Pen Testing #1
Ben Aoki-Sherwood, Kenyon Nystrom, Avery Watts

1. Passive Information Gathering
    a. The domain we investigated was www.coolmathgames.com.
    b. 151.101.194.49
    c. 2026-12-31
    d. We learned that the company behind this domain bought the domain from the company Fastly. The domain registrar they use is Network Solutions, LLC. The company which owns the website is called Coolmath.com, LLC. It is located on 122 E 42nd St, Room 1611, New York, NY, 10168-1693, US. Their phone number is (+1) 212-813-5900. The email address they provided when registering for the domain is domain@fzlz.com. This email address is associated with the copyright/trademark law firm Fross, Zelnick, Lehrman & Zissu, P.C. This firm is also listed as the administrative and technical contact for the domain, so we think that Coolmath.com, LLC contracts with the firm to manage the billing and other legal upkeep of their domain.
2. Host Detection
    a. Local network:
    IP addresses 10.0.2.1, 10.0.2.4, and 10.0.2.15
    b. 10.0.2.1 is the local router, but since Kali is a VM this is technically our computer.
    10.0.2.4 corresponds to Metasploitable , which we also had open.
    10.0.2.15 is of course the ip for the Kali network interface.
    c. For each address, nmap broadcasts an ARP search for each IP address in the 10.0.2 range. If it receives an ARP reply for an IP, it then performs a TCP handshake with that IP address. After that, it knows that this IP is an active host. The IPs that performed a TCP handshake with Kali are the ones listed in the nmap scan results.
    d. Math/CS network:
    IP addresses 137.22.4.5, 137.22.4.17, and 137.22.4.131.
    e. 137.22.4.5 corresponds to elegit.mathcs.carleton.edu.
    137.22.4.17 corresponds to perlman.mathcs.carleton.edu.
    137.22.4.131 corresponds to maize.mathcs.carleton.edu.
    f. When running nmap, it starts by sending TCP SYN packets to all possible endings of the IP address. If an IP address responds with a SYN, ACK packet, then Kali responds with a final ACK to finish the handshake and then resets the connection with a RST, ACK packet. It uses this TCP handshake to verify that this host is open. Note that unlike scanning on the local network, nmap here uses TCP packets instead of ARP requests to scan/"fish" for open hosts.
3. Ports Scanning
    a. IP address 10.0.2.4
    21 / ftp
    22 / ssh
    23 / telnet

25 / smtp
53 / domain
80 / http
111 / rpcbind
139 / netbios-ssn
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

b. mySQL and Postgresql
c. 2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3. This is the key used to encrypt information sent to the ssh port by the ssh client. This is the ssh server's public RSA key to be used in symmetric encryption so that the ssh connection is secure.
d. rpcbind a.k.a portmap tells clients which RPC is running on what port. A remote procedure call (RPC) is used to run processes on systems outside the local system. RPCs involve processes such as tracking *client/server stubs* and *marshalling/unmarshalling*, which in tandem allow for a procedure call sent between server and client to successfully convert into a local call on the intended machine. As we can see in the rpcinfo we got from the nmap -A port scan, rpc gives information on which rpc processes are associated with which ports, and which version of the rpc is available for use on that port.