Practical 2

Tuesday, 2 August 2022 1:12 PM

Part 1

1. 13 ports are open. PureFTPd is the running on the FTP port. Exim smtpd 4.87 is the version of the email server. Two issues with the site is that the OpenSSH version that is running only sends a challenge when the username and public key entered are valid and it also contains a function (process_open) that doesn't prevent write operations in readonly mode, allowing attackers to create zero-length files. MySQL is the database service running on the site.
2. Searched the IP on shodan.io hostname:"www.efiling.nccourts.org"
   then used https://geekflare.com/ to test for the tls versions, and the host has only v1.2 enabled. DigiCert Global is the issuer. Shodan doesn't associate any vulnerabilities with this host (comment on overall security setup?).
3. rsaEncryption. - 2 ports are up
4. Run sudo spiderfoot -l 192.168.57.x:80 and type in mongolbank.mn
5. 2 ports are up. 8 vulneabilities (source). Mod_ssl can dereference a NULL pointer
6. https://www.ssllabs.com/ssltest/index.html
   web4.ucn.cl is running on IIS 5.0 (elimination)
   none of the servers us RC4 ciphers
   none of the servers are susceptible to OpenSSL padding oracle vuln
   contactmonkey.com has the best server settings according to the SSL Report Summary
7. BitNinja Captcha Server according to https://dnschecker.org/website-server-software.php
8. None of them (one isnt up).
9. -
10. -
11. -
12. -
13.

Part 2

Exercise 1

a. Using nmap -T5 -sP -oG - 192.168.2.0-255 | grep Up | awk -F " " '{print $2}' > Up.txt
   cat Up.txt | wc -l = 6 hosts
b. Using sudo nmap -O -iL Up.txt
   3 Windows, 3 Linux
   192.168.2.4 Windows Server 2008
   192.168.2.7 Windows Server 2008
   192.168.2.9 Windows Server 2009
   192.168.2.12 Linux
   192.168.2.15 Linux
   192.168.2.20 Linux
c. Using nbtscan -f Up.txt
   192.168.2.12   ALDRUHN
   192.168.2.4   CALDERA
   192.168.2.15   GNISIS
   192.168.2.20   TEL-MORA
d. Using sudo nmap -p389 -sV -iL Up.txt
   1
e. 192.168.2.12 Aldruhn
f. Using sudo nmap -p21 -sV -iL Up.txt
   3

g. Using sudo nmap -p1583,1433,1434,3306,3351,3050,5432,4022 -sV -iL Up.txt
1

h. Using sudo nmap -p80,443 -sV -iL Up.txt
3

i. Using sudo nmap -p2049 -sV -iL Up.txt
Yes, 192.168.2.20 is running NFS Shares. Versions 2, 3 and 4(100003)

j. Using nmap -T5 -sP -oG - 192.168.0-255.0-255 | grep Up | awk -F " " '{print $2}'
192.168.2.0/24 is the largest domain

Exercise 2

a. Using sudo nmap -Pn -sV -p- -iL Up.txt
192.168.2.12 has the most ports up (39?)

b. Using sudo nmap -Pn -sV -p22 -iL Up.txt
all hosts have ssh services running

c. Using sudo nmap -Pn -sV -p80 -vvvv -iL hostsUp.txt | grep xampp
there are no hosts with xampp running

d. Using sudo nmap -Pn -sV -vv -p1433 -iL Up.txt
there are no hosts with ms-sql-2016 running

e. Using sudo nmap -Pn -sV -p21 --script=ftp-anon -iL hostsUp.txt
192.168.2.4 and 192.168.2
by running the script ftp-anon

f. Using sudo nmap -Pn -sV -p3306 -iL hostsUp.txt
there is one machine with an open port 3306 (192.168.2.12) running MySQL, 2 machines have the port as "filtered"

g. _

h. _