**Social Engineering**

**What is Social Engineering?**

Social engineering is the art of convincing people to reveal confidential information.

**Factors that make companies vulnerable to attacks:**

1. Insufficient security training
2. Unregulated access to information
3. Several organization units
4. Lack of security policies

**Why is Social Engineering effective?**

1. Weakest link is human behavior
2. Difficult to detect
3. No method can guarantee of security from it
4. No specific software or hardware to defend specifically against them

**Phases of a Social Engineering Attack:**

1. Research the target company
2. Select a target
3. Develop a relationship
4. Exploit the relationship

**Types of social engineering:**

Social engineering refers to manipulating people into divulging sensitive information or performing actions that compromise security. Here’s a summary of common types:

1. **Phishing**: Fraudulent emails or websites that trick individuals into revealing personal info.
2. **Spear Phishing**: Targeted phishing attacks aimed at specific individuals or organizations.
3. **Vishing**: Phone-based scams, often impersonating legitimate organizations to steal information.
4. **Baiting**: Offering something enticing (like free software) to lure victims into compromising security.
5. **Pretexting**: Creating a fake scenario to obtain sensitive information, often by impersonating someone with authority.
6. **Quizzes/Surveys**: Fake quizzes or surveys designed to collect personal information.
7. **Tailgating**: Following an authorized person into a secure area without proper access.
8. **Impersonation**: Pretending to be someone else to gain access to systems or resources.
9. **Watering Hole Attack**: Compromising a trusted website frequented by a target group to spread malware.
10. **Business Email Compromise (BEC)**: Impersonating executives to trick employees into making financial transactions.
11. **Social Media Manipulation**: Using social media to gather info or influence individuals into providing access or data.
12. **Scareware**: Fake warnings about system infections designed to install malicious software.
13. **Man-in-the-Middle (MitM)**: Intercepting communications between two parties to steal data.
14. **Credential Stuffing**: Using stolen usernames and passwords to access multiple accounts.
15. **Dumpster Diving**: Searching through trash for discarded sensitive documents.

These tactics exploit human psychology, using trust, fear, greed, or urgency to manipulate victims into compromising security.

**Human-based Social Engineering:**

**Impersonation:**

Pretending to be someone else to gain access to systems or resources.

Examples:

1. Posing as a Legitimate end user
2. Posing as an important user
3. Posing as a technical support agent

**Impersonation (Vishing):**

Phone-based scams, often impersonating legitimate organizations to steal information.

Examples:

1. Abusing the Over-Helpfulness of Help Desks
2. Third-party authorization
3. Tech support

**Reverse Social Engineering:**

The attacker presents him/herself as an authority and the target seeks his or her advice before or after offering the information that the attacker needs.

**Piggybacking:**

The authorized person intentionally or unintentionally allows an unauthorized person to pass through a secure door.

**Tailgating:**

Following an authorized person into a secure area without proper access

**Diversion Theft**:

Diversion theft involves deceiving a company or individual into redirecting goods, money, or assets to a different location or person, often through fraudulent orders or fake identities, leading to theft.

**Computer-based Social Engineering: Phishing**

It is the practice of sending an illegitimate email claiming to be from a legitimate site in an attempt to acquire a user’s personal or account information.

**Types of phishing:**

1. **Spear phishing:**  A targeted phishing attack aimed at specific individuals within an organisation
2. **Whaling:** High profiles executives are targeted like CEOs, CFOs, politicians etc.
3. **Pharming:** The attacker redirects web traffic to a fraudulent website by installing a malicious program on a personal computer or server.
4. **Spimming:** A variant of spam that exploits instant messaging to flood spam across the networks

**Insider Threats/Insider Attacks:**

Inside threats or insider attacks occur when employees, contractors, or trusted individuals exploit their access to company systems or data to steal information, cause harm, or sabotage operations, often for personal gain.

Reasons for such attacks:

1. Financial gain
2. Revenge
3. Helping a competitor
4. Public announcement
5. Theft of confidential data

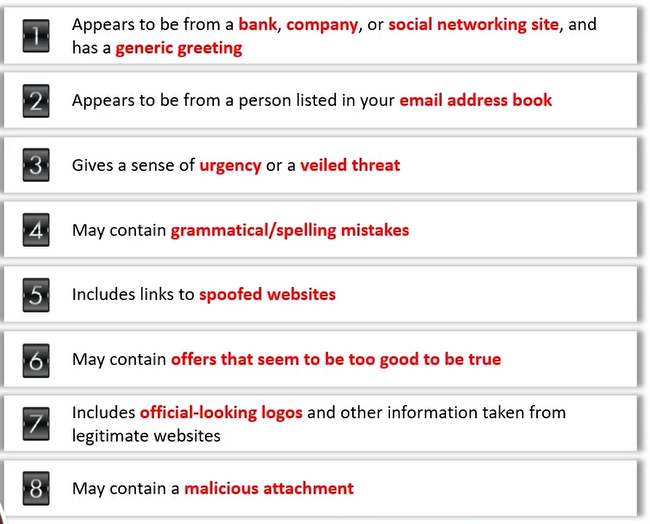
**Types of Insider Threats:**

1. **Malicious Insider**:  
   A malicious insider intentionally misuses their access to steal data, disrupt operations, or harm the organization. This type of insider often seeks personal gain or revenge, causing significant damage.
2. **Negligent Insider**:  
   A negligent insider causes harm by failing to follow security protocols or best practices, often due to carelessness or lack of awareness. This can lead to data breaches or accidental exposure of sensitive information.
3. **Professional Insider**:  
   A professional insider uses their skills and knowledge to exploit access to confidential information, often for financial gain or to assist external parties. They are highly skilled, posing serious security risks.
4. **Compromised Insider**:  
   A compromised insider unknowingly or unwillingly becomes an attacker’s pawn, usually through phishing or malware. Their legitimate access is exploited by external threats to carry out malicious activities.
5. **Accidental Insider**:  
   An accidental insider unintentionally causes a security breach, such as sending sensitive data to the wrong recipient or losing a device. Their actions are not malicious but still result in security vulnerabilities.

**Identity Theft:**

It is a crime in which an imposter steals your personally identifiable information such as name, credit card number, social security etc. to commit fraud or other crimes.

**How to detect Phishing emails?**

****

**Anti-phishing Toolbar:**

1. Netcraft
2. Phish Tank

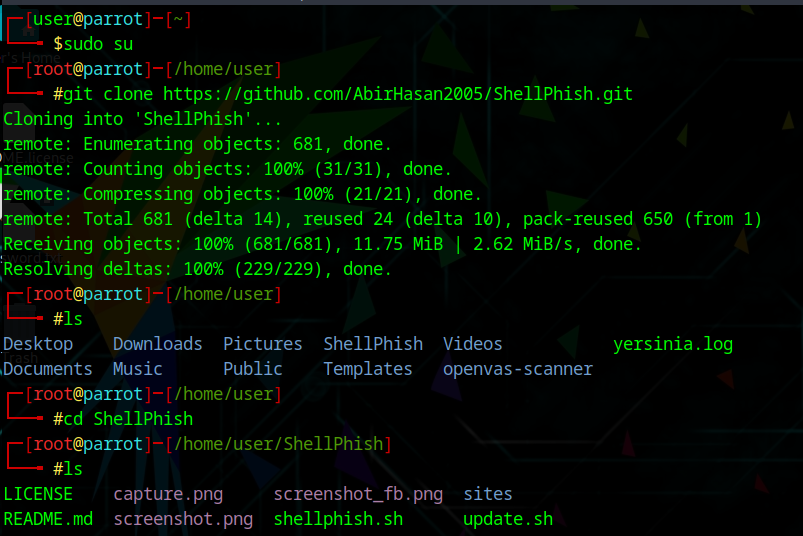
**Social Engineering Tools: Social Engineering Toolkit (SET)**

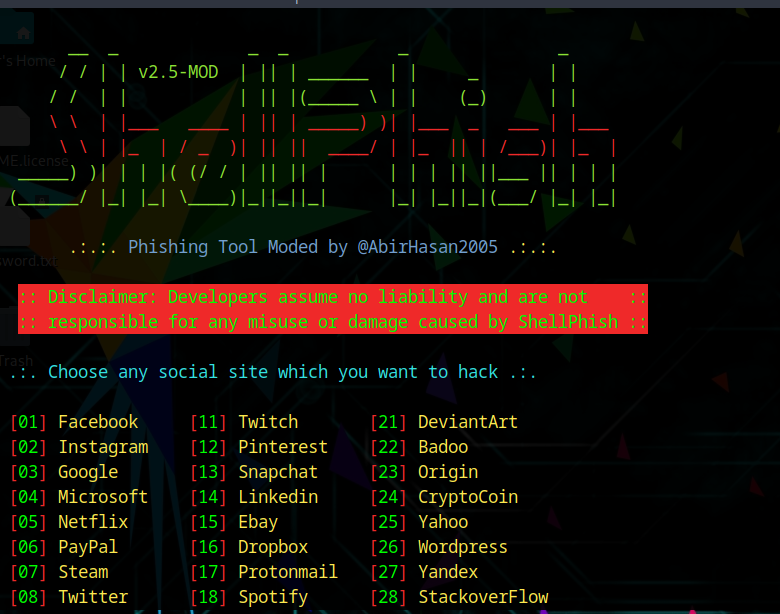
It is an open-source Python-driven tool aimed at penetration testing around social engineering

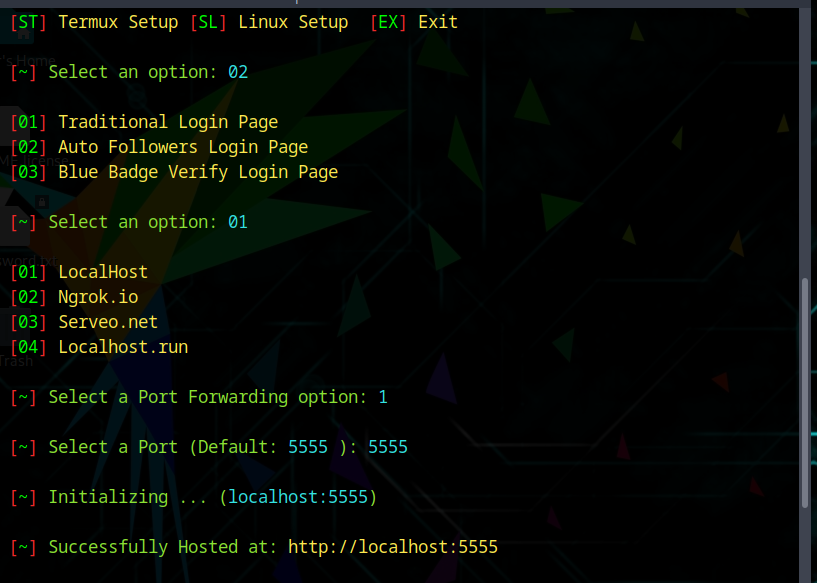
Other tools are:

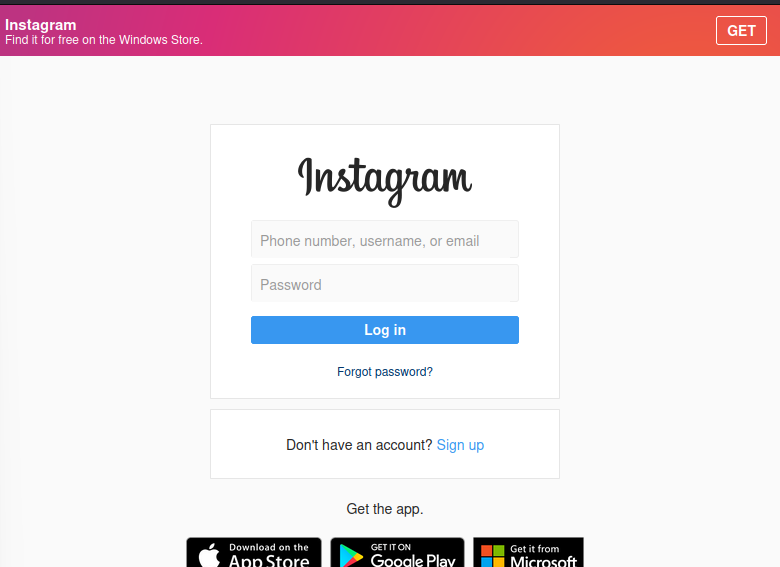
1. Gophish
2. King phisher
3. SpeedPhish Framework
4. MSI simple Phish
5. ShellPhish

**ShellPhish tool:**









**Anti-phishing toolbar:**

