**Assignment 05 – Metasploit Labtainer**

**Labtainer Metasploit Lab Report**

**Department of Computer Science**

**Adelphi university**

**CSC – 380 -001 Computer and Network Security**

**Professor. Sung Kim**

**By – Dikshant Kakadiya**

**Date – April 5th 2024**

**Introduction**

In this lab, we learned about the Metasploit tool. How to install the tool, learn, how to call the tool so that we can start the task.

Metasploit Lab Exercise

This lab was developed for the Labtainer framework by the Naval Postgraduate School, Center for Cybersecurity and Cyber Operations under National Science Foundation Award No. 1438893. This work is in the public domain, and cannot be copyrighted.

# Overview

This Labtainer exercise explores the use of the metasploit tool which is installed on a Kali Linux system (attacker) and is meant to learn simple penetration skills on a purposely vulnerable metasploitable host (victim).

Note: the attacker computer is configured to have IP address 192.168.1.3 while the victim computer is 192.168.1.2

# Performing the lab

The lab is started from the Labtainer working directory on your Linux host, e.g., a Linux VM. From there, issue the command:

labtainer metasploit

The resulting virtual terminal is connected to the attacker computer.

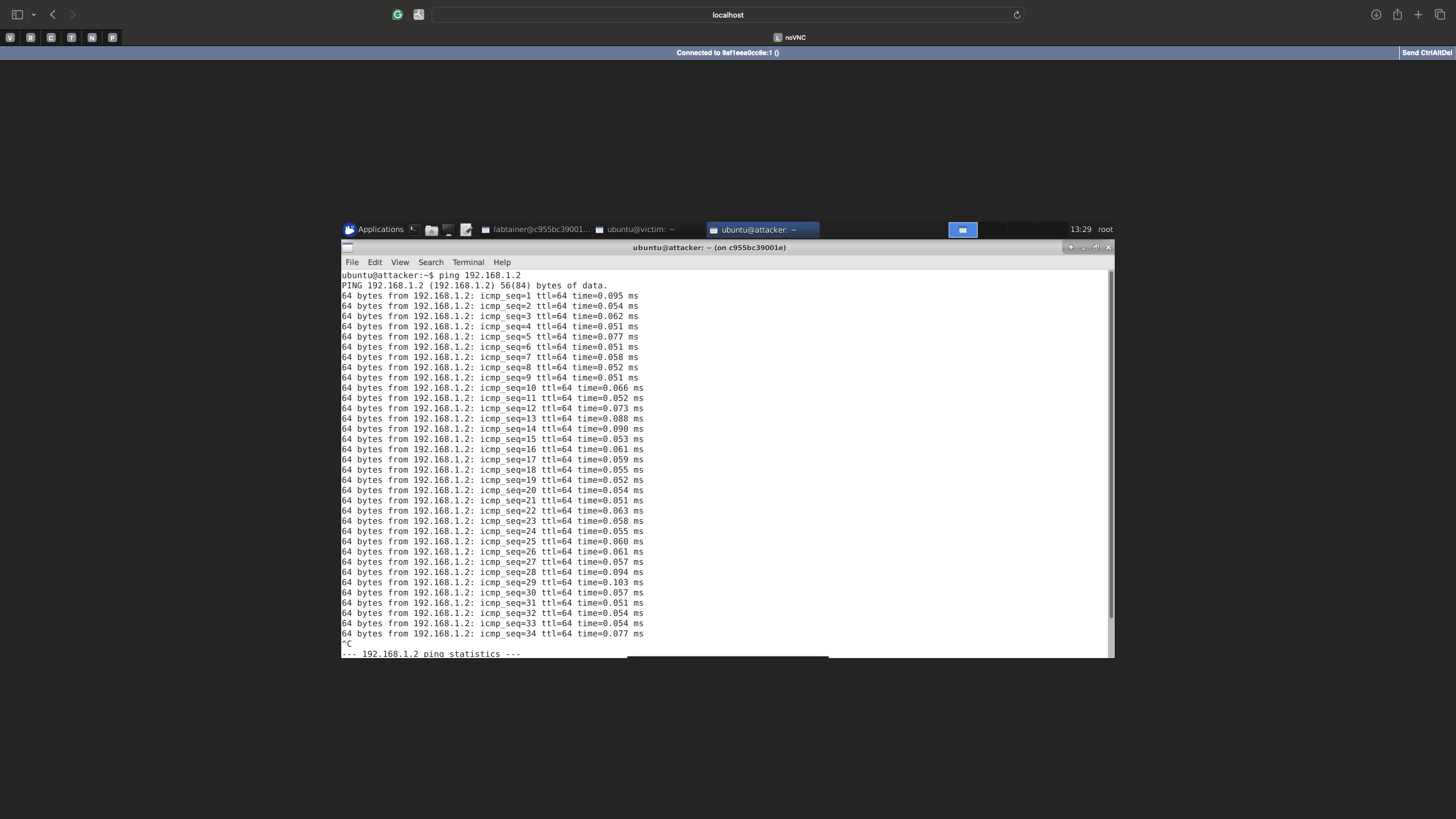
# Tasks

1. **Verify connectivity between attacker and victim**

A simple ping from the attacker system will be sufficient.

ping 192.168.1.2

We used the ping command to locate the server. The screenshot below shows how to use it.

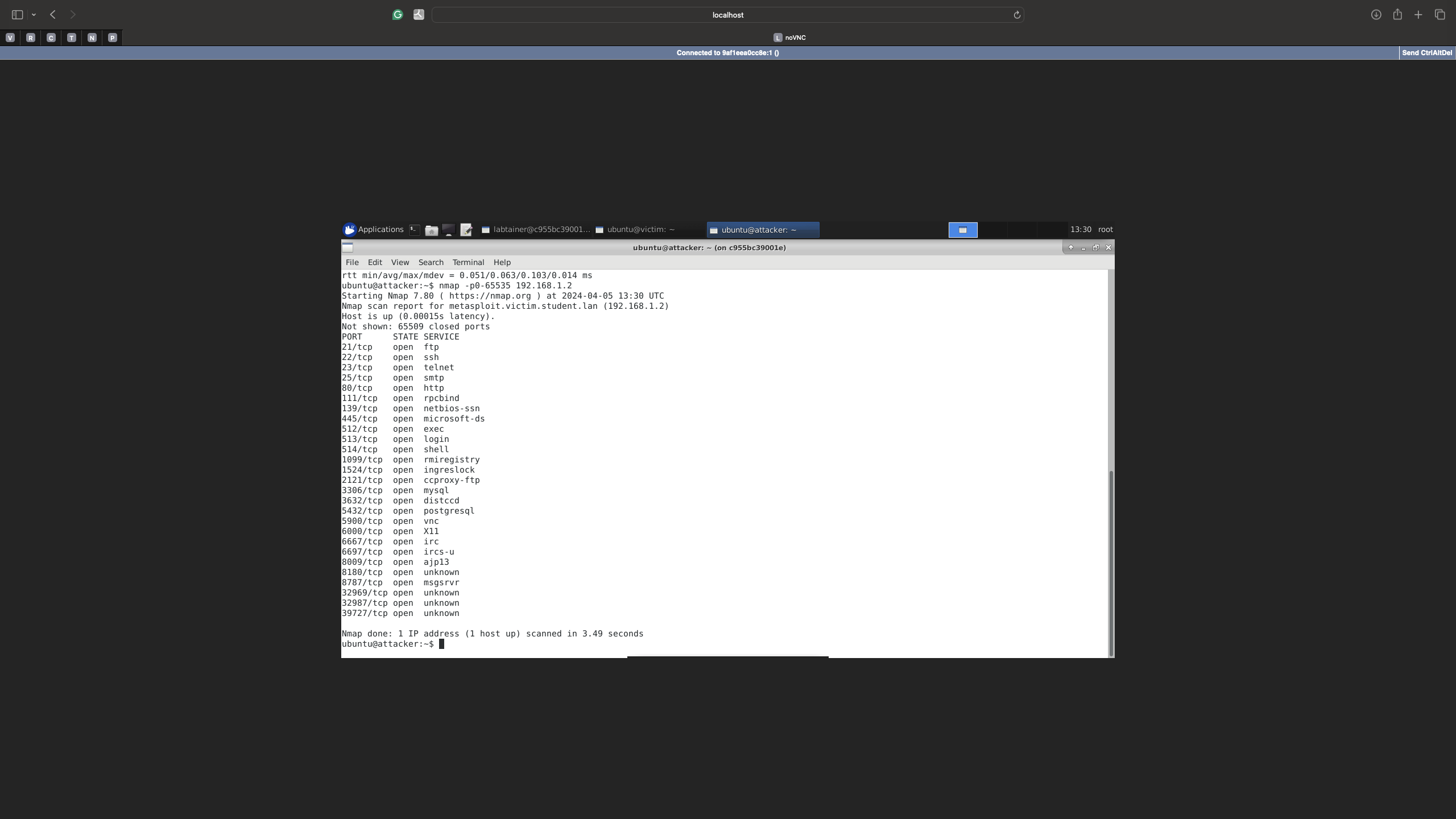


1. **Get a list of vulnerable services on the victim**

An 'nmap' scan of the victim will be sufficient.

nmap -p0-65535 192.168.1.2

we use namp command to scan the server from port 0 to 65535 to see what all ports are open and can be exploited. We can see how to use the command in the below screen short and we can see all the open ports.



1. V**ulnerably configured rlogin service (port 513)**

Remote login to the victim (with root privilege)

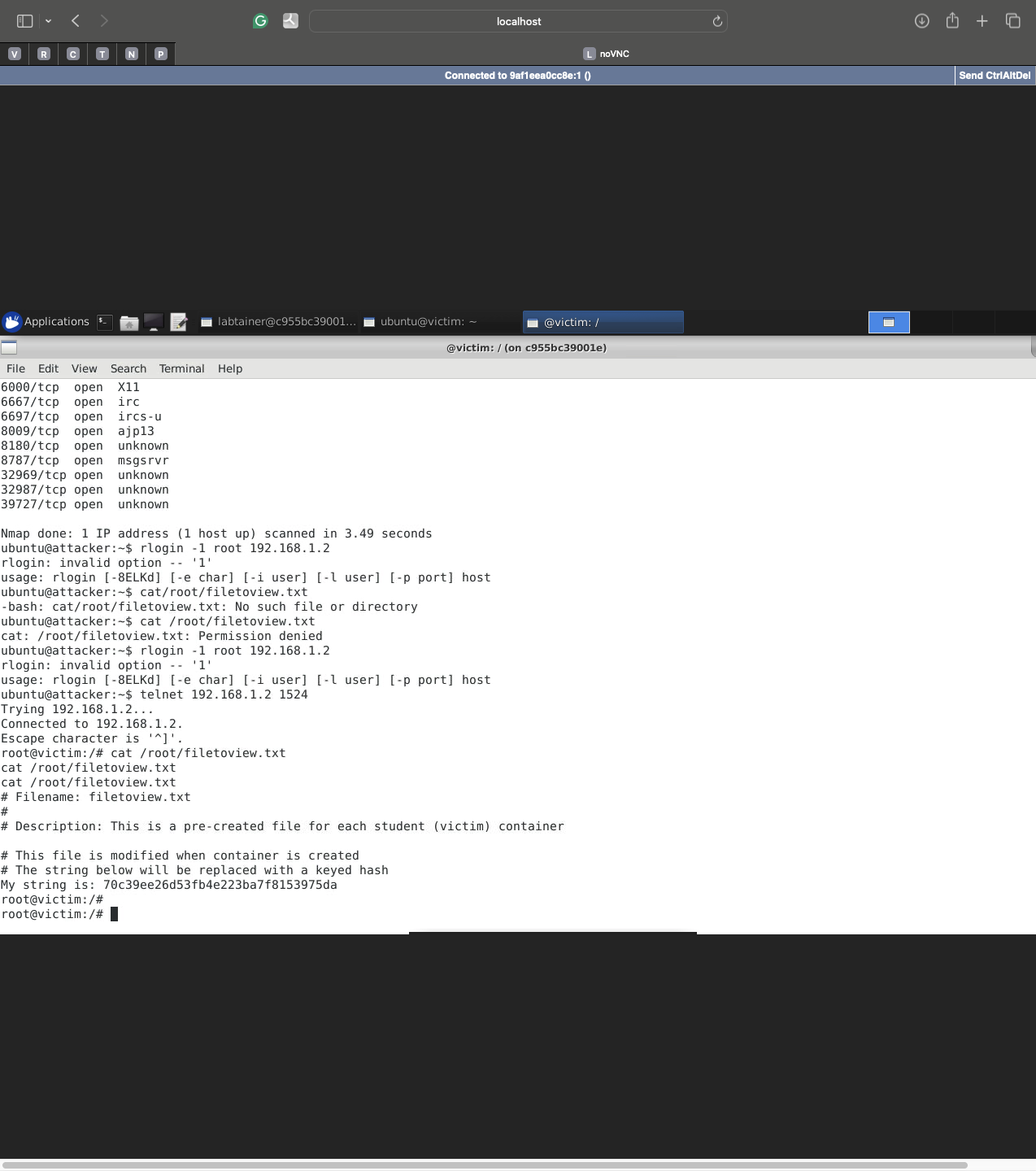
rlogin -l root 192.168.1.2

Display a 'root' file

cat /root/filetoview.txt

Display root file as above

We used the ‘telnet’ command to connect to the victim with root privilege. The screenshot below shows this. Once we got connected, we used the cat command to look into what was written into filetoview.txt

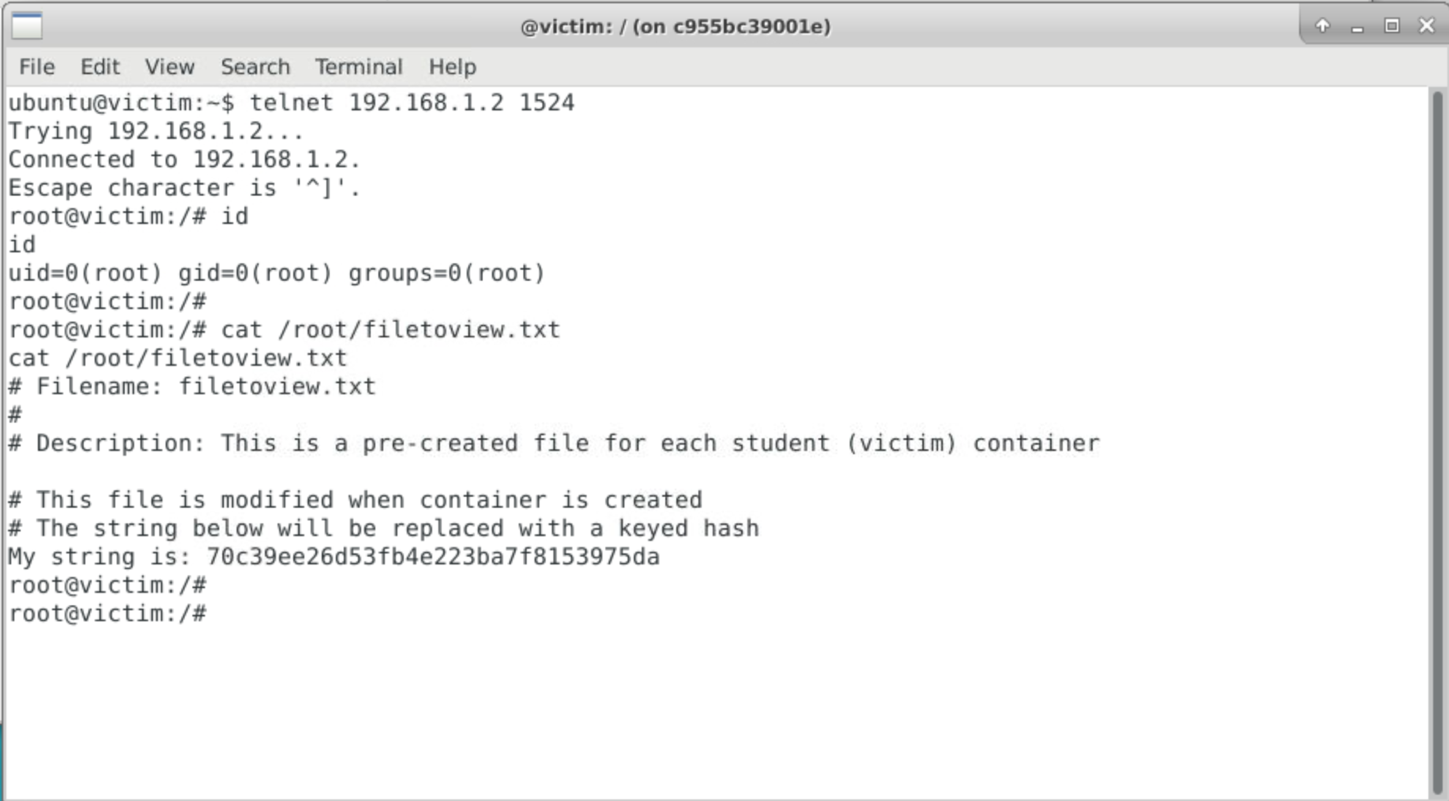


1. **Vulnerable ingreslock service (port 1524)**

Use telnet to access ingreslock service and obtain root privilege

telnet 192.168.1.2 1524

we were able to get root privileges as we can see id = o which is root



1. **Vulnerable distccd service (port 3632)**

Start Metasploit console

sudo msfconsole

Note you will see a warning about a missing database, you can ignore that. search for distccd exploit

search distccd

Use the exploit

use exploit/unix/misc/distcc\_exec

View options related to exploit

options

Set the 'RHOST' option

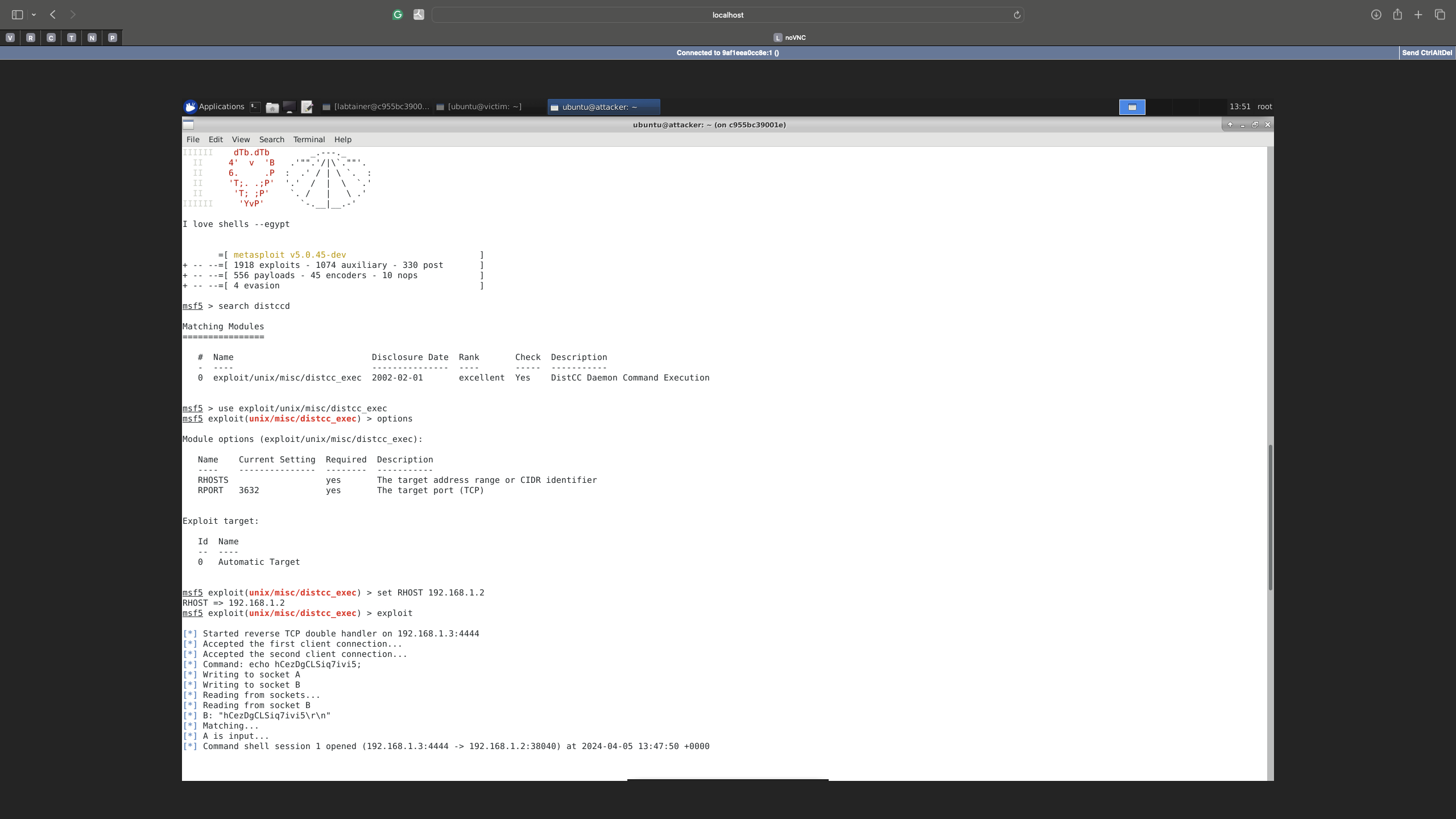
set RHOST 192.168.1.2

Run the exploit

exploit

Note: when the exploit has succeeded, no prompt is shown but a shell is created Display the root file as above

First, we launched the console and then used the search command to find the exploit we used by typing the use command. After that, we can see all the options that we can use by using the option command. Then, we will set the RHOST by using the set command. Then, finally, to run the exploit, we use the command exploit. We followed the steps and were able to successfully complete the attack. We use the cat command to look at the root file. We can see the entire process In a flowing screen-shot



1. **Vulnerable IRC daemon (port 6667)**

Search for unreal\_ircd exploit.

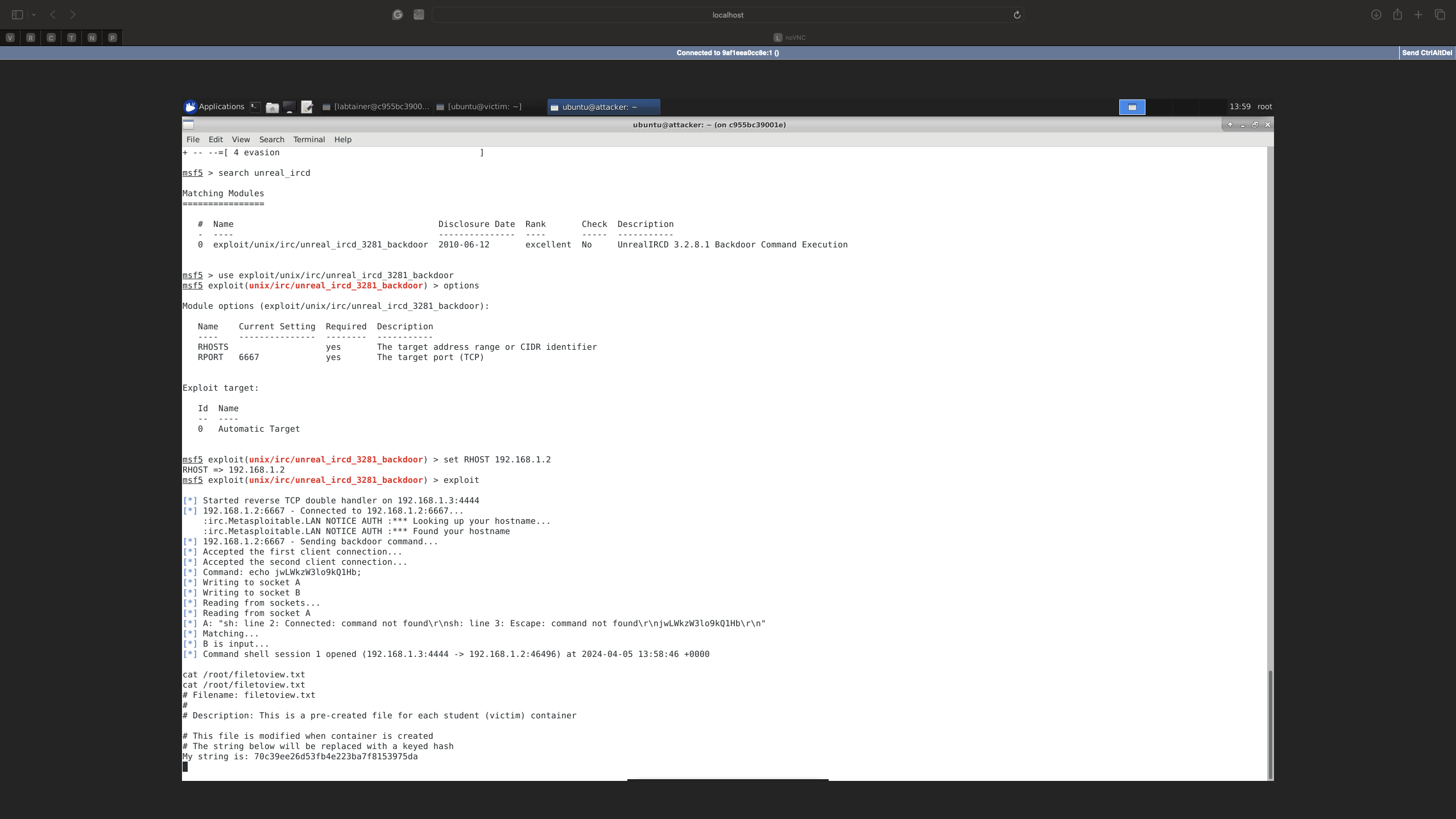
search unreal\_ircd

Use the exploit;

use exploit/unix/irc/unreal\_ircd\_3281\_backdoor

View and set options as necessary (RHOST option) run the exploit and display root file.

First, we launched the console and then used the search command to find the exploit we used by typing the use command. After that, we can see all the options that we can use by using the option command. Then, we will set the RHOST by using the set command. Then, finally, to run the exploit, we use the command exploit. We followed the steps and were able to successfully complete the attack. We use the cat command to look at the root file. We can see the entire process In a flowing screen-shot



1. **Vulnerable VSFtpd service (port 21)**

Search for vsftpd\_234

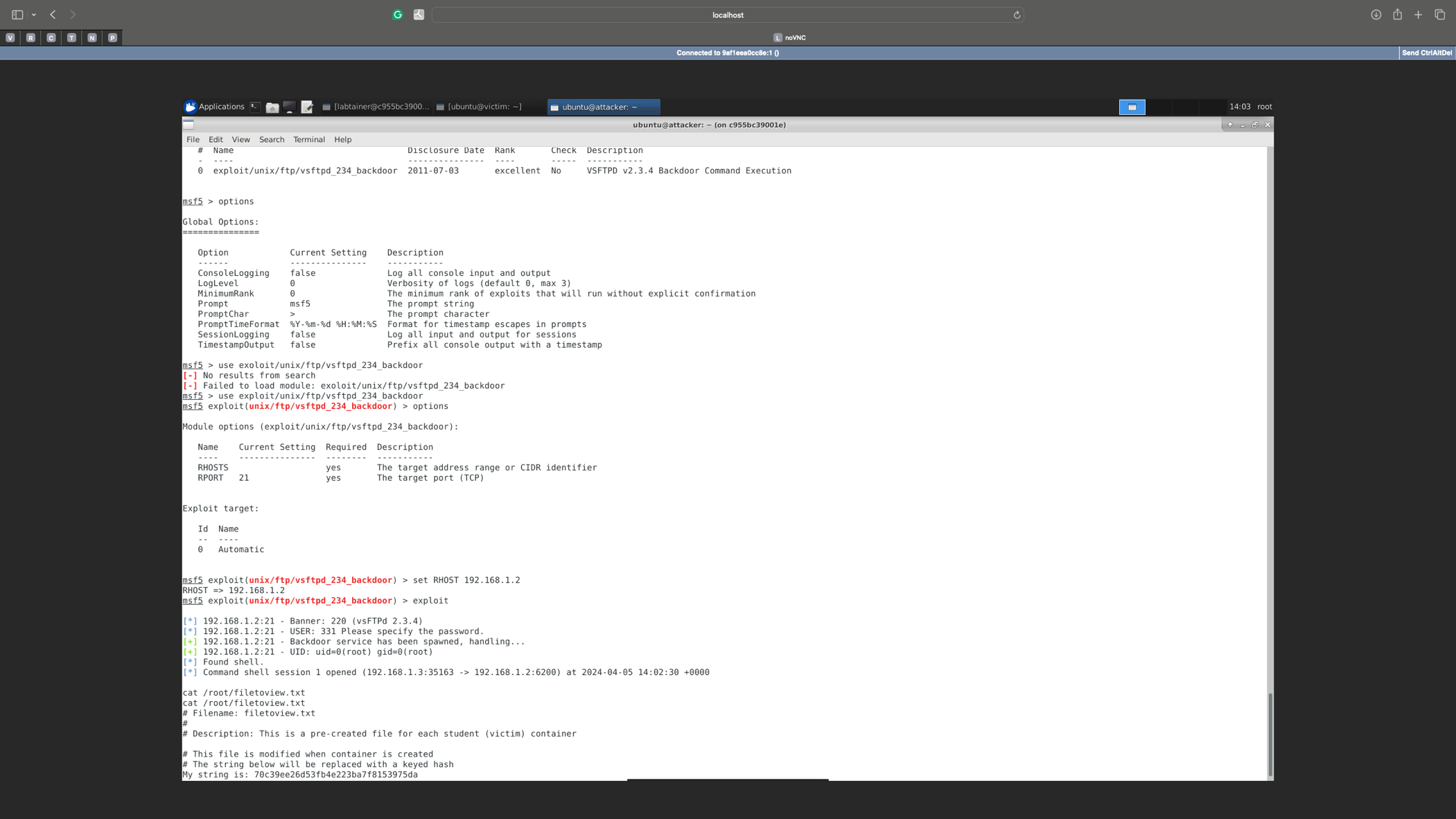
search vsftpd\_234

Use the exploit

use exploit/unix/ftp/vsftpd\_234\_backdoor

View and set options as necessary (RHOST option), run the exploit and display root file

First, we launched the console and then used the search command to find the exploit we used by typing the use command. After that, we can see all the options that we can use by using the option command. Then, we will set the RHOST by using the set command. Then, finally, to run the exploit, we use the command exploit. We followed the steps and were able to successfully complete the attack. We use the cat command to look at the root file. We can see the entire process In a flowing screen-shot



1. **Vulnerable Samba service (port 139)**

Search for samba usermap\_script

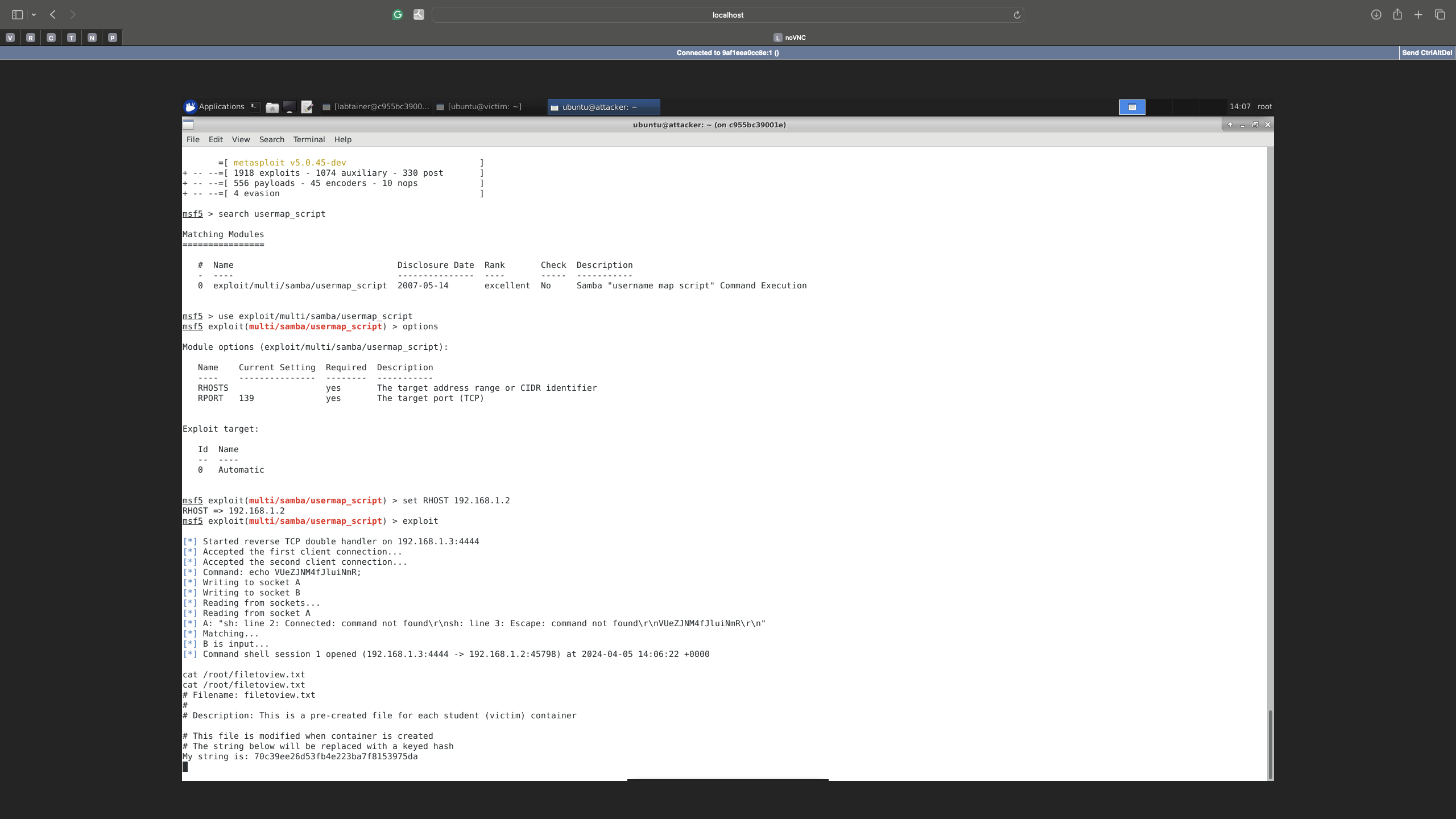
search usermap\_script

Use the exploit

use exploit/multi/samba/usermap\_script

View and set options as necessary (RHOST option), run the exploit and display root file

First, we launched the console and then used the search command to find the exploit we used by typing the use command. After that, we can see all the options that we can use by using the option command. Then, we will set the RHOST by using the set command. Then, finally, to run the exploit, we use the command exploit. We followed the steps and were able to successfully complete the attack. We use the cat command to look at the root file. We can see the entire process In a flowing screen-shot



1. **Vulnerable HTTP (php) service (port 80)**

Search for php\_cgi

search php\_cgi

Use the exploit

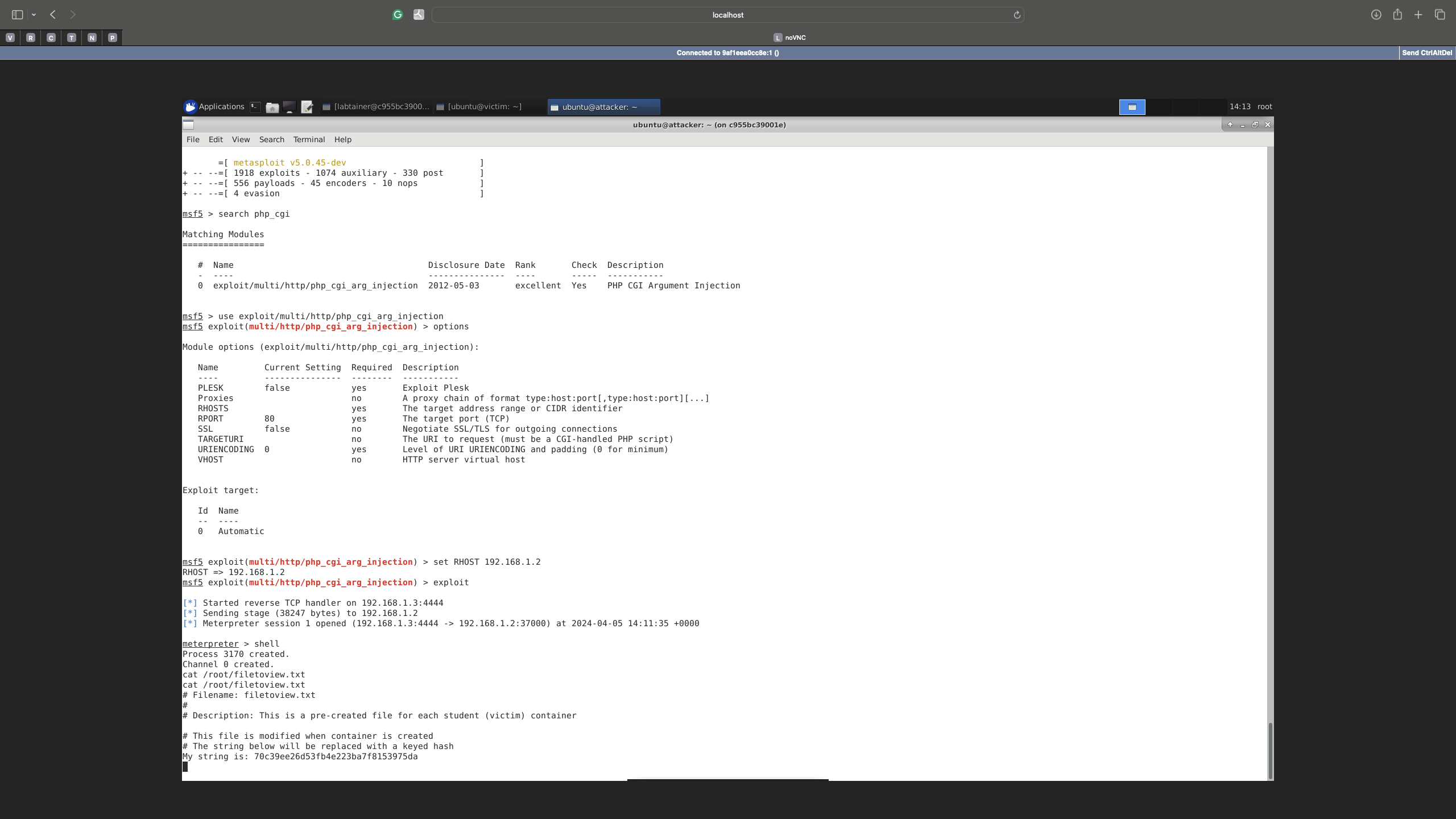
use exploit/multi/http/php\_cgi\_arg\_injection

View and set options as necessary (RHOST option) run the exploit Note: when the exploit is succeeded a 'meterpreter' prompt is shown From meterpreter prompt, drop to a shell

Shell

Display root file

First, we launched the console and then used the search command to find the exploit we used by typing the use command. After that, we can see all the options that we can use by using the option command. Then, we will set the RHOST by using the set command. Then, finally, to run the exploit, we use the command exploit. We followed the steps and were able to successfully complete the attack. We use the cat command to look at the root file. We can see the entire process In a flowing screen-shot



1. **Vulnerable Postgres service (port 5432)**

Search for postgres\_payload

search postgres\_payload

Use the exploit

use exploit/linux/postgres/postgres\_payload

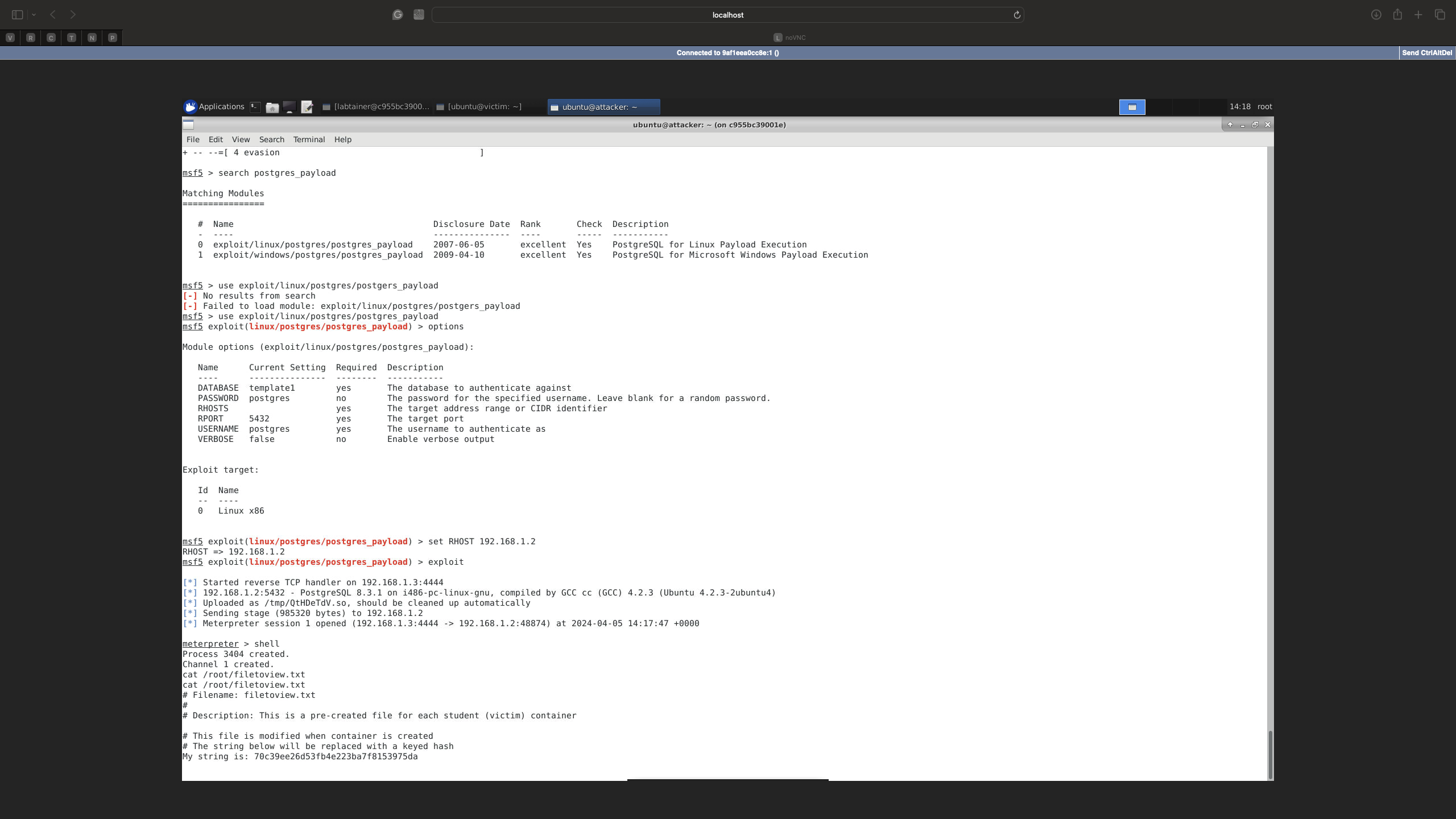
View and set options as necessary (RHOST option) run the exploit

Note: when the exploit is succeeded a 'meterpreter' prompt is shown From meterpreter prompt, drop to a shell.

shell

Display root file

First, we launched the console and then used the search command to find the exploit we used by typing the use command. After that, we can see all the options that we can use by using the option command. Then, we will set the RHOST by using the set command. Then, finally, to run the exploit, we use the command exploit. We followed the steps and were able to successfully complete the attack. We use the cat command to look at the root file. We can see the entire process In a flowing screen-shot



# Stop the Labtainer

When the lab is completed, or you'd like to stop working for a while, run

Stoplab

**Background**

For this lab, we followed the comprehensive and detailed Metasploit Labtainer lab instructions on Moodle; they told us exactly what to do. We didn’t use outside resources.

**Methodology/Results**

We looked at the instructions and followed them step by step; I was able to complete tasks. All of the results of this lab are documented, with images of the work done added when needed.