CIS 700/002: Special Topics: Social Engineering Toolkit

Nikheel Savant & Thejas Kesari
CIS 700/002: Security of EMBS/CPS/IoT
Department of Computer and Information Science
School of Engineering and Applied Science
University of Pennsylvania

17 March 2017

Penn Engineering

PRECISE

Overview

- Intro
- Social Engineering Attacks
  - –Credential Harvesting
  - –Web jacking
  - –Payload / Listening (Trojan)
  - –Spearphishing
- Mailbomb

Social Engineering

- “Psychological manipulation of people into performing actions or divulging confidential information”
- Differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme
- “Social Engineering (SE) is a blend of science, psychology and art. While it is amazing and complex, it is also very simple.”

Social Engineering

- Can be safely assumed that an adversary has at least attempted a social engineering attack prior to a high-impact cyber-physical attack
- Even the strongest technical security protections can be bypassed if a system's legitimate user is manipulated into letting the adversary in

- Primary target: Any cyber-physical system operated by human users or connected to a corporate network

Condor Speaks

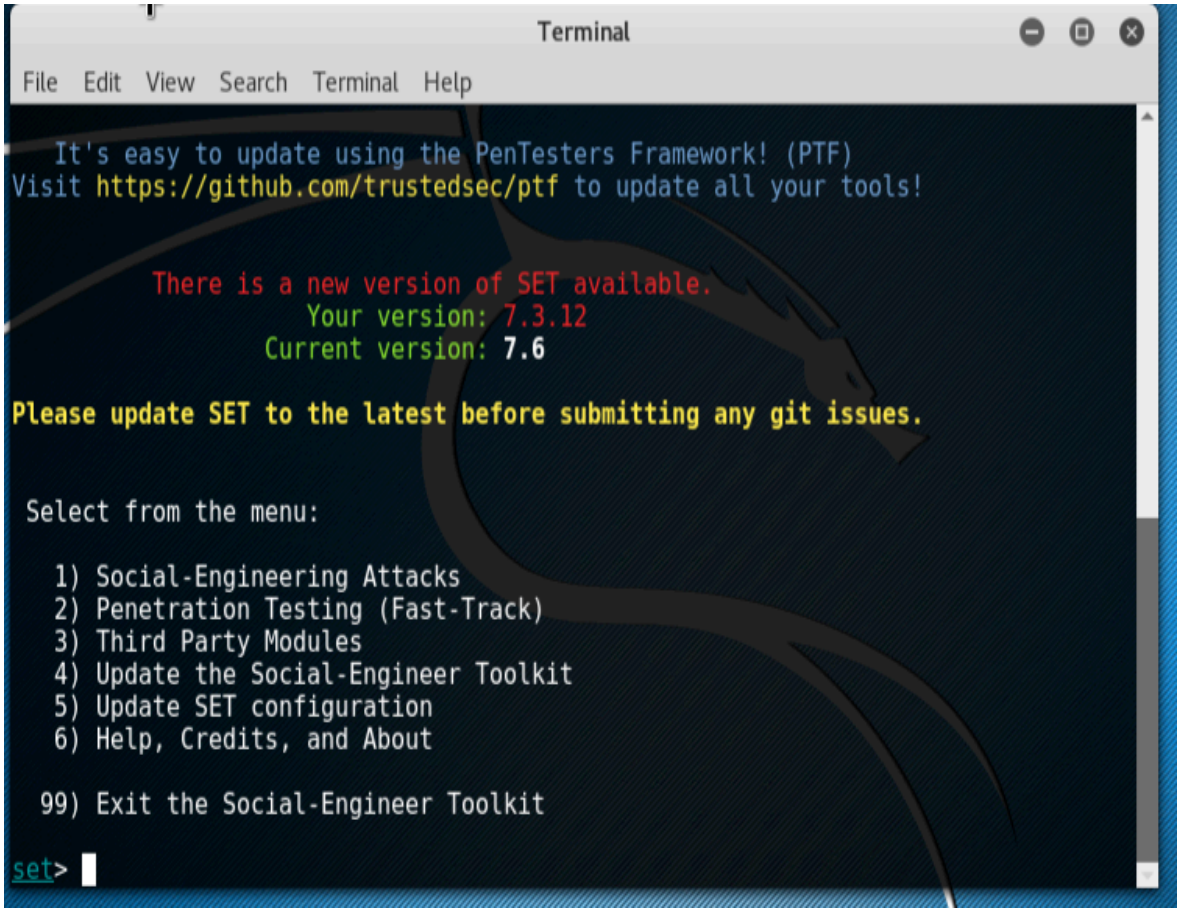
"The human side of computer security is easily exploited and constantly overlooked. Companies spend millions of dollars on firewalls, encryption and secure access devices, and it's money wasted, because none of these measures address the weakest link in the security chain."

-Kevin Mitnick

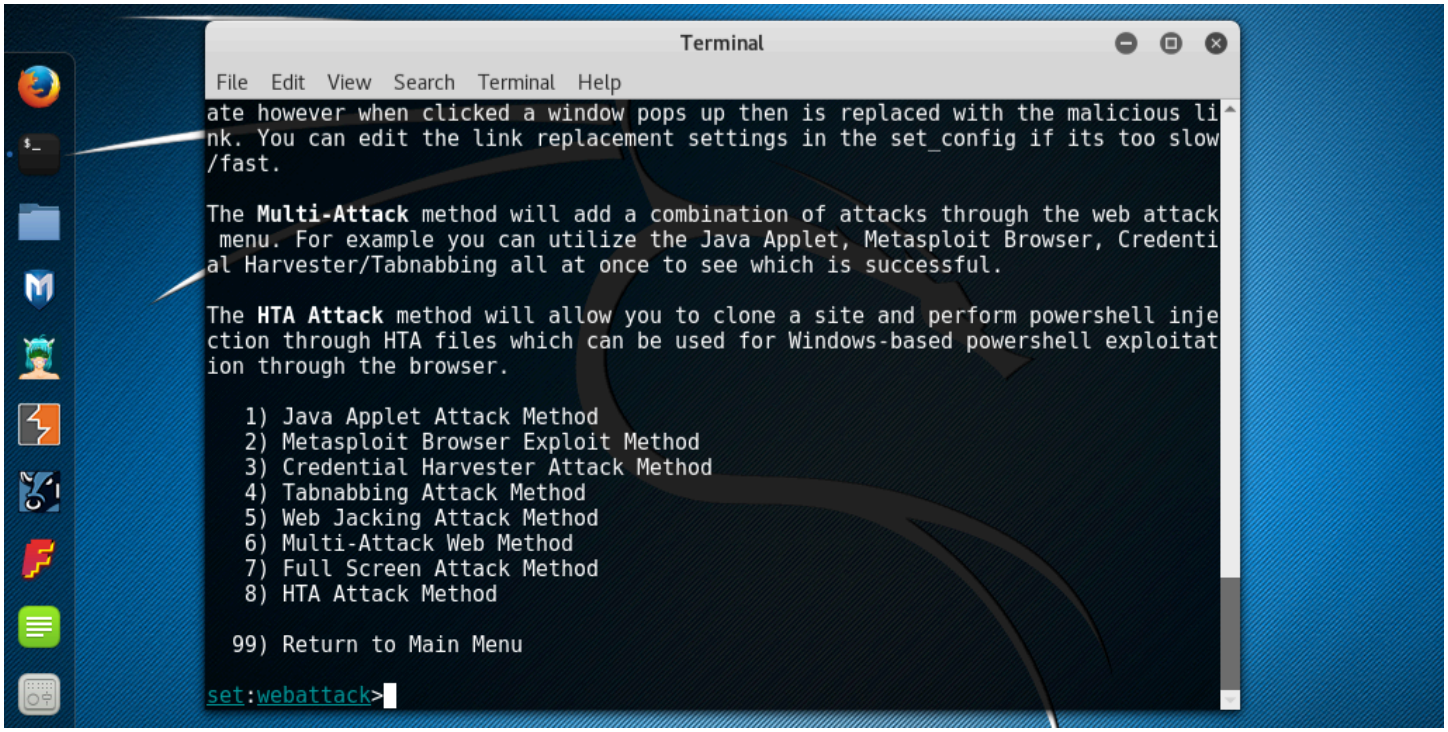
Poulsen, K. (2000). Mitnick to lawmakers: People, phones and weakest links. SecurityFocus, March 2000.

Social Engineering Toolkit

- Developed by TrustedSec
- Written by David Kennedy (ReL1K)
- Open-source and cross-platform
- Offers an array of attacks based on computer phishing


Terminal
File Edit View Search Terminal Help
It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!
There is a new version of SET available.
Your version: 7.3.12
Current version: 7.6
Please update SET to the latest before submitting any git issues.
Select from the 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>

Website Attack Vectors



Credential Harvesting

- Let's harvest Facebook login credentials
- Choose Credential Harvester Attack (3)
- Then choose Site Cloner

Credential Harvesting (Local)

- Obtain local IP address and paste it for POST back
- Enter the URL: www.facebook.com
- And done!

A little further…

- bit.ly or goo.gl to hide disguise the IP
- Custom domain and forward to the said IP address

Credential Harvesting (Local)

- Observe the address when the link opens, try to disguise it better
- Credentials stored in default directory /var/www/html

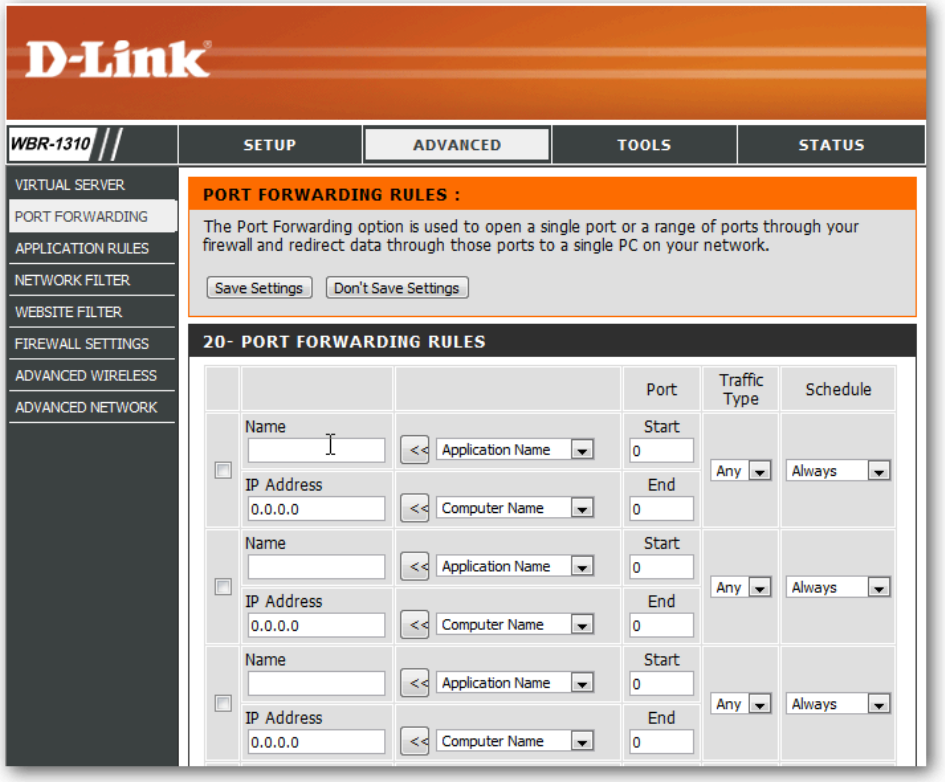
Remote Credential Harvesting (needs router access)

- Obtain public IP address (google “what is my ip”) and paste it for POST back
- Enter the URL: www.facebook.com
- And done! Well, not yet.

Remote Credential Harvesting

- Set a port forwarding rule
- Forward to local IP
- Start port and End port (Internal/External): 80 & 80

Homework: Try harvesting credentials remotely



Web jacking

- Create a fake lookalike and redirect the user there
- User opens the link but gets a message that the website has been moved to another address

Web jacking

- Similar procedure, basically another form of credential harvesting
- Credentials copied to the same directory /var/www/html

- Homework: Try remote web jacking

Backdoor SET Easy Trojan

Steps to be followed

- Select #1 Social-Engineering Attacks
- We need to create a payload and a listener
- Select #4 Create a Payload and Listener

Steps to be followed

- Select #2 option Windows Reverse_TCP Meterpreter
- Use ifconfig to get the ipaddress
- Use PORT 443

Steps to be followed

- Go to specific folder mentioned
- Find payload.exe-> Properties-> Permission->Tick check box Allow executing file as program

Steps to be followed

- Rename the payload.exe as Setup.exe
- Copy paste to your local machine
- Disable Antivirus Real time scanning

Steps to be followed

- Type sessions -i 1
- Press help for all commands:
  - ps - List of running processes
  - keyscan_start
  - keyscan_dump
  - Keyscan_stop
- Homework: Try Backdoor attacks remotely

Spear phishing

Steps to be followed

- Select #1 Social Engineering Attacks
- Select #1 Spear-Phishing
- Select #2 Create a Fileformat Payload

Steps to be followed

- Select #4 MS Word RTF
- Select #5 Windows Meterpreter Reverse_TCP
- Get ipaddress and set port as 443

Steps to be followed

- Select #2 Rename the file
- Select #1 Single Mail address
- Select #2 One-Time Use Email Template

References

- Security through Education, www.social-engineer.org
- Penetration Testing Lab, pentestlab.blog
- Offensive Security, www.offensive-security.com