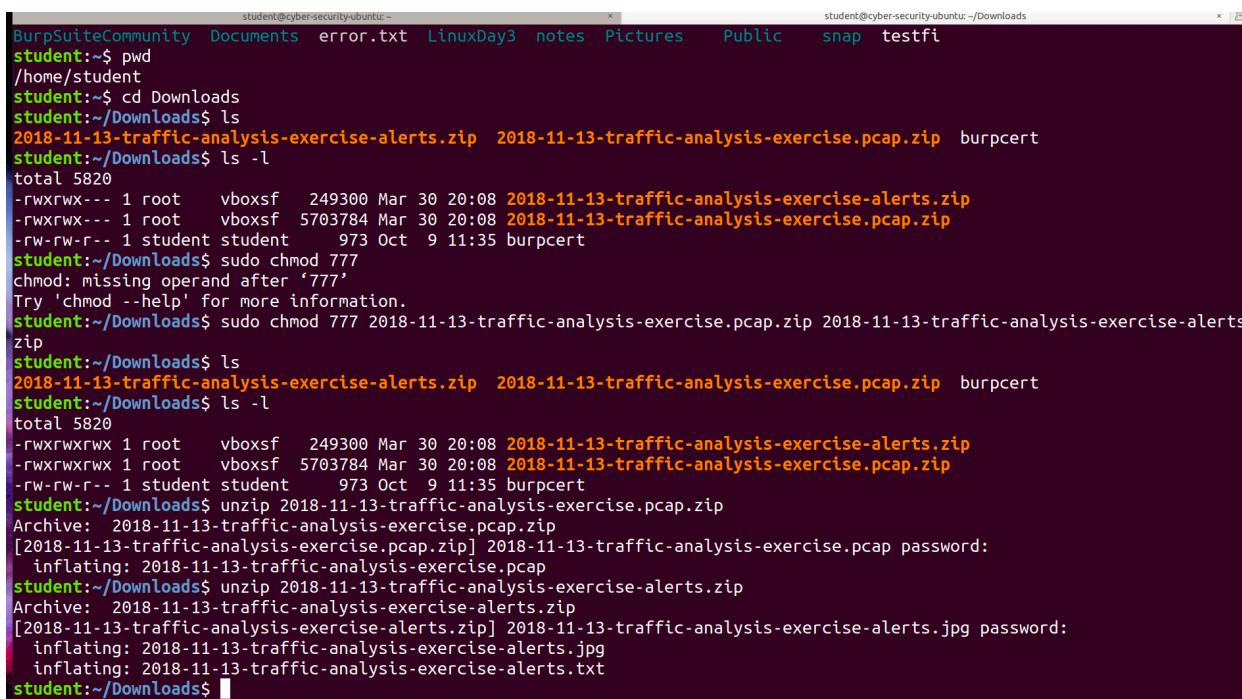

Homework 16 Assignment -Post Incident Report

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.



The screenshot shows a terminal window with two tabs. The left tab is titled 'student@cyber-security-ubuntu: ~' and the right tab is titled 'student@cyber-security-ubuntu: ~/Downloads'. The user is navigating through their home directory and then moving to the 'Downloads' folder. Inside 'Downloads', they list files and then use 'ls -l' to show detailed file information. They then use 'sudo chmod 777' on both '2018-11-13-traffic-analysis-exercise.pcap.zip' and '2018-11-13-traffic-analysis-exercise-alerts.zip'. Finally, they use 'unzip' to extract the contents of both files, specifying the password '2018-11-13-traffic-analysis-exercise.pcap' for the first one and '2018-11-13-traffic-analysis-exercise-alerts.zip' for the second.

```
student@cyber-security-ubuntu: ~
student:~$ pwd
/home/student
student:~$ cd Downloads
student:~/Downloads$ ls
2018-11-13-traffic-analysis-exercise-alerts.zip  2018-11-13-traffic-analysis-exercise.pcap.zip  burpcert
student:~/Downloads$ ls -l
total 5820
-rwxrwx--- 1 root    vboxsf  249300 Mar 30 20:08 2018-11-13-traffic-analysis-exercise-alerts.zip
-rwxrwx--- 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
student:~/Downloads$ sudo chmod 777
chmod: missing operand after '777'
Try 'chmod --help' for more information.
student:~/Downloads$ sudo chmod 777 2018-11-13-traffic-analysis-exercise.pcap.zip 2018-11-13-traffic-analysis-exercise-alerts.zip
student:~/Downloads$ ls
2018-11-13-traffic-analysis-exercise-alerts.zip  2018-11-13-traffic-analysis-exercise.pcap.zip  burpcert
student:~/Downloads$ ls -l
total 5820
-rwxrwxrwx 1 root    vboxsf  249300 Mar 30 20:08 2018-11-13-traffic-analysis-exercise-alerts.zip
-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
student:~/Downloads$ unzip 2018-11-13-traffic-analysis-exercise.pcap.zip
Archive: 2018-11-13-traffic-analysis-exercise.pcap.zip
[2018-11-13-traffic-analysis-exercise.pcap.zip] 2018-11-13-traffic-analysis-exercise.pcap password:
  inflating: 2018-11-13-traffic-analysis-exercise.pcap
student:~/Downloads$ unzip 2018-11-13-traffic-analysis-exercise-alerts.zip
Archive: 2018-11-13-traffic-analysis-exercise-alerts.zip
[2018-11-13-traffic-analysis-exercise-alerts.zip] 2018-11-13-traffic-analysis-exercise-alerts.jpg password:
  inflating: 2018-11-13-traffic-analysis-exercise-alerts.jpg
  inflating: 2018-11-13-traffic-analysis-exercise-alerts.txt
student:~/Downloads$
```

- 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 checksum=38998
Protocol: 6 sport=443 -> dport=49232

Seq=0 Ack=0 Off=5 Res=0 Flags=***** Win=0 urp=995 checksum=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 checksum=38998
Protocol: 6 sport=443 -> dport=49233

Seq=0 Ack=0 Off=5 Res=0 Flags=***** Win=0 urp=33865 checksum=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 checksum=38998
Protocol: 6 sport=443 -> dport=49298

Seq=0 Ack=0 Off=5 Res=0 Flags=***** Win=0 urp=30616 checksum=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 checksum=38998
Protocol: 6 sport=443 -> dport=49299

Seq=0 Ack=0 Off=5 Res=0 Flags=***** Win=0 urp=64542 checksum=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	
438 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 /WE/fatog.php?l=ngul5.xap HTTP/1.1	
1699 389.486203	46.29.160.132	10.22.15.119	HTTP	1466	HTTP/1.1 200 OK	
1734 478.889966	10.22.15.119	192.162.244.171	HTTP	495	GET /images/Owsgd6NxtcG4F/aGTGTFRGYCK/mwdnmTgg8q5u_2/B23I8WXH1qhcd_2BC7kNQ/Splw1VD2F3jUMRCB/dTSK84tk3Pa...	
1735 478.889970	10.22.15.119	192.162.244.171	HTTP	804	GET /index.html (text/html)	
1939 468.121442	10.22.15.119	192.162.244.171	HTTP	269	GET /favicon.ico HTTP/1.1	
1947 488.289077	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 /image/0xku0 FB60uxS8336/xuexjNHY/P5VoU9fs1NStyMFZ_2FZ/6s8umkBGSQ0SSzgZiQ/Jnp65UJ_2B9Qq9qo_2B...	
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 /image/URL_2BVxj_2FFv/c4pM9Z1vBfYRBhzmpmqE8/gTexqC1Lh_2F01W2/AATDXP0c4G4qcXV/_2FXAAoF8eHHNZ8c43/R...	
2229 484.155959	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/trusted/en/authrootssl.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	

Frame 428: 151 bytes on wire (1208 bits), 151 bytes captured (1208 bits)
 Ethernet II, Src: AsusTek_C_d16e:52 (00:11:2f:d1:6e:52), Dst: Cisco_88:ee:5d (00:02:7d:88:ee:5d)
 Internet Protocol Version 4, Src: 10.22.15.119, Dst: 72.246.64.187
 Transmission Control Protocol, Src Port: 49183, Dst Port: 80, Seq: 1, Ack: 1, Len: 97
 Hypertext Transfer Protocol

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>
1	0.054067	10.22.15.119	10.22.15.255	DNS	110	Registration NB DANGER-WIN-PC<00>
2	0.054068	10.22.15.119	10.22.15.255	DNS	127	Standard query 0xd35a SRV _ldap_tcp.Default-First-Site-Name._sites.dc._msdc...geographic.com
3	0.054318	10.22.15.119	10.22.15.255	DNS	193	Standard query response 0xd35a SRV _ldap_tcp.Default-First-Site-Name._sites.dc._msdc...geographic.com...
4	0.054495	10.22.15.2	10.22.15.119	DNS	193	Standard query response 0xc326 SRV _ldap_tcp.Default-First-Site-Name._sites.dc._msdc...geographic.com...
5	0.055199	10.22.15.2	10.22.15.119	DNS	193	Standard query response 0xc326 SRV _ldap_tcp.Default-First-Site-Name._sites.dc._msdc...geographic.com...
6	0.055748	10.22.15.2	10.22.15.119	DNS	99	Standard query 0x9b21 A geographic-dc.geographic.com A 10.22.15.2
7	0.060082	10.22.15.2	10.22.15.119	DNS	108	Standard query response 0x9b21 A geographic-dc.geographic.com A 10.22.15.2
8	0.060082	10.22.15.2	10.22.15.119	CLDAP	213	searchRequest(1) "<ROOT>" baseObject
9	0.109564	10.22.15.2	10.22.15.119	CLDAP	255	searchRequest(2) "<ROOT>" baseObject
10	0.109755	10.22.15.2	10.22.15.119	CLDAP	236	searchResEntry(1) "<ROOT>" searchResDone(1) success [1 result]
11	0.110027	10.22.15.2	10.22.15.119	CLDAP	213	searchRequest(3) "<ROOT>" baseObject
12	0.110124	10.22.15.119	10.22.15.2	CLDAP	236	searchResEntry(2) "<ROOT>" searchResDone(2) success [1 result]
13	0.110199	10.22.15.2	10.22.15.119	CLDAP	236	searchResEntry(3) "<ROOT>" searchResDone(3) success [1 result]
14	0.110334	10.22.15.2	10.22.15.119	CLDAP	66	49155 - 135 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
15	0.227062	10.22.15.119	10.22.15.2	TCP	66	49155 - 135 [SYN, ACK] Seq=0 Ack=1 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
 Question
 Authority RRs: 0
 Additional RRs: 1
 Queries
 Additional records

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

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

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

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/Downloads
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:~/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=2014-6278][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]
12/06-00:05:59.936963 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=2014-6278][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]
12/06-00:05:59.940179 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=2014-6278][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]
12/06-00:05:59.943734 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=2014-6278][Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2014-6277][Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2014-6271]

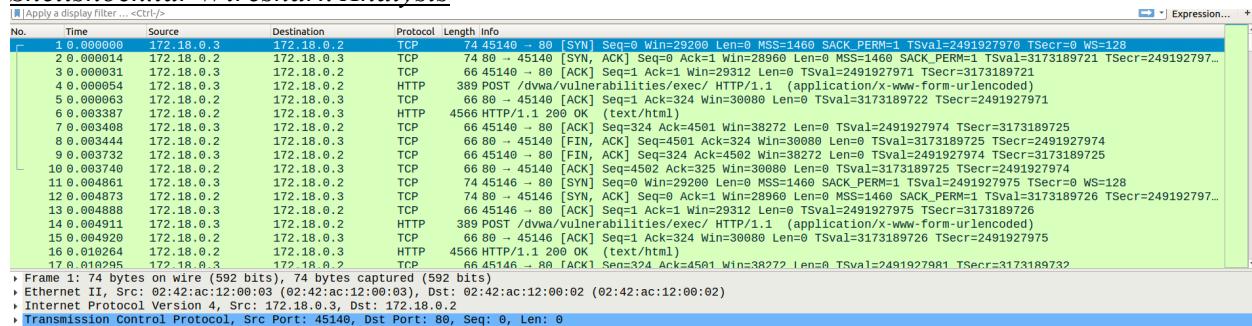
[**] [1:31978:5] OS-OTHER Bash CGI environment variable injection attempt [**]
[Classification: Attempted Administrator Privilege Gain] [Priority: 1]
12/06-00:05:59.948162 172.18.0.3:47316 -> 172.18.0.2:80
TCP TTL:64 TOS:0x0 ID:19126 IpLen:20 DgmLen:340 DF
***A**** Seq: 0xD9CB5927 Ack: 0xB2D8521A Win: 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=2014-6278][Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2014-6277][Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2014-6271]

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.

```

- Hypertext Transfer Protocol
  - POST /dwa/vulnerabilities/exec/ HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): POST /dwa/vulnerabilities/exec/ HTTP/1.1\r\n]
    [POST /dwa/vulnerabilities/exec/ HTTP/1.1\r\n]
    [Severity level: Chat]
    [Grouped requests]
    Request Method: POST
    Request URI: /dwa/vulnerabilities/exec/
    Request Version: HTTP/1.1
    Accept-Encoding: identity\r\n
    Content-Length: 73\r\n
    Host: lab_snort_1\r\n
    User-Agent: commix/v2.6-stable (http://commixproject.com)\r\n
    Connection: close\r\n
    Cookie: security=low;PHPSESSID=12verqe9ahe4e6usmp0jsq81v1\r\n
    Content-Type: application/x-www-form-urlencoded\r\n
    \r\n
    [Full request URL: http://lab_snort_1/dwa/vulnerabilities/exec/]
    [HTTP request 1/1]
    [Response in frame: 3021]
    File Data: 73 bytes
  - HTML Form URL Encoded: application/x-www-form-urlencoded
    > Form item: "ip" = "&&echo UNWBMA$((61+49))$(echo UNWBMA)UNWBMA"
    > Form item: "Submit" = "submittg"

```

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.

```

- Transmission Control Protocol, Src Port: 46690, Dst Port: 80, Seq: 298, Ack: 1, Len: 73
  Source Port: 46690
  Destination Port: 80
  [Stream index: 276]
  [TCP Segment Len: 73]
  Sequence number: 298 (relative sequence number)
  [Next sequence number: 371 (relative sequence number)]
  Acknowledgment number: 1 (relative ack number)
  1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x018 (PSH, ACK)
  Window size value: 229
  [Calculated window size: 29312]
  [Window size scaling factor: 128]
  Checksum: 0x5899 [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
  - Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    > TCP Option - No-Operation (NOP)
    > TCP Option - No-Operation (NOP)
    > TCP Option - Timestamps: TStamp 2492458069, TSecr 3173719820
      Kind: Time Stamp Option (8)
      Length: 10
      Timestamp value: 2492458069
      Timestamp echo reply: 3173719820
    [SEQ/ACK analysis]
    > [Timestamps]
    > TCP payload (73 bytes)
    > TCP segment data (73 bytes)
  > [2 Reassembled TCP Segments (370 bytes): #3015(297), #3017(73)]

```

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

```
instructor:~/Shared/sf_ubuntu_shared$ student
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  2018-01-28-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-traffic-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 password:
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.

```
'Unit_16-HOMEWORK_ASSIGNMENT_Instructions_Resources_shellshock (1).tar'
student:~/Downloads$ sudo cat 2018-08-12-traffic-analysis-exercise-Snort-alerts.txt
[**] [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: 0xAF0 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: 0xAF0 TcpLen: 20

[**] [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: 0xAF0 TcpLen: 20

[**] [1:11192:20] FILE-EXECUTABLE download of executable content [**]
[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:312 IpLen:20 DgmLen:17397 DF
***A*** Seq: 0xEE7B3833 Ack: 0x1CDAE29D Win: 0xAF0 TcpLen: 20
[Xref => http://www.microsoft.com/smallbusiness/resources/technology/security/practice_safe_computing_and_thwart_online_thugs.mspx]
student:~/Downloads$ █
```

Wireshark Analysis

ip.src == 192.168.1.95

No.	Time	Source	Destination	Protocol	Length	Info
3	0.016196	192.168.1.95	224.0.0.22	IGMPv3	60	Membership Report / Leave group 224.0.0.252
4	0.018534	192.168.1.95	224.0.0.22	IGMPv3	60	Membership Report / Join group 224.0.0.252 for any sources
5	0.018774	192.168.1.95	224.0.0.252	LLMNR	73	Standard query 0x4574 ANY Petrov2018-PC
6	0.066525	192.168.1.95	192.168.1.6	DNS	78	Standard query 0x13fc A isatap.localdomain
8	0.089887	192.168.1.95	192.168.1.1	NBNS	110	Registration NB SPUTNIKHOUSe<00>
9	0.090224	192.168.1.95	192.168.1.1	NBNS	110	Registration NB SPUTNIKHOUSe<00>
10	0.090465	192.168.1.95	192.168.1.1	NBNS	110	Registration NB PETROV2018-PC>2>
11	0.119178	192.168.1.95	224.0.0.252	LLMNR	73	Standard query 0x4574 ANY Petrov2018-PC
12	0.299243	192.168.1.95	224.0.0.22	IGMPv3	60	Membership Report / Join group 224.0.0.252 for any sources
13	0.315522	192.168.1.95	192.168.1.6	DNS	97	Standard query 0x3991 SRV _ldap._tcp.dc._msdcs.sputnikhouse.org
15	0.316938	192.168.1.95	192.168.1.6	DNS	92	Standard query 0x738 A sputnikhouse-dc.sputnikhouse.org
17	0.319623	192.168.1.95	224.0.0.252	LLMNR	73	Standard query 0x7e16 ANY Petrov2018-PC
18	0.319832	192.168.1.95	224.0.0.22	IGMPv3	60	Membership Report / Join group 224.0.0.252 for any sources
19	0.321774	192.168.1.95	192.168.1.6	CLDAP	214	searchRequest(1) "<ROOT>" baseObject
20	0.322632	192.168.1.95	192.168.1.6	CLDAP	214	searchRequest(2) "<ROOT>" baseObject
23	0.419781	192.168.1.95	224.0.0.252	LLMNR	73	Standard query 0x7e16 ANY Petrov2018-PC
24	0.424165	192.168.1.95	192.168.1.6	DNS	118	Standard query 0x91e0 SRV _ldap._tcp.Default-First-Site-Name._sites.sputnikhouse.org
26	0.426577	192.168.1.95	192.168.1.6	CLDAP	214	searchRequest(3) "<ROOT>" baseObject

Frame 3: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: BiostarM_68:b1:93 (f4:b5:20:68:b1:93), Dst: IPv4mcast_16 (01:00:5e:00:00:16)
Internet Protocol Version 4, Src: 192.168.1.95, Dst: 224.0.0.22
0100 = Version: 4
.... 0110 = Header Length: 24 bytes (6)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 40
Identification: 0x0002 (2)
Flags: 0x0000
Time to live: 1
Protocol: IGMP (2)
Header checksum: 0x82b0 [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.1.95
Destination: 224.0.0.22
Options: (4 bytes), Router Alert
Internet Group Management Protocol

bootp

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	375	DHCP Request - Transaction ID 0x8361c1ad
2	0.008953	192.168.1.254	192.168.1.95	DHCP	342	DHCP ACK - Transaction ID 0x8361c1ad
288	3.322689	192.168.1.95	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0xca2129c0
289	3.322919	192.168.1.254	192.168.1.95	DHCP	342	DHCP ACK - Transaction ID 0xca2129c0
6562	67.474209	192.168.1.95	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0xcfcd8756b
6563	67.474326	192.168.1.254	192.168.1.95	DHCP	342	DHCP ACK - Transaction ID 0xcfcd8756b
7257	348.893535	192.168.1.95	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0x8eaade5ab
7258	348.893929	192.168.1.254	192.168.1.95	DHCP	342	DHCP ACK - Transaction ID 0x8eaade5ab
396...	901.393733	192.168.1.95	192.168.1.254	DHCP	369	DHCP Request - Transaction ID 0xf9311b6d
396...	901.402910	192.168.1.254	192.168.1.95	DHCP	342	DHCP ACK - Transaction ID 0xf9311b6d
400...	1259.710877	192.168.1.95	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0x7081a16e
400...	1259.710877	192.168.1.254	192.168.1.95	DHCP	342	DHCP ACK - Transaction ID 0x7081a16e

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
Boot 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: 00000000000000000000000000000000
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: 0000000000000000

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