Post Incident Report

“Shellshock”

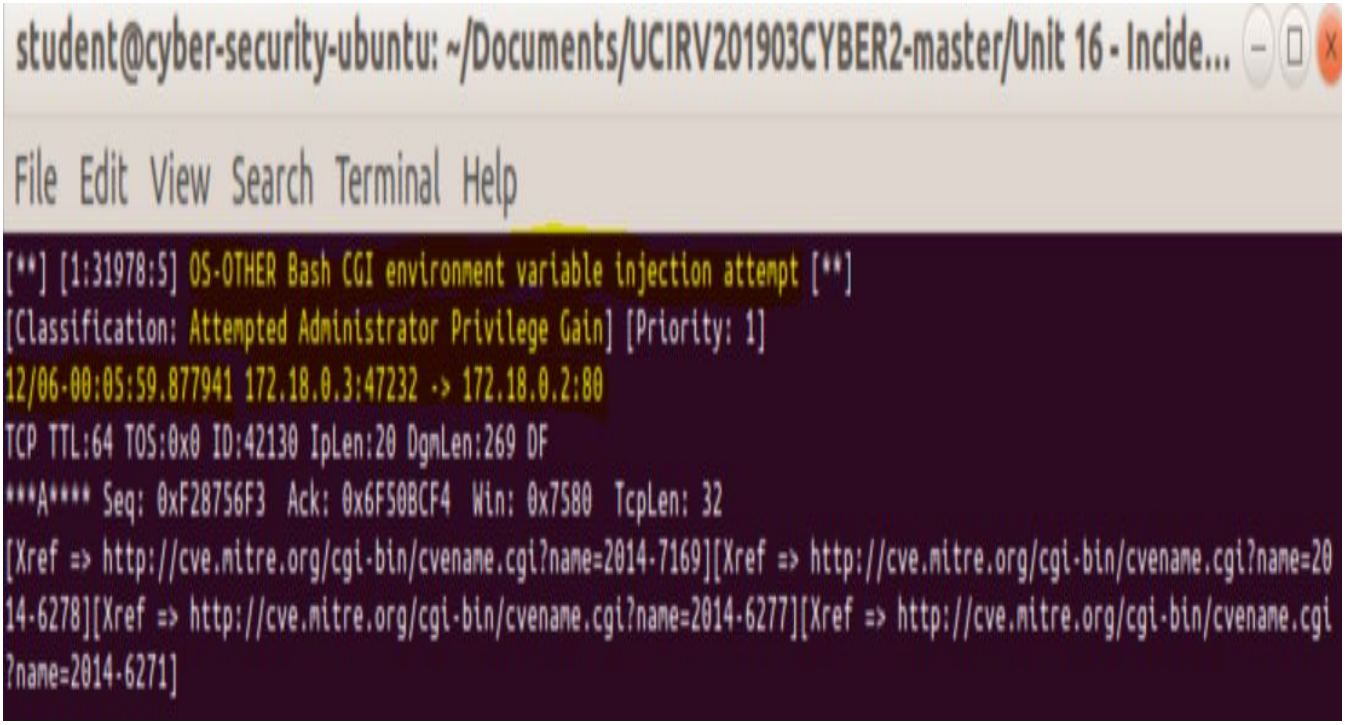
Date of investigation	2019/06/29
Date of incident	2018-12-05 UTC
Outcome	True Positive: Attacker was successful in the code injection in the web server application.
Action Taken	Precautions to the Web server with better sanitation and server needs to be more secured.
Reporting tool	Snort Alert, wireshark
Attack vector (Web, Email, Network, etc.)	Application Attack
Source IP/email	172.18.0.2
Source port	80
Destination IP/email	172.18.0.3
Destination port	47232

Narrative

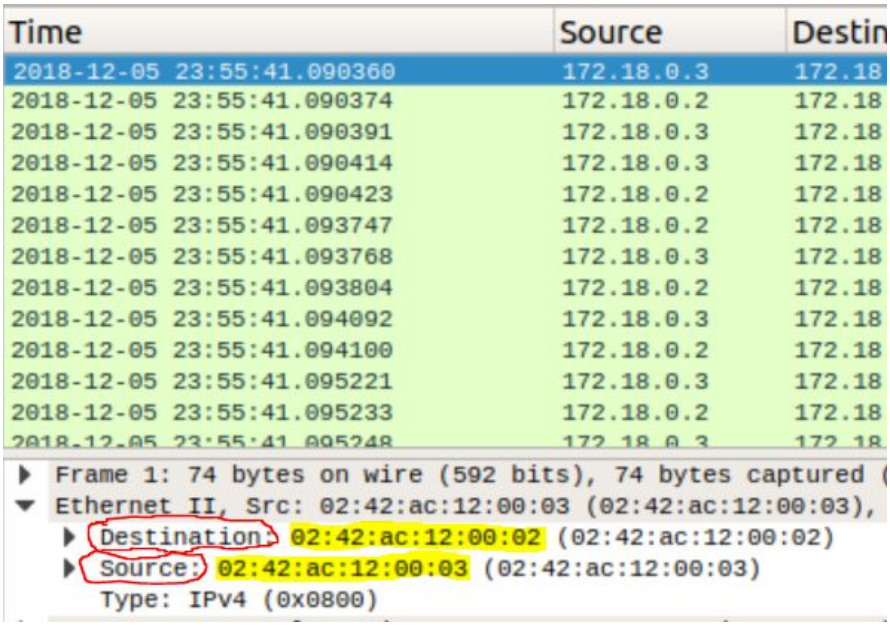
- Alerted by Snort:
    1. OS-OTHER Bash CGI environment variable injection attempt
    2. Attempted Administrator Privilege Gain

Post Incident Report

- Located Source/Destination IP Addresses and timestamp from Alerts:
  Date/Time: 2018-12-05 23:55:41
  SRC/PRT: 172.18.0.2:80
  DST/PRT: 172.18.0.3:47232



- Identified Host-name and Mac address of infected computer in pcap:
  Mac: Dest: 02:42:ac:12:00:02 & Src: 02:42:ac:12:00:03
  Host name: lab_snort_1\r\n

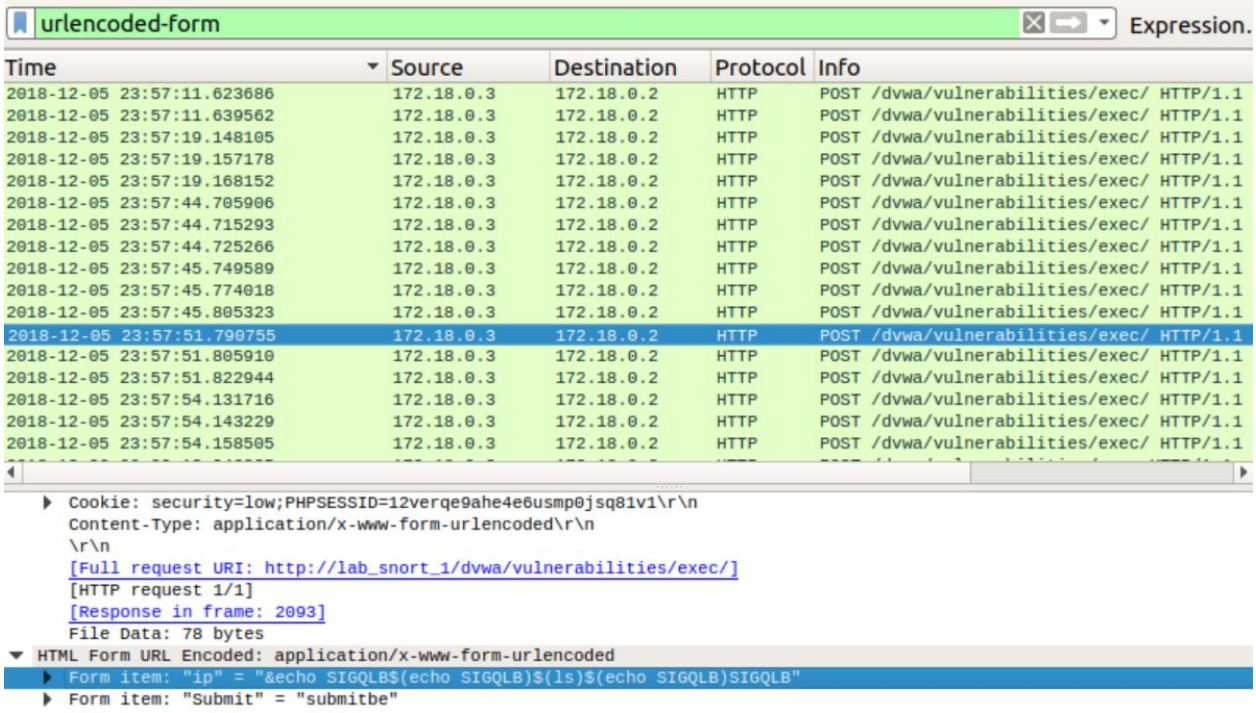


CamboRambo83

Post Incident Report

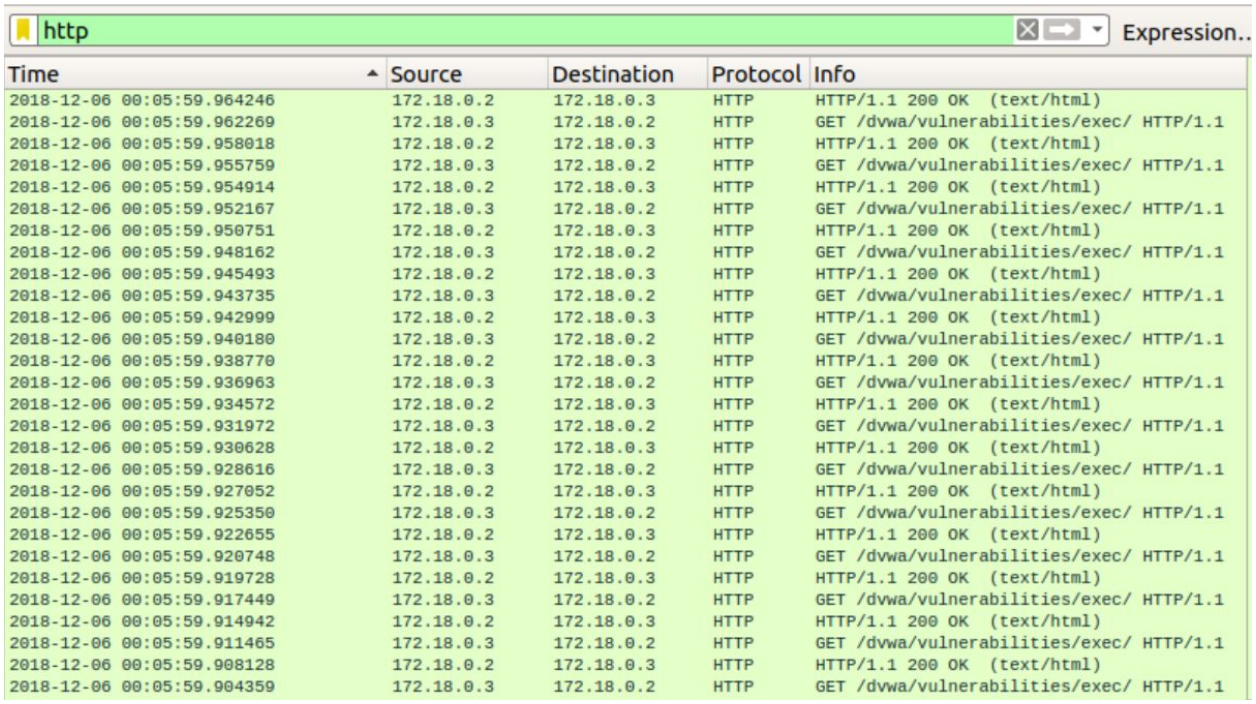
```
Hypertext Transfer Protocol
  POST /dvwa/vulnerabilities/exec/ HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): POST /dvwa/vulnerabilities/exec/ HTTP/1.1\r\n]
    Request Method: POST
    Request URI: /dvwa/vulnerabilities/exec/
    Request Version: HTTP/1.1
  Accept-Encoding: identity\r\n
  Content-Length: 78\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 URI: http://lab_snort_1/dvwa/vulnerabilities/exec/]
  [HTTP request 1/1]
  [Response in frame: 2093]
  File Data: 78 bytes
```

- Identified Filtering on "**urlencoded-form**" in pcap which shows the injection payloads in the packet that included many packets containing many Bash command execution. Under the 'HTML Form URL Encoded, there are values input like &echo SIGQLB$(echo SIGQLB)$(ls)$(echo SIGQLB)SIGQLB'



- The alert is accurate due to the data shown with the code injection attempts.

Post Incident Report



http

Expression..

Time	Source	Destination	Protocol	Info
2018-12-06 00:05:59.964246	172.18.0.2	172.18.0.3	HTTP	HTTP/1.1 200 OK (text/html)
2018-12-06 00:05:59.962269	172.18.0.3	172.18.0.2	HTTP	GET /dvwa/vulnerabilities/exec/ HTTP/1.1
2018-12-06 00:05:59.958018	172.18.0.2	172.18.0.3	HTTP	HTTP/1.1 200 OK (text/html)
2018-12-06 00:05:59.955759	172.18.0.3	172.18.0.2	HTTP	GET /dvwa/vulnerabilities/exec/ HTTP/1.1
2018-12-06 00:05:59.954914	172.18.0.2	172.18.0.3	HTTP	HTTP/1.1 200 OK (text/html)
2018-12-06 00:05:59.952167	172.18.0.3	172.18.0.2	HTTP	GET /dvwa/vulnerabilities/exec/ HTTP/1.1
2018-12-06 00:05:59.950751	172.18.0.2	172.18.0.3	HTTP	HTTP/1.1 200 OK (text/html)
2018-12-06 00:05:59.948162	172.18.0.3	172.18.0.2	HTTP	GET /dvwa/vulnerabilities/exec/ HTTP/1.1
2018-12-06 00:05:59.945493	172.18.0.2	172.18.0.3	HTTP	HTTP/1.1 200 OK (text/html)
2018-12-06 00:05:59.943735	172.18.0.3	172.18.0.2	HTTP	GET /dvwa/vulnerabilities/exec/ HTTP/1.1
2018-12-06 00:05:59.942999	172.18.0.2	172.18.0.3	HTTP	HTTP/1.1 200 OK (text/html)
2018-12-06 00:05:59.940180	172.18.0.3	172.18.0.2	HTTP	GET /dvwa/vulnerabilities/exec/ HTTP/1.1
2018-12-06 00:05:59.938770	172.18.0.2	172.18.0.3	HTTP	HTTP/1.1 200 OK (text/html)
2018-12-06 00:05:59.936963	172.18.0.3	172.18.0.2	HTTP	GET /dvwa/vulnerabilities/exec/ HTTP/1.1
2018-12-06 00:05:59.934572	172.18.0.2	172.18.0.3	HTTP	HTTP/1.1 200 OK (text/html)
2018-12-06 00:05:59.931972	172.18.0.3	172.18.0.2	HTTP	GET /dvwa/vulnerabilities/exec/ HTTP/1.1
2018-12-06 00:05:59.930628	172.18.0.2	172.18.0.3	HTTP	HTTP/1.1 200 OK (text/html)
2018-12-06 00:05:59.928616	172.18.0.3	172.18.0.2	HTTP	GET /dvwa/vulnerabilities/exec/ HTTP/1.1
2018-12-06 00:05:59.927052	172.18.0.2	172.18.0.3	HTTP	HTTP/1.1 200 OK (text/html)
2018-12-06 00:05:59.925350	172.18.0.3	172.18.0.2	HTTP	GET /dvwa/vulnerabilities/exec/ HTTP/1.1
2018-12-06 00:05:59.922655	172.18.0.2	172.18.0.3	HTTP	HTTP/1.1 200 OK (text/html)
2018-12-06 00:05:59.920748	172.18.0.3	172.18.0.2	HTTP	GET /dvwa/vulnerabilities/exec/ HTTP/1.1
2018-12-06 00:05:59.919728	172.18.0.2	172.18.0.3	HTTP	HTTP/1.1 200 OK (text/html)
2018-12-06 00:05:59.917449	172.18.0.3	172.18.0.2	HTTP	GET /dvwa/vulnerabilities/exec/ HTTP/1.1
2018-12-06 00:05:59.914942	172.18.0.2	172.18.0.3	HTTP	HTTP/1.1 200 OK (text/html)
2018-12-06 00:05:59.911465	172.18.0.3	172.18.0.2	HTTP	GET /dvwa/vulnerabilities/exec/ HTTP/1.1
2018-12-06 00:05:59.908128	172.18.0.2	172.18.0.3	HTTP	HTTP/1.1 200 OK (text/html)
2018-12-06 00:05:59.904359	172.18.0.3	172.18.0.2	HTTP	GET /dvwa/vulnerabilities/exec/ HTTP/1.1

- Filtered in Wireshark with “http” which then gave all the web requests that the attacker needed. There were no events of downloading requested, but the attacker had a specific agenda with only listing the contents of the webpage directory.

- From the investigation of the pcap this would definitely be classified as ‘True Positive’. The reason why is due to the success the attacker omitted with the command injection payload in the web application.

- This attack was done internally which had two internal IP addresses. The web server application must be secured with full security sanitation methods including better data input as well, to mitigate this attack.

- This attack was done with a code injection on the web application. It’s most likely to be an Application Attack.