Introduction To Ethical Hacking

Why, What, How, about Ethical Hacking.

By Chinni

What We'll Learn?

- What is Ethical Hacking?
- Why Ethical Hacking is needed?
- Terminology Used In Hacking
- Who are Hackers and Their Types.
- What are Security Policies?
- Hacking Phases
- Types of Attacks

Who is a Hacker?

Hackers are intelligent individuals who spends enormous amounts of time exploring computing resources like networks, websites, mobile devices etc.

By Chinni

What is Hacking?

Hacking refers to exploiting system vulnerabilities and compromising security controls to gain unauthorized or inappropriate access to the system resources.

It involves modifying system or application features to achieve a goal outside of the creator’s original purpose.

What is Ethical Hacking?

Ethical Hacking involves the use of hacking tools, tricks, and techniques to identify vulnerabilities so as to assume system security.

It focuses on simulating techniques used by attackers to verify the existence of exploitable vulnerabilities in the systems security.

By Chinni

Why Ethical Hacking is Necessary?

To Beat the Hacker, you need to think like one.

Ethical hacking is necessary because it allows the countering of attacks from malicious hacker by anticipating methods they can use to break into a system.

- To Prevent hackers from gaining access to information breaches.
- To fight against terrorism and national security breaches.
- To build a system that avoids hackers from penetrating.
- To test if organization’s security settings are in fact secure.

By Chinni

Types of Hackers

- White Hat Hackers
- Black Hat Hackers
- Grey Hat Hackers
- Script Kiddies
- State Sponsored Hackers
- Hacktivists
- Cyber Terrorists
- Suicide Hackers
- Spy Hackers

By Chinni

Terminology

Vulnerability: Vulnerability is a weakness in design or an implementation error that can lead to an unexpected And undesirable event compromising the security of the system. In simple words, a vulnerability is loop hole, Limitation, or weakness that becomes a source for an attacker to enter into the system by bypassing various User authentication.

Exploit: An exploit is a defined way to breach the security of an IT system through vulnerability.
The term exploit is used when any kind of attack has taken place on a system or network. An exploit can Also be defined as malicious software or commands that can cause unanticipated behavior to occur on Legitimate software or hardware by taking advantage of the vulnerabilities.

Zero-day attack: In a 0-day attack, the attacker exploits the vulnerability before the software developer releases the Patch For them.

By Chinni

Hack value: Hack value is a notion among the hackers that something is worth doing or it is interesting. Hackers May feel that breaking down the toughest network security might give them great satisfaction, and that it is something they accomplished that not everyone could do.

Target of evaluation: A target of evaluation is an IT system, product, or component that is identified/subjected to a required security evaluation. This kind of evaluation helps the evaluator understand that functioning, technology, and vulnerabilities of a particular system or product.

Payload: A payload is an action or set of action has to be done on the target, once the exploit successfully launched. It can be any kind of control, or Denial of service or any other crash or something.

By Chinni

Information Security Threats

Natural Threats

1. Floods
2. Earthquakes
3. Natural Disasters
4. Hurricanes

Physical Security Threats

1. Loss or damage of system resources
2. Physical Intrusion
3. Corporate espionage

Human Threats

1. Hackers
2. Insiders
3. Social Engineering
4. Lack of knowledge and Awareness

By Chinni

Level of security in any system can be defined by the strength of three components:

By Chinni

Elements of Information Security

- Confidentiality
- Integrity
- Availability
- Authentication
- Authorization
- Non-Repudiation

Phases of Hacking

- Target Scoping
- Foot Printing And Reconnaissance
- Network Scanning
- Port Scanning
- Vulnerability Analysis
- Searching or Building exploit
- Attack
- Maintaining Access With Trojans and Backdoors
- Clearing Tracks (or) Reporting.

By Chinni

Security Policies

Information Security Policy is a document or set of documents which defines the rules and regulation has to be followed in the company to protect its assets from threats.

Policies BY Types

General Policy
User Policy
IT Policy
Partner Policy
Issue Specific Policy

Policies BY Severity

Promiscuous Policy
Permissive Policy
Prudent Policy
Paranoid Policy

By Chinni

Information Security Warfare

The Term information warfare or INFOWAR refers to the use of information and communication technologies (ICT) to take competitive advantages over an opponent.

Defensive INFOWAR

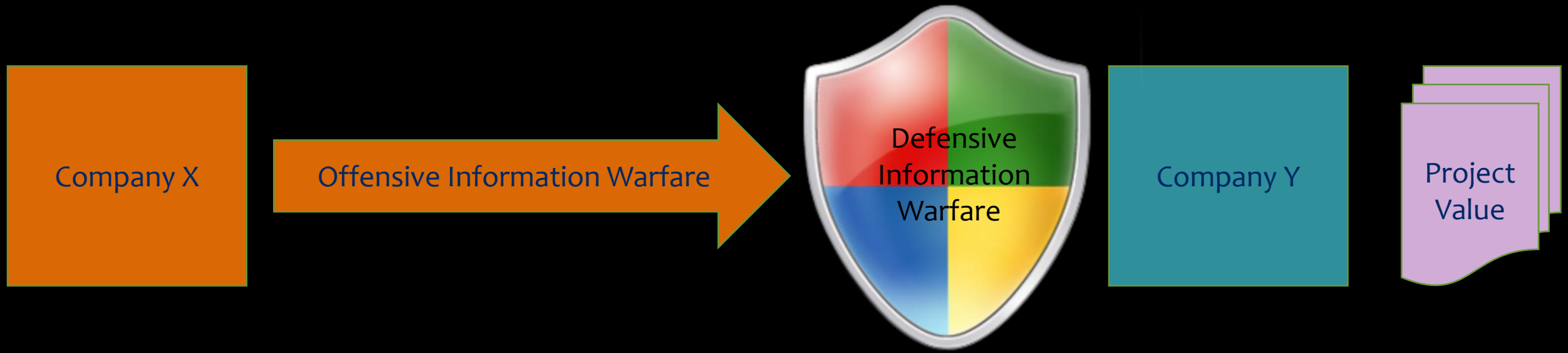
- Prevention
- Alerts
- Detection
- Emergency Preparedness
- Response

Offensive INFOWAR

- Web application attacks
- Web server attacks
- Malware attacks
- MITM attacks
- System hacking

By Chinni

Example Of INFOWAR



If “Company X” Succeeded to Do Offensive INFOWAR “Company Y” reputation will go down and “Company X” will gain advantages like New Projects and Tender Wins Etc.; So “Company Y” Has to secure the Data They have With Defensive INFOWAR.

By Chinni

Useful Links:

Security and vulnerability Research Websites:

1. Securityfocus.com
2. Secunia.com
3. Packetstormsecurity.com
4. Governmentsecurity.org

Exploit Research Websites:

1. Exploit-db.com
2. Corelan.be
3. 1337day.com

Hacking Conferences:

1. Defcon Conference
2. Shmoocon Conference
3. Blackhat Conference
4. Nullcon Conference
5. Malcon Conference
6. Club hack Conference

Hacking Forum Sites:

1. Hackforums.net
2. Alboraaq.com
3. Hackhound.org
4. Garage4hackers.com
5. Irongeek.com
6. Forum.tuts4you.com
7. Icode.org(ic”Zero”de.org)

Hacking Magazines:

1. Phrack.org
2. hacking9.org
3. 2600.Com
4. Magazine.hitb.com
5. www.net-security.org/**insecure**mag.php
6. Club hack Magazine chmag.in
7. Pentest magazine pentestmag.com
8. Hackers5.com

By Chinni

Source : Internet