

# **SRI SANKANRS DEGREE COLLEGE KURNOOL**

Y Prathibha

**Long term internship**

Foot printing and reconnassiance

# **SOCIAL ENGINEERING AND PHISHING ATTACKS**

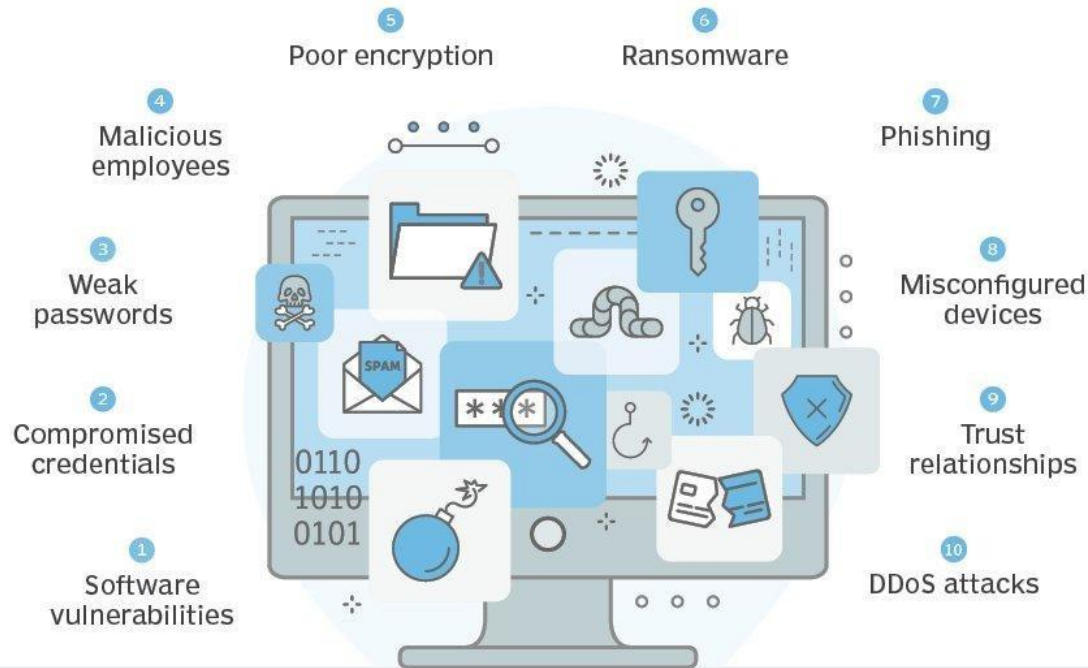
**Case study analysis**

# Case study analysis

- ▣ Social engineering is an attack vector that relies heavily on human interaction and often involves manipulating people into breaking normal security procedures and best practices to gain unauthorized access to systems, networks or physical locations or for financial gain.
- ▣ Threat actors use social engineering techniques to conceal their true identities and motives, presenting themselves as trusted individuals or information sources.
- ▣ The objective is to influence, manipulate or trick users into releasing sensitive information or access within an organization. Many social engineering exploits rely on people's willingness to be helpful or fear of punishment. For example, the attacker might pretend to be a co-worker who has some kind of urgent problem that requires access to additional network resources.
- ▣ Social engineering is a popular tactic among attackers because it is often easier to exploit people than it is to find a network or software vulnerability.
- ▣ Hackers will often use social engineering tactics as a first step in a larger campaign to infiltrate a system or network and steal sensitive data or disperse malware

# Social engineering 10 types common attack

## 10 common attack vectors



# Consequences of cyber attacks

## financial loss and customer trust

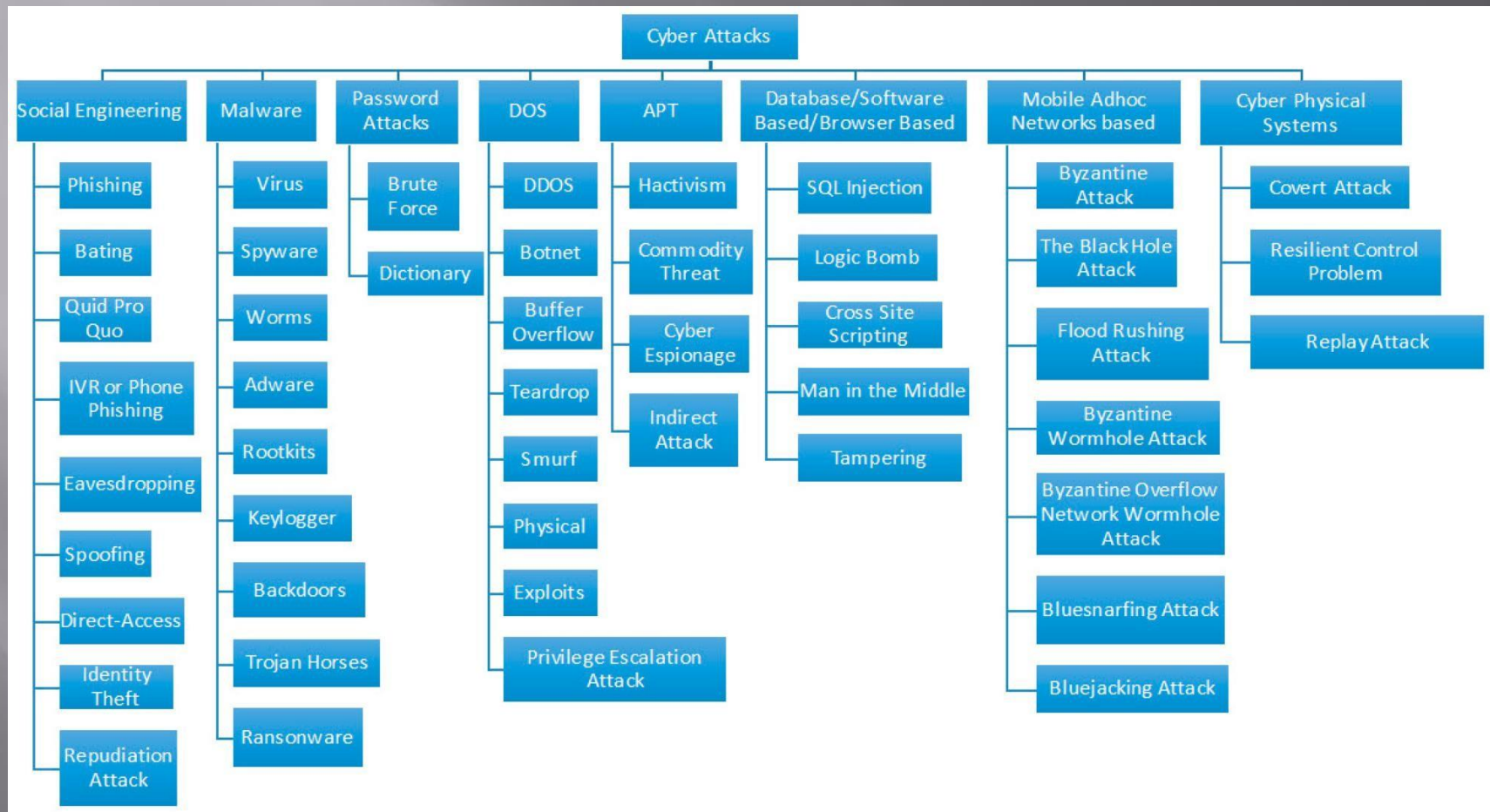
- ▣ Absolutely, discussing the consequences of a cyberattack on an organization's reputation, financial losses, and customer trust is crucial, as these aspects are often the most significant and long-lasting impacts of such incidents.
- ▣ **Reputation Damage:** A cyberattack can inflict severe damage to an organization's reputation. The public perception of the organization may shift from one of trust and reliability to skepticism and distrust. This can be particularly damaging for businesses that handle sensitive customer data, as customers may question the organization's ability to safeguard their information. Moreover, negative media coverage and public scrutiny can further tarnish the organization's image, making it challenging to regain trust and credibility in the eyes of customers, partners, and stakeholders.
- ▣ **Financial Losses:** The financial implications of a cyberattack can be staggering. Beyond the immediate costs associated with mitigating the attack, such as incident response, forensic investigations, and system repairs, there are often indirect financial losses that can be even more significant. These may include loss of revenue due to downtime or disrupted operations, regulatory fines and legal fees, increased insurance premiums, and decreased market value of the organization's stock. Furthermore, the long-term impact on profitability can be substantial if customers choose to take their business elsewhere due to concerns about security and reliability.
- ▣ **Customer Trust:** Perhaps one of the most critical consequences of a cyberattack is the erosion of customer trust. When customers entrust their sensitive information to an organization, they expect it to be handled with care and confidentiality



# Role-play Exercise and social engineering examples

- In no particular order, here are nine common cyber threats that leverage social engineering tactics to gain access to sensitive information. While most of these attacks occur online, several can rear their heads in physical spaces like offices, apartment buildings, and cafes.
- 1. Phishing :
- The most pervasive way of implementing social engineering, hackers will use deceptive emails, websites, and text messages to steal sensitive personal or organizational information from unsuspecting victims.
- Despite how well-known phishing email techniques are, [1 in 5 employees](#) still click on those suspicious links
- 2. Spear Phishing :
- This email scam is used to carry out targeted attacks against individuals or businesses. [Spear phishing](#) is more intricate than your average mass phishing email, as it requires in-depth research on potential targets and their organizations
- 3. Baiting :
- This type of attack can be perpetrated online or in a physical environment. The cyber criminal usually promises the victim a reward in return for sensitive information or knowledge of its whereabouts.
- 4. Malware :
- A category of attacks that includes ransomware, victims are sent an urgently worded message and tricked into installing [malware](#) on their device(s).
- Ironically, a popular tactic is telling the victim that malware has already been installed on their computer and that the sender will remove the software if they pay a fee.
- 5. Pretexting :
- This attack involves the perpetrator assuming a false identity to trick victims into giving up information. Pretexting is often leveraged against organizations with an abundance of client data, like banks, credit card providers, and utility companies.

# Cyber attacks for hanking tools for maitaince for them



# Email phishing attack and analysis

- ▣ A phishing email is a cyber attack that relies on deception to steal confidential information from users and organizations.
- ▣ Phishing victims are tricked into disclosing information that should be kept private. When a phishing email arrives, recipients have no reason to doubt the request.
- ▣ They believe that the party requesting the information – often posing as a familiar platform, a trusted vendor, colleague, or boss – is who they say they are. With the best intentions, phishing email victims respond without a second thought.  
In phishing emails, cyber criminals often ask for the following information:
  - ▣ Date of birth
  - ▣ Social security number
  - ▣ Phone number
  - ▣ Home address
  - ▣ Credit card details
  - ▣ Login details
  - ▣ Password (or other information needed to reset your password)
- ▣ Cyber criminals then use this information to impersonate you and apply for credit cards or loans, open bank accounts, and commit other fraudulent acts.
- ▣ Some cyber criminals use the information collected in an initial phishing email to launch more targeted cyber attacks, such as spear phishing or business email compromises (BEC), that rely on



# Social tool kit and server phishing attack

```
Shell No. 1
File Actions Edit View Help
[—] Created by: David Kennedy (ReL1K) [—]
      Version: 8.0.3
      Codename: 'Maverick'
[—] 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.

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!

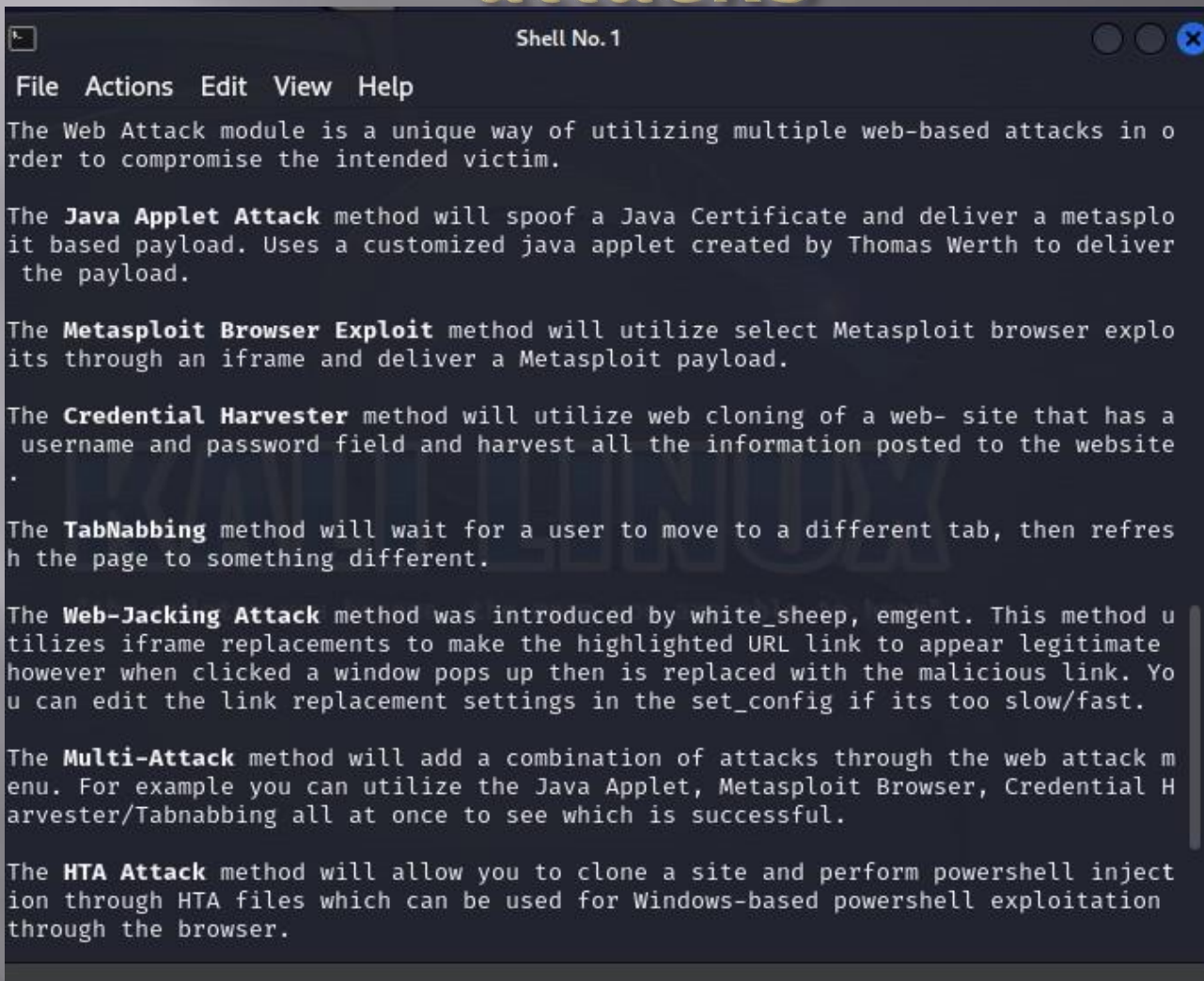
Select from the menu: become, the more you are able to hear*

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> 
```

# Steps for analysis for web attacks



```
File Actions Edit View Help

The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.

The Java Applet Attack method will spoof a Java Certificate and deliver a metasploit based payload. Uses a customized java applet created by Thomas Werth to deliver the payload.

The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.

The Credential Harvester method will utilize web cloning of a website that has a username and password field and harvest all the information posted to the website.

The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_config if it's too slow/fast.

The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation through the browser.
```

# Clone web attacks for fake phishing attacks google sign in

```
Shell No. 1
File Actions Edit View Help

The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.

The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

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

99) Return to Webattack Menu
    "the quieter you become, the more you are able to hear"
set:webattack>1
[-] Credential harvester will allow you to utilize the clone capabilities within S
ET
[-] to harvest credentials or parameters from a website as well as place them into
a report

— * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * —

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
```