Rich's lesson module checklist

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

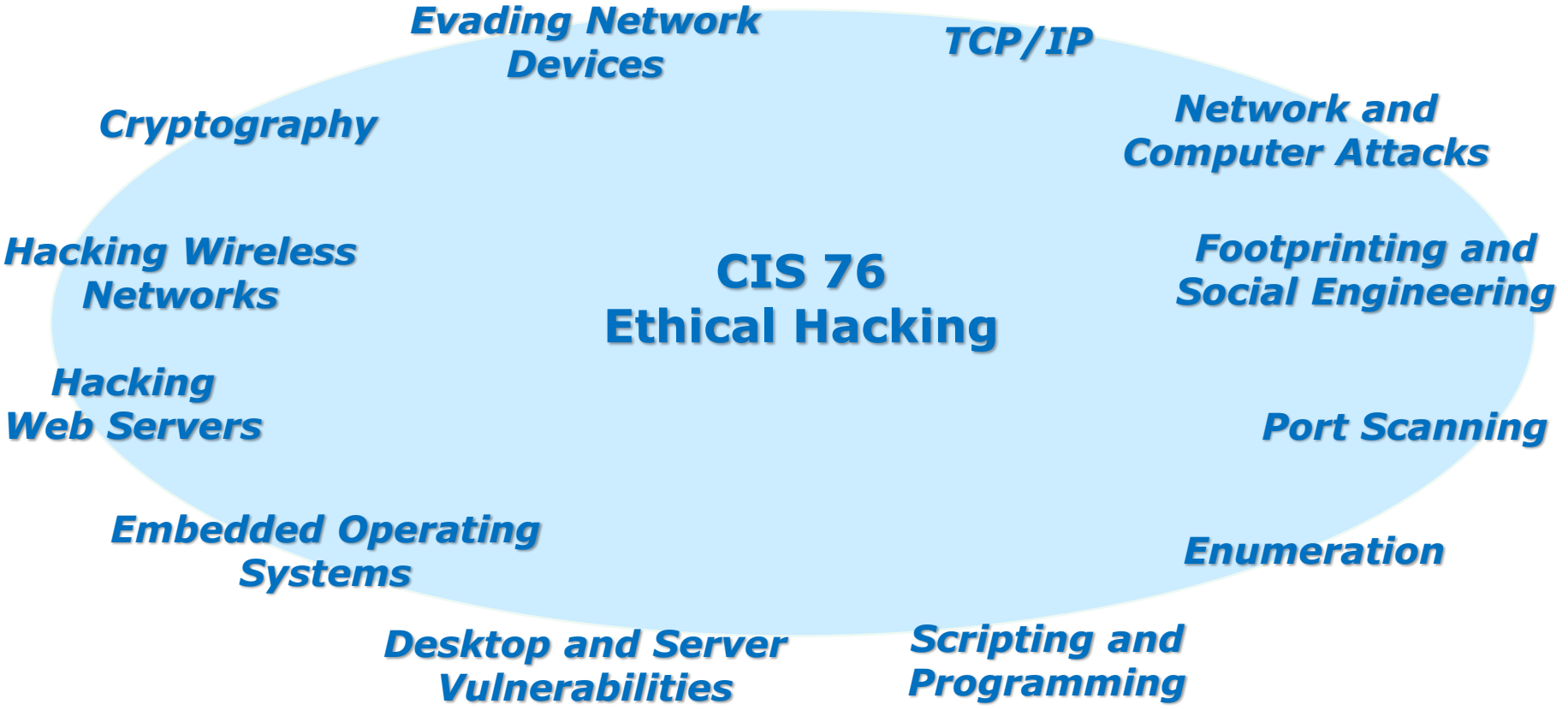
- ❑ Flash cards
- ❑ Properties
- ❑ Page numbers
- ❑ 1st minute quiz
- ❑ Web Calendar summary
- ❑ Web book pages
- ❑ Commands

- ❑ Practice Test #3 tested and ready to go
- ❑ Login credentials for NetLab VE

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

- ❑ Update CCC Confer and 3C Media portals

Last updated 12/5/2017



Student Learner Outcomes

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

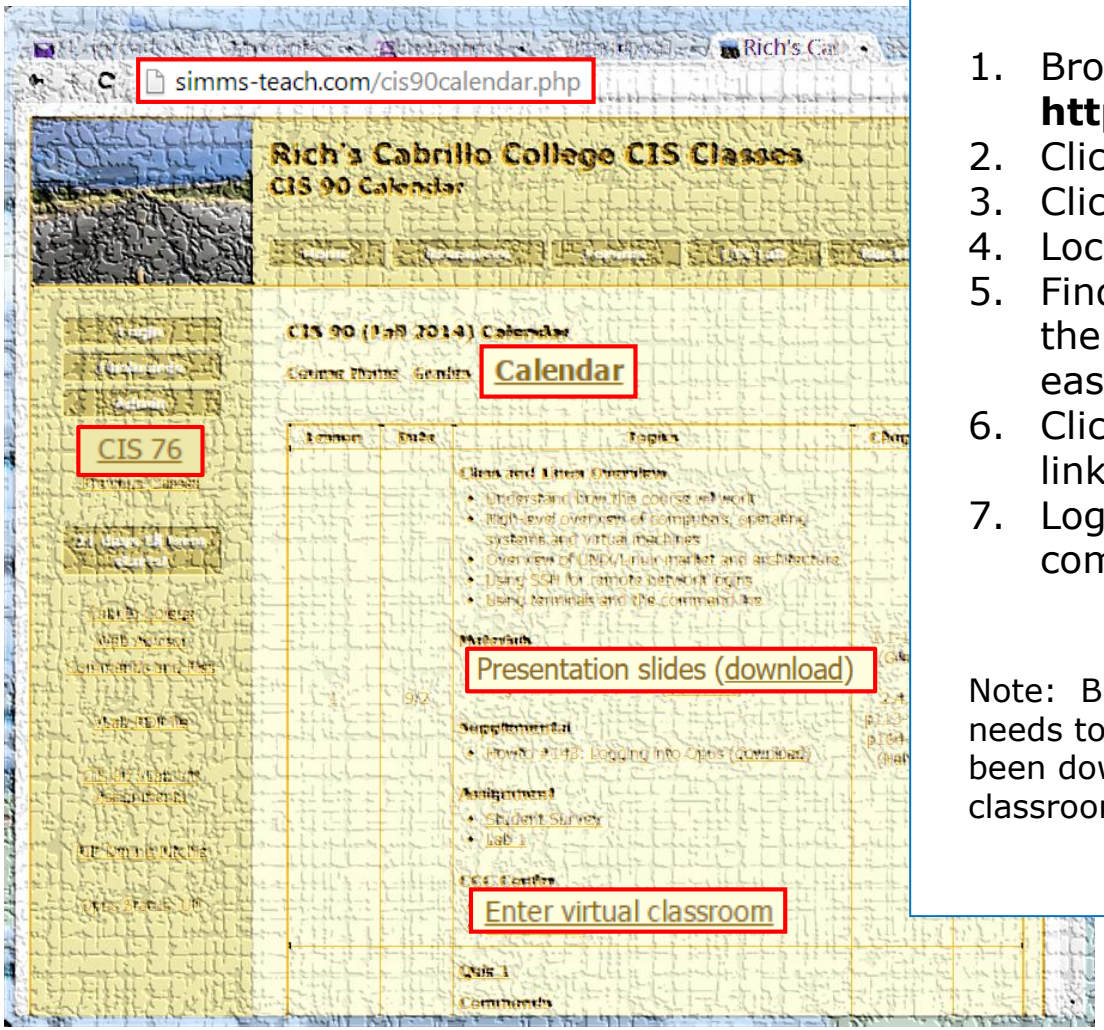
2. Defend a computer and a LAN against a variety of different types of security attacks using a number of hands-on techniques.

Introductions and Credits

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

And thanks to:
- Steven Bolt at for his WASTC EH training.
- Kevin Vaccaro for his CSSIA EH training and Netlab+ pods.
- EC-Council for their online self-paced CEH v9 course.
- Sam Bowne for his WASTC seminars, textbook recommendation and fantastic EH website (https://samsclass.info/).
- Lisa Bock for her great lynda.com EH course.
- John Govsky for many teaching best practices: e.g. the First Minute quizzes, the online forum, and the point grading system (http://teacherjohn.com/).
- Google for everything else!

Student checklist for attending class

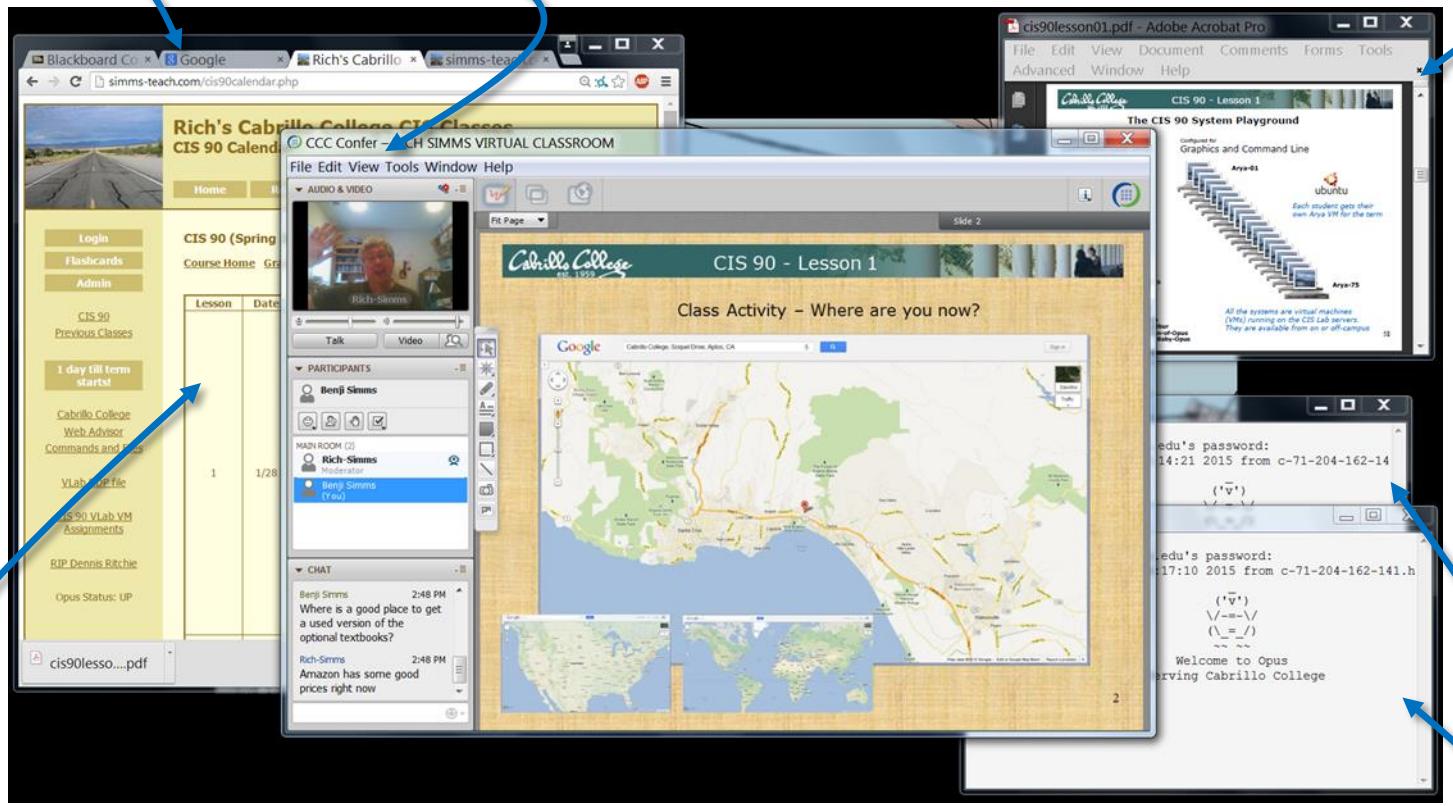


1. Browse to: **http://simms-teach.com**
2. Click the **CIS 76** link.
3. Click the **Calendar** link.
4. Locate today's lesson.
5. Find the **Presentation slides** for the lesson and **download** for easier viewing.
6. Click the **Enter virtual classroom** link to join CCC Confer.
7. Log into Opus-II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

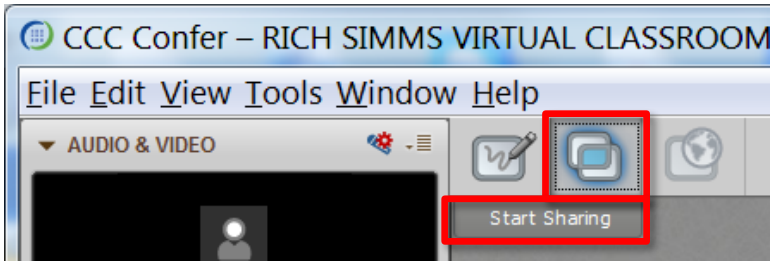
- ❑ *Google*
- ❑ *CCC Confer*
- ❑ *Downloaded PDF of Lesson Slides*



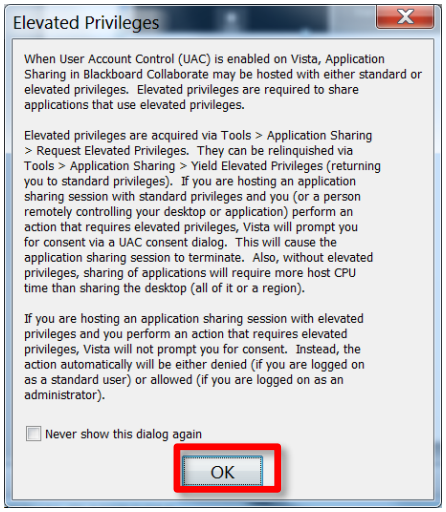
- ❑ *CIS 76 website Calendar page*
- ❑ *One or more login sessions to Opus-II*

Student checklist for sharing desktop with classmates

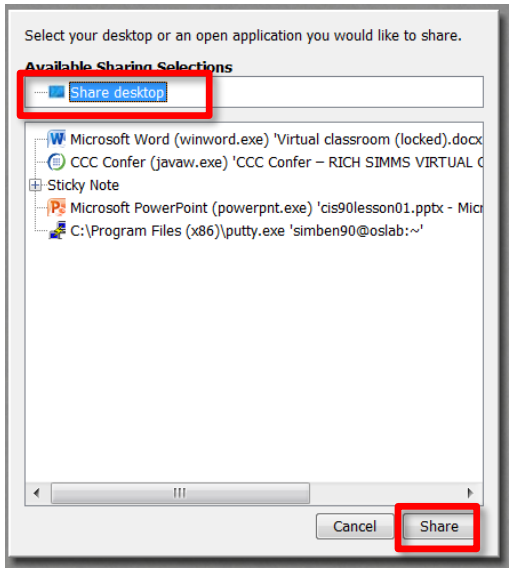
1) Instructor gives you sharing privileges.



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



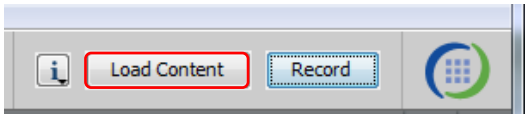
3) Click OK button.



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

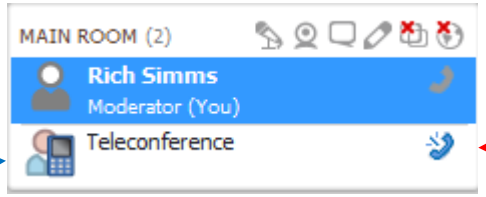
Rich's CCC Confer checklist - setup

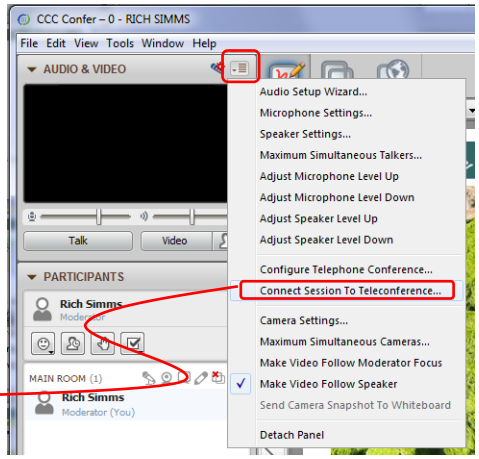
[ ] Preload White Board



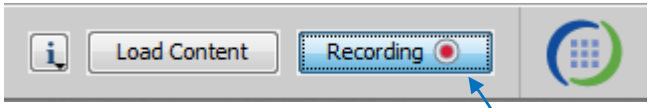
[ ] Connect session to Teleconference

Session now connected to teleconference





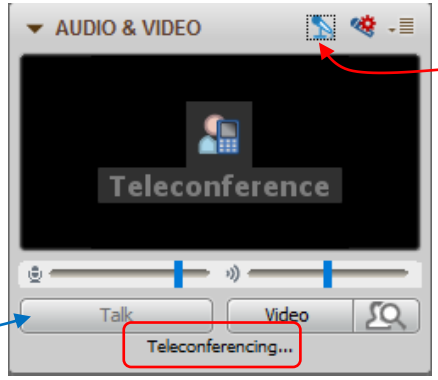
[ ] Is recording on?



Red dot means recording

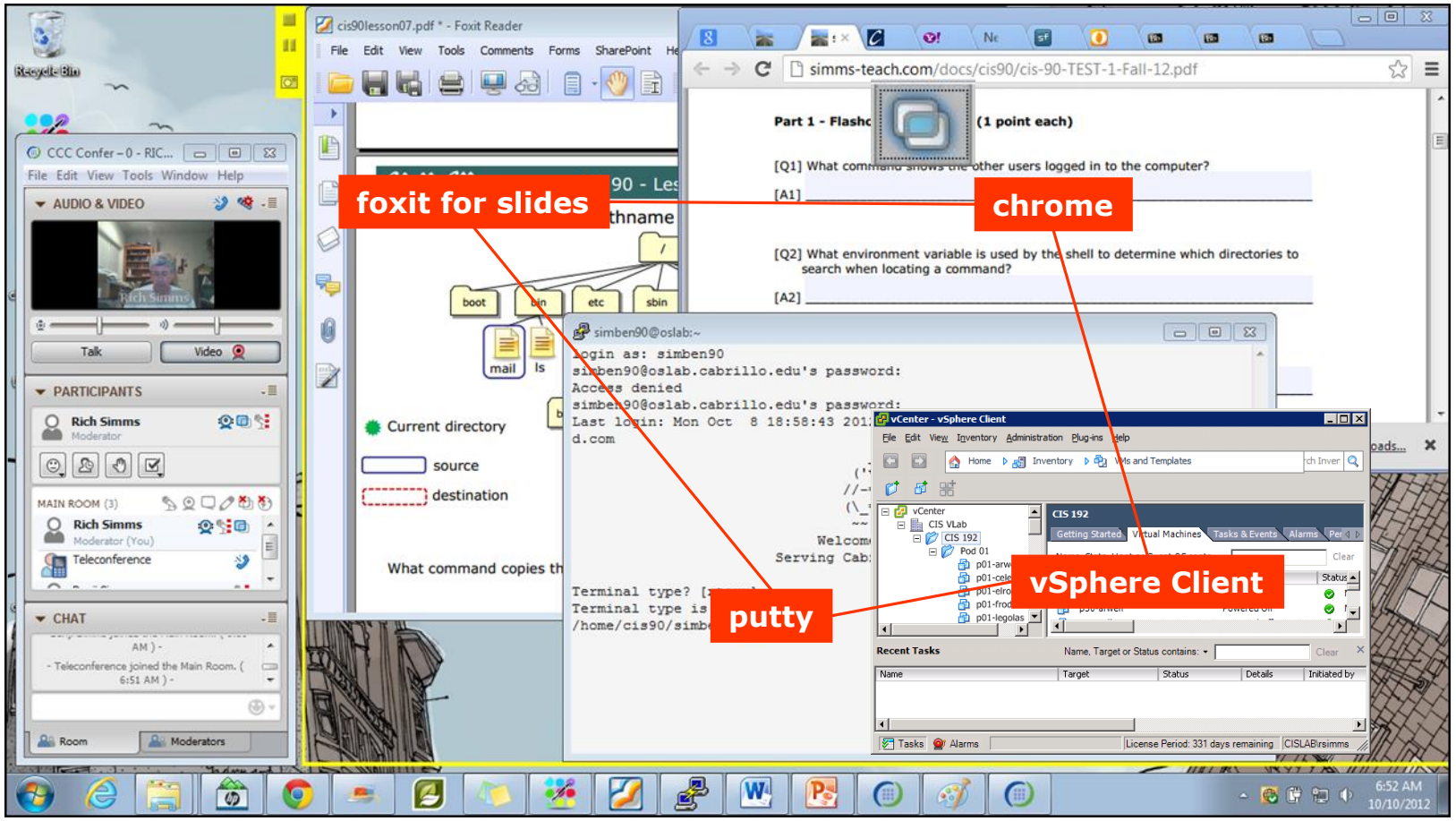
[ ] Use teleconferencing, not mic

Should be grayed out



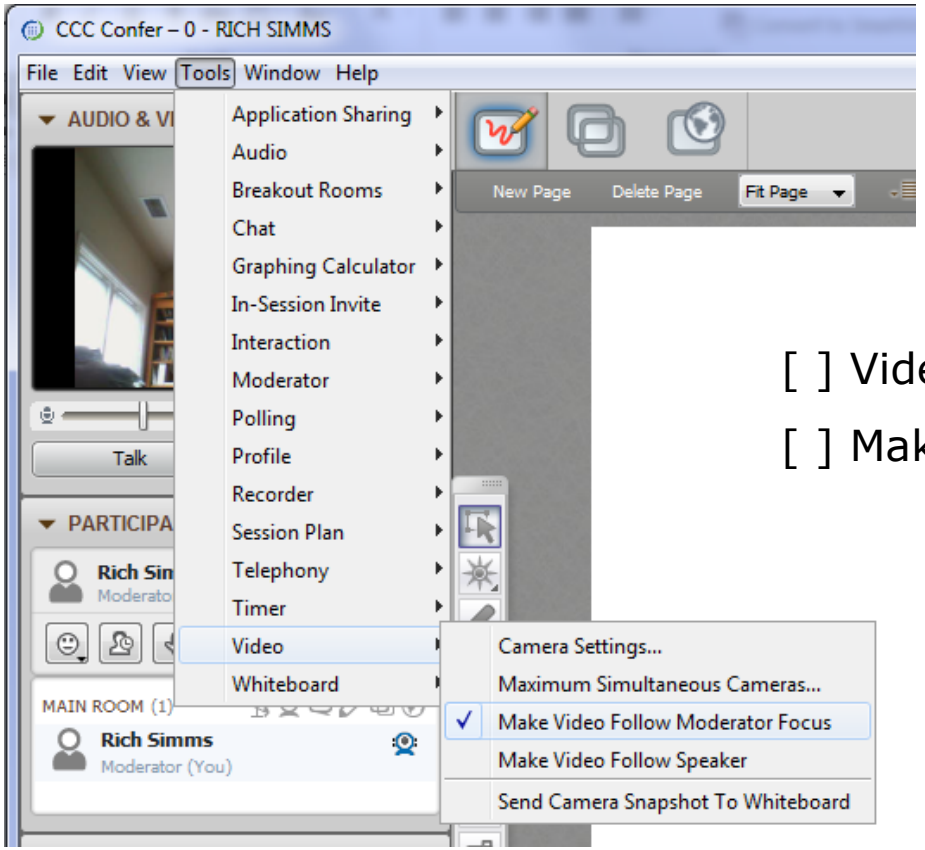
Should change from phone handset icon to little Microphone icon and the Teleconferencing … message displayed

Rich's CCC Confer checklist - screen layout



[ ] layout and share apps

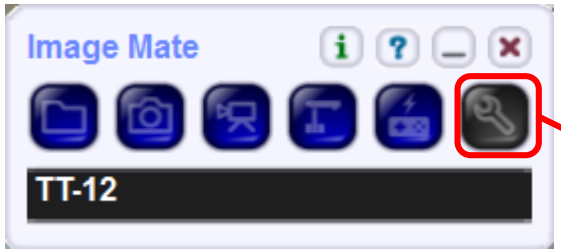
Rich's CCC Confer checklist - webcam setup

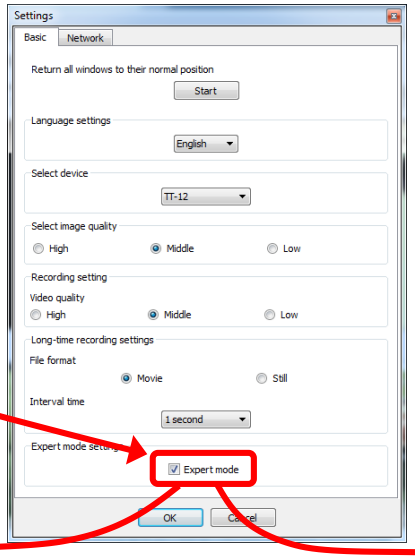


[ ] Video (webcam)

[ ] Make Video Follow Moderator Focus

Rich's CCC Confer checklist - Elmo



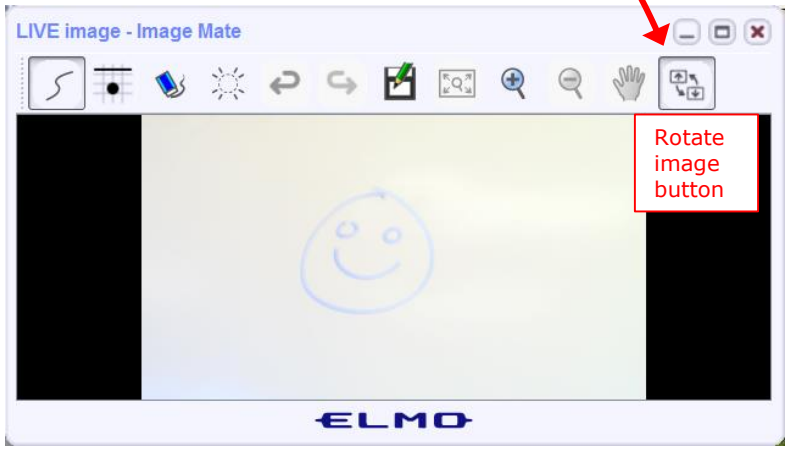


The "rotate image" button is necessary if you use both the side table and the white board.

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

Elmo rotated down to view side table

Elmo rotated up to view white board



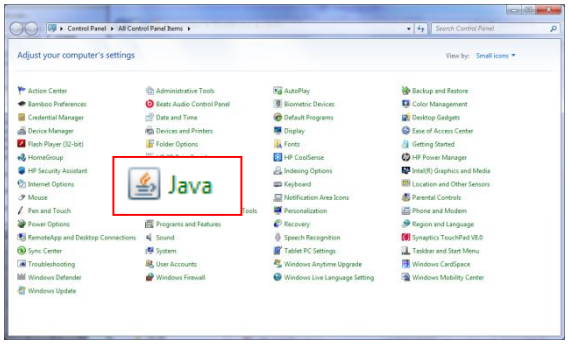
Run and share the Image Mate program just as you would any other app with CCC Confer

Rich's CCC Confer checklist - universal fixes

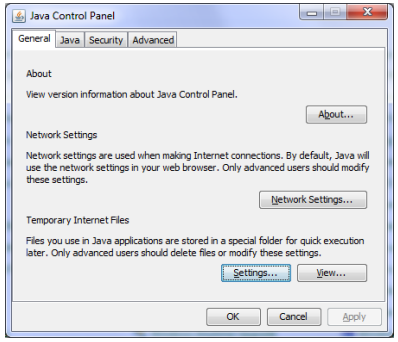
Universal Fix for CCC Confer:

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

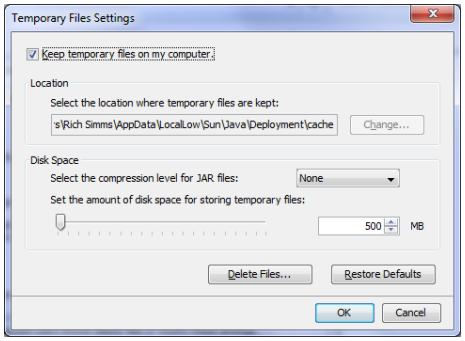
Control Panel (small icons)



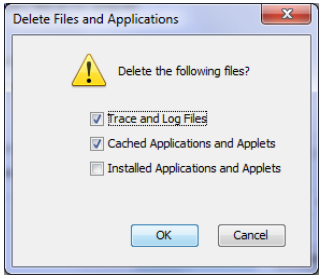
General Tab > Settings…



500MB cache size



Delete these



Google Java download

Start

Sound Check

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

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

Volume
**4 - increase conference volume.*
**7 - decrease conference volume.*
**5 - increase your voice volume.*
**8 - decrease your voice volume.*

CIS 76 - Lesson 15

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


Bruce


Philip


Sam B.


Sam R.


Miguel


Bobby


Garrett


May


Chris


Tanner


Helen


Xu


Mariano


Cameron


Tre


Aga


Ryan M.


Karl-Heinz


Remy


Ryan A.

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

Quiz

No Quiz Today !

Network Protection Systems

Objectives

- Describe how routers protect networks
- Describe firewall technology
- Describe intrusion detection systems
- Describe honeypots

Agenda

- NO QUIZ
- Questions
- In the news
- Best practices
- Housekeeping
- Network devices
- Firewalls
- IDS and IPS
- Final project presentations
- Assignment
- Wrap up

Admonition

Unauthorized hacking is a crime.

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

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

Questions

Questions

How this course works?

Past lesson material?

Previous labs?

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

Chinese Proverb	他問一個問題，五分鐘是個傻子，他不問一個問題仍然是一個傻瓜永遠。 *He who asks a question is a fool for five minutes; he who does not ask a question remains a fool forever.*

In the news

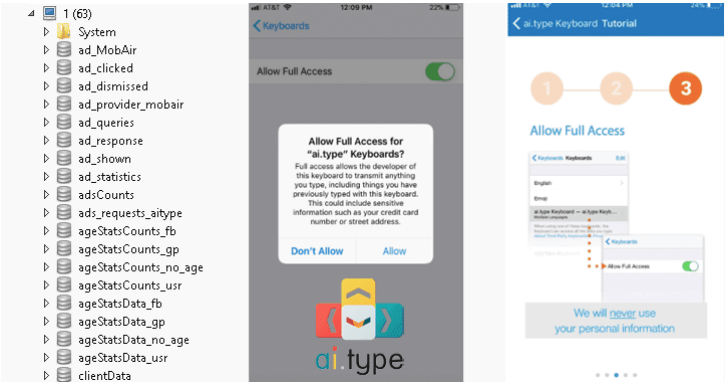
Recent news

Massive Breach Exposes Keyboard App that Collects Personal Data On Its 31 Million Users

Tuesday, December 05, 2017 Mohit Kumar

https://thehackernews.com/2017/12/keyboard-data-breach.html

The Hacker News
Security in a serious way



"Nowadays, many app developers are following irresponsible practices that are worth understanding, and we don't have a better example than this newly-reported incident about a virtual keyboard app."

"Apparently, a misconfigured MongoDB database, owned by the Tel Aviv-based startup AI.type, exposed their entire 577 GB of the database online that includes a shocking amount of sensitive details on their users, which is not even necessary for the app to work."

"...they appear to collect everything from contacts to keystrokes."

Recent news

Hacked Password Service Leakbase Goes Dark

December 2017

https://krebsonsecurity.com/2017/12/hacked-password-service-leakbase-goes-dark/

KrebsonSecurity
In-depth security news and investigation

"Leakbase[dot]pw began selling memberships in September 2016, advertising more than two billion usernames and passwords that were stolen in high-profile breaches at sites like linkedin.com, myspace.com and dropbox.com"

"Leakbase, a Web site that indexed and sold access to billions of usernames and passwords stolen in some of the world largest data breaches, has closed up shop. A source close to the matter says the service was taken down in a law enforcement sting that may be tied to the Dutch police raid of the Hansa dark web market earlier this year."

Recent news

Young Hacker, Who Took Over Jail Network to Get Friend Released Early, Faces Prison

Monday, December 04, 2017 Swati Khandelwal

https://thehackernews.com/2017/12/hacking-jail-records.html

The Hacker News
Security in a serious way

"Konrads Voits from Ann Arbor, Michigan, pleaded guilty in federal court last week for hacking into the Washtenaw County government computer system earlier this year using malware, phishing, and social engineering tricks in an attempt to get his friend released early from jail."

"However, things did not work as Voits wanted them to, and instead, they all backfired on him when jail employees detected changes in their records and alerted the FBI."

"No prisoners were then released early."

Recent news

Here's the NSA Employee Who Kept Top Secret Documents at Home

Friday, December 01, 2017 Swati Khandelwal

https://thehackernews.com/2017/12/nghia-hoang-pho-nsa.html

The Hacker News
Security in a serious way

"In a press release published Friday, the US Justice Department announced that Nghia Hoang Pho, a 67-year-old of Ellicott City, Maryland, took documents that contained top-secret national information from the agency between 2010 and 2015."

"Pho, who worked as a developer for the Tailored Access Operations (TAO) hacking group at the NSA, reportedly moved the stolen classified documents and tools to his personal Windows computer at home, which was running Kaspersky Lab software."

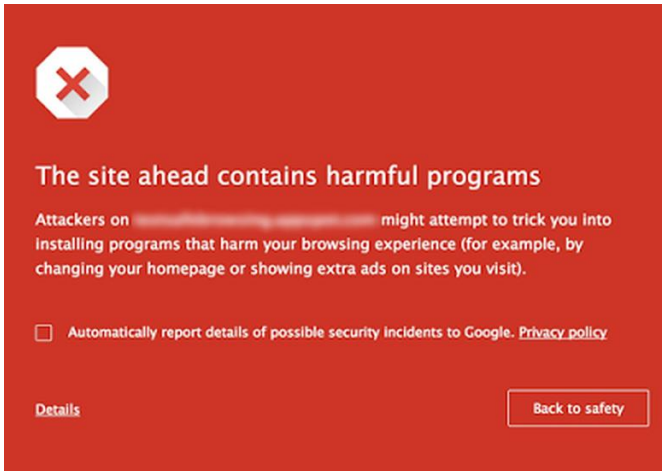
Best Practices

Best Practices

Google cracks down on apps that snoop on you, even if they're not in Play Store

By Liam Tung | December 4, 2017

http://www.zdnet.com/article/google-cracks-down-on-apps-that-snoop-on-you-even-if-theyre-not-in-play-store/



"Google is giving developers two months to ensure their apps don't deviate from its Unwanted Software policy. If an app continues to stray from the policy, users are likely to see its Safe Browsing full-page warnings, which will probably drive users away from the offending software."

"The Safe Browsing warnings will appear "on apps and on websites leading to apps that collect a user's personal data without their consent", Google said on its security blog."

Housekeeping

Housekeeping

1. Don't forget to submit your project tonight by 11:59PM!
   - By email to risimms@cabrillo.edu
   - Or put a copy in the Student Project Folder using the link on the Calendar page. Be sure share permissions on your document to allow me to read it.

2. All eight extra credit labs are available (6 points each) and due the day of the final exam.

3. Last five forum posts are due the day of the final exam.

4. The final exam (Test #3) is next week and the practice test is available after class.

Heads up on Final Exam

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

Tue	12/12	**Test #3 (the final exam)** **Time** • Tuesday 4:00PM - 6:50PM in Room 828 **Materials** • Test (canvas) **CCC Confer** • Enter virtual classroom • Archives Confer or 3CMedia		5 posts Lab X1 Lab X2 Lab X3 Lab X4 Lab X5 Lab X6 Lab X7 Lab X8

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

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

FALL 2017 FINAL EXAMINATIONS SCHEDULE
DECEMBER 11 TO DECEMBER 16

DAYTIME FINAL SCHEDULE

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

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

CIS 76 **Introduction to Cybersecurity: Ethical Hacking**

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

Section	Days	Times	Units	Instructor	Room
98163	T	5:30PM-8:35P	3.00	R.Simms	OL

Section 98163 is an ONLINE course. Meets weekly throughout the semester online by remote technology with an additional 50 min online lab per week. For details, see instructor's web page at go.cabrillo.edu/online.

98164	T	5:30PM-8:35PM	3.00	R.Simms	828
&	Arr.	Arr.		R.Simms	OL

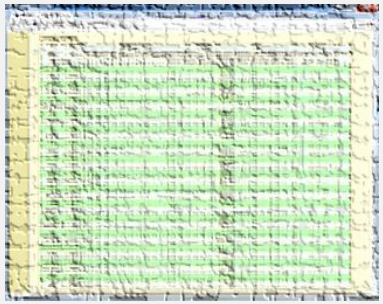
Section 98164 is a Hybrid ONLINE course. Meets weekly throughout the semester at the scheduled times with an additional 50 min online lab per week. For details, see instructor's web page at go.cabrillo.edu/online.

Where to find your grades

Send me your survey to get your LOR code name.

The CIS 76 website Grades page

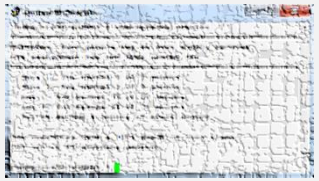
http://simms-teach.com/cis76grades.php



Or check on Opus-II

checkgrades *codename*

(where codename is your LOR codename)



Written by Jesse Warren a past CIS 90 Alumnus

To run checkgrades update your path in .bash_profile with:
PATH=$PATH:/home/cis76/bin

Percentage	Total Points	Letter Grade	Pass/No Pass
90% or higher	504 or higher	A	Pass
80% to 89.9%	448 to 503	B	Pass
70% to 79.9%	392 to 447	C	Pass
60% to 69.9%	336 to 391	D	No pass
0% to 59.9%	0 to 335	F	No pass

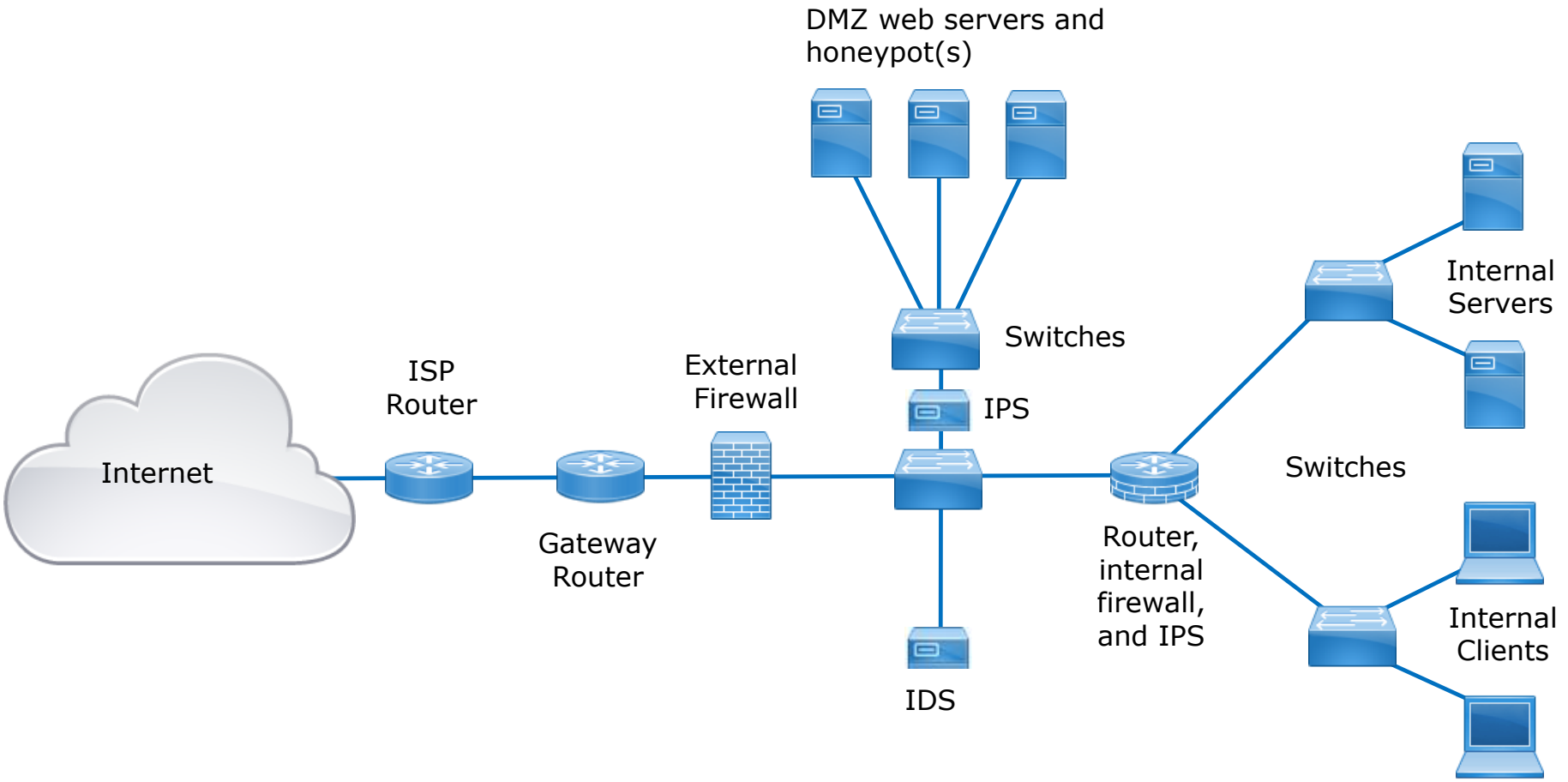
At the end of the term I'll add up all your points and assign you a grade using this table

Points that could have been earned:

10 quizzes:	30 points
10 labs:	300 points
2 tests:	60 points
3 forum quarters:	60 points
Total:	**450 points**

Network Devices

Various Network Devices



Hypothetical topology of switches, routers, firewalls, IDS, IPS and honeypots

Routers

Routers

- Routers are at the intersection of multiple network segments.
- They operate at Layer 3 the "Network" layer.
- Routers look at a packet's destination IP address and a routing table to decide where to send a packet. Kind of like using a sign post in Europe to decide which direction to go.
- If there is no route for a packet's destination, the packet is dropped.

https://www.flickr.com/photos/13426843@N08/4291372540

https://www.flickr.com/photos/38109472@N00/4237980827


Routers


Configuring the routes in routing tables

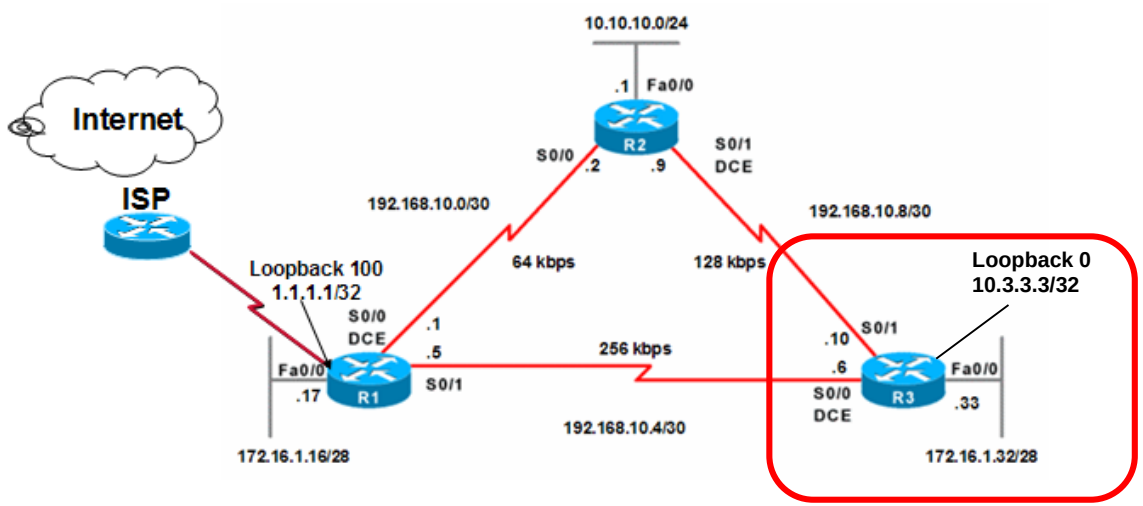
- Manually - you can add static routes by hand. This does not work though if you have lots of routers to configure.
- Dynamic - routing protocols cans be used between participating routers to automatically calculate and populate routing tables with the best routes. Example routing protocols are RIP, OSPF, BGP, EIGRP, etc.

https://www.flickr.com/photos/13426843@N08/4291372540

https://www.flickr.com/photos/38109472@N00/4237980827

Example Cisco Routing Table

```
R3#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 192.168.10.5 to network 0.0.0.0

     192.168.10.0/30 is subnetted, 3 subnets
O       192.168.10.0 [110/1952] via 192.168.10.5, 00:00:23, Serial0/0
C       192.168.10.4 is directly connected, Serial0/0
C       192.168.10.8 is directly connected, Serial0/1
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.1.32/29 is directly connected, FastEthernet0/0
O       172.16.1.16/28 [110/400] via 192.168.10.5, 00:00:23, Serial0/0
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.3.3.3/32 is directly connected, Loopback0
O       10.10.10.0/24 [110/791] v
O*E2 0.0.0.0/0 [110/1] via 192.16
R3#
```

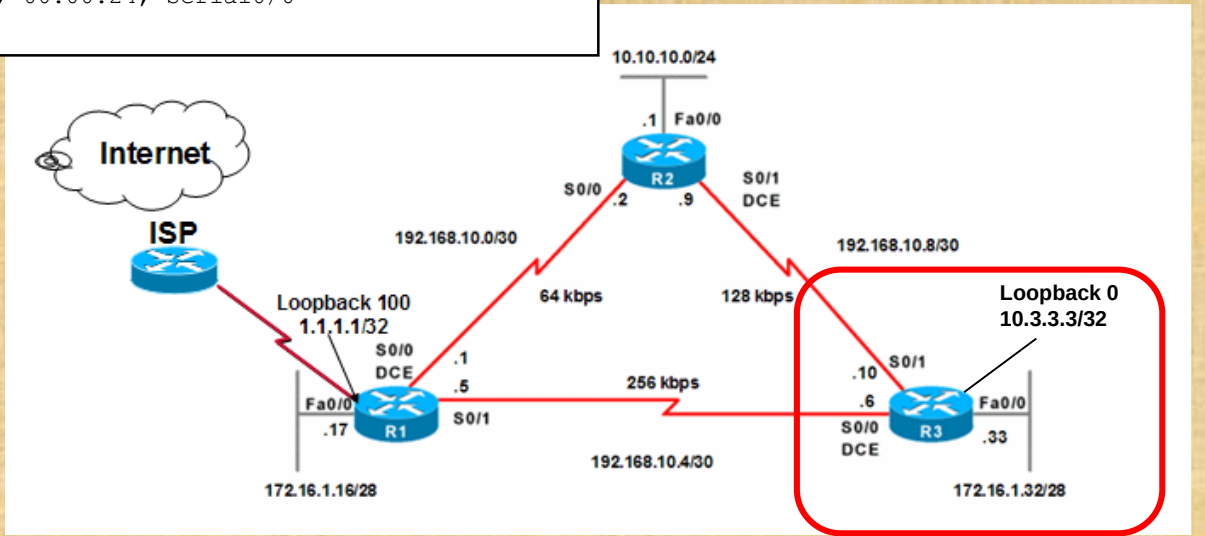


Example Cisco Routing Table

```
R3#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 192.168.10.5 to network 0.0.0.0

     192.168.10.0/30 is subnetted, 3 subnets
O       192.168.10.0 [110/1952] via 192.168.10.5, 00:00:23, Serial0/0
C       192.168.10.4 is directly connected, Serial0/0
C       192.168.10.8 is directly connected, Serial0/1
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.1.32/29 is directly connected, FastEthernet0/0
O       172.16.1.16/28 [110/400] via 192.168.10.5, 00:00:23, Serial0/0
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.3.3.3/32 is directly connected, Loopback0
O       10.10.10.0/24 [110/791] via 192.168.10.9, 00:00:24, Serial0/1
O*E2 0.0.0.0/0 [110/1] via 192.168.10.5, 00:00:24, Serial0/0
R3#
```

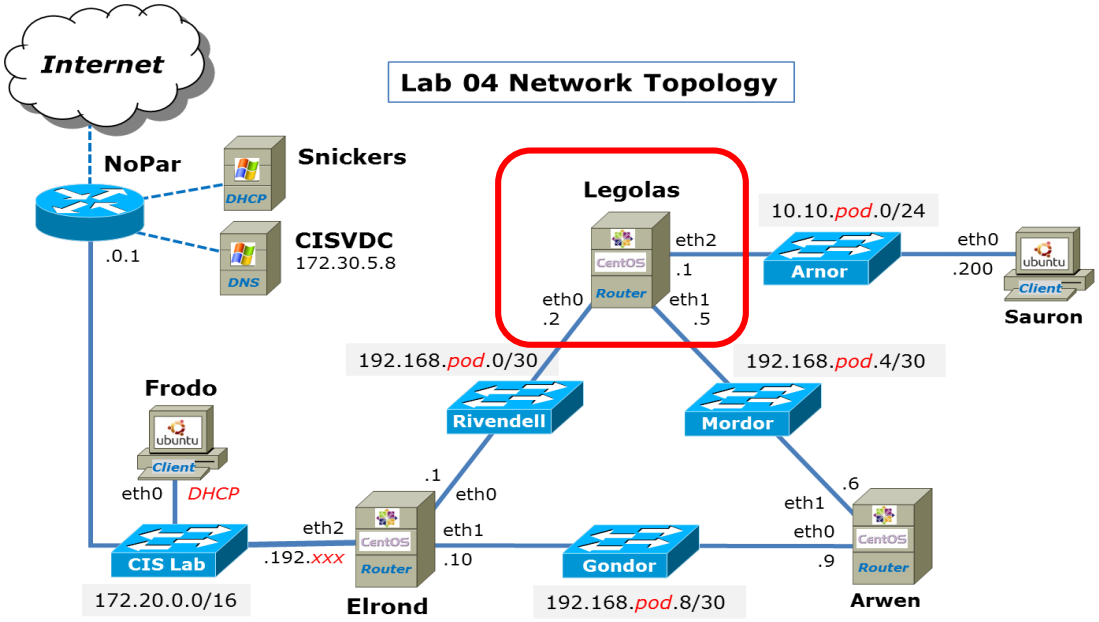
According to this routing table, what would R3 do with a packet destined for 192.168.10.2?

Put your answer in the chat window



Example Linux Routing Table

```
Legolas route -n output (for Pod 3)
-----------------------------------
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.3.0     0.0.0.0         255.255.255.252 U     0      0        0 eth0
192.168.3.4     0.0.0.0         255.255.255.252 U     0      0        0 eth1
192.168.3.8     192.168.3.1     255.255.255.252 UG    2      0        0 eth0
10.10.3.0       0.0.0.0         255.255.255.0   U     0      0        0 eth2
169.254.0.0     0.0.0.0         255.255.0.0     U     1002   0        0 eth0
169.254.0.0     0.0.0.0         255.255.0.0     U     1003   0        0 eth1
169.254.0.0     0.0.0.0         255.255.0.0     U     1004   0        0 eth2
172.20.0.0      192.168.3.1     255.255.0.0     UG    2      0        0 eth0
0.0.0.0         192.168.3.1     0.0.0.0         UG    2      0        0 eth0
```



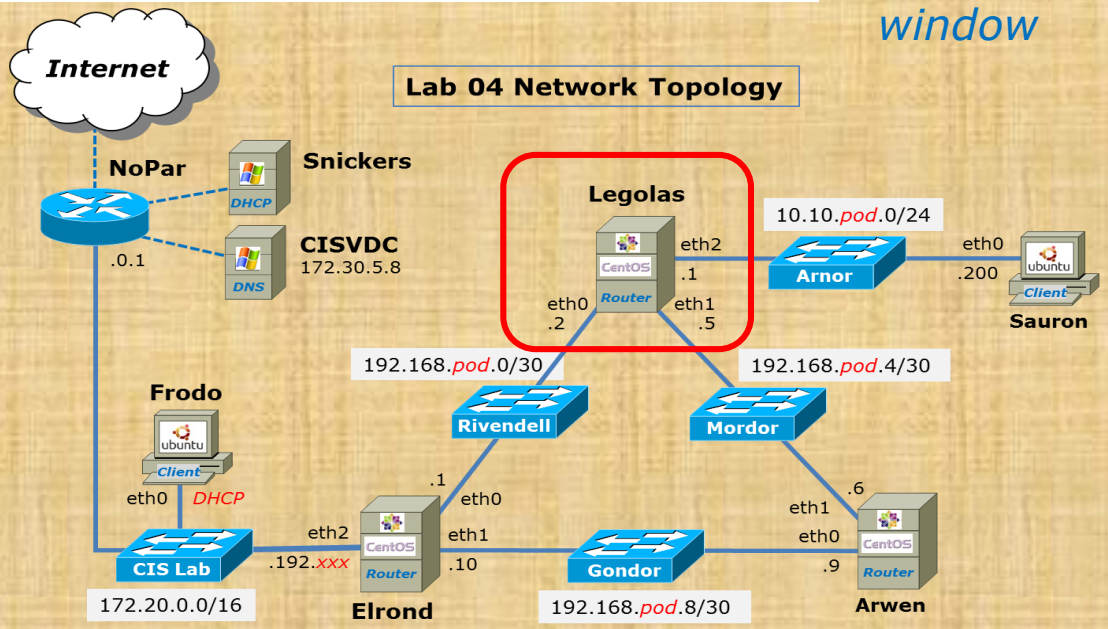
pod=your pod number, *xxx*=one of your assigned IP addresses

Example Linux Routing Table

```
Legolas route -n output (for Pod 3)
-----------------------------------
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.3.0     0.0.0.0         255.255.255.252 U     0      0        0 eth0
192.168.3.4     0.0.0.0         255.255.255.252 U     0      0        0 eth1
192.168.3.8     192.168.3.1     255.255.255.252 UG    2      0        0 eth0
10.10.3.0       0.0.0.0         255.255.255.0   U     0      0        0 eth2
169.254.0.0     0.0.0.0         255.255.0.0     U     1002   0        0 eth0
169.254.0.0     0.0.0.0         255.255.0.0     U     1003   0        0 eth1
169.254.0.0     0.0.0.0         255.255.0.0     U     1004   0        0 eth2
172.20.0.0      192.168.3.1     255.255.0.0     UG    2      0        0 eth0
0.0.0.0         192.168.3.1     0.0.0.0         UG    2      0        0 eth0
```

According to this routing table, what would Legolas do with a packet destined for 192.168.3.6?

Put your answer in the chat window



pod=your pod number, *xxx*=one of your assigned IP addresses


Routers

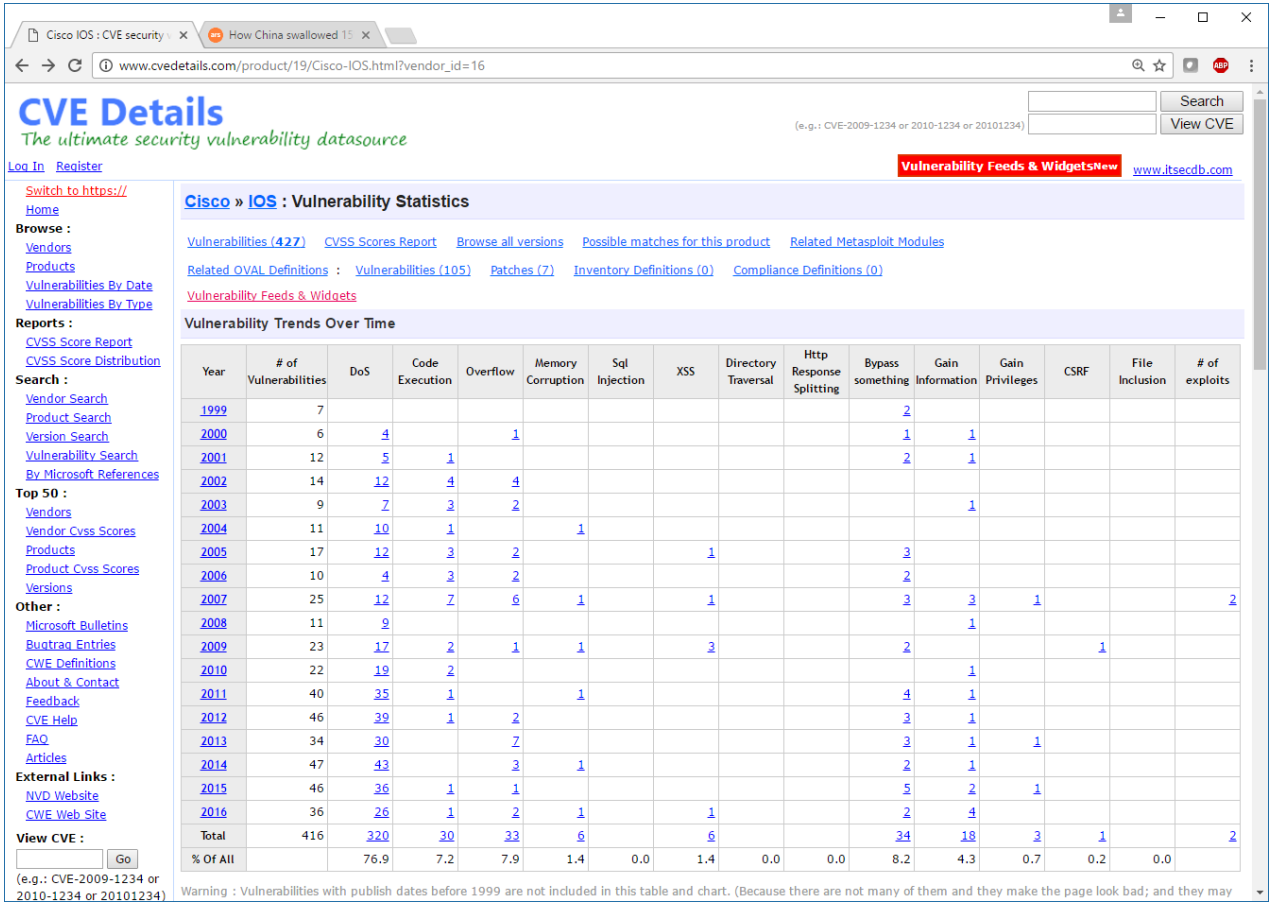

Unfortunately routers can be hacked like everything else

- Vulnerabilities in router operating systems.
- Vulnerabilities in the software that configures or manages routers.
- They can be misconfigured by mistake.
- Tricking them into adding fraudulent routes into their routing tables.

https://www.flickr.com/photos/13426843@N08/4291372540

https://www.flickr.com/photos/38109472@N00/4237980827

Cisco IOS Vulnerabilities

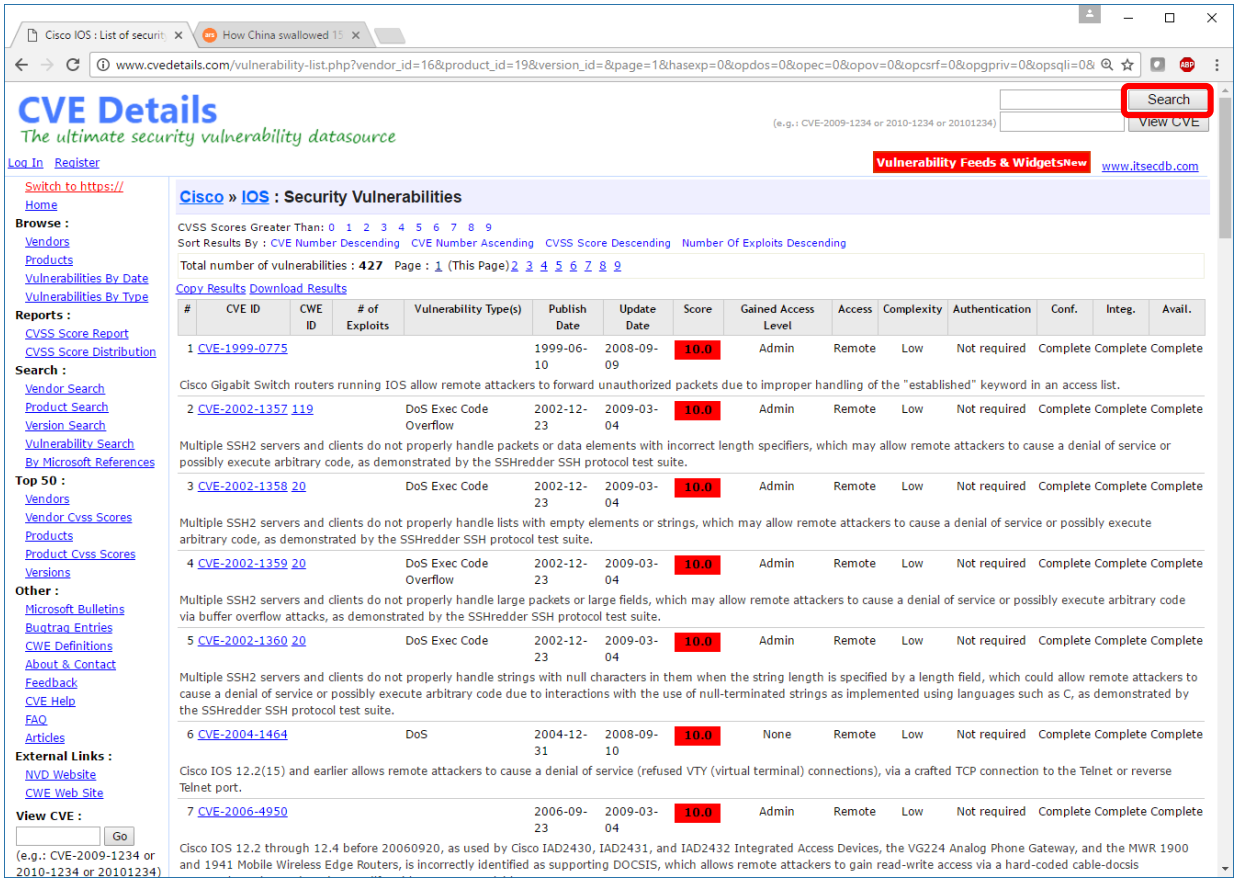


Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
1999	7									2					
2000	6	4		1						1	1				
2001	12	5	1							2	1				
2002	14	12	4	4											
2003	9	7	3	2							1				
2004	11	10	1		1										
2005	17	12	3	2			1			3					
2006	10	4	3	2						2					
2007	25	12	7	6	1		1			3	3	1			2
2008	11	9									1				
2009	23	17	2	1	1		3			2			1		
2010	22	19	2								1				
2011	40	35	1		1					4	1				
2012	46	39	1	2						3	1				
2013	34	30		7						3	1	1			
2014	47	43		3	1					2	1				
2015	46	36	1	1						5	2	1			
2016	36	26	1	2	1		1			2	4				
Total	416	320	30	33	6		6			34	18	3	1		2
% Of All		76.9	7.2	7.9	1.4	0.0	1.4	0.0	0.0	8.2	4.3	0.7	0.2	0.0	

http://www.cvedetails.com/vendor/16/Cisco.html

Cisco IOS Vulnerabilities

Search for Cisco IOS, select Cisco IOS list of vulnerabilities



CVE Details
The ultimate security vulnerability datasource

Cisco » IOS : Security Vulnerabilities

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-1999-0775				1999-06-10	2008-09-09	10.0	Admin	Remote	Low	Not required	Complete	Complete	Complete
	Cisco Gigabit Switch routers running IOS allow remote attackers to forward unauthorized packets due to improper handling of the "established" keyword in an access list.													
2	CVE-2002-1357 119			DoS Exec Code Overflow	2002-12-23	2009-03-04	10.0	Admin	Remote	Low	Not required	Complete	Complete	Complete
	Multiple SSH2 servers and clients do not properly handle packets or data elements with incorrect length specifiers, which may allow remote attackers to cause a denial of service or possibly execute arbitrary code, as demonstrated by the SSHredder SSH protocol test suite.													
3	CVE-2002-1358 20			DoS Exec Code	2002-12-23	2009-03-04	10.0	Admin	Remote	Low	Not required	Complete	Complete	Complete
	Multiple SSH2 servers and clients do not properly handle lists with empty elements or strings, which may allow remote attackers to cause a denial of service or possibly execute arbitrary code, as demonstrated by the SSHredder SSH protocol test suite.													
4	CVE-2002-1359 20			DoS Exec Code Overflow	2002-12-23	2009-03-04	10.0	Admin	Remote	Low	Not required	Complete	Complete	Complete
	Multiple SSH2 servers and clients do not properly handle large packets or large fields, which may allow remote attackers to cause a denial of service or possibly execute arbitrary code via buffer overflow attacks, as demonstrated by the SSHredder SSH protocol test suite.													
5	CVE-2002-1360 20			DoS Exec Code	2002-12-23	2009-03-04	10.0	Admin	Remote	Low	Not required	Complete	Complete	Complete
	Multiple SSH2 servers and clients do not properly handle strings with null characters in them when the string length is specified by a length field, which could allow remote attackers to cause a denial of service or possibly execute arbitrary code due to interactions with the use of null-terminated strings as implemented using languages such as C, as demonstrated by the SSHredder SSH protocol test suite.													
6	CVE-2004-1464			DoS	2004-12-31	2008-09-10	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
	Cisco IOS 12.2(15) and earlier allows remote attackers to cause a denial of service (refused VTY (virtual terminal) connections), via a crafted TCP connection to the Telnet or reverse Telnet port.													
7	CVE-2006-4950				2006-09-23	2009-03-04	10.0	Admin	Remote	Low	Not required	Complete	Complete	Complete
	Cisco IOS 12.2 through 12.4 before 20060920, as used by Cisco IAD2430, IAD2431, and IAD2432 Integrated Access Devices, the VG224 Analog Phone Gateway, and the MWR 1900 and 1941 Mobile Wireless Edge Routers, is incorrectly identified as supporting DOCSIS, which allows remote attackers to gain read-write access via a hard-coded cable-docsis													

http://www.cvedetails.com/vulnerability-list.php?vendor_id=16&product_id=19&version_id=&page=1&hasexp=0&opdos=0&opec=0&opov=0&opcsrf=0&opgpriv=0&opsqli=0&opxss=0&opdirt=0&opmemc=0&ophttprs=0&opbyp=0&opfileinc=0&opginf=0&cvssscoremin=0&cvssscoremax=0&year=0&month=0&cweid=0&order=3&trc=427&sha=bd51a01b646bad788bdc715f12e17fa177698ba8

Activity

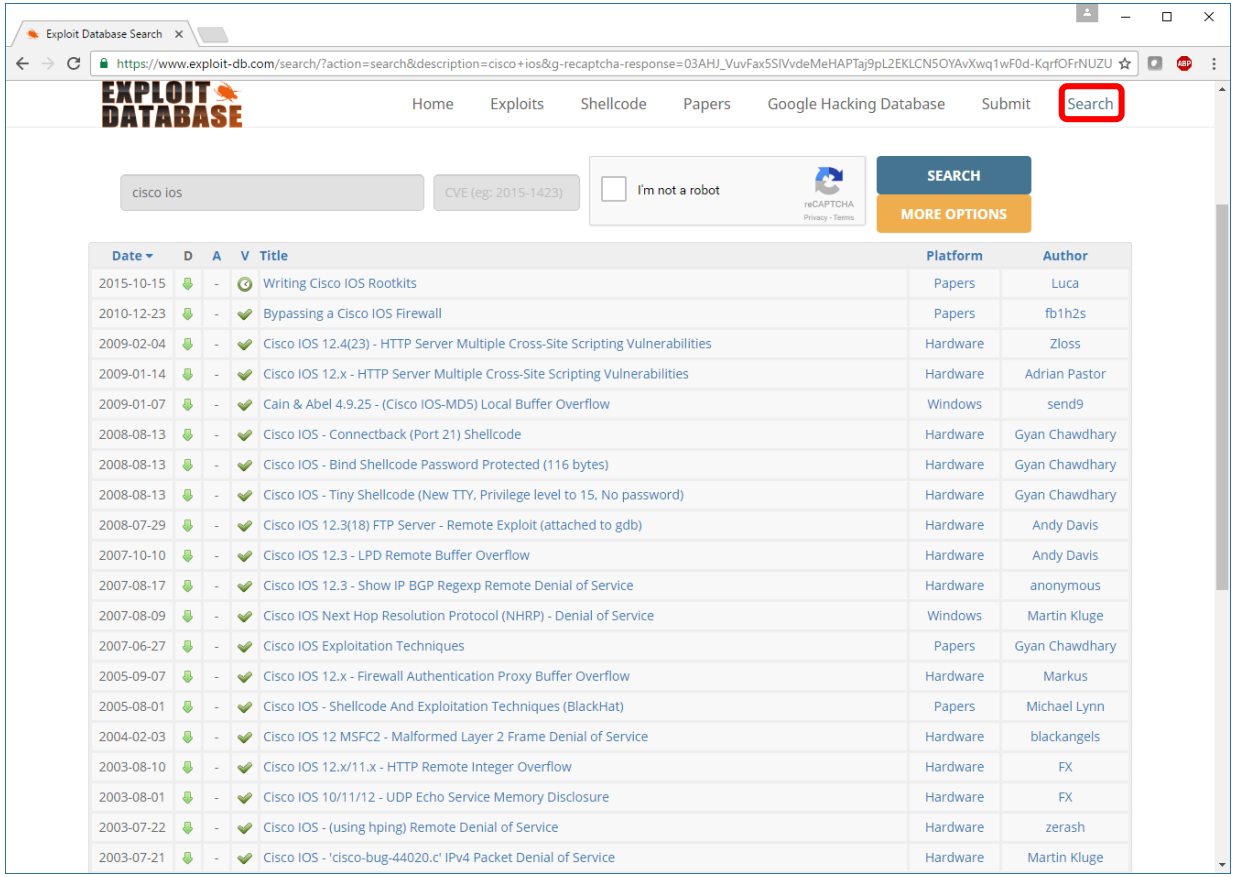
According to CVE Details, what is the most common type of vulnerability found in Cisco's IOS?

http://www.cvedetails.com/vendor/16/Cisco.html

Put your answer in the chat window

Cisco IOS Exploits

Search for Cisco IOS



Date	D	A	V	Title	Platform	Author
2015-10-15		-		Writing Cisco IOS Rootkits	Papers	Luca
2010-12-23		-		Bypassing a Cisco IOS Firewall	Papers	fb1h2s
2009-02-04		-		Cisco IOS 12.4(23) - HTTP Server Multiple Cross-Site Scripting Vulnerabilities	Hardware	Zloss
2009-01-14		-		Cisco IOS 12.x - HTTP Server Multiple Cross-Site Scripting Vulnerabilities	Hardware	Adrian Pastor
2009-01-07		-		Cain & Abel 4.9.25 - (Cisco IOS-MD5) Local Buffer Overflow	Windows	send9
2008-08-13		-		Cisco IOS - Connectback (Port 21) Shellcode	Hardware	Gyan Chawdhary
2008-08-13		-		Cisco IOS - Bind Shellcode Password Protected (116 bytes)	Hardware	Gyan Chawdhary
2008-08-13		-		Cisco IOS - Tiny Shellcode (New TTY, Privilege level to 15, No password)	Hardware	Gyan Chawdhary
2008-07-29		-		Cisco IOS 12.3(18) FTP Server - Remote Exploit (attached to gdb)	Hardware	Andy Davis
2007-10-10		-		Cisco IOS 12.3 - LPD Remote Buffer Overflow	Hardware	Andy Davis
2007-08-17		-		Cisco IOS 12.3 - Show IP BGP Regexp Remote Denial of Service	Hardware	anonymous
2007-08-09		-		Cisco IOS Next Hop Resolution Protocol (NHRP) - Denial of Service	Windows	Martin Kluge
2007-06-27		-		Cisco IOS Exploitation Techniques	Papers	Gyan Chawdhary
2005-09-07		-		Cisco IOS 12.x - Firewall Authentication Proxy Buffer Overflow	Hardware	Markus
2005-08-01		-		Cisco IOS - Shellcode And Exploitation Techniques (BlackHat)	Papers	Michael Lynn
2004-02-03		-		Cisco IOS 12 MSFC2 - Malformed Layer 2 Frame Denial of Service	Hardware	blackangels
2003-08-10		-		Cisco IOS 12.x/11.x - HTTP Remote Integer Overflow	Hardware	FX
2003-08-01		-		Cisco IOS 10/11/12 - UDP Echo Service Memory Disclosure	Hardware	FX
2003-07-22		-		Cisco IOS - (using hping) Remote Denial of Service	Hardware	zerash
2003-07-21		-		Cisco IOS - 'cisco-bug-44020.c' IPv4 Packet Denial of Service	Hardware	Martin Kluge

https://www.exploit-db.com/

Activity

Note that CVE Details and the Exploit Database show a different number of exploits for the Cisco IOS.

Which one has the most?

http://www.cvedetails.com/vendor/16/Cisco.html

https://www.exploit-db.com/

Put your counts and answer in the chat window

Routers

Unfortunately routers can be hacked like everything else

- Vulnerabilities in router operating systems.
- Vulnerabilities in the software that configures or manages routers.
- They can be misconfigured by mistake.
- Tricking them into adding fraudulent routes into their routing tables.

https://www.flickr.com/photos/13426843@N08/4291372540

https://www.flickr.com/photos/38109472@N00/4237980827

China highjacks 15% of Internet traffic

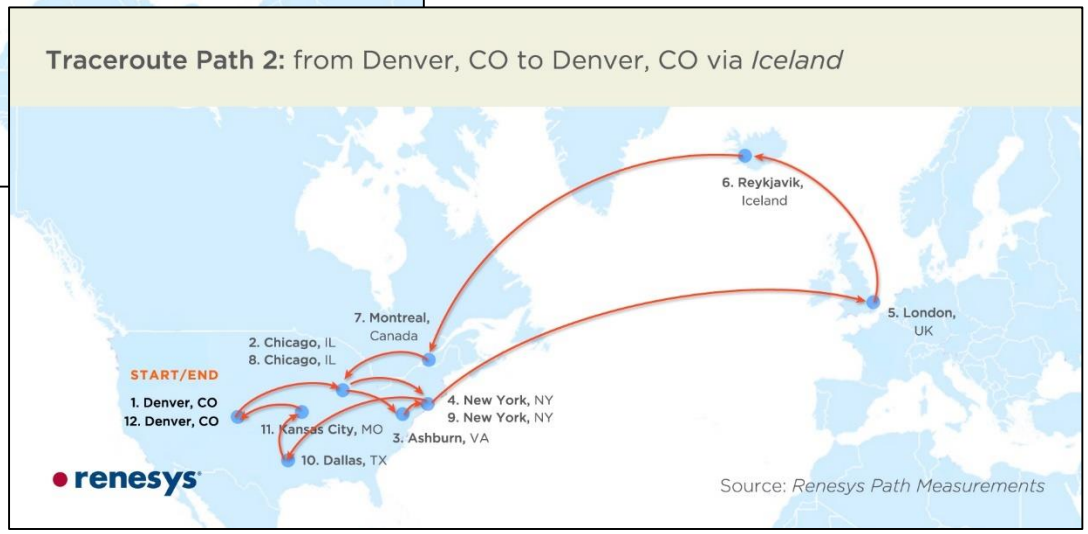
> For about 18 minutes on April 8, 2010, China Telecom advertised erroneous network traffic routes that instructed US and other foreign Internet traffic to travel through Chinese servers. Other servers around the world quickly adopted these paths, routing all traffic to about 15 percent of the Internet's destinations through servers located in China. This incident affected traffic to and from US government (".gov") and military (".mil") sites, including those for the Senate, the army, the navy, the marine corps, the air force, the office of secretary of Defense, the National Aeronautics and Space Administration, the Department of Commerce, the National Oceanic and Atmospheric Administration, and many others. Certain commercial websites were also affected, such as those for Dell, Yahoo!, Microsoft, and IBM.

- Huge man-in-the-middle attack
- BGP can be hijacked by one ISP router advertising fraudulent routes to other routers.
- Traffic is re-routed presumably for eavesdropping purposes

http://arstechnica.com/security/2010/11/how-china-swallowed-15-of-net-traffic-for-18-minutes/

BGP (Border Gateway Protocol) Attack

Rerouting Internet traffic by attacking BGP

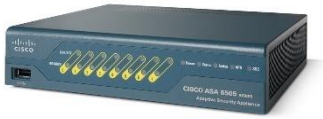


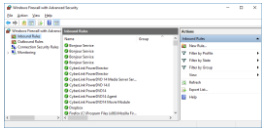
A malicious router advertises fraudulent routes which are then picked up and spread by other routers

https://arstechnica.com/information-technology/2013/11/repeated-attacks-hijack-huge-chunks-of-internet-traffic-researchers-warn/

Firewalls

Firewalls





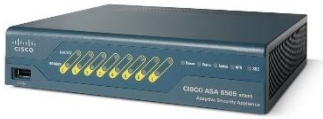
netfilter
firewalling, NAT, and packet mangling for linux

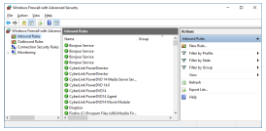
pfSense

SOPHOS

- Controls incoming and outgoing traffic from a network.
- Hardware (e.g. Cisco, Palo Alto Networks) are fast and independent of other operating systems on the network.
- Software firewalls (e.g. netfilter, Windows firewall) are slower and depend on the OS where they are running).

Firewalls





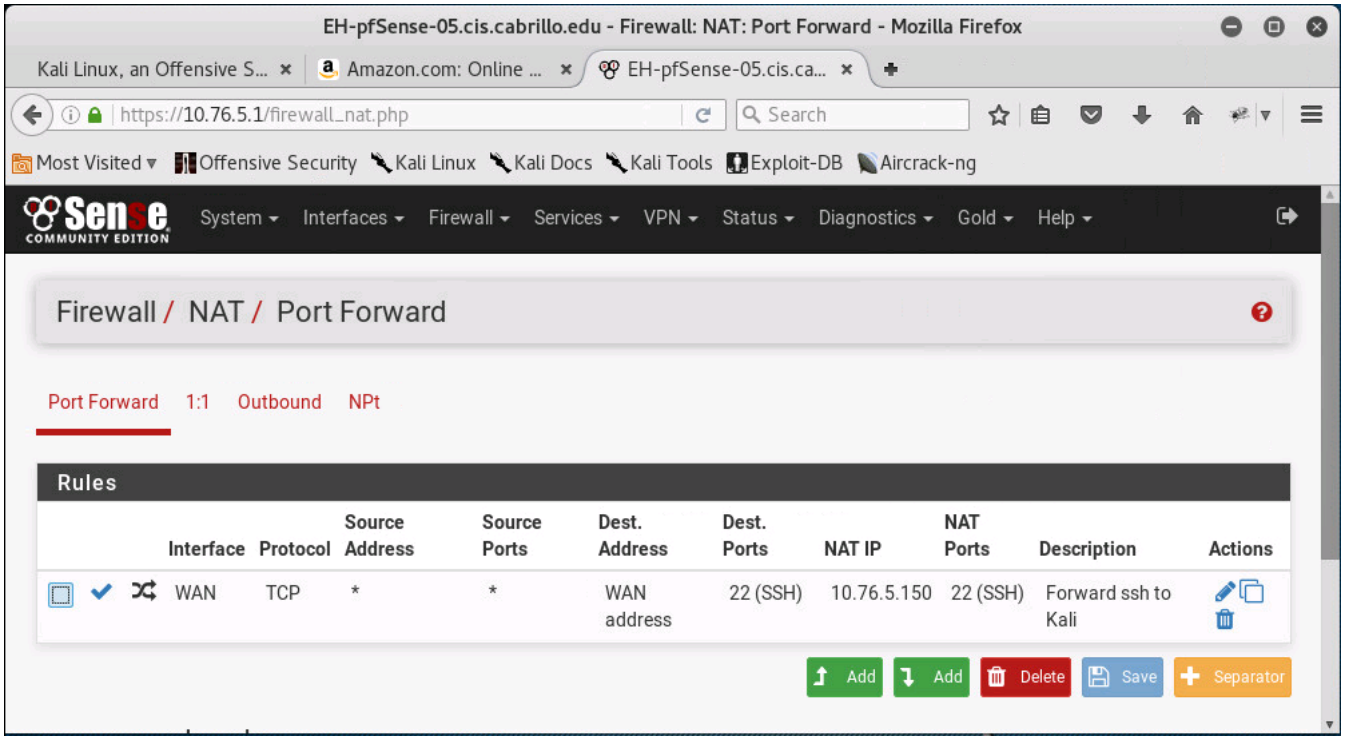
netfilter
firewalling, NAT, and packet mangling for linux

pfSense

SOPHOS

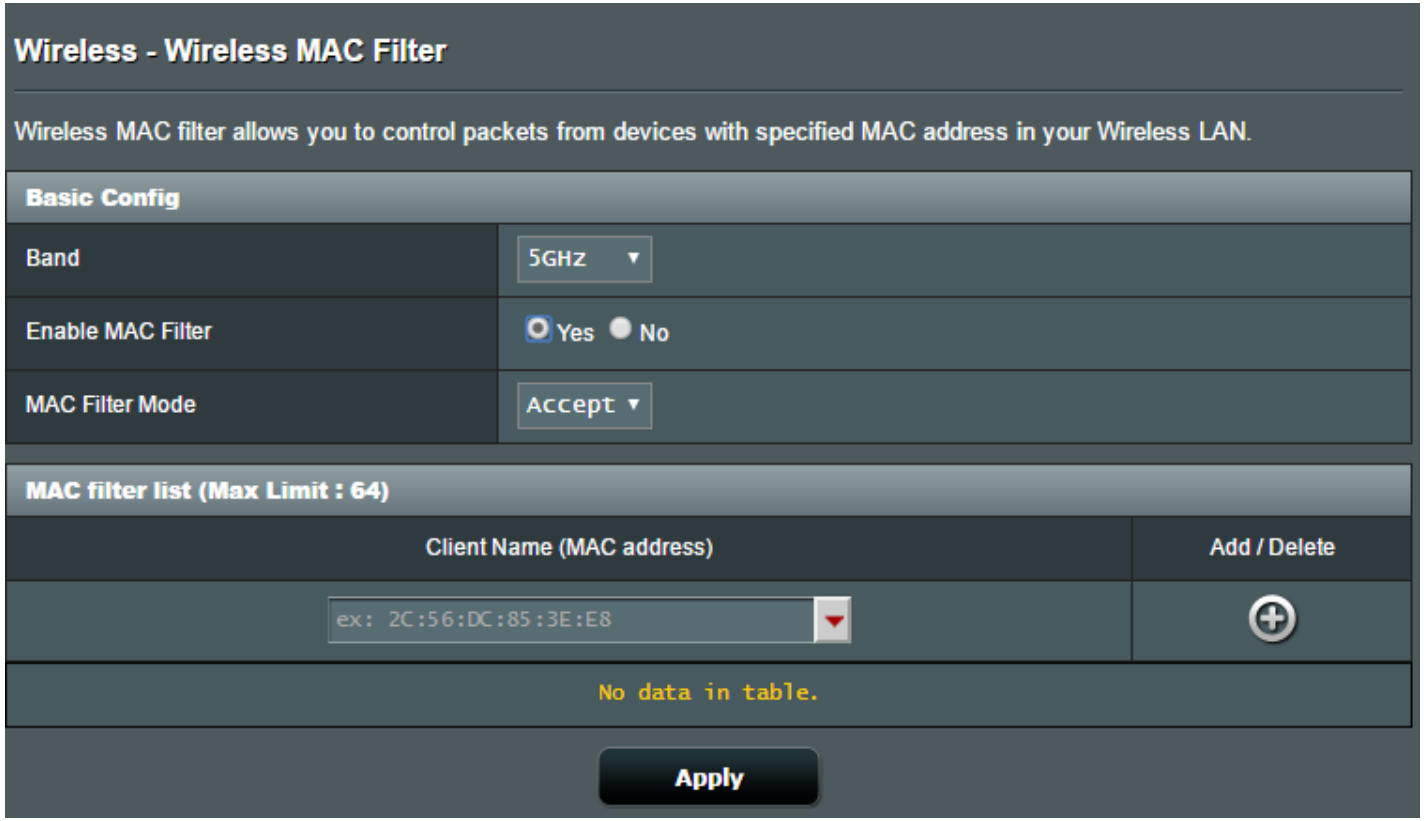
- Network Address Translation
- MAC address filtering
- IP and Port filtering
- Stateful packet inspection
- Application layer inspection

Network Address Translation



Configuring NAT to forward port 22 on the pfSense firewall

Wireless MAC filter



Wireless MAC filter on Asus router

IP Address and Port Filtering

Anatomy Of An Access List

List No.	Rule	Pattern Definition						
access-list xxx (100-199)	permit or deny	IP or ICMP TCP or UDP	Source IP address xxx.xxx.xxx.xxx	Source IP address mask xxx.xxx.xxx.xxx 255=ignore 0=apply	Destination IP address xxx.xxx.xxx.xxx	Destination IP address mask xxx.xxx.xxx.xxx 255=ignore 0=apply	eq=equal gt=greater than lt=less than neq=not equal	TCP or UDP destination port no.
1	2	3	4	5	6	7	8	9

1) Every extended access list has a number from 100 to 199, which identifies the list in two places. When building the list, every line must be labeled with the same access list number. When you apply the list to an interface on the router, you must reference it by the same number. Version 11.2 of the IOS allows you to use a name for the list instead of a number.

2) A permit or deny rule has to be applied to every line or statement on the list.

3) If you are only filtering on IP address, you will specify IP (or ICMP for pings and trace routes) as the protocol. This means that only the IP address is considered for a match. If you are also filtering on UDP or TCP port, you must specify TCP or UDP.

4) Every line in the list must have a source address.

Required Optional

5) Every IP source address in the list must have a mask. The mask lets you determine how much of the preceding IP address to apply to the filter. In most cases, you will simply want to put a 255 corresponding to every octet in the IP address that you want to ignore, and 0 for every octet that you want the packet match to apply to.

6) Every line in the list must have a destination address.

7) Every IP destination address in the list must have a mask. See 5 above.

8) This applies to the TCP or UDP port that you are filtering on. In most cases, you will use the eq, which means equals. This gives you the ability to permit or deny TCP or UDP ports equal to the port specified. There are cases, however, where you will want to apply a range of port numbers, which is where the gt, greater than, or lt, less than, will come in handy.

9) If you have defined the pattern as a TCP or UDP packet, you will have to have an associated port number.

https://www.scribd.com/document/269048661/Anatomy-of-an-Access-List

```
ip access-list extended FIREWALL-IN-20160604
 permit tcp any host 207.62.187.231 eq 22
 permit tcp any host 207.62.187.231 eq www
 permit tcp any host 207.62.187.231 eq 443
```

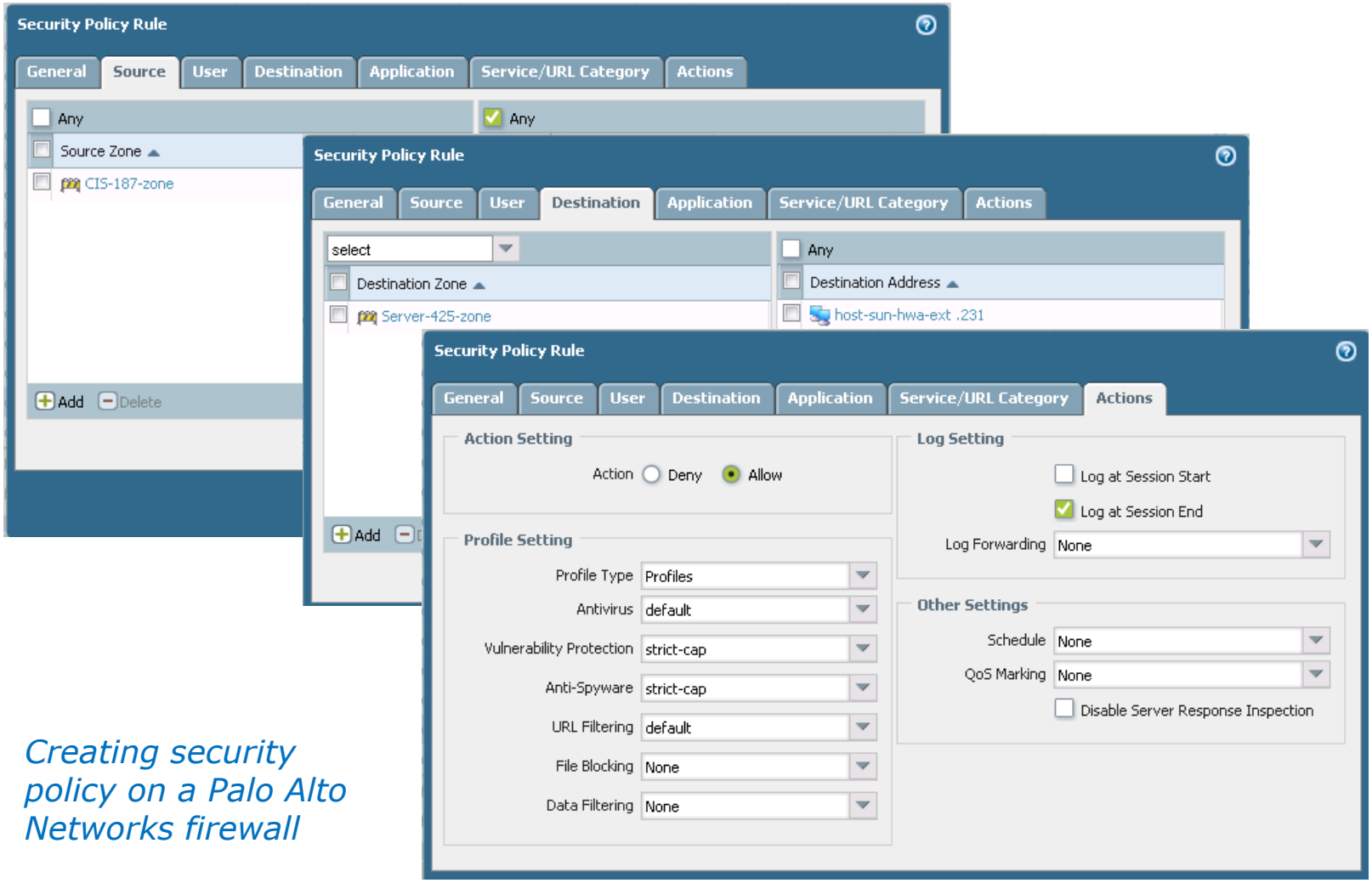
Access List on a Cisco Router

Stateful packet inspection

```
[root@p24-elrond ~]# cat /etc/sysconfig/iptables
# Generated by iptables-save v1.4.7 on Sun Mar 17 13:38:54 2013
*nat
:PREROUTING ACCEPT [274:29705]
:POSTROUTING ACCEPT [17:1421]
:OUTPUT ACCEPT [15:1301]
-A PREROUTING -d 172.20.192.171/32 -i eth0 -j DNAT --to-destination 192.168.24.9
-A POSTROUTING -s 192.168.24.9/32 -o eth0 -j SNAT --to-source 172.20.192.171
-A POSTROUTING -s 192.168.24.0/24 -o eth0 -j SNAT --to-source 172.20.192.170
COMMIT
# Completed on Sun Mar 17 13:38:54 2013
# Generated by iptables-save v1.4.7 on Sun Mar 17 13:38:54 2013
*filter
:INPUT DROP [10:985]
:FORWARD DROP [9:756]
:OUTPUT DROP [0:0]
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -s 192.168.24.0/24 -d 192.168.24.1/32 -i eth1 -m state --state NEW -j ACCEPT
-A INPUT -j LOG --log-prefix "iptables INPUT:" --log-level 6
-A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -s 192.168.24.0/24 -m state --state NEW -j ACCEPT
-A FORWARD -d 192.168.24.9/32 -p tcp -m state --state NEW -m tcp --dport 23 -j ACCEPT
-A FORWARD -j LOG --log-prefix "iptables FORWARD:" --log-level 6
-A OUTPUT -m state --state NEW,RELATED,ESTABLISHED -j ACCEPT
COMMIT
# Completed on Sun Mar 17 13:38:54 2013
[root@p24-elrond ~]#
```


Netfilter (iptables) firewall on Linux server can use TCP connection states

Application layer inspection



Creating security policy on a Palo Alto Networks firewall

23	allow-some-to-sun-hwa	none	universal	CIS-187-zone	any	any	any	Server-425-zone	host-sun-hwa-ext .231	any	any

Application layer inspection

	Name	Location	Count	Rule Name	Threat Name	Host Type	Severity	Action	Packet Capture
☐	strict-cap		Rules: 10	simple-client-critical	any	client	critical	block	single-packet
				simple-client-high	any	client	high	block	single-packet
				simple-client-medium	any	client	medium	block	disable
				simple-client-informational	any	client	informational	default	disable
				simple-client-low	any	client	low	default	disable
				simple-server-critical	any	server	critical	block	single-packet
				simple-server-high	any	server	high	block	single-packet
				more...					

Application layer inspection

(addr.dst in 207.62.187.231)

Receive Time	Type	Name	From Zone	Attacker	Victim	To Port	Application	Action	Severity	Rule
12/04 13:42:28	vulnerability	Unknown HTTP Request Method Found	CIS-187-zone	50.247.81.99	207.62.187.231	80	web-browsing	alert	informational	allow-some-to-sun-hwa
12/04 13:42:25	vulnerability	HTTP OPTIONS Method	CIS-187-zone	50.247.81.99	207.62.187.231	80	web-browsing	alert	informational	allow-some-to-sun-hwa
12/04 13:17:05	vulnerability	Unknown HTTP Request Method Found	CIS-187-zone	50.247.81.99	207.62.187.231	80	web-browsing	alert	informational	allow-some-to-sun-hwa
12/04 13:17:04	vulnerability	HTTP OPTIONS Method	CIS-187-zone	50.247.81.99	207.62.187.231	80	web-browsing	alert	informational	allow-some-to-sun-hwa
12/03 19:07:49	vulnerability	SSH User Authentication Brute Force Attempt	CIS-187-zone	221.194.47.208	207.62.187.231	22	ssh	reset-both	high	allow-some-to-sun-hwa
12/03 19:07:48	vulnerability	SSH User Authentication Brute Force Attempt	CIS-187-zone	221.194.47.208	207.62.187.231	22	ssh	reset-both	high	allow-some-to-sun-hwa
12/03 19:07:48	vulnerability	SSH User Authentication Brute Force Attempt	CIS-187-zone	221.194.47.208	207.62.187.231	22	ssh	reset-both	high	allow-some-to-sun-hwa
12/03 19:07:47	vulnerability	SSH User Authentication Brute Force Attempt	CIS-187-zone	221.194.47.208	207.62.187.231	22	ssh	reset-both	high	allow-some-to-sun-hwa
12/03 14:10:45	vulnerability	Unknown HTTP Request Method Found	CIS-187-zone	71.80.249.170	207.62.187.231	80	web-browsing	alert	informational	allow-some-to-sun-hwa
12/03 14:10:45	vulnerability	HTTP OPTIONS Method	CIS-187-zone	71.80.249.170	207.62.187.231	80	web-browsing	alert	informational	allow-some-to-sun-hwa
12/03 14:10:32	vulnerability	HTTP OPTIONS Method	CIS-187-zone	71.80.249.170	207.62.187.231	80	web-browsing	alert	informational	allow-some-to-sun-hwa
12/03 12:16:40	vulnerability	Unknown HTTP Request Method Found	CIS-187-zone	198.8.80.82	207.62.187.231	80	web-browsing	alert	informational	allow-some-to-sun-hwa
12/03 12:16:38	vulnerability	HTTP OPTIONS Method	CIS-187-zone	198.8.80.82	207.62.187.231	80	web-browsing	alert	informational	allow-some-to-sun-hwa
12/03 11:49:31	vulnerability	Unknown HTTP Request Method Found	CIS-187-zone	198.8.80.82	207.62.187.231	80	web-browsing	alert	informational	allow-some-to-sun-hwa
12/03 11:49:31	vulnerability	HTTP OPTIONS Method	CIS-187-zone	198.8.80.82	207.62.187.231	80	web-browsing	alert	informational	allow-some-to-sun-hwa
12/03 08:13:31	vulnerability	OpenSSH AES-GCM Auth Remote Code Execution Vulnerability	CIS-187-zone	162.243.196.164	207.62.187.231	22	ssh	alert	low	allow-some-to-sun-hwa
12/03 08:13:31	vulnerability	OpenSSH AES-GCM Auth Remote Code Execution	CIS-187-zone	162.243.196.164	207.62.187.231	22	ssh	alert	low	allow-some-to-sun-hwa

1 2 3 4 5 6 7 8 9 10 | Resolve hostname | Displaying logs 301 - 400 | 100 per page | DESC

The PAN firewall catches the brute force attack and resets the connection

Intrusion Detection and Prevention Systems

Intrusion Detection Systems (IDS)

- Software application or hardware device.
- Monitor traffic and alert administrators of potential attacks.
- Scan incoming packets for known exploit signatures, and any behavior or protocol anomalies.
- Host based (HIDS) include anti-virus, Tripwire and OSSEC.
- Network based (NIDS) include SNORT and Suricata.
- Passive IDS only monitors and reports.
- Active IDS will communicate with routers and firewalls to block specific attackers.

Intrusion Prevention Systems (IPS)

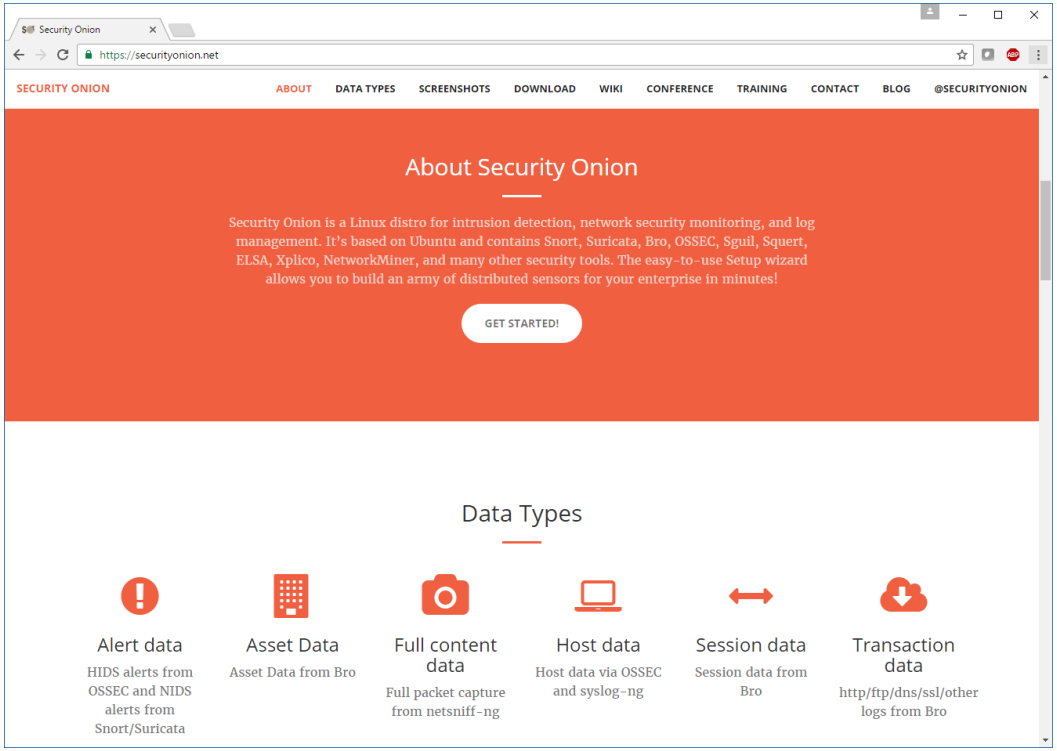
- Like an active IDS except is an inline device with all traffic flowing through it.
- An IPS can automatically stop attacks.
- Palo Alto Networks firewalls can be used as an IDS or an IPS.

IDS Evasion

- Payload obfuscation
  - Encoding and encryption
  - Polymorphism
- Insertion and evasion
  - Fragmentation and small packets
  - Overlapping fragments and TCP segments
  - Protocol ambiguities
  - Low bandwidth attacks
- Denial of service
  - CPU exhaustion
  - Memory exhaustion
  - Operator fatigue

https://en.wikipedia.org/wiki/Intrusion_detection_system_evasion_techniques

Using Security Onion and a PA-500



https://securityonion.net/

Security Onion is installed on a VM using SNORT and observes traffic via a tap port.

It bundles Squert, Sguil, SNORT, ELSA, Bro and more.

The Palo Alto Networks PA-500 is inline and all traffic goes through it

https://www.paloaltonetworks.com/

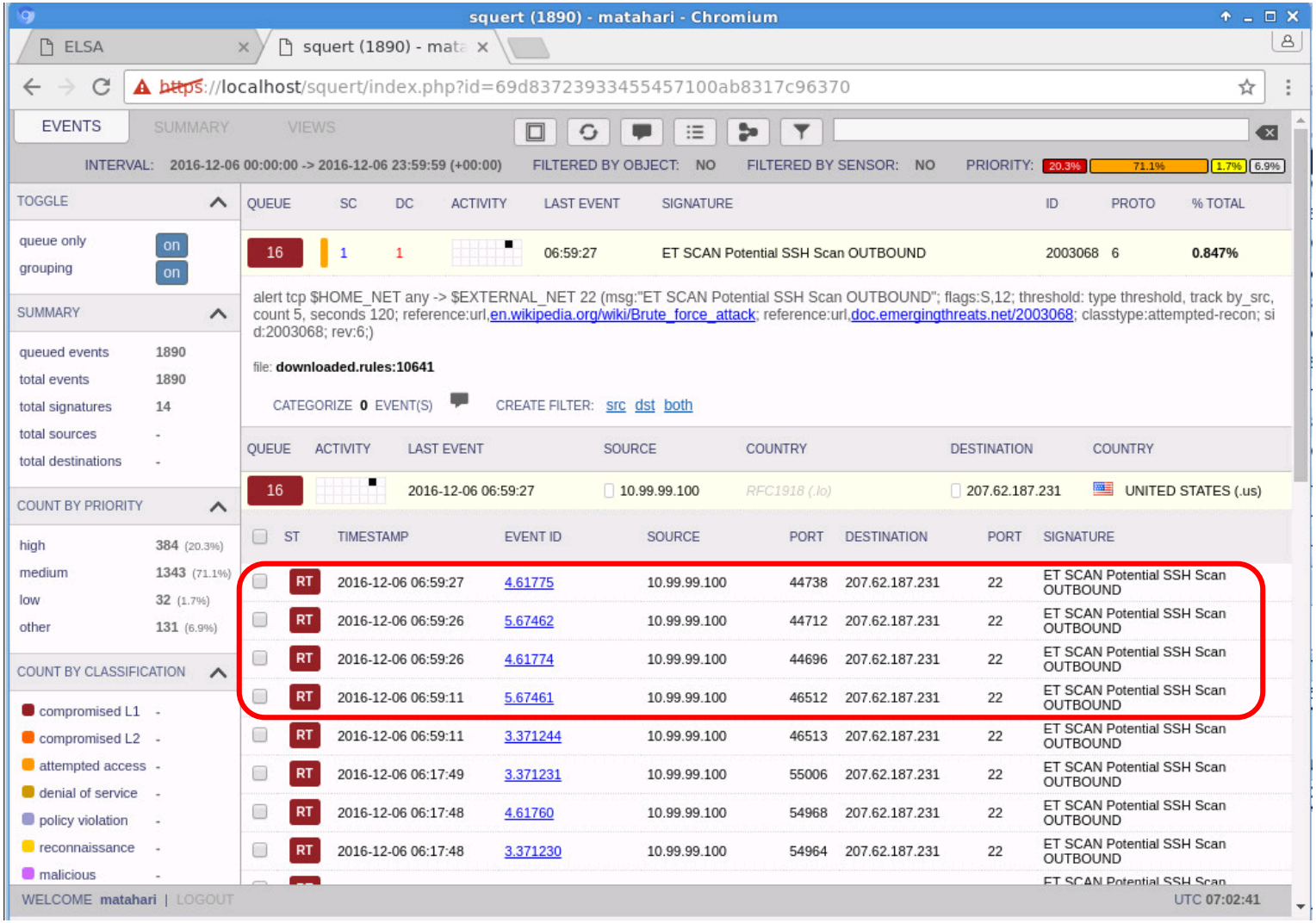
nmap "all" scan

nmap -p 22,80,443 -A 207.62.187.231,243

```
root@pen-kali:~# nmap -p 22,80,443 -A 207.62.187.231,243

Starting Nmap 7.12 ( https://nmap.org ) at 2016-12-05 22:58 PST
Nmap scan report for 207.62.187.231
Host is up (0.00079s latency).
PORT    STATE  SERVICE VERSION
22/tcp  open   ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol 2
.0)
| ssh-hostkey:
|   2048 a8:d2:3e:8f:fd:86:d9:95:ca:81:8f:c6:d7:49:84:f1 (RSA)
|_  256 aa:2d:f1:b6:df:d9:2a:21:02:6b:52:f2:3f:58:19:e2 (ECDSA)
80/tcp  open   http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
443/tcp closed https
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.11 - 4.1
Network Distance: 3 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 443/tcp)
HOP RTT     ADDRESS
1   0.38 ms 10.99.99.1
2   0.45 ms 207.62.187.226
3   0.55 ms 207.62.187.231

Nmap scan report for 207.62.187.243
Host is up (0.00079s latency).
PORT    STATE    SERVICE VERSION
22/tcp  filtered ssh
80/tcp  open     http    Apache httpd 2.0.52 ((Red Hat))
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.0.52 (Red Hat)
|_http-title: Cisco Academy OnLine Curriculum
443/tcp filtered https
```

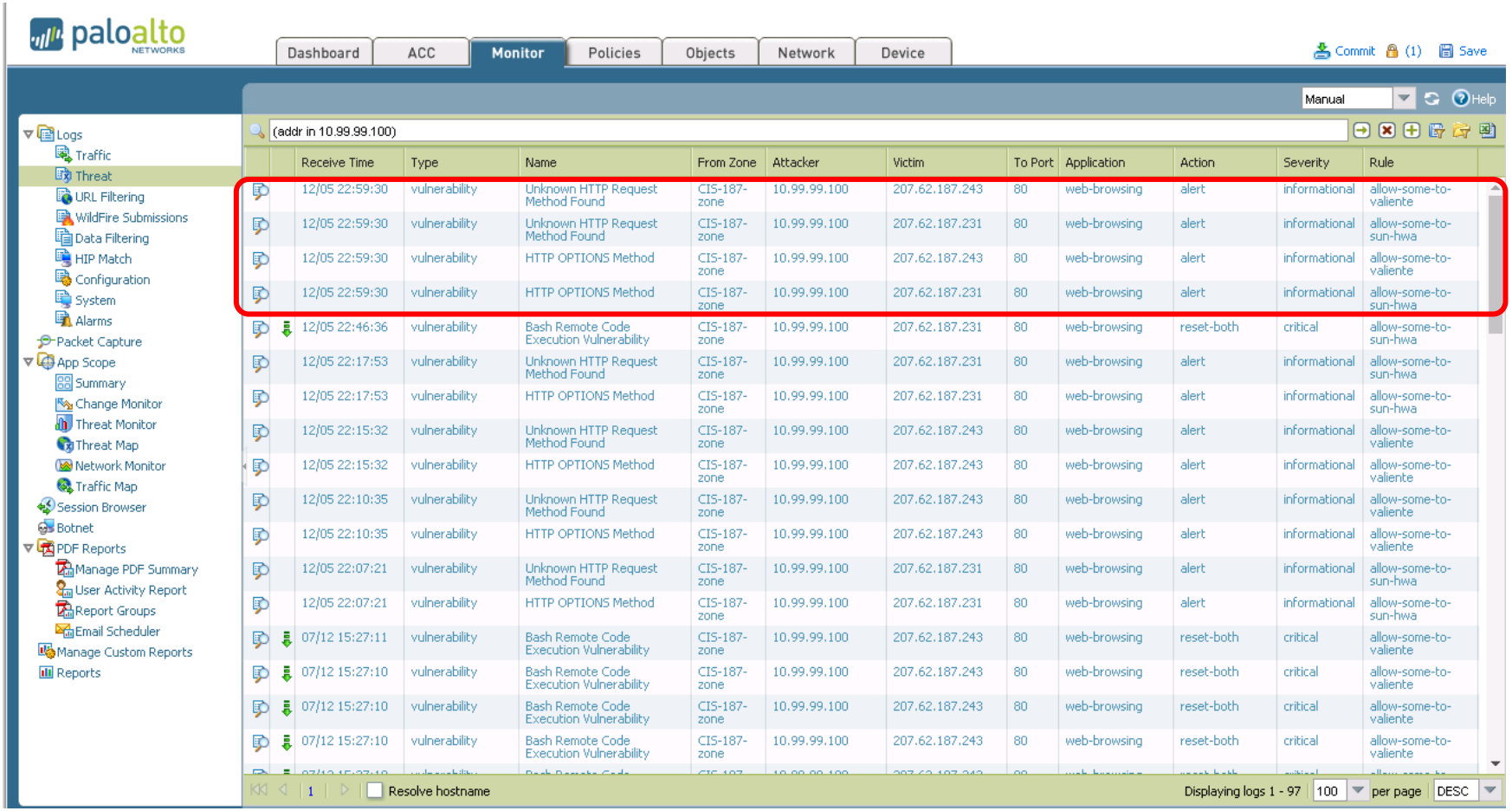
Caught in both Squert and PAN logs

Squert



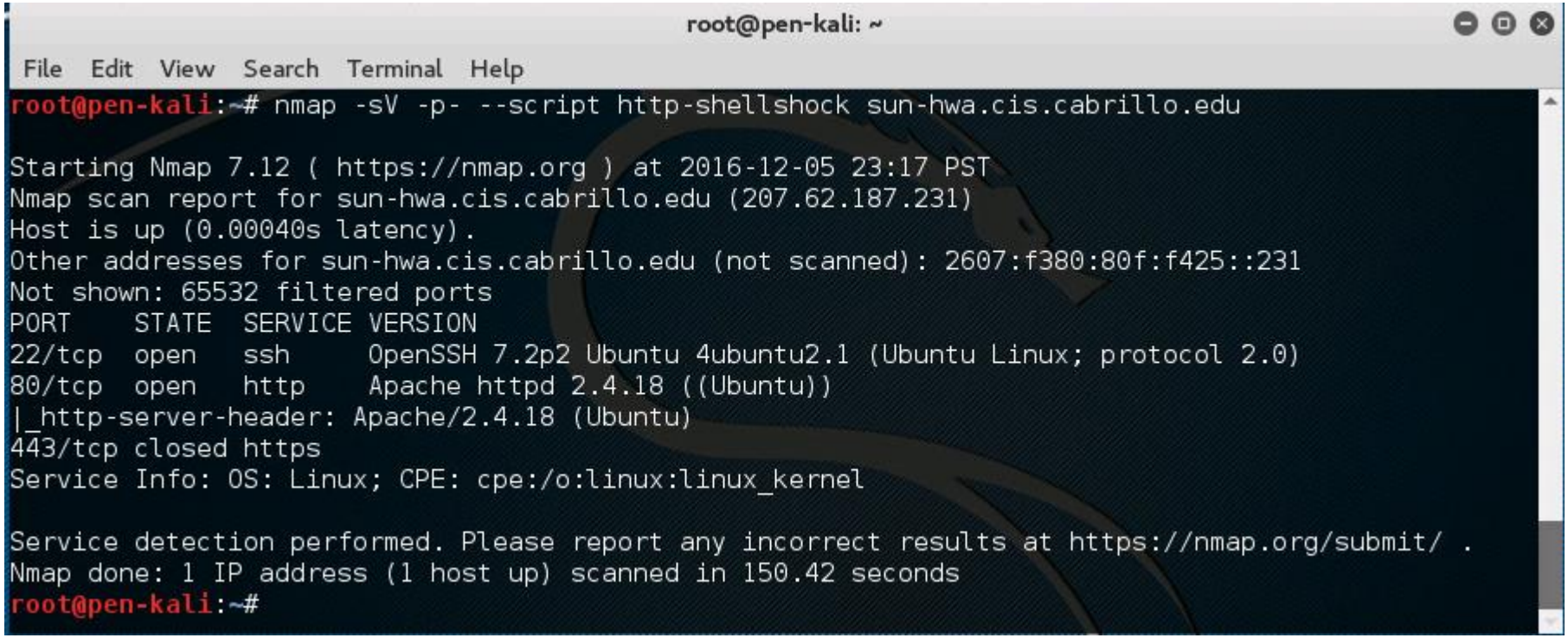
An SSH scan detected in Squert

PAN



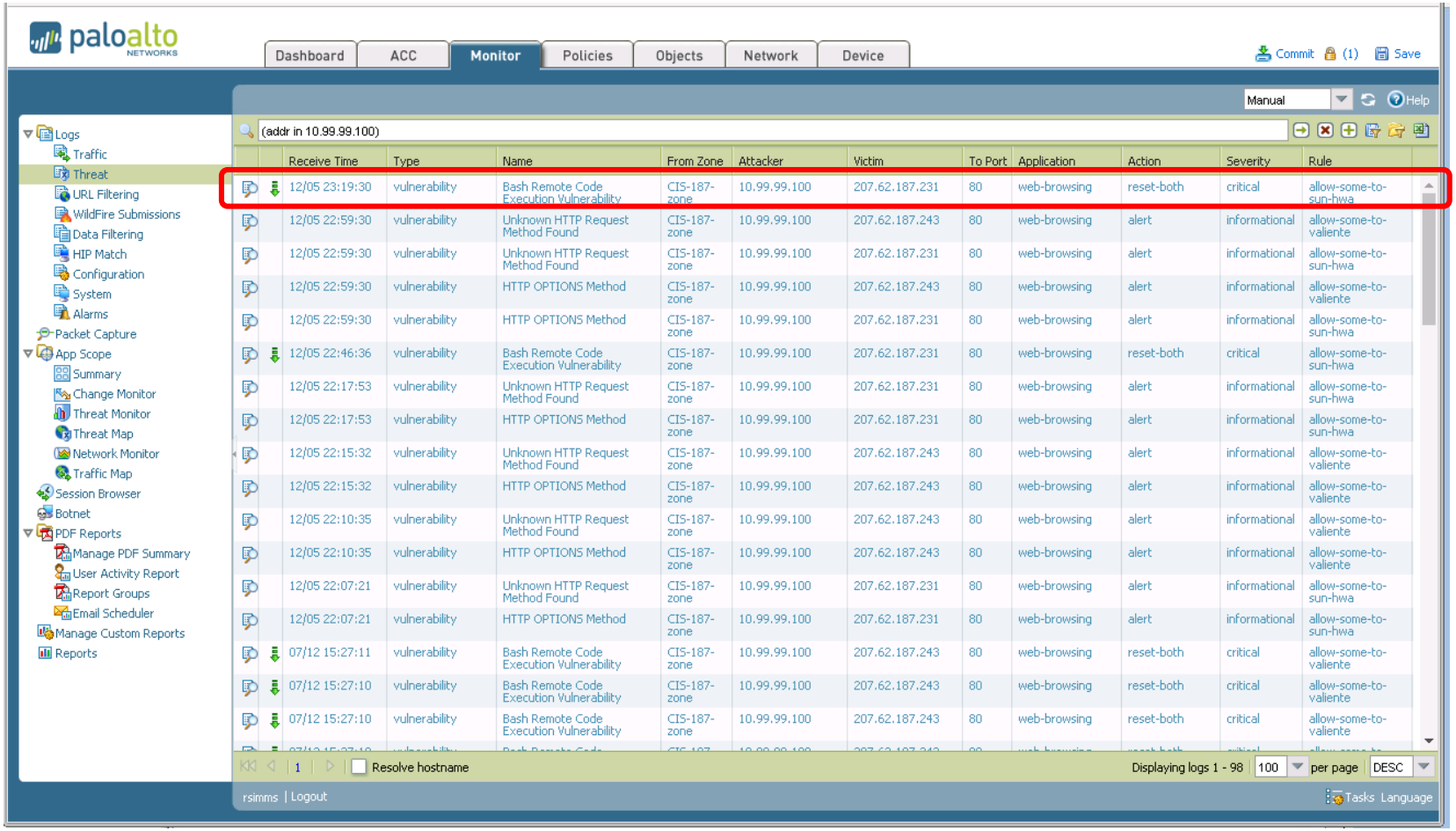
An HTTP scan detected by Palo Alto Networks

nmap "shellshock" scan



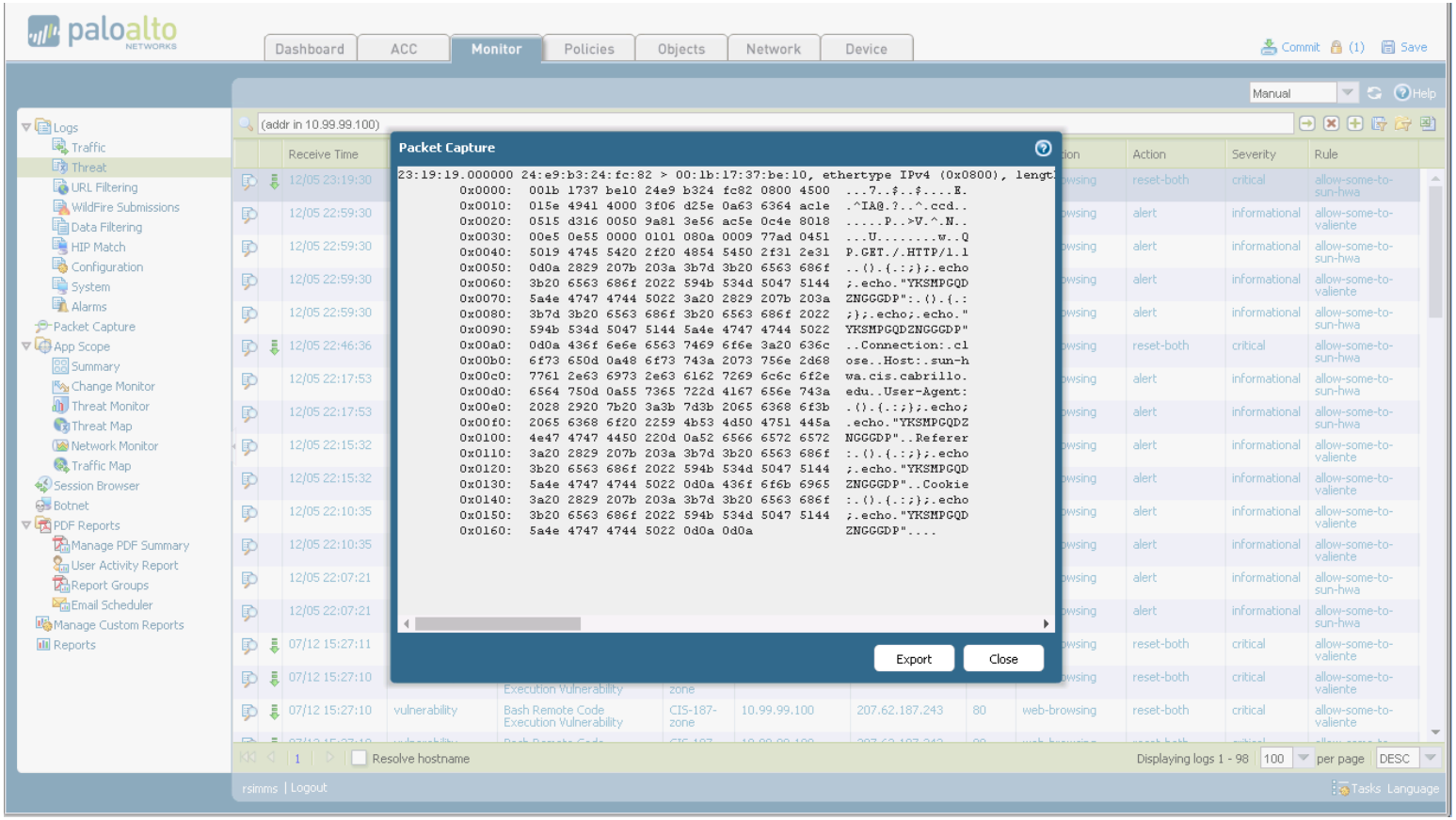
Squert doesn't log anything, but PAN logs it and resets the connection

PAN



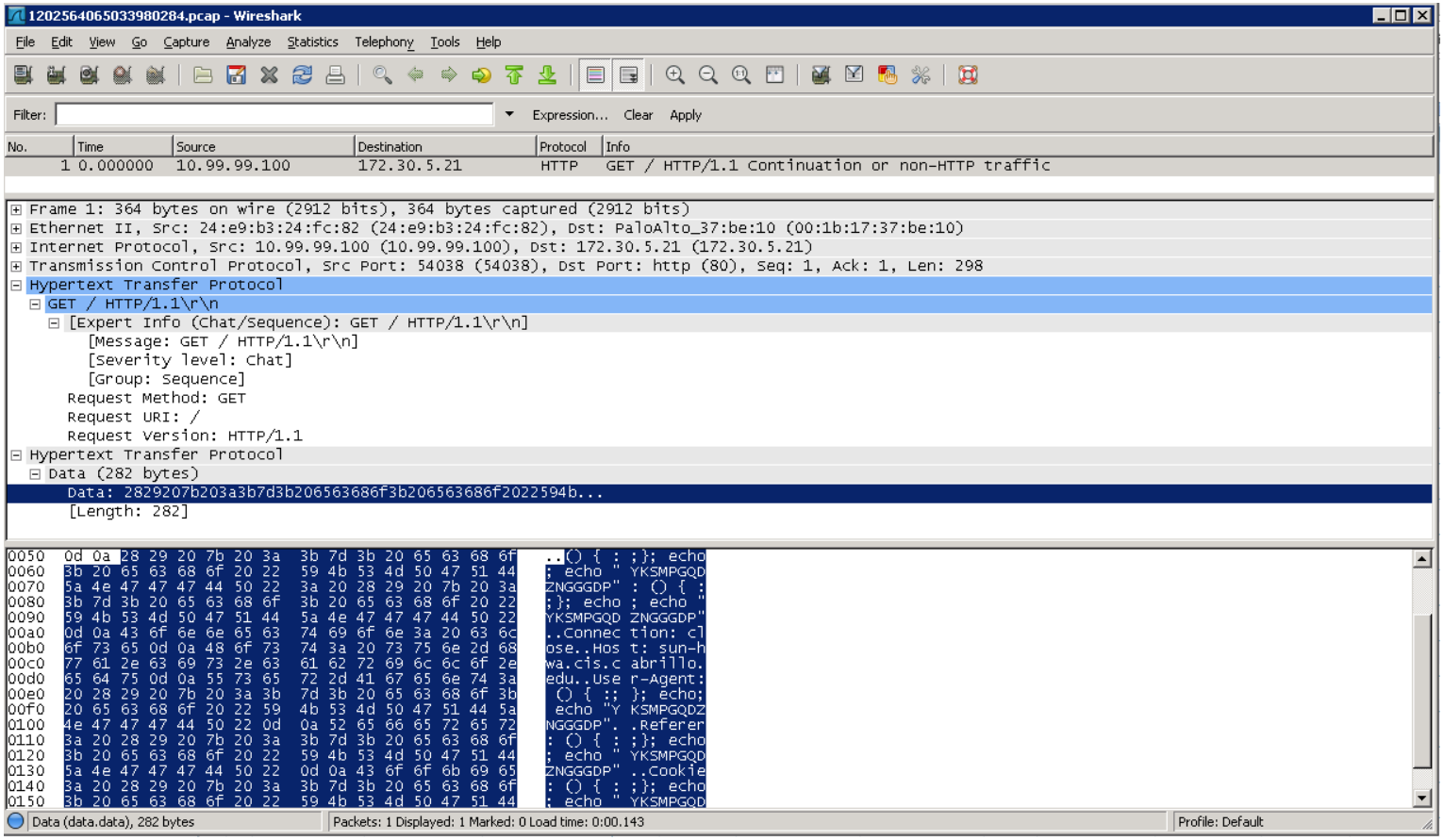
PAN logs it and resets the connection

PAN



One packet captured

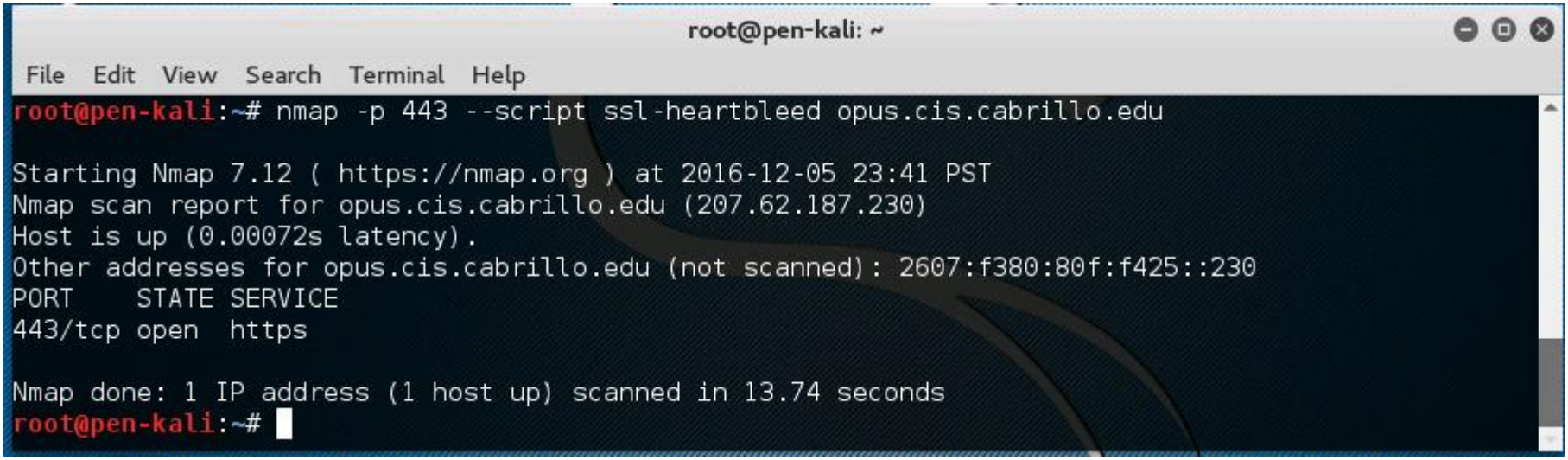
PAN



One packet captured and exported to Wireshark

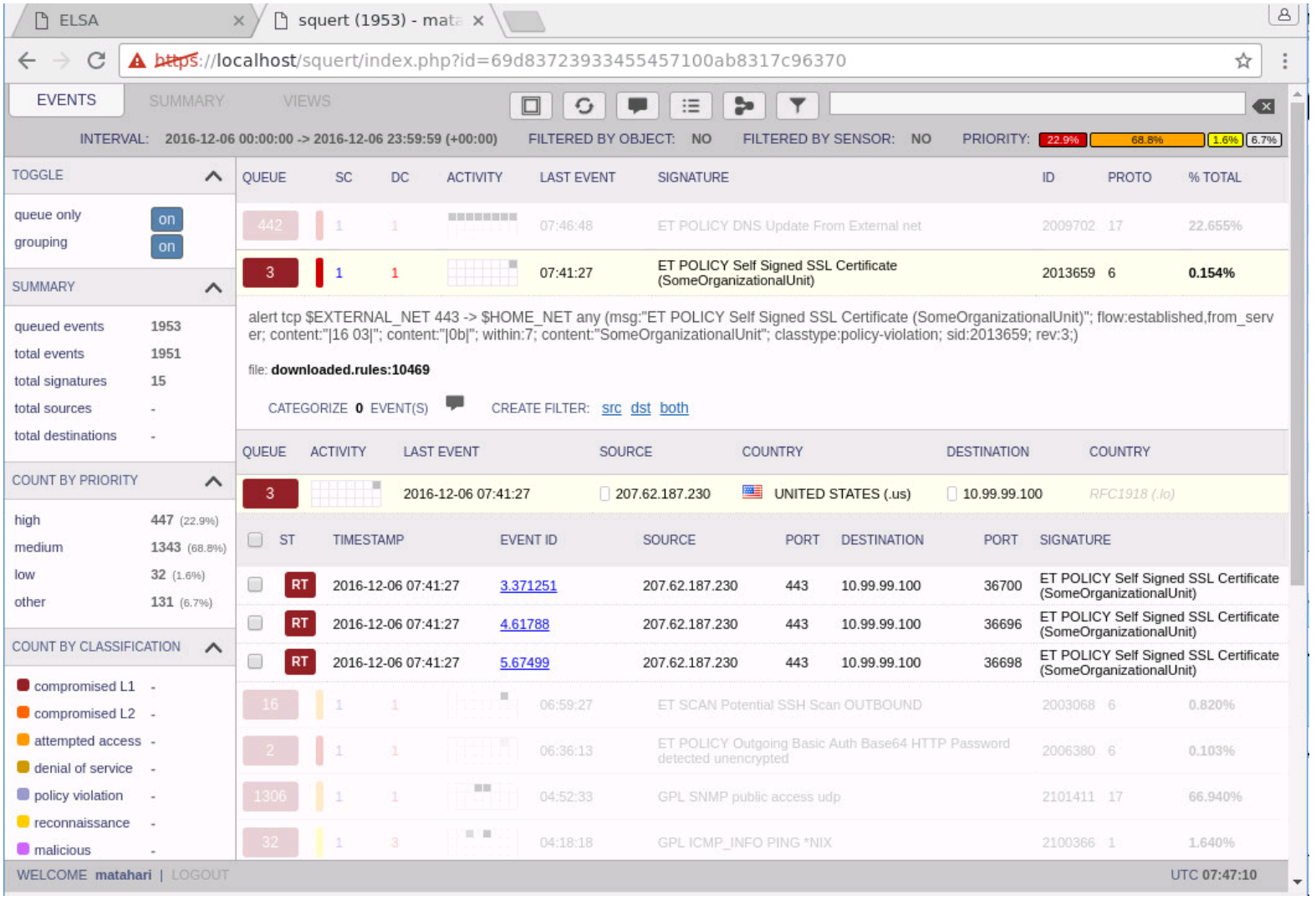
nmap "heartbleed" scan

nmap -p 443 --script ssl-heartbleed opus-ii.cis.cabrillo.edu



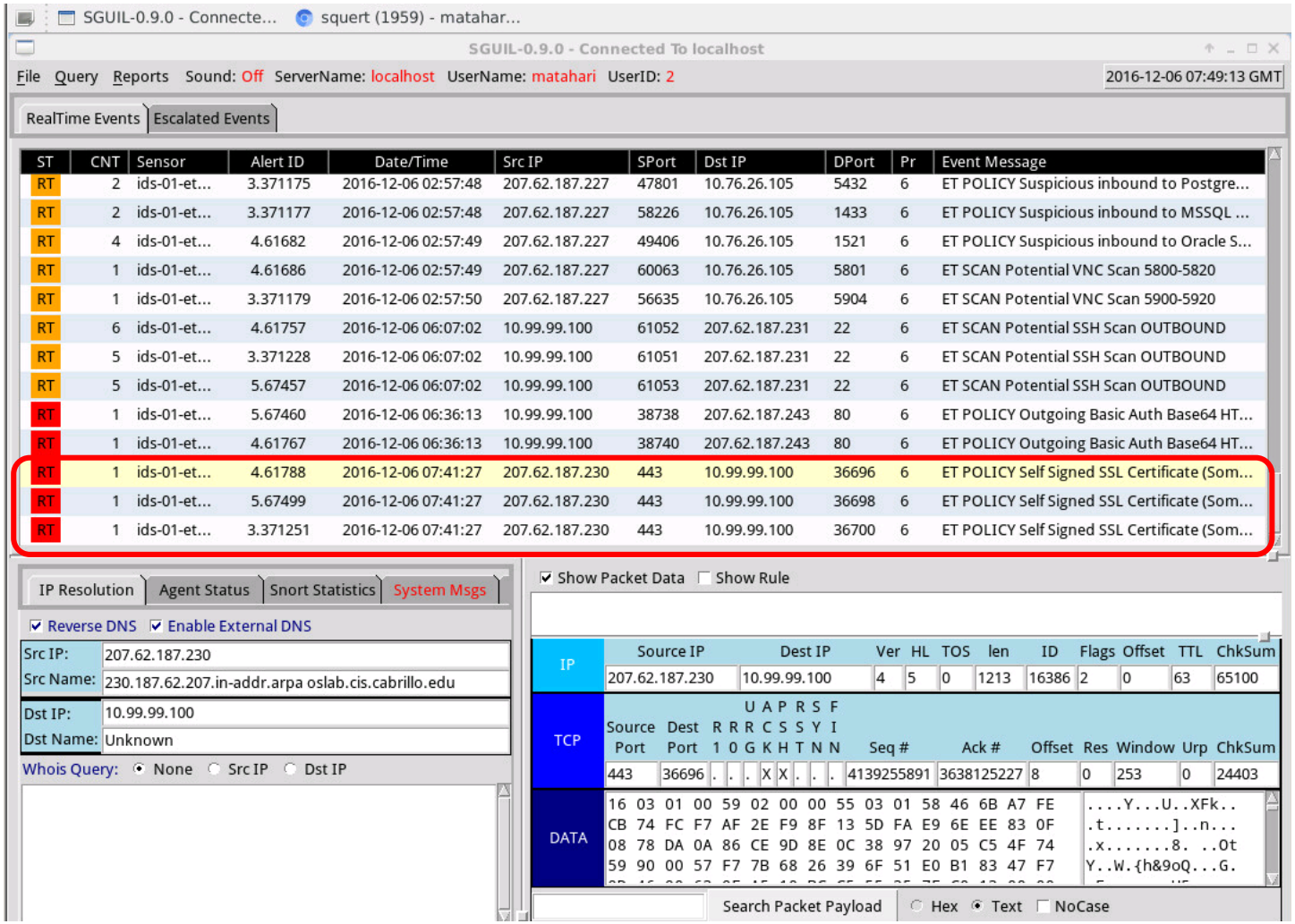
Squert, Sguil and PAN log it

Squert



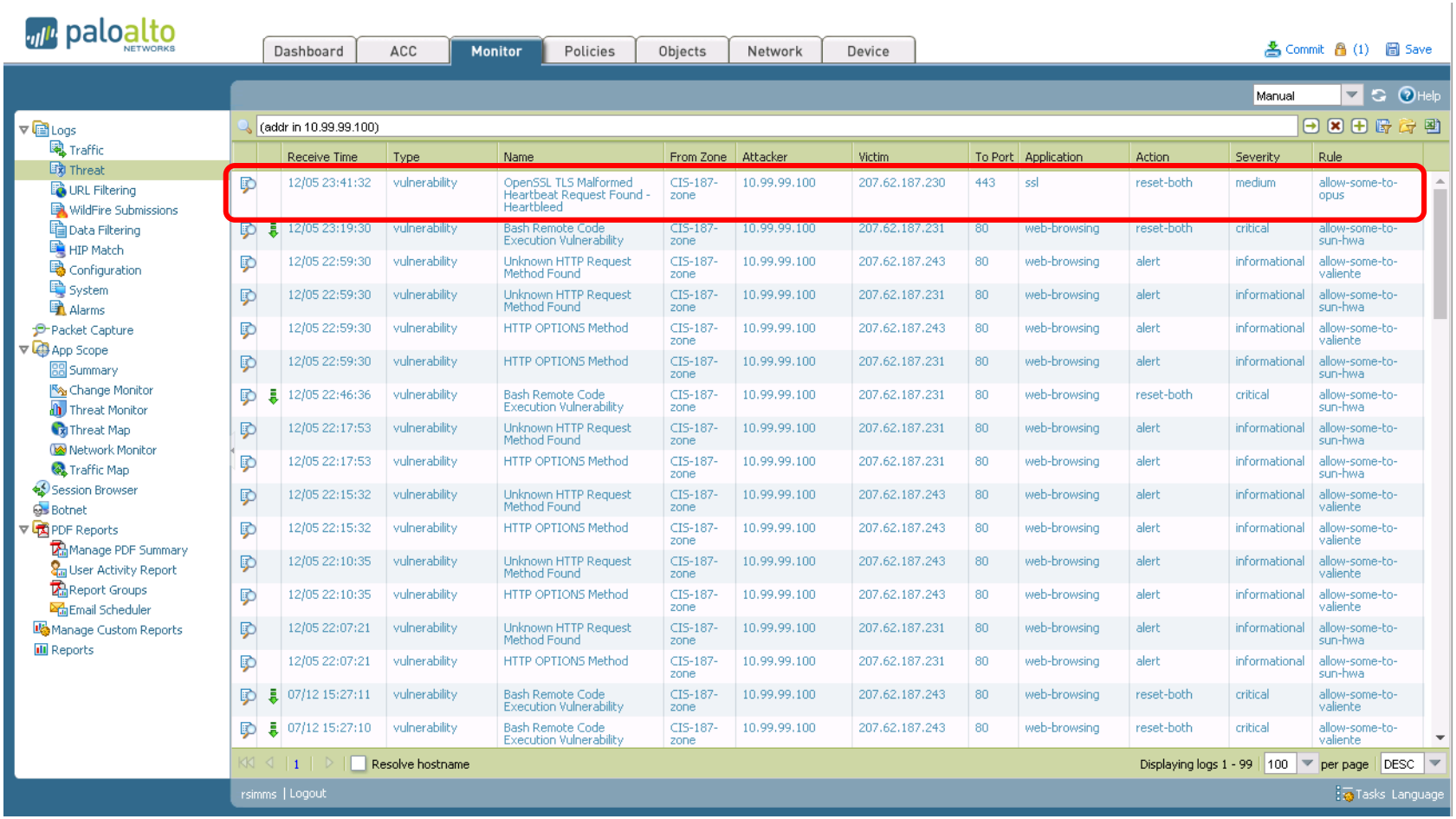
Squert logs the self-signed certificate sent to attacker

Sguil



Sguil logs the self-signed certificate sent to attacker

PAN



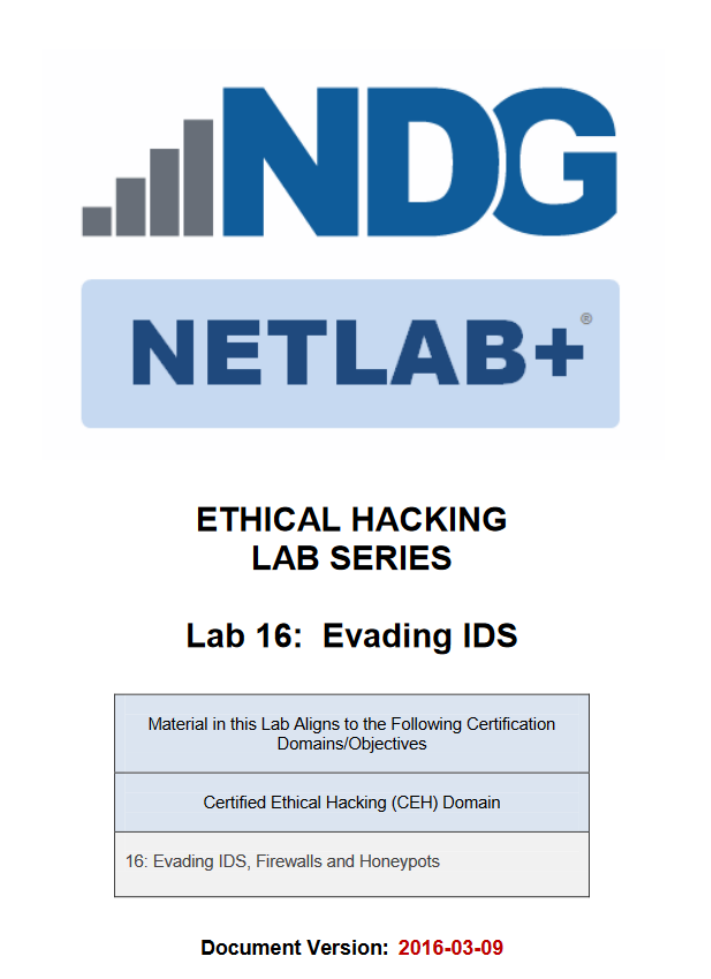
PAN logs it and resets the connection

Honeypots

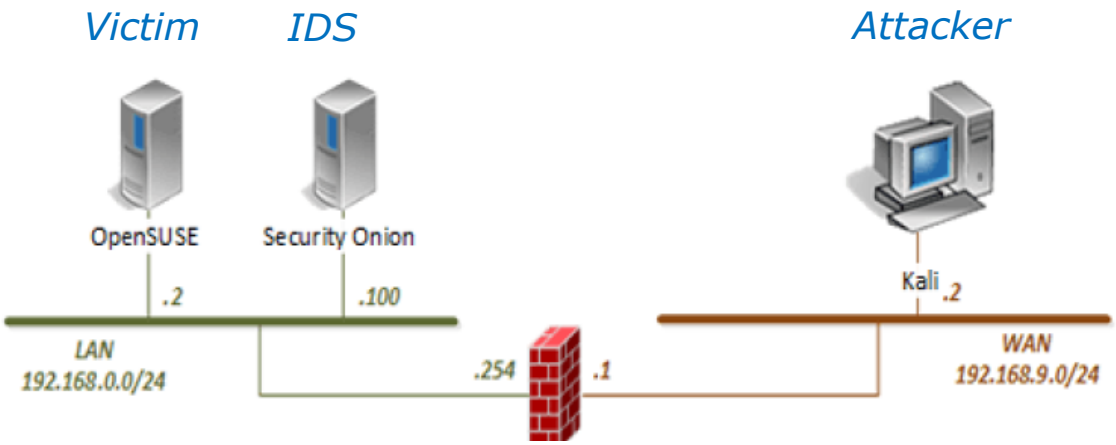
Honeypots

- Decoy servers to lure and trap hackers.
- Configured with vulnerabilities and fake but enticing data.
- Attempts to keep hackers engaged long enough that they can be traced back.
- Allows security professionals to observe how hackers operate and the tools they use.
- Commercial and open source honeypots are available.

Testing an IDS

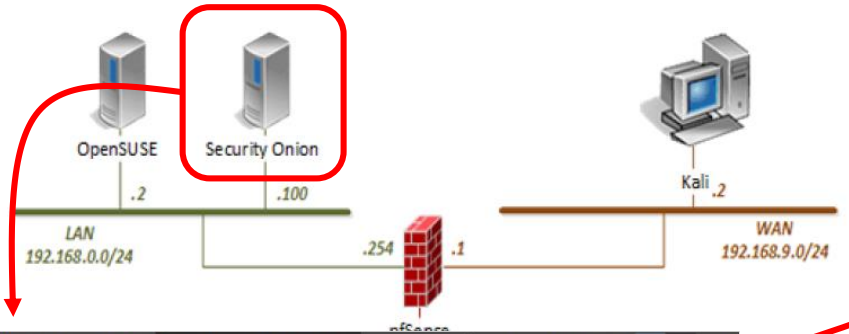


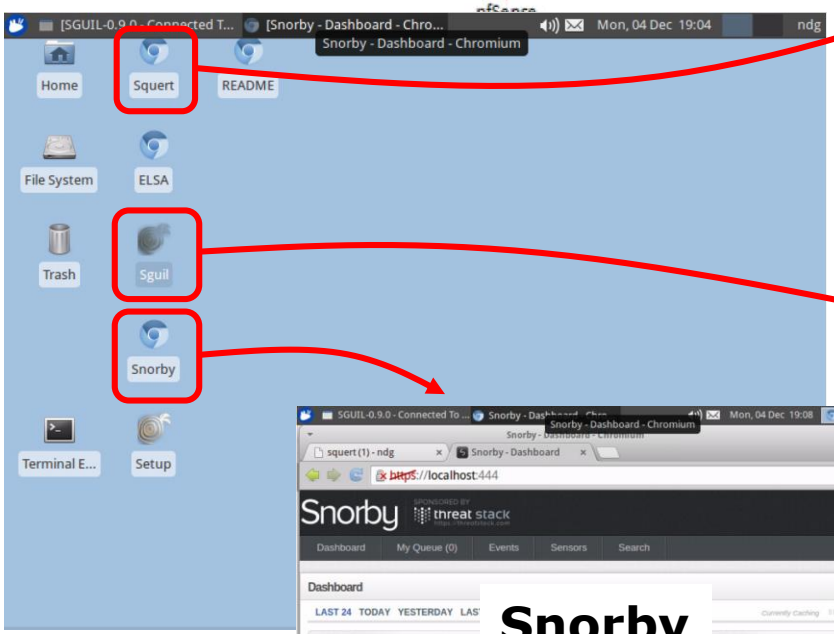
Log into Netlab PE or VE and select Lab 16

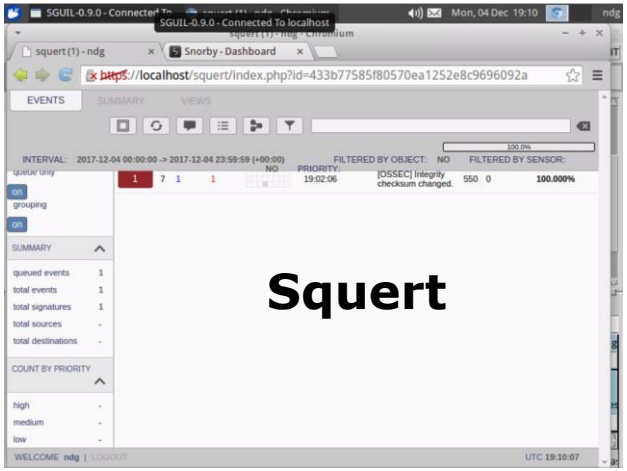


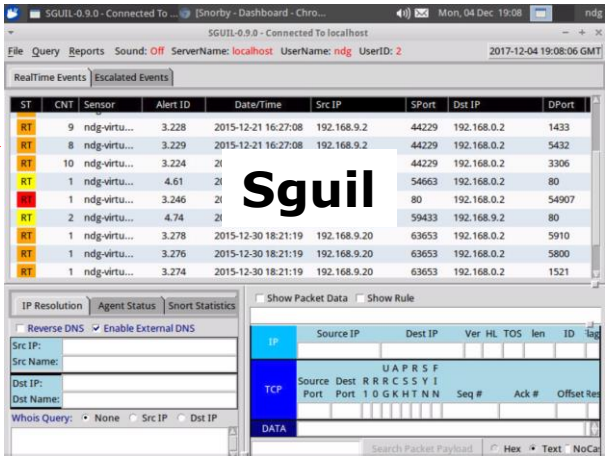
The IDS (Security Onion) is used to monitor the nmap scans Kali is doing on OpenSUSE

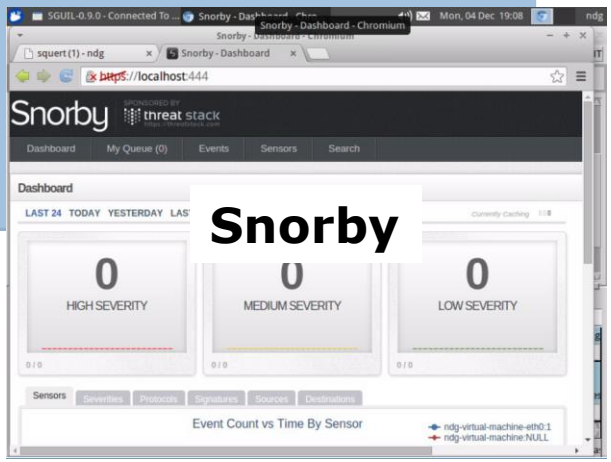
Security Onion





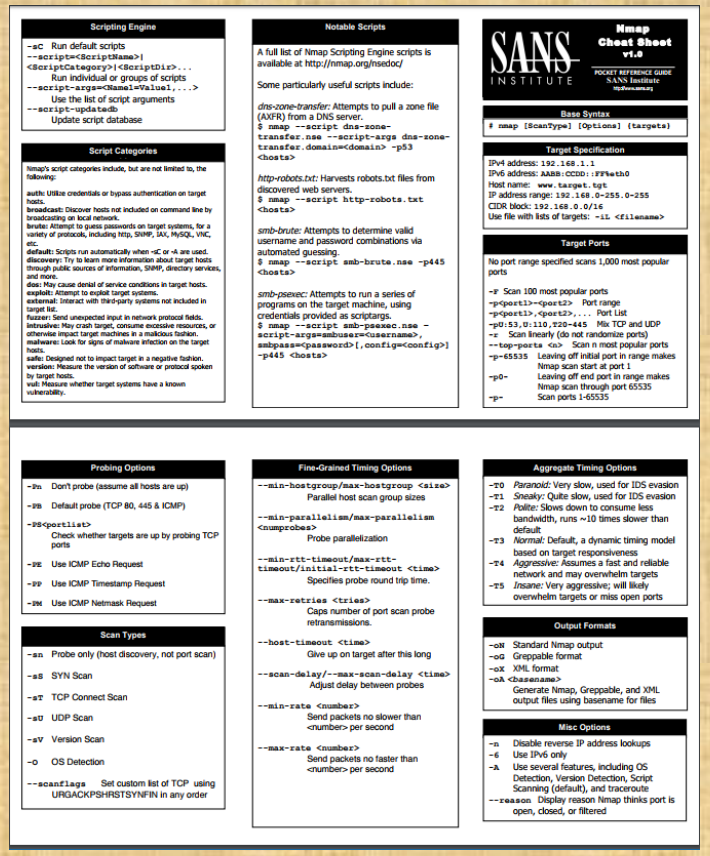






ndg or ndg@ndg.com
password123

Download nmap cheat sheet



Nmap Cheat Sheet v1.0
SANS INSTITUTE — POCKET REFERENCE GUIDE — SANS Institute

Scripting Engine

```
-sC  Run default scripts
--script=<ScriptName>|
<ScriptCategory>|<ScriptDir>...
      Run individual or groups of scripts
--script-args=<Name1=Value1,...>
      Use the list of script arguments
--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 hosts.
broadcast: Discover hosts not included on command line by broadcasting on local network.
brute: Attempt to guess passwords on target systems, for a variety of protocols, including http, SNMP, IAX, MySQL, VNC, etc.
default: Scripts run automatically when -sC or -A are used.
discovery: Try to learn more information about target hosts through public sources of information, SNMP, directory services, and more.
dos: May cause denial of service conditions in target hosts.
exploit: Attempt to exploit target systems.
external: Interact with third-party systems not included in target list.
fuzzer: Send unexpected input in network protocol fields.
intrusive: May crash target, consume excessive resources, or otherwise impact target machines in a malicious fashion.
malware: Look for signs of malware infection on the target hosts.
safe: Designed not to impact target in a negative fashion.
version: Measure the version of software or protocol spoken by target hosts.
vuln: Measure whether target systems have a known vulnerability.

Notable Scripts

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

Some particularly useful scripts include:

dns-zone-transfer: 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>`

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

Base Syntax

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

Target Specification

IPv4 address: `192.168.1.1`
IPv6 address: `AABB:CCDD::FF%eth0`
Host name: `www.target.tgt`
IP address range: `192.168.0-255.0-255`
CIDR block: `192.168.0.0/16`
Use file with lists of targets: `-iL <filename>`

Target Ports

No port range specified scans 1,000 most popular ports

```
-F  Scan 100 most popular ports
-p<port1>-<port2>  Port range
-p<port1>,<port2>,...  Port List
-p0:53,U:110,T20-445  Mix TCP and UDP
-r  Scan linearly (do not randomize ports)
--top-ports <n>  Scan n most popular ports
-p-65535  Leaving off initial port in range makes
          Nmap scan start at port 1
-p0-      Leaving off end port in range makes
          Nmap scan through port 65535
-p-       Scan ports 1-65535
```

Probing Options

```
-Pn  Don't probe (assume all hosts are up)
-PB  Default probe (TCP 80, 445 & ICMP)
-PS<portlist>
     Check whether targets are up by probing TCP ports
-PE  Use ICMP Echo Request
-PP  Use ICMP Timestamp Request
-PM  Use ICMP Netmask Request
```

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
```

Fine-Grained Timing Options

```
--min-hostgroup/max-hostgroup <size>
     Parallel host scan group sizes
--min-parallelism/max-parallelism
<numprobes>
     Probe parallelization
--min-rtt-timeout/max-rtt-
timeout/initial-rtt-timeout <time>
     Specifies probe round trip time.
--max-retries <tries>
     Caps number of port scan probe
     retransmissions.
--host-timeout <time>
     Give up on target after this long
--scan-delay/--max-scan-delay <time>
     Adjust delay between probes
--min-rate <number>
     Send packets no slower than
     <number> per second
--max-rate <number>
     Send packets no faster than
     <number> per second
```

Aggregate Timing Options

```
-T0  Paranoid: Very slow, used for IDS evasion
-T1  Sneaky: Quite slow, used for IDS evasion
-T2  Polite: 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
```

Output Formats

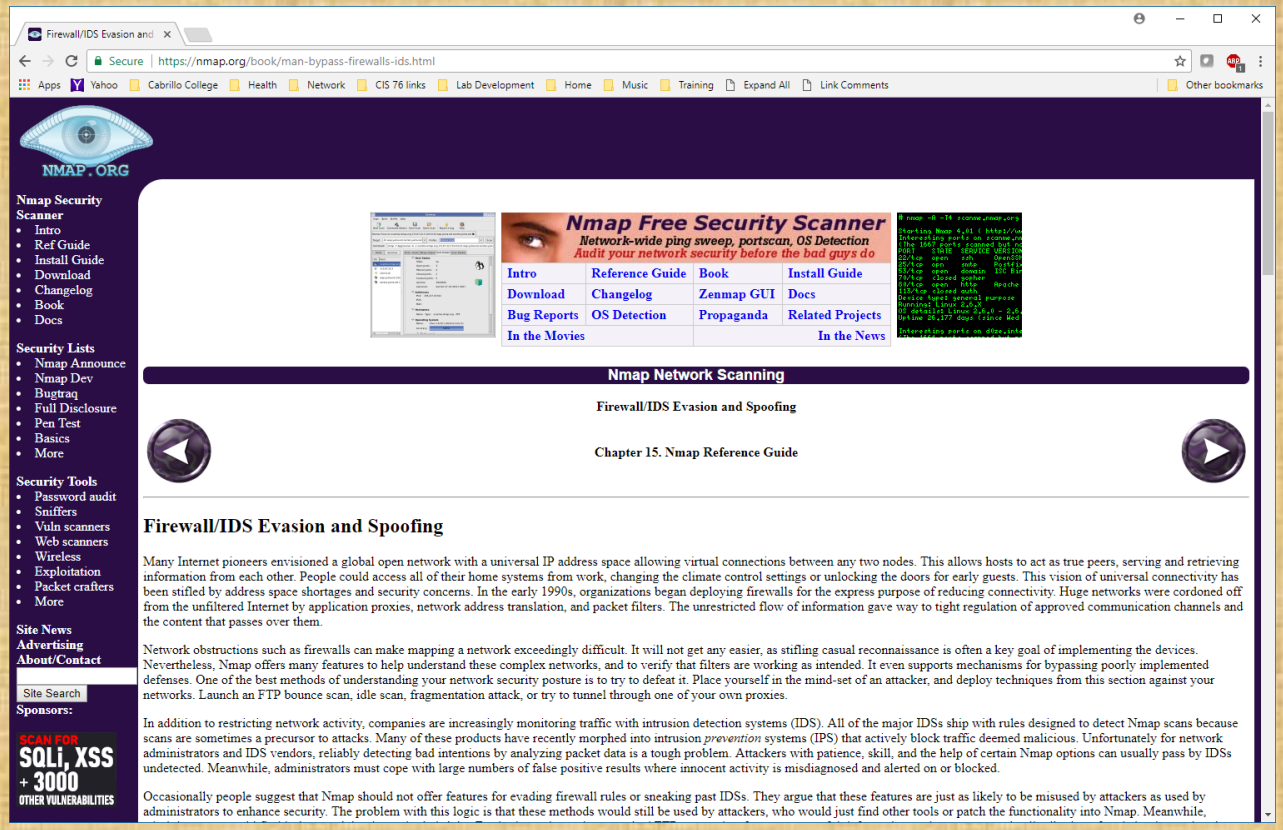
```
-oN  Standard Nmap output
-oG  Greppable format
-oX  XML format
-oA <basename>
     Generate Nmap, Greppable, and XML
     output files using basename for files
```

Misc Options

```
-n  Disable reverse IP address lookups
-6  Use IPv6 only
-A  Use several features, including OS
    Detection, Version Detection, Script
    Scanning (default), and traceroute
--reason  Display reason Nmap thinks port is
          open, closed, or filtered
```

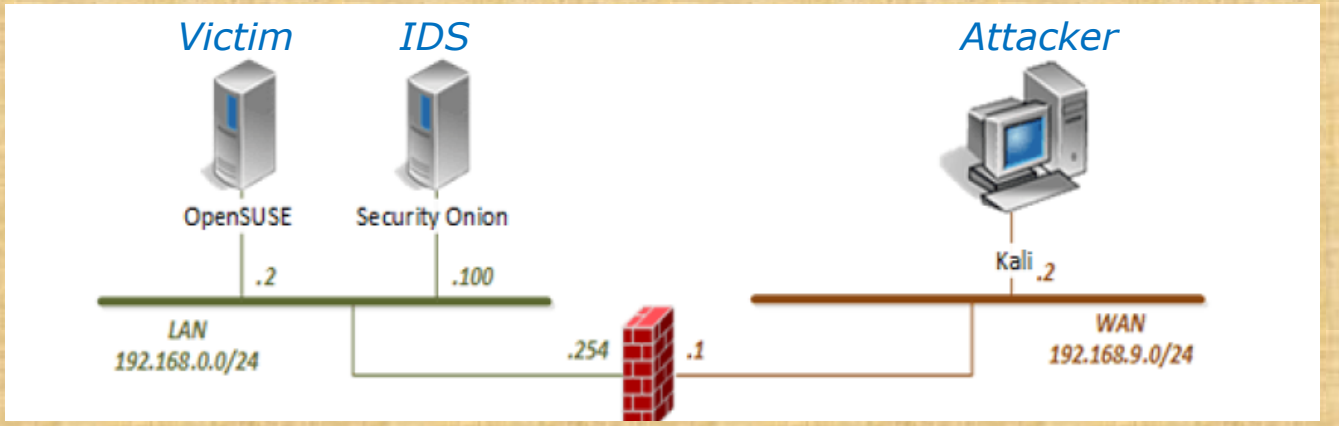
https://blogs.sans.org/pen-testing/files/2013/10/NmapCheatSheetv1.1.pdf

Browse to the nmap Firewall/IDS Evasion Page



https://nmap.org/book/man-bypass-firewalls-ids.html

Test IDS with regular Nmap scan



[Kali] nmap 192.168.0.2

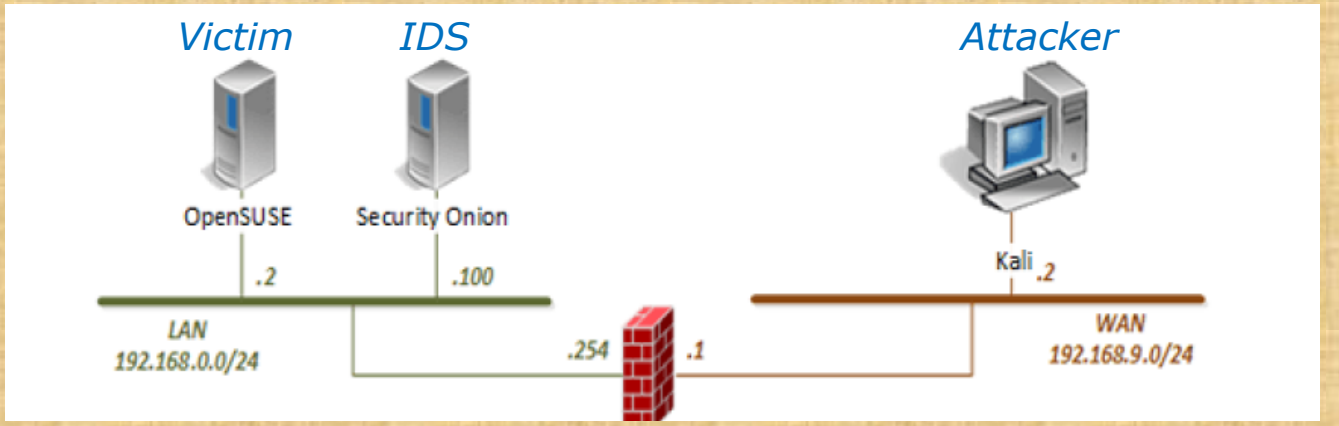
Which tool(s) recorded the scan?

- ❑ Snorby
- ❑ Squert
- ❑ Sguil

Put your answer in the chat window

Top: Record the time of the scan in the logs so you can delineate the next scan.

Test IDS with fragmented scan



[Kali] nmap -f 192.168.0.2

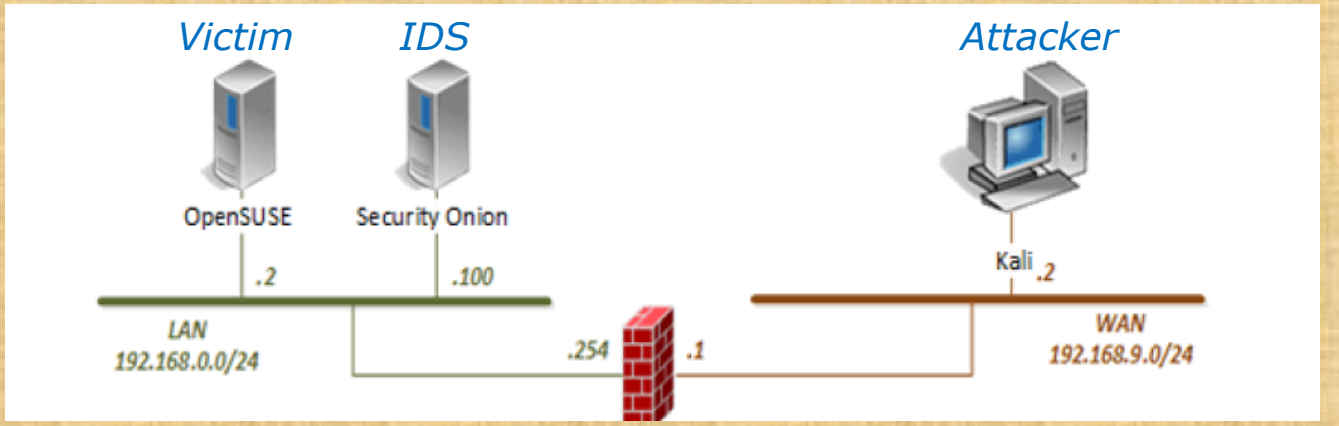
Which tool(s) recorded the scan?

- ❑ Snorby
- ❑ Squert
- ❑ Sguil

Put your answer in the chat window

Top: Record the time of the scan in the logs so you can delineate the next scan.

Test IDS with small MTU scan



Maximum transmission unit must be a multiple of 8

[Kali] nmap --mtu 8 192.168.0.2

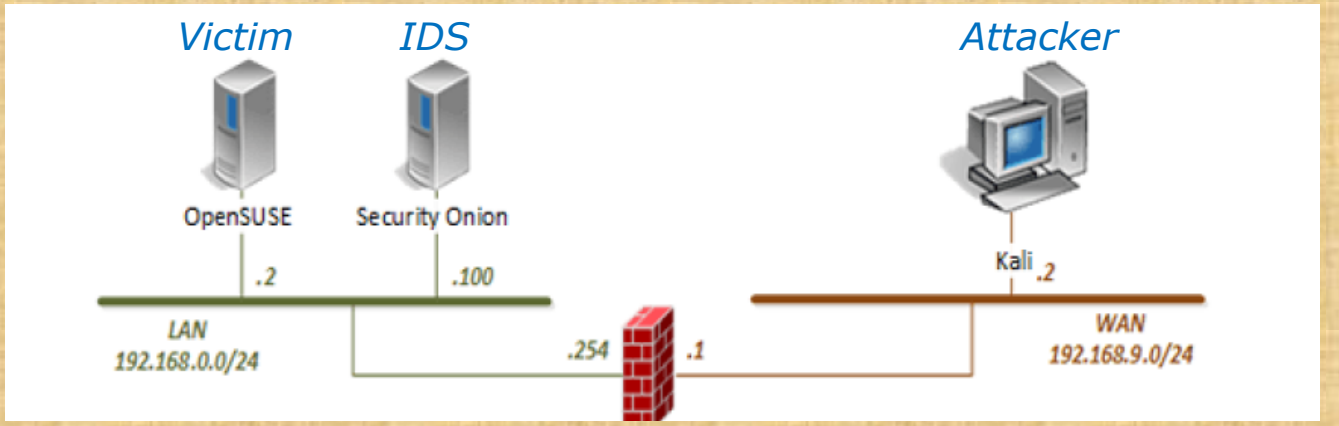
Which tool(s) recorded the scan?

- ❑ Snorby
- ❑ Squert
- ❑ Sguil

Put your answer in the chat window

Top: Record the time of the scan in the logs so you can delineate the next scan.

Test IDS with a decoy scan



Makes it look like scans are coming from several hosts

[Kali] nmap -D 192.168.9.20 192.168.9.30 192.168.9.40 192.168.0.2

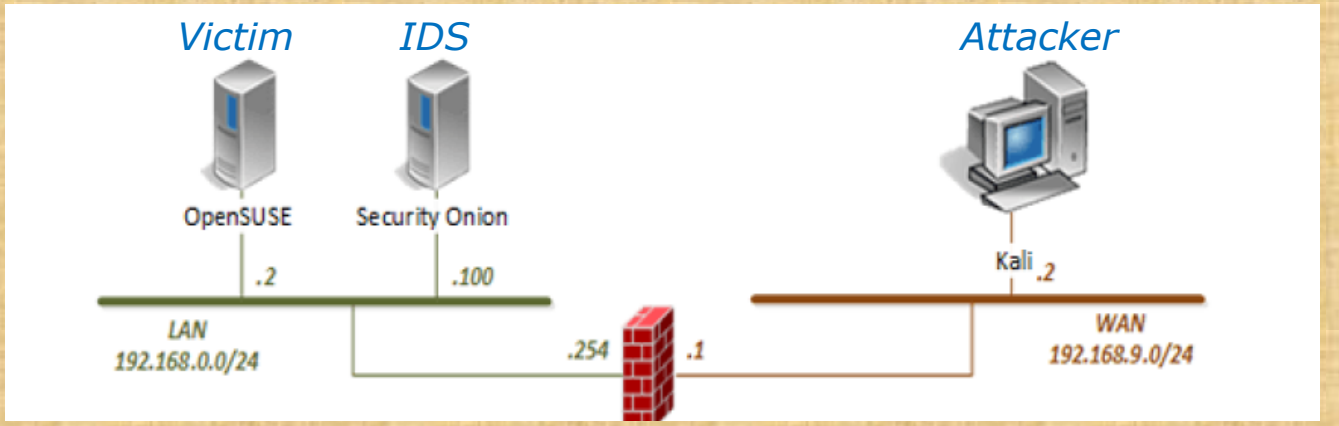
Which tool(s) recorded the scan?

- ❑ Snorby
- ❑ Squert
- ❑ Sguil

Put your answer in the chat window

Top: Record the time of the scan in the logs so you can delineate the next scan.

Test IDS with spoofed MAC scan



[Kali] nmap -sT -PN -spoof-mac 0 192.168.0.2

Which tool(s) recorded the scan?

- ❑ Snorby
- ❑ Squert
- ❑ Sguil

Put your answer in the chat window

Top: Record the time of the scan in the logs so you can delineate the next scan.

Final Project Presentations

Presentations

Grading Rubric (60 points)
5 points - Professional quality document (readability, formatting, spelling, accuracy)
5 points - Scenario and diagram (provides necessary context to understand the lab)
5 points - Vulnerabilities & exploits (accurate summaries and citations) 20 points - Step-by-step instructions (20 steps minimum, 1 point per step)
5 points - Requirements, admonition, prevention (are included). 5 points - Complete appendixes.
10 points - Testing another student's lab and providing them with helpful written feedback.
5 points - [Optional] Presentation and demo to class.

Extra credit (up 30 points)
5 points each for testing additional student labs. You must use the testing spreadsheet above so that all projects get tested equally.

CIS 76 Project

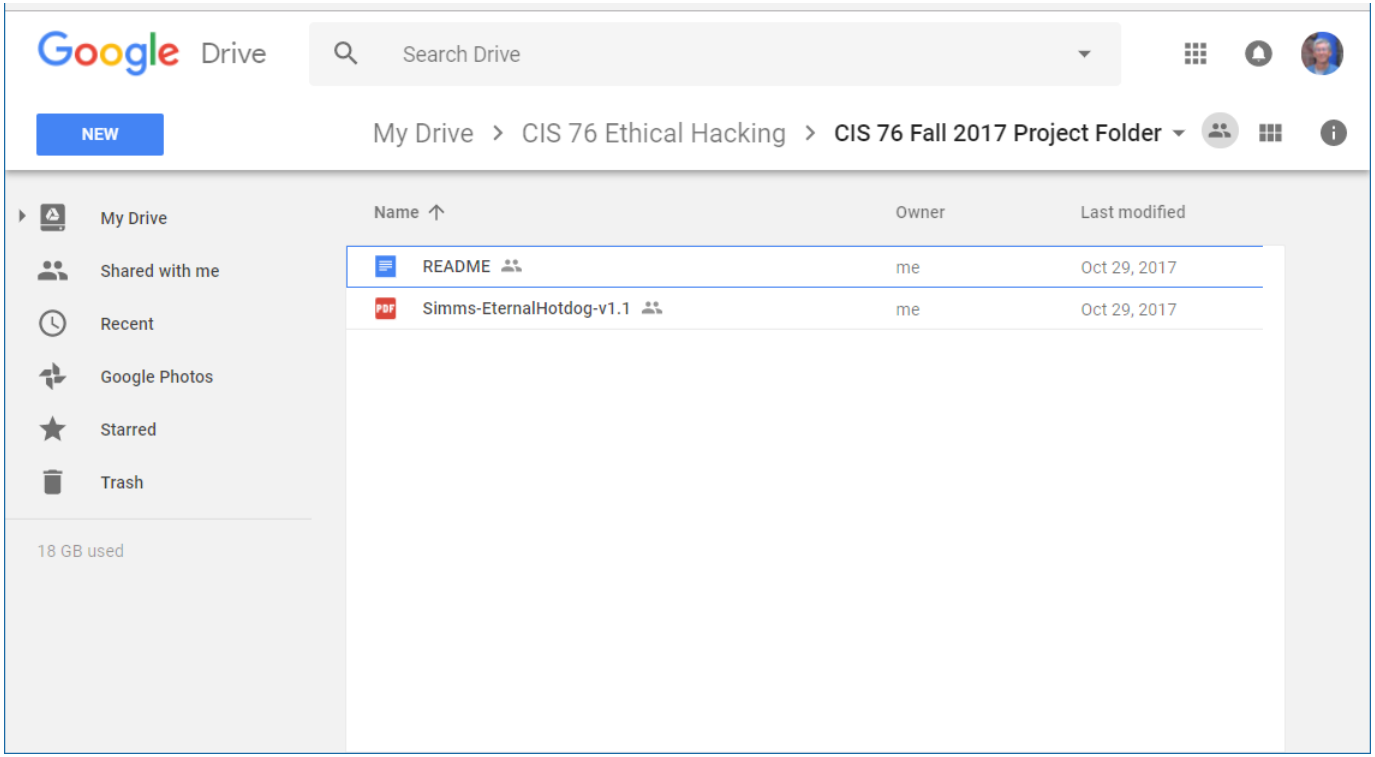
Use this directory to share your project with other classmates

Calendar Page

Assignment

- Project
- Project testing signup sheet
- Student project folder

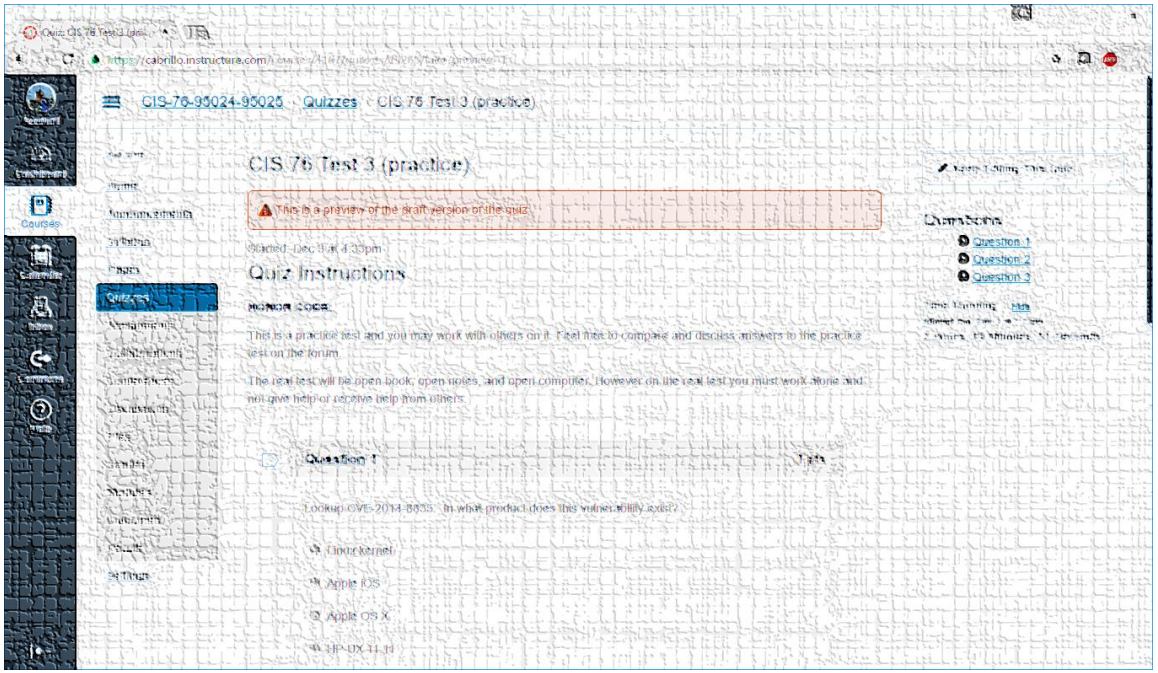
https://simms-teach.com/cis76calendar.php



https://cabrillo.instructure.com/courses/7125/pages/cis-76-project-folder


Assignment

Practice Test



The practice test on Canvas will be available after class.


Wrap up

Next Class is the Final Exam (Test #3)

Tuesday 4:00 PM

Test #3
Five Posts
Extra credit labs

Backup