Authors: Anders Shenholm and Riaz Kelly

1 - Passive Information Gathering

- What domain did you investigate?

  Newzealand.com

- What is its IP address?

  173.223.70.225

- When does the domain's registration expire?

  2026-05-22

What information, if any, did you learn about the people or corporation responsible for the domain in question? (Your answer could be less interesting than you had hoped due to the increasingly common use of domain privacy services. In that case, at least give me information about what you learned about the relevant domain privacy service.)

Name of company (Verisign), Their physical address, contact info (phone, fax, email).

2 - Host Detection

- List the IP addresses for all the active hosts you found on the local network (i.e. the hosts whose IP addresses have the same first 24 bits--i.e. the same W.X.Y of the IP address W.X.Y.Z--as Kali's IP address).

  10.0.2.1

  10.0.2.2

  10.0.2.5

  10.0.2.15 - Kali’s IP address

- What entities do those IP addresses represent?
  - These IP addresses represent the hosts running on the Virtualbox local network (Kali, Metasploitable, others)

- For each possible candidate IP address it was searching in the local network, what steps did nmap take? (You can answer this question by examining the Wireshark captured packets. If you want to make it easier to read the relevant packets, try doing "nmap -sn [just-one-ip-address]" instead of the /24 thing.)

  nmap sent arp packets asking other IP addresses in the local network to report back. If an IP address was taken by an active host, the host would respond by sending a TCP [SYN] packet.

  For the 137.22.4.0/24 network:

- List the IP addresses for all the active hosts you found on the local network
  - 137.22.4.5
  - 137.22.4.17
  - 137.22.4.31
  - 137.22.4.34
  - 137.22.4.35
  - 137.22.4.42
  - 137.22.4.43
  - 137.22.4.46
  - 137.22.4.48
  - 137.22.4.49
  - 137.22.4.55
  - 137.22.4.60
  - 137.22.4.61
- What entities do those IP addresses represent?
  - They represent lab computers used by the CS/math department on campus.
- For each possible candidate IP address it was searching in the network, what steps did nmap take? (You can answer this question by examining the Wireshark captured packets. If you want to make it easier to read the relevant packets, try doing "nmap -sn [just-one-ip-address]" instead of the /24 thing.)

The local IP attempted to open TCP interactions with all possible IP addresses in the 137.22.4.x network. The IP addresses that responded were listed as active hosts.

3 - Port Scanning

Metasploitable is 10.0.2.5 - by far the most open ports

- Which ports does Metasploitable have open, and what services do they correspond to (e.g. port 22 / SSH or port 80 / HTTP)

21 ftp
22 ssh
23 telnet
25 smtp
53 domain
80 http
111 rpcbind
139 netbios-ssn
445 netbios-ssn
512 exec
513 login
514 tcpwrapped
1099 java-rmi
1524 bindshell
2049 nfs
2121 ftp
3306 mysql
5432 postgresql
5900 vnc
6000 X11
6667 irc
8009 ajp13
8180 http

- What database server(s) is/are available on Metasploitable?

    - mySQL
    - postgreSQL
    - Maybe more?

- What is the value of the RSA SSH host key? What is the host key for?
    - 2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3
    - The host key is used for authenticating the host. If the key doesn't work with the key that the SSH server has, then the host won't be authenticated.
- Pick one of the open ports that has a service you have never heard of, and explain what the service does.

  Port 111: rpcbind. rpcbind takes a rpc request (a request to outsource a program) from a client. It passes requests to local RPC servers that are able to do the work.

  https://en.wikipedia.org/wiki/Remote_procedure_call

  https://linux.die.net/man/8/rpcbind