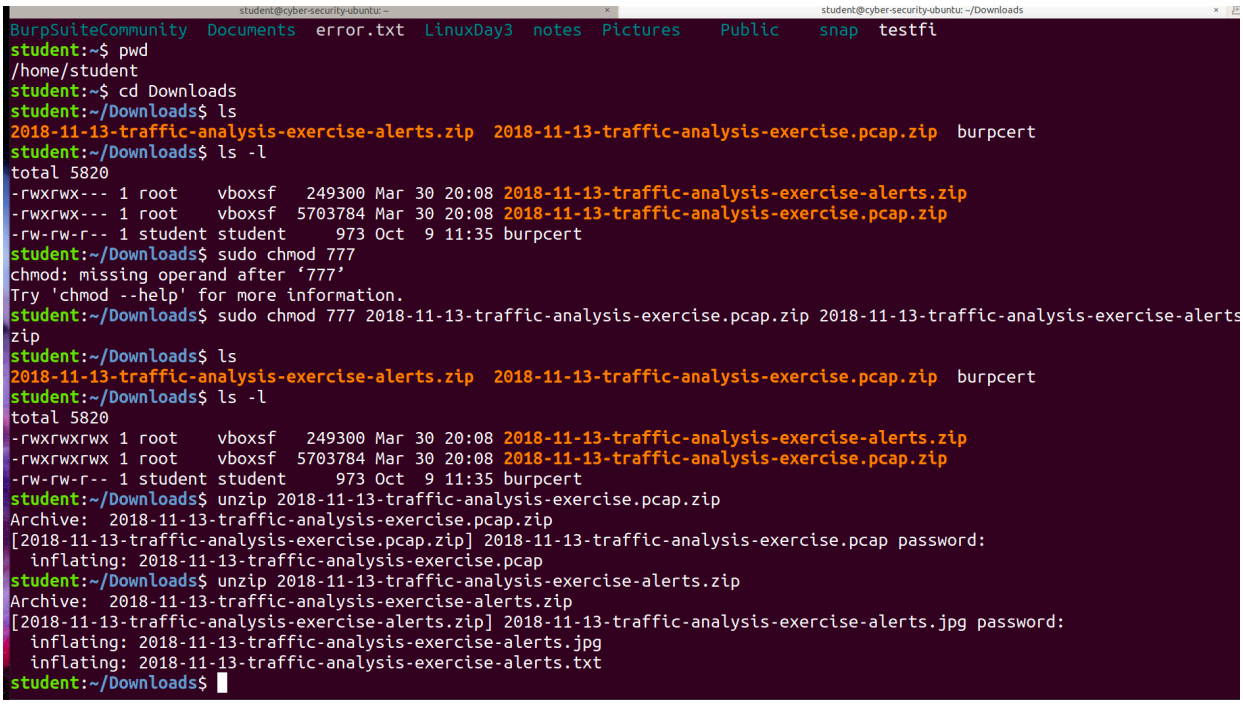
Homework 16 Assignment -Post Incident Report

2018-11-13 - TRAFFIC ANALYSIS EXERCISE - TURKEY AND DEFENCE

Snort is reporting on the zip archive of the pcap 2018-11-13-traffic-analysis-exercise.pcap.zip and the zip archive of the alert 2018-11-13-traffic-analysis-exercise-alerts.zip.



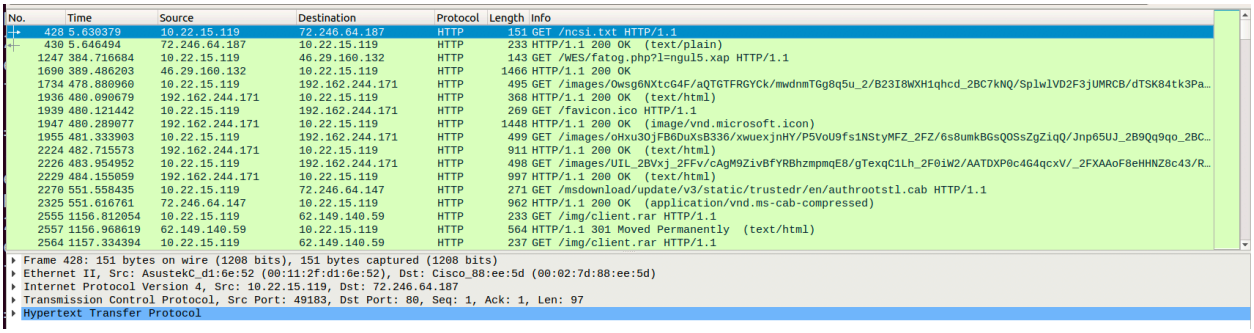
- Created a shared folder
- Changed properties in ubuntu settings
- Change file permissions

```
--------------------------------------------------------------------------------
Date/Time: 2018-11-07 21:03 UTC
ETPRO TROJAN Zeus Panda Banker / Urnsif Malicious SSL Certificate Detected
46.229.214.92 -> 10.22.15.119
IPVer=4 hlen=5 tos=0 dlen=980 ID=0 flags=0 offset=0 ttl=0 chksum=38998
Protocol: 6 sport=443 -> dport=49232

Seq=0 Ack=0 Off=5 Res=0 Flags=******** Win=0 urp=995 chksum=0
--------------------------------------------------------------------------------
Date/Time: 2018-11-07 21:03 UTC
ETPRO TROJAN Zeus Panda Banker / Urnsif Malicious SSL Certificate Detected
46.229.214.92 -> 10.22.15.119
IPVer=4 hlen=5 tos=0 dlen=980 ID=0 flags=0 offset=0 ttl=0 chksum=38998
Protocol: 6 sport=443 -> dport=49233

Seq=0 Ack=0 Off=5 Res=0 Flags=******** Win=0 urp=33865 chksum=0
--------------------------------------------------------------------------------
Date/Time: 2018-11-07 21:20 UTC
ETPRO TROJAN Zeus Panda Banker / Urnsif Malicious SSL Certificate Detected
46.229.214.92 -> 10.22.15.119
IPVer=4 hlen=5 tos=0 dlen=980 ID=0 flags=0 offset=0 ttl=0 chksum=38998
Protocol: 6 sport=443 -> dport=49298

Seq=0 Ack=0 Off=5 Res=0 Flags=******** Win=0 urp=30616 chksum=0
--------------------------------------------------------------------------------
Date/Time: 2018-11-07 21:20 UTC
ETPRO TROJAN Zeus Panda Banker / Urnsif Malicious SSL Certificate Detected
46.229.214.92 -> 10.22.15.119
IPVer=4 hlen=5 tos=0 dlen=980 ID=0 flags=0 offset=0 ttl=0 chksum=38998
Protocol: 6 sport=443 -> dport=49299

Seq=0 Ack=0 Off=5 Res=0 Flags=******** Win=0 urp=64542 chksum=0
student:~/Downloads$
```

Analysis of the alert file reveals a malicious “TROJAN” alert. The destination IP is 46.229.214.92 whereas the source IP is 10.22.15.119. Here, we see the source port 443 and destination 49232. The attack occurred on 11/07/2018 at 21:03.

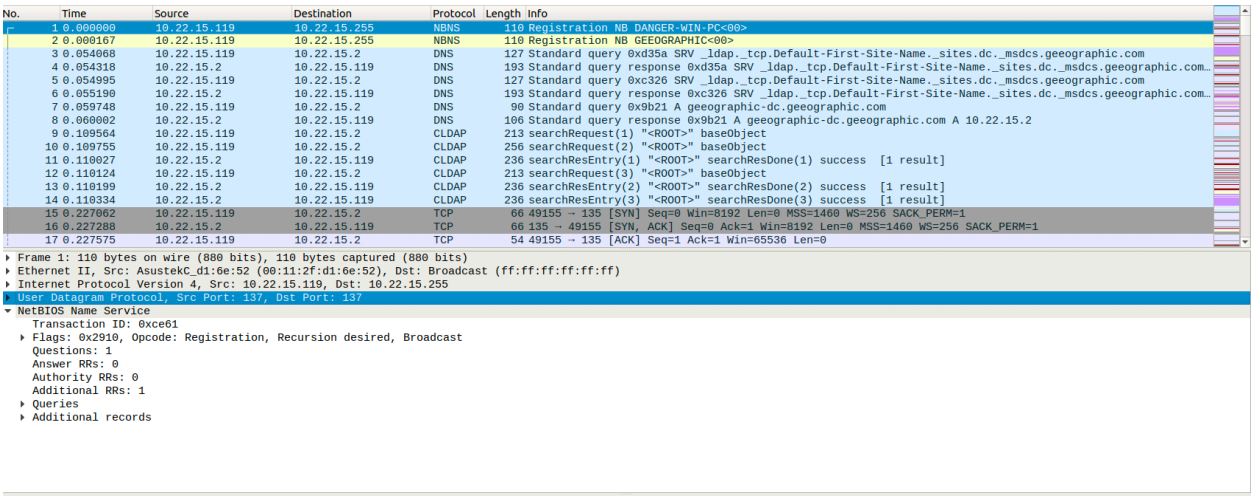
Wireshark Analysis

Wireshark analysis shows snort is flagging the internal IP 10.22.15.119 and the external IP 46.29.160.132. Based on the pcap analysis, there is GET request being sent to the target IP address and the output is a 200 OK response.



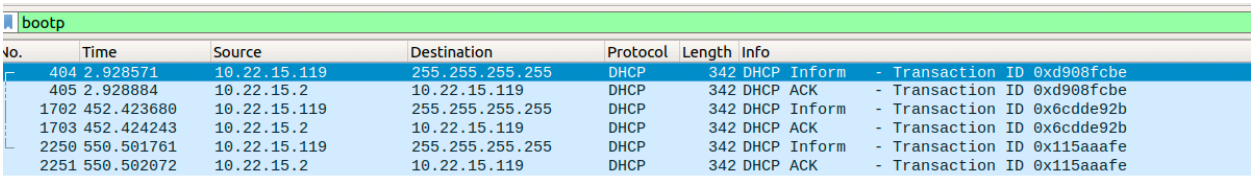
No.	Time	Source	Destination	Protocol	Length	Info
428	5.630379	10.22.15.119	72.246.64.187	HTTP	151	GET /ncsi.txt HTTP/1.1
430	5.646494	72.246.64.187	10.22.15.119	HTTP	233	HTTP/1.1 200 OK (text/plain)
1247	384.716684	10.22.15.119	46.29.160.132	HTTP	143	GET /WES/fatog.php?l=ngul5.xap HTTP/1.1
1690	389.486203	46.29.160.132	10.22.15.119	HTTP	1466	HTTP/1.1 200 OK
1734	478.880960	10.22.15.119	192.162.244.171	HTTP	495	GET /images/Owsg6NXtcG4F/aQTGTFRGYCk/mwdnmTGg8q5u_2/B23I8WXH1qhcd_2BC7kNQ/SplwlVD2F3jUMRCB/dTSK84tk3Pa…
1936	480.090679	192.162.244.171	10.22.15.119	HTTP	368	HTTP/1.1 200 OK (text/html)
1939	480.121442	10.22.15.119	192.162.244.171	HTTP	269	GET /favicon.ico HTTP/1.1
1947	480.289077	192.162.244.171	10.22.15.119	HTTP	1448	HTTP/1.1 200 OK (image/vnd.microsoft.icon)
1955	481.333903	10.22.15.119	192.162.244.171	HTTP	499	GET /images/oHxu3OjFB6DuXsB336/xwuexjnHY/P5VoU9fs1NStyMFZ_2FZ/6s8umkBGsQOSsZgZiqQ/Jnp65UJ_2B9Qq9qo_2BC…
2224	482.715573	192.162.244.171	10.22.15.119	HTTP	911	HTTP/1.1 200 OK (text/html)
2226	483.954952	10.22.15.119	192.162.244.171	HTTP	498	GET /images/UIL_2BVxj_2FFv/cAgM9ZivBfYRBhzmpmqE8/gTexqC1Lh_2F0iW2/AATDXP0c4G4qcxV/_2FXAAoF8eHHNZ8c43/R…
2229	484.155059	192.162.244.171	10.22.15.119	HTTP	997	HTTP/1.1 200 OK (text/html)
2270	551.558435	10.22.15.119	72.246.64.147	HTTP	271	GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab HTTP/1.1
2325	551.616761	72.246.64.147	10.22.15.119	HTTP	962	HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)
2555	1156.812054	10.22.15.119	62.149.140.59	HTTP	233	GET /img/client.rar HTTP/1.1
2557	1156.968619	62.149.140.59	10.22.15.119	HTTP	564	HTTP/1.1 301 Moved Permanently (text/html)
2564	1157.334394	10.22.15.119	62.149.140.59	HTTP	237	GET /img/client.rar HTTP/1.1

Further analysis shows DHCP packets, which indicates a request for an IP address. Applying the bootp filter will show these DHCP packets and their associated IP addresses in the attack, specifically checking the DHCP inform packet to discover host name.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.22.15.119	10.22.15.255	NBNS	110	Registration NB DANGER-WIN-PC<00>
2	0.000167	10.22.15.119	10.22.15.255	NBNS	110	Registration NB GEEOGRAPHIC<00>
3	0.054068	10.22.15.119	10.22.15.2	DNS	127	Standard query 0xd35a SRV _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.geeographic.com
4	0.054318	10.22.15.2	10.22.15.119	DNS	193	Standard query response 0xd35a SRV _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.geeographic.com…
5	0.054995	10.22.15.119	10.22.15.2	DNS	127	Standard query 0xc326 SRV _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.geeographic.com
6	0.055190	10.22.15.2	10.22.15.119	DNS	193	Standard query response 0xc326 SRV _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.geeographic.com…
7	0.059748	10.22.15.119	10.22.15.2	DNS	90	Standard query 0x9b21 A geeographic-dc.geeographic.com
8	0.060002	10.22.15.2	10.22.15.119	DNS	106	Standard query response 0x9b21 A geeographic-dc.geeographic.com A 10.22.15.2
9	0.109564	10.22.15.119	10.22.15.2	CLDAP	213	searchRequest(1) "<ROOT>" baseObject
10	0.109755	10.22.15.119	10.22.15.2	CLDAP	256	searchRequest(2) "<ROOT>" baseObject
11	0.110027	10.22.15.2	10.22.15.119	CLDAP	236	searchResEntry(1) "<ROOT>" searchResDone(1) success [1 result]
12	0.110124	10.22.15.119	10.22.15.2	CLDAP	213	searchRequest(3) "<ROOT>" baseObject
13	0.110199	10.22.15.2	10.22.15.119	CLDAP	236	searchResEntry(2) "<ROOT>" searchResDone(2) success [1 result]
14	0.110334	10.22.15.2	10.22.15.119	CLDAP	236	searchResEntry(3) "<ROOT>" searchResDone(3) success [1 result]
15	0.227062	10.22.15.119	10.22.15.2	TCP	66	49155 → 135 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
16	0.227288	10.22.15.2	10.22.15.119	TCP	66	135 → 49155 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
17	0.227575	10.22.15.119	10.22.15.2	TCP	54	49155 → 135 [ACK] Seq=1 Ack=1 Win=65536 Len=0

```
▸ Frame 1: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
▸ Ethernet II, Src: AsustekC_d1:6e:52 (00:11:2f:d1:6e:52), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▸ Internet Protocol Version 4, Src: 10.22.15.119, Dst: 10.22.15.255
▸ User Datagram Protocol, Src Port: 137, Dst Port: 137
▾ NetBIOS Name Service
    Transaction ID: 0xce61
  ▸ Flags: 0x2910, Opcode: Registration, Recursion desired, Broadcast
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  ▸ Queries
  ▸ Additional records
```



bootp

No.	Time	Source	Destination	Protocol	Length	Info
404	2.928571	10.22.15.119	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0xd908fcbe
405	2.928884	10.22.15.2	10.22.15.119	DHCP	342	DHCP ACK - Transaction ID 0xd908fcbe
1702	452.423680	10.22.15.119	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0x6cdde92b
1703	452.424243	10.22.15.2	10.22.15.119	DHCP	342	DHCP ACK - Transaction ID 0x6cdde92b
2250	550.501761	10.22.15.119	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0x115aaafe
2251	550.502072	10.22.15.2	10.22.15.119	DHCP	342	DHCP ACK - Transaction ID 0x115aaafe

DHCP packets – when a computer requests an IP address

```
▸ Frame 2250: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
▸ Ethernet II, Src: AsustekC_d1:6e:52 (00:11:2f:d1:6e:52), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▸ Internet Protocol Version 4, Src: 10.22.15.119, Dst: 255.255.255.255
▾ User Datagram Protocol, Src Port: 68, Dst Port: 67
    Source Port: 68
    Destination Port: 67
    Length: 308
    Checksum: 0x79d3 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 16]
▾ Bootstrap Protocol (Inform)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x115aaafe
    Seconds elapsed: 0
  ▸ Bootp flags: 0x0000 (Unicast)
    Client IP address: 10.22.15.119
    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: AsustekC_d1:6e:52 (00:11:2f:d1:6e:52)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ▸ Option: (53) DHCP Message Type (Inform)
  ▸ Option: (61) Client identifier
  ▾ Option: (12) Host Name
      Length: 13
      Host Name: Danger-Win-PC
  ▸ Option: (60) Vendor class identifier
  ▸ Option: (55) Parameter Request List
  ▸ Option: (255) End
    Padding: 0000000000000
```

The bootstrap protocol shows the source port 68 and destination port 67. In addition, we are given the host name “Danger-Win-PC” under options. The internet protocol confirms the source and destination IP addresses previously mentioned. Other information shows the MAC address “AsustekC_d1:6e:52” of the internal machine. One can assume that this is a web attack, and a true positive.

SHELLSHOCK.TAR

```
root:/media/sf_Ubuntu_shared# mv 'Unit_16-HOMEWORK_ASSIGNMENT_Instructions_Resources_shellshock (1).tar' /home/student/Downloa
ds
root:/media/sf_Ubuntu_shared# exit
exit
student:/media$ cd home/student
bash: cd: home/student: No such file or directory
student:/media$ cd /home/stuent/Downloads
bash: cd: /home/stuent/Downloads: No such file or directory
student:/media$ cd /home/student
student:~$ ls
anyname             Desktop    Downloads  file.txt   Music  passwd.txt  Projects  sh    Templates  Videos
BurpSuiteCommunity  Documents  error.txt  LinuxDay3  notes  Pictures    Public    snap  testfi
student:~$ cd Downloads
student:~/Downloads$ ls
 2018-11-13-traffic-analysis-exercise-alerts.jpg   2018-11-13-traffic-analysis-exercise.pcap.zip
 2018-11-13-traffic-analysis-exercise-alerts.txt   burpcert
 2018-11-13-traffic-analysis-exercise-alerts.zip  'Unit_16-HOMEWORK_ASSIGNMENT_Instructions_Resources_shellshock (1).tar'
 2018-11-13-traffic-analysis-exercise.pcap
student:~/Downloads$ ls -l
total 20500
-rw-r--r-- 1 student student  300739 Nov 13  2018  2018-11-13-traffic-analysis-exercise-alerts.jpg
-rw-rw-r-- 1 student student    9891 Nov 13  2018  2018-11-13-traffic-analysis-exercise-alerts.txt
-rwxrwxrwx 1 root    vboxsf   249300 Mar 30 20:08  2018-11-13-traffic-analysis-exercise-alerts.zip
-rw-r--r-- 1 student student 7737362 Apr 21  2019  2018-11-13-traffic-analysis-exercise.pcap
-rwxrwxrwx 1 root    vboxsf  5703784 Mar 30 20:08  2018-11-13-traffic-analysis-exercise.pcap.zip
-rw-rw-r-- 1 student student     973 Oct  9 11:35  burpcert
-rwxrwx--- 1 root    vboxsf  6973440 Mar 30 20:55 'Unit_16-HOMEWORK_ASSIGNMENT_Instructions_Resources_shellshock (1).tar'
student:~/Downloads$ sudo chmod 777 'Unit_16-HOMEWORK_ASSIGNMENT_Instructions_Resources_shellshock (1).tar'
student:~/Downloads$ ls -l
total 20500
-rw-r--r-- 1 student student  300739 Nov 13  2018  2018-11-13-traffic-analysis-exercise-alerts.jpg
-rw-rw-r-- 1 student student    9891 Nov 13  2018  2018-11-13-traffic-analysis-exercise-alerts.txt
-rwxrwxrwx 1 root    vboxsf   249300 Mar 30 20:08  2018-11-13-traffic-analysis-exercise-alerts.zip
-rw-r--r-- 1 student student 7737362 Apr 21  2019  2018-11-13-traffic-analysis-exercise.pcap
-rwxrwxrwx 1 root    vboxsf  5703784 Mar 30 20:08  2018-11-13-traffic-analysis-exercise.pcap.zip
-rw-rw-r-- 1 student student     973 Oct  9 11:35  burpcert
-rwxrwxrwx 1 root    vboxsf  6973440 Mar 30 20:55 'Unit_16-HOMEWORK_ASSIGNMENT_Instructions_Resources_shellshock (1).tar'
student:~/Downloads$
```

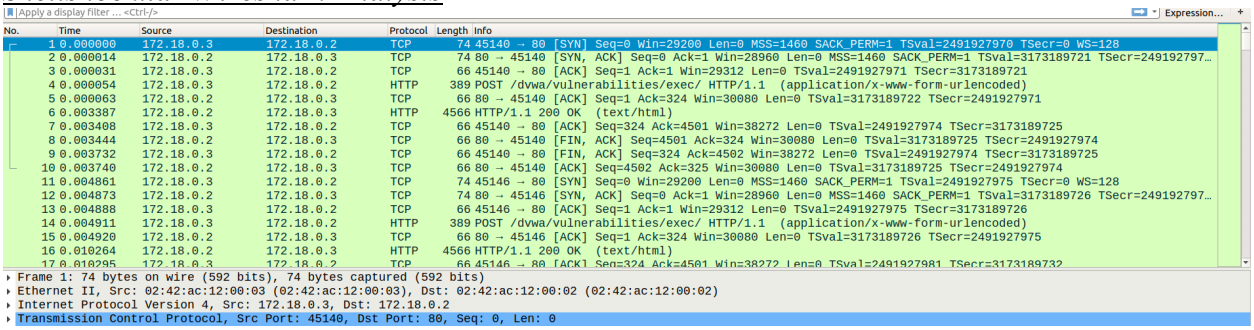
```
student:~/Downloads$ tar -xvf 'Unit_16-HOMEWORK_ASSIGNMENT_Instructions_Resources_shellshock (1).tar'
shellshock/
shellshock/alert
shellshock/serverLogs/
shellshock/serverLogs/error.log
shellshock/serverLogs/other_vhosts_access.log
shellshock/serverLogs/access.log
shellshock/network.pcap
student:~/Downloads$
```

In the second part of the post incident investigation, I used the same shared folder to move the tar file for further analysis. After accessing the tar file and changing student permissions. The image below shows the output when given the command ‘cat shellshock alert’

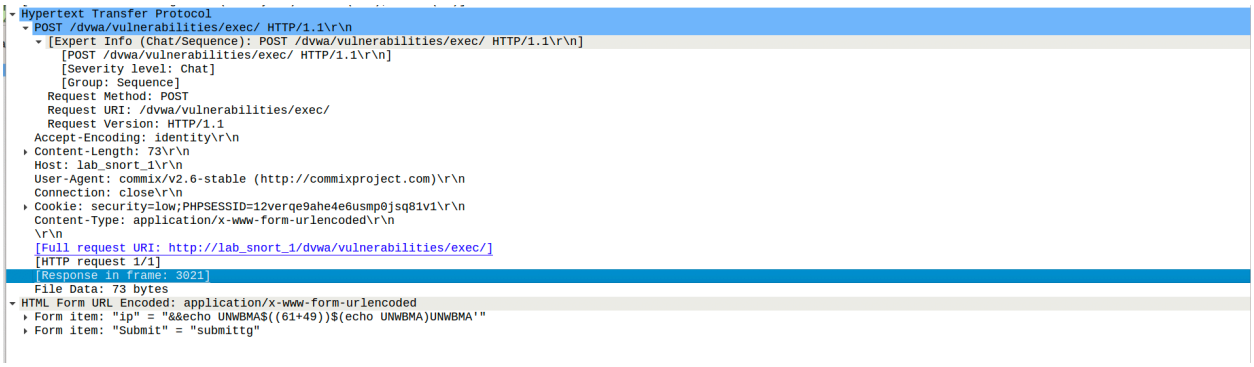
```
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2014-7169][Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2014-6
278][Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2014-6277][Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=20
14-6271]

[**] [1:31978:5] OS-OTHER Bash CGI environment variable injection attempt [**]
[Classification: Attempted Administrator Privilege Gain] [Priority: 1]
12/06-00:05:59.936963 172.18.0.3:47298 -> 172.18.0.2:80
TCP TTL:64 TOS:0x0 ID:47239 IpLen:20 DgmLen:284 DF
***A**** Seq: 0xB7CC5AB4  Ack: 0xF1FBA026  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=2014-6
278][Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2014-6277][Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=20
14-6271]

[**] [1:31978:5] OS-OTHER Bash CGI environment variable injection attempt [**]
[Classification: Attempted Administrator Privilege Gain] [Priority: 1]
12/06-00:05:59.940179 172.18.0.3:47304 -> 172.18.0.2:80
TCP TTL:64 TOS:0x0 ID:3702 IpLen:20 DgmLen:340 DF
***A**** Seq: 0x9705F894  Ack: 0x221D16D2  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=2014-6
278][Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2014-6277][Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=20
14-6271]

[**] [1:31978:5] OS-OTHER Bash CGI environment variable injection attempt [**]
[Classification: Attempted Administrator Privilege Gain] [Priority: 1]
12/06-00:05:59.943734 172.18.0.3:47310 -> 172.18.0.2:80
TCP TTL:64 TOS:0x0 ID:11511 IpLen:20 DgmLen:340 DF
***A**** Seq: 0x782669A6  Ack: 0x883A345F  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=2014-6
278][Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2014-6277][Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=20
14-6271]

[**] [1:31978:5] OS-OTHER Bash CGI environment variable injection attempt [**]
[Classification: Attempted Administrator Privilege Gain] [Priority: 1]
12/06-00:05:59.948162 172.18.0.3:47316 -> 172.18.0.2:80
TCP TTL:64 TOS:0x0 ID:19126 IpLen:20 DgmLen:340 DF
***A**** Seq: 0xD9CB5927  Ack: 0xB2D8521A  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=2014-6
278][Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2014-6277][Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=20
14-6271]

student:~/Downloads$
```

In this example, snort is flagging a shellshock alert; in the form of a possible injection attack. Shellshock uses vulnerabilities in the Unix command execution shellbash to allow hackers to gain remote control of a machine and execute arbitrary code. In the image above, the internal IP 172.18.0.3 machine is attempting to gain administrator access on another internal network 172.18.0.2.

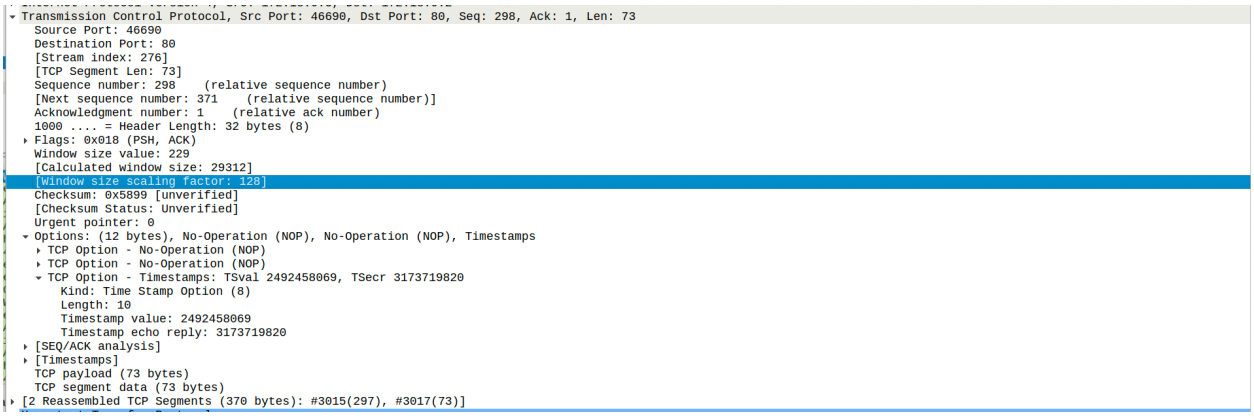
Shellshock.tar Wireshark Analysis



The shellshock/network.pcap shows the source IP address 172.18.0.2 initializes a tcp handshake followed by an HTTP POST request to a vulnerable web server “dvwa”. Further analysis reveals an “encoded url” the source port 45140 and destination port 80.



Here we discover the host name as “lab_snort_1” and user agent commixproject.com. This suggests that the attack is on a web server operating system. In this case, DVWA. Analysis also shows the content type in HTML form – in other words, variables such as “ip” = “&&echo UNWBMA$” and “submit” = “submittg” are set to execute arbitrary code on the web server. It However, it cannot be verified whether the malware was downloaded – indicating a potential false positive.



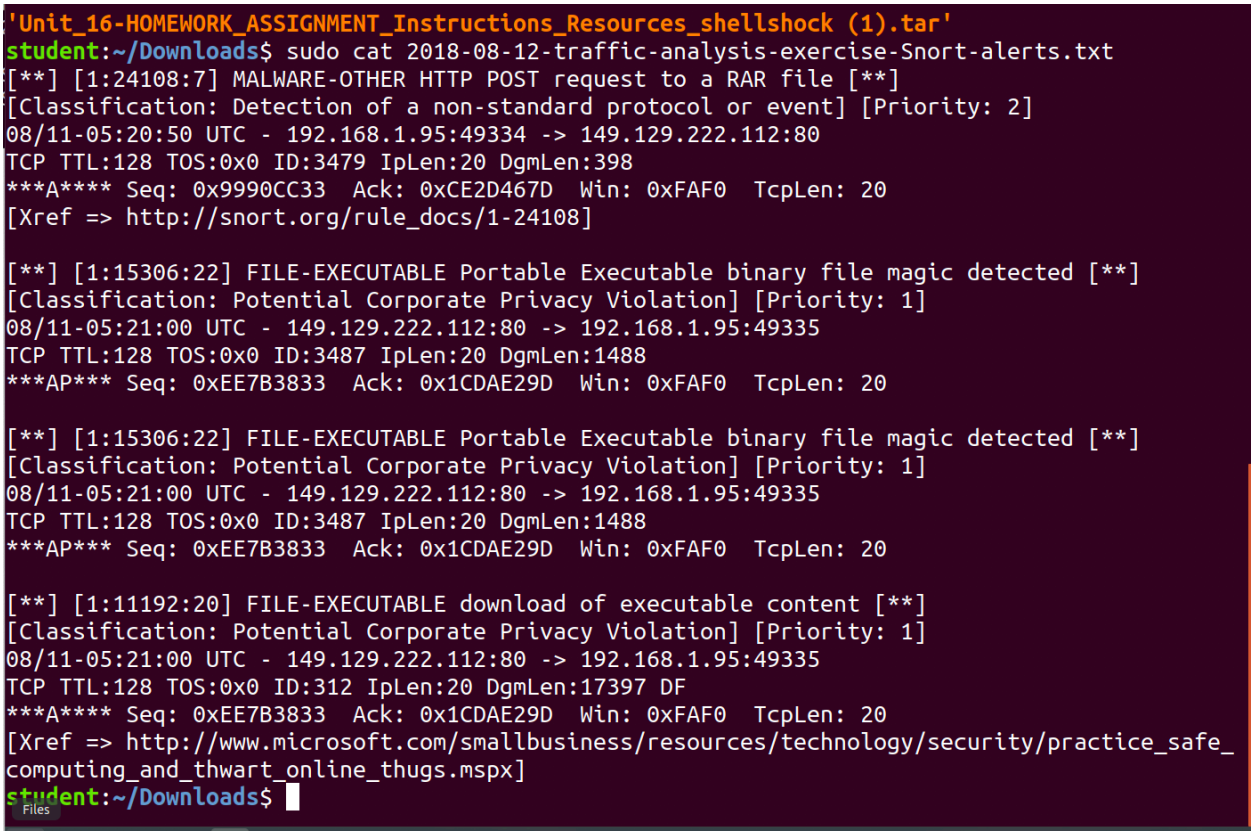
2018-08-12 - TRAFFIC ANALYSIS EXERCISE - SPUTNIK HOUSE

```
student:/media$ sudo bash
[sudo] password for student:
root:/media# ls
instructor  sf_Shared  sf_Ubuntu_shared  student
root:/media# cd sf_Ubuntu_shared
root:/media/sf_Ubuntu_shared# ls
 2018-08-12-traffic-analysis-exercise-alerts.zip   2019-01-28-alerts-for-traffic-analysis-exercise.txt.zip
 2018-08-12-traffic-analysis-exercise-emails.zip  '2019-01-28-traffic-analysis-exercise.pcap (1).zip'
 2018-08-12-traffic-analysis-exercise.pcap.zip     2019-01-28-traffic-analysis-exercise.pcap.zip
root:/media/sf_Ubuntu_shared# ls -l
total 31160
-rwxrwx--- 1 root vboxsf     3227 Mar 30 17:05  2018-08-12-traffic-analysis-exercise-alerts.zip
-rwxrwx--- 1 root vboxsf   309945 Mar 30 17:05  2018-08-12-traffic-analysis-exercise-emails.zip
-rwxrwx--- 1 root vboxsf 24595844 Mar 30 17:05  2018-08-12-traffic-analysis-exercise.pcap.zip
-rwxrwx--- 1 root vboxsf     1057 Mar 30 17:05  2019-01-28-alerts-for-traffic-analysis-exercise.txt.zip
-rwxrwx--- 1 root vboxsf  2163571 Mar 30 20:07 '2019-01-28-traffic-analysis-exercise.pcap (1).zip'
-rwxrwx--- 1 root vboxsf  2163571 Mar 30 17:05  2019-01-28-traffic-analysis-exercise.pcap.zip
root:/media/sf_Ubuntu_shared#
```

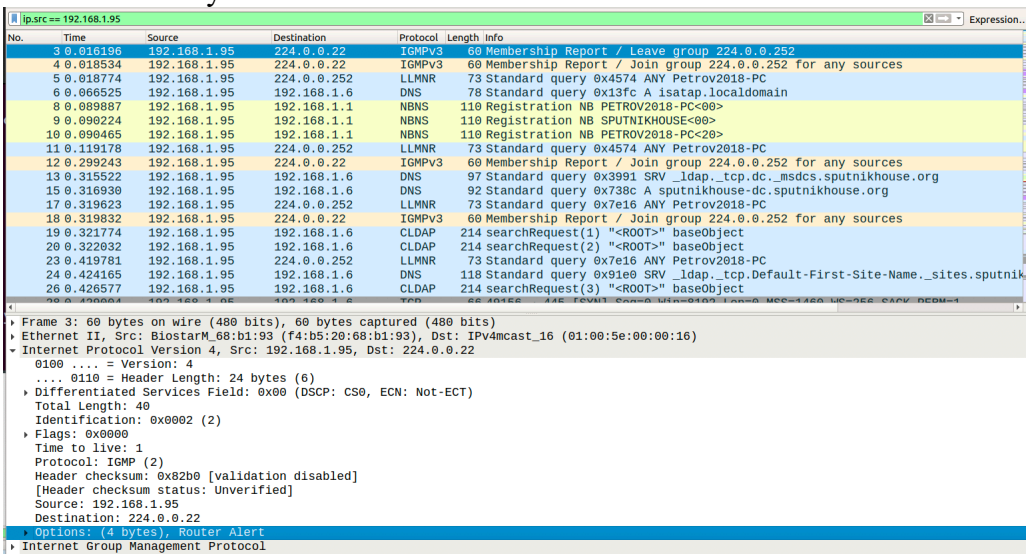
```
root:/media/sf_Ubuntu_shared# mv 2018-08-12-traffic-analysis-exercise-alerts.zip /home/student
root:/media/sf_Ubuntu_shared# mv 2018-08-12-traffic-analysis-exercise.pcap.zip /home/student
root:/media/sf_Ubuntu_shared# exit
exit
student:/media$ cd /home/student
student:~$ ls
2018-08-12-traffic-analysis-exercise-alerts.zip  BurpSuiteCommunity  Downloads  LinuxDay3  passwd.txt  Public  Templates
2018-08-12-traffic-analysis-exercise.pcap.zip    Desktop            error.txt  Music      Pictures    sh      testfi
anyname                                          Documents          file.txt   notes      Projects    snap    Videos
student:~$
```

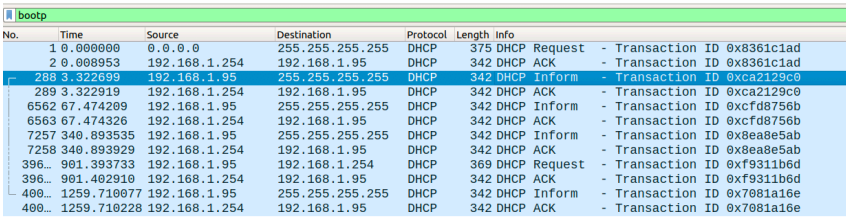
```
student:~$ mv 2018-08-12-traffic-analysis-exercise-alerts.zip Downloads
student:~$ mv 2018-08-12-traffic-analysis-exercise.pcap.zip Downloads
student:~$ cd Downloads
student:~/Downloads$ ls
 2018-08-12-traffic-analysis-exercise-alerts.zip
 2018-08-12-traffic-analysis-exercise.pcap.zip
 2018-11-13-traffic-analysis-exercise-alerts.jpg
 2018-11-13-traffic-analysis-exercise-alerts.txt
 2018-11-13-traffic-analysis-exercise-alerts.zip
 2018-11-13-traffic-analysis-exercise.pcap
 2018-11-13-traffic-analysis-exercise.pcap.zip
 burpcert
 shellshock
'Unit_16-HOMEWORK_ASSIGNMENT_Instructions_Resources_shellshock (1).tar'
student:~/Downloads$ unzip 2018-08-12-traffic-analysis-exercise.pcap.zip
error:  cannot open zipfile [ 2018-08-12-traffic-analysis-exercise.pcap.zip ]
        Permission denied
unzip:  cannot find or open 2018-08-12-traffic-analysis-exercise.pcap.zip, 2018-08-12-traffi
c-analysis-exercise.pcap.zip.zip or 2018-08-12-traffic-analysis-exercise.pcap.zip.ZIP.
student:~/Downloads$ sudo unzip 2018-08-12-traffic-analysis-exercise.pcap.zip
Archive:  2018-08-12-traffic-analysis-exercise.pcap.zip
[2018-08-12-traffic-analysis-exercise.pcap.zip] 2018-08-12-traffic-analysis-exercise.pcap pa
ssword:
password incorrect--reenter:
  inflating: 2018-08-12-traffic-analysis-exercise.pcap
student:~/Downloads$ sudo unzip 2018-08-12-traffic-analysis-exercise-alerts.zip
Archive:  2018-08-12-traffic-analysis-exercise-alerts.zip
[2018-08-12-traffic-analysis-exercise-alerts.zip] 2018-08-12-traffic-analysis-exercise-Snort
-alerts.txt password:
  inflating: 2018-08-12-traffic-analysis-exercise-Snort-alerts.txt
  inflating: 2018-08-12-traffic-analysis-exercise-Suricata-alerts.txt
student:~/Downloads$
```

Snort is flagging an alert and pcap file, with respect to an attack that occurred August 12th 2018 at 05:20 am. Analysis shows that the malicious file is in the form of a “Malware-Other HTTP POST request to a RAR file”. This attack differs from the previous alert, given that It is of higher priority. The internal IP address is 192.168.1.95 whereas the external IP is 149.129.222.112. The classification also indicates detection of a non-standard protocol, confirming that this attack is a true positive.



Wireshark Analysis





Again, there are DHCP packets which indicate that the attacker is requesting an IP address. This suggests that there is communication between the source IP 192.168.1.254 and the destination IP 255.255.255.255 – a broadcast address of the zero network or local network. This network is used to send broadcast packets by BOOTP and DHCP clients. By checking the DHCP inform packet, further analysis about the host can be revealed. In this case, the host is “Petrov2018-PC” and the MAC address is BiostarM_68. However, this attack seems to be a false positive.

```
Frame 288: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
Ethernet II, Src: BiostarM_68:b1:93 (f4:b5:20:68:b1:93), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 192.168.1.95, Dst: 255.255.255.255
User Datagram Protocol, Src Port: 68, Dst Port: 67
Bootstrap Protocol (Inform)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xca2129c0
    Seconds elapsed: 0
  Bootp flags: 0x0000 (Unicast)
    Client IP address: 192.168.1.95
    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: BiostarM_68:b1:93 (f4:b5:20:68:b1:93)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  Option: (53) DHCP Message Type (Inform)
  Option: (61) Client identifier
  Option: (12) Host Name
      Length: 13
      Host Name: Petrov2018-PC
  Option: (60) Vendor class identifier
  Option: (55) Parameter Request List
  Option: (255) End
    Padding: 00000000000000
```

In order to mitigate these malicious attacks, steps that should be taken include creating back-ups prior to the incident so the computer settings can be restored to its original state also wiping the hard drive for the purpose of re-imaging with secure software.

What steps should be taken in regard to network security?

- Install and configure a strong antivirus with IDS/IPS properties
- Configure alerts when suspicious emails and attachments are detected by the IDS / IPS