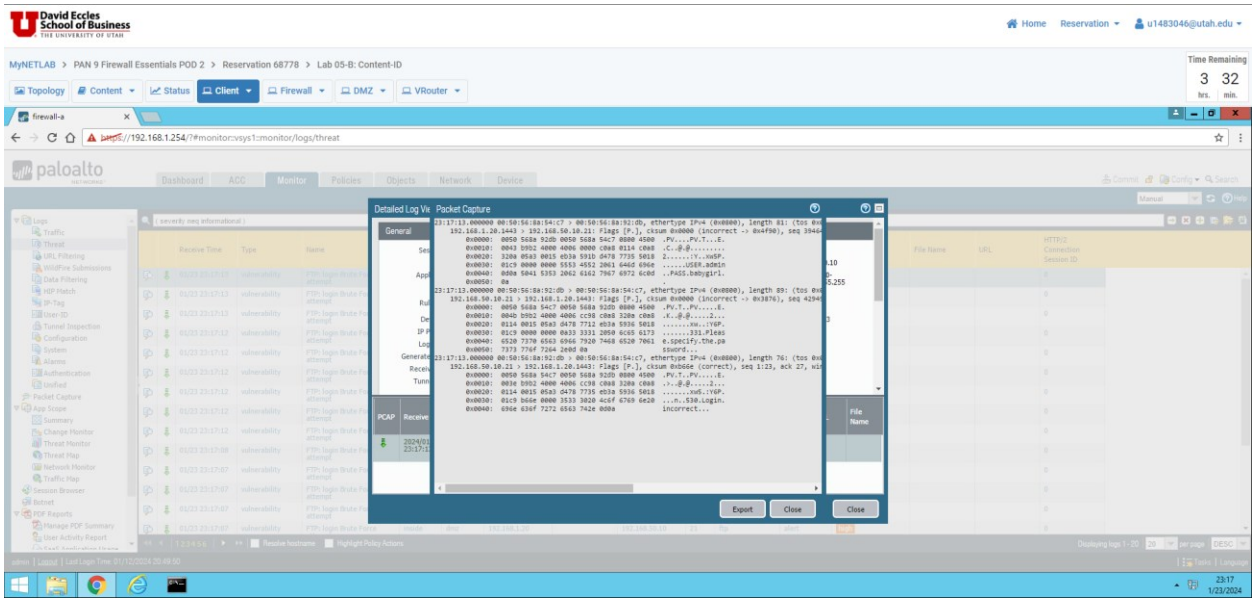
Vu Nguyen

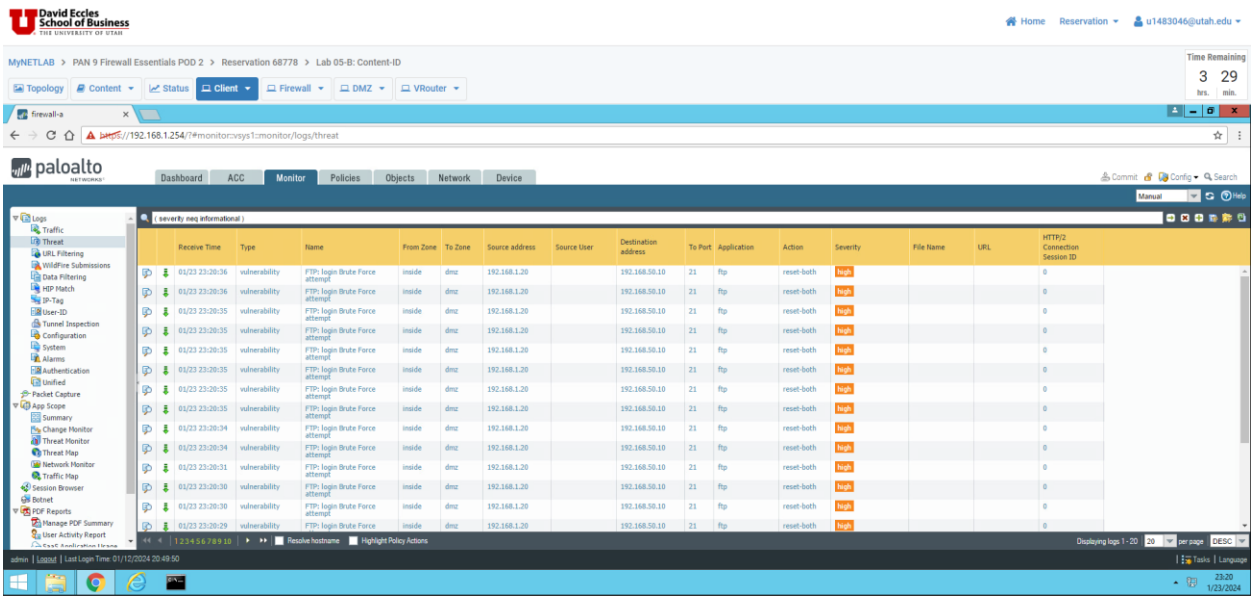
UID: u1483046

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

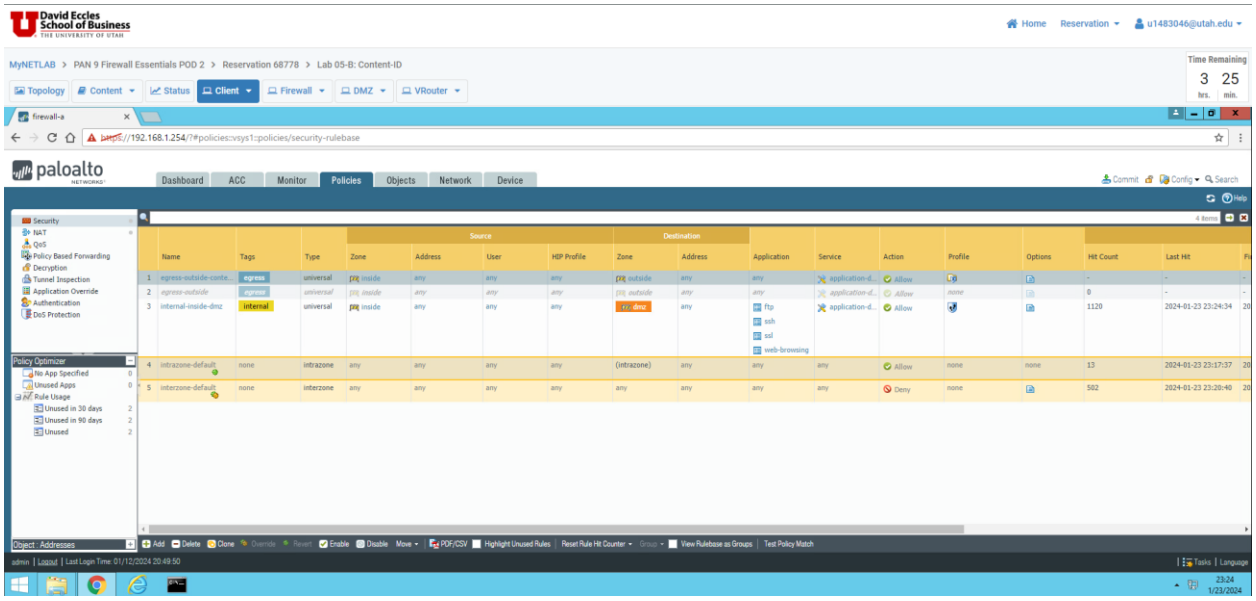
1. Section 1.3, Step 4



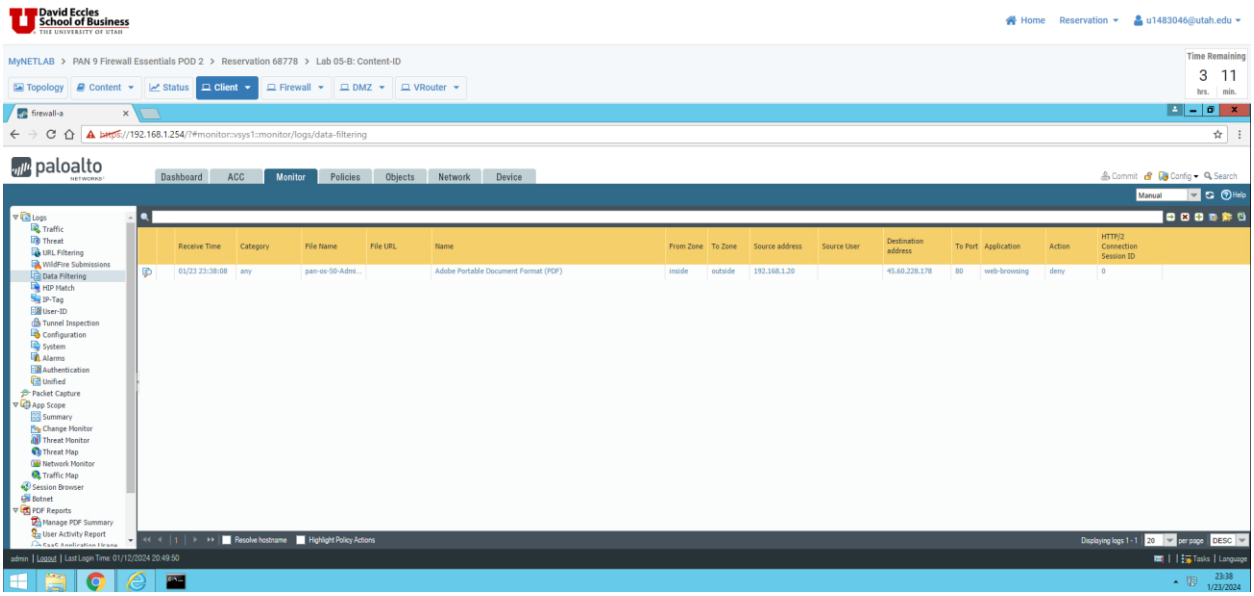
2. Section 1.4, Step 7



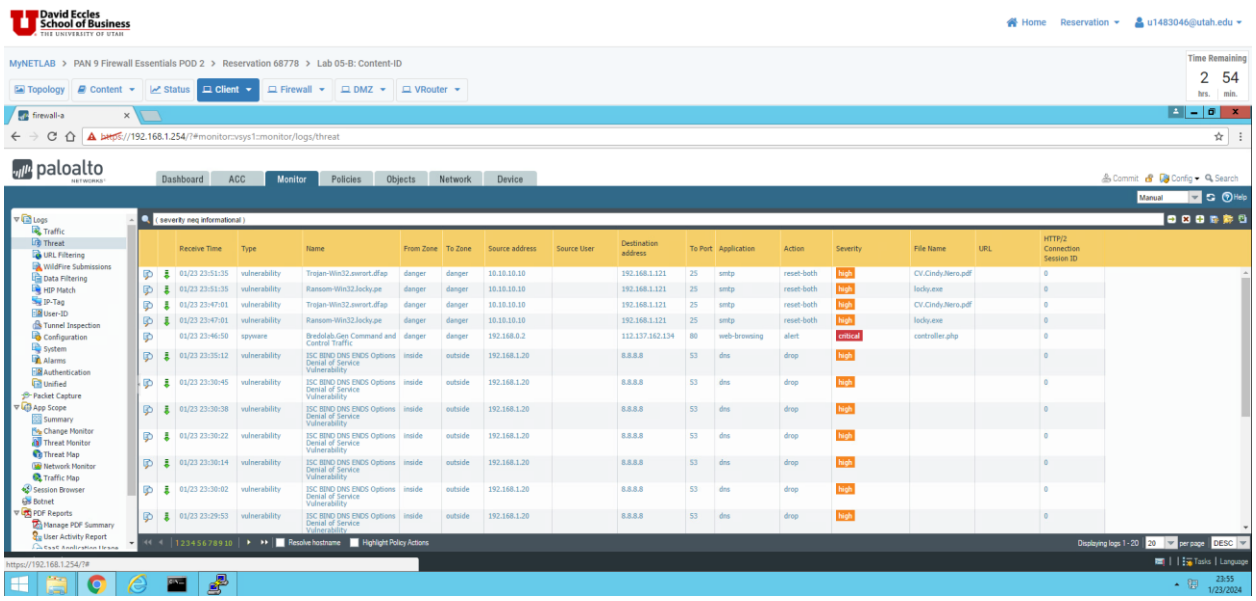
3. Section 1.5, Step 14



4. Section 1.8, Step 5



5. Section 1.17, Step 4


David Eccles School of Business
THE UNIVERSITY OF UTAH
Home
Reservation
u1483046@utah.edu
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/?#monitor:vsys1::monitor/logs/threat
paloalto
Dashboard
ACC
Monitor
Policies
Objects
Network
Device
Commit
Config
Search
Manual
Help
(severity neq informational)
Logs
Traffic
Threat
URL Filtering
WildFire Submissions
Data Filtering
HIP 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
Manage PDF Summary
User Activity Report
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.swrort.dfap danger danger 10.10.10.10 192.168.1.121 25 smtp reset-both high CV.Cindy.Nero.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.swrort.dfap danger danger 10.10.10.10 192.168.1.121 25 smtp reset-both high CV.Cindy.Nero.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 Bredolab.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 ENDS 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 ENDS 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 ENDS 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 ENDS 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 ENDS 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 ENDS 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 ENDS Options Denial of Service Vulnerability inside outside 192.168.1.20 8.8.8.8 53 dns drop high 0
1 2 3 4 5 6 7 8 9 10
Resolve hostname
Highlight Policy Actions
Displaying logs 1-20
20
per page
DESC
Tasks
Language
23:55
1/23/2024