

Vu Nguyen

UID: u1483046

Assignment 6 - PANEDU 05B – CONTENT ID (Lab and Quiz)

1. Section 1.3, Step 4

The screenshot shows the Palo Alto Networks Panorama interface. The left sidebar displays the navigation menu with options like Logs, Traffic, Threat, and Policy. The main pane shows a list of logs with columns for Receive Time, Type, Name, From Zone, To Zone, Source address, Source User, Destination address, To Port, Application, Action, Severity, File Name, URL, and HTTP/2 Connection Session ID. A detailed log view is open, showing a packet capture of an FTP login attempt. The packet details include the source IP (192.168.1.20), destination IP (192.168.1.20), and the application (FTP). The log entry shows a vulnerability type of 'FTP Login Brute Force attempt' with a severity of 'High'.

2. Section 1.4, Step 7

The screenshot shows the Palo Alto Networks Panorama interface. The left sidebar displays the navigation menu with options like Logs, Traffic, Threat, and Policy. The main pane shows a list of logs with columns for Receive Time, Type, Name, From Zone, To Zone, Source address, Source User, Destination address, To Port, Application, Action, Severity, File Name, URL, and HTTP/2 Connection Session ID. The logs show multiple entries for 'FTP Login Brute Force attempt' with a severity of 'High'. The log entry shows a vulnerability type of 'FTP Login Brute Force attempt' with a severity of 'High'.

3. Section 1.5, Step 14

David Eccles School of Business THE UNIVERSITY OF UTAH

MyNETLAB > PAN 9 Firewall Essentials POD 2 > Reservation 68778 > Lab 05-B: Content-ID

Topology Content Status Client Firewall DMZ VRouter

Time Remaining 3 25 hrs. min.

192.168.1.254/#policies/vsys1/policies/security-rulebase

paloalto

Dashboard ACC Monitor Policies Objects Network Device

Security

Policy Based Forwarding

Decryption

Tunnel Inspection

Application Override

Authentication

DoS Protection

Policy Objects

Unused Apps

Unused in 30 days

Unused in 90 days

Unused

Name	Tags	Type	Zone	Address	User	HP Profile	Destination	Application	Service	Action	Profile	Options	Hit Count	Last Hit	Fi
1	egress-outside-internal	egress	universal	any	any	any	any	any	any	allow	none	none	-	-	-
2	egress-outside-internal	egress	universal	any	any	any	any	any	any	allow	none	none	0	-	-
3	internal-inside-dmz	internal	universal	any	any	any	any	any	any	allow	none	none	1120	2024-01-23 23:24:34	20
4	intrazone-default	none	intrazone	any	any	any	any	any	any	allow	none	none	13	2024-01-23 23:17:37	20
5	intrazone-default	none	intrazone	any	any	any	any	any	any	deny	none	none	582	2024-01-23 23:26:40	20

Object: Addresses

Add Delete Clone Overwrite Reset Enable Disable Move PDF/CSV Highlight Unused Rules Repeat Rule Hit Counter Group View Rulebase as Groups Test Policy Match

admin | Logout | Last Login Time 01/12/2024 20:49:50

23:24 1/23/2024

4. Section 1.8, Step 5

David Eccles School of Business THE UNIVERSITY OF UTAH

MyNETLAB > PAN 9 Firewall Essentials POD 2 > Reservation 68778 > Lab 05-B: Content-ID

Topology Content Status Client Firewall DMZ VRouter

Time Remaining 3 11 hrs. min.

192.168.1.254/#monitor/vsys1/monitor/logs/data-filtering

paloalto

Dashboard ACC Monitor Policies Objects Network Device

Manual

Logs

Traffic

Threat

URL Filtering

Wildfire Submissions

Data Filtering

IP Match

IP Tag

User-ID

Tunnel Inspection

Configuration

System

Alarms

Authentication

Unified

Packet Capture

App Scope

Summary

Change Monitor

Threat Monitor

Threat Map

Network Monitor

Traffic Map

Session Browser

Botnet

PDF Reports

Message PDF Summary

User Activity Report

Outpost Authentication Events

Receive Time	Category	File Name	File URL	Name	From Zone	To Zone	Source address	Source User	Destination address	To Port	Application	Action	HTTP2 Connection Session ID
01/23 23:38:08	any	pan-os-SR-Admin...		Adobe Portable Document Format (PDF)	inside	outside	192.168.1.25		45.60.226.178	80	web-browsing	deny	0

admin | Logout | Last Login Time 01/12/2024 20:49:50

23:38 1/23/2024

5. Section 1.17, Step 4

MyNETLAB > PAN 9 Firewall Essentials POD 2 > Reservation 68778 > Lab 05-B: Content-ID

Time Remaining

2
hrs.
54
min.

Topology Content Status Client Firewall DMZ VRouter

firewall-a

https://192.168.1.254/#monitorcvsys1:monitor/logs/threat

paloalto

Dashboard ACC Monitor Policies Objects Network Device

Commit Config Search

- Logs
- Traffic
- Threat
- URL Filtering
- Wildfire Submissions
- Data Filtering
- ADP Match
- IP-Tag
- User-ID
- Tunnel Inspection
- Configuration
- System
- Alarms
- Authentication
- Unified
- Packet Capture
- App Scope
- Summary
- Change Monitor
- Threat Monitor
- Treat Map
- Network Monitor
- Traffic Map
- Session Browser
- Bitnet
- PDF Reports
- Manage PDF Summary
- User Activity Report
- Go to: Authentication Issues

(severity req informational)																
Receive Time	Type	Name	From Zone	To Zone	Source address	Source User	Destination address	To Port	Application	Action	Severity	File Name	URL	HTTP/2 Connection Session ID		
01/23 23:51:35	vulnerability	Trojan-Win32.sword.fmap	danger	danger	10.10.10.10		192.168.1.121	25	smtp	reset both	high	CV.Cindy.Nam.pdf		0		
01/23 23:51:35	vulnerability	Ransom-Win32.locky.pe	danger	danger	10.10.10.10		192.168.1.121	25	smtp	reset both	high	locky.exe		0		
01/23 23:47:01	vulnerability	Trojan-Win32.sword.fmap	danger	danger	10.10.10.10		192.168.1.121	25	smtp	reset both	high	CV.Cindy.Nam.pdf		0		
01/23 23:47:01	vulnerability	Ransom-Win32.locky.pe	danger	danger	10.10.10.10		192.168.1.121	25	smtp	reset both	high	locky.exe		0		
01/23 23:46:50	spyware	Brutalab.Gen.Command and Control Traffic	danger	danger	192.168.0.2		112.137.162.134	80	web-browsing	alert	critical	controller.php		0		
01/23 23:35:12	vulnerability	ISC BIND DNS DNS Options Denial of Service Vulnerability	inside	outside	192.168.1.20		8.8.8.8	53	dns	drop	high			0		
01/23 23:30:45	vulnerability	ISC BIND DNS DNS Options Denial of Service Vulnerability	inside	outside	192.168.1.20		8.8.8.8	53	dns	drop	high			0		
01/23 23:30:38	vulnerability	ISC BIND DNS DNS Options Denial of Service Vulnerability	inside	outside	192.168.1.20		8.8.8.8	53	dns	drop	high			0		
01/23 23:30:22	vulnerability	ISC BIND DNS DNS Options Denial of Service Vulnerability	inside	outside	192.168.1.20		8.8.8.8	53	dns	drop	high			0		
01/23 23:30:14	vulnerability	ISC BIND DNS DNS Options Denial of Service Vulnerability	inside	outside	192.168.1.20		8.8.8.8	53	dns	drop	high			0		
01/23 23:30:02	vulnerability	ISC BIND DNS DNS Options Denial of Service Vulnerability	inside	outside	192.168.1.20		8.8.8.8	53	dns	drop	high			0		
01/23 23:29:53	vulnerability	ISC BIND DNS DNS Options Denial of Service Vulnerability	inside	outside	192.168.1.20		8.8.8.8	53	dns	drop	high			0		

https://192.168.1.254/#



Displaying logs 1 - 20 per page DESC

Tools Language

23:55
1/29/2024