

Client-Side Attacks and Detection Analysis Exercise

Overview

Students will apply their existing analysis knowledge and tool skills (i.e., FireSIGHT and Wireshark) along with additional concepts from this module to analyze a client-side attack. An Ubuntu desktop is demonstrated for tool access and analysis. The lab mimics analysis scenarios often performed in the real world. While other tools may be used in operational environments, the same analysis concepts can be applied to them.

Situation

Several users in your organization received a potential phishing email between **1600 and 1659 UTC on April 15, 2020**. The email links to a news story at IP address 10.167.197[.]38, which is located in China according to WHOIS.

Review FireSIGHT alerts to begin your analysis. Consider if anyone clicked on the link and what the potential consequences may be.

Pivot within FireSIGHT's events to derive likely hypotheses. Correlate these possibilities with lab1.pcap in Wireshark to strengthen your analysis and determine the most likely hypothesis.

Objectives

Follow along with the video demonstration to identify the following information:

- Adversary
 - IP Address: _____
- Victim
 - IP Address: _____
 - Port Exploited (e.g., 80/TCP): _____
 - Protocol Exploited (e.g., HTTP): _____
- Stage 2 Infrastructure
 - IP Address: _____
 - Port Used (e.g., 80/TCP): _____
 - Protocol Used (e.g., HTTP): _____
 - File Provided (e.g., malware.7z): _____
- C2 Infrastructure
 - IP Address: _____
 - Port Used (e.g. 80/TCP) _____
 - Protocol Used (e.g., HTTP): _____

ANALYSIS PROCESS

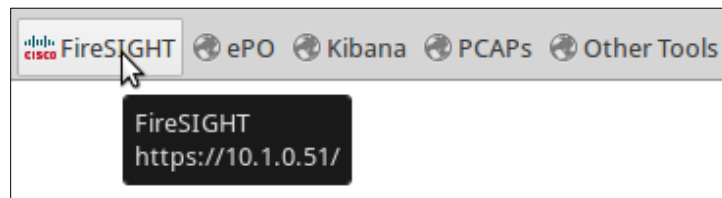
Follow along with the video as it goes through the following steps of analysis.

This section provides answers and a method of solving each of the lab questions. Note that there may be more than one way to arrive at the correct answer. You may discover a different solution to the same problem.

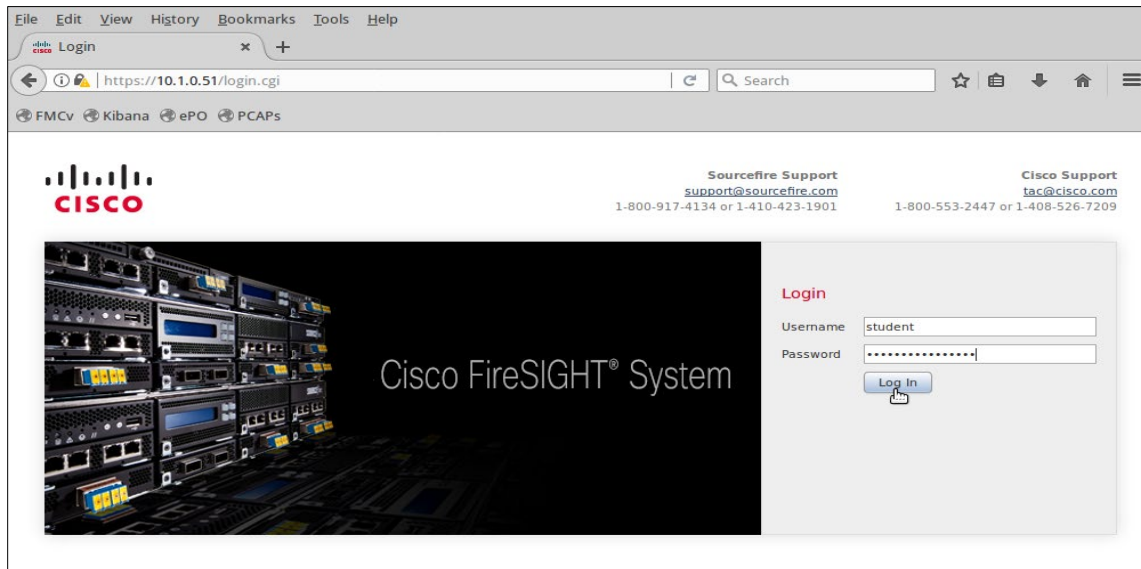
Note: Potential Indicators of Compromise (IoC), such as IP addresses and domain names, should be "de-fanged" as a best practice. De-fanging simply involves the insertion of a character into the IoC that is otherwise invalid in the IoC's context, so that copying/pasting/clicking the IoC won't inadvertently put readers at risk. In this lab, brackets are used to de-fang. When you are asked to enter a value into a field, such as when performing a search, remove any de-fanging characters to ensure the search will properly execute. For example, if you are instructed to enter "256.256.256[.]256", you would enter "256.256.256.256" (removing the brackets).

Step 1: Searching within FireSIGHT

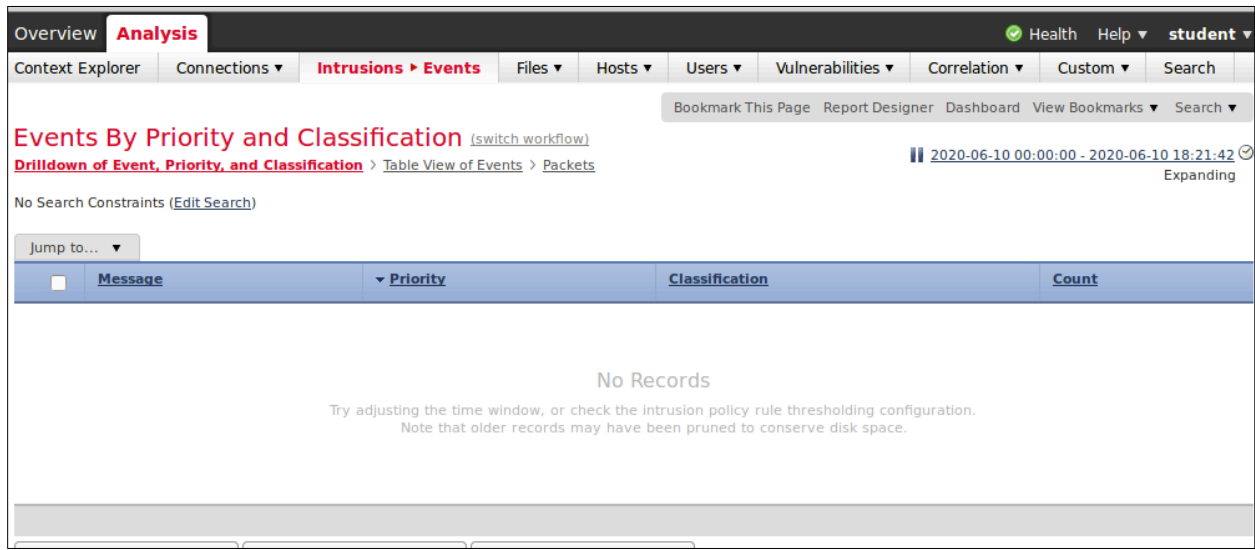
1. Select the **FireSIGHT** bookmark in the open **Mozilla Firefox** web browser.



2. Enter username "Student" and password "12qwaszx!@QWASZX" and then click "Log In".



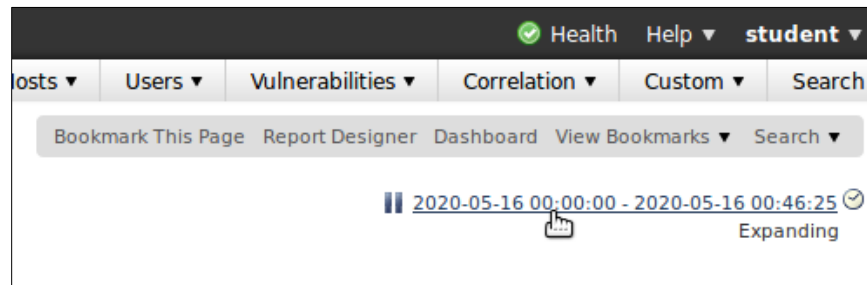
FireSIGHT displays the intrusion events screen by default. Notice no events are listed.



By default, FireSIGHT displays events from midnight of the current day to the current time. One common reason for listing unexpected or no displayed events is forgetting to change this default to the correct timeframe.

Tip: If you need to return to the intrusion events area later, select Analysis >> Intrusions >> Events from the main menu.

3. Begin configuring the correct timeframe mentioned in the instructions by selecting the date/time range near the top-right corner of the window.



A date picker pop-up opens. Ensure the "Events Time Window" tab is selected.

Events Time Window Preferences

Expanding Time Window ▾

Start Time End Time

May 2020 May 2020

2020-05-16 00:00 50 minutes 2020-05-16 00:50

Presets

Last 1 hour 6 hours 1 day 1 week 2 weeks 1 month

Current Day Week Month

Synchronize with Health Monitoring Time Window

Apply Reset

Any changes made will take effect on the next page load.

4. Configure the start and stop times to **April 15, 2020 between 1600 and 1659 UTC**. Under "Start Time" use the arrows within the calendar to choose "April 15, 2020". Select "16" and "00" from the hour and minute drop-down menus below the calendar.

Start Time

April 2020

15

16 : 00

- Next to "End Time", ensure the checkbox is checked. Use the arrows within the calendar to choose "April 15, 2020." Select "16" and "59" from the hour and minute drop-down menus below the calendar.

End Time

April 2020						
Su	Mo	Tu	We	Th	Fr	Sa
29	30	31	1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	1	2
3	4	5	6	7	8	9

16 : 59

- Verify the start and stop times displayed directly above the "Presets" heading are correct. Click "Apply" when finished.

2020-04-15 16:00 **59 minutes** 2020-04-15 16:59

Presets

Last 1 hour 6 hours 1 day 1 week 2 weeks 1 month

Current Day Week Month

Synchronize with Health Monitoring Time Window

Apply Reset

FireSIGHT populates with events from the specified timeframe. Notice there seem to be a lot of events for such a short time period.

Events By Priority and Classification (switch workflow) 2020-04-15 16:00:00 - 2020-04-15 16:59:00
Drilldown of Event, Priority, and Classification > Table View of Events > Packets Static

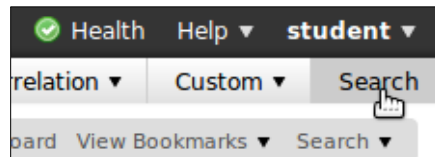
No Search Constraints (Edit Search)

Jump to... ▾

<input type="checkbox"/>	Message	Priority	Classification	Count
⌵ <input type="checkbox"/>	FILE-OTHER Microsoft LNK shortcut arbitrary dll load attempt (1:1000010:1)	high	Attempted User Privilege Gain	1
⌵ <input type="checkbox"/>	OS-WINDOWS DCERPC NCACN-IP-TCP spoolss AddPrinterEx overflow attempt (1:1000022:1)	high	Attempted Administrator Privilege Gain	2
⌵ <input type="checkbox"/>	SENSITIVE-DATA Email Addresses (138:5:1)	medium	Sensitive Data	3
⌵ <input type="checkbox"/>	SDF_COMBO_ALERT (139:1:1)	medium	Sensitive Data	1
⌵ <input type="checkbox"/>	STREAMS_SMALL_SEGMENT (129:12:2)	medium	Potentially Bad Traffic	44
⌵ <input type="checkbox"/>	STREAMS_BAD_RST (129:15:2)	medium	Potentially Bad Traffic	5
⌵ <input type="checkbox"/>	DECODE_IP_OPTION_SET (116:444:2)	medium	Potentially Bad Traffic	4
⌵ <input type="checkbox"/>	HI_CLIENT_NON_RFC_CHAR (119:14:2)	medium	Potentially Bad Traffic	2
⌵ <input type="checkbox"/>	SSL_INVALID_CLIENT_HELLO (137:1:2)	medium	Potentially Bad Traffic	2
⌵ <input type="checkbox"/>	POLICY Inbound.potentially.malicious.file.download.attempt (1:1000000:8)	medium	A Suspicious Filename was Detected	1

A common method of narrowing in on the more important events is to filter with searches on known indicators.

7. Search on the IP address used in the news links of the phishing email. Select "Search" in the Analysis menu to view FireSIGHT's search options.



8. Scroll down to the "Networking" section, enter "10.167.197[.]38" in the "Source/Destination IP" field, and then click "Search".

(unnamed search) Private

Source IP	<input type="text"/>	+	192.168.1.0/24, !192.168.1.3, 2001:db8:8...
Destination IP	<input type="text"/>	+	192.168.1.0/24, !192.168.1.3, 2001:db8:8...
Source / Destination IP	<input type="text" value="10.167.197.38"/>	+	192.168.1.0/24, !192.168.1.3, 2001:db8:8...

FireSIGHT returns a list of grouped events in a tabular format.

Events By Priority and Classification [\(switch workflow\)](#)
 Drilldown of Event, Priority, and Classification > [Table View of Events](#) > [Packets](#) 2020-04-15 16:00:00 - 2020-04-15 16:59:00 Static

▶ Search Constraints ([Edit Search](#) [Save Search](#))

Jump to... ▼

<input type="checkbox"/>	Message	Priority	Classification	Count
↓ <input type="checkbox"/>	FILE-OTHER Microsoft LNK shortcut arbitrary dll load attempt (1:1000010:1)	high	Attempted User Privilege Gain	1
↓ <input type="checkbox"/>	SENSITIVE-DATA Email Addresses (138:5:1)	medium	Sensitive Data	2
↓ <input type="checkbox"/>	POLICY Inbound potentially malicious file download attempt (1:1000000:8)	medium	A Suspicious Filename was Detected	1
↓ <input type="checkbox"/>	HI_CLIENT_UNKNOWN_METHOD (119:31:2)	low	Unknown Traffic	1
↓ <input type="checkbox"/>	APP-DETECT VNC server response (1:560:9)	low	Misc Activity	1
↓ <input type="checkbox"/>	PROTOCOL-ICMP Destination Unreachable Port Unreachable (1:402:15)	low	Misc Activity	1
↓ <input type="checkbox"/>	PROTOCOL-ICMP Echo Reply (1:408:8)	low	Misc Activity	1

◀ Page 1 of 1 ▶ Displaying rows 1-7 of 7 rows

View Copy Download Packets
 View All Copy All Download All Packets

Step 2: Viewing Event Details

1. Click "View All" beneath the search results to display additional details. FireSIGHT displays all individual events instead of grouping them together. Notice it shows useful columns like Time, Source IP, and Destination IP in the current view but is missing others such as the Message field. Scroll horizontally right to view the Message column, but now the first few useful fields are obscured.

Events By Priority and Classification [\(switch workflow\)](#)
 Drilldown of Event, Priority, and Classification > [Table View of Events](#) > [Packets](#) 2020-04-15 16:00:00 - 2020-04-15 16:59:00 Static Disabled Columns

▶ Search Constraints ([Edit Search](#))

Jump to... ▼

<input type="checkbox"/>	Time ×	Priority ×	Impact ×	Inline Result ×	Source IP ×	Source Country ×	Destination IP ×	Destination Country ×
↓ <input type="checkbox"/>	2020-04-15 16:58:09	low	0		192.168.1.202		192.168.1.201	
↓ <input type="checkbox"/>	2020-04-15 16:55:11	low	0		fe80::8ce9:4855:1928:aaf0		fe80::cc00:cc02	
↓ <input type="checkbox"/>	2020-04-15 16:55:06	low	0		fe80::cc00:cc02		fe80::8ce9:4855:1928:aaf0	
↓ <input type="checkbox"/>	2020-04-15 16:55:06	low	0		fe80::8ce9:4855:1928:aaf0		ff02::1:ff00:cc02	
↓ <input type="checkbox"/>	2020-04-15 16:55:06	medium	0		192.168.1.201		224.0.0.22	
↓ <input type="checkbox"/>	2020-04-15 16:55:06	low	0		fe80::8ce9:4855:1928:aaf0		ff02::16	
↓ <input type="checkbox"/>	2020-04-15 16:54:33	medium	0		192.168.1.51		192.168.1.52	
↓ <input type="checkbox"/>	2020-04-15 16:54:32	medium	0		10.245.20.50		192.168.1.201	
↓ <input type="checkbox"/>	2020-04-15 16:54:31	medium	0		192.168.1.201		10.245.20.50	

Last login on Wednesday, 2020-05-13 at 17:55:09 PM from 10.1.0.3 CISCO

By default, FireSIGHT displays all event fields. This prevents viewing of just the most useful columns on a one or two screens. One common work-around is to reduce the number of fields displayed.

- To remove any unnecessary columns, select the "X" next to the header of any column (e.g., Impact).

Note: The remaining CDA exercises assume you will perform a column cleanup in the same manner as this lab.

Jump to...		<input type="checkbox"/> Time ×	<input type="checkbox"/> Priority ×	<input type="checkbox"/> Impact ×	<input type="checkbox"/> Inline Result ×	<input type="checkbox"/> Source IP ×
↓	<input type="checkbox"/>	2020-04-15 16:18:49	low	0		10.167.197.38
↓	<input type="checkbox"/>	2020-04-15 16:18:38	medium	0		10.167.197.38
↓	<input type="checkbox"/>	2020-04-15 16:18:37	medium	0		192.168.2.33

A menu showing all selectable columns appears. Due to the number of columns displayed by default, the easiest approach is to disable all columns and then enable just the needed ones. To do this uncheck "All Columns" at the top of the menu and check those as illustrated in the picture below (e.g., "Destination IP" and "Destination Port/ICMP Code").

<input type="checkbox"/> All Columns	<input type="checkbox"/> Ingress Security Zone	<input type="checkbox"/> Client Tag
Enabled Columns	<input type="checkbox"/> Inline Result	<input type="checkbox"/> Destination User
<input type="checkbox"/> Access Control Policy	<input type="checkbox"/> Intrusion Policy	<input type="checkbox"/> Email Attachments
<input type="checkbox"/> Access Control Rule	<input checked="" type="checkbox"/> Message	<input type="checkbox"/> Email Recipient
<input type="checkbox"/> Application Protocol	<input type="checkbox"/> Network Analysis Policy	<input type="checkbox"/> Email Sender
<input type="checkbox"/> Application Risk	<input type="checkbox"/> Priority	<input type="checkbox"/> HTTP Hostname
<input type="checkbox"/> Business Relevance	<input type="checkbox"/> SSL Status	<input type="checkbox"/> HTTP URI
<input type="checkbox"/> Classification	<input type="checkbox"/> Source Country	<input type="checkbox"/> MPLS Label
<input type="checkbox"/> Client	<input checked="" type="checkbox"/> Source IP	<input type="checkbox"/> Original Client IP
<input type="checkbox"/> Destination Country	<input checked="" type="checkbox"/> Source Port / ICMP Type	<input type="checkbox"/> Web Application Category
<input checked="" type="checkbox"/> Destination IP	<input type="checkbox"/> Source User	<input type="checkbox"/> Web Application Tag
<input checked="" type="checkbox"/> Destination Port / ICMP Code	<input checked="" type="checkbox"/> Time	<input type="button" value="Apply"/> <input type="button" value="Cancel"/>

Scroll down and click "Apply" when finished. FireSIGHT displays the same results but with a limited number of columns.

Events By Priority and Classification (switch workflow)
 Drilldown of Event, Priority, and Classification > **Table View of Events** > Packets 2020-04-15 16:00:00 - 2020-04-15 16:59:00
 Static
 Search Constraints (Edit Search Save Search) Disabled Columns

Jump to... ▼

<input type="checkbox"/>	Time ×	Source IP ×	Destination IP ×	Source Port / ICMP Type ×	Destination Port / ICMP Code ×	Message ×
	2020-04-15 16:18:49	10.167.197.38	192.168.2.33	4444 (krb524) / tcp	49168 / tcp	APP-DETECT VNC server respons
	2020-04-15 16:18:38	10.167.197.38	192.168.2.33	80 (http) / tcp	49167 / tcp	SENSITIVE-DATA Email Addres
	2020-04-15 16:18:37	192.168.2.33	10.167.197.38	49167 / tcp	80 (http) / tcp	POLICY Inbound potentially malic
	2020-04-15 16:18:37	10.167.197.38	192.168.2.33	80 (http) / tcp	49167 / tcp	FILE-OTHER Microsoft LNK shortc
	2020-04-15 16:18:37	192.168.2.33	10.167.197.38	49167 / tcp	80 (http) / tcp	HL_CLIENT_UNKNOWN_METHOD (
	2020-04-15 16:18:33	10.167.197.38	192.168.2.33	3 (Destination Unreachable) / icmp	3 (Port unreachable) / icmp	PROTOCOL-ICMP Destination Unre
	2020-04-15 16:18:33	10.167.197.38	192.168.2.33	0 (Echo Reply) / icmp	0 / icmp	PROTOCOL-ICMP Echo Reply (1:4
	2020-04-15 16:17:05	10.167.197.38	192.168.2.38	49136 / tcp	25 (smtp) / tcp	SENSITIVE-DATA Email Addres

Page 1 of 1 >> Displaying rows 1-8 of 8 rows

View Copy Download Packets
 View All Copy All Download All Packets

- Another useful analysis adjustment is to reorder the events. By default, FireSIGHT orders events by newest-to-oldest chronologically. Changing the order to oldest-to-newest lists events in a more conventional top-down timeline.

Reverse the order of 10.167.197[.]38's logged events from oldest-to-newest by selecting the "Time" heading. (Selecting "Time" again changes ordering back to FireSIGHT's default).

Jump to... ▼

<input type="checkbox"/>	Time ×	Source IP ×
	2020-04-15 16:18:49	10.167.197.38
	2020-04-15 16:18:38	10.167.197.38
	2020-04-15 16:18:37	192.168.2.33
	2020-04-15 16:18:37	10.167.197.38

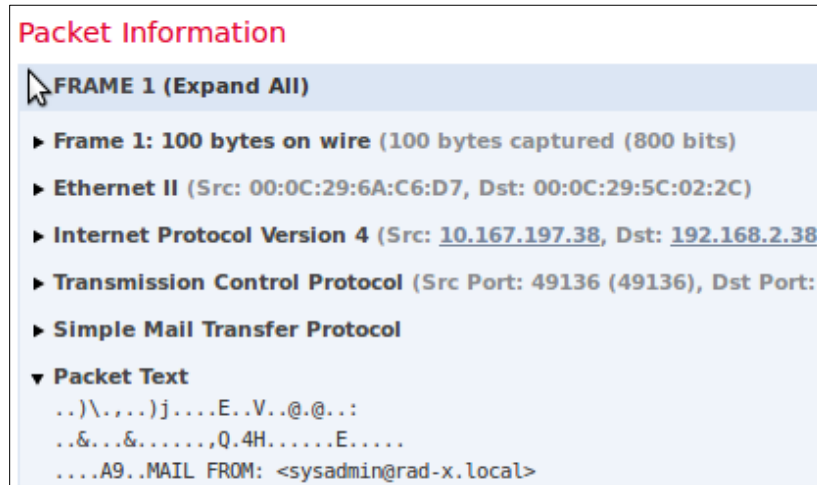
As shown below, the events are now ordered from oldest-to-newest.

<input type="checkbox"/>	Time	Source IP	Destination IP	Source Port / ICMP Type	Destination Port / ICMP Code	Message
<input type="checkbox"/>	2020-04-15 16:17:05	10.167.197.38	192.168.2.38	49136 / tcp	25 (smtp) / tcp	SENSITIVE-DATA Email Addresses
<input type="checkbox"/>	2020-04-15 16:18:33	10.167.197.38	192.168.2.33	0 (Echo Reply) / icmp	0 / icmp	PROTOCOL-ICMP Echo Reply (1.40
<input type="checkbox"/>	2020-04-15 16:18:33	10.167.197.38	192.168.2.33	3 (Destination Unreachable) / icmp	3 (Port unreachable) / icmp	PROTOCOL-ICMP Destination Unre
<input type="checkbox"/>	2020-04-15 16:18:37	192.168.2.33	10.167.197.38	49167 / tcp	80 (http) / tcp	HL_CLIENT_UNKNOWN_METHOD (I
<input type="checkbox"/>	2020-04-15 16:18:37	10.167.197.38	192.168.2.33	80 (http) / tcp	49167 / tcp	FILE-OTHER Microsoft LNK shortcu
<input type="checkbox"/>	2020-04-15 16:18:37	192.168.2.33	10.167.197.38	49167 / tcp	80 (http) / tcp	POLICY Inbound potentially malici
<input type="checkbox"/>	2020-04-15 16:18:38	10.167.197.38	192.168.2.33	80 (http) / tcp	49167 / tcp	SENSITIVE-DATA Email Addresses
<input type="checkbox"/>	2020-04-15 16:18:49	10.167.197.38	192.168.2.33	4444 (krb524) / tcp	49168 / tcp	APP-DETECT VNC server response

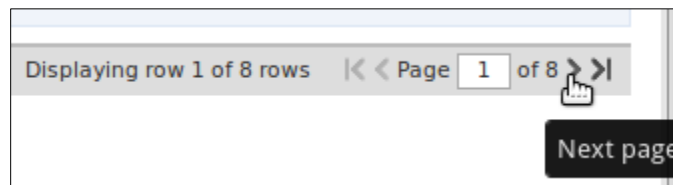
4. Now, it is time to analyze the details of each event. Click "View All" to display the details of the first event.

<input type="checkbox"/>	2020-04-15 16:17:05	10.167.197.38	192.168.2.38	49136 / tcp		
<input type="checkbox"/>	2020-04-15 16:18:33	10.167.197.38	192.168.2.33	0 (Echo Reply) / icmp		
<input type="checkbox"/>	2020-04-15 16:18:33	10.167.197.38	192.168.2.33	3 (Destination Unreachable) / icmp		
<input type="checkbox"/>	2020-04-15 16:18:37	192.168.2.33	10.167.197.38	49167 / tcp		
<input type="checkbox"/>	2020-04-15 16:18:37	10.167.197.38	192.168.2.33	80 (http) / tcp		
<input type="checkbox"/>	2020-04-15 16:18:37	192.168.2.33	10.167.197.38	49167 / tcp		
<input type="checkbox"/>	2020-04-15 16:18:38	10.167.197.38	192.168.2.33	80 (http) / tcp		
<input type="checkbox"/>	2020-04-15 16:18:49	10.167.197.38	192.168.2.33	4444 (krb524) / tcp		

- Review the information in the "Event Information" section of this event. Scroll down to the "Packet Information" section, and then select "Packet Text" to view its payload.



Click ">" to move to the next event.



- Review each of the subsequent events in a similar manner as above until you come to one triggered by a rule with a "HI_CLIENT_UNKNOWN_METHOD" message.
- Select "Packet Text" to view its payload. Notice an "HTTP OPTIONS" request was sent from 192.168.2[.]33 to the potential adversary at 10.167.197[.]38 on TCP port 80.



- Click ">" to proceed to the next packet. Observe the event name, the HTTP URI field "/pPmusTKFGRW/qHHoL.lnk," and the reference in the rule pointing to MS10-046 and MS15-020.

Event	FILE-OTHER Microsoft LNK shortcut arbitrary dll load attempt (1:1000010:1)
Timestamp	2020-04-15 16:18:37
Classification	Attempted User Privilege Gain
Priority	high
Ingress Security Zone	Passive
Device	192.168.1.52
Ingress Interface	eth1
Source IP	10.167.197.38
Source Port / ICMP Type	80 (http) / tcp
Destination IP	192.168.2.33
Destination Port / ICMP Code	49167 / tcp
HTTP Hostname	Not Available
HTTP URI	/pPmusTKFGRW/qHHoL.lnk
Intrusion Policy	RaD-X-1
Access Control Policy	Default Access Control
Access Control Rule	RaD-X
Rule	alert tcp \$EXTERNAL_NET any -> \$HOME_NET any (sid:1000010; gid:1; flow:established,to_client; file_data; content:" 4C 00 00 00 01 14 02 00 A2 DD 08 00 2B 30 30 9D "; distance:0; metadata:policy max-detect-ips drop, policy security-ips drop, service ftp-data, service http, service ima; reference:uri,technet.microsoft.com/en-us/security/bulletin/ms10-046; reference:uri,technet.microsoft.com/en-us/security/bulletin/ms15-020;

Based on this information, it is very likely the adversary's IP address was 10.167.197[.]38 and the victim's IP address was 192.168.2[.]33. The victim appears to have been initially compromised using the HTTP protocol over TCP port 80 via a downloaded LNK file.

- Expand "Packet Text" and slowly scroll to the right to view all of its content. Note the LNK shortcut points to a DLL file located on the adversary's machine.

```
.\.\.1.0...1.6.7...1.9.7...3.8.\.p.P.m.u.s.T.K.F.G.R.W.\.N.f.I.z.L.H.Z.F...d.l.l.....
```

- Go to the next event and review its contents. In "Packet Text", note the victim subsequently made the above HTTP GET request for "/pPmusTKFGRW/NfIzLHZF.dll" to the same 10.167.197[.]38 using the HTTP protocol over TCP port 80. The execution of the original LNK file in the previous packet likely caused this stage 2 download request for NfIzLHZF.dll.

```

▶ Internet Protocol Version 4 (Src: 192.168.2.33, Dst: 10.167.197.38)
▶ Transmission Control Protocol (Src Port: 49167 (49167), Dst Port: 80)
▶ Hypertext Transfer Protocol
▼ Packet Text
..)j....)2DG..E.....@...e....!
..&...P..!E..
P.@=.R..GET /pPmusTKFGRW/NfIzLHZF.dll HTTP/1.1
translate: f
User-Agent: Microsoft-WebDAV-MiniRedir/6.0.6000

```

- Continue on to the next event and review its contents. This one includes multiple frames within one event. Open "Packet Text" for the Frame 1 and note the indications of a Windows executable file being downloaded (i.e., "MZ" and "!This program cannot be run in DOS mode.>").

```

Content-Type: application/octet-stream
Connection: Keep-Alive
Server: Apache
Content-Length: 5120

MZ.....@.....!..L!This program cannot be run in DOS mode.

$. . . . .y.B.= { , = { , = { , . . . . . } , = { - . 5 { , . 0 } . . < { , . 0 } . . < { , . Rich = { , . . . . . PE . . L . . . . .
S . . . . . ! . . . . . 0 . . . . . @ . . . . . P . . . . . @ . . . . .
. . . . . 0 . . . . .
. . . . . @ . . . . . reloc . . . . . @ . . . . . @ . . . . . @ . . . . . B . . . . .

Packet Bytes

FRAME 2 (Expand All)

Frame 2: 1434 bytes on wire (1434 bytes captured (11472 bits))
Ethernet II (Src: 00:0C:29:6A:C6:D7, Dst: 00:0C:29:32:44:47)
Internet Protocol Version 4 (Src: 10.167.197.38, Dst: 192.168.2.33)
Transmission Control Protocol (Src Port: 80 (80), Dst Port: 49167 (49167), Seq: 1381, Ack: 1, Len: 1380)
Packet Text
..)2DG..)j...E...{*@.@.'
..&...!.P..E..n..".P..-.....P.M.Q... ..U.R... ..E.P... ..M.Q... ..j.... ..].....U..Q.E..E..}.t.....

```

The message for this event, "SENSITIVE-DATA Email Addresses (138:5:1)" is not too useful but ended up providing valuable information. The "@" symbols in Frame 2 likely cause this rule to fire.

- Proceed to the final packet. Note the use of the Virtual Network Computing (VNC) protocol over TCP port 4444 from the adversary at 10.167.197[.]38 to the victim for C2.

Rule	alert tcp \$EXTERNAL_NET any -> \$HOME_NET any (msg:"APP-DETECT VNC server content:".0"; depth:2; offset:7; metadata:ruleset community; classtype:misc-act
Summary	This event is generated when network traffic indicating the use of an application
Actions	▶
Packet Information	
FRAME 1 (Expand All)	
▶ Frame 1: 66 bytes on wire (66 bytes captured (528 bits))	
▶ Ethernet II (Src: 00:0C:29:6A:C6:D7, Dst: 00:0C:29:32:44:47)	
▶ Internet Protocol Version 4 (Src: 10.167.197.38, Dst: 192.168.2.33)	
▶ Transmission Control Protocol (Src Port: 4444 (4444), Dst Port: 49168 (49168), Seq: 1, Ack: 1, Len: 12)	
▶ Virtual Network Computing	
▼ Packet Text	
..)2DG..)j...E..4.d@.@... ..&...!.\\...v....N)P...\$g..RFB 003.008	

What happened?

We know an email was sent from an attacking host in China and a user clicked on the link contained within it. FireSIGHT generated a client-side .lnk alert, then a VNC alert followed.

Our next steps may include scrubbing the victim system to investigate scope of the compromise. The attack may also be confirmed by checking the host directly. Tools such as “netstat” can be helpful. Per your request, a technician sends the following netstat output from the suspect host.

```
Command Prompt
C:\Users\instructor>netstat -an

Active Connections

Proto Local Address           Foreign Address         State
TCP   0.0.0.0:135              0.0.0.0:0               LISTENING
TCP   0.0.0.0:49152           0.0.0.0:0               LISTENING
TCP   0.0.0.0:49153           0.0.0.0:0               LISTENING
TCP   0.0.0.0:49154           0.0.0.0:0               LISTENING
TCP   0.0.0.0:49155           0.0.0.0:0               LISTENING
TCP   0.0.0.0:49156           0.0.0.0:0               LISTENING
TCP   0.0.0.0:49157           0.0.0.0:0               LISTENING
TCP   192.168.2.33:139        0.0.0.0:0               LISTENING
TCP   192.168.2.33:49168      10.167.197.38:4444      ESTABLISHED
TCP   [::]:135                [::]:0                  LISTENING
TCP   [::]:445                 [::]:0                  LISTENING
TCP   [::]:5357                [::]:0                  LISTENING
TCP   [::]:135                 [::]:0                  LISTENING
TCP   [::]:135                 [::]:0                  LISTENING
TCP   [::]:135                 [::]:0                  LISTENING
TCP   [::]:135                 [::]:0                  LISTENING
TCP   [::]:135                 [::]:0                  LISTENING
UDP   0.0.0.0:135             0.0.0.0:0               *
```

These results confirm one of our hosts established a separate outbound TCP connection to China, which correlates with the VNC alert. The attacker may now have GUI access to the user’s desktop. The totality of evidence confirms the incident and we must now mitigate it.

The compromised host will most likely become a "zombie" in a malicious bot army. In this role, the host may be used to attack other devices, send spam, launch denial-of-service attacks, exfiltrate information stored on the device, or log keystrokes. Attackers may also "pivot" through the compromised host to attack other hosts "behind" the firewall.

The attacker social engineered the user into clicking on the malicious link and thereby exploited a known Microsoft Windows vulnerability. Social engineering attempts to trick people into taking specific actions. The linked website exploited a vulnerability in Windows .lnk files.

The Windows LNK exploit was patched with MS10-046. This exploited a vulnerability in "Windows Shell" that could allow remote code execution (2286198; <http://technet.microsoft.com/en-us/security/bulletin/MS10-046>).

MS10-046 was the same vulnerability exploited by Stuxnet, but it remained unpatched for several years. The attack required no user interaction; simply visiting a malicious site with Internet Explorer was enough to infect a system.

Prevention techniques against this attack include security awareness with emphasis on educating users not to click on anything in unsuspected emails. Obviously, patching Windows and keeping all software up to date would have eliminated this exploit from working altogether as well.

ANSWERS

- Adversary
 - IP Address: **10.167.197[.]38**
- Victim
 - IP Address: 192.168.2[.]33
 - Port Exploited (e.g., 80/TCP): 80/TCP
 - Protocol Exploited (e.g., HTTP): **HTTP**
- Stage 2 Infrastructure
 - IP Address: 10.167.197[.]38
 - Port Used (e.g., 80/TCP): 80/TCP
 - Protocol Used (e.g., HTTP): HTTP
 - File name: **NflzLHZF.dll**
- C2 Infrastructure
 - IP Address: 10.167.197[.]38
 - Port Used (e.g. 80/TCP) 4444/TCP
 - Protocol Used (e.g., HTTP): **VNC**
 -