UNIT II:

Footprints and Social Engineering: Using Web tools for Foot printing:SamSpade,Web data Extractor, Conducting Competitive Intelligence,Using Domain Name System Transfers.

Port Scanning: Introduction to Port Scanning, Types of Port Scans, Using PortScanningtools:Nmap, Unicornscan, Conducting Ping Sweeps

What is social engineering?

Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

Social engineering attacks happen in one or more steps. A perpetrator first investigates the intended victim to gather necessary background information, such as potential points of entry and weak security protocols, needed to proceed with the attack. Then, the attacker moves to gain the victim's trust and provide stimuli for subsequent actions that break security practices, such as revealing sensitive information or granting access to critical resources.

SamSpade

Scareware involves victims being bombarded with false alarms and fictitious threats. Users are deceived to think their system is infected with malware, prompting them to install software that has no real benefit (other than for the perpetrator) or is malware itself. Scareware is also referred to as deception software, rogue scanner software and fraudware.

A common scareware example is the legitimate-looking popup banners appearing in your browser while surfing the web, displaying such text such as, "Your computer may be infected with harmful spyware programs." It either offers to install the tool (often malware-infected) for you, or will direct you to a malicious

site where your computer becomes infected. Scareware is also distributed via spam email that doles out bogus warnings, or makes offers for users to buy worthless/harmful services.

Domain Name System Transfers

What is DNS?

The domain name system (DNS) is a naming database in which internet domain names are located and translated into Internet Protocol (IP) addresses. The domain name system maps the name people use to locate a website to the IP address that a computer uses to locate that website. For example, if someone types "example.com" into a web browser, a server behind the scenes maps that name to the corresponding IP address. An IP address is similar in structure to 203.0.113.72.

Web browsing and most other internet activities rely on DNS to quickly provide the information necessary to connect users to remote hosts. DNS mapping is distributed throughout the internet in a hierarchy of authority. Access providers and enterprises, as well as governments, universities and other organizations, typically have their own assigned ranges of IP addresses and an assigned domain name. They also typically run DNS servers to manage the mapping of those names to those addresses. Most Uniform Resource Locators (URLs) are built around the domain name of the web server that takes client requests.

How DNS works?

DNS servers convert URLs and domain names into IP addresses that computers can understand and use. They translate what a user types into a browser into something the machine can use to find a webpage. This process of translation and lookup is called DNS resolution.

The basic process of a DNS resolution follows these steps:

1.The user enters a web address or domain name into a browser.

2.The browser sends a message, called a recursive DNS query, to the network to find out which IP or network address the domain corresponds to.

3.The query goes to a recursive DNS server, which is also called a recursive resolver, and is usually managed by the internet service provider (ISP). If the recursive resolver has the address, it will return the address to the user, and the webpage will load.

4.If the recursive DNS server does not have an answer, it will query a series of other servers in the following order: DNS root name servers, top-level domain (TLD) name servers and authoritative name servers.

5.The three server types work together and continue redirecting until they retrieve a DNS record that contains the queried IP address. It sends this information to the recursive DNS server, and the webpage the user is looking for loads. DNS root name servers and TLD servers primarily redirect queries and rarely provide the resolution themselves.

6.The recursive server stores, or caches, the A record for the domain name, which contains the IP address. The next time it receives a request for that domain name, it can respond directly to the user instead of querying other servers.

7.If the query reaches the authoritative server and it cannot find the information, it returns an error message.

The entire process querying the various servers takes a fraction of a second and is usually imperceptible to the user.

DNS servers answer questions from both inside and outside their own domains. When a server receives a request from outside the domain for information about a name or address inside the domain, it provides the authoritative answer.

When a server gets a request from within its domain for a name or address outside that domain, it forwards the request to another server, usually one managed by its ISP.

DNS structure

The domain name is usually contained in a URL. A domain name is made of multiple parts, called labels. The domain hierarchy is read from right to left with each section denoting a subdivision.

The TLD appears after the period in the domain name. Examples of top-level domains include .com, .org and .edu, but there are many others. Some may denote a country code or geographic location, such as .us for the United States or .ca for Canada.

Each label on the left-hand side of the TLD denotes another subdomain of the domain to the right. For example, in the URL www.xxxx.com, "xxxxxx" is a subdomain of .com, and "www." is a subdomain ofxxxxx.com.

There can be up to 127 levels of subdomains, and each label can have up to 63 characters. The total domain character length can have up to 253 characters. Other rules include not starting or ending labels with hyphens and not having a fully numeric TLD name.

The Internet Engineering Task Force (IETF) has specified rules about implementing domain names in Request for Comments (RFC) 1035.

Introduction to Port Scanning

What is port scanning?

Port scanning is a method of determining which ports on a network are open and could be receiving or sending data. It is also a process for sending packets to specific ports on a host and analyzing responses to identify vulnerabilities.

This scanning can’t take place without first identifying a list of active hosts and mapping those hosts to their IP addresses. This activity, called host discovery, starts by doing a network scan.

The goal behind port and network scanning is to identify the organization of IP addresses, hosts, and ports to properly determine open or vulnerable server

locations and diagnose security levels. Both network and port scanning can reveal the presence of security measures in place such as a firewall between the server and the user's device.

After a thorough network scan is complete and a list of active hosts is compiled, port scanning can take place to identify open ports on a network that may enable unauthorized access.

It's important to note that network and port scanning can be used by both IT administrators and cybercriminals to verify or check the security policies of a network and identify vulnerabilities — and in the attackers' case, to exploit any potential weak entry points. In fact, the host discovery element in network scanning is often the first step used by attackers before they execute an attack.

As both scans continue to be used as key tools for attackers, the results of network and port scanning can provide important indications of network security levels for IT administrators trying to keep networks safe from attacks.

What are ports and port numbers?

Computer ports are the central docking point for the flow of information from a program or the Internet, to a device or another computer in the network and vice versa. Think of it as the parking spot for data to be exchanged through electronic, software, or programming-related mechanisms.

Port numbers are used for consistency and programming. The port number combined with an IP address form the vital information kept by every Internet Service Provider in order to fulfill requests. Ports range from 0 to 65,536 and basically rank by popularity.

Ports 0 to 1023 are well known port numbers that are designed for Internet use although they can have specialized purposes as well. They are administered by the Internet Assigned Numbers Authority (IANA). These ports are held by top-tier companies like Apple QuickTime, MSN, SQL services, and other prominent organizations. You may recognize some of the more prominent ports and their assigned services:

Port 20 (UDP) holds File Transfer Protocol (FTP) used for data transfer

Port 22 (TCP) holds Secure Shell (SSH) protocol for secure logins, ftp, and port forwarding

Port 53 (UDP) is the Domain Name System (DNS) which translates names to IP addresses

Port 80 (TCP) is the World Wide Web HTTP

Numbers 1024 through 49151 are considered “registered ports” meaning they are registered by software corporations. Ports 49,151 through 65,536 are dynamic and private ports - and can be used by nearly everyone.

Types of Port Scans

There are several techniques for port scanning, depending on the specific goal. It’s important to note that cybercriminals will also choose a specific port scanning technique based on their goal, or attack strategy.

Listed below are a few of the techniques and how they work:

Ping scans: The simplest port scans are called ping scans. In a network, a ping is used to verify whether or not a network data packet can be distributed to an IP address without errors. Ping scans are internet control message protocol (ICMP) requests and send out an automated blast of several ICMP requests to different servers to bait responses. IT administrators may use this technique to troubleshoot, or disable the ping scan by using a firewall — which makes it impossible for attackers to find the network through pings.

Half-open or SYN scans: A half-open scan, or SYN (short for synchronize) scan, is a tactic that attackers use to determine the status of a port without establishing a full connection. This scan only sends a SYN message and doesn’t complete the connection, leaving the target hanging. It’s a quick and sneaky technique aimed at finding potential open ports on target devices.

XMAS scans: XMAS scans are even quieter and less noticeable by firewalls. For example, FIN packets are usually sent from server or client to terminate a connection after establishing a TCP 3-way handshake and successful transfer of data and this is indicated through a message “no more data is available from the

sender.” FIN packets often go unnoticed by firewalls because SYN packets are primarily being looked for. For this reason, XMAS scans send packets with all of the flags — including FIN — expecting no response, which would mean the port is open. If the port is closed, a RST response would be received. The XMAS scan rarely shows up in monitoring logs and is simply a sneakier way to learn about a network’s protection and firewall.

Port Scanning Tools :Nmap, Unicornscan, Conducting Ping Sweeps

1.Nmap

2.Solarwinds Port Scanner

3.Netcat

4.Advanced Port Scanner

5.NetScan Tools

How to Detect a Port Scan?

There are a few different techniques to detect port scans, which could be attempts to scan your network for vulnerabilities.

One is a dedicated port scan detector software application, like PortSentry or Scanlogd.

Netcat includes port scanning functionality as well as the ability to create a simple chat server or program different packets for testing purposes.

Intrusion detection systems (IDS) are another way to detect port scans. Look for an IDS that uses a wide variety of rules to detect the various kinds of port scans that aren’t merely threshold-based.