

# Monitoring and Logging Network Traffic (3e)

Network Security, Firewalls, and VPNs, Third Edition - Lab 06

Student:

Vidhi Kadakia

Email:

jinsukrishna108@gmail.com

Time on Task:

3 hours, 30 minutes

Progress:

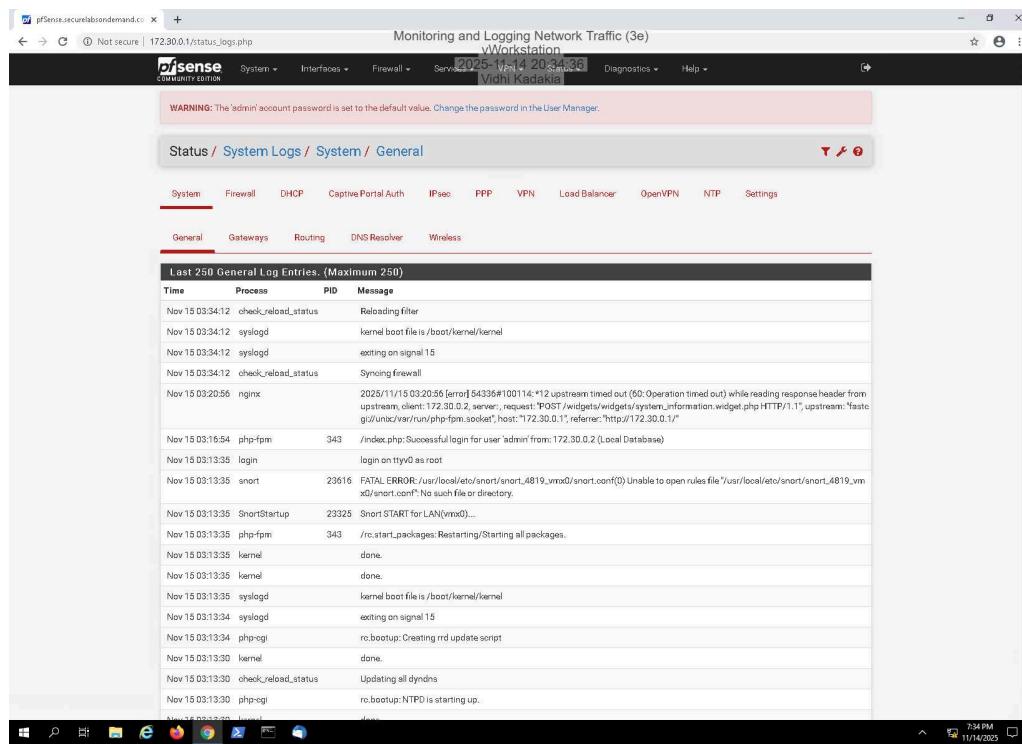
100%

Report Generated: Saturday, November 15, 2025 at 4:41 PM

## Section 1: Hands-On Demonstration

### Part 1: Configure the pfSense Firewall Log

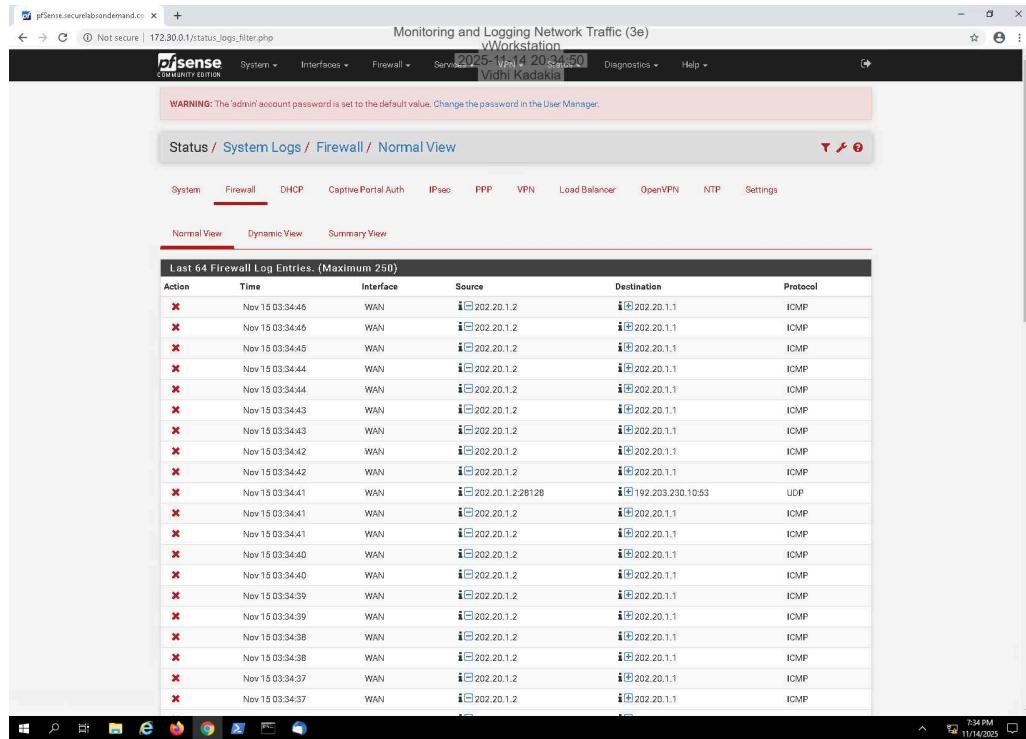
13. Make a screen capture showing the system logs.



The screenshot shows the pfSense web interface with the URL `172.30.0.1/status_logs.php`. The title bar indicates the session is for 'Vidhi Kadakia'. The main navigation menu includes 'Monitoring and Logging Network Traffic (3e)', 'Workstation', 'System', 'Interfaces', 'Firewall', 'Services', 'Status', 'Diagnostics', and 'Help'. The current page is 'Status / System Logs / System / General'. The sub-navigation menu shows tabs for 'General', 'Gateways', 'Routing', 'DNS Resolver', and 'Wireless', with 'General' being the active tab. A red warning message at the top states: 'WARNING: The "admin" account password is set to the default value. Change the password in the User Manager.' Below this, a table titled 'Last 250 General Log Entries. (Maximum 250)' displays log entries. The columns are 'Time', 'Process', 'PID', and 'Message'. The log entries show various system processes like cron, sshd, and snort starting up and performing tasks such as reloading configuration files and updating daemons. The log ends with a note about NTPD starting up.

Time	Process	PID	Message
Nov 15 03:34:12	check_reload_status		Reloading filter
Nov 15 03:34:12	syslogd		kernel boot file is /boot/kernel/kernel
Nov 15 03:34:12	syslogd		exiting on signal 15
Nov 15 03:34:12	check_reload_status		Synching Firewall
Nov 15 03:20:56	nginx		2025/11/15 03:20:56 [error] 54336#100114*:12 upstream timed out (60: Operation timed out) while reading response header from upstream, client: 172.30.0.2, server: , request: "POST /widgets/widgets/system_information.widget.php HTTP/1.1", upstream: "fastcgi://172.30.0.1/vmrun/php-fpm.sock", host: "172.30.0.1", referer: "http://172.30.0.1/"
Nov 15 03:16:54	php-fpm	343	/index.php: Successful login for user 'admin' from: 172.30.0.2 (Local Database)
Nov 15 03:13:35	login		login on ttv0 as root
Nov 15 03:13:35	snort	23616	FATAL ERROR: /usr/local/etc/snort_4819_vms0/snort.conf(0) Unable to open rules file '/usr/local/etc/snort_4819_vms0/snort.conf': No such file or directory.
Nov 15 03:13:35	SnortStartup	23328	Snort START for LAN(vms0)...
Nov 15 03:13:35	php-fpm	343	/etc/init.d/snort start: Starting/Starting all packages.
Nov 15 03:13:35	kernel		done.
Nov 15 03:13:35	kernel		done.
Nov 15 03:13:35	syslogd		kernel boot file is /boot/kernel/kernel
Nov 15 03:13:35	syslogd		exiting on signal 15
Nov 15 03:13:34	php-fcgi		re.bootup: Creating rrd update script
Nov 15 03:13:30	kernel		done.
Nov 15 03:13:30	check_reload_status		Updating all dyndns
Nov 15 03:13:30	php-fcgi		re.bootup: NTPD is starting up.

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



The screenshot shows the pfSense firewall log interface. At the top, there's a warning message: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, the navigation bar includes tabs for Status, System Logs, Firewall, Normal View, Dynamic View, and Summary View. The Firewall tab is selected. The main content area displays a table titled "Last 64 Firewall Log Entries. (Maximum 250)". The table has columns for Action, Time, Interface, Source, Destination, and Protocol. All entries show ICMP traffic between the WAN interface and various internal IP addresses (202.20.1.1 to 202.20.1.12) over ICMP protocol. The log entries are timestamped from Nov 15 03:34:45 to Nov 15 03:34:37.

Action	Time	Interface	Source	Destination	Protocol
×	Nov 15 03:34:45	WAN	202.20.1.2	202.20.1.1	ICMP
×	Nov 15 03:34:45	WAN	202.20.1.2	202.20.1.1	ICMP
×	Nov 15 03:34:45	WAN	202.20.1.2	202.20.1.1	ICMP
×	Nov 15 03:34:44	WAN	202.20.1.2	202.20.1.1	ICMP
×	Nov 15 03:34:44	WAN	202.20.1.2	202.20.1.1	ICMP
×	Nov 15 03:34:43	WAN	202.20.1.2	202.20.1.1	ICMP
×	Nov 15 03:34:43	WAN	202.20.1.2	202.20.1.1	ICMP
×	Nov 15 03:34:42	WAN	202.20.1.2	202.20.1.1	ICMP
×	Nov 15 03:34:42	WAN	202.20.1.2	202.20.1.1	ICMP
×	Nov 15 03:34:41	WAN	202.20.1.2	192.203.230.10:53	UDP
×	Nov 15 03:34:41	WAN	202.20.1.2	202.20.1.1	ICMP
×	Nov 15 03:34:41	WAN	202.20.1.2	202.20.1.1	ICMP
×	Nov 15 03:34:40	WAN	202.20.1.2	202.20.1.1	ICMP
×	Nov 15 03:34:40	WAN	202.20.1.2	202.20.1.1	ICMP
×	Nov 15 03:34:39	WAN	202.20.1.2	202.20.1.1	ICMP
×	Nov 15 03:34:39	WAN	202.20.1.2	202.20.1.1	ICMP
×	Nov 15 03:34:38	WAN	202.20.1.2	202.20.1.1	ICMP
×	Nov 15 03:34:38	WAN	202.20.1.2	202.20.1.1	ICMP
×	Nov 15 03:34:37	WAN	202.20.1.2	202.20.1.1	ICMP
×	Nov 15 03:34:37	WAN	202.20.1.2	202.20.1.1	ICMP

## Part 2: Configure a Snort Intrusion Detection System

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

The screenshot shows the pfSense web interface for managing Snort Pass Lists. The title bar indicates the URL is 172.30.0.1/snort/snort\_passlist.php and the page title is "Monitoring and Logging Network Traffic (3e) vWorkstation". The top navigation bar includes links for System, Interfaces, Firewall, Services, Diagnostics, and Help. A user message at the top states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, the breadcrumb navigation shows "Services / Snort / Pass Lists". The main content area displays a table titled "Configured Pass Lists" with one row:

List Name	Assigned Alias	Description	Actions
passlist_LAN_IDS	LAN_HOME_NETWORKIDS	LAN	

At the bottom right of the interface, there are standard pfSense navigation icons: a magnifying glass, a gear, a network icon, and a power icon. The status bar at the bottom right shows the date and time: 7:42 PM, 11/14/2025.

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

The screenshot shows the pfSense web interface for managing Snort interfaces. The title bar indicates the URL is 172.30.0.1/snort/snort\_interfaces.php and the page title is "Monitoring and Logging Network Traffic (3e) vWorkstation". The top navigation bar includes links for System, Interfaces, Firewall, Services, Diagnostics, and Help. A user message at the top states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, the breadcrumb navigation shows "Services / Snort / Interfaces". The main content area displays a table titled "Interface Settings Overview" with one row:

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

At the bottom right of the interface, there are standard pfSense navigation icons: a magnifying glass, a gear, a network icon, and a power icon. The status bar at the bottom right shows the date and time: 7:44 PM, 11/14/2025.

# Monitoring and Logging Network Traffic (3e)

## Network Security, Firewalls, and VPNs, Third Edition - Lab 06

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

The screenshot shows the pfSense web interface under the 'Diagnostics' tab, specifically the 'Ping' section. A warning message at the top states: 'WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.' The 'Ping' form has the following settings: Hostname: 172.30.0.2, IP Protocol: IPv4, Source address: DMZ, and Maximum number of pings: 3. Below the form is a 'Ping' button. The 'Results' section displays the ping statistics for three packets transmitted to 172.30.0.2. The output is as follows:

```
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=0.328 ms
64 bytes from 172.30.0.2: icmp_seq=1 ttl=128 time=0.311 ms
64 bytes from 172.30.0.2: icmp_seq=2 ttl=128 time=0.347 ms
...
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.311/0.329/0.347/0.015 ms
```

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

The screenshot shows the pfSense web interface under the 'Services' tab, specifically the 'Snort / Alerts' section. A warning message at the top states: 'WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.' The 'Alert Log View Settings' section includes an 'Interface to Inspect' dropdown set to 'LAN (vmx0)', an 'Auto-refresh view' checkbox, and a 'Save' button. The 'Alert Log Actions' section has a 'Download' button. The 'Alert Log View Filter' section shows a table with 6 entries in the Active Log. The columns are: Date, Action, Prio, Proto, Class, Source IP, SPort, Destination IP, DPort, GID:SID, and Description. The entries are as follows:

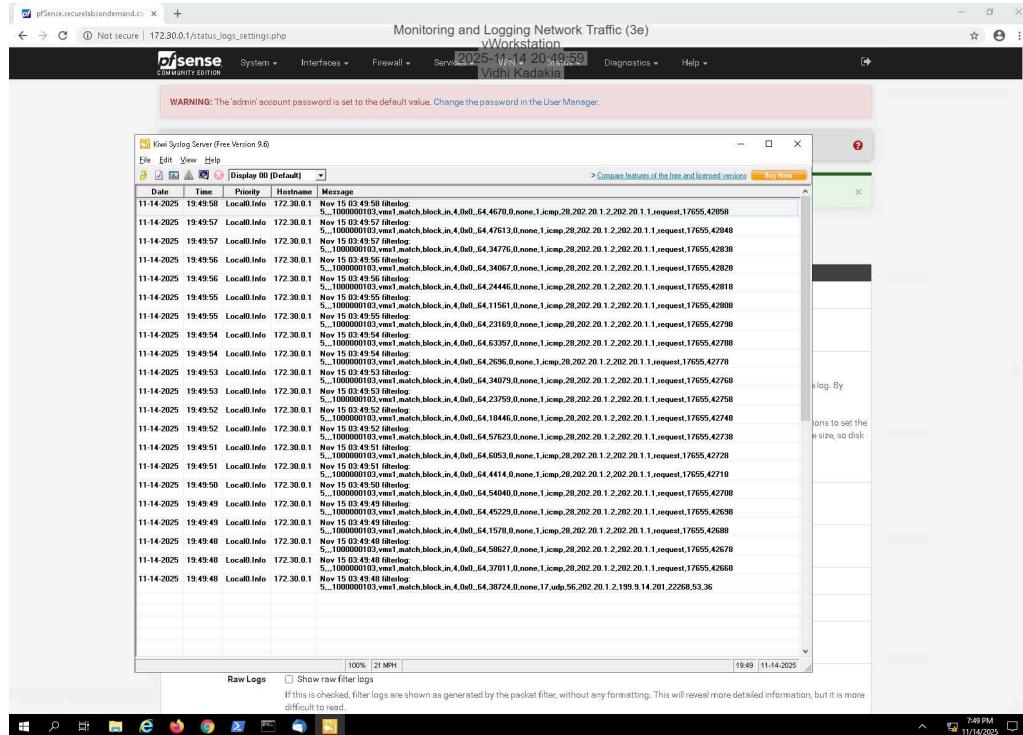
Date	Action	Prio	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2025-11-15 03:45:40	⚠️	3	ICMP	Misc activity	172.31.0.1 Q ⊕		172.30.0.2 Q ⊕		1:2100366	GPL_ICMP_INFO PING *NIX
2025-11-15 03:45:40	⚠️	3	ICMP	Misc activity	172.31.0.1 Q ⊕		172.30.0.2 Q ⊕		1:2100368	GPL_ICMP_INFO PING BSDtype
2025-11-15 03:45:39	⚠️	3	ICMP	Misc activity	172.31.0.1 Q ⊕		172.30.0.2 Q ⊕		1:2100366	GPL_ICMP_INFO PING *NIX
2025-11-15 03:45:39	⚠️	3	ICMP	Misc activity	172.31.0.1 Q ⊕		172.30.0.2 Q ⊕		1:2100366	GPL_ICMP_INFO PING BSDtype
2025-11-15 03:45:38	⚠️	3	ICMP	Misc activity	172.31.0.1 Q ⊕		172.30.0.2 Q ⊕		1:2100368	GPL_ICMP_INFO PING *NIX
2025-11-15 03:45:38	⚠️	3	ICMP	Misc activity	172.31.0.1 Q ⊕		172.30.0.2 Q ⊕		1:2100368	GPL_ICMP_INFO PING BSDtype

# Monitoring and Logging Network Traffic (3e)

Network Security, Firewalls, and VPNs, Third Edition - Lab 06

## 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.



## 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.

The screenshot shows the pfSense web interface for managing Snort monitoring. The URL is `pfSense.securelabondemand.co`. The top navigation bar includes links for System, Interfaces, Firewall, Services, Diagnostics, and Help. A user session is shown at the top right: `vWorkstation`, `2025-11-14 20:55:21`, and `Vidhi Kadakia`.

A red warning message at the top states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager."

The main content area displays the "Services / Snort / Interfaces" page. The "Snort Interfaces" tab is selected. A table titled "Interface Settings Overview" lists two interfaces:

Interface	Snort Status	Pattern Match	Blocking Mode	Description	Actions
LAN (vmx0)	<span style="color: green;">C</span> <span style="color: blue;">B</span>	AC-BNFA	DISABLED	LAN	<span style="color: blue;">Edit</span> <span style="color: orange;">Delete</span>
DMZ (vmx2)	<span style="color: green;">C</span> <span style="color: blue;">B</span>	AC-BNFA	DISABLED	WAN	<span style="color: blue;">Edit</span> <span style="color: orange;">Delete</span>

At the bottom of the interface, there is a footer with the pfSense logo and copyright information: "pfSense is developed and maintained by Netgate. © ESP 2004 - 2025 View license." The system status bar at the bottom right shows the time as 7:55 PM and the date as 11/14/2025.

# Monitoring and Logging Network Traffic (3e)

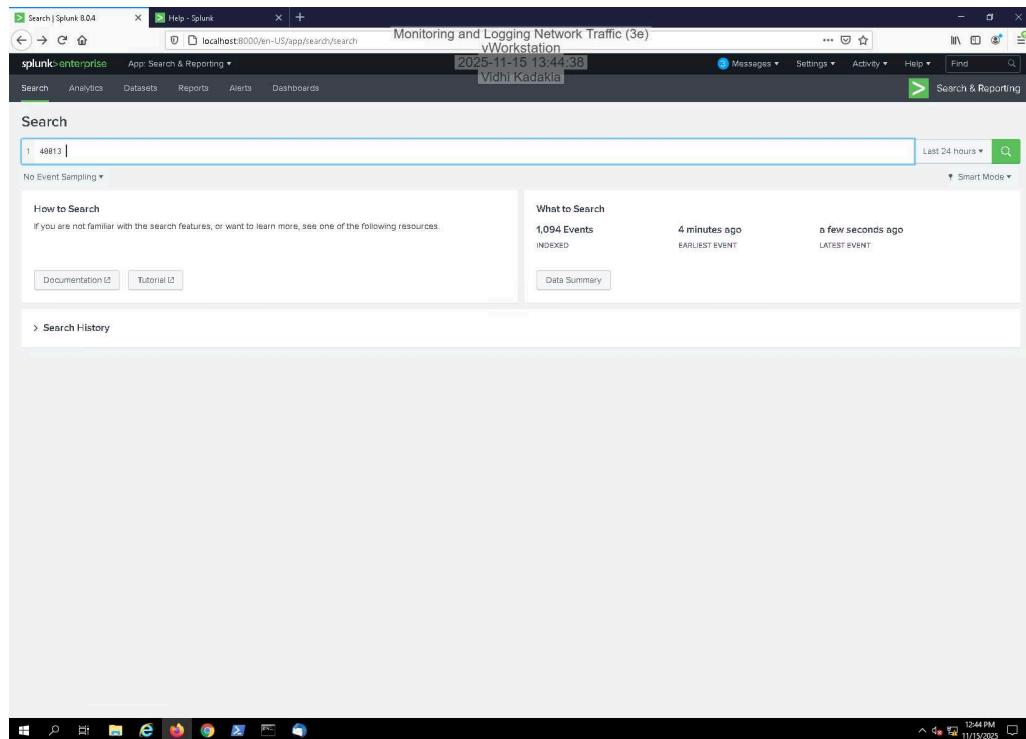
Network Security, Firewalls, and VPNs, Third Edition - Lab 06

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

The screenshot shows the pfSense web interface under the 'Snort' category. A red banner at the top states 'WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.' Below this, a message says 'Snort is live-reloading the new rule set.' The 'Snort Interfaces' tab is selected. Under 'Automatic Flowbit Resolution', there is a checkbox for 'Resolve Flowbits' which is checked. The 'Select the rulesets (Categories) Snort will load at startup' section shows two categories: 'Category is auto-enabled by SID Mgmt conf files' and 'Category is auto-disabled by SID Mgmt conf files'. The 'Enable' section lists several rule sets under 'Snort GPLv2 Community Rules' and 'Snort OPENAPI Rules'. Most checkboxes are unchecked except for the first one under 'Snort GPLv2 Community Rules'. The 'Save' button is visible at the bottom right of the configuration area.

## Part 2: Implement Security Information and Event Management with Splunk

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

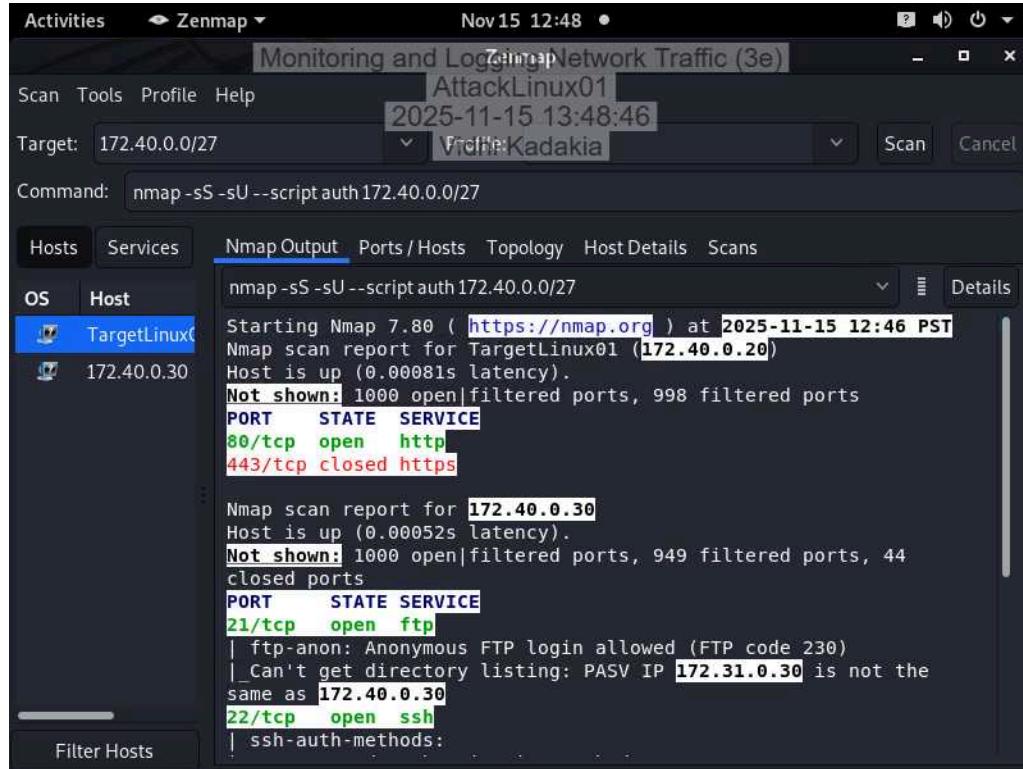


## Part 3: Simulate and Detect a Perimeter Network Attack

# Monitoring and Logging Network Traffic (3e)

Network Security, Firewalls, and VPNs, Third Edition - Lab 06

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



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

The screenshot shows the Splunk interface with the following details:

- Search Bar:** Monitoring and Logging Network Traffic (3e) | 2025-11-15 13:49:38 | Vidhi Kadakia
- Search Query:** snort
- Results:** 954 events (Nov 14/25 12:00:00 0000 PM to Nov 15/25 12:49:00 0000 PM) - No Event Sampling
- Event List:** A list of 954 events with columns for Time, Event, and various log fields. Key entries include:
  - Nov 15 12:48:04 pfSense.securelabsondemand.com Nov 15 20:48:04 snort[79465]: [1:2081219:19] ET SDN Potential SSH Scan [Classification: Attempted Information Leak]
  - Nov 15 12:47:38 pfSense.securelabsondemand.com Nov 15 20:47:38 snort[79465]: [1:2101281:11] GPL WEB\_SERVER 403 Forbidden [Classification: Attempted Information Leak]
  - Nov 15 12:47:38 pfSense.securelabsondemand.com Nov 15 20:47:38 snort[79465]: [1:2089358:5] ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)
  - Nov 15 12:47:38 pfSense.securelabsondemand.com Nov 15 20:47:38 snort[79465]: [1:2081281:11] GPL WEB\_SERVER 403 Forbidden [Classification: Attempted Information Leak]
  - Nov 15 12:47:38 pfSense.securelabsondemand.com Nov 15 20:47:38 snort[79465]: [1:2081281:11] GPL WEB\_SERVER 403 Forbidden [Classification: Attempted Information Leak]
  - Nov 15 12:47:38 pfSense.securelabsondemand.com Nov 15 20:47:38 snort[79465]: [1:2089358:5] ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)
  - Nov 15 12:47:38 pfSense.securelabsondemand.com Nov 15 20:47:38 snort[79465]: [1:2081281:11] GPL WEB\_SERVER 403 Forbidden [Classification: Attempted Information Leak]
  - Nov 15 12:47:38 pfSense.securelabsondemand.com Nov 15 20:47:38 snort[79465]: [1:2081281:11] GPL WEB\_SERVER 403 Forbidden [Classification: Attempted Information Leak]

## **Monitoring and Logging Network Traffic (3e)**

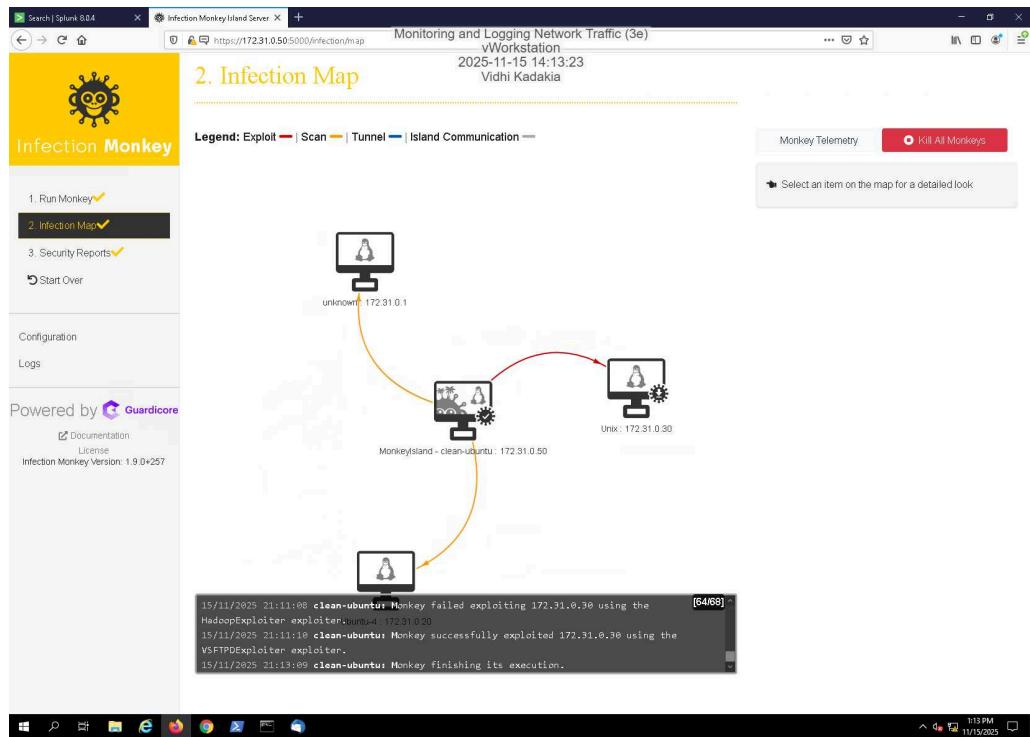
Network Security, Firewalls, and VPNs, Third Edition - Lab 06

---

## 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)

Network Security, Firewalls, and VPNs, Third Edition - Lab 06

Make a screen capture showing the resulting Security Report.

The screenshot shows a Windows desktop environment with a browser window open to the 'Infection Monkey Island Server' at <https://172.31.0.50:5000/report/security>. The title bar indicates the page is titled 'Monitoring and Logging Network Traffic (3e)'. The main content area displays a 'Security Report' for 'Infection Monkey'. The report includes an 'Overview' section with a warning message: 'Critical security issues were detected!'. It details the first monkey run started on 16/11/2025 20:55:09, which took 18 minutes and 1 seconds. The monkey propagated to several machines, including 'clean-ubuntu'. The configuration used for the monkeys included brute-forcing with usernames 'Administrator', 'root', and 'user', and passwords 'roo\*\*\*\*\*', '123\*\*\*\*\*', 'pas\*\*\*\*\*', and '123\*\*\*\*\*'. The interface also shows a sidebar with navigation links like 'Run Monkey', 'Infection Map', and 'Security Reports' (which is currently selected), along with sections for 'Configuration' and 'Logs'. A footer notes the 'Guardcore' powered version 1.9.0+257.

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

The DMZ breach simulation revealed several major security concerns. Infection Monkey successfully exploited a critical VSFTPD vulnerability, showing that unpatched services pose an immediate risk. The monkey was able to move laterally from the DMZ into the internal LAN, indicating weak network segmentation and insufficient firewall controls. Multiple reused or weak credentials were discovered, making lateral movement even easier. The simulation also showed that hosts across different network segments could communicate freely without restriction. Most importantly, none of the monkey's exploit attempts, scanning behavior, or credential attacks were detected or blocked, revealing significant gaps in network monitoring. Overall, the results demonstrate that both patching and internal visibility need major improvement.

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

## Monitoring and Logging Network Traffic (3e)

Network Security, Firewalls, and VPNs, Third Edition - Lab 06

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

**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 Snort logs in Splunk were hard to read because most of the important details were buried inside long syslog messages instead of being broken into clear fields. It was difficult to quickly see things like source IP, destination IP, or the signature that triggered the alert. To make the logs easier to analyze, I would add proper field extractions for IPs, ports, severity, and signature names. I would also remove extra syslog noise and add labels for network zones so it's easier to understand where the traffic came from

**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?

Splunk was able to capture Snort alerts from the Infection Monkey scan, so it does detect traces of the attack, but it didn't highlight them clearly without manual searching. I recommend enabling better field parsing for Snort logs and creating alerts for suspicious scans or DMZ-to-LAN traffic. Adding dashboards and automated correlation rules would make Splunk far more helpful during real incidents. With these improvements, Splunk would provide clearer and faster detection of similar breaches in the future.