Penetration Testing

Ankit Sanghi, Ginnie White, Eric Neidhart

1. Passive Information Gathering:

Questions:

- What is an IANA ID?

Answers:

- We looked at google.com.
- IP address: 142.250.190.78
- The registration expires September 13th, 2028
- We learned that Google is very up to date with its registration terms (they're good until 2028) and that no one can change the domain. The latter bit makes sense, as Google is so commonly used and so massive that changing the domain would probably derail a significant portion of the internet.
- When we run nslookup on the IP address, we get a large number of results with different domain names, with the output being identical between the -query=any being present or not (whereas with the domain name, the nslookup [domain name] only gave a single 'non-authoritative' ip address).

2. Host Detection

- Local Network
    - We found 10.0.2.1, 10.0.2.2, 10.0.2.4, and 10.0.2.15.
    - 10.0.2.15 is Kali's main IP address. The other IP addresses are other active hosts on the local system.
    - Nsmap sends out a broadcast message to each possible IP address that begins with 10.0.2.X. These count as ARP protocols. The information attached to the packet says "Who has 10.0.2.X? Tell 10.0.2.15". If another host responds, it will tell the 10.0.2.15 IP address (the one we're using)
- Remote Network (interpreted as just the 'what is nmap doing' question)
    - We found the following hosts open: 137.22.3.10, 137.22.3.104, 137.22.3.118, 137.22.3.126, 137.22.3.145, 137.22.3.152, 137.22.3.156, 137.22.3.171, 137.22.3.217, 137.22.3.218.
    - These are all ITS servers that are on the Carleton local network.
    - For each possible candidate in the IP address range, it first sends an TCP request. If there is a response, then nmap does a DNS lookup for that IP address in order to list out the domain names of each IP address it found.
    - We found a total of 28 IP addresses within the given range.

    - This session has no ARP requests since the IP address being looked for is not on the local network. It did conduct DNS lookups for each IP address to identify the domain of each IP address.

3. Port Scanning
    - Metasploitable has the following ports open:
        - 21: ftp
        - 22: ssh
        - 23: telnet
        - 25: smtp
        - 53: domain
        - 80: http
        - 111: rpcbind
        - 139: netbios-ssm
        - 445: microsoft-ds
        - 512: exec
        - 513: login
        - 514: shell
        - 1099: rmiregistry
        - 1524: ingreslock
        - 2049: nfs
        - 2121: ccproxy-ftp
        - 3306: mysql
        - 5432: postgresql
        - 5900: vnc
        - 6000: X11
        - 6667: irc
        - 8009: ajp13
        - 8180: unknown
    - PostgreSQL and MySQL are the two database servers on Metasploitable.
    - The RSA host key is: 56:56:24:0F:21:1D:DE:A7:2B:AE:61:B1:24:3D:E8:F3. This is used to encrypt the traffic between the client trying to ssh into the server and the server.
    - We have never heard of ingreslock. It's on port 1524 and turns out it is a malicious backdoor placed by a hacker. Anyone can log into Metasploitable through this port as root.