**Q.1:**

|  |  |  |
| --- | --- | --- |
| **Registrant** | REDACTED FOR PRIVACY (DT) | |
| **Registrant Org** | Apple Inc. | |
| **Registrant Country** | us | |
| **Registrar** | CSC CORPORATE DOMAINS, INC. CSC Corporate Domains, Inc. IANA ID: 299 URL: www.cscprotectsbrands.com,http://cscdbs.com Whois Server: whois.corporatedomains.com  (p) | |
| **Registrar Status** | clientTransferProhibited, serverDeleteProhibited, serverTransferProhibited, serverUpdateProhibited | |
| **Dates** | 12,994 days old Created on 1987-02-19 Expires on 2023-02-20 Updated on 2022-02-16 |  |
| **Name Servers** | A.NS.APPLE.COM (has 17,265 domains) B.NS.APPLE.COM (has 17,265 domains) C.NS.APPLE.COM (has 17,265 domains) D.NS.APPLE.COM (has 17,265 domains) |  |
| **Tech Contact** | REDACTED FOR PRIVACY (DT) Apple Inc. One Apple Park Way, Cupertino, CA, 95014, us (p) (f) | |
| **IP Address** | 17.253.144.10 - 42 other sites hosted on this server |  |
| **IP Location** | United States - California - San Jose - Apple Inc. | |
| **ASN** | United States AS714 APPLE-ENGINEERING, US (registered Nov 30, -0001) | |
| **IP History** | 172 changes on 172 unique IP addresses over 18 years |  |
| **Registrar History** | 4 registrars with 1 drop |  |

**Website**

|  |  |  |
| --- | --- | --- |
| **Website Title** | None given. |  |
| **Terms** | 1,125 (Unique: 428, Linked: 253) | |
| **Images** | 0 (Alt tags missing: 0) | |
| **Links** | 135   (Internal: 109, Outbound: 1) | |

**Whois Record ( last updated on 2022-09-17 )**

Domain Name: apple.com  
Registry Domain ID: 1225976\_DOMAIN\_COM-VRSN  
Registrar WHOIS Server: whois.corporatedomains.com  
Registrar URL: www.cscprotectsbrands.com  
        http://cscdbs.com  
Updated Date: 2022-02-16T01:15:06+00:00  
        2022-02-16  
Creation Date: 1987-02-19T00:00:00+00:00  
        1987-02-19  
Registrar Registration Expiration Date: 2023-02-20T05:00:00+00:00  
        2023-02-20  
Registrar: CSC CORPORATE DOMAINS, INC.  
        CSC Corporate Domains, Inc.  
Sponsoring Registrar IANA ID: 299  
Registrar Abuse Contact Email: [](https://reversewhois.domaintools.com/?email=d244ffa66364e7c1b179f5f23f518363)  
Registrar Abuse Contact Phone: 18887802723  
Status:   
        clientTransferProhibited  
        serverDeleteProhibited  
        serverTransferProhibited  
        serverUpdateProhibited  
Registry Registrant ID:   
Registrant Name: REDACTED FOR PRIVACY (DT)  
Registrant Organization: Apple Inc.  
Registrant Street: One Apple Park Way  
Registrant City: Cupertino  
Registrant State/Province: CA  
Registrant Postal Code: 95014  
Registrant Country: us  
Registrant Phone: 14089961010  
Registrant Phone Ext:   
Registrant Fax: 14089741560  
Registrant Fax Ext:   
Registrant Email: REDACTED FOR PRIVACY (DT)  
Registry Admin ID:   
Admin Name: REDACTED FOR PRIVACY (DT)  
Admin Organization: Apple Inc.  
Admin Street: One Apple Park Way  
Admin City: Cupertino  
Admin State/Province: CA  
Admin Postal Code: 95014  
Admin Country: us  
Admin Phone: REDACTED FOR PRIVACY (DT)  
Admin Phone Ext:   
Admin Fax: REDACTED FOR PRIVACY (DT)  
Admin Fax Ext:   
Admin Email: REDACTED FOR PRIVACY (DT)  
Registry Tech ID:   
Tech Name: REDACTED FOR PRIVACY (DT)  
Tech Organization: Apple Inc.  
Tech Street: One Apple Park Way  
Tech City: Cupertino  
Tech State/Province: CA  
Tech Postal Code: 95014  
Tech Country: us  
Tech Phone: REDACTED FOR PRIVACY (DT)  
Tech Phone Ext:   
Tech Fax: REDACTED FOR PRIVACY (DT)  
Tech Fax Ext:   
Tech Email: REDACTED FOR PRIVACY (DT)  
Registry Billing ID:   
Billing Name:   
Billing Organization:   
Billing Street:   
Billing City:   
Billing State/Province:   
Billing Postal Code:   
Billing Country:   
Billing Phone:   
Billing Phone Ext:   
Billing Fax:   
Billing Fax Ext:   
Billing Email:   
Nameservers:   
        a.ns.apple.com  
        b.ns.apple.com  
        c.ns.apple.com  
        d.ns.apple.com  
DNSSEC: unsigned

IP Addresses:

Your own computer’s IP: 192.168.56.1

Kali Linux VM’s IP: 192.168.56.105

Metasploit-3 VM’s IP: 192.168.56.101

**Q.2:**

─# nmap --top-ports 2000 192.168.56.101

Starting Nmap 7.91 ( https://nmap.org ) at 2022-09-17 17:04 EDT

Nmap scan report for 192.168.56.101

Host is up (0.00017s latency).

Not shown: 1988 closed ports

PORT STATE SERVICE

21/tcp open ftp

80/tcp open http

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds

3389/tcp open ms-wbt-server

49152/tcp open unknown

49153/tcp open unknown

49154/tcp open unknown

49155/tcp open unknown

49156/tcp open unknown

49157/tcp open unknown

MAC Address: 08:00:27:46:8C:27 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 12.91 seconds

└─# nmap --top-ports 2000 192.168.56.101 192.168.56.1

Starting Nmap 7.91 ( https://nmap.org ) at 2022-09-17 17:02 EDT

Nmap scan report for 192.168.56.101

Host is up (0.00031s latency).

Not shown: 1988 closed ports

PORT STATE SERVICE

21/tcp open ftp

80/tcp open http

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds

3389/tcp open ms-wbt-server

49152/tcp open unknown

49153/tcp open unknown

49154/tcp open unknown

49155/tcp open unknown

49156/tcp open unknown

49157/tcp open unknown

MAC Address: 08:00:27:46:8C:27 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.56.1

Host is up (0.00014s latency).

All 2000 scanned ports on 192.168.56.1 are filtered

MAC Address: 0A:00:27:00:00:15 (Unknown)

Nmap done: 2 IP addresses (2 hosts up) scanned in 40.55 seconds

**Q.3:**

└─# nmap -sP 192.168.56.1-254

Starting Nmap 7.91 ( https://nmap.org ) at 2022-09-17 17:02 EDT

Nmap scan report for 192.168.56.1

Host is up (0.00012s latency).

MAC Address: 0A:00:27:00:00:15 (Unknown)

Nmap scan report for 192.168.56.100

Host is up (0.00011s latency).

MAC Address: 08:00:27:DD:4E:2F (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.56.101

Host is up (0.00018s latency).

MAC Address: 08:00:27:46:8C:27 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.56.105

Host is up.

Nmap done: 254 IP addresses (4 hosts up) scanned in 4.15 seconds

**Q.4:**

└─# nmap -sV 192.168.56.1-254

Starting Nmap 7.91 ( https://nmap.org ) at 2022-09-17 16:59 EDT

Nmap scan report for 192.168.56.1

Host is up (0.00018s latency).

All 1000 scanned ports on 192.168.56.1 are filtered

MAC Address: 0A:00:27:00:00:15 (Unknown)

Nmap scan report for 192.168.56.100

Host is up (0.000041s latency).

All 1000 scanned ports on 192.168.56.100 are filtered

MAC Address: 08:00:27:DD:4E:2F (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.56.101

Host is up (0.00035s latency).

Not shown: 988 closed ports

PORT STATE SERVICE VERSION

21/tcp open ftp Microsoft ftpd

80/tcp open http Microsoft IIS httpd 7.5

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

445/tcp open microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds

3389/tcp open ssl/ms-wbt-server?

49152/tcp open msrpc Microsoft Windows RPC

49153/tcp open msrpc Microsoft Windows RPC

49154/tcp open msrpc Microsoft Windows RPC

49155/tcp open msrpc Microsoft Windows RPC

49156/tcp open msrpc Microsoft Windows RPC

49157/tcp open msrpc Microsoft Windows RPC

MAC Address: 08:00:27:46:8C:27 (Oracle VirtualBox virtual NIC)

Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Nmap scan report for 192.168.56.105

Host is up (0.0000040s latency).

Not shown: 992 closed ports

PORT STATE SERVICE VERSION

88/tcp filtered kerberos-sec

3306/tcp filtered mysql

8888/tcp filtered sun-answerbook

9000/tcp filtered cslistener

9001/tcp filtered tor-orport

9002/tcp filtered dynamid

9003/tcp filtered unknown

9090/tcp filtered zeus-admin

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 254 IP addresses (4 hosts up) scanned in 87.11 seconds

**Q.5:**

└─# nmap -Pn --script vuln 192.168.56.101

Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.

Starting Nmap 7.91 ( https://nmap.org ) at 2022-09-17 16:53 EDT

Nmap scan report for 192.168.56.101

Host is up (0.00026s latency).

Not shown: 988 closed ports

PORT STATE SERVICE

21/tcp open ftp

|\_sslv2-drown:

80/tcp open http

|\_http-csrf: Couldn't find any CSRF vulnerabilities.

|\_http-dombased-xss: Couldn't find any DOM based XSS.

|\_http-stored-xss: Couldn't find any stored XSS vulnerabilities.

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds

3389/tcp open ms-wbt-server

|\_sslv2-drown:

49152/tcp open unknown

49153/tcp open unknown

49154/tcp open unknown

49155/tcp open unknown

49156/tcp open unknown

49157/tcp open unknown

MAC Address: 08:00:27:46:8C:27 (Oracle VirtualBox virtual NIC)

Host script results:

|\_samba-vuln-cve-2012-1182: NT\_STATUS\_ACCESS\_DENIED

|\_smb-vuln-ms10-054: false

|\_smb-vuln-ms10-061: NT\_STATUS\_ACCESS\_DENIED

| smb-vuln-ms17-010:

| VULNERABLE:

| Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)

| State: VULNERABLE

| IDs: CVE:CVE-2017-0143

| Risk factor: HIGH

| A critical remote code execution vulnerability exists in Microsoft SMBv1

| servers (ms17-010).

|

| Disclosure date: 2017-03-14

| References:

| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

| https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

|\_ https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

Nmap done: 1 IP address (1 host up) scanned in 150.64 seconds

* There was a high-risk factor vulnerability which was listed as:

Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)

**Q.6:**

# nmap -sV --script=http-malware-host 192.168.56.101

Starting Nmap 7.91 ( https://nmap.org ) at 2022-09-17 16:50 EDT

Nmap scan report for 192.168.56.101

Host is up (0.00020s latency).

Not shown: 988 closed ports

PORT STATE SERVICE VERSION

21/tcp open ftp Microsoft ftpd

80/tcp open http Microsoft IIS httpd 7.5

|\_http-malware-host: Host appears to be clean

|\_http-server-header: Microsoft-IIS/7.5

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

445/tcp open microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds

3389/tcp open ms-wbt-server?

49152/tcp open msrpc Microsoft Windows RPC

49153/tcp open msrpc Microsoft Windows RPC

49154/tcp open msrpc Microsoft Windows RPC

49155/tcp open msrpc Microsoft Windows RPC

49156/tcp open msrpc Microsoft Windows RPC

49157/tcp open msrpc Microsoft Windows RPC

MAC Address: 08:00:27:46:8C:27 (Oracle VirtualBox virtual NIC)

Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 61.71 seconds

* It looks like after running this command that the scan shows that there is no malware being reported and that the host appears to be clean.

**Q.7:**

I think one of my biggest takeaways from this Practical Exercise is how much information can be gathered just from an IP address and how many different commands can be used to gather that information. I always knew that IP addresses were important, but never knew that they were this extensive. One takeaway that I also learned from this exercise is that this on a different scale is the first step towards ethical hacking, a lot of information can be gathered through reconnaissance in a public format before any hacking ever occurs. It is almost crazy to think about how much information is out there and publicly available if the right skills are used. The NSE scripting engine, which is new to me, is an important function to be able to check for some vulnerabilities in an automated way.