Eli Arbogast

5/12/2021

Portscanning Assignment

1. Passive information gathering
    a. Things I don't understand: What is a name server? Why is there Registrar Abuse contact info? What is a DNSSEC?
    b. Domain: eliarbogast.com (domain I bought but haven't set up with anything yet, using a free and slightly sketchy host for web files)
    c. IP: 185.27.134.170
    d. Registry Expiry Date: 2022-03-12T01:09:11Z
    e. I already know the answer from experience, but the registrar is listed as a domain from Google. Info beyond that is not provided.
2. Host detection
    a. Hosts: 192.168.70.2 and 192.168.70.128
    b. These IP's represent Metasploitable and my host computer's IP addresses
    c. First, Nmap asks "who has [IP Address]" and then gives the ip address to report that information to. Then, the host of [IP Address] responds by listing[IP Address] is at such and such physical [MAC Address]
    d. Hosts: 137.22.4.5 and 137.22.4.17
    e. These hosts represent open hosts on the Carleton CS network (maybe instances of Metasploitable running?? Really not sure here…)
    f. Same steps as above, plus [SYN] starting a TCP session plus two packets of [TCP Retransmission]

3. Port Scanning

a. PORT STATE SERVICE

i. 21/tcp open ftp

ii. 22/tcp open ssh

iii. 23/tcp open telnet

iv. 25/tcp open smtp

v. 53/tcp open domain

vi. 80/tcp open http

vii. 111/tcp open rpcbind

viii. 139/tcp open netbios-ssn

ix. 445/tcp open microsoft-ds

x. 512/tcp open exec

xi. 513/tcp open login

xii. 514/tcp open shell

xiii. 1099/tcp open rmiregistry

xiv. 1524/tcp open ingreslock

xv. 2049/tcp open nfs

xvi. 2121/tcp open ccproxy-ftp

xvii. 3306/tcp open mysql

xviii. 5432/tcp open postgresql

xix. 5900/tcp open vnc

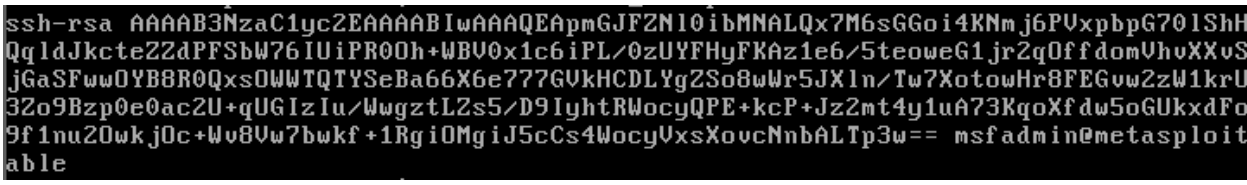
xx. 6000/tcp open X11

xxi. 6667/tcp open irc

xxii. 8009/tcp open ajp13

xxiii. 8180/tcp open unknown

b. MySQL, PostgreSQL

c. 

i. “The RSA key is a private key based on the RSA algorithm. The private key is used for authentication and a symmetric key exchange during the establishment of an SSL/TLS session.” - https://stackoverflow.com/questions/34783135/what-is-an-rsa-host-key

d. 1524 ingreslock: Used to lock parts of the Ingres SQL database management system