Robbie Young Joven, Avery Hall

Pen Testing #1 Responses

1. Passive information gathering
    - What domain did you investigate?
        - chess.com
    - What is its IP address?
        - 34.117.44.137
    - When does the domain's registration expire?
        - 2027-07-01
    - What information, if any, did you learn about the people or corporation responsible for the domain in question?
        - The registrar(s) are GoDaddy.com, LLC and DomainsByProxy.com, LLC (these are partner registrars owned by the same person)
        - Registrar admin phone number is +1 480 624 2599
        - The registrant (chess.com) is located at 2155 E Warner Rd in Tempe, Arizona
2. Host detection
    - List the IP addresses for all the active hosts you found on the local network
        - 172.16.64.1
        - 172.16.64.2
        - 172.16.64.128
        - 172.16.64.129
    - What entities do those IP addresses represent?
        - 172.16.64.1 is some sort of gateway (our research suggests that addresses ending in .1 conventionally represent gateways)
        - 172.16.64.2 may be a gateway
        - 172.16.64.128 is the Metasploitable VM (after quitting just Metasploitable this is the host that disappeared)
        - 172.16.64.129 is the Kali VM (this is initial IP that we found using ifconfig in the Kali terminal)
    - For each possible candidate IP address it was searching in the local network, what steps did nmap take?
        - nmap sends ARP Broadcast messages for each possible IP on the network (of which there are 256), and then attempts to establish TCP connections with them to identify which are active.
    - Repeat the previous three bullets, but 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

        - 137.22.4.19
        - 137.22.4.20
        - 137.22.4.22
        - 137.22.4.79
        - 137.22.4.131
      - What entities do those IP addresses represent?
        - 137.22.4.5 - elegit.mathcs.carleton.edu
        - 137.22.4.17 - perlman.mathcs.carleton.edu
        - 137.22.4.19 - ada.mathcs.carleton.edu
        - 137.22.4.20 - *no associated domain*
        - 137.22.4.22 - *no associated domain*
        - 137.22.4.79 - onlin310-08.mathcs.carleton.edu
        - 137.22.4.131 - maize.mathcs.carleton.edu
      - For each possible candidate IP address it was searching in the local network, what steps did nmap take?
        - This nmap also pings all possible IPs on the network. However, this time nmap somehow knows the IP addresses already, possibly through ARP caching as we happened to run through this process twice, such that there are only two ARP messages total. The first is an ARP Broadcast message from Kali asking the network about the MAC address associated with Kali's IP (for some weird reason), and the second is a response to this broadcast. nmap again tries to establish TCP connections with the already known IP addresses to identify which are active.

3. Port Scanning
   - Which ports does Metasploitable have open, and what services do they correspond to (e.g. port 22 / SSH or port 80 / HTTP)?
     - port 21 / ftp
     - port 22 / ssh
     - port 23 / telnet
     - port 25 / smtp
     - port 53 / domain
     - port 80 / http
     - port 111 / rpcbind
     - port 139 / netbios-ssn
     - port 445 / microsoft-ds
     - port 512 / exec
     - port 513 / login
     - port 514 / shell
     - port 1099 / rmiregistry

  - port 1524 / ingreslock
  - port 2049 / nfs
  - port 2121 / ccproxy-ftp
  - port 3306 / mysql
  - port 5432 / postgresql
  - port 5900 / vnc
  - port 6000 / X11
  - port 6667 / irc
  - port 8009 / ajp13
  - port 8180 / unknown
- What database server(s) is/are available on Metasploitable?
  - mysql and postgresql (ingreslock seems to “Ingreslock is used legitimately to lock parts of an Ingres database. However, there are known trojans that also use port 1524 as a backdoor”)
- 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
- Pick one of the open ports that has a service you have never heard of, and explain what the service does.
  - telnet: A protocol that enables two-way text-based remote communication using a virtual terminal connection. Historically it was frequently used to provide access to a command-line interface on a remote host, but has since been largely replaced with SSH due to security concerns.