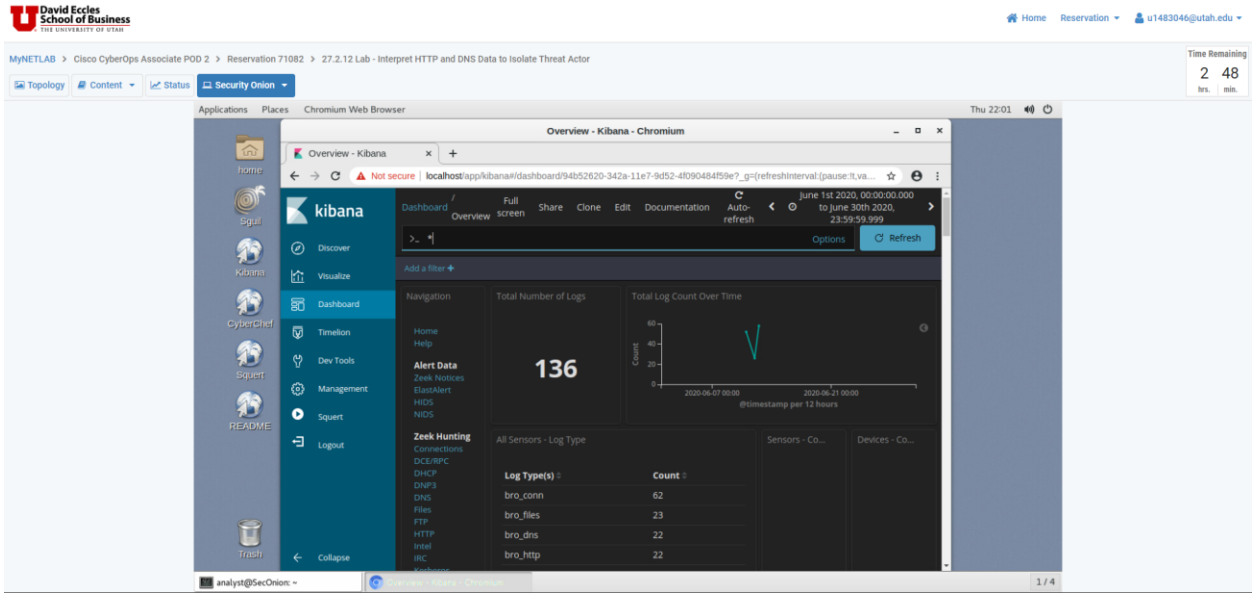
Vu Nguyen

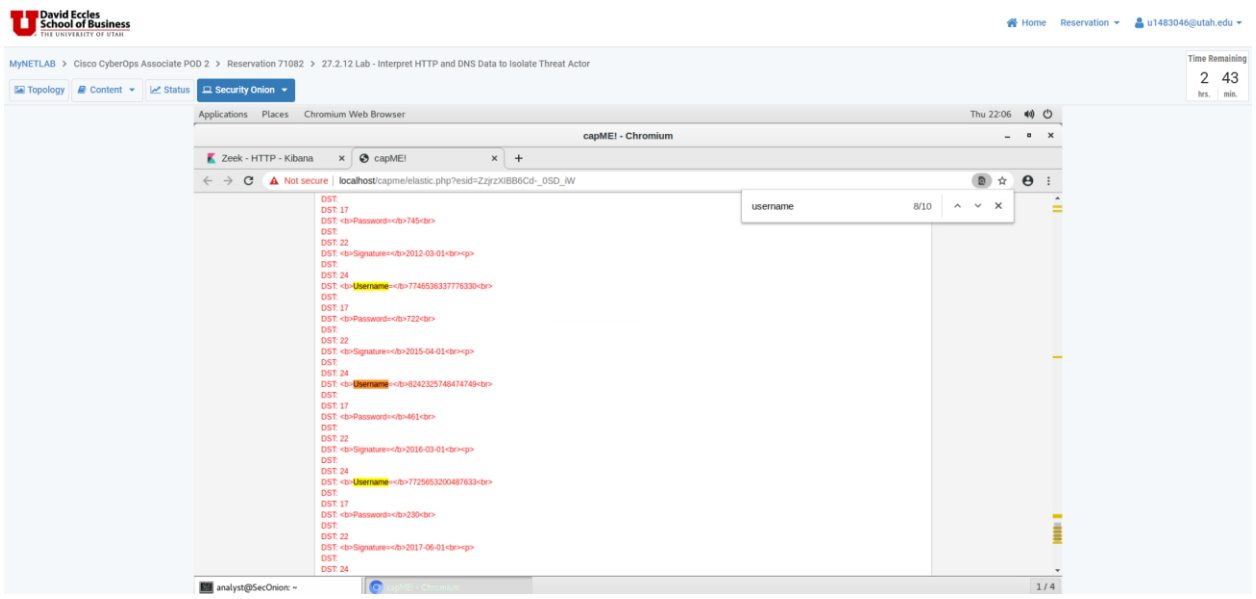
UID: u1483046

Assignment 28 - Threat Detection and Containment (Lab and Quiz)

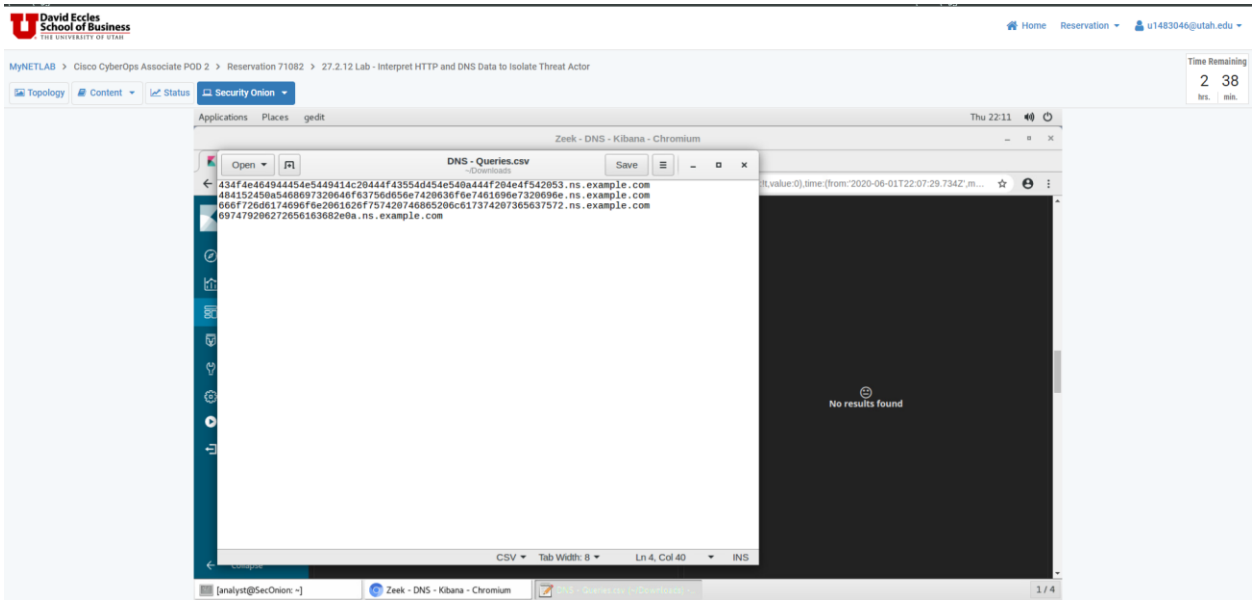
1. Lab 27.2.12, Part 1, Step 1g:



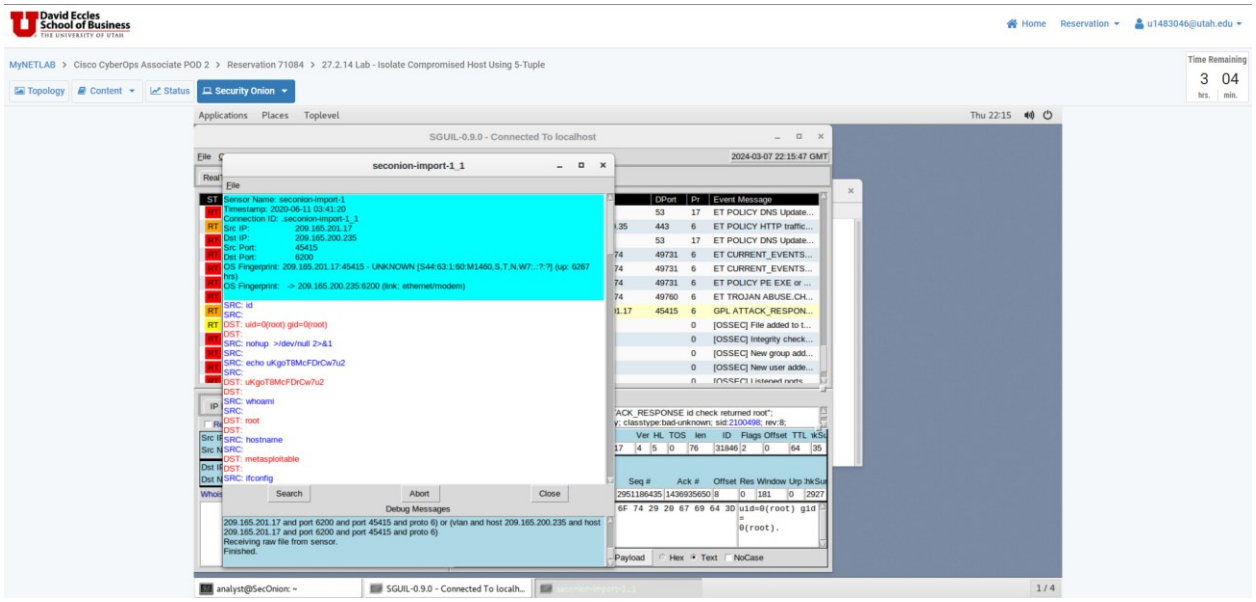
2. Lab 27.2.12, Part 1, Step 3d:



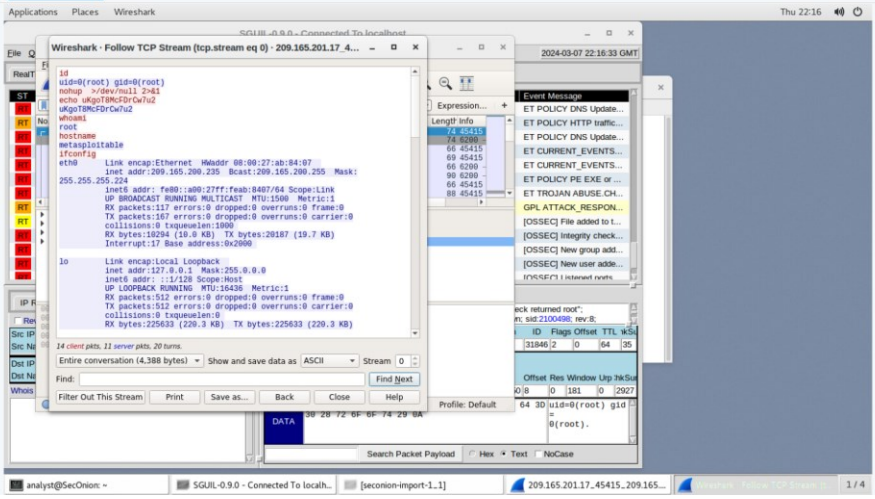
3. Lab 27.2.12, Part 2, Step 3b:



4. Lab 27.2.14, Part 1, Step 1f:



5. Lab 27.2.14, Part 2, Step 1b:


Applications Places Wireshark
Thu 22:16
Wireshark · Follow TCP Stream (tcp.stream eq 0) · 209.165.201.17_4...
id
uid=0(root) gid=0(root)
nohup >/dev/null 2>&1
echo uKgoT8McFDrCw7u2
uKgoT8McFDrCw7u2
whoami
root
hostname
metasploitable
ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:ab:84:07
inet addr:209.165.200.235 Bcast:209.165.200.255 Mask:255.255.255.224
inet6 addr: fe80::a00:27ff:feab:8407/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:117 errors:0 dropped:0 overruns:0 frame:0
TX packets:167 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:10294 (10.0 KB) TX bytes:20187 (19.7 KB)
Interrupt:17 Base address:0x2000
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:512 errors:0 dropped:0 overruns:0 frame:0
TX packets:512 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:225633 (220.3 KB) TX bytes:225633 (220.3 KB)
14 client pkts, 11 server pkts, 20 turns.
Entire conversation (4,388 bytes)
Show and save data as ASCII
Stream 0
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help
Profile: Default
Event Message
ET POLICY DNS Update...
ET POLICY HTTP traffic...
ET POLICY DNS Update...
ET CURRENT_EVENTS...
ET CURRENT_EVENTS...
ET POLICY PE EXE or ...
ET TROJAN ABUSE.CH...
GPL ATTACK_RESPON...
[OSSEC] File added to t...
[OSSEC] Integrity check...
[OSSEC] New group add...
[OSSEC] New user adde...
DATA
Search Packet Payload
Hex
Text
NoCase
analyst@SecOnion: ~
SGUIL-0.9.0 - Connected To localh...
[seconion-import-1_1]
209.165.201.17_45415_209.165...
1 / 4