Social Forensication

A Multidisciplinary Approach to Successful Social Engineering

Joe Gray, CISSP-ISSMP, GSNA, GCIH, OSWP

Hack in Paris 2019

The thoughts and opinions in this presentation do not necessarily reflect those of IBM.

Disclaimer

The thoughts and opinions in this presentation do not necessarily reflect those of IBM.

About Me

- Senior Security Architect
- 2017 DerbyCon Social Engineering Capture the Flag (SECTF) winner
- On 3rd Place Team in NOLACon OSINT CTF (Password Inspection Agency)
- Served in the US Navy, Navigating Submarines
- CISSP-ISSMP, GSNA, GCIH, OSWP
- Forbes Contributor
- Currently Authoring Social Engineering and OSINT Book with No Starch Press
- Maintained blog and podcast at https://advancedpersistentsecurity.net
- Trains (spoken taps out a lot) in Brazilian Jiu Jitsu

- Just started offering OSINT training (OSINT Associates)

DerbyCon VII Black Badge

DerbyCon VII Closing Ceremony

Objectives

- Discuss the basics of Social Engineering
- Discuss existing attacks and techniques in Social Engineering using USB devices
- Explain the Memory Forensics and Rogue Wifi AP and Wireless Hacking Attacks
- For each of the two attacks, provide:
  - The considerations prior to execution
  - Execution of the attack
  - Mitigations for the attack
  - Demonstrations for each attack

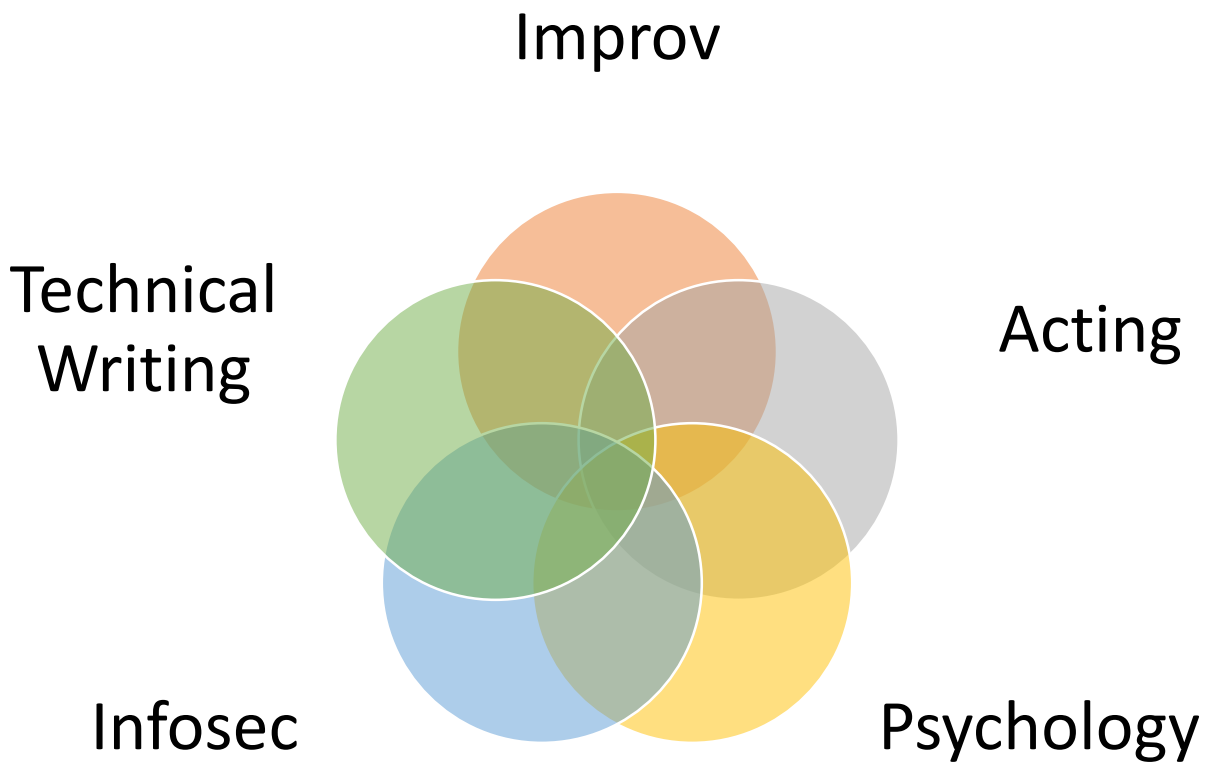
Basics of Social Engineering

- Human Hacking
- Aims to influence the following:
  - Perform an action
  - Provide Information

Types of Social Engineering

- Phishing
- Vishing
- **Physical**
- Dumpster Diving
- Baiting

The Complexity of Social Engineering

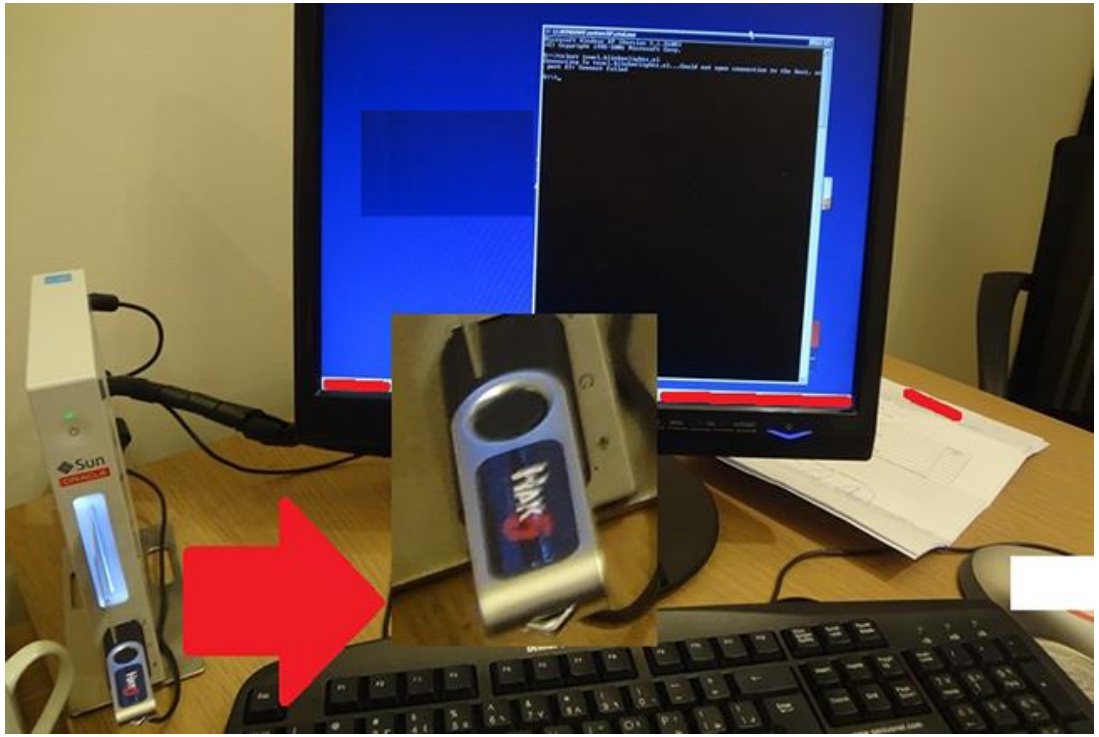


Cialdini's 6 Principles of Persuasion

- Reciprocity
- Commitment & Consistency
- Social Proof
- Liking
- Authority
- Scarcity

Attack #1:

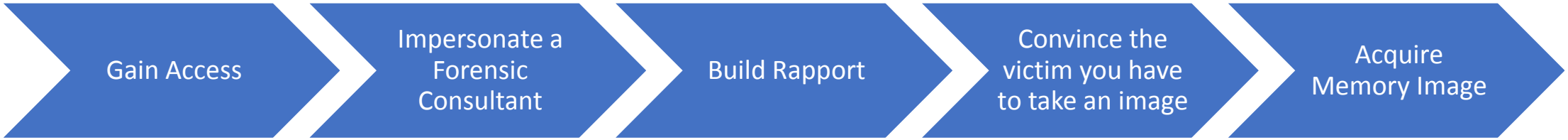
Existing Techniques and Research



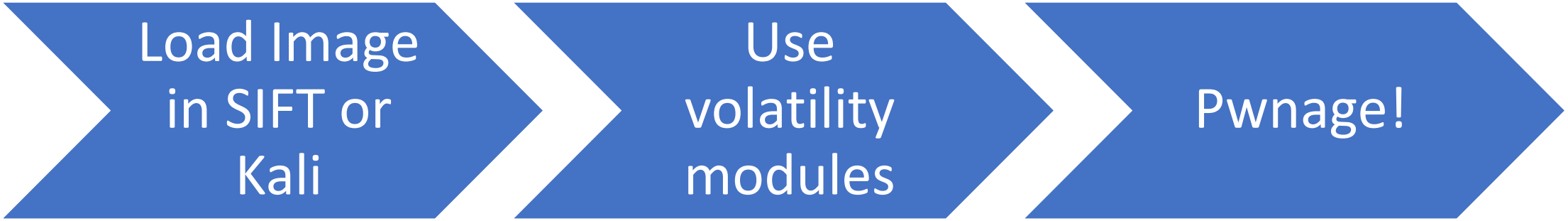
Minimum (paid) tools you'll need

Minimum (free/other) tools you'll need

Process


Gain Access
Impersonate a Forensic Consultant
Build Rapport
Convince the victim you have to take an image
Acquire Memory Image

Pwnage



- More Attacks Later

Process


PHASE 1
PHASE 2
PHASE 3
Collect underpants
?
Profit
I DON'T GET IT.

Gaining Access

- Vista Print
- Quickidcard.com
- Clipboard
- Laptop and Briefcase or backpack (more evil on this later)
- Solid Pretext

The story....

Getting the Image

No DLP

- USB Drive or Ducky
- Powershell Script to Priv Esc or Prompt User
- Run FTK Imager
- Gather Image
- Walk out the door

DLP

- Rubber Ducky
- Ducky Script
- Need Ducky Code
- Need TwinDucky
- PS to Priv Esc or Create Admin User
- Run FTK Imager
- Gather Image
- Make a Break for It

The Attack and Payload

- We need some OSINT
  - Layer 8
  - Windows, Linux, or Mac?
    - Proper Connectors or Dongles
  - DLP?
  - AV/EDR?
  - User rights?
  - InfoSec culture

- Time to collect?

Limitations

- The user
- The user's permissions
  - If they aren't an admin, you may experience complications
- The vulnerability management posture
  - If the user is not an admin, you're going to have to pwn something
- Time
  - The time to collect is roughly 2-2.25 (minutes) * number of GB of RAM
  - Tested on DDR4
    - 2GB: 4:30
    - 12GB: 25:45

Demo

- PowerUp
- Pwn or UAC bypass
- FTK

Using Volatility

- Open Source Memory Forensics tool
- Native to SIFT and Kali
- Initial Variables (to make life easier)
  - Filename
    - Export VOLATILITY_LOCATION=file:///</path>/<filename>
  - Profile
    - Export VOLATILITY_PROFILE=Win10SPxx64

Useful Volatility Modules

- Hashdump
- Mimikatz
- Imageinfo
- Connscan
- Consoles
- Dumpcerts
- Iehostory
- Clipboard
- **Chrome***
- **Firefox***
- Netscan
- Notepad
- Privs
- Screenshot
- Timeliner
- Verinfo
- windows
- Svcscan
- Privs
- Cmdline/cmdscan

Limitations

- The operating system
  - FTK Imager Lite only supports Windows
  - Rekall will work with Mac
  - Linux has Lime
- The operating system
  - Windows 7 is easy to forensicate
  - Windows 10 is more difficult
  - Mac and Linux have plugins but not as robust
- Time

Demo

- Volatility Overview

Rogue Wi-Fi AP

- Why?
- How?

Demo

- Fake AP
- WiFi Pineapple

Through the Hacking Glass

- Mission Statement: To provide free and low cost training resources to enable information security professionals and aspiring professionals to expand their skill sets and marketability to close the skills gap. This is based on the frequent occurrence of a paradigm of employers seeking entry-level people with experience beyond typical formal education curricula. This further allows professionals and those seeking to enter industry the opportunity to gain experience beyond the walls of academic institutions or capture the flags (CTFs).

- Twitter: @hackingglass
- Facebook: facebook.com/hackingglass

Upcoming Speaking Engagements

- 8/9-10: The Diana Initiative (a Defcon Adjacent Conference; Las Vegas, NV)
- 10/10-11: HackerHalted (Atlanta, GA)
- 10/12: Texas Cyber Summit (San Antonio, TX)
- 10/22: Wild West Hackin Fest

Hacker Halted 2019

- October 10-11
- Atlanta, GA USA
- Free Admission
  - Coupon Code: Joe100
    or https://hackerhalted2019.eventbrite.com?discount=Joe100
- Discount on Training
  - Coupon Code: JJHHTRN (15% off training)
- Register at: - https://hackerhalted2019.eventbrite.com
- Winn will be there, come heckle him

Questions?

@C_3PJoe / @advpersistsec / @hackingglass / @OSINTAssociates

AdvancedPersistentSecurity.net

osint.associates

The thoughts and opinions in this presentation do not necessarily reflect those of IBM.

Links

- Privilege Escalation
  - https://github.com/pentestmonkey/windows-privesc-check
  - https://github.com/FuzzySecurity/PowerShell-Suite
    - Bypass UAC
      - Various methods including Matt Graeber's PSReflect
  - https://github.com/GDSSecurity/Windows-Exploit-Suggester
  - https://github.com/0xbadjuju/Tokenvator/wiki/Token-Privileges
  - https://github.com/rasta-mouse/Watson
  - https://github.com/AlessandroZ/BeRoot

More Links

- https://github.com/jocephus/social-forensication
- Hak5 Products Script Repos
  - Rubber Ducky
  - Bash Bunny
  - WiFi Pineapple
- DuckyGenerator


LOONEY TUNES