Menu Options

1 *Social-Engineering Attacks*	Various social engineering attacks
2 *Penetration Testing (Fast Track)*	Attack vectors with a series of exploits and automation aspects to assist in penetration testing
3 *Third Party Modules*	Third party modules such as RATTE and google analytic attacks
4 *Update the Social-Engineer Toolkit*	Updates SET and all of its modules
5 *Update SET configuration*	Applies any updates made to the set.config file
6 *Help, Credits, and About*	Shows all of the credits as well as links to the official SET documentation
99 *Exit the Social-Engineer Toolkit*	Exits SET as well as exiting any menu from within the modules

Social Engineering Attacks

Spear-Phishing Attack Vectors

Allows you to specially craft emails and send to any number of people with attached fileformat malicious payloads

Website Attack Vectors

The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim. Attacks include Java Applet, Metasploit Browser Exploit, Credential Harvester, Tabnabbing and Web Jacking

Infectious Media generator

Social Engineering Attacks (cont)

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

Create a Payload and Listener

Various Windows payload/listeners ranging from meterpreter sessions to VNC servers on the victim

Mass Mailer Attack

Sends phishing email to single email or various pulled from a user created list

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. Devices are registered as USB Keyboard's and will bypass any autorun disabled or endpoint protection on the system

Wireless Access Point Attack Vector

Creates a rogue access point and redirect victims back to the SET web server when associated

QRCode Generator Attack Vector

Creates a QRCode for any URL entered. Can be paired with additional attack vectors within SET to deploy the QRCode to the victim

Powershell Attack Vectors

Allows you to create PowerShell Specific attacks such as shellcode injectors, reverse shells and bind shells

Penetration Testing (Fast-Track)

Microsoft SQL Bruter

Will attempt to identify live MSSQL servers and brute force the weak account passwords that may be found. If that occurs, SET will then compromise the affected system by deploying a binary to hexadecimal attack vector which will take a raw binary, convert it to hexadecimal and use a staged approach in deploying the hexadecimal form of the binary onto the underlying system

Custom Exploits

Obscure exploits that are primarily python driven. Exploits include MS08-067, Firefox 3.6.16 mChannel object use, Solarwinds remote SQL injection, RDP denial of service, MySQL Authentication Bypass and F5 Root Authentication bypass

SCCM Attack Vector

Utilizes SCCM configurations to deploy malicious software. Requires an SMSServer name and packageID you want to package on the website

Dell DRAC/Chassiss Default Checker

Identifies the default installations of Dell DRAC and chassis installations. If found allows you to access remote administration capabilities to compromise the entire infrastructure

RID_ENUM - User Enumeration Attack

Enumerate user accounts through a rid cycling attack through null sessions. Used internally against a domain controller

PSEXEC Powershell Injection

Injects a meterpreter backdoor through powershell memory injection. Will circumvent Anti-Virus since it never touches the disk