Royal University of Bhutan

འབྲུག་རྒྱལ་འཛིན་གནོན་ལག་སློབ་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་ཁབ་ཀྱི་གཙུག་ལག་སློབ་གྲྭ།

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 taken from test books, articles, films, plays, handouts, internet, or any other source, whether published or unpublished.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

Table of Contents:

Royal University of Bhutan

འབྲུག་རྒྱལ་ཁབ་ཀྱི་གཙུག་ལག་སློབ་གྲྭ།

College of Science and Technology

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་ཁབ་ཀྱི་གཙུག་ལག་སློབ་གྲྭ།

College of Science and Technology

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.

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.

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

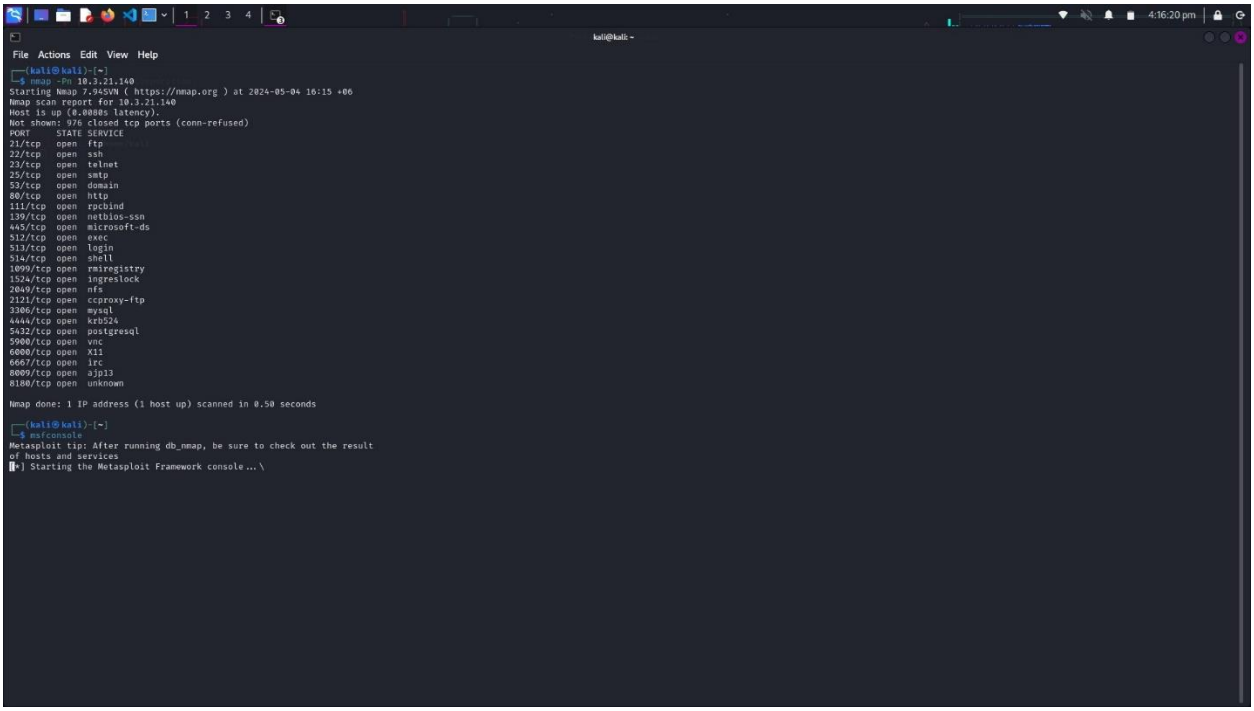
Network Compromise Walkthrough

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.

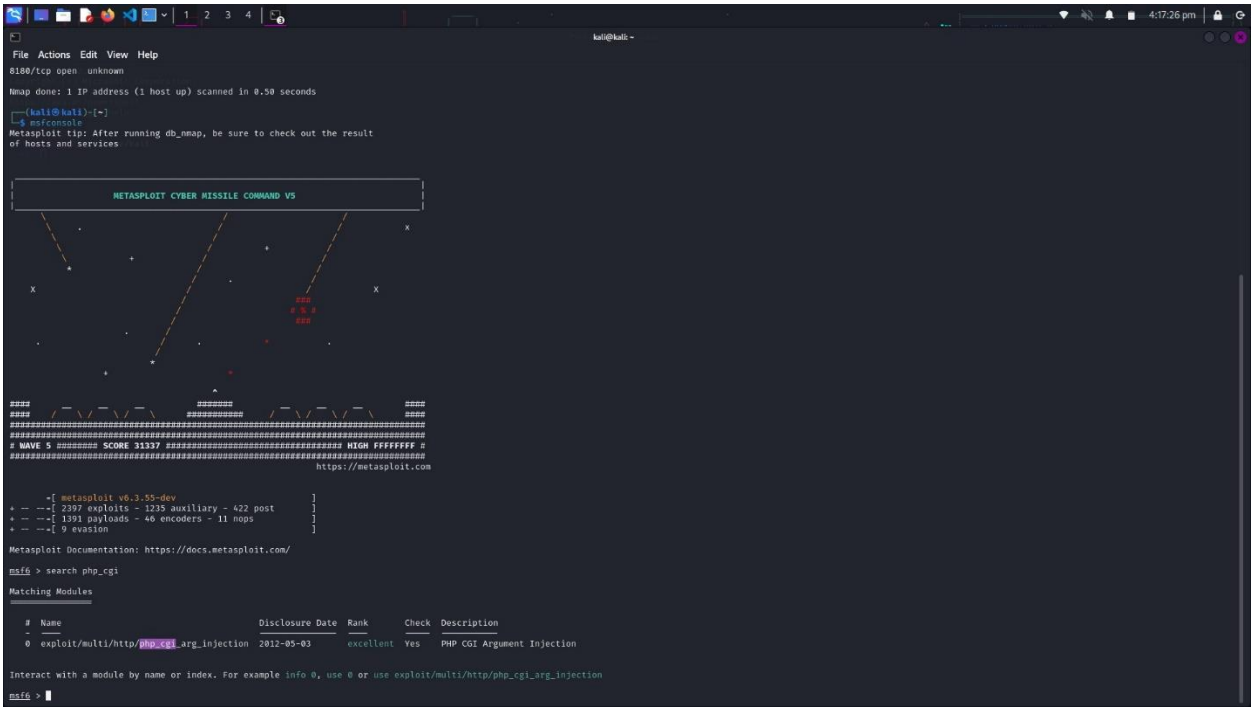
Detailed walked through:

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.

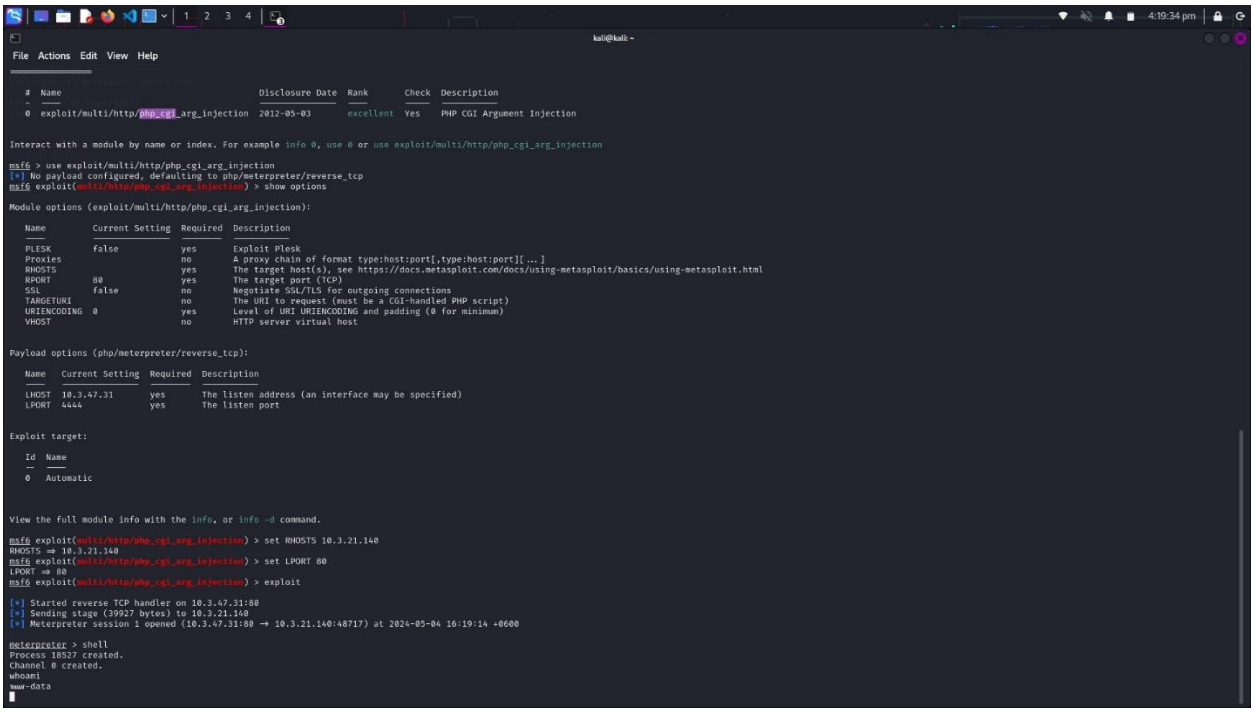
Port 80



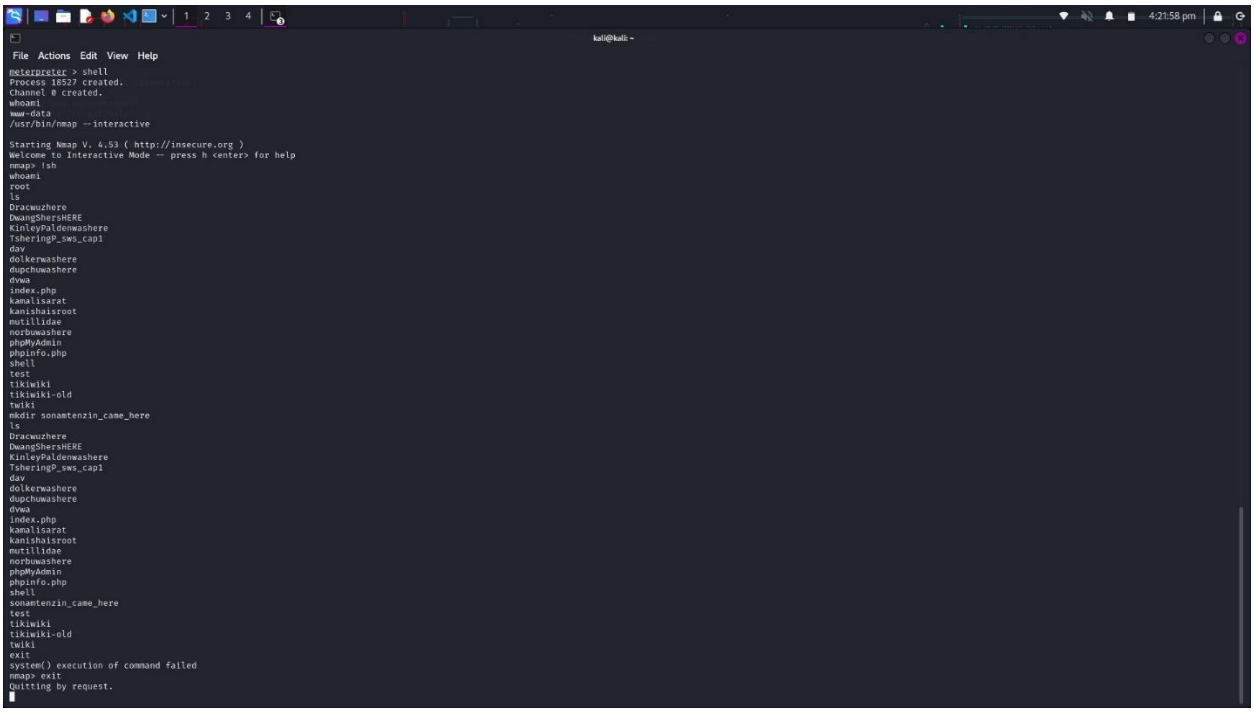
Scanning all the ports gave me the information that there were 17 ways I could have got into the system to get root access.



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

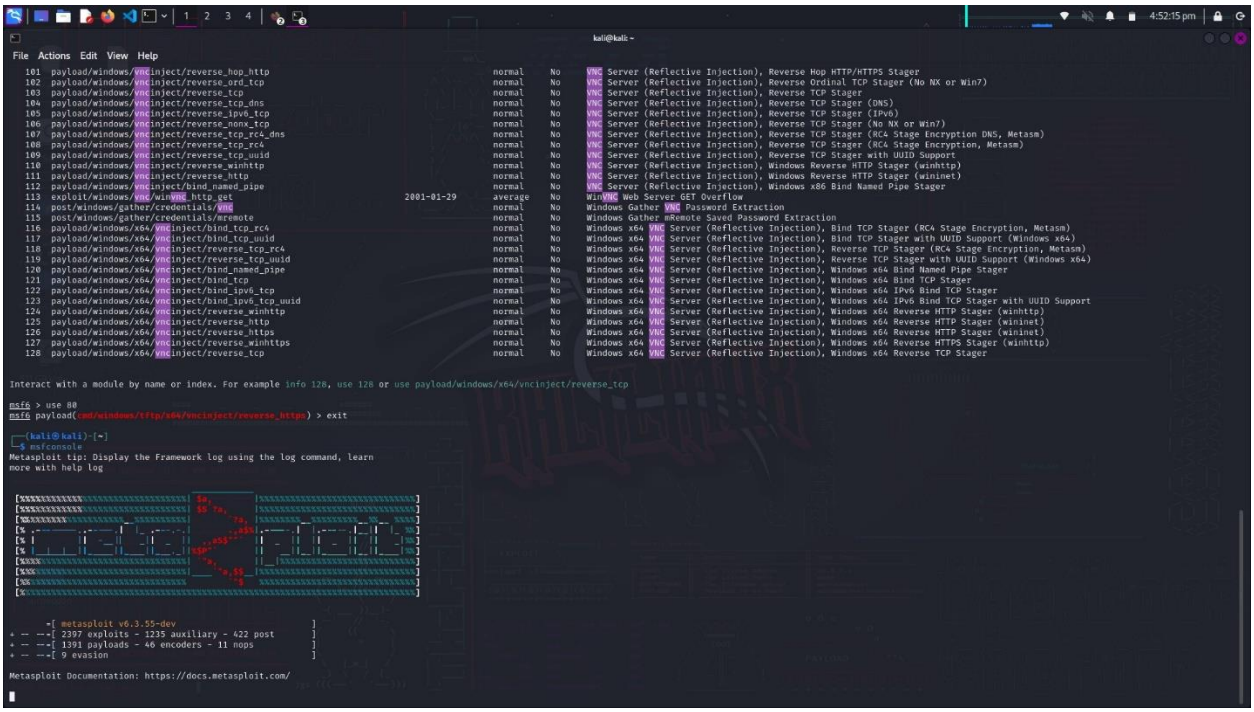


Setting the host to 10.3.21.140 nad LPORT to 80 and initiating the exploit.

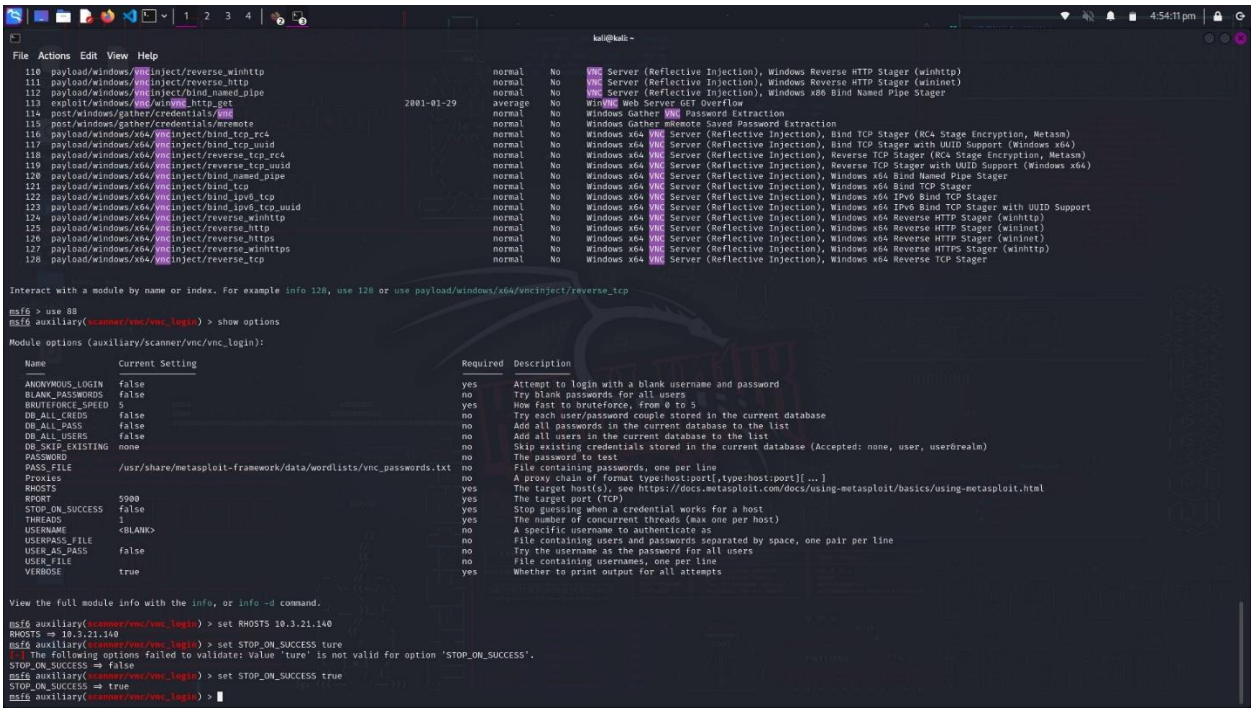


I checked my privilege by using the whoami and I have got the root privilege.

Port 5900



Firing up the Metasploit again to gain access through port 5900

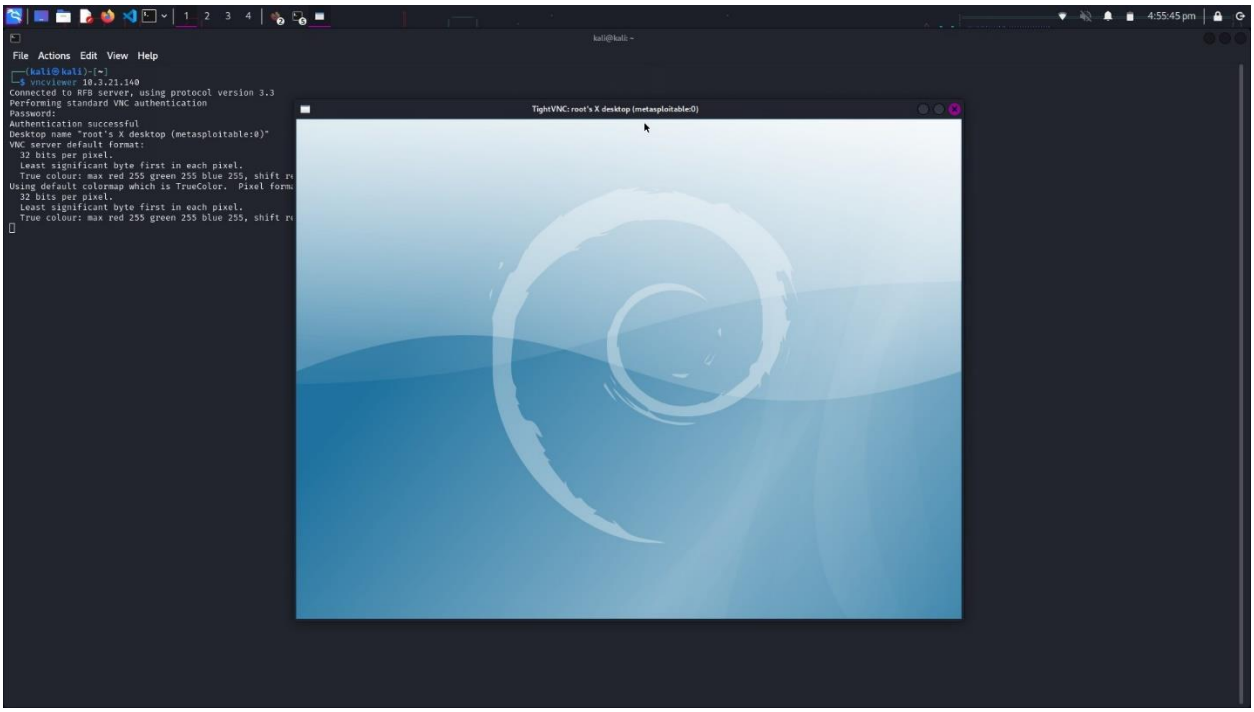


Setting the port number and the host again to begin the exploit.

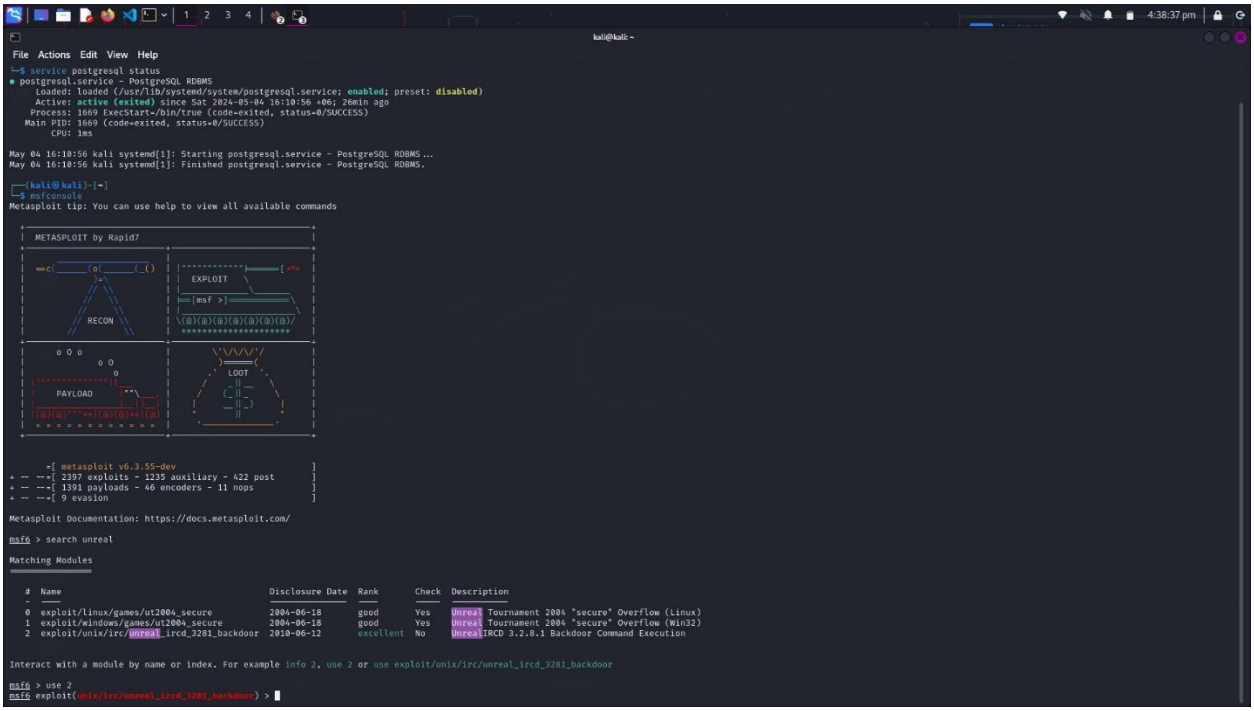
Royal University of Bhutan

འབྲུག་རྒྱལ་ཁབ་ཀྱི་གསོ་ལག་སློབ་གྲྭ།

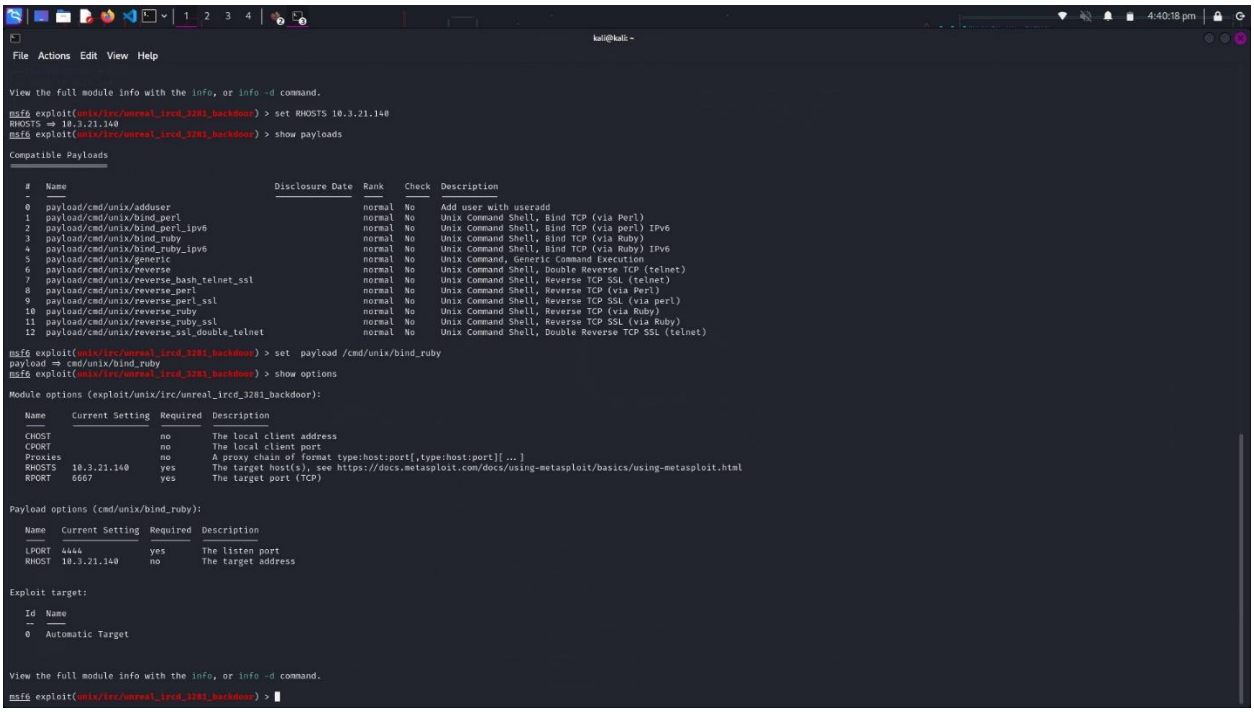
College of Science and Technology
Rinchending: Bhutan



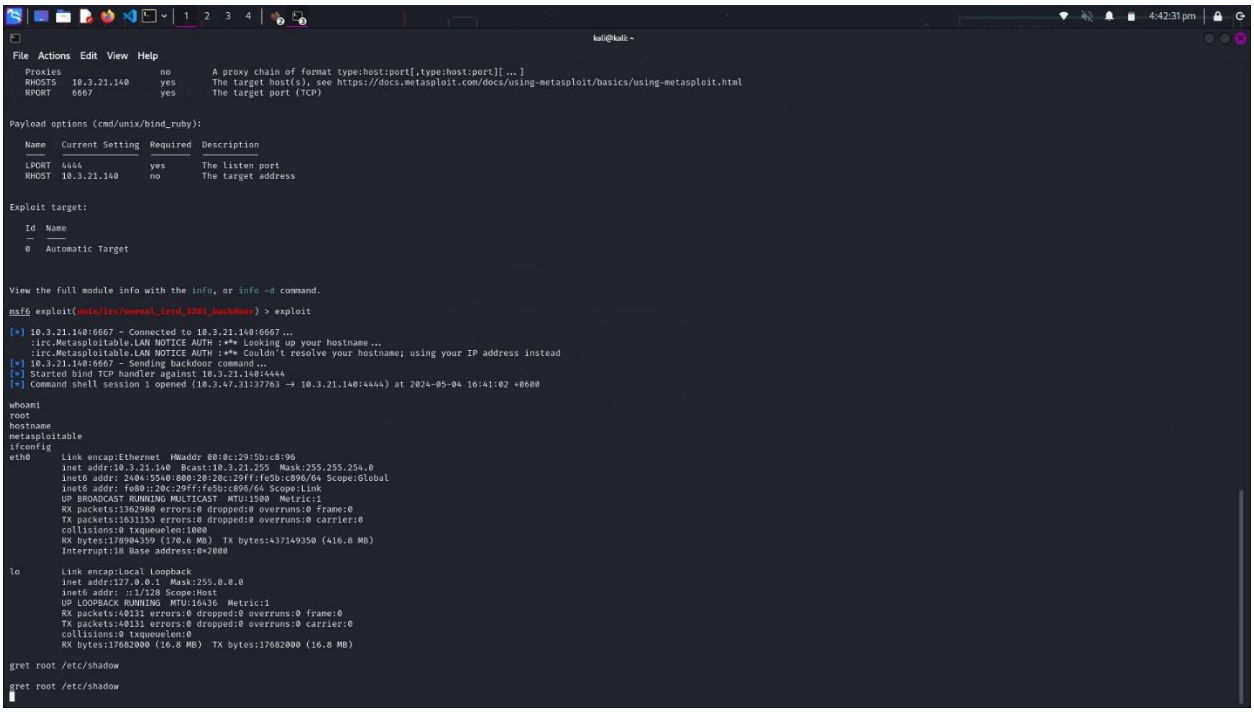
Port 6667



Searching for the right module to use against this current port.



Selecting the host and the port number once again.



This image proves that I have successfully gained root access.