Student:	Email:
Jalen Salgado	jsalgado1915@gmail.com

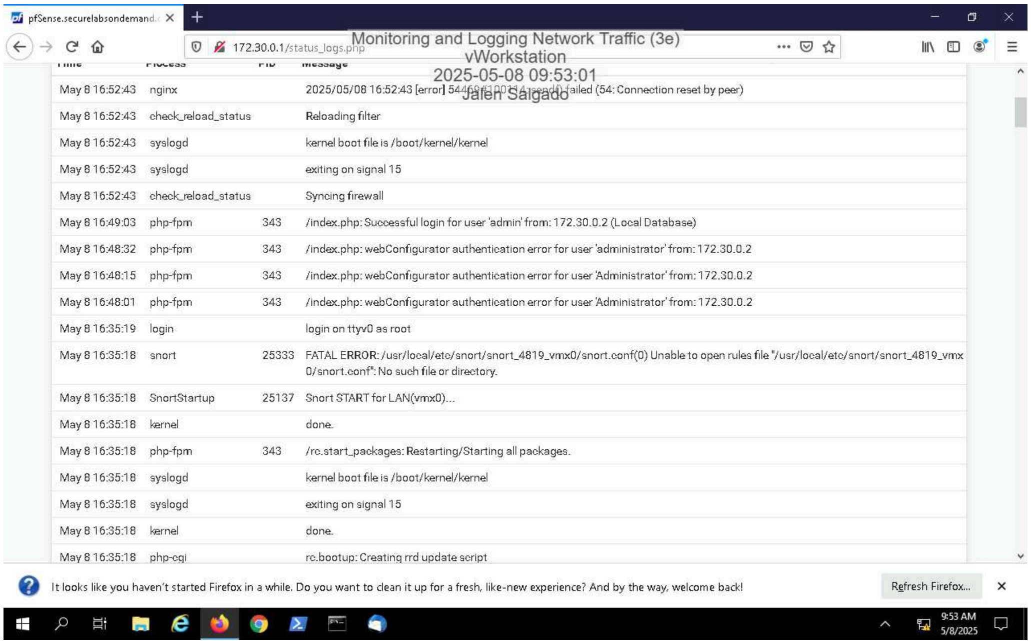
Time on Task:	Progress:
2 hours, 20 minutes	100%

Report Generated: Saturday, July 26, 2025 at 2:11 PM

Section 1: Hands-On Demonstration

Part 1: Configure the pfSense Firewall Log

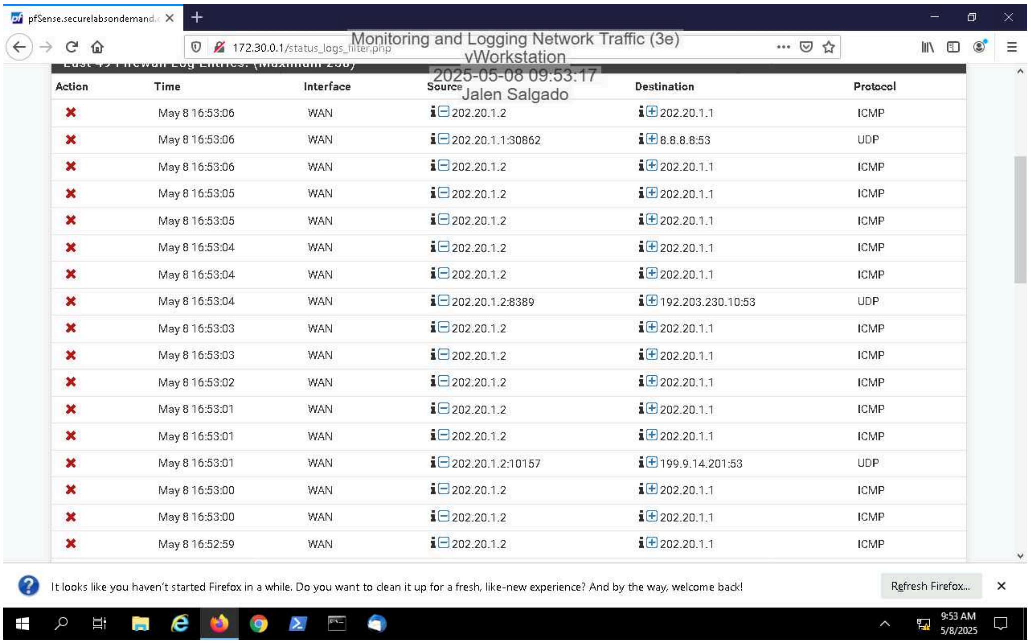
13. **Make a screen capture** showing the **system logs**.



```
Time             Process              PID    Message
May 8 16:52:43   nginx                       2025/05/08 16:52:43 [error] 54469#100114: send() failed (54: Connection reset by peer)
May 8 16:52:43   check_reload_status         Reloading filter
May 8 16:52:43   syslogd                     kernel boot file is /boot/kernel/kernel
May 8 16:52:43   syslogd                     exiting on signal 15
May 8 16:52:43   check_reload_status         Syncing firewall
May 8 16:49:03   php-fpm              343    /index.php: Successful login for user 'admin' from: 172.30.0.2 (Local Database)
May 8 16:48:32   php-fpm              343    /index.php: webConfigurator authentication error for user 'administrator' from: 172.30.0.2
May 8 16:48:15   php-fpm              343    /index.php: webConfigurator authentication error for user 'Administrator' from: 172.30.0.2
May 8 16:48:01   php-fpm              343    /index.php: webConfigurator authentication error for user 'Administrator' from: 172.30.0.2
May 8 16:35:19   login                       login on ttyv0 as root
May 8 16:35:18   snort                25333  FATAL ERROR: /usr/local/etc/snort/snort_4819_vmx0/snort.conf(0) Unable to open rules file "/usr/local/etc/snort/snort_4819_vmx
                                             0/snort.conf": No such file or directory.
May 8 16:35:18   SnortStartup         25137  Snort START for LAN(vmx0)...
May 8 16:35:18   kernel                      done.
May 8 16:35:18   php-fpm              343    /rc.start_packages: Restarting/Starting all packages.
May 8 16:35:18   syslogd                     kernel boot file is /boot/kernel/kernel
May 8 16:35:18   syslogd                     exiting on signal 15
May 8 16:35:18   kernel                      done.
May 8 16:35:18   php-cgi                     rc.bootup: Creating rrd update script
```

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**.



pfSense.securelabsondemand.
172.30.0.1/status_logs_filter.php

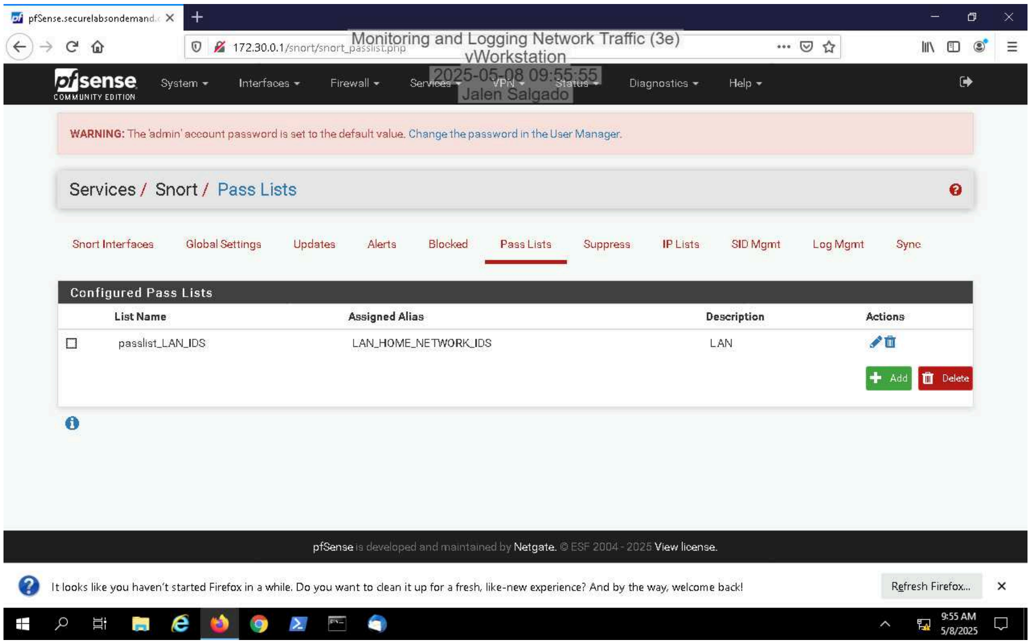
Monitoring and Logging Network Traffic (3e)
vWorkstation
2025-05-08 09:53:17
Jalen Salgado

Action	Time	Interface	Source	Destination	Protocol
✖	May 8 16:53:06	WAN	202.20.1.2	202.20.1.1	ICMP
✖	May 8 16:53:06	WAN	202.20.1.1:30862	8.8.8.8:53	UDP
✖	May 8 16:53:06	WAN	202.20.1.2	202.20.1.1	ICMP
✖	May 8 16:53:05	WAN	202.20.1.2	202.20.1.1	ICMP
✖	May 8 16:53:05	WAN	202.20.1.2	202.20.1.1	ICMP
✖	May 8 16:53:04	WAN	202.20.1.2	202.20.1.1	ICMP
✖	May 8 16:53:04	WAN	202.20.1.2	202.20.1.1	ICMP
✖	May 8 16:53:04	WAN	202.20.1.2:8389	192.203.230.10:53	UDP
✖	May 8 16:53:03	WAN	202.20.1.2	202.20.1.1	ICMP
✖	May 8 16:53:03	WAN	202.20.1.2	202.20.1.1	ICMP
✖	May 8 16:53:02	WAN	202.20.1.2	202.20.1.1	ICMP
✖	May 8 16:53:01	WAN	202.20.1.2	202.20.1.1	ICMP
✖	May 8 16:53:01	WAN	202.20.1.2	202.20.1.1	ICMP
✖	May 8 16:53:01	WAN	202.20.1.2:10157	199.9.14.201:53	UDP
✖	May 8 16:53:00	WAN	202.20.1.2	202.20.1.1	ICMP
✖	May 8 16:53:00	WAN	202.20.1.2	202.20.1.1	ICMP
✖	May 8 16:52:59	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**.



pfSense.securelabsondemand.
172.30.0.1/snort/snort_passlist.php
pf sense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help

Monitoring and Logging Network Traffic (3e)
vWorkstation
2025-05-08 09:55:55
Jalen Salgado

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

Services / Snort / Pass Lists

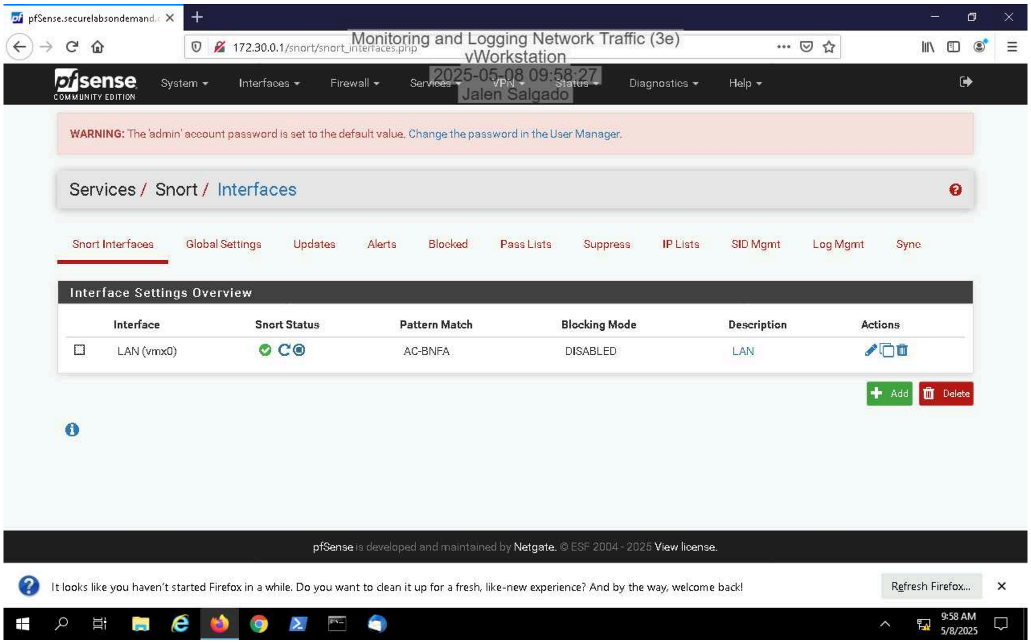
Configured Pass Lists

	List Name	Assigned Alias	Description	Actions
□	passlist_LAN_IDS	LAN_HOME_NETWORK_IDS	LAN	

pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 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
2025-05-08 09:58:27
Jalen Salgado

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

Services / Snort / Interfaces

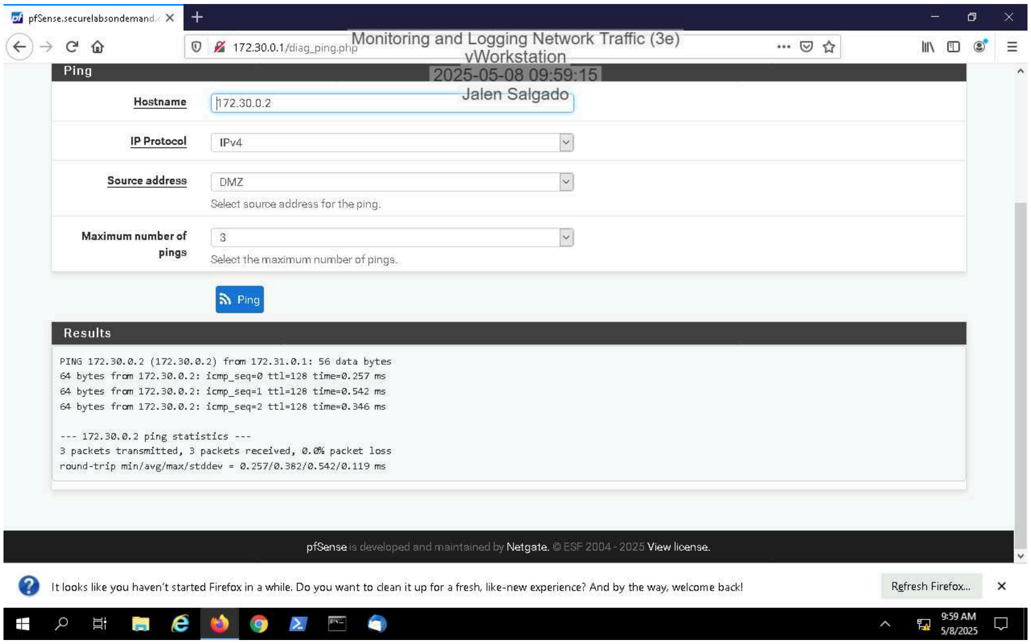
Interface Settings Overview

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

pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 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
2025-05-08 09:59:15
Jalen Salgado

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.

Results

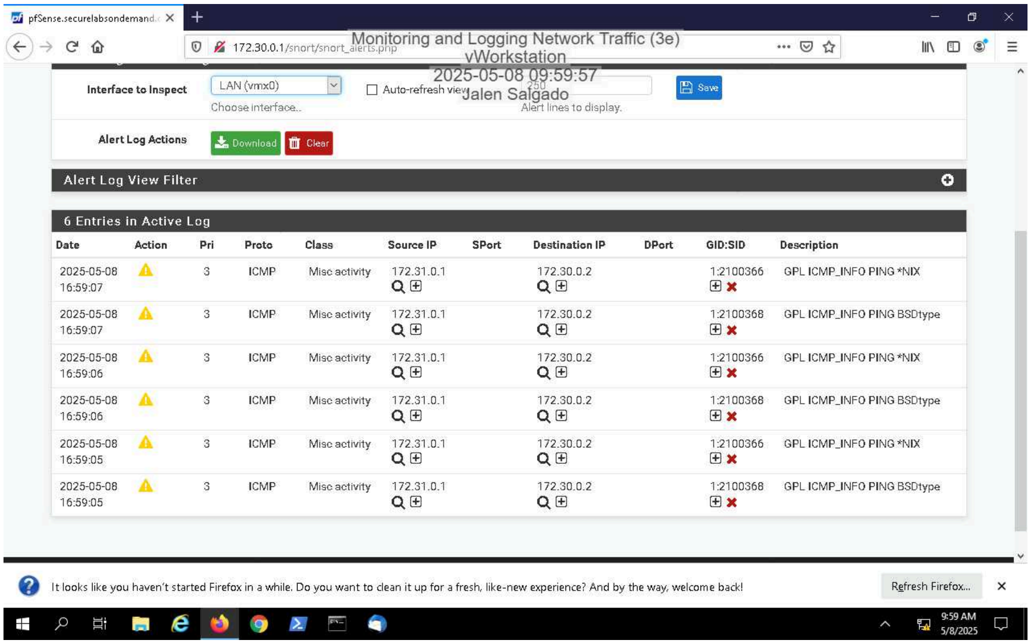
```
PING 172.30.0.2 (172.30.0.2) from 172.31.0.1: 56 data bytes
64 bytes from 172.30.0.2: icmp_seq=0 ttl=128 time=0.257 ms
64 bytes from 172.30.0.2: icmp_seq=1 ttl=128 time=0.542 ms
64 bytes from 172.30.0.2: icmp_seq=2 ttl=128 time=0.346 ms

--- 172.30.0.2 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.257/0.382/0.542/0.119 ms
```

pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 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
2025-05-08 09:59:57
Jalen Salgado

Interface to Inspect: LAN (vmx0) — Choose interface...
□ Auto-refresh view — 250 — Alert lines to display. — Save

Alert Log Actions: Download — Clear

Alert Log View Filter

6 Entries in Active Log

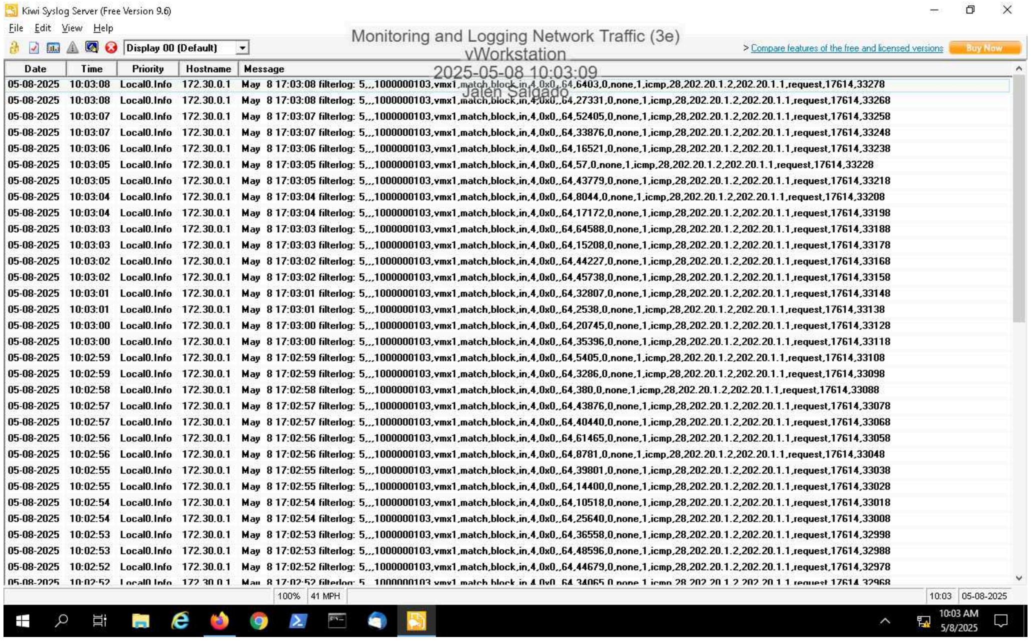
Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2025-05-08 16:59:07	⚠	3	ICMP	Misc activity	172.31.0.1		172.30.0.2		1:2100366	GPL ICMP_INFO PING *NIX
2025-05-08 16:59:07	⚠	3	ICMP	Misc activity	172.31.0.1		172.30.0.2		1:2100368	GPL ICMP_INFO PING BSDtype
2025-05-08 16:59:06	⚠	3	ICMP	Misc activity	172.31.0.1		172.30.0.2		1:2100366	GPL ICMP_INFO PING *NIX
2025-05-08 16:59:06	⚠	3	ICMP	Misc activity	172.31.0.1		172.30.0.2		1:2100368	GPL ICMP_INFO PING BSDtype
2025-05-08 16:59:05	⚠	3	ICMP	Misc activity	172.31.0.1		172.30.0.2		1:2100366	GPL ICMP_INFO PING *NIX
2025-05-08 16:59:05	⚠	3	ICMP	Misc activity	172.31.0.1		172.30.0.2		1:2100368	GPL ICMP_INFO PING BSDtype

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! — Refresh Firefox...

9:59 AM
5/8/2025

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**.


Kiwi Syslog Server (Free Version 9.6)
File
Edit
View
Help
Display 00 (Default)
> Compare features of the free and licensed versions
Buy Now

Monitoring and Logging Network Traffic (3e)
vWorkstation
2025-05-08 10:03:09
Jalen Salgado

```
Date        Time      Priority     Hostname     Message
05-08-2025  10:03:08  Local0.Info  172.30.0.1   May  8 17:03:08 filterlog: 5,,,1000000103,vmx1,match,block,in,4,0x0,,64,6403,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,17614,33278
05-08-2025  10:03:08  Local0.Info  172.30.0.1   May  8 17:03:08 filterlog: 5,,,1000000103,vmx1,match,block,in,4,0x0,,64,27331,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,17614,33268
05-08-2025  10:03:07  Local0.Info  172.30.0.1   May  8 17:03:07 filterlog: 5,,,1000000103,vmx1,match,block,in,4,0x0,,64,52405,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,17614,33258
05-08-2025  10:03:07  Local0.Info  172.30.0.1   May  8 17:03:07 filterlog: 5,,,1000000103,vmx1,match,block,in,4,0x0,,64,33876,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,17614,33248
05-08-2025  10:03:06  Local0.Info  172.30.0.1   May  8 17:03:06 filterlog: 5,,,1000000103,vmx1,match,block,in,4,0x0,,64,16521,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,17614,33238
05-08-2025  10:03:05  Local0.Info  172.30.0.1   May  8 17:03:05 filterlog: 5,,,1000000103,vmx1,match,block,in,4,0x0,,64,57,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,17614,33228
05-08-2025  10:03:05  Local0.Info  172.30.0.1   May  8 17:03:05 filterlog: 5,,,1000000103,vmx1,match,block,in,4,0x0,,64,43779,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,17614,33218
05-08-2025  10:03:04  Local0.Info  172.30.0.1   May  8 17:03:04 filterlog: 5,,,1000000103,vmx1,match,block,in,4,0x0,,64,8044,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,17614,33208
05-08-2025  10:03:04  Local0.Info  172.30.0.1   May  8 17:03:04 filterlog: 5,,,1000000103,vmx1,match,block,in,4,0x0,,64,17172,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,17614,33198
05-08-2025  10:03:03  Local0.Info  172.30.0.1   May  8 17:03:03 filterlog: 5,,,1000000103,vmx1,match,block,in,4,0x0,,64,64588,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,17614,33188
05-08-2025  10:03:03  Local0.Info  172.30.0.1   May  8 17:03:03 filterlog: 5,,,1000000103,vmx1,match,block,in,4,0x0,,64,15208,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,17614,33178
05-08-2025  10:03:02  Local0.Info  172.30.0.1   May  8 17:03:02 filterlog: 5,,,1000000103,vmx1,match,block,in,4,0x0,,64,44227,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,17614,33168
05-08-2025  10:03:02  Local0.Info  172.30.0.1   May  8 17:03:02 filterlog: 5,,,1000000103,vmx1,match,block,in,4,0x0,,64,45738,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,17614,33158
05-08-2025  10:03:01  Local0.Info  172.30.0.1   May  8 17:03:01 filterlog: 5,,,1000000103,vmx1,match,block,in,4,0x0,,64,32807,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,17614,33148
05-08-2025  10:03:01  Local0.Info  172.30.0.1   May  8 17:03:01 filterlog: 5,,,1000000103,vmx1,match,block,in,4,0x0,,64,2538,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,17614,33138
05-08-2025  10:03:00  Local0.Info  172.30.0.1   May  8 17:03:00 filterlog: 5,,,1000000103,vmx1,match,block,in,4,0x0,,64,20745,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,17614,33128
05-08-2025  10:03:00  Local0.Info  172.30.0.1   May  8 17:03:00 filterlog: 5,,,1000000103,vmx1,match,block,in,4,0x0,,64,35396,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,17614,33118
05-08-2025  10:02:59  Local0.Info  172.30.0.1   May  8 17:02:59 filterlog: 5,,,1000000103,vmx1,match,block,in,4,0x0,,64,5405,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,17614,33108
05-08-2025  10:02:59  Local0.Info  172.30.0.1   May  8 17:02:59 filterlog: 5,,,1000000103,vmx1,match,block,in,4,0x0,,64,3286,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,17614,33098
05-08-2025  10:02:58  Local0.Info  172.30.0.1   May  8 17:02:58 filterlog: 5,,,1000000103,vmx1,match,block,in,4,0x0,,64,380,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,17614,33088
05-08-2025  10:02:57  Local0.Info  172.30.0.1   May  8 17:02:57 filterlog: 5,,,1000000103,vmx1,match,block,in,4,0x0,,64,43876,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,17614,33078
05-08-2025  10:02:57  Local0.Info  172.30.0.1   May  8 17:02:57 filterlog: 5,,,1000000103,vmx1,match,block,in,4,0x0,,64,40440,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,17614,33068
05-08-2025  10:02:56  Local0.Info  172.30.0.1   May  8 17:02:56 filterlog: 5,,,1000000103,vmx1,match,block,in,4,0x0,,64,61465,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,17614,33058
05-08-2025  10:02:56  Local0.Info  172.30.0.1   May  8 17:02:56 filterlog: 5,,,1000000103,vmx1,match,block,in,4,0x0,,64,8781,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,17614,33048
05-08-2025  10:02:55  Local0.Info  172.30.0.1   May  8 17:02:55 filterlog: 5,,,1000000103,vmx1,match,block,in,4,0x0,,64,39801,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,17614,33038
05-08-2025  10:02:55  Local0.Info  172.30.0.1   May  8 17:02:55 filterlog: 5,,,1000000103,vmx1,match,block,in,4,0x0,,64,14400,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,17614,33028
05-08-2025  10:02:54  Local0.Info  172.30.0.1   May  8 17:02:54 filterlog: 5,,,1000000103,vmx1,match,block,in,4,0x0,,64,10518,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,17614,33018
05-08-2025  10:02:54  Local0.Info  172.30.0.1   May  8 17:02:54 filterlog: 5,,,1000000103,vmx1,match,block,in,4,0x0,,64,25640,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,17614,33008
05-08-2025  10:02:53  Local0.Info  172.30.0.1   May  8 17:02:53 filterlog: 5,,,1000000103,vmx1,match,block,in,4,0x0,,64,36558,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,17614,32998
05-08-2025  10:02:53  Local0.Info  172.30.0.1   May  8 17:02:53 filterlog: 5,,,1000000103,vmx1,match,block,in,4,0x0,,64,48596,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,17614,32988
05-08-2025  10:02:52  Local0.Info  172.30.0.1   May  8 17:02:52 filterlog: 5,,,1000000103,vmx1,match,block,in,4,0x0,,64,44679,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,17614,32978
05-08-2025  10:02:52  Local0.Info  172.30.0.1   May  8 17:02:52 filterlog: 5,,,1000000103,vmx1,match,block,in,4,0x0,,64,34065,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,17614,32968
```

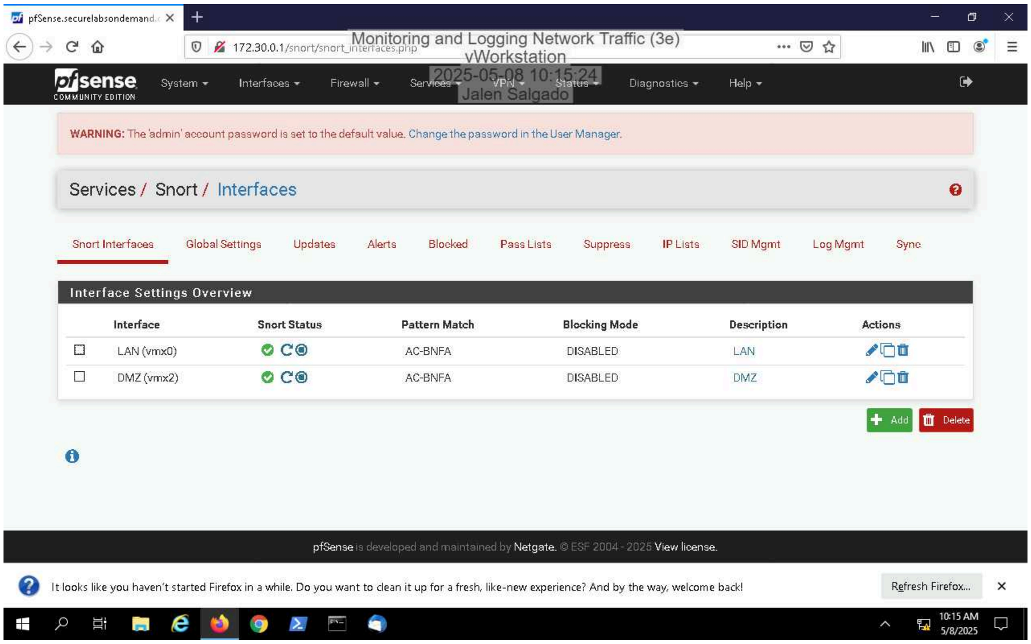
100% 41 MPH 10:03 05-08-2025

10:03 AM
5/8/2025

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
2025-05-08 10:15:24
Jalen Salgado

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

Services / Snort / Interfaces

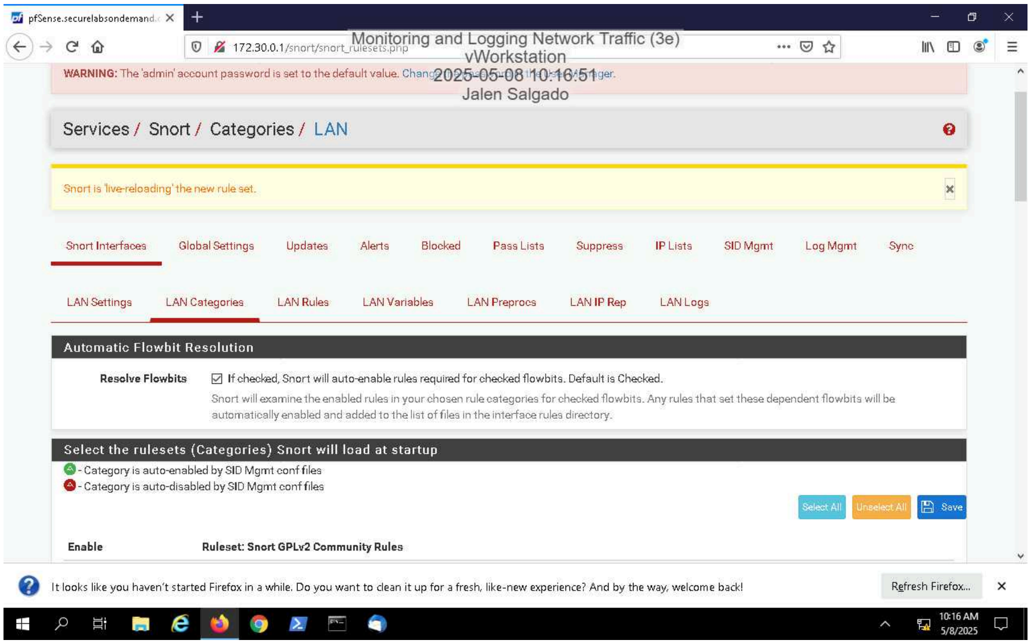
Interface Settings Overview

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

pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 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!

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



Monitoring and Logging Network Traffic (3e)
vWorkstation
2025-05-08 10:16:51
Jalen Salgado

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

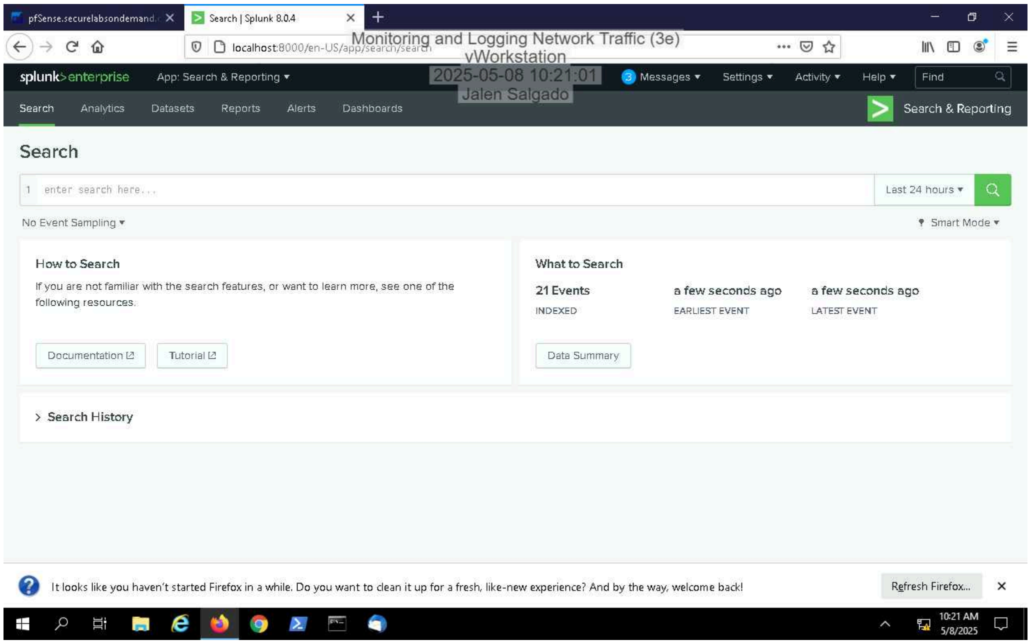
● - Category is auto-enabled by SID Mgmt conf files
● - Category is auto-disabled by SID Mgmt conf files

Enable **Ruleset: Snort GPLv2 Community Rules**

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
2025-05-08 10:21:01
Jalen Salgado

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

Search

How to Search

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

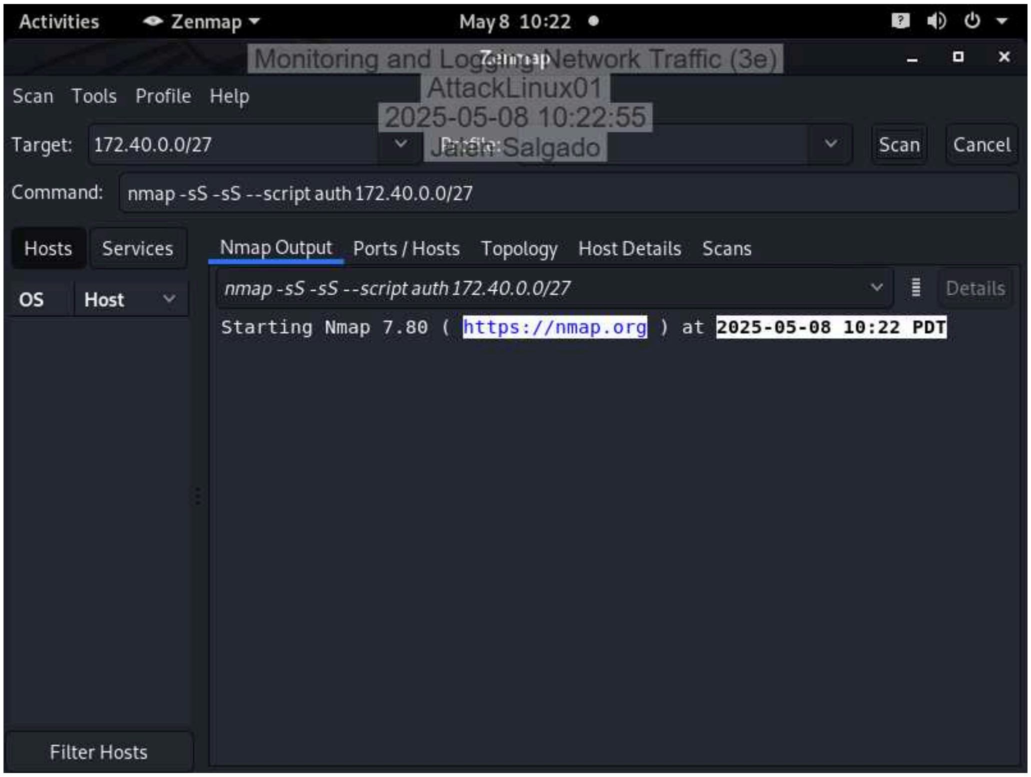
What to Search

21 Events	a few seconds 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**.



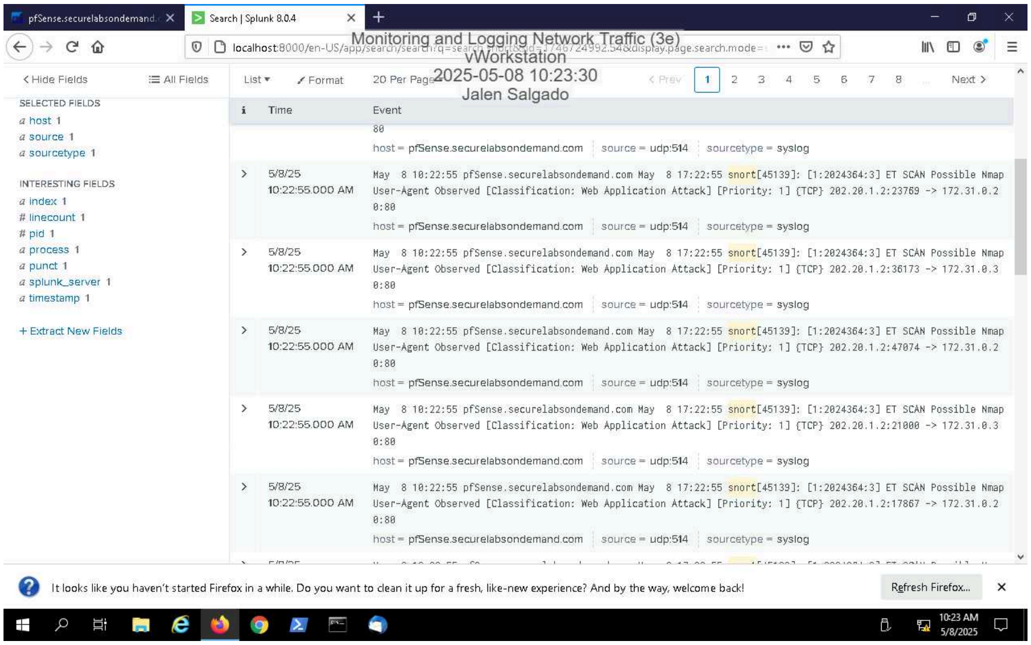
Target: 172.40.0.0/27

Profile:

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

```
nmap -sS -sS --script auth 172.40.0.0/27
Starting Nmap 7.80 ( https://nmap.org ) at 2025-05-08 10:22 PDT
```

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



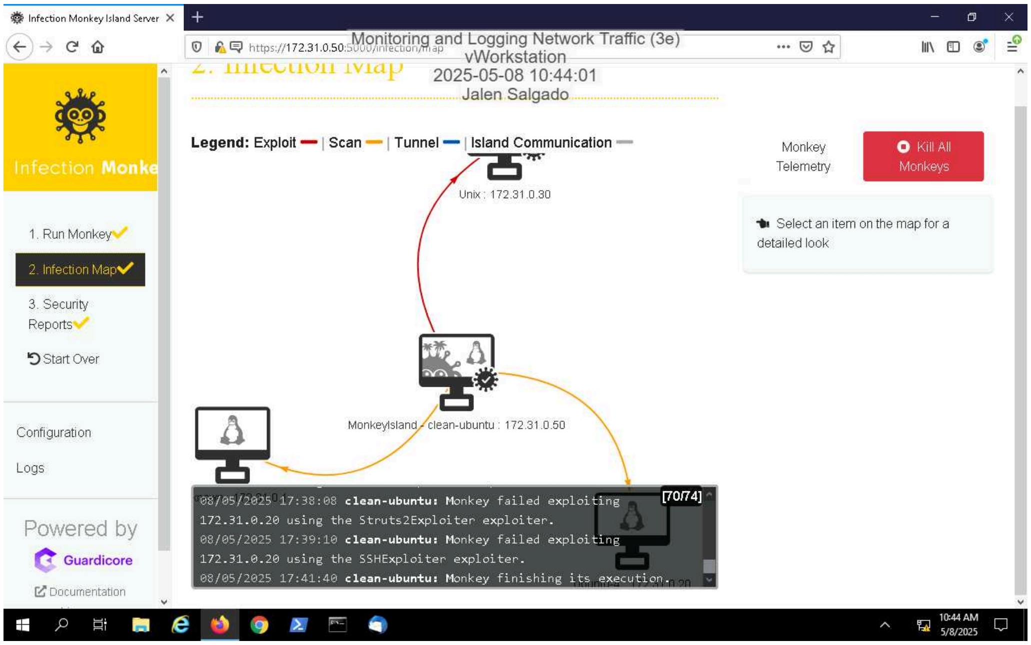
i	Time	Event
		80 host = pfSense.securelabsondemand.com source = udp:514 sourcetype = syslog
>	5/8/25 10:22:55.000 AM	May 8 10:22:55 pfSense.securelabsondemand.com May 8 17:22:55 snort[45139]: [1:2024364:3] ET SCAN Possible Nmap User-Agent Observed [Classification: Web Application Attack] [Priority: 1] {TCP} 202.20.1.2:23769 -> 172.31.0.2 0:80 host = pfSense.securelabsondemand.com source = udp:514 sourcetype = syslog
>	5/8/25 10:22:55.000 AM	May 8 10:22:55 pfSense.securelabsondemand.com May 8 17:22:55 snort[45139]: [1:2024364:3] ET SCAN Possible Nmap User-Agent Observed [Classification: Web Application Attack] [Priority: 1] {TCP} 202.20.1.2:36173 -> 172.31.0.3 0:80 host = pfSense.securelabsondemand.com source = udp:514 sourcetype = syslog
>	5/8/25 10:22:55.000 AM	May 8 10:22:55 pfSense.securelabsondemand.com May 8 17:22:55 snort[45139]: [1:2024364:3] ET SCAN Possible Nmap User-Agent Observed [Classification: Web Application Attack] [Priority: 1] {TCP} 202.20.1.2:47074 -> 172.31.0.2 0:80 host = pfSense.securelabsondemand.com source = udp:514 sourcetype = syslog
>	5/8/25 10:22:55.000 AM	May 8 10:22:55 pfSense.securelabsondemand.com May 8 17:22:55 snort[45139]: [1:2024364:3] ET SCAN Possible Nmap User-Agent Observed [Classification: Web Application Attack] [Priority: 1] {TCP} 202.20.1.2:21000 -> 172.31.0.3 0:80 host = pfSense.securelabsondemand.com source = udp:514 sourcetype = syslog
>	5/8/25 10:22:55.000 AM	May 8 10:22:55 pfSense.securelabsondemand.com May 8 17:22:55 snort[45139]: [1:2024364:3] ET SCAN Possible Nmap User-Agent Observed [Classification: Web Application Attack] [Priority: 1] {TCP} 202.20.1.2:17867 -> 172.31.0.2 0:80 host = pfSense.securelabsondemand.com source = udp:514 sourcetype = syslog

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

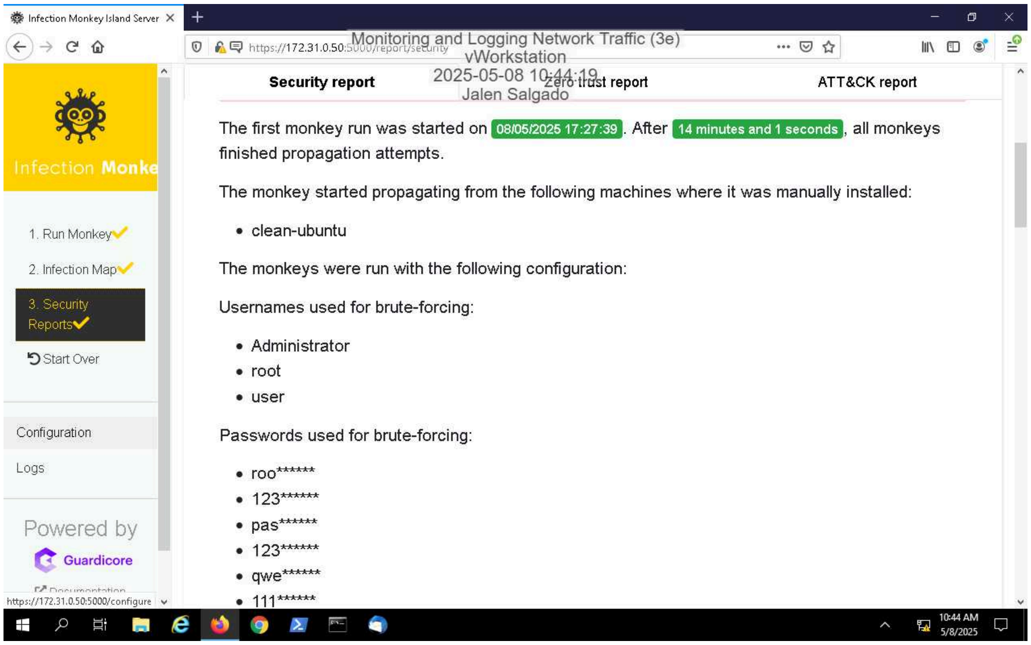
Make a screen capture showing the **resulting Infection Map**.



Monitoring and Logging Network Traffic (3e)
vWorkstation
2025-05-08 10:44:01
Jalen Salgado

```
08/05/2025 17:38:08 clean-ubuntu: Monkey failed exploiting
172.31.0.20 using the Struts2Exploiter exploiter.
08/05/2025 17:39:10 clean-ubuntu: Monkey failed exploiting
172.31.0.20 using the SSHExploiter exploiter.
08/05/2025 17:41:40 clean-ubuntu: Monkey finishing its execution.
```

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



Monitoring and Logging Network Traffic (3e)
vWorkstation
2025-05-08 10:44:19
Jalen Salgado

The first monkey run was started on 08/05/2025 17:27:39. After 14 minutes and 1 seconds, all monkeys finished propagation attempts.

The monkey started propagating from the following machines where it was manually installed:

- clean-ubuntu

The monkeys were run with the following configuration:

Usernames used for brute-forcing:

- Administrator
- root
- user

Passwords used for brute-forcing:

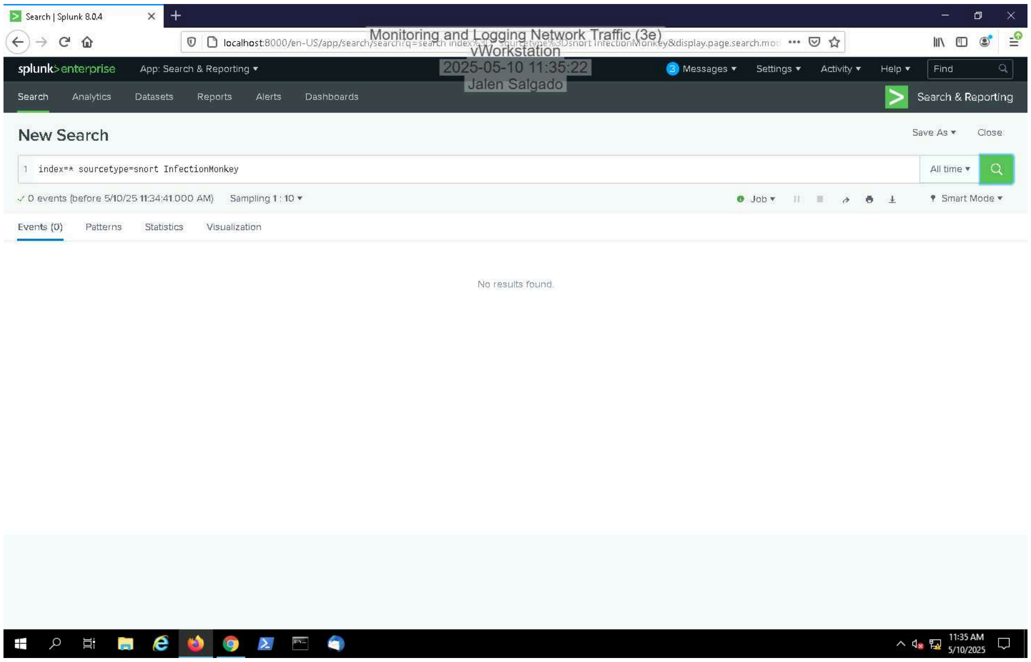
- roo******
- 123******
- pas******
- 123******
- qwe******
- 111******

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

alot of the vulnerabilites came from using the basic username and password settings also immediate threats were also from things that werent update properly

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
2025-05-10 11:35:22
Jalen Salgado

localhost:8000/en-US/app/search/search?q=search index%3D* sourcetype%3Dsnort InfectionMonkey&display.page.search.mod

New Search

```
index=* sourcetype=snort InfectionMonkey
```

✓ 0 events (before 5/10/25 11:34:41.000 AM) Sampling 1 : 10

No results found.

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?

The main concern is that no results were returned despite running a known attack simulation. This could be due to Snort not logging traffic correctly or Splunk not ingesting the logs. Even with logs present, many Snort alerts lack structured fields like destination IP, protocol, or severity level, which limits effective analysis. I would recommend including fields such as threat category, asset tags, and normalized timestamps to make the logs easier to parse and correlate during investigations

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?

During the Infection Monkey simulation, I attempted to retrieve related Snort alerts in Splunk. Despite correctly querying for events, no results were returned. This indicates either a lack of logging from Snort or an ingestion/configuration issue with Splunk. To improve detection, I recommend reviewing Snort’s output settings and ensuring Splunk is monitoring the correct log source. Additionally, enriching logs with structured fields like severity, IPs, and attack type would enhance detection accuracy. With the right configurations, Splunk can be a powerful tool for identifying and responding to simulated or real threats.