Social-Engineering in the 21st Century

- Social-Engineering attacks are at an all time high.
- Harder to break in on the external perimeter, adaptation occurs towards our weakest link, the human element.
SET v0.6 – Codename

“Arnold Palmer”
Basics of SET

• Open-Source purely Python driven.

• Integration into Metasploit for both the exploit repository for client-side attacks and payloads.

• Multiple attack vectors specifically designed for Social-Engineering.

• For good, not bad, help pentesters and organizations test their security program.
SET Attack Vectors

- Spear-Phishing – Spoof or utilize already established email addresses to do spear-phishing attacks with fileformat attack vectors.

- Web Attacks – Multiple attack vectors including java applet, client-side exploits, tabnabbing, man left in the middle, and the credential harvester.

- Malicious USB/DVD/CD – Autorun creation, allows you to deploy MSF payloads in a simple autorun.
SET Attack Vectors Cont.

- Arduino / Teensy USB HID Attack Vector – Multiple payload selection for the USB keyboard HID attacks.
SET DEMO

USB HID Attack Vector
USB HID Attack Vector

- Simulates a keyboard being plugged in (not flash)

- Drop a payload onto a system either through PowerShell or WSCRIPT.

- Can also drop executables through similar hex2bin conversion methods.
Integrating into Existing Hardware

- Most new keyboards have integrated USB Hubs.
All put together…

• Keyboard still works perfectly… We have our malicious stuff just sitting there waiting…
SET DEMO
TabNabbing
SET TabNabbing

- User visits site, it states please wait…

- Victim switches to different tab.

- Cloned site is now presented, victim thinks he/she was logged off or forgot about this tab.

- Enter information into post parameters and credentials are harvested.
SET No-DEMO

Man-Left-In-The-Middle
SET MLITM

• Special thanks to Kos for his hard work, it’s his baby, just added to SET.

• Utilizing either a pre-compromised site or XSS, injecting website of SET into the vulnerable site.

• HTTP Referrers are used in order to harvest the credentials off of the site.
SET
Credential Harvester
SET Credential Harvester

- Allows you to clone a website and automatically rewrite the post parameters to allow you to intercept and harvest credentials.

- Redirects victim back to the original site to make it seem less conspicuous.

- Can be used in wide-scale harvesting, reports export in both HTML and XML formats and can be easily used to generate reports.
SET DEMO

Java Applet Attack Vector
Thomas Werth Attack Vector

• Released at ShmooCon, this attack vector allows you to create a malicious Java Applet.

• User hits “run” and the payload is executed on the victims machine.

• Redirects user back to original site to make attack less conspicuous.

• New in SET v0.6, heavy obfuscation of java and payload for A/V bypass and fixed major issues with Linux/OSX payload deployment. Applet source just opened today!
SET DEMO

Spear Phishing
Spear Phishing Attack Vector

- Utilize Sendmail, Gmail, or your own open-mail relay to perform targeted attacks.

- Utilizes fileformat exploits in order to compromise the victim.

- Spoof email addresses to the victim.

- Allow as many email addresses as you want.
SET No-Demo

USB/DVD/CD Infectious Method
USB/DVD/CD Infectious Method

• Simple yet effective, will create a folder in the SET root that automatically creates the autorun.inf and generates a metasploit payload for you.

• Used when deploying CD/DVD’s for social-engineering attacks.

• Still somewhat of a basic attack vector but plans on improvement.
SET v0.6

Improvements from 0.5
SET 0.6 CodeName: “Arnold Palmer”

- Added the new TabNabbing Attack Vector
- Java Applet is now OPEN SOURCE!
- Ability to select either Pythons HTTP server or Apache integration
- Added the new Man Left in the Middle Attack vector
- Added the new Teensy USB HID Attack Vector
- Over 45 bug fixes.
- Added the latest Adobe, LNK, and IE exploits.
- Added Ettercap DNS poison attacks
So why SET?

- Hackers are doing this to us on a regular basis, they are only getting more sophisticated and we aren’t doing squat to fix it.

- SET is aimed at user awareness and security program testing, FIX YOUR HUMANS!

- Making sure the security controls you put in place stop these types of attacks.

- Because contributing to the community in an open-source fashion is great.
Why is it effective?

• We are humans, we are programmed from birth through our lives to act and behave a certain way.

• Our brains all work the same way, we are all vulnerable and there really is no patch.
If you aren’t doing SE as apart of your regular penetration tests you are seriously missing out.

If you don’t know about this, you should learn…

Success ratio’s for compromise with SET are estimated at around 94%.
Learning more about SE

- http://www.social-engineer.org
The SE.org Framework

PART I: GENERAL DISCUSSION
I. Social Engineering Defined
II. Categories of Social Engineers
   A. Hackers
   B. Penetration Testers
   C. Spies or Espionage
   D. Identity Thieves
   E. Disgruntled Employees
   F. Information Brokers
   G. Scam Artists
   H. Executive Recruiters
   I. Sales People
   J. Governments
   K. Everyday People
III. Why Attackers Might Use Social
IV. Typical Goals
V. The Attack Cycle
VI. Common Attacks
   A. Customer Service
   B. Tech Support
   C. Delivery Person
   D. Phone
VII. Real World Examples

PART II: INFORMATION GATHERING
I. How to Gather Information
   A. Research
   B. Dumpster Diving
II. Sources
   A. Traditional
   B. Non-Traditional
III. Communication Models

PART III: ELICITATION
I. Definition
II. Goals
III. Preloading
IV. Becoming a

PRETEXTING DEFINED

Pretexting is defined as the act of creating an invented scenario to persuade a target victim to release information or perform some action. It is more than just creating a lie. In some cases it can be creating a whole new identity and then using that identity to manipulate the receipt of information. Pretexting can also be used to impersonate people in certain jobs and roles that they never themselves take their actions. Pretexting is also a way to create a fake solution. Social engineers will have to develop many different presents over their career. All of them will have one thing in common: research. Good information gather techniques can make or break a good pretext. Being able to mimic the perfect tech-support rep is useless if your target does not use outside support.

PART IV: PRETEXT
I. Definition
II. Principles and Importance of Pretexting
III. Successful

Pretexting is also used in other areas of life other than social engineering. Sales, public speaking, so-called house sales, NLP experts and even doctors, lawyers, therapists and the like all have to use a form of pretexting. They all have to create a scenario where a person is comfortable with releasing information they normally would not.

PART V: PSYCH
I. Definition

REFERENCES

SecMonico.com
The SE.org Podcast

- Main Host: LoganWHD
- Co Host: Muts, Elwood, and ReL1K
How do you fix this issue?

- Put an emphasis on user restrictions and limiting users from hurting themselves. That means tight egress controls, no administrative rights, kernel level process hooks for monitoring and preventing, behavioral analysis, and heavy monitoring.

- Training the users on common attack vectors, your never going to be bulletproof but at least the ability to thwart the majority of them makes you much better than the most.

- Remove all employees from your organization and replace them with robots.
Questions? 😊

http://www.secmaniac.com
davek@social-engineer.org
Twitter: Dave_ReL1K