Widgets-R-US Penetration Test Report

Project: Penetration Testing of New Fileshare Server

Target System: Metasploitable 2
Scope: Testing the new fileshare server

Table of Contents

1.Introduction

The goal of this penetration test is to gain a better understanding of Widgets-R-U's newly provisioned fileshare server. In summary, the assessment will aim to identify and exploit vulnerabilities end-to-end in relation to the server extract sensitive information like user credentials then offer recommendations on improvements that can be made as far as security of the system is concerned.

2. Testing Methodology

The testing will follow these phases:

- **Reconnaissance:** Gather information about the target.
- **Gaining Access**: Exploit vulnerabilities to gain initial access.
- **Privilege Escalation**: Gain higher-level permissions.

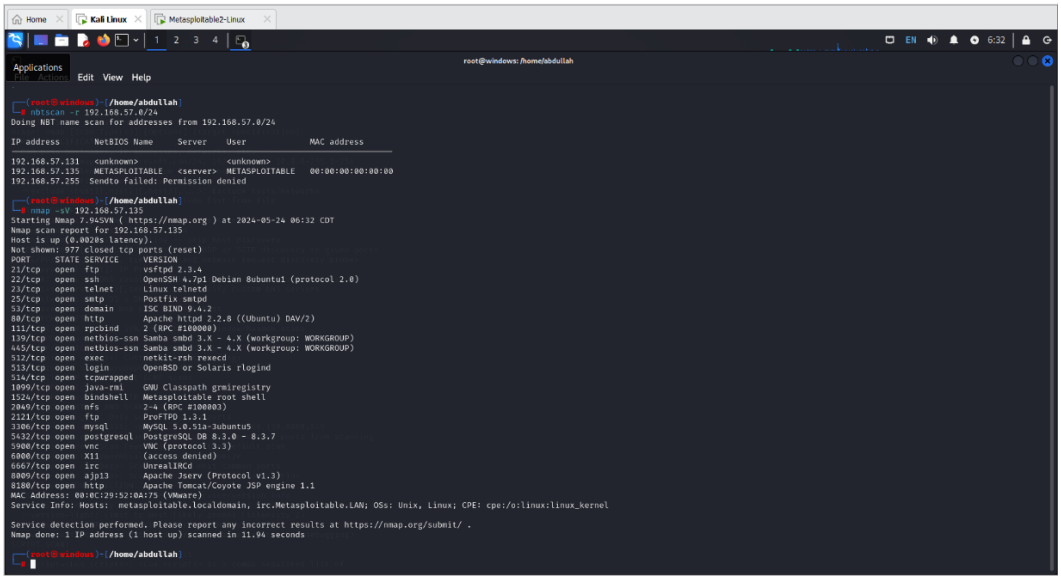
- **Exfiltration:** Extract sensitive data.
- **Reporting:** Document findings and provide recommendations.

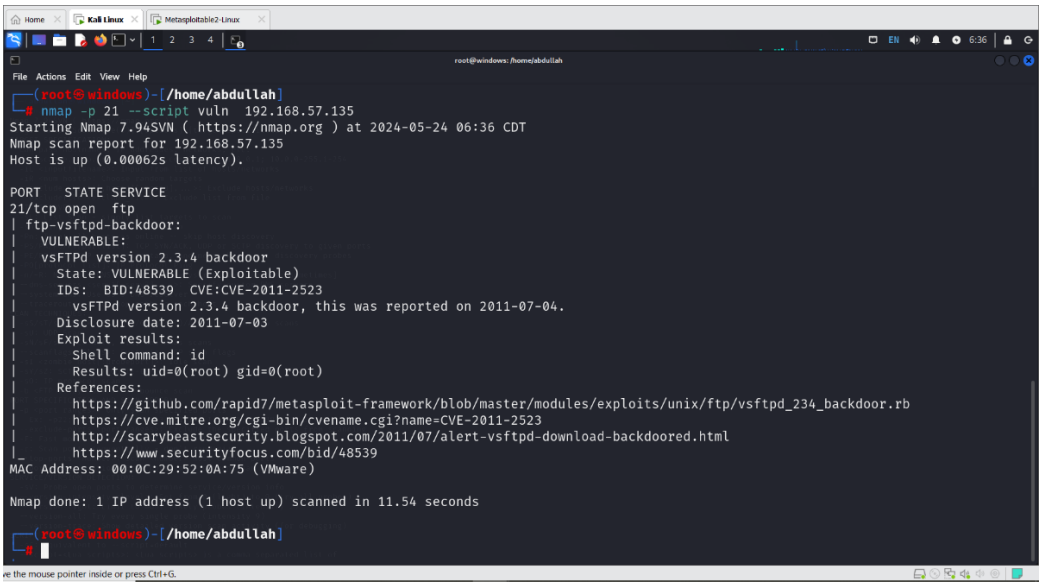
3. Steps Taken

Initial Reconnaissance

Tool Used: Nmap

Finding vulnerability





Output Summary:

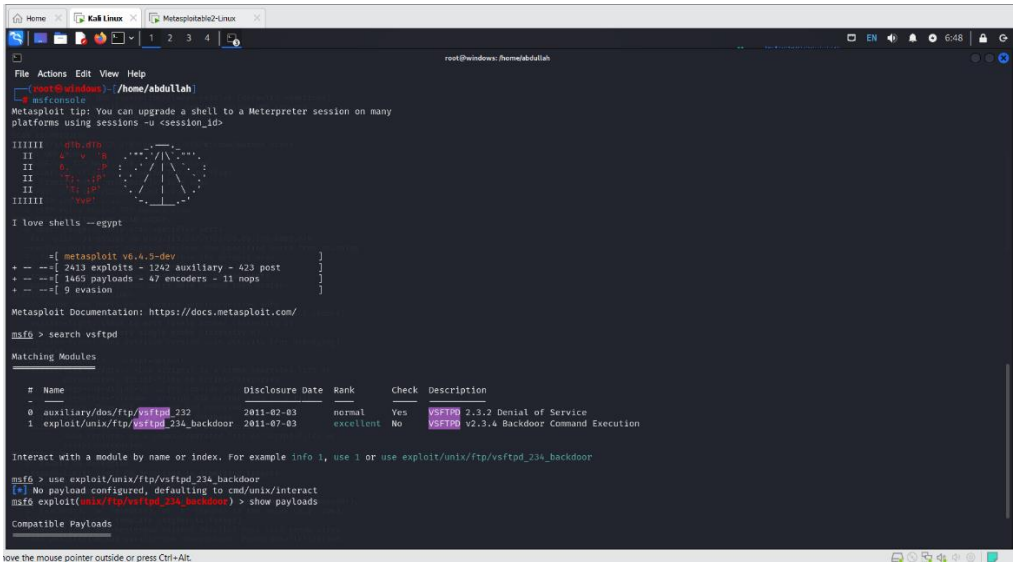
- Several services detected including SSH, FTP, Telnet, and MySQL.

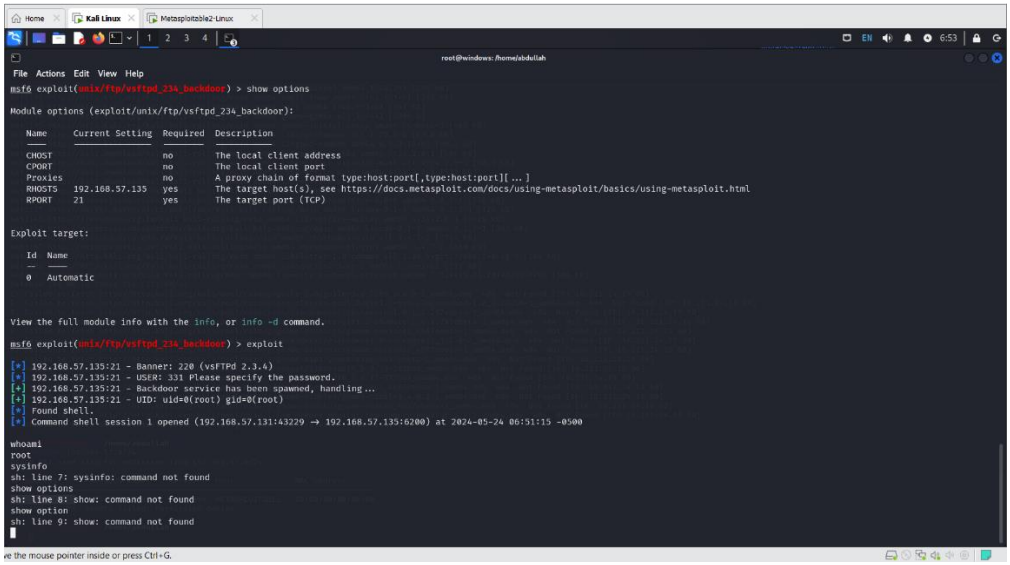
- Open ports: 21 (FTP), 22 (SSH), 23 (Telnet), 80 (HTTP), 3306 (MySQL).

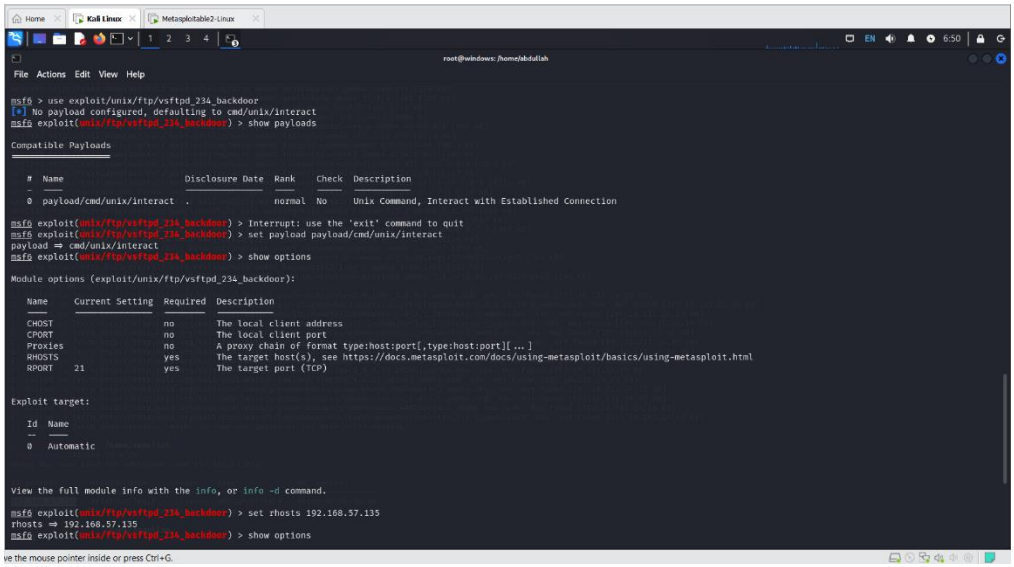
Gaining Access

Exploitation:

- **Using Metasploit**:
    - Command: **msfconsole**
    - Exploit used: **vsftpd_234_backdoor**
    - Successful login to the system.







Outcome: Gained initial access through FTP service.

Privilege Escalation:

Password Hash Extraction:

- Tool: **John the Ripper**

```
┌──(root㉿windows)-[/home/abdullah]
└─# john /home/abdullah/Desktop/shadow.txt --wordlist=usr/share/wordlists/rockyou.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8×3])
Will run 8 OpenMP threads
fopen: usr/share/wordlists/rockyou.txt: No such file or directory
```

4. Credentials Discovered

User ID	Password
root	msfadmin
klog	123456789
sys	batman
service	service

```
┌──(root㉿windows)-[/home/abdullah]
└─# john /home/abdullah/Desktop/shadow.txt --wordlist=/usr/share/wordlists/rockyou.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8×3])
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
123456789        (klog)
batman           (sys)
service          (service)
3g 0:00:01:00 29.74% (ETA: 09:08:02) 0.04954g/s 72233p/s 289151c/s 289151C/s r2pemo..r2366592
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
```

5. Files Exfiltrated

Sensitive Files Identified:

- **/etc/passwd**
- **/etc/shadow**

```
pango
passwd
passwd-
pcmcia
perl
php5
popularity-contest.conf
postfix
postgresql
postgresql-common
ppp
printcap
profile
profile.d
proftpd
protocols
purple
python
python2.5
rc.local
rc0.d
rc1.d
rc2.d
rc3.d
rc4.d
rc5.d
rc6.d
rcS.d
resolv.conf
resolvconf
rmt
rpc
samba
screenrc
securetty
security
services
sgml
shadow
shadow-
shells
```

6. Recommendations

1. Disable Unnecessary Services:

- Services like Telnet and FTP should be disabled or replaced with more secure alternatives like SSH and SFTP.

2. Strong Password Policies:

- Enforce strong password policies including complexity requirements and regular rotation.

3. Patch Management:

- Regularly update and patch all software to protect against known vulnerabilities.

4. Intrusion Detection Systems (IDS):

- Implement IDS to monitor and alert on suspicious activities.

5. Least Privilege Principle:

- Apply the principle of least privilege to limit user access based on role requirements.

6. Disable Anonymous Logins:

- Ensure anonymous logins are disabled for services like FTP.