University of Missouri – Columbia

Social-Engineering Toolkit

**By:**

Andy Schuster (ABSDM2)

**Course:**

INFOTC 3910 Bazan Antequera - Advanced Cyber Security

**Topic:**

It comes as no surprise that Kali Linux has lots of pre-installed tools. After playing around with various different programs and commands, I came across Social-Engineer Toolkit. This tool is pre-installed on Kali Linux. I fooled around with the menu and was impressed with how simple and useful most of the attacks are. This was interested to me because it is very user friendly. It did not take a lot of time to figure it out and there are multiple vectors attacks that can be used. This toolkit can be used in a real world setting fairly easily. Instead of having to create a exact replica of a google login page, for example, you are able to clone it with SET.

**Research:**

The Social-Engineer Toolkit (SET) is an open-source penetration testing framework designed for social engineering. SET has a number of custom attack vectors that allow you to make a believable attack in a fraction of time. These kinds of tools use human behaviors to trick them to the attack vectors (Tutorialspoint) SET can be accesses in the Kali Linux terminal by default and is a menu-based layout (no GUI). It can also be installed on Mac OS as well as other Linux systems (T, 2020). The toolkit has pre-installed attacks. Some of these attacks include sending mass phishing emails, QRCode Generator Attack Vector, Infectious Media Generator, even some third-party user made attacks and so many more. The attacks built into the toolkit are designed to be targeted and focused attacks against a person or organization used during a penetration test (Wright, 2018). For a pocket-sized social engineering toolkit, users have flashed Kali Linux OS to their raspberry Pi. As stated above, SET is preinstalled on Kali linux so flashing the OS onto the raspberry pi gives their pi all of the tools necessary to have a small, yet full capable, hacking device (CyberSecurityAssociates). A popular use for SET is using is as a penetrate test against users. One way this can be done is by web-based attacks. The attacker can use a template or even clone a site then use a phishing email to get the target to use their false site. Because it is a template or a cloned site, the target user will hardly notice any changes. The phishing email may say something along the lines of “Your account is at risk. Sign in now”. Something that gains the targets attention and makes them rush to open the link. Once they log in, using port forwarding, it will sign them in as usual leaving the target clueless while simultaneously sending the login information to the attacker. This is one of many attacks that have become very common with SET. You are also able to execute multiple attacks against multiple targets. For instance, if you start out with a mass phishing attempt you can then use a web template and place that link in the mass email. You can then get the credentials of multiple targets when they use the web template form.

**Applications:**

**Starting Social-Engineering Toolkit:** To start the toolkit, you can run the command “setoolkit” in terminal. You are also able to open it through the Kali Linux GUI. Both of these options will open the toolkit menu in terminal. The screenshot below shows what the terminal menu will look like upon starting.

Text

Description automatically generated

**Choosing an attack:** The toolkit has various different options. This includes phishing attempts, cloning webpages, even to Qrcode Attacks. To demonstrate, I will run through cloning a webpage to obtain user log in credentials. To get started we will choose one on the menu, Social-Engineering Attacks. Then we will choose option two, Website Attack Vectors. From there, we are greeting with the different web attacks. A screenshot is below.

Text

Description automatically generated

Once web attack is selected, we can then choose option three: Credential Harvester Attack Method. In this attack vector, a website will be cloned, and when the victim enters the user credentials, the usernames and passwords will be posted back to your machine and then the victim will be redirected back to the legitimate site (Samarasekera, 2020). Once we choose the Credential Harvester Attack Method, we are then asked which method we want to use. Option one: Web Templates allows the attacker to use a predefined webpage as an attack. Option two: Site Cloner allows the attacker to use their own URL. This can be a login URL. The last option is Custom Import which allows the attacker to use their own website.

Text

Description automatically generated

**Running the attack:** Using a web template, we are asked what IP address we want to use for the POST back. The POST back is where we want the victims results to go. The IP address in the screenshot below is my systems IP address so this is the IP that I will use. We then get to pick the template we would like to use. Currently the options are “ava Required, Google, and Twitter.

Text

Description automatically generated

After picking the Twitter template, we are in action. Once we are connected to the IP, we will see the traffic coming in.

Text

Description automatically generated

The screenshot below shows the IP of my attacking system in my target systems internet browser. You can see the Twitter login page. If I had my own server set up, I could easily change the IP to something like “Twitte.r” so the target would be less likely to suspect anything. When the target system user enters their username and password, it will then be transferred to the attacker system terminal.

Graphical user interface, application

Description automatically generated

**Sources:**

Tutorialspoint. (n.d.). *Kali Linux - Social Engineering - Tutorialspoint*. Retrieved November 22, 2020, from https://www.tutorialspoint.com/kali\_linux/kali\_linux\_social\_engineering.htm

T. (2020). *trustedsec/social-engineer-toolkit*. GitHub. https://github.com/trustedsec/social-engineer-toolkit

Wright, D. M. W. (2018, March 3). *What is Social-engineer Toolkit? - Quora*. Quora. https://www.quora.com/What-is-Social-engineer-Toolkit

CyberSecurityAssociates. (n.d.) Social Engineering Toolkit (SET) Pi – Student Worksheet. https://static1.squarespace.com/static/5ba4e5c87a1fbd36d01467bc/t/5c408ae4aa4a999d5 49c3954/1547733737022/024-SET-Student.pdf

Samarasekera, K. (2020, March 26). *Credential Harvester Attack - Kaviru Samarasekera*. Medium. https://medium.com/@kaviru.mihisara/credential-harvester-attack-73335c4a5bb8