Assignment 0x03

Frank Kaiser – 1742945, Jan Martin – 1796943

January 7, 2018

Contents

1 Part 1: nmap

1.1 Find the address of that other host with a nmap ping scan.

To do a ping scan you can use the -sn flag. For the aggressive spee template -T4 does the job. This results in: `nmap -sn  -T4 10.8.200-209.0-255`

Result:
Starting Nmap 7.40 (https://nmap.org) at 2018-01-04 20:25 CET Nmap scan report for 10.8.205.198 Host is up (0.00098s latency). Nmap done: 2560 IP addresses (1 host up) scanned in 133.49 seconds

So the machine was found at IP-address 10.8.205.198

1.2 Would nmaps ping scan have found the host if the administrator of the target host had implemented firewall rules that drop ICMP echo packets?

Probably not.

1.3 Perform a nmap TCP connect port scan.

nmap -sT -T4 10.8.200-209.0-255

```
Starting Nmap 7.40 ( https://nmap.org ) at 2018-01-04 20:37 CET
Nmap scan report for 10.8.205.198
Nmap scan report for 10.8.205.198
Host is up (0.0027s latency).
Not shown: 860 closed ports
PORT      STATE SERVICE
1/tcp     open  tcpmux
4/tcp     open  unknown
6/tcp     open  unknown
7/tcp     open  echo
9/tcp     open  discard
13/tcp    open  daytime
17/tcp    open  qotd
19/tcp    open  chargen
20/tcp    open  ftp-data
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
37/tcp    open  time
42/tcp    open  nameserver
43/tcp    open  whois
49/tcp    open  tacacs
53/tcp    open  domain
```

```
70/tcp     open   gopher
79/tcp     open   finger
80/tcp     open   http
88/tcp     open   kerberos-sec
106/tcp    open   pop3pw
110/tcp    open   pop3
111/tcp    open   rpcbind
113/tcp    open   ident
119/tcp    open   nntp
135/tcp    open   msrpc
139/tcp    open   netbios-ssn
143/tcp    open   imap
161/tcp    open   snmp
163/tcp    open   cmip-man
179/tcp    open   bgp
199/tcp    open   smux
389/tcp    open   ldap
406/tcp    open   imsp
427/tcp    open   svrloc
443/tcp    open   https
444/tcp    open   snpp
445/tcp    open   microsoft-ds
464/tcp    open   kpasswd5
465/tcp    open   smtps
500/tcp    open   isakmp
512/tcp    open   exec
513/tcp    open   login
514/tcp    open   shell
515/tcp    open   printer
543/tcp    open   klogin
544/tcp    open   kshell
548/tcp    open   afp
554/tcp    open   rtsp
563/tcp    open   snews
636/tcp    open   ldapssl
749/tcp    open   kerberos-adm
765/tcp    open   webster
777/tcp    open   multiling-http
783/tcp    open   spamassassin
808/tcp    open   ccproxy-http
873/tcp    open   rsync
901/tcp    open   samba-swat
990/tcp    open   ftps
992/tcp    open   telnets
993/tcp    open   imaps
995/tcp    open   pop3s
```

```
1001/tcp   open   webpush
1080/tcp   open   socks
1093/tcp   open   proofd
1094/tcp   open   rootd
1099/tcp   open   rmiregistry
1236/tcp   open   bvcontrol
1300/tcp   open   h323hostcallsc
1352/tcp   open   lotusnotes
1433/tcp   open   ms-sql-s
1434/tcp   open   ms-sql-m
1524/tcp   open   ingreslock
1812/tcp   open   radius
1863/tcp   open   msnp
2000/tcp   open   cisco-sccp
2003/tcp   open   finger
2010/tcp   open   search
2049/tcp   open   nfs
2103/tcp   open   zephyr-clt
2105/tcp   open   eklogin
2111/tcp   open   kx
2119/tcp   open   gsigatekeeper
2121/tcp   open   ccproxy-ftp
2135/tcp   open   gris
2401/tcp   open   cvspserver
2601/tcp   open   zebra
2602/tcp   open   ripd
2604/tcp   open   ospfd
2605/tcp   open   bgpd
2607/tcp   open   connection
2608/tcp   open   wag-service
2811/tcp   open   gsiftp
3260/tcp   open   iscsi
3306/tcp   open   mysql
3493/tcp   open   nut
3689/tcp   open   rendezvous
3690/tcp   open   svn
4224/tcp   open   xtell
4899/tcp   open   radmin
5002/tcp   open   rfe
5050/tcp   open   mmcc
5051/tcp   open   ida-agent
5060/tcp   open   sip
5061/tcp   open   sip-tls
5190/tcp   open   aol
5222/tcp   open   xmpp-client
5269/tcp   open   xmpp-server
```

```
5555/tcp  open  freeciv
5666/tcp  open  nrpe
6000/tcp  open  X11
6001/tcp  open  X11:1
6002/tcp  open  X11:2
6003/tcp  open  X11:3
6004/tcp  open  X11:4
6005/tcp  open  X11:5
6006/tcp  open  X11:6
6007/tcp  open  X11:7
6346/tcp  open  gnutella
6566/tcp  open  sane-port
6667/tcp  open  irc
7000/tcp  open  afs3-fileserver
7001/tcp  open  afs3-callback
7002/tcp  open  afs3-prserver
7004/tcp  open  afs3-kaserver
7007/tcp  open  afs3-bos
7100/tcp  open  font-service
8021/tcp  open  ftp-proxy
8081/tcp  open  blackice-icecap
8088/tcp  open  radan-http
9101/tcp  open  jetdirect
9102/tcp  open  jetdirect
9103/tcp  open  jetdirect
9418/tcp  open  git
10000/tcp open  snet-sensor-mgmt
10082/tcp open  amandaidx
13722/tcp open  netbackup
13782/tcp open  netbackup
13783/tcp open  netbackup
```

1.4 Explain how the disadvantages of the basic TCP connect scan can be overcome by other scan types.

You could do an Idle Scan using the -sl flag. 1) A SYN scan will send a SYN -packet to the port and the target will respond with SYN/ACK messages if the port is open and with RST if the port is closed. 2) A machine that receives SYN/ACK packet will repond with a RST. 3) Every IP packet on the Internet has a fragment identification number (IP ID). Since many operating systems simply increment this number for each packet they send, probing for the IPID can tell an attacker how many packets have been sent since the last probe.

By combining these traits, it is possible to scan a target network while forging your identity so that it looks like an innocent zombie machine did the scanning

Idle scan consists of three steps:

- Probe zombie's IP ID and record it.
- Forge SYN packet from zombie and send it to desired port. Depending on the target's reaction the IP ID may be incremented.
- Repeat step 1 again and compare the recordings.

The zombie's IP ID should now have increased by either one or two. One means the zombie hasn't sent out any packets, except for its reply to the attacker's probe. This means the port is not open. Two indicates the zombie sent out a packet between the two probes. This usually means the port is open. Note that via this scan method closed and filtered ports can not be distinguished.

See: `https://nmap.org/book/idlescan.html`

1.5 Perform a version detection scan to filter out the dummy ports. On which ports are real services running?

```
nmap –sV –F –T4 10.8.200−209.0−255
Nmap scan report for 10.8.205.198
Host is up (0.00068s latency).
Not shown: 48 closed ports
PORT      STATE SERVICE    VERSION
7/tcp     open  tcpwrapped
9/tcp     open  tcpwrapped
13/tcp    open  tcpwrapped
21/tcp    open  tcpwrapped
22/tcp    open  ssh        OpenSSH 7.4p1 Debian 10+deb9u2 (protocol 2.0)
23/tcp    open  tcpwrapped
37/tcp    open  tcpwrapped
53/tcp    open  tcpwrapped
79/tcp    open  tcpwrapped
80/tcp    open  http       nginx 1.10.3
88/tcp    open  tcpwrapped
106/tcp   open  tcpwrapped
110/tcp   open  tcpwrapped
111/tcp   open  tcpwrapped
113/tcp   open  tcpwrapped
119/tcp   open  tcpwrapped
135/tcp   open  tcpwrapped
139/tcp   open  tcpwrapped
143/tcp   open  tcpwrapped
179/tcp   open  tcpwrapped
199/tcp   open  tcpwrapped
389/tcp   open  tcpwrapped
427/tcp   open  tcpwrapped
443/tcp   open  ssl/http   nginx 1.10.3
```

```
444/tcp   open  tcpwrapped
445/tcp   open  tcpwrapped
465/tcp   open  tcpwrapped
513/tcp   open  tcpwrapped
514/tcp   open  tcpwrapped
515/tcp   open  tcpwrapped
543/tcp   open  tcpwrapped
544/tcp   open  tcpwrapped
548/tcp   open  tcpwrapped
554/tcp   open  tcpwrapped
873/tcp   open  tcpwrapped
990/tcp   open  tcpwrapped
993/tcp   open  tcpwrapped
995/tcp   open  tcpwrapped
1433/tcp  open  tcpwrapped
2000/tcp  open  tcpwrapped
2049/tcp  open  tcpwrapped
2121/tcp  open  tcpwrapped
3306/tcp  open  tcpwrapped
4899/tcp  open  tcpwrapped
5051/tcp  open  tcpwrapped
5060/tcp  open  tcpwrapped
5190/tcp  open  tcpwrapped
5666/tcp  open  tcpwrapped
6000/tcp  open  tcpwrapped
6001/tcp  open  tcpwrapped
8081/tcp  open  tcpwrapped
10000/tcp open  tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

When receiving 'tcpwrapped' it indicates a valid TCP-handshake was performed but then closes the connection. Due to the high amount of tcpwrapped services we can assume that this is a defence mechanism to hide real services. In this case "tcpwrapped" indicates that the service is a dummy.

Real services are running on ports 22, 80 and 443.

1.6 Scan the port range 10000 to 65535 and determine on which port the web application is running.

```
nmap -sT -T4 -p 10000-65535 10.8.200-209.0-255

Starting Nmap 7.40 ( https://nmap.org ) at 2018-01-04 21:04 CET
Stats: 0:02:56 elapsed; 0 hosts completed (0 up), 2560 undergoing Ping S
Nmap scan report for 10.8.205.198
Host is up (0.0017s latency).
Not shown: 55501 closed ports
PORT      STATE SERVICE
```

```
10000/tcp open  snet-sensor-mgmt
10050/tcp open  zabbix-agent
10051/tcp open  zabbix-trapper
10080/tcp open  amanda
10081/tcp open  famdc
10082/tcp open  amandaidx
10083/tcp open  amidxtape
10809/tcp open  nbd
11112/tcp open  dicom
11201/tcp open  smsqp
11371/tcp open  pksd
13720/tcp open  netbackup
13721/tcp open  netbackup
13722/tcp open  netbackup
13724/tcp open  vnetd
13782/tcp open  netbackup
13783/tcp open  netbackup
15345/tcp open  xpilot
17001/tcp open  unknown
17002/tcp open  unknown
17003/tcp open  unknown
17004/tcp open  unknown
17500/tcp open  db-lsp
20011/tcp open  unknown
20012/tcp open  ss-idi-disc
22125/tcp open  dcap
22128/tcp open  gsidcap
22273/tcp open  wnn6
24554/tcp open  binkp
27374/tcp open  subseven
30865/tcp open  unknown
55329/tcp open  unknown
57000/tcp open  unknown
60177/tcp open  unknown
60179/tcp open  unknown

Nmap done: 2560 IP addresses (1 host up) scanned in 275.04 seconds
```

The desired machine it at this address: http://10.8.205.198:55329/

2 Part 2: Brute forcing a login of a web application

2.1 How is form data sent from the browser to the server?

Form contents are expressed as a property list of attribute names and values. This can for example be achieved as a suffix on the URL given by the 'ACTION' attribute. The list will be encoded as sequence of name=value elements separated by the '&' character. Example: `URL?org=Acme%20Foods&commerce&users=42`

2.2 Analyze the login form with the developer tools of your browser.

First we created a ssh-tunnel via `ssh -L 15900:10.8.205.198:55329 -l <user> 88.99.184.129` and connected to it from our browser via `127.0.0.1:15900`

When just reloading the page an error "Security token does not match" appears.

2.3 Your final objective is to find a working pair of username and password with which you can log into the web server.

Due to time limitations we were not able to find the correct username and password to log in.

To bruteforce the password we would write a script with nested for loops going from 1 to 31 and from 1 to 12 respectively and appending m and f at each string. Then this will be inserted as password.