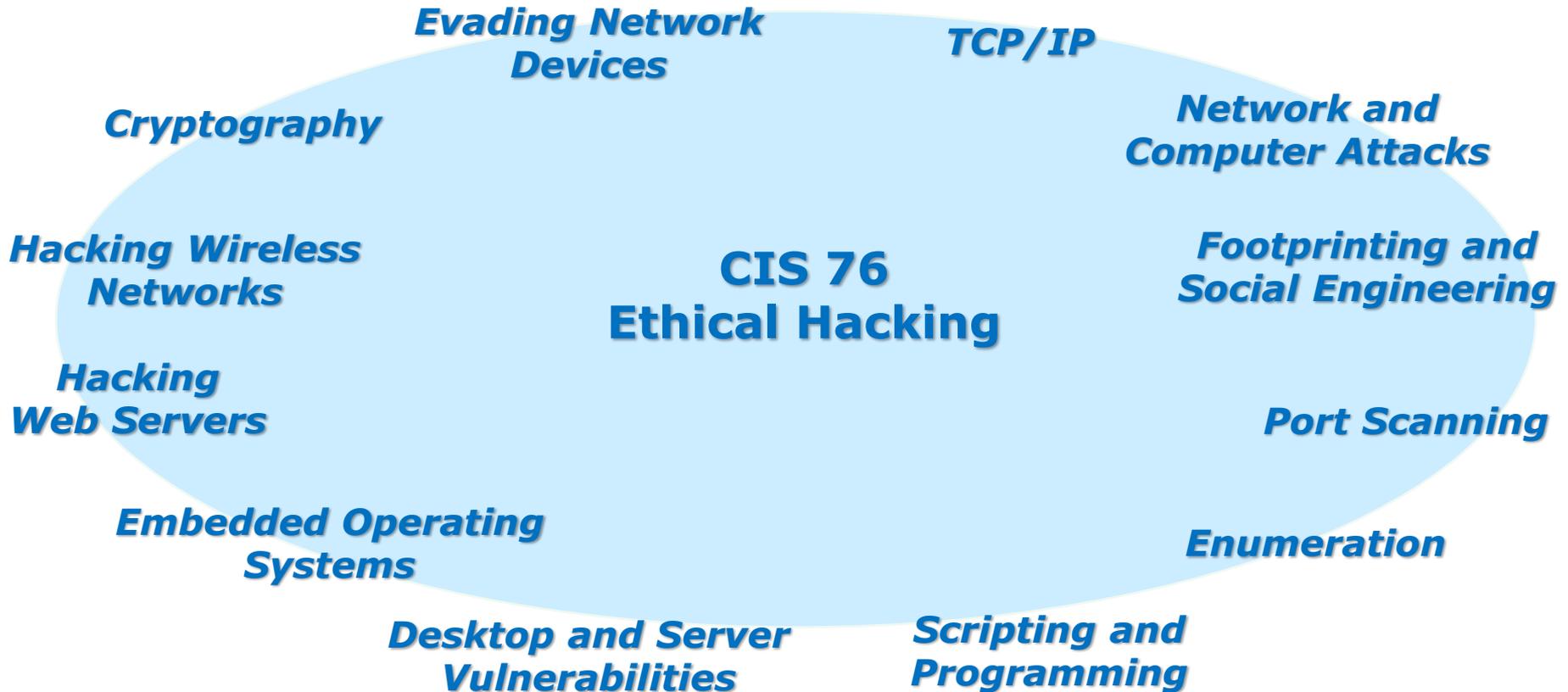




## Rich's lesson module checklist

- Slides and lab posted
- WB converted from PowerPoint
- Print out agenda slide and annotate page numbers
  
- Flash cards
- Properties
- Page numbers
- 1<sup>st</sup> 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

The screenshot shows a web browser window with the URL [simms-teach.com/cis90calendar.php](http://simms-teach.com/cis90calendar.php). The page title is "Rich's Cabrillo College CIS Classes CIS 90 Calendar". On the left sidebar, there are several navigation links, with "CIS 76" highlighted in a red box. The main content area features a "Calendar" link in a red box. Below this is a table with columns for "Lesson", "Date", "Topics", and "Link". The table lists various topics and links, with "Presentation slides (download)" and "Enter virtual classroom" highlighted in red boxes.

Lesson	Date	Topics	Link
		<b>Class and Lab Overview</b> <ul style="list-style-type: none"> <li>Understand how the course will work</li> <li>High-level overview of computers, operating systems and virtual machines</li> <li>Overview of LINUX/Linux market and architecture</li> <li>Using SSH for remote network exits</li> <li>Using terminals and the command line</li> </ul>	
	9/2	<b>Methods</b> <a href="#">Presentation slides (download)</a>	
		<b>Supplemental</b> <ul style="list-style-type: none"> <li>Howto #148: Logging into Opus (command)</li> </ul>	
		<b>Assignments</b> <ul style="list-style-type: none"> <li>Student Survey</li> <li>Lab 1</li> </ul>	
		<b>CCC Center</b> <a href="#">Enter virtual classroom</a>	
		<b>Quiz 1</b>	
		<b>Commands</b>	

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

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

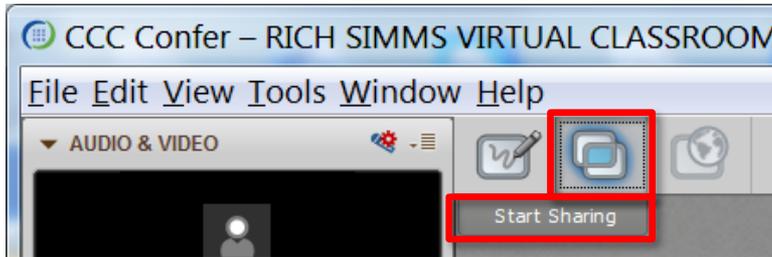
CIS 76 website Calendar page

One or more login sessions to Opus-II

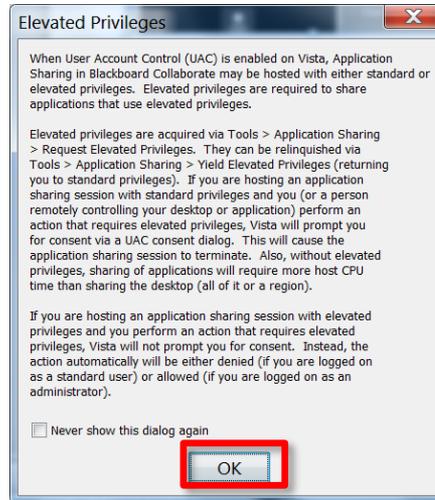


# Student checklist for sharing desktop with classmates

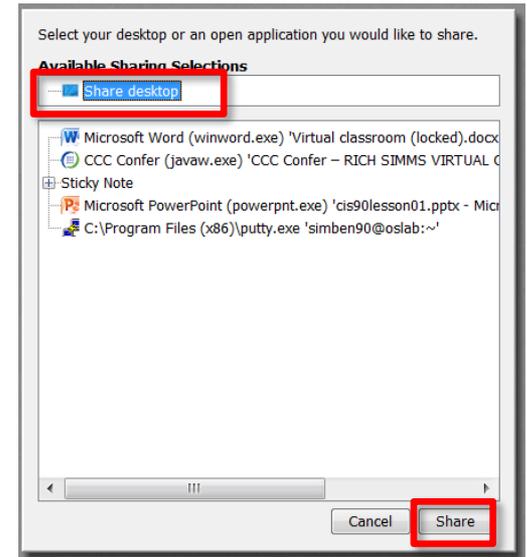
1) Instructor gives you sharing privileges.



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



3) Click OK button.



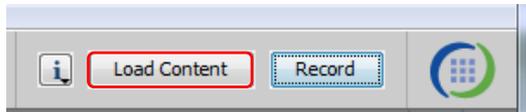
4) Select "Share desktop" and click Share button.



# Rich's CCC Confer checklist - setup

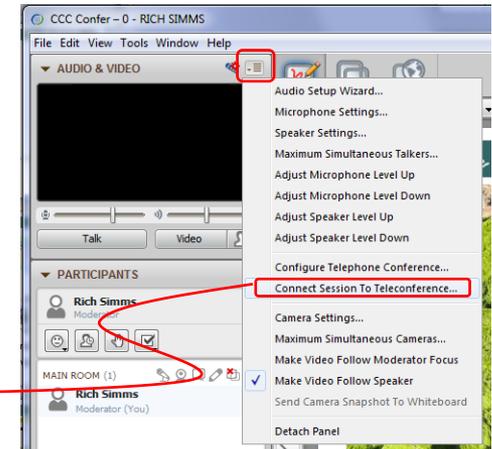
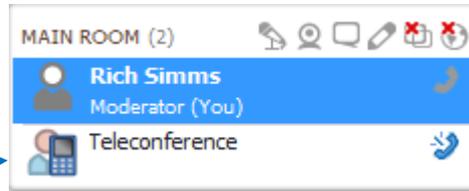


[ ] Preload White Board

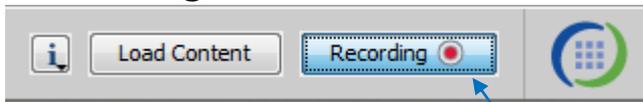


[ ] Connect session to Teleconference

*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



The screenshot displays a Windows desktop with several applications open:

- CCC Confer - 0 - RIC...:** A video conference window showing a participant named Rich Simms. It includes controls for audio and video, a list of participants, and a chat window.
- foxit for slides:** A Foxit Reader window displaying a PDF document titled 'cis90lesson07.pdf'. A red box highlights the application with the label 'foxit for slides'.
- chrome:** A Google Chrome browser window displaying a document from 'simms-teach.com/docs/cis90/cis-90-TEST-1-Fall-12.pdf'. A red box highlights the application with the label 'chrome'.
- putty:** A PuTTY terminal window showing a login session for 'simben90@oslab'. The terminal output includes:

```
login as: simben90
simben90@oslab.cabrillo.edu's password:
Access denied
simben90@oslab.cabrillo.edu's password:
Last login: Mon Oct  8 18:58:43 2012 from 10.10.10.10
```

A red box highlights the application with the label 'putty'.
- vSphere Client:** A VMware vSphere Client window showing the management interface for a virtual machine named 'CIS 192'. A red box highlights the application with the label 'vSphere Client'.

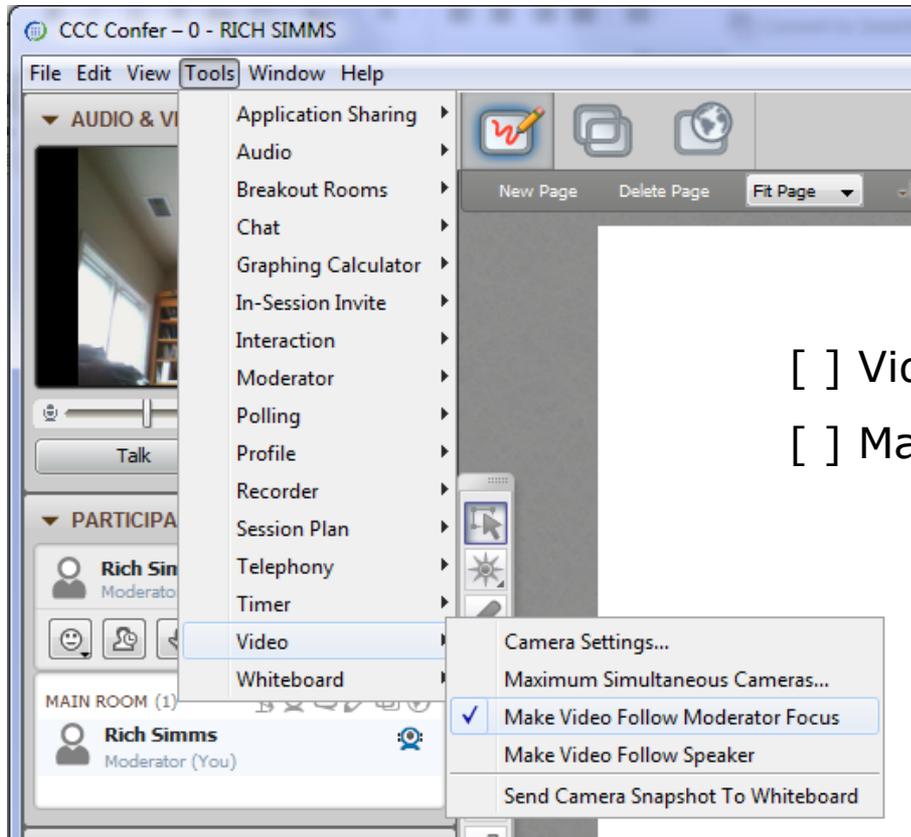
Other visible elements include a file explorer window showing a directory structure with folders like 'boot', 'bin', 'etc', and 'sbin', and a taskbar at the bottom with various application icons and a system tray showing the time as 6:52 AM on 10/10/2012.

[ ] layout and share apps





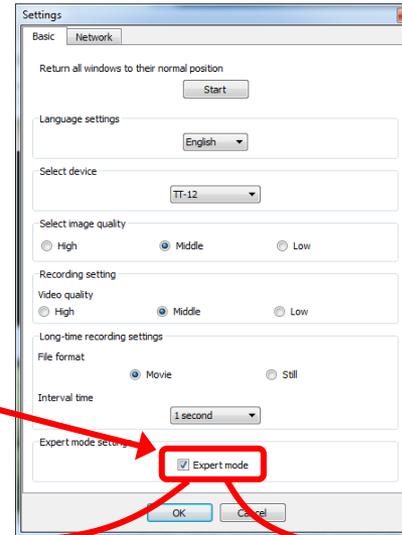
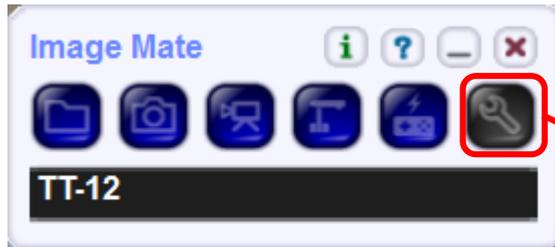
# Rich's CCC Confer checklist - webcam setup



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



# Rich's CCC Confer checklist - Elmo



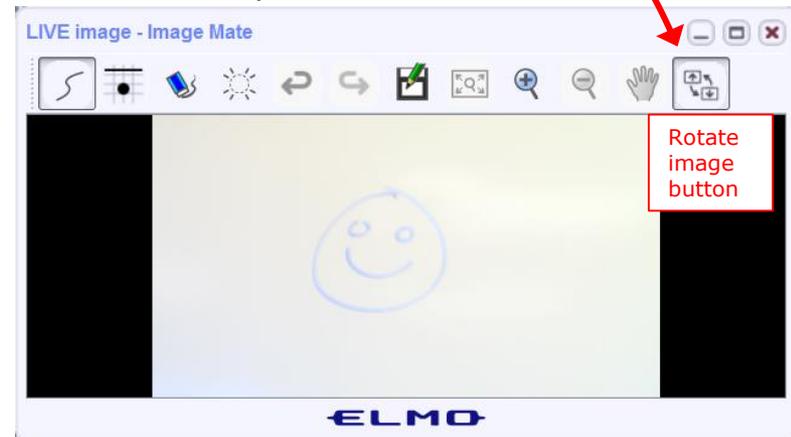
The "rotate image" button is necessary if you use both the side table and the white board.

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

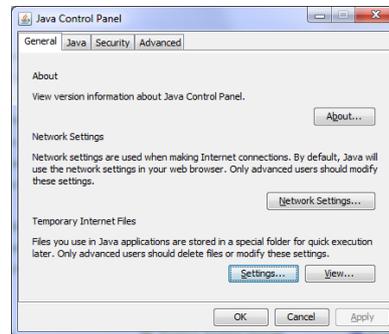
Universal Fix for CCC Confer:

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

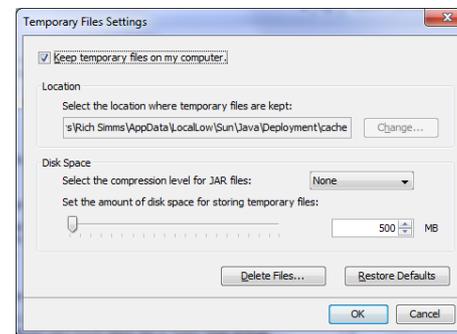
Control Panel (small icons)



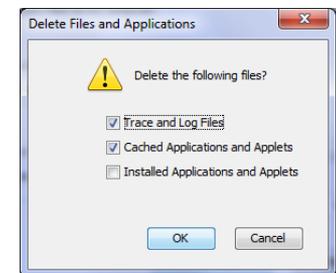
General Tab > Settings...



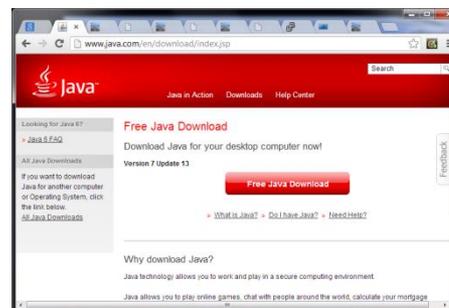
500MB cache size



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.*



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.

## 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

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

How this course works?

Past lesson material?

Previous labs?

Chinese  
Proverb

他問一個問題，五分鐘是個傻子，他不問一個問題仍然是一個傻瓜永遠。

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



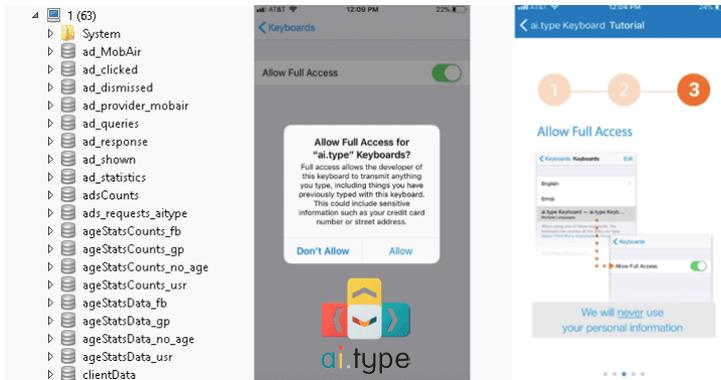
# In the news

## Recent news

### 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>



*"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/>



*"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, mspace.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>



*"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>



*"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."*



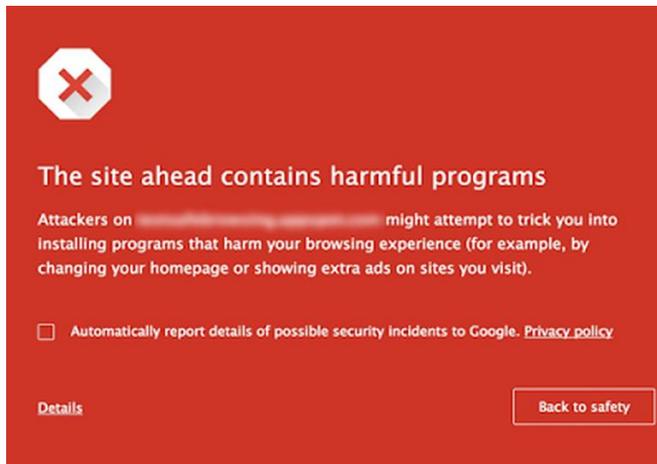
# Best Practices

## 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](mailto: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**

<b>Tue</b>	12/12	<b>Test #3 (the final exam)</b>	<a href="#">5 posts</a> <a href="#">Lab X1</a> <a href="#">Lab X2</a> <a href="#">Lab X3</a> <a href="#">Lab X4</a> <a href="#">Lab X5</a> <a href="#">Lab X6</a> <a href="#">Lab X7</a> <a href="#">Lab X8</a>
		<b>Time</b> <ul style="list-style-type: none"> <li>Tuesday 4:00PM - 6:50PM in Room 828</li> </ul> <b>Materials</b> <ul style="list-style-type: none"> <li>Test (<a href="#">canvas</a>)</li> </ul> <b>CCC Confer</b> <ul style="list-style-type: none"> <li><a href="#">Enter virtual classroom</a></li> <li>Archives <a href="#">Confer</a> or <a href="#">3CMedia</a></li> </ul>	

*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
<i>Classes starting between:</i>		
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
<hr/>		
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
<hr/>		
Friday am	9:00 am-11:50 am	Friday, December 15
Friday pm	1:00 pm-3:50 pm	Friday, December 15
<hr/>		
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

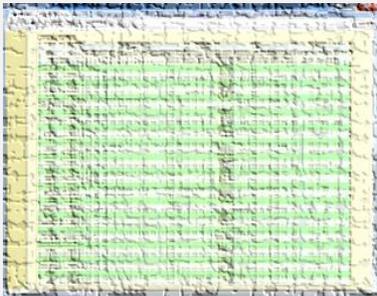
Section	Days	Times	Units	Instructor	Room
98163	T	5:30PM-8:35P	3.00	R.Simms	OL
Section 98163 is an ONLINE course. Meets weekly throughout the semester online by remote technology with an additional 50 min online lab per week. For details, see instructor's web page at <a href="http://go.cabrillo.edu/online">go.cabrillo.edu/online</a> .					
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 <a href="http://go.cabrillo.edu/online">go.cabrillo.edu/online</a> .					

## 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

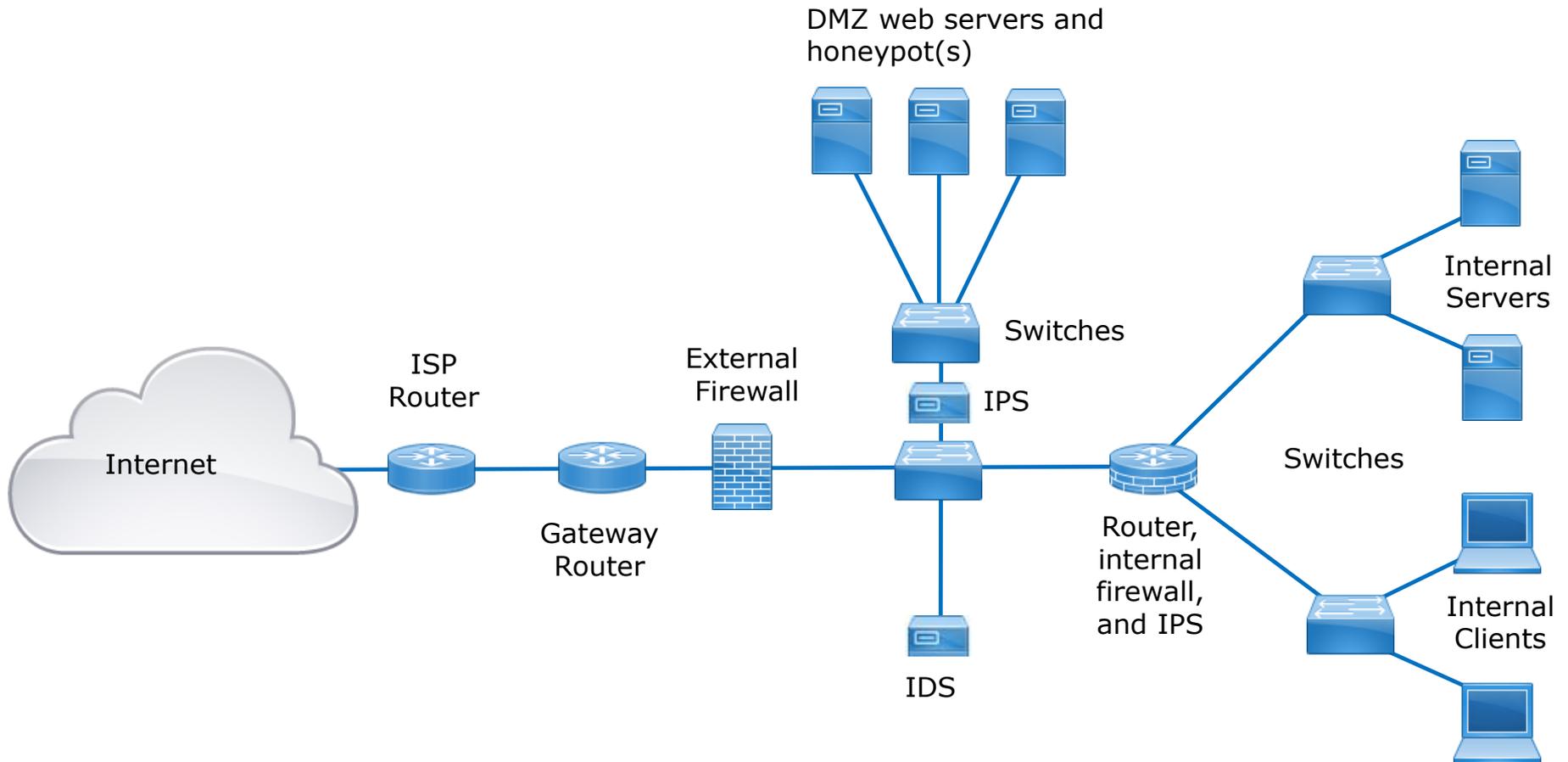
### Points that could have been earned:

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

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

# 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 can 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>

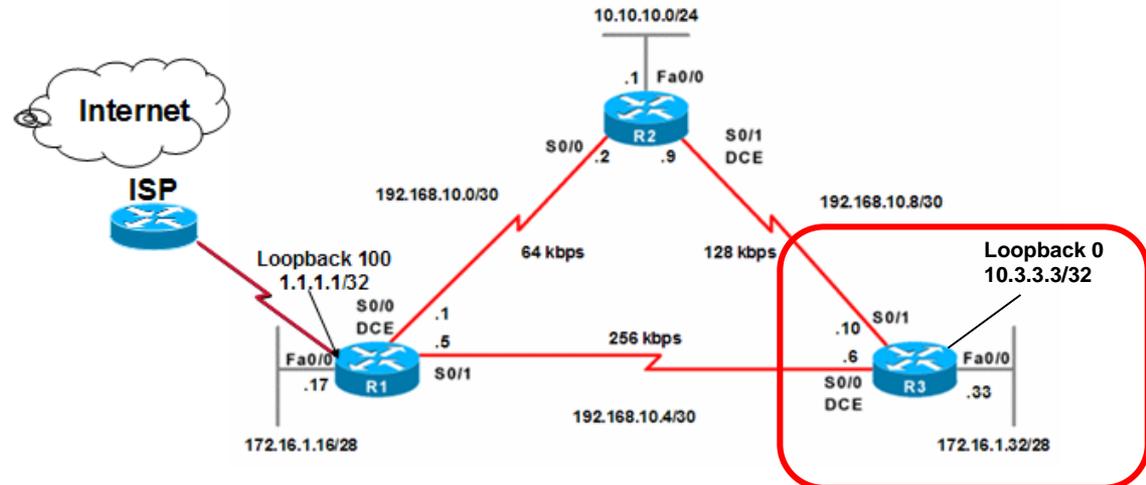
# Example Cisco Routing Table

```
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 192.168.10.5
R3#
```



# Example Cisco Routing Table

```

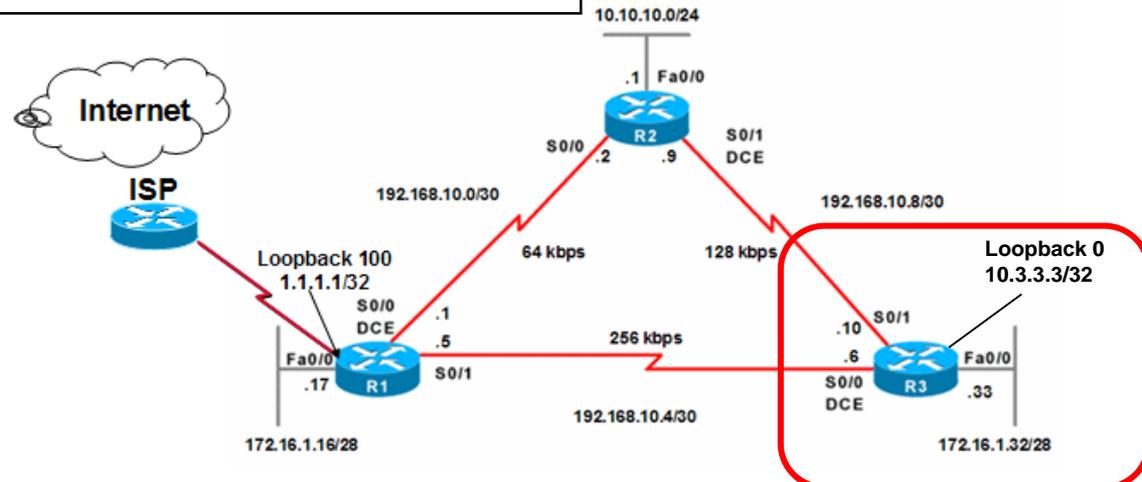
R3#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       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, Serial10/0
C   192.168.10.4 is directly connected, Serial10/0
C   192.168.10.8 is directly connected, Serial10/1
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, Serial10/0
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, Serial10/1
O*E2 0.0.0.0/0 [110/1] via 192.168.10.5, 00:00:24, Serial10/0
R3#
    
```

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

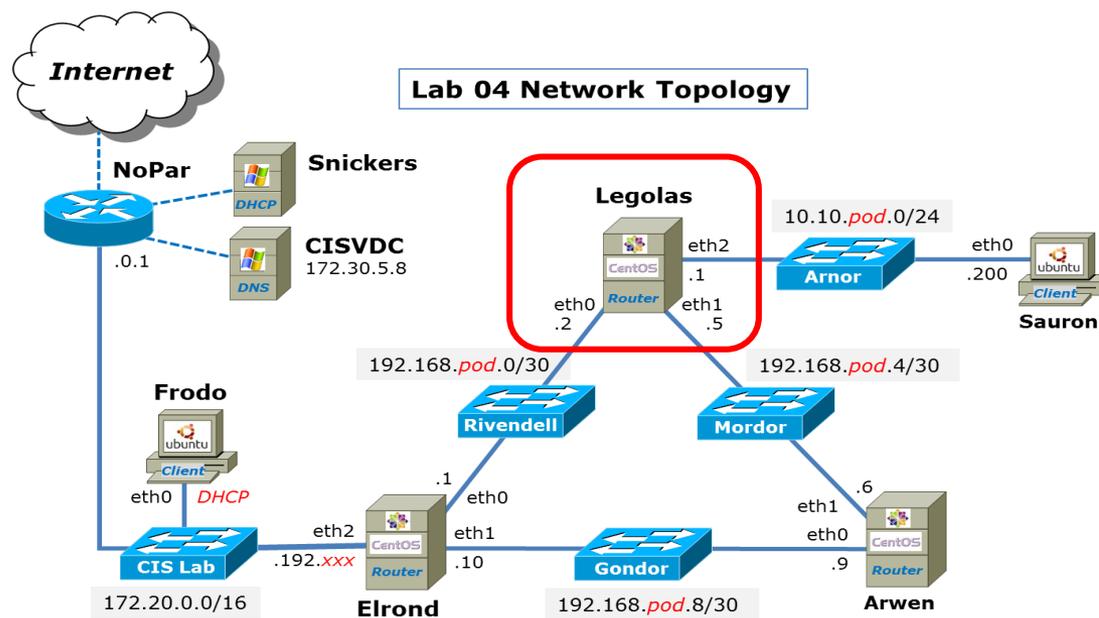
*Put your answer in the chat window*



# 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

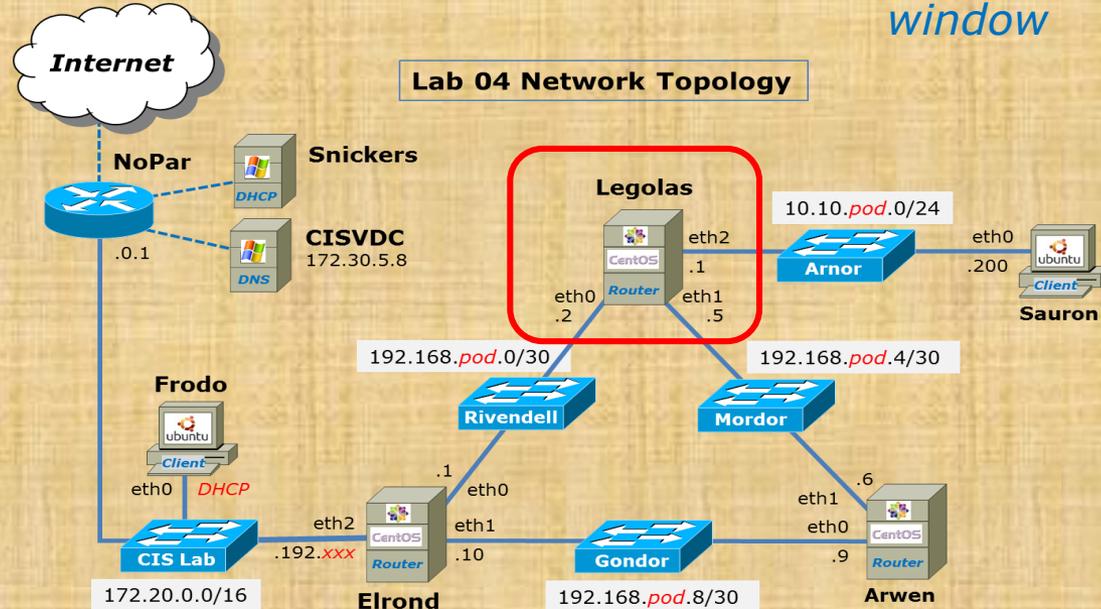
# Example Linux Routing Table

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

**CVE Details**  
The ultimate security vulnerability datasource

Search:  Search  
View CVE

Log In Register **Vulnerability Feeds & Widgets** [www.itsecdb.com](http://www.itsecdb.com)

**Cisco » IOS : Vulnerability Statistics**

Vulnerabilities (427) CVSS Scores Report Browse all versions Possible matches for this product Related Metasploit Modules  
 Related OVAL Definitions : Vulnerabilities (105) Patches (7) Inventory Definitions (0) Compliance Definitions (0)  
 Vulnerability Feeds & Widgets

**Vulnerability Trends Over Time**

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	2	2							1				
2004	11	10	1		1										
2005	17	12	3	2			1			3					
2006	10	4	2	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		2	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	

Warning : Vulnerabilities with publish dates before 1999 are not included in this table and chart. (Because there are not many of them and they make the page look bad; and they may

<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

Search:

**Cisco » IOS : Security Vulnerabilities**

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9  
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Total number of vulnerabilities : 427 Page : 1 (This Page) 2 3 4 5 6 7 8 9

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	<a href="#">CVE-1999-0775</a>				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	<a href="#">CVE-2002-1357 119</a>			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	<a href="#">CVE-2002-1358 20</a>			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	<a href="#">CVE-2002-1359 20</a>			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	<a href="#">CVE-2002-1360 20</a>			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	<a href="#">CVE-2004-1464</a>			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	<a href="#">CVE-2006-4950</a>				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&opdir=0&opmemc=0&ophttps=0&opbyp=0&opfileinc=0&opginf=0&cvssscoremin=0&cvssscoremax=0&year=0&month=0&cweid=0&order=3&trc=427&sha=bd51a01b646bad788bdc715f12e17fa177698ba8](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&opdir=0&opmemc=0&ophttps=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

The screenshot shows a web browser window with the URL [https://www.exploit-db.com/search/?action=search&description=cisco+ios&g-recaptcha-response=03AHJ\\_VuvFax5SIVvdeMeHAPTaj9pL2EKLCN5OYAvXwq1wF0d-KqrFOFrNUZU](https://www.exploit-db.com/search/?action=search&description=cisco+ios&g-recaptcha-response=03AHJ_VuvFax5SIVvdeMeHAPTaj9pL2EKLCN5OYAvXwq1wF0d-KqrFOFrNUZU). The search results are displayed in a table with columns for Date, D, A, V, Title, Platform, and Author.

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 hijacks 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

Traceroute Path 1: from Guadalajara, Mexico to Washington, D.C. via *Belarus*



*Rerouting  
Internet traffic  
by attacking BGP*

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

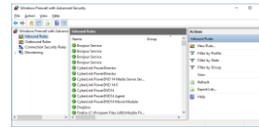
Traceroute Path 2: from Denver, CO to Denver, CO via *Iceland*





# Firewalls

## Firewalls



- 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



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

# Network Address Translation



EH-pfSense-05.cabrillo.edu - Firewall: NAT: Port Forward - Mozilla Firefox

Kali Linux, an Offensive S... x Amazon.com: Online ... x EH-pfSense-05.cis.ca... x

https://10.76.5.1/firewall\_nat.php

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

**Sense** COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Gold Help

Firewall / NAT / Port Forward

Port Forward 1:1 Outbound NPT

Rules											
	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	WAN	TCP	*	*	WAN address	22 (SSH)	10.76.5.150	22 (SSH)	Forward ssh to Kali

*Configuring NAT to forward port 22 on the pfSense firewall*

## Wireless MAC filter

**Wireless - Wireless MAC Filter**

Wireless MAC filter allows you to control packets from devices with specified MAC address in your Wireless LAN.

**Basic Config**

Band	5GHz ▾
Enable MAC Filter	<input checked="" type="radio"/> Yes <input type="radio"/> No
MAC Filter Mode	Accept ▾

**MAC filter list (Max Limit : 64)**

Client Name (MAC address)	Add / Delete
<input type="text" value="ex: 2C:56:DC:85:3E:E8"/> ▾	
No data in table.	

**Apply**

# 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.	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.
<span style="background-color: #d9e1f2; border: 1px solid black; padding: 2px;">Required</span> <span style="background-color: #cfe2f3; border: 1px solid black; padding: 2px; margin-left: 20px;">Optional</span>								

<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 ~]#
```



# 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	any	Server-425-zone	host-sun-hwa-ext .231	any	any
----	-----------------------	------	-----------	--------------	-----	-----	-----	-----	-----------------	-----------------------	-----	-----



# Application layer inspection

<input type="checkbox"/>	Name	Location	Count	Rule Name	Threat Name	Host Type	Severity	Action	Packet Capture
<input type="checkbox"/>	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

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.



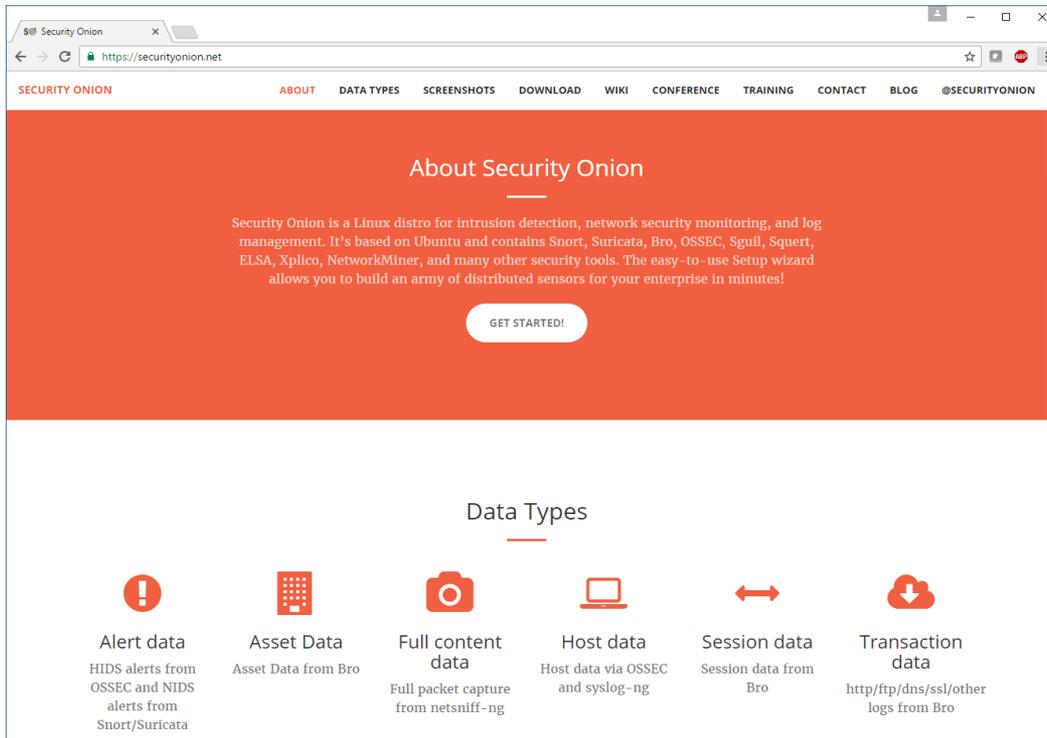
## Intrusion Prevention Systems (IPS)

- 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

# Using Security Onion and a PA-500



*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.*

<https://securityonion.net/>

*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
```

# Squert

The screenshot shows the Squert web interface in a Chromium browser window. The URL is `https://localhost/squert/index.php?id=69d83723933455457100ab8317c96370`. The interface displays a summary of events and a detailed list of events.

**Summary:**

- Interval: 2016-12-06 00:00:00 -> 2016-12-06 23:59:59 (+00:00)
- Filtered by Object: NO
- Filtered by Sensor: NO
- Priority: 20.3% (red), 71.1% (yellow), 1.7% (green), 6.9% (blue)
- Queue: 16 (red)
- SC: 1 (yellow)
- DC: 1 (red)
- Activity: 06:59:27
- Last Event: ET SCAN Potential SSH Scan OUTBOUND
- Signature: 2003068
- Proto: 6
- % Total: 0.847%

**Alert:** alert tcp \$HOME\_NET any -> \$EXTERNAL\_NET 22 (msg:"ET SCAN Potential SSH Scan OUTBOUND"; flags:S,12; threshold: type threshold, track by\_src, count 5, seconds 120; reference:url:en.wikipedia.org/wiki/Brute\_force\_attack; reference:url:doc.emergingthreats.net/2003068; classtype:attempted-recon; sid:2003068; rev:6;)

**File:** downloaded.rules:10641

**Summary Table:**

QUEUE	ACTIVITY	LAST EVENT	SOURCE	COUNTRY	DESTINATION	COUNTRY
16		2016-12-06 06:59:27	10.99.99.100	RFC1918 (.lo)	207.62.187.231	UNITED STATES (.us)

**Event List Table:**

ST	TIMESTAMP	EVENT ID	SOURCE	PORT	DESTINATION	PORT	SIGNATURE
RT	2016-12-06 06:59:27	<a href="#">4.61775</a>	10.99.99.100	44738	207.62.187.231	22	ET SCAN Potential SSH Scan OUTBOUND
RT	2016-12-06 06:59:26	<a href="#">5.67462</a>	10.99.99.100	44712	207.62.187.231	22	ET SCAN Potential SSH Scan OUTBOUND
RT	2016-12-06 06:59:26	<a href="#">4.61774</a>	10.99.99.100	44696	207.62.187.231	22	ET SCAN Potential SSH Scan OUTBOUND
RT	2016-12-06 06:59:11	<a href="#">5.67461</a>	10.99.99.100	46512	207.62.187.231	22	ET SCAN Potential SSH Scan OUTBOUND
RT	2016-12-06 06:59:11	<a href="#">3.371244</a>	10.99.99.100	46513	207.62.187.231	22	ET SCAN Potential SSH Scan OUTBOUND
RT	2016-12-06 06:17:49	<a href="#">3.371231</a>	10.99.99.100	55006	207.62.187.231	22	ET SCAN Potential SSH Scan OUTBOUND
RT	2016-12-06 06:17:48	<a href="#">4.61760</a>	10.99.99.100	54968	207.62.187.231	22	ET SCAN Potential SSH Scan OUTBOUND
RT	2016-12-06 06:17:48	<a href="#">3.371230</a>	10.99.99.100	54964	207.62.187.231	22	ET SCAN Potential SSH Scan OUTBOUND

**Count by Priority:**

- high: 384 (20.3%)
- medium: 1343 (71.1%)
- low: 32 (1.7%)
- other: 131 (6.9%)

**Count by Classification:**

- compromised L1
- compromised L2
- attempted access
- denial of service
- policy violation
- reconnaissance
- malicious

WELCOME matahari | LOGOUT UTC 07:02:41

An SSH scan detected in Squert

## PAN

The screenshot displays the Palo Alto Networks management interface. The 'Monitor' tab is active, showing a list of logs. A search filter '(addr in 10.99.99.100)' is applied. The logs table contains the following data:

Receive Time	Type	Name	From Zone	Attacker	Victim	To Port	Application	Action	Severity	Rule
12/05 22:59:30	vulnerability	Unknown HTTP Request Method Found	CIS-187-zone	10.99.99.100	207.62.187.243	80	web-browsing	alert	informational	allow-some-to-valiente
12/05 22:59:30	vulnerability	Unknown HTTP Request Method Found	CIS-187-zone	10.99.99.100	207.62.187.231	80	web-browsing	alert	informational	allow-some-to-sun-hwa
12/05 22:59:30	vulnerability	HTTP OPTIONS Method	CIS-187-zone	10.99.99.100	207.62.187.243	80	web-browsing	alert	informational	allow-some-to-valiente
12/05 22:59:30	vulnerability	HTTP OPTIONS Method	CIS-187-zone	10.99.99.100	207.62.187.231	80	web-browsing	alert	informational	allow-some-to-sun-hwa
12/05 22:46:36	vulnerability	Bash Remote Code Execution Vulnerability	CIS-187-zone	10.99.99.100	207.62.187.231	80	web-browsing	reset-both	critical	allow-some-to-sun-hwa
12/05 22:17:53	vulnerability	Unknown HTTP Request Method Found	CIS-187-zone	10.99.99.100	207.62.187.231	80	web-browsing	alert	informational	allow-some-to-sun-hwa
12/05 22:17:53	vulnerability	HTTP OPTIONS Method	CIS-187-zone	10.99.99.100	207.62.187.231	80	web-browsing	alert	informational	allow-some-to-sun-hwa
12/05 22:15:32	vulnerability	Unknown HTTP Request Method Found	CIS-187-zone	10.99.99.100	207.62.187.243	80	web-browsing	alert	informational	allow-some-to-valiente
12/05 22:15:32	vulnerability	HTTP OPTIONS Method	CIS-187-zone	10.99.99.100	207.62.187.243	80	web-browsing	alert	informational	allow-some-to-valiente
12/05 22:10:35	vulnerability	Unknown HTTP Request Method Found	CIS-187-zone	10.99.99.100	207.62.187.243	80	web-browsing	alert	informational	allow-some-to-valiente
12/05 22:10:35	vulnerability	HTTP OPTIONS Method	CIS-187-zone	10.99.99.100	207.62.187.243	80	web-browsing	alert	informational	allow-some-to-valiente
12/05 22:07:21	vulnerability	Unknown HTTP Request Method Found	CIS-187-zone	10.99.99.100	207.62.187.231	80	web-browsing	alert	informational	allow-some-to-sun-hwa
12/05 22:07:21	vulnerability	HTTP OPTIONS Method	CIS-187-zone	10.99.99.100	207.62.187.231	80	web-browsing	alert	informational	allow-some-to-sun-hwa
07/12 15:27:11	vulnerability	Bash Remote Code Execution Vulnerability	CIS-187-zone	10.99.99.100	207.62.187.243	80	web-browsing	reset-both	critical	allow-some-to-valiente
07/12 15:27:10	vulnerability	Bash Remote Code Execution Vulnerability	CIS-187-zone	10.99.99.100	207.62.187.243	80	web-browsing	reset-both	critical	allow-some-to-valiente
07/12 15:27:10	vulnerability	Bash Remote Code Execution Vulnerability	CIS-187-zone	10.99.99.100	207.62.187.243	80	web-browsing	reset-both	critical	allow-some-to-valiente
07/12 15:27:10	vulnerability	Bash Remote Code Execution Vulnerability	CIS-187-zone	10.99.99.100	207.62.187.243	80	web-browsing	reset-both	critical	allow-some-to-valiente

The interface also shows a left-hand navigation menu with categories like Logs, Threat, and PDF Reports. The bottom status bar indicates 'Displaying logs 1 - 97' with a '100' per page setting and a 'DESC' sort order.

*An HTTP scan detected by Palo Alto Networks*

## nmap "shellshock" scan

```
root@pen-kali: ~  
File Edit View Search Terminal Help  
root@pen-kali:~# nmap -sV -p- --script http-shellshock sun-hwa.cis.cabrillo.edu  
Starting Nmap 7.12 ( https://nmap.org ) at 2016-12-05 23:17 PST  
Nmap scan report for sun-hwa.cis.cabrillo.edu (207.62.187.231)  
Host is up (0.00040s latency).  
Other addresses for sun-hwa.cis.cabrillo.edu (not scanned): 2607:f380:80f:f425::231  
Not shown: 65532 filtered ports  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol 2.0)  
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))  
|_http-server-header: Apache/2.4.18 (Ubuntu)  
443/tcp   closed https  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 150.42 seconds  
root@pen-kali:~#
```

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

## PAN

The screenshot shows the Palo Alto Networks Panorama interface. The 'Monitor' tab is active, displaying a list of logs for the address '10.99.99.100'. The logs table has the following columns: Receive Time, Type, Name, From Zone, Attacker, Victim, To Port, Application, Action, Severity, and Rule. The first row is highlighted with a red box.

Receive Time	Type	Name	From Zone	Attacker	Victim	To Port	Application	Action	Severity	Rule
12/05 23:19:30	vulnerability	Bash Remote Code Execution Vulnerability	CIS-187-zone	10.99.99.100	207.62.187.231	80	web-browsing	reset-both	critical	allow-some-to-sun-hwa
12/05 22:59:30	vulnerability	Unknown HTTP Request Method Found	CIS-187-zone	10.99.99.100	207.62.187.243	80	web-browsing	alert	informational	allow-some-to-valiente
12/05 22:59:30	vulnerability	Unknown HTTP Request Method Found	CIS-187-zone	10.99.99.100	207.62.187.231	80	web-browsing	alert	informational	allow-some-to-sun-hwa
12/05 22:59:30	vulnerability	HTTP OPTIONS Method	CIS-187-zone	10.99.99.100	207.62.187.243	80	web-browsing	alert	informational	allow-some-to-valiente
12/05 22:59:30	vulnerability	HTTP OPTIONS Method	CIS-187-zone	10.99.99.100	207.62.187.231	80	web-browsing	alert	informational	allow-some-to-sun-hwa
12/05 22:46:36	vulnerability	Bash Remote Code Execution Vulnerability	CIS-187-zone	10.99.99.100	207.62.187.231	80	web-browsing	reset-both	critical	allow-some-to-sun-hwa
12/05 22:17:53	vulnerability	Unknown HTTP Request Method Found	CIS-187-zone	10.99.99.100	207.62.187.231	80	web-browsing	alert	informational	allow-some-to-sun-hwa
12/05 22:17:53	vulnerability	HTTP OPTIONS Method	CIS-187-zone	10.99.99.100	207.62.187.231	80	web-browsing	alert	informational	allow-some-to-sun-hwa
12/05 22:15:32	vulnerability	Unknown HTTP Request Method Found	CIS-187-zone	10.99.99.100	207.62.187.243	80	web-browsing	alert	informational	allow-some-to-valiente
12/05 22:15:32	vulnerability	HTTP OPTIONS Method	CIS-187-zone	10.99.99.100	207.62.187.243	80	web-browsing	alert	informational	allow-some-to-valiente
12/05 22:10:35	vulnerability	Unknown HTTP Request Method Found	CIS-187-zone	10.99.99.100	207.62.187.243	80	web-browsing	alert	informational	allow-some-to-valiente
12/05 22:10:35	vulnerability	HTTP OPTIONS Method	CIS-187-zone	10.99.99.100	207.62.187.243	80	web-browsing	alert	informational	allow-some-to-valiente
12/05 22:07:21	vulnerability	Unknown HTTP Request Method Found	CIS-187-zone	10.99.99.100	207.62.187.231	80	web-browsing	alert	informational	allow-some-to-sun-hwa
12/05 22:07:21	vulnerability	HTTP OPTIONS Method	CIS-187-zone	10.99.99.100	207.62.187.231	80	web-browsing	alert	informational	allow-some-to-sun-hwa
07/12 15:27:11	vulnerability	Bash Remote Code Execution Vulnerability	CIS-187-zone	10.99.99.100	207.62.187.243	80	web-browsing	reset-both	critical	allow-some-to-valiente
07/12 15:27:10	vulnerability	Bash Remote Code Execution Vulnerability	CIS-187-zone	10.99.99.100	207.62.187.243	80	web-browsing	reset-both	critical	allow-some-to-valiente
07/12 15:27:10	vulnerability	Bash Remote Code Execution Vulnerability	CIS-187-zone	10.99.99.100	207.62.187.243	80	web-browsing	reset-both	critical	allow-some-to-valiente

At the bottom of the interface, there is a status bar showing 'Displaying logs 1 - 98' and '100 per page'. The user 'rsimms' is logged in.

*PAN logs it and resets the connection*

## PAN

The screenshot shows the Palo Alto Networks Panorama interface. The 'Monitor' tab is active, displaying a log table. A 'Packet Capture' window is overlaid on the table, showing the details of a captured packet. The log table has columns for 'Receive Time', 'Action', 'Severity', and 'Rule'. The packet capture window shows the raw packet data in hexadecimal and ASCII, including an IP header and an HTTP GET request.

Receive Time	Action	Severity	Rule	
12/05 23:19:30	allowing	reset-both	critical	allow-some-to-sun-hwa
12/05 22:59:30	allowing	alert	informational	allow-some-to-valiente
12/05 22:59:30	allowing	alert	informational	allow-some-to-sun-hwa
12/05 22:59:30	allowing	alert	informational	allow-some-to-valiente
12/05 22:59:30	allowing	alert	informational	allow-some-to-sun-hwa
12/05 22:46:36	allowing	reset-both	critical	allow-some-to-sun-hwa
12/05 22:17:53	allowing	alert	informational	allow-some-to-sun-hwa
12/05 22:17:53	allowing	alert	informational	allow-some-to-sun-hwa
12/05 22:15:32	allowing	alert	informational	allow-some-to-valiente
12/05 22:15:32	allowing	alert	informational	allow-some-to-valiente
12/05 22:10:35	allowing	alert	informational	allow-some-to-valiente
12/05 22:10:35	allowing	alert	informational	allow-some-to-sun-hwa
12/05 22:07:21	allowing	alert	informational	allow-some-to-sun-hwa
12/05 22:07:21	allowing	alert	informational	allow-some-to-sun-hwa
07/12 15:27:11	allowing	reset-both	critical	allow-some-to-valiente
07/12 15:27:10	allowing	reset-both	critical	allow-some-to-valiente
07/12 15:27:10	allowing	reset-both	critical	allow-some-to-valiente

**Packet Capture**

```

23:19:19.000000 24:e9:b3:24:fc:82 > 00:1b:17:37:be:10, ethertype IPv4 (0x0800), length 60
0x0000: 001b 1737 be10 24e9 b324 fc82 0800 4500 ...7..f...f...E.
0x0010: 015e 4941 4000 3106 d25e 0a63 6364 ac1e ...^IA&?...^ccd..
0x0020: 0515 d316 0050 9a81 3e56 ac5e 0c4e 8018 ...P...V...^N..
0x0030: 00e5 0e55 0000 0101 080a 0009 77ad 0451 ...U.....w..Q
0x0040: 5019 4745 5420 2120 4854 5450 2f31 2e31 P.GET./HTTP/1.1
0x0050: 0d0a 2829 207b 203a 3b7d 3b20 6563 686f ..().(:);;echo
0x0060: 3b20 6563 686f 2022 594b 534d 5047 5144 ;;echo."YKSMPCQD
0x0070: 5a4e 4747 4744 5022 3a20 2829 207b 203a ZNGGGDP"..().(:
0x0080: 3b7d 3b20 6563 686f 3b20 6563 686f 2022 ;);;echo;echo."
0x0090: 594b 534d 5047 5144 5a4e 4747 4744 5022 YKSMPCQDZNGGGDP"
0x00a0: 0d0a 436f 6e6e 6563 7469 6f6e 3a20 636c ..Connection:.cl
0x00b0: 6f73 650d 0a48 6f73 743a 2073 756e 2d68 ose..Host:.sun-h
0x00c0: 7761 2e63 6973 2e63 6162 7269 6c6c 6f2e wa.cis.cabrillo.
0x00d0: 6564 750d 0a55 7365 722d 4167 656e 743a edu..User-Agent:
0x00e0: 2028 2920 7b20 3a3b 7d3b 2065 6368 6f3b ..().(:);;echo;
0x00f0: 2065 6368 6f20 2259 4b53 4d50 4751 445a .echo."YKSMPCQDZ
0x0100: 4e47 4747 4450 220d 0a52 6566 6572 6572 NGGGDP"..Referer
0x0110: 3a20 2829 207b 203a 3b7d 3b20 6563 686f ..().(:);;echo
0x0120: 3b20 6563 686f 2022 594b 534d 5047 5144 ;;echo."YKSMPCQD
0x0130: 5a4e 4747 4744 5022 0d0a 436f 6f6b 6965 ZNGGGDP"..Cookie
0x0140: 3a20 2829 207b 203a 3b7d 3b20 6563 686f ..().(:);;echo
0x0150: 3b20 6563 686f 2022 594b 534d 5047 5144 ;;echo."YKSMPCQD
0x0160: 5a4e 4747 4744 5022 0d0a 0d0a
    
```

One packet captured

## PAN

1202564065033980284.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
1	0.000000	10.99.99.100	172.30.5.21	HTTP	GET / HTTP/1.1 Continuation or non-HTTP traffic

Frame 1: 364 bytes on wire (2912 bits), 364 bytes captured (2912 bits)  
 Ethernet II, Src: 24:e9:b3:24:fc:82 (24:e9:b3:24:fc:82), Dst: PaloAlto\_37:be:10 (00:1b:17:37:be:10)  
 Internet Protocol, Src: 10.99.99.100 (10.99.99.100), Dst: 172.30.5.21 (172.30.5.21)  
 Transmission Control Protocol, Src Port: 54038 (54038), Dst Port: http (80), Seq: 1, Ack: 1, Len: 298  
 Hypertext Transfer Protocol  
   GET / HTTP/1.1\r\n  
     [Expert Info (chat/sequence): GET / HTTP/1.1\r\n]  
       [Message: GET / HTTP/1.1\r\n]  
       [severity level: chat]  
       [Group: sequence]  
       Request Method: GET  
       Request URI: /  
       Request Version: HTTP/1.1  
 Hypertext Transfer Protocol  
   Data (282 bytes)  
     data: 2829207b203a3b7d3b206563686f3b206563686f2022594b...  
     [Length: 282]

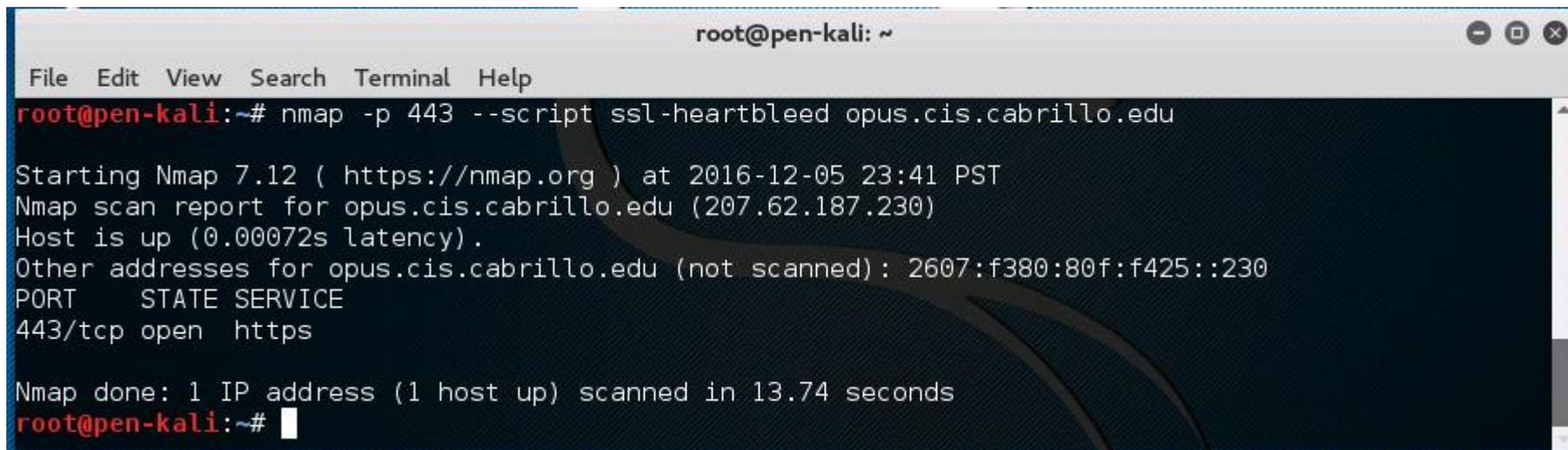
Offset	Hex	ASCII
0050	0d 0a 28 29 20 7b 20 3a 3b 7d 3b 20 65 63 68 6f	..{\ : }; echo
0060	3b 20 65 63 68 6f 20 22 59 4b 53 4d 50 47 51 44	: echo "YKSMRGQD
0070	5a 4e 47 47 47 44 50 22 3a 20 28 29 20 7b 20 3a	ZNGGGDP" : {\ :
0080	3b 7d 3b 20 65 63 68 6f 3b 20 65 63 68 6f 20 22	}; echo ; echo "
0090	59 4b 53 4d 50 47 51 44 5a 4e 47 47 47 44 50 22	YKSMRGQD ZNGGGDP"
00a0	0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 63 6c	..connection: cl
00b0	6f 73 65 0d 0a 48 6f 73 74 3a 20 73 75 6e 2d 68	ose..Host: sun-h
00c0	77 61 2e 63 69 73 2e 63 61 62 72 69 6c 6c 6f 2e	wa.cis.cabrillo.
00d0	65 64 75 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a	edu..User-Agent:
00e0	20 28 29 20 7b 20 3a 3b 7d 3b 20 65 63 68 6f 3b	{ : }; echo;
00f0	20 65 63 68 6f 20 22 59 4b 53 4d 50 47 51 44 5a	echo "YKSMRGQDZ
0100	4e 47 47 47 44 50 22 0d 0a 52 65 66 65 72 65 72	NGGGDP".Referer
0110	3a 20 28 29 20 7b 20 3a 3b 7d 3b 20 65 63 68 6f	: {\ : }; echo
0120	3b 20 65 63 68 6f 20 22 59 4b 53 4d 50 47 51 44	: echo "YKSMRGQD
0130	5a 4e 47 47 47 44 50 22 0d 0a 43 6f 6f 6b 69 65	ZNGGGDP" ..Cookie
0140	3a 20 28 29 20 7b 20 3a 3b 7d 3b 20 65 63 68 6f	: {\ : }; echo
0150	3b 20 65 63 68 6f 20 22 59 4b 53 4d 50 47 51 44	: echo "YKSMRGQD

Data (data.data), 282 bytes      Packets: 1 Displayed: 1 Marked: 0 Load time: 0:00.143      Profile: Default

*One packet captured and exported to Wireshark*

## nmap "heartbleed" scan

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

A terminal window titled "root@pen-kali: ~" with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the execution of the command "nmap -p 443 --script ssl-heartbleed opus.cis.cabrillo.edu". The output indicates that the host is up and that port 443/tcp is open and running https. The scan was completed in 13.74 seconds.

```
root@pen-kali: ~  
File Edit View Search Terminal Help  
root@pen-kali:~# nmap -p 443 --script ssl-heartbleed opus.cis.cabrillo.edu  
Starting Nmap 7.12 ( https://nmap.org ) at 2016-12-05 23:41 PST  
Nmap scan report for opus.cis.cabrillo.edu (207.62.187.230)  
Host is up (0.00072s latency).  
Other addresses for opus.cis.cabrillo.edu (not scanned): 2607:f380:80f:f425::230  
PORT      STATE SERVICE  
443/tcp  open  https  
  
Nmap done: 1 IP address (1 host up) scanned in 13.74 seconds  
root@pen-kali:~#
```

*Squert, Sguil and PAN log it*

# Squert

The screenshot shows the Squert web interface. The browser address bar displays `https://localhost/squert/index.php?id=69d83723933455457100ab8317c96370`. The interface has tabs for 'EVENTS', 'SUMMARY', and 'VIEWS'. A status bar at the top shows the interval as '2016-12-06 00:00:00 -> 2016-12-06 23:59:59 (+00:00)' and filtered by object and sensor as 'NO'. Priority filters are shown as 22.9%, 68.8%, 1.6%, and 6.7%.

The main table has columns: TOGGLE, QUEUE, SC, DC, ACTIVITY, LAST EVENT, SIGNATURE, ID, PROTO, and % TOTAL. A summary table on the left shows: queued events (1953), total events (1951), total signatures (15), total sources (-), and total destinations (-). A 'COUNT BY PRIORITY' table shows: high (447, 22.9%), medium (1343, 68.8%), low (32, 1.6%), and other (131, 6.7%). A 'COUNT BY CLASSIFICATION' table shows: compromised L1, compromised L2, attempted access, denial of service, policy violation, reconnaissance, and malicious.

The main table highlights a log entry with a red '3' in the queue column and a red '1' in the SC and DC columns. The activity is 'ET POLICY Self Signed SSL Certificate (SomeOrganizationalUnit)' and the last event is '07:41:27'. The signature is 'ET POLICY Self Signed SSL Certificate (SomeOrganizationalUnit)' with ID 2013659, protocol 6, and 0.154% total. Below this, an alert message is shown: 'alert tcp \$EXTERNAL\_NET 443 -> \$HOME\_NET any (msg:"ET POLICY Self Signed SSL Certificate (SomeOrganizationalUnit)"; flow:established,from\_server; content:"|16 03|"; content:"|0b|"; within:7; content:"SomeOrganizationalUnit"; classtype:policy-violation; sid:2013659; rev:3;)'. A file path is listed as 'file: downloaded.rules:10469'. There are options to 'CATEGORIZE 0 EVENT(S)' and 'CREATE FILTER: src dst both'.

A secondary table shows details for the highlighted event: QUEUE 3, ACTIVITY, LAST EVENT 2016-12-06 07:41:27, SOURCE 207.62.187.230, COUNTRY UNITED STATES (.us), DESTINATION 10.99.99.100, and COUNTRY RFC1918 (.lo). Below this is a table with columns: ST, TIMESTAMP, EVENT ID, SOURCE, PORT, DESTINATION, PORT, SIGNATURE. It lists three events with 'RT' in the ST column and event IDs 3.371251, 4.61788, and 5.67499.

At the bottom, there is a 'WELCOME matahari | LOGOUT' message and 'UTC 07:47:10'.

*Squert logs the self-signed certificate sent to attacker*

## Sguil

SGUIL-0.9.0 - Connected To localhost  
 File Query Reports Sound: Off ServerName: localhost UserName: matahari UserID: 2 2016-12-06 07:49:13 GMT

RealTime Events Escalated Events

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	2	ids-01-et...	3.371175	2016-12-06 02:57:48	207.62.187.227	47801	10.76.26.105	5432	6	ET POLICY Suspicious inbound to Postgre...
RT	2	ids-01-et...	3.371177	2016-12-06 02:57:48	207.62.187.227	58226	10.76.26.105	1433	6	ET POLICY Suspicious inbound to MSSQL ...
RT	4	ids-01-et...	4.61682	2016-12-06 02:57:49	207.62.187.227	49406	10.76.26.105	1521	6	ET POLICY Suspicious inbound to Oracle S...
RT	1	ids-01-et...	4.61686	2016-12-06 02:57:49	207.62.187.227	60063	10.76.26.105	5801	6	ET SCAN Potential VNC Scan 5800-5820
RT	1	ids-01-et...	3.371179	2016-12-06 02:57:50	207.62.187.227	56635	10.76.26.105	5904	6	ET SCAN Potential VNC Scan 5900-5920
RT	6	ids-01-et...	4.61757	2016-12-06 06:07:02	10.99.99.100	61052	207.62.187.231	22	6	ET SCAN Potential SSH Scan OUTBOUND
RT	5	ids-01-et...	3.371228	2016-12-06 06:07:02	10.99.99.100	61051	207.62.187.231	22	6	ET SCAN Potential SSH Scan OUTBOUND
RT	5	ids-01-et...	5.67457	2016-12-06 06:07:02	10.99.99.100	61053	207.62.187.231	22	6	ET SCAN Potential SSH Scan OUTBOUND
RT	1	ids-01-et...	5.67460	2016-12-06 06:36:13	10.99.99.100	38738	207.62.187.243	80	6	ET POLICY Outgoing Basic Auth Base64 HT...
RT	1	ids-01-et...	4.61767	2016-12-06 06:36:13	10.99.99.100	38740	207.62.187.243	80	6	ET POLICY Outgoing Basic Auth Base64 HT...
RT	1	ids-01-et...	4.61788	2016-12-06 07:41:27	207.62.187.230	443	10.99.99.100	36696	6	ET POLICY Self Signed SSL Certificate (Som...
RT	1	ids-01-et...	5.67499	2016-12-06 07:41:27	207.62.187.230	443	10.99.99.100	36698	6	ET POLICY Self Signed SSL Certificate (Som...
RT	1	ids-01-et...	3.371251	2016-12-06 07:41:27	207.62.187.230	443	10.99.99.100	36700	6	ET POLICY Self Signed SSL Certificate (Som...

IP Resolution Agent Status Snort Statistics System Msgs

Reverse DNS  Enable External DNS

Src IP: 207.62.187.230  
 Src Name: 230.187.62.207.in-addr.arpa.oslab.cis.cabrillo.edu  
 Dst IP: 10.99.99.100  
 Dst Name: Unknown  
 Whois Query:  None  Src IP  Dst IP

Show Packet Data  Show Rule

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
IP	207.62.187.230	10.99.99.100	4	5	0	1213	16386	2	0	63	65100
TCP	Source Port	Dest Port	R	R	R	C	S	S	S	I	
TCP	443	36696	.	.	.	X	.	.	.		
TCP	Seq #	Ack #	Offset	Res	Window	Urp	ChkSum				
TCP	4139255891	3638125227	8	0	253	0	24403				
DATA	<pre> 16 03 01 00 59 02 00 00 55 03 01 58 46 6B A7 FE  ....Y...U..XFk.. CB 74 FC F7 AF 2E F9 8F 13 5D FA E9 6E EE 83 0F  .t.....].n... 08 78 DA 0A 86 CE 9D 8E 0C 38 97 20 05 C5 4F 74  .x.....8. ..0t 59 90 00 57 F7 7B 68 26 39 6F 51 E0 B1 83 47 F7  Y..W.{h&amp;9oQ...G. </pre>										

Search Packet Payload  Hex  Text  NoCase

*Sguil logs the self-signed certificate sent to attacker*

## PAN

The screenshot shows the Palo Alto Networks PAN interface. The 'Monitor' tab is active, displaying a log table for the address '10.99.100'. The first log entry is highlighted with a red box. The log entry details are as follows:

Receive Time	Type	Name	From Zone	Attacker	Victim	To Port	Application	Action	Severity	Rule
12/05 23:41:32	vulnerability	OpenSSL TLS Malformed Heartbeat Request Found - Heartbleed	CIS-187-zone	10.99.100	207.62.187.230	443	ssl	reset-both	medium	allow-some-to-opus

The interface also shows a sidebar with navigation options like Traffic, Threat, and Logs, and a bottom status bar indicating 'Displaying logs 1 - 99'.

*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



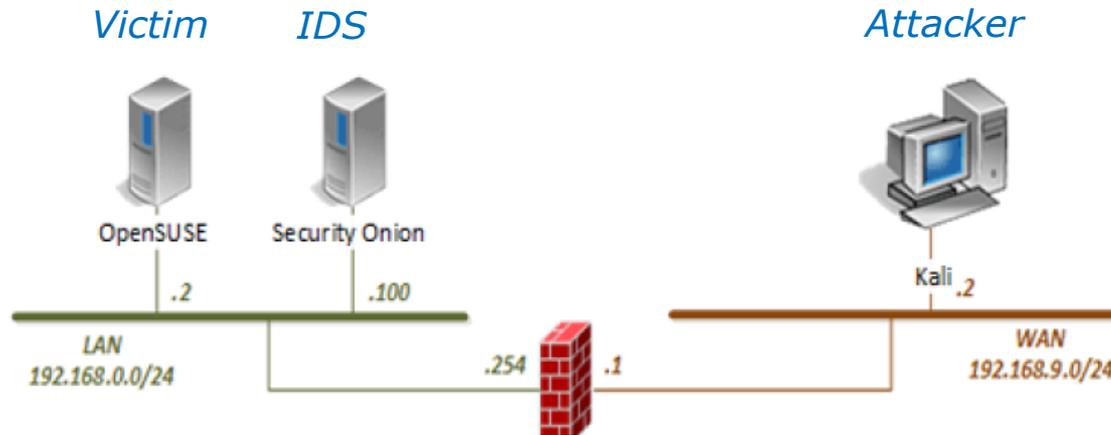
**ETHICAL HACKING  
LAB SERIES**

**Lab 16: Evading IDS**

Material in this Lab Aligns to the Following Certification Domains/Objectives
Certified Ethical Hacking (CEH) Domain
16: Evading IDS, Firewalls and Honey pots

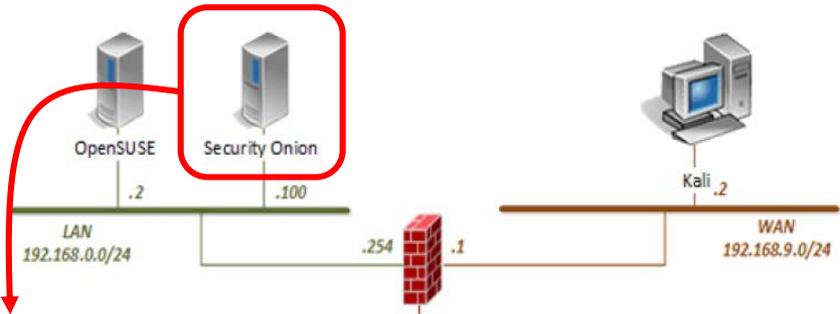
**Document Version: 2016-03-09**

*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



**Squert**

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort
RT	9	ndg-virtu...	3.228	2015-12-21 16:27:08	192.168.9.2	44229	192.168.0.2	1433
RT	8	ndg-virtu...	3.229	2015-12-21 16:27:08	192.168.9.2	44229	192.168.0.2	5432
RT	10	ndg-virtu...	3.224	2i		44229	192.168.0.2	3306
RT	1	ndg-virtu...	4.61	2i		54663	192.168.0.2	80
RT	1	ndg-virtu...	3.246	2i		80	192.168.0.2	54907
RT	2	ndg-virtu...	4.74	2i		59433	192.168.9.2	80
RT	1	ndg-virtu...	3.278	2015-12-30 18:21:19	192.168.9.20	63653	192.168.0.2	5910
RT	1	ndg-virtu...	3.276	2015-12-30 18:21:19	192.168.9.20	63653	192.168.0.2	5800
RT	1	ndg-virtu...	3.274	2015-12-30 18:21:19	192.168.9.20	63653	192.168.0.2	1521

**Sguil**

**Snorby**

*ndg or ndg@ndg.com  
password123*

# Download nmap cheat sheet

### Scripting Engine

```
--c Run default scripts
--script=<scriptname>
<scriptcategory>|<scriptid>...
Run individual or groups of scripts
--script-args=<name1=value1,...>
Use the list of script arguments
--script-updateads
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, SSH, IM, NNTP, VNC, etc.
- default:** Scripts run automatically when -c or -i are used.
- discovery:** Try to learn more information about target hosts through public sources of information, SNMP, directory services, and more.
- den:** 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.
- features:** Test unexpected input in network protocol fields.
- intrusive:** May crash target, consume excessive resources, or otherwise impact target machines in a multitude of fashions.
- 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.
- wait:** 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=mbusname=<mbusname>, smbpass=<password>[, confile=<confile>] -p445 -<hosts>
```

### Nmap Cheat Sheet v1.0

POCKET REFERENCE GUIDE  
by SANS INSTITUTE

#### Basic Syntax

```
$ nmap [ScanType] [Options] [target]
```

#### Target Specification

```
IPv4 address: 192.168.1.1
IPv6 address: aaab::cdd:1::ff:eth0
Host name: www.target.tgt
IP address range: 192.168.0-255.0-255
CIDR block: 192.168.0/24
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
-p{0,1,3,0,110,720-445} Mix TCP and UDP
-iF Scan locally (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

```
-n Don't probe (assume all hosts are up)
-PB Default probe (TCP 80, 445 & ICMP)
--psort{lis} Check whether targets are up by probing TCP ports
--PE Use ICMP Echo Request
--PP Use ICMP Timestamp Request
--PR 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 URGACKPSHSTSYNFIN 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 <numsec> Send packets no slower than <number> per second
--max-rate <numsec> 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

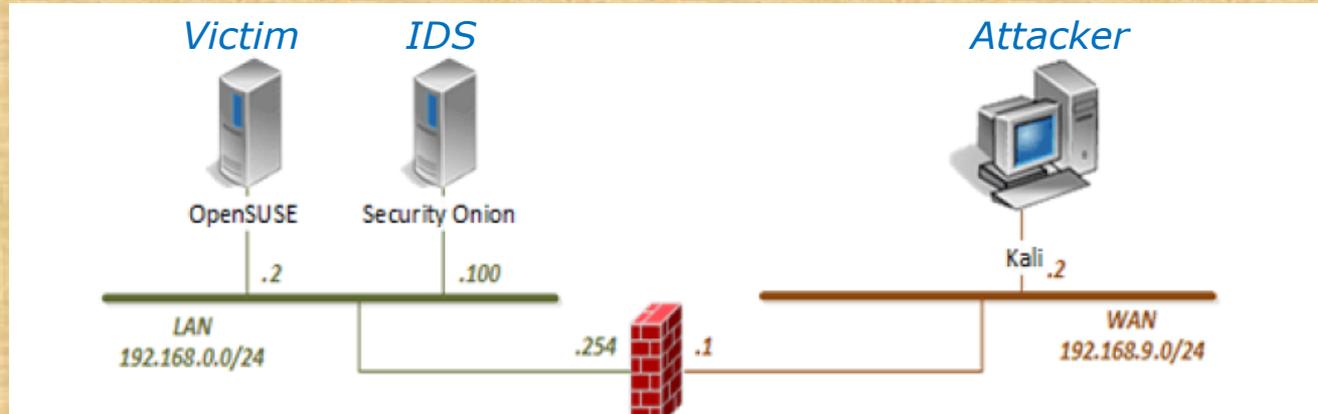
```
-n Disable reverse IP address lookups
-6 Use IPv6 only
-A Use several features, including OS Detection, Version Detection, Script Scanning (default), and traceroute
--reason Display reason Nmap thinks port is open, closed, or filtered
```

# Browse to the nmap Firewall/IDS Evasion Page

The screenshot shows a web browser window with the URL <https://nmap.org/book/man-bypass-firewalls-ids.html>. The page features a dark blue header with the Nmap logo and navigation links. The main content area is titled "Nmap Network Scanning" and "Firewall/IDS Evasion and Spoofing". Below this, it displays "Chapter 15. Nmap Reference Guide" and the specific page title "Firewall/IDS Evasion and Spoofing". The text discusses the history of network security, the challenges of mapping networks, and the use of Nmap for evading firewalls and IDS. A sidebar on the left contains various navigation options like "Nmap Security Scanner", "Security Lists", and "Security Tools".

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

## Test IDS with regular Nmap scan



**[Kali] nmap 192.168.0.2**

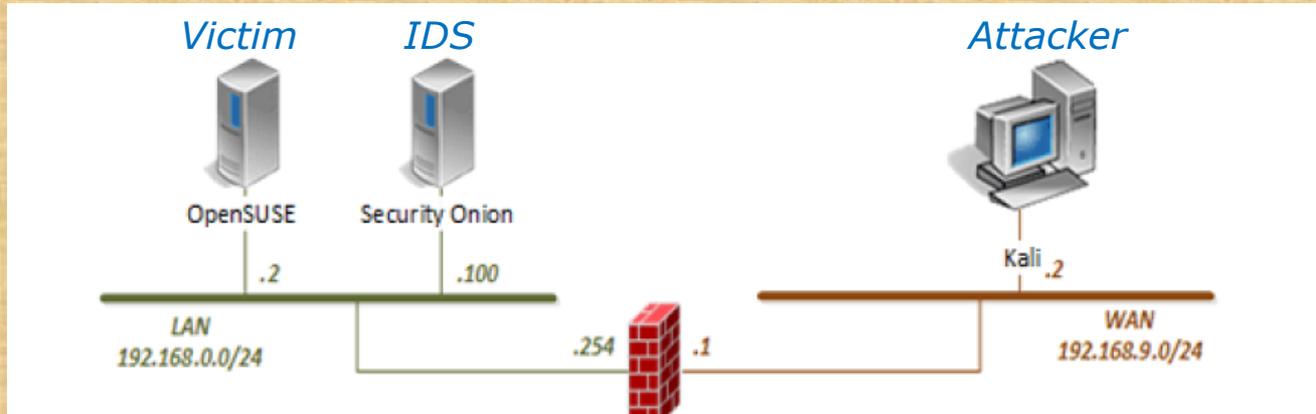
Which tool(s) recorded the scan?

- Snorby
- Squert
- Sguil

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

*Put your answer in the chat window*

## Test IDS with fragmented scan



**[Kali] nmap -f 192.168.0.2**

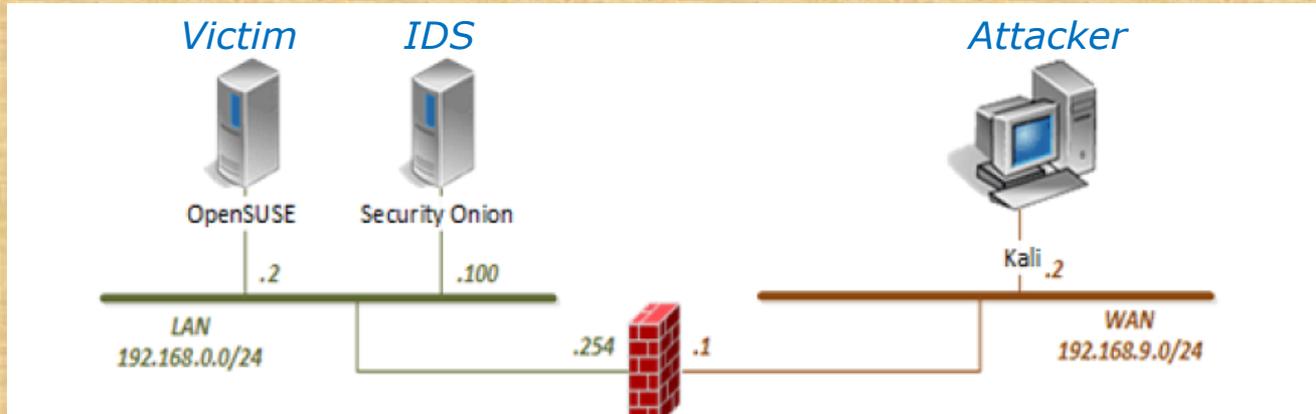
Which tool(s) recorded the scan?

- Snorby
- Squert
- Sguil

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

*Put your answer in the chat window*

## Test IDS with small MTU scan



*Maximum transmission unit must be a multiple of 8*

**[Kali] nmap --mtu 8 192.168.0.2**

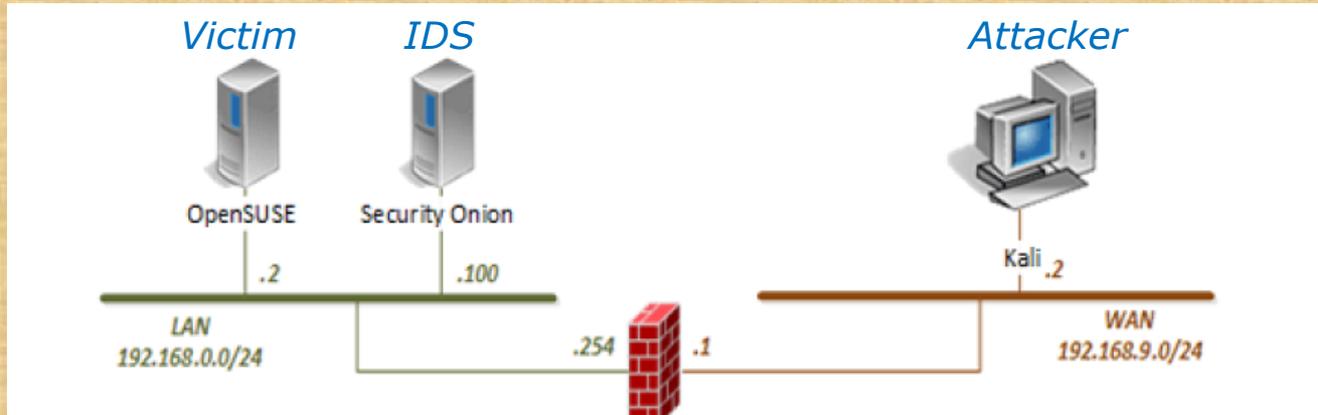
Which tool(s) recorded the scan?

- Snorby
- Squert
- Sguil

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

*Put your answer in the chat window*

## 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**

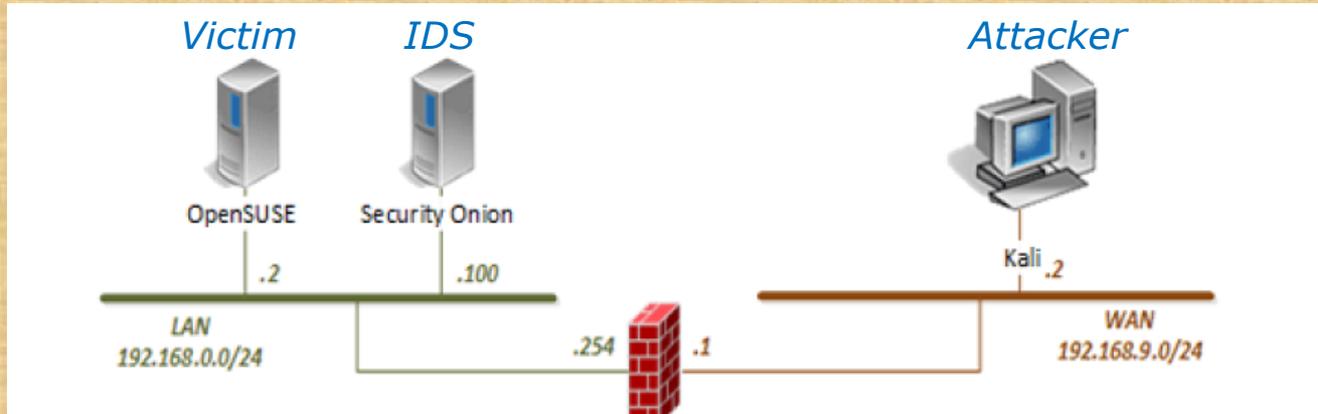
Which tool(s) recorded the scan?

- 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 -spooof-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>

The screenshot shows the Google Drive interface. At the top, there is a search bar and a navigation breadcrumb: "My Drive > CIS 76 Ethical Hacking > CIS 76 Fall 2017 Project Folder". Below the breadcrumb, there is a table of files:

Name ↑	Owner	Last modified
README	me	Oct 29, 2017
Simms-EternalHotdog-v1.1	me	Oct 29, 2017

On the left side of the interface, there is a sidebar with navigation options: My Drive, Shared with me, Recent, Google Photos, Starred, and Trash. At the bottom of the sidebar, it indicates "18 GB used".

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

# Assignment







# Wrap up

Next Class is the Final Exam (Test #3)

*Tuesday 4:00 PM*

Test #3  
Five Posts  
Extra credit labs



# Backup