

PROJECT 4

FIREWALL AND IDS CONFIGURATION

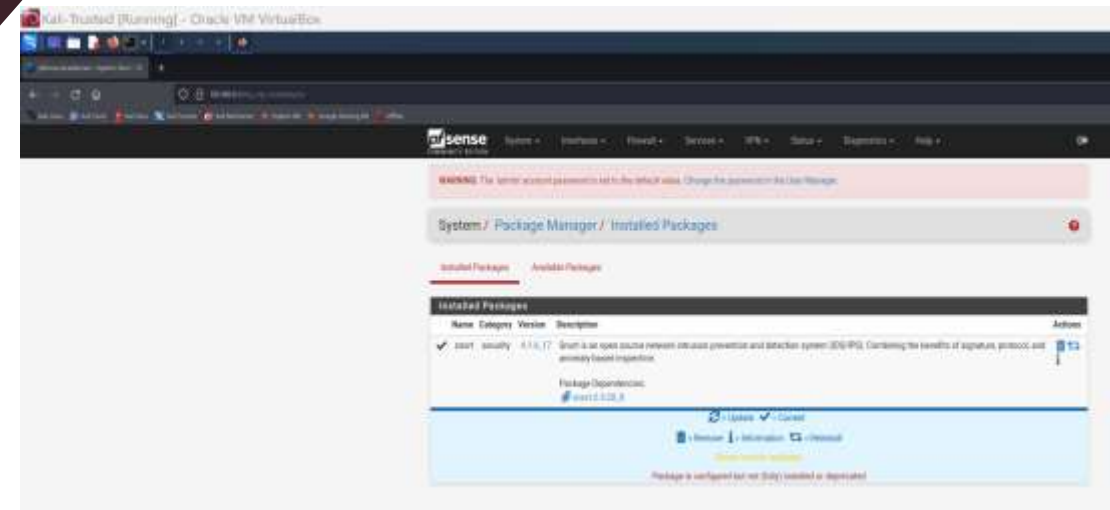
URVESH GANDHI



Summary

- **Install Snort on pfSense:**
Installing Snort on the pfSense package manager & configure it.
 - **Log Suspicious Activity:**
To monitor log suspicious activity on both Untrusted and DMZ network interfaces set up snort
 - **Configure Alerts for Exploits:**
Configure Snort to detect and alert on specific exploits used in your previous project
 - **lock FTP Traffic:**
Create firewall rules to block FTP traffic from Untrusted network to DMZ interface .
 - **Testing and Verification:**
Using Wireshark test snort alerts and firewall rule effectiveness.
-

DOWNLOAD AND INSTALL SNORT ON THE PFSENSE FIREWALL.



Use of Snort

- Snort Installation and Setup
 - Monitoring and Logging Suspicious Activity
 - Alert Configuration for Exploits:
 - Blocking FTP Traffic
 - Testing and Verification
-

Snort interface settings

Services / Snort / Interface Settings / DMZ - Categories

Snort Interfaces

Global Settings

Updates

Alerts

Blocked

Pass Lists

Suppress

IP Lists

SID Mgmt

Log Mgmt

Sync

DMZ Settings

DMZ Categories

DMZ Rules

DMZ Variables

DMZ Preprocs

DMZ IP Rep

DMZ Logs

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.


Snort Subscriber IPS Policy Selection

Use IPS Policy

☐ If checked, Snort will use rules from one of three pre-defined IPS policies in the Snort Subscriber rules. Default is Not Checked.
Selecting this option disables manual selection of Snort Subscriber categories in the list below, although Emerging Threats categories may still be selected if enabled on the Global Settings tab. These will be added to the pre-defined Snort IPS policy rules from the Snort VBT.

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

Cancel All

Unsubscribe All

Save

Enable	Ruleset: ET Open Rules	Enable	Ruleset: Snort Text Rules	Enable	Ruleset: Snort SO Rules	Snort OPENAPPID rules are not enabled.
<input type="checkbox"/>	emerging-activex.rules	<input type="checkbox"/>	snort_app-detect.rules	<input type="checkbox"/>	snort_browser-chrome.so.rules	
<input type="checkbox"/>	emerging-attack_response.rules	<input type="checkbox"/>	snort_attack-responses.rules	<input type="checkbox"/>	snort_browser-ie.so.rules	
<input type="checkbox"/>	emerging-botcc-portgrouped.rules	<input type="checkbox"/>	snort_backdoor.rules	<input type="checkbox"/>	snort_browser-other.so.rules	
<input type="checkbox"/>	emerging-botcc.rules	<input type="checkbox"/>	snort_bad-traffic.rules	<input type="checkbox"/>	snort_browser-webkit.so.rules	
<input type="checkbox"/>	emerging-chat.rules	<input type="checkbox"/>	snort_blacklist.rules	<input type="checkbox"/>	snort_exploit-kit.so.rules	
<input type="checkbox"/>	emerging-clammy.rules	<input type="checkbox"/>	snort_botnet-cnc.rules	<input type="checkbox"/>	snort_file-executable.so.rules	
<input type="checkbox"/>	emerging-compromised.rules	<input type="checkbox"/>	snort_browser-chrome.rules	<input type="checkbox"/>	snort_file-flash.so.rules	
<input type="checkbox"/>	emerging-current_events.rules	<input type="checkbox"/>	snort_browser-firefox.rules	<input type="checkbox"/>	snort_file-image.so.rules	
<input type="checkbox"/>	emerging-deleted.rules	<input type="checkbox"/>	snort_browser-ie.rules	<input type="checkbox"/>	snort_file-java.so.rules	
<input type="checkbox"/>	emerging-dns.rules	<input type="checkbox"/>	snort_browser-other.rules	<input type="checkbox"/>	snort_file-multimedia.so.rules	
<input type="checkbox"/>	emerging-dos.rules	<input type="checkbox"/>	snort_browser-plugins.rules	<input type="checkbox"/>	snort_file-office.so.rules	
<input type="checkbox"/>	emerging-drop.rules	<input type="checkbox"/>	snort_browser-webkit.rules	<input type="checkbox"/>	snort_file-other.so.rules	
<input type="checkbox"/>	emerging-dshield.rules	<input type="checkbox"/>	snort_chat.rules	<input type="checkbox"/>	snort_file-pdf.so.rules	
<input type="checkbox"/>	emerging-exploit.rules	<input type="checkbox"/>	snort_content-replace.rules	<input type="checkbox"/>	snort_indicator-shellcode.so.rules	
<input type="checkbox"/>	emerging-ftp.rules	<input type="checkbox"/>	snort_ddos.rules	<input type="checkbox"/>	snort_malware-cnc.so.rules	
<input type="checkbox"/>	emerging-games.rules	<input type="checkbox"/>	snort_deleted.rules	<input type="checkbox"/>	snort_malware-other.so.rules	

Snort custom rules

The screenshot displays the Snort web interface, specifically the 'DMZ Rules' configuration page. The interface includes a top navigation bar with links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. 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 breadcrumb trail is 'Services / Snort / Interface Settings / DMZ - Rules'. Below this, there are tabs for 'Snort Interfaces', 'Global Settings', 'Updates', 'Alerts', 'Blocked', 'Pass Lists', 'Suppress', 'IP Lists', 'SID Mgmt', 'Log Mgmt', and 'Sync'. Under the 'DMZ' section, there are sub-tabs for 'DMZ Settings', 'DMZ Categories', 'DMZ Rules' (which is active), 'DMZ Variables', 'DMZ Preprocs', 'DMZ IP Rep', and 'DMZ Logs'. The 'Available Rule Categories' section shows a 'Category Selection' dropdown set to 'custom.rules'. Below this, the 'Defined Custom Rules' section contains a text area with two rules: 'alert tcp any any -> 10.200.0.0/29 21 (msg:"ALERT: YSETPS Backdoor Attempt"; flow:to_server,established; content:' and 'alert tcp any any -> 10.200.0.0/29 21 (msg:"Blocking FTP Traffic from untrusted to DMZ"; sid:100001; rev:1;'. At the bottom right, there are buttons for 'Save', 'Cancel', and 'Clear'.

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Services / Snort / Interface Settings / DMZ - Rules

Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

DMZ Settings DMZ Categories DMZ Rules DMZ Variables DMZ Preprocs DMZ IP Rep DMZ Logs

Available Rule Categories

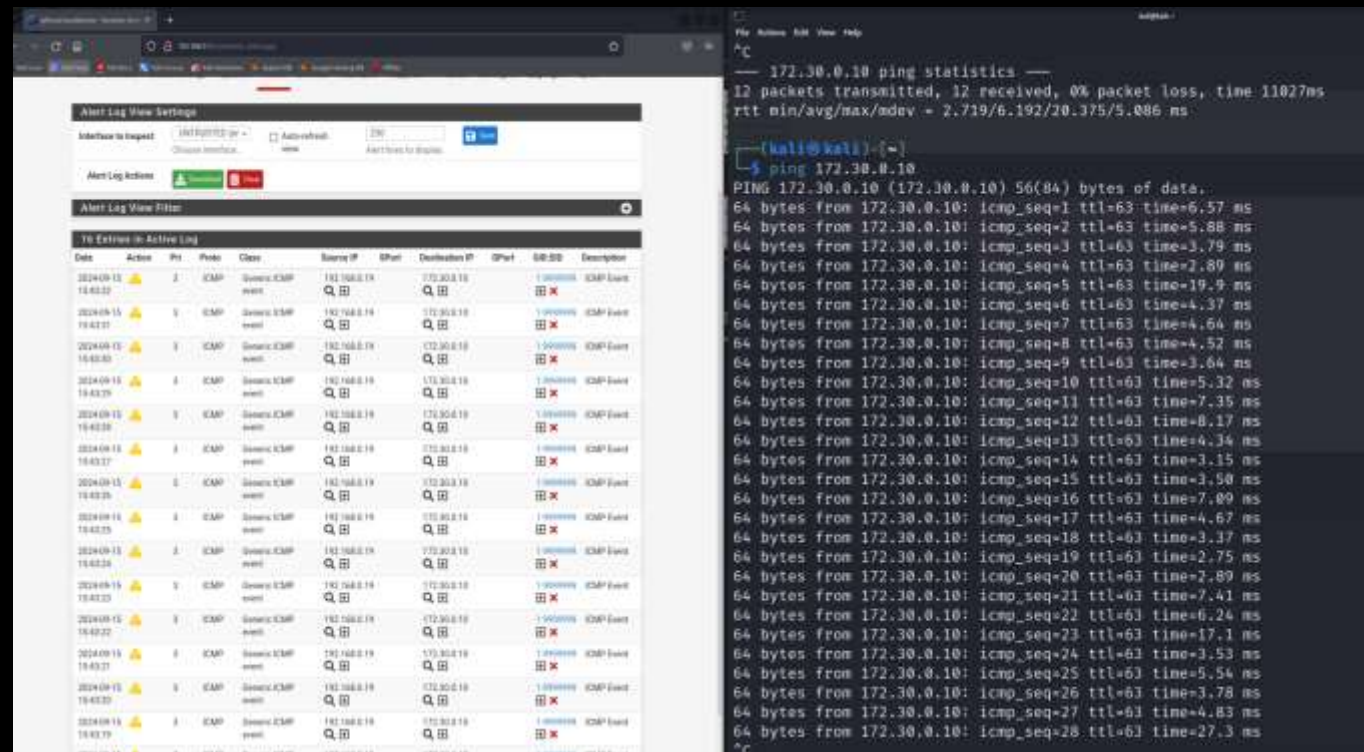
Category Selection: custom.rules
Select the rule category to view and manage.

Defined Custom Rules

```
alert tcp any any -> 10.200.0.0/29 21 (msg:"ALERT: YSETPS Backdoor Attempt"; flow:to_server,established; content:
alert tcp any any -> 10.200.0.0/29 21 (msg:"Blocking FTP Traffic from untrusted to DMZ"; sid:100001; rev:1; )
```

Save Cancel Clear

log suspicious activity on the Untrusted interface



The image displays two side-by-side screenshots. The left screenshot shows the 'Alert Log View Settings' and 'Alert Log View Filter' sections of a network security monitoring interface. Below these, a table titled '16 Entries in Active Log' lists detected alerts. The right screenshot shows a terminal window with the output of a ping command from a Kali Linux machine to 172.30.0.10, showing successful connectivity with 0% packet loss.

Alert Log View Settings

Interface to inspect: Auto-refresh: ☐ Alert log to display:

Alert Log View Filter

16 Entries in Active Log

Date	Action	Port	Proto	Class	Source IP	SPort	Destination IP	DPort	SID	Description
2024-09-15 14:02:02	Alert	8	ICMP	Generic ICMP event	172.30.0.10	Q	172.30.0.10	Q	1	ICMP Event
2024-09-15 14:02:03	Alert	8	ICMP	Generic ICMP event	172.30.0.10	Q	172.30.0.10	Q	1	ICMP Event
2024-09-15 14:02:04	Alert	8	ICMP	Generic ICMP event	172.30.0.10	Q	172.30.0.10	Q	1	ICMP Event
2024-09-15 14:02:05	Alert	8	ICMP	Generic ICMP event	172.30.0.10	Q	172.30.0.10	Q	1	ICMP Event
2024-09-15 14:02:06	Alert	8	ICMP	Generic ICMP event	172.30.0.10	Q	172.30.0.10	Q	1	ICMP Event
2024-09-15 14:02:07	Alert	8	ICMP	Generic ICMP event	172.30.0.10	Q	172.30.0.10	Q	1	ICMP Event
2024-09-15 14:02:08	Alert	8	ICMP	Generic ICMP event	172.30.0.10	Q	172.30.0.10	Q	1	ICMP Event
2024-09-15 14:02:09	Alert	8	ICMP	Generic ICMP event	172.30.0.10	Q	172.30.0.10	Q	1	ICMP Event
2024-09-15 14:02:10	Alert	8	ICMP	Generic ICMP event	172.30.0.10	Q	172.30.0.10	Q	1	ICMP Event
2024-09-15 14:02:11	Alert	8	ICMP	Generic ICMP event	172.30.0.10	Q	172.30.0.10	Q	1	ICMP Event
2024-09-15 14:02:12	Alert	8	ICMP	Generic ICMP event	172.30.0.10	Q	172.30.0.10	Q	1	ICMP Event
2024-09-15 14:02:13	Alert	8	ICMP	Generic ICMP event	172.30.0.10	Q	172.30.0.10	Q	1	ICMP Event
2024-09-15 14:02:14	Alert	8	ICMP	Generic ICMP event	172.30.0.10	Q	172.30.0.10	Q	1	ICMP Event
2024-09-15 14:02:15	Alert	8	ICMP	Generic ICMP event	172.30.0.10	Q	172.30.0.10	Q	1	ICMP Event
2024-09-15 14:02:16	Alert	8	ICMP	Generic ICMP event	172.30.0.10	Q	172.30.0.10	Q	1	ICMP Event

Terminal Output:

```
172.30.0.10 ping statistics ---
12 packets transmitted, 12 received, 0% packet loss, time 11027ms
rtt min/avg/max/mdev = 2.719/6.192/20.375/5.086 ms

(kali@kali) ~
$ ping 172.30.0.10
PING 172.30.0.10 (172.30.0.10) 56(84) bytes of data:
64 bytes from 172.30.0.10: icmp_seq=1 ttl=63 time=6.57 ms
64 bytes from 172.30.0.10: icmp_seq=2 ttl=63 time=5.88 ms
64 bytes from 172.30.0.10: icmp_seq=3 ttl=63 time=3.79 ms
64 bytes from 172.30.0.10: icmp_seq=4 ttl=63 time=2.89 ms
64 bytes from 172.30.0.10: icmp_seq=5 ttl=63 time=19.9 ms
64 bytes from 172.30.0.10: icmp_seq=6 ttl=63 time=4.37 ms
64 bytes from 172.30.0.10: icmp_seq=7 ttl=63 time=4.64 ms
64 bytes from 172.30.0.10: icmp_seq=8 ttl=63 time=4.52 ms
64 bytes from 172.30.0.10: icmp_seq=9 ttl=63 time=3.64 ms
64 bytes from 172.30.0.10: icmp_seq=10 ttl=63 time=5.32 ms
64 bytes from 172.30.0.10: icmp_seq=11 ttl=63 time=7.35 ms
64 bytes from 172.30.0.10: icmp_seq=12 ttl=63 time=8.17 ms
64 bytes from 172.30.0.10: icmp_seq=13 ttl=63 time=4.34 ms
64 bytes from 172.30.0.10: icmp_seq=14 ttl=63 time=3.15 ms
64 bytes from 172.30.0.10: icmp_seq=15 ttl=63 time=3.98 ms
64 bytes from 172.30.0.10: icmp_seq=16 ttl=63 time=7.09 ms
64 bytes from 172.30.0.10: icmp_seq=17 ttl=63 time=4.67 ms
64 bytes from 172.30.0.10: icmp_seq=18 ttl=63 time=3.37 ms
64 bytes from 172.30.0.10: icmp_seq=19 ttl=63 time=2.75 ms
64 bytes from 172.30.0.10: icmp_seq=20 ttl=63 time=2.89 ms
64 bytes from 172.30.0.10: icmp_seq=21 ttl=63 time=7.41 ms
64 bytes from 172.30.0.10: icmp_seq=22 ttl=63 time=6.24 ms
64 bytes from 172.30.0.10: icmp_seq=23 ttl=63 time=17.1 ms
64 bytes from 172.30.0.10: icmp_seq=24 ttl=63 time=3.53 ms
64 bytes from 172.30.0.10: icmp_seq=25 ttl=63 time=5.54 ms
64 bytes from 172.30.0.10: icmp_seq=26 ttl=63 time=3.78 ms
64 bytes from 172.30.0.10: icmp_seq=27 ttl=63 time=4.83 ms
64 bytes from 172.30.0.10: icmp_seq=28 ttl=63 time=27.3 ms
^C
```

log suspicious activity on the DMZ interface

Alert Log View: Settings

Interface to Ingest:

OSSEC (syslog)

Auto refresh:

250

Save

Alert Log Activity

Add

Refresh

Alert Log View Filter

81 Entries in Active Log

Date	Action	IP	Proto	Class	Source IP	S-Port	Destination IP	D-Port	SID:SE	Description
2004-09-15 16:12:12			TCP	Web Application Attack	192.168.8.19	52276	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:13			TCP	Web Application Attack	192.168.8.19	52280	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:13			TCP	Web Application Attack	192.168.8.19	52186	10.200.8.12	8080	12024864 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:13			TCP	Web Application Attack	192.168.8.19	52176	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:13			TCP	Web Application Attack	192.168.8.19	52186	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:13			TCP	Web Application Attack	192.168.8.19	52186	10.200.8.12	8080	12024864 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:12			TCP	Web Application Attack	192.168.8.19	52186	10.200.8.12	8080	12024864 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52182	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024864 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11			TCP	Web Application Attack	192.168.8.19	52180	10.200.8.12	8080	12024854 ID X	ET SCAN Possible Nmap User-Agent Observed
2004-09-15 16:12:11										

```
64 bytes from 10.200.0.9: icmp_seq=6 ttl=64 time=2.89 ms
64 bytes from 10.200.0.9: icmp_seq=7 ttl=64 time=1.91 ms
64 bytes from 10.200.0.9: icmp_seq=8 ttl=64 time=2.65 ms
64 bytes from 10.200.0.9: icmp_seq=9 ttl=64 time=2.31 ms
64 bytes from 10.200.0.9: icmp_seq=10 ttl=64 time=2.58 ms
64 bytes from 10.200.0.9: icmp_seq=11 ttl=64 time=2.80 ms
64 bytes from 10.200.0.9: icmp_seq=12 ttl=64 time=3.25 ms
64 bytes from 10.200.0.9: icmp_seq=13 ttl=64 time=2.36 ms
64 bytes from 10.200.0.9: icmp_seq=14 ttl=64 time=2.32 ms
64 bytes from 10.200.0.9: icmp_seq=15 ttl=64 time=3.35 ms
64 bytes from 10.200.0.9: icmp_seq=16 ttl=64 time=3.09 ms
64 bytes from 10.200.0.9: icmp_seq=17 ttl=64 time=3.85 ms
64 bytes from 10.200.0.9: icmp_seq=18 ttl=64 time=2.59 ms
64 bytes from 10.200.0.9: icmp_seq=19 ttl=64 time=2.49 ms
64 bytes from 10.200.0.9: icmp_seq=20 ttl=64 time=2.92 ms
64 bytes from 10.200.0.9: icmp_seq=21 ttl=64 time=1.78 ms
64 bytes from 10.200.0.9: icmp_seq=22 ttl=64 time=2.88 ms
64 bytes from 10.200.0.9: icmp_seq=23 ttl=64 time=8.49 ms
64 bytes from 10.200.0.9: icmp_seq=24 ttl=64 time=1.48 ms
64 bytes from 10.200.0.9: icmp_seq=25 ttl=64 time=1.50 ms
64 bytes from 10.200.0.9: icmp_seq=26 ttl=64 time=2.32 ms
^C
```

```

— 10.200.0.9 ping statistics —
26 packets transmitted, 26 received, 0% packet loss, time 2510ms
rtt min/avg/max/mdev = 1.456/2.783/8.488/1.337 ms

```

```
(kali@kali)-[~]  
$ nmap -sS 10.200.0.10
```

```
You requested a scan type which requires root privileges.
QUITTING!
```

```
(kali@kali)~$ nmap -script=wulf 10.200.0.8/29
Starting Nmap 7.92 ( https://nmap.org ) at 2024-09-15 17:11 EDT
```


Snort to alert to Web Server port(21) exploit

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

Services / Snort / Alerts

Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists BD Mgmt Log Mgmt Sync

Alert Log View Settings

Interface to inspect: DMZ (em1) Auto-refresh view: 250 Alert lines to display: Save

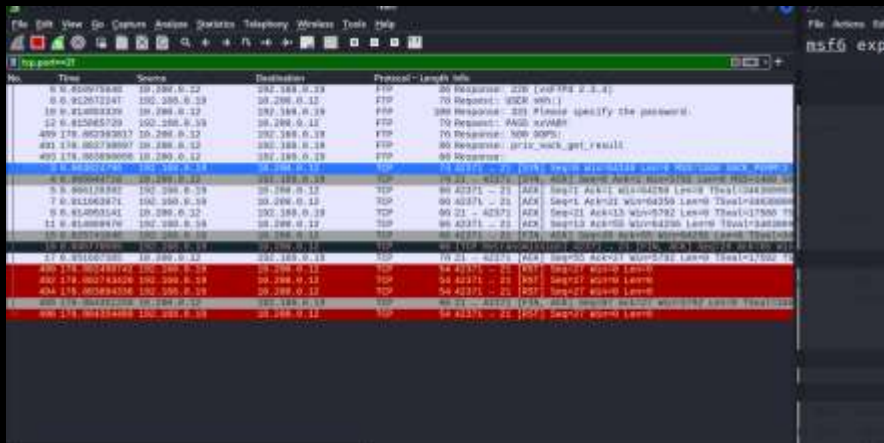
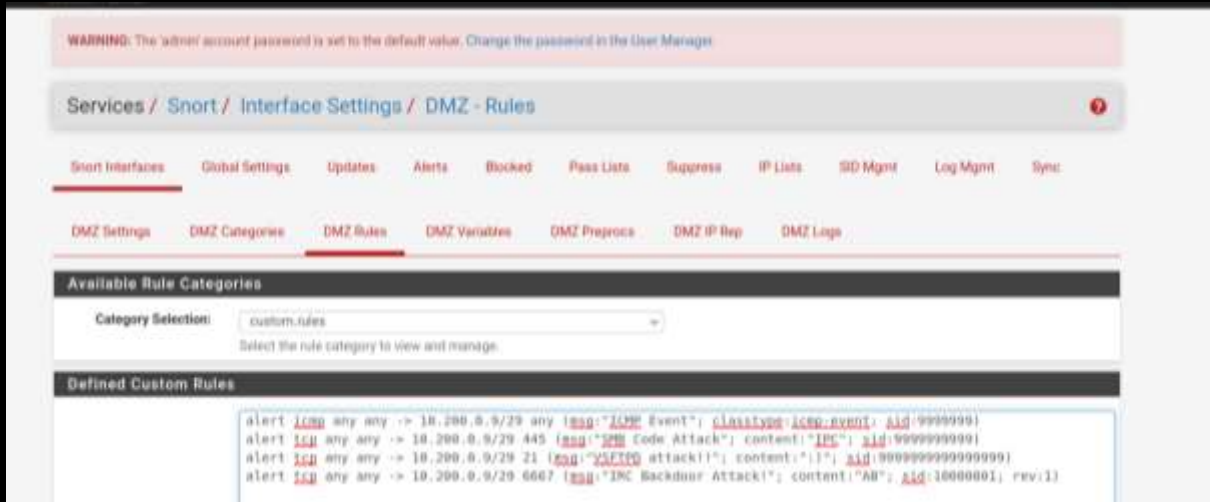
Alert Log Actions: Download Clear

Alert Log View Filter: 0

104 Entries in Active Log

Date	Action	Pt	Proto	Class	Source IP	SPort	Destination IP	DPort	OID:SID	Description
2024-09-21 21:01:43	⚠	0	TCP		192.168.0.19	34163	10.200.0.12	21	1:10000002	ALERT: VSFTPD Backdoor Attempt
2024-09-21 21:12:13	⚠	0	TCP		192.168.0.19	43207	10.200.0.12	21	1:10000002	ALERT: VSFTPD Backdoor Attempt
2024-09-21 21:02:55	⚠	0	TCP		192.168.0.19	38641	10.200.0.12	21	1:10000002	ALERT: VSFTPD Backdoor Attempt
2024-09-21 13:07:23	⚠	0	TCP		192.168.0.19	43947	10.200.0.12	21	1:10000002	ALERT: VSFTPD Backdoor Attempt
2024-09-15 16:12:12	⚠	1	TCP	Web Application Attack	192.168.0.19	42078	10.200.0.12	80	1:3024264	ET SCAN Possible Nmap User-Agent Observed
2024-09-15 16:13:02	⚠	1	TCP	Web Application Attack	192.168.0.19	50652	10.200.0.12	80	1:3024264	ET SCAN Possible Nmap User-Agent Observed
2024-09-15	⚠	1	TCP	Web Application	192.168.0.19	50642	10.200.0.12	80	1:3024264	ET SCAN Possible Nmap User-Agent

```
msf6 exploit(unix/ftp/vsftpd_23k_backdoor) > exploit
[*] 10.200.0.12:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 10.200.0.12:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_23k_backdoor) >
```



FIREWALL RULES TO BLOCK FTP TRAFFIC

Recommendations to improve server security



Keep Systems and
Software Updated



Enable and
Configure a Firewall



Secure Remote
Access



Implement Regular
Security Audits and
Monitoring



Implement Security
Policies and Training



Regular Backups
and Disaster
Recovery



Closing Remark

- Completing this project determine the capability to secure network infrastructures by implementing firewalls, configuring an IDS/IPS with Snort, and blocking specific network traffic to prevent unauthorized access. Here we learn some lessons in monitoring and analyzing traffic and creating some rules to detect and respond to potentials threats. Regular updates, security measures and continuous monitoring will help continuing protection of our systems.

