Rich's lesson module checklist

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

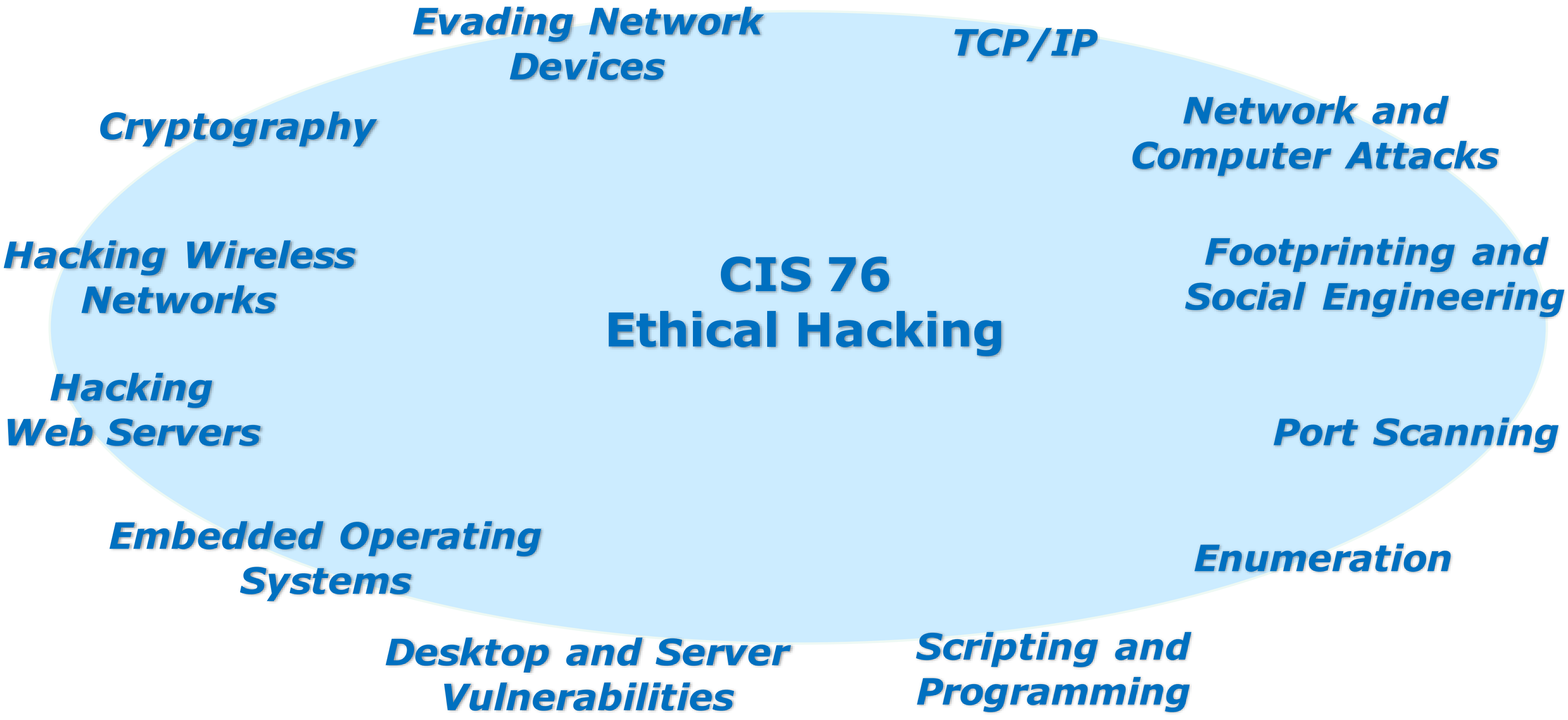
- □ Flash cards
- □ Properties
- □ Page numbers
- □ 1st minute quiz
- □ Web Calendar summary
- □ Web book pages
- □ Commands

- □ Practice Test #3 tested and ready to go

- □ 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 12/6/2016



Evading Network Devices

TCP/IP

Cryptography

Network and Computer Attacks

Hacking Wireless Networks

CIS 76
Ethical Hacking

Footprinting and Social Engineering

Hacking Web Servers

Port Scanning

Embedded Operating Systems

Enumeration

Desktop and Server Vulnerabilities

Scripting and Programming

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

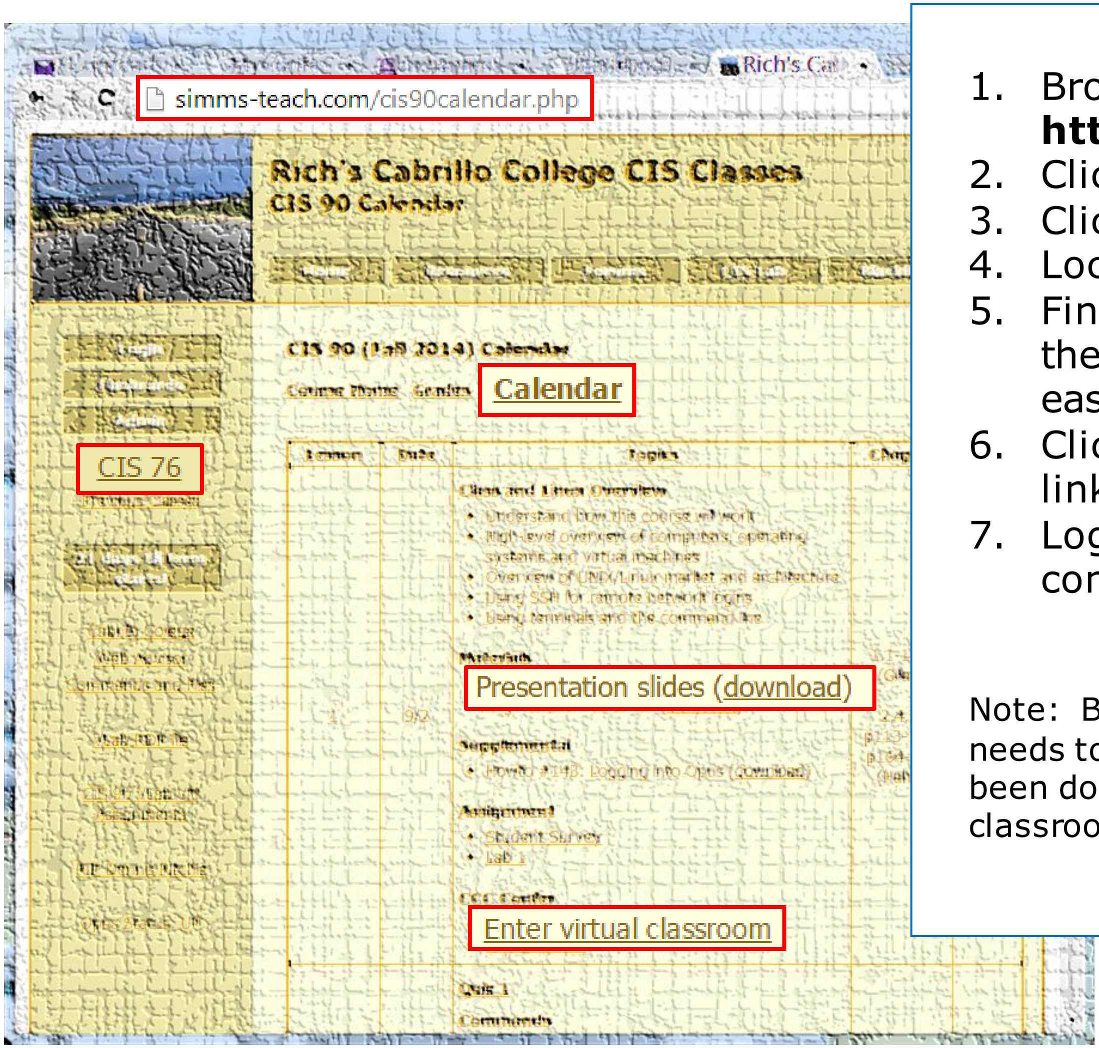
Rich Simms

- 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

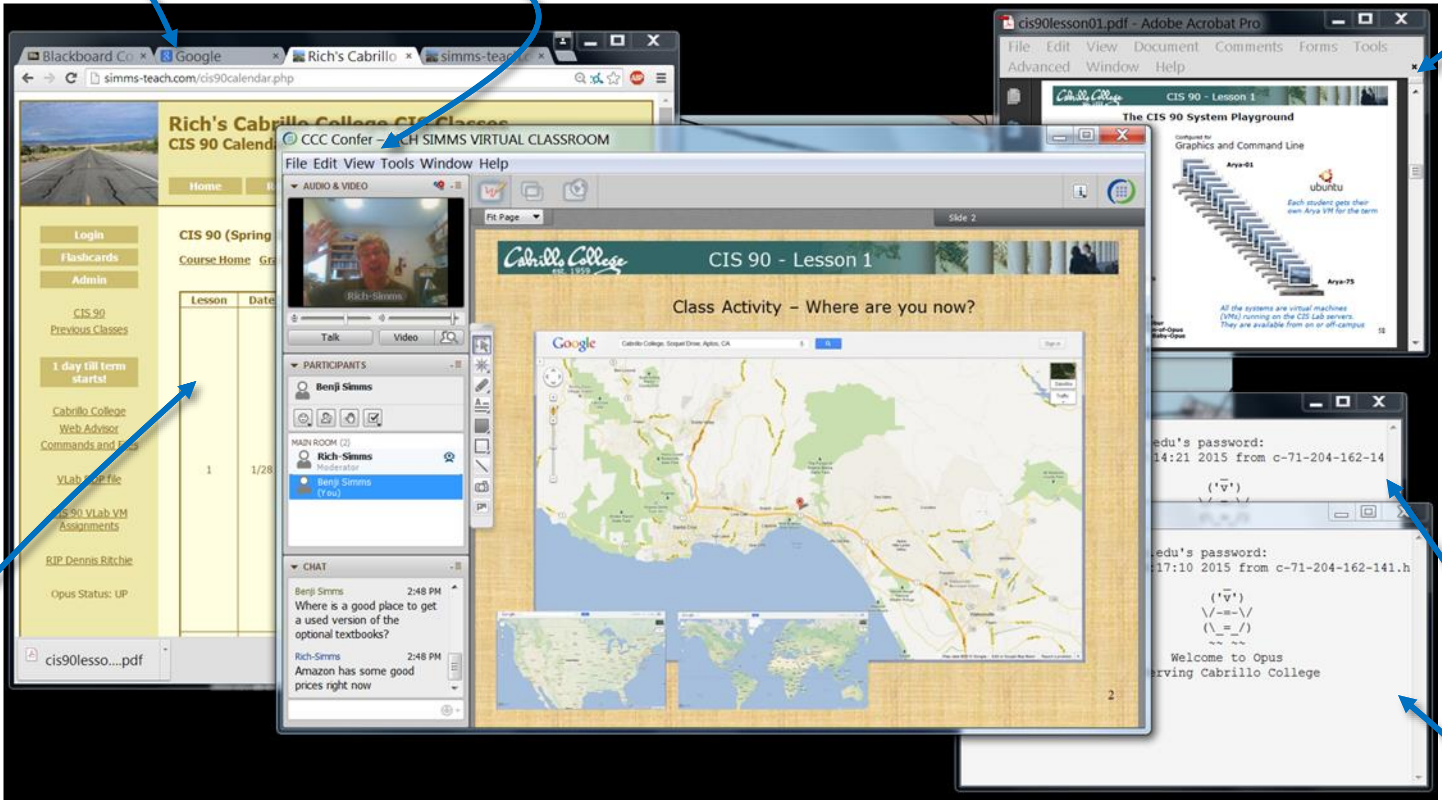

simms-teach.com/cis90calendar.php
Rich's Cabrillo College CIS Classes
CIS 90 Calendar
Calendar
CIS 76
Presentation slides (download)
Enter virtual classroom

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

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

Student checklist for suggested screen layout

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


Blackboard Co
Google
Rich's Cabrillo
simms-teach
simms-teach.com/cis90calendar.php
Rich's Cabrillo College CIS Classes
CIS 90 Calend
Home
Login
Flashcards
Admin
CIS 90 (Spring
Course Home
CIS 90
Previous Classes
1 day till term starts!
Cabrillo College
Web Advisor
Commands and Files
VLab RDP file
CIS 90 VLab VM Assignments
RIP Dennis Ritchie
Opus Status: UP
Lesson
Date
1
1/28
cis90lesso....pdf
CCC Confer – RICH SIMMS VIRTUAL CLASSROOM
File Edit View Tools Window Help
AUDIO & VIDEO
Rich-Simms
Talk
Video
PARTICIPANTS
Benji Simms
MAIN ROOM (2)
Rich-Simms
Moderator
Benji Simms
(You)
CHAT
Fit Page
Slide 2
CIS 90 - Lesson 1
Class Activity – Where are you now?
Google
Cabrillo College, Soquel Drive, Aptos, CA
2
cis90lesson01.pdf - Adobe Acrobat Pro
File Edit View Document Comments Forms Tools Advanced Window Help
CIS 90 - Lesson 1
The CIS 90 System Playground
Graphics and Command Line
Arya-01
ubuntu
Each student gets their own Arya VM for the term
Arya-75
All the systems are virtual machines (VMs) running on the CIS Lab servers. They are available from on or off-campus

Benji Simms 2:48 PM
Where is a good place to get a used version of the optional textbooks?

Rich-Simms 2:48 PM
Amazon has some good prices right now

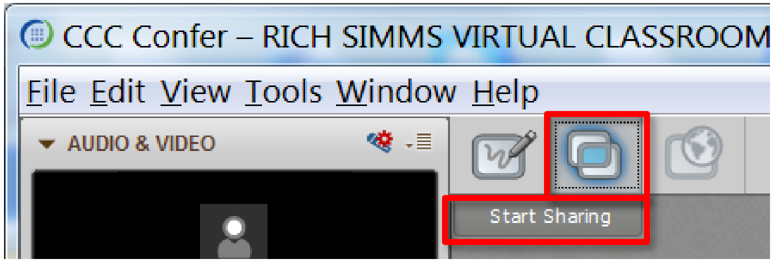
```
edu's password:
14:21 2015 from c-71-204-162-14
    ('v')
```

```
edu's password:
17:10 2015 from c-71-204-162-141.h
      ('v')
     \/-=-\/
     (\_=_/)
      ~~ ~~
   Welcome to Opus
rving Cabrillo College
```

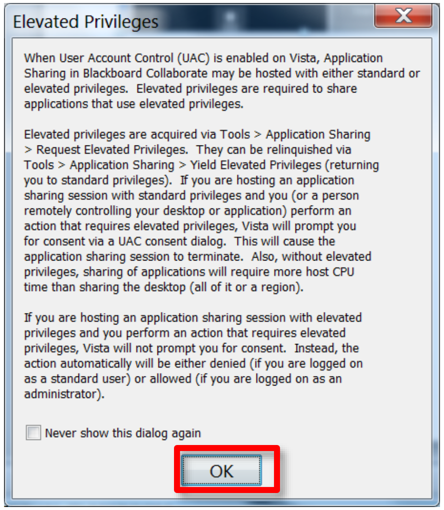
- ❑ CIS 76 website Calendar page
- ❑ One or more login sessions to Opus

Student checklist for sharing desktop with classmates

1) Instructor gives you sharing privileges.


CCC Confer – RICH SIMMS VIRTUAL CLASSROOM
File Edit View Tools Window Help
AUDIO & VIDEO
Start Sharing

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


Elevated Privileges

When User Account Control (UAC) is enabled on Vista, Application Sharing in Blackboard Collaborate may be hosted with either standard or elevated privileges. Elevated privileges are required to share applications that use elevated privileges.

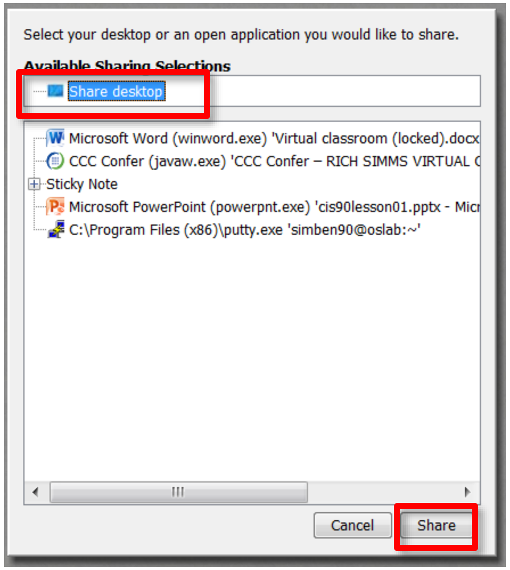
Elevated privileges are acquired via Tools > Application Sharing > Request Elevated Privileges. They can be relinquished via Tools > Application Sharing > Yield Elevated Privileges (returning you to standard privileges). If you are hosting an application sharing session with standard privileges and you (or a person remotely controlling your desktop or application) perform an action that requires elevated privileges, Vista will prompt you for consent via a UAC consent dialog. This will cause the application sharing session to terminate. Also, without elevated privileges, sharing of applications will require more host CPU time than sharing the desktop (all of it or a region).

If you are hosting an application sharing session with elevated privileges and you perform an action that requires elevated privileges, Vista will not prompt you for consent. Instead, the action automatically will be either denied (if you are logged on as a standard user) or allowed (if you are logged on as an administrator).

□ Never show this dialog again

OK

3) Click OK button.


Select your desktop or an open application you would like to share.

Available Sharing Selections

Share desktop

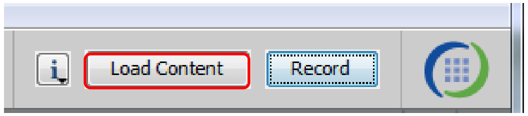
Microsoft Word (winword.exe) 'Virtual classroom (locked).docx
CCC Confer (javaw.exe) 'CCC Confer – RICH SIMMS VIRTUAL C
Sticky Note
Microsoft PowerPoint (powerpnt.exe) 'cis90lesson01.pptx - Micr
C:\Program Files (x86)\putty.exe 'simben90@oslab:~'

Cancel Share

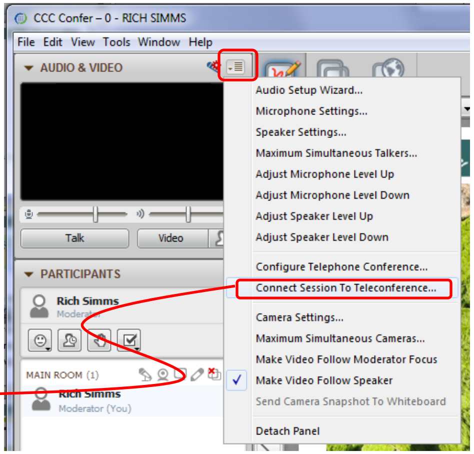
4) Select "Share desktop" and click Share button.

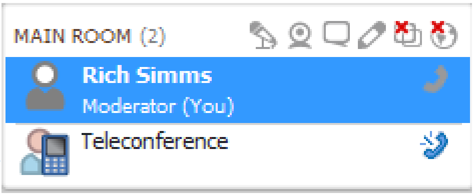
Rich's CCC Confer checklist - setup

[ ] Preload White Board



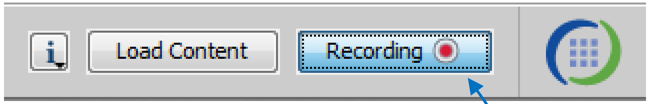
[ ] Connect session to Teleconference


CCC Confer – 0 - RICH SIMMS
File Edit View Tools Window Help
AUDIO & VIDEO
Audio Setup Wizard...
Microphone Settings...
Speaker Settings...
Maximum Simultaneous Talkers...
Adjust Microphone Level Up
Adjust Microphone Level Down
Adjust Speaker Level Up
Adjust Speaker Level Down
Configure Telephone Conference...
Connect Session To Teleconference...
Camera Settings...
Maximum Simultaneous Cameras...
Make Video Follow Moderator Focus
✓ Make Video Follow Speaker
Send Camera Snapshot To Whiteboard
Detach Panel
Talk
Video
PARTICIPANTS
Rich Simms
MAIN ROOM (1)
Rich Simms
Moderator (You)

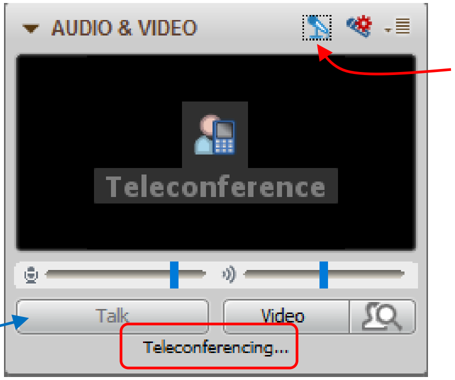


Session now connected to teleconference

[ ] Is recording on?



Red dot means recording

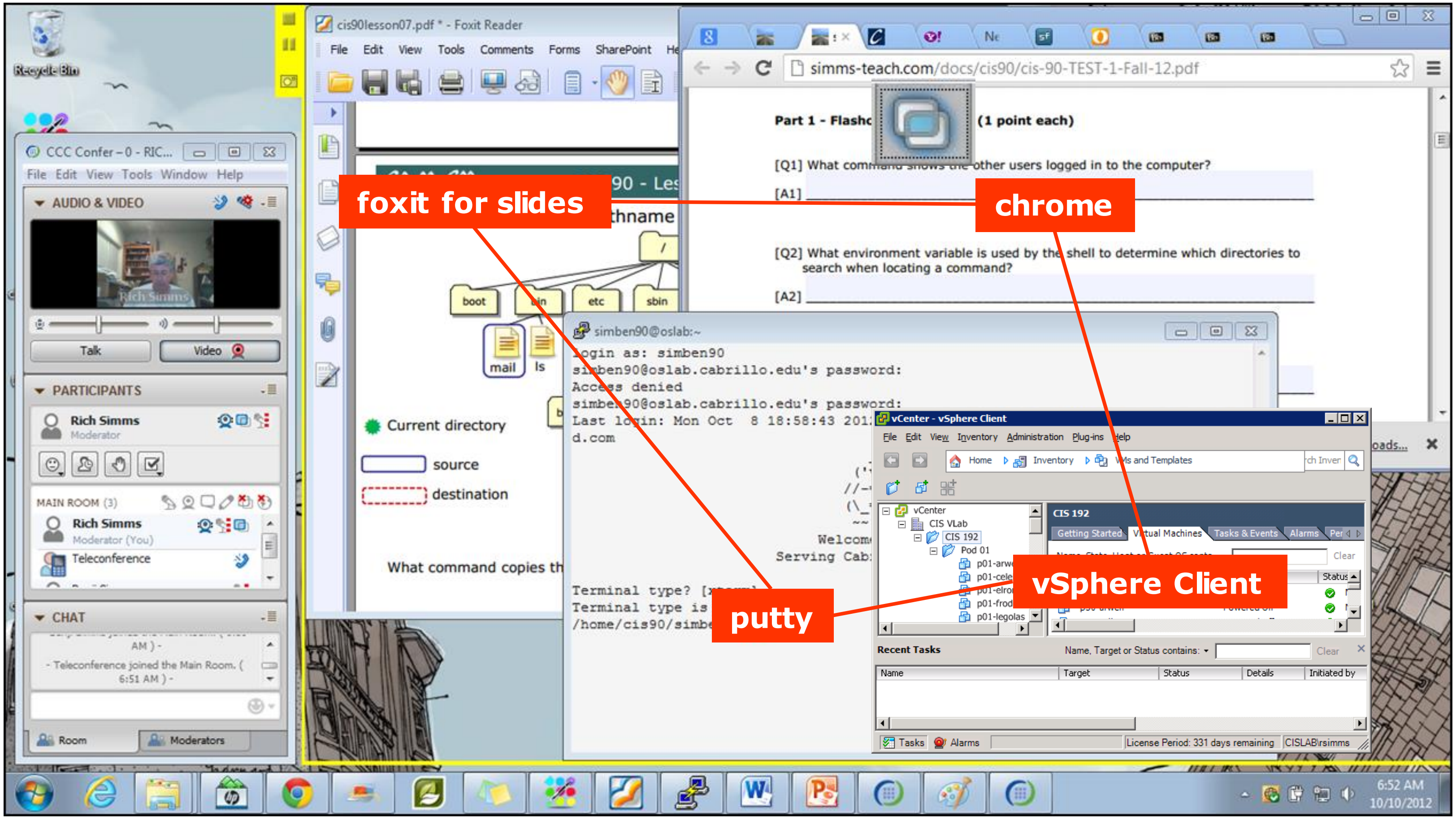


Should change from phone handset icon to little Microphone icon and the Teleconferencing ... message displayed

[ ] Use teleconferencing, not mic

Should be grayed out

Rich's CCC Confer checklist - screen layout



foxit for slides

chrome

putty

vSphere Client

simms-teach.com/docs/cis90/cis-90-TEST-1-Fall-12.pdf

Part 1 - Flashc **(1 point each)**

[Q1] What command shows the other users logged in to the computer?

[A1] ______________________________

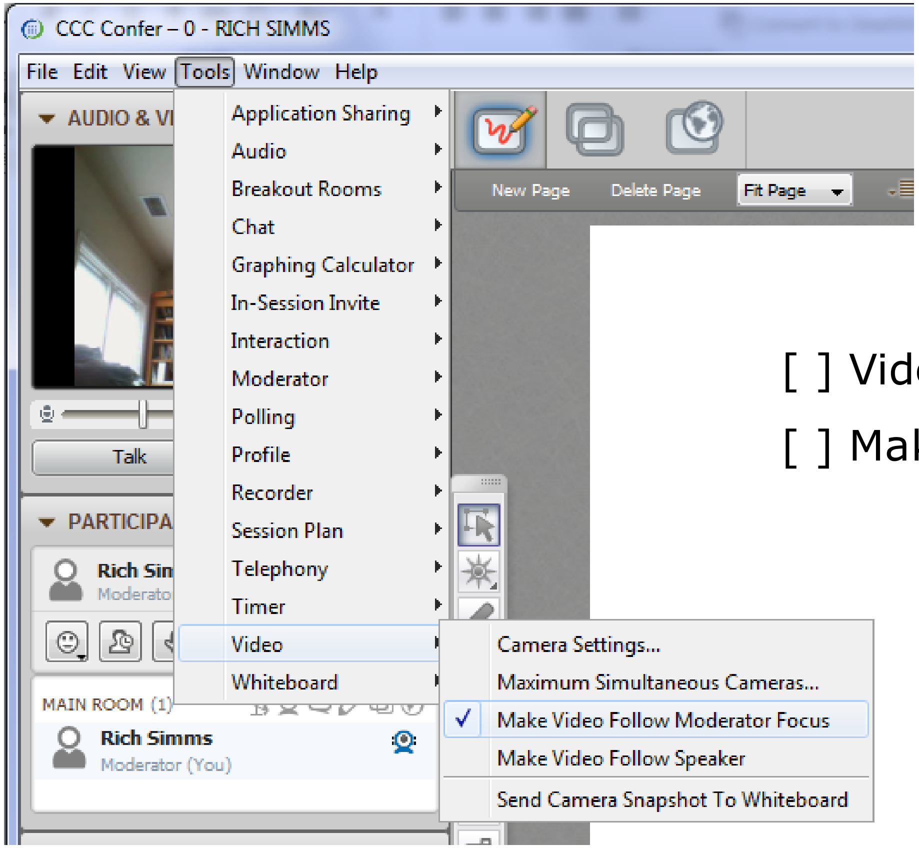
[Q2] What environment variable is used by the shell to determine which directories to search when locating a command?

[A2] ______________________________

```
login as: simben90
simben90@oslab.cabrillo.edu's password:
Access denied
simben90@oslab.cabrillo.edu's password:
Last login: Mon Oct  8 18:58:43 201
d.com

Welcom
Serving Cab

Terminal type? [x
Terminal type is
/home/cis90/simbe
```

[ ] layout and share apps

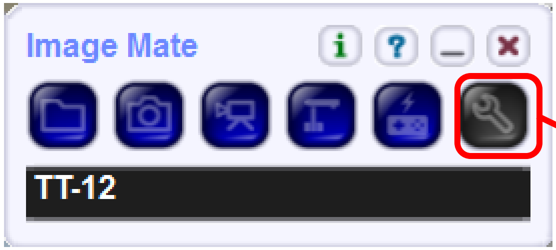
Rich's CCC Confer checklist - webcam setup

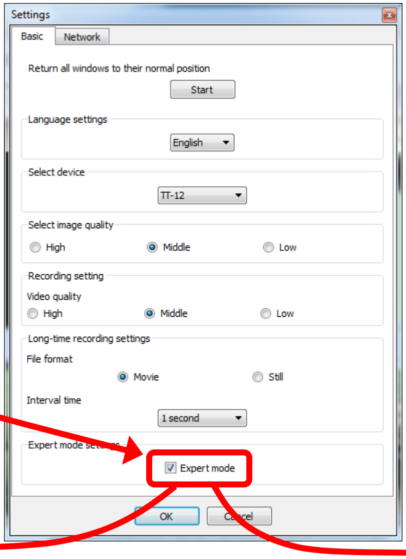


[ ] Video (webcam)

[ ] Make Video Follow Moderator Focus

Rich's CCC Confer checklist - Elmo





Settings

Basic | Network

Return all windows to their normal position

Start

Language settings: English

Select device: TT-12

Select image quality: ○ High ● Middle ○ Low

Recording setting

Video quality: ○ High ● Middle ○ Low

Long-time recording settings

File format: ● Movie ○ Still

Interval time: 1 second

Expert mode settings

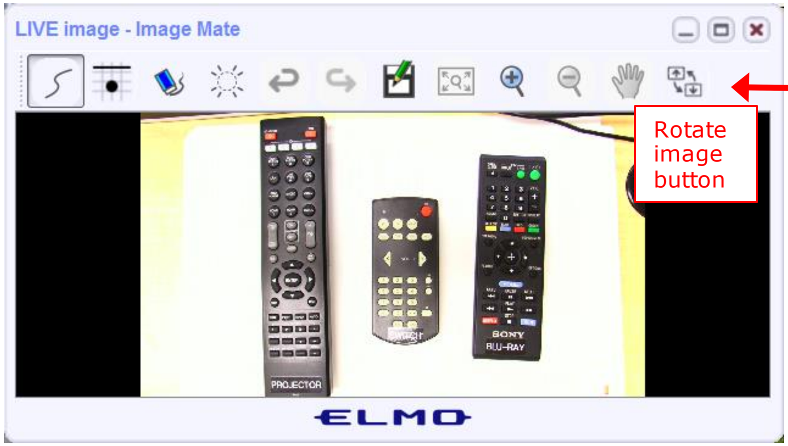
☑ Expert mode

OK | Cancel

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

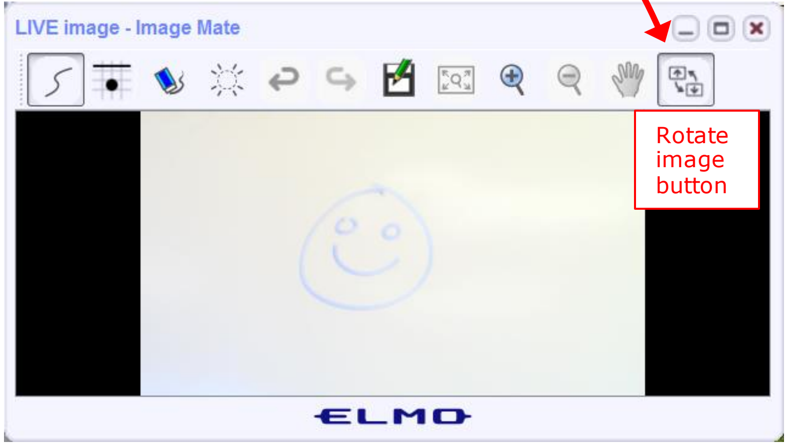
Quite interesting that they consider you to be an "expert" in order to use this button!

Elmo rotated down to view side table



Rotate image button

Elmo rotated up to view white board



Rotate image button

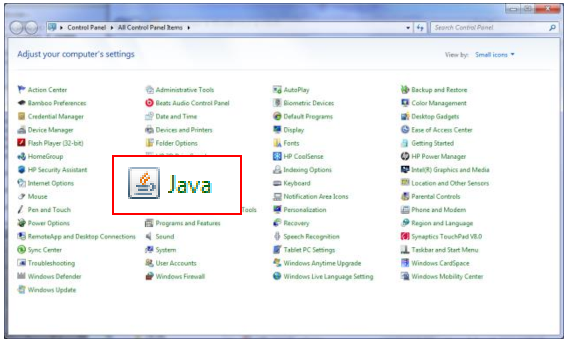
Run and share the Image Mate program just as you would any other app with CCC Confer

Rich's CCC Confer checklist - universal fixes

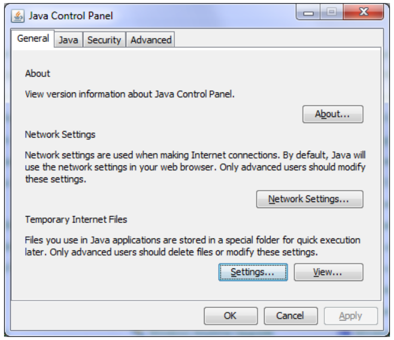
Universal Fix for CCC Confer:

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...



About

View version information about Java Control Panel.

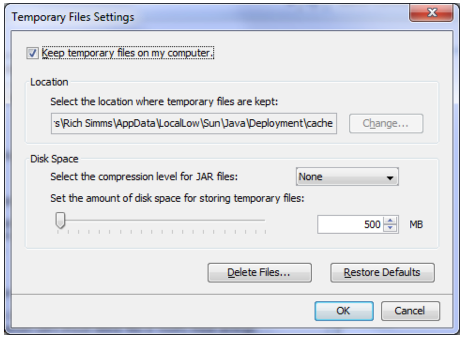
Network Settings

Network settings are used when making Internet connections. By default, Java will use the network settings in your web browser. Only advanced users should modify these settings.

Temporary Internet Files

Files you use in Java applications are stored in a special folder for quick execution later. Only advanced users should delete files or modify these settings.

500MB cache size



☑ Keep temporary files on my computer.

Location

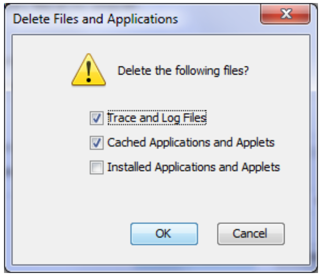
Select the location where temporary files are kept: s\Rich Simms\AppData\LocalLow\Sun\Java\Deployment\cache

Disk Space

Select the compression level for JAR files: None

Set the amount of disk space for storing temporary files: 500 MB

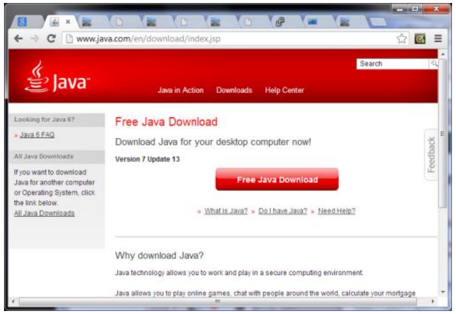
Delete these



Delete the following files?

☑ Trace and Log Files
☑ Cached Applications and Applets
□ Installed Applications and Applets

Google Java download



If you want to download Java for another computer or Operating System, click the link below.
All Java Downloads

Free Java Download

Download Java for your desktop computer now!

Version 7 Update 13

Why download Java?

Java technology allows you to work and play in a secure computing environment.

Java allows you to play online games, chat with people around the world, calculate your mortgage

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**

Ryan

Jordan

Takashi

Michael W.

Sean

Tim

Luis

Brian

Carter

Dave R.

David H.

Roberto

Nelli

Mike C.

Deryck

Alex

Thomas

Wes

Jennifer

Marcos

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

- 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

"Avalanche" (crimeware-as-a-service)

https://www.us-cert.gov/ncas/alerts/TA16-336A

http://arstechnica.com/security/2016/12/legal-raids-in-five-countries-seize-botnet-servers-sinkhole-800000-domains/

http://searchsecurity.techtarget.com/news/450404086/EU-US-authorities-take-down-Avalanche-global-crimeware-network

- Authorities for 30 countries have dismantled Avalanche.
- Four year investigation.
- Avalanche used as many as 500,000 infected computers world-wide.
- Cyber criminals used Avalanche botnet infrastructure to distribute malware and target over 40 financial institutions.
- Victim's lost sensitive personal information.
- Victim's compromised systems used in the botnet.
- Used "money mule" schemes to transport or launder stolen money.
- Used fast flux DNS techniques (changing DNS records frequently) to hide from authorities.

Recent news

Tor network compromised

http://www.techspot.com/news/57583-hackers-have-compromised-the-once-anonymous-tor-network.html

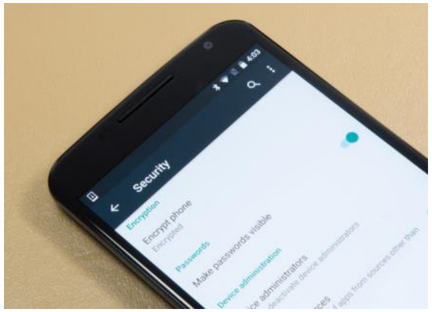
Thanks Marcos

- Tor allows users to anonymously browse the Internet.
- Unknown attackers gathered information on sites users visited.
- Not likely to have seen what pages were loaded.
- They monitored Tor traffic relays to gather information.
- They introduced hundreds of their own traffic relays into the network.
- Tor project suspects attackers were researchers in the CERT department at Carnegie Mellon.

Recent news

Android malware "Gooligan" compromises a million Google accounts

http://arstechnica.com/security/2016/11/1-million-android-accounts-compromised-by-android-malware-called-gooligan/



- A family of Android based malware that install Adware and installs apps from Google Play to raise their reputation.
- Named "Gooligan" by researchers at Check Point Software Technologies.
- Discovered 86 infected apps in third party stores.
- The malware could also get installed by malicious links in phishing messages.
- The malware uses rooting to gain privileged access.
- The rooted phones download additional software to steal Google authentication tokens.
- The tokens can be used to access Gmail, Google Docs, Google Mobile Services, Google Play, Google Drive etc. without a password.

Recent news

Russian bank hacked

http://www.wsj.com/articles/hackers-steal-31-million-from-accounts-at-russian-central-bank-1480701080

https://www.hackread.com/russian-central-bank-hacked-31-mil-gone/

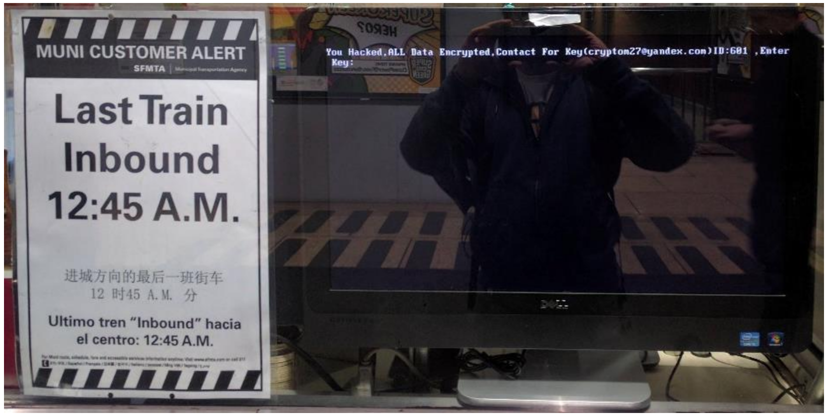
- 2 billion rubles ($31.3 million) was stolen by hackers.
- They attempted stealing 5 billion rubles but thwarted by the bank's intervention.
- A few weeks ago Russian banks experienced a string of DDoS attacks.
- An FSB investigation found the attack was carried out by servers based in the Netherlands.
- In addition the FSB investigation found fake stories were planted on social media, using servers in the Ukraine, attempting to discredit the Russian banking system and that it was close to collapse.

Recent news

San Francisco Muni hit by ransomware

http://arstechnica.com/security/2016/11/san-francisco-transit-ransomware-attacker-likely-used-year-old-java-exploit/

http://arstechnica.com/security/2016/11/san-francisco-muni-hit-by-black-friday-ransomware-attack/



You Hacked,ALL Data Encrypted,Contact For Key(cryptom27@yandex.com)ID:601 ,Enter Key:

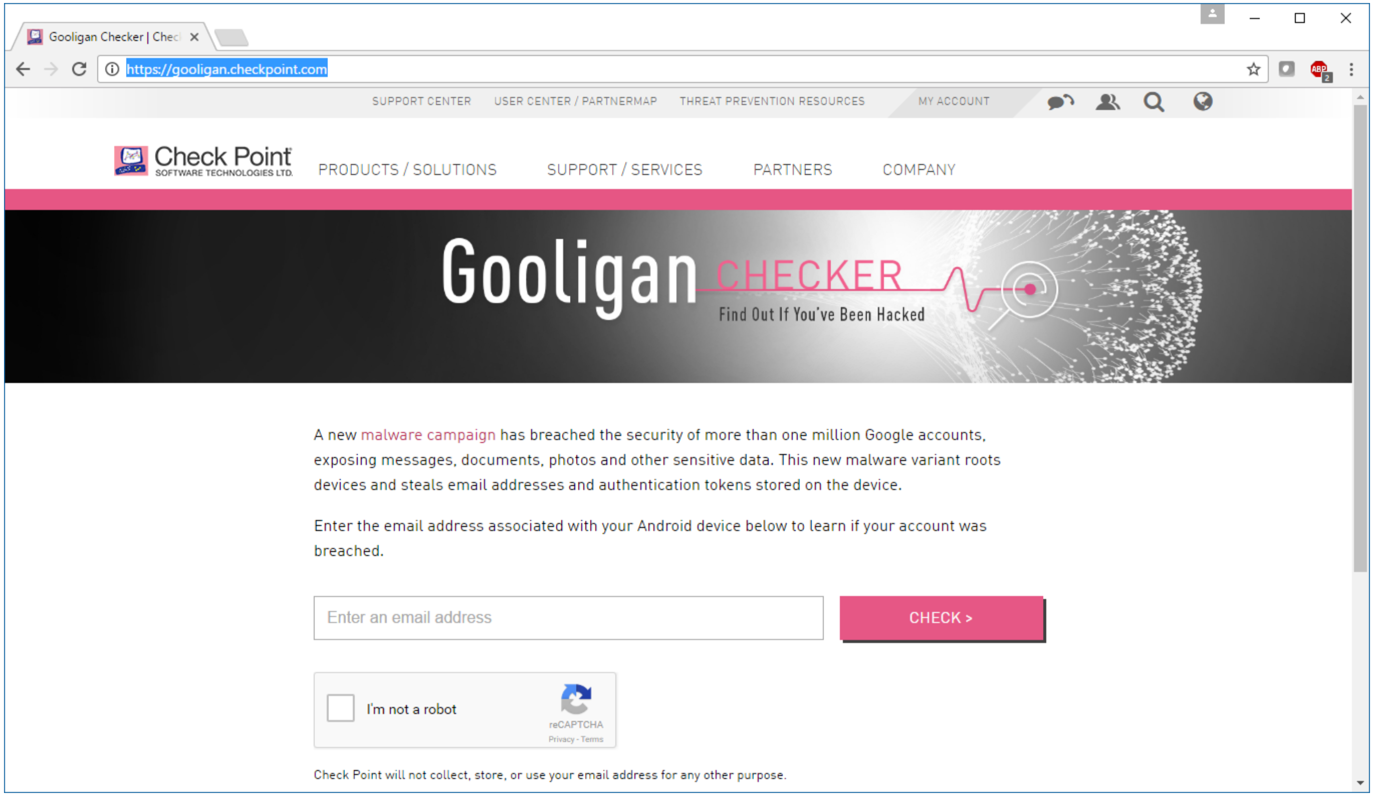
You hacked, all Data Encrypted,Contact For Key(cryptom27@Yandex.com) ID:601 ,EnterKey:

- Attack on Black Friday on the Muni's network took down ticketing machines, servers and agent desktops.
- Hackers demanded 100 bit-coins ($73,000).
- Appears they took advantage of a "deserialization" vulnerability in a Oracle WebLogic server.
- Used malware known as Mamba and HDDCryptor which attacks the victim's network and all the computers on that network.
- It appears the Muni was not specifically targeted but was a target of opportunity in a vulnerability scan.
- Passengers rode for free that day.

Best Practices

Best Practices

Gooligan Checker



A new malware campaign has breached the security of more than one million Google accounts, exposing messages, documents, photos and other sensitive data. This new malware variant roots devices and steals email addresses and authentication tokens stored on the device.

Enter the email address associated with your Android device below to learn if your account was breached.

Enter an email address

CHECK >

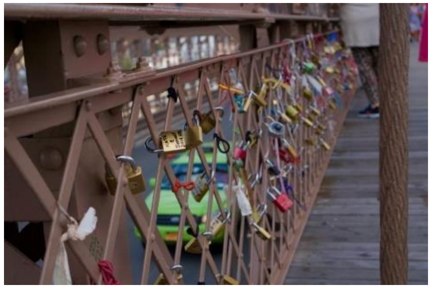
□ I'm not a robot

Check Point will not collect, store, or use your email address for any other purpose.

https://gooligan.checkpoint.com/

Best Practices

Beginners guide to beefing up your online privacy and security



http://arstechnica.com/security/2016/12/a-beginners-guide-to-beefing-up-your-privacy-and-security-online/

- Install updates (especially browser and OS).
- Use strong passwords and passcodes.
- Encrypt your phones and computers.
- Use two-factor authentication.
- Use a password managers (example products, 1Passord and LastPass).
- Encrypt SMS and voice calls (example products, Signal).
- Use VPNs on public Wi-Fi (example services, Private Internet Access).
- Secure end-to-end email (example ProtonMail).
- Delete old emails.
- For more in-depth strategies see EFF's Surveillance Self-Defense page.

https://ssd.eff.org/

Housekeeping

war is not healthy for children and other living things
ICE COLD
Coffee!
You can sleep when you're dead!
LATTE
TOURIST MAP OF THE WORLD
New Z
Sports Blaster
We're Proud To Ser

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 allow me to read it.

2. All four extra credit labs are available (15 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 now.

CIS 76 Project

The lab you create should contain the following sections:

a) Title, your name, date and course number.
b) Overview - short introductory paragraph summarizing the lab.
c) Admonition - a warning to the reader against unauthorized hacking.
d) Requirements - everything needed to create a secure test bed and demonstrate the attack.
e) The vulnerability(ies) - description and history including reference citations.
f) The exploit(s) - description of the exploit and how it works including reference citations.
g) Setup - step-by-step instructions <u>with screen shots</u> demonstrating how to set up the test bed, configure systems and networks including reference citations.
h) Attack - step-by-step instructions <u>with screen shots</u> on how to carry out the attack including reference citations.
i) Prevention - list of preventative measures for preventing the attack including reference citations.
j) Appendix A - List of references for each citation.
k) Appendix B - Test reports you received from classmates that tested your lab.
l) Appendix C - Other classmate’s labs you tested.

Excerpt from the Project document

CIS 76 Project

Grading Rubric (60 points + 30 points extra credit)

Up to 5 points - Professional quality document containing all sections mentioned above.
Up to 3 points - Description and history of vulnerability.
Up to 3 points - Description of exploit and how it works.
Up to 3 points - Document all equipment, software and materials required.
Up to 10 points - Document step-by-step instructions to set up the test bed.
Up to 15 points - Document step-by-step instructions to carry out the attack.
Up to 3 points - List of best practices to prevent future attacks.
Up to 15 points - Testing another student's lab (see below).
Up to 3 points - Presentation and demo to class (10 minutes max).

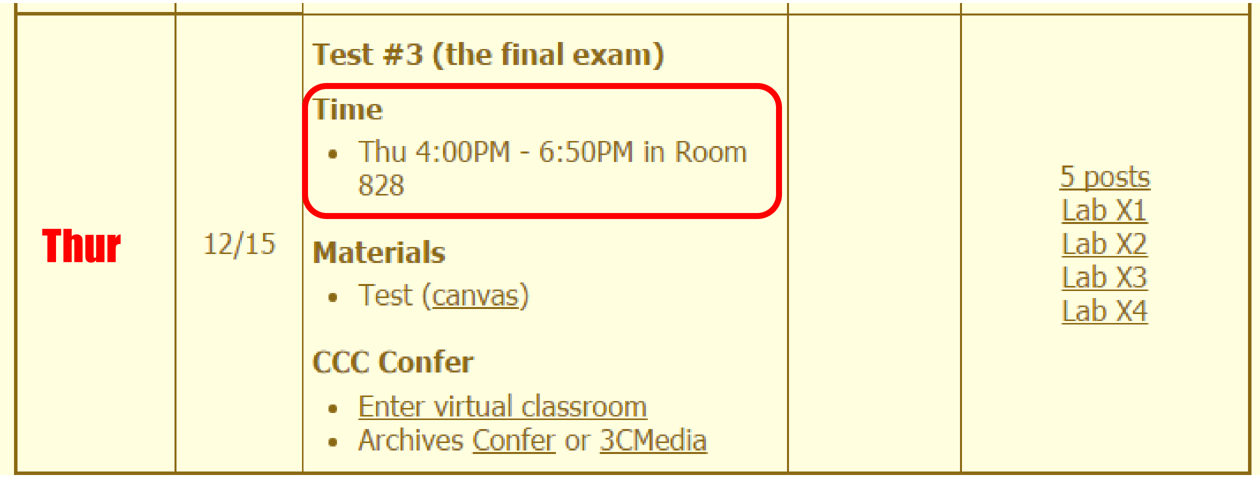
Extra credit (up 30 points) 15 points each for testing additional student labs. You must use the testing spreadsheet above so that all projects get tested equally.

Remember late work is not accepted. If you run out of time submit what you have completed for partial credit.

Excerpt from the Project document

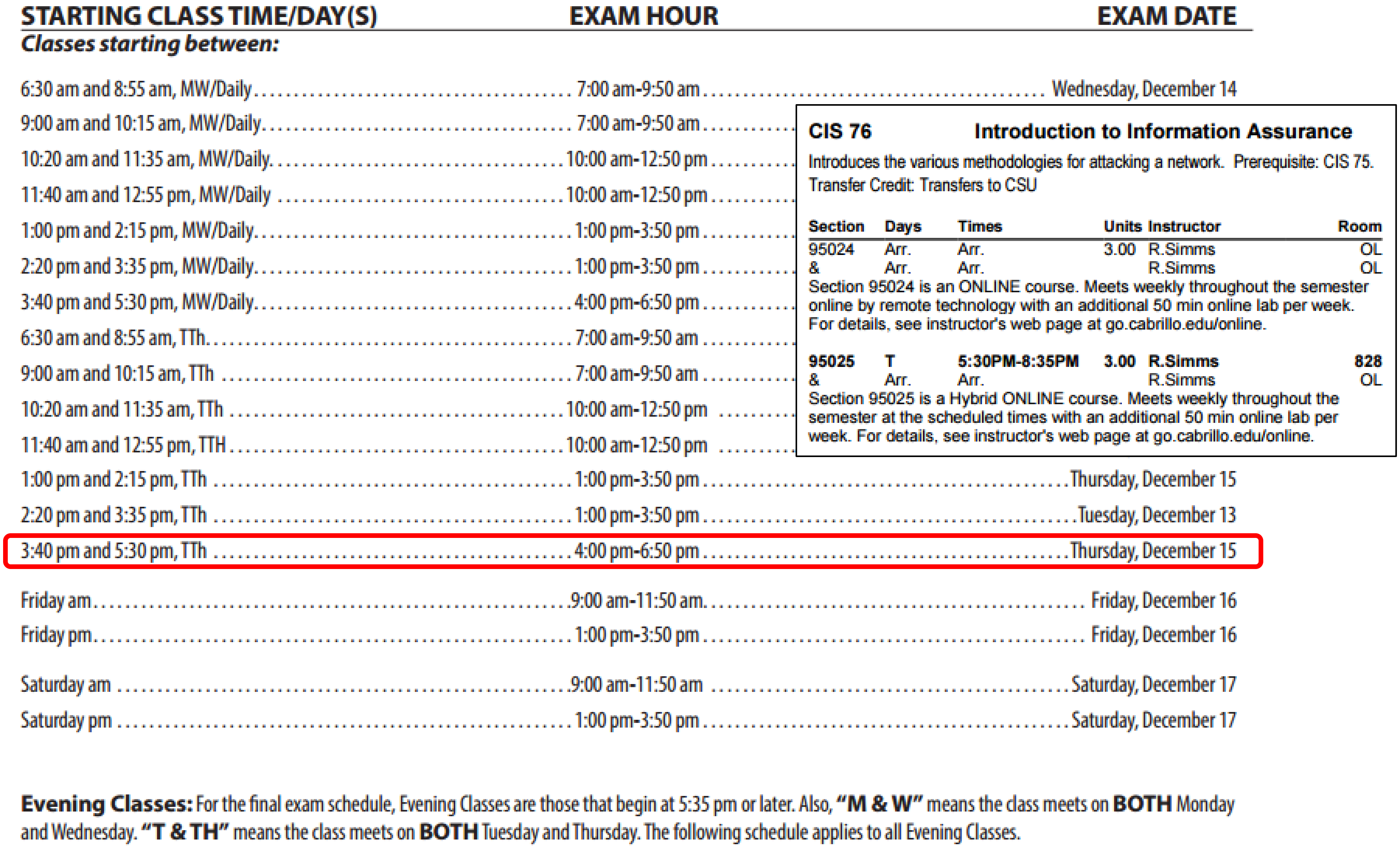
Final Exam

Test #3 (final exam) is THURSDAY Dec 15 4:00PM-6:50PM



Thur	12/15	**Test #3 (the final exam)** **Time** • Thu 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

- 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)



STARTING CLASS TIME/DAY(S) *Classes starting between:*	EXAM HOUR	EXAM DATE
6:30 am and 8:55 am, MW/Daily	7:00 am-9:50 am	Wednesday, December 14
9:00 am and 10:15 am, MW/Daily	7:00 am-9:50 am	
10:20 am and 11:35 am, MW/Daily	10:00 am-12:50 pm	
11:40 am and 12:55 pm, MW/Daily	10:00 am-12:50 pm	
1:00 pm and 2:15 pm, MW/Daily	1:00 pm-3:50 pm	
2:20 pm and 3:35 pm, MW/Daily	1:00 pm-3:50 pm	
3:40 pm and 5:30 pm, MW/Daily	4:00 pm-6:50 pm	
6:30 am and 8:55 am, TTh	7:00 am-9:50 am	
9:00 am and 10:15 am, TTh	7:00 am-9:50 am	
10:20 am and 11:35 am, TTh	10:00 am-12:50 pm	
11:40 am and 12:55 pm, TTH	10:00 am-12:50 pm	
1:00 pm and 2:15 pm, TTh	1:00 pm-3:50 pm	Thursday, December 15
2:20 pm and 3:35 pm, TTh	1:00 pm-3:50 pm	Tuesday, December 13
3:40 pm and 5:30 pm, TTh	4:00 pm-6:50 pm	Thursday, December 15
Friday am	9:00 am-11:50 am.	Friday, December 16
Friday pm	1:00 pm-3:50 pm	Friday, December 16
Saturday am	9:00 am-11:50 am	Saturday, December 17
Saturday pm	1:00 pm-3:50 pm	Saturday, December 17

CIS 76 **Introduction to Information Assurance**

Introduces the various methodologies for attacking a network. Prerequisite: CIS 75.
Transfer Credit: Transfers to CSU

Section	Days	Times	Units	Instructor	Room
95024	Arr.	Arr.	3.00	R.Simms	OL
&	Arr.	Arr.		R.Simms	OL

Section 95024 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.

Section	Days	Times	Units	Instructor	Room
95025	**T**	**5:30PM-8:35PM**	**3.00**	**R.Simms**	**828**
&	Arr.	Arr.		R.Simms	OL

Section 95025 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.

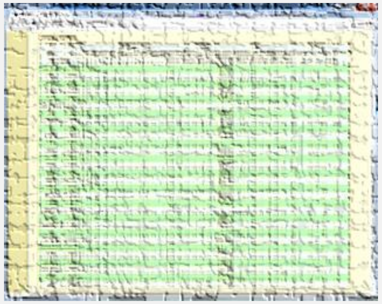
Evening Classes: For the final exam schedule, Evening Classes are those that begin at 5:35 pm or later. Also, **"M & W"** means the class meets on **BOTH** Monday and Wednesday. **"T & TH"** means the class meets on **BOTH** Tuesday and Thursday. The following schedule applies to all Evening Classes.

Where to find your grades

Send me your survey to get your LOR code name.

The CIS 76 website Grades page

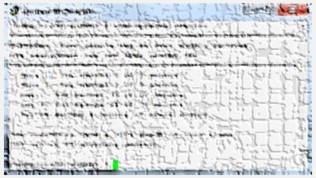
http://simms-teach.com/cis76grades.php



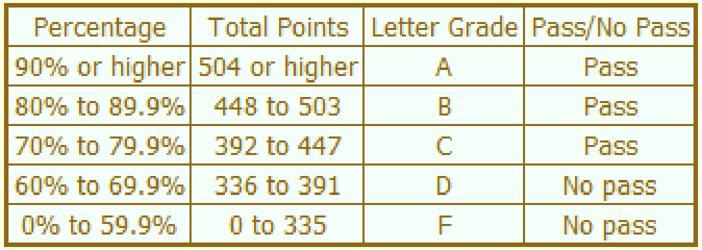
Or check on Opus

`checkgrades` *`codename`*

(where codename is your LOR codename)



Written by Jesse Warren a past CIS 90 Alumnus



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

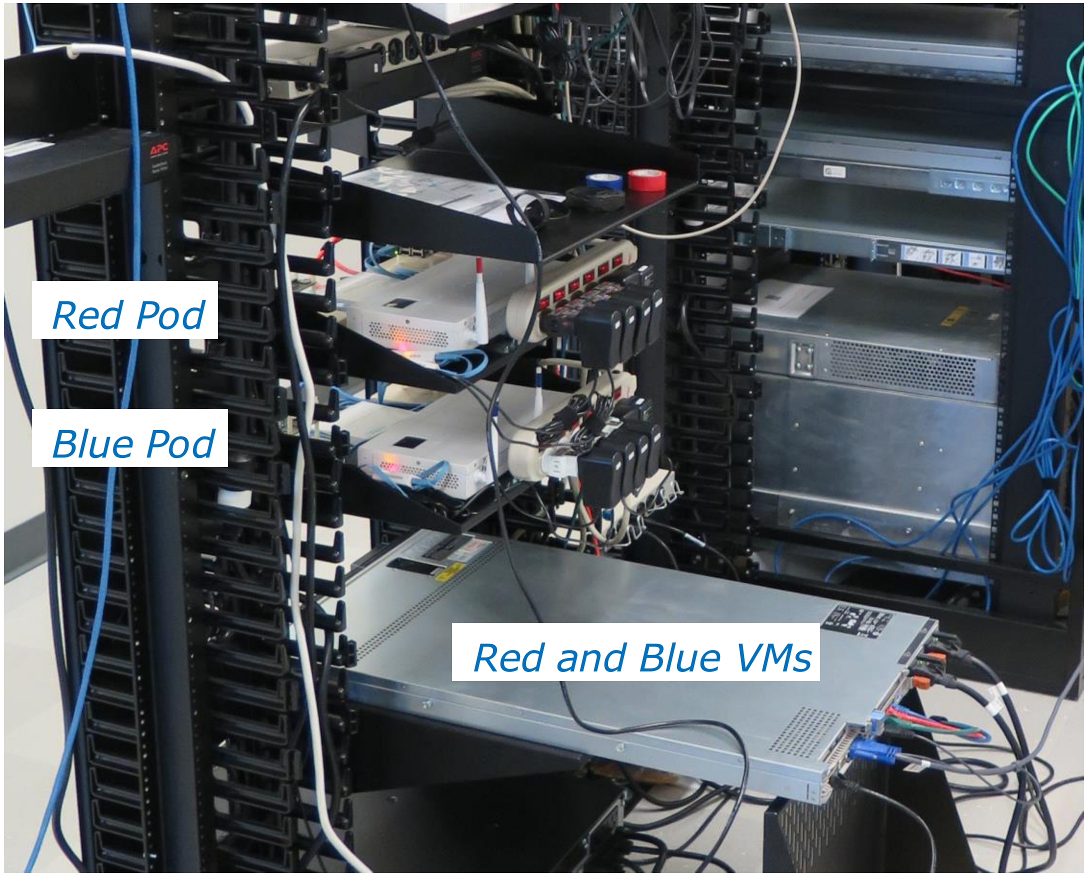
At the end of the term I'll add up all your points and assign you a grade using this table

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**

Red and Blue Teams

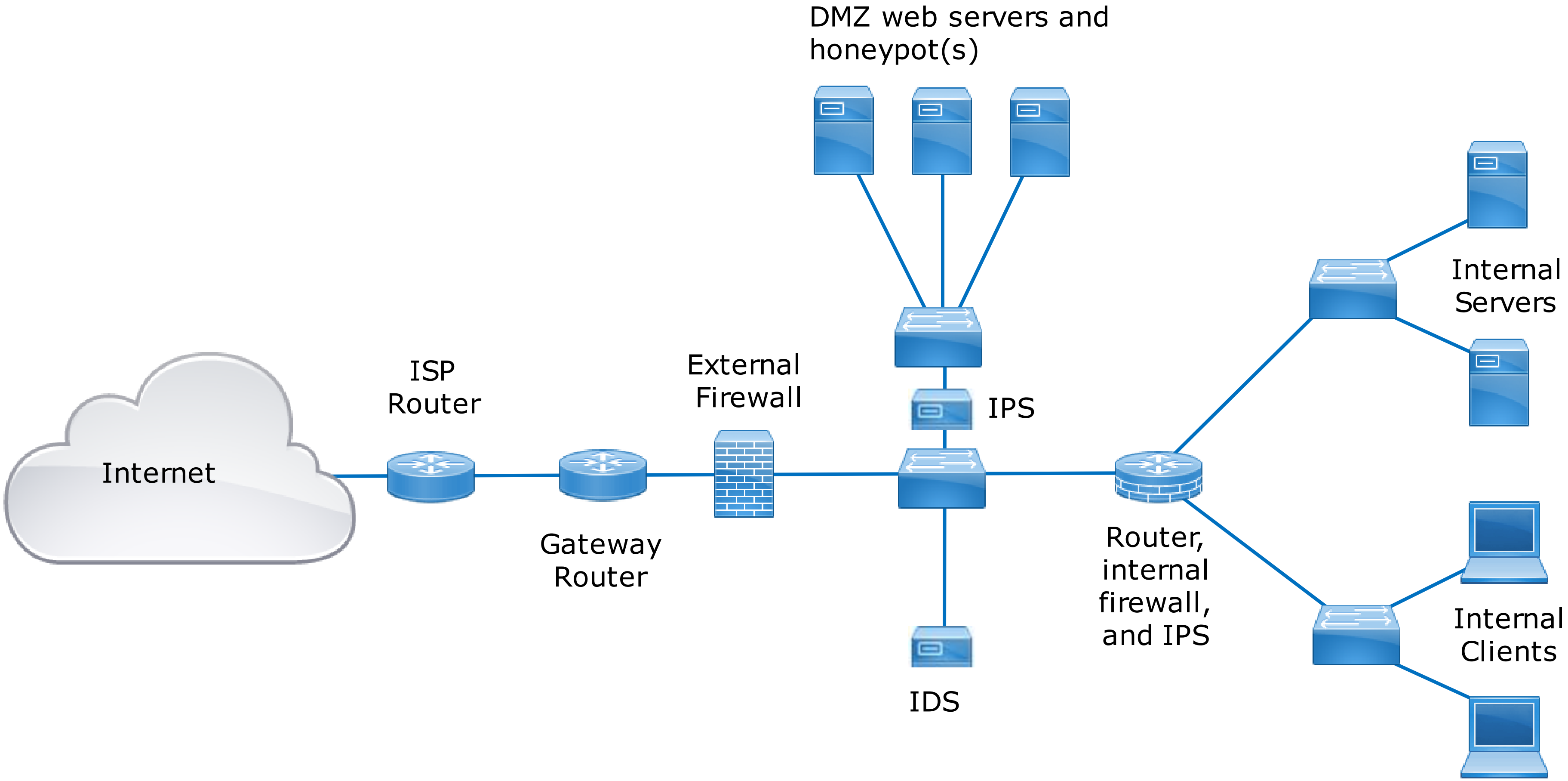
Red and Blue Pods in Microlab Lab Rack



Send me an email if you would like to join a team

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 forward 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.

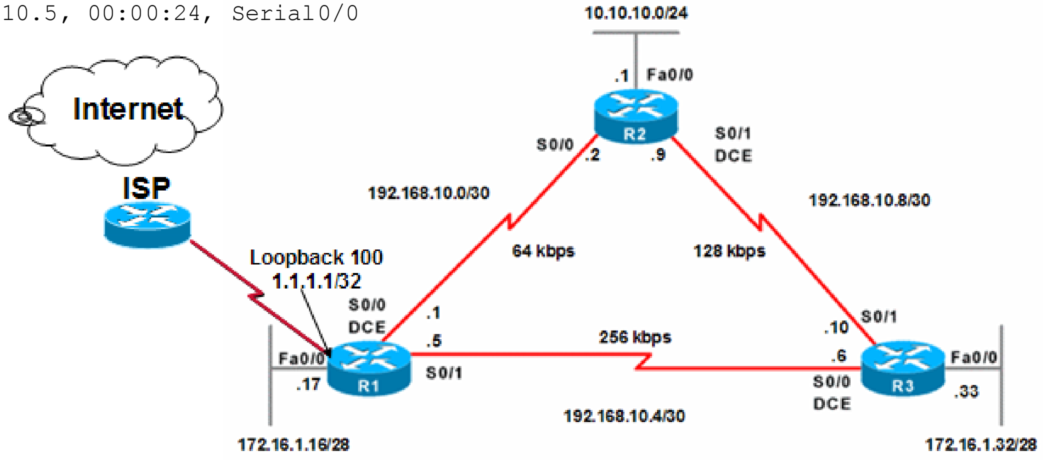
- Dynamic - routing protocols cans be used between participating routers to automatically calculate and populate routing tables with the best routes. Example routing protocols are RIP, OSPF, BGP, EIGRP, etc.

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

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

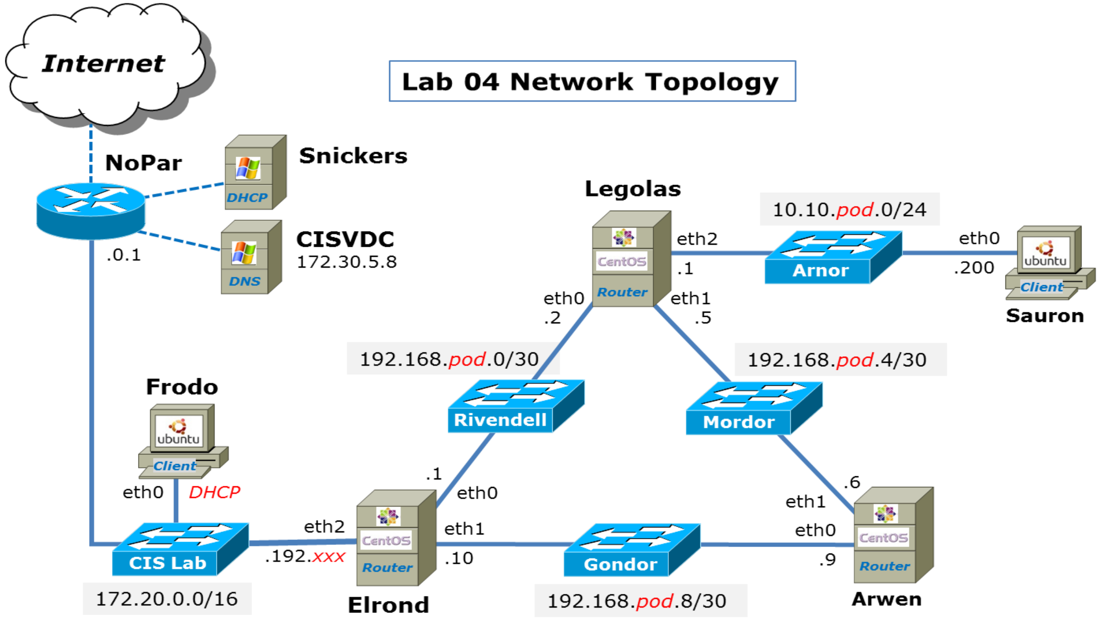
Example Cisco Routing Table

```
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] 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#
```



Example Linux Routing Table

```
Legolas route -n output
-----------------------
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

Routers

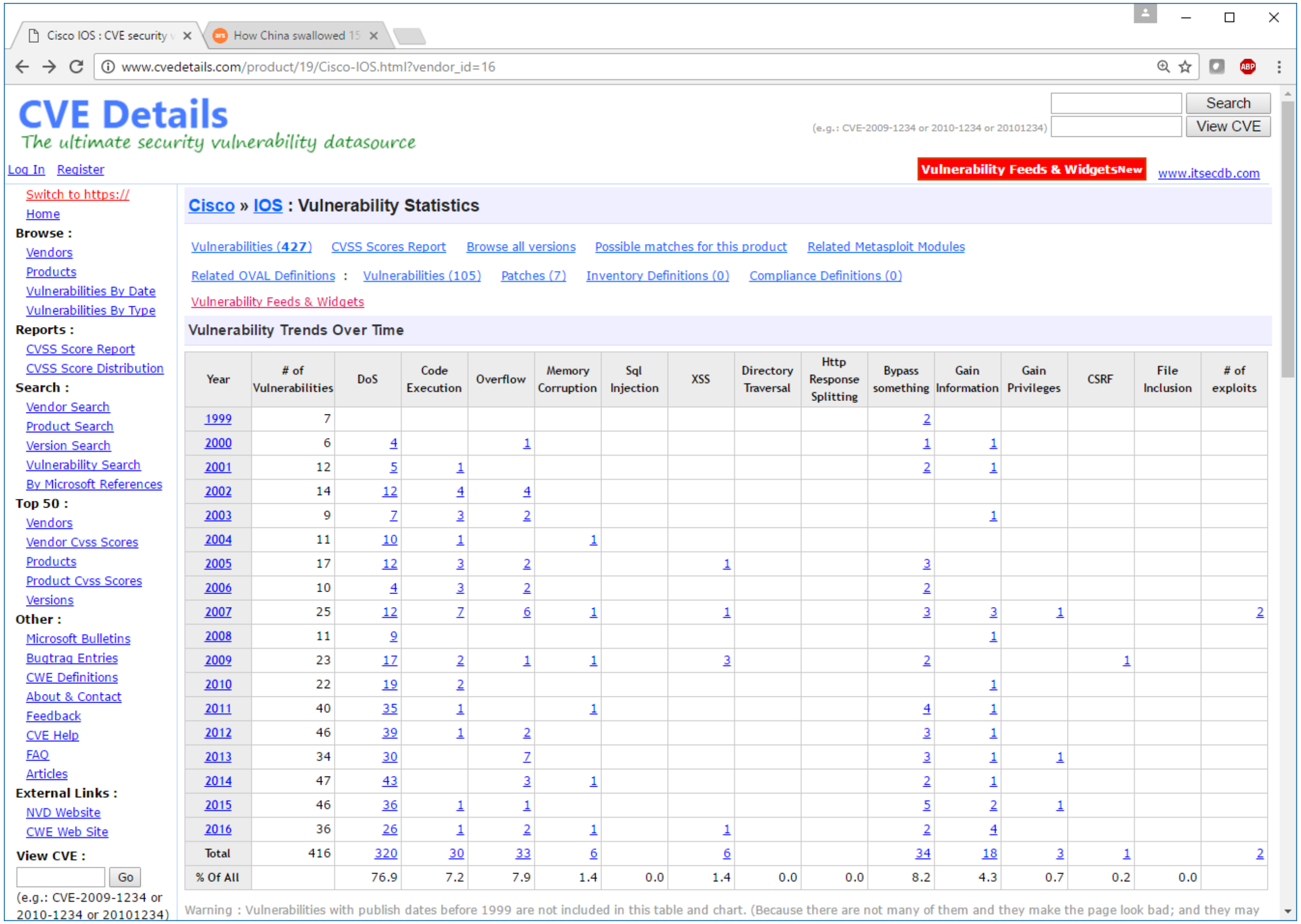
Unfortunately routers can be hacked like everything else

- 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



Cisco IOS : CVE security v ×   How China swallowed 15 ×

www.cvedetails.com/product/19/Cisco-IOS.html?vendor_id=16

CVE Details

The ultimate security vulnerability datasource

Search

View CVE

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

Log In   Register

Vulnerability Feeds & WidgetsNew   www.itsecdb.com

Switch to https://

Home

Browse :
- Vendors
- Products
- Vulnerabilities By Date
- Vulnerabilities By Type

Reports :
- CVSS Score Report
- CVSS Score Distribution

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

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

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

External Links :
- NVD Website
- CWE Web Site

View CVE :

Go

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

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

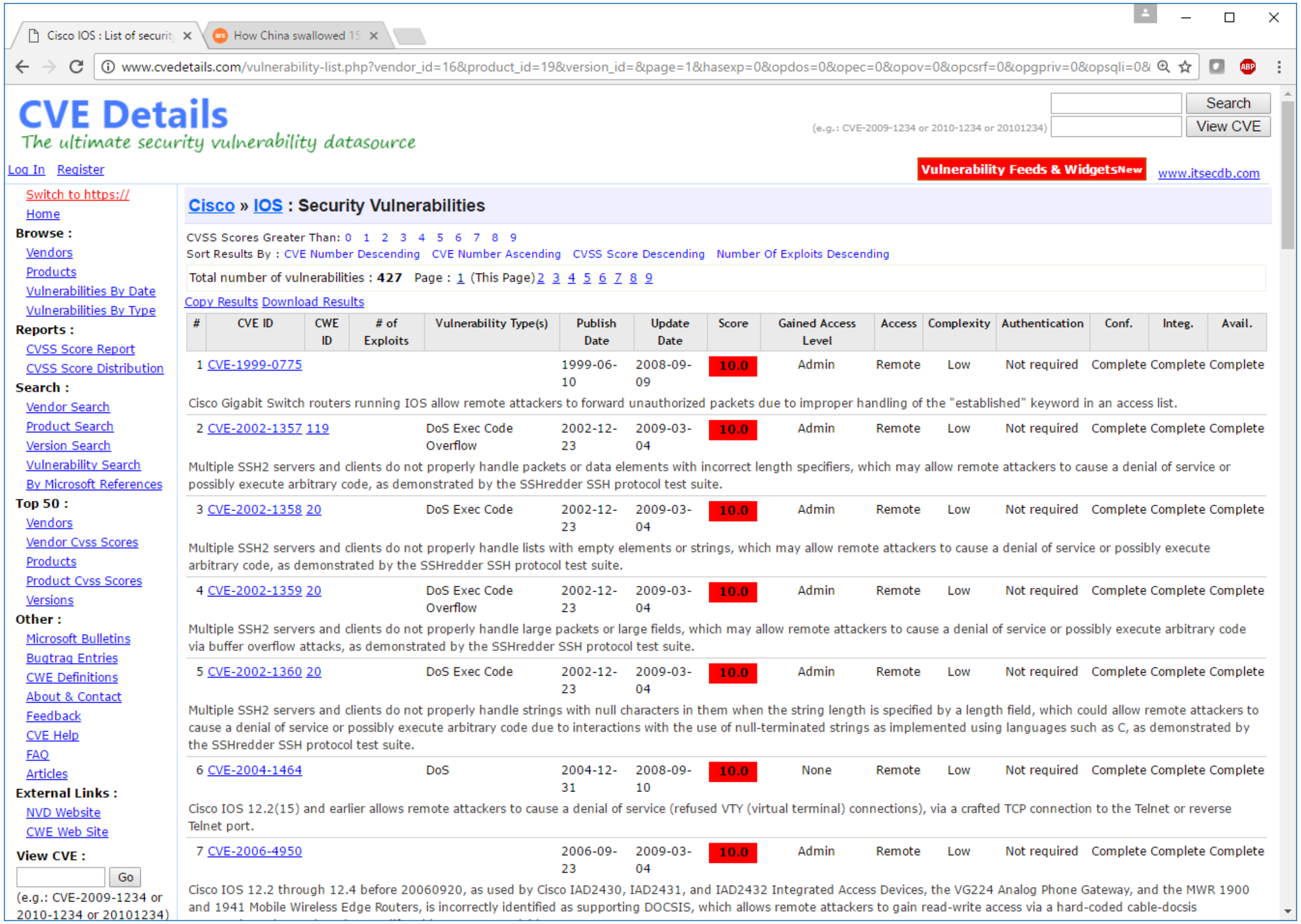
Vulnerability Trends Over Time

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	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	

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


Cisco IOS : List of securit
How China swallowed 15
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&
Search
View CVE
(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)
Vulnerability Feeds & WidgetsNew
www.itsecdb.com

CVE Details

The ultimate security vulnerability datasource

Log In Register

Switch to https://
Home
Browse :
Vendors
Products
Vulnerabilities By Date
Vulnerabilities By Type
Reports :
CVSS Score Report
CVSS Score Distribution
Search :
Vendor Search
Product Search
Version Search
Vulnerability Search
By Microsoft References
Top 50 :
Vendors
Vendor Cvss Scores
Products
Product Cvss Scores
Versions
Other :
Microsoft Bulletins
Bugtraq Entries
CWE Definitions
About & Contact
Feedback
CVE Help
FAQ
Articles
External Links :
NVD Website
CWE Web Site
View CVE :
Go
(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

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

Copy Results Download Results

<table>
<tr><th>#</th><th>CVE ID</th><th>CWE ID</th><th># of Exploits</th><th>Vulnerability Type(s)</th><th>Publish Date</th><th>Update Date</th><th>Score</th><th>Gained Access Level</th><th>Access</th><th>Complexity</th><th>Authentication</th><th>Conf.</th><th>Integ.</th><th>Avail.</th></tr>
<tr><td>1</td><td>CVE-1999-0775</td><td></td><td></td><td></td><td>1999-06-10</td><td>2008-09-09</td><td>10.0</td><td>Admin</td><td>Remote</td><td>Low</td><td>Not required</td><td>Complete</td><td>Complete</td><td>Complete</td></tr>
<tr><td colspan="15">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.</td></tr>
<tr><td>2</td><td>CVE-2002-1357</td><td>119</td><td></td><td>DoS Exec Code Overflow</td><td>2002-12-23</td><td>2009-03-04</td><td>10.0</td><td>Admin</td><td>Remote</td><td>Low</td><td>Not required</td><td>Complete</td><td>Complete</td><td>Complete</td></tr>
<tr><td colspan="15">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.</td></tr>
<tr><td>3</td><td>CVE-2002-1358</td><td>20</td><td></td><td>DoS Exec Code</td><td>2002-12-23</td><td>2009-03-04</td><td>10.0</td><td>Admin</td><td>Remote</td><td>Low</td><td>Not required</td><td>Complete</td><td>Complete</td><td>Complete</td></tr>
<tr><td colspan="15">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.</td></tr>
<tr><td>4</td><td>CVE-2002-1359</td><td>20</td><td></td><td>DoS Exec Code Overflow</td><td>2002-12-23</td><td>2009-03-04</td><td>10.0</td><td>Admin</td><td>Remote</td><td>Low</td><td>Not required</td><td>Complete</td><td>Complete</td><td>Complete</td></tr>
<tr><td colspan="15">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.</td></tr>
<tr><td>5</td><td>CVE-2002-1360</td><td>20</td><td></td><td>DoS Exec Code</td><td>2002-12-23</td><td>2009-03-04</td><td>10.0</td><td>Admin</td><td>Remote</td><td>Low</td><td>Not required</td><td>Complete</td><td>Complete</td><td>Complete</td></tr>
<tr><td colspan="15">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.</td></tr>
<tr><td>6</td><td>CVE-2004-1464</td><td></td><td></td><td>DoS</td><td>2004-12-31</td><td>2008-09-10</td><td>10.0</td><td>None</td><td>Remote</td><td>Low</td><td>Not required</td><td>Complete</td><td>Complete</td><td>Complete</td></tr>
<tr><td colspan="15">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.</td></tr>
<tr><td>7</td><td>CVE-2006-4950</td><td></td><td></td><td></td><td>2006-09-23</td><td>2009-03-04</td><td>10.0</td><td>Admin</td><td>Remote</td><td>Low</td><td>Not required</td><td>Complete</td><td>Complete</td><td>Complete</td></tr>
<tr><td colspan="15">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</td></tr>
</table>

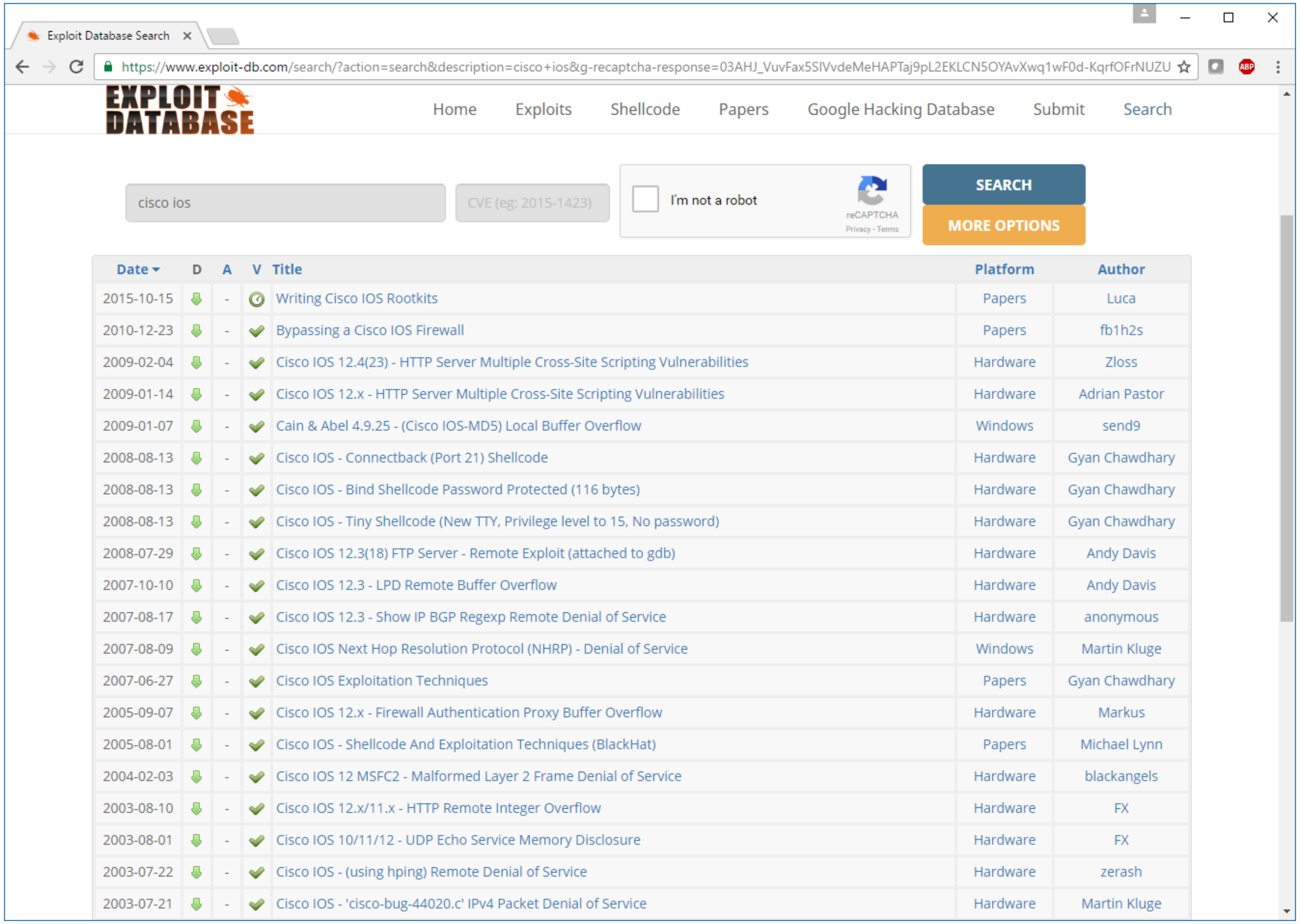
http://www.cvedetails.com/vulnerability-list.php?vendor_id=16&product_id=19&version_id=&page=1&hasexp=0&opdos=0&opec=0&opov=0&opcsrf=0&opgpriv=0&opsqli=0&opxss=0&opdirt=0&opmemc=0&ophttprs=0&opbyp=0&opfileinc=0&opginf=0&cvssscoremin=0&cvssscoremax=0&year=0&month=0&cweid=0&order=3&trc=427&sha=bd51a01b646bad788bdc715f12e17fa177698ba8

Activity

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

Put your answer in the chat window

Cisco IOS Exploits



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/search/?action=search&description=cisco+ios&g-recaptcha-response=03AHJ_VuvFax5SlVvdeMeHAPTaj9pL2EKLCN5OYAvXwq1wF0d-KqrfOFrNUZUYLmueKtoSD7gJHYfTXvHA-8HGvMVQwzk1fxWePnpS56tGGni9VPf3mM2iyfvOhIfljXLPr5sZv1_k_ythChKQhDEk1PPgljYBd6nOLdn3nrIAv-HABmMMc0FagR61Y8wXgkqK5Trm75BtqHf32PkKk7wzCq-NE_pirs1R7zZVsmqBMQxuo0G1DzA1-ceuR-ujl5ISy2cXFjj1YQwuB2NSWKIu4jcD-ZGj2zGLeFSUFcxUWezUQcdipBr24w4Wt5Yk87pfzL8dsDZ57wZ3u5SWFijnzTaFd_SR3u5O1VHXP76IZneo7f35hzE1rXYK9ZTqYql5zkgRlu0_awSyBt4KOd_IHxDF4gXm0TdWBnQAjYaNNtHVcy2SOm6pySXtaVxUCRM8Cyq_N1OT5OEKpE1R9vTcNg_jYw48D4MA6exoy2T11c5P1PUnem1NAeyBjk8xsprN9Eq8pYrFPsnXHirQ-1mDRQKWKvBzYAjW6aFUNwCQPJWMldRASeVO5OKdZs1NevGiwCOwhL8WRotKVoIDpt6fj25EPhSOg1he5dJe0O8M4vjmTZzXI3JUZFbg9FG1CiU62GN1ngRfMyxmvYw9HpOvfuAATjaa5cw30iLLjclgFkDZQAT5alDkVRxLxfudK5KLwh_kiNDIAR51xFC5yOcsxtmrzk0cVt1g8ZyrfQKvVeGVdu6Zv_mKnWqMz3Xs9GViEmfI6DjB1Onfq-c8M9C-6MhyRf88FBmwhEO2r8VNZR8ZPE9Fh0S34csEWAwU2MzZNae7OnYrshIZ8pxqZEFKdXhoeeLz6S7hhM_hxO_RBwywQnxaHyv04UTtZQWZxshXY6QMjFhwhktRhldKLSXz2q8ymVdcVhXbaQ

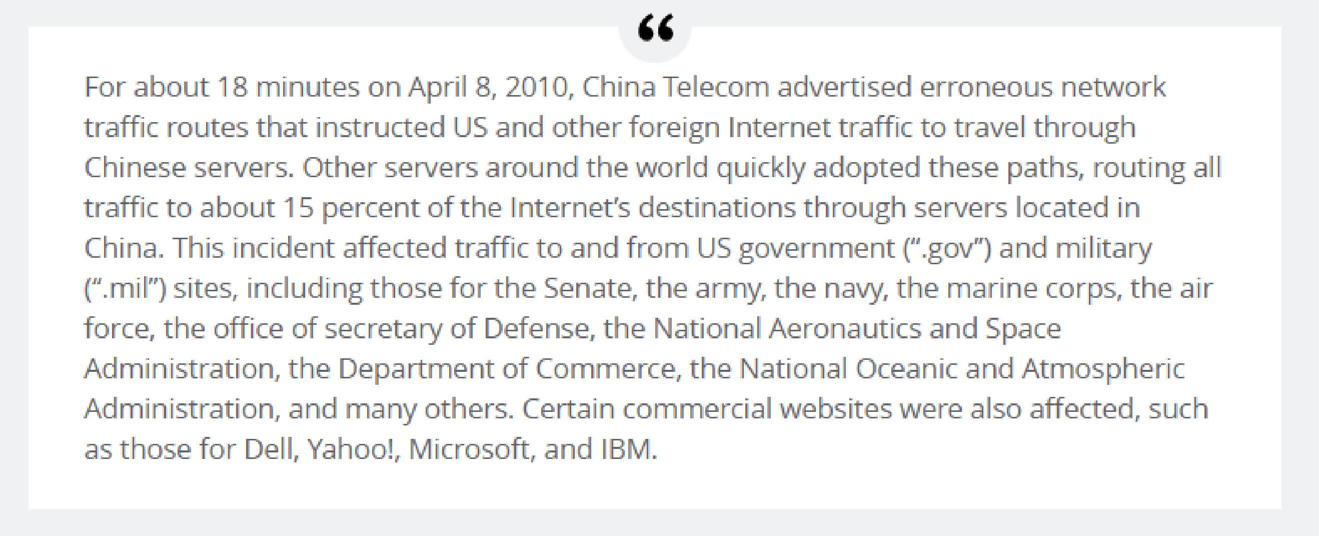
Activity

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

Which one has the most?

Put your answer in the chat window

China highjacks 15% of Internet traffic

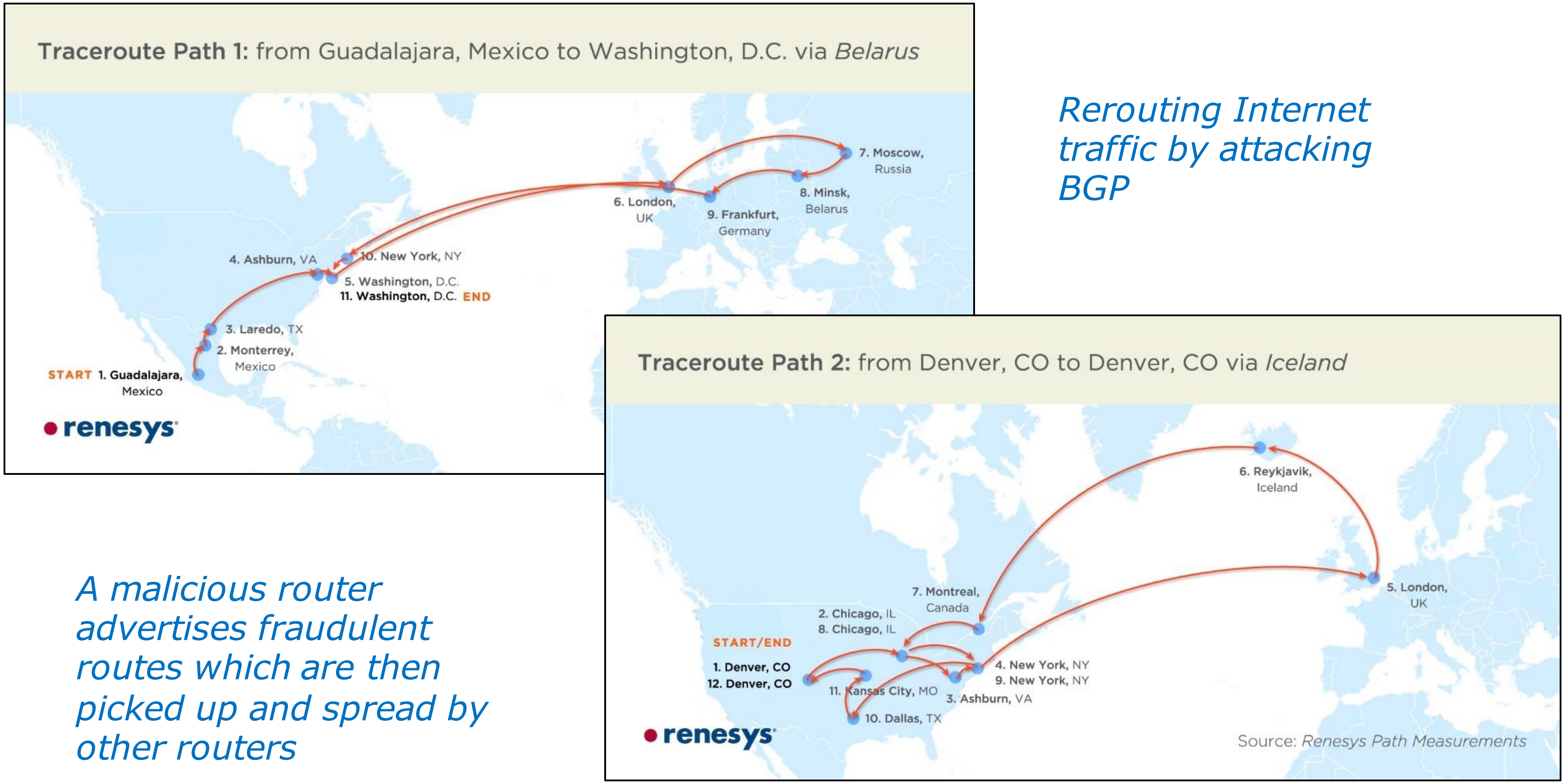


> For about 18 minutes on April 8, 2010, China Telecom advertised erroneous network traffic routes that instructed US and other foreign Internet traffic to travel through Chinese servers. Other servers around the world quickly adopted these paths, routing all traffic to about 15 percent of the Internet's 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 get 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*

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

Source: *Renesys Path Measurements*

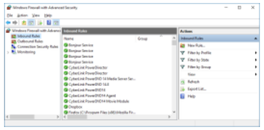
Rerouting Internet traffic by attacking BGP

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

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

Firewalls

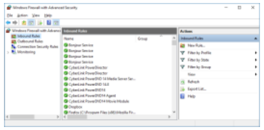
Firewalls



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

Firewall Technologies

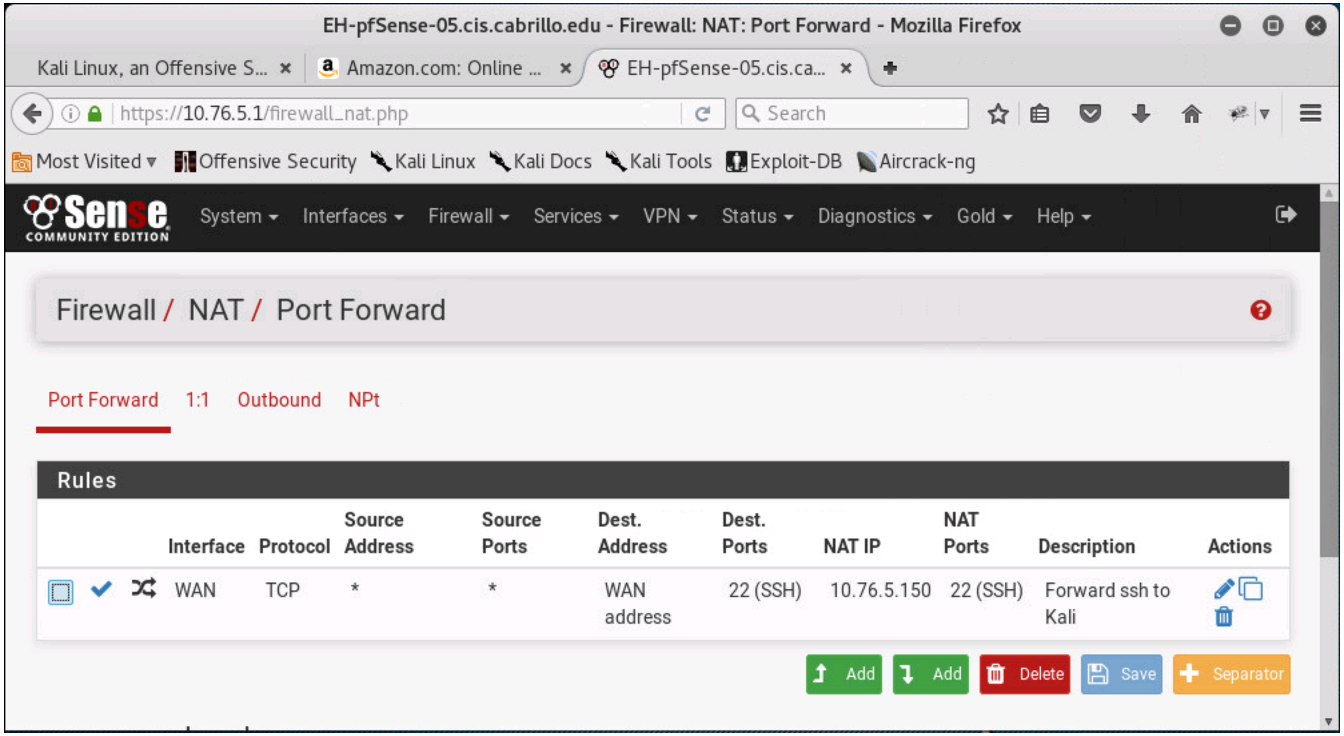
netfilter
firewalling, NAT, and packet mangling for linux



pfSense

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

Network Address Translation



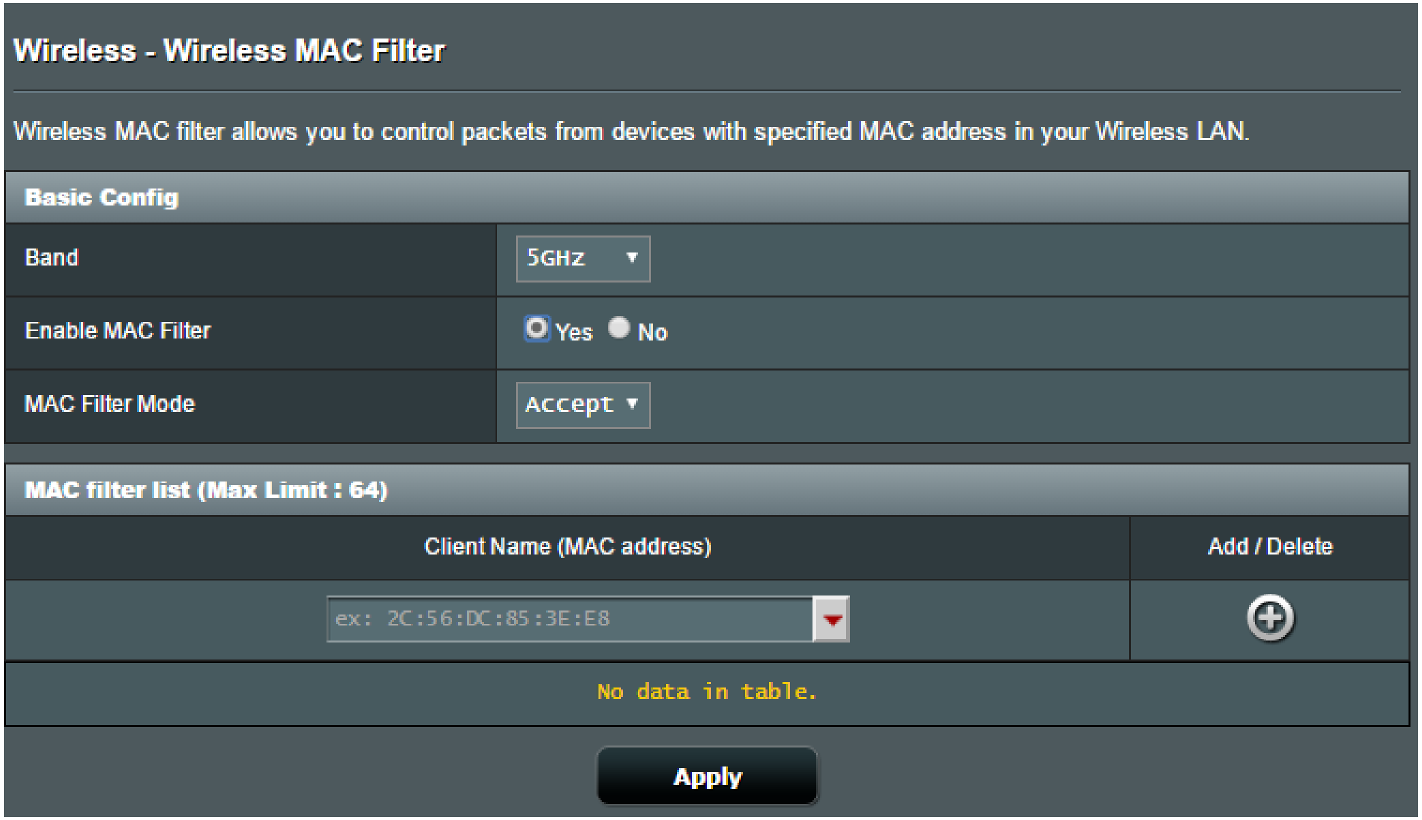
Firewall / NAT / Port Forward

Rules

			Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
□	✓		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	● Yes ○ No
MAC Filter Mode	Accept ▾

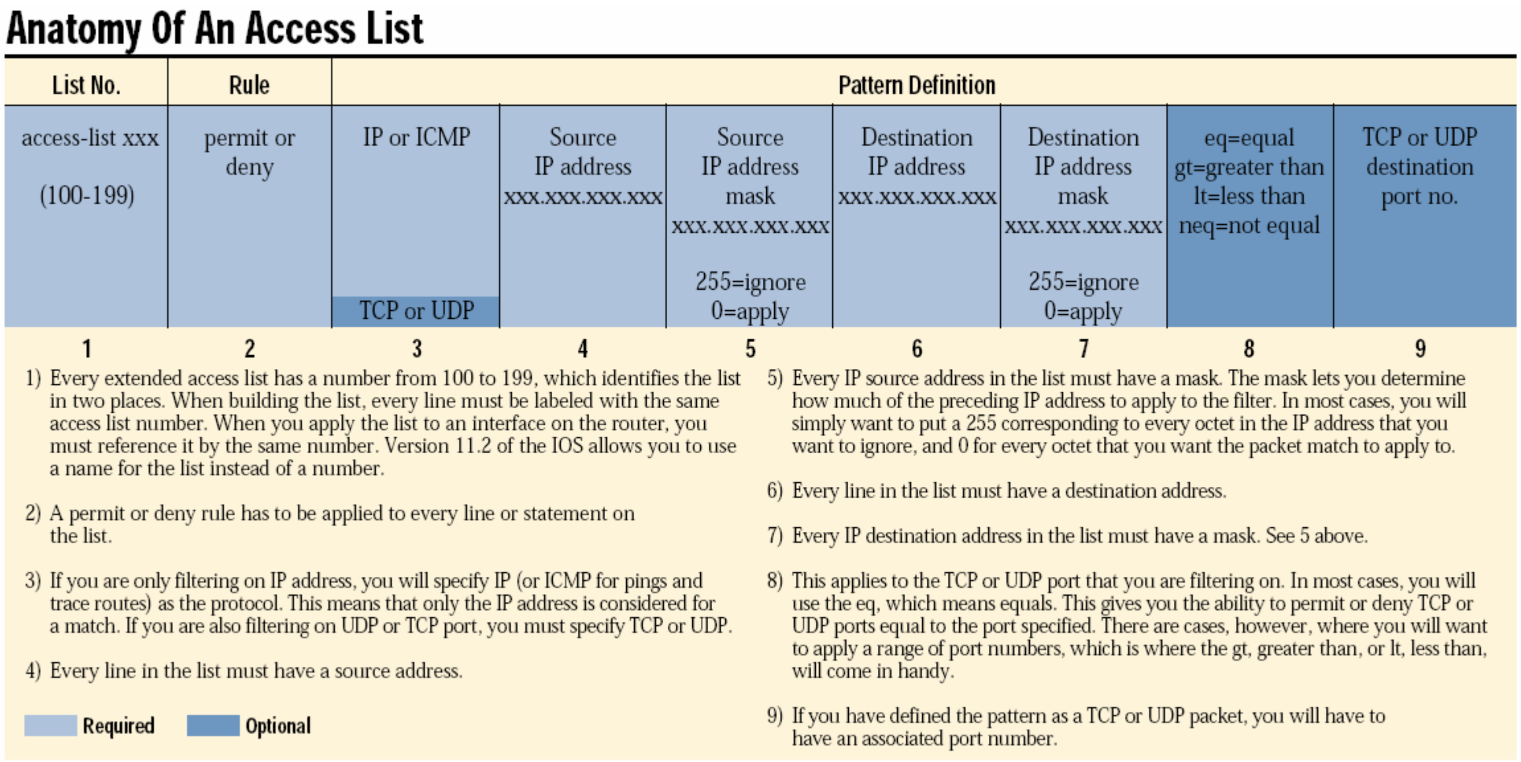
MAC filter list (Max Limit : 64)

Client Name (MAC address)	Add / Delete
ex: 2C:56:DC:85:3E:E8 ▾	⊕

No data in table.

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
```

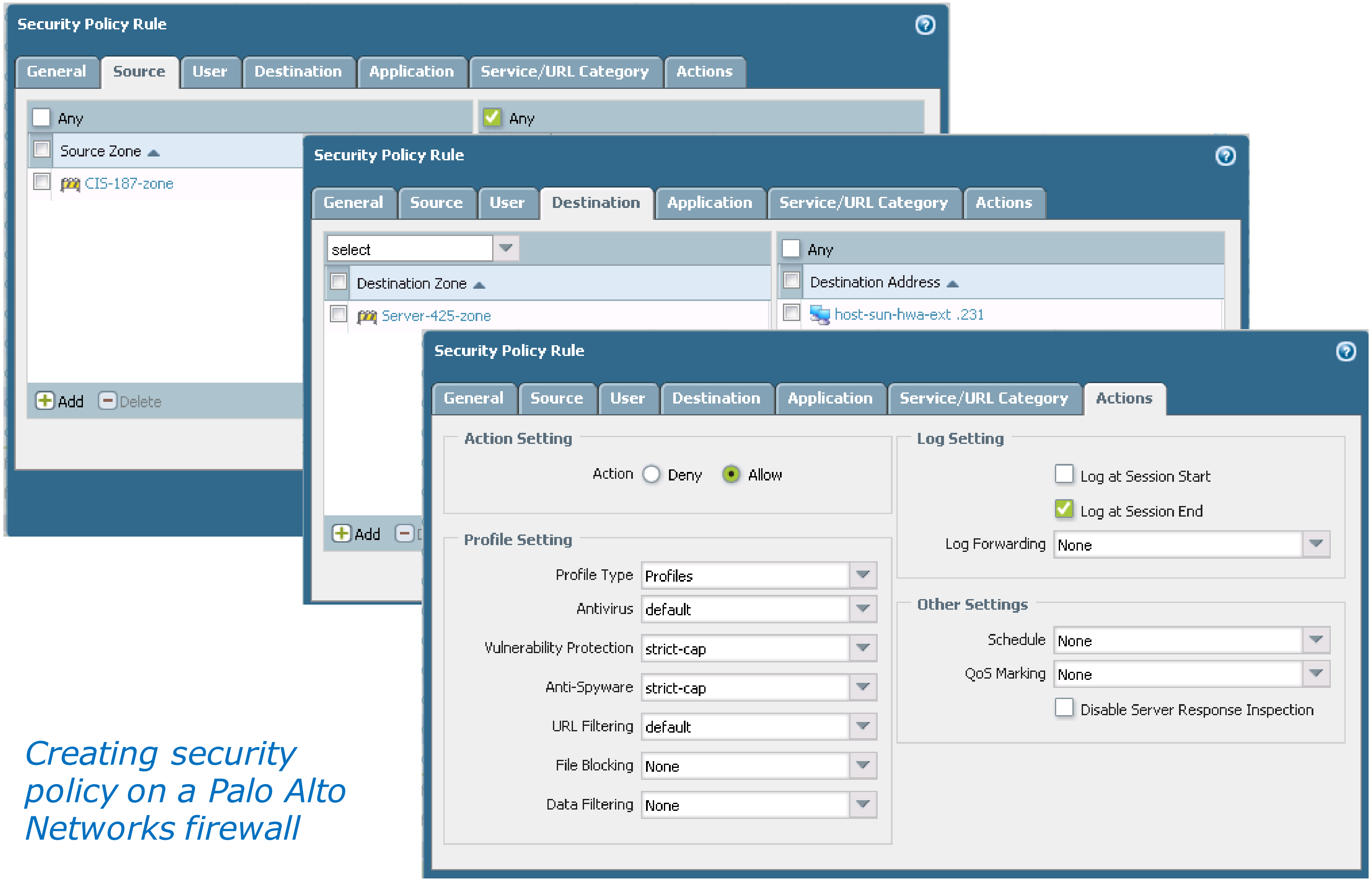
Access List on a Cisco Router

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



Security Policy Rule

General | Source | User | Destination | Application | Service/URL Category | Actions

- □ Any
- □ Source Zone ▲
- □ CIS-187-zone
- ☑ Any
- Add | Delete

Security Policy Rule

General | Source | User | Destination | Application | Service/URL Category | Actions

- select
- □ Destination Zone ▲
- □ Server-425-zone
- □ Any
- □ Destination Address ▲
- □ host-sun-hwa-ext .231
- Add

Security Policy Rule

General | Source | User | Destination | Application | Service/URL Category | Actions

Action Setting

Action ○ Deny ● Allow

Profile Setting

Profile Type	Profiles
Antivirus	default
Vulnerability Protection	strict-cap
Anti-Spyware	strict-cap
URL Filtering	default
File Blocking	None
Data Filtering	None

Log Setting

- □ Log at Session Start
- ☑ Log at Session End
- Log Forwarding: None

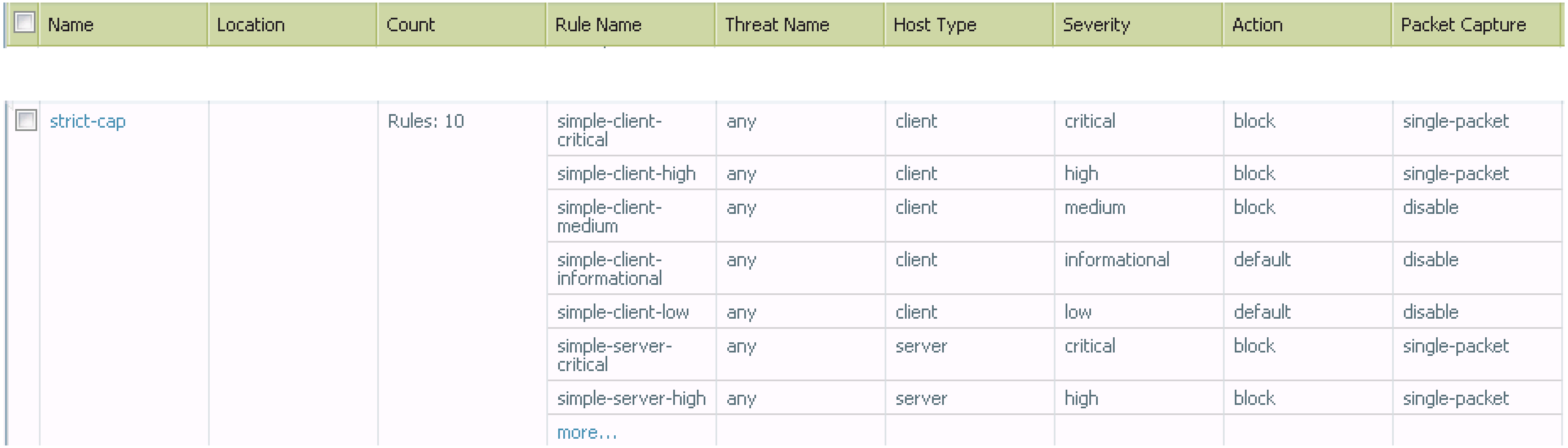
Other Settings

- Schedule: None
- QoS Marking: None
- □ Disable Server Response Inspection

Creating security policy on a Palo Alto Networks firewall

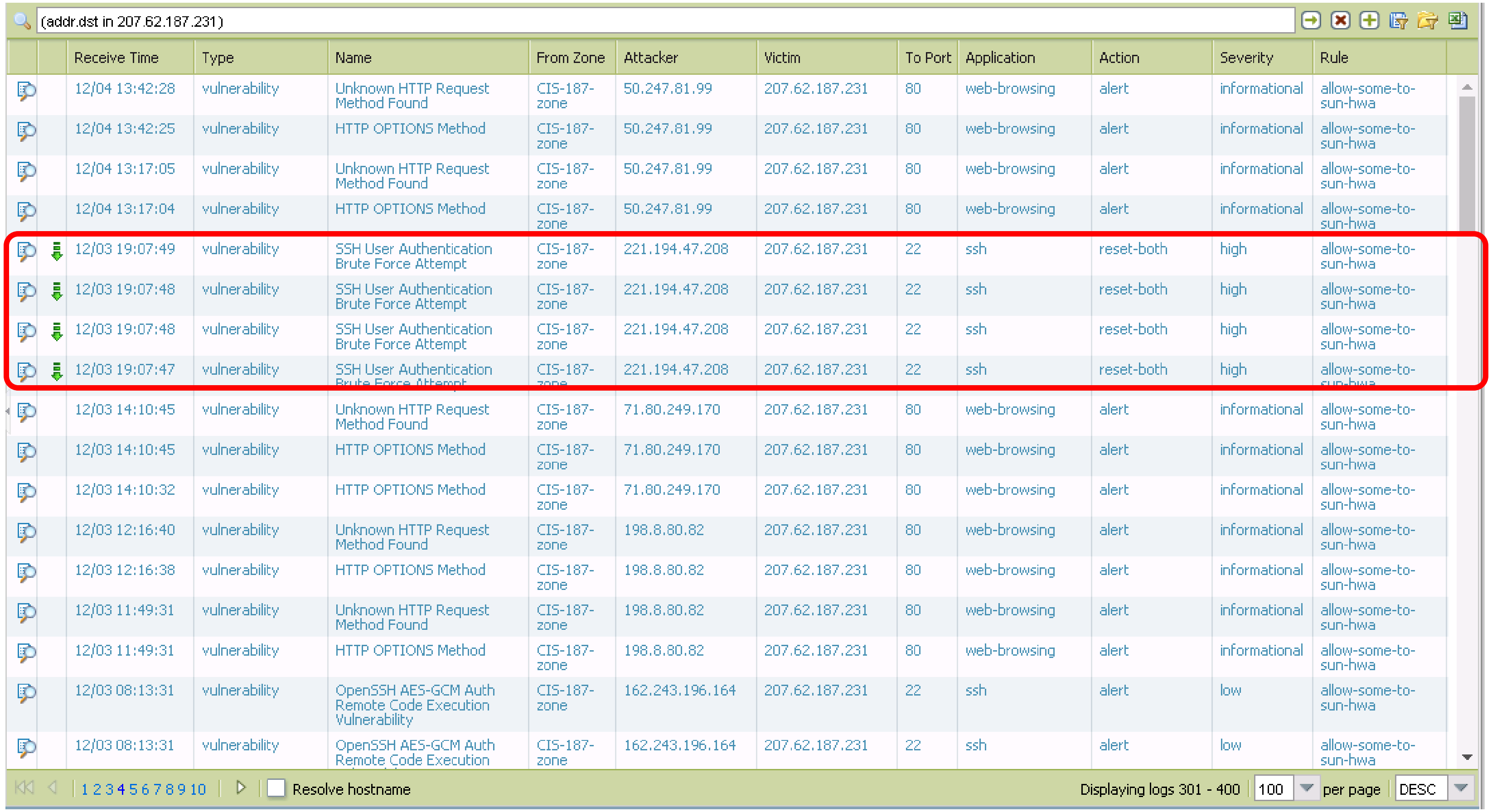
23	allow-some-to-sun-hwa	none	universal	CIS-187-zone	any	any	any	Server-425-zone	host-sun-hwa-ext .231	any	any

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

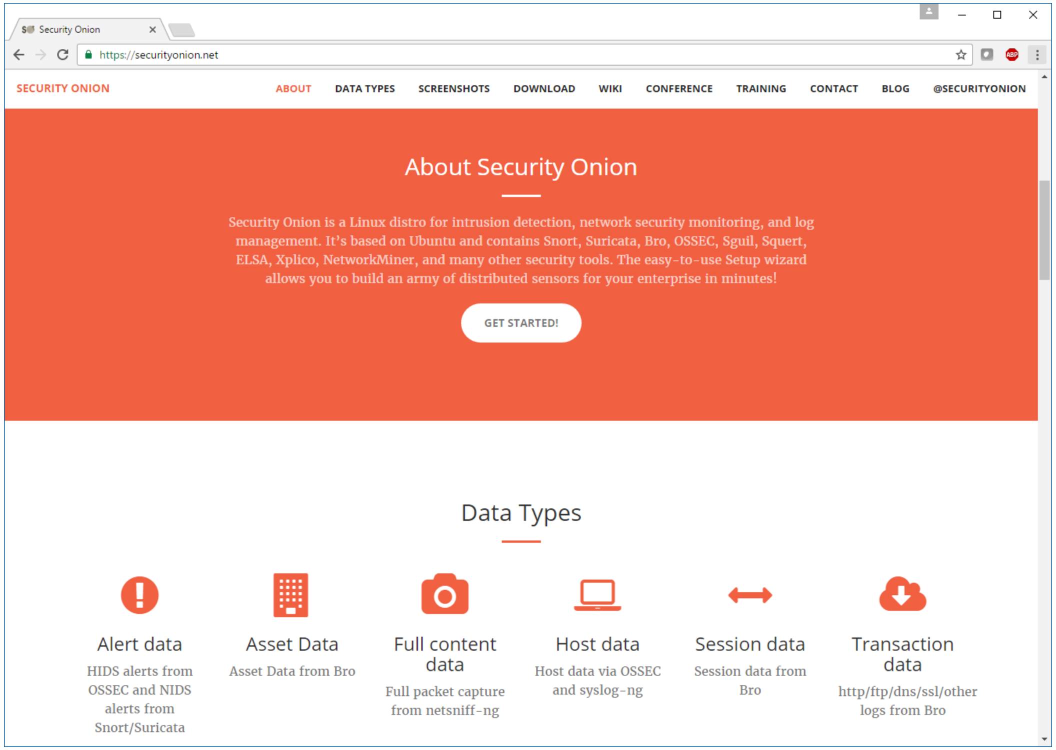
- Payload obfuscation
  - Encoding and encryption
  - Polymorphism

- 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



About Security Onion

Security Onion is a Linux distro for intrusion detection, network security monitoring, and log management. It's based on Ubuntu and contains Snort, Suricata, Bro, OSSEC, Sguil, Squert, ELSA, Xplico, NetworkMiner, and many other security tools. The easy-to-use Setup wizard allows you to build an army of distributed sensors for your enterprise in minutes!

Data Types

Alert data
HIDS alerts from OSSEC and NIDS alerts from Snort/Suricata

Asset Data
Asset Data from Bro

Full content data
Full packet capture from netsniff-ng

Host data
Host data via OSSEC and syslog-ng

Session data
Session data from Bro

Transaction data
http/ftp/dns/ssl/other logs from Bro

https://securityonion.net/

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

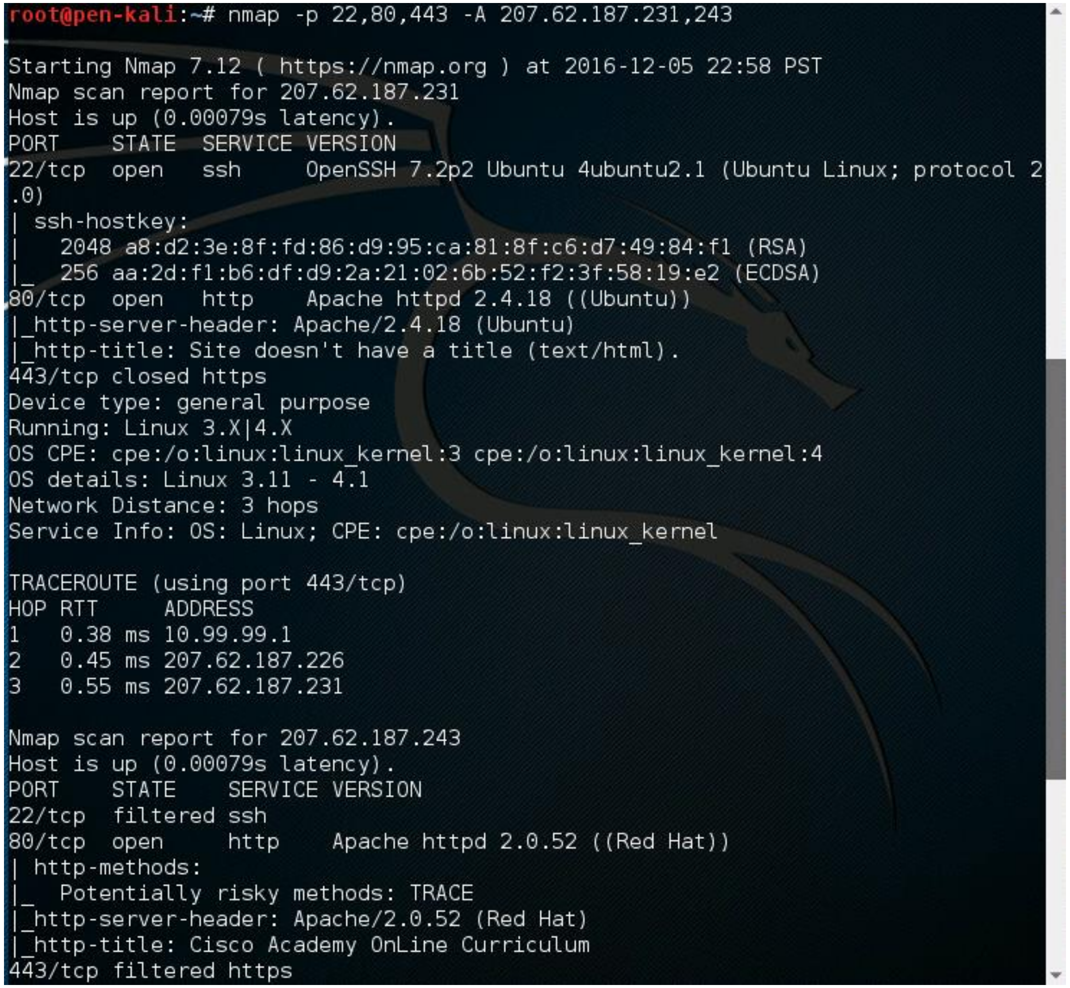
It bundles Squert, Sguil, SNORT, ELSA, Bro and more.

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

https://www.paloaltonetworks.com/

nmap "all" scan

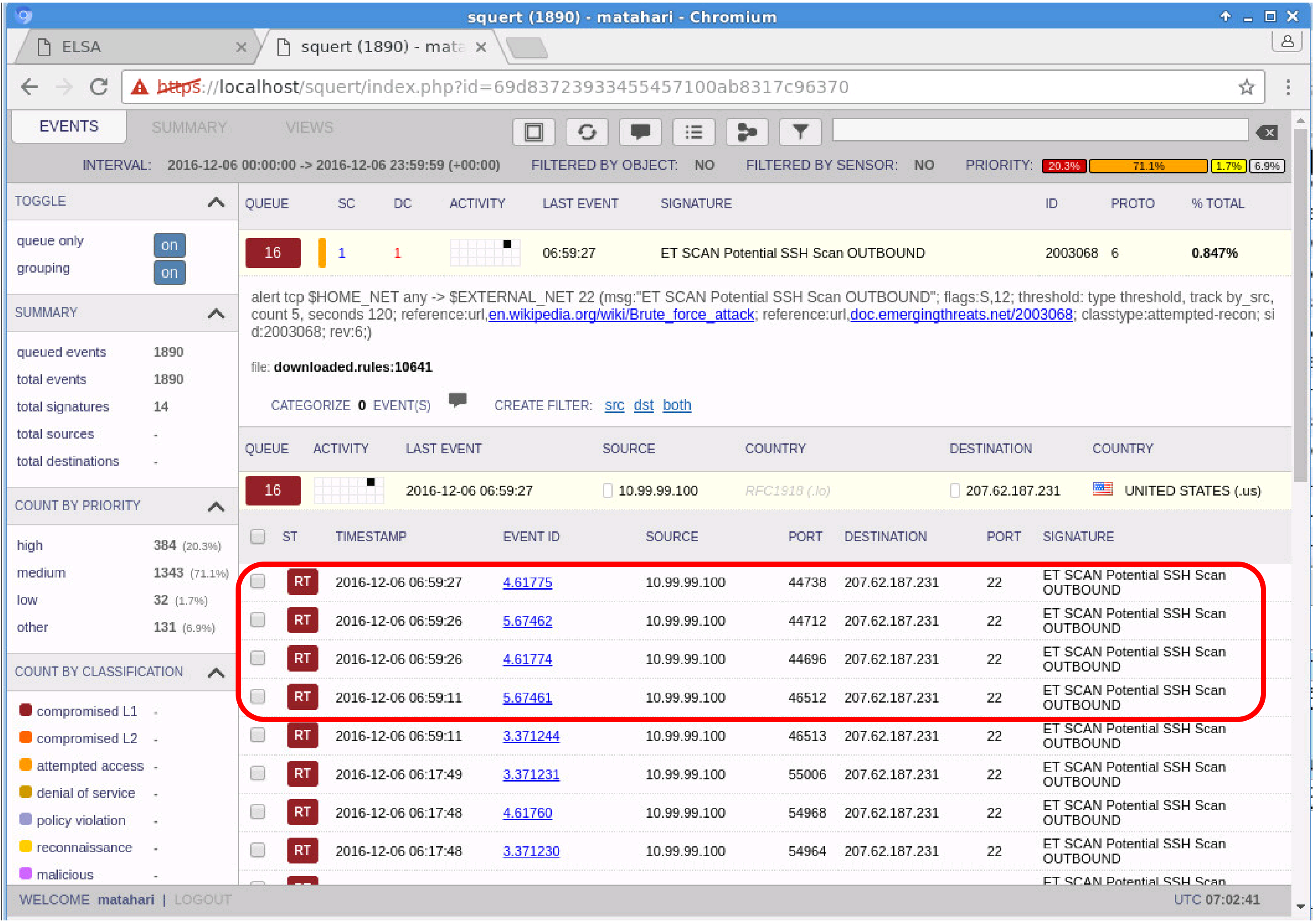
nmap -p 22,80,443 -A 207.62.187.231,243



```
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



squert (1890) - matahari - Chromium
ELSA
squert (1890) - mata
https://localhost/squert/index.php?id=69d83723933455457100ab8317c96370
EVENTS
SUMMARY
VIEWS

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% 71.1% 1.7% 6.9%

TOGGLE

queue only	on
grouping	on

SUMMARY

queued events	1890
total events	1890
total signatures	14
total sources	-
total destinations	-

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	-

QUEUE	SC	DC	ACTIVITY	LAST EVENT	SIGNATURE	ID	PROTO	% TOTAL
16	1	1		06:59:27	ET SCAN Potential SSH Scan OUTBOUND	2003068	6	0.847%

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**

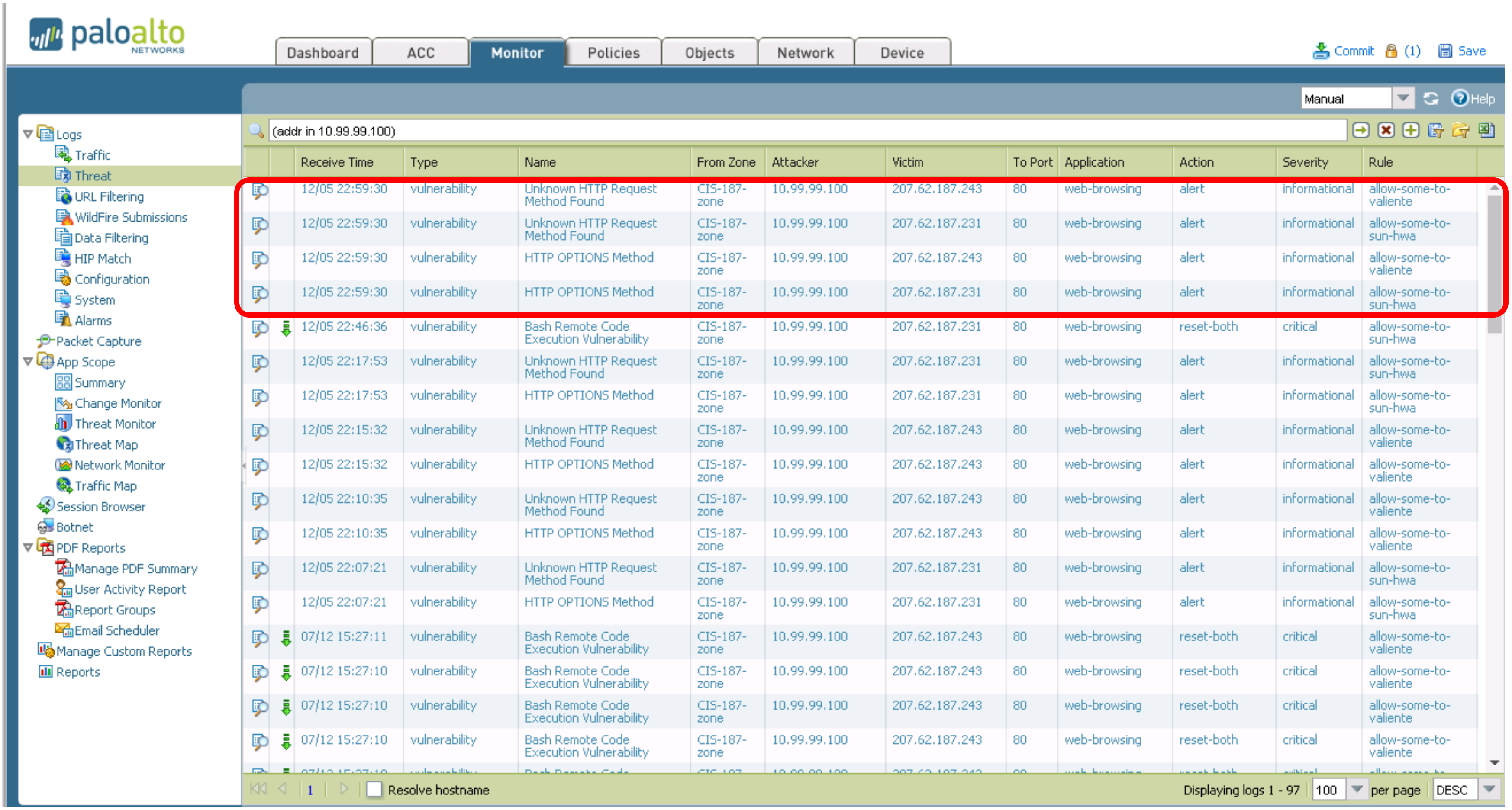
CATEGORIZE **0** EVENT(S) CREATE FILTER: src dst both

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)

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

WELCOME **matahari** | LOGOUT UTC **07:02:41**

PAN



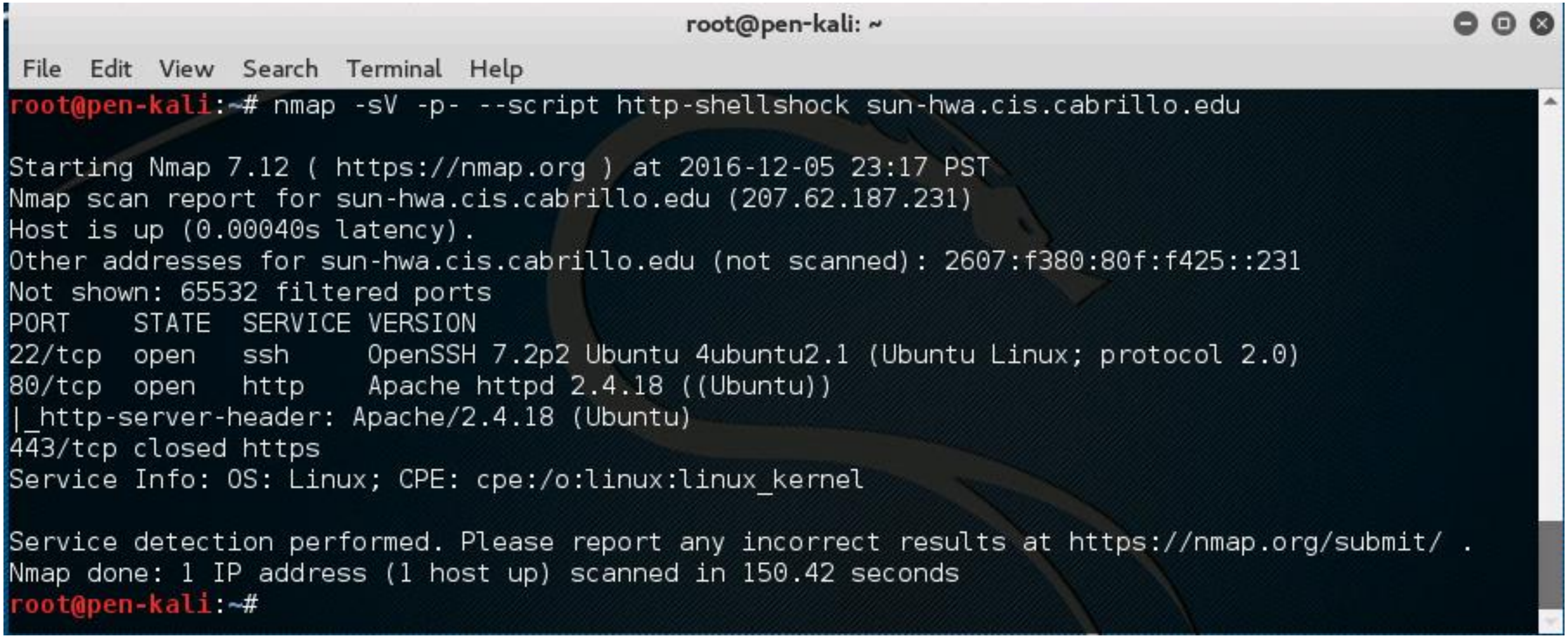
(addr in 10.99.99.100)

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

1 □ Resolve hostname

Displaying logs 1 - 97 100 per page DESC

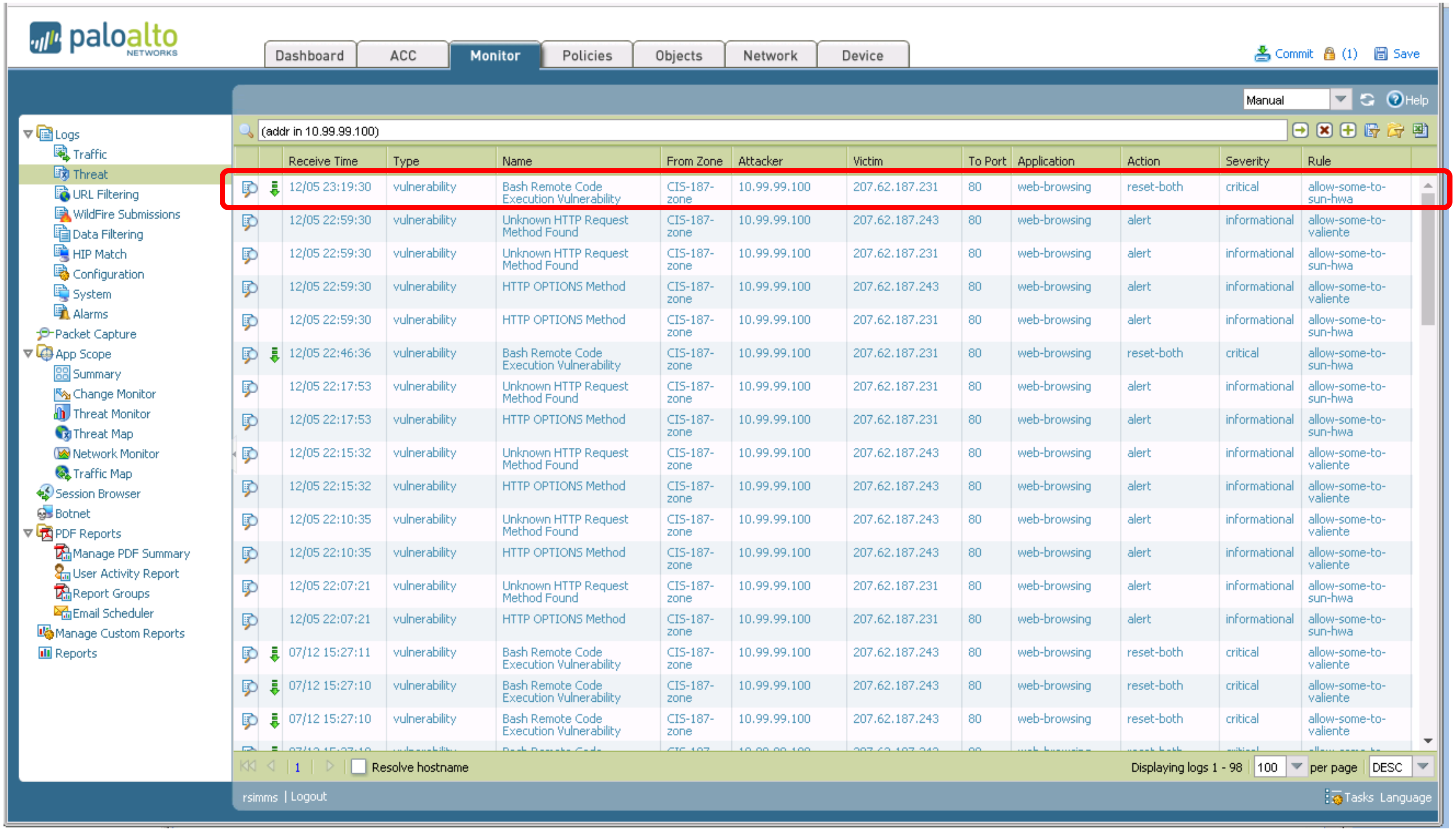
nmap "shellshock" scan



```
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



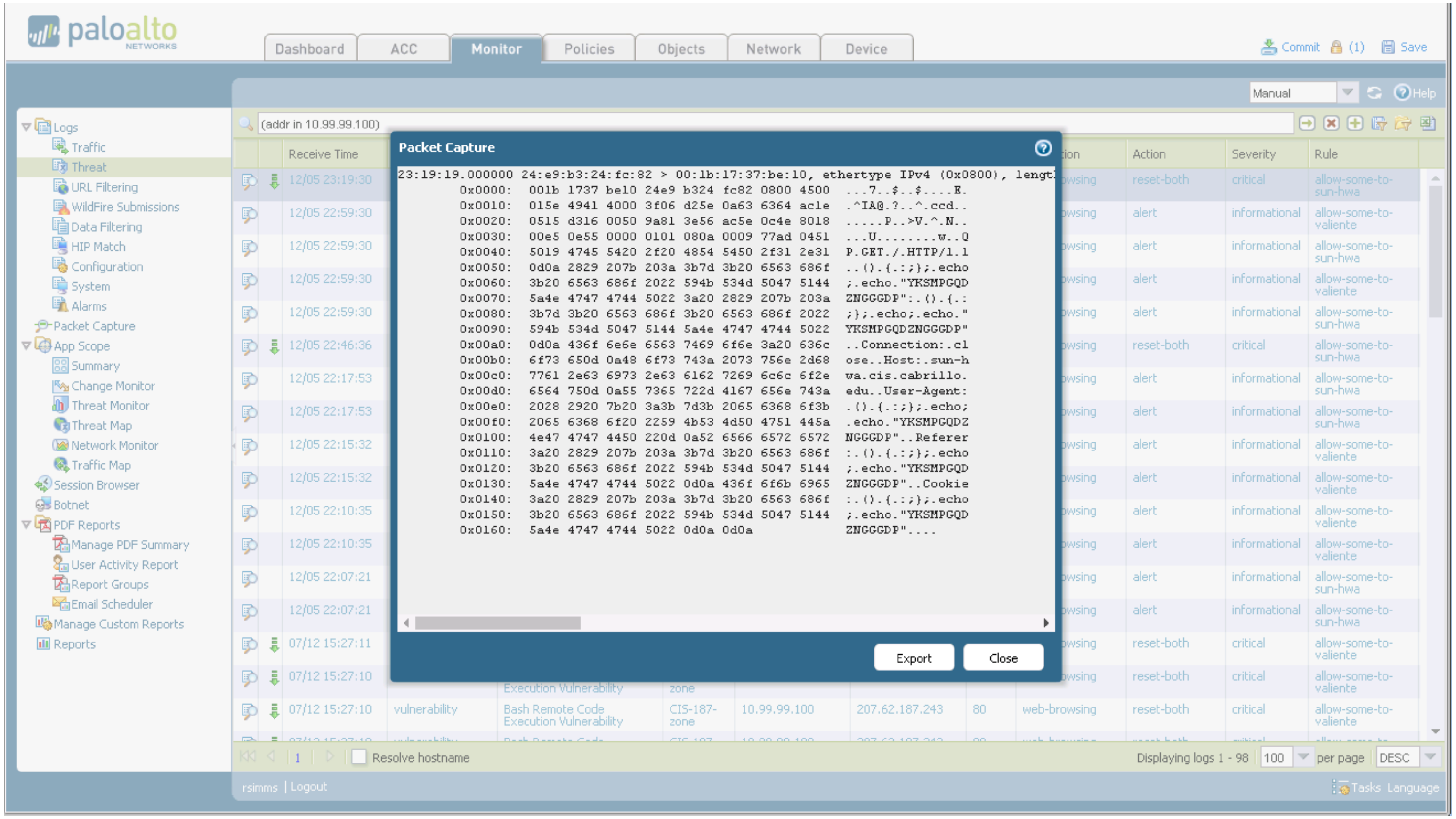
(addr in 10.99.99.100)

	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
⬇	07/12 15:27:10	vulnerability	Bash Remote Code	CIS-187-	10.99.99.100	207.62.187.243	80	web-browsing	reset-both	critical	allow-some-to-

Displaying logs 1 - 98 100 per page

PAN logs it and resets the conection

PAN



(addr in 10.99.99.100)

Packet Capture

```
23:19:19.000000 24:e9:b3:24:fc:82 > 00:1b:17:37:be:10, ethertype IPv4 (0x0800), lengt
        0x0000:  001b 1737 be10 24e9 b324 fc82 0800 4500  ...7..$..$....E.
        0x0010:  015e 4941 4000 3f06 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 2f20 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."YKSMPGQD
        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  YKSMPGQDZNGGGDP"
        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."YKSMPGQDZ
        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."YKSMPGQD
        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."YKSMPGQD
        0x0160:  5a4e 4747 4744 5022 0d0a 0d0a            ZNGGGDP"....
```

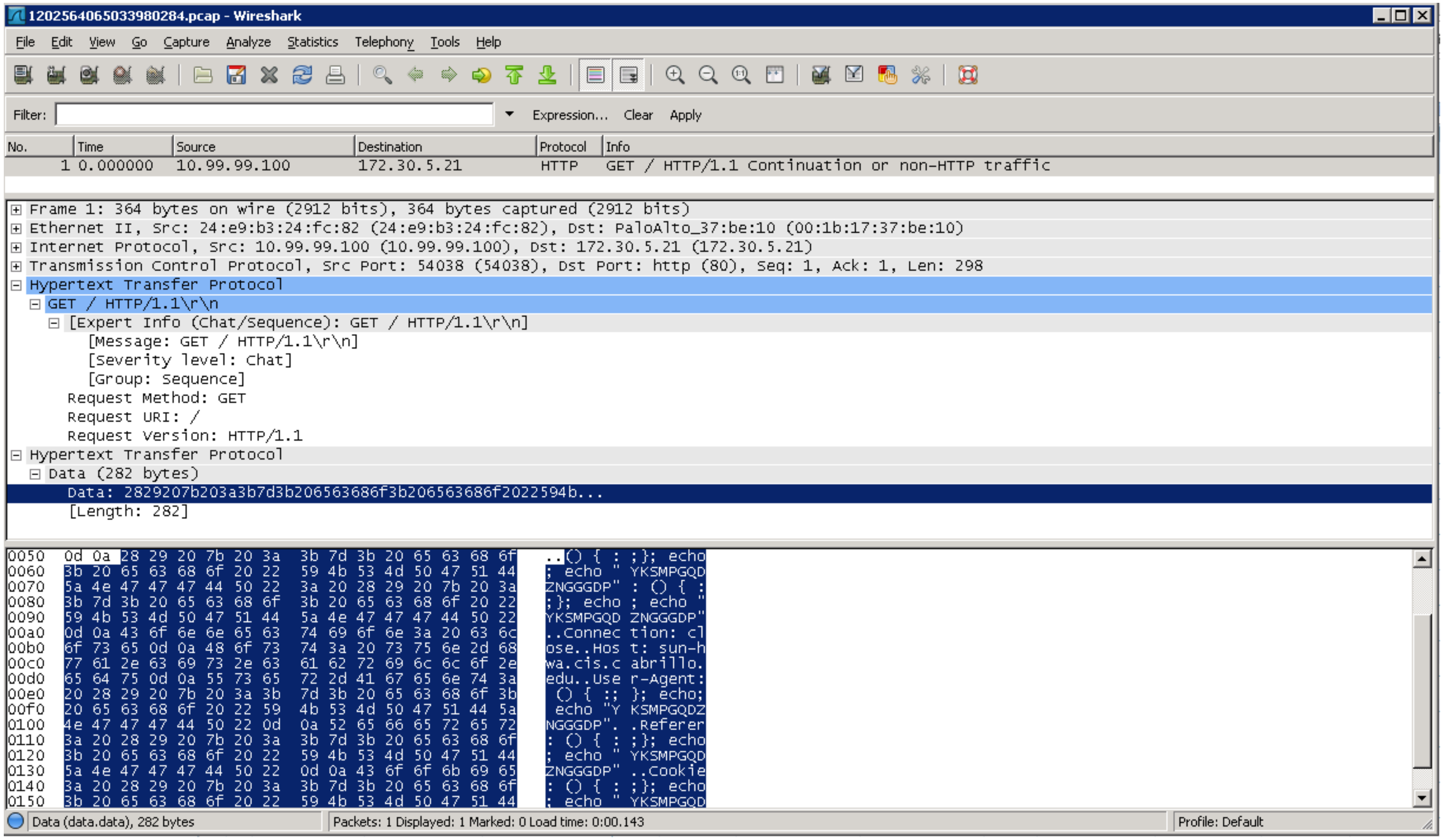
Receive Time							ion	Action	Severity	Rule
12/05 23:19:30							wsing	reset-both	critical	allow-some-to-sun-hwa
12/05 22:59:30							wsing	alert	informational	allow-some-to-valiente
12/05 22:59:30							wsing	alert	informational	allow-some-to-sun-hwa
12/05 22:59:30							wsing	alert	informational	allow-some-to-valiente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

1 □ Resolve hostname Displaying logs 1 - 98 100 per page DESC

rsimms | Logout

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]
```

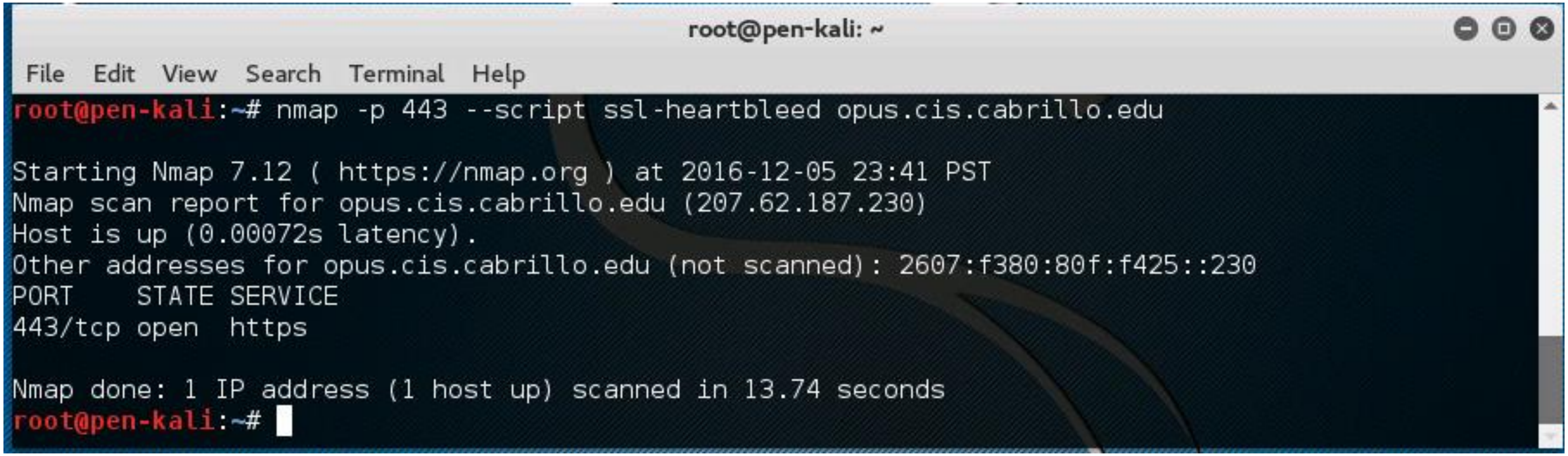
```
0050  0d 0a 28 29 20 7b 20 3a  3b 7d 3b 20 65 63 68 6f   ..() { : ;}; echo
0060  3b 20 65 63 68 6f 20 22  59 4b 53 4d 50 47 51 44   ; echo " YKSMPGQD
0070  5a 4e 47 47 47 44 50 22  3a 20 28 29 20 7b 20 3a   ZNGGGDP" : () { :
0080  3b 7d 3b 20 65 63 68 6f  3b 20 65 63 68 6f 20 22   ;}; echo ; echo "
0090  59 4b 53 4d 50 47 51 44  5a 4e 47 47 47 44 50 22   YKSMPGQD ZNGGGDP"
00a0  0d 0a 43 6f 6e 6e 65 63  74 69 6f 6e 3a 20 63 6c   ..Connec tion: cl
00b0  6f 73 65 0d 0a 48 6f 73  74 3a 20 73 75 6e 2d 68   ose..Hos t: sun-h
00c0  77 61 2e 63 69 73 2e 63  61 62 72 69 6c 6c 6f 2e   wa.cis.c abrillo.
00d0  65 64 75 0d 0a 55 73 65  72 2d 41 67 65 6e 74 3a   edu..Use r-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 "Y KSMPGQDZ
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 " YKSMPGQD
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 " YKSMPGQD
```

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

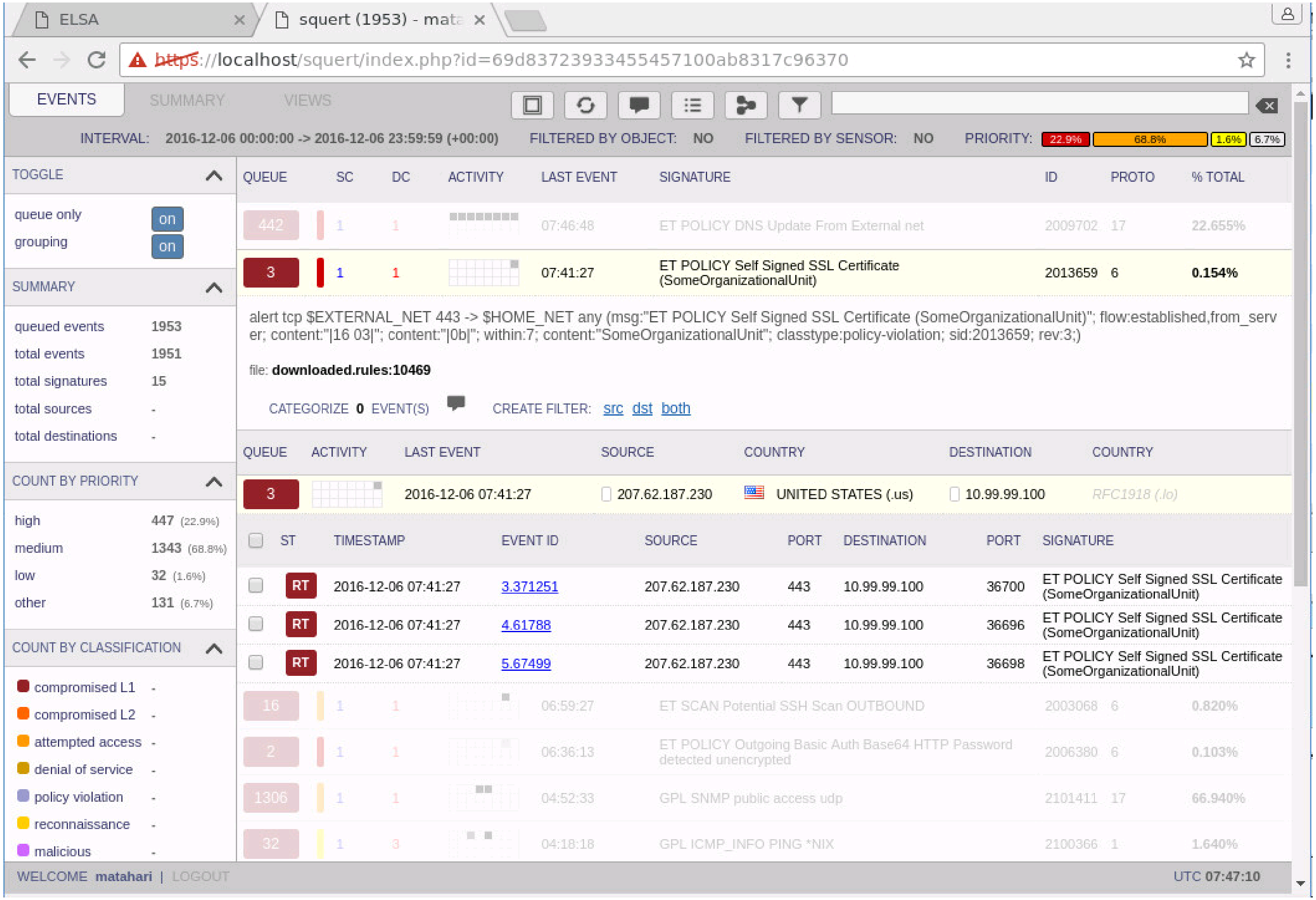
nmap -p 443 --script ssl-heartbleed opus.cis.cabrillo.edu



```
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



~~https~~://localhost/squert/index.php?id=69d83723933455457100ab8317c96370

INTERVAL: 2016-12-06 00:00:00 -> 2016-12-06 23:59:59 (+00:00) FILTERED BY OBJECT: NO FILTERED BY SENSOR: NO PRIORITY: 22.9% 68.8% 1.6% 6.7%

TOGGLE

queue only	on
grouping	on

SUMMARY

queued events	1953
total events	1951
total signatures	15
total sources	-
total destinations	-

COUNT BY PRIORITY

high	447	(22.9%)
medium	1343	(68.8%)
low	32	(1.6%)
other	131	(6.7%)

COUNT BY CLASSIFICATION

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

QUEUE	SC	DC	ACTIVITY	LAST EVENT	SIGNATURE	ID	PROTO	% TOTAL
442	1	1		07:46:48	ET POLICY DNS Update From External net	2009702	17	22.655%
3	1	1		07:41:27	ET POLICY Self Signed SSL Certificate (SomeOrganizationalUnit)	2013659	6	0.154%

```
alert tcp $EXTERNAL_NET 443 -> $HOME_NET any (msg:"ET POLICY Self Signed SSL Certificate (SomeOrganizationalUnit)"; flow:established,from_serv
er; content:"|16 03|"; content:"|0b|"; within:7; content:"SomeOrganizationalUnit"; classtype:policy-violation; sid:2013659; rev:3;)
```

file: **downloaded.rules:10469**

CATEGORIZE **0** EVENT(S) CREATE FILTER: src dst both

QUEUE	ACTIVITY	LAST EVENT	SOURCE	COUNTRY	DESTINATION	COUNTRY
3		2016-12-06 07:41:27	207.62.187.230	UNITED STATES (.us)	10.99.99.100	*RFC1918 (.lo)*

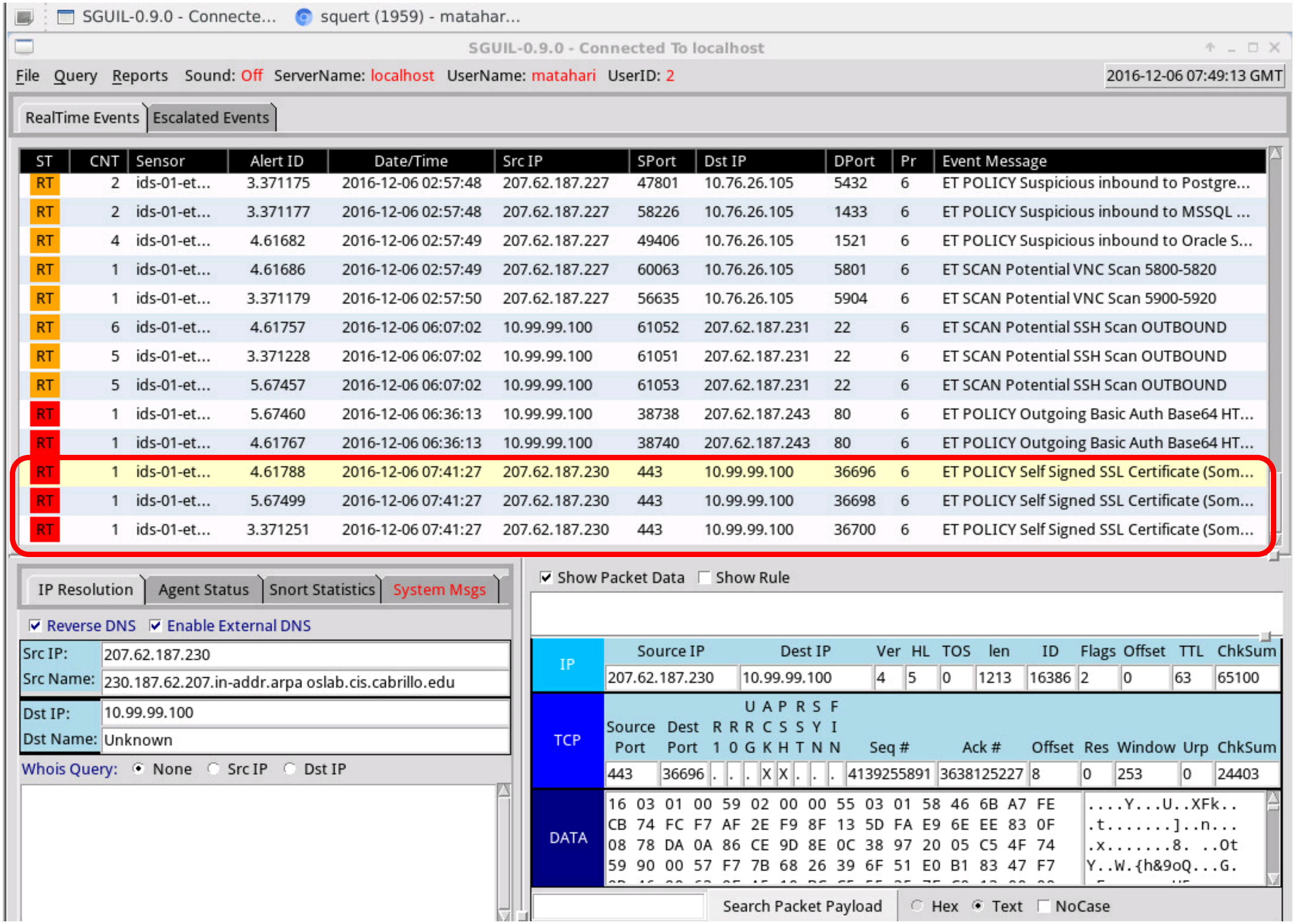
□	ST	TIMESTAMP	EVENT ID	SOURCE	PORT	DESTINATION	PORT	SIGNATURE
□	RT	2016-12-06 07:41:27	3.371251	207.62.187.230	443	10.99.99.100	36700	ET POLICY Self Signed SSL Certificate (SomeOrganizationalUnit)
□	RT	2016-12-06 07:41:27	4.61788	207.62.187.230	443	10.99.99.100	36696	ET POLICY Self Signed SSL Certificate (SomeOrganizationalUnit)
□	RT	2016-12-06 07:41:27	5.67499	207.62.187.230	443	10.99.99.100	36698	ET POLICY Self Signed SSL Certificate (SomeOrganizationalUnit)

QUEUE	SC	DC	ACTIVITY	LAST EVENT	SIGNATURE	ID	PROTO	% TOTAL
16	1	1		06:59:27	ET SCAN Potential SSH Scan OUTBOUND	2003068	6	0.820%
2	1	1		06:36:13	ET POLICY Outgoing Basic Auth Base64 HTTP Password detected unencrypted	2006380	6	0.103%
1306	1	1		04:52:33	GPL SNMP public access udp	2101411	17	66.940%
32	1	3		04:18:18	GPL ICMP_INFO PING *NIX	2100366	1	1.640%

WELCOME **matahari** | LOGOUT UTC **07:47:10**

Squert logs the self-signed certificate sent to attacker

Sguil



Sound: Off ServerName: localhost UserName: matahari UserID: 2 2016-12-06 07:49:13 GMT

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...

☑ 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
	207.62.187.230	10.99.99.100	4	5	0	1213	16386	2	0	63	65100

TCP	Source Port	Dest Port	R 1	R 0	U R G	A C K	P S H	R S T	S Y N	F I N	Seq #	Ack #	Offset	Res	Window	Urp	ChkSum
	443	36696	.	.	.	X	X	.	.	.	4139255891	3638125227	8	0	253	0	24403

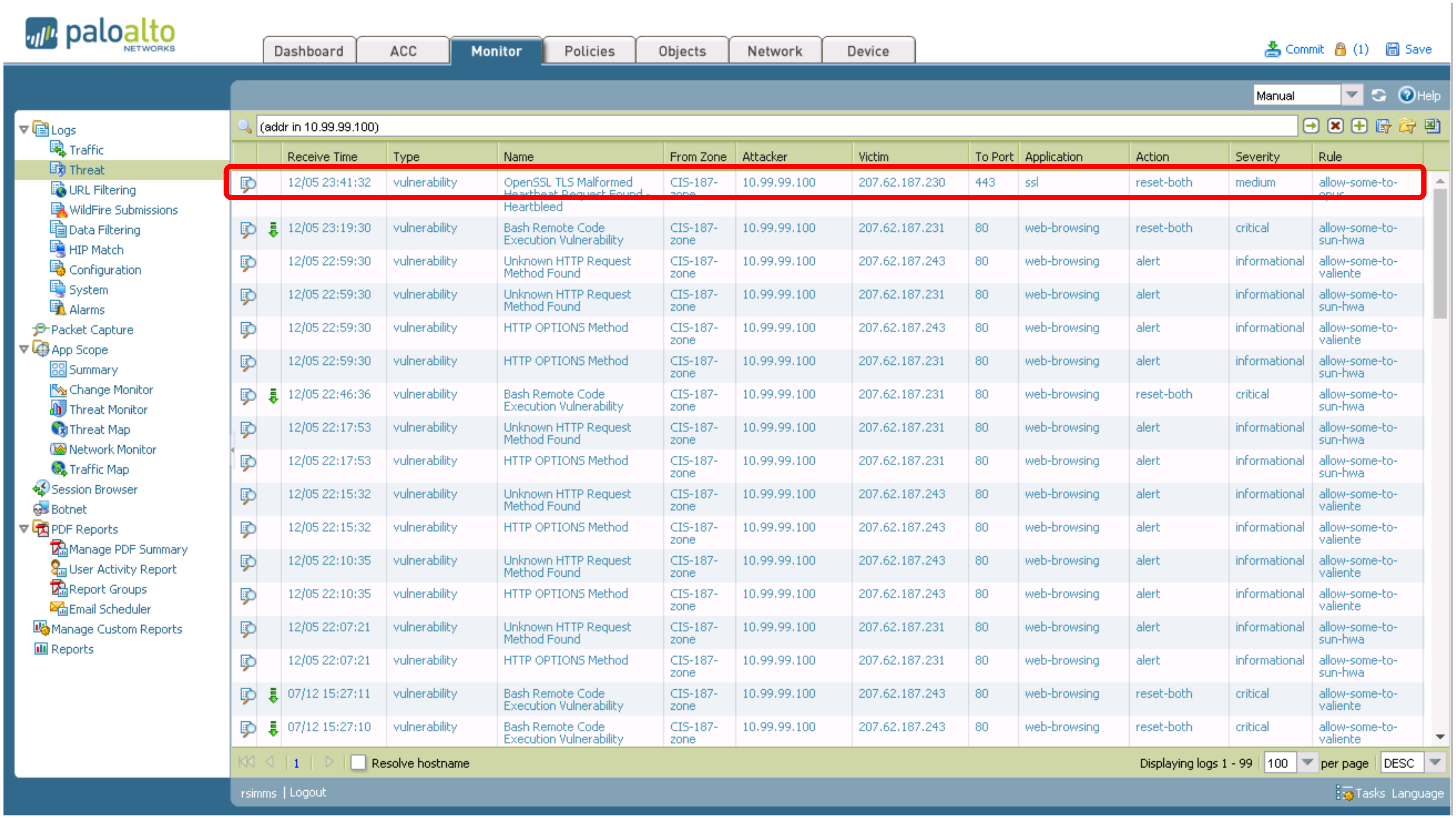
DATA

```
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. ..Ot
59 90 00 57 F7 7B 68 26 39 6F 51 E0 B1 83 47 F7   Y..W.{h&9oQ...G.
```

○ Hex ● Text □ NoCase

Sguil logs the self-signed certificate sent to attacker

PAN



(addr in 10.99.99.100)

	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	10.99.99.100	207.62.187.230	443	ssl	reset-both	medium	allow-some-to-opus
⬇	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

1 □ Resolve hostname

Displaying logs 1 - 99 100 per page DESC

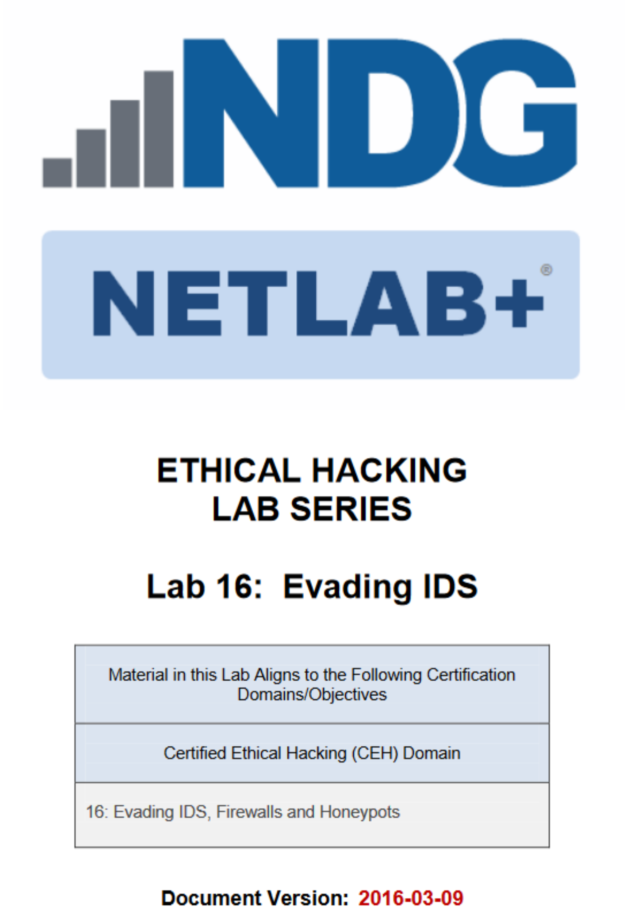
PAN logs it and resets the connection

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



NDG

NETLAB+®

ETHICAL HACKING
LAB SERIES

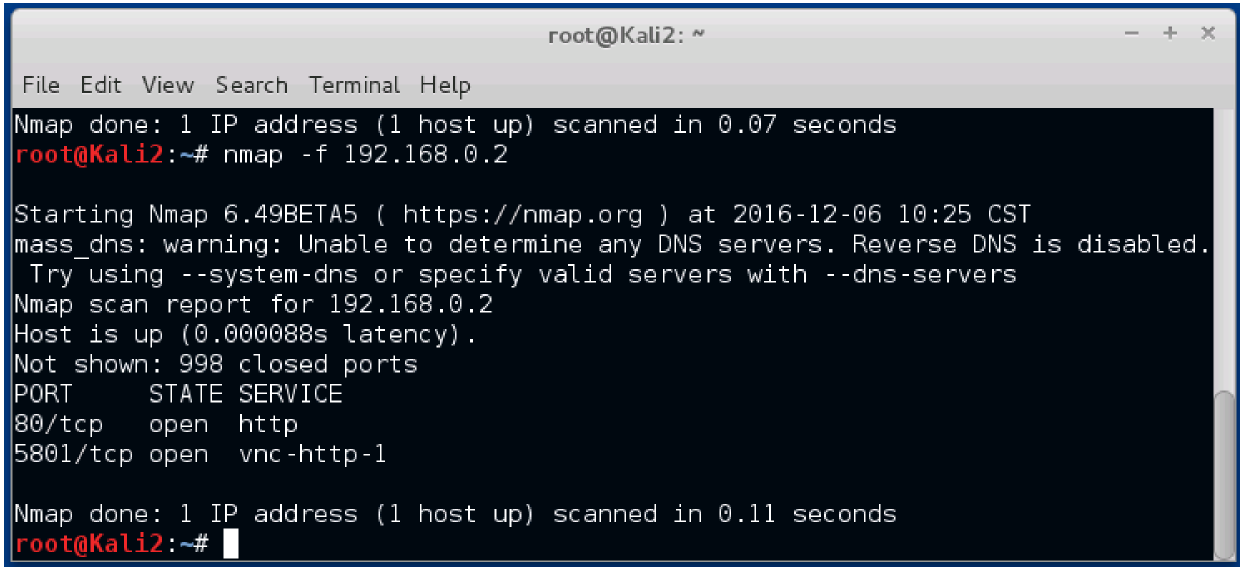
Lab 16: Evading IDS

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

Document Version: 2016-03-09

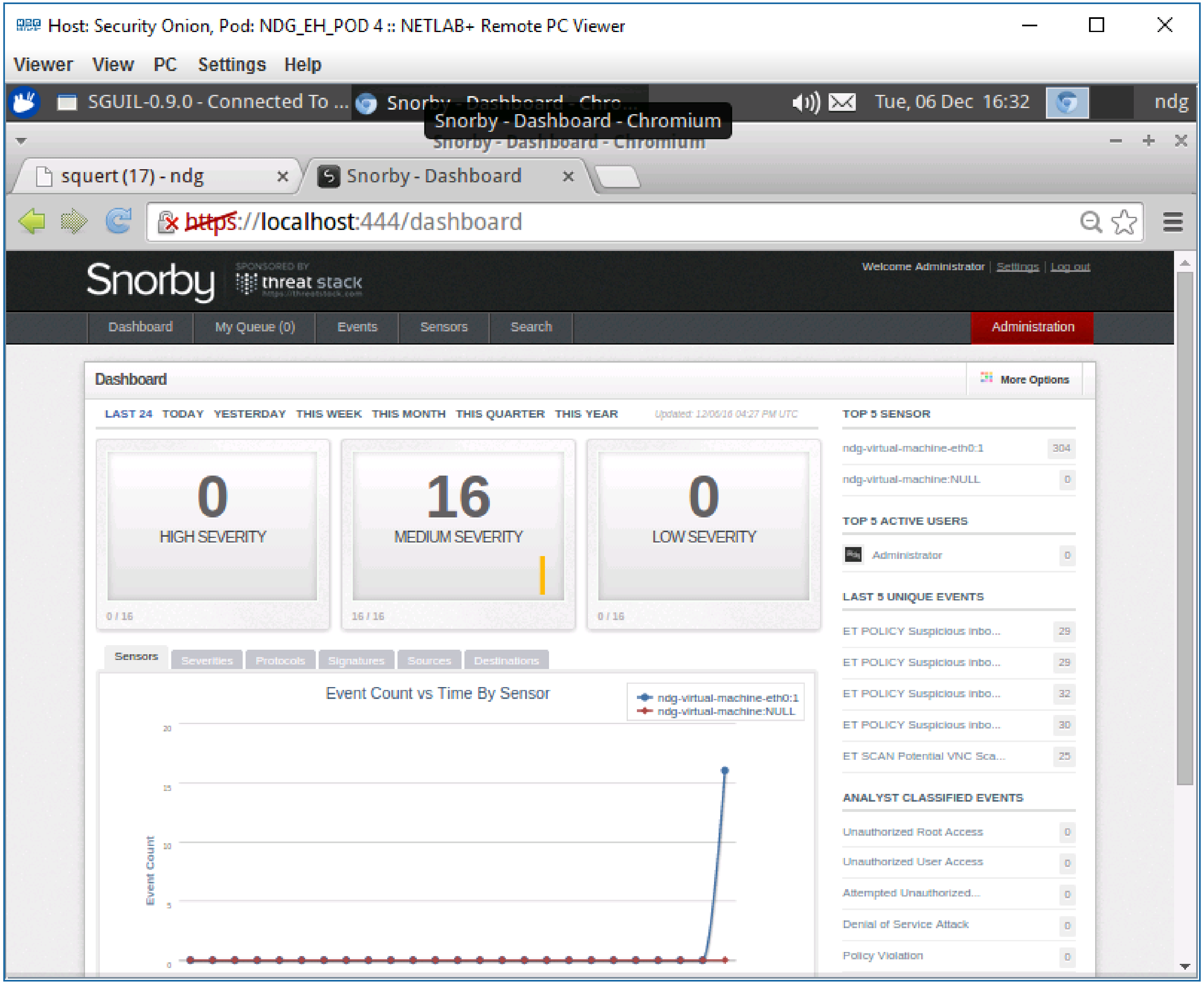
Test IDS Results with Fragmented Scan

nmap -f 192.168.0.2



```
Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
root@Kali2:~# nmap -f 192.168.0.2

Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2016-12-06 10:25 CST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
 Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.0.2
Host is up (0.000088s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
80/tcp   open  http
5801/tcp open  vnc-http-1

Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
root@Kali2:~#
```

This does a fragmented scan



Host: Security Onion, Pod: NDG_EH_POD 4 :: NETLAB+ Remote PC Viewer

SGUIL-0.9.0 - Connected To ... | Snorby - Dashboard - Chro... | Tue, 06 Dec 16:32 | ndg

Snorby - Dashboard - Chromium

squert (17) - ndg | Snorby - Dashboard

~~https~~://localhost:444/dashboard

Welcome Administrator | Settings | Log out

Dashboard

LAST 24 TODAY YESTERDAY THIS WEEK THIS MONTH THIS QUARTER THIS YEAR Updated: 12/06/16 04:27 PM UTC

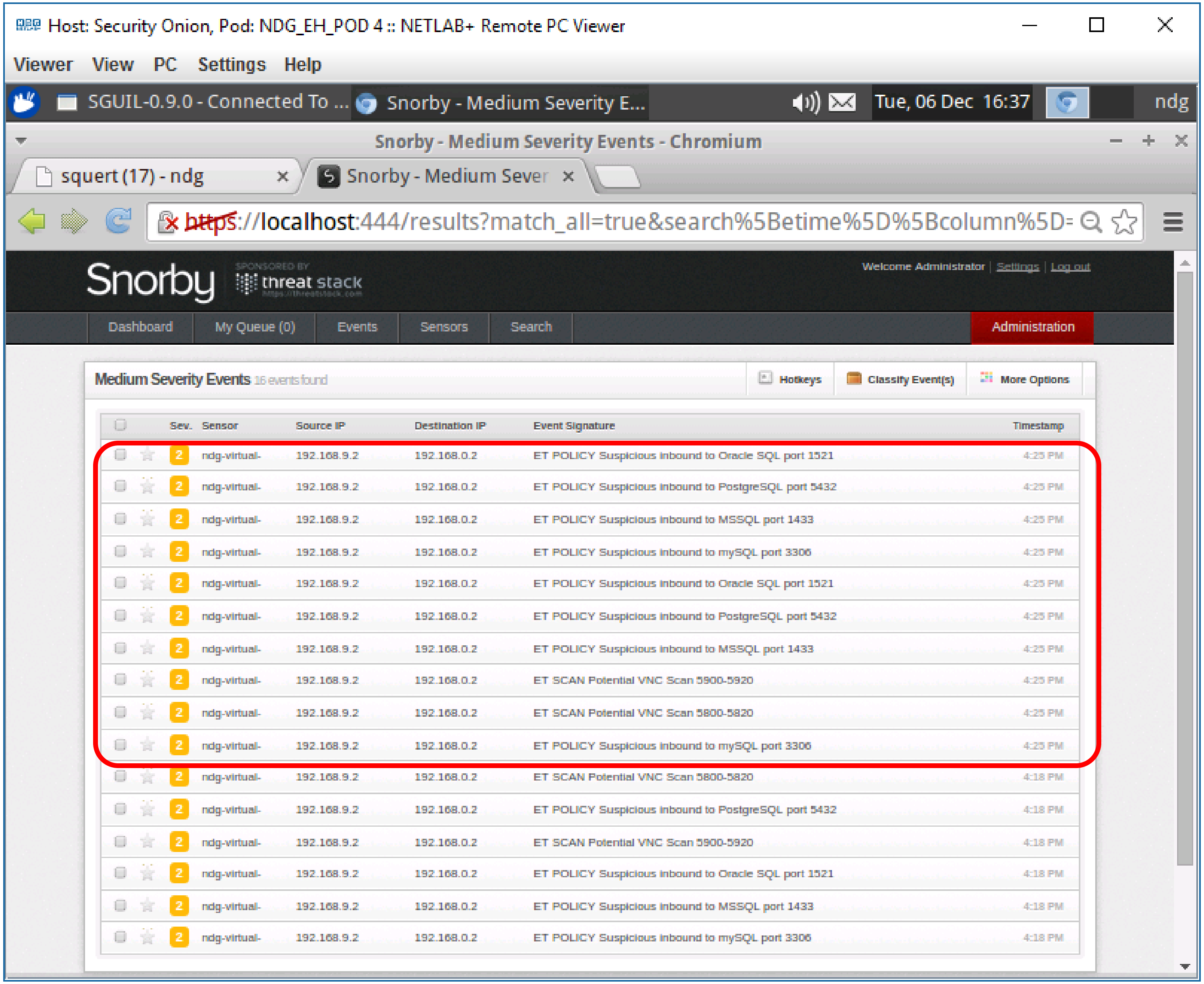
HIGH SEVERITY	MEDIUM SEVERITY	LOW SEVERITY
0	16	0
0 / 16	16 / 16	0 / 16

TOP 5 SENSOR	
ndg-virtual-machine-eth0:1	304
ndg-virtual-machine:NULL	0

TOP 5 ACTIVE USERS	
Administrator	0

LAST 5 UNIQUE EVENTS	
ET POLICY Suspicious inbo...	29
ET POLICY Suspicious inbo...	29
ET POLICY Suspicious inbo...	32
ET POLICY Suspicious inbo...	30
ET SCAN Potential VNC Sca...	25

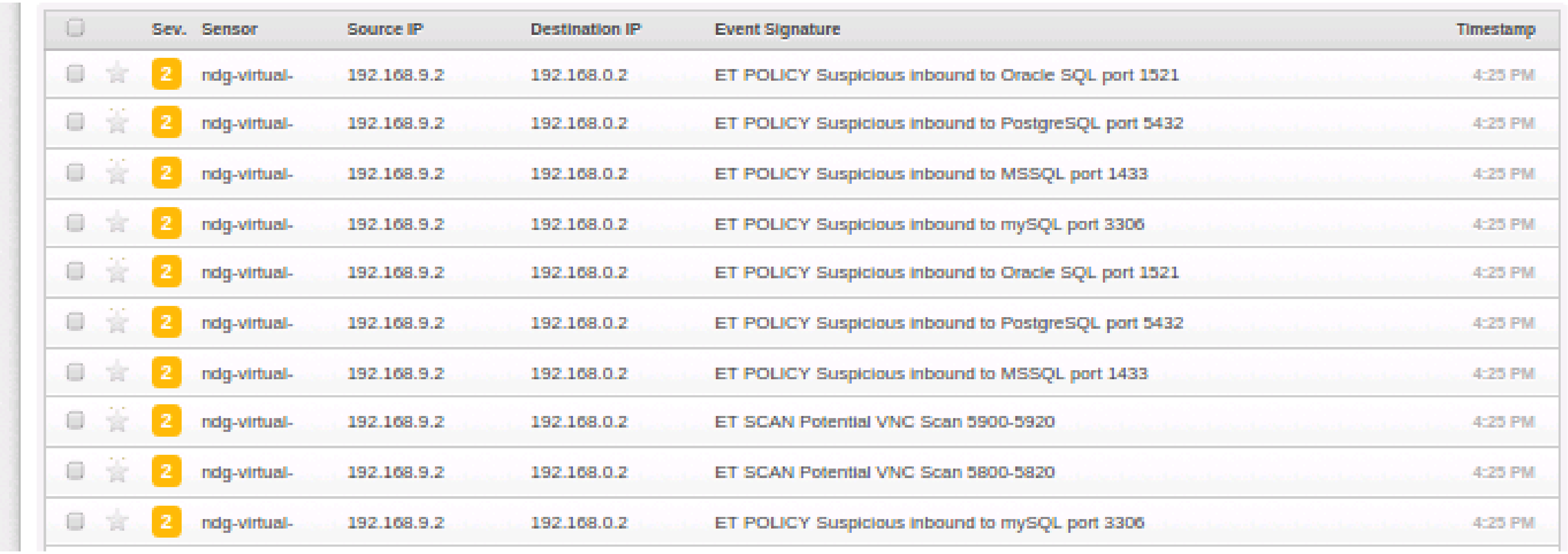
ANALYST CLASSIFIED EVENTS	
Unauthorized Root Access	0
Unauthorized User Access	0
Attempted Unauthorized...	0
Denial of Service Attack	0
Policy Violation	0



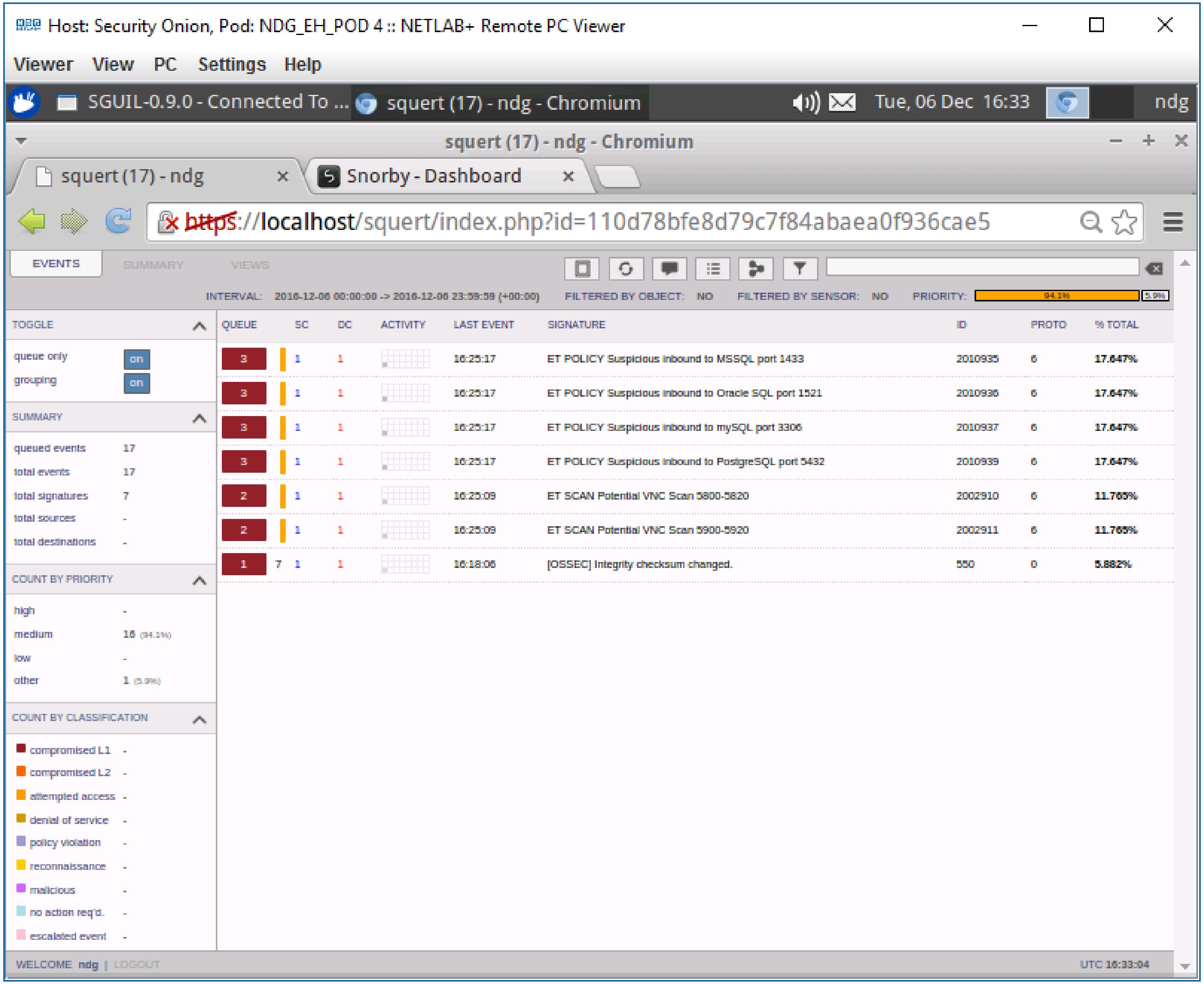
Host: Security Onion, Pod: NDG_EH_POD 4 :: NETLAB+ Remote PC Viewer
Viewer View PC Settings Help
SGUIL-0.9.0 - Connected To ...
Snorby - Medium Severity E...
Tue, 06 Dec 16:37
ndg
Snorby - Medium Severity Events - Chromium
squert (17) - ndg
Snorby - Medium Sever
https://localhost:444/results?match_all=true&search%5Betime%5D%5Bcolumn%5D=
Snorby
SPONSORED BY threat stack
Welcome Administrator | Settings | Log out
Dashboard
My Queue (0)
Events
Sensors
Search
Administration
Hotkeys
Classify Event(s)
More Options

Medium Severity Events 16 events found

□		Sev.	Sensor	Source IP	Destination IP	Event Signature	Timestamp
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET POLICY Suspicious inbound to Oracle SQL port 1521	4:25 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET POLICY Suspicious inbound to PostgreSQL port 5432	4:25 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET POLICY Suspicious inbound to MSSQL port 1433	4:25 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET POLICY Suspicious inbound to mySQL port 3306	4:25 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET POLICY Suspicious inbound to Oracle SQL port 1521	4:25 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET POLICY Suspicious inbound to PostgreSQL port 5432	4:25 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET POLICY Suspicious inbound to MSSQL port 1433	4:25 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET SCAN Potential VNC Scan 5900-5920	4:25 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET SCAN Potential VNC Scan 5800-5820	4:25 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET POLICY Suspicious inbound to mySQL port 3306	4:25 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET SCAN Potential VNC Scan 5800-5820	4:18 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET POLICY Suspicious inbound to PostgreSQL port 5432	4:18 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET SCAN Potential VNC Scan 5900-5920	4:18 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET POLICY Suspicious inbound to Oracle SQL port 1521	4:18 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET POLICY Suspicious inbound to MSSQL port 1433	4:18 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET POLICY Suspicious inbound to mySQL port 3306	4:18 PM



□		Sev.	Sensor	Source IP	Destination IP	Event Signature	Timestamp
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET POLICY Suspicious inbound to Oracle SQL port 1521	4:25 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET POLICY Suspicious inbound to PostgreSQL port 5432	4:25 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET POLICY Suspicious inbound to MSSQL port 1433	4:25 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET POLICY Suspicious inbound to mySQL port 3306	4:25 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET POLICY Suspicious inbound to Oracle SQL port 1521	4:25 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET POLICY Suspicious inbound to PostgreSQL port 5432	4:25 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET POLICY Suspicious inbound to MSSQL port 1433	4:25 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET SCAN Potential VNC Scan 5900-5920	4:25 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET SCAN Potential VNC Scan 5800-5820	4:25 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET POLICY Suspicious inbound to mySQL port 3306	4:25 PM


Host: Security Onion, Pod: NDG_EH_POD 4 :: NETLAB+ Remote PC Viewer
Viewer
View
PC
Settings
Help
SGUIL-0.9.0 - Connected To ...
squert (17) - ndg - Chromium
Tue, 06 Dec 16:33
ndg
squert (17) - ndg - Chromium
squert (17) - ndg
Snorby - Dashboard
EVENTS
SUMMARY
VIEWS

~~https~~://localhost/squert/index.php?id=110d78bfe8d79c7f84abaea0f936cae5

INTERVAL: 2016-12-06 00:00:00 -> 2016-12-06 23:59:59 (+00:00) FILTERED BY OBJECT: NO FILTERED BY SENSOR: NO PRIORITY: 94.1% 5.9%

TOGGLE

queue only	on
grouping	on

SUMMARY

queued events	17
total events	17
total signatures	7
total sources	-
total destinations	-

COUNT BY PRIORITY

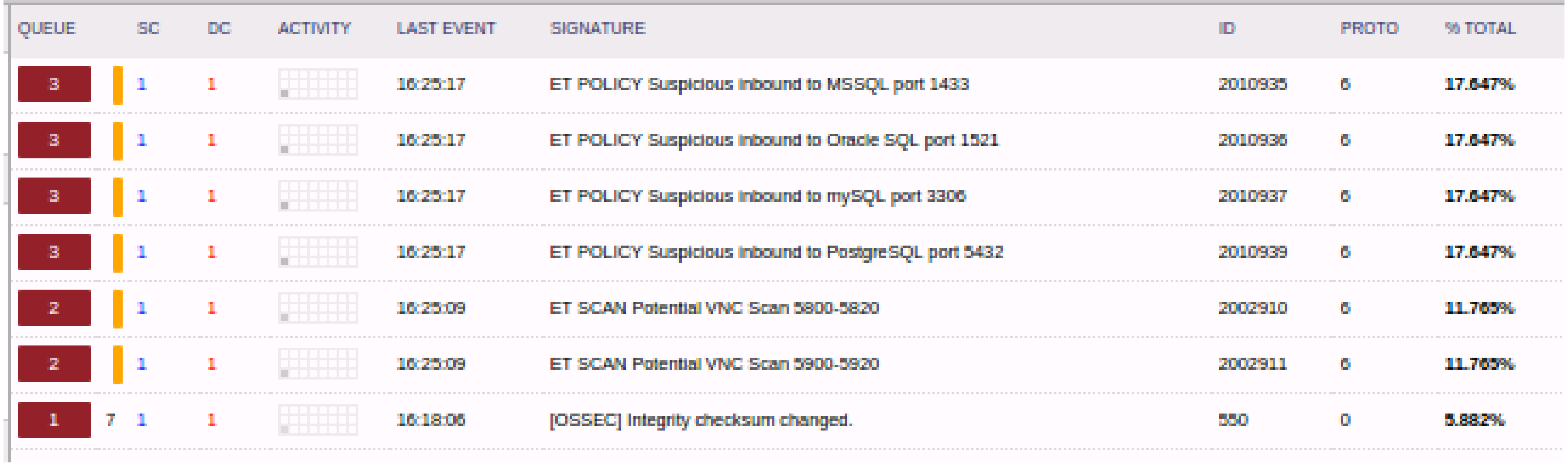
high	-
medium	16 (94.1%)
low	-
other	1 (5.9%)

COUNT BY CLASSIFICATION

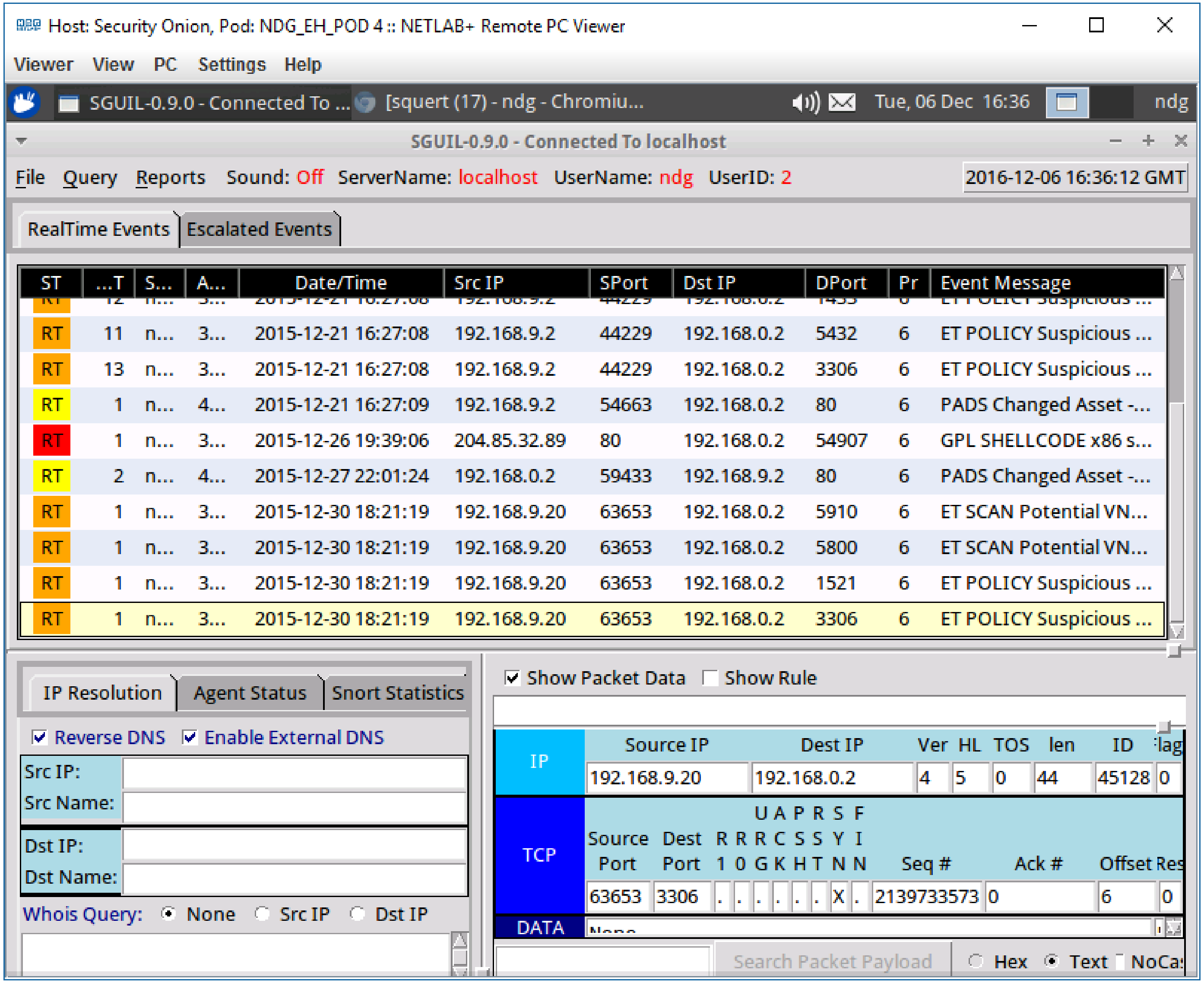
🟥	compromised L1	-
🟧	compromised L2	-
🟧	attempted access	-
🟫	denial of service	-
🟪	policy violation	-
🟨	reconnaissance	-
🟪	malicious	-
🟦	no action req'd.	-
🟥	escalated event	-

QUEUE		SC	DC	ACTIVITY	LAST EVENT	SIGNATURE	ID	PROTO	% TOTAL
3		1	1		16:25:17	ET POLICY Suspicious inbound to MSSQL port 1433	2010935	6	17.647%
3		1	1		16:25:17	ET POLICY Suspicious inbound to Oracle SQL port 1521	2010936	6	17.647%
3		1	1		16:25:17	ET POLICY Suspicious inbound to mySQL port 3306	2010937	6	17.647%
3		1	1		16:25:17	ET POLICY Suspicious inbound to PostgreSQL port 5432	2010939	6	17.647%
2		1	1		16:25:09	ET SCAN Potential VNC Scan 5800-5820	2002910	6	11.765%
2		1	1		16:25:09	ET SCAN Potential VNC Scan 5900-5920	2002911	6	11.765%
1	7	1	1		16:18:06	[OSSEC] Integrity checksum changed.	550	0	5.882%

WELCOME ndg | LOGOUT UTC 16:33:04



QUEUE		SC	DC	ACTIVITY	LAST EVENT	SIGNATURE	ID	PROTO	% TOTAL
3		1	1		16:25:17	ET POLICY Suspicious inbound to MSSQL port 1433	2010935	6	17.647%
3		1	1		16:25:17	ET POLICY Suspicious inbound to Oracle SQL port 1521	2010936	6	17.647%
3		1	1		16:25:17	ET POLICY Suspicious inbound to mySQL port 3306	2010937	6	17.647%
3		1	1		16:25:17	ET POLICY Suspicious inbound to PostgreSQL port 5432	2010939	6	17.647%
2		1	1		16:25:09	ET SCAN Potential VNC Scan 5800-5820	2002910	6	11.765%
2		1	1		16:25:09	ET SCAN Potential VNC Scan 5900-5920	2002911	6	11.765%
1	7	1	1		16:18:06	[OSSEC] Integrity checksum changed.	550	0	5.882%



Host: Security Onion, Pod: NDG_EH_POD 4 :: NETLAB+ Remote PC Viewer

Viewer View PC Settings Help

SGUIL-0.9.0 - Connected To ... [squert (17) - ndg - Chromiu... Tue, 06 Dec 16:36 ndg

SGUIL-0.9.0 - Connected To localhost

File Query Reports Sound: Off ServerName: localhost UserName: ndg UserID: 2 2016-12-06 16:36:12 GMT

RealTime Events Escalated Events

ST	...T	S...	A...	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	11	n...	3...	2015-12-21 16:27:08	192.168.9.2	44229	192.168.0.2	5432	6	ET POLICY Suspicious ...
RT	13	n...	3...	2015-12-21 16:27:08	192.168.9.2	44229	192.168.0.2	3306	6	ET POLICY Suspicious ...
RT	1	n...	4...	2015-12-21 16:27:09	192.168.9.2	54663	192.168.0.2	80	6	PADS Changed Asset -...
RT	1	n...	3...	2015-12-26 19:39:06	204.85.32.89	80	192.168.0.2	54907	6	GPL SHELLCODE x86 s...
RT	2	n...	4...	2015-12-27 22:01:24	192.168.0.2	59433	192.168.9.2	80	6	PADS Changed Asset -...
RT	1	n...	3...	2015-12-30 18:21:19	192.168.9.20	63653	192.168.0.2	5910	6	ET SCAN Potential VN...
RT	1	n...	3...	2015-12-30 18:21:19	192.168.9.20	63653	192.168.0.2	5800	6	ET SCAN Potential VN...
RT	1	n...	3...	2015-12-30 18:21:19	192.168.9.20	63653	192.168.0.2	1521	6	ET POLICY Suspicious ...
RT	1	n...	3...	2015-12-30 18:21:19	192.168.9.20	63653	192.168.0.2	3306	6	ET POLICY Suspicious ...

☑ Reverse DNS ☑ Enable External DNS

Src IP:
Src Name:
Dst IP:
Dst Name:

Whois Query: ● None ○ Src IP ○ Dst IP

☑ Show Packet Data □ Show Rule

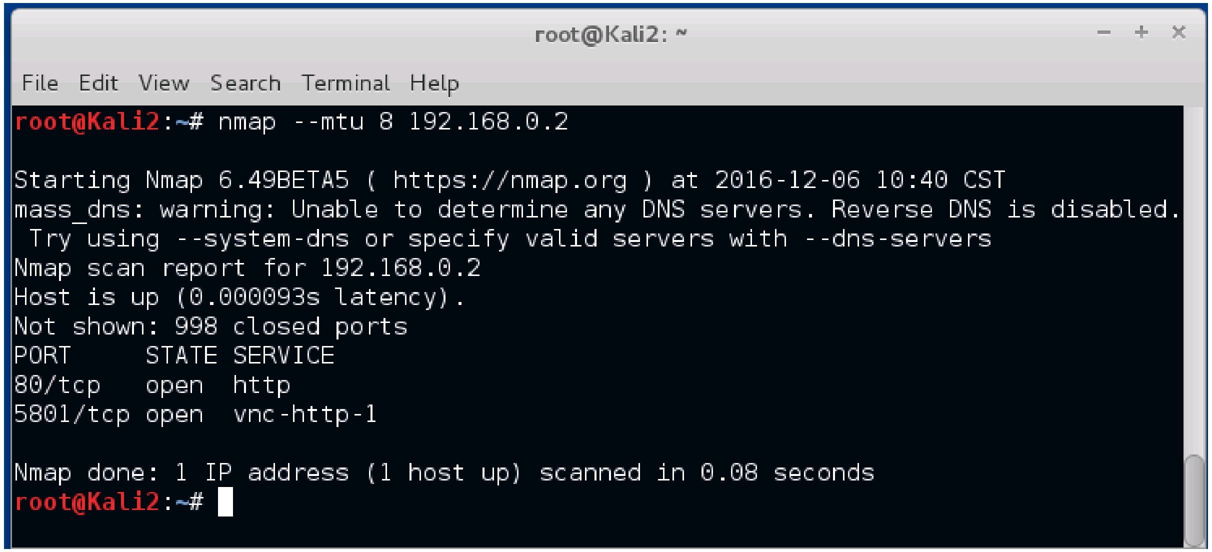
IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	lag
	192.168.9.20	192.168.0.2	4	5	0	44	45128	0

TCP	Source Port	Dest Port	R 1	R 0	U R G	A C K	P S H	R S T	S Y N	F I N	Seq #	Ack #	Offset	Res
	63653	3306	.	.	.	.	.	.	X	.	2139733573	0	6	0

DATA None

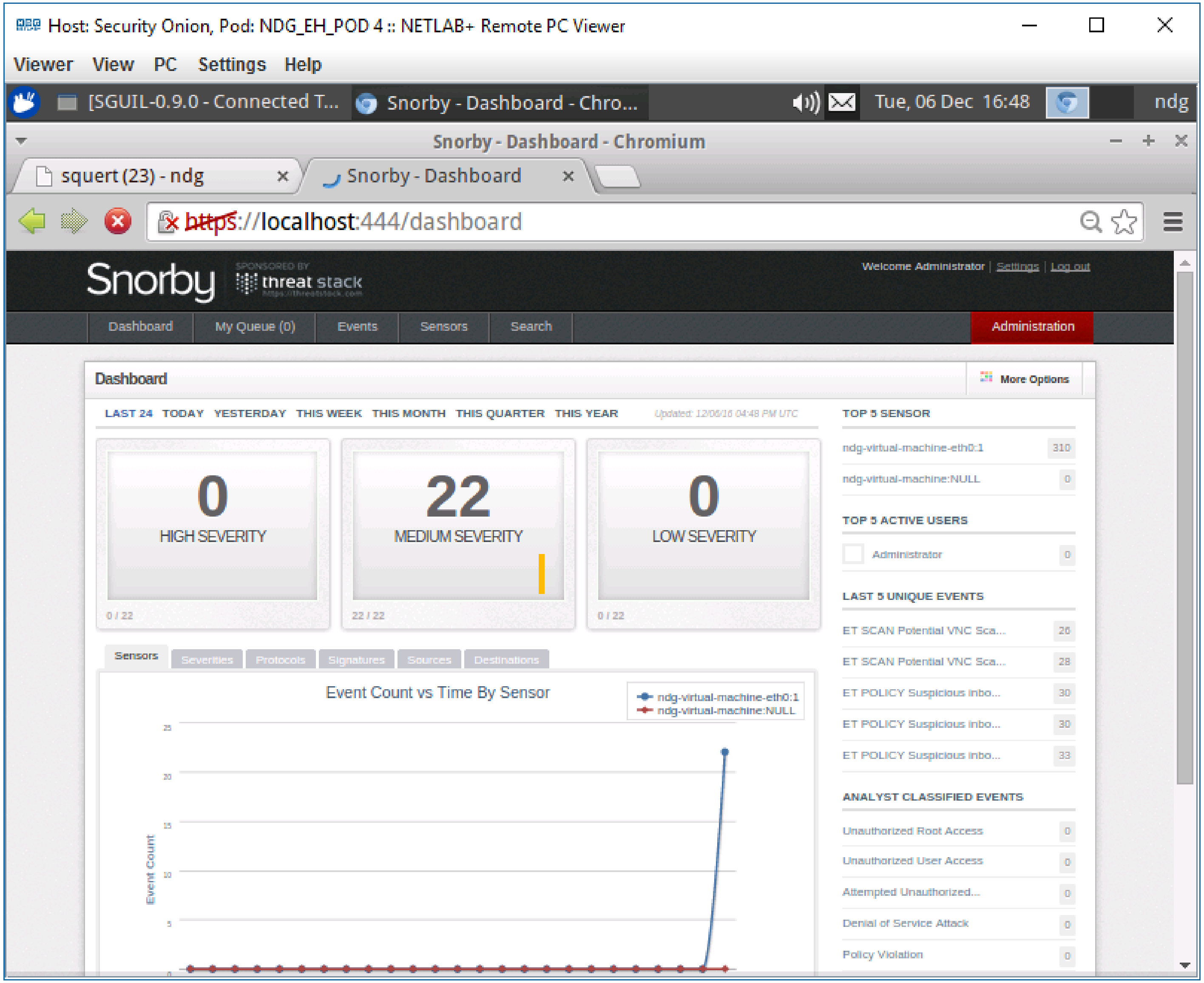
Test IDS Results with Low MTU Scan

nmap --mtu 8 192.168.0.2



```
root@Kali2:~# nmap --mtu 8 192.168.0.2

Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2016-12-06 10:40 CST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
 Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.0.2
Host is up (0.000093s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
80/tcp   open  http
5801/tcp open  vnc-http-1

Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
root@Kali2:~#
```

This does a fragmented scan by limiting the MTU (maximum transmission unit)


Host: Security Onion, Pod: NDG_EH_POD 4 :: NETLAB+ Remote PC Viewer
Viewer
View
PC
Settings
Help
[SGUIL-0.9.0 - Connected T...
Snorby - Dashboard - Chro...
Tue, 06 Dec 16:48
ndg
Snorby - Dashboard - Chromium
squert (23) - ndg
Snorby - Dashboard
~~https~~://localhost:444/dashboard
Snorby
SPONSORED BY threat stack https://threatstack.com
Welcome Administrator | Settings | Log out
Dashboard
My Queue (0)
Events
Sensors
Search
Administration
More Options
Sensors
Severities
Protocols
Signatures
Sources
Destinations
Event Count vs Time By Sensor
ndg-virtual-machine-eth0:1
ndg-virtual-machine:NULL
Event Count
25
20
15
10
5
0

Dashboard

LAST 24 TODAY YESTERDAY THIS WEEK THIS MONTH THIS QUARTER THIS YEAR Updated: 12/06/16 04:48 PM UTC

0 HIGH SEVERITY 0 / 22	22 MEDIUM SEVERITY 22 / 22	0 LOW SEVERITY 0 / 22

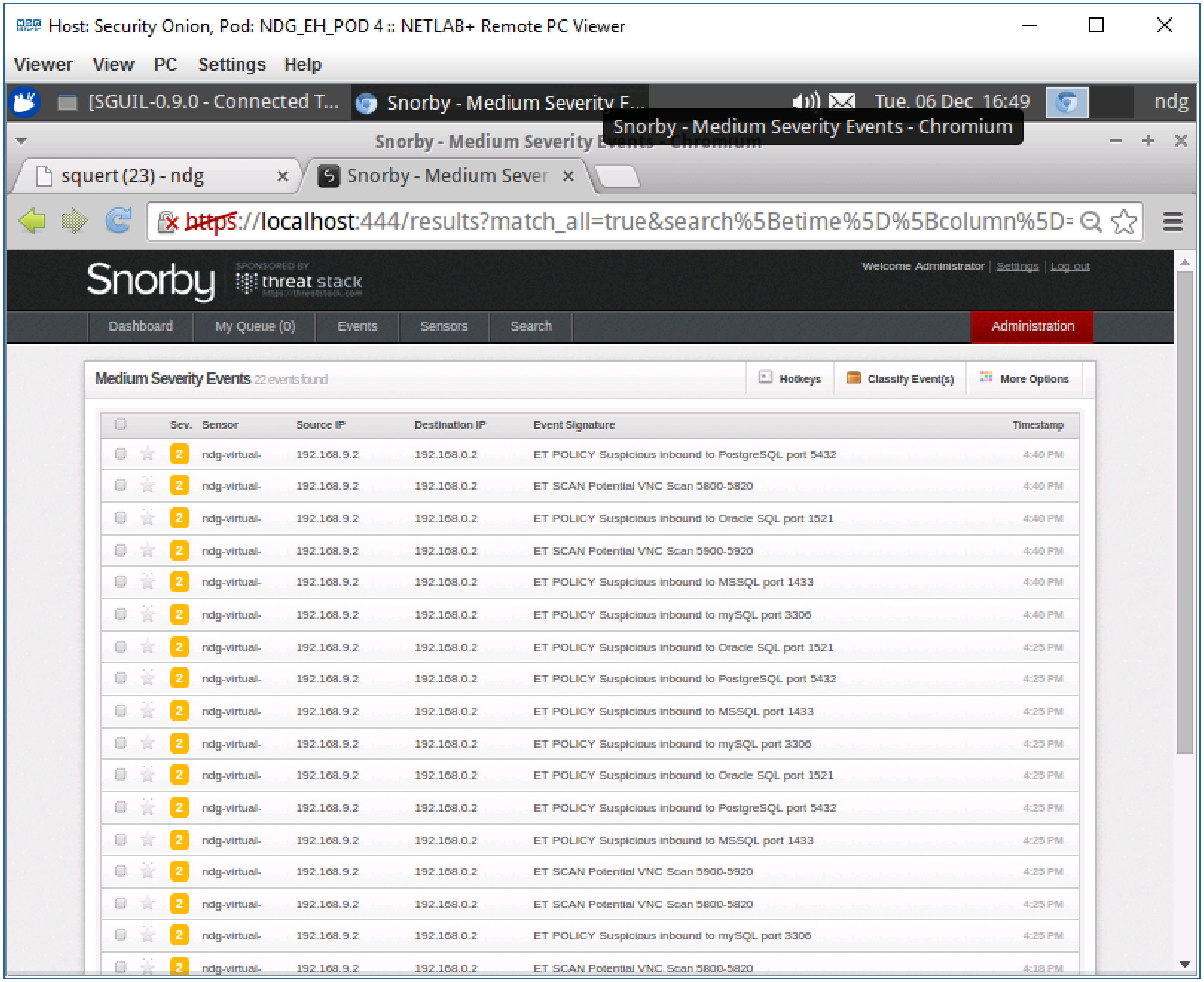
TOP 5 SENSOR	
ndg-virtual-machine-eth0:1	310
ndg-virtual-machine:NULL	0

TOP 5 ACTIVE USERS	
Administrator	0

LAST 5 UNIQUE EVENTS	
ET SCAN Potential VNC Sca...	26
ET SCAN Potential VNC Sca...	28
ET POLICY Suspicious inbo...	30
ET POLICY Suspicious inbo...	30
ET POLICY Suspicious inbo...	33

ANALYST CLASSIFIED EVENTS	
Unauthorized Root Access	0
Unauthorized User Access	0
Attempted Unauthorized...	0
Denial of Service Attack	0
Policy Violation	0

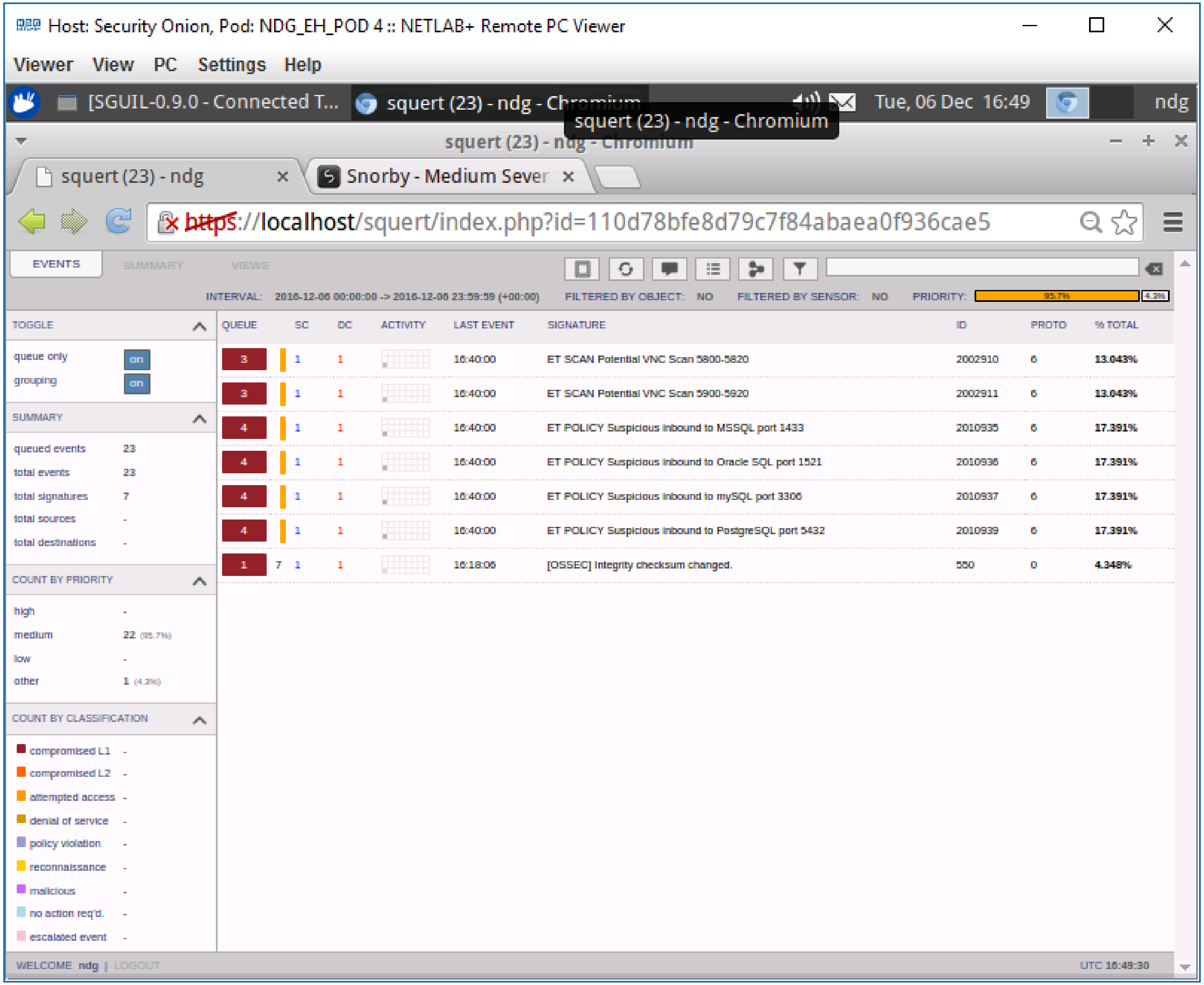
Snorby did catch last scan


Host: Security Onion, Pod: NDG_EH_POD 4 :: NETLAB+ Remote PC Viewer
Viewer
View
PC
Settings
Help
[SGUIL-0.9.0 - Connected T...
Snorby - Medium Severity E...
Tue. 06 Dec 16:49
ndg
Snorby - Medium Severity Events - Chromium
squert (23) - ndg
Snorby - Medium Sever
~~https~~://localhost:444/results?match_all=true&search%5Betime%5D%5Bcolumn%5D=
Snorby
SPONSORED BY threat stack
Welcome Administrator | Settings | Log out
Dashboard
My Queue (0)
Events
Sensors
Search
Administration
Hotkeys
Classify Event(s)
More Options

Medium Severity Events 22 events found

□		Sev.	Sensor	Source IP	Destination IP	Event Signature	Timestamp
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET POLICY Suspicious inbound to PostgreSQL port 5432	4:40 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET SCAN Potential VNC Scan 5800-5820	4:40 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET POLICY Suspicious inbound to Oracle SQL port 1521	4:40 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET SCAN Potential VNC Scan 5900-5920	4:40 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET POLICY Suspicious inbound to MSSQL port 1433	4:40 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET POLICY Suspicious inbound to mySQL port 3306	4:40 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET POLICY Suspicious inbound to Oracle SQL port 1521	4:25 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET POLICY Suspicious inbound to PostgreSQL port 5432	4:25 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET POLICY Suspicious inbound to MSSQL port 1433	4:25 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET POLICY Suspicious inbound to mySQL port 3306	4:25 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET POLICY Suspicious inbound to Oracle SQL port 1521	4:25 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET POLICY Suspicious inbound to PostgreSQL port 5432	4:25 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET POLICY Suspicious inbound to MSSQL port 1433	4:25 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET SCAN Potential VNC Scan 5900-5920	4:25 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET SCAN Potential VNC Scan 5800-5820	4:25 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET POLICY Suspicious inbound to mySQL port 3306	4:25 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET SCAN Potential VNC Scan 5800-5820	4:18 PM

Snorby did catch last scan


Host: Security Onion, Pod: NDG_EH_POD 4 :: NETLAB+ Remote PC Viewer
Viewer
View
PC
Settings
Help
[SGUIL-0.9.0 - Connected T...
squert (23) - ndg - Chromium
Tue, 06 Dec 16:49
ndg
squert (23) - ndg - Chromium
squert (23) - ndg
Snorby - Medium Sever
EVENTS
SUMMARY
VIEWS

~~https~~://localhost/squert/index.php?id=110d78bfe8d79c7f84abaea0f936cae5

INTERVAL: 2016-12-06 00:00:00 -> 2016-12-06 23:59:59 (+00:00) FILTERED BY OBJECT: NO FILTERED BY SENSOR: NO PRIORITY: 95.7% 4.3%

TOGGLE

queue only	on
grouping	on

SUMMARY

queued events	23
total events	23
total signatures	7
total sources	-
total destinations	-

COUNT BY PRIORITY

high	-
medium	22 (95.7%)
low	-
other	1 (4.3%)

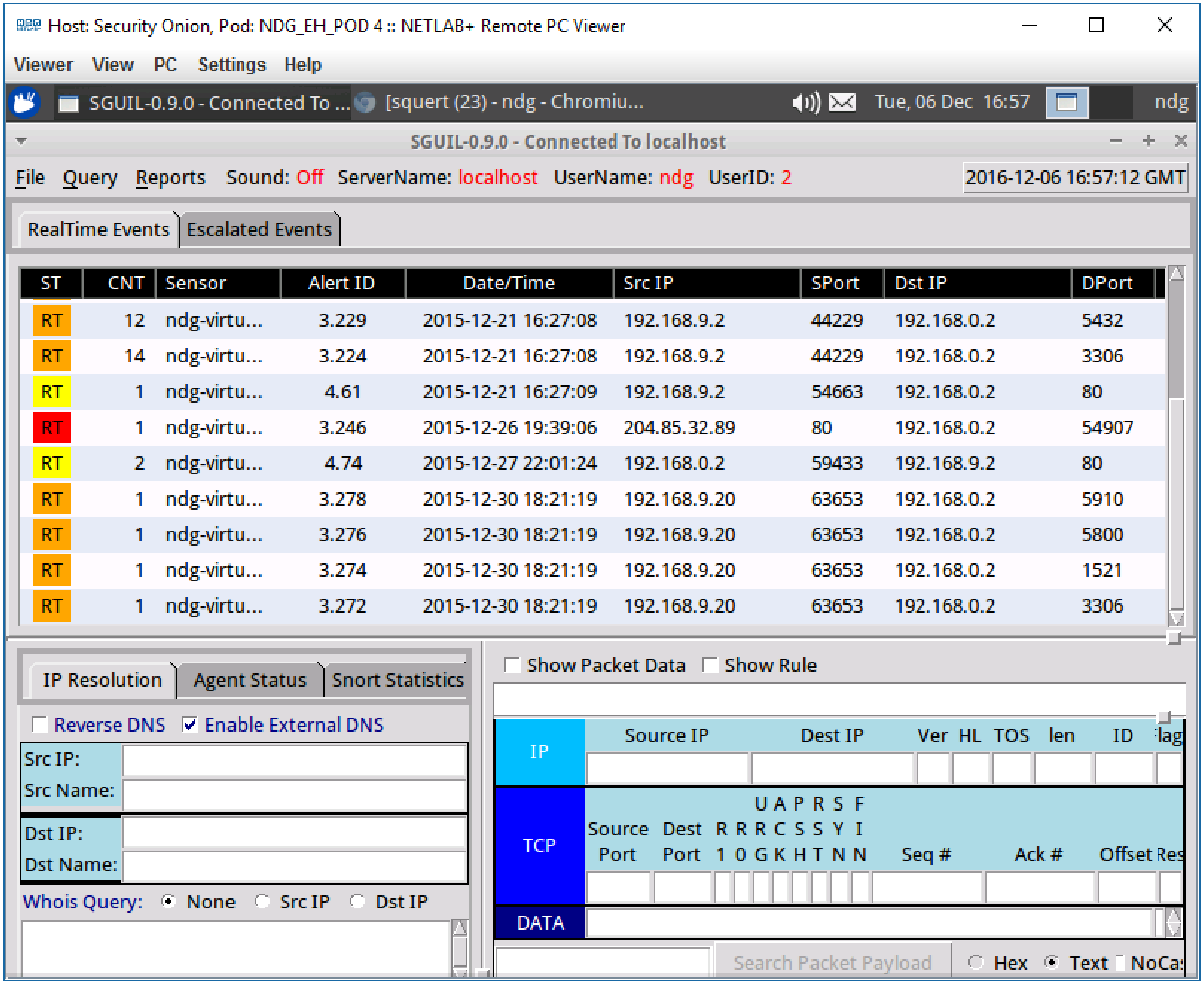
COUNT BY CLASSIFICATION

🟥 compromised L1	-
🟧 compromised L2	-
🟧 attempted access	-
🟫 denial of service	-
🟪 policy violation	-
🟨 reconnaissance	-
🟪 malicious	-
🟦 no action req'd.	-
🟥 escalated event	-

QUEUE		SC	DC	ACTIVITY	LAST EVENT	SIGNATURE	ID	PROTO	% TOTAL
3		1	1		16:40:00	ET SCAN Potential VNC Scan 5800-5820	2002910	6	13.043%
3		1	1		16:40:00	ET SCAN Potential VNC Scan 5900-5920	2002911	6	13.043%
4		1	1		16:40:00	ET POLICY Suspicious inbound to MSSQL port 1433	2010935	6	17.391%
4		1	1		16:40:00	ET POLICY Suspicious inbound to Oracle SQL port 1521	2010936	6	17.391%
4		1	1		16:40:00	ET POLICY Suspicious inbound to mySQL port 3306	2010937	6	17.391%
4		1	1		16:40:00	ET POLICY Suspicious inbound to PostgreSQL port 5432	2010939	6	17.391%
1	7	1	1		16:18:06	[OSSEC] Integrity checksum changed.	550	0	4.348%

WELCOME ndg | LOGOUT UTC 16:49:30

Squert did catch last scan



Host: Security Onion, Pod: NDG_EH_POD 4 :: NETLAB+ Remote PC Viewer

Viewer View PC Settings Help

SGUIL-0.9.0 - Connected To ... [squert (23) - ndg - Chromiu... Tue, 06 Dec 16:57 ndg

SGUIL-0.9.0 - Connected To localhost

File Query Reports Sound: Off ServerName: localhost UserName: ndg UserID: 2 2016-12-06 16:57:12 GMT

RealTime Events | Escalated Events

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort
RT	12	ndg-virtu...	3.229	2015-12-21 16:27:08	192.168.9.2	44229	192.168.0.2	5432
RT	14	ndg-virtu...	3.224	2015-12-21 16:27:08	192.168.9.2	44229	192.168.0.2	3306
RT	1	ndg-virtu...	4.61	2015-12-21 16:27:09	192.168.9.2	54663	192.168.0.2	80
RT	1	ndg-virtu...	3.246	2015-12-26 19:39:06	204.85.32.89	80	192.168.0.2	54907
RT	2	ndg-virtu...	4.74	2015-12-27 22:01:24	192.168.0.2	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
RT	1	ndg-virtu...	3.272	2015-12-30 18:21:19	192.168.9.20	63653	192.168.0.2	3306

IP Resolution | Agent Status | Snort Statistics

□ Reverse DNS ☑ Enable External DNS

Src IP:

Src Name:

Dst IP:

Dst Name:

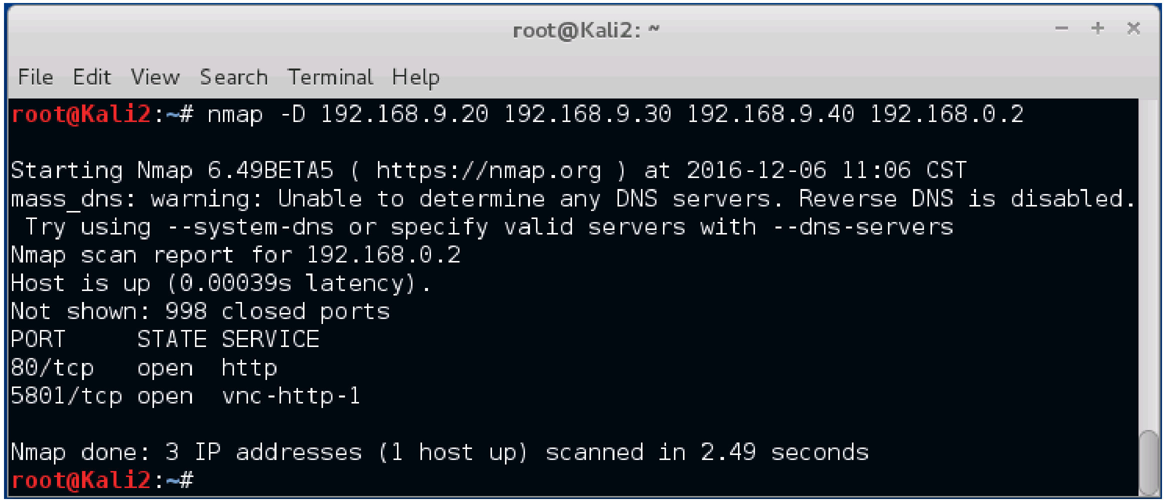
Whois Query: ● None ○ Src IP ○ Dst IP

□ Show Packet Data □ Show Rule

Sguil did NOT catch last scan

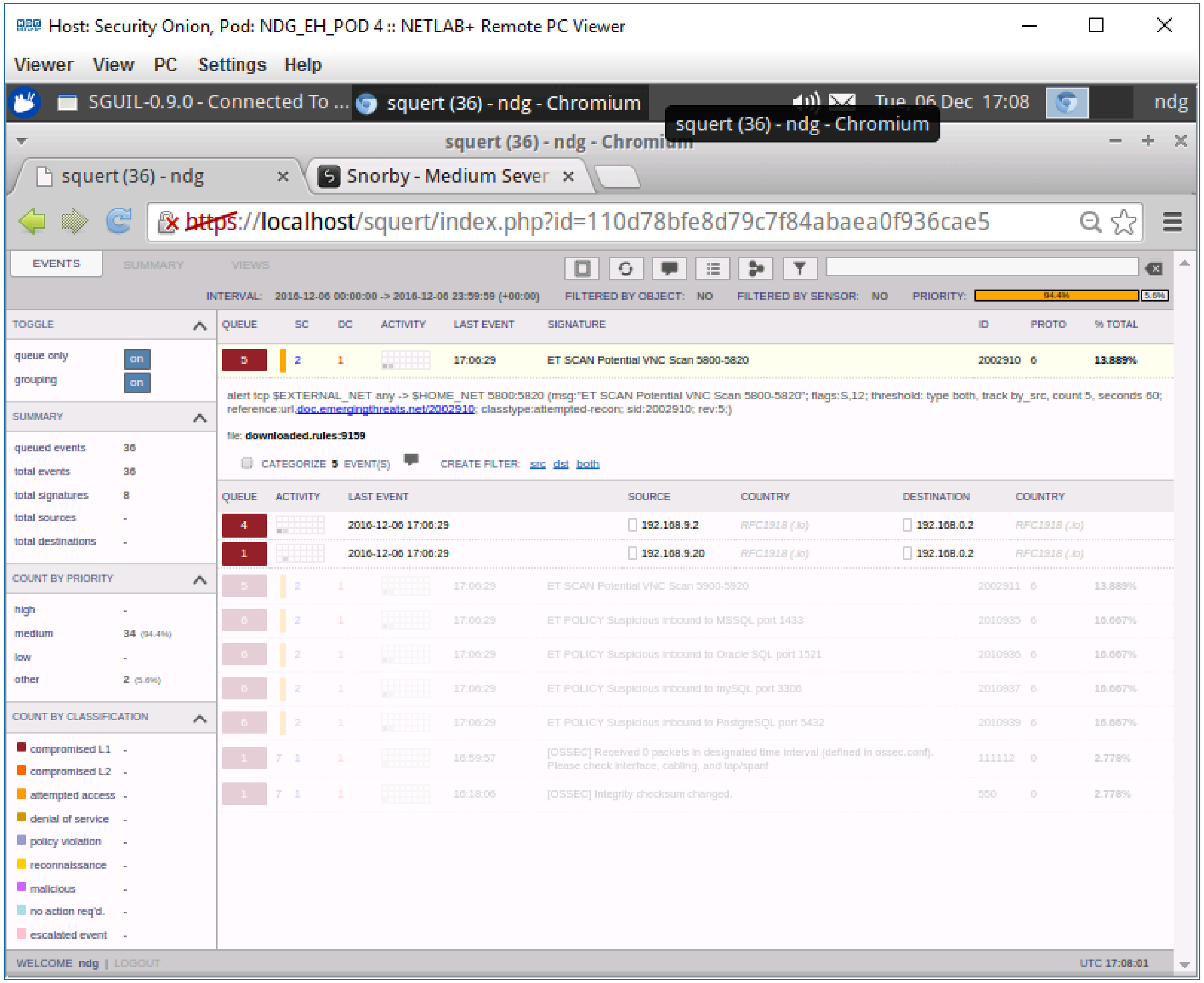
Test IDS Results with Decoy Scan

nmap -D 192.168.0.20 192.168.0.30 192.168.0.40 192.168.0.2



```
root@Kali2:~# nmap -D 192.168.9.20 192.168.9.30 192.168.9.40 192.168.0.2

Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2016-12-06 11:06 CST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
 Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.0.2
Host is up (0.00039s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
80/tcp   open  http
5801/tcp open  vnc-http-1

Nmap done: 3 IP addresses (1 host up) scanned in 2.49 seconds
root@Kali2:~#
```

Cloaked scan using decoy source addresses


Host: Security Onion, Pod: NDG_EH_POD 4 :: NETLAB+ Remote PC Viewer
Viewer View PC Settings Help
SGUIL-0.9.0 - Connected To ...
squert (36) - ndg - Chromium
Tue, 06 Dec 17:08
ndg
squert (36) - ndg - Chromium
squert (36) - ndg
Snorby - Medium Sever
EVENTS
SUMMARY
VIEWS

~~https~~://localhost/squert/index.php?id=110d78bfe8d79c7f84abaea0f936cae5

INTERVAL: 2016-12-06 00:00:00 -> 2016-12-06 23:59:59 (+00:00) FILTERED BY OBJECT: NO FILTERED BY SENSOR: NO PRIORITY: 94.4% 5.6%

TOGGLE	
queue only	on
grouping	on

SUMMARY	
queued events	36
total events	36
total signatures	8
total sources	-
total destinations	-

COUNT BY PRIORITY	
high	-
medium	34 (94.4%)
low	-
other	2 (5.6%)

COUNT BY CLASSIFICATION	
🟥 compromised L1	-
🟧 compromised L2	-
🟧 attempted access	-
🟫 denial of service	-
🟪 policy violation	-
🟨 reconnaissance	-
🟪 malicious	-
🟦 no action req'd.	-
🟥 escalated event	-

QUEUE	SC	DC	ACTIVITY	LAST EVENT	SIGNATURE	ID	PROTO	% TOTAL
5	2	1		17:06:29	ET SCAN Potential VNC Scan 5800-5820	2002910	6	13.889%

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 5800:5820 (msg:"ET SCAN Potential VNC Scan 5800-5820"; flags:S,12; threshold: type both, track by_src, count 5, seconds 60; reference:url,doc.emergingthreats.net/2002910; classtype:attempted-recon; sid:2002910; rev:5;)
```

file: **downloaded.rules:9159**

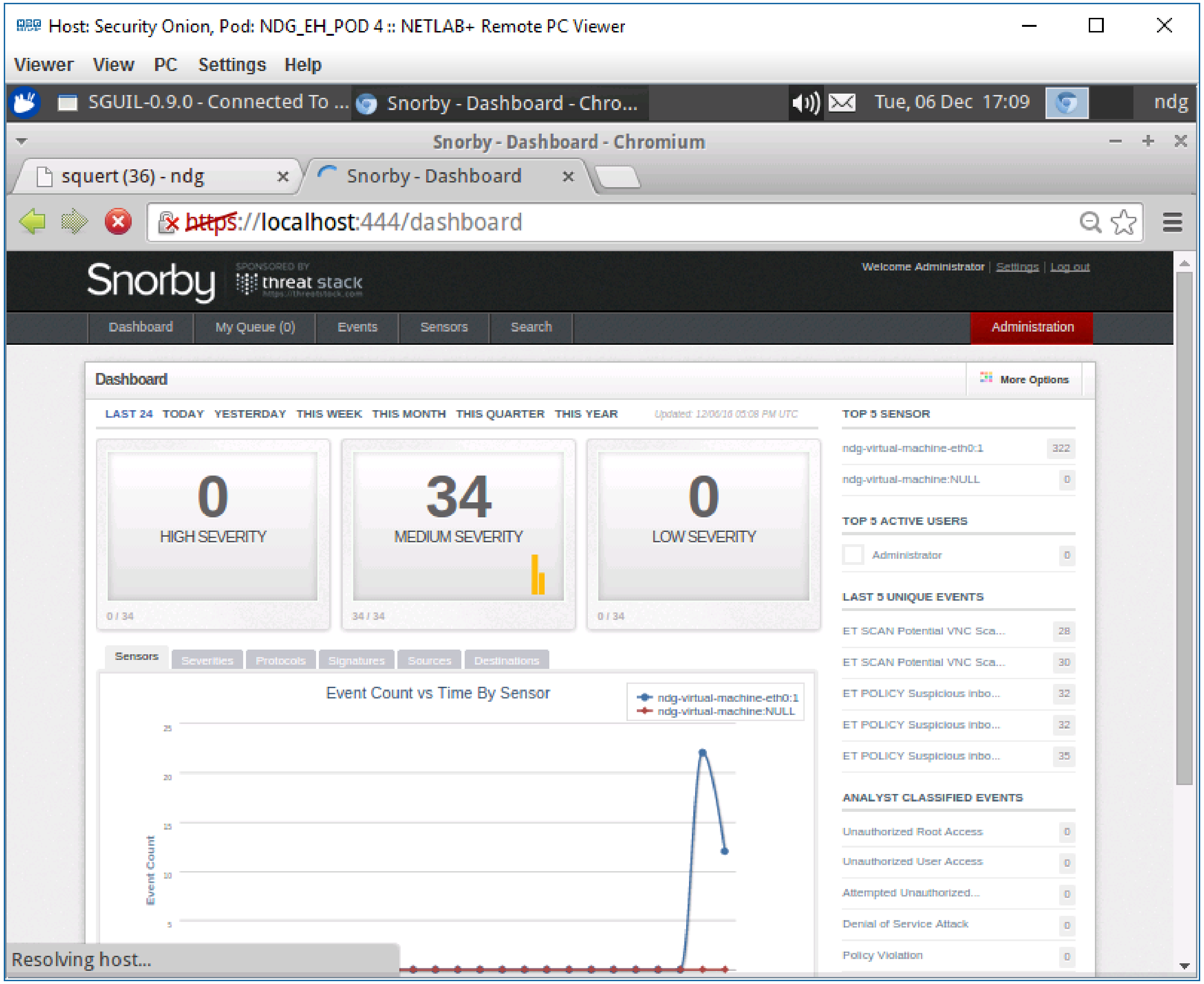
□ CATEGORIZE **5** EVENT(S) CREATE FILTER: src dst both

QUEUE	ACTIVITY	LAST EVENT	SOURCE	COUNTRY	DESTINATION	COUNTRY
4		2016-12-06 17:06:29	□ 192.168.9.2	RFC1918 (.lo)	□ 192.168.0.2	RFC1918 (.lo)
1		2016-12-06 17:06:29	□ 192.168.9.20	RFC1918 (.lo)	□ 192.168.0.2	RFC1918 (.lo)

QUEUE	SC	DC	ACTIVITY	LAST EVENT	SIGNATURE	ID	PROTO	% TOTAL
5	2	1		17:06:29	ET SCAN Potential VNC Scan 5900-5920	2002911	6	13.889%
6	2	1		17:06:29	ET POLICY Suspicious inbound to MSSQL port 1433	2010935	6	16.667%
6	2	1		17:06:29	ET POLICY Suspicious inbound to Oracle SQL port 1521	2010936	6	16.667%
6	2	1		17:06:29	ET POLICY Suspicious inbound to mySQL port 3306	2010937	6	16.667%
6	2	1		17:06:29	ET POLICY Suspicious inbound to PostgreSQL port 5432	2010939	6	16.667%
1	7 1	1		16:59:57	[OSSEC] Received 0 packets in designated time interval (defined in ossec.conf). Please check interface, cabling, and tap/span!	111112	0	2.778%
1	7 1	1		16:18:06	[OSSEC] Integrity checksum changed.	550	0	2.778%

WELCOME ndg | LOGOUT UTC 17:08:01

Squert caught the decoy addresses



Host: Security Onion, Pod: NDG_EH_POD 4 :: NETLAB+ Remote PC Viewer

Viewer View PC Settings Help

SGUIL-0.9.0 - Connected To ... | Snorby - Dashboard - Chro... | Tue, 06 Dec 17:09 | ndg

Snorby - Dashboard - Chromium

squert (36) - ndg | Snorby - Dashboard

~~https~~://localhost:444/dashboard

Snorby SPONSORED BY threat stack

Welcome Administrator | Settings | Log out

Dashboard | My Queue (0) | Events | Sensors | Search | Administration

Dashboard | More Options

LAST 24 TODAY YESTERDAY THIS WEEK THIS MONTH THIS QUARTER THIS YEAR Updated: 12/06/16 05:08 PM UTC

0	34	0
HIGH SEVERITY	MEDIUM SEVERITY	LOW SEVERITY
0 / 34	34 / 34	0 / 34

Sensors | Severities | Protocols | Signatures | Sources | Destinations

Event Count vs Time By Sensor

TOP 5 SENSOR

ndg-virtual-machine-eth0:1	322
ndg-virtual-machine:NULL	0

TOP 5 ACTIVE USERS

Administrator	0

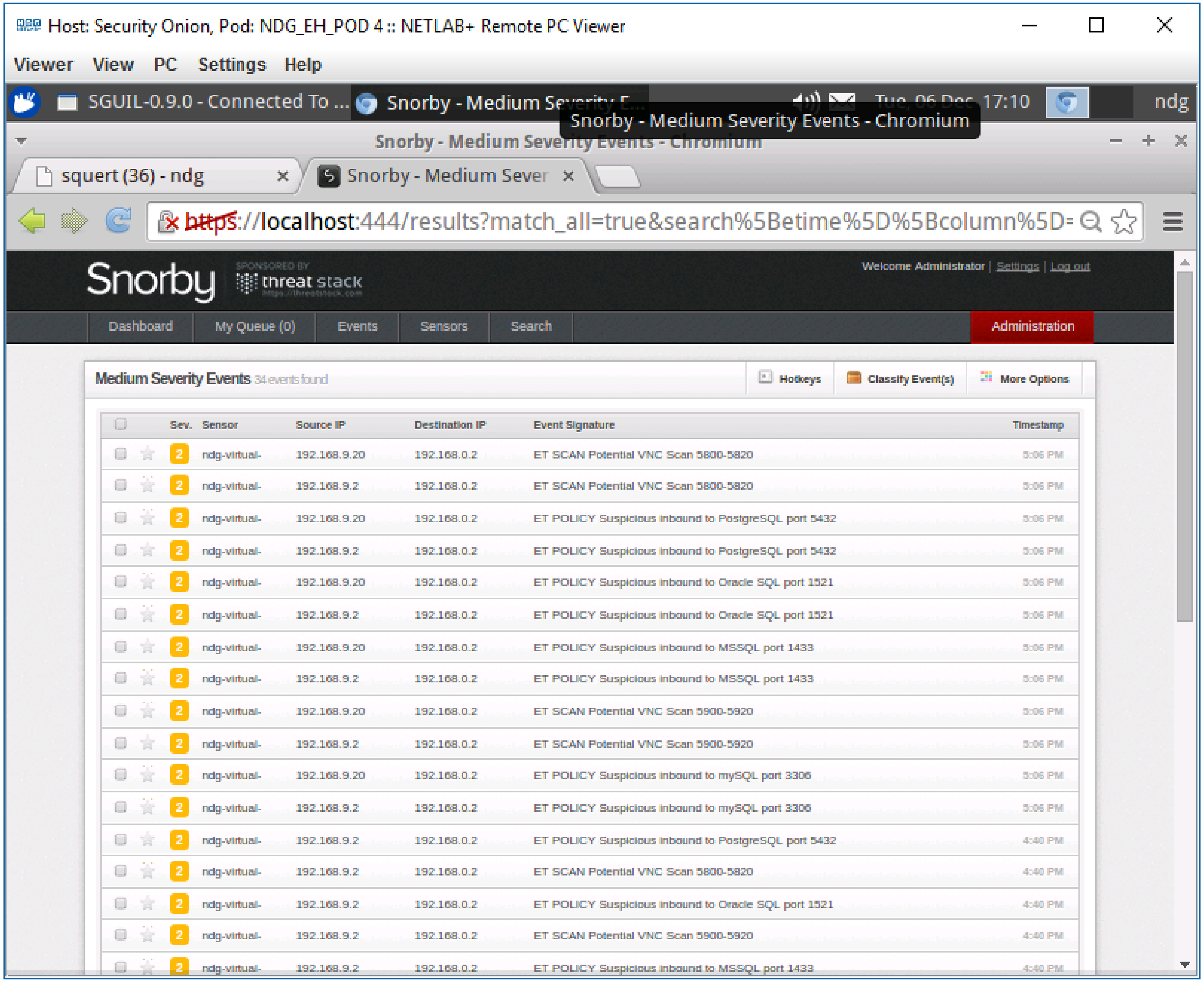
LAST 5 UNIQUE EVENTS

ET SCAN Potential VNC Sca...	28
ET SCAN Potential VNC Sca...	30
ET POLICY Suspicious inbo...	32
ET POLICY Suspicious inbo...	32
ET POLICY Suspicious inbo...	35

ANALYST CLASSIFIED EVENTS

Unauthorized Root Access	0
Unauthorized User Access	0
Attempted Unauthorized...	0
Denial of Service Attack	0
Policy Violation	0

Resolving host...

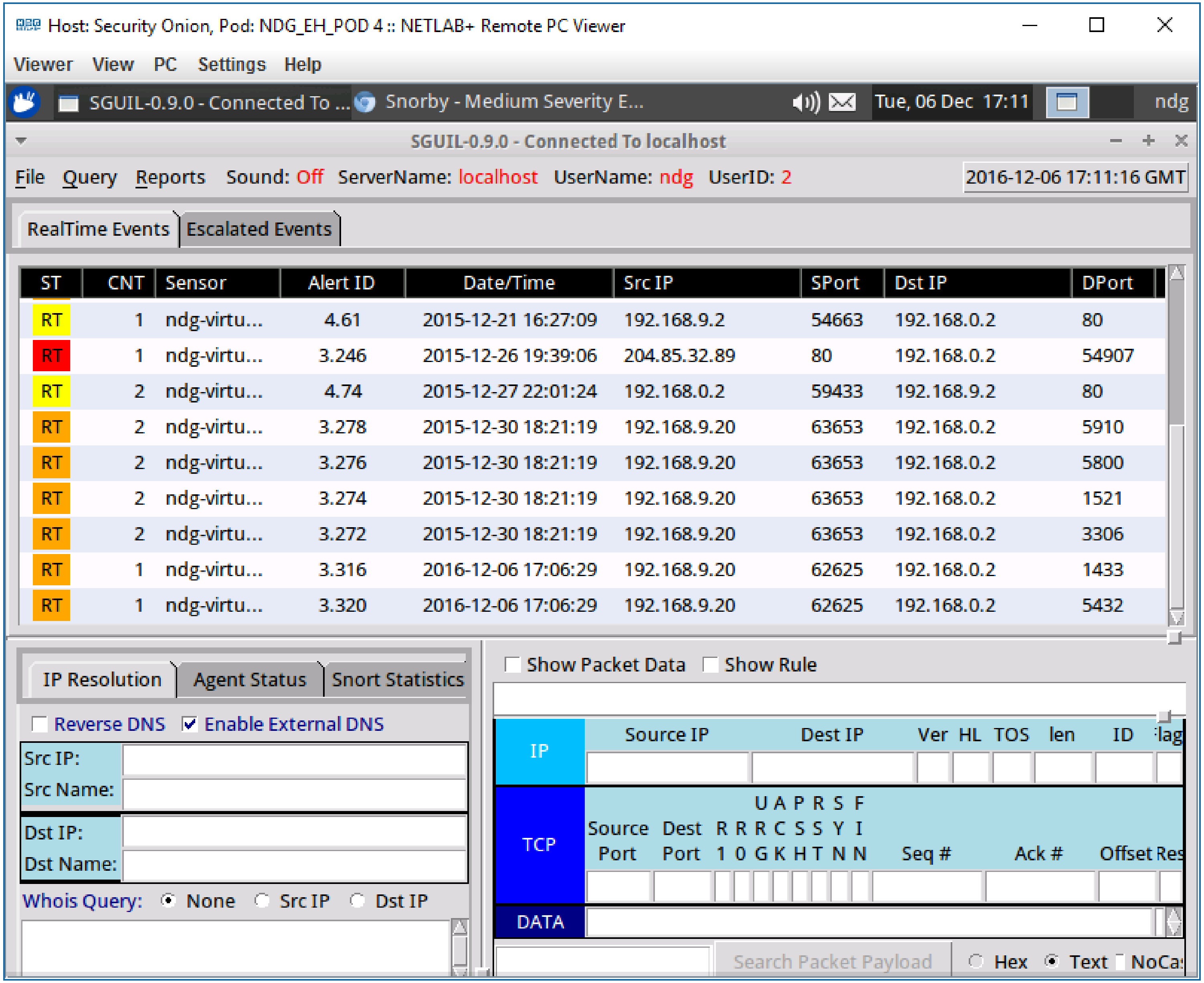

Host: Security Onion, Pod: NDG_EH_POD 4 :: NETLAB+ Remote PC Viewer
Viewer
View
PC
Settings
Help
SGUIL-0.9.0 - Connected To ...
Snorby - Medium Severity E...
Tue, 06 Dec 17:10
ndg
Snorby - Medium Severity Events - Chromium
squert (36) - ndg
Snorby - Medium Sever
Snorby
SPONSORED BY
threat stack
Welcome Administrator | Settings | Log out
Dashboard
My Queue (0)
Events
Sensors
Search
Administration
Hotkeys
Classify Event(s)
More Options

~~https~~://localhost:444/results?match_all=true&search%5Betime%5D%5Bcolumn%5D=

Medium Severity Events 34 events found

□		Sev.	Sensor	Source IP	Destination IP	Event Signature	Timestamp
□	☆	2	ndg-virtual-	192.168.9.20	192.168.0.2	ET SCAN Potential VNC Scan 5800-5820	5:06 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET SCAN Potential VNC Scan 5800-5820	5:06 PM
□	☆	2	ndg-virtual-	192.168.9.20	192.168.0.2	ET POLICY Suspicious inbound to PostgreSQL port 5432	5:06 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET POLICY Suspicious inbound to PostgreSQL port 5432	5:06 PM
□	☆	2	ndg-virtual-	192.168.9.20	192.168.0.2	ET POLICY Suspicious inbound to Oracle SQL port 1521	5:06 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET POLICY Suspicious inbound to Oracle SQL port 1521	5:06 PM
□	☆	2	ndg-virtual-	192.168.9.20	192.168.0.2	ET POLICY Suspicious inbound to MSSQL port 1433	5:06 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET POLICY Suspicious inbound to MSSQL port 1433	5:06 PM
□	☆	2	ndg-virtual-	192.168.9.20	192.168.0.2	ET SCAN Potential VNC Scan 5900-5920	5:06 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET SCAN Potential VNC Scan 5900-5920	5:06 PM
□	☆	2	ndg-virtual-	192.168.9.20	192.168.0.2	ET POLICY Suspicious inbound to mySQL port 3306	5:06 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET POLICY Suspicious inbound to mySQL port 3306	5:06 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET POLICY Suspicious inbound to PostgreSQL port 5432	4:40 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET SCAN Potential VNC Scan 5800-5820	4:40 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET POLICY Suspicious inbound to Oracle SQL port 1521	4:40 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET SCAN Potential VNC Scan 5900-5920	4:40 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET POLICY Suspicious inbound to MSSQL port 1433	4:40 PM

Snorby caught the decoy addresses



Host: Security Onion, Pod: NDG_EH_POD 4 :: NETLAB+ Remote PC Viewer

Viewer View PC Settings Help
SGUIL-0.9.0 - Connected To ... Snorby - Medium Severity E...
Tue, 06 Dec 17:11 ndg

SGUIL-0.9.0 - Connected To localhost

Sound: Off ServerName: localhost UserName: ndg UserID: 2 2016-12-06 17:11:16 GMT

RealTime Events Escalated Events

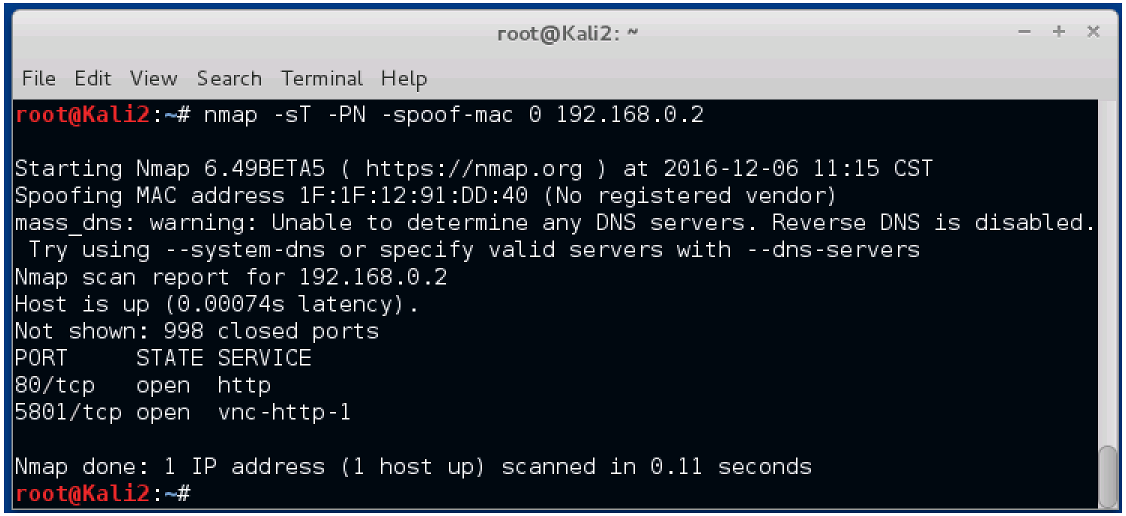
ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort
RT	1	ndg-virtu...	4.61	2015-12-21 16:27:09	192.168.9.2	54663	192.168.0.2	80
RT	1	ndg-virtu...	3.246	2015-12-26 19:39:06	204.85.32.89	80	192.168.0.2	54907
RT	2	ndg-virtu...	4.74	2015-12-27 22:01:24	192.168.0.2	59433	192.168.9.2	80
RT	2	ndg-virtu...	3.278	2015-12-30 18:21:19	192.168.9.20	63653	192.168.0.2	5910
RT	2	ndg-virtu...	3.276	2015-12-30 18:21:19	192.168.9.20	63653	192.168.0.2	5800
RT	2	ndg-virtu...	3.274	2015-12-30 18:21:19	192.168.9.20	63653	192.168.0.2	1521
RT	2	ndg-virtu...	3.272	2015-12-30 18:21:19	192.168.9.20	63653	192.168.0.2	3306
RT	1	ndg-virtu...	3.316	2016-12-06 17:06:29	192.168.9.20	62625	192.168.0.2	1433
RT	1	ndg-virtu...	3.320	2016-12-06 17:06:29	192.168.9.20	62625	192.168.0.2	5432

IP Resolution Agent Status Snort Statistics
☐ Reverse DNS ☑ Enable External DNS
Src IP:
Src Name:
Dst IP:
Dst Name:
Whois Query: ● None ○ Src IP ○ Dst IP
☐ Show Packet Data ☐ Show Rule
IP Source IP Dest IP Ver HL TOS len ID lag
TCP Source Port Dest Port U R G A C K P S H R S T S Y N F I N R 1 R 0 Seq # Ack # Offset Res
DATA
Search Packet Payload ○ Hex ● Text NoCa

Sguil only sees the decoy addresses

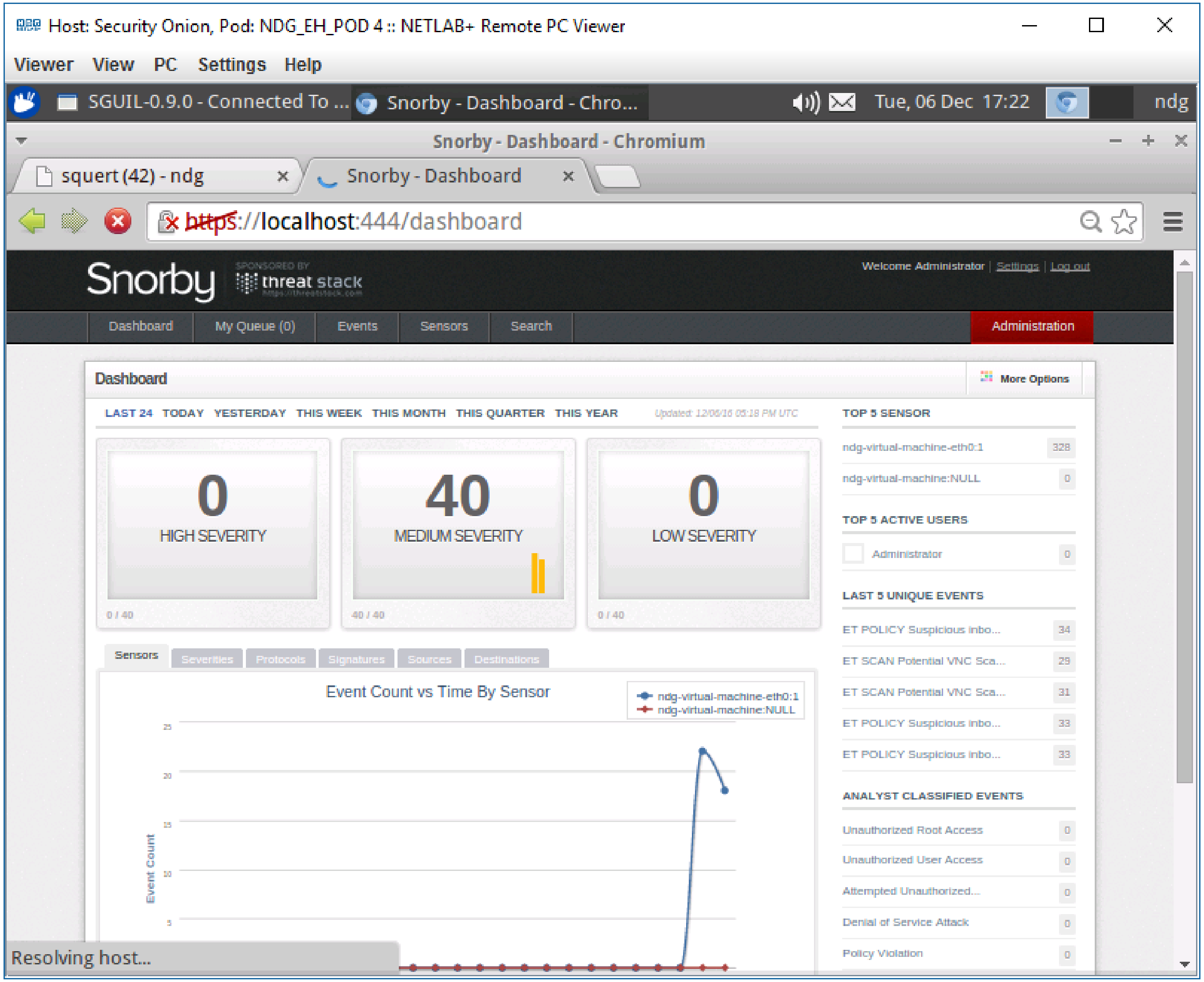
Test IDS Results with Spoofed MAC Scan

nmap -sT -PN -spoof-mac 0 192.168.0.2



```
root@Kali2:~# nmap -sT -PN -spoof-mac 0 192.168.0.2

Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2016-12-06 11:15 CST
Spoofing MAC address 1F:1F:12:91:DD:40 (No registered vendor)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
 Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.0.2
Host is up (0.00074s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
80/tcp   open  http
5801/tcp open  vnc-http-1

Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
root@Kali2:~#
```

Scanning with spoofed MAC address



~~https~~://localhost:444/dashboard

Dashboard

Updated: 12/06/16 05:18 PM UTC

0 HIGH SEVERITY 0 / 40

40 MEDIUM SEVERITY 40 / 40

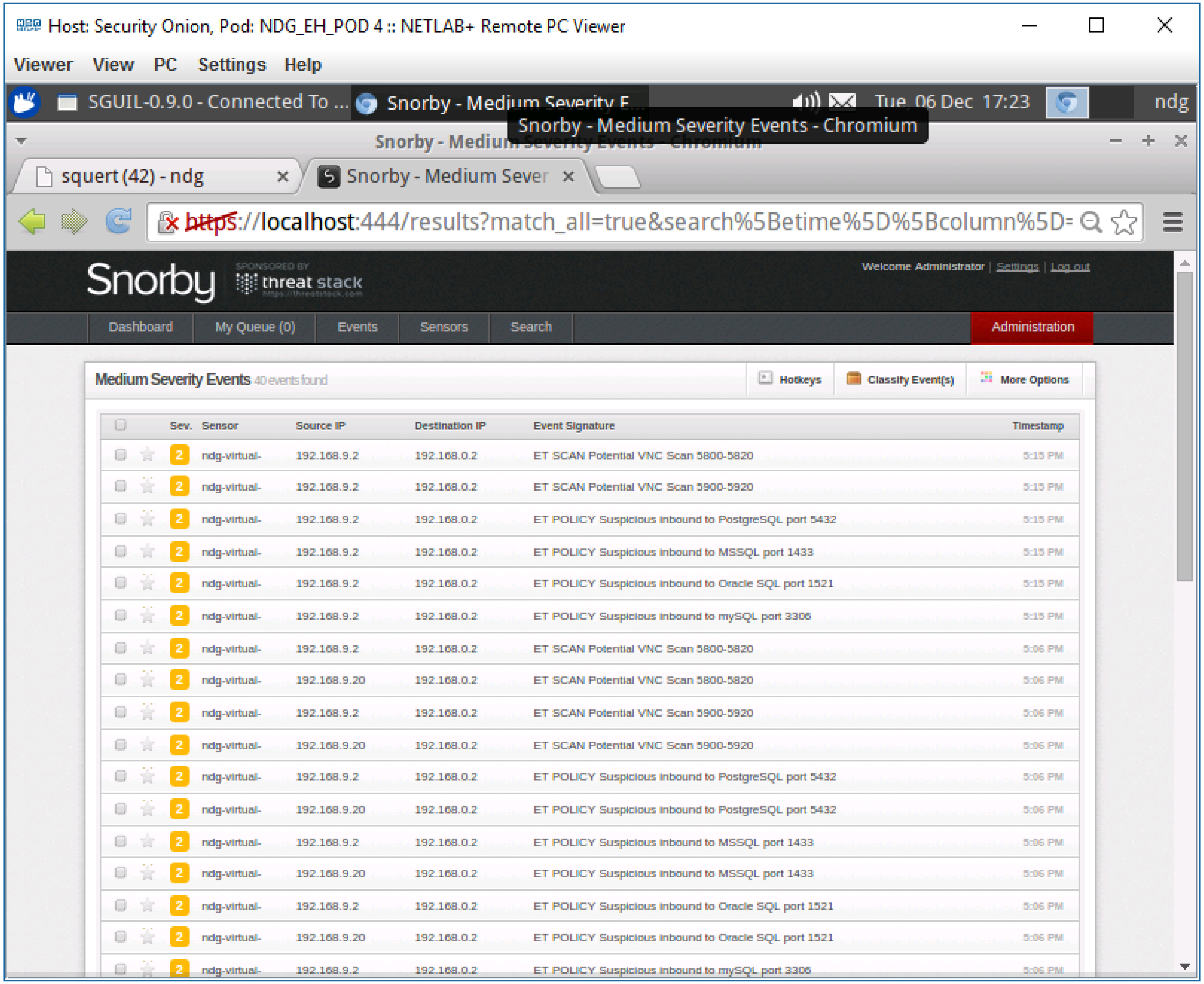
0 LOW SEVERITY 0 / 40

TOP 5 SENSOR	
ndg-virtual-machine-eth0:1	328
ndg-virtual-machine:NULL	0

TOP 5 ACTIVE USERS	
Administrator	0

LAST 5 UNIQUE EVENTS	
ET POLICY Suspicious inbo...	34
ET SCAN Potential VNC Sca...	29
ET SCAN Potential VNC Sca...	31
ET POLICY Suspicious inbo...	33
ET POLICY Suspicious inbo...	33

ANALYST CLASSIFIED EVENTS	
Unauthorized Root Access	0
Unauthorized User Access	0
Attempted Unauthorized...	0
Denial of Service Attack	0
Policy Violation	0



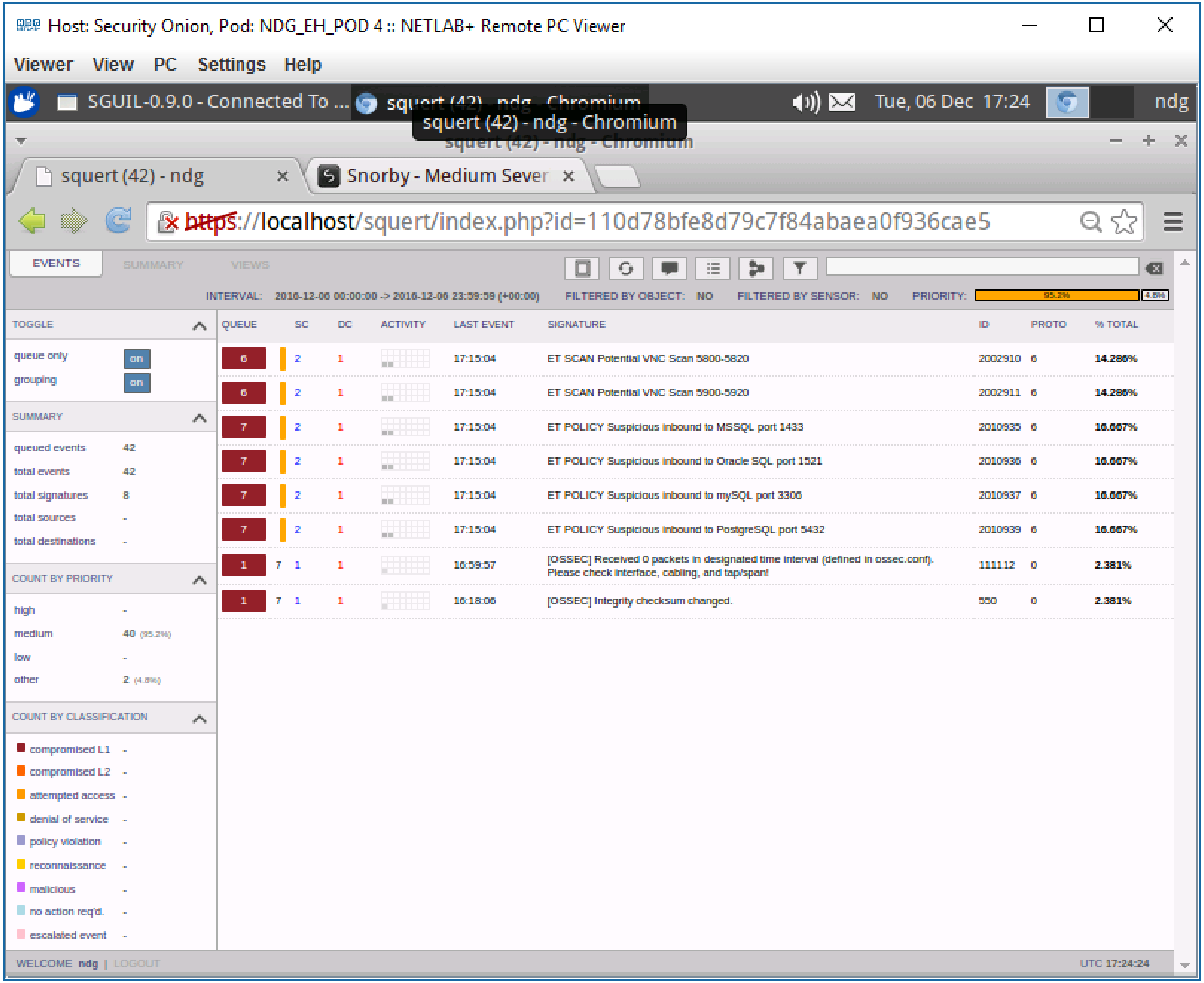
Host: Security Onion, Pod: NDG_EH_POD 4 :: NETLAB+ Remote PC Viewer

Viewer
View
PC
Settings
Help
SGUIL-0.9.0 - Connected To ...
Snorby - Medium Severity E...
Tue 06 Dec 17:23
ndg
Snorby - Medium Severity Events - Chromium
squert (42) - ndg
Snorby - Medium Sever

~~https~~://localhost:444/results?match_all=true&search%5Betime%5D%5Bcolumn%5D=

Medium Severity Events 40 events found

□		Sev.	Sensor	Source IP	Destination IP	Event Signature	Timestamp
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET SCAN Potential VNC Scan 5800-5820	5:15 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET SCAN Potential VNC Scan 5900-5920	5:15 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET POLICY Suspicious inbound to PostgreSQL port 5432	5:15 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET POLICY Suspicious inbound to MSSQL port 1433	5:15 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET POLICY Suspicious inbound to Oracle SQL port 1521	5:15 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET POLICY Suspicious inbound to mySQL port 3306	5:15 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET SCAN Potential VNC Scan 5800-5820	5:06 PM
□	☆	2	ndg-virtual-	192.168.9.20	192.168.0.2	ET SCAN Potential VNC Scan 5800-5820	5:06 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET SCAN Potential VNC Scan 5900-5920	5:06 PM
□	☆	2	ndg-virtual-	192.168.9.20	192.168.0.2	ET SCAN Potential VNC Scan 5900-5920	5:06 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET POLICY Suspicious inbound to PostgreSQL port 5432	5:06 PM
□	☆	2	ndg-virtual-	192.168.9.20	192.168.0.2	ET POLICY Suspicious inbound to PostgreSQL port 5432	5:06 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET POLICY Suspicious inbound to MSSQL port 1433	5:06 PM
□	☆	2	ndg-virtual-	192.168.9.20	192.168.0.2	ET POLICY Suspicious inbound to MSSQL port 1433	5:06 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET POLICY Suspicious inbound to Oracle SQL port 1521	5:06 PM
□	☆	2	ndg-virtual-	192.168.9.20	192.168.0.2	ET POLICY Suspicious inbound to Oracle SQL port 1521	5:06 PM
□	☆	2	ndg-virtual-	192.168.9.2	192.168.0.2	ET POLICY Suspicious inbound to mySQL port 3306	5:06 PM



Host: Security Onion, Pod: NDG_EH_POD 4 :: NETLAB+ Remote PC Viewer

Viewer View PC Settings Help
SGUIL-0.9.0 - Connected To ...
squert (42) - ndg - Chromium
Tue, 06 Dec 17:24
ndg
squert (42) - ndg - Chromium
squert (42) - ndg
Snorby - Medium Sever

~~https~~://localhost/squert/index.php?id=110d78bfe8d79c7f84abaea0f936cae5

INTERVAL: 2016-12-06 00:00:00 -> 2016-12-06 23:59:59 (+00:00) FILTERED BY OBJECT: NO FILTERED BY SENSOR: NO PRIORITY: 95.2% 4.8%

TOGGLE

queue only	on
grouping	on

SUMMARY

queued events	42
total events	42
total signatures	8
total sources	-
total destinations	-

COUNT BY PRIORITY

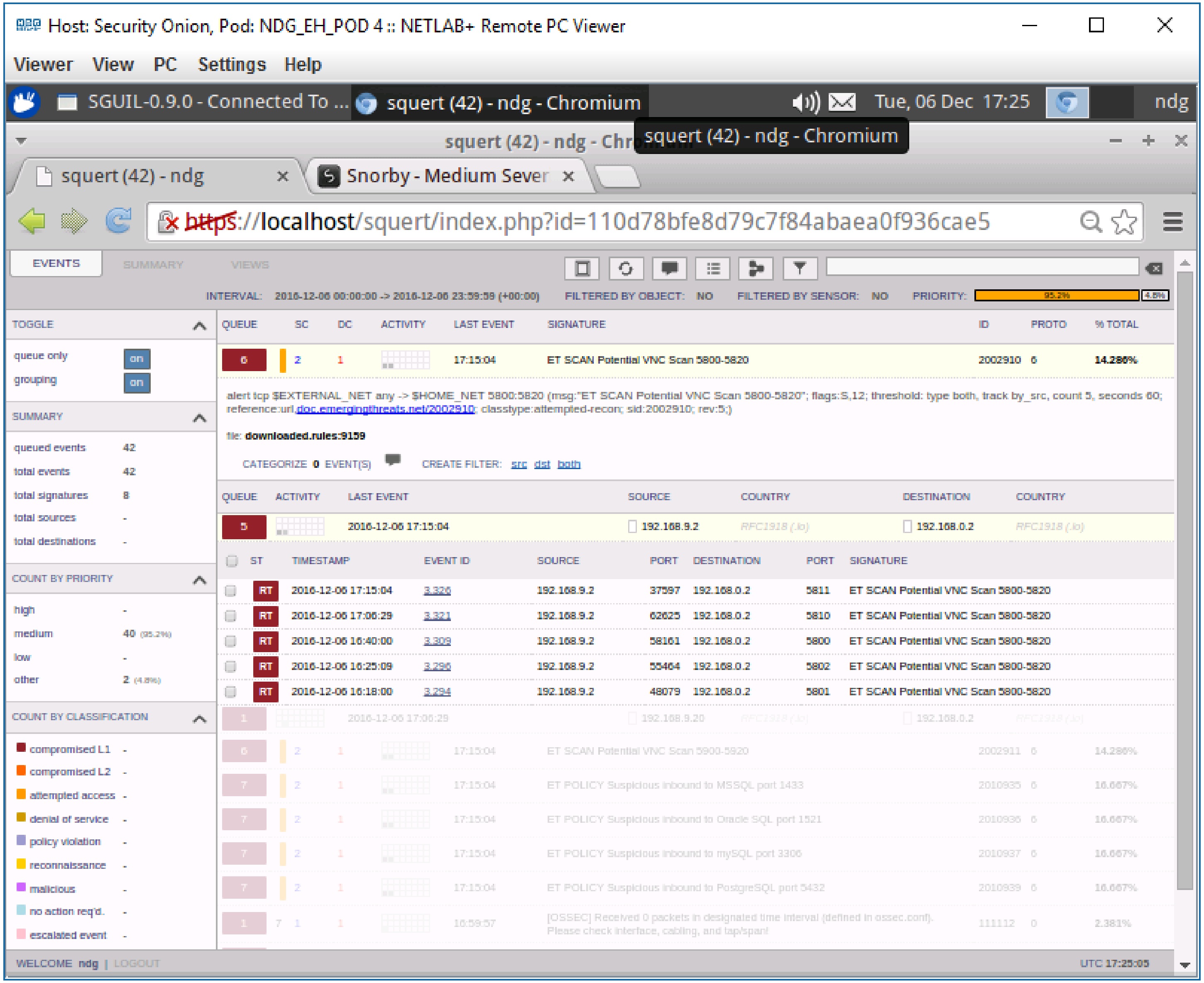
high	-
medium	40 (95.2%)
low	-
other	2 (4.8%)

COUNT BY CLASSIFICATION

🟥 compromised L1	-
🟧 compromised L2	-
🟧 attempted access	-
🟨 denial of service	-
🟪 policy violation	-
🟨 reconnaissance	-
🟪 malicious	-
🟦 no action req'd.	-
🟥 escalated event	-

QUEUE		SC	DC	ACTIVITY	LAST EVENT	SIGNATURE	ID	PROTO	% TOTAL
6		2	1		17:15:04	ET SCAN Potential VNC Scan 5800-5820	2002910	6	14.286%
6		2	1		17:15:04	ET SCAN Potential VNC Scan 5900-5920	2002911	6	14.286%
7		2	1		17:15:04	ET POLICY Suspicious inbound to MSSQL port 1433	2010935	6	16.667%
7		2	1		17:15:04	ET POLICY Suspicious inbound to Oracle SQL port 1521	2010936	6	16.667%
7		2	1		17:15:04	ET POLICY Suspicious inbound to mySQL port 3306	2010937	6	16.667%
7		2	1		17:15:04	ET POLICY Suspicious inbound to PostgreSQL port 5432	2010939	6	16.667%
1	7	1	1		16:59:57	[OSSEC] Received 0 packets in designated time interval (defined in ossec.conf). Please check interface, cabling, and tap/span!	111112	0	2.381%
1	7	1	1		16:18:06	[OSSEC] Integrity checksum changed.	550	0	2.381%

WELCOME ndg | LOGOUT UTC 17:24:24


Host: Security Onion, Pod: NDG_EH_POD 4 :: NETLAB+ Remote PC Viewer
Viewer
View
PC
Settings
Help
SGUIL-0.9.0 - Connected To ...
squert (42) - ndg - Chromium
Tue, 06 Dec 17:25
ndg
squert (42) - ndg - Chromium
squert (42) - ndg
Snorby - Medium Sever
~~https~~://localhost/squert/index.php?id=110d78bfe8d79c7f84abaea0f936cae5
EVENTS
SUMMARY
VIEWS

INTERVAL: 2016-12-06 00:00:00 -> 2016-12-06 23:59:59 (+00:00) FILTERED BY OBJECT: NO FILTERED BY SENSOR: NO PRIORITY: 95.2% 4.8%

TOGGLE

queue only	on
grouping	on

SUMMARY

queued events	42
total events	42
total signatures	8
total sources	-
total destinations	-

COUNT BY PRIORITY

high	-
medium	40 (95.2%)
low	-
other	2 (4.8%)

COUNT BY CLASSIFICATION

🟥 compromised L1	-
🟧 compromised L2	-
🟧 attempted access	-
🟫 denial of service	-
🟪 policy violation	-
🟨 reconnaissance	-
🟪 malicious	-
🟦 no action req'd.	-
🟥 escalated event	-

QUEUE	SC	DC	ACTIVITY	LAST EVENT	SIGNATURE	ID	PROTO	% TOTAL
6	2	1		17:15:04	ET SCAN Potential VNC Scan 5800-5820	2002910	6	14.286%

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 5800:5820 (msg:"ET SCAN Potential VNC Scan 5800-5820"; flags:S,12; threshold: type both, track by_src, count 5, seconds 60; reference:url,doc.emergingthreats.net/2002910; classtype:attempted-recon; sid:2002910; rev:5;)
```

file: **downloaded.rules:9159**

CATEGORIZE **0** EVENT(S) CREATE FILTER: src dst both

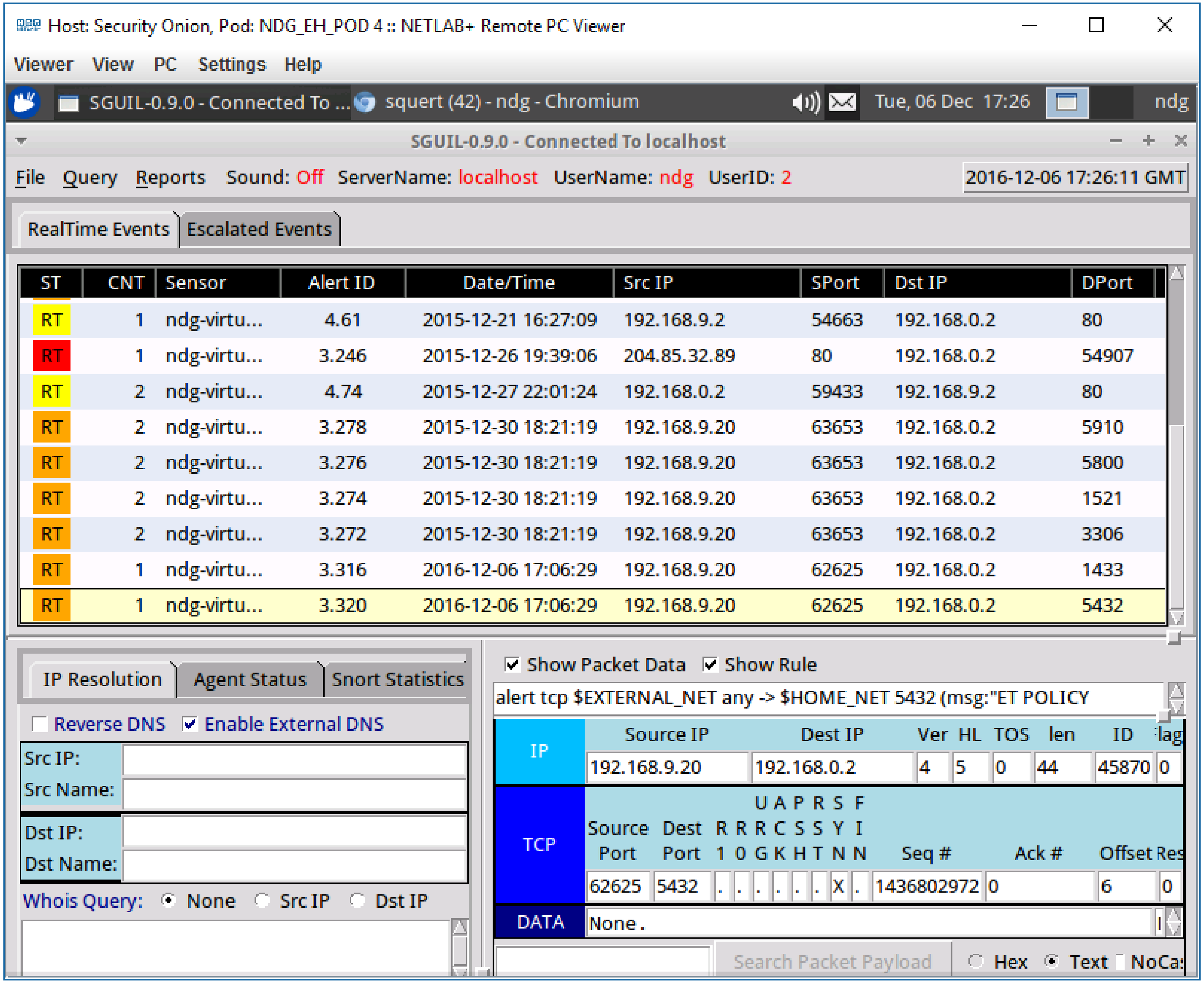
QUEUE	ACTIVITY	LAST EVENT	SOURCE	COUNTRY	DESTINATION	COUNTRY
5		2016-12-06 17:15:04	192.168.9.2	RFC1918 (.lo)	192.168.0.2	RFC1918 (.lo)

☐	ST	TIMESTAMP	EVENT ID	SOURCE	PORT	DESTINATION	PORT	SIGNATURE
☐	RT	2016-12-06 17:15:04	3.326	192.168.9.2	37597	192.168.0.2	5811	ET SCAN Potential VNC Scan 5800-5820
☐	RT	2016-12-06 17:06:29	3.321	192.168.9.2	62625	192.168.0.2	5810	ET SCAN Potential VNC Scan 5800-5820
☐	RT	2016-12-06 16:40:00	3.309	192.168.9.2	58161	192.168.0.2	5800	ET SCAN Potential VNC Scan 5800-5820
☐	RT	2016-12-06 16:25:09	3.296	192.168.9.2	55464	192.168.0.2	5802	ET SCAN Potential VNC Scan 5800-5820
☐	RT	2016-12-06 16:18:00	3.294	192.168.9.2	48079	192.168.0.2	5801	ET SCAN Potential VNC Scan 5800-5820

QUEUE	ACTIVITY	LAST EVENT	SOURCE	COUNTRY	DESTINATION	COUNTRY
1		2016-12-06 17:06:29	192.168.9.20	RFC1918 (.lo)	192.168.0.2	RFC1918 (.lo)

QUEUE	SC	DC	ACTIVITY	LAST EVENT	SIGNATURE	ID	PROTO	% TOTAL
6	2	1		17:15:04	ET SCAN Potential VNC Scan 5900-5920	2002911	6	14.286%
7	2	1		17:15:04	ET POLICY Suspicious inbound to MSSQL port 1433	2010935	6	16.667%
7	2	1		17:15:04	ET POLICY Suspicious inbound to Oracle SQL port 1521	2010936	6	16.667%
7	2	1		17:15:04	ET POLICY Suspicious inbound to mySQL port 3306	2010937	6	16.667%
7	2	1		17:15:04	ET POLICY Suspicious inbound to PostgreSQL port 5432	2010939	6	16.667%
1	7 1	1		16:59:57	[OSSEC] Received 0 packets in designated time interval (defined in ossec.conf). Please check interface, cabling, and tap/span!	111112	0	2.381%

WELCOME ndg | LOGOUT UTC 17:25:05


Host: Security Onion, Pod: NDG_EH_POD 4 :: NETLAB+ Remote PC Viewer
Viewer
View
PC
Settings
Help
SGUIL-0.9.0 - Connected To ...
squert (42) - ndg - Chromium
Tue, 06 Dec 17:26
ndg
SGUIL-0.9.0 - Connected To localhost
File
Query
Reports
RealTime Events
Escalated Events
IP Resolution
Agent Status
Snort Statistics
Search Packet Payload

Sound: Off ServerName: localhost UserName: ndg UserID: 2 2016-12-06 17:26:11 GMT

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort
RT	1	ndg-virtu...	4.61	2015-12-21 16:27:09	192.168.9.2	54663	192.168.0.2	80
RT	1	ndg-virtu...	3.246	2015-12-26 19:39:06	204.85.32.89	80	192.168.0.2	54907
RT	2	ndg-virtu...	4.74	2015-12-27 22:01:24	192.168.0.2	59433	192.168.9.2	80
RT	2	ndg-virtu...	3.278	2015-12-30 18:21:19	192.168.9.20	63653	192.168.0.2	5910
RT	2	ndg-virtu...	3.276	2015-12-30 18:21:19	192.168.9.20	63653	192.168.0.2	5800
RT	2	ndg-virtu...	3.274	2015-12-30 18:21:19	192.168.9.20	63653	192.168.0.2	1521
RT	2	ndg-virtu...	3.272	2015-12-30 18:21:19	192.168.9.20	63653	192.168.0.2	3306
RT	1	ndg-virtu...	3.316	2016-12-06 17:06:29	192.168.9.20	62625	192.168.0.2	1433
RT	1	ndg-virtu...	3.320	2016-12-06 17:06:29	192.168.9.20	62625	192.168.0.2	5432

□ Reverse DNS ☑ Enable External DNS

Src IP:

Src Name:

Dst IP:

Dst Name:

Whois Query: ● None ○ Src IP ○ Dst IP

☑ Show Packet Data ☑ Show Rule

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 5432 (msg:"ET POLICY
```

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	lag
	192.168.9.20	192.168.0.2	4	5	0	44	45870	0

TCP	Source Port	Dest Port	R 1	R 0	U R G	A C K	P S H	R S T	S Y N	F I N	Seq #	Ack #	Offset	Res
	62625	5432	.	.	.	.	.	.	X	.	1436802972	0	6	0

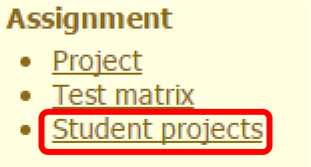
DATA None .

○ Hex ● Text □ NoCa

Final Project Presentations

CIS 76 Project

Calendar Page

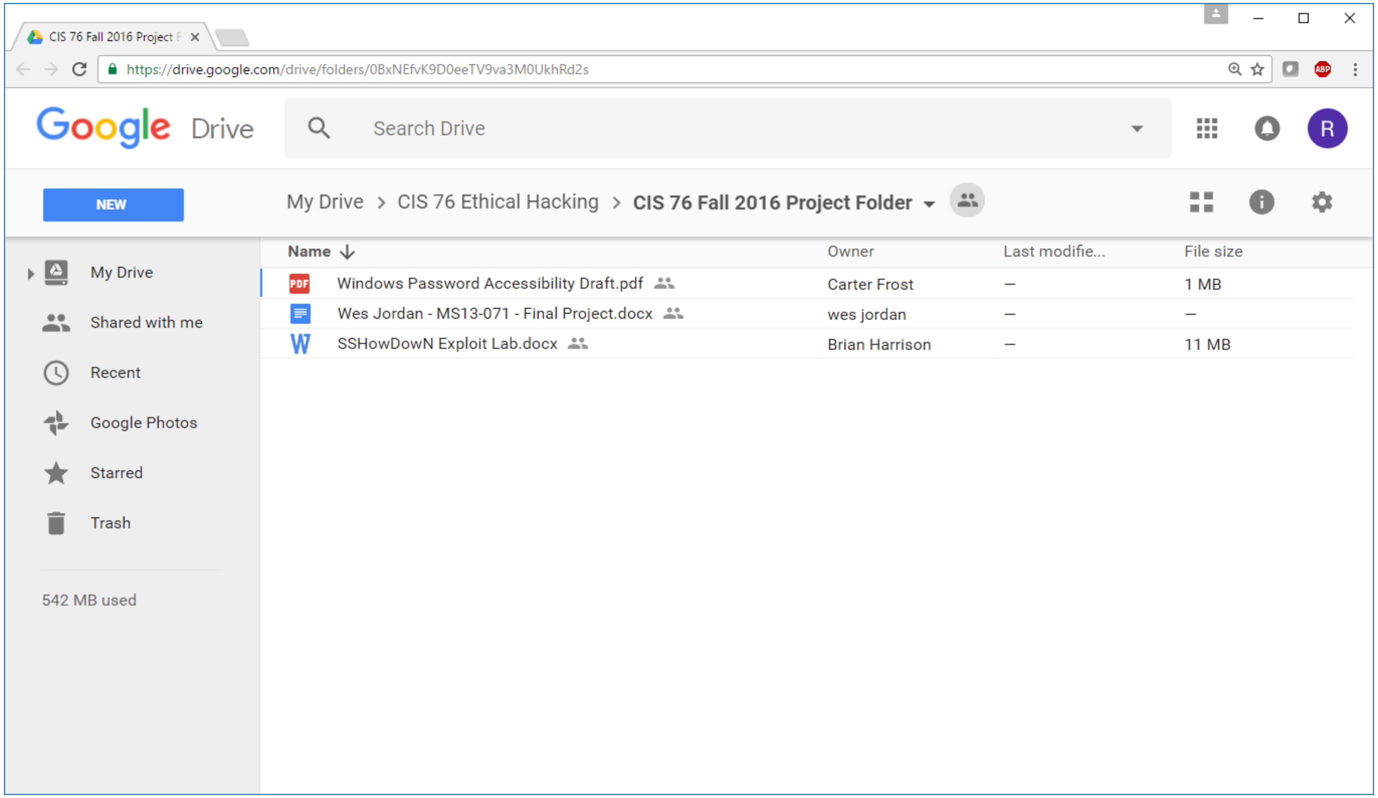


Assignment

- Project
- Test matrix
- Student projects

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

Use this directory to share your project with other classmates for testing



CIS 76 Fall 2016 Project F

https://drive.google.com/drive/folders/0BxNEfvK9D0eeTV9va3M0UkhRd2s

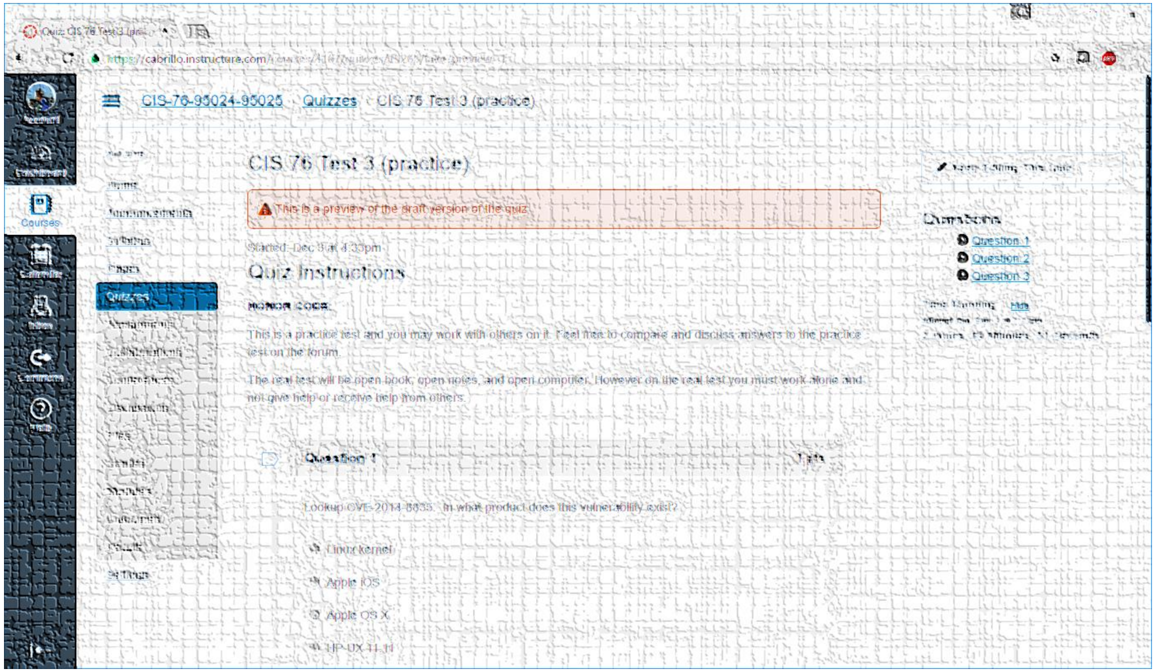
My Drive > CIS 76 Ethical Hacking > CIS 76 Fall 2016 Project Folder

Name	Owner	Last modifie...	File size
Windows Password Accessibility Draft.pdf	Carter Frost	–	1 MB
Wes Jordan - MS13-071 - Final Project.docx	wes jordan	–	–
SSHowDowN Exploit Lab.docx	Brian Harrison	–	11 MB

https://cabrillo.instructure.com/courses/4167/pages/cis-76-project-folder

Assignment

Practice Test



Quiz: CIS 76 Test 3 (pr...

https://cabrillo.instructure.com/[illegible]

CIS-76-95024-95025 › Quizzes › CIS 76 Test 3 (practice)

Courses

Quizzes

CIS 76 Test 3 (practice)

This is a preview of the draft version of the quiz

Started: Dec 3 at 4:33pm

Quiz Instructions

HONOR CODE:

This is a practice test and you may work with others on it. Feel free to compare and discuss answers to the practice test on the forum.

The real test will be open book, open notes, and open computer. However on the real test you must work alone and not give help or receive help from others.

Question 1

Lookup CVE-2014-8835. In what product does this vulnerability exist?

○ Linux kernel

○ Apple iOS

○ Apple OS X

○ HP-UX 11.11

Keep Editing This Quiz

Questions

- Question 1
- Question 2
- Question 3

Time Running: Hide

The practice test is on Canvas

Wrap up

Next Class is the Final Exam (Test #3)

Thursday 4:00 PM

Test #3
Five Posts
Lab X1 (extra credit)
Lab X2 (extra credit)
Lab X3 (extra credit)
Lab X4 (extra credit)

Backup