Eric Gassel and Josiah Misplon

1. Passive information gathering

a. whois amazon.com - parts of the output we don't understand
   - "Registrar WHOIS Server: whois.markmonitor.com"
     - Registrar is Mark Monitor Inc. We are not sure what exactly the purpose Mark Monitor is serving.
   - We aren't sure why Amazon's legal department is also listed as a Registrar (can there be multiple registrars?)

b. What to hand in
   i. We investigated amazon.com.
   ii. amazon.com's IP address:

   "Name: amazon.com
   Address: 54.239.28.85
   Name: amazon.com
   Address: 176.32.103.205
   Name: amazon.com
   Address: 205.251.242.103"
   Why are there three IP addresses?

   iii. The domain's registration expires October 31, 2024

   "Registry Expiry Date: 2024-10-31T04:00:00Z"

   iv. In general, we found a lot of information on contacting (through phone, fax, mail, or email) Amazon or its subsidiaries - with references to network operations and reporting abuse. We found that Amazon's Legal Department has a connection to a P.O. box in Reno, NV. We found from "whois 176.32.103.205" (which correlates to the second IP address) that Amazon has a data services center (though maybe just for legal purposes) in Dublin, Ireland. From running whois on the first and third IP addresses, we can see the legal address of Amazon Inc. in Seattle. The whois

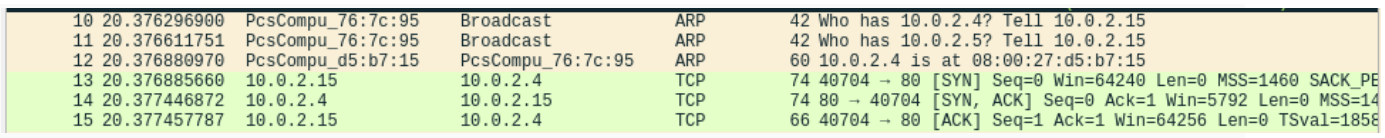
command for the first IP address gave an encrypted certificate as an output. *What does this certificate correlate to*?

2. Host detection

a. 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).
   i. Kali IP address: 10.0.2.15
   ii. results:
      1. 10.0.2.1
      2. 10.0.2.4
      3. 10.0.2.15

b. What entities do those IP addresses represent?
   i. 10.0.2.1 - router
   ii. 10.0.2.4 - that is the Metasploitable VM
   iii. 10.0.2.15 - Kali (our own machine)

c. 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.)
   i. It sent out a ARP packet asking “Who has 10.0.2.X? Tell 10.0.2.15” for every X in the range [2,255]. If it received a response of who had a given IP address, it then did a TCP handshake with that IP.



10	20.376296900	PcsCompu_76:7c:95	Broadcast	ARP	42 Who has 10.0.2.4? Tell 10.0.2.15
11	20.376611751	PcsCompu_76:7c:95	Broadcast	ARP	42 Who has 10.0.2.5? Tell 10.0.2.15
12	20.376880970	PcsCompu_d5:b7:15	PcsCompu_76:7c:95	ARP	60 10.0.2.4 is at 08:00:27:d5:b7:15
13	20.376885660	10.0.2.15	10.0.2.4	TCP	74 40704 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PE
14	20.377446872	10.0.2.4	10.0.2.15	TCP	74 80 → 40704 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=14
15	20.377457787	10.0.2.15	10.0.2.4	TCP	66 40704 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1858

d. Same question, but for the 137.22.4.0/24 network
   i. list of IP addresses & what they correspond to:
      1. 137.22.4.5 - elegit.mathcs.carleton.edu
      2. 137.22.4.17 - perlman.mathcs.carleton.edu

3. 137.22.4.131 - maize.mathcs.carleton.edu

ii. In this case, nmap sent out TCP [SYN] packets to each of the addresses of the form 137.22.4.X (for X in the range [1, 255]). If some IP address responded with its own TCP {SYN], [ACK] packet, then nmap finished the TCP handshake.

3. Port Scanning

a. Metasploitable open ports

Port - Service

i. 21 - ftp
ii. 22 - ssh
iii. 23 - telnet
iv. 25 - smtp
v. 53 - domain
vi. 80 - http
vii. 111 - rpcbind
viii. 139 - netbios-ssn
ix. 445 - microsoft-ds
x. 512 - exec
xi. 513 - login
xii. 514 - shell
xiii. 1099 - rmiregistry
xiv. 1524 - ingreslock
xv. 2049 - nfs
xvi. 2121 - ccproxy-ftp
xvii. 3306 mysql
xviii. 5432 - postgresql
xix. 5900 - vnc
xx. 6000 - X11
xxi. 6667 - irc
xxii. 8009/tcp open ajp13

xxiii. 8180 - unknown

b. What database servers is/are available on Metasploitable?
    i. 3306 - mysql
    ii. 5432 - postgresql
c. RSA SSH host key: 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3
    i. The host key is used to establish a secure connection with SSH using public key encryption between the Metasploitable machine and anyone else
d. port 1524 - ingreslock (source - Ingreslock Vulnerability)
    i. Ingres database is an SQL database that is commonly used to support large commercial and government applications. As applications became larger there were additional services added in the process of developing the Ingres application which led to assigning port 1524 to a service called ingreslock which is meant to lockdown specific areas of the database application. Inadvertently, ingreslock has a backdoor associated with it that automatically binds when a connection is made with this port, allowing someone (without any authorization) to have root level access (which is generally a bad security practice).

Why would a security system with this kind of vulnerability be used?