Mary Blanchard and Kaitlyn Peterson

1. Passive information gathering

Domain: webkinz.com

IP address: This site has two IP addresses: 34.206.131.141 and 54.157.55.105.

The domain's registry expires May 3rd of 2023 and the registrar registration expires May 2nd 2023. We believe the first date represents when webkinz.com has to be renewed with its registrar, godaddy.com, and the second date is when the registrar has to renew their registration with the hosting web server, AWS.

In the whois lookup, we discovered that the domain name is registered through godaddy.com. We learned that the overseeing organization Ganz (which owns webkinz) is the "registrant," and we could see their state/province as well as the contact information for various purposes (registrar, tech, admin). There were several different AWS name servers listed as hosting the domain, which was a bit confusing. We did not run into any domain privacy issues, but we did see the Terms of Use for the lookup tools that we used, which told us our permissions for using the whois service and the information it provides, as well as a reliability disclaimer from the registrar's whois service.

When we looked up the IP address using whois, we got a lot more specific information about the Amazon Web Server, and no mentions of webkinz at all. This included the street address of Amazon Technologies Inc, how to file a complaint, and more contact information for abuse, routing, admins, and more.

nslookup tended to have less information, and only reported the IP addresses. The netcraft lookup gave us a nicely formatted summary of the information that we had already seen (about the registrar and about AWS), as well as additional information about the tools that webkinz uses, such as javascript, html5, and certain web trackers.

2. Host detection

IP addresses for all the active hosts on the local network:

192.168.237.1

192.168.237.2

192.168.237.128

192.168.237.129 Metasploitable

Each of these IP addresses represents an endpoint connected to the network that has at least one port open. This makes it an “active host” on the network. We tried to use arp -a to see the names of these machines, but it listed a ? followed by the MAC address of the machine at each of the IP addresses that it found.

For each possible candidate IP address, nmap used ARP Protocol and issued a broadcast, asking “who has {possible IP address}? Tell 192.168.12.129.”

If this host was active, it responded using ARP Protocol with “{IP address} is at {MAC address}.”

IP addresses for all the active hosts on the 137.22.4.0/24 network:

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	unknown
137.22.4.22	unknown
137.22.4.72	olin310-07.mathcs.carleton.edu
137.22.4.131	maize.mathcs.carleton.edu

This time, the IP addresses showing up in our nmap scan are active hosts on the Carleton mathcs network. In contrast with the reports on the local network, the scan of the remote network included the hostname with its IP address for some. However, we did not get any information from arp -a.

This time, nmap attempts to initialize a TCP handshake by sending a [SYN] to each of the possible candidate IP addresses. It does so twice for each possible IP address, sending one to port 80 (HTTP) and the other to port 443 (HTTPS).
If the network responds with [SYN, ACK], it will send a TCP reset to terminate the connection ([RST, ACK]).
Occasionally the network will respond with [RST, ACK], terminating the connection itself.

3. Port scanning

Ports that Metasploitable has open and their corresponding services:

PORT/SERVICE
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

Database servers available on Metasploitable:

3306 - MySQL

5432 - PostgreSQL

RSA SSH host key: 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3
This key is for single sign-on to the SSH host without a password, it allows the user to use public-key authentication with the SSH server. Jeff showed us how to do this in class. :)

Port 445 says it is for “microsoft-ds,” which we had not heard of. The -A option showed that this port was running something called Samba. A brief search showed that Windows machines use this port for file sharing and print services over the network. Typically it uses SMB, or Server Message Block protocol. On the Metasploitable machine, which is running Linux, the software called Samba allows the machine to communicate with Windows machines in order to do the filesharing.