**Advanced Executive Program in Cybersecurity**

Virtual Internship Project Problem Statement



**Penetration Tester**

**Problem statement:**

You are working as a Penetration Tester for El Banco Bank. You are running a gray-box penetration test to probe for vulnerabilities that hackers with nefarious intent might be able to exploit to gather secure data and intelligence.

As a first step, you must gather more information about the target's environment and network-related information using the tools at your disposal.

**Background of the problem statement:**

El Banco Bank is one of the fastest growing banks in Europe with more than 1200 branches across the country and manages €200 billion in assets.

Handling millions of dollars of banking transactions per day, its customers hugely depend upon the security of their banking data. The recent surge in cyber-attacks and data breaches has become a significant issue for every organization.

**Expected deliverables:**

**Disclaimer:**

**Please note I have taken permission from instructor to carry out scans on my personal lab VMs**

**TASK 1:**

Perform a half-open scan against the target network to quickly identify all open ports in the network

**Answer**

**Please scroll down for output of command - └─# nmap -sT -p "\*" 192.168.1.1/24**

**TASK 2:**

Perform an aggressive mode that enables OS detection, version detection, script scanning, and traceroute in the network

**Answer**

**Please scroll down for output of command - └─# nmap -sS -A -sC -p "\*" 192.168.1.1/24 and └─# nmap -sS -A -sC 192.168.1.1/24**

**TASK 3:**

While examining web server logs, you notice some HyperText Transfer Protocol (HTTP) GET requests that look suspicious. You need to carefully examine the logs, identify the attacks, and determine the appropriate mitigation control.

**Log #1:**

|  |
| --- |
| "18.66.78.71 - - [22/Dec/2021:16:18:20 +0300] "GET /media/system/js/caption.js HTTP/1.1" 200 751 "http://18.66.78.71/?wvstest=javascript:domxssExecutionSink(1,%22'%5C%22%3E%3Cxsstag%3E()locxss%22)" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21"" |

**Log #2**

|  |
| --- |
| "18.66.78.71 - - [22/Dec/2021:15:20:03 +0300] "GET /DVWA/vulnerabilities/fi/?page=%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2fetc%2fpasswd HTTP/1.1" 200 2190 "http://18.66.78.71/DVWA/" "Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.16 Safari/537.36"" |

**Log #3**

|  |
| --- |
| "18.66.78.71 - - [22/Dec/2021:15:19:59 +0300] "GET /DVWA/vulnerabilities/fi/?page=%27AND%201%3dcast(0x5f21403264696c656d6d61%20as%20varchar(8000))%20or%20%271%27%3d%27 HTTP/1.1" 200 1433 "http://18.66.78.71/DVWA/" "Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.16 Safari/537.36"" |

Task 1 – Output - answer

**└─# nmap -sT -p "\*" 192.168.1.1/24**

Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-24 07:41 IST

Stats: 0:00:01 elapsed; 0 hosts completed (0 up), 255 undergoing ARP Ping Scan

ARP Ping Scan Timing: About 26.27% done; ETC: 07:41 (0:00:03 remaining)

Stats: 0:00:01 elapsed; 0 hosts completed (0 up), 255 undergoing ARP Ping Scan

ARP Ping Scan Timing: About 27.65% done; ETC: 07:41 (0:00:03 remaining)

Stats: 0:00:01 elapsed; 0 hosts completed (0 up), 255 undergoing ARP Ping Scan

ARP Ping Scan Timing: About 29.22% done; ETC: 07:41 (0:00:02 remaining)

Nmap scan report for www.huaweimobilewifi.com (192.168.1.1)

Host is up (0.0030s latency).

Not shown: 8349 closed tcp ports (conn-refused)

PORT STATE SERVICE

53/tcp open domain

80/tcp open http

MAC Address: 74:60:FA:E1:6E:45 (Huawei Technologies)

Nmap scan report for 192.168.1.101

Host is up (0.020s latency).

Not shown: 8348 filtered tcp ports (no-response)

PORT STATE SERVICE

135/tcp open msrpc

2179/tcp open vmrdp

7680/tcp open pando-pub

MAC Address: CC:2F:71:C4:7A:5C (Intel Corporate)

Nmap scan report for 192.168.1.102

Host is up (0.0027s latency).

Not shown: 8350 closed tcp ports (conn-refused)

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 08:00:27:73:47:D9 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.1.103

Host is up (0.021s latency).

All 8351 scanned ports on 192.168.1.103 are in ignored states.

Not shown: 8351 closed tcp ports (conn-refused)

MAC Address: 08:00:27:22:46:4F (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.1.106

Host is up (0.0075s latency).

Not shown: 8325 closed tcp ports (conn-refused)

PORT STATE SERVICE

21/tcp open ftp

22/tcp open ssh

23/tcp open telnet

25/tcp open smtp

53/tcp open domain

80/tcp open http

111/tcp open rpcbind

139/tcp open netbios-ssn

445/tcp open microsoft-ds

512/tcp open exec

513/tcp open login

514/tcp open shell

1099/tcp open rmiregistry

1524/tcp open ingreslock

2049/tcp open nfs

2121/tcp open ccproxy-ftp

3306/tcp open mysql

3632/tcp open distccd

5432/tcp open postgresql

5900/tcp open vnc

6000/tcp open X11

6667/tcp open irc

6697/tcp open ircs-u

8009/tcp open ajp13

8180/tcp open unknown

8787/tcp open msgsrvr

MAC Address: 08:00:27:F8:23:C1 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.1.104

Host is up (0.00015s latency).

All 8351 scanned ports on 192.168.1.104 are in ignored states.

Not shown: 8351 closed tcp ports (conn-refused)

Nmap done: 256 IP addresses (6 hosts up) scanned in 65.14 seconds

Task 2 – Output- answer

**└─# nmap -sS -A -sC -p "\*" 192.168.1.1/24**

Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-24 08:20 IST

Nmap scan report for 192.168.1.102

Host is up (0.0017s latency).

Not shown: 8350 closed tcp ports (reset)

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 2048 86:c7:72:b5:5e:27:29:73:54:14:ec:c2:bc:af:93:0b (RSA)

| 256 34:af:4a:4a:da:ef:0b:41:bb:cc:7f:fd:55:2f:1e:bf (ECDSA)

|\_ 256 6a:2e:09:bf:c7:0a:01:92:40:b1:11:45:4c:21:04:d8 (ED25519)

MAC Address: 08:00:27:73:47:D9 (Oracle VirtualBox virtual NIC)

Device type: general purpose

Running: Linux 4.X|5.X

OS CPE: cpe:/o:linux:linux\_kernel:4 cpe:/o:linux:linux\_kernel:5

OS details: Linux 4.15 - 5.6

Network Distance: 1 hop

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

TRACEROUTE

HOP RTT ADDRESS

1 1.71 ms 192.168.1.102

Nmap scan report for 192.168.1.103

Host is up (0.0018s latency).

All 8351 scanned ports on 192.168.1.103 are in ignored states.

Not shown: 8351 closed tcp ports (reset)

MAC Address: 08:00:27:22:46:4F (Oracle VirtualBox virtual NIC)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop

TRACEROUTE

HOP RTT ADDRESS

1 1.81 ms 192.168.1.103

Nmap scan report for 192.168.1.106

Host is up (0.0018s latency).

Not shown: 8325 closed tcp ports (reset)

PORT STATE SERVICE VERSION

21/tcp open ftp vsftpd 2.3.4

| ftp-syst:

| STAT:

| FTP server status:

| Connected to 192.168.1.104

| Logged in as ftp

| TYPE: ASCII

| No session bandwidth limit

| Session timeout in seconds is 300

| Control connection is plain text

| Data connections will be plain text

| vsFTPd 2.3.4 - secure, fast, stable

|\_End of status

|\_ftp-anon: Anonymous FTP login allowed (FTP code 230)

22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)

| ssh-hostkey:

| 1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)

|\_ 2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)

23/tcp open telnet?

25/tcp open smtp?

|\_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN

53/tcp open domain ISC BIND 9.4.2

| dns-nsid:

|\_ bind.version: 9.4.2

80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)

|\_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2

|\_http-title: Metasploitable2 - Linux

111/tcp open rpcbind 2 (RPC #100000)

| rpcinfo:

| program version port/proto service

| 100000 2 111/tcp rpcbind

| 100000 2 111/udp rpcbind

| 100003 2,3,4 2049/tcp nfs

| 100003 2,3,4 2049/udp nfs

| 100005 1,2,3 35838/udp mountd

| 100005 1,2,3 38139/tcp mountd

| 100021 1,3,4 41310/udp nlockmgr

| 100021 1,3,4 54274/tcp nlockmgr

| 100024 1 34053/udp status

|\_ 100024 1 36187/tcp status

139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

445/tcp open netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)

512/tcp open exec?

513/tcp open login?

514/tcp open shell?

1099/tcp open java-rmi GNU Classpath grmiregistry

1524/tcp open bindshell Metasploitable root shell

2049/tcp open nfs 2-4 (RPC #100003)

2121/tcp open ccproxy-ftp?

3306/tcp open mysql?

|\_ssl-cert: ERROR: Script execution failed (use -d to debug)

|\_tls-alpn: ERROR: Script execution failed (use -d to debug)

|\_tls-nextprotoneg: ERROR: Script execution failed (use -d to debug)

|\_mysql-info: ERROR: Script execution failed (use -d to debug)

|\_ssl-date: ERROR: Script execution failed (use -d to debug)

|\_sslv2: ERROR: Script execution failed (use -d to debug)

3632/tcp open distccd distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))

5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7

| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX

| Not valid before: 2010-03-17T14:07:45

|\_Not valid after: 2010-04-16T14:07:45

|\_ssl-date: 2022-08-24T02:56:32+00:00; -1s from scanner time.

5900/tcp open vnc VNC (protocol 3.3)

| vnc-info:

| Protocol version: 3.3

| Security types:

|\_ VNC Authentication (2)

6000/tcp open X11 (access denied)

6667/tcp open irc UnrealIRCd

6697/tcp open irc UnrealIRCd

8009/tcp open ajp13 Apache Jserv (Protocol v1.3)

|\_ajp-methods: Failed to get a valid response for the OPTION request

8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1

|\_http-favicon: Apache Tomcat

|\_http-title: Apache Tomcat/5.5

8787/tcp open drb Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)

MAC Address: 08:00:27:F8:23:C1 (Oracle VirtualBox virtual NIC)

Device type: general purpose

Running: Linux 2.6.X

OS CPE: cpe:/o:linux:linux\_kernel:2.6

OS details: Linux 2.6.9 - 2.6.33

Network Distance: 1 hop

Service Info: Host: irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux\_kernel

Host script results:

| smb-os-discovery:

| OS: Unix (Samba 3.0.20-Debian)

| Computer name: metasploitable

| NetBIOS computer name:

| Domain name: localdomain

| FQDN: metasploitable.localdomain

|\_ System time: 2022-08-23T22:54:32-04:00

|\_smb2-time: Protocol negotiation failed (SMB2)

|\_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

|\_clock-skew: mean: 1h19m59s, deviation: 2h18m45s, median: -1s

| smb-security-mode:

| account\_used: guest

| authentication\_level: user

| challenge\_response: supported

|\_ message\_signing: disabled (dangerous, but default)

TRACEROUTE

HOP RTT ADDRESS

1 1.77 ms 192.168.1.106

Nmap scan report for 192.168.1.104

Host is up (0.000039s latency).

All 8351 scanned ports on 192.168.1.104 are in ignored states.

Not shown: 8351 closed tcp ports (reset)

Too many fingerprints match this host to give specific OS details

Network Distance: 0 hops

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

Nmap done: 256 IP addresses (4 hosts up) scanned in 384.72 seconds

**└─# nmap -sS -A -sC 192.168.1.1/24**

Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-24 08:06 IST

Nmap scan report for www.huaweimobilewifi.com (192.168.1.1)

Host is up (0.040s latency).

Not shown: 998 closed tcp ports (reset)

PORT STATE SERVICE VERSION

53/tcp open domain Unbound

80/tcp open http WebServer

|\_http-server-header: WebServer

| fingerprint-strings:

| GenericLines:

| HTTP/1.1 400 Bad Request

| Server: WebServer

| Date: Thu, 01 Jan 1970 00:00:00 GMT

| Cache-Control: no-cache,no-store

| Content-Type: text/html; charset=iso-8859-1

| Content-Length: 231

| Connection: close

| <HTML>

| <HEAD><TITLE>400 Bad Request</TITLE></HEAD>

| <BODY BGCOLOR="#cc9999" TEXT="#000000" LINK="#2020ff" VLINK="#4040cc">

| <H4>400 Bad Request</H4><br>

| <HR>Can't parse request.</HR>

| <ADDRESS>WebServer</ADDRESS>

| </BODY></HTML>

| HTTPOptions, RTSPRequest, SIPOptions:

| HTTP/1.1 501 Not Implemented

| Server: WebServer

| Date: Thu, 01 Jan 1970 00:00:00 GMT

| Cache-Control: no-cache,no-store

| Content-Type: text/html; charset=iso-8859-1

| Content-Length: 250

| Connection: close

| <HTML>

| <HEAD><TITLE>501 Not Implemented</TITLE></HEAD>

| <BODY BGCOLOR="#cc9999" TEXT="#000000" LINK="#2020ff" VLINK="#4040cc">

| <H4>501 Not Implemented</H4><br>

| <HR>That method is not implemented.</HR>

| <ADDRESS>WebServer</ADDRESS>

|\_ </BODY></HTML>

| http-title: Site doesn't have a title (text/html).

|\_Requested resource was http://www.huaweimobilewifi.com/html/index.html

1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :

SF-Port80-TCP:V=7.92%I=7%D=8/24%Time=63058EB0%P=x86\_64-pc-linux-gnu%r(HTTP

SF:Options,1C9,"HTTP/1\.1\x20501\x20Not\x20Implemented\r\nServer:\x20WebSe

SF:rver\r\nDate:\x20Thu,\x2001\x20Jan\x201970\x2000:00:00\x20GMT\r\nCache-

SF:Control:\x20no-cache,no-store\r\nContent-Type:\x20text/html;\x20charset

SF:=iso-8859-1\r\nContent-Length:\x20250\r\nConnection:\x20close\r\n\r\n<H

SF:TML>\n\x20<HEAD><TITLE>501\x20Not\x20Implemented</TITLE></HEAD>\n\x20<B

SF:ODY\x20BGCOLOR=\"#cc9999\"\x20TEXT=\"#000000\"\x20LINK=\"#2020ff\"\x20V

SF:LINK=\"#4040cc\">\n\x20<H4>501\x20Not\x20Implemented</H4><br>\n\x20<HR>

SF:That\x20method\x20is\x20not\x20implemented\.</HR>\n\x20<ADDRESS>WebServ

SF:er</ADDRESS>\n\x20</BODY></HTML>\n")%r(RTSPRequest,1C9,"HTTP/1\.1\x2050

SF:1\x20Not\x20Implemented\r\nServer:\x20WebServer\r\nDate:\x20Thu,\x2001\

SF:x20Jan\x201970\x2000:00:00\x20GMT\r\nCache-Control:\x20no-cache,no-stor

SF:e\r\nContent-Type:\x20text/html;\x20charset=iso-8859-1\r\nContent-Lengt

SF:h:\x20250\r\nConnection:\x20close\r\n\r\n<HTML>\n\x20<HEAD><TITLE>501\x

SF:20Not\x20Implemented</TITLE></HEAD>\n\x20<BODY\x20BGCOLOR=\"#cc9999\"\x

SF:20TEXT=\"#000000\"\x20LINK=\"#2020ff\"\x20VLINK=\"#4040cc\">\n\x20<H4>5

SF:01\x20Not\x20Implemented</H4><br>\n\x20<HR>That\x20method\x20is\x20not\

SF:x20implemented\.</HR>\n\x20<ADDRESS>WebServer</ADDRESS>\n\x20</BODY></H

SF:TML>\n")%r(GenericLines,1B2,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nServ

SF:er:\x20WebServer\r\nDate:\x20Thu,\x2001\x20Jan\x201970\x2000:00:00\x20G

SF:MT\r\nCache-Control:\x20no-cache,no-store\r\nContent-Type:\x20text/html

SF:;\x20charset=iso-8859-1\r\nContent-Length:\x20231\r\nConnection:\x20clo

SF:se\r\n\r\n<HTML>\n\x20<HEAD><TITLE>400\x20Bad\x20Request</TITLE></HEAD>

SF:\n\x20<BODY\x20BGCOLOR=\"#cc9999\"\x20TEXT=\"#000000\"\x20LINK=\"#2020f

SF:f\"\x20VLINK=\"#4040cc\">\n\x20<H4>400\x20Bad\x20Request</H4><br>\n\x20

SF:<HR>Can't\x20parse\x20request\.</HR>\n\x20<ADDRESS>WebServer</ADDRESS>\

SF:n\x20</BODY></HTML>\n")%r(SIPOptions,1C9,"HTTP/1\.1\x20501\x20Not\x20Im

SF:plemented\r\nServer:\x20WebServer\r\nDate:\x20Thu,\x2001\x20Jan\x201970

SF:\x2000:00:00\x20GMT\r\nCache-Control:\x20no-cache,no-store\r\nContent-T

SF:ype:\x20text/html;\x20charset=iso-8859-1\r\nContent-Length:\x20250\r\nC

SF:onnection:\x20close\r\n\r\n<HTML>\n\x20<HEAD><TITLE>501\x20Not\x20Imple

SF:mented</TITLE></HEAD>\n\x20<BODY\x20BGCOLOR=\"#cc9999\"\x20TEXT=\"#0000

SF:00\"\x20LINK=\"#2020ff\"\x20VLINK=\"#4040cc\">\n\x20<H4>501\x20Not\x20I

SF:mplemented</H4><br>\n\x20<HR>That\x20method\x20is\x20not\x20implemented

SF:\.</HR>\n\x20<ADDRESS>WebServer</ADDRESS>\n\x20</BODY></HTML>\n");

MAC Address: 74:60:FA:E1:6E:45 (Huawei Technologies)

Device type: general purpose

Running: Linux 2.6.X|3.X

OS CPE: cpe:/o:linux:linux\_kernel:2.6 cpe:/o:linux:linux\_kernel:3

OS details: Linux 2.6.32 - 3.10

Network Distance: 1 hop

TRACEROUTE

HOP RTT ADDRESS

1 40.16 ms www.huaweimobilewifi.com (192.168.1.1)

Nmap scan report for 192.168.1.101

Host is up (0.00078s latency).

Not shown: 998 filtered tcp ports (no-response)

PORT STATE SERVICE VERSION

135/tcp open msrpc Microsoft Windows RPC

2179/tcp open vmrdp?

MAC Address: CC:2F:71:C4:7A:5C (Intel Corporate)

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Device type: general purpose|specialized

Running (JUST GUESSING): Microsoft Windows XP (92%), AVtech embedded (87%), FreeBSD 6.X|10.X (86%)

OS CPE: cpe:/o:microsoft:windows\_xp::sp3 cpe:/o:freebsd:freebsd:6.2 cpe:/o:freebsd:freebsd:10.3

Aggressive OS guesses: Microsoft Windows XP SP3 (92%), AVtech Room Alert 26W environmental monitor (87%), Microsoft Windows XP SP2 (87%), FreeBSD 6.2-RELEASE (86%), FreeBSD 10.3-STABLE (85%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 1 hop

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE

HOP RTT ADDRESS

1 0.78 ms 192.168.1.101

Nmap scan report for 192.168.1.102

Host is up (0.0017s latency).

Not shown: 999 closed tcp ports (reset)

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 2048 86:c7:72:b5:5e:27:29:73:54:14:ec:c2:bc:af:93:0b (RSA)

| 256 34:af:4a:4a:da:ef:0b:41:bb:cc:7f:fd:55:2f:1e:bf (ECDSA)

|\_ 256 6a:2e:09:bf:c7:0a:01:92:40:b1:11:45:4c:21:04:d8 (ED25519)

MAC Address: 08:00:27:73:47:D9 (Oracle VirtualBox virtual NIC)

Device type: general purpose

Running: Linux 4.X|5.X

OS CPE: cpe:/o:linux:linux\_kernel:4 cpe:/o:linux:linux\_kernel:5

OS details: Linux 4.15 - 5.6

Network Distance: 1 hop

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

TRACEROUTE

HOP RTT ADDRESS

1 1.73 ms 192.168.1.102

Nmap scan report for 192.168.1.103

Host is up (0.0017s latency).

All 1000 scanned ports on 192.168.1.103 are in ignored states.

Not shown: 1000 closed tcp ports (reset)

MAC Address: 08:00:27:22:46:4F (Oracle VirtualBox virtual NIC)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop

TRACEROUTE

HOP RTT ADDRESS

1 1.65 ms 192.168.1.103

Nmap scan report for 192.168.1.106

Host is up (0.0017s latency).

Not shown: 977 closed tcp ports (reset)

PORT STATE SERVICE VERSION

21/tcp open ftp vsftpd 2.3.4

| ftp-syst:

| STAT:

| FTP server status:

| Connected to 192.168.1.104

| Logged in as ftp

| TYPE: ASCII

| No session bandwidth limit

| Session timeout in seconds is 300

| Control connection is plain text

| Data connections will be plain text

| vsFTPd 2.3.4 - secure, fast, stable

|\_End of status

|\_ftp-anon: Anonymous FTP login allowed (FTP code 230)

22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)

| ssh-hostkey:

| 1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)

|\_ 2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)

23/tcp open telnet Linux telnetd

25/tcp open smtp Postfix smtpd

| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX

| Not valid before: 2010-03-17T14:07:45

|\_Not valid after: 2010-04-16T14:07:45

|\_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN

53/tcp open domain ISC BIND 9.4.2

| dns-nsid:

|\_ bind.version: 9.4.2

80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)

|\_http-title: Metasploitable2 - Linux

|\_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2

111/tcp open rpcbind 2 (RPC #100000)

| rpcinfo:

| program version port/proto service

| 100000 2 111/tcp rpcbind

| 100000 2 111/udp rpcbind

| 100003 2,3,4 2049/tcp nfs

| 100003 2,3,4 2049/udp nfs

| 100005 1,2,3 35838/udp mountd

| 100005 1,2,3 38139/tcp mountd

| 100021 1,3,4 41310/udp nlockmgr

| 100021 1,3,4 54274/tcp nlockmgr

| 100024 1 34053/udp status

|\_ 100024 1 36187/tcp status

139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

445/tcp open netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)

512/tcp open exec netkit-rsh rexecd

513/tcp open login

514/tcp open tcpwrapped

1099/tcp open java-rmi GNU Classpath grmiregistry

1524/tcp open bindshell Metasploitable root shell

2049/tcp open nfs 2-4 (RPC #100003)

2121/tcp open ftp ProFTPD 1.3.1

3306/tcp open mysql MySQL 5.0.51a-3ubuntu5

|\_ssl-cert: ERROR: Script execution failed (use -d to debug)

|\_sslv2: ERROR: Script execution failed (use -d to debug)

| mysql-info:

| Protocol: 10

| Version: 5.0.51a-3ubuntu5

| Thread ID: 30

| Capabilities flags: 43564

| Some Capabilities: SupportsTransactions, Speaks41ProtocolNew, Support41Auth, ConnectWithDatabase, LongColumnFlag, SwitchToSSLAfterHandshake, SupportsCompression

| Status: Autocommit

|\_ Salt: q#XrU5D7&Yk2U7OjJnlR

5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7

|\_ssl-date: 2022-08-24T02:39:01+00:00; 0s from scanner time.

| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX

| Not valid before: 2010-03-17T14:07:45

|\_Not valid after: 2010-04-16T14:07:45

5900/tcp open vnc VNC (protocol 3.3)

| vnc-info:

| Protocol version: 3.3

| Security types:

|\_ VNC Authentication (2)

6000/tcp open X11 (access denied)

6667/tcp open irc UnrealIRCd

8009/tcp open ajp13 Apache Jserv (Protocol v1.3)

|\_ajp-methods: Failed to get a valid response for the OPTION request

8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1

|\_http-title: Apache Tomcat/5.5

|\_http-favicon: Apache Tomcat

MAC Address: 08:00:27:F8:23:C1 (Oracle VirtualBox virtual NIC)

Device type: general purpose

Running: Linux 2.6.X

OS CPE: cpe:/o:linux:linux\_kernel:2.6

OS details: Linux 2.6.9 - 2.6.33

Network Distance: 1 hop

Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux\_kernel

Host script results:

|\_smb2-time: Protocol negotiation failed (SMB2)

| smb-os-discovery:

| OS: Unix (Samba 3.0.20-Debian)

| Computer name: metasploitable

| NetBIOS computer name:

| Domain name: localdomain

| FQDN: metasploitable.localdomain

|\_ System time: 2022-08-23T22:38:38-04:00

| smb-security-mode:

| account\_used: <blank>

| authentication\_level: user

| challenge\_response: supported

|\_ message\_signing: disabled (dangerous, but default)

|\_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

|\_clock-skew: mean: 1h20m00s, deviation: 2h18m35s, median: 0s

TRACEROUTE

HOP RTT ADDRESS

1 1.69 ms 192.168.1.106

Nmap scan report for 192.168.1.104

Host is up (0.000038s latency).

All 1000 scanned ports on 192.168.1.104 are in ignored states.

Not shown: 1000 closed tcp ports (reset)

Too many fingerprints match this host to give specific OS details

Network Distance: 0 hops

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

Nmap done: 256 IP addresses (6 hosts up) scanned in 185.69 seconds

<https://www.youtube.com/watch?v=PzRQhpbYbeg>

<https://www.youtube.com/watch?v=_3Wgx1FabIo>

<https://www.youtube.com/results?search_query=DOM+cross+site+scripting>

<https://www.youtube.com/watch?v=ABwS2MIxFPQ>

<https://www.youtube.com/watch?v=yJSnggHSH1U>

<https://www.youtube.com/watch?v=H_bMkEyk3xs>