

SOCIAL ENGINEERING

MUHAMMAD SAMAAK

#WHOAMI

Gold medalist in Taekwondo

<https://github.com/Wir3Gh0st>

<https://github.com/OffS3c>

@Wir3Gh0st 

SOCIAL? ENGINEERING



*The Art of manipulating people into
giving up sensitive information
or gaining their trust*

NO Anti-virus No Protection



*The real Vulnerability is our Human Brain
You just need to know how to Exploit it*

Real World Examples





Back in 2013, the Associated Press **Twitter** account was taken over by the Syrian Electronic Army (**SEA**) thought **Phishing**



Within moments, the stock market dropped the Dow Jones Industrial Average dropped **150** points as the tweet was retweeted

Fake News

Its found on Social Media Websites. This Attack Work so well because its claim to show something which everyone wants to see



Learn Social Engineering from **Elliot**



What is Social Engineering Toolkit ?

Basic of Social **Engineering** Toolkit

- Also known as SET
- Open Source
- Purely Python
- SET is written by **David Kennedy**

Download Link: <https://github.com/trustedsec/social-engineer-toolkit>

Already Built in : Kali Linux , BlackBox Linux , Parrot Security etc

Brain of SET

SET by default works **perfect** for most people but there can be situations when you have to modify the **settings** according to the scenario and requirements.

```
root@kali: /etc/setoolkit
File Edit View Search Terminal Help
GNU nano 2.7.4 File: set.config
#####
#####
##
## The following config file will allow you to customize settings within
## the Social-Engineer Toolkit. The lines that do not have comment code
## ("##") are the fields you want to toy with. They are pretty easy to
## understand.
##
## The Metasploit path is the default path for where Metasploit is located.
## Metasploit is required for SET to function properly.
##
## The "ETTERCAP" option specifies if you want to use ARP cache poisoning in
## conjunction with the web attacks; note that ARP cache poisoning is only
## for internal subnets only and does not work against people on the Internet.
##
## The "SENDMAIL" option allows you to spoof source IP addresses utilizing an
## program called Sendmail. Sendmail is not installed by default on Kali.
## To spoof email addresses when performing the mass email attacks, you must
## install Sendmail manually using the command: "apt-get install sendmail"
#
## Note that "ETTERCAP" and "SENDMAIL" options only accept ON or OFF switches.
##
## Note that the "Metasploit_PATH" option cannot have a '/' after the folder name.
##
## There are additional options; read the comments for additional descriptions.
##
## CONFIG_VERSION=7.5
##
#####
#####
```

Config File Pat : /etc/setoolkit/set_config

```
.M" ""bgd `7MM" ""YMM MMP" "MM" "YMM
.MI "Y MM `7 P' MM `7
.MMb. MM d MM
`YMMNq. MMmmMM MM
`MM `MM Y MM
Mb dM MM ,M MM
P"Ybmmd" .JMMmmmmMM .JMML.
```

```
[---] The Social-Engineer Toolkit (SET) [---]
[---] Created by: David Kennedy (ReLlK) [---]
        Version: 7.6.2
        Codename: 'Vault7'
[---] Follow us on Twitter: @TrustedSec [---]
[---] Follow me on Twitter: @HackingDave [---]
[---] Homepage: https://www.trustedsec.com [---]
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.
```

Join us on irc.freenode.net in channel #setoolkit

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: <https://www.trustedsec.com>

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: 7.6.2
Current version: 7.6.3

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> █

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) SMS Spoofing Attack Vector
- 11) Third Party Modules

- 99) Return back to the main menu.

set>

Website Attack Vectors

- 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) Full Screen Attack Method
 - 8) HTA Attack Method
-
- 99) Return to Main Menu

Teensy?

#Teensy

Development Board

Support **Ar**duino IDE

Emulate the Keyboard and Mouse

Bypass Auto run Capability

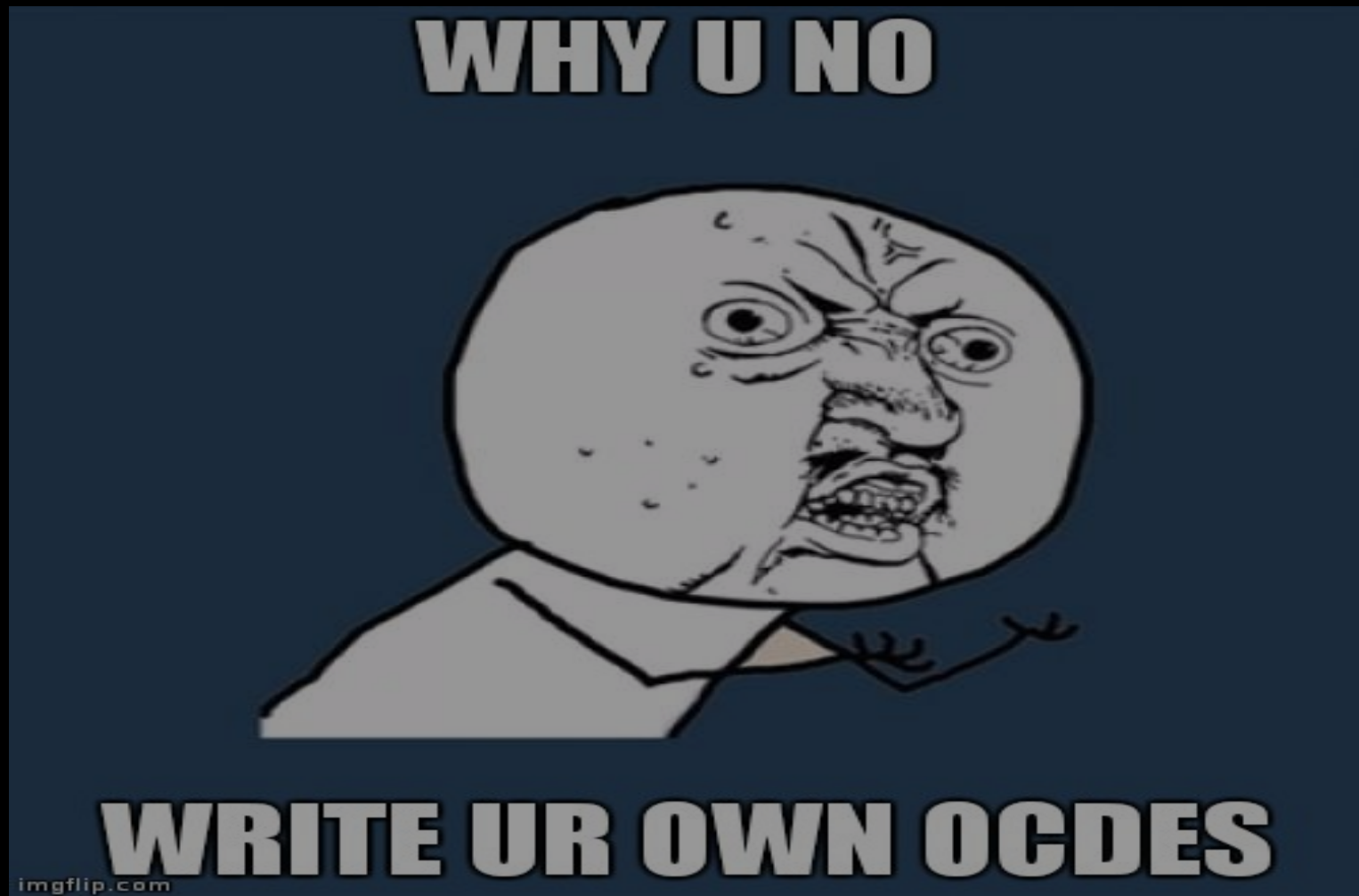
PWNED in 20 seconds

#Arduino-Based Attack Vector

- 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) Teensy Multi Attack Dip Switch + SDCard Attack
- 14) HID Msbuild compile to memory Shellcode Attack

- 99) Return to Main Menu

Seriously ?



DEMO

Developing your own **SET** modules

Basic Structure

```
import src.core.setcore as core
import sys
```

```
MAIN="Demo"
AUTHOR="Samaak"
```

```
#### MAIN ####
```

```
def main():
    core.java_applet_attack("https://gmail.com", "443", "reports/")
    pause=raw_input("This module has finished completing. Press <enter> to continue")
```

Core function calls Example

- `core.grab_ipaddress()`
- `core.check_beautifulsoup()`
- `core.update_set()`
- `core.site_cloner(website,exportpath,)`
- `core.meterpreter_reverse_tcp_exe(port)`
- `core.metasploit_listener_start(payload,port)`
- `core.start_web_server(directory)`
- `core.java_applet_attack(website,port,directory)`

QUESTIONS ?