Social-Engineer Toolkit (SET): Pwning the Person

By Russ McRee – ISSA Senior Member, Puget Sound (Seattle), USA Chapter

Prerequisites/dependencies

Python interpreter
Metasploit
BackTrack 5 R3 also includes SET

My first discussion of Dave Kennedy's (@dave_rel1k) Social-Engineer Toolkit (SET) came during exploration of the Pwnie Express PwnPlug Elite[1] for March 2012's *toolsmith*.[2] It was there I talked about the Site Cloner feature found under Website Attack Vectors and Credential Harvesting Attack Methods. Unless you've been hiding your head in the sand ("if I can't see the security problem, then it doesn't exist") you're likely aware that targeted attacks such as spear phishing, whaling, and social engineering in general are prevalent. Additionally, penetration testing teams will inevitably fall back on this tactic if it's left in scope for one reason: it always works. SET serves to increase awareness for all the possible social engineering vectors; trust me, it is useful for striking much fear in the hearts of executives and senior leaders at client, enterprise, and military briefings. It's also useful for *really* understanding the attacker mindset. With distributions such at BackTrack including SET, fully configured and ready to go, it's an absolute no brainer to add to your awareness briefing and/or pen-testing regimen.

Dave is the affable and dynamic CEO of TrustedSec (@trustedsec) and, as SET's creator, describes it in his own words:

> *The Social-Engineer Toolkit has been an amazing ride and the support for the community has been great. When I first started the toolkit, the main purpose was to help out on social engineering gigs, but it's completely changed to an entire framework for social engineering and the community. SET has progressed from a simple set of python commands and web servers to a full suite of attacks that can be used for a number of occasions. With the new version of SET that I'm working on, I want to continue to add customizations to the toolkit where it allows you to utilize the multi-attack vector and utilize it in a staged approach that's all customized. When I'm doing social engineering gigs, I change my pretext (attack) on a regular basis. Currently, I custom code some of my options such as credential harvester first then followed by the Java Applet. I want to bring these functionalities to SET and continue forward with the ability to change the way the attack works based on the situation you need. I use my real-life social engineering experiences with SET to improve it; if you have any ideas, always email me to add features!*

Be sure to catch Dave's presentation videos from DEFCON and DerbyCom, amongst others, on the TrustedSec SET page.[3]

Quick installation notes

It's easiest to run SET from BackTrack. Boot to it via USB or optical media, or run it as a virtual machine. Navigate to *Applications* | *BackTrack* | *Exploitation Tools* | *Social Engineering Tools* | *Social Engineering Toolkit* | *set* and you're off to the races.

Alternatively, on any system where you have a Python interpreter and a Git (version control/source code management) client, you can have SET up and running in minutes. Ideally, the system you choose to run SET from should have Metasploit configured too as SET calls certain Metasploit payloads, but it's not a hard, fast dependency. If no Metasploit, many SET features won't work, simple. But if you plan to go full goose bozo…you catch my drift.

I installed SET on Ubuntu 12.10 as well as Windows 7 64-bit as simply as running `git clone https://github.com/trustedsec/social-engineer-toolkit/ set/` from a Bash shell (Ubuntu) or Git Shell (Windows). **Note**: if you're running anti-malware on a Windows system where SET is to be installed, be sure to build an exclusion for the SET path or AV will eat some key exploits (six to be exact). A total bonus for you and me occurred as I wrote this. On 24 JAN, Dave released version 4.4.1 of SET, codename "The Goat." If you read the CHANGES file in SET's readme directory, you'll learn that this release includes some significant Java Applet updates, encoding and encryption functionality enhancements, and improvements for multi_pyinjector. I updated my BackTrack 5 R3 instance to SET 4.4.1 by changing directory to `/pentest/exploits`, issuing `mv set set_back`, then the above mentioned git command. Almost instantly, a shiny new SET ready for a few laps around the track. Your SET instance needs to be available via the Internet for remote targets to phone home to, or exposed to your local network for enterprise customers. You'll be presenting a variety of offerings to your intended victims via the SET server IP or domain name.

1 http://pwnieexpress.com/products/pwnplug-elite.
2 http://holisticinfosec.org/toolsmith/pdf/march2012.pdf.
3 https://www.trustedsec.com/downloads/social-engineer-toolkit/.

SET unleashed

Now to rapid fire some wonderful social engineering opportunities at you. How often do you or someone you know wander up to a sign or stop at a web page with a QR code and just automatically scan it with your smart phone? What if I want to send you to any site of my choosing? I'll simply generate a QR code with the URL destination I want to direct you to. If I'm a really bad human being, that site might be offering up the Blackhole exploit kit or something similar. Alternatively, as SET recommends when you choose this module, "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."

From the SET menu, choose *1) Social-Engineering Attacks*, then *9) QRCode Generator Attack Vector*, and enter your desired destination URL. SET will generate the QR code and write it to `/pentest/exploits/set/reports-qr_attack.png` as seen in figure 1.

Figure 1 – QR Code attack generated by SET

From SET's main menu, *3)Third Party Modules* will offer you the RATTE Java Applet Attack (Remote Administration Tool Tommy Edition), and *2) Website Attack Vectors* | *1) Java Applet Attack Method* will provide templates or site cloning with which you can delivery one heck of a punch via the QR code vector.

Our good friend Java is rife for social engineer targeting opportunities and SET offers mayhem aplenty to capitalize on this fact. Here's a sequence to follow from the SET menu:

`1) Social-Engineering Attacks | 2) Website Attack Vectors | 1) Java Applet Attack Method | 1) Web Templates`

Answer *yes* or *no* to NAT/Port Forwarding, enter your SET server IP or hostname, and select *1* for the Java Required template as seen in figure 2.

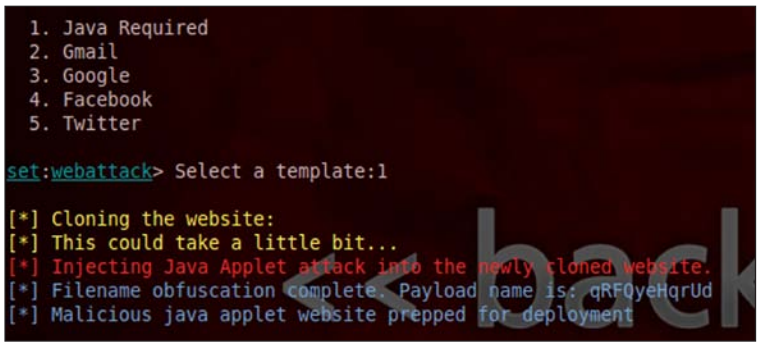

Figure 2 – Java Applet prepped for deployment

Figure 3 – Java Applet prepped for deployment

You'll then need to choose what payload you wish to generate. Methinks ye olde *Windows Reverse_TCP Meterpreter Shell* (#2 on the list) is always a safe bet. Select it accordingly. From the list of encodings, #16 on the list (Backdoored Executable) is described as the best bet. Make it so. Accept 443 as the default listener port and wait while SET generates injection code as seen in figure 3.

The Metasploit framework will then launch (wake up, Neo... the matrix has you…follow the white rabbit) and the handlers will standby for your victim to come their way.

Now, as the crafty social engineer that you are, you devise an email campaign to remind users of the "required Java update." By the way, this campaign can be undertaken directly from SET as well via *1) Social-Engineering Attacks* | *5) Mass Mailer Attack*. When one or more of your victims receives the email and clicks the embedded link, they'll be sent to your SET server where much joy awaits them as seen in figure 4 (next page).

When the victim selects *Run*, and trust me he will, the SET terminal on the SET server will advise you that a Meterpreter session has been opened with the victim as seen in figure 5 (next page).

For our last little bit of fun, let's investigate *3) Infectious Media Generator under 1) Social-Engineering Attacks*. If you select *File-Format Exploits*, after setting up your listener, you'll be presented with a smorgasbord of payload. I selected *16) Foxit PDF Reader v4.1.1 Title Stack Buffer Overflow* as I had on old VM with an old Foxit version on it. Sweet! When I opened the fileformat exploit PDF created by SET with the Foxit 4.1.1, well…you know what happened next.

As discussed in the PwnPlug article, don't forget the Credential Harvester Attack Methods under Website Attack Vectors. This is quite literally my favorite delivery vehicle as it is utterly bomb proof. Nothing like

Figure 4 – Victim presented with Java required and "trusted" applet

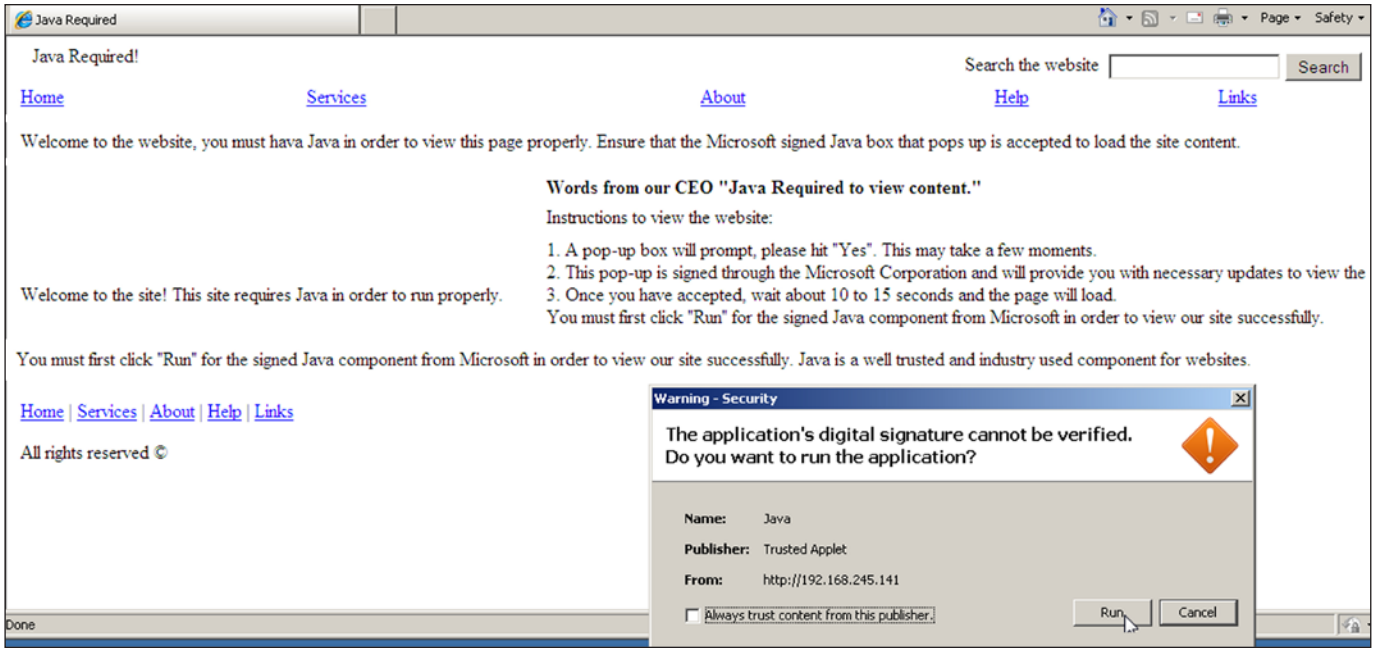

Figure 5 – Anyone want a shell?

using the templates for your favorite social media sites (you know who you are) and watching as credentials roll in.

In conclusion

Evil-me really loves SET; it's more fun than a clown on fire. Remember, as always with tools of this ilk, you're the good guy in this screenplay. Use SET to increase awareness, put the fear of God in your management, motivate your clients, and school the occasional developer. Anything else is flat out illegal. ☺ As Dave mentioned, if you have ideas for new features or enhancements for SET, he really appreciates feedback from the community.

Ping me via email if you have questions or suggestions for topic via russ at holisticinfosec dot org or hit me on Twitter @holisticinfosec.

Cheers…until next month.

Acknowledgements

—Dave Kennedy, Founder, TrustedSec, SET project lead

About the Author

Russ McRee manages the Security Analytics team (security incident management, penetration testing, monitoring) for Microsoft's Online Services Security & Compliance organization. In addition to toolsmith, he's written for numerous other publications, speaks regularly at events such as DEFCON, Black Hat, and RSA, and is a SANS Internet Storm Center handler. As an advocate for a holistic approach to the practice of information assurance Russ maintains holisticinfosec.org. He serves in the Washington State Guard as the Cybersecurity Advisor to the Washington Military Department. Reach him at russ at holisticinfosec dot org or @holisticinfosec.