Student: Sunil Tiwari

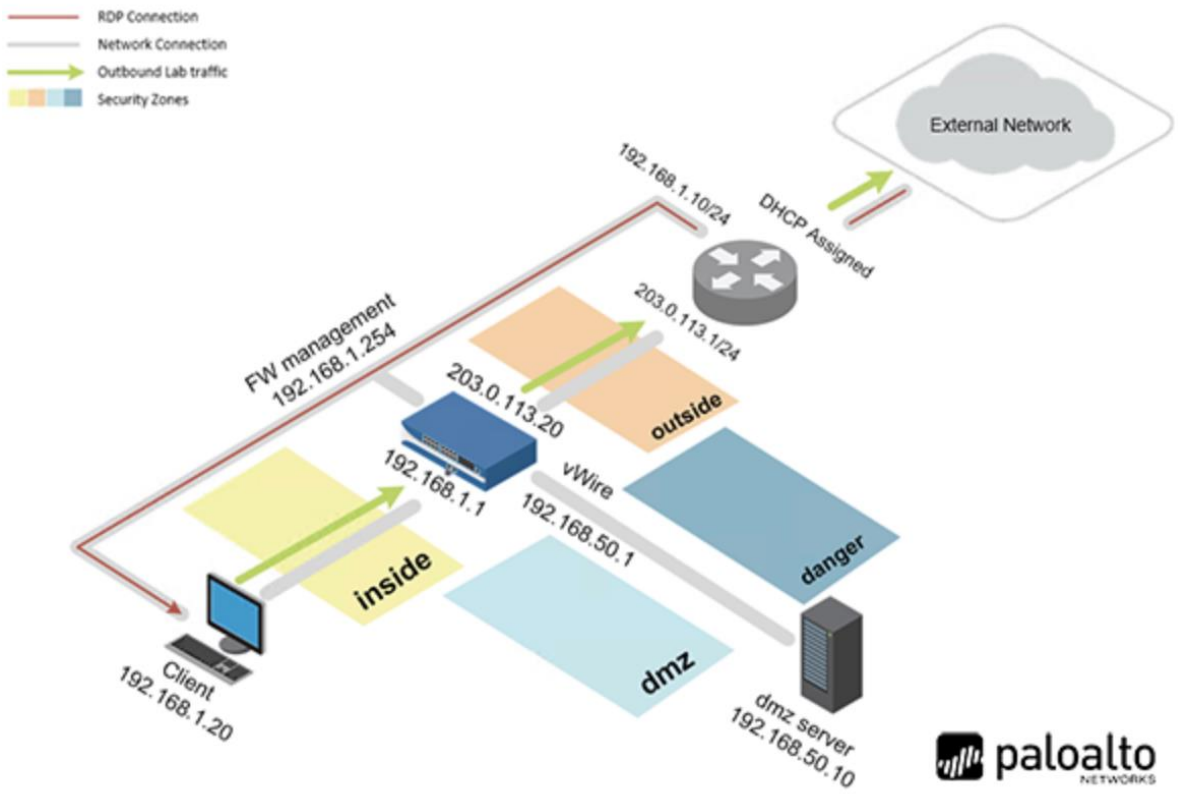
Lab: PANEDU 05B - Content-ID

Date: September 4th, 2025

Objective:

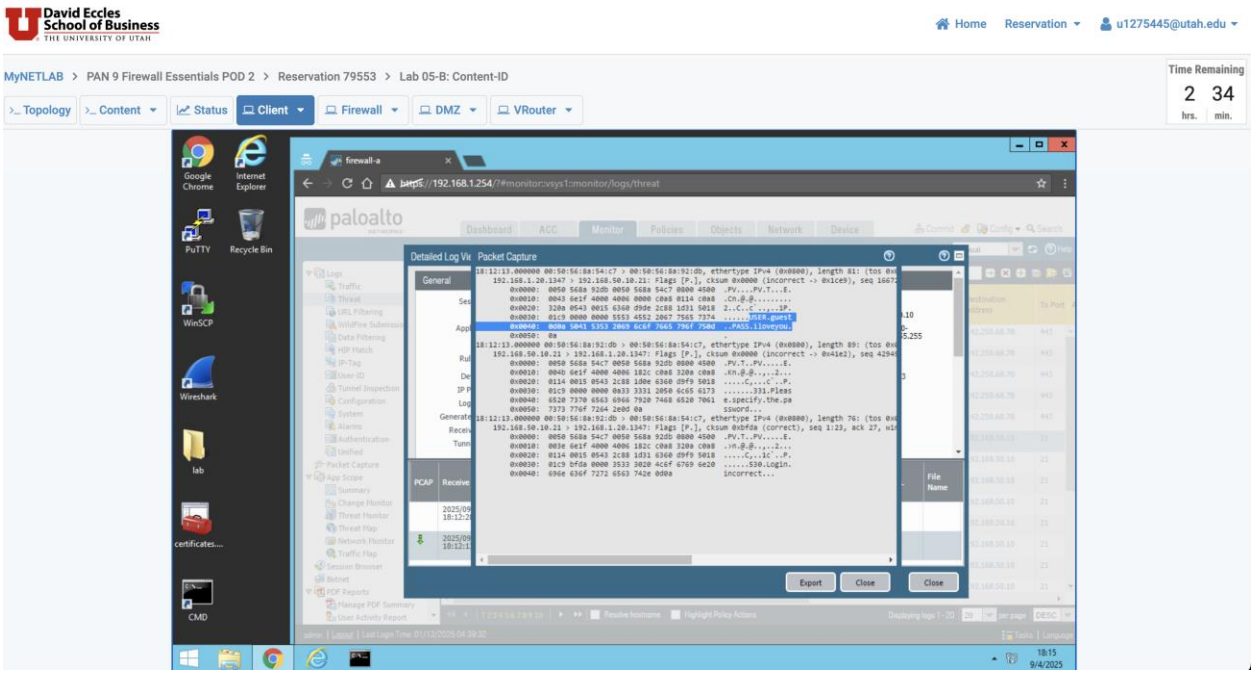
1. Configure and test a Vulnerability Security Profile
2. Configure and test a File Blocking Security Profile
3. Use the Virtual Wire mode and configure the danger zone
4. Generate threats and observe the actions taken

Topology:



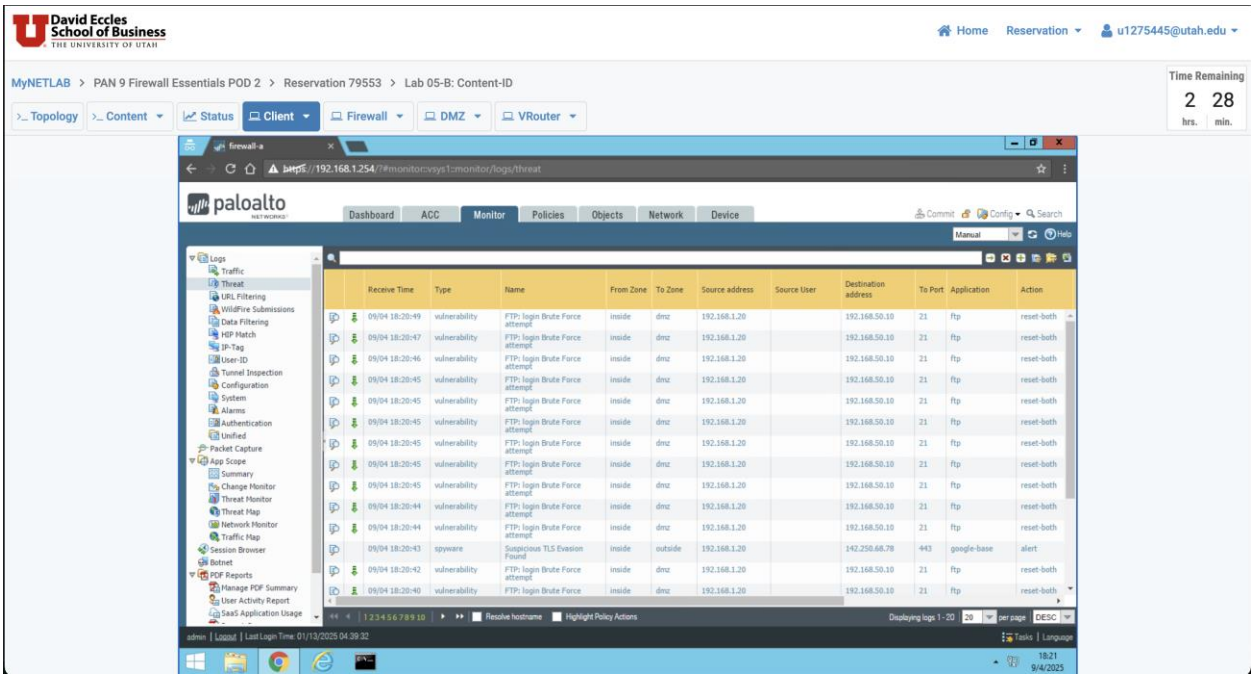
Section 1.3 — Review the Logs

Step 4



Section 1.4 — Update the Vulnearabiity Profile

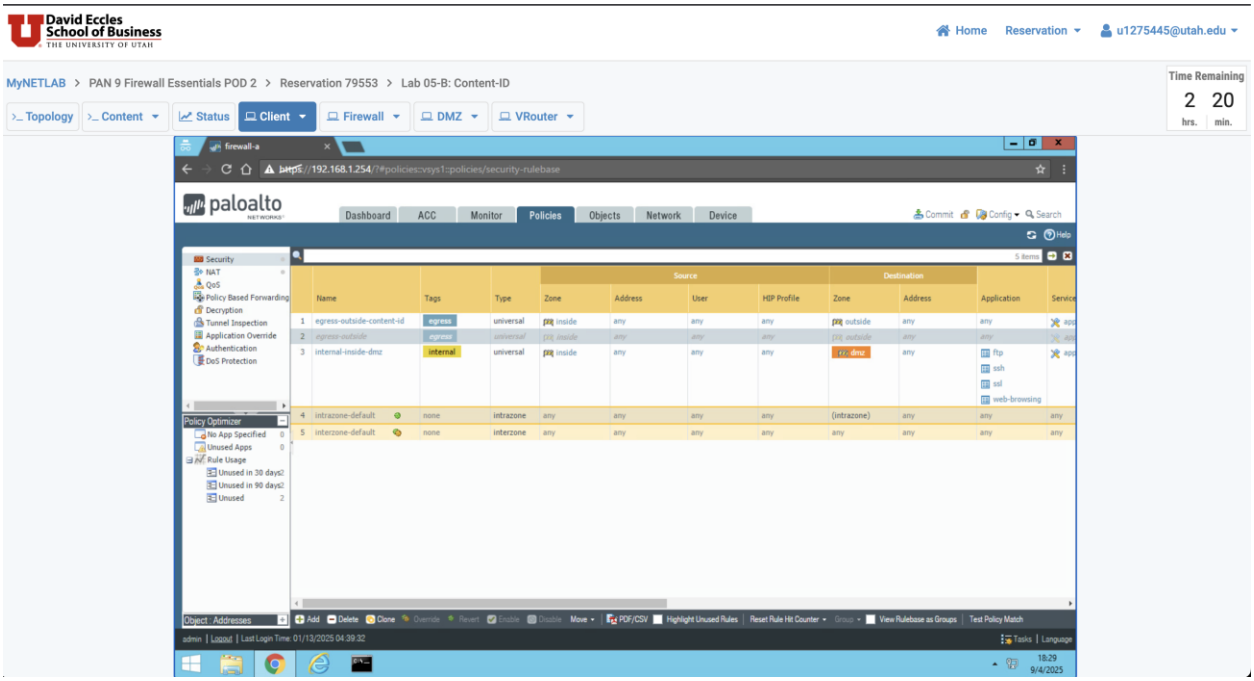
Step 7: Reran the ftp-brute.bat script to initiate new FTP brute force attempts. Monitored and reviewed the logs to verify that the attack attempts were successfully reset. The script was allowed to run for a minimum of one minute.



Section 1.5 — Create a Security Profile Groups — Specifies set of Security Profiles that can

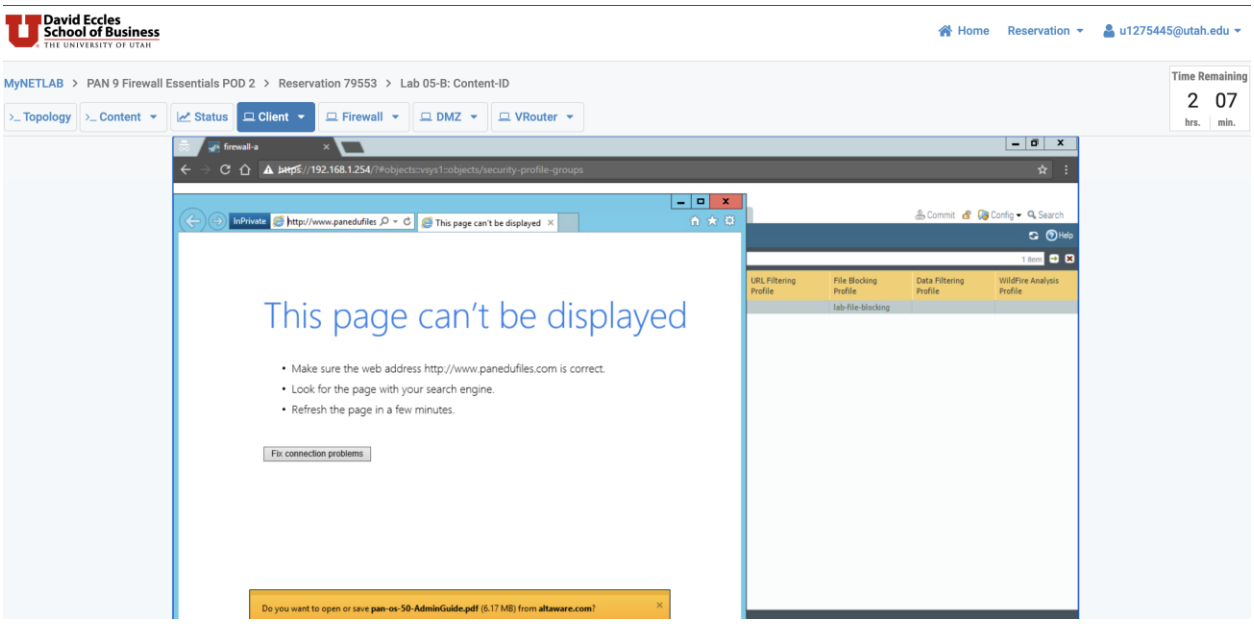
be treated as a unit and then added to a Security Profile Rules.

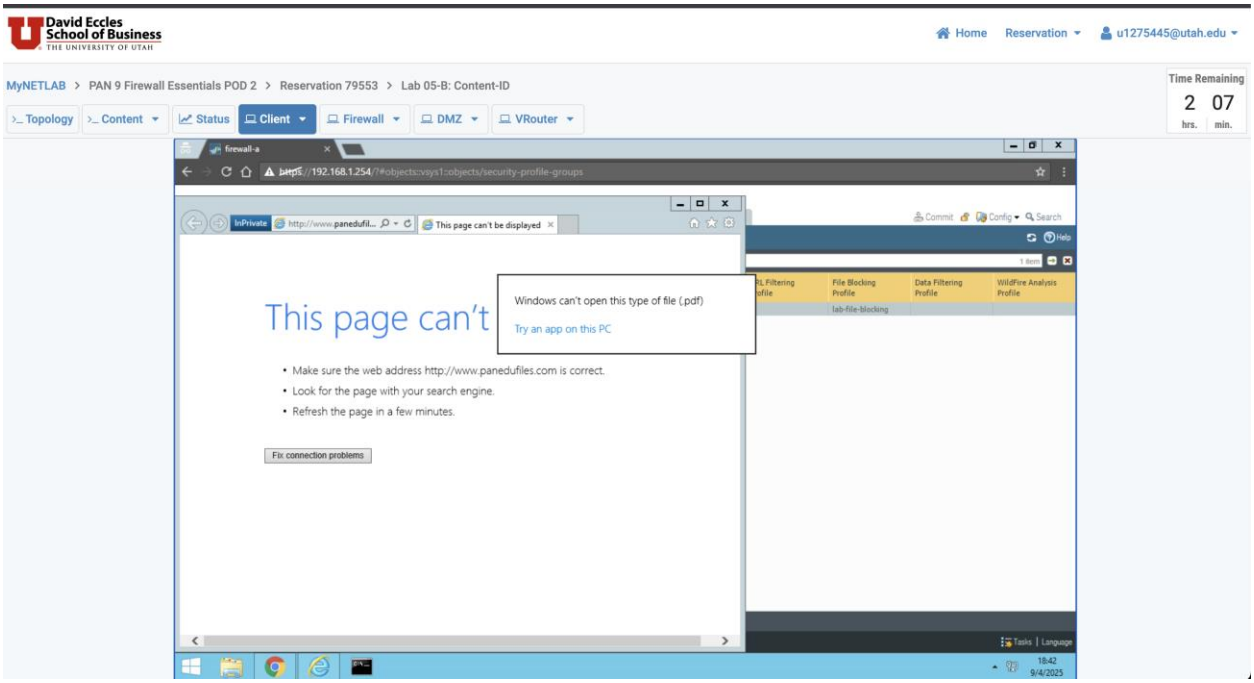
Step 14



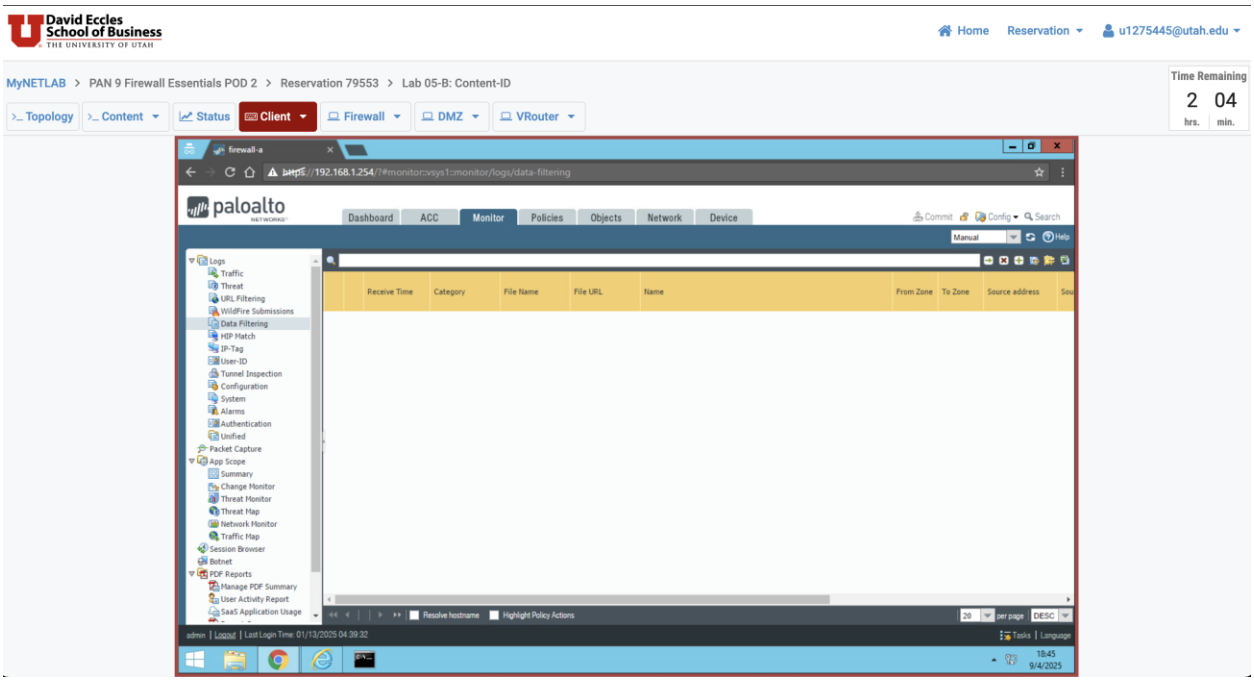
Section 1.8 —

Step 5: Created a File Blocking rule for pdf file and upon trying to download the file from the site: http://www.panedufiles.com, the system blocked the pdf file download.





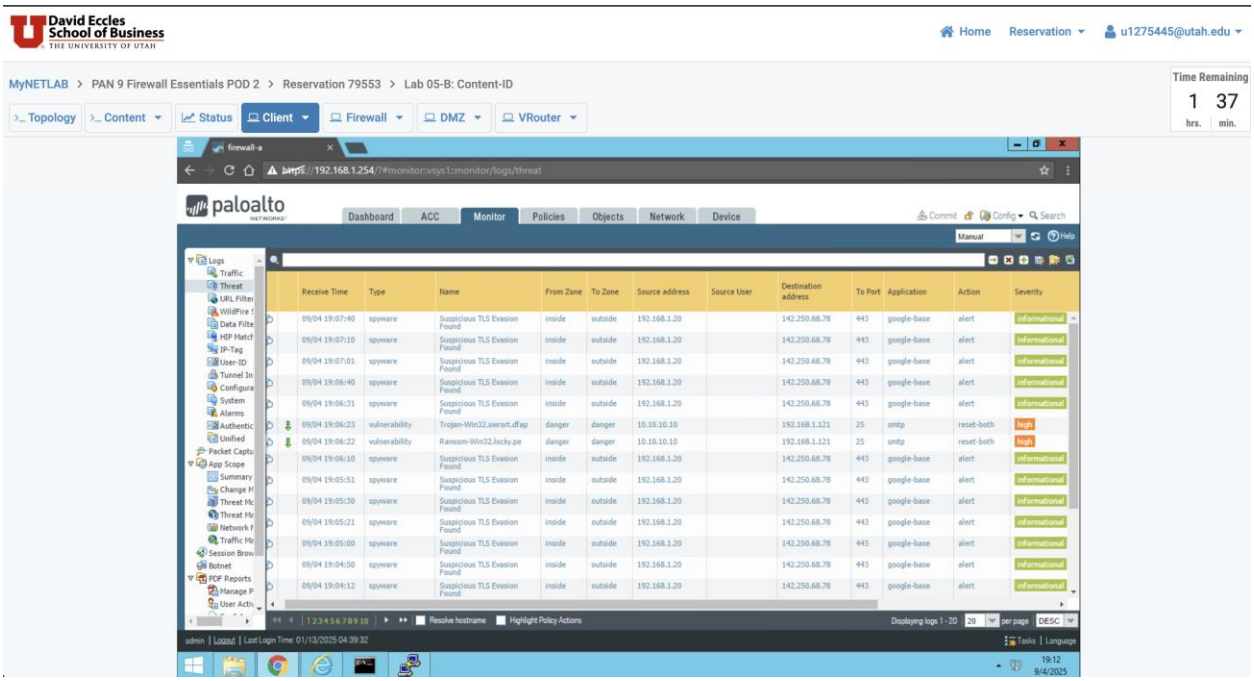
Per the lab instructions, if this scenario were performed in a real-world environment, the firewall would be expected to block the PDF download and log the event. However, since this is a virtual lab, I encountered an internet connection error while accessing the download site and was therefore unable to capture the logs, as shown below.



Section 1.17 —

For this step, I modified the Security Profile Group lab-spg by setting the file-blocking profile action to “None.” As a result, when executing the command sh /tg/malware.sh from putty-traffic-detection, the firewall allowed the file transfer, but still detected and blocked actions based on the identified severity-threat type. The relevant logs were successfully captured, as shown below.

Step 4


David Eccles School of Business
THE UNIVERSITY OF UTAH
Home
Reservation
u1275445@utah.edu
MyNETLAB > PAN 9 Firewall Essentials POD 2 > Reservation 79553 > Lab 05-B: Content-ID
Time Remaining
1 hrs.
37 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
Logs
Traffic
Threat
URL Filter
WildFire
Data Filte
HIP Match
IP-Tag
User-ID
Tunnel In
Configura
System
Alarms
Authentic
Unified
Packet Captu
App Scope
Summary
Change M
Threat Mo
Threat Mo
Network M
Traffic Mo
Session Brow
Botnet
PDF Reports
Manage P
User Activ
Receive Time
Type
Name
From Zone
To Zone
Source address
Source User
Destination address
To Port
Application
Action
Severity
09/04 19:07:40 spyware Suspicious TLS Evasion Found inside outside 192.168.1.20 142.250.68.78 443 google-base alert informational
09/04 19:07:10 spyware Suspicious TLS Evasion Found inside outside 192.168.1.20 142.250.68.78 443 google-base alert informational
09/04 19:07:01 spyware Suspicious TLS Evasion Found inside outside 192.168.1.20 142.250.68.78 443 google-base alert informational
09/04 19:06:40 spyware Suspicious TLS Evasion Found inside outside 192.168.1.20 142.250.68.78 443 google-base alert informational
09/04 19:06:31 spyware Suspicious TLS Evasion Found inside outside 192.168.1.20 142.250.68.78 443 google-base alert informational
09/04 19:06:23 vulnerability Trojan-Win32.swrort.dfap danger danger 10.10.10.10 192.168.1.121 25 smtp reset-both high
09/04 19:06:22 vulnerability Ransom-Win32.Jocky.pe danger danger 10.10.10.10 192.168.1.121 25 smtp reset-both high
09/04 19:06:10 spyware Suspicious TLS Evasion Found inside outside 192.168.1.20 142.250.68.78 443 google-base alert informational
09/04 19:05:51 spyware Suspicious TLS Evasion Found inside outside 192.168.1.20 142.250.68.78 443 google-base alert informational
09/04 19:05:30 spyware Suspicious TLS Evasion Found inside outside 192.168.1.20 142.250.68.78 443 google-base alert informational
09/04 19:05:21 spyware Suspicious TLS Evasion Found inside outside 192.168.1.20 142.250.68.78 443 google-base alert informational
09/04 19:05:00 spyware Suspicious TLS Evasion Found inside outside 192.168.1.20 142.250.68.78 443 google-base alert informational
09/04 19:04:50 spyware Suspicious TLS Evasion Found inside outside 192.168.1.20 142.250.68.78 443 google-base alert informational
09/04 19:04:12 spyware Suspicious TLS Evasion Found inside outside 192.168.1.20 142.250.68.78 443 google-base alert informational
1 2 3 4 5 6 7 8 9 10
Resolve hostname
Highlight Policy Actions
Displaying logs 1 - 20
20
per page
DESC
admin | Logout | Last Login Time: 01/13/2025 04:39:32
Tasks | Language
19:12
9/4/2025