Last updated 10/4/2016

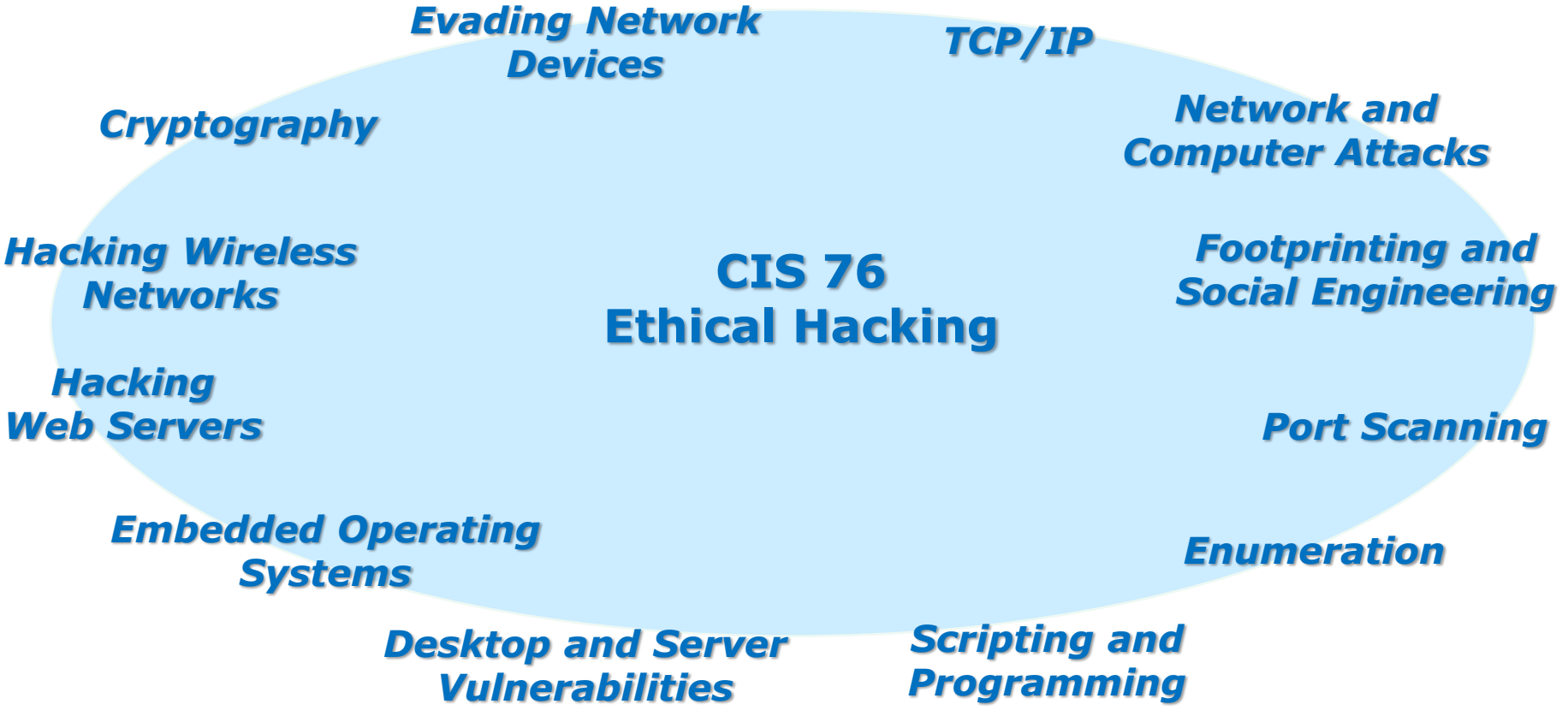
Rich's lesson module checklist

- ❑ 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.

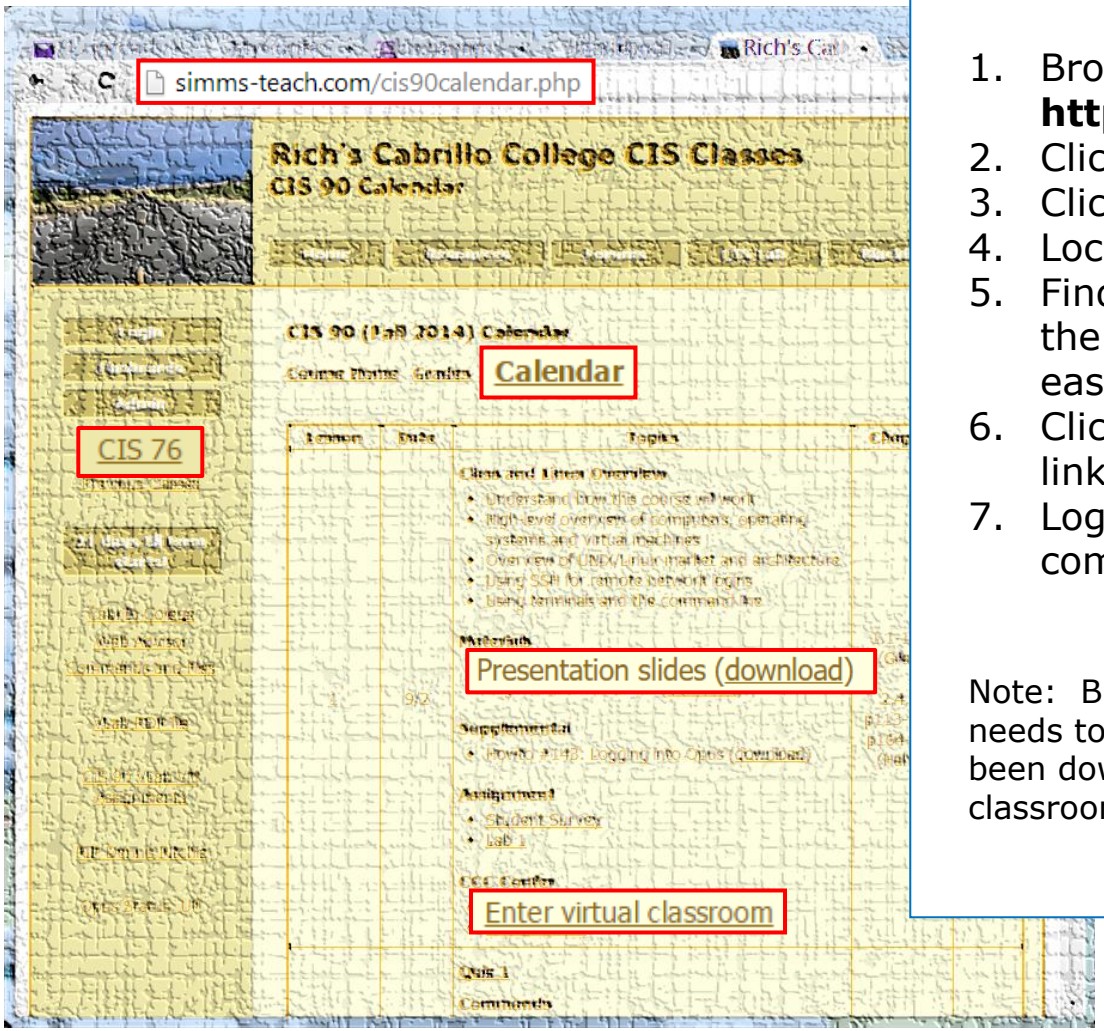
2. Defend a computer and a LAN against a variety of different types of security attacks using a number of hands-on techniques.

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

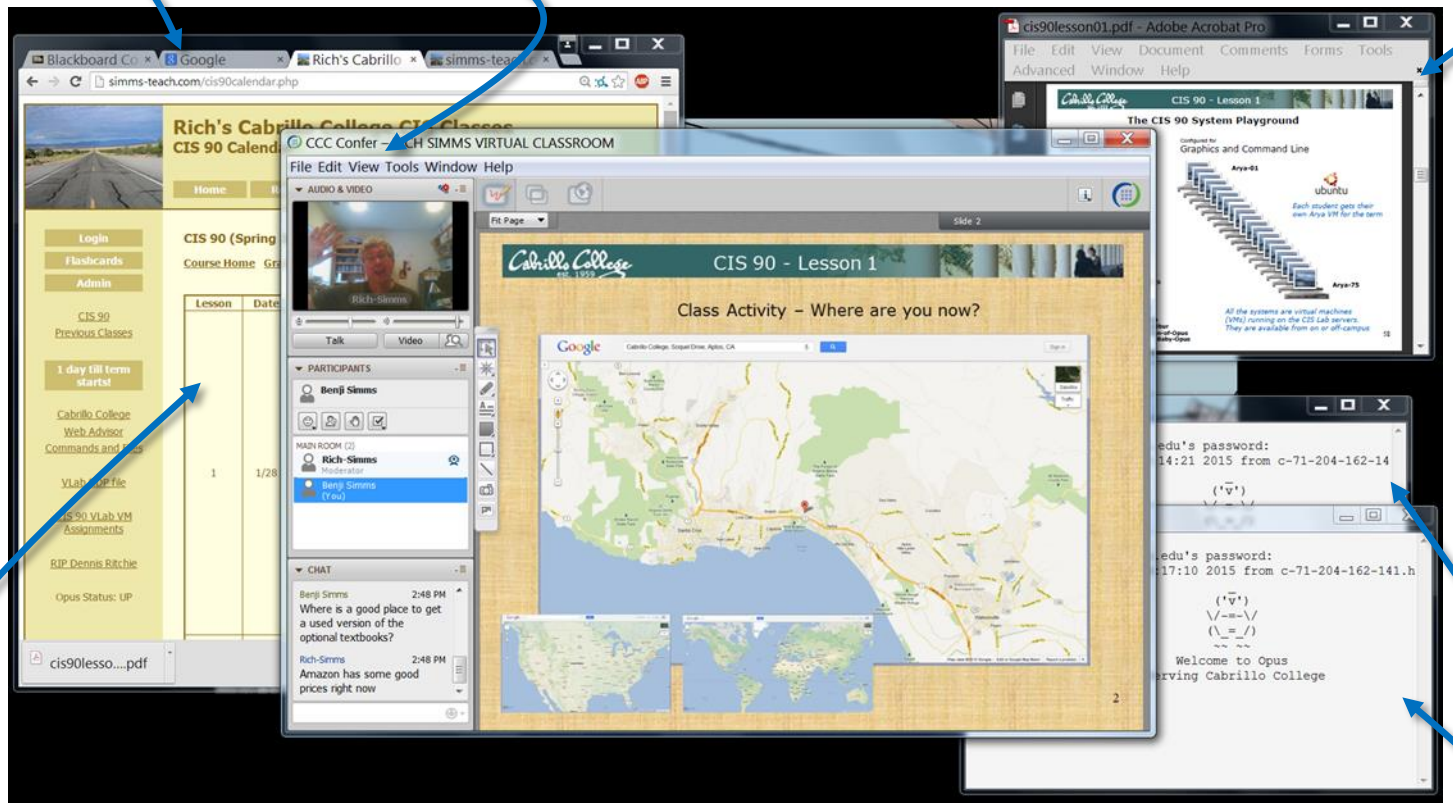


1. Browse to: **http://simms-teach.com**
2. Click the **CIS 76** link.
3. Click the **Calendar** link.
4. Locate today's lesson.
5. Find the **Presentation slides** for the lesson and **download** for easier viewing.
6. Click the **Enter virtual classroom** link to join CCC Confer.
7. Log into Opus with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

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

Student checklist for suggested screen layout

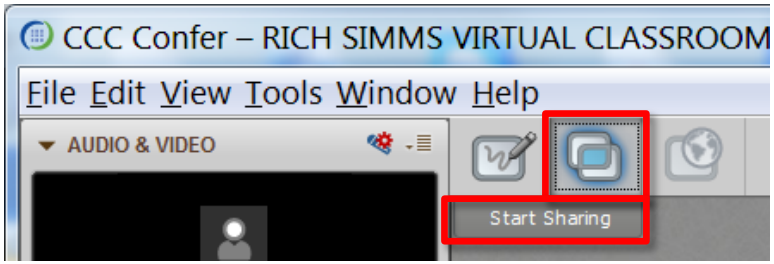
- ❑ *Google*
- ❑ *CCC Confer*
- ❑ *Downloaded PDF of Lesson Slides*



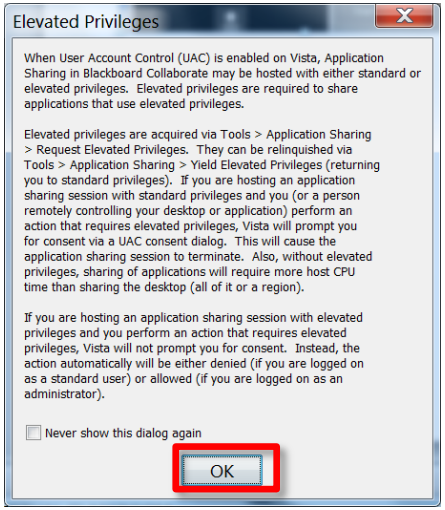
- ❑ *CIS 76 website Calendar page*
- ❑ *One or more login sessions to Opus*

Student checklist for sharing desktop with classmates

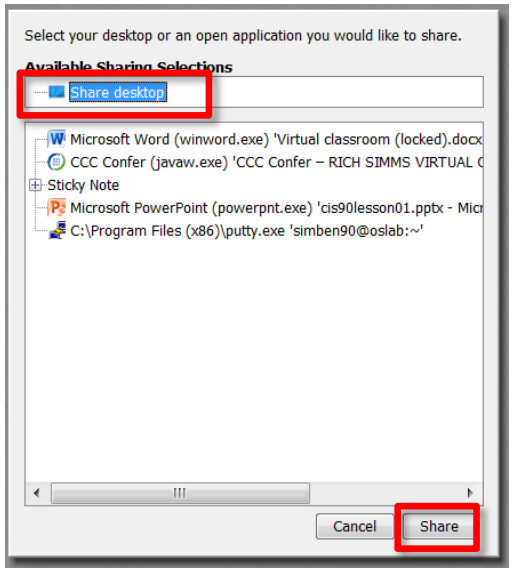
1) Instructor gives you sharing privileges.



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



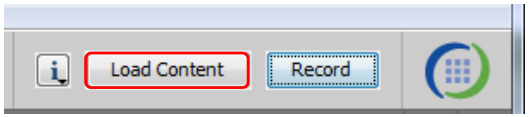
3) Click OK button.



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

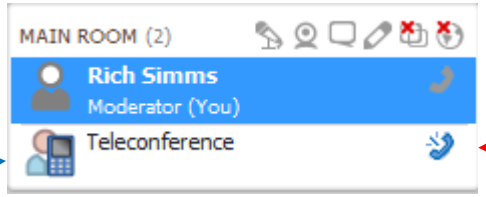
Rich's CCC Confer checklist - setup

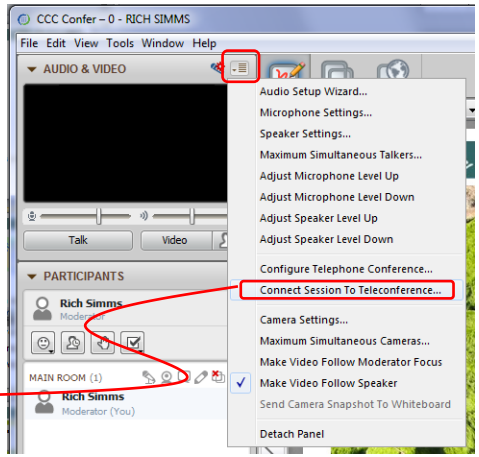
[ ] Preload White Board



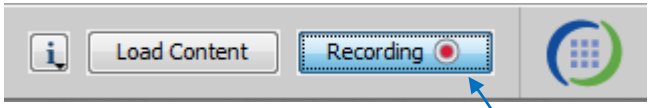
[ ] Connect session to Teleconference

Session now connected to teleconference





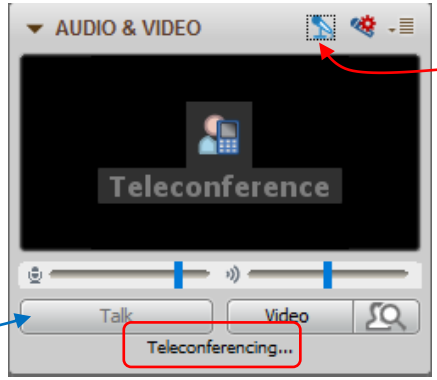
[ ] Is recording on?



Red dot means recording

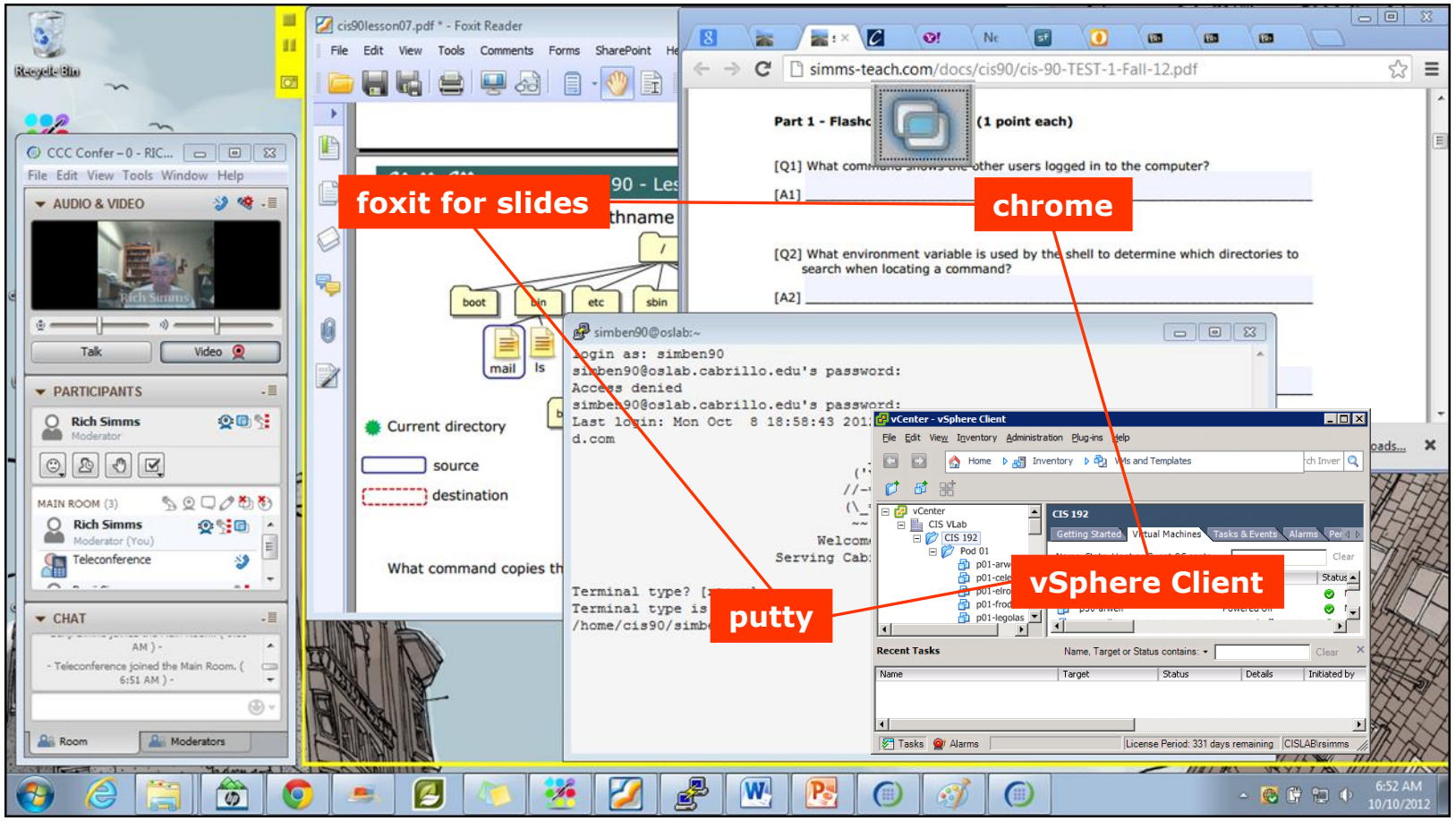
[ ] Use teleconferencing, not mic

Should be grayed out



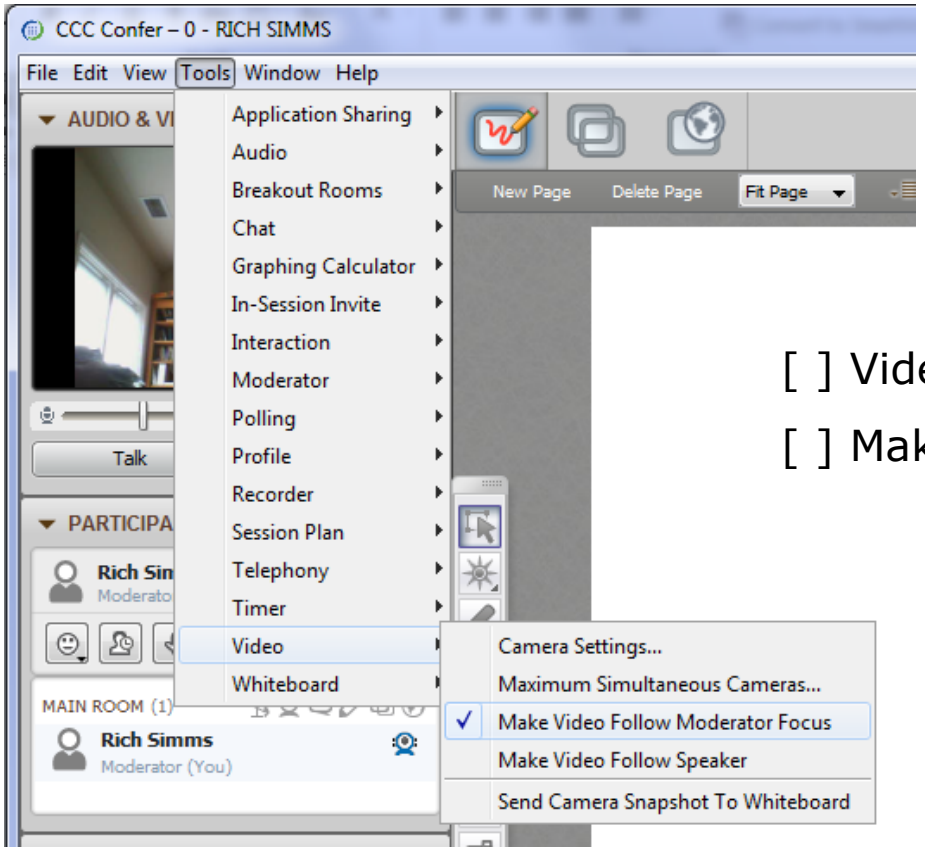
Should change from phone handset icon to little Microphone icon and the Teleconferencing … message displayed

Rich's CCC Confer checklist - screen layout



[ ] layout and share apps

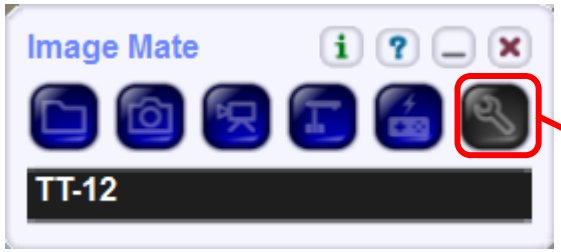
Rich's CCC Confer checklist - webcam setup

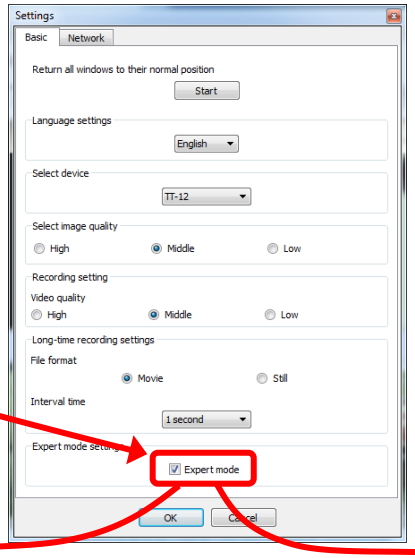


[ ] Video (webcam)

[ ] Make Video Follow Moderator Focus

Rich's CCC Confer checklist - Elmo



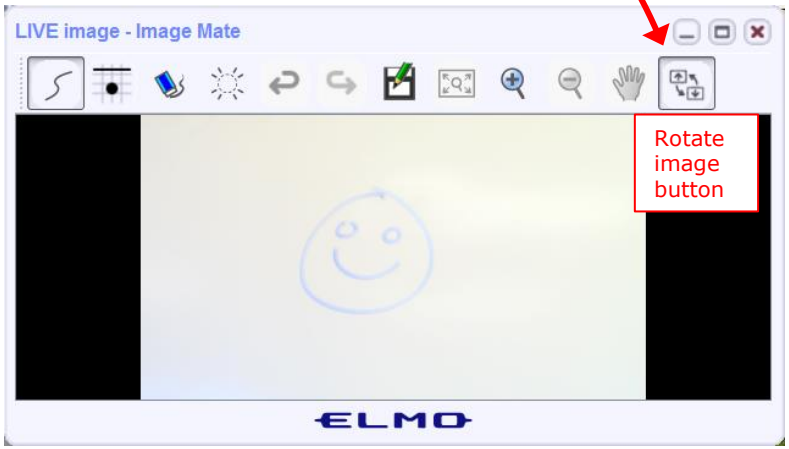


The "rotate image" button is necessary if you use both the side table and the white board.

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

Elmo rotated down to view side table

Elmo rotated up to view white board



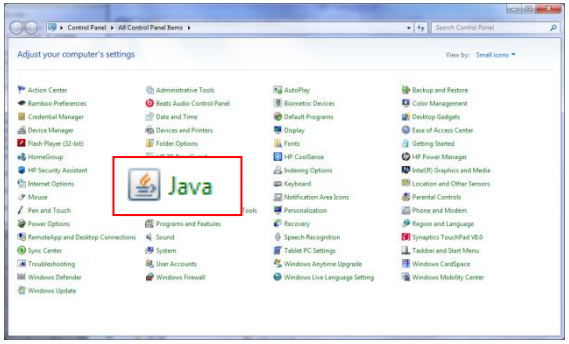
Run and share the Image Mate program just as you would any other app with CCC Confer

Rich's CCC Confer checklist - universal fixes

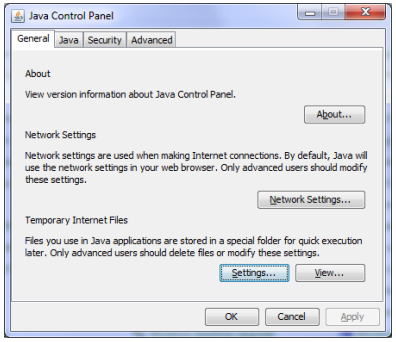
Universal Fix for CCC Confer:

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

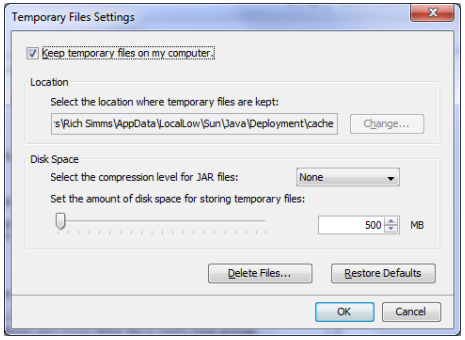
Control Panel (small icons)



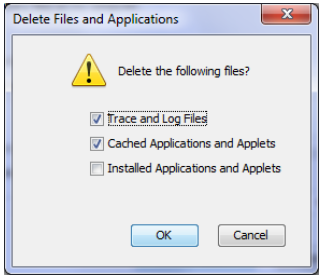
General Tab > Settings…



500MB cache size



Delete these



Google Java download

Start

Sound Check

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

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

CIS 76 - Lesson 6

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

Scanning

Objectives	Agenda
• Understand different types of port scans • Look at port scan tools • Understand vulnerability scans • Look at vulnerability scan tools	• 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

https://www.us-cert.gov/ncas/bulletins/SB16-277

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:

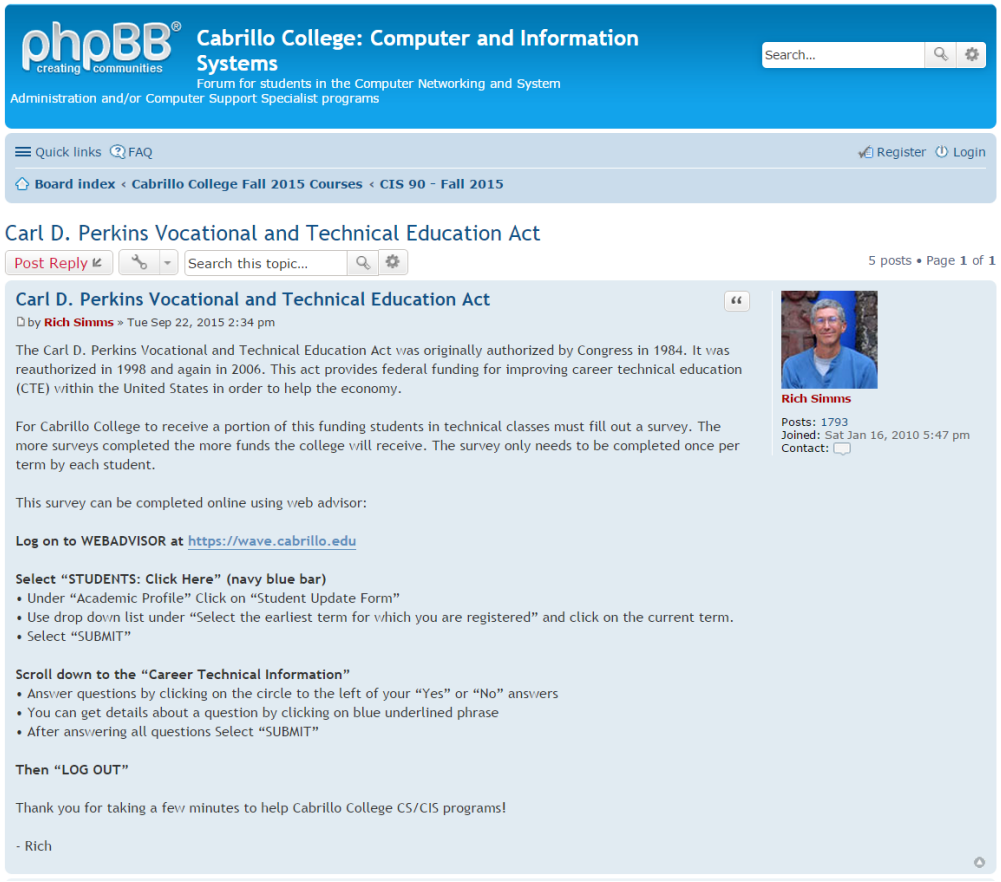
This test is open book, open notes, and open computer.

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 creating communities

Cabrillo College: Computer and Information Systems

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

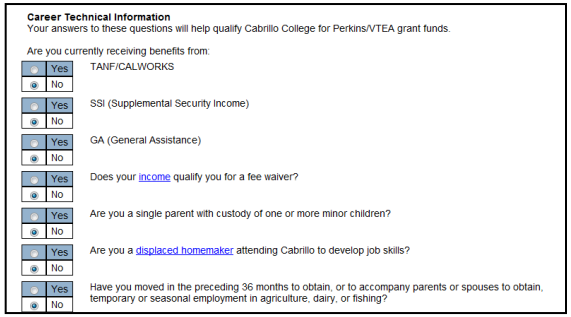
Rich Simms

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:

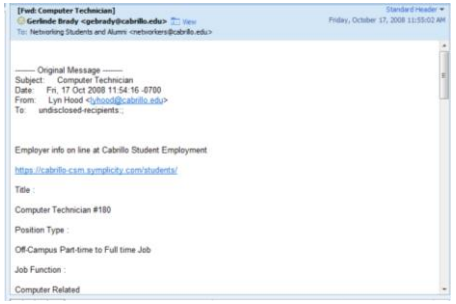
Yes / No	TANF/CALWORKS
Yes / No	SSI (Supplemental Security Income)
Yes / No	GA (General Assistance)
Yes / No	Does your income qualify you for a fee waiver?
Yes / No	Are you a single parent with custody of one or more minor children?
Yes / No	Are you a displaced homemaker attending Cabrillo to develop job skills?
Yes / No	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?

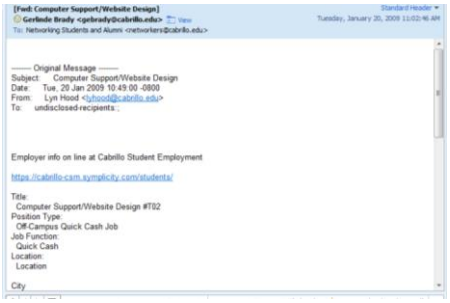
Cabrillo Networking Program Mailing list

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

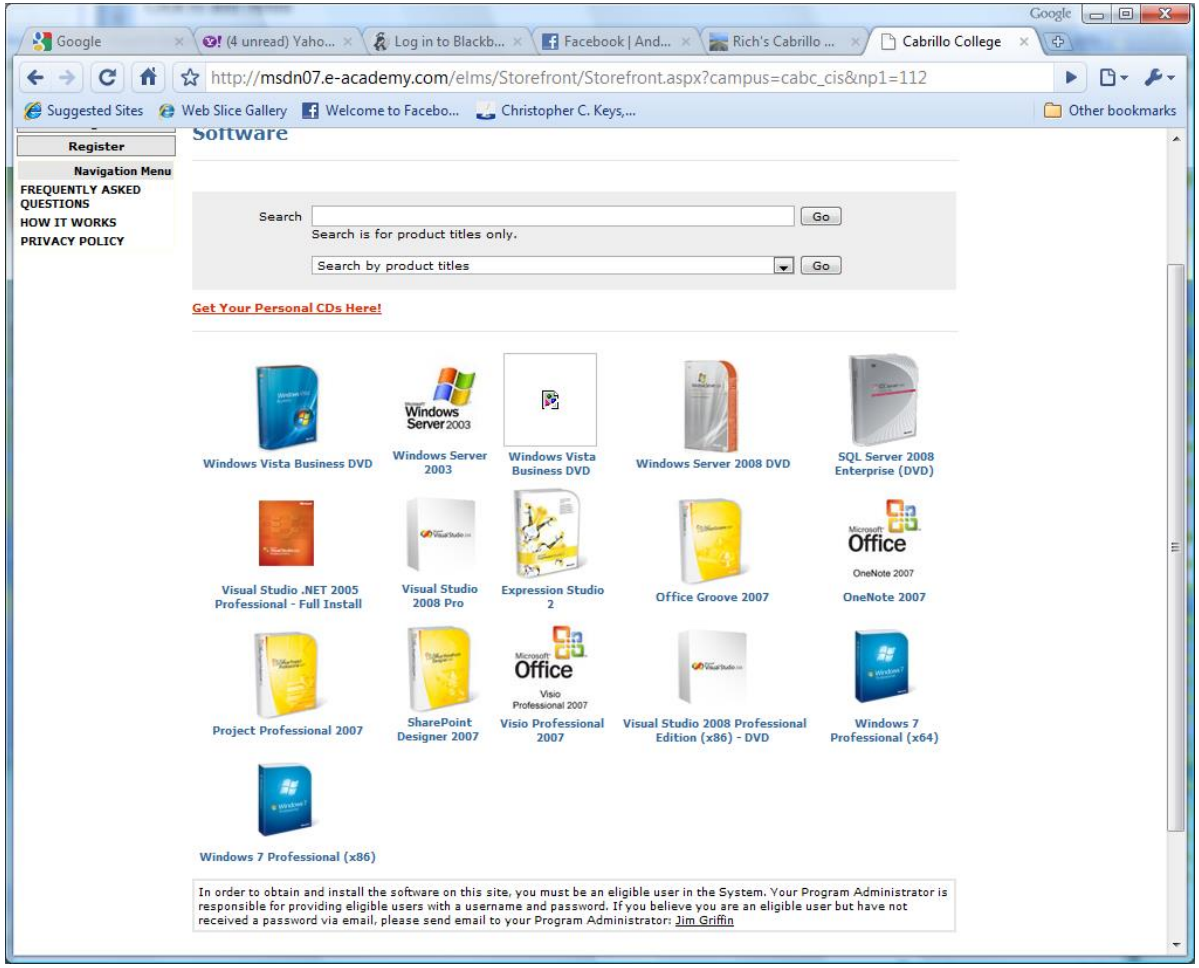
networkers-subscribe@cabrillo.edu

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





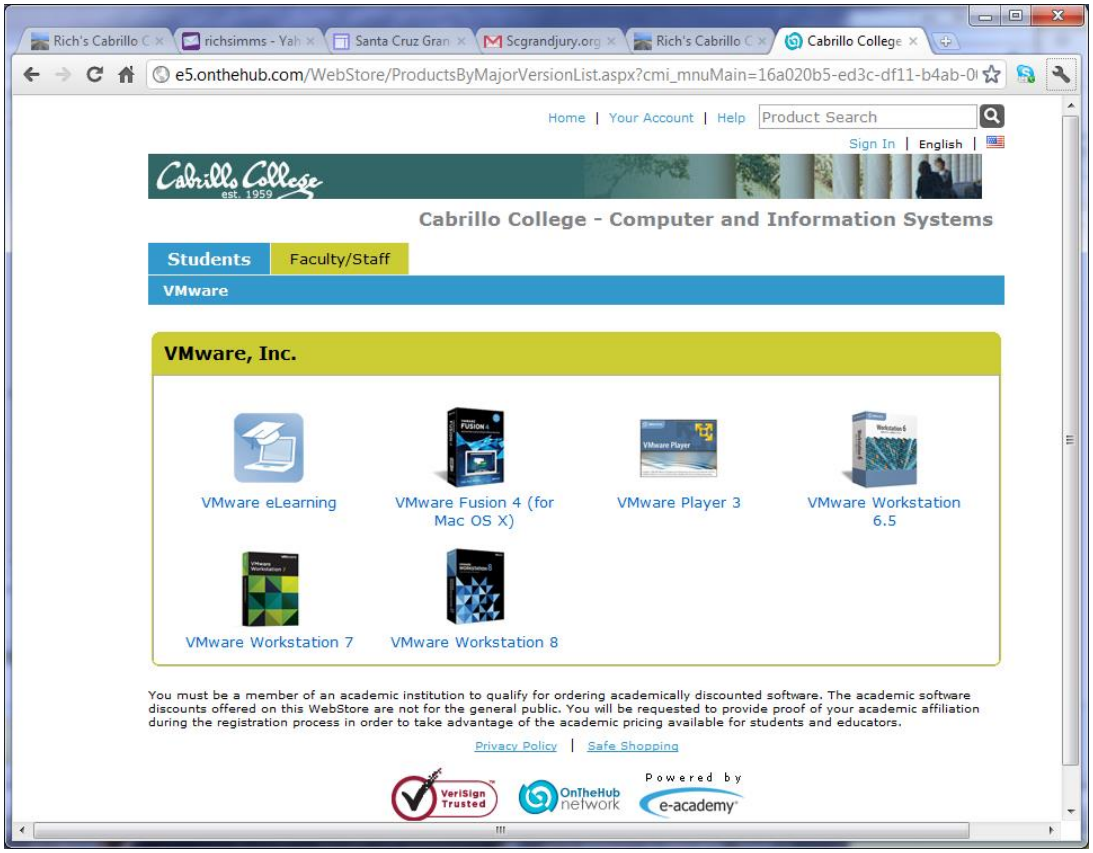
Microsoft Academic Webstore



- 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

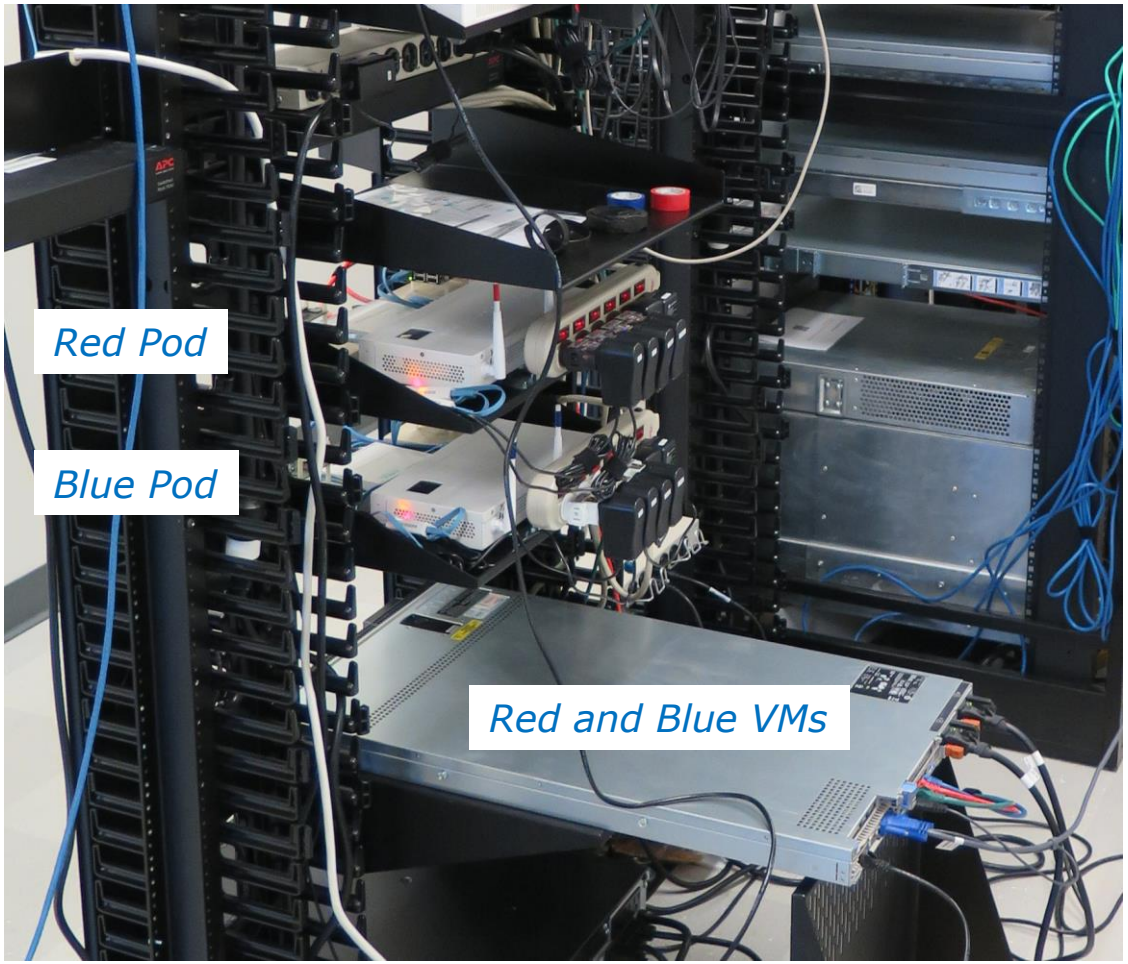
VMware Academic Webstore



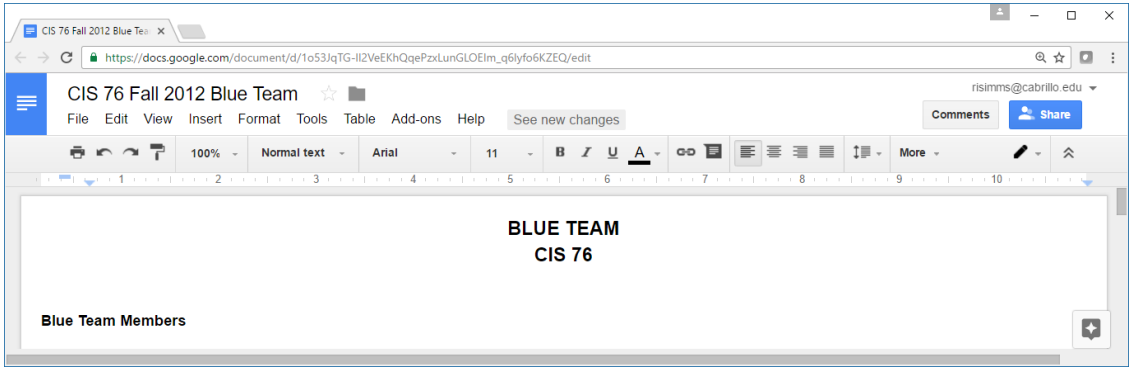
- VMware software for students registered in a CIS or CS class at Cabrillo
- Available after registration is final (two weeks after first class)

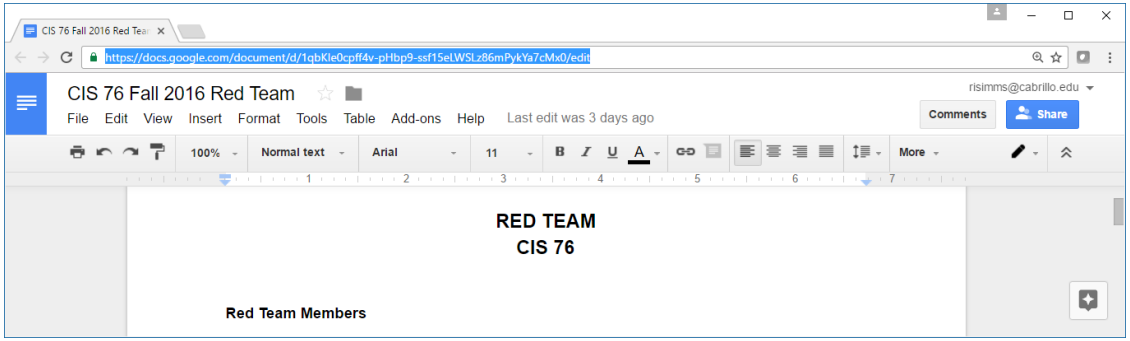
To get to this page, go to **http://simms-teach.com/resources** and click on the appropriate link in the Tools and Software section

Red and Blue Pods in Microlab Lab Rack

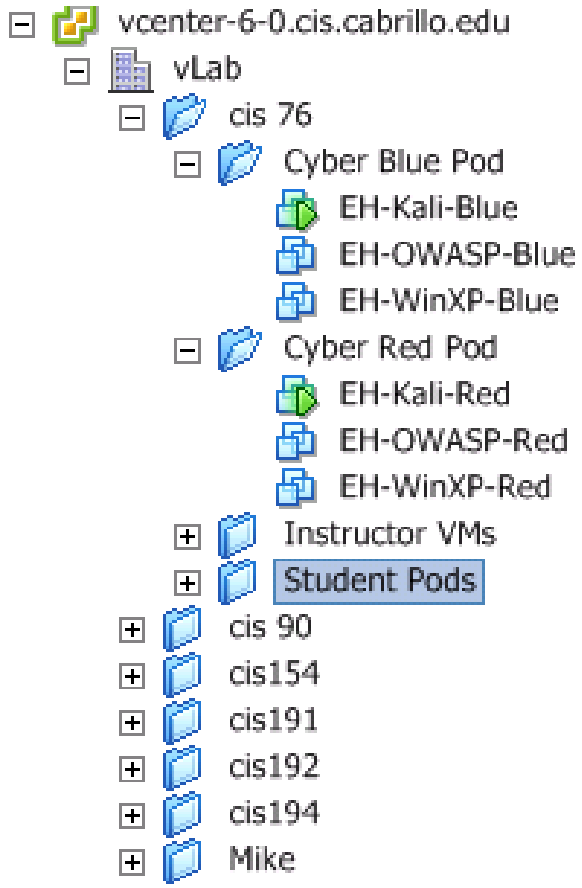


Each team has their own private Google Docs document





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

http://www.techrepublic.com/blog/it-security/the-five-phases-of-a-successful-network-penetration/

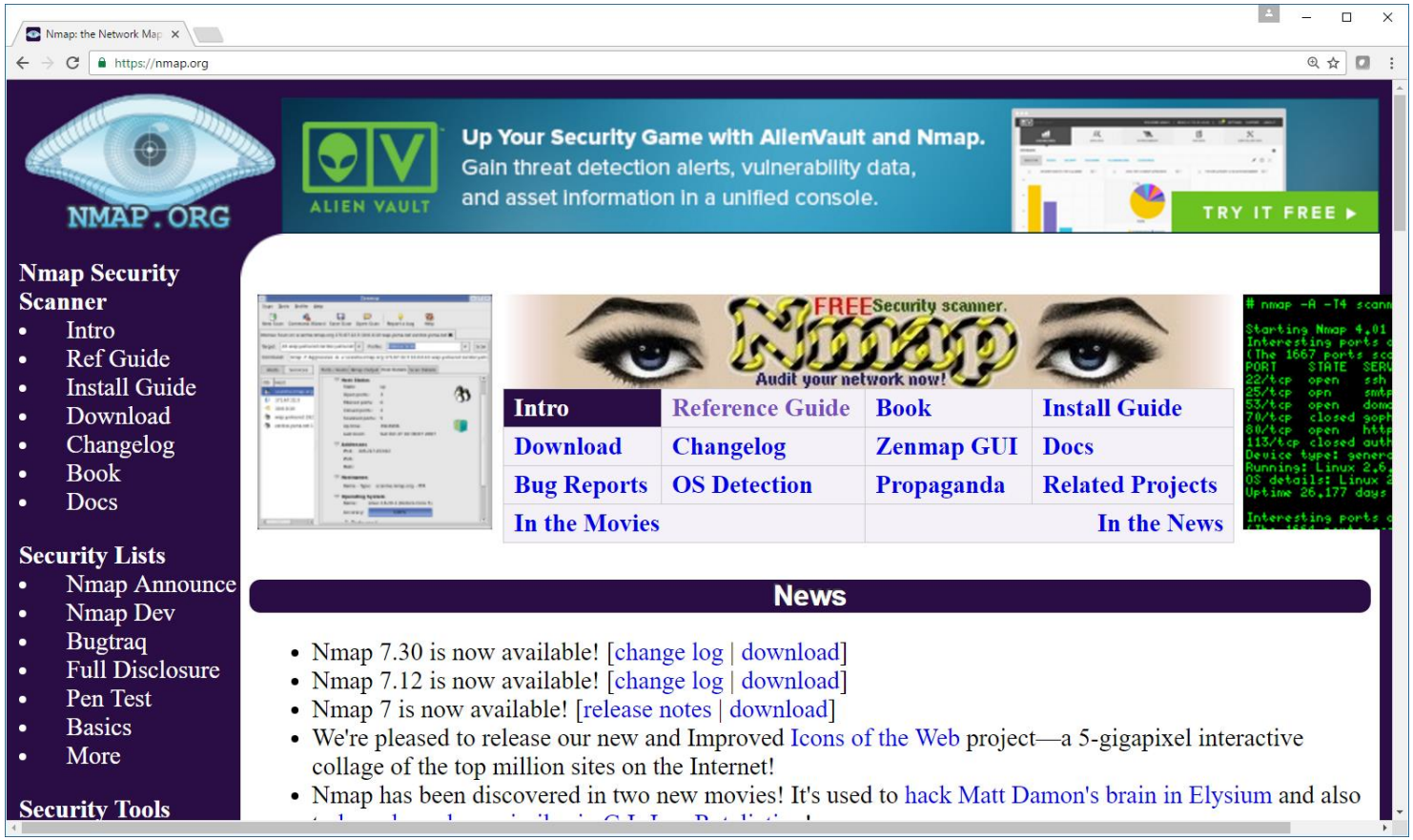
Scanning

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.

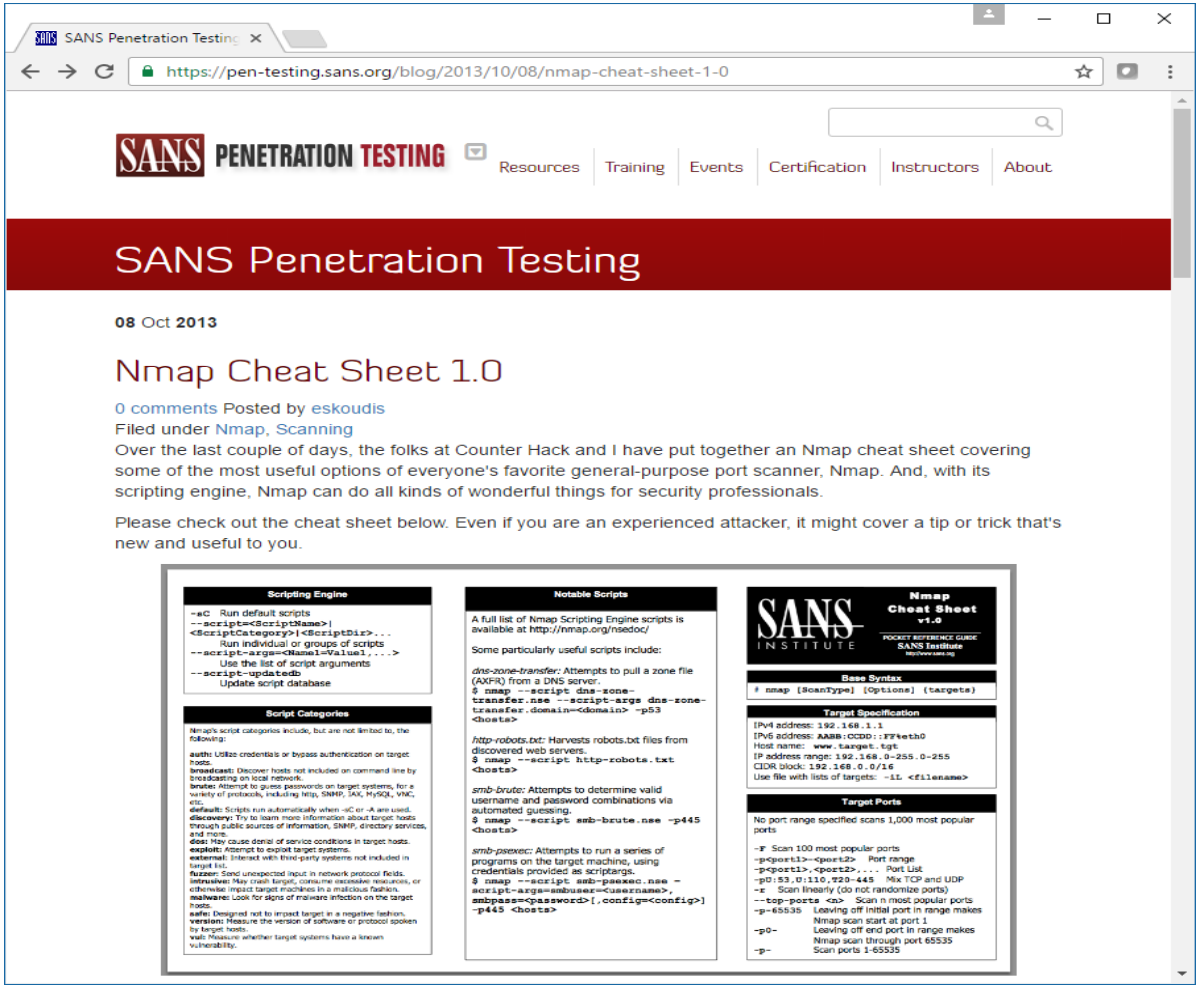
nmap

nmap.org



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

SANS Nmap Cheat Sheet



https://pen-testing.sans.org/blog/2013/10/08/nmap-cheat-sheet-1-0

Connect Scan

same subnet
no firewall

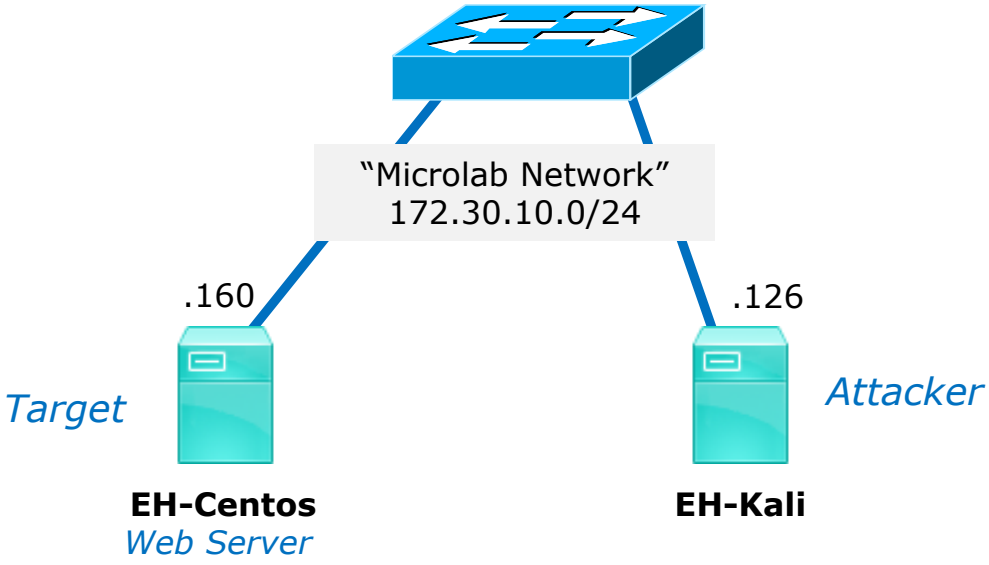
Connect Scan

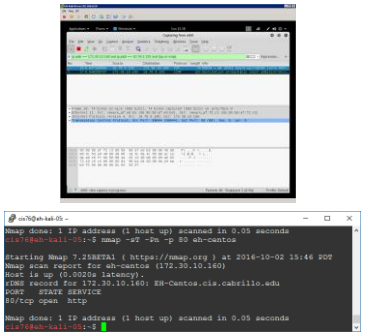
- Completes the three-way handshake
- Detectable and can be logged as a TCP connection (see example below)
- Result is one of three states: Open, Closed, and Filtered

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


"Microlab Network"
172.30.10.0/24
.160
.126
Target
Attacker
EH-Centos
Web Server
EH-Kali



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

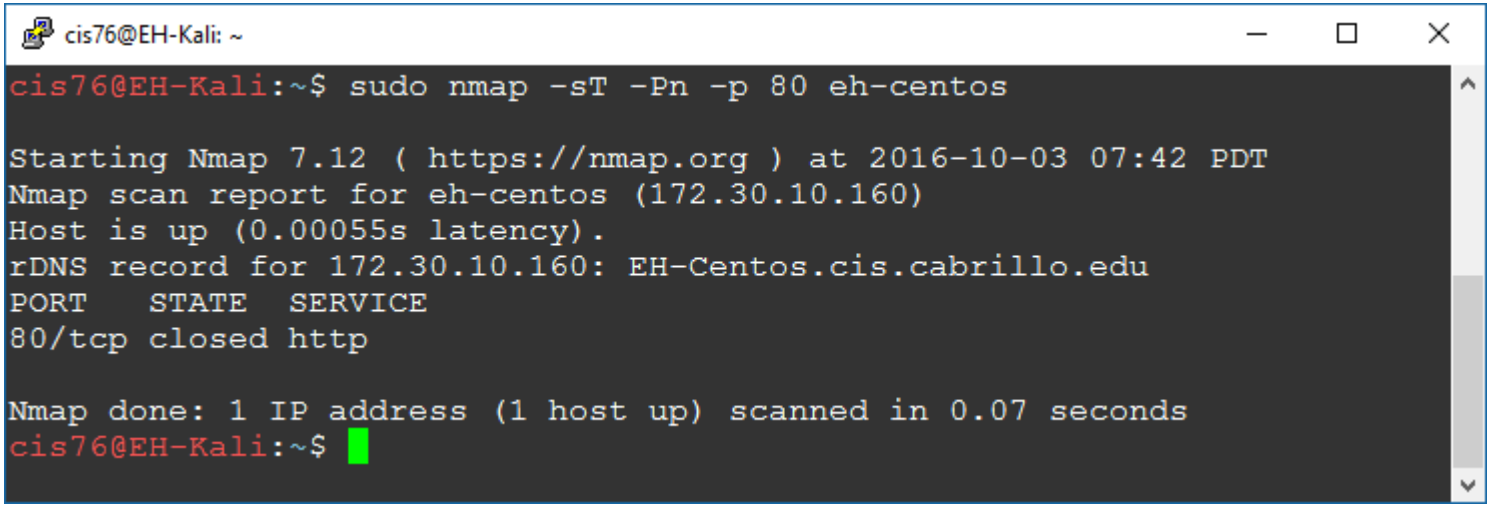
```
[rsimms@EH-Centos ~]$ sudo service iptables status
iptables: Firewall is not running.
[rsimms@EH-Centos ~]$

[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…



Connect Scan

Service	Firewall	Result
Running	no firewall	Open
Stopped	no firewall	Closed

Connect Scan

different subnets
firewall on target

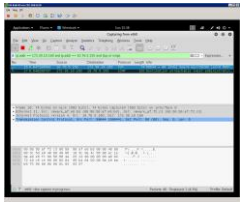
Connect Scan

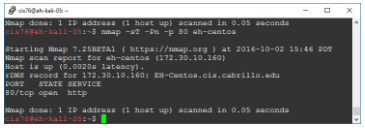
- Completes the three-way handshake.
- Detectable and can be logged as a TCP connection (see example below).
- Scan results:
  - If SYN-ACK received: "open".
  - If RST received: "closed".
  - If no reply or ICMP error: "filtered".

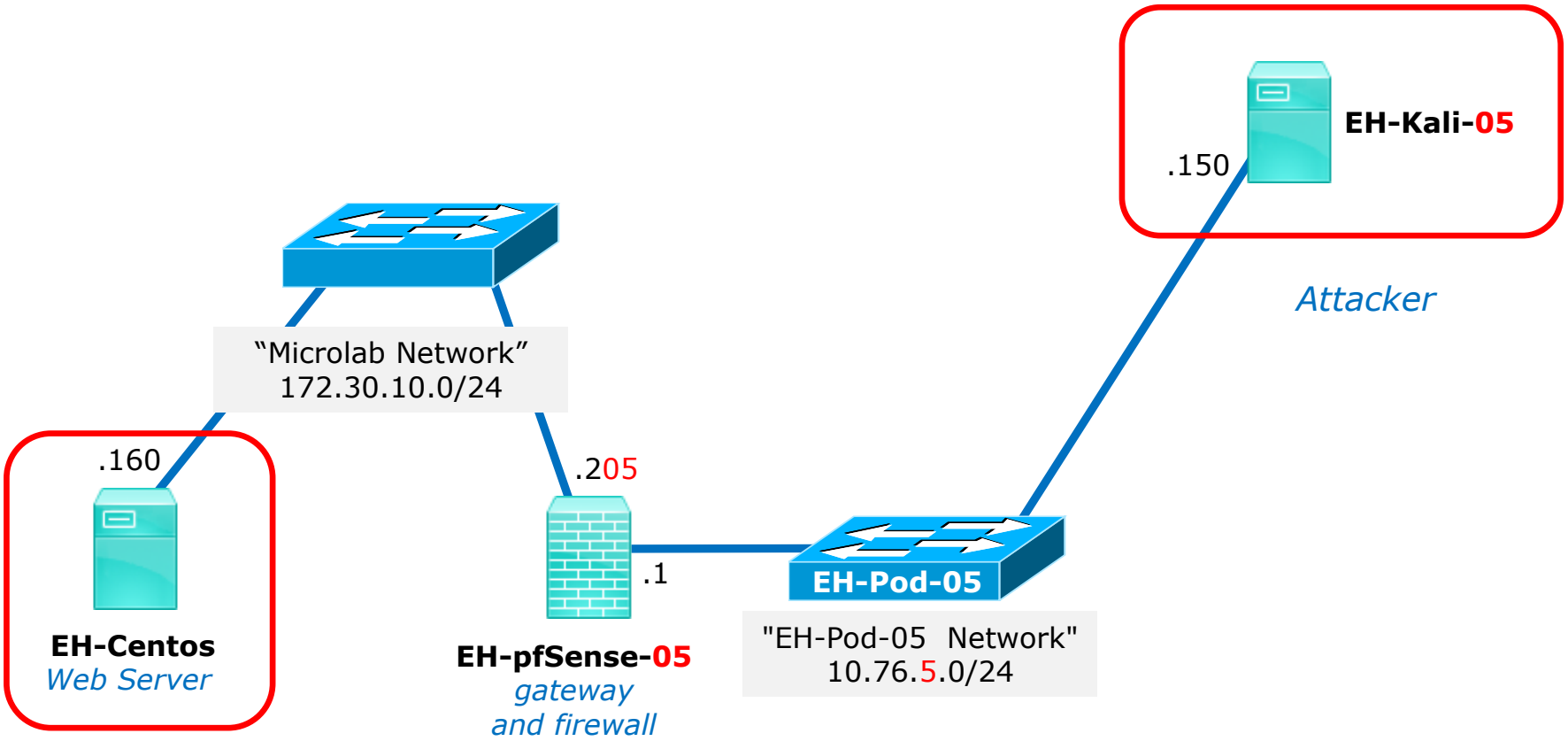
Top unknown TCP connections

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






EH-Kali-05
.150
Attacker
"Microlab Network"
172.30.10.0/24
.160
.205
.1
EH-Pod-05
EH-Centos
Web Server
EH-pfSense-05
gateway
and firewall
"EH-Pod-05 Network"
10.76.5.0/24
Target

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
```

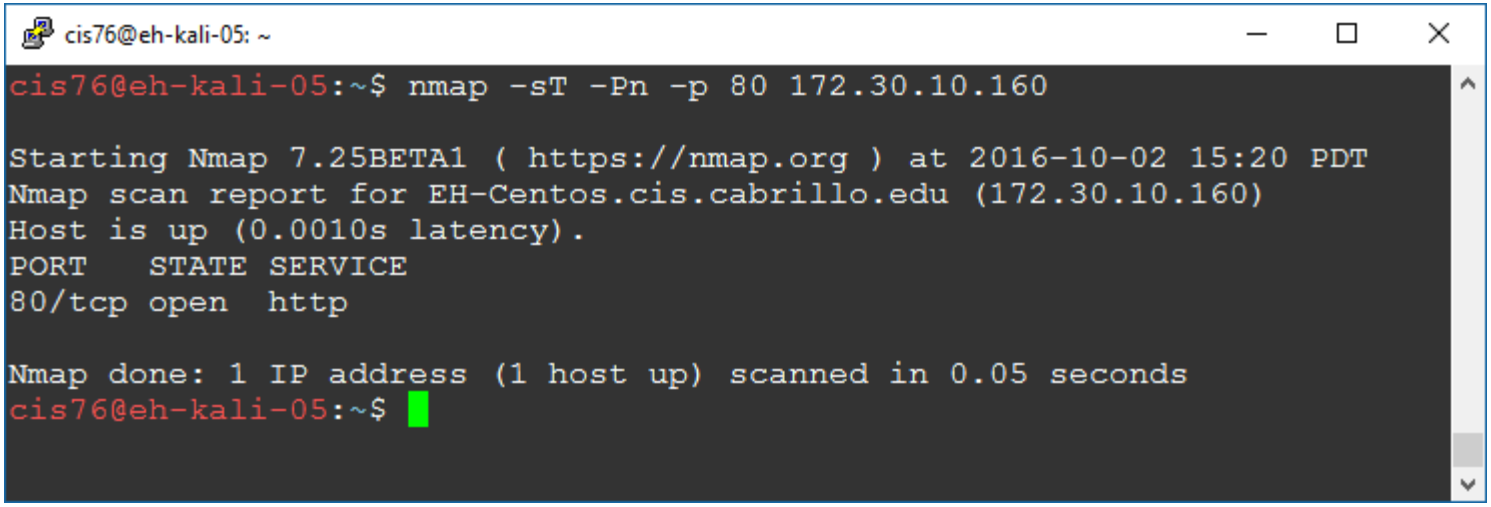
```
[root@EH-Centos ~]# service httpd status
httpd (pid  4196) is running...
[root@EH-Centos ~]#
```

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…



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:~$
```

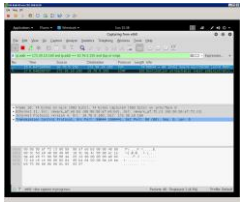
Connect Scan

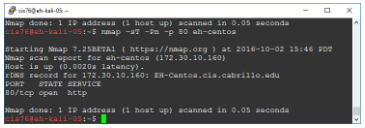
Service	Firewall	Result
Running	ACCEPT	Open
Running	DROP	Filtered
Running	REJECT	Filtered
Stopped	ACCEPT	Closed
Stopped	DROP	Filtered
Stopped	REJECT	Filtered

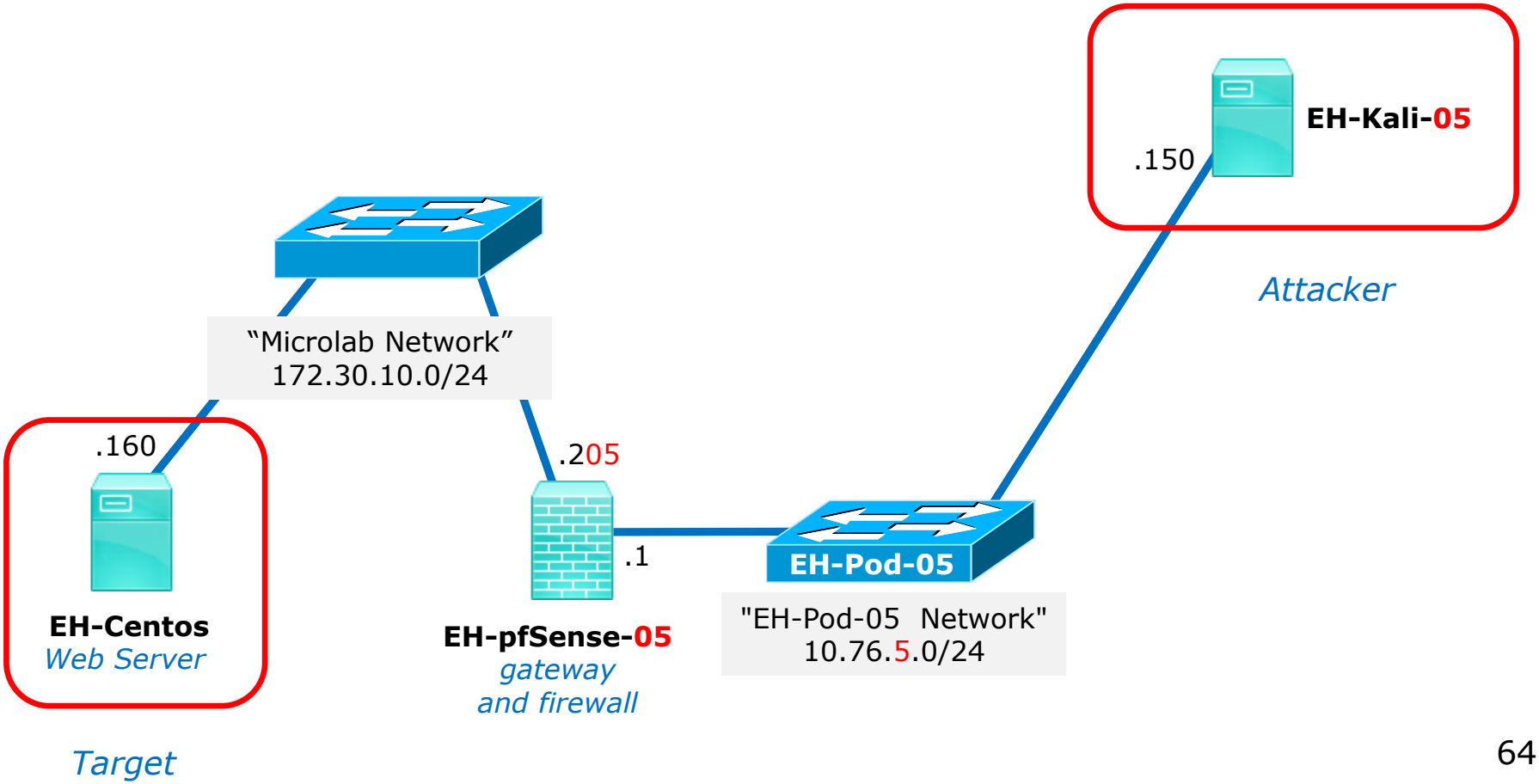
Syn Scan

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".




Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds
cis76@eh-kali-05:~$ nmap -sT -Pn -p 80 eh-centos
Starting Nmap 7.25BETA1 (https://nmap.org) at 2016-10-02 15:46 PDT
Nmap scan report for eh-centos (172.30.10.160)
Host is up (0.0020s 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:~$


EH-Kali-05
.150
Attacker
"Microlab Network"
172.30.10.0/24
.160
.205
.1
EH-Pod-05
EH-Centos
Web Server
EH-pfSense-05
gateway
and firewall
"EH-Pod-05 Network"
10.76.5.0/24
Target

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

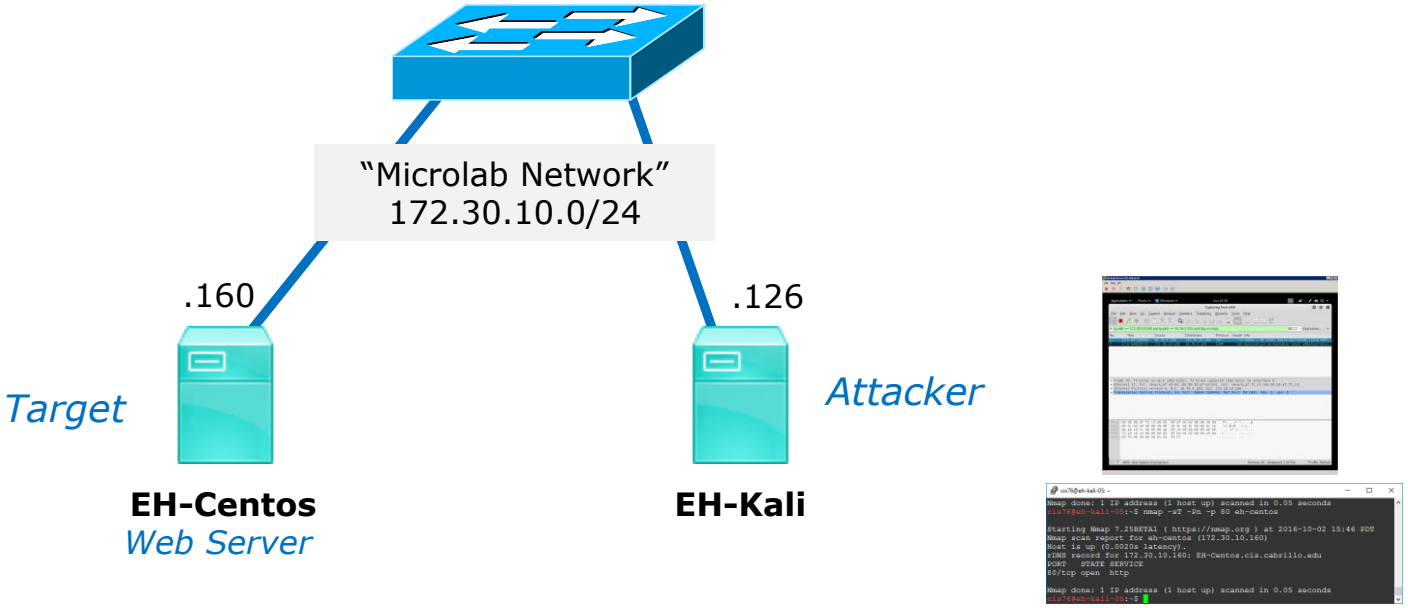
Null Scan (Linux)

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

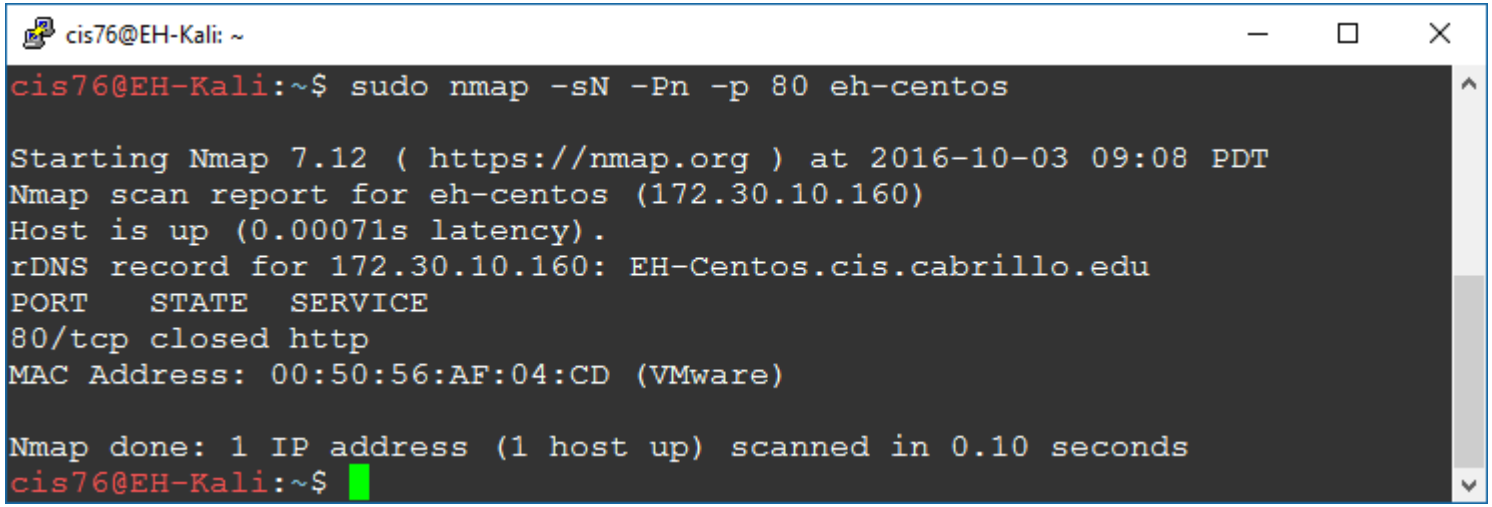
```
[root@EH-Centos ~]# service iptables status
iptables: Firewall is not running.
[root@EH-Centos ~]#

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

Null Scan

Firewall action = no firewall and Service = Stopped

Victim resets connection

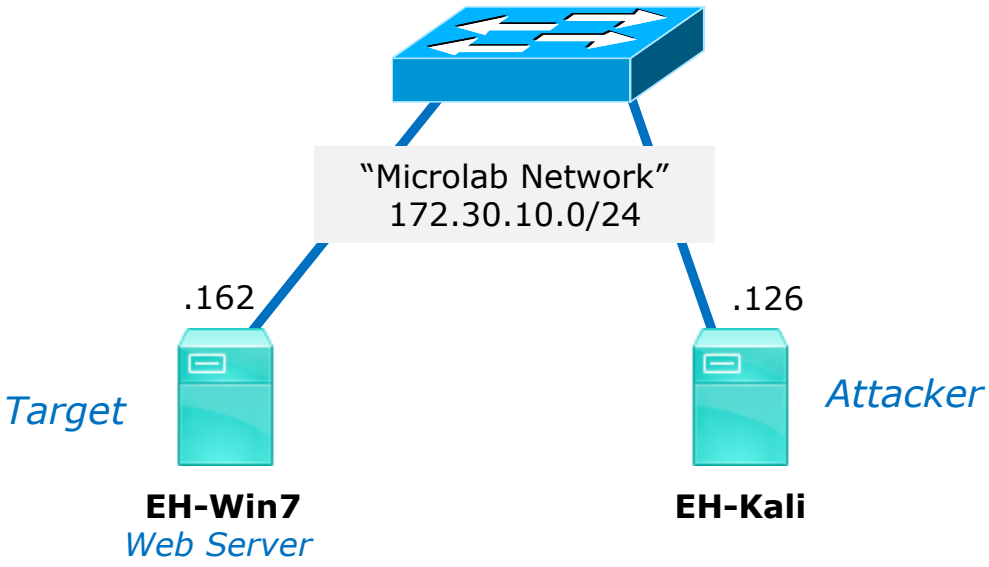
Source	Destination	Protocol	Length	Info
172.30.10.126	172.30.10.160	TCP	54	61631 → 80 [<None>] Seq=1 Win=102…
172.30.10.160	172.30.10.126	TCP	60	80 → 61631 [RST, ACK] Seq=1 Ack=1…

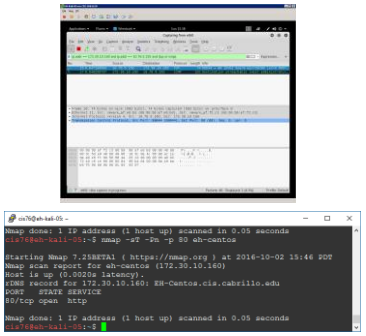


Null Scan (Linux)

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

Null Scan (Windows 7)



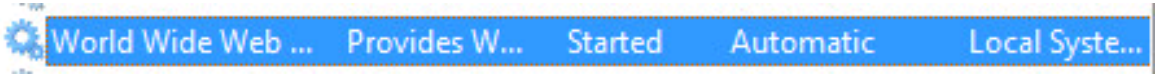


Switched to Win 7 target to see how Windows implements RFC 793 (Transmission Control Protocols)

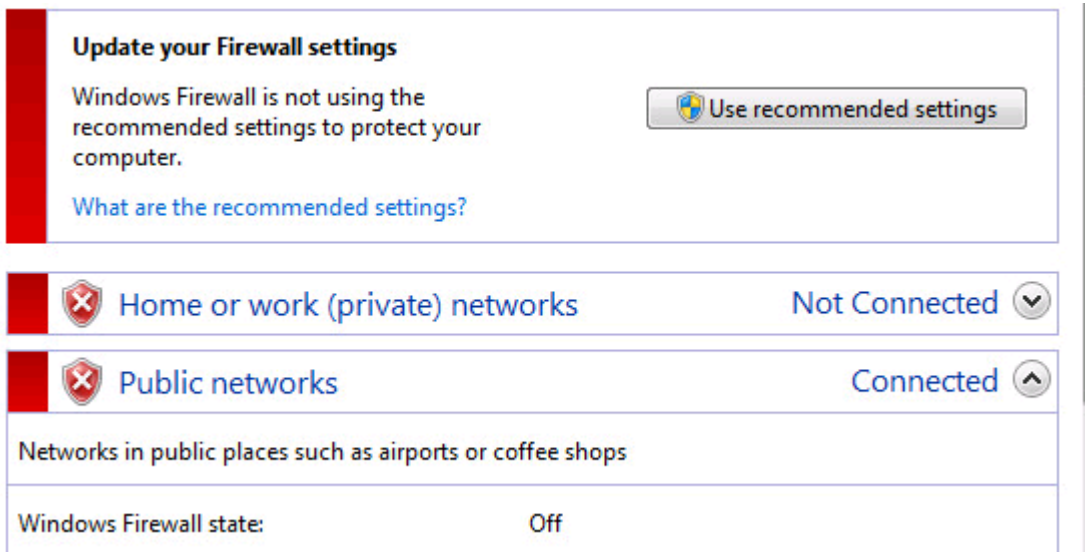
Null Scan

Firewall action = no firewall and Service = Running

Web service running



Firewall off

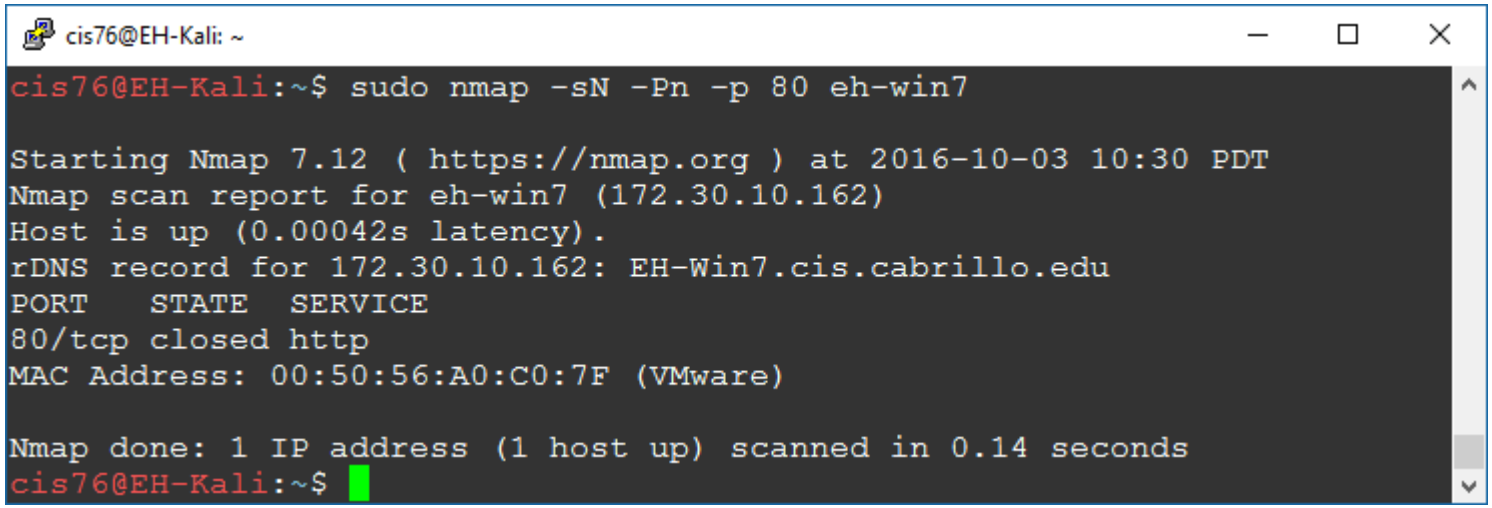


Null Scan

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 [<None>] Seq=1 Win=102…
172.30.10.162	172.30.10.126	TCP	60	80 → 56023 [RST, ACK] Seq=1 Ack=1…

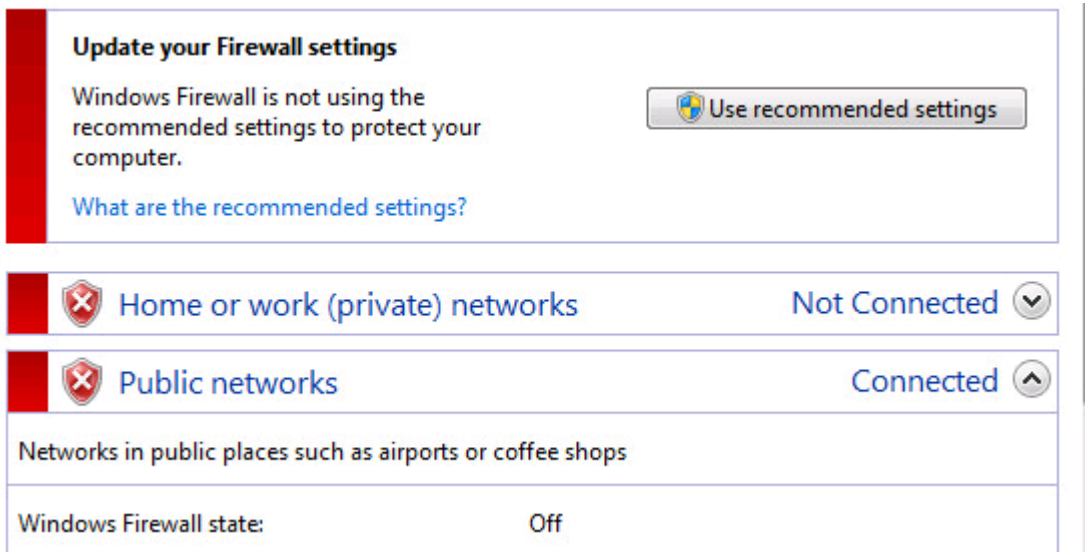


Null Scan

Firewall action = no firewall and Service = Stopped

Web service stopped

Firewall off

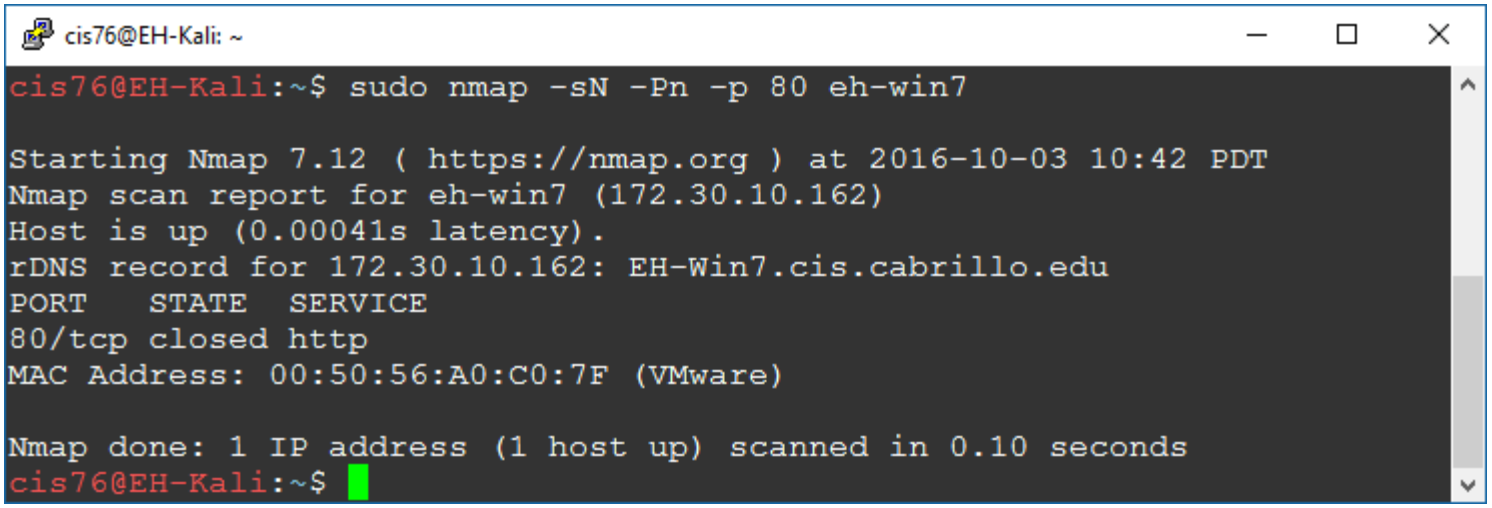


Null Scan

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 [<None>] Seq=1 Win=102…
172.30.10.162	172.30.10.126	TCP	60	80 → 50775 [RST, ACK] Seq=1 Ack=1…



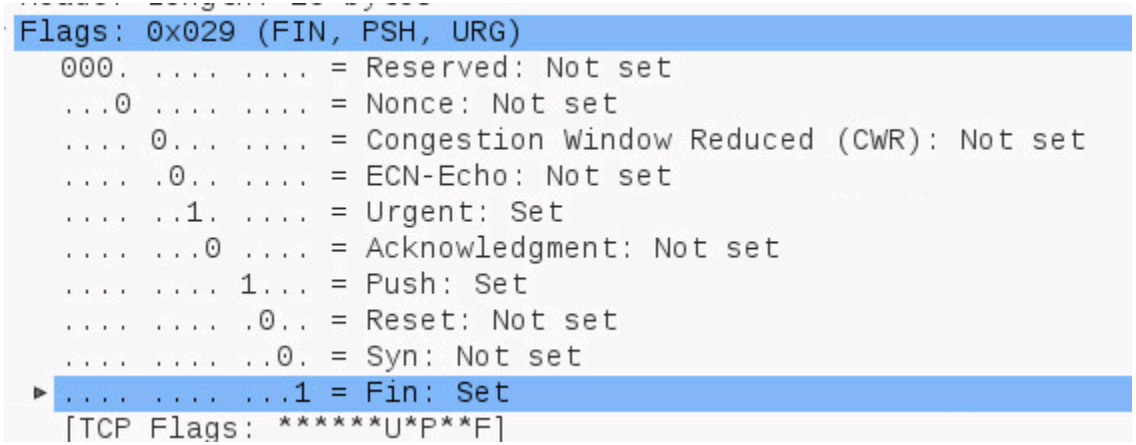
Null Scan (Windows 7)

Service	Firewall	Result
Running	no firewall	Closed
Stopped	no firewall	Closed

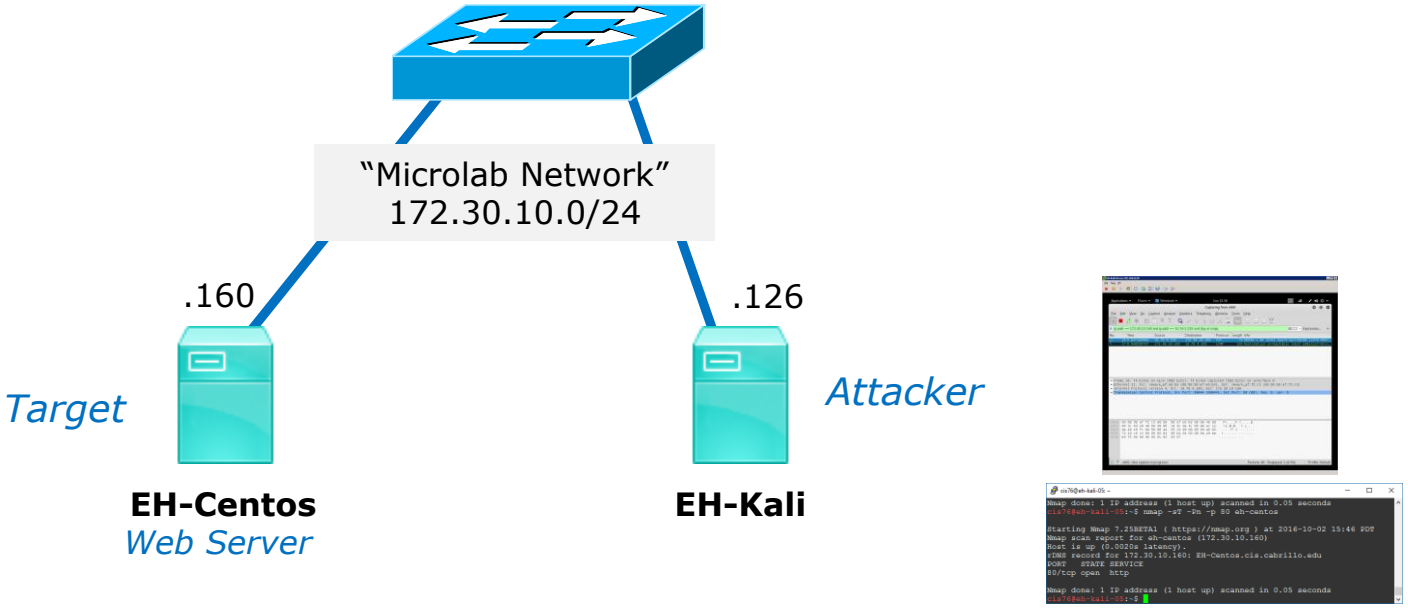
XMAS Scan

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"



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



Switched to Kali on the same subnet because NULL 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

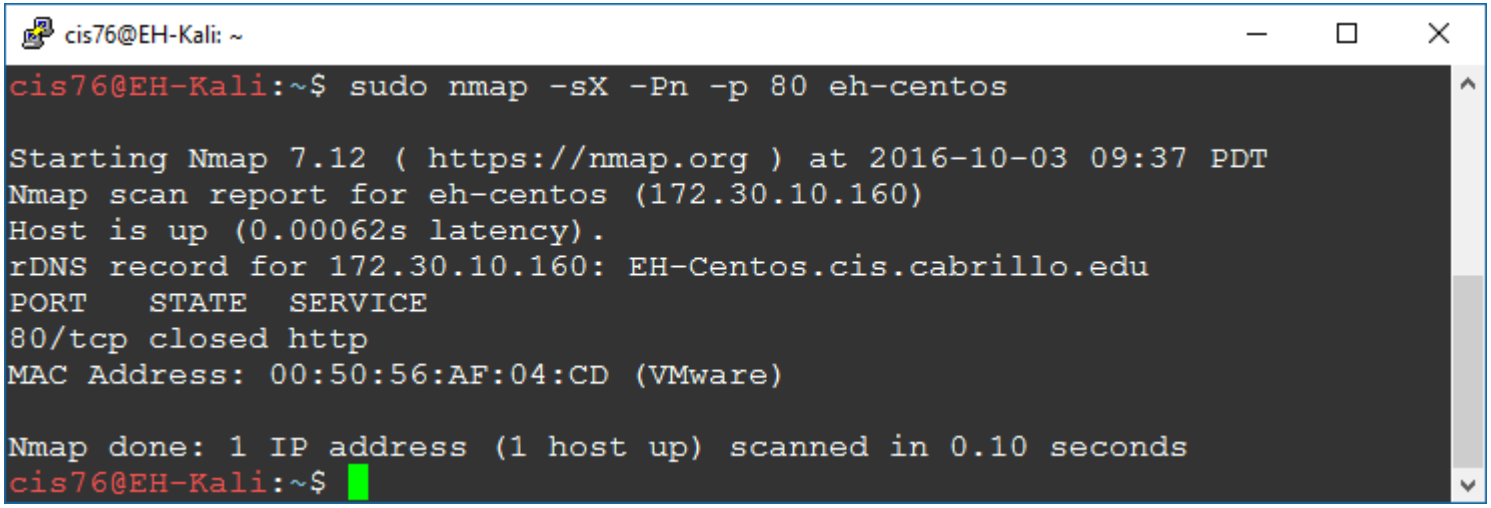
```
[root@EH-Centos ~]# service iptables status
iptables: Firewall is not running.
[root@EH-Centos ~]#

[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…



XMAS Scan (Linux)

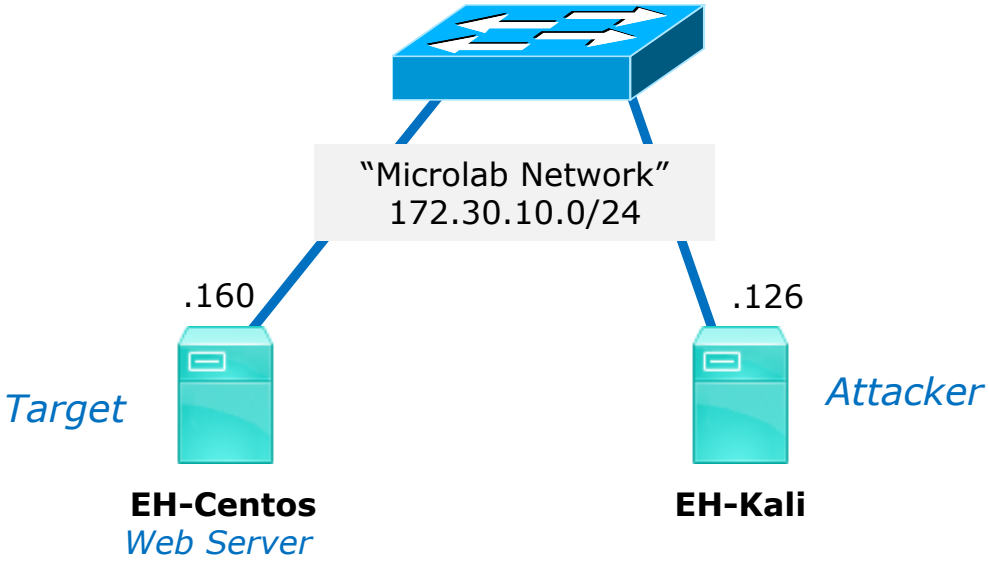
Service	Firewall	Result
Running	no firewall	Open or filtered
Stopped	no firewall	Closed

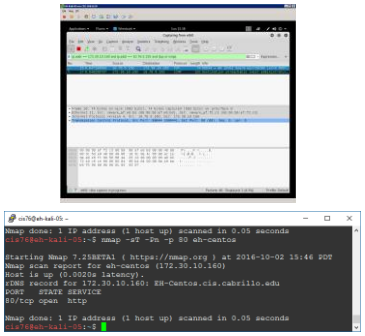
ACK Scan

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

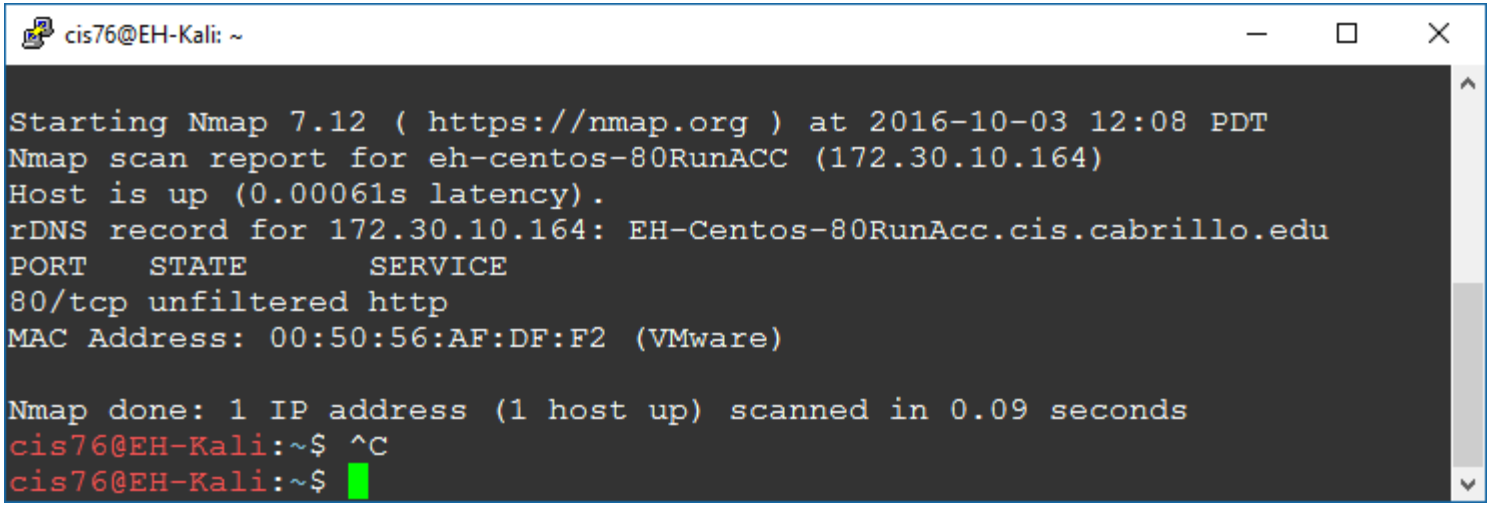
```
[root@EH-Centos-80RunAcc ~]# cat /etc/sysconfig/iptables
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-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



hping3

hping3

http://www.hping.org/

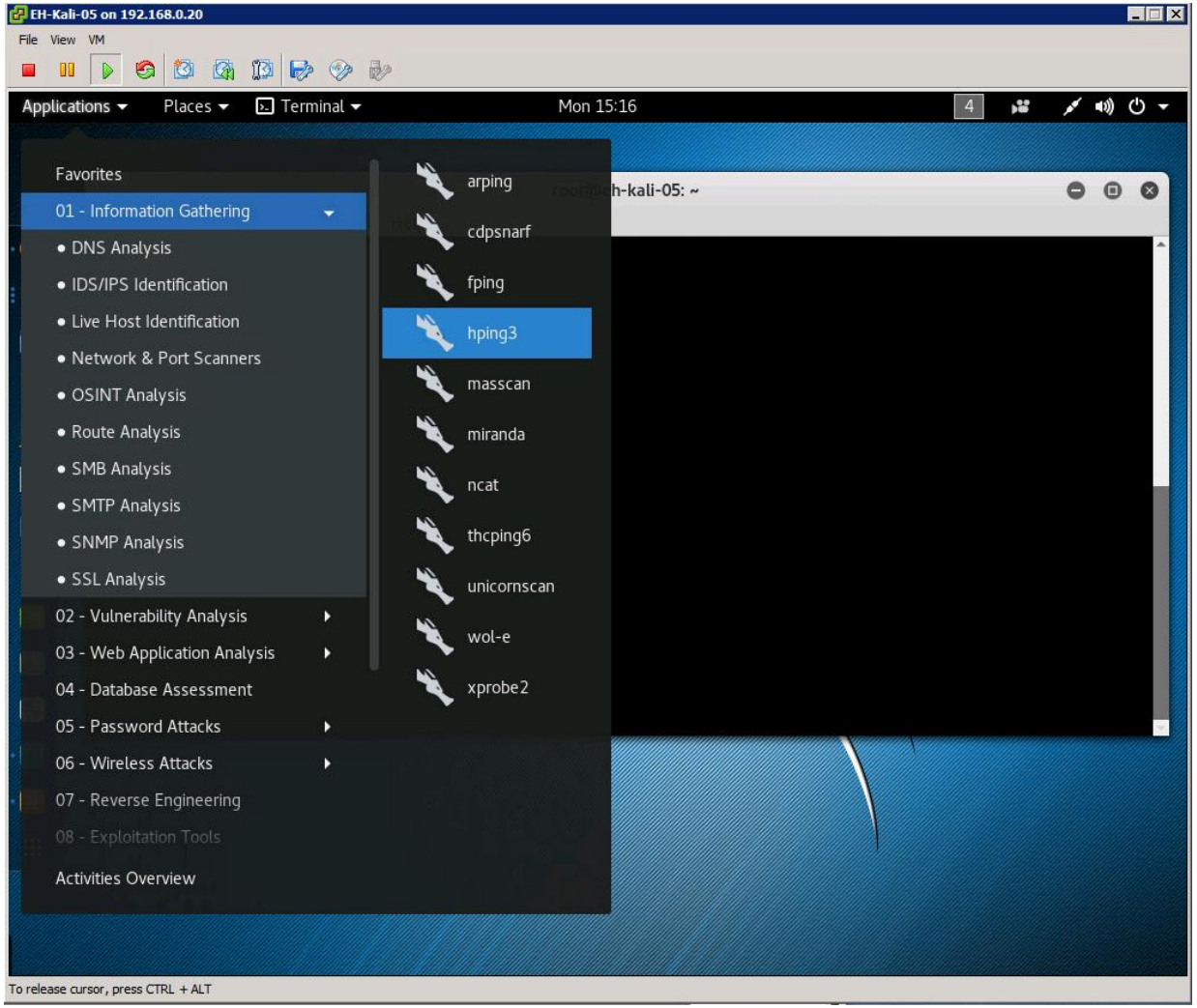
hping3

"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."

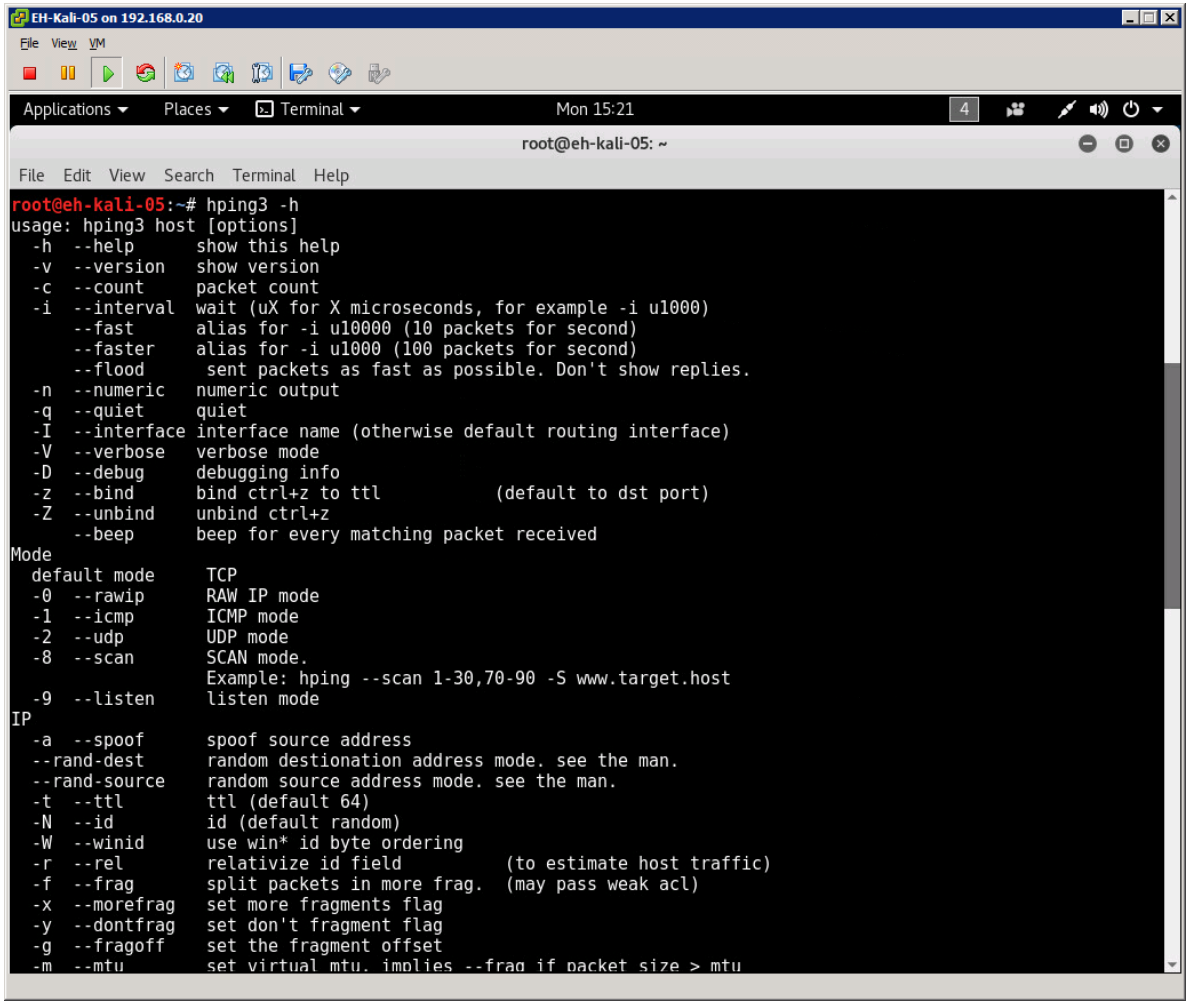
-- hping3 website

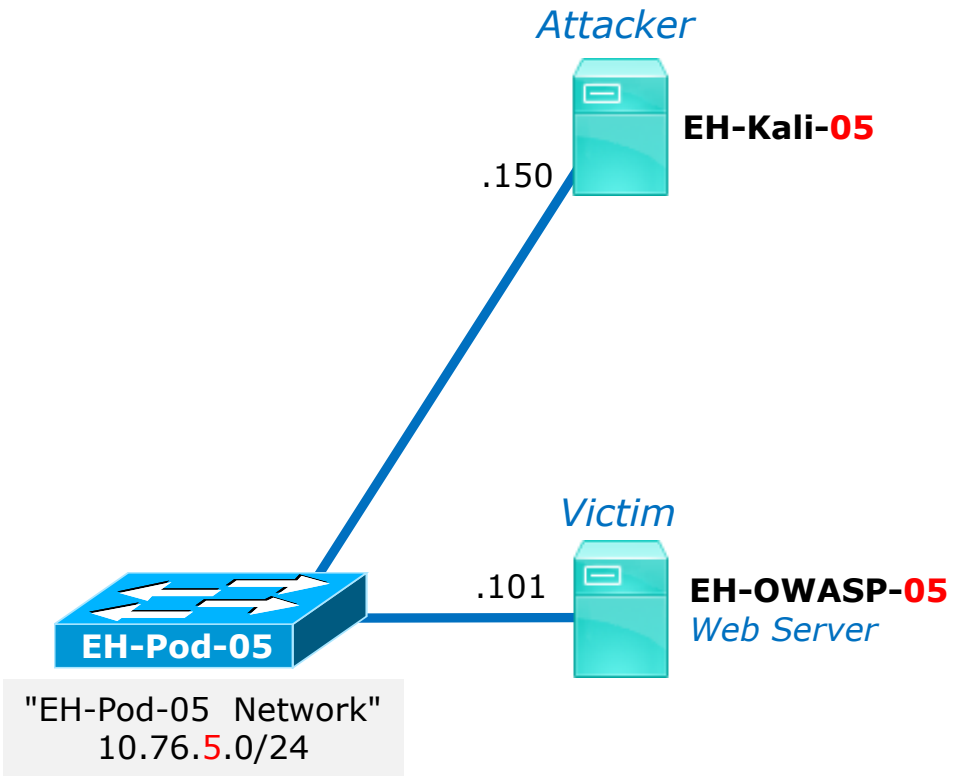
http://www.hping.org/

hping3


EH-Kali-05 on 192.168.0.20
File View VM
Applications Places Terminal Mon 15:16
Favorites
01 - Information Gathering
• DNS Analysis
• IDS/IPS Identification
• Live Host Identification
• Network & Port Scanners
• OSINT Analysis
• Route Analysis
• SMB Analysis
• SMTP Analysis
• SNMP Analysis
• SSL Analysis
02 - Vulnerability Analysis
03 - Web Application Analysis
04 - Database Assessment
05 - Password Attacks
06 - Wireless Attacks
07 - Reverse Engineering
08 - Exploitation Tools
Activities Overview
arping
cdpsnarf
fping
hping3
masscan
miranda
ncat
thcping6
unicornscan
wol-e
xprobe2
h-kali-05: ~
To release cursor, press CTRL + ALT

hping3


EH-Kali-05 on 192.168.0.20
File View VM
Applications Places Terminal Mon 15:21
root@eh-kali-05: ~
File Edit View Search Terminal Help
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 --spoof spoof source address
--rand-dest random destionation 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


Attacker
EH-Kali-05
.150
Victim
.101
EH-OWASP-05
Web Server
EH-Pod-05
"EH-Pod-05 Network"
10.76.5.0/24

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
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
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: 5858585858585858585858585858585858585858
   [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 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:~#
```

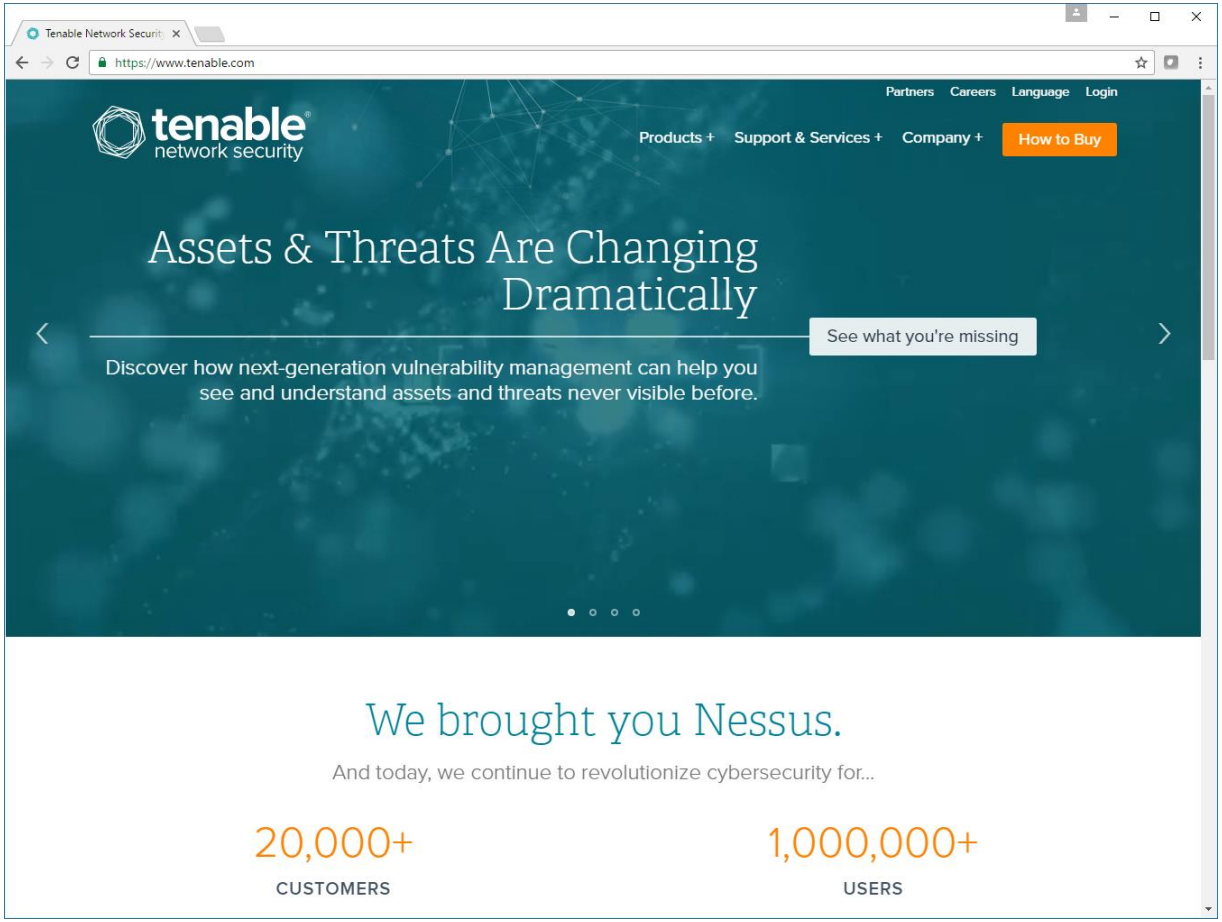
Source	Destination	Protocol	Length	Info
6.131.101.238	10.76.5.101	TCP	56	2401 → 80 [<None>] Seq=1 Win=512 L…
89.180.202.142	10.76.5.101	TCP	56	2402 → 80 [<None>] Seq=1 Win=512 L…
33.37.155.186	10.76.5.101	TCP	56	2621 → 80 [<None>] Seq=1 Win=512 L…
199.187.218.250	10.76.5.101	TCP	56	2622 → 80 [<None>]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

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



https://www.tenable.com/

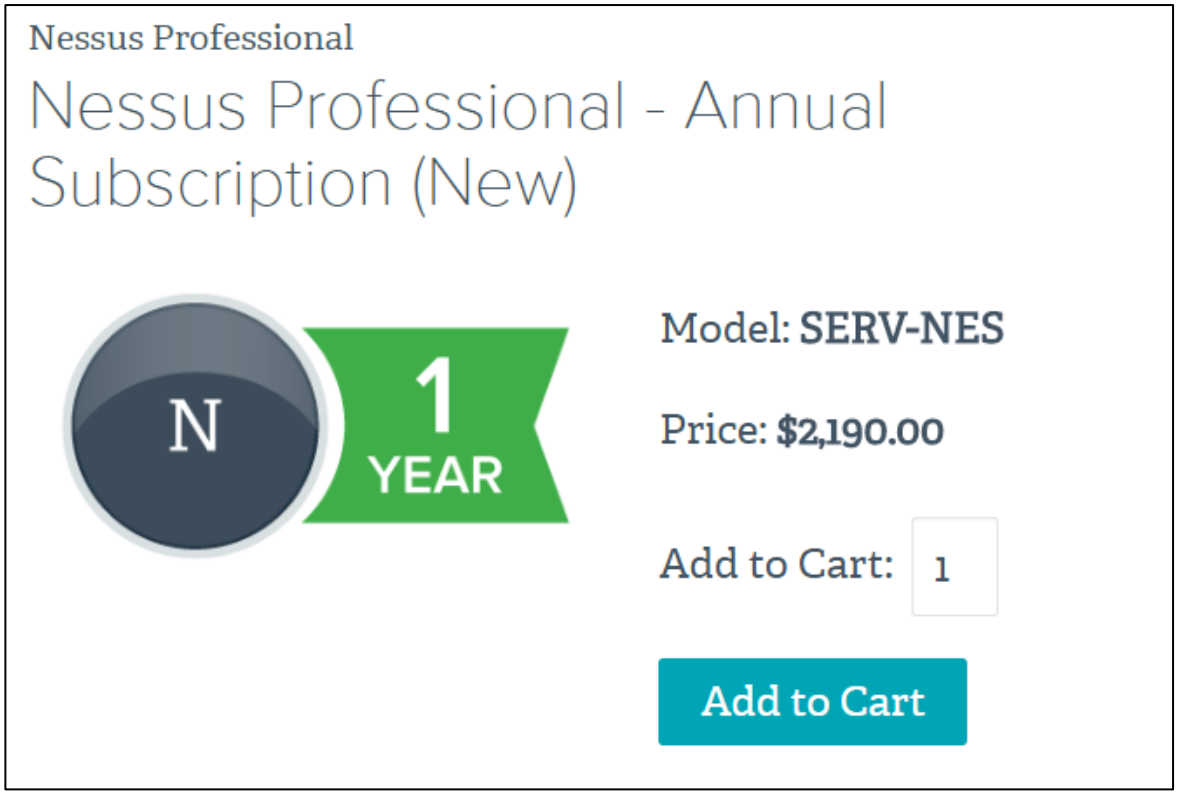
nessus

"**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



https://store.tenable.com/index.php?main_page=product_info&cPath=1&products_id=94

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

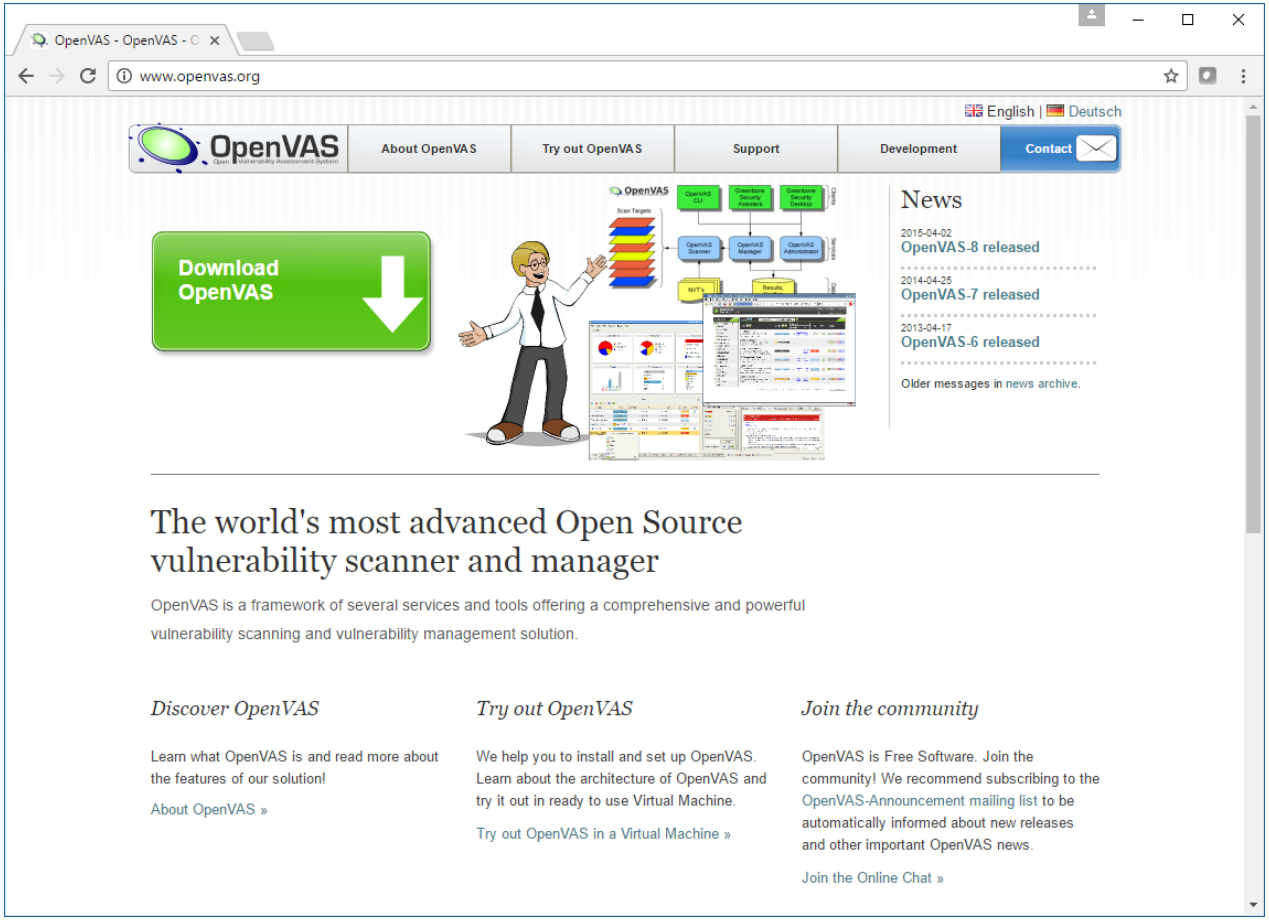
"Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files/programs, checks for outdated versions of over 1250 servers, and version specific problems on over 270 servers. It also checks for 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

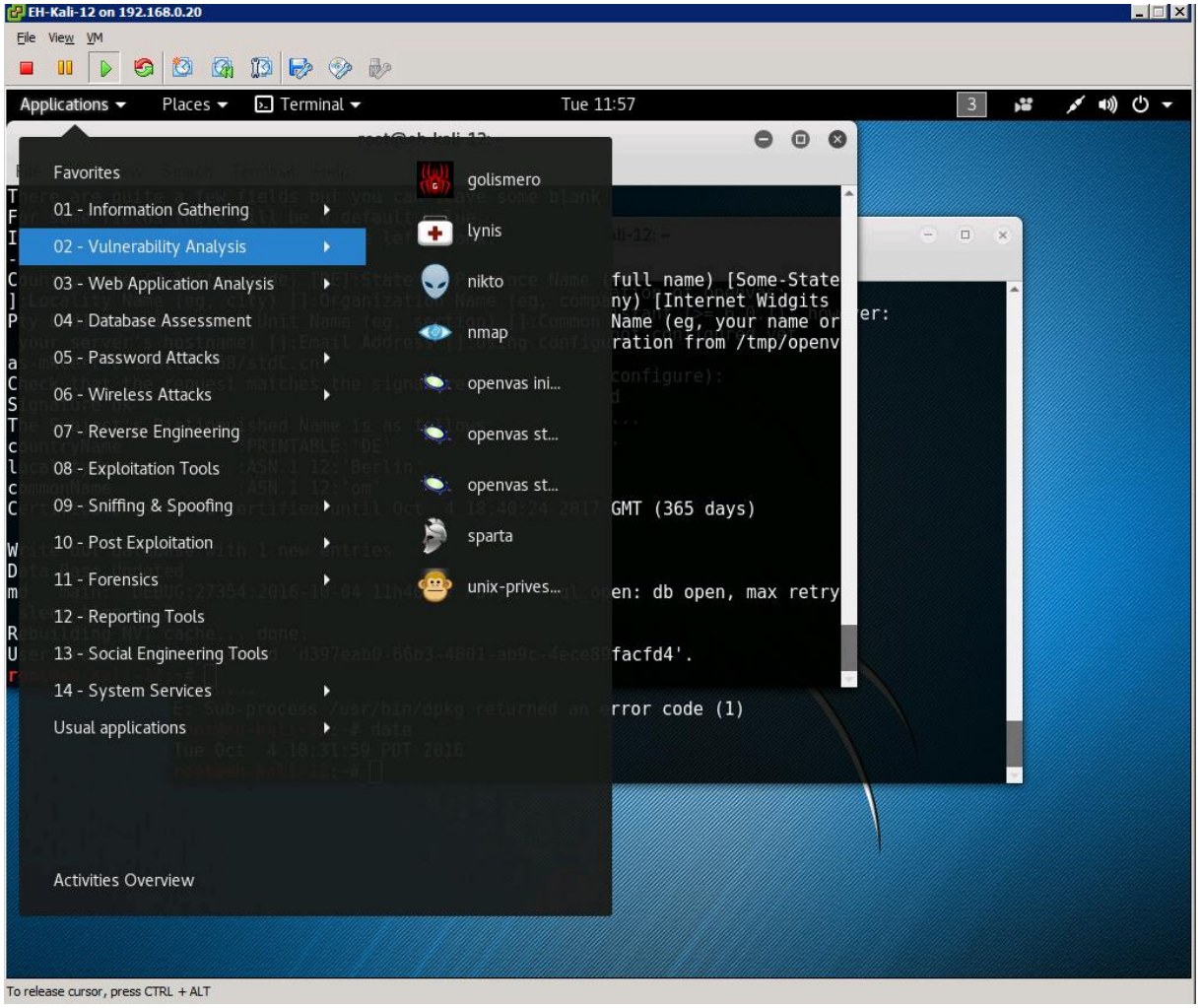
OpenVAS

OpenVAS



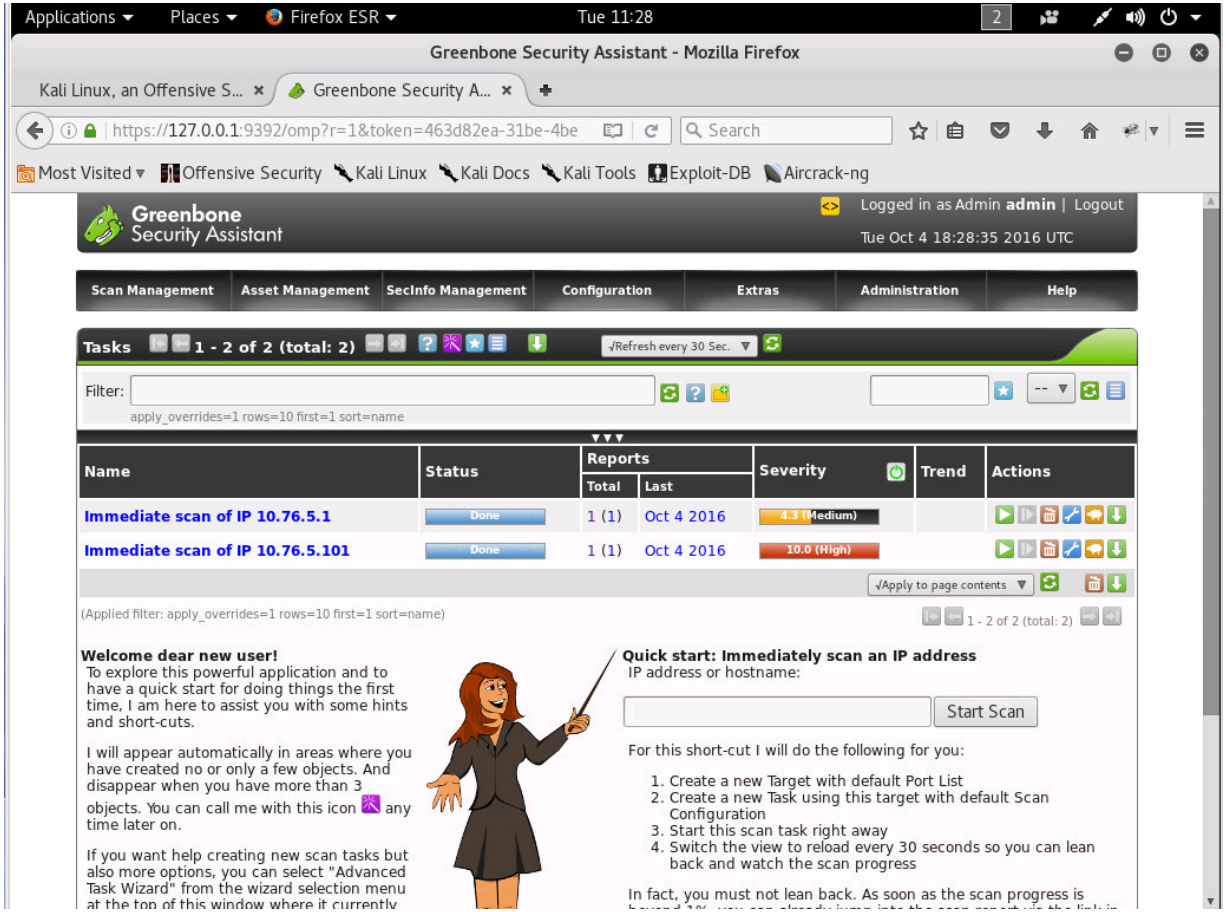
http://www.openvas.org/

OpenVAS



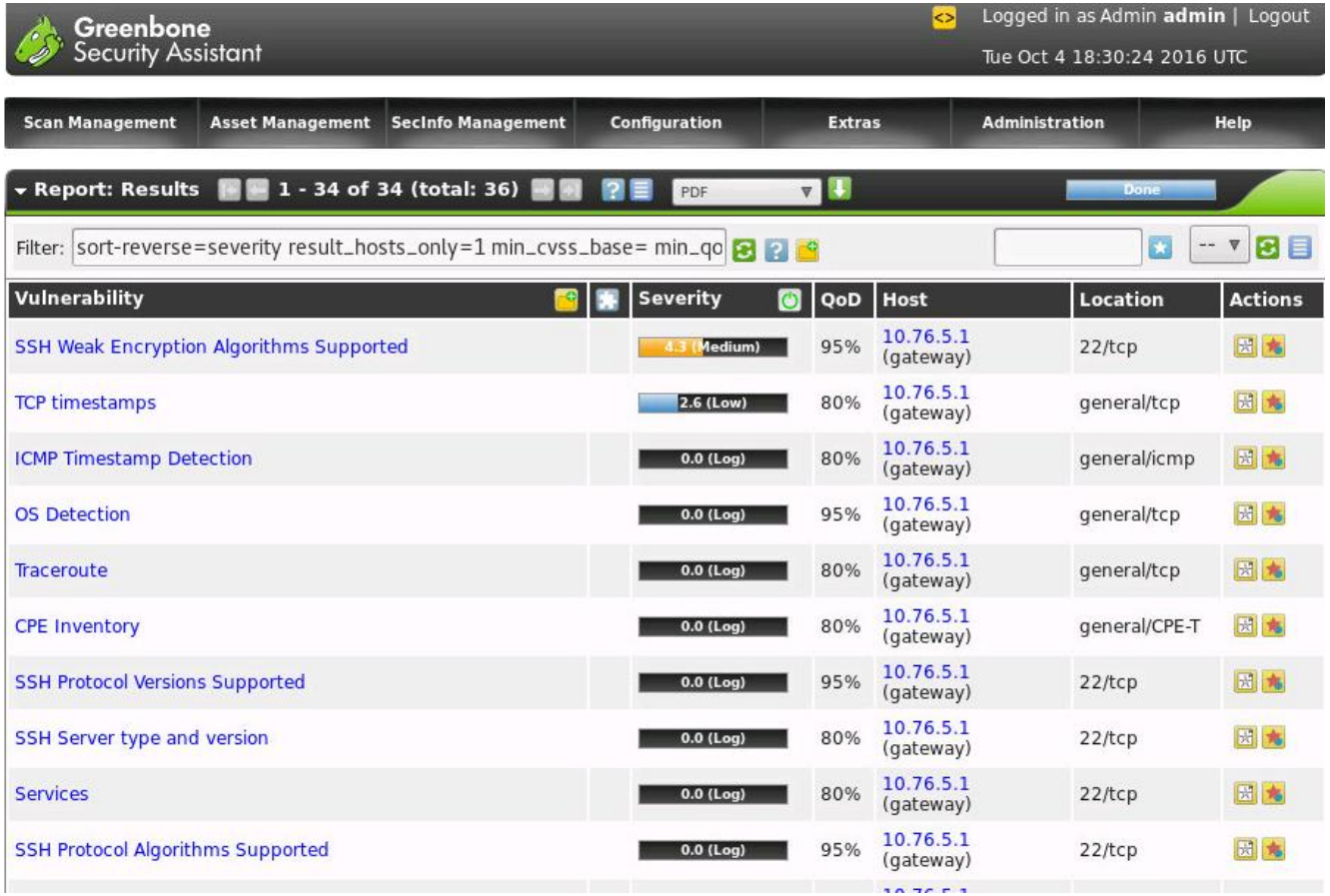
Doesn't come with Kali, use apt-get install openvas

OpenVAS



http://www.openvas.org/

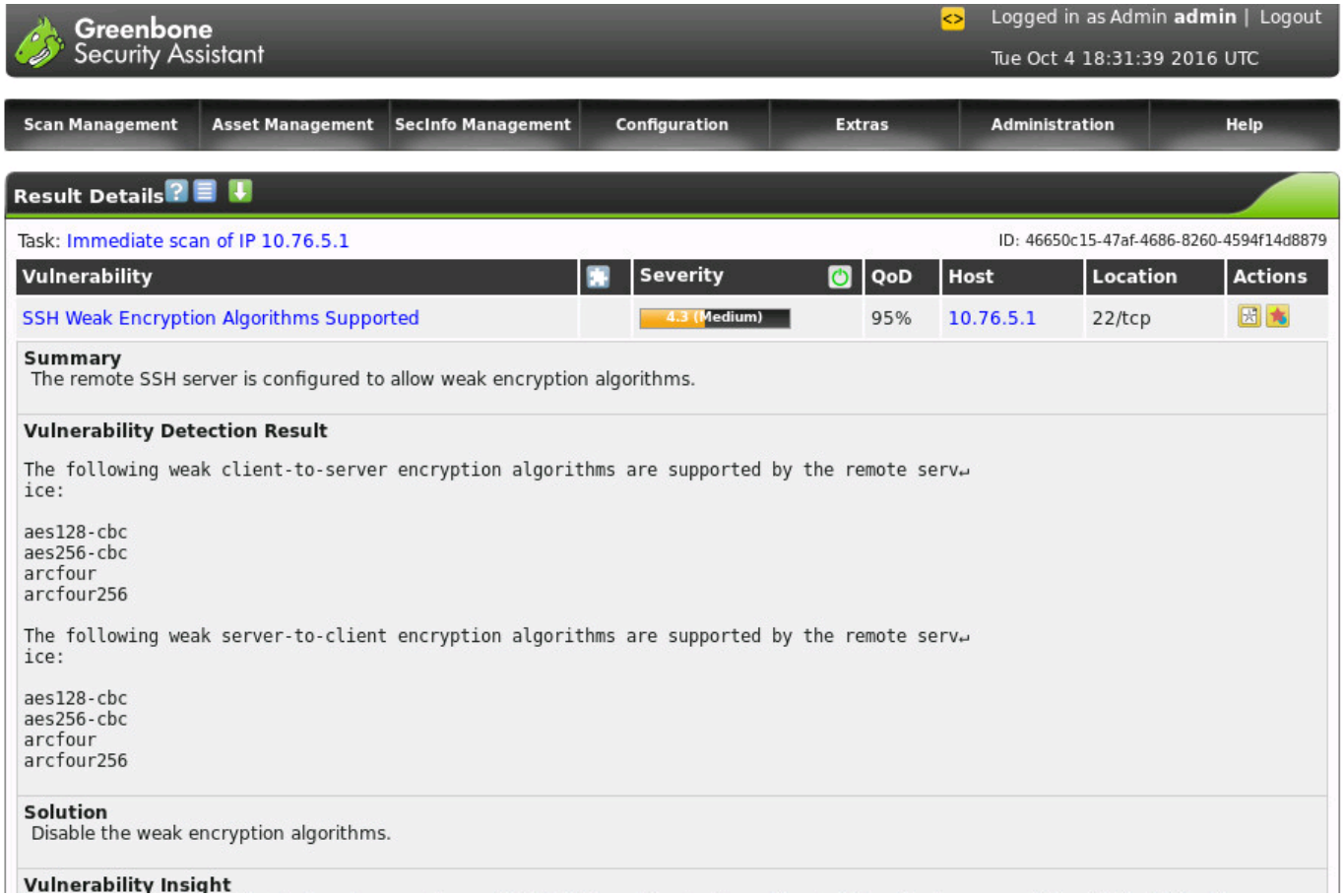
OpenVAS



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	

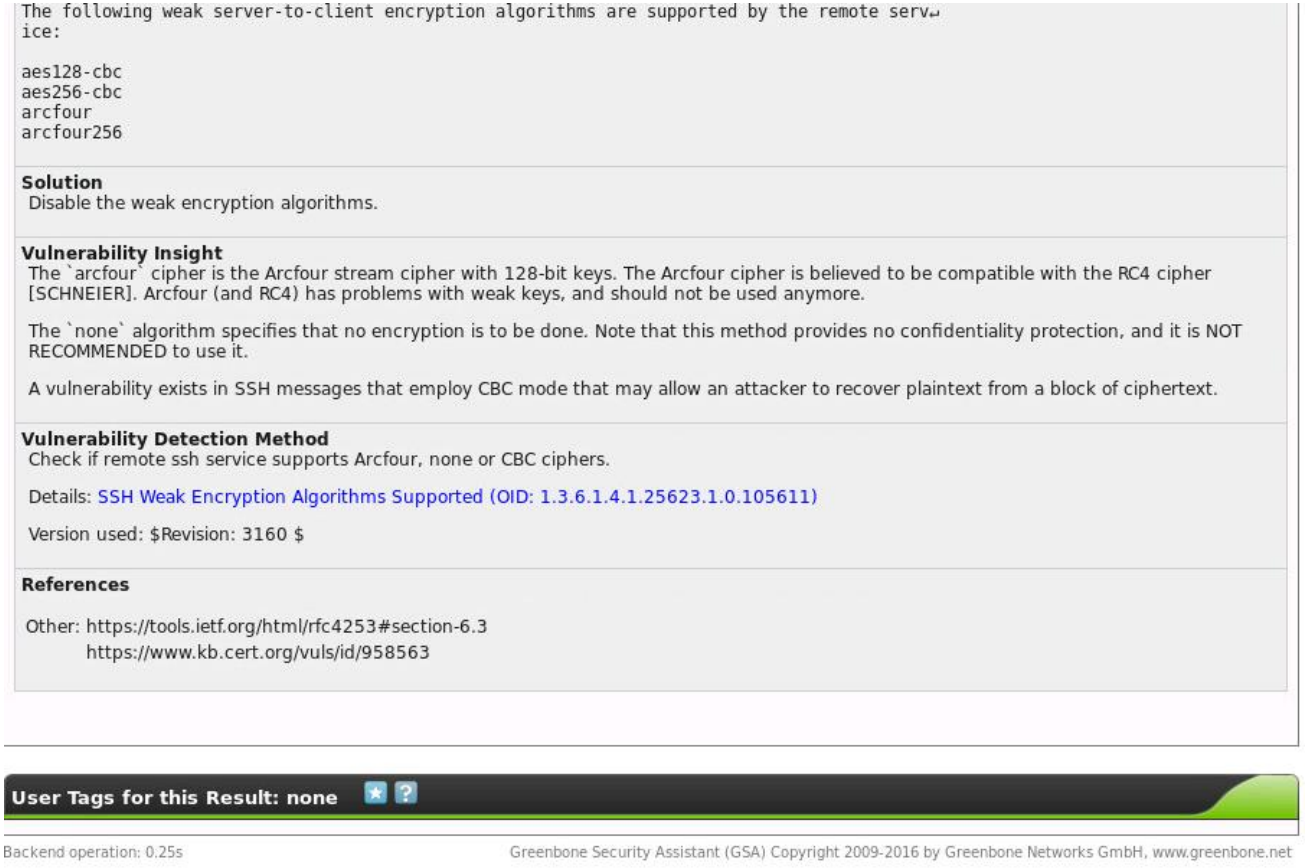
http://www.openvas.org/

OpenVAS



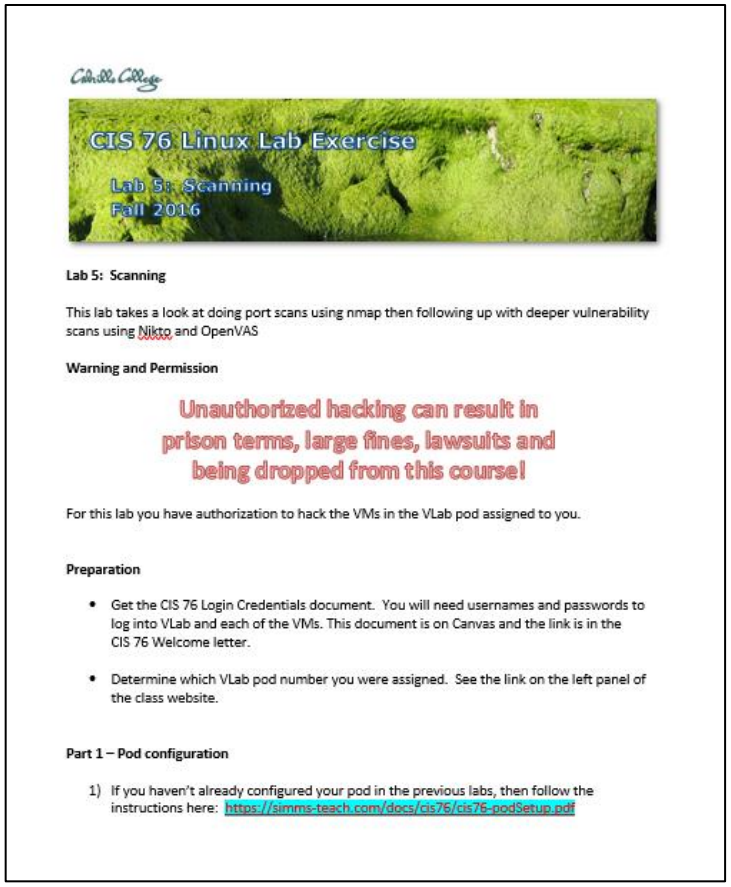
http://www.openvas.org/

OpenVAS



http://www.openvas.org/


Assignment



Cabrillo College

CIS 76 Linux Lab Exercise

Lab 5: Scanning
Fall 2016

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]*

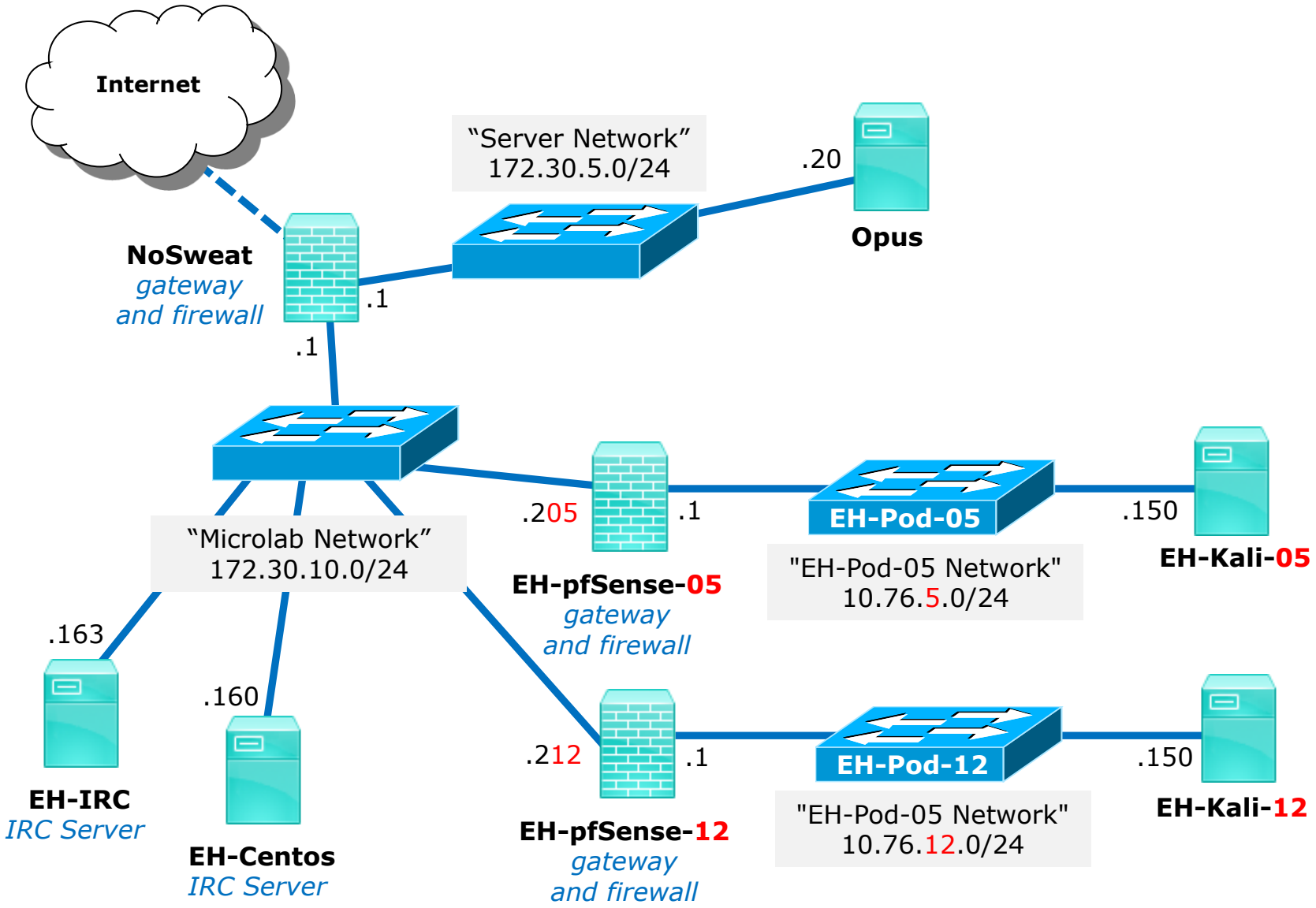
[ ] Add Steganography file to /home/cis76/depot

```
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


Internet
"Server Network"
172.30.5.0/24
.20
Opus
NoSweat
gateway
and firewall
.1
.1
"Microlab Network"
172.30.10.0/24
.205
.1
EH-pfSense-05
gateway
and firewall
EH-Pod-05
"EH-Pod-05 Network"
10.76.5.0/24
.150
EH-Kali-05
.163
EH-IRC
IRC Server
.160
EH-Centos
IRC Server
.212
.1
EH-pfSense-12
gateway
and firewall
EH-Pod-12
"EH-Pod-05 Network"
10.76.12.0/24
.150
EH-Kali-12