Aiden Chang

Passive information gathering

- Domain name: Google.com
- IP address: 216.58.192.142
- Expires: 2028-09-13T00:00:00-0700
- When the corporation made the domain, when was it last updated, contact information on the relevant people managing the domain, Registrar Registration Expiration Date, IP address, servers running, the sources that provide this information.

Host detection

- Detected IP addresses on local network: 10.0.2.2, 10.0.2.3, 10.0.2.4, 10.0.2.15
- These IP addresses represent machines on a]the local network of my device.
- It sends out a broadcast message asking for the IP address, and tells it to tell it to 10.0.2.15 which is were virtual box is.
    - 1 0.000000000 PcsCompu_19:60:88 Broadcast ARP 42 Who has 10.0.2.2? Tell 10.0.2.15
    - 2 0.000203721 RealtekU_12:35:02 PcsCompu_19:60:88 ARP 60 10.0.2.2 is at 52:54:00:12:35:02
    - 3 0.032034500 10.0.2.15 137.22.198.41 DNS 81 Standard query 0xe0c3 PTR 2.2.0.10.in-addr.arpa
    - 4 0.043436121 137.22.198.41 10.0.2.15 DNS 158 Standard query response 0xe0c3 No such name PTR 2.2.0.10.in-addr.arpa SOA prisoner.iana.org
- IP Addresses detected:

Nmap scan report for elegit.mathcs.carleton.edu (137.22.4.5)

Host is up (0.0099s latency).

Nmap scan report for perlman.mathcs.carleton.edu (137.22.4.17)

Host is up (0.0043s latency).

Nmap scan report for ada.mathcs.carleton.edu (137.22.4.19)

Host is up (0.0042s latency).

Nmap scan report for cmc306-15.mathcs.carleton.edu (137.22.4.32)

Host is up (0.0046s latency).

Nmap scan report for cmc306-04.mathcs.carleton.edu (137.22.4.34)

Host is up (0.0046s latency).

Nmap scan report for cmc306-08.mathcs.carleton.edu (137.22.4.35)

Host is up (0.0046s latency).

Nmap scan report for cmc306-16.mathcs.carleton.edu (137.22.4.37)

Host is up (0.0046s latency).

Nmap scan report for cmc306-05.mathcs.carleton.edu (137.22.4.42)

Host is up (0.0046s latency).

Nmap scan report for cmc304-09.mathcs.carleton.edu (137.22.4.43)

Host is up (0.0046s latency).

Nmap scan report for cmc306-07.mathcs.carleton.edu (137.22.4.46)

Host is up (0.0051s latency).

Nmap scan report for kstclair63264.mathcs.carleton.edu (137.22.4.47)

Host is up (0.0051s latency).

Nmap scan report for cmc306-03.mathcs.carleton.edu (137.22.4.48)

Host is up (0.0051s latency).

Nmap scan report for cmc306-12.mathcs.carleton.edu (137.22.4.49)

Host is up (0.0051s latency).

Nmap scan report for cmc304-04.mathcs.carleton.edu (137.22.4.55)

Host is up (0.0050s latency).

Nmap scan report for cmc304-10.mathcs.carleton.edu (137.22.4.60)

Host is up (0.0046s latency).

Nmap scan report for cmc304-03.mathcs.carleton.edu (137.22.4.61)

Host is up (0.0046s latency).

Nmap scan report for cmc306-11.mathcs.carleton.edu (137.22.4.66)

Host is up (0.0034s latency).

Nmap scan report for cmc306-13.mathcs.carleton.edu (137.22.4.75)

Host is up (0.0033s latency).

Nmap scan report for cmc304-11.mathcs.carleton.edu (137.22.4.77)

Host is up (0.0046s latency).

Nmap scan report for mirage.mathcs.carleton.edu (137.22.4.81)

Host is up (0.0034s latency).

Nmap scan report for cmc304-07.mathcs.carleton.edu (137.22.4.87)

Host is up (0.0034s latency).

Nmap scan report for cmc304-01.mathcs.carleton.edu (137.22.4.91)

Host is up (0.0045s latency).

Nmap scan report for mmontee68381.mathcs.carleton.edu (137.22.4.98)

Host is up (0.0038s latency).

Nmap scan report for wcc02760832.its.carleton.edu (137.22.4.101)

Host is up (0.0038s latency).

Nmap scan report for cmc306-02.mathcs.carleton.edu (137.22.4.102)

Host is up (0.0043s latency).

Nmap scan report for cmc306-17.mathcs.carleton.edu (137.22.4.106)

Host is up (0.0035s latency).

Nmap scan report for cmc306-06.mathcs.carleton.edu (137.22.4.110)

Host is up (0.0033s latency).

Nmap scan report for cmc304-06.mathcs.carleton.edu (137.22.4.111)

Host is up (0.0033s latency).

Nmap scan report for cmc304-05.mathcs.carleton.edu (137.22.4.113)

Host is up (0.0032s latency).

Nmap scan report for cmc304-02.mathcs.carleton.edu (137.22.4.114)

Host is up (0.0032s latency).

Nmap scan report for cmc306-09.mathcs.carleton.edu (137.22.4.115)

Host is up (0.0031s latency).

Nmap scan report for maize.mathcs.carleton.edu (137.22.4.131)

Host is up (0.0045s latency).

Nmap scan report for wcc03168380.its.carleton.edu (137.22.4.141)

Host is up (0.0041s latency).

Nmap scan report for mtietest2.mathcs.carleton.edu (137.22.4.146)

Host is up (0.0049s latency).

Nmap scan report for dhurlber68123.its.carleton.edu (137.22.4.147)

Host is up (0.0049s latency).

Nmap scan report for cmc11960185.its.carleton.edu (137.22.4.155)

Host is up (0.0038s latency).

Nmap scan report for awb1.mathcs.carleton.edu (137.22.4.175)

Host is up (0.0054s latency).

Nmap scan report for cosc50410.mathcs.carleton.edu (137.22.4.182)

Host is up (0.0034s latency).

Nmap scan report for cmc306-10.mathcs.carleton.edu (137.22.4.188)

Host is up (0.0029s latency).

Nmap scan report for libr425-01r.its.carleton.edu (137.22.4.208)

Host is up (0.0055s latency).

Nmap scan report for mantis.mathcs.carleton.edu (137.22.4.212)

Host is up (0.0055s latency).

Nmap scan report for t5.mathcs.carleton.edu (137.22.4.225)

Host is up (0.0034s latency).

Nmap scan report for mtietesting.mathcs.carleton.edu (137.22.4.234)

Host is up (0.0055s latency).

- These IP addresses represent different devices connected to Carleton's network with IP address starting with 137.22.4
- Our local IP address sends a ping to a specific IP address, sends a SYN and ACK tcp packet, then receives a reply from the IP address

Port scanning

- Ports open on metasploitable

21/tcp open ftp

22/tcp open ssh

23/tcp open telnet

25/tcp open smtp

53/tcp open domain

80/tcp open http

111/tcp open rpcbind

139/tcp open netbios-ssn

445/tcp open microsoft-ds

512/tcp open exec

513/tcp open login

514/tcp open shell

1099/tcp open rmiregistry

1524/tcp open ingreslock

2049/tcp open nfs

2121/tcp open ccproxy-ftp

3306/tcp open mysql

5432/tcp open postgresql

5900/tcp open vnc

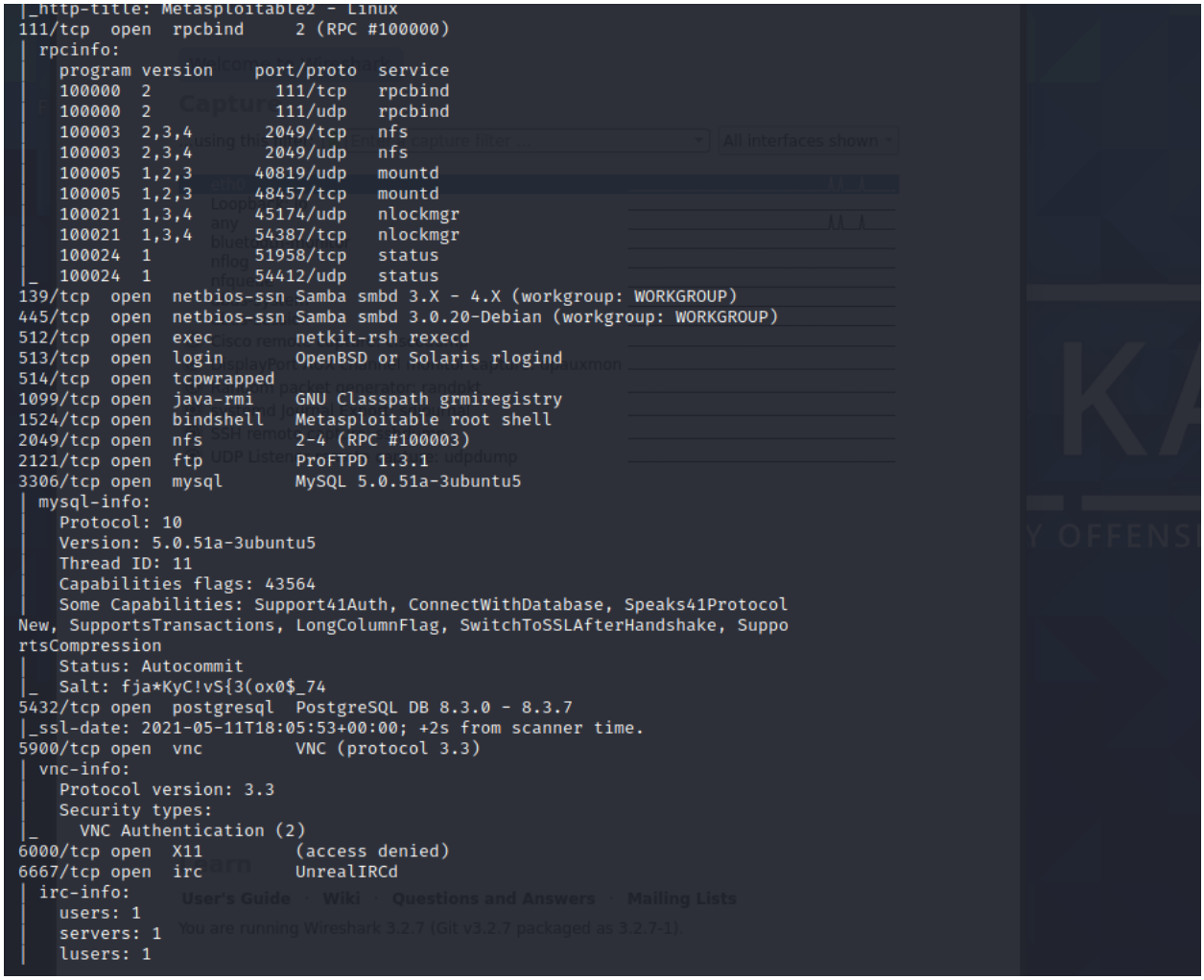
6000/tcp open X11

6667/tcp open irc

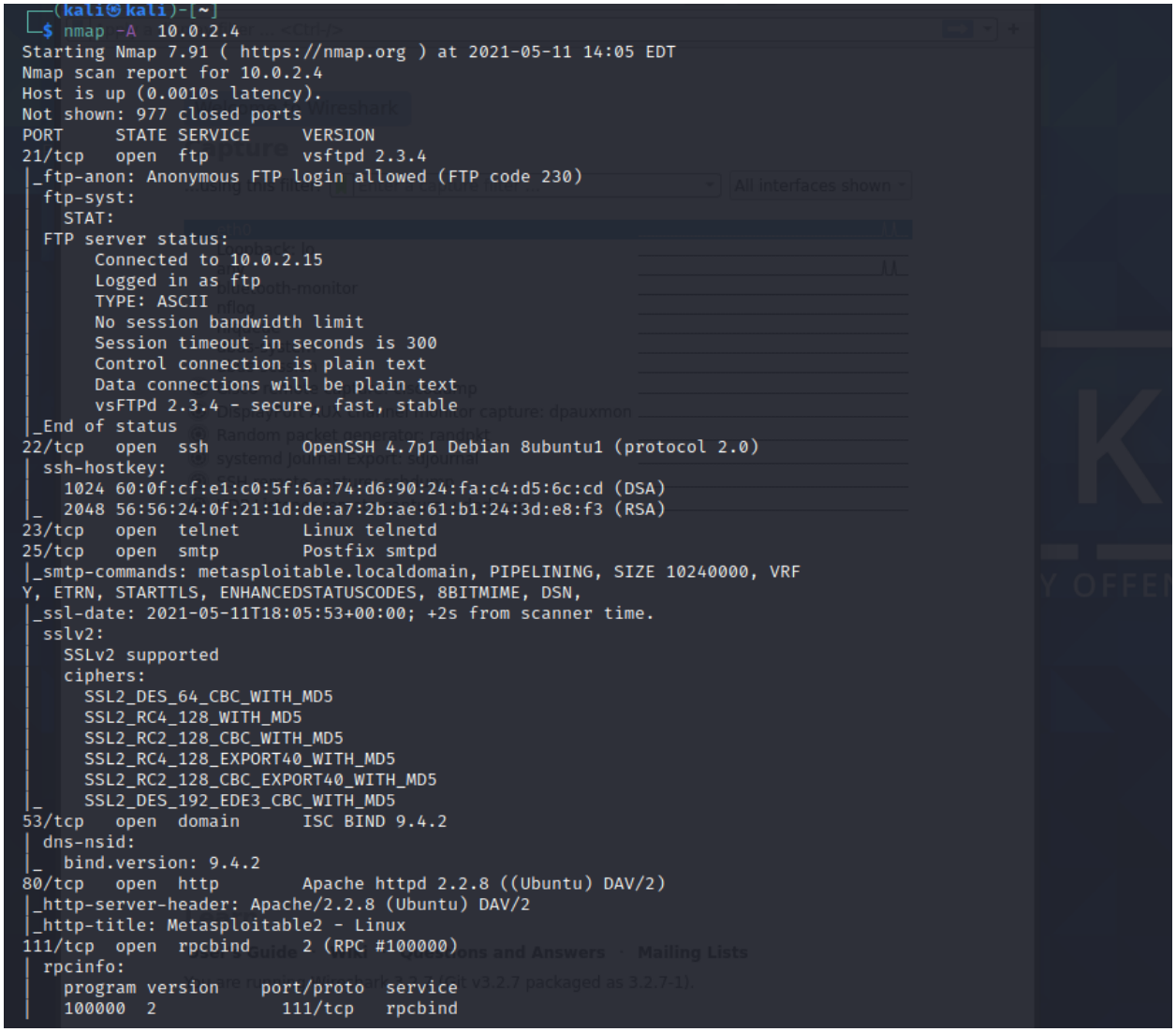
8009/tcp open ajp13

8180/tcp open unknown

- RSA SSH host key is 2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3. This is the key used for authenticating computers using the SSH protocol.
- The database on metasploitable is postgresql
- On port 25, SMTP(simple mail transfer protocol) this port is used to send and receive emails. Emails are sent to a service called mailgun.



```
|_http-title: Metasploitable2 - Linux
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      40819/udp   mountd
|   100005  1,2,3      48457/tcp   mountd
|   100021  1,3,4      45174/udp   nlockmgr
|   100021  1,3,4      54387/tcp   nlockmgr
|   100024  1          51958/tcp   status
|_  100024  1          54412/udp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 11
|   Capabilities flags: 43564
|   Some Capabilities: Support41Auth, ConnectWithDatabase, Speaks41Protocol
New, SupportsTransactions, LongColumnFlag, SwitchToSSLAfterHandshake, Suppo
rtsCompression
|   Status: Autocommit
|_  Salt: fja*KyC!vS{3(ox0$_74
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2021-05-11T18:05:53+00:00; +2s from scanner time.
5900/tcp open  vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
| irc-info:
|   users: 1
|   servers: 1
|   lusers: 1
```



```
┌──(kali㉿kali)-[~]
└─$ nmap -A  10.0.2.4
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-11 14:05 EDT
Nmap scan report for 10.0.2.4
Host is up (0.0010s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.0.2.15
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRF
Y, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
|_ssl-date: 2021-05-11T18:05:53+00:00; +2s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_    SSL2_DES_192_EDE3_CBC_WITH_MD5
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
```

```
6667/tcp open  irc         UnrealIRCd
| irc-info:
|   users: 1
|   servers: 1
|   lusers: 1
|   lservers: 0
|   server: irc.Metasploitable.LAN
|   version: Unreal3.2.8.1. irc.Metasploitable.LAN
|   uptime: 0 days, 0:05:39
|   source ident: nmap
|   source host: C29CBC04.EB72D3BE.7B559A54.IP
|_  error: Closing Link: ttlspjkhe[10.0.2.15] (Quit: ttlspjkhe)
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/5.5
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; O
Ss: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 1h00m01s, deviation: 1h59m59s, median: 1s
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MA
C: <unknown> (unknown)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2021-05-11T14:05:43-04:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)

Service detection performed. Please report any incorrect results at https:/
/nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.46 seconds
```