Lecture : Social Engineering

BKACAD's Security Training

Table of Content

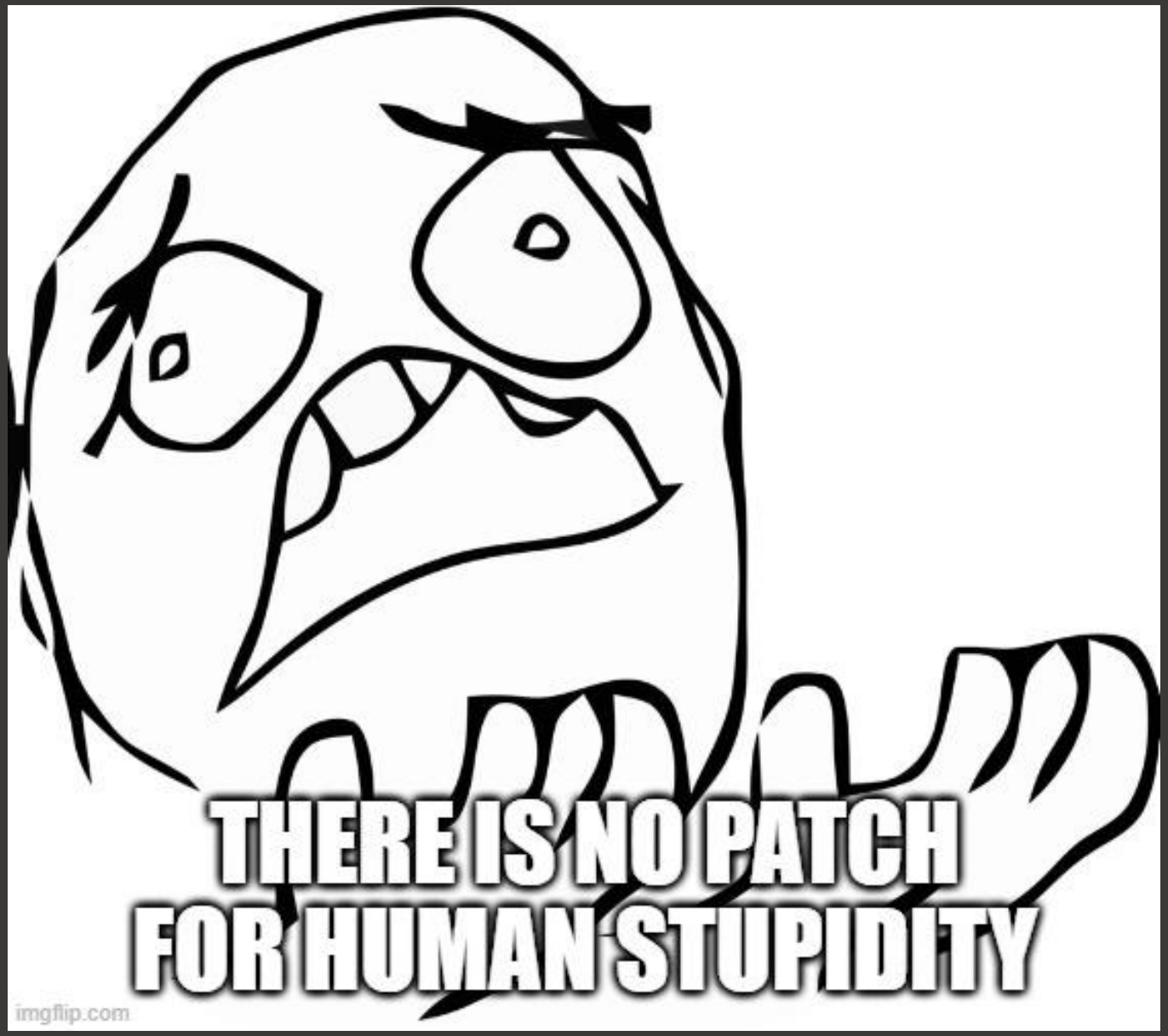

THERE IS NO PATCH
FOR HUMAN STUPIDITY
imgflip.com

Table of Content

Social Engineering

Concept

Is the art of convincing people to reveal confidential information.

Targets: Help desk personnel, technical supporters, admins,…

Depend on the fact that people are unaware of their valuable information and careless about protecting it

Social Engineering

Impact

Economic Losses

Damage to Goodwill

Loss of Privacy

Dangers of Terrorism

Lawsuits and Arbitration

Temporary or Permanent Closure

Social Engineering

Factors that make companies vulnerable to attacks

Insufficient Security Training

Unregulated Access to the Information

Several Organizational Unit

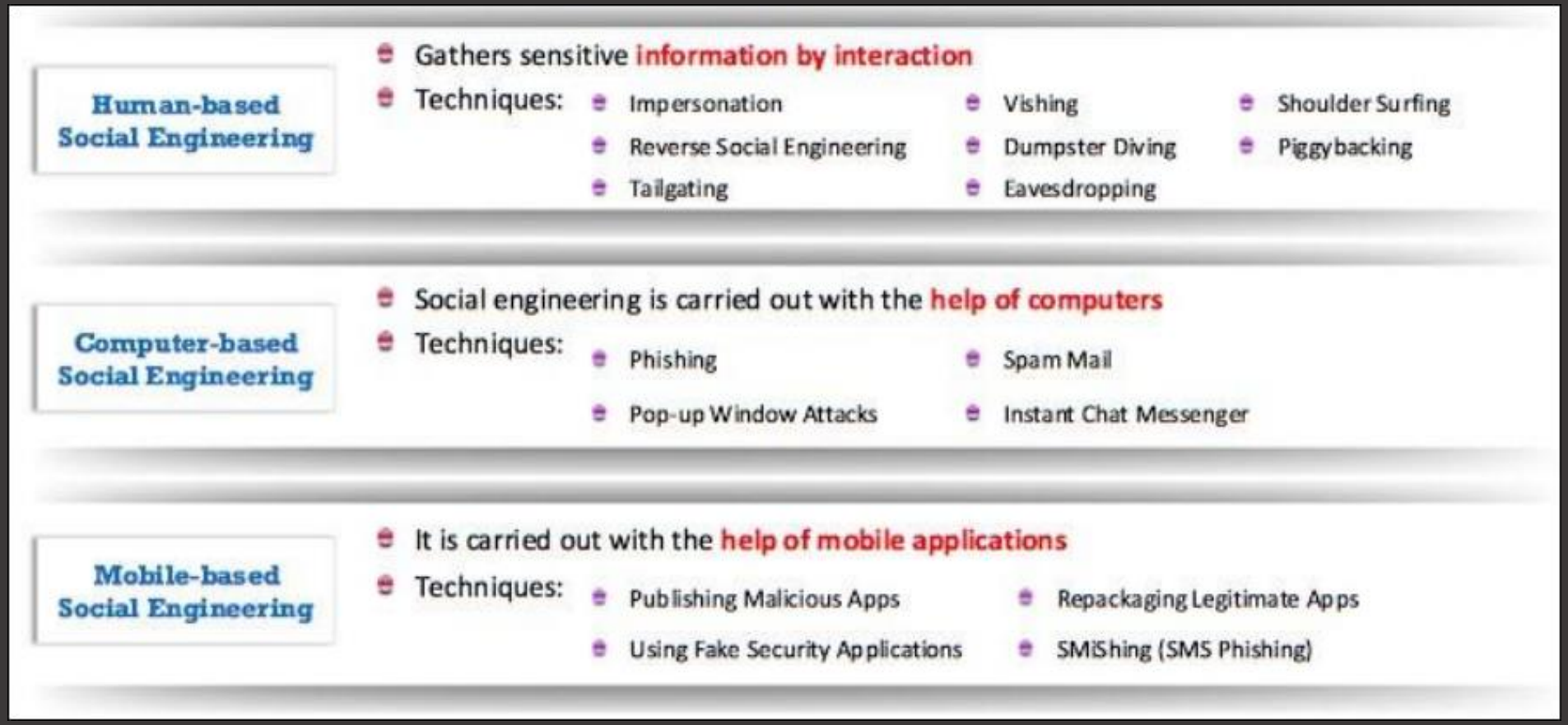
Lack of Security Policies

Table of Content

Phases of SE Attack

Table of Content

Types of SE Attack



Types of SE Attack

Human-based: Impersonation

The attacker pretends to be someone legitimate or an authorized person

Help attacker tricking a target to reveal sensitive information

Types of SE Attack

Human-based: Vishing

Is an impersonation technique in which attacker tricks individuals to reveal person and financial information using voice technology like: VoIP, Telephone system,…

Types of SE Attack

Human-based: Eavesdropping

Unauthorized listening of conversations or reading messages

Interception of audio, video or written communication

Can be done using communication channels such as telephone lines, email, etc…

Types of SE Attack

Human-based: Shoulder Surfing

Using direct Observation techniques such as looking over someone's shoulder to get PIN code, passwords,…

Also be done from a longer distance with using vision enhancing devices

Types of SE Attack

Human-based: Dumpster Diving

Looking for treasure in someone else's trash

Types of SE Attack

Human-based: Reverse Social Engineering

When attacker presents himself as an authority and the target seek her/him advice after or before offering the information that attacker need

Types of SE Attack

Human-based: Piggybacking

“I forgot my ID badge at home. Please help me!”

An authorized person allows an unauthorized person to pass through a secure door

Types of SE Attack

Human-based: Tailgating

An unauthorized person wearing fake ID badge enter secure area by closely following authorized person through a secure door requiring access keys

Types of SE Attack

Computer-based: Pop-up Windows

Automatically pop up while user surfing the internet and ask for user's information like passwords

Types of SE Attack

Computer-based: Hoax Letter

Email that issue warnings a non-existent computer virus in network company.

Lead to loss of time and productivity

Types of SE Attack

Computer-based: Hoax Letter

Email that issue warnings a non-existent computer virus in network company.

Lead to loss of time and productivity

Types of SE Attack

Computer-based: Chain Letter

Email that offer free-gift and the condition that user has to forward the email for friends

Types of SE Attack

Computer-based: Instant Chat Messenger

Gathering information by chatting with gathering information such as: birthday, maiden names,…

Types of SE Attack

Computer-based: Spam Email

Unwanted email to collect financial information, social security number, network information,…

Types of SE Attack

Computer-based: Phishing

Is technique in which an attacker send an email or provide a link that acquire a user's personal or account information.

Types of SE Attack

Computer-based: Phishing

Types:

- Spear Phishing: Targeted phishing attack aimed at specific person or group in orgs
- Whaling: Target high profile like – CEO, CFO,…
- Pharming: Redirect web Traffic using DNS cache poison or host file modification

Types of SE Attack

Mobile-based: SMiShing

SMS + Phishing

Types of SE Attack

Mobile-based: Other attacks

Fake Security Application

Publishing Malicious Apps

Repackaging Legitimate Apps

=> Will be presented in Lecture: Android Security

Types of SE Attack

Exercise

1. At Kali machine, Fake Facebook site with tool named SET

Hint: `setoolkit`

Table of Content

Table of Content

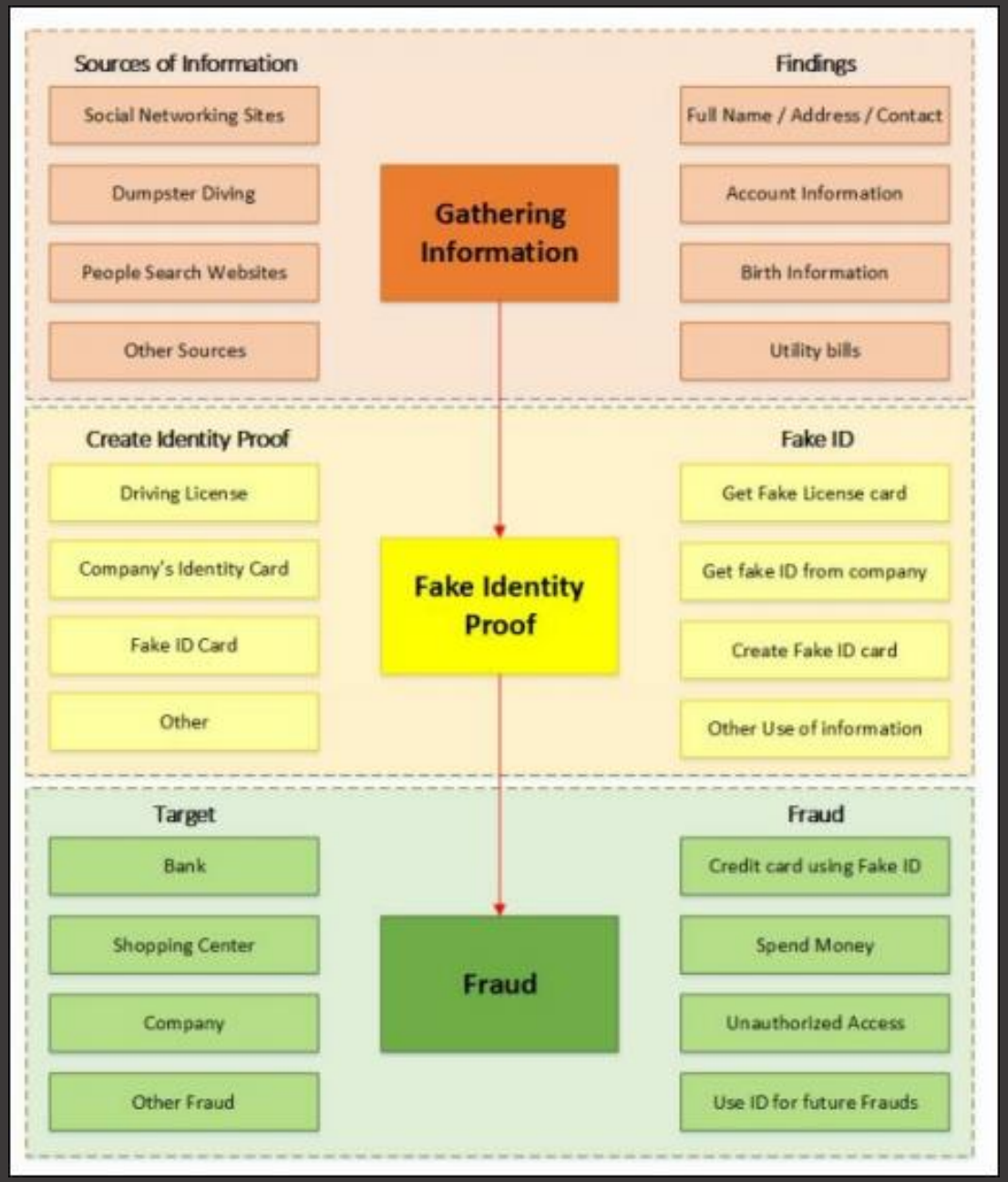

Sources of Information
Social Networking Sites
Dumpster Diving
People Search Websites
Other Sources
Gathering Information
Findings
Full Name / Address / Contact
Account Information
Birth Information
Utility bills
Create Identity Proof
Driving License
Company's Identity Card
Fake ID Card
Other
Fake Identity Proof
Fake ID
Get Fake License card
Get fake ID from company
Create Fake ID card
Other Use of information
Target
Bank
Shopping Center
Company
Other Fraud
Fraud
Fraud
Credit card using Fake ID
Spend Money
Unauthorized Access
Use ID for future Frauds

Table of Content

Countermeasure

Solutions

Training awareness

Monitoring + logging

Physical Security

Privacy & Policy in corporate