

Vu Nguyen

UID: u1483046

Assignment 13 - PANEDU 12 - Monitoring and Reporting (Lab and Quiz)

1. Section 1.2, Step 5

The screenshot displays the Palo Alto Networks Panorama interface. The top navigation bar includes 'Dashboard', 'ACC', 'Monitor', 'Policies', 'Objects', 'Network', and 'Device'. The 'Monitor' tab is active, and the 'Session Browser' is selected in the left-hand menu. The main pane shows a table of session logs with columns: Start Time, From Zone, To Zone, Source, Destination, From Port, To Port, Protocol, Application, Rule, Ingress I/F, Egress I/F, Bytes, Virtual System, and Clear. The table contains several rows of session data, including details for a session from 192.168.3.131 to 204.14.234.85. A 'Detail' pane on the right shows session information such as Session ID, Time To Live, Virtual System, Application, Protocol, Security Rule, QoS Class, To Host Session, Traversal Tunnel, Session End Log, and Session In Agent.

2. Section 1.4, Step 8

The screenshot displays the Palo Alto Networks Panorama interface. The top navigation bar includes 'Dashboard', 'ACC', 'Monitor', 'Policies', 'Objects', 'Network', and 'Device'. The 'Monitor' tab is active, and the 'Threat Activity' is selected in the left-hand menu. The main pane shows a table of threat activity logs with columns: Time, Severity, Application, and Risk. The table is currently empty, displaying 'No data to display'. The 'Threat Activity' pane on the right shows a list of threats, including 'Threat Activity' and 'Blocked Activity'.

3. Section 1.5, Step 15

David Eccles School of Business
THE UNIVERSITY OF UTAH

MyNETLAB > PAN 9 Firewall Essentials POD 2 > Reservation 69285 > Lab 12: Monitoring and Reporting

Topology Content Status Client Firewall DMZ VRouter

Time Remaining: 2 28 hrs. min.

firewall-a

192.168.1.254#monitor:sys1:monitor/logs/threat

paloalto

Dashboard ACC Monitor Policies Objects Network Device

Log In-Tag 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 Manage PDF Summary User Activity Report Packet Sniff/Inspection Source

Severity: msg informational

Receive Time	Type	Name
02/05 22:05:05	spware	BrakidLab Gen Command and Control Traffic
08/01 20:44:43	spware	Suspicious Domain
08/01 20:35:55	virus	Eicar Test File

Detailed Log View

General	Source	Destination
<p>Session ID: 212</p> <p>Action: alert</p> <p>Application: web-browsing</p> <p>Rule: danger-simulated-traffic</p> <p>Rule UUID: c2a3e64-5445-40b9-9137-9873105a0c0f</p> <p>Device SH: IP Protocol</p> <p>IP Protocol: tcp</p> <p>Log Action:</p> <p>Generated Time: 2024/02/05 22:05:05</p> <p>Receive Time: 2024/02/05 22:05:05</p> <p>Tunnel Type: N/A</p>	<p>Source User: labjgblm</p> <p>Source: 192.168.0.2</p> <p>Country: 192.168.0.2</p> <p>Port: 1038</p> <p>Zone: danger</p> <p>Interface: ethernet1/4</p>	<p>Destination User: 112.137.162.134</p> <p>Destination: 112.137.162.134</p> <p>Port: 80</p> <p>Zone: danger</p> <p>Interface: ethernet1/5</p>

Details

Threat Type	Threat Name
spware	BrakidLab Gen Command and Control Traffic

PCAP	Receive Time	Type	Application	Action	Rule	Rule UUID	Bytes	Severity	Catag	URL Catag	Verdict	URL	File Name
	2024/02/05 22:05:05	spware	web-browsing	alert	danger-simulated-traffic	c2a3e64-5445-40b9-9137-9873105a0c0f		critical	any				contro...

Displaying logs 1 - 3

2021 3/6/2024

4. Section 1.7, Step 6

David Eccles School of Business
THE UNIVERSITY OF UTAH

MyNETLAB > PAN 9 Firewall Essentials POD 2 > Reservation 69285 > Lab 12: Monitoring and Reporting

Topology Content Status Client Firewall DMZ VRouter

Time Remaining: 2 18 hrs. min.

firewall-a

192.168.1.254#monitor:sys1:monitor/custom-reports

paloalto

Dashboard ACC Monitor Policies Objects Network Device

Log In-Tag 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 Manage PDF Summary User Activity Report SaaS Application Usage Report Groups Email Scheduler Manage Custom Reports Reports

Custom Report

Report Setting: top-applications (100%)

Application	Rule	Bytes	URLs	Sessions
1 dns	egress-outside	88.6K	0	267
2	egress-outside content-id	16.7K	0	51
3 google-base	egress-outside	612.5K	0	128
4	egress-outside content-id	1.5M	0	13
5	danger-simulated-traffic	45.9K	0	1
6 paloalto-updates	egress-outside	281.9K	0	30
7	egress-outside content-id	57.7K	0	6
8 paloalto-wildfire-cloud	egress-outside	402.7K	0	28
9 web-browsing	internal-inside dns	12.2K	0	12
10	danger-simulated-traffic	223.1K	0	5

Export to PDF Export to CSV Export to XML

OK Cancel

20240205_2231_re...pdf user-activity-report.pdf

2021 3/6/2024

5. Section 1.9, Step 5

David Eccles School of Business
THE UNIVERSITY OF UTAH

Home Reservation u1483046@utah.edu

MyNETLAB > PAN 9 Firewall Essentials POD 2 > Reservation 69285 > Lab 12: Monitoring and Reporting

Topology Content Status Client Firewall DMZ VRouter

Time Remaining
2 13
hrs. min.

192.168.1.254/#monitor:veys1:monitor/pdf-reports/email-scheduler

paloalto

Dashboard ACC Monitor Policies Objects Network Device

Control Config Search

Help

IP-Tag
User-ID
Tunnel Inspection
Configuration
System
Alarms
Authentication
Unidirectional
Packet Capture
App Scope
Summary
Change Monitor
Threat Monitor
Threat Map
Network Monitor
Traffic Map
Session Browser
Botnet
PDF Reports
Manage PDF Summary
User Activity Report
SaaS Application Usage
Report Groups
Email Scheduler
Manage Custom Reports
Reports

Email Profile

Name lab-sntp-profile

Servers Custom Log Format

Name	Email Display Name	From	To	Additional Recipient	Email Gateway
lab-sntp	Palo Alto Networks EDU Admin	edu-lab-admin@paloaltohawaii.edu	u1483046@utah.edu		192.168.1.20

Add Delete

Enter the IP address or FQDN of the Email gateway

OK Cancel

views | Legend | Last Login Time: 05/08/2024 12:01:02

20240205_2231_re...pdf user-activity-report.pdf

Show all X

20:36 2/9/2024