LAB1 – KALI LINUX OVERVIEW

# RECONNAISSANCE

This is the first step of Hacking. It is also called as Footprinting 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,

* Network
* Host
* People involved

There are two types of Footprinting:

* Active: Directly interacting with the target to gather information about the target. Eg 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.

**Thực hiện**

1.1 Kiểm tra IP Kali linux và kết nối internet

A computer screen shot of a computer program

Description automatically generated

Gợi ý: ifconfig

A screen shot of a computer program

Description automatically generated

1.2 Kiểm tra DNS Server hiện tại

A computer screen with white text

Description automatically generated

Gợi ý: whois, nslookup

1.3 Kiểm tra các host đang online trong cùng lớp mạng

A screen shot of a computer

Description automatically generated

Gợi ý: nmap

# SCANNING

Three types of scanning are involved:

**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 haking process.

**Thực hiện**

2.1 Kiểm tra kết nối đến host đang online

A screen shot of a computer program

Description automatically generated

Gợi ý: hping3

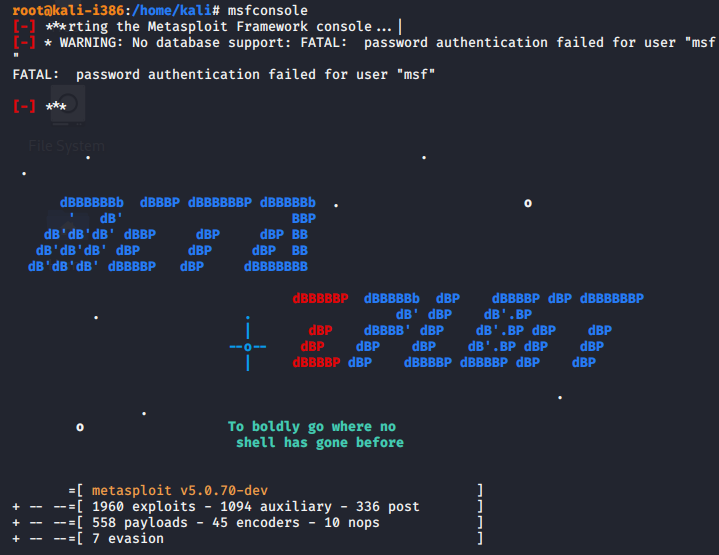
2.2 Port scanning

A screen shot of a computer

Description automatically generated

Gợi ý: nmap, zenmap

2.3 Vulnerability Scanning



Gợi ý: OpenVAS, Nessus

Gợi ý: kiểm tra OpenVAS đã cài đặt ?

🡪 sử dụng openvas kiểm tra lỗ hổng của IP victim

# 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.

**Thực hiện**

3.1 Khởi động công cụ khai thác

A screen shot of a computer

Description automatically generated

3.2 Sử dụng thư viện khai thác xác định lỗi mặc định trên máy victim

A screenshot of a computer

Description automatically generated

3.3 Định nghĩa các tham số phù hợp module khai thác

A computer screen with white text

Description automatically generated

3.4 Chủ động khai thác

A computer screen with white text

Description automatically generated

3.5 Kiểm tra quyền truy cập hiện tại sau khi đã chiếm quyền máy victim

A computer screen shot of a program

Description automatically generated

Gợi ý: mongodb, msfinit, msfconsole, … các lệnh cmd trên windows, …

# 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.

**Thực hiện**

4.1 Tạo user khác trên máy victim có quyền admin bằng câu lệnh

A screen shot of a computer

Description automatically generated

4.2 Mở port SSH/Telnet/RDP trên máy victim bằng câu lệnh.

A screen shot of a computer

Description automatically generated

# GET DATA

After getting a session you know that an attacker can easily get your info, steal your contacts, messages, app data and many more.

**Thực hiện**

5.1 Tạo thử tập tin C:\DATA.txt có nội dung tùy ý trên máy nạn nhân

A white screen with black text

Description automatically generated

5.2 Lấy tập tin C:\DATA.txt trên máy victim về Desktop của Kali linux

A computer screen with white text

Description automatically generated

A screenshot of a computer

Description automatically generated

# 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.

**Thực hiện**

6.1 Xóa log windows

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A computer screen shot of a black screen

Description automatically generated

6.2 Xóa log khai thác

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

6.3 Thoát khai thác

A screenshot of a computer

Description automatically generated