Student:	Email:
Mani Sai Voore	mvoore@cbu.edu

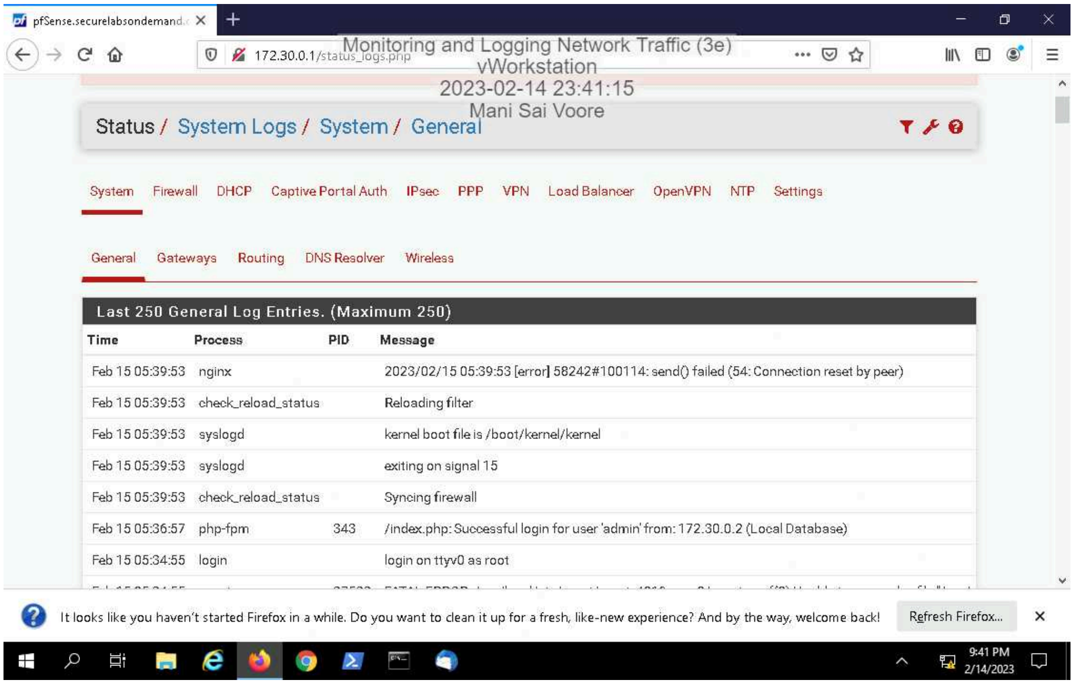
Time on Task:	Progress:
10 hours, 54 minutes	100%

Report Generated: Friday, February 17, 2023 at 8:42 PM

Section 1: Hands-On Demonstration

Part 1: Configure the pfSense Firewall Log

13. **Make a screen capture** showing the **system logs**.

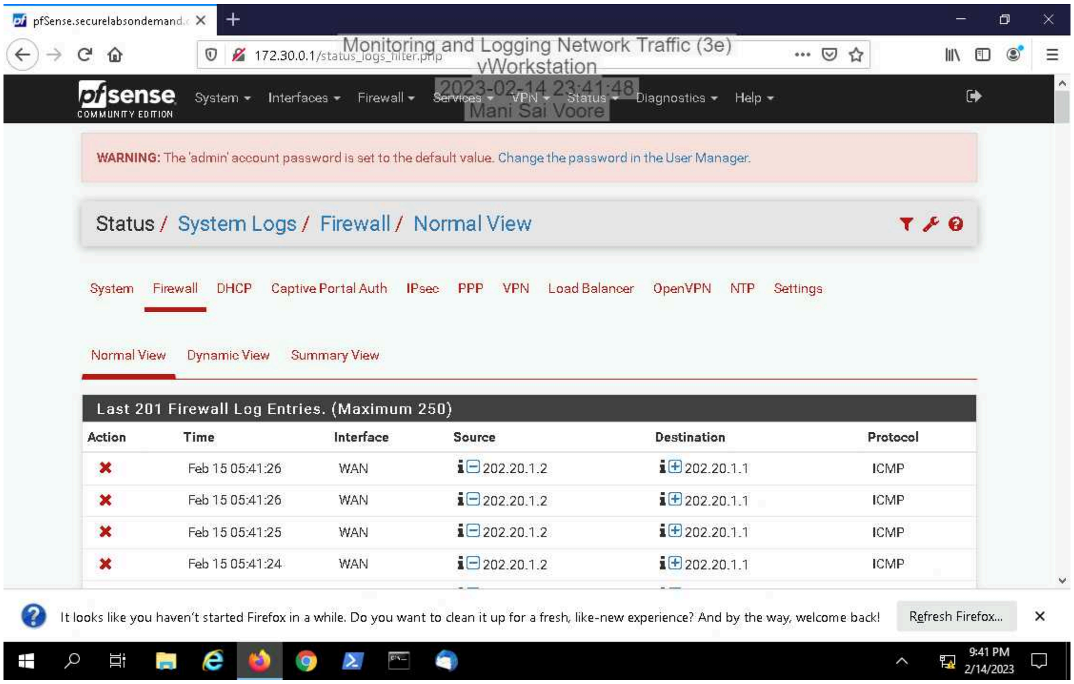


Last 250 General Log Entries. (Maximum 250)

Time	Process	PID	Message
Feb 15 05:39:53	nginx		2023/02/15 05:39:53 [error] 58242#100114: send() failed (54: Connection reset by peer)
Feb 15 05:39:53	check_reload_status		Reloading filter
Feb 15 05:39:53	syslogd		kernel boot file is /boot/kernel/kernel
Feb 15 05:39:53	syslogd		exiting on signal 15
Feb 15 05:39:53	check_reload_status		Syncing firewall
Feb 15 05:36:57	php-fpm	343	/index.php: Successful login for user 'admin' from: 172.30.0.2 (Local Database)
Feb 15 05:34:55	login		login on ttyv0 as root

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

15. **Make a screen capture** showing the **firewall logs**.



Monitoring and Logging Network Traffic (3e)
vWorkstation
2023-02-14 23:41:48
Mani Sai Voore

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Status / System Logs / Firewall / Normal View

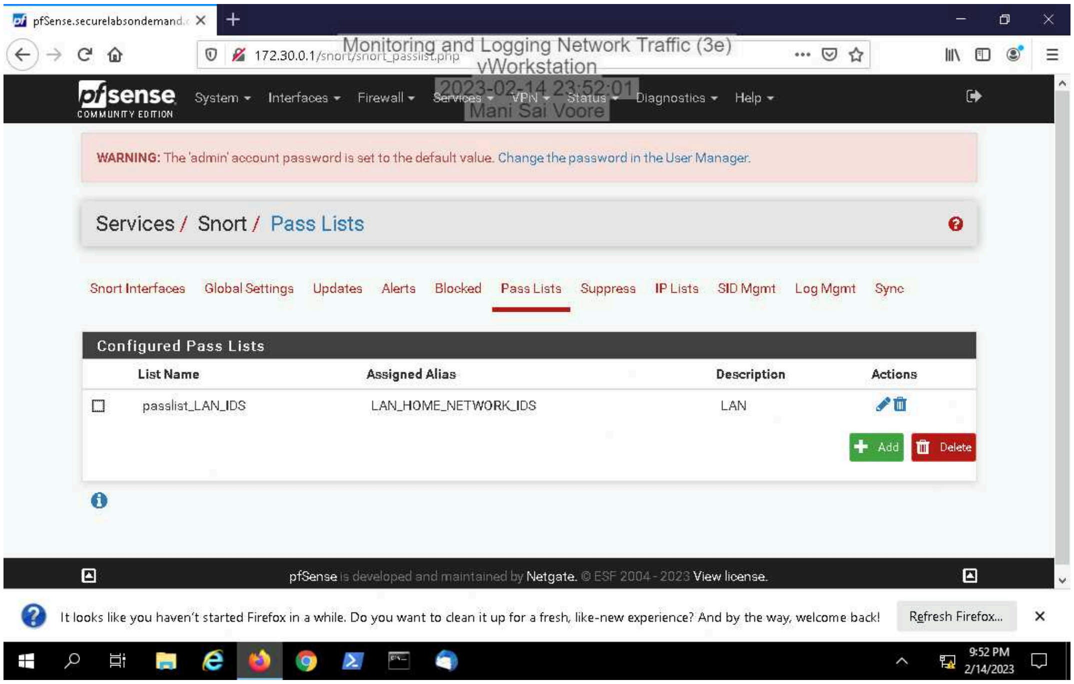
Last 201 Firewall Log Entries. (Maximum 250)

Action	Time	Interface	Source	Destination	Protocol
✖	Feb 15 05:41:26	WAN	202.20.1.2	202.20.1.1	ICMP
✖	Feb 15 05:41:26	WAN	202.20.1.2	202.20.1.1	ICMP
✖	Feb 15 05:41:25	WAN	202.20.1.2	202.20.1.1	ICMP
✖	Feb 15 05:41:24	WAN	202.20.1.2	202.20.1.1	ICMP

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Part 2: Configure a Snort Intrusion Detection System

14. **Make a screen capture** showing the **updated Pass Lists page**.



Monitoring and Logging Network Traffic (3e)
vWorkstation
2023-02-14 23:52:01
Mani Sai Voore

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Services / Snort / Pass Lists

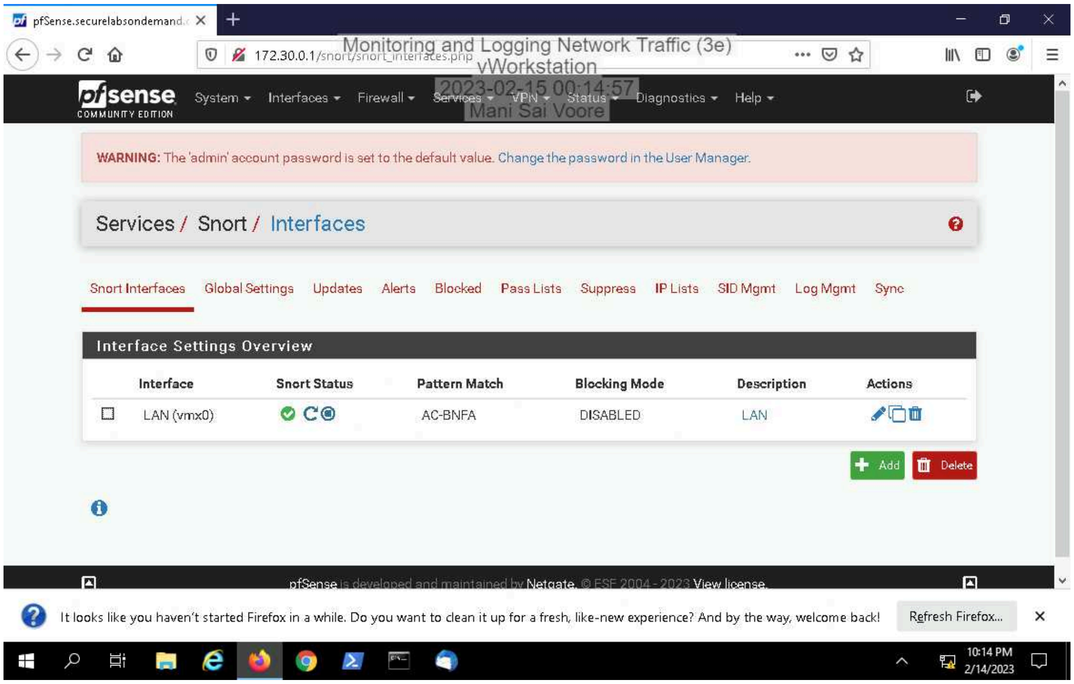
Configured Pass Lists

	List Name	Assigned Alias	Description	Actions
□	passlist_LAN_IDS	LAN_HOME_NETWORK_IDS	LAN	

pfSense is developed and maintained by Netgate. © ESF 2004 - 2023 View license.

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

28. **Make a screen capture** showing the **active Snort status on the LAN interface**.



Monitoring and Logging Network Traffic (3e)
vWorkstation
2023-02-15 00:14:57
Mani Sai Voore

pfSense.securelabsondemand.
172.30.0.1/snort/snort_interfaces.php
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Services / Snort / Interfaces

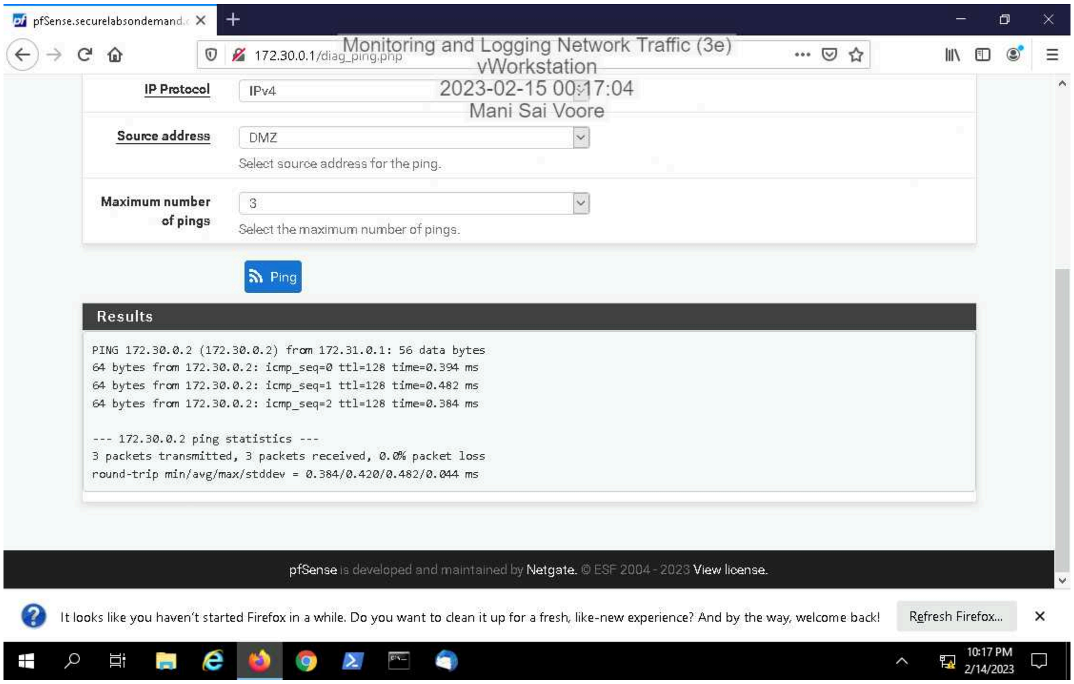
Interface Settings Overview

	Interface	Snort Status	Pattern Match	Blocking Mode	Description	Actions
□	LAN (vmx0)	✓	AC-BNFA	DISABLED	LAN	

Add
Delete
pfSense is developed and maintained by Netgate. © ESF 2004 - 2023 View license.

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

33. **Make a screen capture** showing the **successful ping results**.



Monitoring and Logging Network Traffic (3e)
vWorkstation
2023-02-15 00:17:04
Mani Sai Voore

IP Protocol: IPv4

Source address: DMZ
Select source address for the ping.

Maximum number of pings: 3
Select the maximum number of pings.

Results

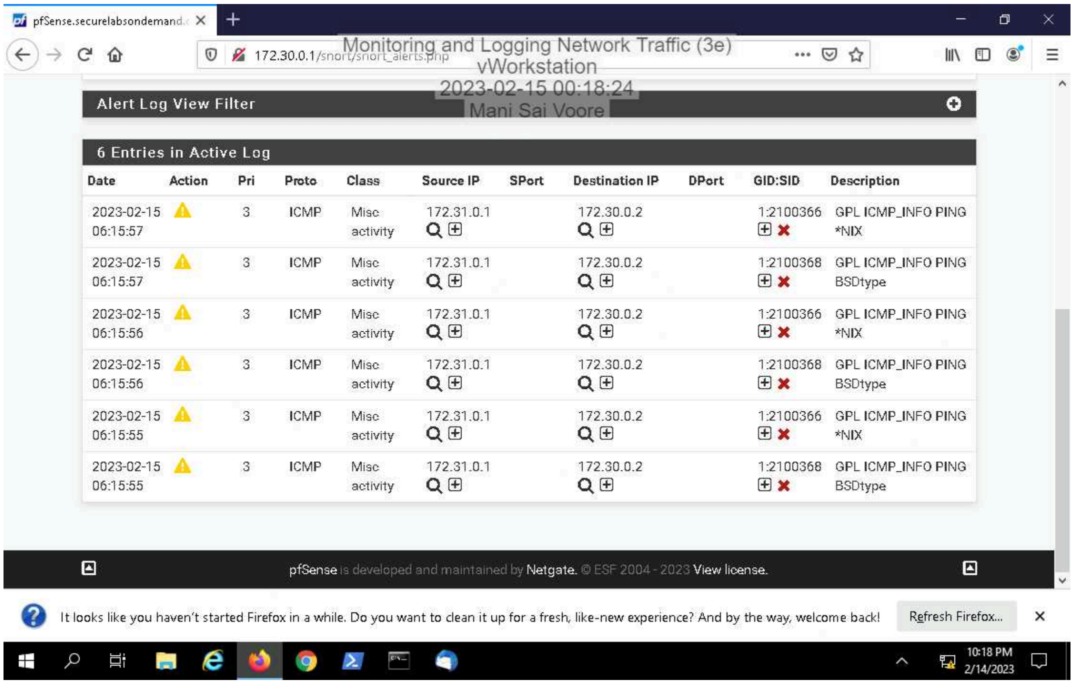
```
PING 172.30.0.2 (172.30.0.2) from 172.31.0.1: 56 data bytes
64 bytes from 172.30.0.2: icmp_seq=0 ttl=128 time=0.394 ms
64 bytes from 172.30.0.2: icmp_seq=1 ttl=128 time=0.482 ms
64 bytes from 172.30.0.2: icmp_seq=2 ttl=128 time=0.384 ms

--- 172.30.0.2 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.384/0.420/0.482/0.044 ms
```

pfSense is developed and maintained by Netgate. © ESF 2004 - 2023 View license.

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

38. **Make a screen capture** showing the **ICMP alerts in the Snort Active Log**.



pfSense.securelabsondemand.
172.30.0.1/snort/snort_alerts.php

Monitoring and Logging Network Traffic (3e)
vWorkstation
2023-02-15 00:18:24
Mani Sai Voore

Alert Log View Filter

6 Entries in Active Log

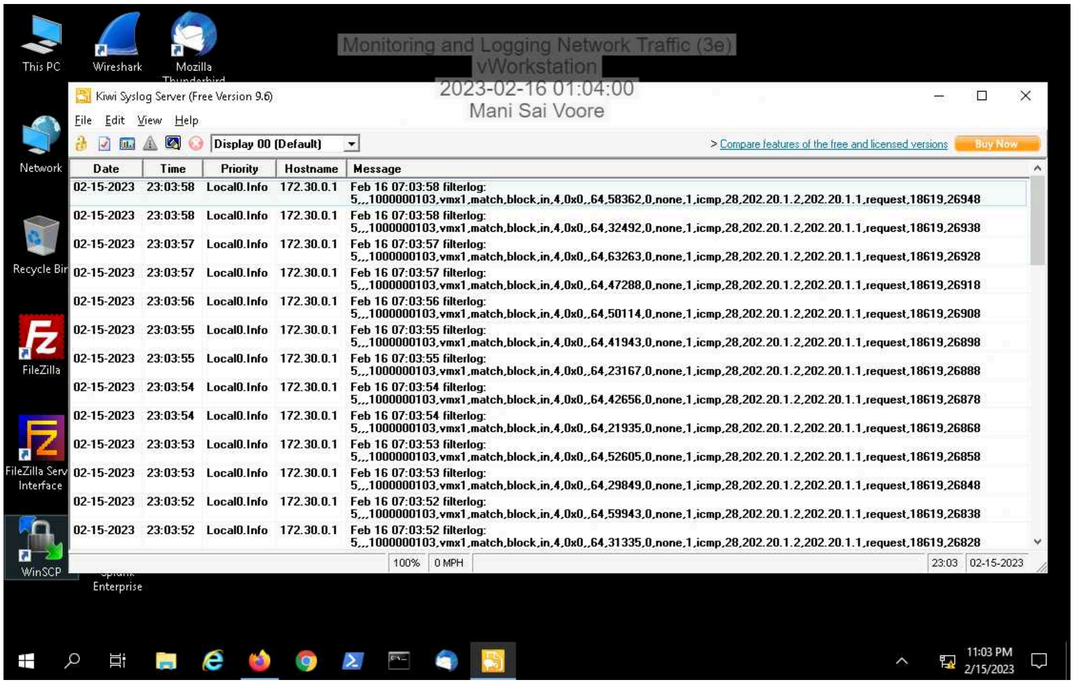
Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2023-02-15 06:15:57	⚠	3	ICMP	Misc activity	172.31.0.1		172.30.0.2		1:2100366	GPL ICMP_INFO PING *NIX
2023-02-15 06:15:57	⚠	3	ICMP	Misc activity	172.31.0.1		172.30.0.2		1:2100368	GPL ICMP_INFO PING BSDtype
2023-02-15 06:15:56	⚠	3	ICMP	Misc activity	172.31.0.1		172.30.0.2		1:2100366	GPL ICMP_INFO PING *NIX
2023-02-15 06:15:56	⚠	3	ICMP	Misc activity	172.31.0.1		172.30.0.2		1:2100368	GPL ICMP_INFO PING BSDtype
2023-02-15 06:15:55	⚠	3	ICMP	Misc activity	172.31.0.1		172.30.0.2		1:2100366	GPL ICMP_INFO PING *NIX
2023-02-15 06:15:55	⚠	3	ICMP	Misc activity	172.31.0.1		172.30.0.2		1:2100368	GPL ICMP_INFO PING BSDtype

pfSense is developed and maintained by Netgate. © ESF 2004 - 2023 View license.

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Part 3: Implement Firewall Log Forwarding with Kiwi Syslog Server

17. **Make a screen capture** showing the **pfSense firewall log events in Kiwi Syslog Server**.



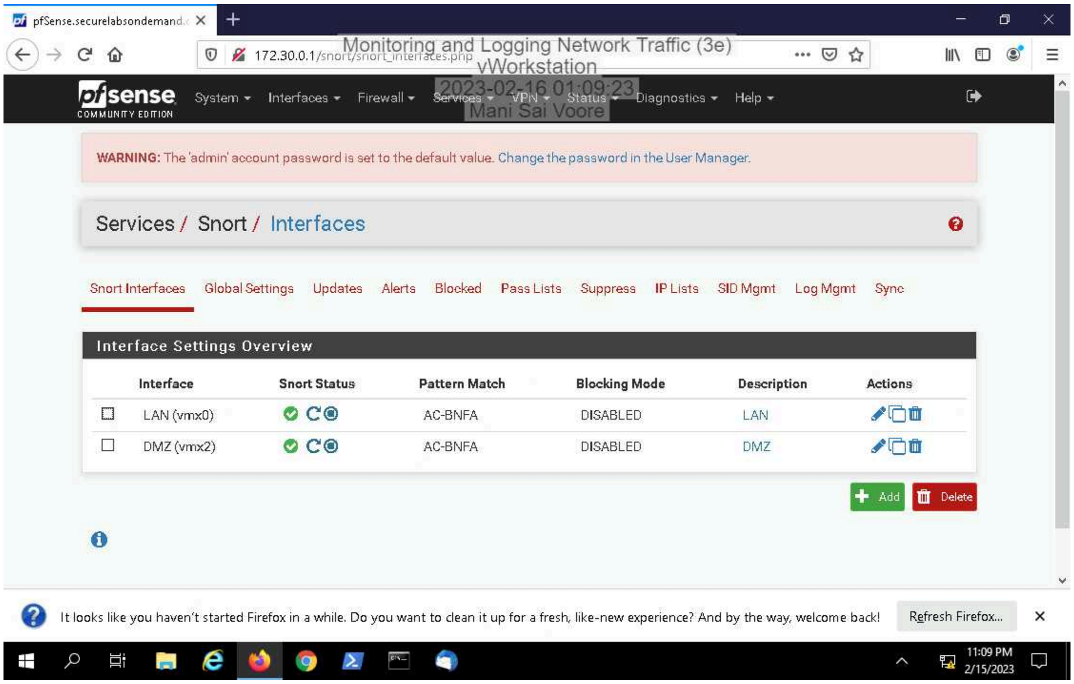
Monitoring and Logging Network Traffic (3e)
vWorkstation
2023-02-16 01:04:00
Mani Sai Voore

Date	Time	Priority	Hostname	Message
02-15-2023	23:03:58	Local0.Info	172.30.0.1	Feb 16 07:03:58 filterlog: 5,,,1000000103,vmx1,match,block,in,4,0x0,,64,58362,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,18619,26948
02-15-2023	23:03:58	Local0.Info	172.30.0.1	Feb 16 07:03:58 filterlog: 5,,,1000000103,vmx1,match,block,in,4,0x0,,64,32492,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,18619,26938
02-15-2023	23:03:57	Local0.Info	172.30.0.1	Feb 16 07:03:57 filterlog: 5,,,1000000103,vmx1,match,block,in,4,0x0,,64,63263,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,18619,26928
02-15-2023	23:03:57	Local0.Info	172.30.0.1	Feb 16 07:03:57 filterlog: 5,,,1000000103,vmx1,match,block,in,4,0x0,,64,47288,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,18619,26918
02-15-2023	23:03:56	Local0.Info	172.30.0.1	Feb 16 07:03:56 filterlog: 5,,,1000000103,vmx1,match,block,in,4,0x0,,64,50114,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,18619,26908
02-15-2023	23:03:55	Local0.Info	172.30.0.1	Feb 16 07:03:55 filterlog: 5,,,1000000103,vmx1,match,block,in,4,0x0,,64,41943,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,18619,26898
02-15-2023	23:03:55	Local0.Info	172.30.0.1	Feb 16 07:03:55 filterlog: 5,,,1000000103,vmx1,match,block,in,4,0x0,,64,23167,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,18619,26888
02-15-2023	23:03:54	Local0.Info	172.30.0.1	Feb 16 07:03:54 filterlog: 5,,,1000000103,vmx1,match,block,in,4,0x0,,64,42656,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,18619,26878
02-15-2023	23:03:54	Local0.Info	172.30.0.1	Feb 16 07:03:54 filterlog: 5,,,1000000103,vmx1,match,block,in,4,0x0,,64,21935,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,18619,26868
02-15-2023	23:03:53	Local0.Info	172.30.0.1	Feb 16 07:03:53 filterlog: 5,,,1000000103,vmx1,match,block,in,4,0x0,,64,52605,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,18619,26858
02-15-2023	23:03:53	Local0.Info	172.30.0.1	Feb 16 07:03:53 filterlog: 5,,,1000000103,vmx1,match,block,in,4,0x0,,64,29849,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,18619,26848
02-15-2023	23:03:52	Local0.Info	172.30.0.1	Feb 16 07:03:52 filterlog: 5,,,1000000103,vmx1,match,block,in,4,0x0,,64,59943,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,18619,26838
02-15-2023	23:03:52	Local0.Info	172.30.0.1	Feb 16 07:03:52 filterlog: 5,,,1000000103,vmx1,match,block,in,4,0x0,,64,31335,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,18619,26828

Section 2: Applied Learning

Part 1: Configure Snort Monitoring on the DMZ

17. **Make a screen capture** showing the **active Snort status on the DMZ interface**.



Monitoring and Logging Network Traffic (3e)
vWorkstation
2023-02-16 01:09:23
Mani Sai Voore

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

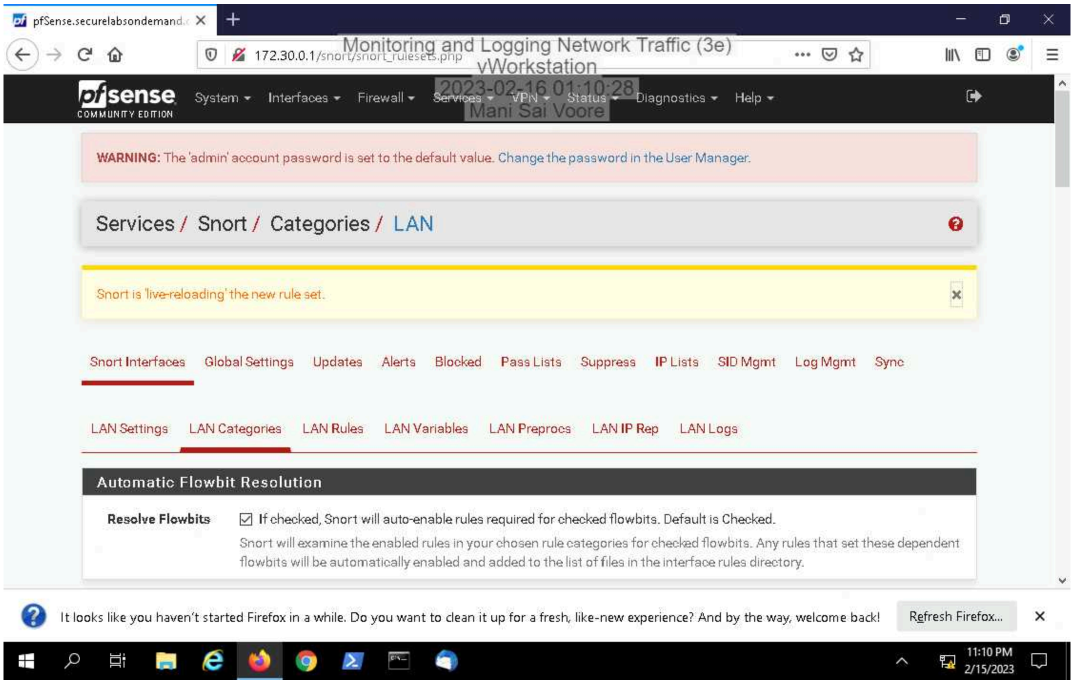
Services / Snort / Interfaces

Interface Settings Overview

	Interface	Snort Status	Pattern Match	Blocking Mode	Description	Actions
□	LAN (vmx0)	✓	AC-BNFA	DISABLED	LAN	
□	DMZ (vmx2)	✓	AC-BNFA	DISABLED	DMZ	

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

20. **Make a screen capture** showing the **Snort GPLv2 Community Rules enabled and "live-reloading" message**.



Monitoring and Logging Network Traffic (3e)
vWorkstation
2023-02-16 01:10:28
Mani Sai Voore

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Services / Snort / Categories / LAN

Snort is 'live-reloading' the new rule set.

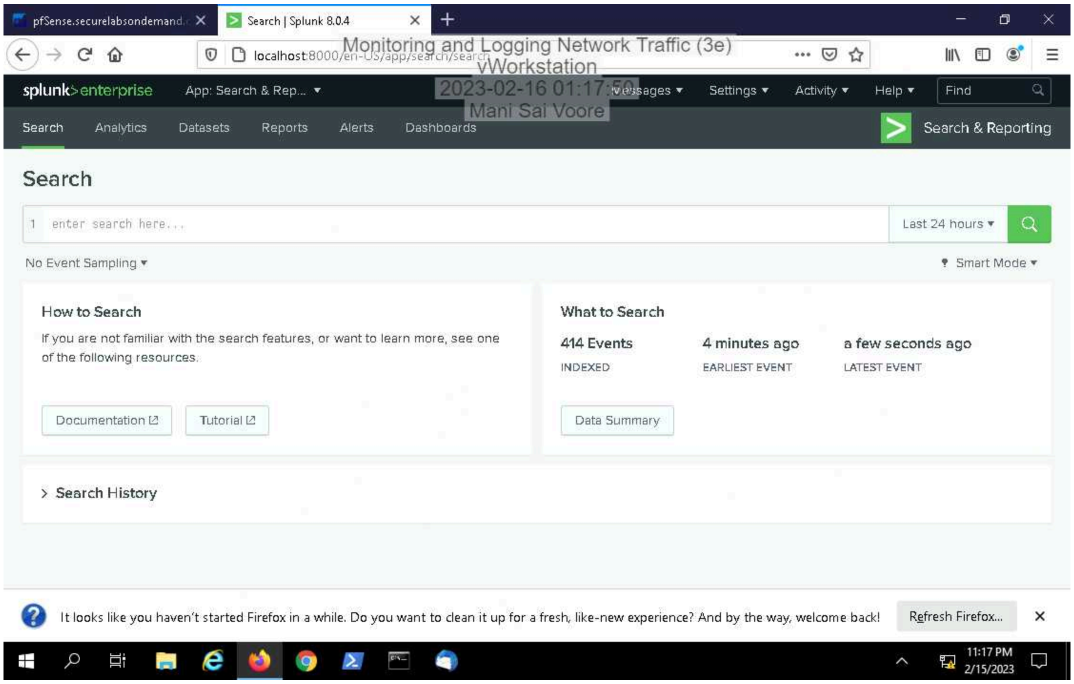
Automatic Flowbit Resolution

Resolve Flowbits ☑ If checked, Snort will auto-enable rules required for checked flowbits. Default is Checked.
Snort will examine the enabled rules in your chosen rule categories for checked flowbits. Any rules that set these dependent flowbits will be automatically enabled and added to the list of files in the interface rules directory.

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Part 2: Implement Security Information and Event Management with Splunk

13. **Make a screen capture** showing the **indexed events in Splunk**.



Monitoring and Logging Network Traffic (3e)
vWorkstation
2023-02-16 01:17:50
Mani Sai Voore

Search

How to Search

If you are not familiar with the search features, or want to learn more, see one of the following resources.

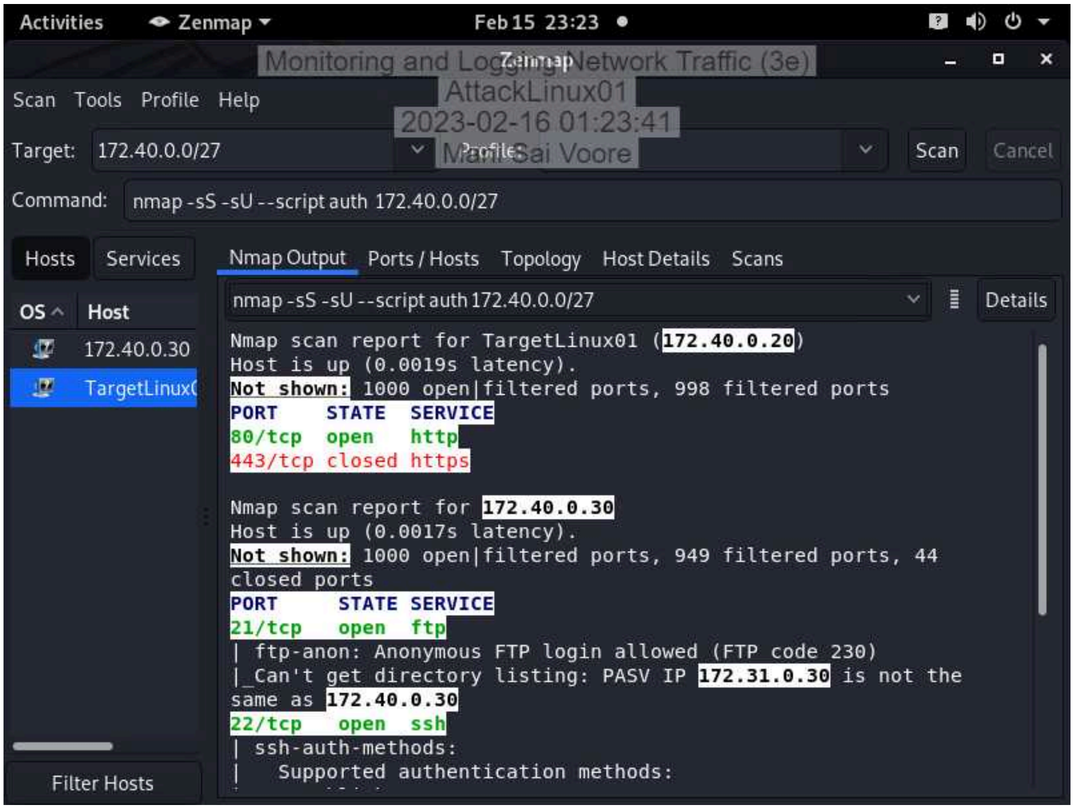
What to Search

414 Events	4 minutes ago	a few seconds ago
INDEXED	EARLIEST EVENT	LATEST EVENT

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Part 3: Simulate and Detect a Perimeter Network Attack

6. **Make a screen capture** showing the **Nmap scan report**.



Target: 172.40.0.0/27

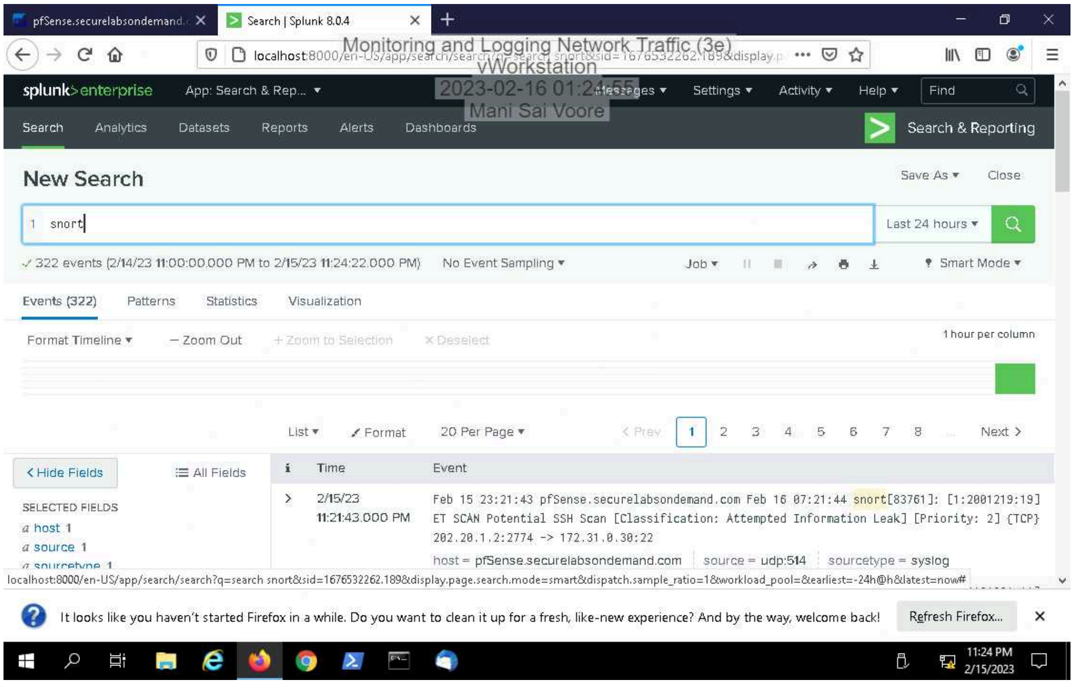
Command: nmap -sS -sU --script auth 172.40.0.0/27

```
nmap -sS -sU --script auth 172.40.0.0/27

Nmap scan report for TargetLinux01 (172.40.0.20)
Host is up (0.0019s latency).
Not shown: 1000 open|filtered ports, 998 filtered ports
PORT    STATE  SERVICE
80/tcp  open   http
443/tcp closed https

Nmap scan report for 172.40.0.30
Host is up (0.0017s latency).
Not shown: 1000 open|filtered ports, 949 filtered ports, 44
closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: PASV IP 172.31.0.30 is not the
same as 172.40.0.30
22/tcp   open  ssh
| ssh-auth-methods:
|   Supported authentication methods:
```

9. **Make a screen capture** showing the **search results in Splunk**.



Monitoring and Logging Network Traffic (3e)
vWorkstation
2023-02-16 01:24:55
Mani Sai Voore

snort

✓ 322 events (2/14/23 11:00:00.000 PM to 2/15/23 11:24:22.000 PM)

i	Time	Event
>	2/15/23 11:21:43.000 PM	Feb 15 23:21:43 pfSense.securelabsondemand.com Feb 16 07:21:44 snort[83761]: [1:2001219:19] ET SCAN Potential SSH Scan [Classification: Attempted Information Leak] [Priority: 2] {TCP} 202.20.1.2:2774 -> 172.31.0.30:22 host = pfSense.securelabsondemand.com source = udp:514 sourcetype = syslog

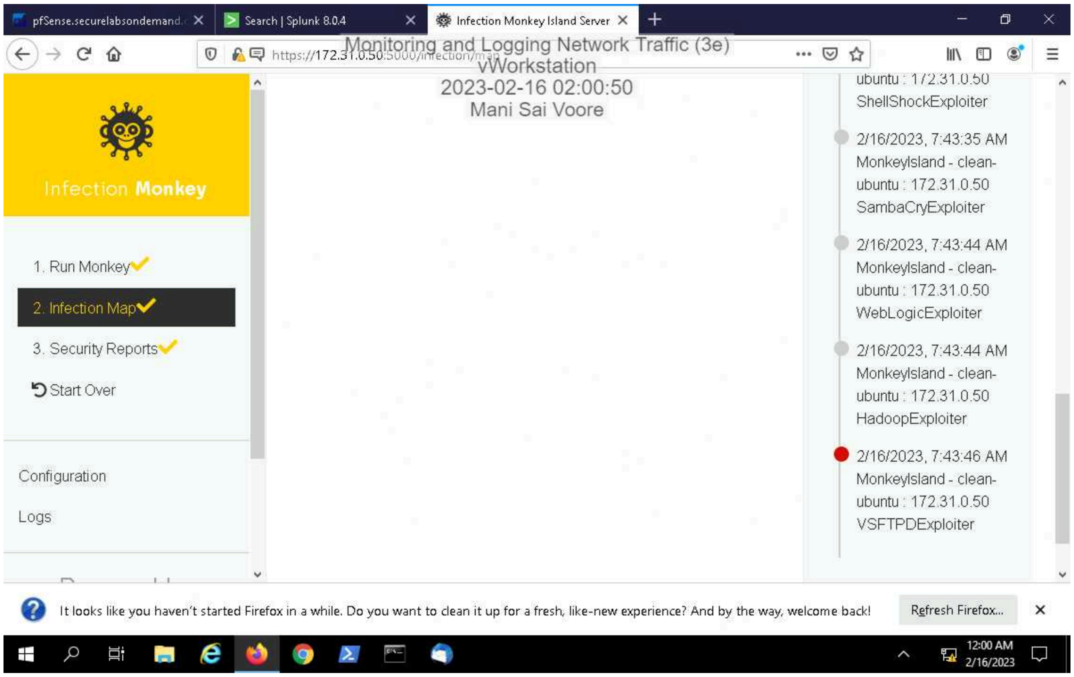
localhost:8000/en-US/app/search/search?q=search snort&sid=1676532262.189&display.page.search.mode=smart&dispatch.sample_ratio=1&workload_pool=&earliest=-24h@h&latest=now#

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Section 3: Challenge and Analysis

Part 1: Simulate a DMZ Breach with Infection Monkey

Make a screen capture showing the **resulting Infection Map**.



Monitoring and Logging Network Traffic (3e)
vWorkstation
2023-02-16 02:00:50
Mani Sai Voore

ubuntu : 172.31.0.50
ShellShockExploiter

2/16/2023, 7:43:35 AM
MonkeyIsland - clean-ubuntu : 172.31.0.50
SambaCryExploiter

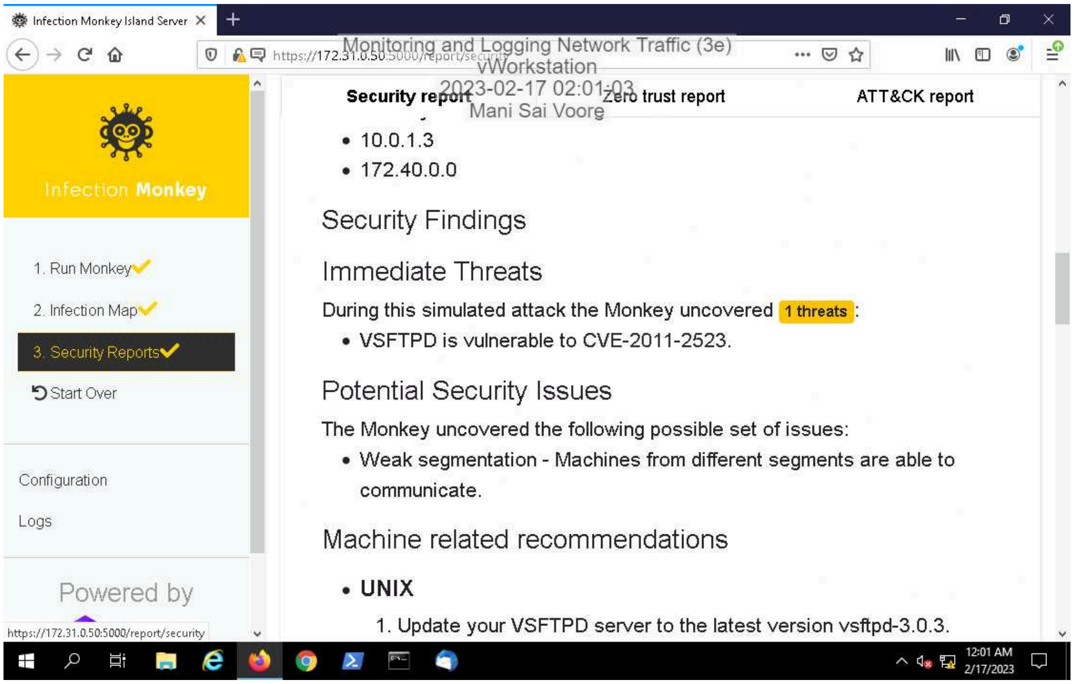
2/16/2023, 7:43:44 AM
MonkeyIsland - clean-ubuntu : 172.31.0.50
WebLogicExploiter

2/16/2023, 7:43:44 AM
MonkeyIsland - clean-ubuntu : 172.31.0.50
HadoopExploiter

2/16/2023, 7:43:46 AM
MonkeyIsland - clean-ubuntu : 172.31.0.50
VSFTPDExploiter

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Make a screen capture showing the **resulting Security Report**.



Monitoring and Logging Network Traffic (3e)
vWorkstation
2023-02-17 02:01:03
Mani Sai Voore

- 10.0.1.3
- 172.40.0.0

Security Findings

Immediate Threats

During this simulated attack the Monkey uncovered 1 threats:

- VSFTPD is vulnerable to CVE-2011-2523.

Potential Security Issues

The Monkey uncovered the following possible set of issues:

- Weak segmentation - Machines from different segments are able to communicate.

Machine related recommendations

- UNIX

1. Update your VSFTPD server to the latest version vsftpd-3.0.3.

Summarize your DMZ breach simulation results, highlighting what you found to be the greatest concerns from a network monitoring perspective.

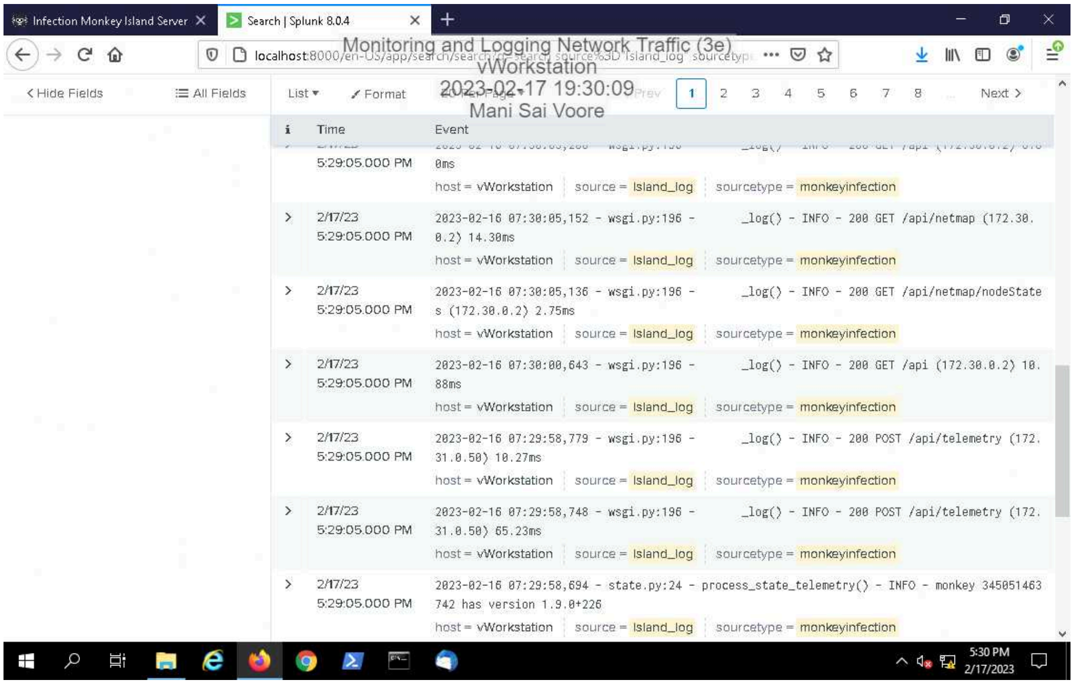
During the DMZ breach simulation there are 2 major concern were identified:
1. vulnerability of the VSFTD to CVE-2011-2523 which can make attacker to easily gain access to system.

2. Weak segmentation (Segmentation means : allows machine from different segments to communicate each other)of network this allow attackers to gain sensitive information or systems.

thus, highlights the important from network monitoring perspective.

Part 2: Detect a Simulated DMZ Breach with Snort and Splunk

Make a screen capture showing the **results of your search query for Infection Monkey traffic in Splunk**.



Monitoring and Logging Network Traffic (3e)
vWorkstation
2023-02-17 19:30:09
Mani Sai Voore

```
5:29:05.000 PM   0ms
                 host = vWorkstation | source = Island_log | sourcetype = monkeyinfection

2/17/23          2023-02-16 07:30:05,152 - wsgi.py:196 -       _log() - INFO - 200 GET /api/netmap (172.30.
5:29:05.000 PM   0.2) 14.30ms
                 host = vWorkstation | source = Island_log | sourcetype = monkeyinfection

2/17/23          2023-02-16 07:30:05,136 - wsgi.py:196 -       _log() - INFO - 200 GET /api/netmap/nodeState
5:29:05.000 PM   s (172.30.0.2) 2.75ms
                 host = vWorkstation | source = Island_log | sourcetype = monkeyinfection

2/17/23          2023-02-16 07:30:00,643 - wsgi.py:196 -       _log() - INFO - 200 GET /api (172.30.0.2) 10.
5:29:05.000 PM   88ms
                 host = vWorkstation | source = Island_log | sourcetype = monkeyinfection

2/17/23          2023-02-16 07:29:58,779 - wsgi.py:196 -       _log() - INFO - 200 POST /api/telemetry (172.
5:29:05.000 PM   31.0.50) 10.27ms
                 host = vWorkstation | source = Island_log | sourcetype = monkeyinfection

2/17/23          2023-02-16 07:29:58,748 - wsgi.py:196 -       _log() - INFO - 200 POST /api/telemetry (172.
5:29:05.000 PM   31.0.50) 65.23ms
                 host = vWorkstation | source = Island_log | sourcetype = monkeyinfection

2/17/23          2023-02-16 07:29:58,694 - state.py:24 - process_state_telemetry() - INFO - monkey 345051463
5:29:05.000 PM   742 has version 1.9.0+226
                 host = vWorkstation | source = Island_log | sourcetype = monkeyinfection
```

Infection Monkey Island Server
Search | Splunk 8.0.4
localhost:8000/en-US/app/search/search?q=search source%3D"Island_log" sourcetyp
< Hide Fields
All Fields
List
Format
Prev
1 2 3 4 5 6 7 8
Next >
i
Time
Event
5:30 PM
2/17/2023

Describe any concerns about the structure of the query result or the data elements it contains. What data fields would you add, remove, or edit to make log analysis more effective?

When running a query in Splunk and retrieving results, excessive data from the source log can hinder quick identification of relevant information. To address this, add important data fields like host, Source, timestamp, error and remove unwanted ones like tag or event type. Proper use of search commands and filters can yield valuable insights for informed decision making.

Write a brief memo to your manager describing Splunk's usefulness in detecting traces of your simulated breach. What configuration changes would you recommend? How would you enhance its functionality?

I'd like to highlight the effectiveness of Splunk in detecting traces of a recent simulated breach exercise. Splunk's ability to ingest, index, and analyze logs from various sources allowed us to identify any suspicious or anomalous activity in our system logs, track the attacker's movements, and investigate the incidents promptly. However, I suggest some configuration changes to enhance Splunk's functionality, including fine-tuning alerting thresholds, implementing machine learning algorithms to predict potential threats, increasing the log retention period, and integrating a SOAR tool and threat intelligence feeds. With these enhancements, Splunk can provide us with a robust security monitoring platform to identify and respond to threats more effectively.