EE379K Enterprise Network Security Lab 2 Report

Student: Brian Cheung bc32427
Professor: Mohit Tiwari
TA: Antonio Espinoza
Department of Electrical & Computer Engineering
The University of Texas at Austin

September 22, 2019

Part 1 - Vulnerable Web Apps

The task was to implement

1a - Set up a web-service in a container

1b - Getting familiar with strace

One of the methods to detect an exploit on the DVWA is to look for suspicious system calls using `strace`. Since DVWA was ran with Docker, a process called `containerd` executes the system calls for the container.
To get the PID of `containerd`, the following was run:

```
$ ps -ef | grep containerd
root      1155     1  0 09:36 ?        00:00:08 /usr/bin/containerd
```

`strace` can be attached to `containerd` and all of its forked child processes by running the following command:

```
$ sudo strace -p 1155 -o strace.txt -f
```

```
$ docker run --rm -it -p 80:80 vulnerables/web-dvwa
```

Injected bash command: `; echo "malware" > /tmp/maliciousfile`

```
28552 execve("/bin/sh", ["sh", "-c", "ping  -c 4 ; echo \"malware\" > /t"...], [/* 9
...
28552 open("/tmp/maliciousfile", O_WRONLY|O_CREAT|O_TRUNC, 0666) = 3
28552 fcntl(1, F_DUPFD, 10)             = 10
28552 close(1)                          = 0
28552 fcntl(10, F_SETFD, FD_CLOEXEC)    = 0
28552 dup2(3, 1)                        = 1
28552 close(3)                          = 0
28552 write(1, "malware\n", 8)          = 8
28552 dup2(10, 1)                       = 1
28552 close(10)                         = 0
28552 exit_group(0)                     = ?
28552 +++ exited with 0 +++
```

Part 2 - SELinux

The task was to implement

2a - Set up

Conclusion

The lab took about 40 hours which was a bit longer than expected. It was pretty interesting learning about socket connections in different languages and how GET requests are built using socket connections. I think some parts of the lab were a little unclear and needed further clarification. Overall, this lab served its purpose in providing a more hands-on experience that helped improve my understanding of networking.

References

[1] name, "title."