Student:	Email:
Nick Derleth	nderle02664@fontbonne.edu

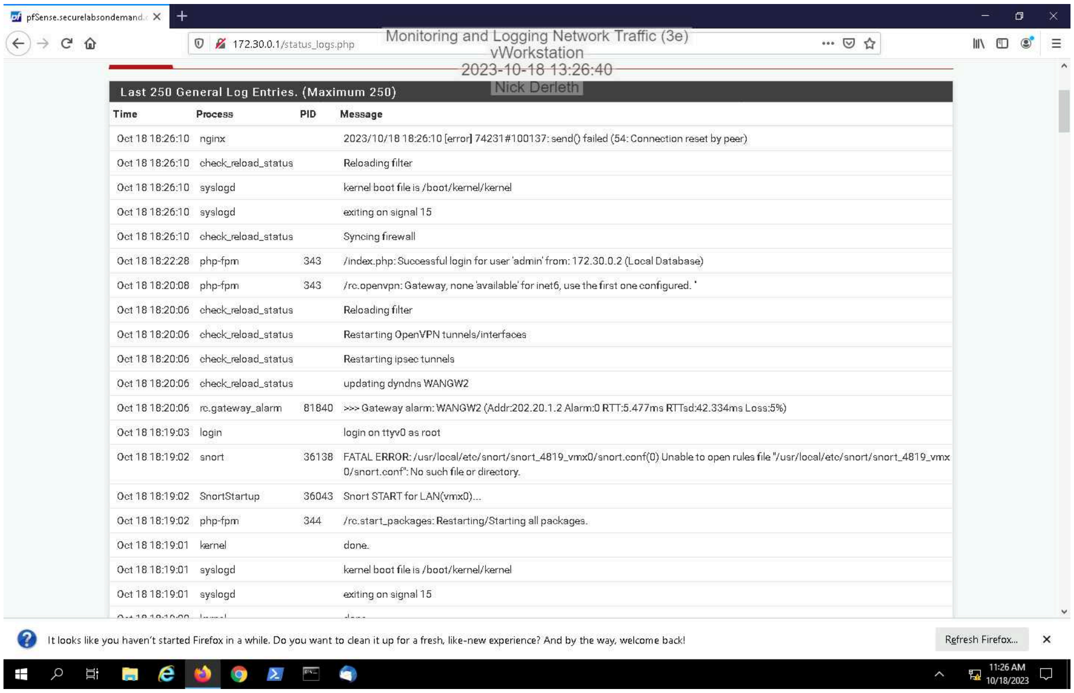
Time on Task:	Progress:
8 hours, 21 minutes	83%

Report Generated: Sunday, November 19, 2023 at 11:13 PM

Section 1: Hands-On Demonstration

Part 1: Configure the pfSense Firewall Log

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

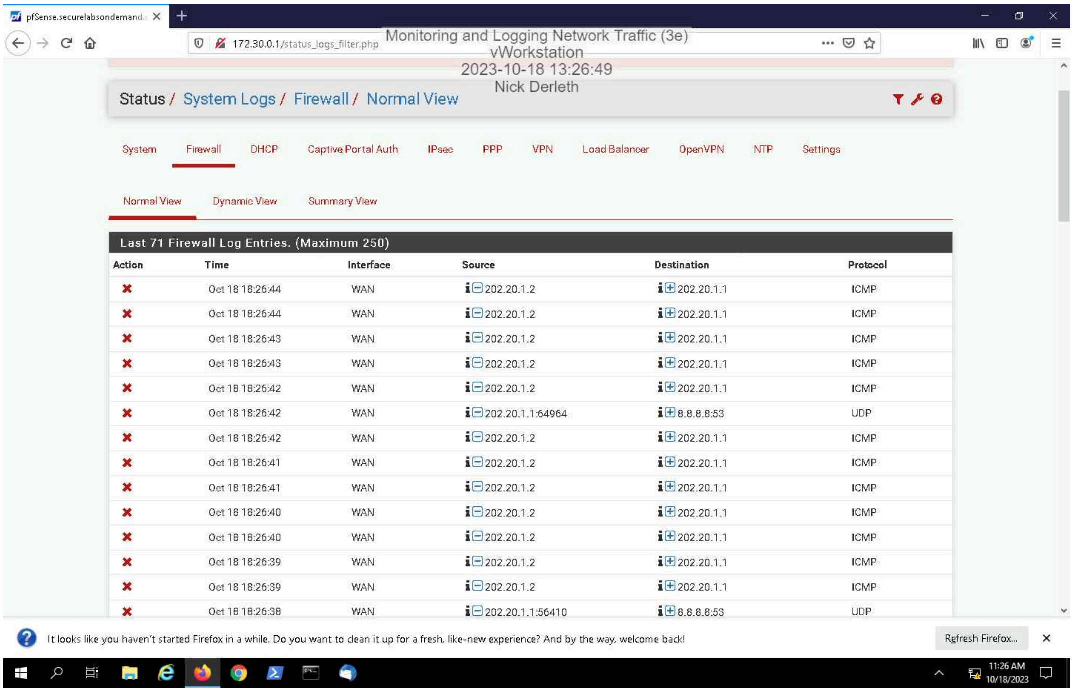

pfSense.securelabsondemand.
172.30.0.1/status_logs.php
Monitoring and Logging Network Traffic (3e)
vWorkstation
2023-10-18 13:26:40
Nick Derleth
Refresh Firefox...
11:26 AM
10/18/2023

Last 250 General Log Entries. (Maximum 250)

Time	Process	PID	Message
Oct 18 18:26:10	nginx		2023/10/18 18:26:10 [error] 74231#100137: send() failed (54: Connection reset by peer)
Oct 18 18:26:10	check_reload_status		Reloading filter
Oct 18 18:26:10	syslogd		kernel boot file is /boot/kernel/kernel
Oct 18 18:26:10	syslogd		exiting on signal 15
Oct 18 18:26:10	check_reload_status		Syncing firewall
Oct 18 18:22:28	php-fpm	343	/index.php: Successful login for user 'admin' from: 172.30.0.2 (Local Database)
Oct 18 18:20:08	php-fpm	343	/rc.openvpn: Gateway, none 'available' for inet6, use the first one configured. '
Oct 18 18:20:06	check_reload_status		Reloading filter
Oct 18 18:20:06	check_reload_status		Restarting OpenVPN tunnels/interfaces
Oct 18 18:20:06	check_reload_status		Restarting ipsec tunnels
Oct 18 18:20:06	check_reload_status		updating dyndns WANGW2
Oct 18 18:20:06	rc.gateway_alarm	81840	>>> Gateway alarm: WANGW2 (Addr:202.20.1.2 Alarm:0 RTT:5.477ms RTTsd:42.334ms Loss:5%)
Oct 18 18:19:03	login		login on ttyv0 as root
Oct 18 18:19:02	snort	36138	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.
Oct 18 18:19:02	SnortStartup	36043	Snort START for LAN(vmx0)...
Oct 18 18:19:02	php-fpm	344	/rc.start_packages: Restarting/Starting all packages.
Oct 18 18:19:01	kernel		done.
Oct 18 18:19:01	syslogd		kernel boot file is /boot/kernel/kernel
Oct 18 18:19:01	syslogd		exiting on signal 15

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**.



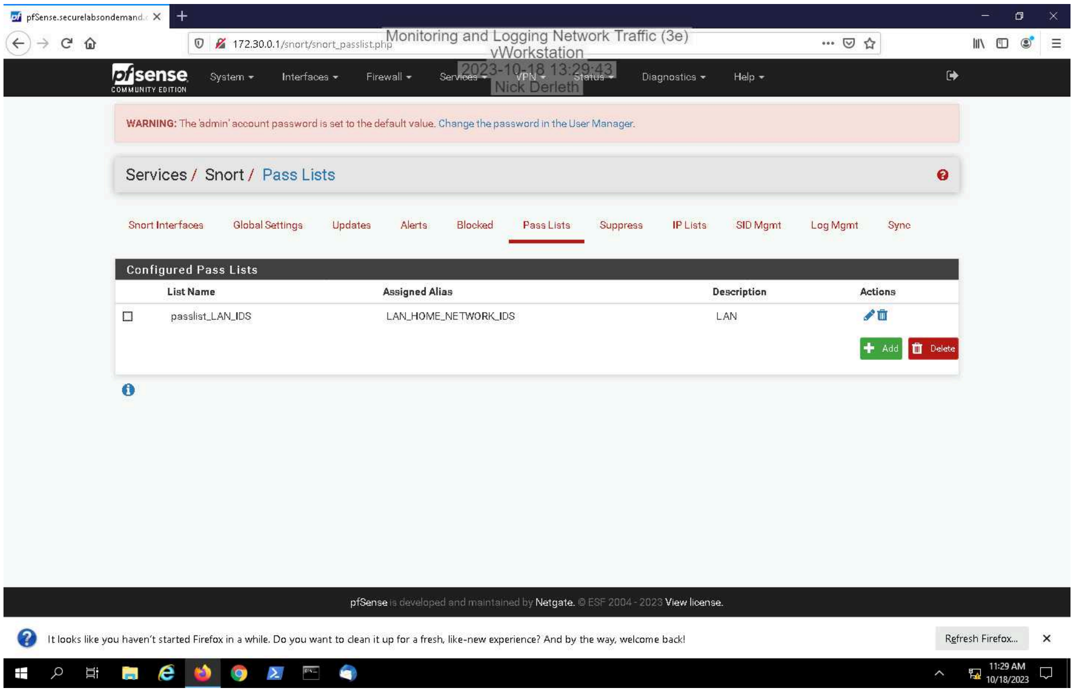
Last 71 Firewall Log Entries. (Maximum 250)

Action	Time	Interface	Source	Destination	Protocol
✖	Oct 18 18:26:44	WAN	202.20.1.2	202.20.1.1	ICMP
✖	Oct 18 18:26:44	WAN	202.20.1.2	202.20.1.1	ICMP
✖	Oct 18 18:26:43	WAN	202.20.1.2	202.20.1.1	ICMP
✖	Oct 18 18:26:43	WAN	202.20.1.2	202.20.1.1	ICMP
✖	Oct 18 18:26:42	WAN	202.20.1.2	202.20.1.1	ICMP
✖	Oct 18 18:26:42	WAN	202.20.1.1:64964	8.8.8.8:53	UDP
✖	Oct 18 18:26:42	WAN	202.20.1.2	202.20.1.1	ICMP
✖	Oct 18 18:26:41	WAN	202.20.1.2	202.20.1.1	ICMP
✖	Oct 18 18:26:41	WAN	202.20.1.2	202.20.1.1	ICMP
✖	Oct 18 18:26:40	WAN	202.20.1.2	202.20.1.1	ICMP
✖	Oct 18 18:26:40	WAN	202.20.1.2	202.20.1.1	ICMP
✖	Oct 18 18:26:39	WAN	202.20.1.2	202.20.1.1	ICMP
✖	Oct 18 18:26:39	WAN	202.20.1.2	202.20.1.1	ICMP
✖	Oct 18 18:26:38	WAN	202.20.1.1:56410	8.8.8.8:53	UDP

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
Monitoring and Logging Network Traffic (3e)
vWorkstation
2023-10-18 13:29:43
Nick Derleth
pfsense COMMUNITY EDITION
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.

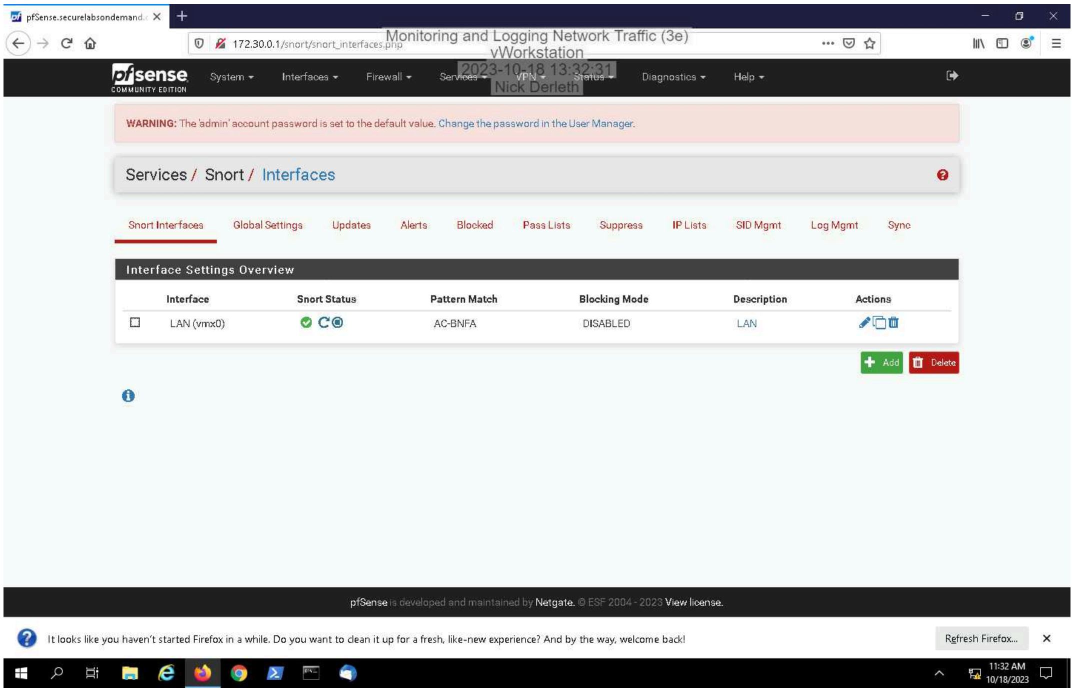
Configured Pass Lists

	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
2023-10-18 13:32:31
Nick Derleth

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

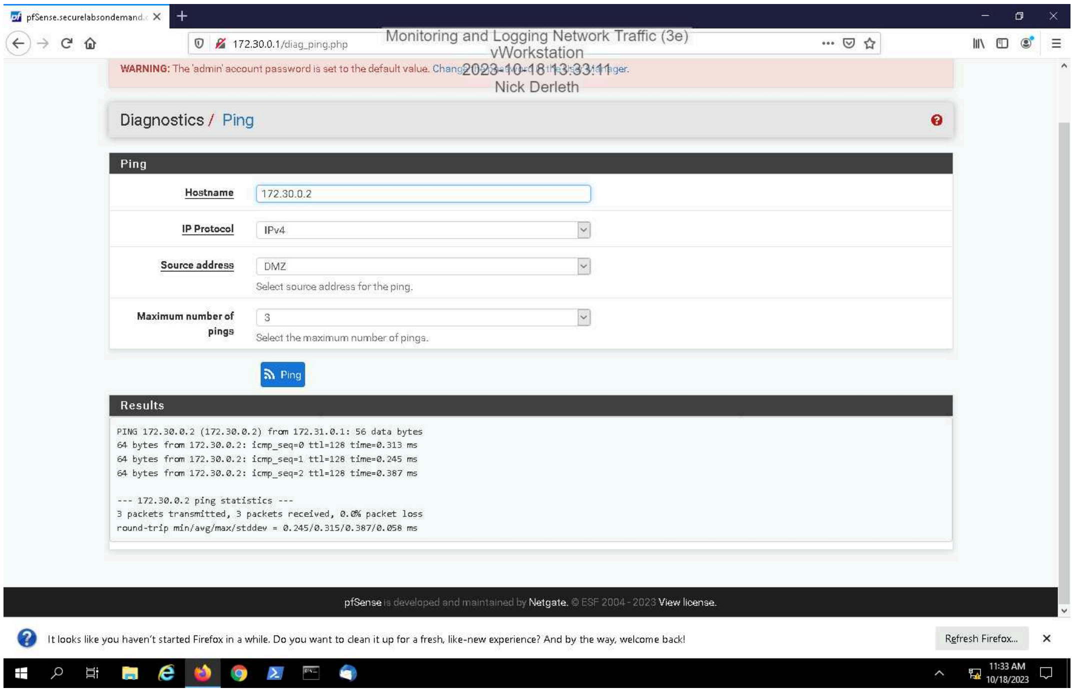
Interface Settings Overview

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

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
2023-10-18 13:33:11
Nick Derleth

172.30.0.1/diag_ping.php

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.

Results

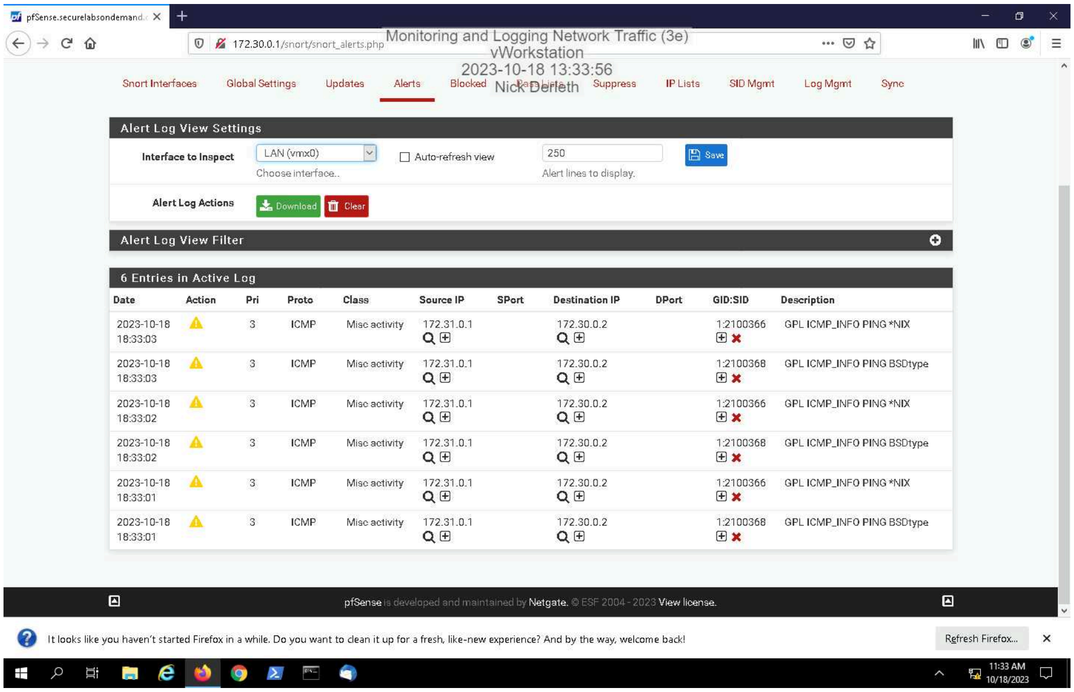
```
PING 172.30.0.2 (172.30.0.2) from 172.31.0.1: 56 data bytes
64 bytes from 172.30.0.2: icmp_seq=0 ttl=128 time=0.313 ms
64 bytes from 172.30.0.2: icmp_seq=1 ttl=128 time=0.245 ms
64 bytes from 172.30.0.2: icmp_seq=2 ttl=128 time=0.387 ms

--- 172.30.0.2 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.245/0.315/0.387/0.058 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**.



Monitoring and Logging Network Traffic (3e)
vWorkstation
2023-10-18 13:33:56
Nick Derleth

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

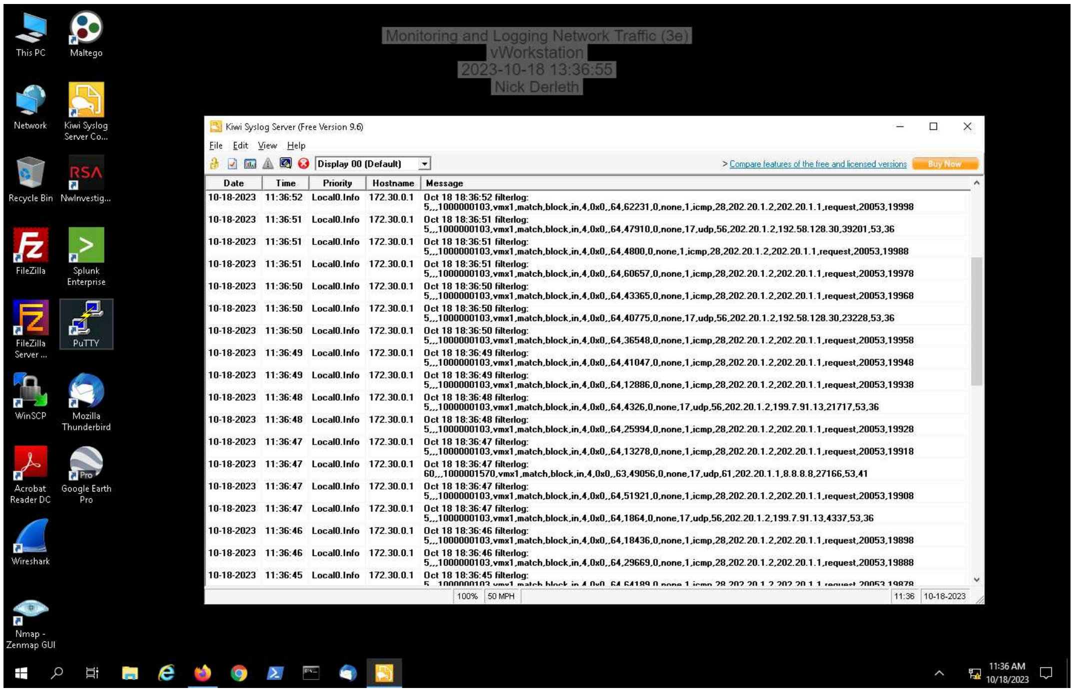
Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2023-10-18 18:33:03	⚠	3	ICMP	Misc activity	172.31.0.1		172.30.0.2		1:2100366	GPL ICMP_INFO PING *NIX
2023-10-18 18:33:03	⚠	3	ICMP	Misc activity	172.31.0.1		172.30.0.2		1:2100368	GPL ICMP_INFO PING BSDtype
2023-10-18 18:33:02	⚠	3	ICMP	Misc activity	172.31.0.1		172.30.0.2		1:2100366	GPL ICMP_INFO PING *NIX
2023-10-18 18:33:02	⚠	3	ICMP	Misc activity	172.31.0.1		172.30.0.2		1:2100368	GPL ICMP_INFO PING BSDtype
2023-10-18 18:33:01	⚠	3	ICMP	Misc activity	172.31.0.1		172.30.0.2		1:2100366	GPL ICMP_INFO PING *NIX
2023-10-18 18:33:01	⚠	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**.



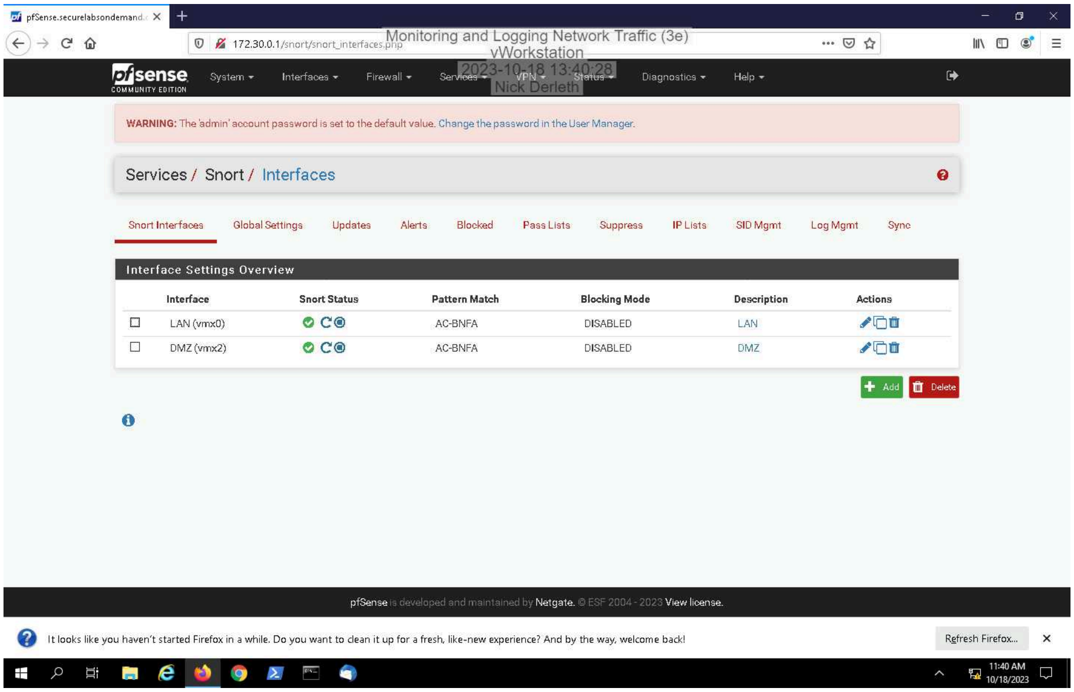
Monitoring and Logging Network Traffic (3e)
vWorkstation
2023-10-18 13:36:55
Nick Derleth

```
Date        Time      Priority     Hostname     Message
10-18-2023  11:36:52  Local0.Info  172.30.0.1   Oct 18 18:36:52 filterlog:
                                                5,,,1000000103,vmx1,match,block,in,4,0x0,,64,62231,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,20053,19998
10-18-2023  11:36:51  Local0.Info  172.30.0.1   Oct 18 18:36:51 filterlog:
                                                5,,,1000000103,vmx1,match,block,in,4,0x0,,64,47910,0,none,17,udp,56,202.20.1.2,192.58.128.30,39201,53,36
10-18-2023  11:36:51  Local0.Info  172.30.0.1   Oct 18 18:36:51 filterlog:
                                                5,,,1000000103,vmx1,match,block,in,4,0x0,,64,4800,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,20053,19988
10-18-2023  11:36:51  Local0.Info  172.30.0.1   Oct 18 18:36:51 filterlog:
                                                5,,,1000000103,vmx1,match,block,in,4,0x0,,64,60657,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,20053,19978
10-18-2023  11:36:50  Local0.Info  172.30.0.1   Oct 18 18:36:50 filterlog:
                                                5,,,1000000103,vmx1,match,block,in,4,0x0,,64,43365,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,20053,19968
10-18-2023  11:36:50  Local0.Info  172.30.0.1   Oct 18 18:36:50 filterlog:
                                                5,,,1000000103,vmx1,match,block,in,4,0x0,,64,40775,0,none,17,udp,56,202.20.1.2,192.58.128.30,23228,53,36
10-18-2023  11:36:50  Local0.Info  172.30.0.1   Oct 18 18:36:50 filterlog:
                                                5,,,1000000103,vmx1,match,block,in,4,0x0,,64,36548,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,20053,19958
10-18-2023  11:36:49  Local0.Info  172.30.0.1   Oct 18 18:36:49 filterlog:
                                                5,,,1000000103,vmx1,match,block,in,4,0x0,,64,41047,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,20053,19948
10-18-2023  11:36:49  Local0.Info  172.30.0.1   Oct 18 18:36:49 filterlog:
                                                5,,,1000000103,vmx1,match,block,in,4,0x0,,64,12886,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,20053,19938
10-18-2023  11:36:48  Local0.Info  172.30.0.1   Oct 18 18:36:48 filterlog:
                                                5,,,1000000103,vmx1,match,block,in,4,0x0,,64,4326,0,none,17,udp,56,202.20.1.2,199.7.91.13,21717,53,36
10-18-2023  11:36:48  Local0.Info  172.30.0.1   Oct 18 18:36:48 filterlog:
                                                5,,,1000000103,vmx1,match,block,in,4,0x0,,64,25994,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,20053,19928
10-18-2023  11:36:47  Local0.Info  172.30.0.1   Oct 18 18:36:47 filterlog:
                                                5,,,1000000103,vmx1,match,block,in,4,0x0,,64,13278,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,20053,19918
10-18-2023  11:36:47  Local0.Info  172.30.0.1   Oct 18 18:36:47 filterlog:
                                                60,,,1000001570,vmx1,match,block,in,4,0x0,,63,49056,0,none,17,udp,61,202.20.1.1,8.8.8.8,27166,53,41
10-18-2023  11:36:47  Local0.Info  172.30.0.1   Oct 18 18:36:47 filterlog:
                                                5,,,1000000103,vmx1,match,block,in,4,0x0,,64,51921,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,20053,19908
10-18-2023  11:36:47  Local0.Info  172.30.0.1   Oct 18 18:36:47 filterlog:
                                                5,,,1000000103,vmx1,match,block,in,4,0x0,,64,1864,0,none,17,udp,56,202.20.1.2,199.7.91.13,4337,53,36
10-18-2023  11:36:46  Local0.Info  172.30.0.1   Oct 18 18:36:46 filterlog:
                                                5,,,1000000103,vmx1,match,block,in,4,0x0,,64,18436,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,20053,19898
10-18-2023  11:36:46  Local0.Info  172.30.0.1   Oct 18 18:36:46 filterlog:
                                                5,,,1000000103,vmx1,match,block,in,4,0x0,,64,29669,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,20053,19888
10-18-2023  11:36:45  Local0.Info  172.30.0.1   Oct 18 18:36:45 filterlog:
                                                5,,,1000000103,vmx1,match,block,in,4,0x0,,64,64189,0,none,1,icmp,28,202.20.1.2,202.20.1.1,request,20053,19878
```

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
2023-10-18 13:40:28
Nick Derleth

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

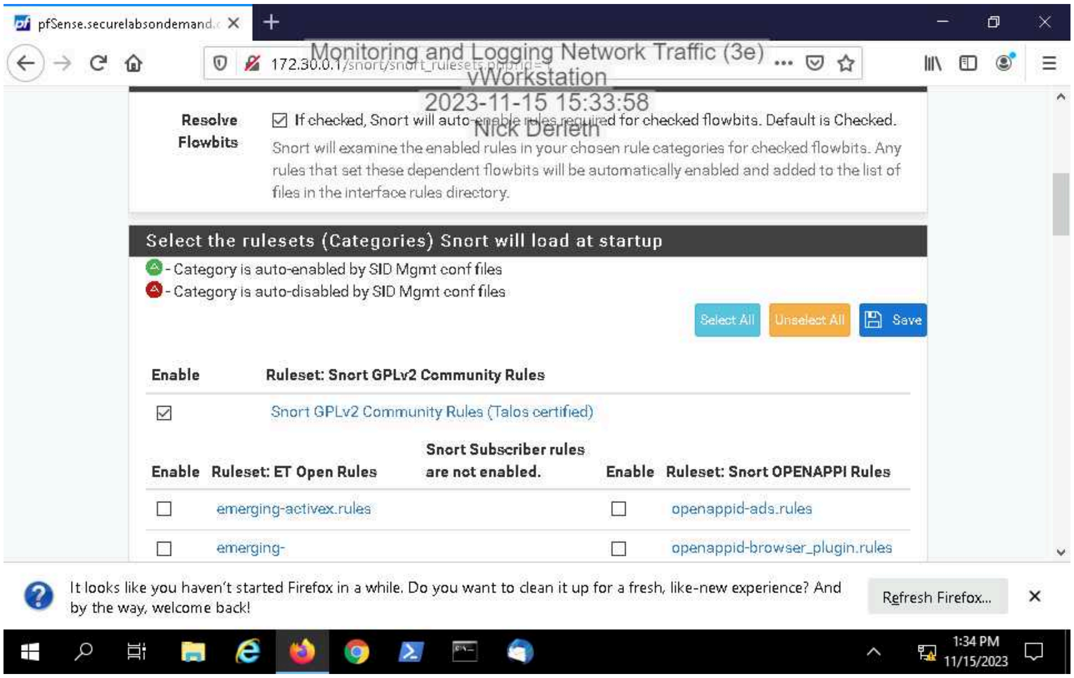
Interface Settings Overview

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

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!

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



Monitoring and Logging Network Traffic (3e)
vWorkstation
2023-11-15 15:33:58
Nick Derleth

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)

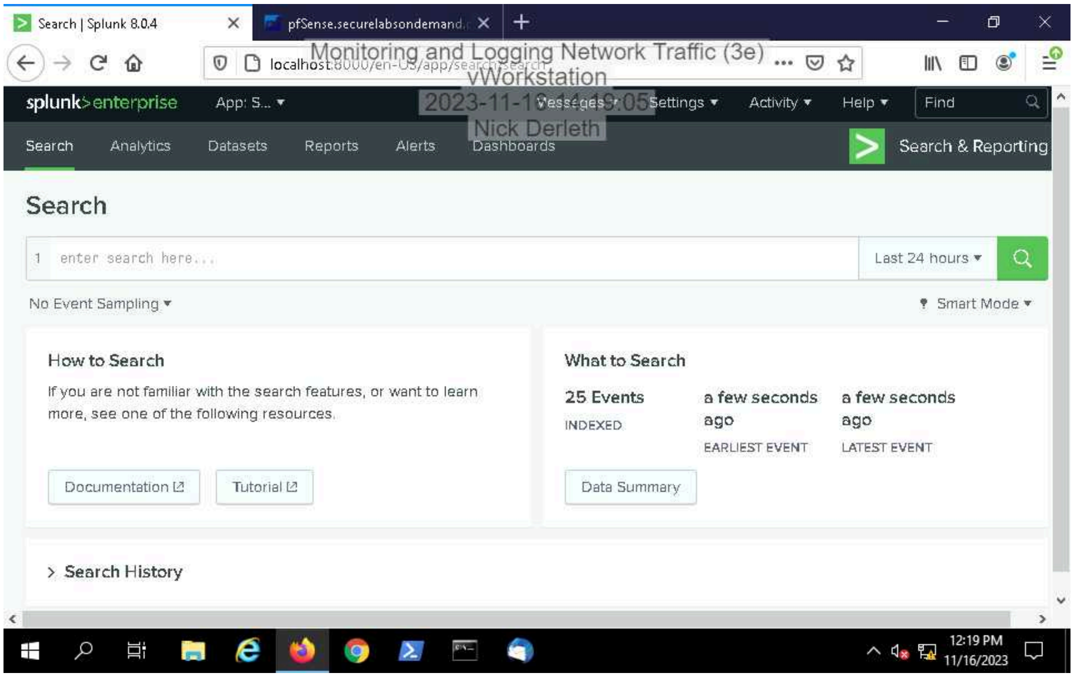
Enable	Ruleset: ET Open Rules	Snort Subscriber rules are not enabled.	Enable	Ruleset: Snort OPENAPPI Rules
☐	emerging-activex.rules		☐	openappid-ads.rules
☐	emerging-		☐	openappid-browser_plugin.rules

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!

pfSense.securelabsondemand.
172.30.0.1/snort/snort_rulesets.php?id=
Select All
Unselect All
Save
Refresh Firefox...
1:34 PM
11/15/2023

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
2023-11-16 14:19:05
Nick Derleth

Search

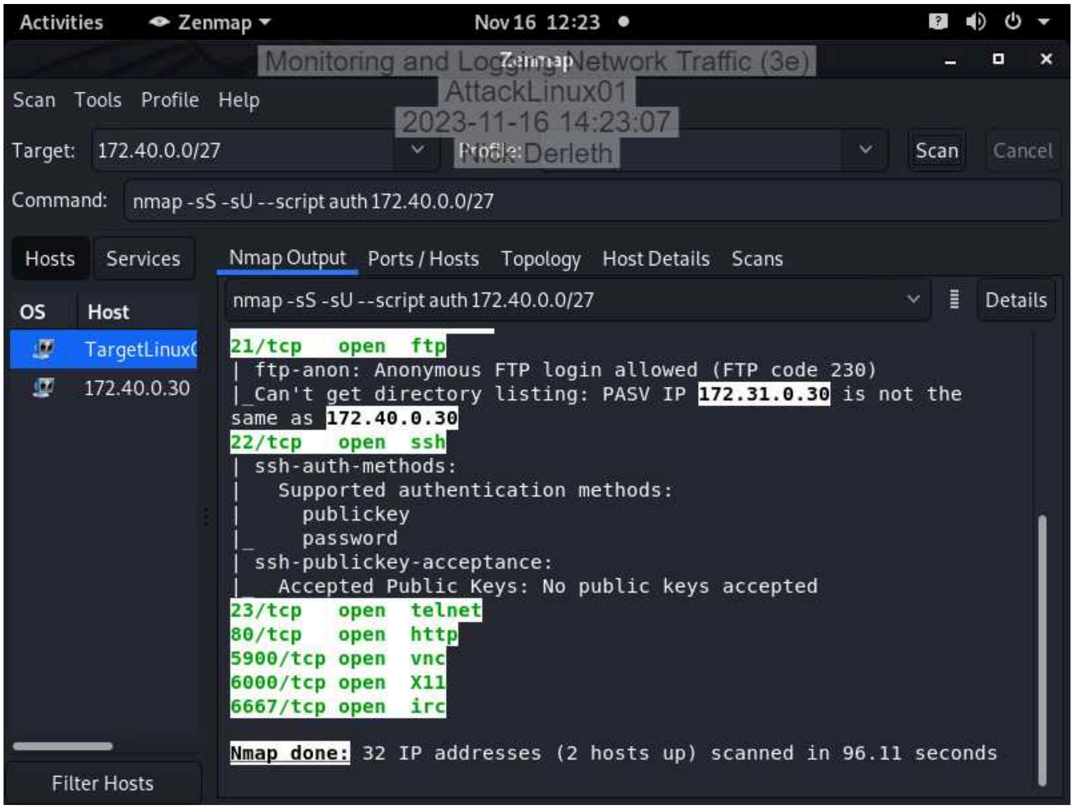
How to Search
If you are not familiar with the search features, or want to learn more, see one of the following resources.

What to Search

25 Events	a few seconds ago	a few seconds ago
INDEXED	EARLIEST EVENT	LATEST EVENT

Part 3: Simulate and Detect a Perimeter Network Attack

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



Monitoring and Logging Network Traffic (3e)
AttackLinux01
2023-11-16 14:23:07
Nick Derleth

Target: 172.40.0.0/27

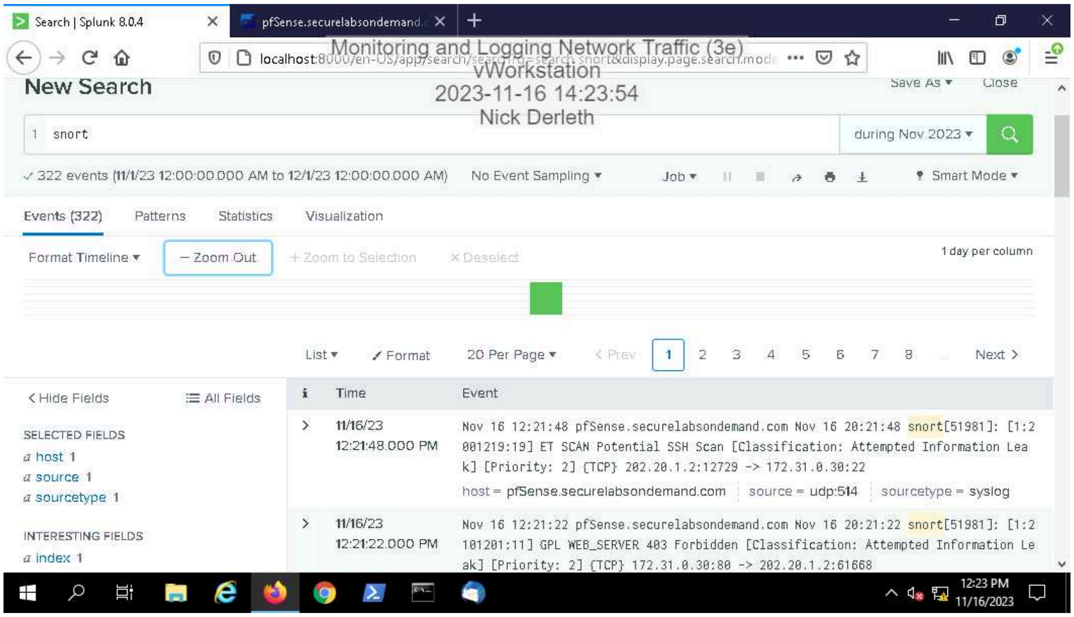
Command: nmap -sS -sU --script auth 172.40.0.0/27

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

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 96.11 seconds
```

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



Monitoring and Logging Network Traffic (3e)
vWorkstation
2023-11-16 14:23:54
Nick Derleth

New Search

1 snort — during Nov 2023 ▾

✓ 322 events (11/1/23 12:00:00.000 AM to 12/1/23 12:00:00.000 AM) No Event Sampling ▾

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

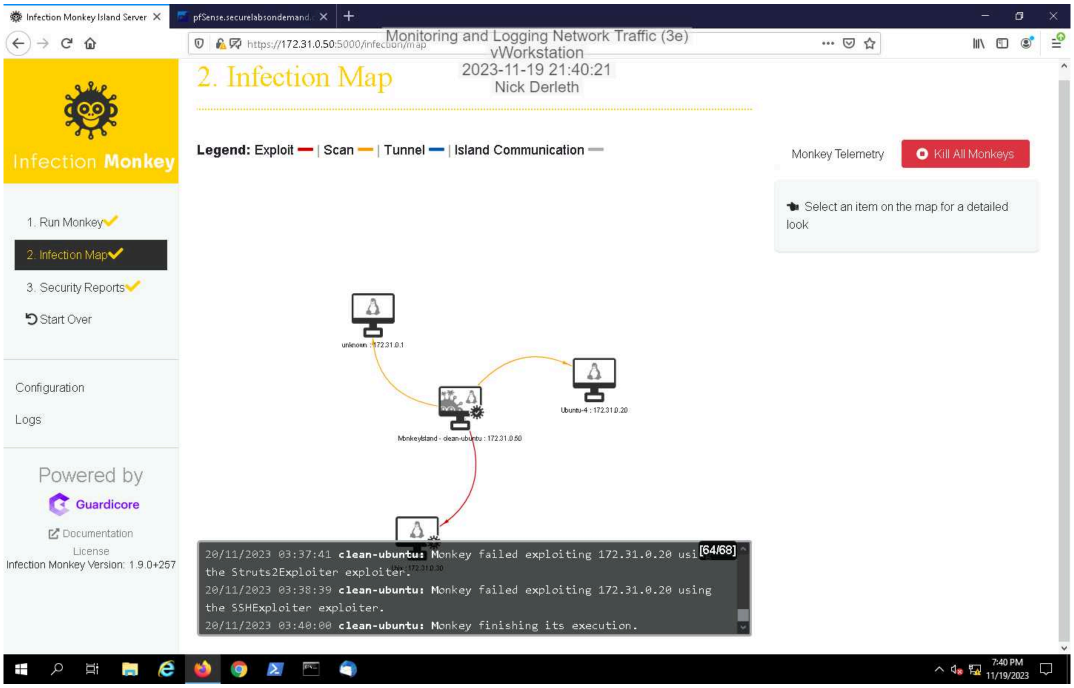
INTERESTING FIELDS
a index 1

i	Time	Event
›	11/16/23 12:21:48.000 PM	Nov 16 12:21:48 pfSense.securelabsondemand.com Nov 16 20:21:48 snort[51981]: [1:2001219:19] ET SCAN Potential SSH Scan [Classification: Attempted Information Leak] [Priority: 2] {TCP} 202.20.1.2:12729 -> 172.31.0.30:22 host = pfSense.securelabsondemand.com source = udp:514 sourcetype = syslog
›	11/16/23 12:21:22.000 PM	Nov 16 12:21:22 pfSense.securelabsondemand.com Nov 16 20:21:22 snort[51981]: [1:2101201:11] GPL WEB_SERVER 403 Forbidden [Classification: Attempted Information Leak] [Priority: 2] {TCP} 172.31.0.30:80 -> 202.20.1.2:61668

Section 3: Challenge and Analysis

Part 1: Simulate a DMZ Breach with Infection Monkey

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

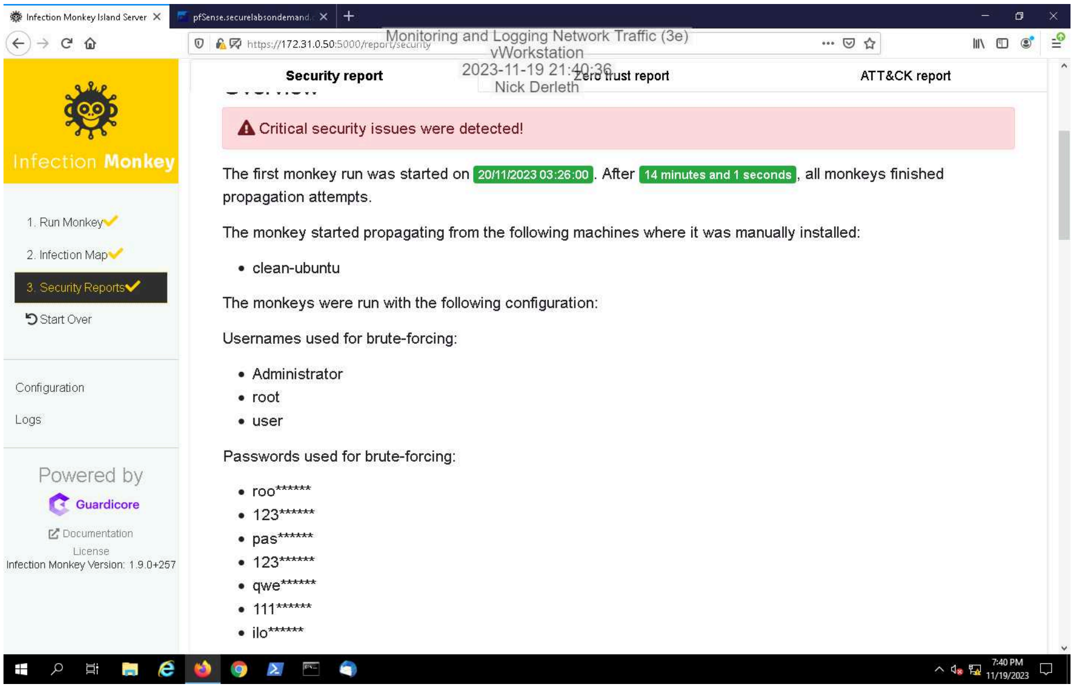


Monitoring and Logging Network Traffic (3e)
vWorkstation
2023-11-19 21:40:21
Nick Derleth

Select an item on the map for a detailed look

```
20/11/2023 03:37:41 clean-ubuntu: Monkey failed exploiting 172.31.0.20 usi
the Struts2Exploiter exploiter.
20/11/2023 03:38:39 clean-ubuntu: Monkey failed exploiting 172.31.0.20 using
the SSHExploiter exploiter.
20/11/2023 03:40:00 clean-ubuntu: Monkey finishing its execution.
```

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



Monitoring and Logging Network Traffic (3e)
vWorkstation
2023-11-19 21:40:36
Nick Derleth

⚠ Critical security issues were detected!

The first monkey run was started on 20/11/2023 03:26:00. 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******
- ilo******

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

The most common and likely exploitable vulnerabilities are the weak usernames and passwords as well as failing to update vital software.

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**.

Incomplete

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?

Incomplete

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?

Incomplete