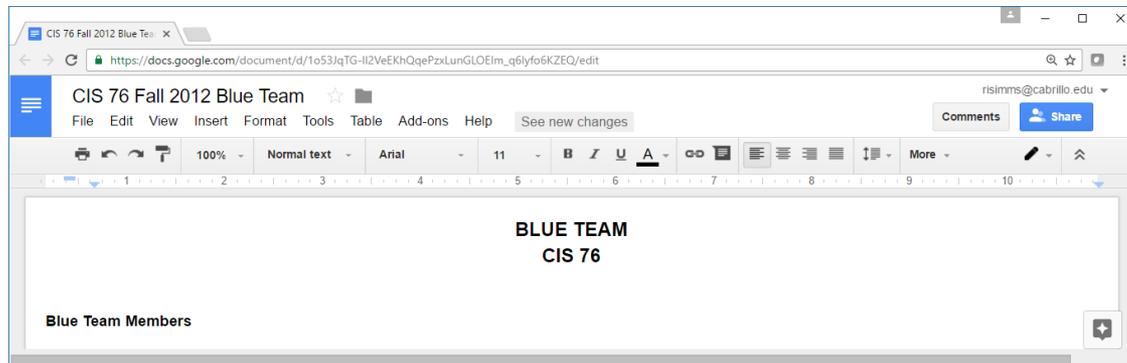
- VMware software for students registered in a CIS or CS class at Cabrillo
- Available after registration is final (two weeks after first class)

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

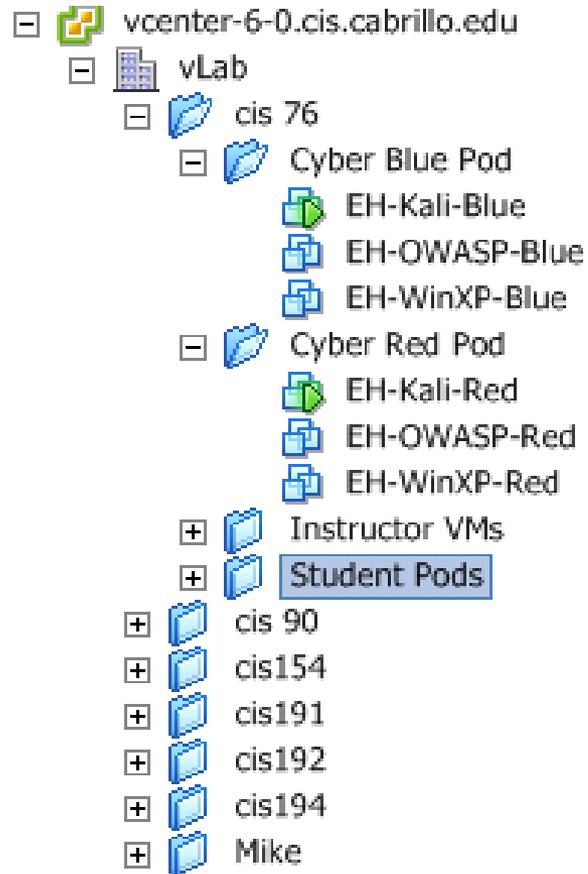
Red and Blue Pods in Microlab Lab Rack



Each team has their own private Google Docs document



Accessing Red and Blue Pods via VLab



*Send me an email
if you would like to
join one of the
teams*



Scanning

EC-Council Five Phases of Hacking

Phase 1 - Reconnaissance

Phase 2 - Scanning

Phase 3 - Gaining Access

Phase 4 - Maintaining Access

Phase 5 - Clearing Tracks

Scanning

Objectives

- Discover all open services on a host server.
- Detect firewalls.
- Identify vulnerabilities.

Process:

- Scan all ports (not just well-know ports) and make a list of open services.
- Record evidence of firewalls (stateful or not stateful)
- Scan open services and identify the products and versions in use.
- Identify vulnerabilities in those products using vulnerability scans and research.

nmap

nmap.org

The screenshot shows the nmap.org website with the following elements:

- Navigation Menu (Left):**
 - Nmap Security Scanner**
 - Intro
 - Ref Guide
 - Install Guide
 - Download
 - Changelog
 - Book
 - Docs
 - Security Lists**
 - Nmap Announce
 - Nmap Dev
 - Bugtraq
 - Full Disclosure
 - Pen Test
 - Basics
 - More
 - Security Tools**
- Central Banner:** "Up Your Security Game with AlienVault and Nmap. Gain threat detection alerts, vulnerability data, and asset information in a unified console." Includes an AlienVault logo and a "TRY IT FREE" button.
- Image:** A large graphic featuring a pair of eyes and the text "FREE Security scanner. Nmap Audit your network now!".
- Navigation Grid:**

Intro	Reference Guide	Book	Install Guide
Download	Changelog	Zenmap GUI	Docs
Bug Reports	OS Detection	Propaganda	Related Projects
In the Movies			In the News
- Terminal Output (Right):**

```
# nmap -H -T4 scanme.nmap.org
Starting Nmap 4.01
Interesting ports on scanme.nmap.org:
|_ The 1667 ports scanned but not shown below are of the closed state.
|_ 22/tcp open  ssh
|_ 25/tcp open  smtp
|_ 53/tcp open  domain
|_ 70/tcp closed gopher
|_ 80/tcp open  http
|_ 115/tcp closed auth
Device type: generic
Running: Linux 2.6.
OS details: Linux 2.6.
Uptime: 20,177 days
Interesting ports on scanme.nmap.org:
```
- News Section:**
 - Nmap 7.30 is now available! [[change log](#) | [download](#)]
 - Nmap 7.12 is now available! [[change log](#) | [download](#)]
 - Nmap 7 is now available! [[release notes](#) | [download](#)]
 - We're pleased to release our new and Improved [Icons of the Web](#) project—a 5-gigapixel interactive collage of the top million sites on the Internet!
 - Nmap has been discovered in two new movies! It's used to [hack Matt Damon's brain in Elysium](#) and also [to hack the world in Mission: Impossible - Rogue Nation](#)

SANS Nmap Cheat Sheet

SANS PENETRATION TESTING

Resources Training Events Certification Instructors About

SANS Penetration Testing

08 Oct 2013

Nmap Cheat Sheet 1.0

0 comments Posted by eskoudis
Filed under Nmap, Scanning

Over the last couple of days, the folks at Counter Hack and I have put together an Nmap cheat sheet covering some of the most useful options of everyone's favorite general-purpose port scanner, Nmap. And, with its scripting engine, Nmap can do all kinds of wonderful things for security professionals.

Please check out the cheat sheet below. Even if you are an experienced attacker, it might cover a tip or trick that's new and useful to you.

Scripting Engine	Notable Scripts	Nmap Cheat Sheet v1.0
<pre>--c Run default scripts --script=<ScriptName> <ScriptCategory> <ScriptDir>... Run individual or groups of scripts --script-args=<Name1=Value1,...> Use the list of script arguments --script-updateadb Update script database</pre>	<p>A full list of Nmap Scripting Engine scripts is available at http://nmap.org/nsedoc/</p> <p>Some particularly useful scripts include:</p> <p>dns-zone-transfer: Attempts to pull a zone file (AXFR) from a DNS server. <code>\$ nmap --script dns-zone-transfer.nse --script-args dns-zone-transfer.domain=<domain> -p53 <host></code></p> <p>http-robots.txt: Harvests robots.txt files from discovered web servers. <code>\$ nmap --script http-robots.txt <host></code></p> <p>smb-brute: Attempts to determine valid username and password combinations via automated guessing. <code>\$ nmap --script smb-brute.nse -p445 <host></code></p> <p>smb-psexec: Attempts to run a series of programs on the target machine, using credentials provided as scriptargs. <code>\$ nmap --script smb-psexec.nse --script-args=ambuser=<username>,ambpass=<password>,config=<config> -p445 <host></code></p>	<p>Basic Syntax</p> <pre>\$ nmap [ScanType] [Options] [targets]</pre> <p>Target Specification</p> <p>[IPv4 address]: 192.168.1.1 [IPv6 address]: AAAA:CCCC::FFfeth0 Host name: www.target.tgt IP address range: 192.168.0-255.0-255 CIDR block: 192.168.0.0/16 Use file with lists of targets: -iL <filename></p> <p>Target Ports</p> <p>No port range specified scans 1,000 most popular ports</p> <ul style="list-style-type: none"> -F Scan 100 most popular ports -p<port1>-<port2> Port range -p<port1>,<port2>,... Port List -pU:53,D:110,T20-445 Mix TCP and UDP -E Scan linearly (do not randomize ports) -T<tcp-ports <-> Scan in most popular ports -p-65535 Leaving off initial port in range makes Nmap scan start at port 1 -p0- Leaving off end port in range makes Nmap scan through port 65535 -p- Nmap scan through port 65535 -p- Scan ports 1-65535

Connect Scan

same subnet
no firewall

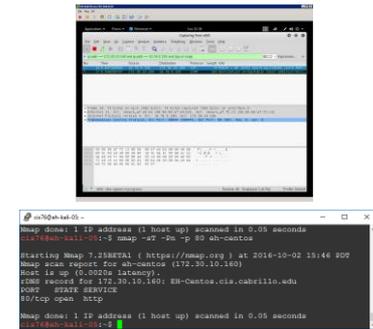
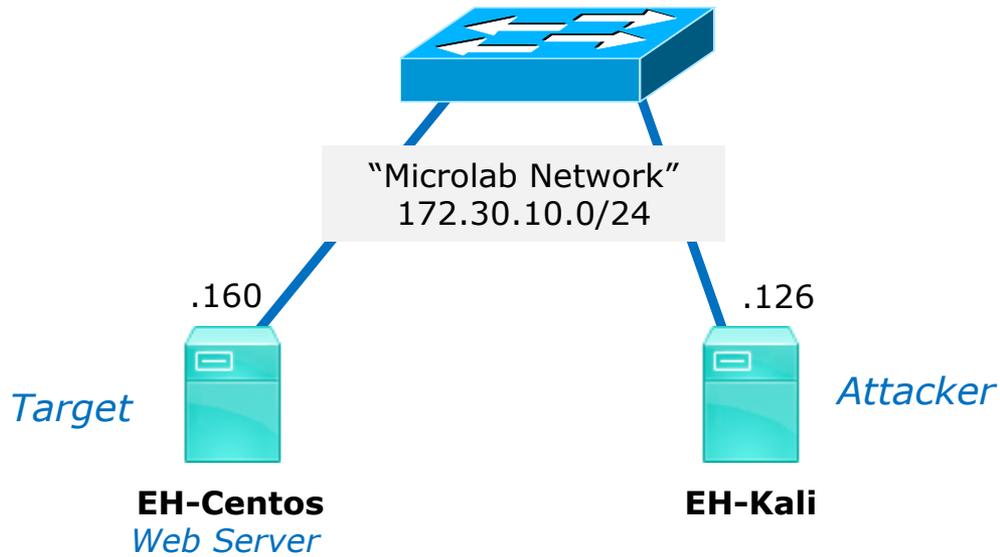
Connect Scan

- Completes the three-way handshake
- Detectable and can be logged as a TCP connection (see example below)
- Result is one of three states: Open, Closed, and Filtered

Top unknown TCP connections

NoSweat : Sunday, October 02, 2016

Device SN	Source Zone	Destination Zone	Source address	Source Host Name	Source User	Destination address	Destination Host Name	Destination User	IP Protocol	Destination Port
0006C105618	CIS-187-zone	Server-425-zone	177.66.85.46	177.66.85.46		207.62.187.235	rick.cis.cabrillo.edu		tcp	22
0006C105618	CIS-187-zone	Server-425-zone	196.26.121.236	isp2-uc-121-236.igen.co.za		207.62.187.235	rick.cis.cabrillo.edu		tcp	22
0006C105618	CIS-187-zone	Server-425-zone	167.249.144.2	167.249.144.2		207.62.187.233	jeff.cis.cabrillo.edu		tcp	22
0006C105618	CIS-187-zone	Server-425-zone	169.229.3.91	researchscan1.EECS.Berkeley.EDU		207.62.187.233	jeff.cis.cabrillo.edu		tcp	80
0006C105618	CIS-187-zone	Server-425-zone	183.129.160.229	183.129.160.229		207.62.187.242	torc0.cis.cabrillo.edu		tcp	22
0006C105618	CIS-187-zone	Server-425-zone	183.129.160.229	183.129.160.229		207.62.187.235	rick.cis.cabrillo.edu		tcp	22
0006C105618	CIS-187-zone	Server-425-zone	183.129.160.229	183.129.160.229		207.62.187.229	pengo.cis.cabrillo.edu		tcp	22
0006C105618	CIS-187-zone	Server-425-zone	183.129.160.229	183.129.160.229		207.62.187.233	jeff.cis.cabrillo.edu		tcp	22
0006C105618	CIS-187-zone	Server-425-zone	183.129.160.229	183.129.160.229		207.62.187.231	sun-hwa.cis.cabrillo.edu		tcp	22
0006C105618	CIS-187-zone	Server-425-zone	209.193.83.8	209-193-83-8.mammothnetworks.com		207.62.187.242	torc0.cis.cabrillo.edu		tcp	22
0006C105618	CIS-187-zone	Server-425-zone	94.190.1.153	153.1.190.94.interra.ru		207.62.187.241	matera.cis.cabrillo.edu		tcp	22
0006C105618	CIS-187-zone	Server-425-zone	106.184.3.122	li1068-122.members.linode.com		207.62.187.230	oslab.cis.cabrillo.edu		tcp	25



Connect Scan

Firewall action = no firewall and Service = Running

Victim

```
[rsimms@EH-Centos ~]$ sudo service iptables status
iptables: Firewall is not running.
[rsimms@EH-Centos ~]$

[root@EH-Centos ~]# service httpd status
httpd (pid 4196) is running...
[root@EH-Centos ~]#
```

Connect Scan

Firewall action = no firewall and Service = Running

Attacker resets connection after three-way handshake completes

Source	Destination	Protocol	Length	Info
172.30.10.126	172.30.10.160	TCP	74	37808 → 80 [SYN] Seq=0 Win=29200 ...
172.30.10.160	172.30.10.126	TCP	74	80 → 37808 [SYN, ACK] Seq=0 Ack=1...
172.30.10.126	172.30.10.160	TCP	66	37808 → 80 [ACK] Seq=1 Ack=1 Win=...
172.30.10.126	172.30.10.160	TCP	66	37808 → 80 [RST, ACK] Seq=1 Ack=1...

```

cis76@EH-Kali: ~
cis76@EH-Kali:~$ sudo nmap -sT -Pn -p 80 eh-centos

Starting Nmap 7.12 ( https://nmap.org ) at 2016-10-03 07:35 PDT
Nmap scan report for eh-centos (172.30.10.160)
Host is up (0.0012s latency).
rDNS record for 172.30.10.160: EH-Centos.cis.cabrillo.edu
PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
cis76@EH-Kali:~$ █
  
```

Connect Scan

Firewall action = no firewall and Service = Stopped

Victim

```
[rsimms@EH-Centos ~]$ sudo service iptables status
iptables: Firewall is not running.
[rsimms@EH-Centos ~]$

[rsimms@EH-Centos ~]$ sudo service httpd status
httpd is stopped
[rsimms@EH-Centos ~]$
```

Connect Scan

Firewall action = no firewall and Service = Stopped

Victim resets connection

Source	Destination	Protocol	Length	Info
172.30.10.126	172.30.10.160	TCP	74	37810 → 80 [SYN] Seq=0 Win=29200 ...
172.30.10.160	172.30.10.126	TCP	60	80 → 37810 [RST, ACK] Seq=1 Ack=1...

```

cis76@EH-Kali: ~
cis76@EH-Kali:~$ sudo nmap -sT -Pn -p 80 eh-centos

Starting Nmap 7.12 ( https://nmap.org ) at 2016-10-03 07:42 PDT
Nmap scan report for eh-centos (172.30.10.160)
Host is up (0.00055s latency).
rDNS record for 172.30.10.160: EH-Centos.cis.cabrillo.edu
PORT      STATE SERVICE
80/tcp    closed http

Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
cis76@EH-Kali:~$ █
  
```

Connect Scan

Service	Firewall	Result
Running	no firewall	Open
Stopped	no firewall	Closed

Connect Scan

different subnets
firewall on target

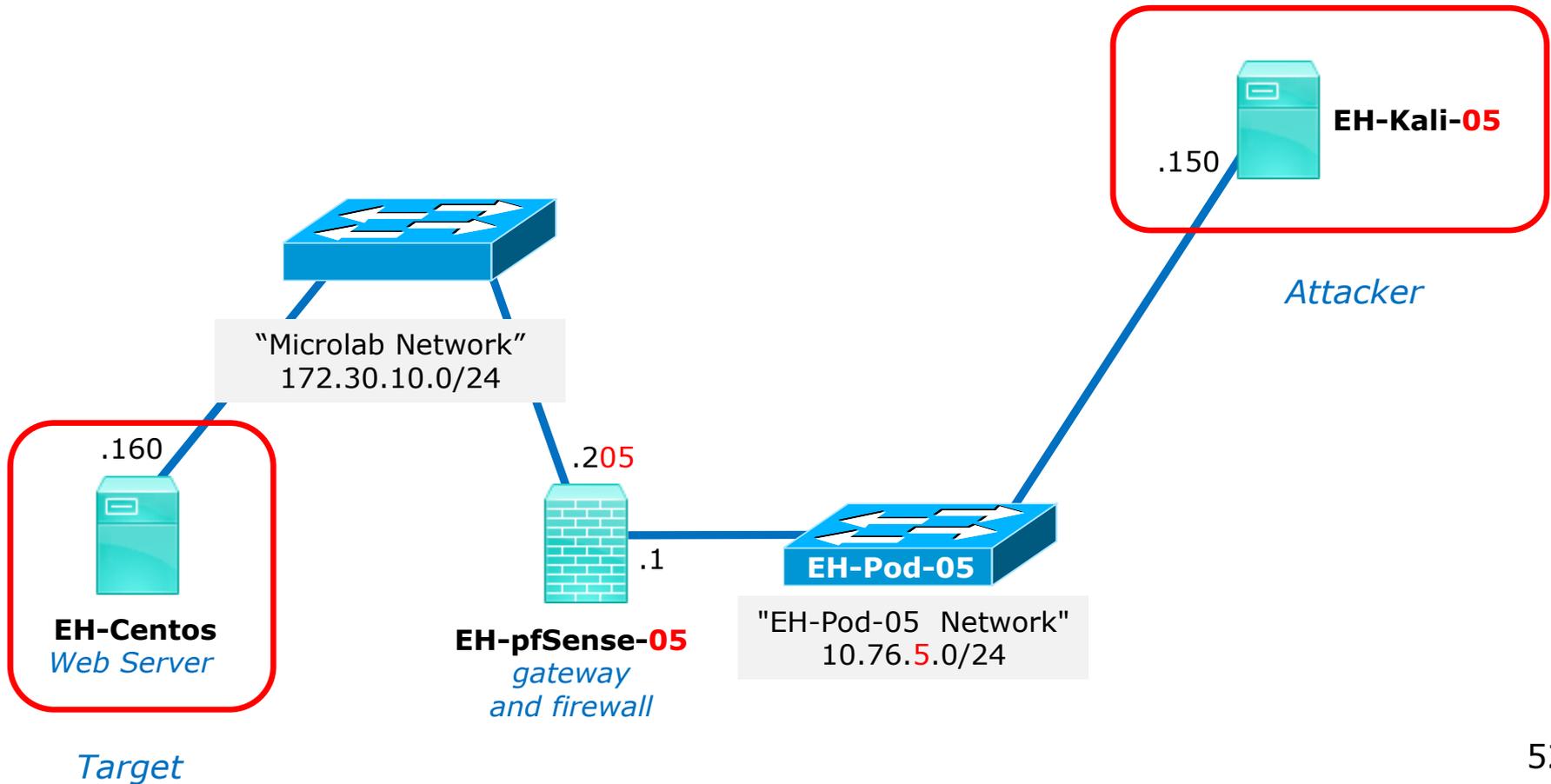
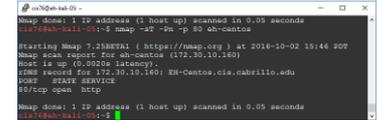
Connect Scan

- Completes the three-way handshake.
- Detectable and can be logged as a TCP connection (see example below).
- Scan results:
 - If SYN-ACK received: "open".
 - If RST received: "closed".
 - If no reply or ICMP error: "filtered".

Top unknown TCP connections

NoSweat : Sunday, October 02, 2016

Device SN	Source Zone	Destination Zone	Source address	Source Host Name	Source User	Destination address	Destination Host Name	Destination User	IP Protocol	Destination Port
0006C105618	CIS-187-zone	Server-425-zone	177.66.85.46	177.66.85.46		207.62.187.235	rick.cis.cabrillo.edu		tcp	22
0006C105618	CIS-187-zone	Server-425-zone	196.26.121.236	isp2-uc-121-236.igen.co.za		207.62.187.235	rick.cis.cabrillo.edu		tcp	22
0006C105618	CIS-187-zone	Server-425-zone	167.249.144.2	167.249.144.2		207.62.187.233	jeff.cis.cabrillo.edu		tcp	22
0006C105618	CIS-187-zone	Server-425-zone	169.229.3.91	researchscan1.EECS.Berkeley.EDU		207.62.187.233	jeff.cis.cabrillo.edu		tcp	80
0006C105618	CIS-187-zone	Server-425-zone	183.129.160.229	183.129.160.229		207.62.187.242	torc0.cis.cabrillo.edu		tcp	22
0006C105618	CIS-187-zone	Server-425-zone	183.129.160.229	183.129.160.229		207.62.187.235	rick.cis.cabrillo.edu		tcp	22
0006C105618	CIS-187-zone	Server-425-zone	183.129.160.229	183.129.160.229		207.62.187.229	pengo.cis.cabrillo.edu		tcp	22
0006C105618	CIS-187-zone	Server-425-zone	183.129.160.229	183.129.160.229		207.62.187.233	jeff.cis.cabrillo.edu		tcp	22
0006C105618	CIS-187-zone	Server-425-zone	183.129.160.229	183.129.160.229		207.62.187.231	sun-hwa.cis.cabrillo.edu		tcp	22
0006C105618	CIS-187-zone	Server-425-zone	209.193.83.8	209-193-83-8.mammothnetworks.com		207.62.187.242	torc0.cis.cabrillo.edu		tcp	22
0006C105618	CIS-187-zone	Server-425-zone	94.190.1.153	153.1.190.94.interra.ru		207.62.187.241	matera.cis.cabrillo.edu		tcp	22
0006C105618	CIS-187-zone	Server-425-zone	106.184.3.122	li1068-122.members.linode.com		207.62.187.230	oslab.cis.cabrillo.edu		tcp	25



Connect Scan

Firewall action = ACCEPT and Service = running

```
[root@EH-Centos ~]# cat /etc/sysconfig/iptables
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 21 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 23 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 25 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

```
[root@EH-Centos ~]# service httpd status
httpd (pid 4196) is running...
[root@EH-Centos ~]#
```

Connect Scan

Firewall action = ACCEPT and Service = running

Three-way handshake completes then attacker resets connection

Source	Destination	Protocol	Length	Info
10.76.5.150	172.30.10.160	TCP	74	59626 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=...
172.30.10.160	10.76.5.150	TCP	74	80 → 59626 [SYN, ACK] Seq=0 Ack=1 Win=14480...
10.76.5.150	172.30.10.160	TCP	66	59626 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=...
10.76.5.150	172.30.10.160	TCP	66	59626 → 80 [RST, ACK] Seq=1 Ack=1 Win=29312...

```

cis76@eh-kali-05: ~
cis76@eh-kali-05:~$ nmap -sT -Pn -p 80 172.30.10.160

Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2016-10-02 15:20 PDT
Nmap scan report for EH-Centos.cis.cabrillo.edu (172.30.10.160)
Host is up (0.0010s latency).
PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds
cis76@eh-kali-05:~$

```

Connect Scan

Firewall action = ACCEPT and Service = stopped

```
[root@EH-Centos ~]# cat /etc/sysconfig/iptables
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 21 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 23 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 25 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

```
[root@EH-Centos ~]# service httpd status
httpd is stopped
[root@EH-Centos ~]#
```

Connect Scan

Firewall action = ACCEPT and Service = stopped

Target responds by resetting the connection

Source	Destination	Protocol	Length	Info
10.76.5.150	172.30.10.160	TCP	74	59638 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=...
172.30.10.160	10.76.5.150	TCP	60	80 → 59638 [RST, ACK] Seq=1 Ack=1 Win=0 Len=...

```

cis76@eh-kali-05: ~
cis76@eh-kali-05:~$
cis76@eh-kali-05:~$ nmap -sT -Pn -p 80 eh-centos

Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2016-10-02 15:24 PDT
Nmap scan report for eh-centos (172.30.10.160)
Host is up (0.00053s latency).
rDNS record for 172.30.10.160: EH-Centos.cis.cabrillo.edu
PORT      STATE      SERVICE
80/tcp    closed    http

Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
cis76@eh-kali-05:~$
  
```

Connect Scan

Firewall action = DROP and Service = Running

```
[root@EH-Centos ~]# cat /etc/sysconfig/iptables
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 21 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 23 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 25 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j DROP
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

```
[root@EH-Centos ~]# service httpd status
httpd (pid 4196) is running...
[root@EH-Centos ~]#
```

Connect Scan

Firewall action = DROP and Service = Running

Target does not respond and attacker times-out.

Time	Source	Destination	Protocol	Length	Info
1.133752897	10.76.5.150	172.30.10.160	TCP	74	59640 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=...
2.132546814	10.76.5.150	172.30.10.160	TCP	74	[TCP Retransmission] 59640 → 80 [SYN] Seq=0...
2.135034272	10.76.5.150	172.30.10.160	TCP	74	59642 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=...
3.132571397	10.76.5.150	172.30.10.160	TCP	74	[TCP Retransmission] 59642 → 80 [SYN] Seq=0...

```

cis76@eh-kali-05: ~
Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
cis76@eh-kali-05:~$ nmap -sT -Pn -p 80 eh-centos

Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2016-10-02 15:32 PDT
Nmap scan report for eh-centos (172.30.10.160)
Host is up.
rDNS record for 172.30.10.160: EH-Centos.cis.cabrillo.edu
PORT      STATE      SERVICE
80/tcp    filtered  http

Nmap done: 1 IP address (1 host up) scanned in 2.05 seconds
cis76@eh-kali-05:~$
  
```

Connect Scan

Firewall action = REJECT with error and Service = Running

```
[root@EH-Centos ~]# cat /etc/sysconfig/iptables
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 21 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 23 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 25 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j REJECT --reject-with
icmp-host-prohibited
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

```
[root@EH-Centos ~]# service httpd status
httpd (pid 4196) is running...
[root@EH-Centos ~]#
```

Connect Scan

Firewall action = REJECT with error and Service = Running

Target replies with ICMP error

Time	Source	Destination	Protocol	Length	Info
0.047180593	10.76.5.150	172.30.10.160	TCP	74	59644 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=...
0.048259737	172.30.10.160	10.76.5.150	ICMP	102	Destination unreachable (Host administrativ...

```

cis76@eh-kali-05: ~
Nmap done: 1 IP address (1 host up) scanned in 2.05 seconds
cis76@eh-kali-05:~$ nmap -sT -Pn -p 80 eh-centos

Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2016-10-02 15:37 PDT
Nmap scan report for eh-centos (172.30.10.160)
Host is up (0.0012s latency).
rDNS record for 172.30.10.160: EH-Centos.cis.cabrillo.edu
PORT      STATE      SERVICE
80/tcp    filtered  http

Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds
cis76@eh-kali-05:~$
  
```



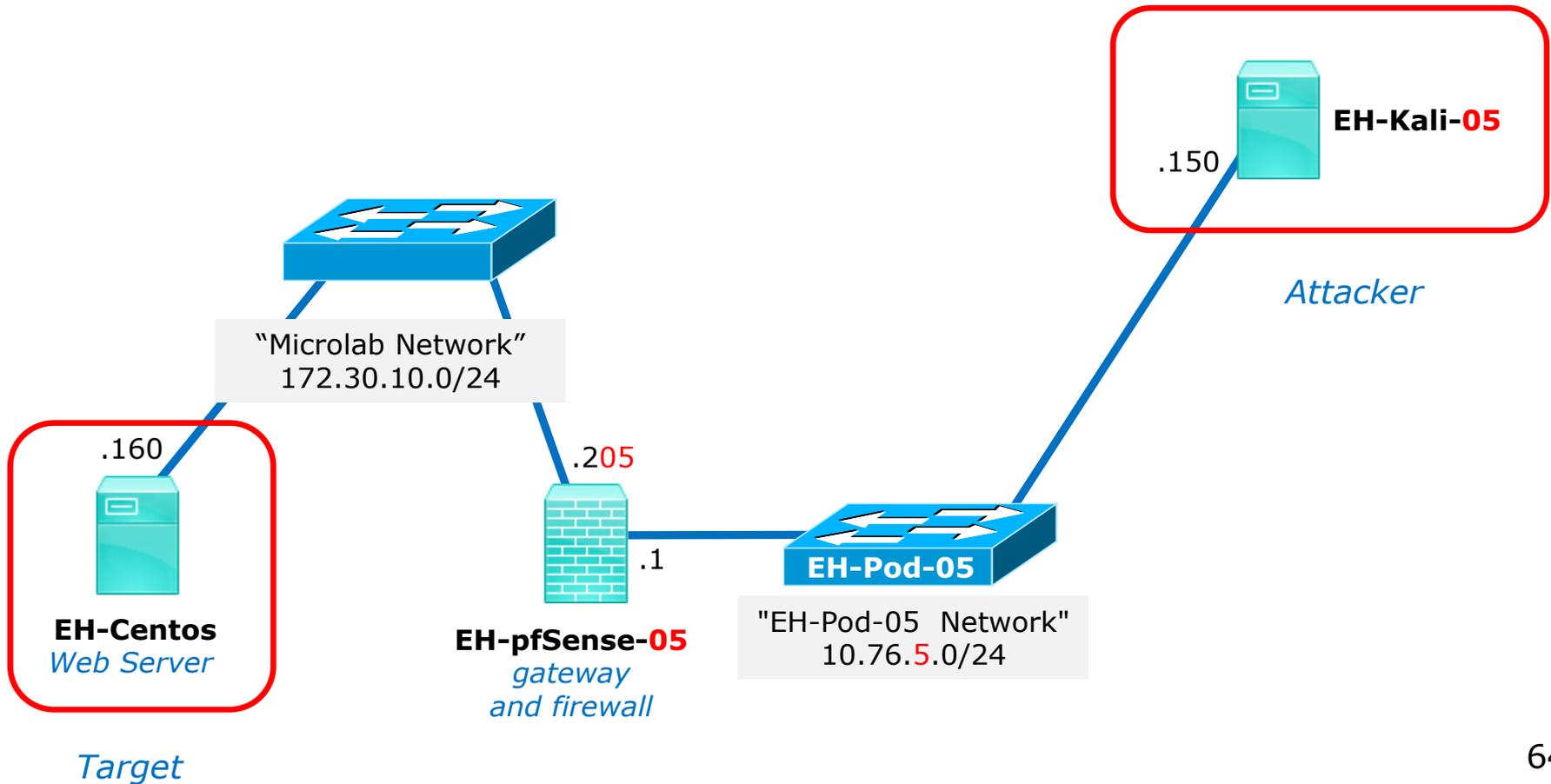
Connect Scan

Service	Firewall	Result
Running	ACCEPT	Open
Running	DROP	Filtered
Running	REJECT	Filtered
Stopped	ACCEPT	Closed
Stopped	DROP	Filtered
Stopped	REJECT	Filtered

Syn Scan

Syn Scan

- Attacker resets the connection attempt before three-way handshake can complete.
- Stealthy because connection is never created.
- Scan results:
 - If SYN-ACK received: "open".
 - If RST received: "closed".
 - If no reply or ICMP error: "filtered".



Syn Scan

Firewall action = ACCEPT and Service = running

```
[root@EH-Centos ~]# cat /etc/sysconfig/iptables
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 21 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 23 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 25 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

```
[root@EH-Centos ~]# service httpd status
httpd (pid 4196) is running...
[root@EH-Centos ~]#
```

Syn Scan

Firewall action = ACCEPT and Service = running

Attacker resets connection rather than completing the three-way handshake

Time	Source	Destination	Protocol	Length	Info
5.758937315	10.76.5.150	172.30.10.160	TCP	58	40565 → 80 [SYN] Seq=0 Win=1024 Len=...
5.759359381	172.30.10.160	10.76.5.150	TCP	60	80 → 40565 [SYN, ACK] Seq=0 Ack=1 Wi...
5.759394088	10.76.5.150	172.30.10.160	TCP	54	40565 → 80 [RST] Seq=1 Win=0 Len=0

```

cis76@eh-kali-05: ~
cis76@eh-kali-05:~$ sudo nmap -sS -Pn -p 80 eh-centos

Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2016-10-02 16:37 PDT
Nmap scan report for eh-centos (172.30.10.160)
Host is up (0.00044s latency).
rDNS record for 172.30.10.160: EH-Centos.cis.cabrillo.edu
PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds
cis76@eh-kali-05:~$

```

Syn Scan

Firewall action = ACCEPT and Service = stopped

```
[root@EH-Centos ~]# cat /etc/sysconfig/iptables
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 21 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 23 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 25 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

```
[root@EH-Centos ~]# service httpd status
httpd is stopped
[root@EH-Centos ~]#
```

Syn Scan

Firewall action = ACCEPT and Service = stopped

Target port responds by resetting the connection

Source	Destination	Protocol	Length	Info
10.76.5.150	172.30.10.160	TCP	58	58885 → 80 [SYN] Seq=0 Win=1024 Len=...
172.30.10.160	10.76.5.150	TCP	60	80 → 58885 [RST, ACK] Seq=1 Ack=1 Wi...

```

cis76@eh-kali-05: ~
cis76@eh-kali-05:~$ sudo nmap -sS -Pn -p 80 eh-centos
Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2016-10-23 16:59 PDT
Nmap scan report for eh-centos (172.30.10.160)
Host is up (0.0024s latency).
rDNS record for 172.30.10.160: EH-Centos.cis.cabrillo.edu
PORT      STATE  SERVICE
80/tcp    closed http
Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
cis76@eh-kali-05:~$

```

Syn Scan

Firewall action = DROP and Service = Running

```
[root@EH-Centos ~]# cat /etc/sysconfig/iptables
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 21 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 23 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 25 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j DROP
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

```
[root@EH-Centos ~]# service httpd status
httpd (pid 4196) is running...
[root@EH-Centos ~]#
```

Syn Scan

Firewall action = DROP and Service = Running

Target does not respond and attacker times-out

Source	Destination	Protocol	Length	Info
10.76.5.150	172.30.10.160	TCP	58	48809 → 80 [SYN] Seq=0 Win=1024 Len=...
10.76.5.150	172.30.10.160	TCP	58	48810 → 80 [SYN] Seq=0 Win=1024 Len=...

```

cis76@eh-kali-05: ~
cis76@eh-kali-05:~$ sudo nmap -sS -Pn -p 80 eh-centos

Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2016-10-02 16:44 PDT
Nmap scan report for eh-centos (172.30.10.160)
Host is up.
rDNS record for 172.30.10.160: EH-Centos.cis.cabrillo.edu
PORT      STATE      SERVICE
80/tcp    filtered  http

Nmap done: 1 IP address (1 host up) scanned in 2.05 seconds
cis76@eh-kali-05:~$ █
  
```

Syn Scan

Firewall action = REJECT with error and Service = Running

```
[root@EH-Centos ~]# cat /etc/sysconfig/iptables
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 21 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 23 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 25 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j REJECT --reject-with
icmp-host-prohibited
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

```
[root@EH-Centos ~]# service httpd status
httpd (pid 4196) is running...
[root@EH-Centos ~]#
```

Syn Scan

Firewall action = REJECT with error and Service = Running

Target replies with ICMP error

Source	Destination	Protocol	Length	Info
10.76.5.150	172.30.10.160	TCP	58	52464 → 80 [SYN] Seq=0 Win=1024 Len=...
172.30.10.160	10.76.5.150	ICMP	86	Destination unreachable (Host admini...

```

cis76@eh-kali-05: ~
cis76@eh-kali-05:~$ sudo nmap -sS -Pn -p 80 eh-centos

Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2016-10-02 16:49 PDT
Nmap scan report for eh-centos (172.30.10.160)
Host is up (0.00076s latency).
rDNS record for 172.30.10.160: EH-Centos.cis.cabrillo.edu
PORT      STATE      SERVICE
80/tcp    filtered  http

Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
cis76@eh-kali-05:~$ █
  
```

Syn Scan

Service	Firewall	Result
Running	ACCEPT	Open
Running	DROP	Filtered
Running	REJECT	Filtered
Stopped	ACCEPT	Closed
Stopped	DROP	Filtered
Stopped	REJECT	Filtered



Null, XMAS and FIN Scans

Null, XMAS, and FIN scans

- These scan types work the same way using different TCP flags.
- Scan results:
 - If RST received: "closed".
 - If no reply: "open or filtered".
 - If ICMP unreachable error is received: "filtered".
- These scan types are slightly more stealthy than a SYN scan and may be able to evade certain non-stateful firewalls and packet filtering routers. However they can be detected by most modern IDS products.

<https://nmap.org/book/man-port-scanning-techniques.html>

Null, XMAS, and FIN scans

"The big downside is that not all systems follow RFC 793 to the letter. A number of systems send RST responses to the probes regardless of whether the port is open or not. This causes all of the ports to be labeled closed. Major operating systems that do this are Microsoft Windows, many Cisco devices, BSDI, and IBM OS/400. This scan does work against most Unix-based systems though. Another downside of these scans is that they can't distinguish open ports from certain filtered ones, leaving you with the response open|filtered."

<https://nmap.org/book/man-port-scanning-techniques.html>

Null Scan (Linux)

Null Scan

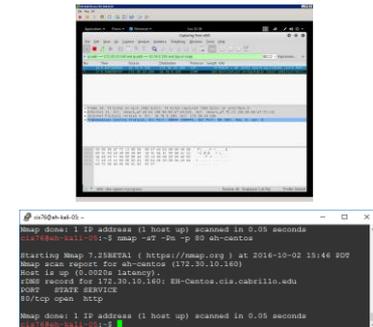
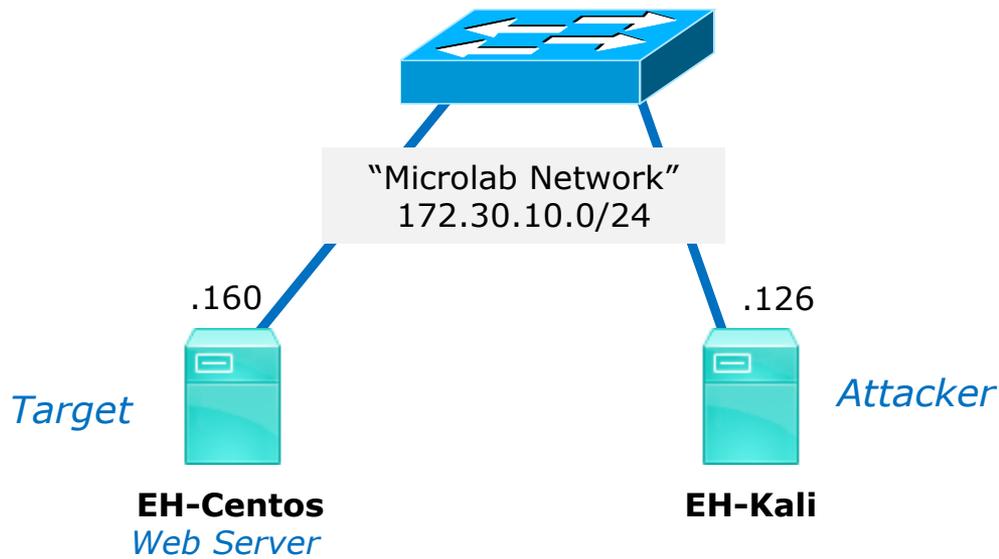
- All TCP flags are off
- Result is one of two states: Closed, "Open or Filtered"

```

Flags: 0x000 (<None>)
 000. .... = Reserved: Not set
...0 .... = Nonce: Not set
... 0... = Congestion Window Reduced (CWR): Not set
... .0.. = ECN-Echo: Not set
... ..0. = Urgent: Not set
... ...0 = Acknowledgment: Not set
... .... 0... = Push: Not set
... .... .0.. = Reset: Not set
... .... ..0. = Syn: Not set
... .... ...0 = Fin: Not set
[TCP Flags: *****]

```

Switched to Kali on the same subnet because NULL scans didn't get through pfSense firewall



Switched to Kali on the same subnet because NULL scans didn't get through pfSense firewall

Null Scan

Firewall action = no firewall and Service = Running

```
[rsimms@EH-Centos ~]$ sudo service iptables status
iptables: Firewall is not running.
[rsimms@EH-Centos ~]$

[root@EH-Centos ~]# service httpd status
httpd (pid 4196) is running...
[root@EH-Centos ~]#
```

Null Scan

Firewall action = no firewall and Service = Running

No response by victim

Source	Destination	Protocol	Length	Info
172.30.10.126	172.30.10.160	TCP	54	65106 → 80 [<None>] Seq=1 Win=102...
172.30.10.126	172.30.10.160	TCP	54	65107 → 80 [<None>] Seq=1 Win=102...

```

cis76@EH-Kali: ~
cis76@EH-Kali:~$ sudo nmap -sN -Pn -p 80 eh-centos

Starting Nmap 7.12 ( https://nmap.org ) at 2016-10-03 09:03 PDT
Nmap scan report for eh-centos (172.30.10.160)
Host is up (0.00059s latency).
rDNS record for 172.30.10.160: EH-Centos.cis.cabrillo.edu
PORT      STATE      SERVICE
80/tcp    open|filtered http
MAC Address: 00:50:56:AF:04:CD (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
cis76@EH-Kali:~$
  
```

Null Scan

Firewall action = no firewall and Service = Stopped

```
[root@EH-Centos ~]# service iptables status
iptables: Firewall is not running.
[root@EH-Centos ~]#

[root@EH-Centos ~]# service httpd status
httpd is stopped
[root@EH-Centos ~]#
```

Null Scan

Firewall action = no firewall and Service = Stopped

Victim resets connection

Source	Destination	Protocol	Length	Info
172.30.10.126	172.30.10.160	TCP	54	61631 → 80 [<u><None></u>] Seq=1 Win=102...
172.30.10.160	172.30.10.126	TCP	60	80 → 61631 [<u>RST, ACK</u>] Seq=1 Ack=1...

```

cis76@EH-Kali: ~
cis76@EH-Kali:~$ sudo nmap -sN -Pn -p 80 eh-centos

Starting Nmap 7.12 ( https://nmap.org ) at 2016-10-03 09:08 PDT
Nmap scan report for eh-centos (172.30.10.160)
Host is up (0.00071s latency).
rDNS record for 172.30.10.160: EH-Centos.cis.cabrillo.edu
PORT      STATE  SERVICE
80/tcp    closed http
MAC Address: 00:50:56:AF:04:CD (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
cis76@EH-Kali:~$

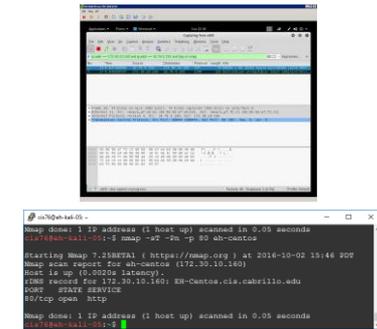
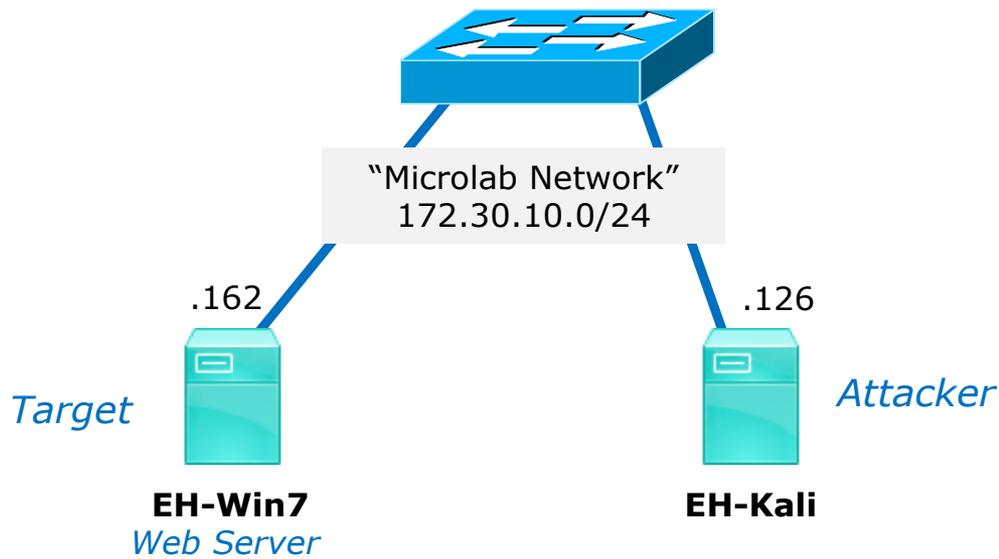
```

Null Scan (Linux)

Service	Firewall	Result
Running	no firewall	Open or filtered
Stopped	no firewall	Closed



Null Scan (Windows 7)

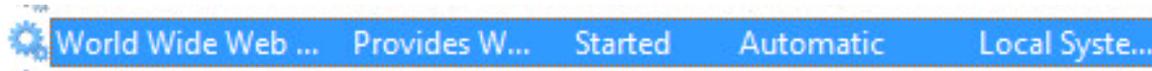


Switched to Win 7 target to see how Windows implements RFC 793 (Transmission Control Protocols)

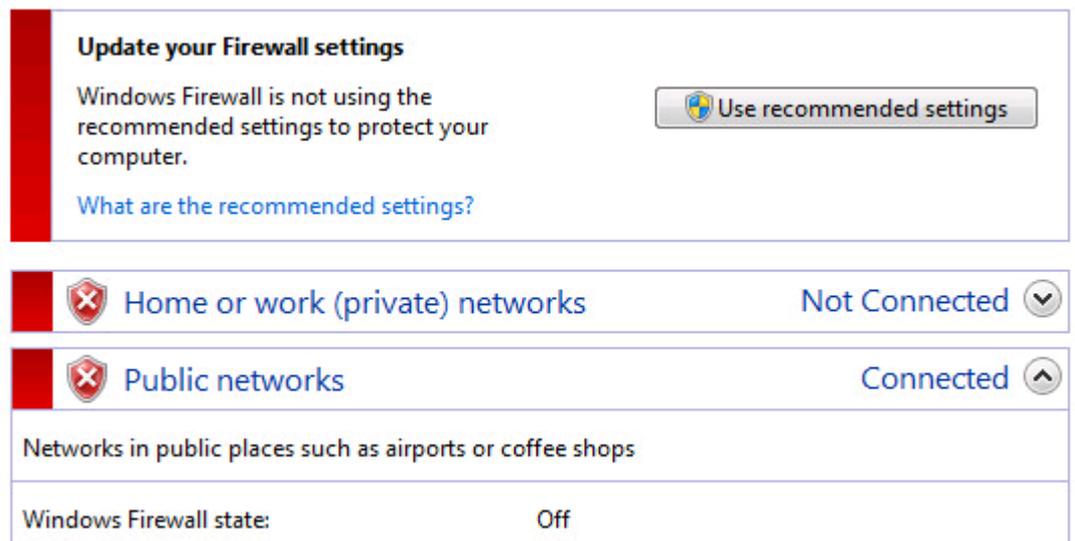
Null Scan

Firewall action = no firewall and Service = Running

Web service running



Firewall off



Null Scan

Firewall action = no firewall and Service = Running

Windows 7 sends reset when port is actually open

Source	Destination	Protocol	Length	Info
172.30.10.126	172.30.10.162	TCP	54	56023 → 80 [<u><None></u>] Seq=1 Win=102...
172.30.10.162	172.30.10.126	TCP	60	80 → 56023 [<u>RST, ACK</u>] Seq=1 Ack=1...

```

cis76@EH-Kali: ~
cis76@EH-Kali:~$ sudo nmap -sN -Pn -p 80 eh-win7

Starting Nmap 7.12 ( https://nmap.org ) at 2016-10-03 10:30 PDT
Nmap scan report for eh-win7 (172.30.10.162)
Host is up (0.00042s latency).
rDNS record for 172.30.10.162: EH-Win7.cis.cabrillo.edu
PORT      STATE  SERVICE
80/tcp    closed http
MAC Address: 00:50:56:A0:C0:7F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
cis76@EH-Kali:~$
  
```

Null Scan

Firewall action = no firewall and Service = Stopped

Web service stopped



Firewall off

A screenshot of the Windows Firewall settings window. The main heading is 'Update your Firewall settings'. Below it, a message states: 'Windows Firewall is not using the recommended settings to protect your computer.' A button labeled 'Use recommended settings' is visible. A link says 'What are the recommended settings?'. Below this, there are two network profiles: 'Home or work (private) networks' with a status of 'Not Connected' and a dropdown arrow, and 'Public networks' with a status of 'Connected' and an up arrow. At the bottom, it says 'Windows Firewall state: Off'.

Update your Firewall settings

Windows Firewall is not using the recommended settings to protect your computer.

[What are the recommended settings?](#)

[Use recommended settings](#)

Home or work (private) networks Not Connected

Public networks Connected

Networks in public places such as airports or coffee shops

Windows Firewall state: Off

Null Scan

Firewall action = no firewall and Service = Stopped

Windows sends reset when port is closed

Source	Destination	Protocol	Length	Info
172.30.10.126	172.30.10.162	TCP	54	50775 → 80 [<u><None></u>] Seq=1 Win=102...
172.30.10.162	172.30.10.126	TCP	60	80 → 50775 [<u>RST, ACK</u>] Seq=1 Ack=1...

```

cis76@EH-Kali: ~
cis76@EH-Kali:~$ sudo nmap -sN -Pn -p 80 eh-win7

Starting Nmap 7.12 ( https://nmap.org ) at 2016-10-03 10:42 PDT
Nmap scan report for eh-win7 (172.30.10.162)
Host is up (0.00041s latency).
rDNS record for 172.30.10.162: EH-Win7.cis.cabrillo.edu
PORT      STATE SERVICE
80/tcp    closed http
MAC Address: 00:50:56:A0:C0:7F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
cis76@EH-Kali:~$
  
```



Null Scan (Windows 7)

Service	Firewall	Result
Running	no firewall	Closed
Stopped	no firewall	Closed

XMAS Scan

XMAS Scan

- All FIN, PSH and URG flags are on
- Works like a null scan, closed port responds with reset
- Result is one of two states: Closed, "Open or Filtered"

```

-----
Flags: 0x029 (FIN, PSH, URG)
 000. .... = Reserved: Not set
 ...0 .... = Nonce: Not set
 .... 0... = Congestion Window Reduced (CWR): Not set
 .... .0.. = ECN-Echo: Not set
 .... ..1. = Urgent: Set
 .... ...0 = Acknowledgment: Not set
 .... .... 1... = Push: Set
 .... .... .0.. = Reset: Not set
 .... .... ..0. = Syn: Not set
 ▶ .... .... ...1 = Fin: Set
 [TCP Flags: *****U*P**F]

```

Switched to Kali on the same subnet because XMAS scans didn't get through pfSense firewall

XMAS Scan

Firewall action = no firewall and Service = Running

```
[rsimms@EH-Centos ~]$ sudo service iptables status
iptables: Firewall is not running.
[rsimms@EH-Centos ~]$

[root@EH-Centos ~]# service httpd status
httpd (pid 4196) is running...
[root@EH-Centos ~]#
```

XMAS Scan

Firewall action = no firewall and Service = Running

No response by victim

Source	Destination	Protocol	Length	Info
172.30.10.126	172.30.10.160	TCP	54	38146 → 80 [FIN, PSH, URG] Seq=1 ...
172.30.10.126	172.30.10.160	TCP	54	38147 → 80 [FIN, PSH, URG] Seq=1 ...

```

cis76@EH-Kali: ~
cis76@EH-Kali:~$ sudo nmap -sX -Pn -p 80 eh-centos

Starting Nmap 7.12 ( https://nmap.org ) at 2016-10-03 09:31 PDT
Nmap scan report for eh-centos (172.30.10.160)
Host is up (0.00047s latency).
rDNS record for 172.30.10.160: EH-Centos.cis.cabrillo.edu
PORT      STATE      SERVICE
80/tcp    open|filtered http
MAC Address: 00:50:56:AF:04:CD (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
cis76@EH-Kali:~$

```

XMAS Scan

Firewall action = no firewall and Service = Stopped

```
[root@EH-Centos ~]# service iptables status
iptables: Firewall is not running.
[root@EH-Centos ~]#

[root@EH-Centos ~]# service httpd status
httpd is stopped
[root@EH-Centos ~]#
```

XMAS Scan

Firewall action = no firewall and Service = Stopped

Victim resets connection

Source	Destination	Protocol	Length	Info
172.30.10.126	172.30.10.160	TCP	54	63013 → 80 [FIN, PSH, URG] Seq=1 ...
172.30.10.160	172.30.10.126	TCP	60	80 → 63013 [RST, ACK] Seq=1 Ack=2...

```

cis76@EH-Kali: ~
cis76@EH-Kali:~$ sudo nmap -sX -Pn -p 80 eh-centos

Starting Nmap 7.12 ( https://nmap.org ) at 2016-10-03 09:37 PDT
Nmap scan report for eh-centos (172.30.10.160)
Host is up (0.00062s latency).
rDNS record for 172.30.10.160: EH-Centos.cis.cabrillo.edu
PORT      STATE  SERVICE
80/tcp    closed http
MAC Address: 00:50:56:AF:04:CD (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
cis76@EH-Kali:~$
  
```

XMAS Scan (Linux)

Service	Firewall	Result
Running	no firewall	Open or filtered
Stopped	no firewall	Closed

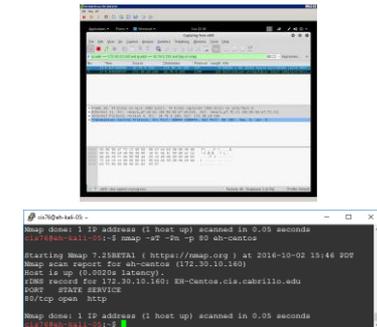
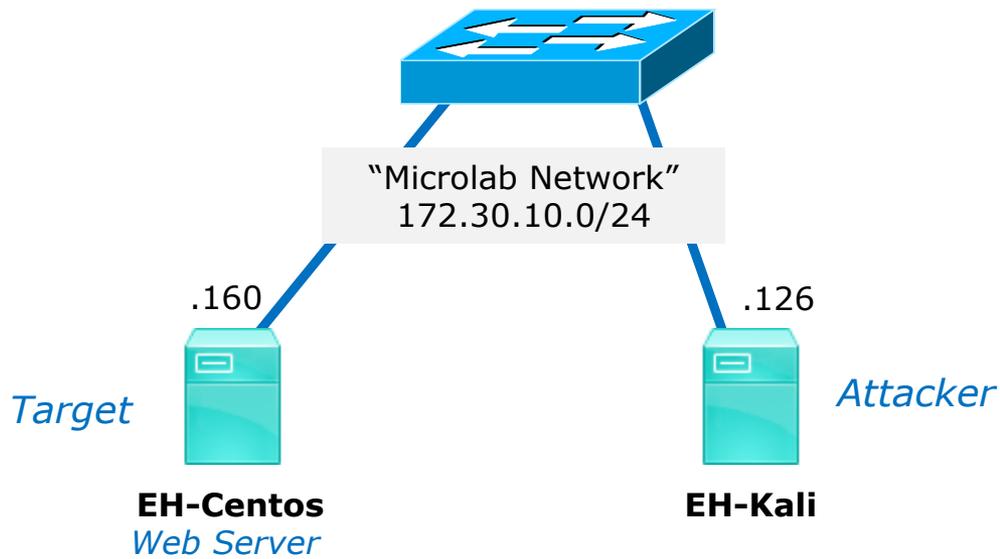
ACK Scan

ACK Scan

- Only the ACK flag is set.
- Attempts to determine the presence of a stateful firewall, not whether a port is open or closed.
- A stateful firewall always looks for a SYN to start the three-way handshake.
- If the port responds with a reset (whether open or closed) then it is considered unfiltered (no firewall or filter was fooled).
- If there is no response or an ICMP error message is returned then the port is considered filtered (whether open or closed).

```

Flags: 0x010 (ACK)
 000. .... = Reserved: Not set
 ...0 .... = Nonce: Not set
 .... 0... = Congestion Window Reduced (CWR): Not set
 .... .0.. = ECN-Echo: Not set
 .... ..0. = Urgent: Not set
 .... ...1 .... = Acknowledgment: Set
 .... .... 0... = Push: Not set
 .... .... .0.. = Reset: Not set
 .... .... ..0. = Syn: Not set
 .... .... ...0 = Fin: Not set
 [TCP Flags: *****A****]
  
```



Does EH-CentOS have an active stateful firewall?

ACK Scan

Firewall action = no firewall and Service = Running

```
[root@EH-Centos ~]# service iptables status
iptables: Firewall is not running.
[root@EH-Centos ~]#

[root@EH-Centos ~]# service httpd status
httpd (pid 9055) is running...
[root@EH-Centos ~]#
```

ACK Scan

Firewall action = no firewall and Service = Running

A reset from the victim indicates there is no stateful firewall

Source	Destination	Protocol	Length	Info
172.30.10.126	172.30.10.160	TCP	54	58579 → 80 [ACK] Seq=1 Ack=1 Win=...
172.30.10.160	172.30.10.126	TCP	60	80 → 58579 [RST] Seq=1 Win=0 Len=0

```

cis76@EH-Kali: ~
cis76@EH-Kali:~$ sudo nmap -sA -Pn -p 80 eh-centos

Starting Nmap 7.12 ( https://nmap.org ) at 2016-10-03 11:41 PDT
Nmap scan report for eh-centos (172.30.10.160)
Host is up (0.00055s latency).
rDNS record for 172.30.10.160: EH-Centos.cis.cabrillo.edu
PORT      STATE      SERVICE
80/tcp    unfiltered http
MAC Address: 00:50:56:AF:04:CD (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
cis76@EH-Kali:~$
  
```

ACK Scan

Firewall action = REJECT and Service = Running

```
[root@EH-Centos-80RunRej ~]# cat /etc/sysconfig/iptables
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 21 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 23 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 25 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j REJECT --
reject-with icmp-host-prohibited
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
[root@EH-Centos-80RunRej ~]#

[root@EH-Centos-80RunRej ~]# service httpd status
httpd (pid 1940) is running...
[root@EH-Centos-80RunRej ~]#
```

ACK Scan

Firewall action = REJECT and Service = Running

Getting the ICMP error implies victim has a firewall

Source	Destination	Protocol	Length	Info
172.30.10.126	172.30.10.165	TCP	54	59994 → 80 [ACK] Seq=1 Ack=1 Win=...
172.30.10.165	172.30.10.126	ICMP	82	Destination unreachable (Host adm...)

```

cis76@EH-Kali: ~
cis76@EH-Kali:~$ sudo nmap -sA -Pn -p 80 eh-centos-80RunRej
Starting Nmap 7.12 ( https://nmap.org ) at 2016-10-03 11:47 PDT
Nmap scan report for eh-centos-80RunRej (172.30.10.165)
Host is up (0.00065s latency).
rDNS record for 172.30.10.165: EH-Centos-80RunRej.cis.cabrillo.edu
PORT      STATE      SERVICE
80/tcp    filtered  http
MAC Address: 00:50:56:AF:E2:5B (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
cis76@EH-Kali:~$

```

ACK Scan

Firewall action = ACCEPT and Service = Running

```
[root@EH-Centos-80RunAcc ~]# cat /etc/sysconfig/iptables
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 21 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 23 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 25 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
[root@EH-Centos-80RunAcc ~]#

[root@EH-Centos-80RunAcc ~]# service httpd status
httpd (pid 1938) is running...
[root@EH-Centos-80RunAcc ~]#
```

ACK Scan

Firewall action = ACCEPT and Service = Running

Victim has firewall that was fooled, packet made it to the open port

Source	Destination	Protocol	Length	Info
172.30.10.126	172.30.10.164	TCP	54	51747 → 80 [ACK] Seq=1 Ack=1 Win=...
172.30.10.164	172.30.10.126	TCP	60	80 → 51747 [RST] Seq=1 Win=0 Len=0

```

cis76@EH-Kali: ~
Starting Nmap 7.12 ( https://nmap.org ) at 2016-10-03 12:08 PDT
Nmap scan report for eh-centos-80RunACC (172.30.10.164)
Host is up (0.00061s latency).
rDNS record for 172.30.10.164: EH-Centos-80RunAcc.cis.cabrillo.edu
PORT      STATE      SERVICE
80/tcp    unfiltered http
MAC Address: 00:50:56:AF:DF:F2 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
cis76@EH-Kali:~$ ^C
cis76@EH-Kali:~$ █
  
```



hping3

hping3

The screenshot shows the homepage of hping.org. At the top, there is a navigation menu with links for AdChoices, Windows Download, IP Port Scan, Linux Download, and Security Home. The main content area features a 'Home' section with a description of hping as a command-line oriented TCP/IP packet assembler/analyser. Below this is a circular advertisement for 'turbonomic THE OFFICIAL PUBLIC CLOUD GUIDE' with a 'FREE DOWNLOAD' button. To the right, there is a red sidebar with links for home, download, license, authors, documentation, and contacts, along with translations for 'antirez'. Below the sidebar is a section titled 'More free software' listing various tools like WBox HTTP testing, Sisopen, Visitors, Jim interpreter, TcpCAM, Php interactive, Tcl IRCd, EncrIRC, and aco2html. At the bottom, a paragraph explains that hping can be used in many ways beyond security testing, followed by a bulleted list of capabilities.

Home

hping is a command-line oriented TCP/IP packet assembler/analyser. The interface is inspired to the ping(8) unix command, but hping isn't only able to send ICMP echo requests. It supports TCP, UDP, ICMP and RAW-IP protocols, has a traceroute mode, the ability to send files between a covered channel, and many other features.

home
download
license
authors
documentation
contacts

» hping wiki
 » antirez (en)
 » antirez (it)
 » see also

More free software

WBox HTTP testing
 Sisopen
 Visitors
 Jim interpreter
 TcpCAM
 Php interactive
 Tcl IRCd
 EncrIRC
 aco2html

While hping was mainly used as a security tool in the past, it can be used in many ways by people that don't care about security to test networks and hosts. A subset of the stuff you can do using hping:

- Firewall testing
- Advanced port scanning
- Network testing, using different protocols, TOS, fragmentation
- Manual path MTU discovery
- Advanced traceroute, under all the supported protocols
- Remote OS fingerprinting
- Remote uptime guessing
- TCP/IP stacks auditing
- hping can also be useful to students that are learning TCP/IP.

<http://www.hping.org/>

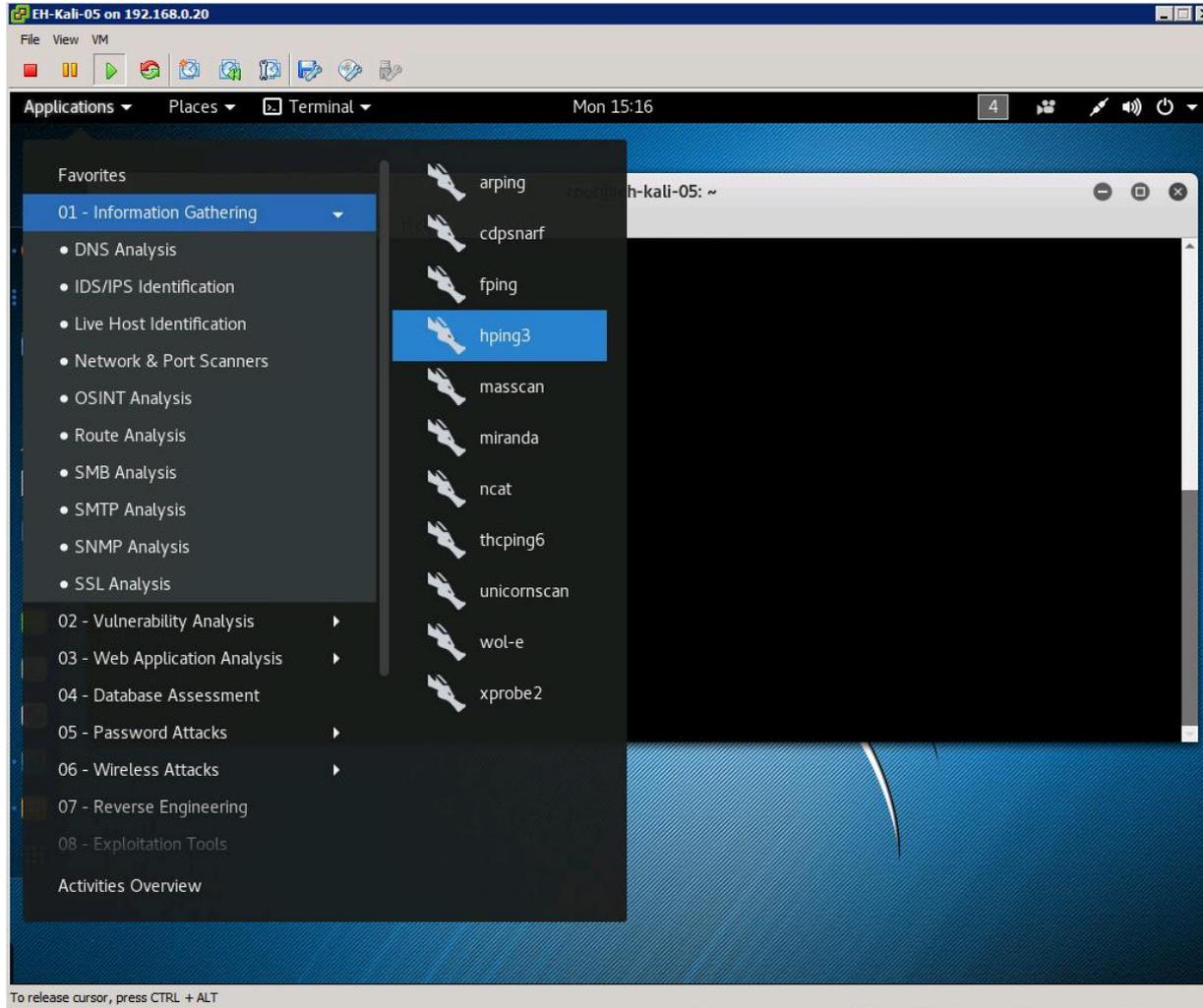
hping3

"hping is a command-line oriented TCP/IP packet assembler/analyzer. The interface is inspired to the ping(8) unix command, but hping isn't only able to send ICMP echo requests. It supports TCP, UDP, ICMP and RAW-IP protocols, has a traceroute mode, the ability to send files between a covered channel, and many other features."

-- hping3 website

<http://www.hping.org/>

hping3



hping3

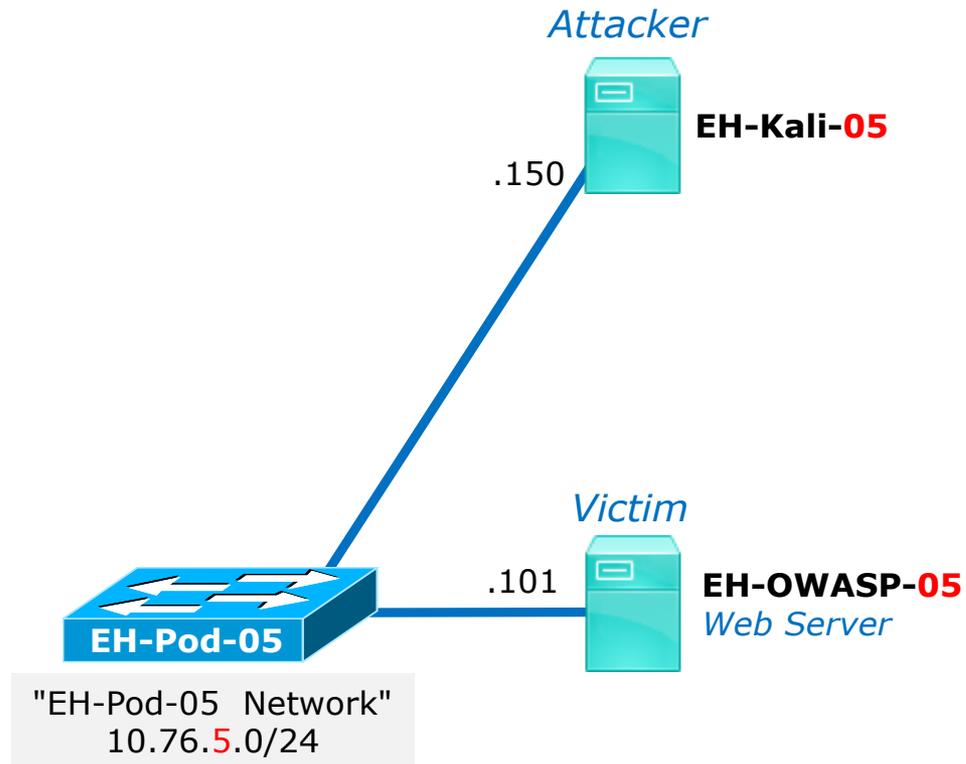
```

EH-Kali-05 on 192.168.0.20
File Edit View Search Terminal Help
root@eh-kali-05: ~
root@eh-kali-05:~# hping3 -h
usage: hping3 host [options]
-h --help      show this help
-v --version   show version
-c --count     packet count
-i --interval  wait (uX for X microseconds, for example -i u1000)
               --fast      alias for -i u10000 (10 packets for second)
               --faster    alias for -i u1000 (100 packets for second)
               --flood     sent packets as fast as possible. Don't show replies.
-n --numeric   numeric output
-q --quiet     quiet
-I --interface interface name (otherwise default routing interface)
-V --verbose   verbose mode
-D --debug     debugging info
-z --bind      bind ctrl+z to ttl           (default to dst port)
-Z --unbind   unbind ctrl+z
--beep        beep for every matching packet received

Mode
default mode  TCP
-0 --rawip    RAW IP mode
-1 --icmp     ICMP mode
-2 --udp      UDP mode
-8 --scan     SCAN mode.
Example: hping --scan 1-30,70-90 -S www.target.host
-9 --listen   listen mode

IP
-a --spooft   spoof source address
--rand-dest   random destination address mode. see the man.
--rand-source random source address mode. see the man.
-t --ttl      ttl (default 64)
-N --id       id (default random)
-W --winid    use win* id byte ordering
-r --rel      relativize id field           (to estimate host traffic)
-f --frag     split packets in more frag. (may pass weak acl)
-x --morefrag set more fragments flag
-y --dontfrag set don't fragment flag
-g --fragoff  set the fragment offset
-m --mtu      set virtual mtu. implies --frag if packet size > mtu

```



hping3

hping3 -c 2 10.76.5.101

```

root@eh-kali-05: ~
root@eh-kali-05:~# hping3 -c 2 10.76.5.101
HPING 10.76.5.101 (eth0 10.76.5.101): NO FLAGS are set, 40 headers + 0 data bytes
len=46 ip=10.76.5.101 ttl=64 DF id=0 sport=0 flags=RA seq=0 win=0 rtt=0.4 ms
len=46 ip=10.76.5.101 ttl=64 DF id=0 sport=0 flags=RA seq=1 win=0 rtt=0.3 ms

--- 10.76.5.101 hping statistic ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 0.3/0.3/0.4 ms
root@eh-kali-05:~#
  
```

Source	Destination	Protocol	Length	Info
10.76.5.150	10.76.5.101	TCP	54	2344 → 0 [<none>] Seq=1 Win=512 Len=0</none>
10.76.5.101	10.76.5.150	TCP	60	0 → 2344 [RST, ACK] Seq=1 Ack=1 Win=...
10.76.5.150	10.76.5.101	TCP	54	2345 → 0 [<none>] Seq=1 Win=512 Len=0</none>
10.76.5.101	10.76.5.150	TCP	60	0 → 2345 [RST, ACK] Seq=1 Ack=1 Win=...

```

Flags: 0x000 (<None>)
 000. .... = Reserved: Not set
...0 .... = Nonce: Not set
.... 0... = Congestion Window Reduced (CWR): Not set
.... 0... = ECN-Echo: Not set
.... ..0. = Urgent: Not set
.... ...0 = Acknowledgment: Not set
.... .... 0... = Push: Not set
.... .... 0... = Reset: Not set
.... .... 0. = Syn: Not set
.... .... ..0 = Fin: Not set
[TCP Flags: *****]
  
```

*This does two null scans
of port 0 on 10.76.5.1*

hping3

hping3 --scan 79-84 -S 10.76.5.101

```

root@eh-kali-05: ~
root@eh-kali-05:~# hping3 --scan 79-84 -S 10.76.5.101
Scanning 10.76.5.101 (10.76.5.101), port 79-84
6 ports to scan, use -V to see all the replies
+---+-----+-----+-----+-----+-----+
|port| serv name | flags |ttl| id  | win | len |
+---+-----+-----+-----+-----+-----+
  80 http      : .S..A... 64   0 5840 46
All replies received. Done.
Not responding ports:
root@eh-kali-05:~#
  
```

Source	Destination	Protocol	Length	Info
10.76.5.150	10.76.5.101	TCP	54	1546 → 79 [SYN] Seq=0 Win=512 Len=0
10.76.5.150	10.76.5.101	TCP	54	1546 → 80 [SYN] Seq=0 Win=512 Len=0
10.76.5.150	10.76.5.101	TCP	54	1546 → 81 [SYN] Seq=0 Win=512 Len=0
10.76.5.150	10.76.5.101	TCP	54	1546 → 82 [SYN] Seq=0 Win=512 Len=0
10.76.5.150	10.76.5.101	TCP	54	1546 → 83 [SYN] Seq=0 Win=512 Len=0
10.76.5.150	10.76.5.101	TCP	54	1546 → 84 [SYN] Seq=0 Win=512 Len=0
10.76.5.101	10.76.5.150	TCP	60	79 → 1546 [RST, ACK] Seq=1 Ack=1 W...
10.76.5.101	10.76.5.150	TCP	60	80 → 1546 [SYN, ACK] Seq=0 Ack=1 W...
10.76.5.150	10.76.5.101	TCP	54	1546 → 80 [RST] Seq=1 Win=0 Len=0
10.76.5.101	10.76.5.150	TCP	60	81 → 1546 [RST, ACK] Seq=1 Ack=1 W...
10.76.5.101	10.76.5.150	TCP	60	82 → 1546 [RST, ACK] Seq=1 Ack=1 W...
10.76.5.101	10.76.5.150	TCP	60	83 → 1546 [RST, ACK] Seq=1 Ack=1 W...
10.76.5.101	10.76.5.150	TCP	60	84 → 1546 [RST, ACK] Seq=1 Ack=1 W...

This does a SYN scan of ports 79-84

[TCP Flags: *****S*]

hping3

hping3 --udp --rand-source --data 20 -c 5 10.76.5.101

```

root@eh-kali-05: ~
root@eh-kali-05:~# hping3 --udp --rand-source --data 20 -c 5 10.76.5.101
HPING 10.76.5.101 (eth0 10.76.5.101): udp mode set, 28 headers + 20 data bytes

--- 10.76.5.101 hping statistic ---
5 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@eh-kali-05:~# █
    
```

Source	Destination	Protocol	Length	Info
184.136.23.38	10.76.5.101	UDP	62	1421 → 0 Len=20
248.130.42.248	10.76.5.101	UDP	62	1422 → 0 Len=20
57.39.179.18	10.76.5.101	UDP	62	1423 → 0 Len=20
124.230.14.100	10.76.5.101	UDP	62	1424 → 0 Len=20
154.193.225.251	10.76.5.101	UDP	62	1425 → 0 Len=20

```

Data (20 bytes)
Data: 5858585858585858585858585858585858585858585858
[Length: 20]
    
```

This sends 5 UDP packets from random IP addresses (spoofing) with 20 bytes of data to eh-owasp-05

0020	05 65 05 8d 00 00 00 1c a7 56	58 58 58 58 58 58	.e..... .vXXXXXX
0030	58 58 58 58 58 58 58 58	58 58 58 58 58 58	XXXXXXXX XXXXXX

hping3

hping3 -S -p 80 -c 3 10.76.5.101

```

root@eh-kali-05: ~
root@eh-kali-05:~# hping3 -S -p 80 -c 3 10.76.5.101
HPING 10.76.5.101 (eth0 10.76.5.101): S set, 40 headers + 0 data bytes
len=46 ip=10.76.5.101 ttl=64 DF id=0 sport=80 flags=SA seq=0 win=5840 rtt=2.9 ms
len=46 ip=10.76.5.101 ttl=64 DF id=0 sport=80 flags=SA seq=1 win=5840 rtt=0.4 ms
len=46 ip=10.76.5.101 ttl=64 DF id=0 sport=80 flags=SA seq=2 win=5840 rtt=0.4 ms

--- 10.76.5.101 hping statistic ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.4/1.2/2.9 ms
root@eh-kali-05:~# history

```

Source	Destination	Protocol	Length	Info
10.76.5.150	10.76.5.101	TCP	56	2164 → 80 [SYN] Seq=0 Win=512 Len=0
10.76.5.101	10.76.5.150	TCP	62	80 → 2164 [SYN, ACK] Seq=0 Ack=1 W...
10.76.5.150	10.76.5.101	TCP	56	2164 → 80 [RST] Seq=1 Win=0 Len=0
10.76.5.150	10.76.5.101	TCP	56	2165 → 80 [SYN] Seq=0 Win=512 Len=0
10.76.5.101	10.76.5.150	TCP	62	80 → 2165 [SYN, ACK] Seq=0 Ack=1 W...
10.76.5.150	10.76.5.101	TCP	56	2165 → 80 [RST] Seq=1 Win=0 Len=0
10.76.5.150	10.76.5.101	TCP	56	2166 → 80 [SYN] Seq=0 Win=512 Len=0
10.76.5.101	10.76.5.150	TCP	62	80 → 2166 [SYN, ACK] Seq=0 Ack=1 W...
10.76.5.150	10.76.5.101	TCP	56	2166 → 80 [RST] Seq=1 Win=0 Len=0

[TCP Flags: *****S*]

This does 3 SYN scans of port 80 on eh-owasp-05. Note the connection is never completed.

hping3

Only used to see how long it takes to send the packets

time hping3 -V -p 80 --rand-source --flood 10.76.5.101

```

root@eh-kali-05: ~
root@eh-kali-05:~# time hping3 -V -p 80 --rand-source --flood 10.76.5.101
using eth0, addr: 10.76.5.150, MTU: 1500
HPING 10.76.5.101 (eth0 10.76.5.101): NO FLAGS are set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 10.76.5.101 hping statistic ---
351972 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

real    0m3.506s
user    0m0.316s
sys     0m1.408s
root@eh-kali-05:~#
  
```

Source	Destination	Protocol	Length	Info
6.131.101.238	10.76.5.101	TCP	56	2401 → 80 [<none>] Seq=1 Win=512 L...</none>
89.180.202.142	10.76.5.101	TCP	56	2402 → 80 [<none>] Seq=1 Win=512 L...</none>
33.37.155.186	10.76.5.101	TCP	56	2621 → 80 [<none>] Seq=1 Win=512 L...</none>
199.187.218.250	10.76.5.101	TCP	56	2622 → 80 [<none>] Seq=1 Win=512 L...</none>
27.32.137.124	10.76.5.101	TCP	56	2623 → 80 [<none>] Seq=1 Win=512 L...</none>
111.243.110.32	10.76.5.101	TCP	56	2624 → 80 [<none>] Seq=1 Win=512 L...</none>

This command sent 351,972 spoofed packets in three and a half seconds! --flood is "fast as you can", -V is verbose.



Vulnerability Scans



Nessus

nessus

The screenshot shows the Tenable Network Security website homepage. The browser address bar displays "https://www.tenable.com". The page features a dark teal header with the Tenable logo and navigation links for "Partners", "Careers", "Language", and "Login". A main navigation bar includes "Products +", "Support & Services +", "Company +", and a prominent orange "How to Buy" button. The central hero section has a dark teal background with a network diagram and the headline "Assets & Threats Are Changing Dramatically". Below the headline is a sub-headline: "Discover how next-generation vulnerability management can help you see and understand assets and threats never visible before." A white button with the text "See what you're missing" is positioned to the right. At the bottom of the hero section are four small white circles. Below the hero section, the text "We brought you Nessus." is displayed in a light teal font, followed by "And today, we continue to revolutionize cybersecurity for...". Two statistics are shown: "20,000+ CUSTOMERS" and "1,000,000+ USERS", both in orange text.

<https://www.tenable.com/>

nessus

"**Nessus**, the industry-leading vulnerability scanner, has been adopted by millions of users worldwide. Nessus discovers all assets on your network -- even hard-to-find assets like containers, VMs, mobile and guest devices – and informs you clearly and accurately about their vulnerabilities and prioritizes what you need to fix first. Nessus is available as both a cloud and on-premises vulnerability scanning and management solution."

-- Tenable website

<https://www.tenable.com/products>

nessus

Nessus Professional

Nessus Professional - Annual Subscription (New)



Model: **SERV-NES**

Price: **\$2,190.00**

Add to Cart:

Add to Cart

nessus



Nessus® Home allows you to scan your personal home network (up to 16 IP addresses per scanner) with the same high-speed, in-depth assessments and agentless scanning convenience that Nessus subscribers enjoy.

Please note that Nessus Home does not provide access to support, allow you to perform compliance checks or content audits, or allow you to use the Nessus virtual appliance. If you require support and these [additional features](#), please purchase a [Nessus](#) subscription.

Nessus Home is available for personal use in a home environment only. It is not for use by any commercial organization.

<https://www.tenable.com/products/nessus-home>



Nikto

Nikto

"Nikto is an Open Source ([GPL](#)) web server scanner which performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files/programs, checks for outdated versions of over 1250 servers, and version specific problems on over 270 servers. It also checks for server configuration items such as the presence of multiple index files, HTTP server options, and will attempt to identify installed web servers and software. Scan items and plugins are frequently updated and can be automatically updated."

- Nikto website

<https://cirt.net/nikto2>

OpenVAS

OpenVAS

OpenVAS - OpenVAS - C x

www.openvas.org

English | Deutsch

OpenVAS About OpenVAS Try out OpenVAS Support Development Contact

Download OpenVAS

OpenVAS

OpenVAS CLI OpenVAS Scanner OpenVAS Manager OpenVAS Administrator OpenVAS Results

News

2015-04-02
OpenVAS-8 released

2014-04-25
OpenVAS-7 released

2013-04-17
OpenVAS-6 released

Older messages in news archive.

The world's most advanced Open Source vulnerability scanner and manager

OpenVAS is a framework of several services and tools offering a comprehensive and powerful vulnerability scanning and vulnerability management solution.

Discover OpenVAS

Learn what OpenVAS is and read more about the features of our solution!
[About OpenVAS »](#)

Try out OpenVAS

We help you to install and set up OpenVAS. Learn about the architecture of OpenVAS and try it out in ready to use Virtual Machine.
[Try out OpenVAS in a Virtual Machine »](#)

Join the community

OpenVAS is Free Software. Join the community! We recommend subscribing to the OpenVAS-Announcement mailing list to be automatically informed about new releases and other important OpenVAS news.
[Join the Online Chat »](#)

<http://www.openvas.org/>

OpenVAS

Applications ▾ Places ▾ Firefox ESR ▾ Tue 11:28

Greenbone Security Assistant - Mozilla Firefox

Kali Linux, an Offensive S... x Greenbone Security A... x

https://127.0.0.1:9392/omp?r=1&token=463d82ea-31be-4be

Most Visited ▾ Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng

Greenbone Security Assistant Logged in as Admin admin | Logout
Tue Oct 4 18:28:35 2016 UTC

Scan Management Asset Management SecInfo Management Configuration Extras Administration Help

Tasks 1 - 2 of 2 (total: 2) Refresh every 30 Sec.

Filter: apply_overrides=1 rows=10 first=1 sort=name

Name	Status	Reports		Severity	Trend	Actions
		Total	Last			
Immediate scan of IP 10.76.5.1	Done	1 (1)	Oct 4 2016	4.3 (Medium)		
Immediate scan of IP 10.76.5.101	Done	1 (1)	Oct 4 2016	10.0 (High)		

(Applied filter: apply_overrides=1 rows=10 first=1 sort=name) 1 - 2 of 2 (total: 2)

Welcome dear new user!
To explore this powerful application and to have a quick start for doing things the first time, I am here to assist you with some hints and short-cuts.

I will appear automatically in areas where you have created no or only a few objects. And disappear when you have more than 3 objects. You can call me with this icon any time later on.

If you want help creating new scan tasks but also more options, you can select "Advanced Task Wizard" from the wizard selection menu at the top of this window where it currently

Quick start: Immediately scan an IP address
IP address or hostname:

For this short-cut I will do the following for you:

1. Create a new Target with default Port List
2. Create a new Task using this target with default Scan Configuration
3. Start this scan task right away
4. Switch the view to reload every 30 seconds so you can lean back and watch the scan progress

In fact, you must not lean back. As soon as the scan progress is

<http://www.openvas.org/>

OpenVAS

Greenbone Security Assistant Logged in as Admin **admin** | Logout
Tue Oct 4 18:30:24 2016 UTC

Scan Management | Asset Management | SecInfo Management | Configuration | Extras | Administration | Help

▼ Report: Results 1 - 34 of 34 (total: 36) PDF Done

Filter: sort-reverse=severity result_hosts_only=1 min_cvss_base= min_qo

Vulnerability	Severity	QoD	Host	Location	Actions
SSH Weak Encryption Algorithms Supported	4.3 (Medium)	95%	10.76.5.1 (gateway)	22/tcp	
TCP timestamps	2.6 (Low)	80%	10.76.5.1 (gateway)	general/tcp	
ICMP Timestamp Detection	0.0 (Log)	80%	10.76.5.1 (gateway)	general/icmp	
OS Detection	0.0 (Log)	95%	10.76.5.1 (gateway)	general/tcp	
Traceroute	0.0 (Log)	80%	10.76.5.1 (gateway)	general/tcp	
CPE Inventory	0.0 (Log)	80%	10.76.5.1 (gateway)	general/CPE-T	
SSH Protocol Versions Supported	0.0 (Log)	95%	10.76.5.1 (gateway)	22/tcp	
SSH Server type and version	0.0 (Log)	80%	10.76.5.1 (gateway)	22/tcp	
Services	0.0 (Log)	80%	10.76.5.1 (gateway)	22/tcp	
SSH Protocol Algorithms Supported	0.0 (Log)	95%	10.76.5.1 (gateway)	22/tcp	

<http://www.openvas.org/>

OpenVAS

 **Greenbone**
Security Assistant

 Logged in as Admin **admin** | Logout
Tue Oct 4 18:31:39 2016 UTC

Scan Management
Asset Management
SecInfo Management
Configuration
Extras
Administration
Help

Result Details   

Task: [Immediate scan of IP 10.76.5.1](#) ID: 46650c15-47af-4686-8260-4594f14d8879

Vulnerability	Severity	QoD	Host	Location	Actions
SSH Weak Encryption Algorithms Supported	4.3 (Medium)	95%	10.76.5.1	22/tcp	 

Summary
The remote SSH server is configured to allow weak encryption algorithms.

Vulnerability Detection Result

The following weak client-to-server encryption algorithms are supported by the remote service:

```

aes128-cbc
aes256-cbc
arcfour
arcfour256
        
```

The following weak server-to-client encryption algorithms are supported by the remote service:

```

aes128-cbc
aes256-cbc
arcfour
arcfour256
        
```

Solution
Disable the weak encryption algorithms.

Vulnerability Insight

<http://www.openvas.org/>

OpenVAS

The following weak server-to-client encryption algorithms are supported by the remote service:

aes128-cbc
aes256-cbc
arcfour
arcfour256

Solution

Disable the weak encryption algorithms.

Vulnerability Insight

The `arcfour` cipher is the Arcfour stream cipher with 128-bit keys. The Arcfour cipher is believed to be compatible with the RC4 cipher [SCHNEIER]. Arcfour (and RC4) has problems with weak keys, and should not be used anymore.

The `none` algorithm specifies that no encryption is to be done. Note that this method provides no confidentiality protection, and it is NOT RECOMMENDED to use it.

A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to recover plaintext from a block of ciphertext.

Vulnerability Detection Method

Check if remote ssh service supports Arcfour, none or CBC ciphers.

Details: [SSH Weak Encryption Algorithms Supported \(OID: 1.3.6.1.4.1.25623.1.0.105611\)](#)

Version used: \$Revision: 3160 \$

References

Other: <https://tools.ietf.org/html/rfc4253#section-6.3>
<https://www.kb.cert.org/vuls/id/958563>

User Tags for this Result: none

Backend operation: 0.25s

Greenbone Security Assistant (GSA) Copyright 2009-2016 by Greenbone Networks GmbH, www.greenbone.net

<http://www.openvas.org/>

Assignment



Cabrillo College



Lab 5: Scanning

This lab takes a look at doing port scans using nmap then following up with deeper vulnerability scans using ~~Nikto~~ and OpenVAS

Warning and Permission

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

For this lab you have authorization to hack the VMs in the VLab pod assigned to you.

Preparation

- Get the CIS 76 Login Credentials document. You will need usernames and passwords to log into VLab and each of the VMs. This document is on Canvas and the link is in the CIS 76 Welcome letter.
- Determine which VLab pod number you were assigned. See the link on the left panel of the class website.

Part 1 - Pod configuration

- 1) If you haven't already configured your pod in the previous labs, then follow the instructions here: <https://simms-teach.com/docs/cis76/cis76-podSetup.pdf>

*Lab 5 due
next week*



Wrap up

Next Class

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

Lab 5

Quiz questions for next class:

Insure the apache2 service is running on your OWASP VM:

- From your pod Kali, do a SYN scan of your OWASP VM, what is the status of port 80?
- From your pod Kali, do a ACK scan on port 80 on your OWASP VM. Is a stateful firewall present?
- From your pod Kali, do a NULL scan on port 25 of your OWASP VM. Is an SMTP service running?



Test 1



Notes to instructor

[] Schedule end of practice test on Canvas *[T-30]*

[] Remove password on real test on Canvas *[T-0]*

[] Add Steganography file to /home/cis76/depot

```
cp ~/cis76/test01/bryce-76.jpg /home/cis76/depot [at job T-0]
```

[] Schedule end of real test on Canvas *[at splashdown-1]*



Test 1



Backup

