Operation: Zero Trace

An introduction into the realm of ethical hacking

Edwin Choi

C:\root\Table_of_Contents

```
No  Name
--  ----
1.  Definition_of_an_ethical_hacker
2.  Comparisons_between_types_of_hackers
3.  Ethical_hacking_roadmap
4.  Modus_Operandi_of_ethical_hackers
5.  Stages_of_penetration_testing
6.  Methods_of_attack
7.  End
```

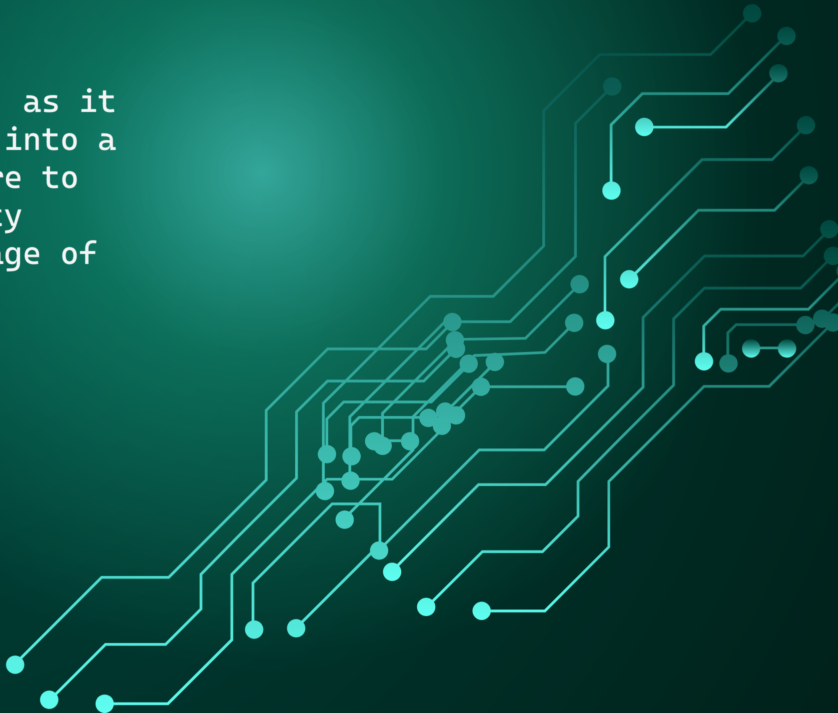
ETHICAL HACKING – DEFINITION

If individuals can hack for malicious reasons,
is it possible to hack for a noble cause?

Ethical hacking is the solution to this question, as it relies on receiving permission prior to breaking into a system or network. The intent lies not in a desire to cause harm, but rather, to detect and fix security problems before malicious actors can take advantage of them.

Other aliases:

- Penetration Testing
- White-Hat Hacking



COMPARISONS BETWEEN TYPES OF HACKERS

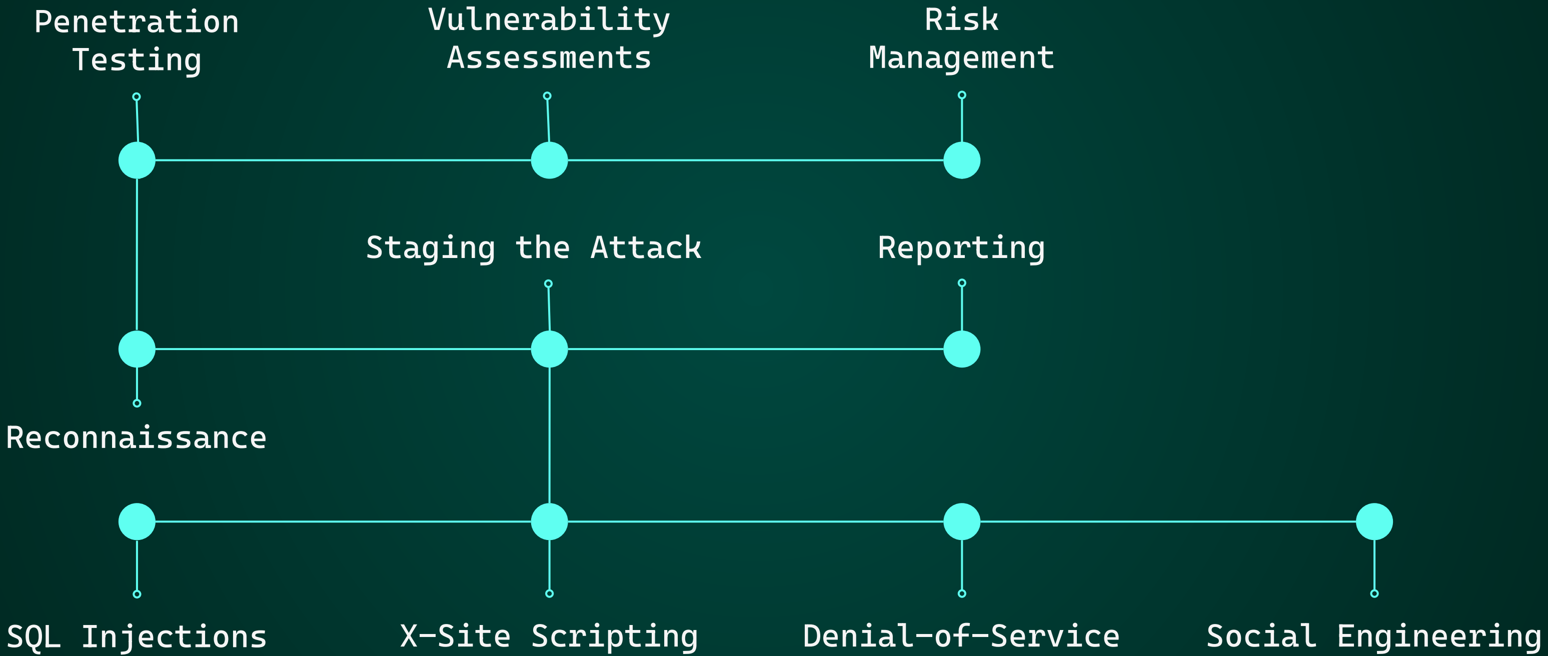
ETHICAL HACKER

- Performs work after being granted explicit permission
- Abides by state & federal laws
- Work is aimed at preventing and fixing potential problems

MALICIOUS HACKER

- Enters computer systems and networks without permission
- Activities are often in violation of the law
- Intent is often to cause harm or steal data

OPERATIONS ROADMAP



Penetration Testing

Vulnerability Assessments

Risk Management

Staging the Attack

Reporting

Reconnaissance

SQL Injections

X-Site Scripting

Denial-of-Service

Social Engineering

MODUS OPERANDI

PENETRATION TESTING

An ethical hacker imitates the movements of a malicious actor to gain unauthorized access to a company's systems. Typically involves 3 stages.

VULNERABILITY ASSESSMENTS

The ethical hacker uses manual and automated methods to detect and document vulnerabilities within a given system.

RISK MANAGEMENT

New and emerging threats are identified and used to analyze how they can threaten a company's network security.

PENETRATION TESTING

Phase 1 – Reconnaissance

During this stage, the pen tester gathers information on the various types of devices, such as computers and mobile devices, within a company's network that they have been tasked with breaching.

Recon attempts may involve the use of online profile tracking, open port scanning, network traffic inspections, and social engineering.

PENETRATION TESTING

Phase 2 – Staging the Attack

Once the pen tester scopes out potential vulnerabilities within the given system, they commence attack operations. These methods may include, but are not limited to, the following:

- SQL injections
- Cross-site scripting
- Denial-of-Service (DoS) attacks
- Social engineering

At the end, the attack methods used are covered up, both to demonstrate how an actual hacker could hide in the system and also to prevent them from taking advantage of such routes.

PENETRATION TESTING

Phase 3 – Reporting

At the conclusion of the emulated attack, the pen tester documents all of their activities performed during the operation. This report outlines all of the vulnerabilities exploited, the assets and data accessed, and how security systems were evaded.

The pen tester then provides the client with suggestions on how to prioritize and patch these aforementioned system vulnerabilities.

METHODS OF ATTACK

SQL INJECTION

Malicious code is entered into input fields on a website or app in an effort to extract sensitive data from it.

SOCIAL ENGINEERING

Company employees are targeted with phishing, baiting, pretexting, and other tactics with the aim of having them comprising network security.

DENIAL OF SERVICE

Servers, apps, and other network resources are flooded with traffic in an effort to take them offline.

CROSS-SITE SCRIPTING

The pen tester attempts to plant malicious code into a company's website.

END OF LINE

CREDITS: This presentation template was created by **Slidesgo**, including icons by **Flaticon**, and infographics & images by **Freepik**

Please keep this slide for attribution