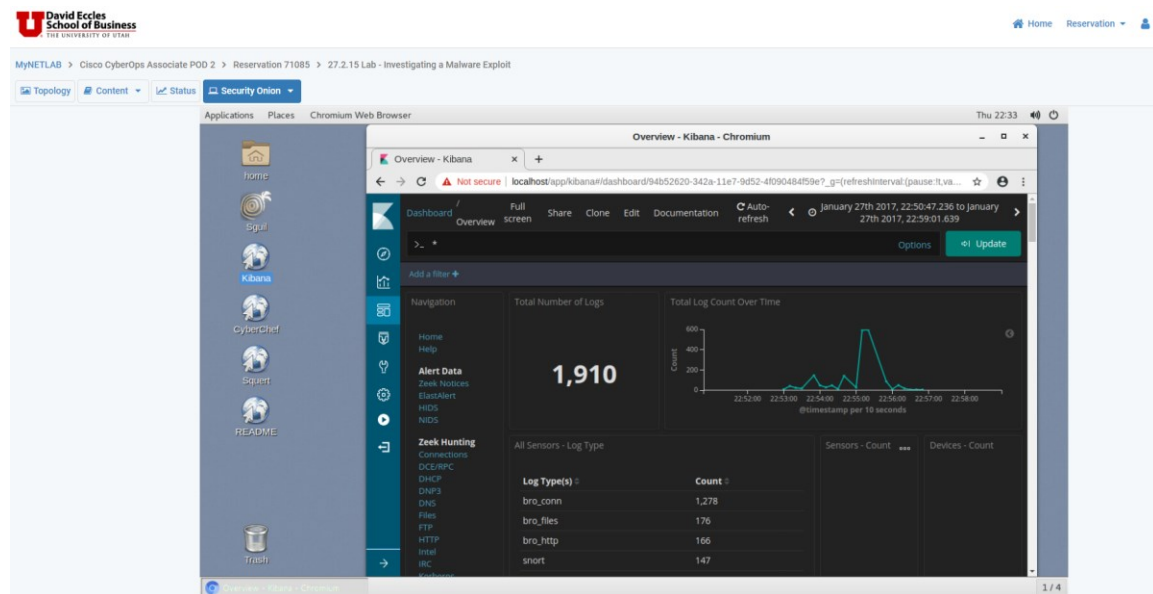


Vu Nguyen

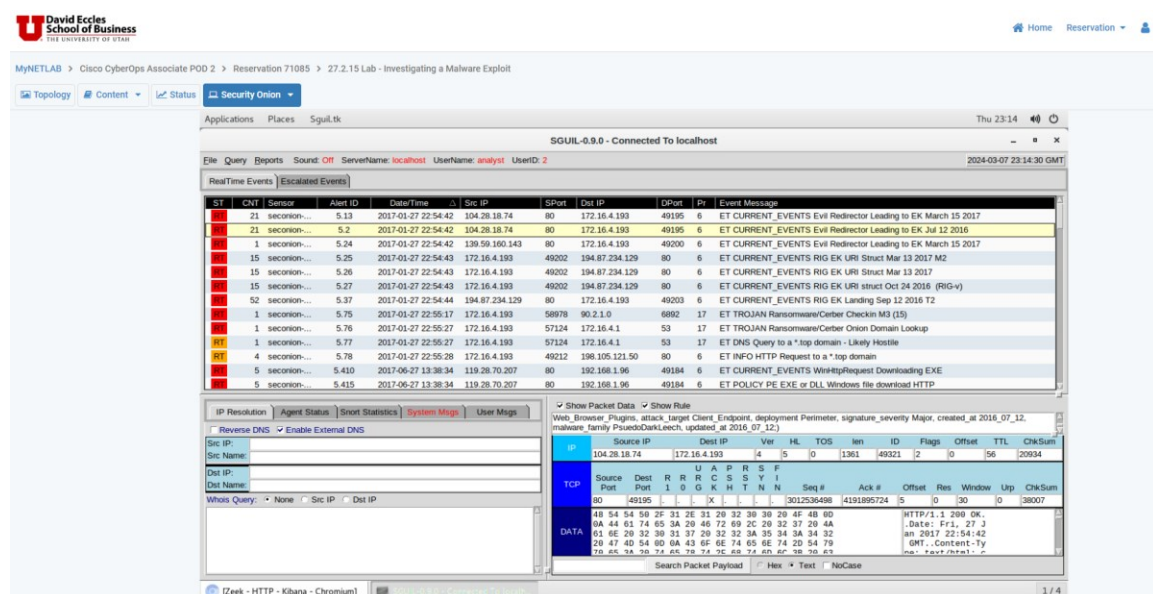
UID: u1483046

Assignment 29 - Investigating a Malware Exploit (Lab, Q&A and Quiz)

1. Lab 27.2.15, Part 1, Step 2a:



2. Lab 27.2.15, Part 2, Step 2c:



3. Lab 27.2.15, Part 2, Step 3f:

Applications Places Unknown

NetworkMiner 2.4

File Tools Help

Hosts (2) Files (13) Images Messages Credentials Sessions (1) DNS Parameters (57) Keywords | Anon

Sort Hosts On: Address (ascending) Sort and Refresh

Hosts: 172.16.4.193 (Windows) 194.87.234.129 (Iyu.benme.com)

Case Panel

File: 172.16.4.193:443

Message

CURRENT_EVENTS Evil Redirector Leading to EK March 15 2017

POLICY DNS Update From External net

INFO Packed Executable Download

POLICY PE EXE or DLL Windows file download HTTP

INFO Executable Retrieved With Minimal HTTP Headers - Potential Second Stage ...

INFO GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1

CURRENT_EVENTS Evil Redirector Leading to EK Jul 12 2010

POLICY DNS Update From External net

POLICY Data POST to an image file (gif)

CURRENT_EVENTS Evil Redirector Leading to EK March 15 2017

CURRENT_EVENTS RIG EK URI Struct Mar 13 2017 M2

POLICY HTTP traffic on port 443 (POST)

CURRENT_EVENTS RIG EK URI Struct Mar 13 2017

Reload Case Files

Buffered Frames to Parse:

Src IP: 172.16.4.193

Dest IP: 194.87.234.129

Whois Query: None Src IP Dist IP

Search Packet Payload Hex Text NoCase

1 / 4

Applications Places Unknown

NetworkMiner 2.4

File Tools Help

Hosts (2) Files (13) Images Messages Credentials Sessions (1) DNS Parameters (57) Keywords | Anon

Filter keywords: Case sensitive ExactPhrase Any column Clear Apply

Frame nr. Filename Extension Size Source host S. port Dst. port

4 index.html 13198475.html 5 212 B 194.87.234.129 (Iyu.benme.com) TCP 80 17

10 index.html 48463872.html 90 745 B 194.87.234.129 (Iyu.benme.com) TCP 80 17

95 index.html 67899866.swf 16 261 B 194.87.234.129 (Iyu.benme.com) TCP 80 17

Case Panel

File: 172.16.4.193:443

Message

CURRENT_EVENTS Evil Redirector Leading to EK March 15 2017

POLICY DNS Update From External net

INFO Packed Executable Download

POLICY PE EXE or DLL Windows file download HTTP

INFO Executable Retrieved With Minimal HTTP Headers - Potential Second Stage ...

INFO GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1

CURRENT_EVENTS Evil Redirector Leading to EK Jul 12 2010

POLICY DNS Update From External net

POLICY Data POST to an image file (gif)

CURRENT_EVENTS Evil Redirector Leading to EK March 15 2017

CURRENT_EVENTS RIG EK URI Struct Mar 13 2017 M2

POLICY HTTP traffic on port 443 (POST)

CURRENT_EVENTS RIG EK URI Struct Mar 13 2017

Reload Case Files

Buffered Frames to Parse:

Src IP: 172.16.4.193

Dest IP: 194.87.234.129

Whois Query: None Src IP Dist IP

Search Packet Payload Hex Text NoCase

1 / 4

4. Lab 27.2.15, Part 3, Step 3b:

David Eccles School of Business THE UNIVERSITY OF STANFORD

MyNETLAB > Cisco CyberOps Associate POD 2 > Reservation 71085 > 27.2.15 Lab - Investigating a Malware Exploit

Topology Content Status Security Onion

Applications Places Wireshark

File Edit View Go Capture Analyze

Packet # Hostname Content Type Size Filename

Packet	Hostname	Content Type	Size	Filename
29	www.homeimprovement.com	text/css	1,058 bytes	postratings-css.css?ver=1.83
33	www.homeimprovement.com	text/css	1,819 bytes	daves-wordpress-live-search_default_gray.css

Save Save All Close Help

Packets: 37 / Displayed: 3 (8.1%) Profile: Default

5. Lab 27.2.15, Part 3, Step 4a:

David Eccles School of Business THE UNIVERSITY OF STANFORD

MyNETLAB > Cisco CyberOps Associate POD 2 > Reservation 71085 > 27.2.15 Lab - Investigating a Malware Exploit

Topology Content Status Security Onion

Applications Places Wireshark

File Edit View Go Capture Analyze

Packet # Hostname Content Type Size Filename

Packet	Hostname	Content Type	Size	Filename
91	tyu.benme.com	text/html	5,313 bytes	tsi=Vivaldi&ts=Vivaldi-25x76-40d1-5x76
122	tyu.benme.com	application/x-shockwave-flash	50 kB	hq=CERJN8_svk7p5P1LgRbVgU3n456WwB5

Save Save All Close Help

Packets: 125 / Displayed: 3 (2.4%) Profile: Default