Chapter 1

Introduction to Ethical Hacking

Theory

Ethical Hacking

Hacking

Hacking is the process of exploiting system vulnerabilities and compromising security systems to gain unauthorized access to the system resources. It involves modifying system or application features to achieve a goal outside of the creator’s original purpose.

Ethical Hacking

Ethical Hacking is the process to identify vulnerabilities to assure system security by use of hacking tools, tricks, and techniques. It focuses on simulating methods used by attackers to verify the existence of exploitable vulnerabilities in the system's security.

Hacker

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

Ethical Hacker

Ethical Hacker is an expert in computer internals and networking concepts, who tries to find out potential vulnerabilities on the target systems before a hacker could use, without actually doing any harm to the information systems on behalf of the owners of the IT Assets.

Types of Hackers

Black Hat (Crackers): Individuals utilize computing skills for malicious or destructive activities.

White Hat: Individuals utilizing hacking skills for the defensive purpose

Gray Hat: Individuals who work both offensively and defensively

Suicide Hackers: Hackers who aim to shut down the critical infrastructure for a cause and are not worried about facing punishment.

Script Kiddies: An unskilled hacker who compromises the system by running scripts, tools, and software developed by real hackers.

Cyber Terrorists: Individuals with hacking skills, motivated by religious or political beliefs to create fear by large-scale disruption of computer networks.

Hacktivist: Hackers who promote a political agenda by hacking, especially by defacing or disabling websites.

Government Sponsored: Individuals employed by the government to penetrate and gain confidential information.

Why Ethical Hacking is Necessary

Ethical Hacker needs to think like malicious Hacker. Ethical hacking is necessary to defend against malicious hackers attempts, by anticipating methods they can use to break into a system.

- To fight against cyber crimes.
- To protect information from getting into wrong hands.
- To build a defensive mechanism that avoids hackers from penetrating.
- To test the organization’s infrastructure security.

Steps to Perform Ethical Hacking

1. **Reconnaissance** refers to the pre-attack phase where an attacker observes a target before launching an attack. It may include the target organization's clients, employees, operations, network, and systems
2. **Scanning** is the phase immediately preceding the attack. Here, the attacker uses the details gathered during reconnaissance to identify specific vulnerabilities. An attacker can gather critical network information such as the mapping of systems, routers, and firewalls by using simple tools such as the standard Windows utility Traceroute.
3. **Gaining Access** In this phase in which real hacking occurs. Attackers use vulnerabilities identified during the reconnaissance and scanning phase to gain access to the target system or network. Attackers gain access to the target system locally, over a LAN, or over the Internet.
4. **Maintaining Access** of the target machine and remain undetected. Attackers install a backdoor or a Trojan to gain repeat access. They can also install rootkits at the kernel level to gain full administrative access to the target computer. Rootkits are used to gain access at the operating system level, while a Trojan horse gains access at the application level. Both rootkits and Trojans require users to install them locally.
5. **Clearing Tracks** is for avoiding legal trouble, attackers will overwrite the server, System and application logs to Avoid suspicion and erase all evidence of their actions. Attackers can execute scripts in the Trojan or rootkit to replace the critical system and log files to hide their presence in the system.

Terminology

Vulnerability: In simple words, vulnerability is a loophole, Limitation, or weakness that becomes a source for an attacker to enter into the system.

Exploit: It is a software tool designed to take advantage of a flaw (vulnerability) in a system for malicious purposes.

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

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

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

What is Information Security

Information security, sometimes shortened to **InfoSec**, is the practice of preventing unauthorized access, disclosure, disruption, destruction, modification, inspection, recording or destruction of information.

Information security's primary focus is the balanced protection of the confidentiality, integrity, and availability of data and focuses on efficient policy implementation, organization productivity.

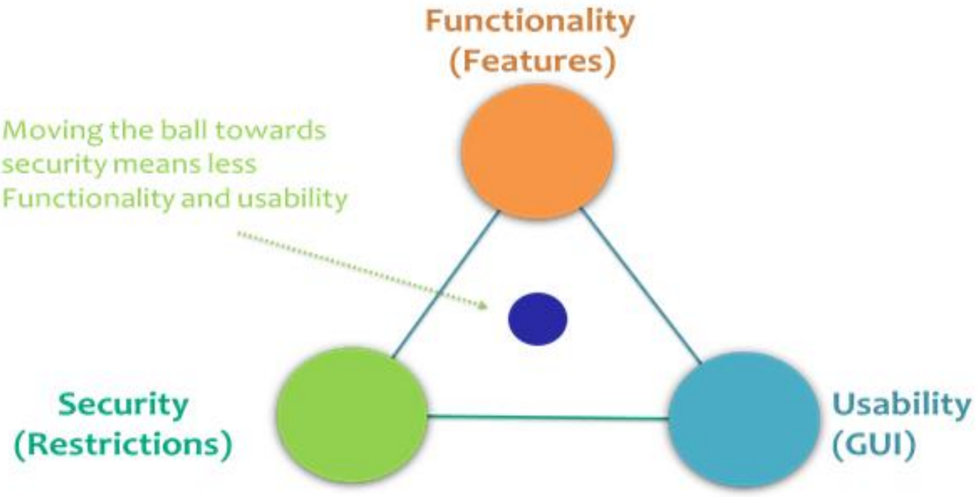
Elements of Information Security

Information Security is a state of well-being of information and infrastructure in which the possibility of theft, tampering, and disruption of information and services is kept low or tolerable.

- Confidentiality
- Authenticity
- Integrity
- Non-Repudiation
- Authorization
- Availability

The Security, Functionality and Usability Triangle

The strength of these three components can define the level of Security in any system.


Functionality
(Features)
Moving the ball towards security means less Functionality and usability
Security
(Restrictions)
Usability
(GUI)

Requirements to run Kali Linux on the Host machine

Hardware:

- Minimum 4/8 GB RAM
- AMD2016 Model / intel core i3/i5/i7 processor
- Minimum 80 GB Hard disk
- Minimum 15 Mbps internet speed

Software

- Virtual box software
- Kali Linux virtual machine image file (.ova)
- Metasploitable 2 virtual machine

Useful Links Source: Internet

Security and vulnerability Research Websites:

- Securityfocus.com
- Secunia.com
- Packetstormsecurity.com
- Governmentsecurity.org

Exploit Research Websites:

- Exploit-db.com
- Corelan.be
- 1337day.com

Hacking Conferences:

- Defcon Conference
- Shmoocon Conference
- Blackhat Conference
- Nullcon Conference
- Malcon Conference
- Club hack Conference

Hacking Forum Sites:

- Hackforums.net
- Alboraaq.com
- Hackhound.org
- Garage4hackers.com
- Irongeek.com
- Forum.tuts4you.com
- Ic0de.org(ic”Zero”de.org)

Hacking Magazines:

- Phrack.org
- hackin9.org
- 2600.Com
- Magazine.hitb.com
- Pentest magazine
- Hack
- ers5.com
- Club hack Magazine chmag.in