SNS COLLEGE OF ENGINEERING

Coimbatore-35
An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A+' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF CSE (IoT & Cyber Security including Blockchain Technology)

19SB502 – CYBER FORENSIC AND INVESTIGATIONS

III YEAR/ V SEMESTER

UNIT 5 - ETHICAL HACKING IN WEB

TOPIC 1 – Social Engineering

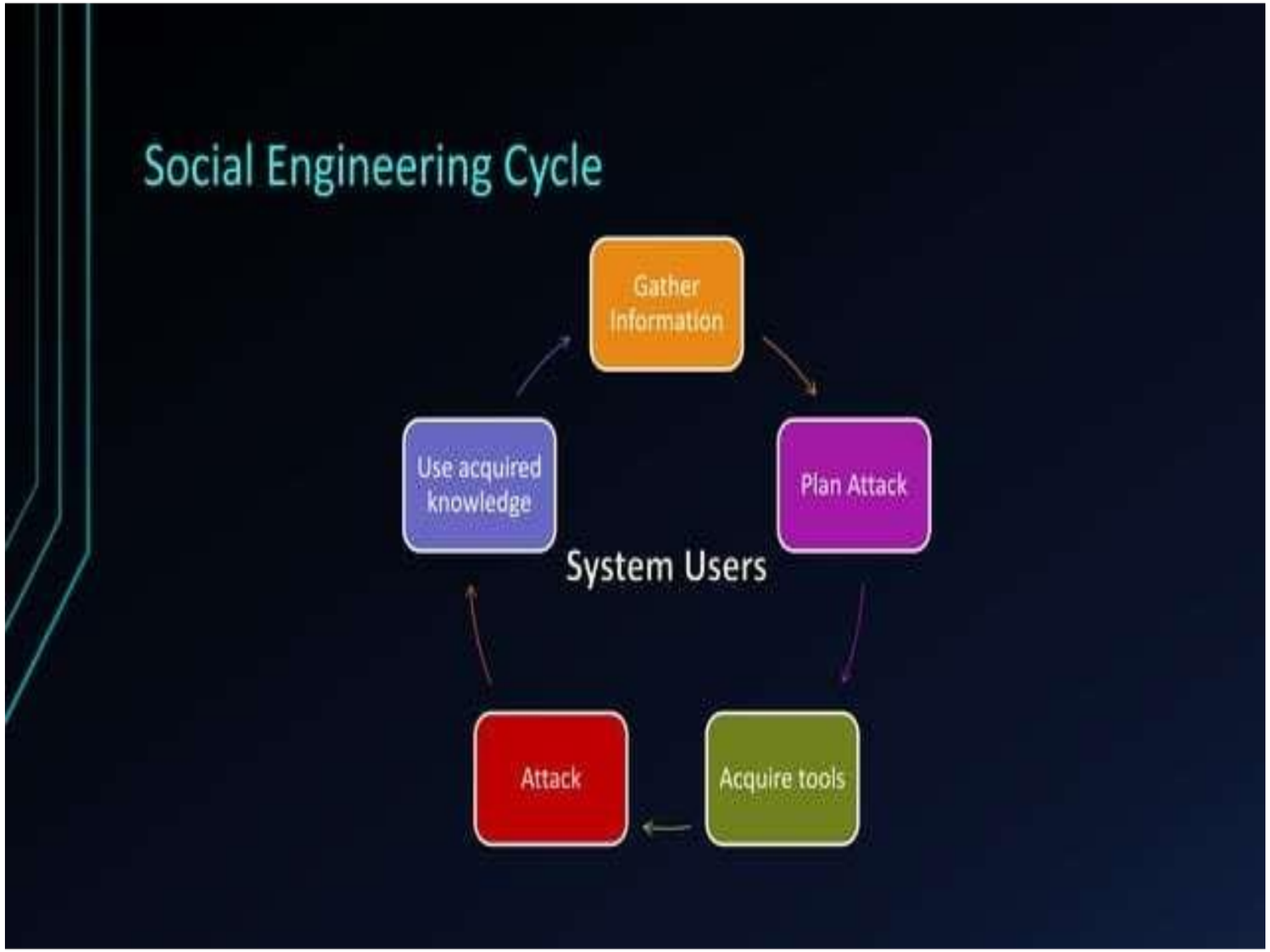

Social Engineering
In a security context, Social Engineering can be defined as:
A combination of social, psychological and information gathering techniques that are used to manipulate people for nefarious purposes.
It target humans rather then technology to exploit weakness in an organizations security.

Social Engineering

- Is the art of manipulating people so they give up confidential information
- Attacker uses human interaction to obtain or compromises information
- Tricking people to get information
- Most common type of SE happens over the phone

Kevin Mitnick - Famous Social Engineer

"People are generally helpful, especially to someone who is nice, knowledgeable or insister."


Social Engineering Cycle
Gather Information
Plan Attack
Acquire tools
Attack
Use acquired knowledge
System Users

Techniques of Social Engineering

- Pretexting
- Phishing
- Vishing
- Baiting
- Quid pro quo
- Diversion Theft

Pretexting

- Creating fake or invented scenario

Phishing

- Obtaining information through email, websites
- Websites like http://shadowave.co

From: Kristi Payne <Kristi.Payne@usw.salvationarmy.org>
To:
Cc:
Subject: System Administrator

Your password will expire in 3 Days Click Here to validate your e-mail.

Thanks
System Administrator

Phishing Example

Sending fake mail to victim

Spear Phishing

- More specific to the victim
- Target individual

Vishing

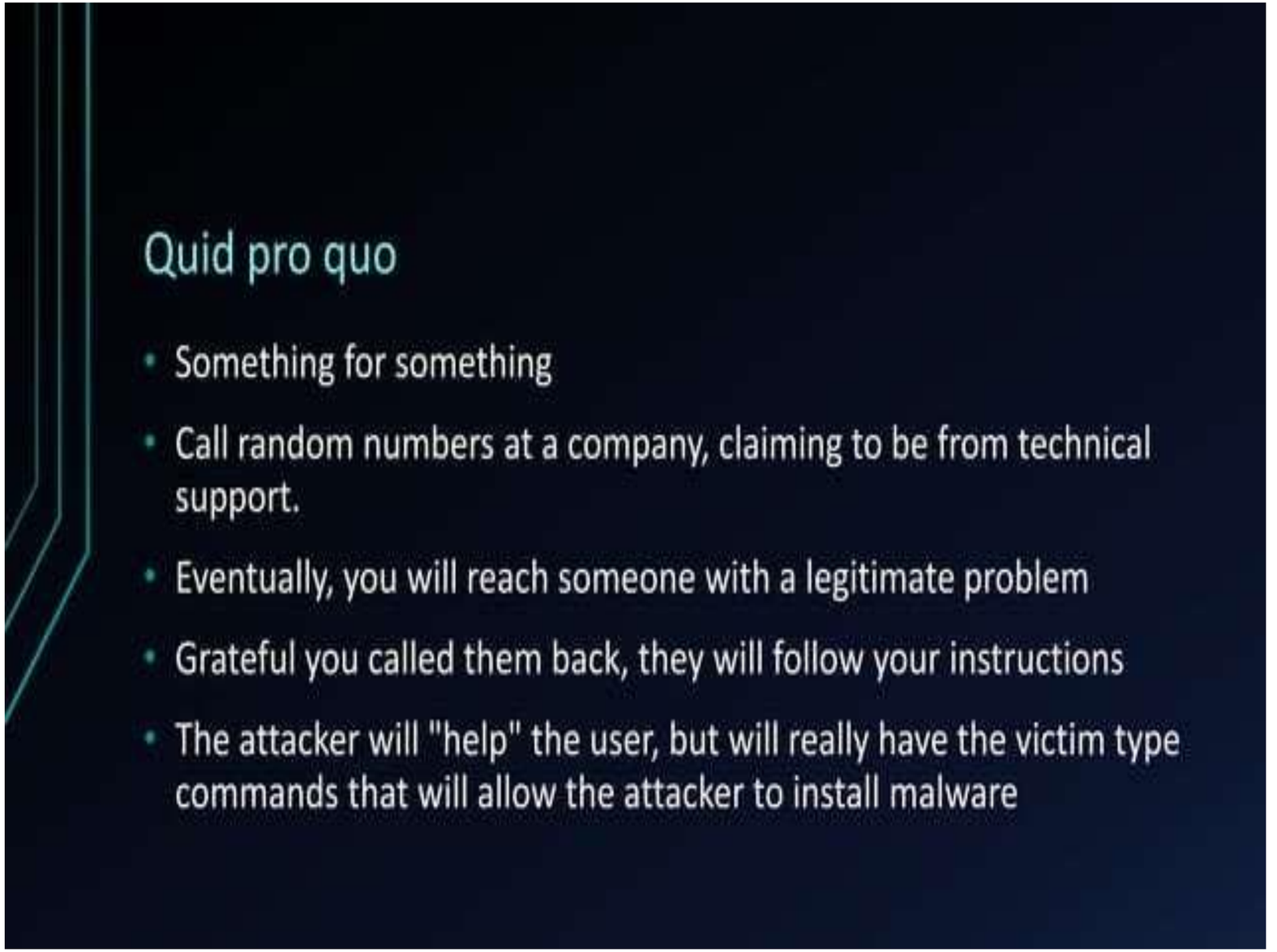
- Phone Phishing

Baiting

- Using Trojan Horse that uses physical media and relies on the greed of the victim

Web Click Baiting

- Something on Internet makes you to click


Quid pro quo
Something for something
Call random numbers at a company, claiming to be from technical support.
Eventually, you will reach someone with a legitimate problem
Grateful you called them back, they will follow your instructions
The attacker will "help" the user, but will really have the victim type commands that will allow the attacker to install malware

Diversion Theft

- Divert actual delivery location to some other place and theft information.

Weakest Link?

- No matter how strong your:

1. Firewalls
2. Intrusion Detection System
3. Cryptography
4. Antivirus software

- We are the weakest link in computer security !
- People are more vulnerable than computers

General Safety / Prevention

- Before transmitting personal information over the internet, check the connection is secure and check the URL is correct
- If unsure email message is legitimate, contact the person or company by another means to verify
- Be aware of excited content on the Internet.
- Making policies to verify different source rather than single source.

THANK YOU