Installation & Getting Started

Website	https://github.com/trustedsec/social-engineer-toolkit
Install	git clone https://github.com/trustedsec/social-engineer-toolkit/ setoolkit/ cd setoolkit pip3 install -r requirements.txt python setup.py
User Manual	https://github.com/trustedsec/social-engineer-toolkit/-raw/master/readme/User_Manual.pdf
Creator Website	https://www.trustedsec.com/tools/the-social-engineer-toolkit-set/
Launch SET	$ setoolkit ---> [Run as root or provide sudo password at prompt.]

Main -> 1. Social-Engineering Attacks

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

set:infectious (SE Attack Option #3)

1	File-Format Exploits
2	Standard Metasploit Executable
99	Return to Main Menu

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.

set:mailer (SE Attack - Option #5)

1	E-Mail Attack Single Email Address
2	E-Mail Attack Mass Mailer
99	Return to main menu

Social Engineer Toolkit Mass E-Mailer

There are two options on the mass e-mailer, the first would be to send an email to one individual person. The second option will allow you to import a list and send it to as many people as you want within that list.

set:arduino (SE Attack Option #6)

1	Powershell HTTP GET MSF Payload
2	WSCRIPT HTTP GET MSF Payload
3	Powershell based Reverse Shell Payload
4	Internet Explorer/FireFox Beef Jack Payload
5	Go to malicious java site and accept applet Payload
6	Gnome wget Download Payload
7	Binary 2 Teensy Attack (Deploy MSF payloads)
8	SDCard 2 Teensy Attack (Deploy Any EXE)
9	SDCard 2 Teensy Attack (Deploy on OSX)
10	X10 Arduino Sniffer PDE and Libraries
11	X10 Arduino Jammer PDE and Libraries
12	Powershell Direct ShellCode Teensy Attack
13	Peensy Multi Attack Dip Switch + SDCard Attack
14	HID Msbuild compile to memory Shellcode Attack
99	Return to Main Menu

The Arduino-Based Attack Vector utilizes the Arduin-based device to program the device. You can leverage the Teensy's, which have onboard storage and can allow for remote code execution on the physical system. Since the devices are registered as USB Keyboard's it will bypass any autorun disabled or endpoint protection on the
system.

To purchase a Teensy, visit: http://www.pjrc.com/store/teensy.html
Select a payload to create the pde file to import into Arduino:

set:powershell - (SE Attacks - Option #9)	
1	Powershell Alphanumeric Shellcode Injector
2	Powershell Reverse Shell
3	Powershell Bind Shell
4	Powershell Dump SAM Database
99	Return to Main Menu

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.

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

set:phishing menu (SE Attack Option #1)	
1	Perform a Mass Email Attack
2	Create a FileFormat Payload
3	Create a Social-Engineering Template
99	Return to Main Menu

The Spearphishing module allows you to specially craft email messages and send them to a large (or small) number of people with attached fileformat malicious payloads. If you want to spoof your email address, be sure "Sendmail" is installed (apt-get install sendmail) and change the config/set_config SENDMAIL=OFF flag to SENDMAIL=ON.

set:webattack (SE Attack Option #2)	
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	HTA Attack Method
99	Return to Main Menu

set:payloads (SE Attacks - Option #4)	
1 - Windows Shell Reverse_TCP	Spawn a command shell on victim and send back to attacker
2 - Windows Revers-e_TCP Meterpreter	Spawn a meterpreter shell on victim and send back to attacker
3 - Windows Revers-e_TCP VNC DLL	Spawn a VNC server on victim and send back to attacker
4 - Windows Shell Reverse_TCP X64	Windows X64 Command Shell, Reverse TCP Inline
5 - Windows Meterpreter Reverse_TCP X64	Connect back to the attacker (Windows x64), Meterpreter
6 - Windows Meterpreter Egress Buster	Spawn a meterpreter shell and find a port home via multiple ports
7 - Windows Meterpreter Reverse HTTPS	Tunnel communication over HTTP using SSL and use Meterpreter
8 - Windows Meterpreter Reverse DNS	Use a hostname instead of an IP address and use Reverse Meterpreter
9 - Download/Run your Own Executable	Downloads an executable and runs it
[CTRL-C]	Return to Main Menu

set:wireless (SE Attack - Option #7)

1	Start the SET Wireless Attack Vector Access Point
2	Stop the SET Wireless Attack Vector Access Point
99	Return to Main Menu

The Wireless Attack module will create an access point leveraging your wireless card and redirect all DNS queries to you. The concept is fairly simple, SET will create a wireless access point, dhcp server, and spoof DNS to redirect traffic to the attacker machine. It will then exit out of that menu with everything running as a child process.

This attack vector requires AirBase-NG, AirMon-NG, DNSSpoof, and dhcpd3.

QR Code - (SE Attacks Option #8)

[URL]	Enter the URL you want the QRCode to go to:
99	Return to Main Menu

The QRCode Attack Vector will create a QRCode for you with whatever URL you want.

When you have the QRCode Generated, select an additional attack vector within SET and deploy the QRCode to your victim. For example, generate a QRCode of the SET Java Applet and send the QRCode via a mailer.

Main 2 --> Penetration Testing (Fast-Track)

1	Microsoft SQL Bruter
2	Custom Exploits
3	SCCM Attack Vector
4	Dell DRAC/Chassis Default Checker
5	RID_ENUM - User Enumeration Attack
6	PSEXEC Powershell Injection
99	Return to Main Menu

Main --> 3. Third Party Modules

1	Google Analytics Attack by @ZonkSec
2	RATTE Java Applet Attack (Remote Administration Tool Tommy Edition) - Read the readme/RATTE_README.txt first
3	RATTE (Remote Administration Tool Tommy Edition) Create Payload only. Read the readme/RATTE-Readme.txt first

Main --> 3. Third Party Modules (cont)

99	Return to the previous menu

[-] Please read the readme/modules.txt for information on how to create your own modules.