Authors: Charlie Roslansky, Silas Rhyneer

1. **Passive Information Gathering**

- Domain investigated: wikipedia.org
- 208.80.153.224 (range is 208.80.152.0 - 208.80.155.255)
- Expiration date: 2023-01-13T00:12:14Z
- We found information on the registrar (server, contact info, etc.) as well the mailing address associated with wikipedia, and the names and contact info of various people and servers involved in wikipedia.

Questions

- What's the difference between these two things:
  - Server: 137.22.198.41
  - Address: 137.22.198.41#53
- Why do they keep track of their own nameservers? Isn't the name server used with DNS to find wikipedia's IP? So what purpose does wikipedia have for storing it?

2. **Host Detection**

- # Host detection from our own IP
- Found 4 hosts:
  - 192.168.172.1
  - 192.168.172.2
  - 192.168.172.130
  - 192.168.172.131
- Entities:
  - Internet Assigned Numbers Authority
  - Also IANA
  - Also IANA
  - Also IANA
  - These addresses don't represent activity from IANA as anyone can use them. These IP addresses probably come from our machine.
- It sends out an ARP broadcast message asking who has [ip address], and asks them to message back to its own IP address.
- # Host detection on carleton network
- Found 3 hosts:
  - 137.22.4.5
  - 137.22.4.17
  - 137.22.4.131
- Entities:
  - elegit
  - perlman
  - maize
- It sends out a TCP SYN request for each possible address

3.

- **Open ports:**
    - Http/80/8180
    - Ssh/22
    - Telnet/23
    - Smtp/25
    - Domain/53
    - rpc-bind/111
    - Netbios/139
    - Netbios/445
    - Exec/512
    - login/513
    - ftp/21/2121
    - mysql/3306
    - postgresql/5432
    - java-rmi/1099
    - bindshell/1524
    - tcpwrapped/514
    - nfs/2049
    - vnc/5900
    - x11/6000
    - irc/6667
    - ajp13/8009
- Postgresql and mysql are databases
- RSA host key: 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3
    - This is the public key for connecting to the device using ssh
- Rpcbind, it redirects the client to the proper port number for the requested service/. RPC services will register with the rpcbind utility, allowing those processes to be accessed remotely. This port communicates using TCP wrapped messages.