

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

```

[nasa2024@kali]~$ nmap -v -sV -p1-65535 10.0.2.16
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 11:06 EDT
NSE: Loaded 46 scripts for scanning.
Initiating Ping Scan at 11:06
Scanning 10.0.2.16 [2 ports]
Completed Ping Scan at 11:06, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:06
Completed Parallel DNS resolution of 1 host. at 11:07, 6.55s elapsed
Initiating Connect Scan at 11:07
Scanning 10.0.2.16 [65535 ports]
Discovered open port 80/tcp on 10.0.2.16
Discovered open port 22/tcp on 10.0.2.16
Discovered open port 45679/tcp on 10.0.2.16
Discovered open port 45678/tcp on 10.0.2.16
Discovered open port 8787/tcp on 10.0.2.16
Completed Connect Scan at 11:07, 6.74s elapsed (65535 total ports)
Initiating Service scan at 11:07
Scanning 5 services on 10.0.2.16
Completed Service scan at 11:08, 87.34s elapsed (5 services on 1 host)
NSE: Script scanning 10.0.2.16.
Initiating NSE at 11:08
Completed NSE at 11:08, 0.05s elapsed
Initiating NSE at 11:08
Completed NSE at 11:08, 1.10s elapsed
Nmap scan report for 10.0.2.16
Host is up (0.0085s latency).
Not shown: 65530 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.6 (protocol 2.0)
80/tcp    open  http      nginx
8787/tcp  open  msgrsrv?
45678/tcp open  tcpwrappd
45679/tcp open  tcpwrappd
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port8787-TCP:V=7.94SVN%I=7%D=6/3%T=665DDC25%P=x86_64-pc-linux-gnu%r(
SF-GetRequest,C76,"HTTP/1.1\x20200K\r\nServer:\x20Werkzeug/3.0.3\x
SF:20Python/3.11.9\r\nDate:\x20Mon,\x2003\x20Jun\x202024\x2015:07:16\x20
SF:GMT\r\nContent-Type:\x20text/html;\x20charset=utf-8\r\nContent-Length:\
SF:203015\r\nConnection:\x20close\r\n\r\n<!DOCTYPE\x20html>\n<html\x20lan
SF:g="en">\n<head>\n<x20\x20\x20\x20meta\x20charset="UTF-8">\n<x20\x20\x20
SF:0\x20\x20meta\x20name="viewport"\x20content="width=device-width,\x2
SF:0initial-scale=1.0">\n<x20\x20\x20\x20<title>Home</title>\n<x20\x20\x20
SF:20\x20<link\x20href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/
SF:dist/css/bootstrap.min.css"\x20rel="stylesheet"\x20integrity="sha
SF:384-QWTKyZyPPEjISvSWARU90FeRpk6VctnVnDr5pNlyT2bRjxh0JmHY6hW\+ALEwTH\
SF:\x20crossorigin="anonymous">\n<x20\x20\x20\x20<link\x20rel="styleshe
SF:et"\x20href="/static/css/styles.css">\n</head>\n<body>\n<x20\x20\x20
SF:0\x20<div\x20class="container"\x20style="text-align:\x20center;\x20d
SF:isplay:\x20flex;\x20flex-direction:\x20column;\x20gap:\x2010px;">\n<x20

```

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.4G2SgmpAnl6ZwhBNrtXqRK8hgJV8Da.`
2. Save the password as a text file in the Kali VM.

```
nasa2024@kali-[~] $ echo \  
'$2b$12$MUZRi07d.hFjdek1NPPbh.4G2SgmpAnl6ZwhBNrtXqRK8hgJV8Da' \  
> 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.
```

