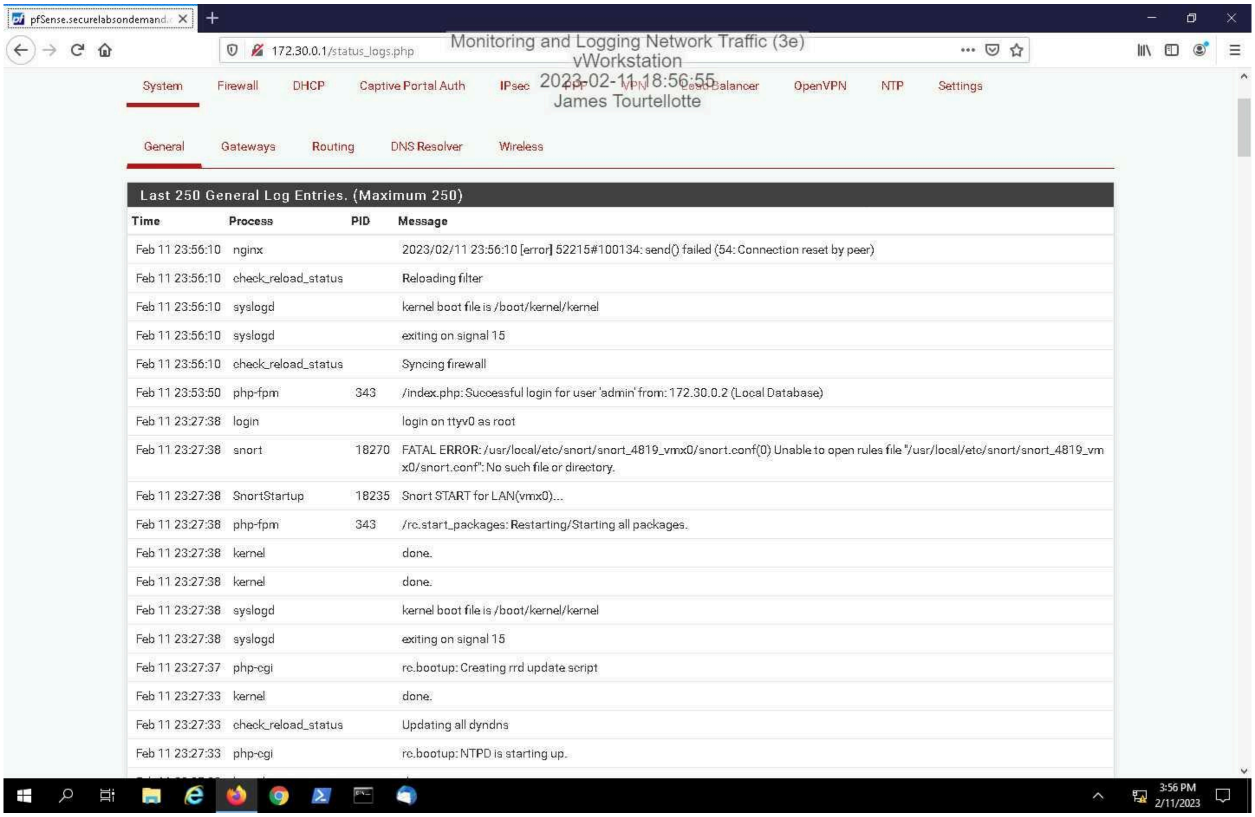
James Everett Tourtellotte IV
ITN 263
2/12/2023

Lab #6: Monitoring and Logging Network Traffic

Lab #6 Screen Captures

Screen Capture 1, Section 1:

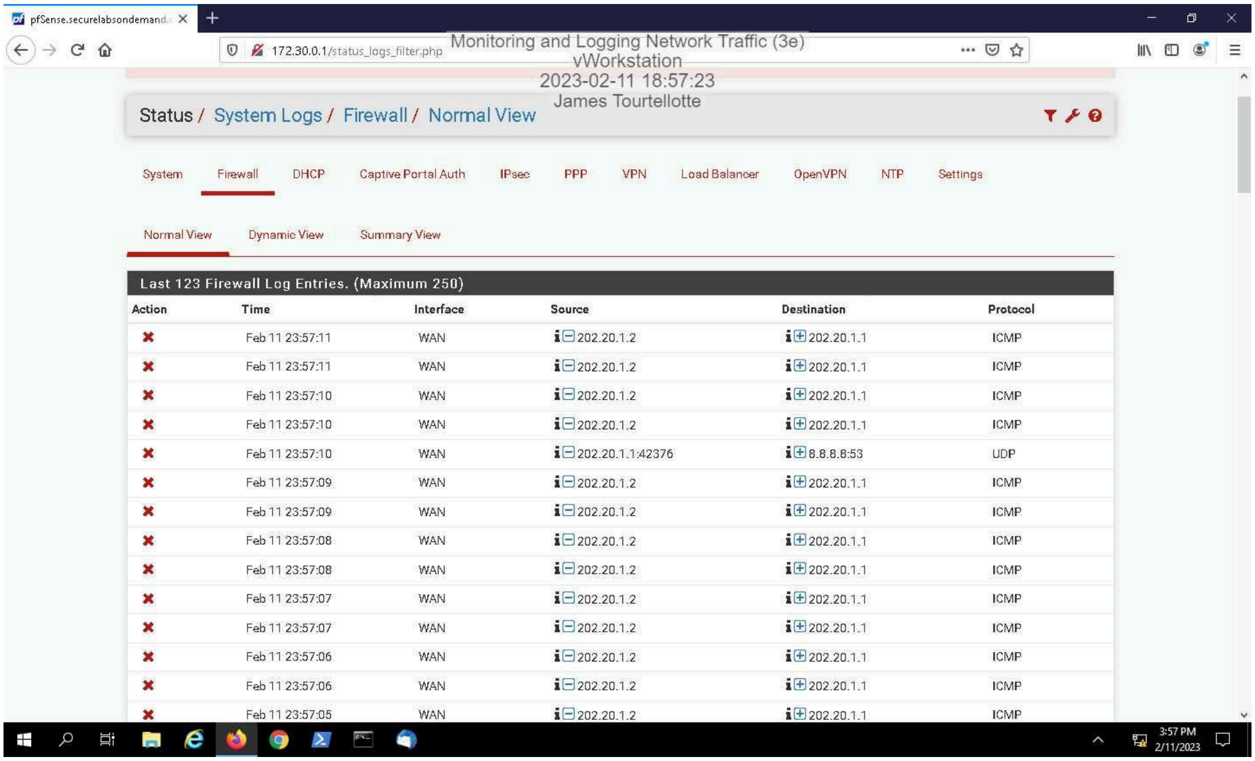


Monitoring and Logging Network Traffic (3e)
vWorkstation
2023-02-11 18:56:55
James Tourtellotte

Last 250 General Log Entries. (Maximum 250)

Time	Process	PID	Message
Feb 11 23:56:10	nginx		2023/02/11 23:56:10 [error] 52215#100134: send() failed (54: Connection reset by peer)
Feb 11 23:56:10	check_reload_status		Reloading filter
Feb 11 23:56:10	syslogd		kernel boot file is /boot/kernel/kernel
Feb 11 23:56:10	syslogd		exiting on signal 15
Feb 11 23:56:10	check_reload_status		Syncing firewall
Feb 11 23:53:50	php-fpm	343	/index.php: Successful login for user 'admin' from: 172.30.0.2 (Local Database)
Feb 11 23:27:38	login		login on ttyv0 as root
Feb 11 23:27:38	snort	18270	FATAL ERROR: /usr/local/etc/snort/snort_4819_vmx0/snort.conf(0) Unable to open rules file "/usr/local/etc/snort/snort_4819_vmx0/snort.conf": No such file or directory.
Feb 11 23:27:38	SnortStartup	18235	Snort START for LAN(vmx0)...
Feb 11 23:27:38	php-fpm	343	/rc.start_packages: Restarting/Starting all packages.
Feb 11 23:27:38	kernel		done.
Feb 11 23:27:38	kernel		done.
Feb 11 23:27:38	syslogd		kernel boot file is /boot/kernel/kernel
Feb 11 23:27:38	syslogd		exiting on signal 15
Feb 11 23:27:37	php-cgi		rc.bootup: Creating rrd update script
Feb 11 23:27:33	kernel		done.
Feb 11 23:27:33	check_reload_status		Updating all dyndns
Feb 11 23:27:33	php-cgi		rc.bootup: NTPD is starting up.

Screen Capture 2, Section 1:

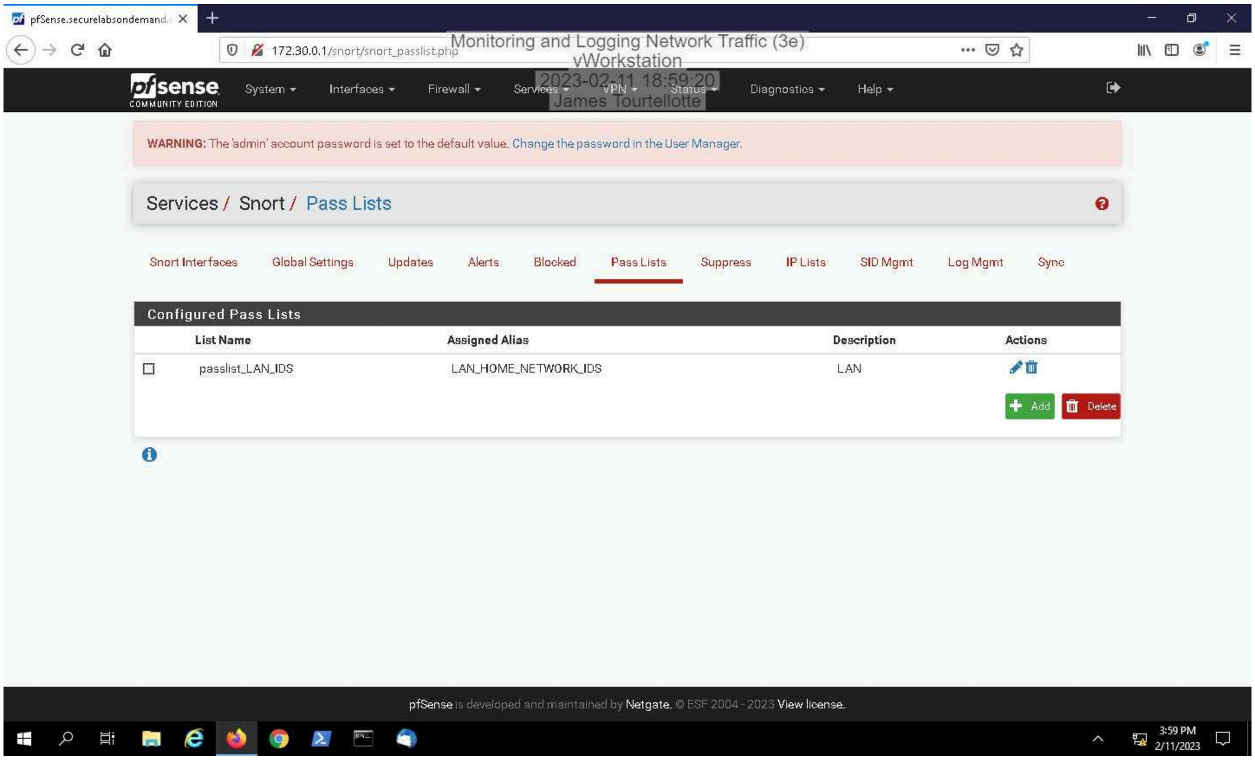


Monitoring and Logging Network Traffic (3e)
vWorkstation
2023-02-11 18:57:23
James Tourtellotte

Last 123 Firewall Log Entries. (Maximum 250)

Action	Time	Interface	Source	Destination	Protocol
✖	Feb 11 23:57:11	WAN	202.20.1.2	202.20.1.1	ICMP
✖	Feb 11 23:57:11	WAN	202.20.1.2	202.20.1.1	ICMP
✖	Feb 11 23:57:10	WAN	202.20.1.2	202.20.1.1	ICMP
✖	Feb 11 23:57:10	WAN	202.20.1.2	202.20.1.1	ICMP
✖	Feb 11 23:57:10	WAN	202.20.1.1:42376	8.8.8.8:53	UDP
✖	Feb 11 23:57:09	WAN	202.20.1.2	202.20.1.1	ICMP
✖	Feb 11 23:57:09	WAN	202.20.1.2	202.20.1.1	ICMP
✖	Feb 11 23:57:08	WAN	202.20.1.2	202.20.1.1	ICMP
✖	Feb 11 23:57:08	WAN	202.20.1.2	202.20.1.1	ICMP
✖	Feb 11 23:57:07	WAN	202.20.1.2	202.20.1.1	ICMP
✖	Feb 11 23:57:07	WAN	202.20.1.2	202.20.1.1	ICMP
✖	Feb 11 23:57:06	WAN	202.20.1.2	202.20.1.1	ICMP
✖	Feb 11 23:57:06	WAN	202.20.1.2	202.20.1.1	ICMP
✖	Feb 11 23:57:05	WAN	202.20.1.2	202.20.1.1	ICMP

Screen Capture 3, Section 1:



Monitoring and Logging Network Traffic (3e)
vWorkstation
2023-02-11 18:59:20
James Tourtellotte

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

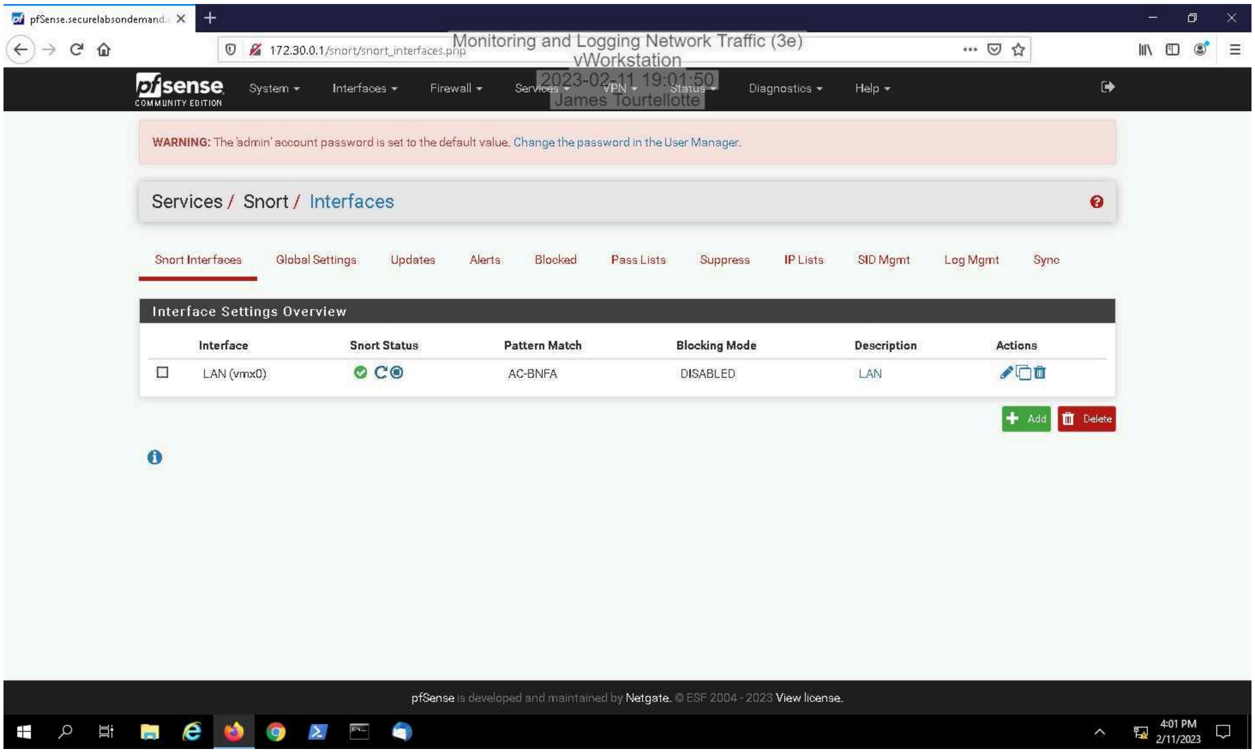
Services / Snort / Pass Lists

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.

Screen Capture 4, Section 1:



Monitoring and Logging Network Traffic (3e)
vWorkstation
2023-02-11 19:01:50
James Tourtellotte

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

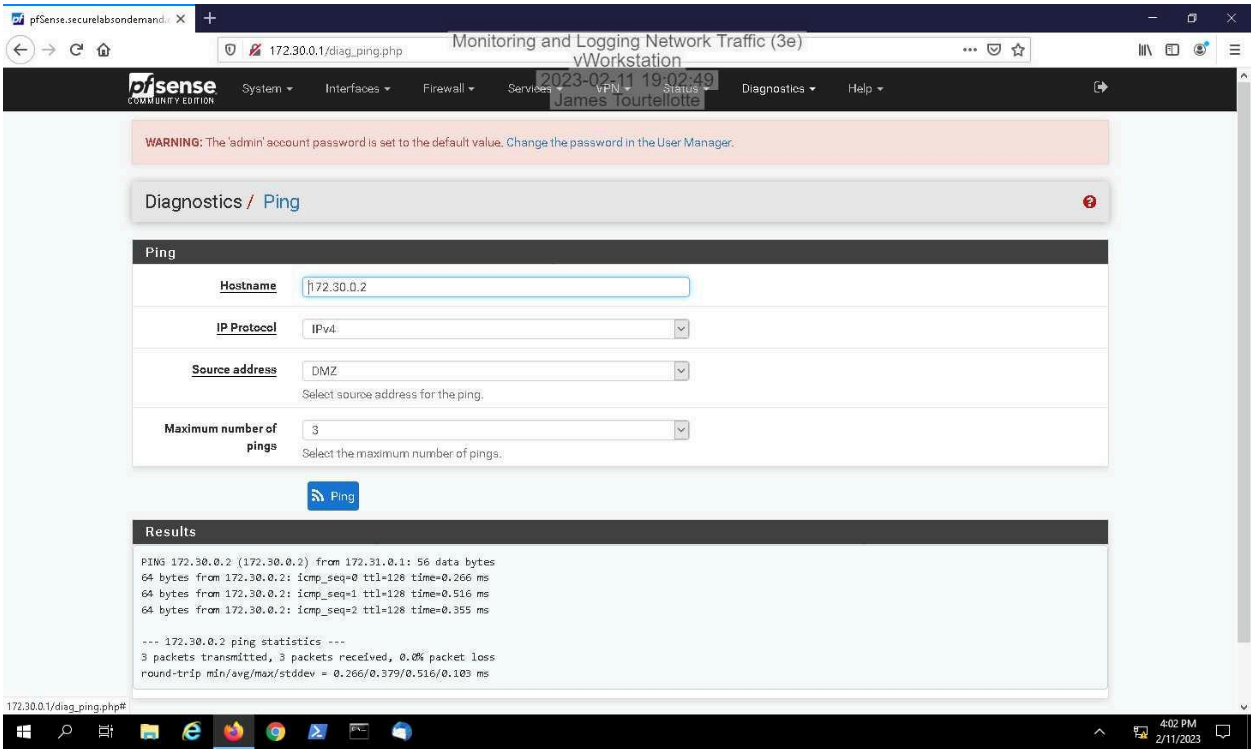
Services / Snort / Interfaces

Interface Settings Overview

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

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

Screen Capture 5, Section 1:



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

Diagnostics / Ping

Ping

Hostname: 172.30.0.2

IP Protocol: IPv4

Source address: DMZ
Select source address for the ping.

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

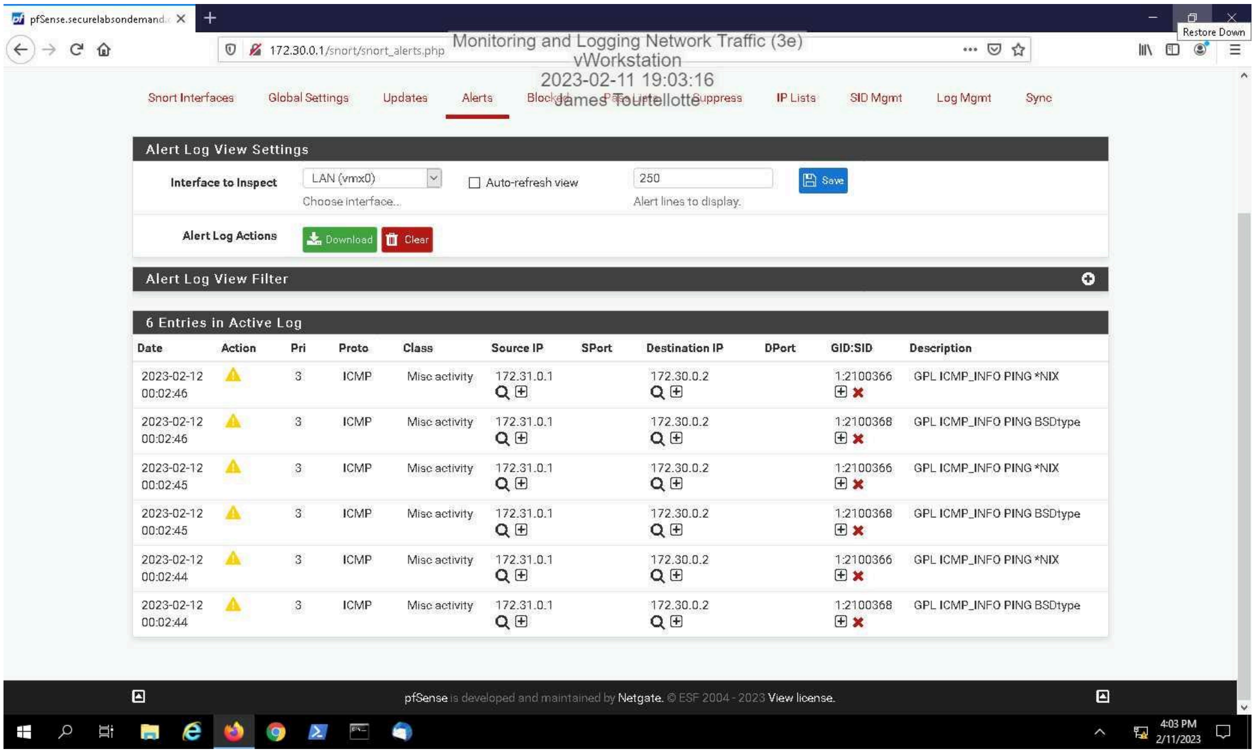
Ping

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=0.266 ms
64 bytes from 172.30.0.2: icmp_seq=1 ttl=128 time=0.516 ms
64 bytes from 172.30.0.2: icmp_seq=2 ttl=128 time=0.355 ms

--- 172.30.0.2 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.266/0.379/0.516/0.103 ms
```

Screen Capture 6, Section 1:



Monitoring and Logging Network Traffic (3e)
vWorkstation
2023-02-11 19:03:16
James Tourtellotte

Alert Log View Settings

Interface to Inspect: LAN (vmx0)
Choose interface...

☐ Auto-refresh view

250
Alert lines to display.

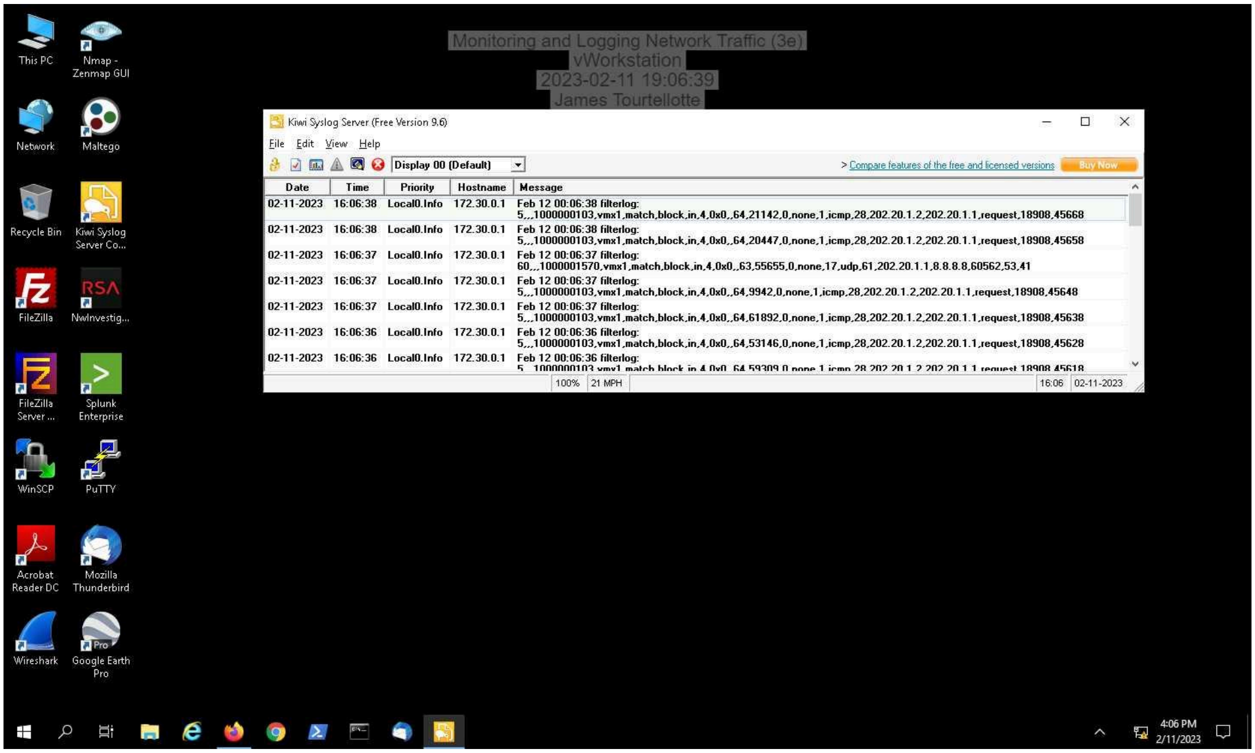
Alert Log Actions

Alert Log View Filter

6 Entries in Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2023-02-12 00:02:46	⚠	3	ICMP	Misc activity	172.31.0.1		172.30.0.2		1:2100366	GPL ICMP_INFO PING *NIX
2023-02-12 00:02:46	⚠	3	ICMP	Misc activity	172.31.0.1		172.30.0.2		1:2100368	GPL ICMP_INFO PING BSDtype
2023-02-12 00:02:45	⚠	3	ICMP	Misc activity	172.31.0.1		172.30.0.2		1:2100366	GPL ICMP_INFO PING *NIX
2023-02-12 00:02:45	⚠	3	ICMP	Misc activity	172.31.0.1		172.30.0.2		1:2100368	GPL ICMP_INFO PING BSDtype
2023-02-12 00:02:44	⚠	3	ICMP	Misc activity	172.31.0.1		172.30.0.2		1:2100366	GPL ICMP_INFO PING *NIX
2023-02-12 00:02:44	⚠	3	ICMP	Misc activity	172.31.0.1		172.30.0.2		1:2100368	GPL ICMP_INFO PING BSDtype

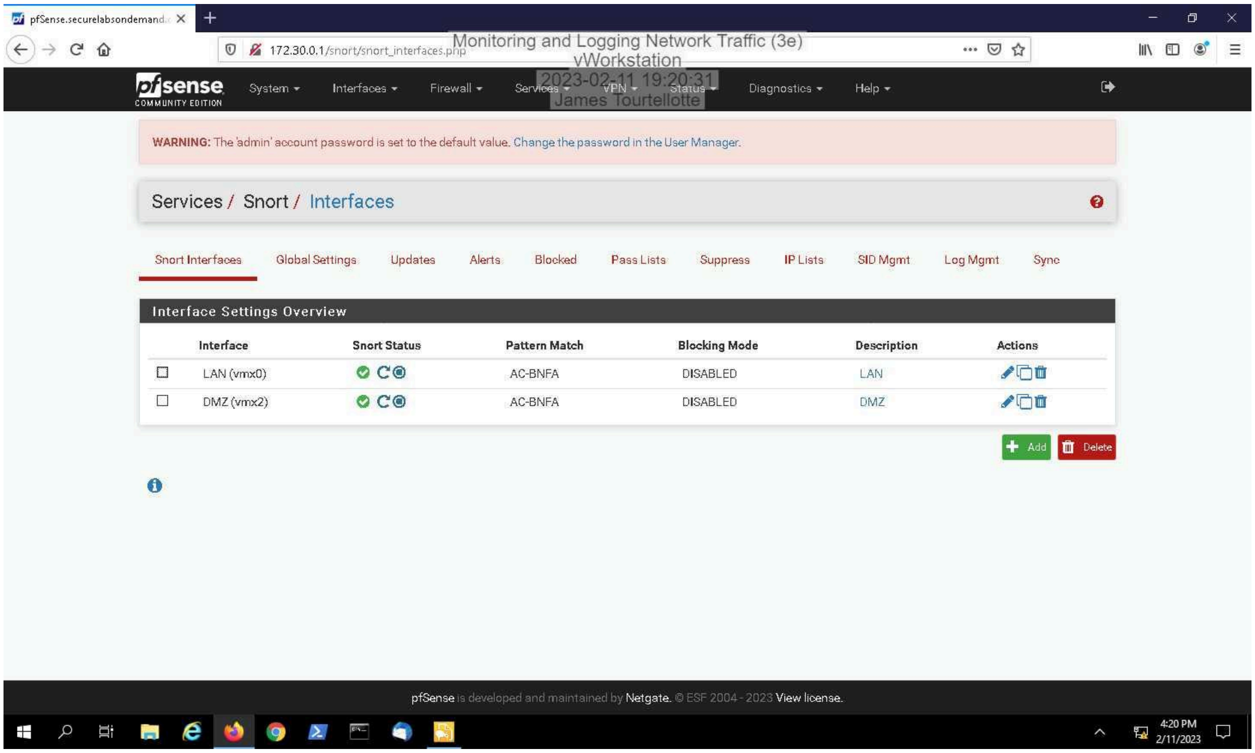
Screen Capture 7, Section 1:


Monitoring and Logging Network Traffic (3e)
vWorkstation
2023-02-11 19:06:39
James Tourtellotte

Kiwi Syslog Server (Free Version 9.6)

```
Date        Time      Priority     Hostname    Message
02-11-2023  16:06:38  Local0.Info  172.30.0.1  Feb 12 00:06:38 filterlog:
                                               5,,,1000000103,vmx1,match,block,in,4,0x0,,64,21142,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,18908,45668
02-11-2023  16:06:38  Local0.Info  172.30.0.1  Feb 12 00:06:38 filterlog:
                                               5,,,1000000103,vmx1,match,block,in,4,0x0,,64,20447,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,18908,45658
02-11-2023  16:06:37  Local0.Info  172.30.0.1  Feb 12 00:06:37 filterlog:
                                               60,,,1000001570,vmx1,match,block,in,4,0x0,,63,55655,0,none,17,udp,61,202.20.1.1,8.8.8.8,60562,53,41
02-11-2023  16:06:37  Local0.Info  172.30.0.1  Feb 12 00:06:37 filterlog:
                                               5,,,1000000103,vmx1,match,block,in,4,0x0,,64,9942,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,18908,45648
02-11-2023  16:06:37  Local0.Info  172.30.0.1  Feb 12 00:06:37 filterlog:
                                               5,,,1000000103,vmx1,match,block,in,4,0x0,,64,61892,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,18908,45638
02-11-2023  16:06:36  Local0.Info  172.30.0.1  Feb 12 00:06:36 filterlog:
                                               5,,,1000000103,vmx1,match,block,in,4,0x0,,64,53146,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,18908,45628
02-11-2023  16:06:36  Local0.Info  172.30.0.1  Feb 12 00:06:36 filterlog:
                                               5,,,1000000103,vmx1,match,block,in,4,0x0,,64,59309,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,18908,45618
```

Screen Capture 1, Section 2:


Monitoring and Logging Network Traffic (3e)
vWorkstation
2023-02-11 19:20:31
James Tourtellotte

172.30.0.1/snort/snort_interfaces.php

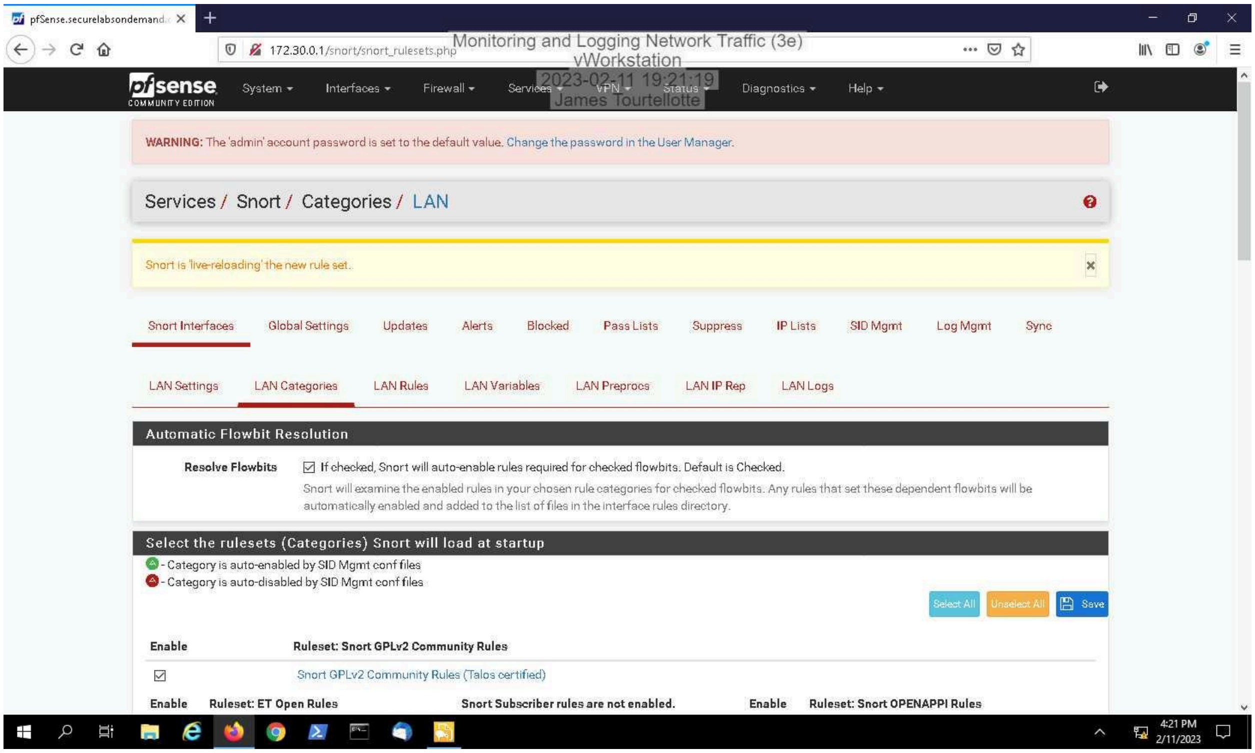
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

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	

Screen Capture 2, Section 2:



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.

Select the rulesets (Categories) Snort will load at startup

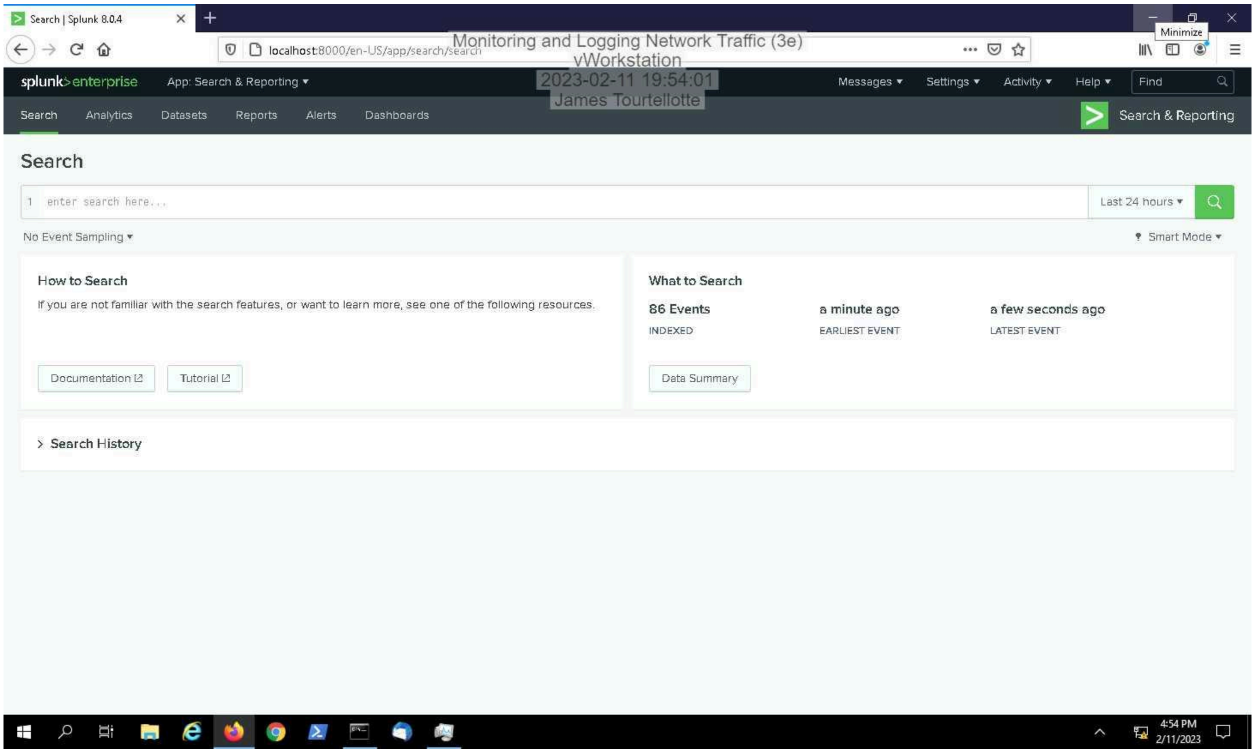
🟢 - Category is auto-enabled by SID Mgmt conf files

🔴 - Category is auto-disabled by SID Mgmt conf files

Enable	Ruleset: Snort GPLv2 Community Rules
☑	Snort GPLv2 Community Rules (Talos certified)

Enable **Ruleset: ET Open Rules** **Snort Subscriber rules are not enabled.** **Enable** **Ruleset: Snort OPENAPPI Rules**

Screen Capture 3, Section 2:



Monitoring and Logging Network Traffic (3e)
vWorkstation
2023-02-11 19:54:01
James Tourtellotte

localhost:8000/en-US/app/search/search

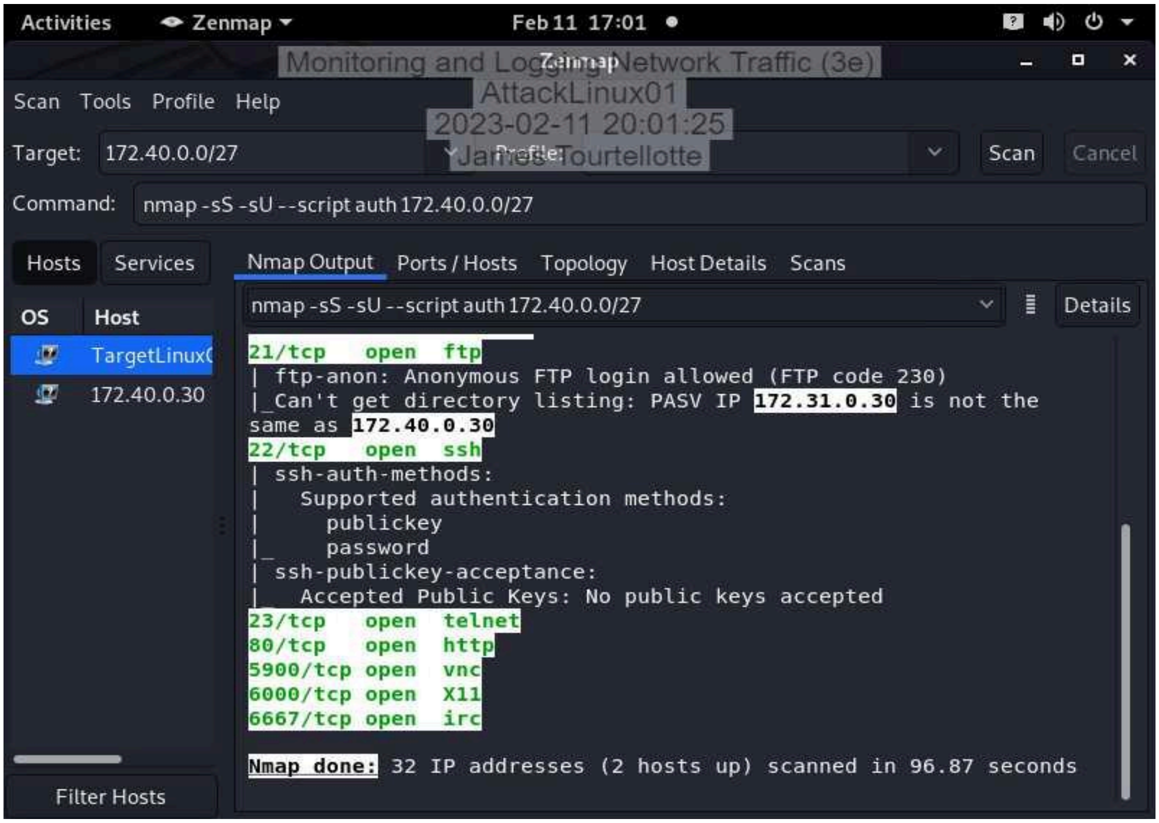
What to Search

86 Events INDEXED | a minute ago EARLIEST EVENT | a few seconds ago LATEST EVENT

How to Search

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

Screen Capture 4, Section 2:



Target: 172.40.0.0/27

Profile:

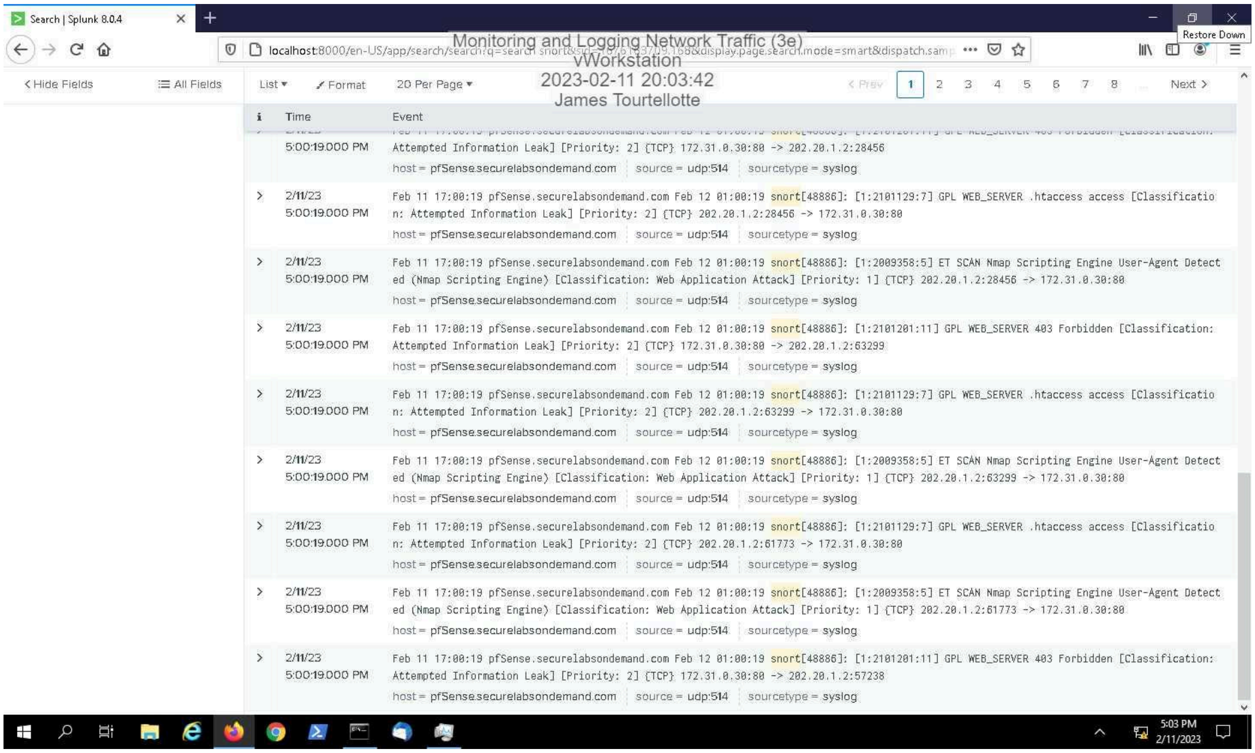
Command: nmap -sS -sU --script auth 172.40.0.0/27

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

```
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:
|     publickey
|_    password
| ssh-publickey-acceptance:
|_  Accepted Public Keys: No public keys accepted
23/tcp   open  telnet
80/tcp   open  http
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc

Nmap done: 32 IP addresses (2 hosts up) scanned in 96.87 seconds
```

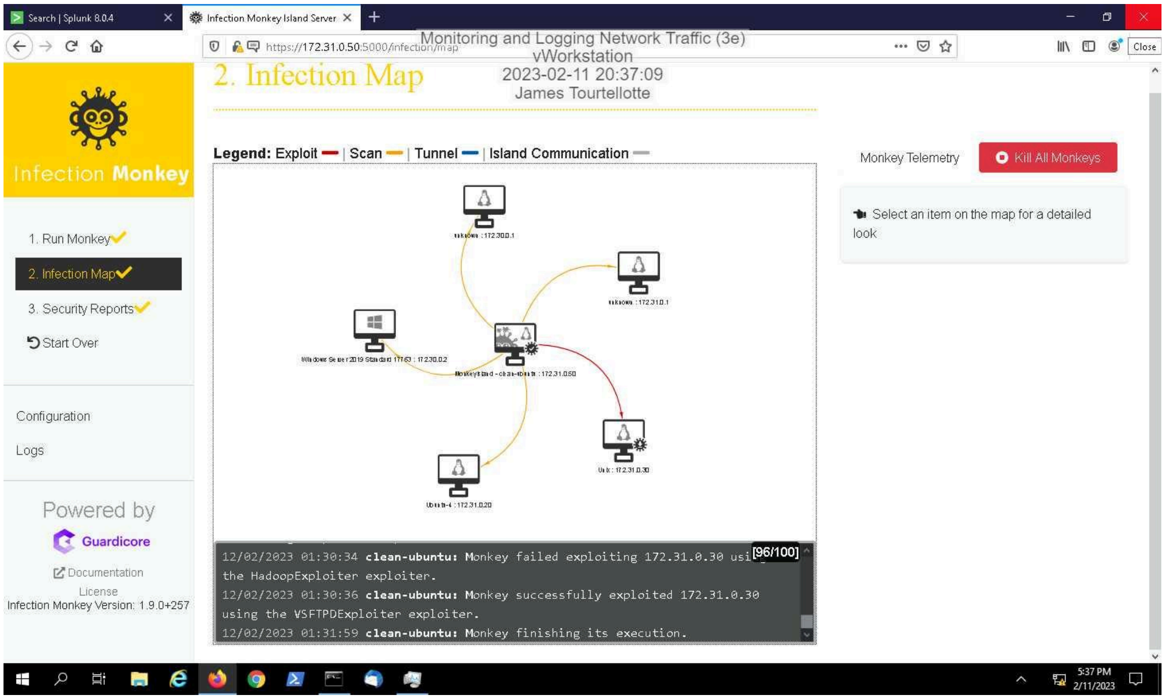
Screen Capture 5, Section 2:



Monitoring and Logging Network Traffic (3e)
vWorkstation
2023-02-11 20:03:42
James Tourtellotte

```
i  Time                  Event
   5:00:19.000 PM        Attempted Information Leak] [Priority: 2] {TCP} 172.31.0.30:80 -> 202.20.1.2:28456
                         host = pfSense.securelabsondemand.com   source = udp:514   sourcetype = syslog
>  2/11/23               Feb 11 17:00:19 pfSense.securelabsondemand.com Feb 12 01:00:19 snort[48886]: [1:2101129:7] GPL WEB_SERVER .htaccess access [Classificatio
   5:00:19.000 PM        n: Attempted Information Leak] [Priority: 2] {TCP} 202.20.1.2:28456 -> 172.31.0.30:80
                         host = pfSense.securelabsondemand.com   source = udp:514   sourcetype = syslog
>  2/11/23               Feb 11 17:00:19 pfSense.securelabsondemand.com Feb 12 01:00:19 snort[48886]: [1:2009358:5] ET SCAN Nmap Scripting Engine User-Agent Detect
   5:00:19.000 PM        ed (Nmap Scripting Engine) [Classification: Web Application Attack] [Priority: 1] {TCP} 202.20.1.2:28456 -> 172.31.0.30:80
                         host = pfSense.securelabsondemand.com   source = udp:514   sourcetype = syslog
>  2/11/23               Feb 11 17:00:19 pfSense.securelabsondemand.com Feb 12 01:00:19 snort[48886]: [1:2101201:11] GPL WEB_SERVER 403 Forbidden [Classification:
   5:00:19.000 PM        Attempted Information Leak] [Priority: 2] {TCP} 172.31.0.30:80 -> 202.20.1.2:63299
                         host = pfSense.securelabsondemand.com   source = udp:514   sourcetype = syslog
>  2/11/23               Feb 11 17:00:19 pfSense.securelabsondemand.com Feb 12 01:00:19 snort[48886]: [1:2101129:7] GPL WEB_SERVER .htaccess access [Classificatio
   5:00:19.000 PM        n: Attempted Information Leak] [Priority: 2] {TCP} 202.20.1.2:63299 -> 172.31.0.30:80
                         host = pfSense.securelabsondemand.com   source = udp:514   sourcetype = syslog
>  2/11/23               Feb 11 17:00:19 pfSense.securelabsondemand.com Feb 12 01:00:19 snort[48886]: [1:2009358:5] ET SCAN Nmap Scripting Engine User-Agent Detect
   5:00:19.000 PM        ed (Nmap Scripting Engine) [Classification: Web Application Attack] [Priority: 1] {TCP} 202.20.1.2:63299 -> 172.31.0.30:80
                         host = pfSense.securelabsondemand.com   source = udp:514   sourcetype = syslog
>  2/11/23               Feb 11 17:00:19 pfSense.securelabsondemand.com Feb 12 01:00:19 snort[48886]: [1:2101129:7] GPL WEB_SERVER .htaccess access [Classificatio
   5:00:19.000 PM        n: Attempted Information Leak] [Priority: 2] {TCP} 202.20.1.2:61773 -> 172.31.0.30:80
                         host = pfSense.securelabsondemand.com   source = udp:514   sourcetype = syslog
>  2/11/23               Feb 11 17:00:19 pfSense.securelabsondemand.com Feb 12 01:00:19 snort[48886]: [1:2009358:5] ET SCAN Nmap Scripting Engine User-Agent Detect
   5:00:19.000 PM        ed (Nmap Scripting Engine) [Classification: Web Application Attack] [Priority: 1] {TCP} 202.20.1.2:61773 -> 172.31.0.30:80
                         host = pfSense.securelabsondemand.com   source = udp:514   sourcetype = syslog
>  2/11/23               Feb 11 17:00:19 pfSense.securelabsondemand.com Feb 12 01:00:19 snort[48886]: [1:2101201:11] GPL WEB_SERVER 403 Forbidden [Classification:
   5:00:19.000 PM        Attempted Information Leak] [Priority: 2] {TCP} 172.31.0.30:80 -> 202.20.1.2:57238
                         host = pfSense.securelabsondemand.com   source = udp:514   sourcetype = syslog
```

Screen Capture 1, Section 3:



Monitoring and Logging Network Traffic (3e)
vWorkstation
2023-02-11 20:37:09
James Tourtellotte

```
12/02/2023 01:30:34 clean-ubuntu: Monkey failed exploiting 172.31.0.30 usi[96/100]
the HadoopExploiter exploiter.
12/02/2023 01:30:36 clean-ubuntu: Monkey successfully exploited 172.31.0.30
using the VSFTPDExploiter exploiter.
12/02/2023 01:31:59 clean-ubuntu: Monkey finishing its execution.
```