Network Administration/System Administration (NTU CSIE, Spring 2024) Lab 15 - Nmap & Password Cracking

B12902110 呂承諺

June 3, 2024

1 Nmap

Steps

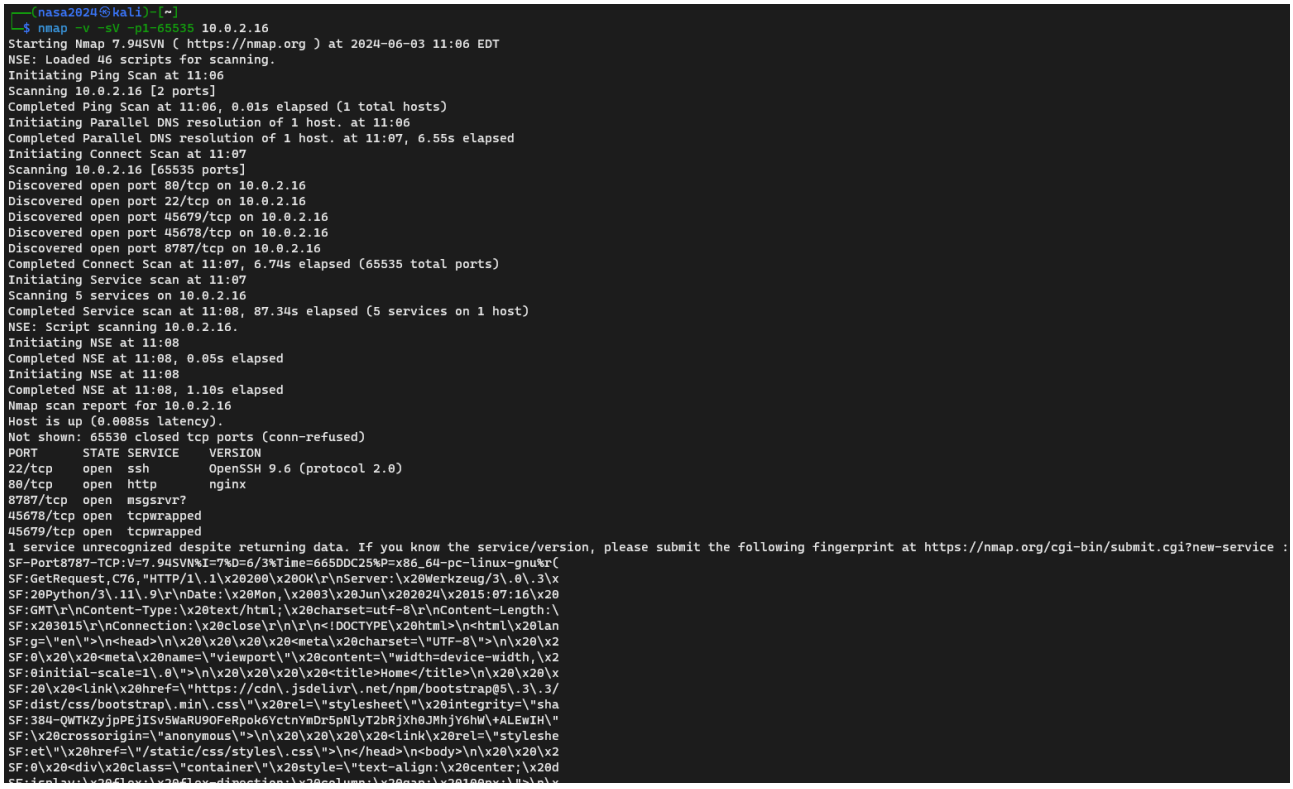
1. SSH into the Kali VM from the Debian VM.

```
nasa2024@debian:~$ ssh -p 10022 localhost
```

2. Scan open ports on `10.0.2.16` with Nmap.

```
nasa2024@kali-[~] $ nmap -v -sV -p1-65535 10.0.2.16
```

Result



2 Password Cracking

Steps

1. Access `http://localhost:18787/` on the Debian VM. We see that user `admin` has a hashed password of `$2b$12$MUZRi07d.hFjdek1NPPbh.4G2SgpmpAnl6ZwhBNrtXqRK8hgJV8Da`.

2. Save the password as a text file in the Kali VM.

```
nasa2024@kali-[~] $ echo \
  '$2b$12$MUZRi07d.hFjdek1NPPbh.4G2SgpmpAnl6ZwhBNrtXqRK8hgJV8Da' \
  > admin_password.txt
```

3. Unzip `/usr/share/wordlists/rockyou.txt.gz`

```
nasa2024@kali-[/usr/share/wordlists] $ sudo gunzip rockyou.txt.gz
```

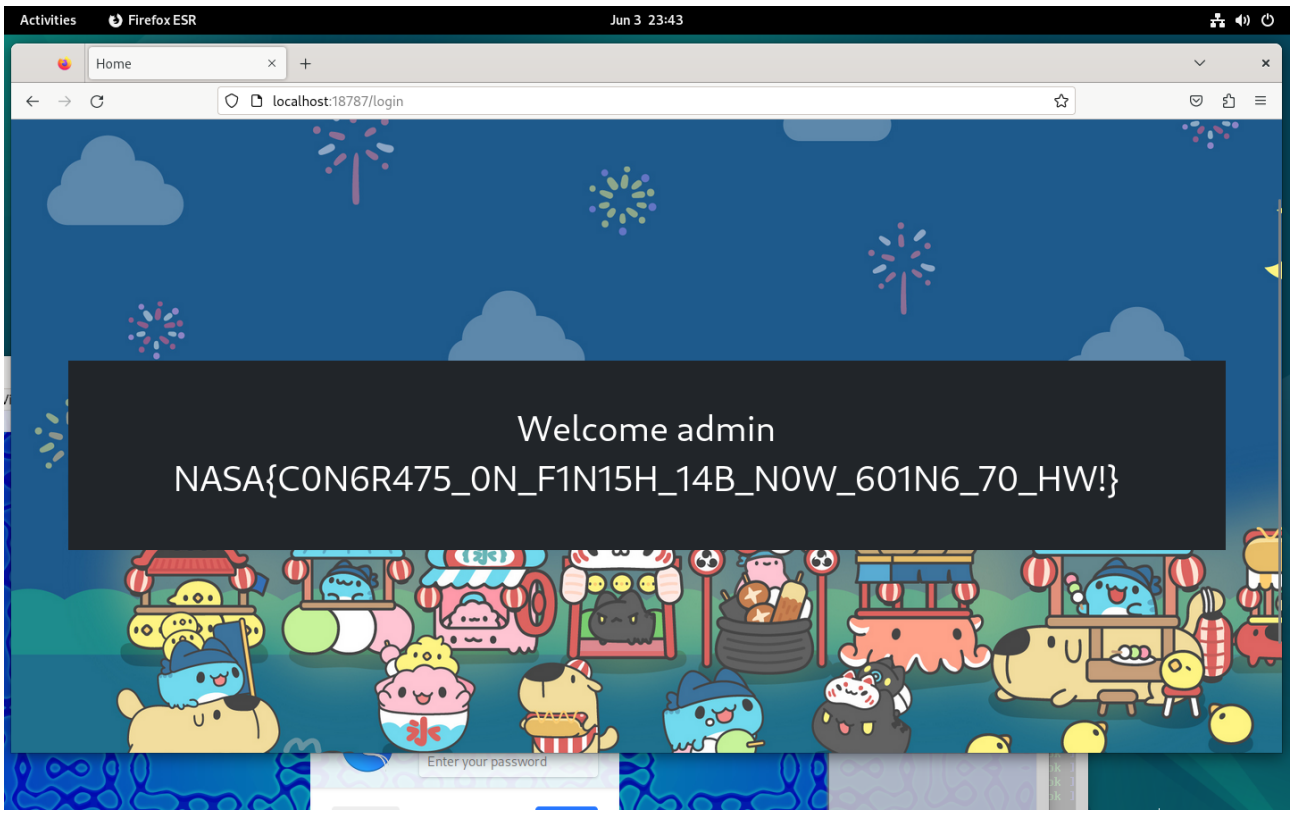
4. Use `john` to crack the password.

```
nasa2024@kali-[~] $ john \
  --wordlist=/usr/share/wordlists/rockyou.txt \
  admin_password.txt
```

5. The cracked password is `iloveyou4`. Use it to login to the website and obtain the flag.

Result

```
┌──(nasa2024㉿kali)-[~]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt admin_password.txt
Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 4096 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
iloveyou4        (?)
1g 0:00:07:30 DONE (2024-06-03 11:37) 0.002218g/s 11.06p/s 11.06c/s 11.06C/s super1..ramos
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```


Activities
Firefox ESR
Jun 3 23:43
Home
localhost:18787/login
Welcome admin
NASA{C0N6R475_0N_F1N15H_14B_N0W_601N6_70_HW!}
Enter your password