

Applying Defense-in-Depth Strategies to Secure Network Assets (4e)

Ethical Hacking, Fourth Edition - Lab 10

Student:

Isaiah Mosley

Email:

isaiahmosley80@gmail.com

Time on Task:

104 hours, 46 minutes

Progress:

100%

Report Generated: Tuesday, December 2, 2025 at 1:25 PM

Hands-On Demonstration

Part 1: Update the Firewall Rules

10. Make a screen capture showing the Port Forward rules for WebServer01.

The screenshot shows the pfSense Firewall / NAT / Port Forward configuration page. The interface is titled 'Firewall / NAT / Port Forward' with the 'Port Forward' tab selected. 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.' Below this, there is a table titled 'Rules' listing three port forward entries:

	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
<input type="checkbox"/>	WAN	TCP	*	*	202.20.1.10	80 (HTTP)	172.31.0.10	80 (HTTP)	Web Access	
<input type="checkbox"/>	WAN	TCP	*	*	202.20.1.10	22 (SSH)	172.31.0.10	22 (SSH)	Remote Shell Access	
<input type="checkbox"/>	WAN	ICMP	*	*	202.20.1.10	*	172.31.0.10	*	Connectivity testing	

At the bottom of the table, there are buttons for 'Add', 'Edit', 'Delete', 'Save', and 'Separator'. A legend below the table defines the icons: a green arrow pointing right for 'Pass' and a red X for 'Linked rule'.

Applying Defense-in-Depth Strategies to Secure Network Assets (4e)

Ethical Hacking, Fourth Edition - Lab 10

14. Make a screen capture showing the permissive DMZ ruleset.

The screenshot shows the pfSense Firewall Ruleset configuration for the DMZ. The interface is a web-based management tool with a dark header bar. The main content area has a light background. At the top, there's a banner with a warning about the 'admin' account password being set to default. Below this, the title 'Firewall / Rules / DMZ' is displayed, with the 'DMZ' tab selected. A table titled 'Rules (Drag to Change Order)' lists four rules:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/0 B	IPv4 ICMP	*	*	This Firewall	*	*	none			
0/0 B	IPv4 TCP	*	*	*	80 (HTTP)	*	none		Web	
0/0 B	IPv4 TCP	*	*	*	22 (SSH)	*	none		SSH Access	

At the bottom of the table are buttons for 'Add', 'Edit', 'Delete', 'Save', and 'Separate'. The status bar at the bottom right shows the date and time as 11:28 PM 4/5/2025.

25. Make a screen capture showing the updated firewall ruleset for the DMZ.

The screenshot shows the pfSense Firewall Ruleset configuration for the DMZ after changes have been applied. The interface is identical to the previous screenshot. The main content area has a light background. A message box at the top states: 'The changes have been applied successfully. The firewall rules are now reloading in the background. Monitor the filter reload progress.' Below this, the title 'Firewall / Rules / DMZ' is displayed, with the 'DMZ' tab selected. A table titled 'Rules (Drag to Change Order)' lists five rules, with the first rule having a red 'X' icon indicating it has been disabled:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/0 B	IPv4 *	*	*	LAN net	*	*	none		Deny DMZ to LAN	
0/0 B	IPv4 ICMP	*	*	This Firewall	*	*	none			
0/0 B	IPv4 TCP	*	*	*	80 (HTTP)	*	none		Web	
0/0 B	IPv4 TCP	*	*	*	22 (SSH)	*	none		SSH Access	

At the bottom of the table are buttons for 'Add', 'Edit', 'Delete', 'Save', and 'Separate'. The status bar at the bottom right shows the date and time as 12:35 AM 4/6/2025.

Part 2: Configure a Network-based IDS on pfSense

Applying Defense-in-Depth Strategies to Secure Network Assets (4e)

Ethical Hacking, Fourth Edition - Lab 10

23. Make a screen capture showing a Balanced IPS policy.

The screenshot shows the pfSense web interface at http://172.30.0.1/snort/snort_rulesets.php?id=0. The title bar indicates "Applying Defense-in-Depth Strategies to Secure Network Assets (4e)". The main content area is titled "Services / Snort / Interface Settings / DMZ - Categories". The "DMZ Categories" tab is selected. The "Automatic Flowbit Resolution" section contains a checkbox for "Resolve Flowbits" which is checked. The "Snort Subscriber IPS Policy Selection" section has a checkbox for "Use IPS Policy" which is checked. The "IPS Policy Selection" dropdown is set to "Balanced". Below it, a note states: "Short IPS policies are: Connectivity, Balanced, Security or Max-Detect. Connectivity blocks most major threats with few or no false positives. Balanced is a good starter policy. It is speedy, has good base coverage level, and covers most threats of the day. It includes all rules in Connectivity. Security is a stringent policy. It contains everything in the first two plus policy-type rules such as a Flash object in an Excel file. Max-Detect is a policy created for testing network traffic through your device. This policy should be used with caution on production systems!". The "Select the rulesets (Categories) Snort will load at startup" section lists categories: "Category is auto-enabled by SID Mgmt conf files" (green dot) and "Category is auto-disabled by SID Mgmt conf files" (red dot). Buttons for "Select All", "Unselect All", and "Save" are at the bottom.

30. Make a screen capture showing that the Snort (DMZ) Interface is running in the Interface Settings Overview.

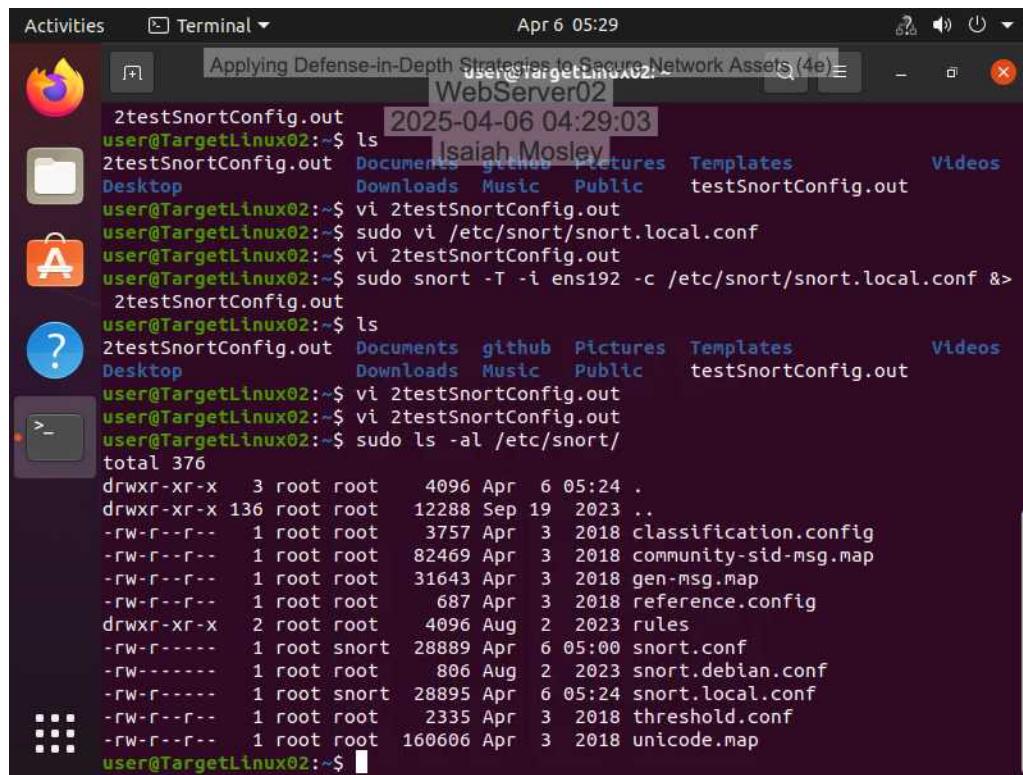
The screenshot shows the pfSense web interface at http://172.30.0.1/snort/snort_interfaces.php. The title bar indicates "Applying Defense-in-Depth Strategies to Secure Network Assets (4e)". The main content area is titled "Services / Snort / Interfaces". The "Short Interfaces" tab is selected. The "Interface Settings Overview" table shows one entry: "Interface": "DMZ (vmx2)", "Snort Status": "OK (C)", "Pattern Match": "AC-BNFA", "Blocking Mode": "DISABLED", "Description": "DMZ Smart Interface", and "Actions" with edit and delete icons. A note at the bottom left says "i". The pfSense footer at the bottom states "pfSense is developed and maintained by Netgate. © ESF 2004-2025 View license." and the date "4/6/2025".

Part 3: Configure a Host-based IDS (HIDS) on Linux

Applying Defense-in-Depth Strategies to Secure Network Assets (4e)

Ethical Hacking, Fourth Edition - Lab 10

38. Make a screen capture showing the contents of the /etc/snort directory with your local config file.



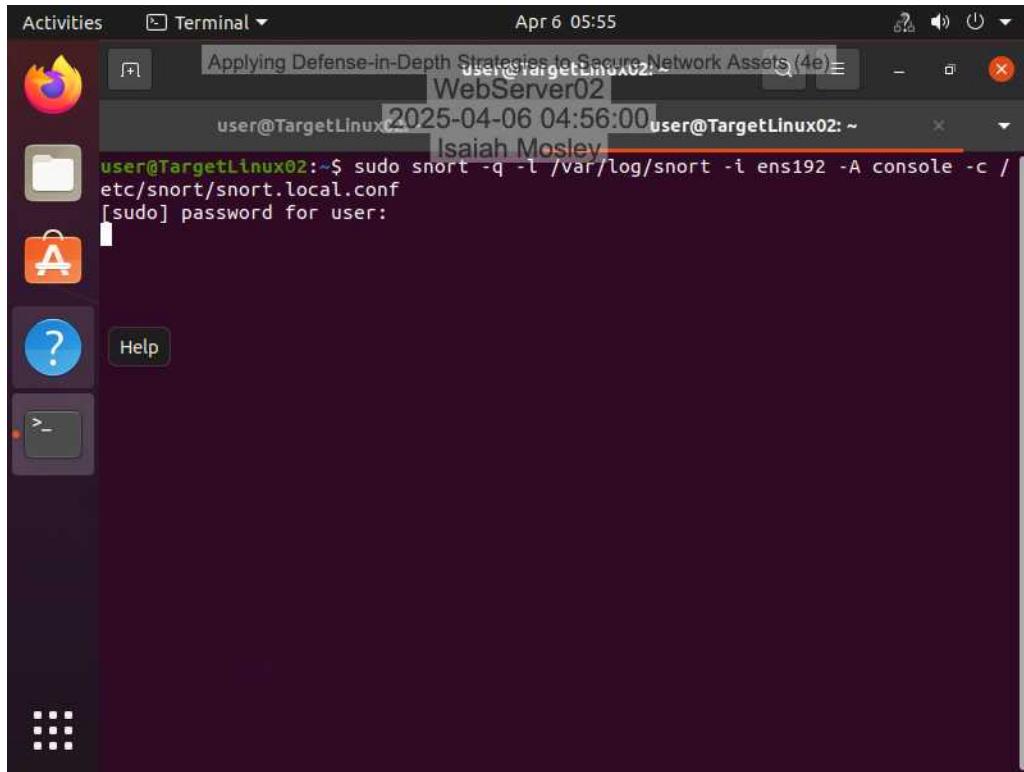
The screenshot shows a terminal window titled "Terminal" with the command "ls" run in the directory "/etc/snort". The output lists several configuration files and a "rules" directory. The terminal window is part of a desktop environment with icons for a browser, file manager, and other applications visible in the background.

```
user@TargetLinux02:~$ ls
2testSnortConfig.out  2025-04-06 04:29:03
user@TargetLinux02:~$ ls
2testSnortConfig.out  Documents  github  Pictures  Templates  Videos
Desktop              Downloads  Music   Public    testSnortConfig.out
user@TargetLinux02:~$ vi 2testSnortConfig.out
user@TargetLinux02:~$ sudo vi /etc/snort/snort.local.conf
user@TargetLinux02:~$ vi 2testSnortConfig.out
user@TargetLinux02:~$ sudo snort -T -i ens192 -c /etc/snort/snort.local.conf &>
2testSnortConfig.out
user@TargetLinux02:~$ ls
2testSnortConfig.out  Documents  github  Pictures  Templates  Videos
Desktop              Downloads  Music   Public    testSnortConfig.out
user@TargetLinux02:~$ vi 2testSnortConfig.out
user@TargetLinux02:~$ vi 2testSnortConfig.out
user@TargetLinux02:~$ sudo ls -al /etc/snort/
total 376
drwxr-xr-x  3 root root  4096 Apr  6 05:24 .
drwxr-xr-x 136 root root 12288 Sep 19 2023 ..
-rw-r--r--  1 root root  3757 Apr  3 2018 classification.config
-rw-r--r--  1 root root 82469 Apr  3 2018 community-sid-msg.map
-rw-r--r--  1 root root 31643 Apr  3 2018 gen-msg.map
-rw-r--r--  1 root root   687 Apr  3 2018 reference.config
drwxr-xr-x  2 root root  4096 Aug  2 2023 rules
-rw-r----- 1 root snort 28889 Apr  6 05:00 snort.conf
-rw-----  1 root root   806 Aug  2 2023 snort.debian.conf
-rw-r----- 1 root snort 28895 Apr  6 05:24 snort.local.conf
-rw-r--r--  1 root root  2335 Apr  3 2018 threshold.conf
-rw-r--r--  1 root root 160606 Apr  3 2018 unicode.map
user@TargetLinux02:~$
```

Applying Defense-in-Depth Strategies to Secure Network Assets (4e)

Ethical Hacking, Fourth Edition - Lab 10

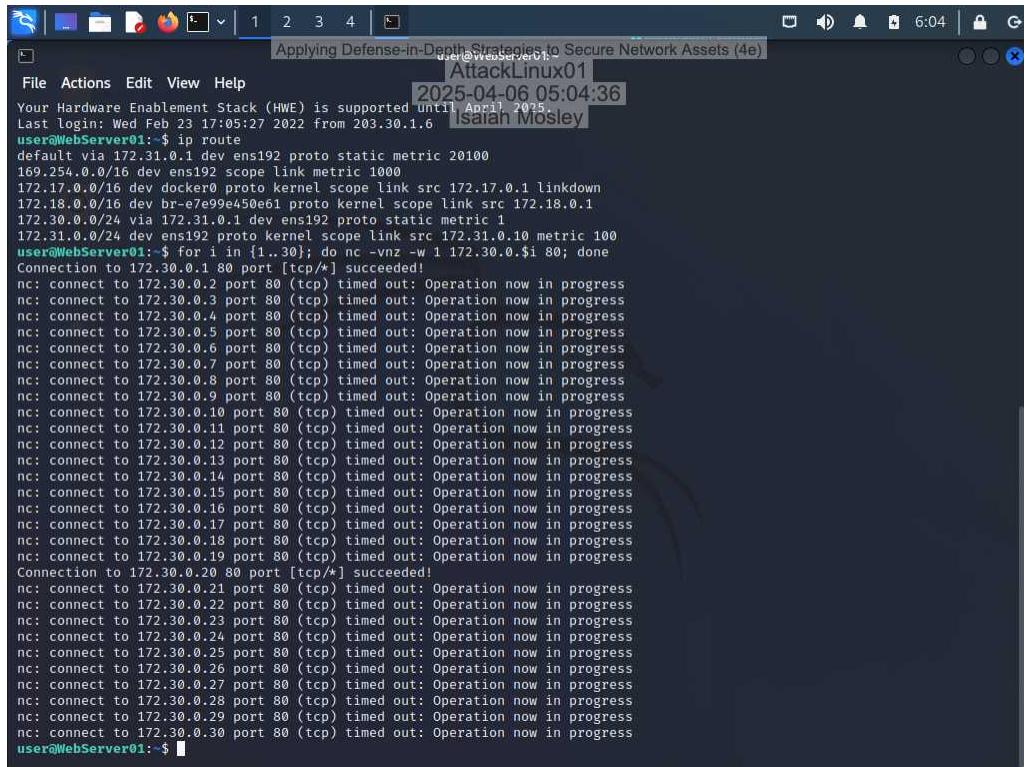
51. Make a screen capture showing the successful start of Snort as HIDS on WebServer02.



Applied Learning

Part 1: Validate Your IDS Security Controls

9. Make a screen capture showing the successful Netcat connection to WebServer02 at 172.30.0.20.



The screenshot shows a terminal window titled "AttackLinux01" running on "WebServer01". The terminal displays a netcat listener script being run on port 80. The output shows numerous failed connection attempts from various ports (e.g., 172.30.0.1-30) to port 80, all resulting in "Operation now in progress".

```
user@WebServer01:~$ nc -l -p 80
2025-04-06 05:04:36
Your Hardware Enablement Stack (HWE) is supported until April 2015
Last login: Wed Feb 23 17:05:27 2022 from 203.30.1.6 [Sarah Mosley]
user@WebServer01:~$ for i in {1..30}; do nc -vnz -w 1 172.30.0.$i 80; done
Connection to 172.30.0.1 80 port [tcp/*] succeeded!
nc: connect to 172.30.0.2 port 80 (tcp) timed out: Operation now in progress
nc: connect to 172.30.0.3 port 80 (tcp) timed out: Operation now in progress
nc: connect to 172.30.0.4 port 80 (tcp) timed out: Operation now in progress
nc: connect to 172.30.0.5 port 80 (tcp) timed out: Operation now in progress
nc: connect to 172.30.0.6 port 80 (tcp) timed out: Operation now in progress
nc: connect to 172.30.0.7 port 80 (tcp) timed out: Operation now in progress
nc: connect to 172.30.0.8 port 80 (tcp) timed out: Operation now in progress
nc: connect to 172.30.0.9 port 80 (tcp) timed out: Operation now in progress
nc: connect to 172.30.0.10 port 80 (tcp) timed out: Operation now in progress
nc: connect to 172.30.0.11 port 80 (tcp) timed out: Operation now in progress
nc: connect to 172.30.0.12 port 80 (tcp) timed out: Operation now in progress
nc: connect to 172.30.0.13 port 80 (tcp) timed out: Operation now in progress
nc: connect to 172.30.0.14 port 80 (tcp) timed out: Operation now in progress
nc: connect to 172.30.0.15 port 80 (tcp) timed out: Operation now in progress
nc: connect to 172.30.0.16 port 80 (tcp) timed out: Operation now in progress
nc: connect to 172.30.0.17 port 80 (tcp) timed out: Operation now in progress
nc: connect to 172.30.0.18 port 80 (tcp) timed out: Operation now in progress
nc: connect to 172.30.0.19 port 80 (tcp) timed out: Operation now in progress
Connection to 172.30.0.20 80 port [tcp/*] succeeded!
nc: connect to 172.30.0.21 port 80 (tcp) timed out: Operation now in progress
nc: connect to 172.30.0.22 port 80 (tcp) timed out: Operation now in progress
nc: connect to 172.30.0.23 port 80 (tcp) timed out: Operation now in progress
nc: connect to 172.30.0.24 port 80 (tcp) timed out: Operation now in progress
nc: connect to 172.30.0.25 port 80 (tcp) timed out: Operation now in progress
nc: connect to 172.30.0.26 port 80 (tcp) timed out: Operation now in progress
nc: connect to 172.30.0.27 port 80 (tcp) timed out: Operation now in progress
nc: connect to 172.30.0.28 port 80 (tcp) timed out: Operation now in progress
nc: connect to 172.30.0.29 port 80 (tcp) timed out: Operation now in progress
nc: connect to 172.30.0.30 port 80 (tcp) timed out: Operation now in progress
user@WebServer01:~$
```

Applying Defense-in-Depth Strategies to Secure Network Assets (4e)

Ethical Hacking, Fourth Edition - Lab 10

17. Make a screen capture showing the login page of the internal GitLab server at localhost/users/sign_in.

The screenshot shows a Firefox browser window with the title bar "Applying Defense-in-Depth Strategies to Secure Network Assets (4e)" and the tab "Sign in - GitLab". The address bar displays "localhost/users/sign_in" and the date "2025-04-06 05:10:47". The user "Isaiah Mosley" is logged in. Below the address bar, the Kali Linux desktop environment is visible with various icons. The main content area shows the GitLab login form with fields for "Username or email" and "Password", a "Remember me" checkbox, and a "Sign in" button. A "Forgot your password?" link is also present. At the bottom of the form, there is a link "Don't have an account yet? Register now".

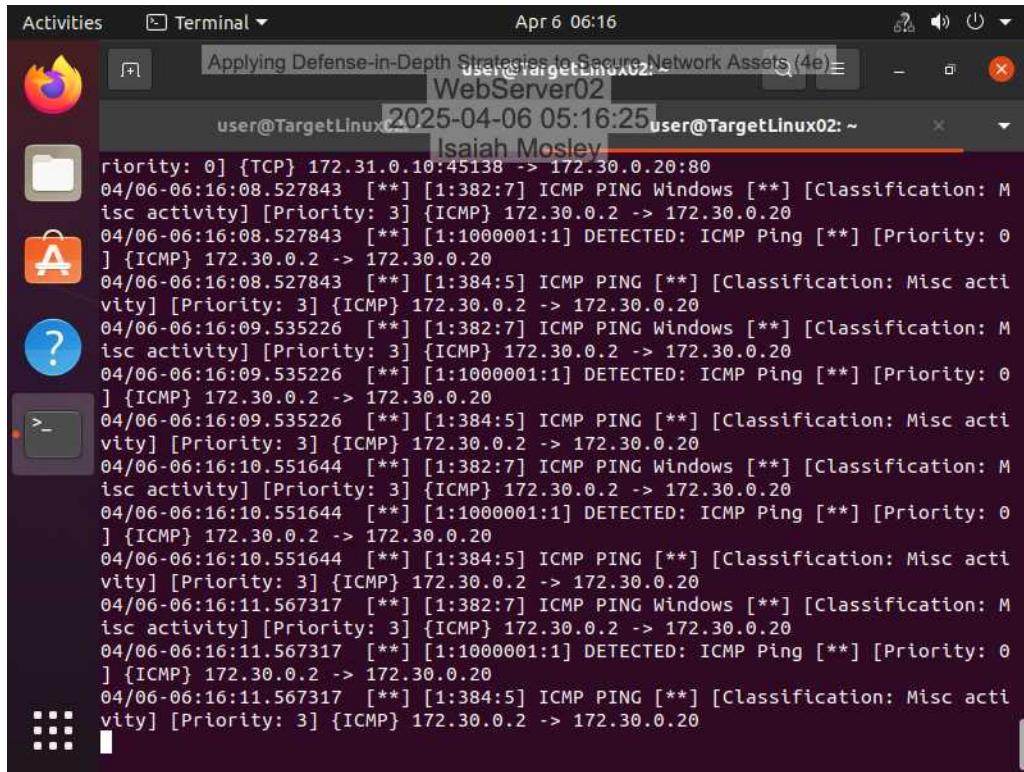
25. Make a screen capture showing the Attempted Information Leak alert.

The screenshot shows a Firefox browser window with the title bar "Applying Defense-in-Depth Strategies to Secure Network Assets (4e)" and the tab "vWorkstation". The address bar displays "172.30.0.1/inort/alerts.php?instance=0". The user "Isaiah Mosley" is logged in. The browser status bar shows "It looks like you haven't started Firefox a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back! Refresh Firefox...". The main content area is the pfSense "Services / Snort / Alerts" interface. It shows a "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." message. The "Alert Log View Settings" section is active, showing settings for "Interface to Inspect" (DMZ (vmx2)), "Auto-refresh view" (250), and "Alert lines to display". The "Alert Log Actions" section includes "Download" and "Clear" buttons. The "Alert Log View Filter" section allows filtering by Source IP Address, Destination IP Address, Date, Priority, GID, SID, Description, Classification, Action, and Exact Match. The "Alert Log" table header includes columns for Date, Action, Prio, Proto, Class, Source IP, SPort, Destination IP, DPort, GID:SID, and Description. One entry is listed: "2025-04-06 09:59:39" with action "Attempt" and class "TCP" for "Attempted Information Leak" from source IP 203.30.1.6 to destination IP 172.31.0.10 on port 22, with GID:SID 1:2001219 and description "ET SCAN Potential SSH Scan".

Applying Defense-in-Depth Strategies to Secure Network Assets (4e)

Ethical Hacking, Fourth Edition - Lab 10

30. Make a screen capture showing these Snort HIDS alerts.



The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "user@TargetLinux02: ~" and the subtitle is "Isaiah Mosley". The terminal displays a series of Snort HIDS alerts from April 6, 2016, at 05:16:25. The alerts are all of type "DETECTED: ICMP Ping" with priority 0. They involve ICMP PING requests from various IP addresses (e.g., 172.31.0.10, 172.30.0.2) to 172.30.0.20. The classification for these alerts is "Misc activity". The terminal window is part of a desktop interface with icons for a browser, file manager, terminal, and system tray visible.

```
priority: 0] {TCP} 172.31.0.10:45138 -> 172.30.0.20:80  
04/06:06:16:08.527843 [**] [1:382:7] ICMP PING Windows [**] [Classification: Misc activity] [Priority: 3] {ICMP} 172.30.0.2 -> 172.30.0.20  
04/06:06:16:08.527843 [**] [1:1000001:1] DETECTED: ICMP Ping [**] [Priority: 0] {ICMP} 172.30.0.2 -> 172.30.0.20  
04/06:06:16:08.527843 [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 172.30.0.2 -> 172.30.0.20  
04/06:06:16:09.535226 [**] [1:382:7] ICMP PING Windows [**] [Classification: Misc activity] [Priority: 3] {ICMP} 172.30.0.2 -> 172.30.0.20  
04/06:06:16:09.535226 [**] [1:1000001:1] DETECTED: ICMP Ping [**] [Priority: 0] {ICMP} 172.30.0.2 -> 172.30.0.20  
04/06:06:16:09.535226 [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 172.30.0.2 -> 172.30.0.20  
04/06:06:16:10.551644 [**] [1:382:7] ICMP PING Windows [**] [Classification: Misc activity] [Priority: 3] {ICMP} 172.30.0.2 -> 172.30.0.20  
04/06:06:16:10.551644 [**] [1:1000001:1] DETECTED: ICMP Ping [**] [Priority: 0] {ICMP} 172.30.0.2 -> 172.30.0.20  
04/06:06:16:10.551644 [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 172.30.0.2 -> 172.30.0.20  
04/06:06:16:11.567317 [**] [1:382:7] ICMP PING Windows [**] [Classification: Misc activity] [Priority: 3] {ICMP} 172.30.0.2 -> 172.30.0.20  
04/06:06:16:11.567317 [**] [1:1000001:1] DETECTED: ICMP Ping [**] [Priority: 0] {ICMP} 172.30.0.2 -> 172.30.0.20  
04/06:06:16:11.567317 [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 172.30.0.2 -> 172.30.0.20
```

Part 2: Configure and Validate Protection Mode (IPS) on Network-based IDS

Applying Defense-in-Depth Strategies to Secure Network Assets (4e)

Ethical Hacking, Fourth Edition - Lab 10

27. Make a screen capture showing the blocked IP in the *Last 500 Hosts Blocked by Snort* widget.

The screenshot shows the pfSense Services / Snort / Blocked Hosts interface. At the top, there is a warning message: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, the "Blocked" tab is selected in the navigation bar. The main section is titled "Blocked Hosts and Log View Settings". It includes buttons for "Download" (green) and "Clear" (red), and a refresh checkbox. The "Last 500 Hosts Blocked by Snort" table lists one entry:

#	IP	Alert Descriptions and Event Times	Remove
1	203.30.1.6	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine) – 2025-04-06 10:33:09 ET SCAN Potential SSH Scan – 2025-04-06 10:33:09	X

A note at the bottom states: "1 host IP address is currently being blocked Snort on Legacy Blocking Mode interfaces."

30. Make a screen capture showing the blocked connection from the DMZ to the LAN.

The screenshot shows the pfSense Status / Log Filter interface. The table displays numerous log entries for "Deny DMZ to LAN" events, primarily from the "DMZ" interface. The columns include timestamp, source IP, destination IP, and protocol (TCP/S, TCP/S, TCP/S, etc.). The log entries are as follows:

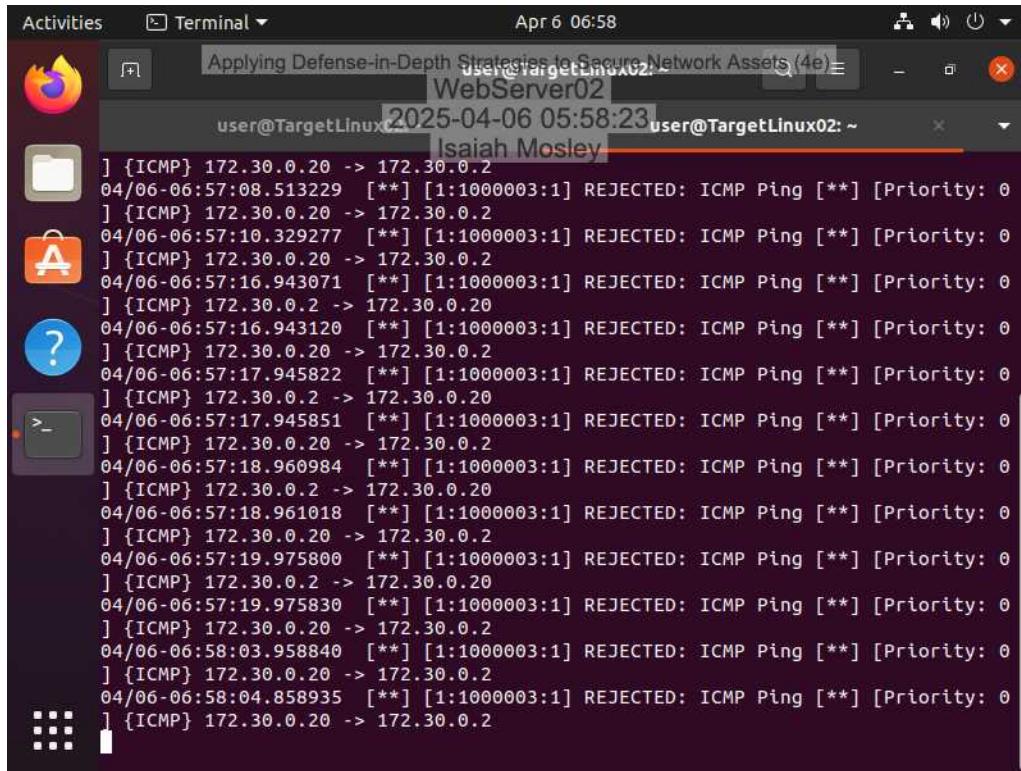
Time	Source IP	Destination IP	Action
Apr 6 10:30:50	DMZ	172.31.0.1034610	Deny DMZ to LAN (1743924843)
Apr 6 10:30:50	DMZ	172.31.0.1034612	Deny DMZ to LAN (1743924843)
Apr 6 10:30:46	DMZ	172.31.0.1034606	Deny DMZ to LAN (1743924843)
Apr 6 10:30:44	DMZ	172.31.0.1034608	Deny DMZ to LAN (1743924843)
Apr 6 10:30:34	DMZ	172.31.0.1034612	Deny DMZ to LAN (1743924843)
Apr 6 10:30:34	DMZ	172.31.0.1034610	Deny DMZ to LAN (1743924843)
Apr 6 10:30:28	DMZ	172.31.0.1034608	Deny DMZ to LAN (1743924843)
Apr 6 10:30:26	DMZ	172.31.0.1034610	Deny DMZ to LAN (1743924843)
Apr 6 10:30:26	DMZ	172.31.0.1034612	Deny DMZ to LAN (1743924843)
Apr 6 10:30:22	DMZ	172.31.0.1034612	Deny DMZ to LAN (1743924843)
Apr 6 10:30:22	DMZ	172.31.0.1034610	Deny DMZ to LAN (1743924843)
Apr 6 10:30:20	DMZ	172.31.0.1034608	Deny DMZ to LAN (1743924843)
Apr 6 10:30:20	DMZ	172.31.0.1034612	Deny DMZ to LAN (1743924843)
Apr 6 10:30:20	DMZ	172.31.0.1034610	Deny DMZ to LAN (1743924843)
Apr 6 10:30:20	DMZ	172.31.0.1034612	Deny DMZ to LAN (1743924843)
Apr 6 10:30:20	DMZ	172.31.0.1034610	Deny DMZ to LAN (1743924843)
Apr 6 10:30:19	DMZ	172.31.0.1034612	Deny DMZ to LAN (1743924843)
Apr 6 10:30:19	DMZ	172.31.0.1034610	Deny DMZ to LAN (1743924843)
Apr 6 10:30:16	DMZ	172.31.0.1034608	Deny DMZ to LAN (1743924843)
Apr 6 10:30:14	DMZ	172.31.0.1034608	Deny DMZ to LAN (1743924843)
Apr 6 10:30:13	DMZ	172.31.0.1034606	Deny DMZ to LAN (1743924843)
Apr 6 10:30:13	DMZ	172.31.0.1034608	Deny DMZ to LAN (1743924843)
Apr 6 10:29:57	DMZ	172.31.0.1034606	Deny DMZ to LAN (1743924843)
Apr 6 10:29:49	DMZ	172.31.0.1034606	Deny DMZ to LAN (1743924843)
Apr 6 10:29:45	DMZ	172.31.0.1034606	Deny DMZ to LAN (1743924843)
Apr 6 10:29:43	DMZ	172.31.0.1034606	Deny DMZ to LAN (1743924843)
Apr 6 10:29:42	DMZ	172.31.0.1034606	Deny DMZ to LAN (1743924843)
Apr 6 10:22:46	WAN	0.0.0.0	block began IPv4 networks from WAN (11001)
Apr 6 05:22:38	WAN	0.0.0.0	(11003)
Sep 19 15:41:28	WAN	203.30.1.640895	8.8.4.53

Part 3: Explore Protection Mode Options (HIPS) on Host-based IDS

Applying Defense-in-Depth Strategies to Secure Network Assets (4e)

Ethical Hacking, Fourth Edition - Lab 10

24. Make a screen capture showing the ping responses from WebServer02.



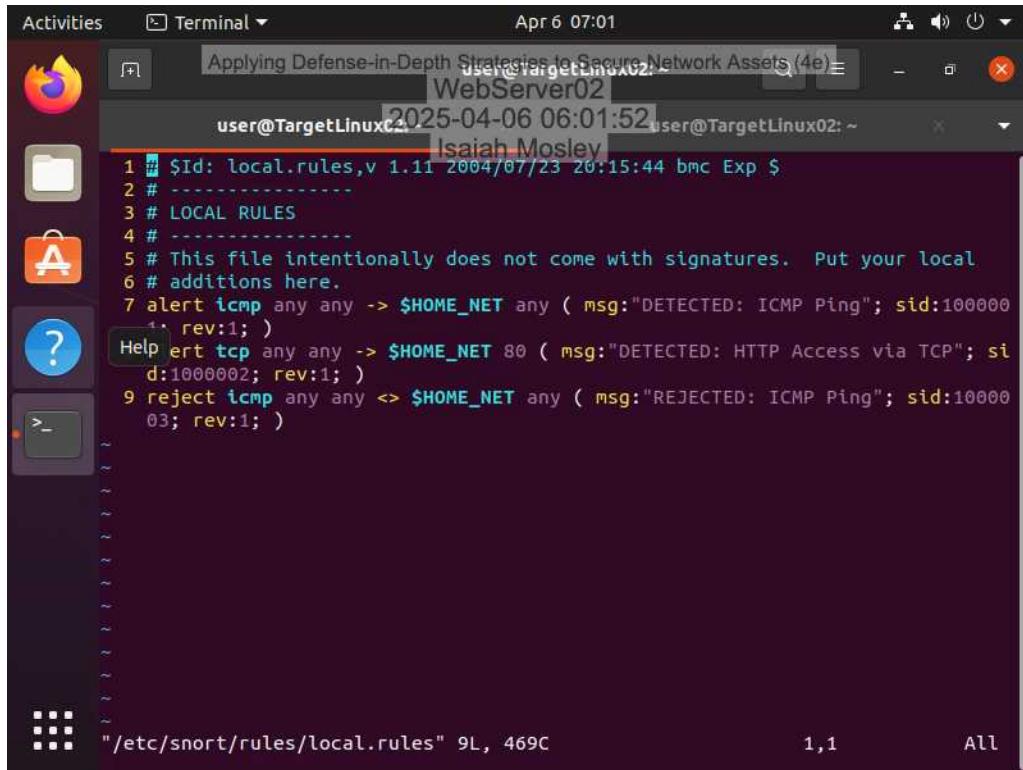
The screenshot shows a terminal window titled "user@TargetLinux02: ~" with the command "ls" running. The terminal output displays a series of log entries from a firewall or security system, all showing ICMP packets being rejected. The log entries are as follows:

```
[{ICMP} 172.30.0.20 -> 172.30.0.2  
04/06-06:57:08.513229 [**] [1:1000003:1] REJECTED: ICMP Ping [**] [Priority: 0]  
] {ICMP} 172.30.0.20 -> 172.30.0.2  
04/06-06:57:10.329277 [**] [1:1000003:1] REJECTED: ICMP Ping [**] [Priority: 0]  
] {ICMP} 172.30.0.20 -> 172.30.0.2  
04/06-06:57:16.943071 [**] [1:1000003:1] REJECTED: ICMP Ping [**] [Priority: 0]  
] {ICMP} 172.30.0.2 -> 172.30.0.20  
04/06-06:57:16.943120 [**] [1:1000003:1] REJECTED: ICMP Ping [**] [Priority: 0]  
] {ICMP} 172.30.0.20 -> 172.30.0.2  
04/06-06:57:17.945822 [**] [1:1000003:1] REJECTED: ICMP Ping [**] [Priority: 0]  
] {ICMP} 172.30.0.2 -> 172.30.0.20  
04/06-06:57:17.945851 [**] [1:1000003:1] REJECTED: ICMP Ping [**] [Priority: 0]  
] {ICMP} 172.30.0.20 -> 172.30.0.2  
04/06-06:57:18.960984 [**] [1:1000003:1] REJECTED: ICMP Ping [**] [Priority: 0]  
] {ICMP} 172.30.0.2 -> 172.30.0.20  
04/06-06:57:18.961018 [**] [1:1000003:1] REJECTED: ICMP Ping [**] [Priority: 0]  
] {ICMP} 172.30.0.20 -> 172.30.0.2  
04/06-06:57:19.975800 [**] [1:1000003:1] REJECTED: ICMP Ping [**] [Priority: 0]  
] {ICMP} 172.30.0.2 -> 172.30.0.20  
04/06-06:57:19.975830 [**] [1:1000003:1] REJECTED: ICMP Ping [**] [Priority: 0]  
] {ICMP} 172.30.0.20 -> 172.30.0.2  
04/06-06:58:03.958840 [**] [1:1000003:1] REJECTED: ICMP Ping [**] [Priority: 0]  
] {ICMP} 172.30.0.20 -> 172.30.0.2  
04/06-06:58:04.858935 [**] [1:1000003:1] REJECTED: ICMP Ping [**] [Priority: 0]  
] {ICMP} 172.30.0.20 -> 172.30.0.2
```

Applying Defense-in-Depth Strategies to Secure Network Assets (4e)

Ethical Hacking, Fourth Edition - Lab 10

- 26. Make a screen capture showing output that indicates that the rejection rules fired.**



```
Activities Terminal Apr 6 07:01
[+] Applying Defense-in-Depth Strategies to Secure Network Assets (4e) WebServer02
user@TargetLinux02: ~ 2025-04-06 06:01:52 user@TargetLinux02: ~ Isaiah Mosley

1 # $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
2 #
3 # LOCAL RULES
4 #
5 # This file intentionally does not come with signatures. Put your local
6 # additions here.
7 alert icmp any any -> $HOME_NET any ( msg:"DETECTED: ICMP Ping"; sid:100000
8     , rev:1; )
8 alert tcp any any -> $HOME_NET 80 ( msg:"DETECTED: HTTP Access via TCP"; si
9     d:1000002; rev:1; )
9 reject icmp any any <-> $HOME_NET any ( msg:"REJECTED: ICMP Ping"; sid:10000
10    , rev:1; )

"/etc/snort/rules/local.rules" 9L, 469C 1,1 All
```

- 27. Document this protection deficiency and suggest an alternative for protecting the vulnerable WebServer02 from insider attacks for Secure Labs on Demand.**

Snort needs to operate in inline mode for the "drops" features to take effect. Additionally, alerting needs to be initiated for the specified alert/drop option pair, which enables the "drops" options function successfully.

"enable_decode_drops"-This is the option if in inline mode, which alerts drop packets are on.

Challenge and Analysis

Part 1: Snort: Identifying and Suppressing False Positive Alerts

Record your reasoning that leads to the conclusion that these alerts are false positives.

After viewing the http_inspect alerts, i concluded that they were set off by a authorized HTTP traffic that doesn't present as a malicious threat. The alerts are constant with normal behavior within the environment, which is classified as false positives. By suppressing them, it will help minimize the alert fatigue and focus the attention on actual threats.

Make a screen capture showing the suppression list in the Snort interface.

