VIT UNIVERSITY SCHOOL OF COMPUTER SCIENCE ENGINEERING

Chapter 1: ETHICAL HACKING

By
Dr. Ravi Verma

Contents To Be Discuss

- **Phases involved in Hacking**
- **Reconnaissance**
- **Foot-Printing**
- **Scanning**
- **Gaining Access**
- **Maintaining Access**
- **Clearing Track**
- **Foot Printing**
- **What kind of information can be gathered from Foot-printing?**
- **Sources**

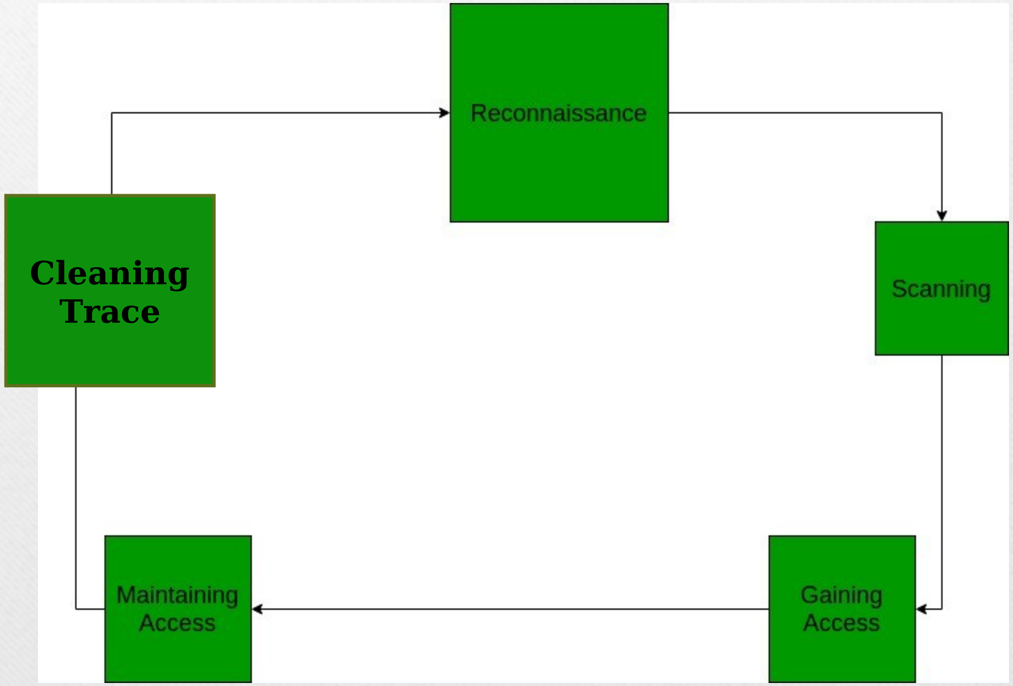
Contents To Be Discuss Cont. …

- Advantages
- Counter Measures
- How Scanning proceed in Ethical Hacking
- Objectives of Network Scanning
- Scanning Types
- Scanning Methodologies
- Port Scanning
- Vulnerability Scanning

Phases involved in Hacking

- This is not to motivate you to hack and shut down websites but to **provide a general idea** of how the daily hacks are performed and to protect yourself from such incidents at least take some precautions.
- There are mainly 5 phases in hacking. Not necessarily a hacker has to follow these 5 steps in a sequential manner. It’s a stepwise process and when followed yields a better result.

Phases involved in Hacking Cont..



Phases involved in Hacking Cont..

- The process of legal and authorized attempts to discover and successfully exploiting the computer system in an attempt to make the computer system more secure is called Ethical Hacking. This process includes a probe for vulnerability and providing proof of concept (POC) attacks to visualize that vulnerabilities are actually present in the system.

Reconnaissance

- This is the first step of Hacking. It is also called as Foot printing and information gathering Phase. This is the preparatory phase where we collect as much information as possible about the target. We usually collect information about three groups,

1. Network
2. Host
3. People involved

Foot-Printing

- There are two types of Foot-Printing
- **Active:** Directly interacting with the target to gather information about the target. Ex. Using Nmap tool to scan the target.
- **Passive:** Trying to collect the information about the target without directly accessing the target. This involves collecting information from social media, public websites etc.

Scanning

- **Port scanning:** This phase involves scanning the target for the information like open ports, Live systems, various services running on the host.
- **Vulnerability Scanning:** Checking the target for weaknesses or vulnerabilities which can be exploited. Usually done with help of automated tools.
- **Network Mapping:** Finding the topology of network, routers, firewalls servers if any, and host information and drawing a network diagram with the available information. This map may serve as a valuable piece of information throughout the hacking process.

Gaining Access

- This phase is where an attacker breaks into the system/network using various tools or methods. After entering into a system, he has to increase his privilege to administrator level so he can install an application he needs or modify data or hide data.

Maintaining Access

- Hacker may just hack the system to show it was vulnerable or he can be so mischievous that he wants to maintain or persist the connection in the background without the knowledge of the user. This can be done using Trojans, Rootkits or other malicious files. The aim is to maintain the access to the target until he finishes the tasks he planned to accomplish in that target.

Clearing Track

- No thief wants to get caught. An intelligent hacker always clears all evidence so that in the later point of time, no one will find any traces leading to him.
- This involves modifying/corrupting/deleting the values of Logs, modifying registry values and uninstalling all applications he used and deleting all folders he created.

Foot Printing

- **Foot-printing** means gathering information about a target system which can be used to execute a successful cyber attack. To get this information, a hacker might use various methods with variant tools. This information is the first road for the hacker to crack a system.

1. **Active Foot-printing:**
   Active foot-printing means to perform foot-printing by getting in direct touch with the target machine.
2. **Passive Foot-printing:**
   Passive foot printing means collecting information of a system located at a remote distance from the attacker.

What kind of information can be gathered from Foot-printing?

- Operating system of the target machine.
- Firewall.
- IP address.
- Network map.
- Security configurations of the target machine.
- Email id, password.
- Server configurations.
- URLs.
- VPN.

Sources

- **Social Media:**
  Most people has the tendency to release most of their information online. Hackers use this sensitive information in a big deal. They may create a fake account for looking real to be added as friend or to follow someone's account for grabbing their information.
- **JOB websites:**
  Organizations share some confidential data in many JOB websites like monsterindia.com. For example, a company posted on a website : "Job Opening for lighttpd 2.0 Server Administrator". From this information can be gathered that an organization uses lighttpd web server of version 2.0 .

Sources Cont..

Google:

Search engines such as Google have the ability to perform more powerful searches than one can think and one had gone through. It can be used by hackers and attackers to do something that has been termed Google hacking. Basic search techniques combined with advanced operators can do a great damage. Server operators exist like “inurl:”,”allinurl:”,”filetype:”, etc.

Sources Cont..

- **Social Engineering:**
  There are various techniques that fall in this category. A few of them are: **Eavesdropping –** Attacker tries to record personal conversation of the target victim with someone that’s being held over communication mediums like Telephone.
- **Shoulder Surfing –** In this technique Attacker tries to catch the personal information like Email id, password, etc; of the victim by looking over the victim’s shoulder while the same is entering(typing/writing) his/her personal details for some work.

Sources Cont..

- **Archive.org:**
  Archived version refers to the older version of the website which existed in a time before and many features of the website has been changed. archive.org is a website that collects snapshots of all the website at a regular interval of time. This site can be used to get some information that does not exist now but existed before on the site.

Sources Cont..

- **An Organization’s Website:** Its the best place to begin for an attacker. If an attacker wants to look for open source information, which is information freely provided to clients, customers, or the general public then simply the best option is: “ORGANISATION’s WEBSITE”.

Sources Cont..

- **Using Neo Trace:**
  Neo-Trace is a powerful tool for getting path information. The graphical display, displays the route between you and the remote site, including all intermediate nodes and their information. Neo-Trace is a well-known GUI route tracer program. Along with a graphical route, it also displays information on each node such as IP address, contact information, and location.

Sources Cont..

- **Who is:**
  This is a website which serves a good purpose for Hackers. Through this website information about the domain name, email-id, domain owner, etc; a website can be traced. Basically, this serves a way for Website Footprinting.

Advantages

- Footprinting allows Hackers to gather the basic security configurations of a target machine along with network route and data flow.
- Once attacker finds the vulnerabilities he/she focuses towards a specific area of the target machine.
- It allows the hacker to identify as to which attack is more handy to hack the target system.

Counter Measures

- Avoid posting confidential data in social media websites.
- Avoid accepting unwanted friend requests on social media platforms.
- Promotion of education on various hacking tricks.
- Usage of footprinting techniques for identifying and removing sensitive information from social media platforms.
- Proper configuration of web servers to avoid loss of information about system configuration.

How Scanning proceed in Ethical Hacking

- Scanning is another essential step, which is necessary, and it refers to the package of techniques and procedures used to identify hosts, ports, and various services within a network. Network scanning is one of the components of intelligence gathering and information retrieving mechanism an attacker used to create an overview scenario of the target organization (target organization: means the group of people or organization which falls in the prey of the Hacker).

Scanning Types

- Network Scanning
- Port Scanning
- Vulnerability Scanning

Objectives of Network Scanning

1. To discover live hosts/computer, IP address, and open ports of the victim.
2. To discover services that are running on a host computer.
3. To discover the Operating System and system architecture of the target.
4. To discover and deal with vulnerabilities in Live hosts.

Scanning Methodologies

1. Hackers and Pen-testers check for Live systems.
2. Check for open ports (The technique is called Port Scanning, which will be discussed below)
3. Scanning beyond IDS (Intrusion Detection System)
4. Banner Grabbing: is the method for obtaining information regarding the targeted system on a network and services running on its open ports. Telnet and ID Serve are the tools used mainly to perform a Banner-grabbing attack. This information may be used by intruders/hackers to portray the lists of applicable exploits.
5. Scan for vulnerability
6. Prepare Proxies

Port Scanning

- It is a conventional technique used by penetration testers and hackers to search for open doors from which hackers can access any organization's system. During this scan, hackers need to find out those live hosts, firewalls installed, operating systems used, different devices attached to the system, and the targeted organization's topology. Once the Hacker fetches the victim organization's IP address by scanning TCP and UDP ports, the Hacker maps this organization's network under his/her grab. Amap is a tool to perform port scanning.

Vulnerability Scanning

- It is the proactive identification of the system's vulnerabilities within a network in an automated manner to determine whether the system can be exploited or threatened. In this case, the computer should have to be connected to the internet.

Question Please?

THANK YOU