Name : Abhishek Srivastava.
Reg. No : 19BCE10071
Subject : Ethical Hacking
Slott : B11 + B12 + B13
Date : 08-03-2022

MIDTERM

Q2] (a)

Footprinting is a hacking technique which is used to gather as much data as possible about a specific targeted computer system, an infrastructure and networks to identify opportunities to penetrate them. It is one of the best ~~methods~~ method of finding vulnerabilities.

The process of cybersecurity footprinting involves profiling organisations and collecting data about the network, host, employees, and third-party partners. This information includes the following :-

1. OS used
2. firewalls
3. Network maps
4. IP address
5. DNS information
6. Information security configuration.
7. URL's
8. VPN
9. Staff ID.
10. Email and phone number.

Two types of footprinting.

1) Active : It includes using tools ~~like~~ and techniques.

2) Passive : It involves collecting data about specific target using innocuous methods.
Eg: Google.

Footprinting flipkart.com

1) Whois footprinting
It gives us DNS details, Contact details, Registration & expiry date and Domain Name data.

Tools :

→ Whois Lookup : Search flipkart.com
→ Whois Record : Search flipkart.com.

2) DNS Footprinting
It gives all DNS Records. There are 10 types of DNS record that provide important information about target location.

Tools :

→ Domain Dossier
→ DNS record
→ DNS Dumpster
→ DNSDumpster.com

] Perform search for flipkart.com

3) Website footprinting

This technique extract the following details:

1) Achieved description
2) CMS
3) Scripts performed.
4) Web crawling
5) Metadata
6) Website monitoring System.

Tools:

→ Archive.org
→ Built with

4) WhatWeb

WhatWeb is a tool for Kali Linux.

Command: whatweb www.flipkart.com.

It gives all information about website.

5) Web Crawling

HTTrack is a free opensource web crawler. It allows complete website to our computer.

6) Web Data Extraction.

Used to Extract web data

Tool: Webdata Extraction Pro.

7) Web Spider

8) Website Watcher.

Q2) (b)

Scanning is a set of procedures for identifying live hosts, ports and services, discovering the operating System and its architecture, finding vulnerabilities and threats to Network.

Scanning IP Address (Using nmap).

Nmap is a free open-source network scanner.

$ nmap 192.168.55.191

Make sure not to perform network scanning with permission.

Q1]

(a) Threads

A thread is a flow of execution through the process code, with its own program counter, system register and stack. A thread is also called light weight process. It provides a way to improve application performance through parallelism. It minimises context switching time, provides concurrency, and better system utilization.

Types → User level threads
→ Kernel level threads.

(b) Virus

A virus is a computer program that attacks itself to legitimate programs and files without the user's consent. Virus can consume computer resources such as CPU and Memory. The attackers program or files are said to be infected. A computer virus is used to:

- Access private data.
- Display Annoying messages.
- Corrupt computers data.
- Log the user's keystroke.

(c) Vulnerabilities

Vulnerability is defined as an issue in the software code that the hacker can exploit to harm the system. It can be a gap in the implementation of cyber security procedures or a weakness in the controls.

Major types of Vulnerability:-

i. Faulty defenses.
ii. Resource Management not adequate.
iii. Insecure Connections.
iv. End user error and misuse.

(d) Attack

An attack is when an individual or an organisation deliberately and maliciously attempts to breach the information system of another individual or organisation.

Types:-

→ OS attacks
→ Misconfiguration attack.
→ Application level attack
→ Shrink wrap code attack.

Q3]

ARP poisoning (also known as ARP spoofing) is a cyber attack carried out through malicious ARP messages.

In ARP attack is difficult to detect, and once it's in place, the impact is impossible to ignore.

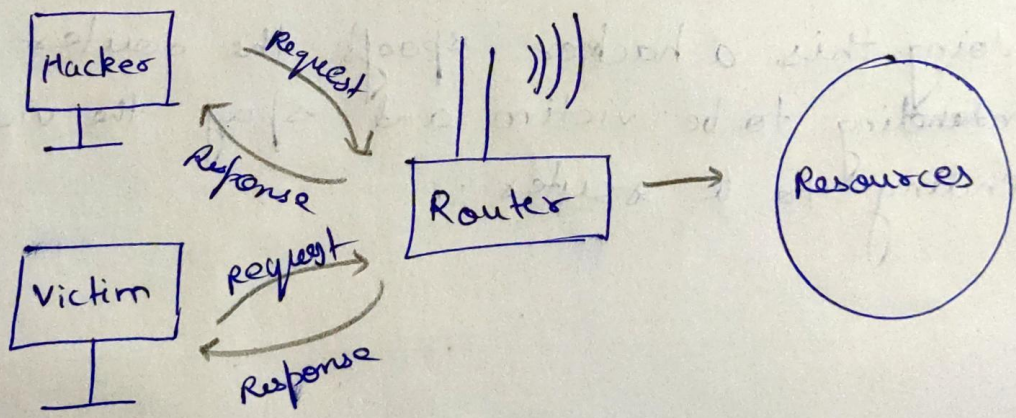
The hacker who performs ARP poisoning, gains access to every document in our network.

This attack constructs a large number of forced ARP request and replies packet to overload the switch.

Man in the Middle attack using ARP poisoning

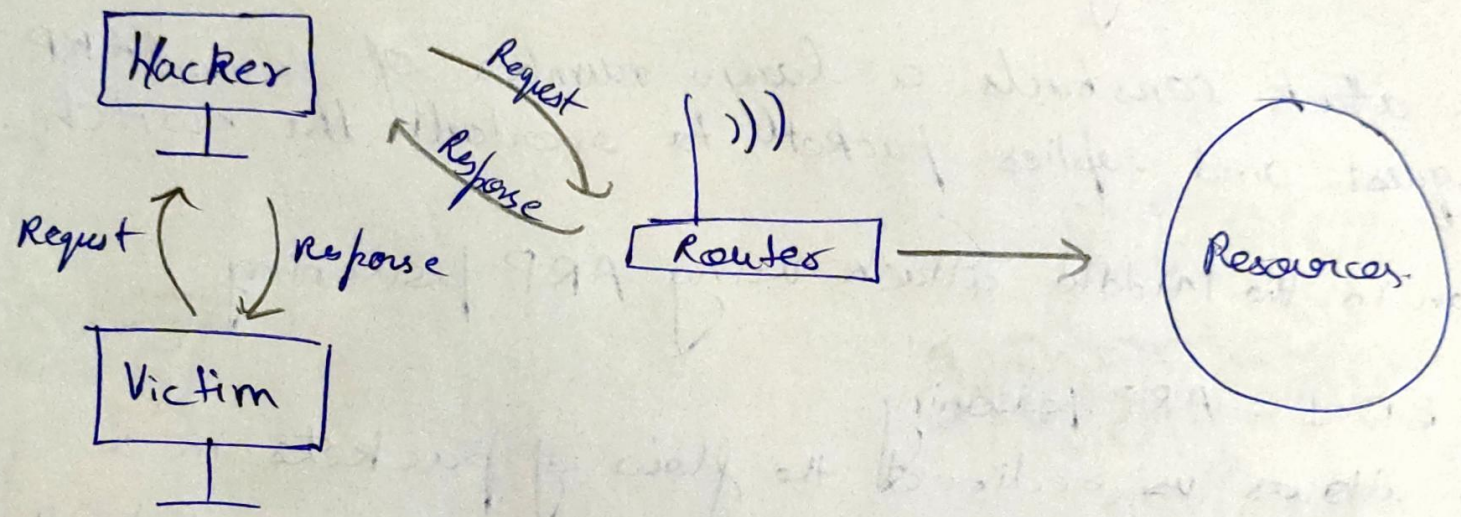
STEP-1 : ARP poisoning.

It allows us redirect the flow of packets in a computer network. Typical Network flow is like this:



STEP-2

But when a hacker becomes Man in the Middle by ARP spoofing then all the request and responses start flowing through hacker's system.



STEP-3

By doing this, a hacker spoofs the router by pretending to be victim and spoof the victim pretending to be router.

Q4]

The Five major Steps involved in ethical hacking:-

STEP 1

Reconnaissance - In this step we gather data of the target computer. It is of two types.

Active Reconnaissance
- Involves direct communication with target.

Passive Reconnaissance
- Involves indirect methods to collect information.

STEP 2

Scanning- Hacker scans the collected data and deploys the appropriate tools to hack the aimed system.

STEP-3

Gaining Access - In this step, the hacker gain access to the target System, network or application using specific tools.

STEP-4

Maintaining Access - In this step the hacker try to maintain access for future attacks without the user knowing about it. Malicious files are available online to do this job.

STEP-5

Covering tracks- In this step the hacker tries to cover all the tracks so that he doesn't get caught by the security personnel.

Q5]

Penetration testing, also known as Pen test, is a simulated cyber security attack against your computer system to check for exploitable vulnerabilities.

Penetration testing involves attempted breaching of any number of application systems to uncover vulnerabilities.

Penetration testing report also suggests counter measures which can be taken to reduce the risk of the system being hacked.

Control over Remote Machine.

Options:-

→ TeamViewer
→ LogMeIn
→ Splashtop
→ UltraVNC
→ Windows Remote desktop protocol.