CYBER SECURITY

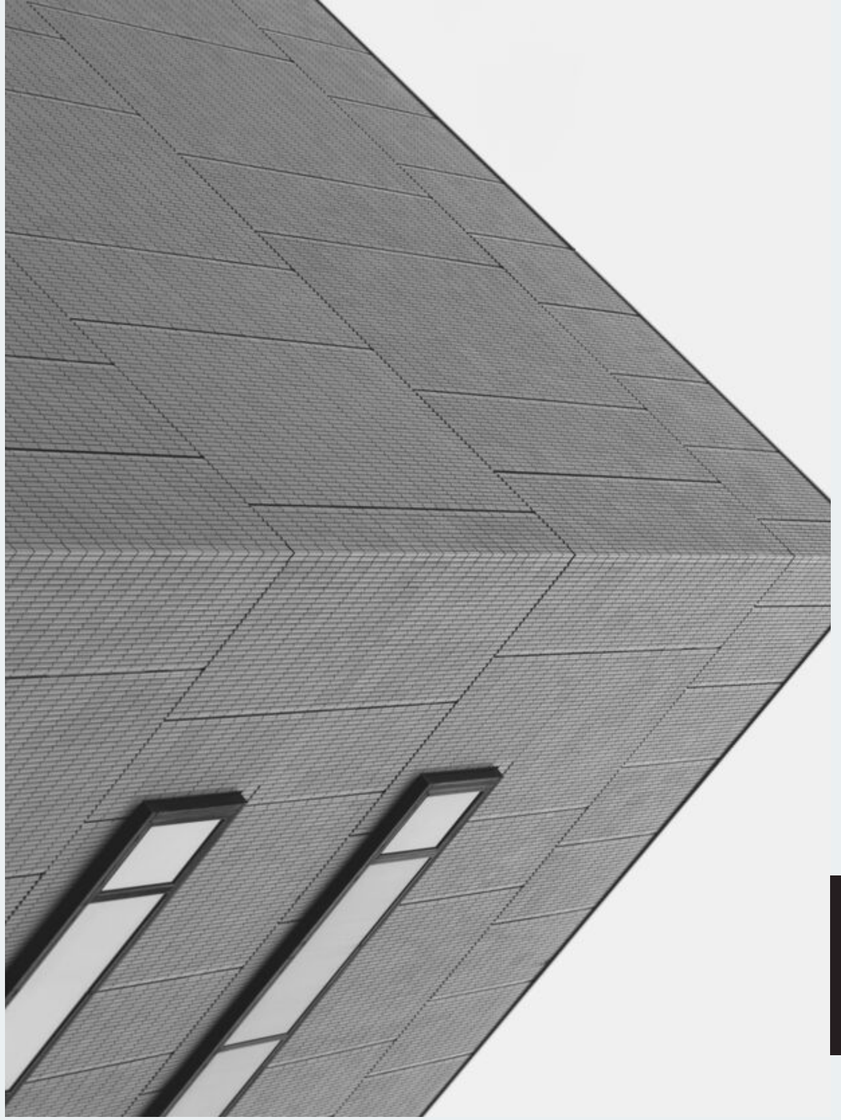
Introduction to Cyber Security :the hacking concept

Presented by judy Ngurel

AkiraChix
SHE BUILDS • SHE SERVES • SHE LEADS

Cyber Security

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks.



RED TEAMING

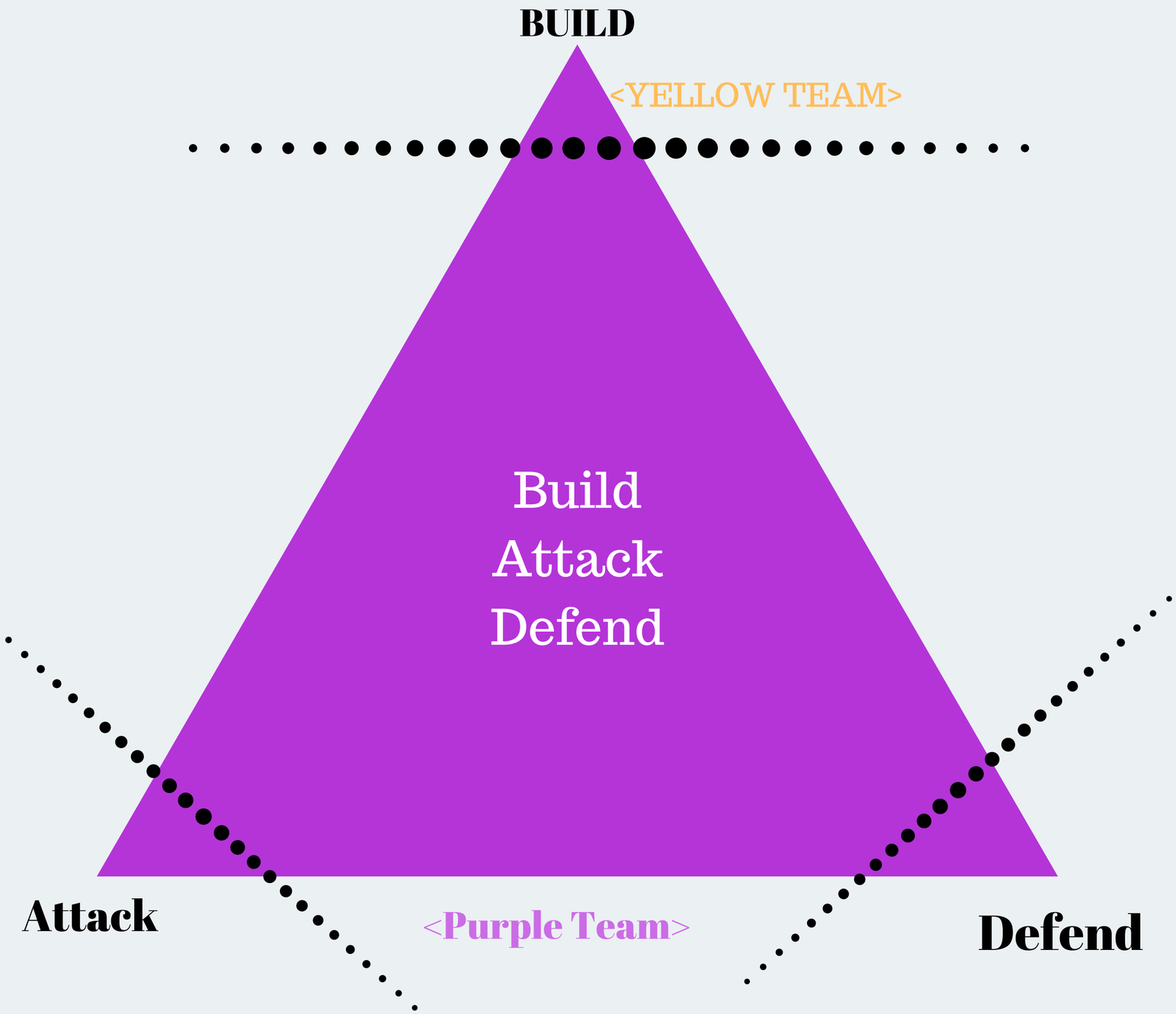
is the practice of rigorously challenging plans, policies, systems and assumptions by adopting an adversarial approach

BLUE TEAMING

refer to the internal security team that defends against both real attackers and Red Teams

PURPLE TEAMING

exist to ensure and maximize the effectiveness of the Red and Blue teams



Build
Attack
Defend

AREAS OF CYBER SECURITY

NETWORK SECURITY

APPLICATION SECURITY

SOCIAL ENGINEERING

AREAS OF CYBER SECURITY

REVERSE ENGINEERING

MALWARE ANALYSIS

DIGITAL FORENSICS

PENETRATION TESTING

PenTest, like forensics, is almost as much an art as it is a science – you can only be taught so far, technical techniques and tools are all very well, but you really need a mind that can think sideways and approach a task from as many angles as possible.

PHASES OF PENETRATION TESTING

FOOTPRINTING

Tools and tricks to get the information about the computer, IP and mac address, related user and system.

SCANNING

Before starting the pentesting, pentester must have some information about network and system.so pentester scan the entire network with some tool like Nmap, Zenmap, ping and hping etc.

ENUMERATION

During the enumeration phase, possible entry points into the tested systems are identified. The information collected during the reconnaissance phase is put to use

SYSTEM HACKING

System hacking login to system without credentials not only bypass the credentials but also you can work in system as root user by privilege escalation.

How social engineering Works?

Social engineering cycle

GATHER INFORMATION:

This is the first stage, the learns as much as he can about the intended victim. The information is gathered from company websites, other publications and sometimes by talking to the users of the target system.

PLAN ATTACK

The attackers outline how he/she intends to execute the attack

ACQUIRE TOOLS

These include computer programs that an attacker will use when launching the attack.

USE ACQUIRED KNOWLEDGE

Information gathered during the social engineering tactics such as pet names, birthdates of the organization founders, etc. is used in attacks such as password guessing.

Common Social Engineering Techniques:

FAMILIARITY EXPLOIT

Users are less suspicious of people they are familiar with. An attacker can familiarize him/herself with the users of the target system prior to the social engineering attack. The attacker may interact with users during meals, when users are smoking he may join, on social events, etc. This makes the attacker familiar to the users. Let’s suppose that the user works in a building that requires an access code or card to gain access; the attacker may follow the users as they enter such places. The users are most like to hold the door open for the attacker to go in as they are familiar with them. The attacker can also ask for answers to questions such as where you met your spouse, the name of your high school math teacher, etc. The users are most likely to reveal answers as they trust the familiar face. This information could be used to hack email accounts and other accounts that ask similar questions if one forgets their password

INTIMIDATING CIRCUMSTANCES

People tend to avoid people who intimidate others around them. Using this technique, the attacker may pretend to have a heated argument on the phone or with an accomplice in the scheme. The attacker may then ask users for information which would be used to compromise the security of the users' system. The users are most likely give the correct answers just to avoid having a confrontation with the attacker. This technique can also be used to avoid been checked at a security check point.

PHISHING

This technique uses trickery and deceit to obtain private data from users. The social engineer may try to impersonate a genuine website such as Yahoo and then ask the unsuspecting user to confirm their account name and password. This technique could also be used to get credit card information or any other valuable personal data

TAILGATING

This technique involves following users behind as they enter restricted areas. As a human courtesy, the user is most likely to let the social engineer inside the restricted area

EXPLOITING HUMAN CURIOSITY

Using this technique, the social engineer may deliberately drop a virus infected flash disk in an area where the users can easily pick it up. The user will most likely plug the flash disk into the computer. The flash disk may auto run the virus, or the user may be tempted to open a file with a name such as Employees Revaluation Report 2013.docx which may actually be an infected file

EXPLOITING HUMAN GREED:

Using this technique, the social engineer may lure the user with promises of making a lot of money online by filling in a form and confirm their details using credit card details, etc.