Welcome Everyone

Please be waited session is about to start !!

Author

SANDEEP K

Introduction to Ethical Hacking and Information Gathering

MODULE-1

Module Overview

- Introduction to Ethical Hacking
- Information Security Overview
- Information Security Threats and Attack Vectors
- Ethical Hacking Concepts
- Information Security Controls
- Penetration Testing Concepts
- Information Security Laws and Standards
- Footprinting and Reconnaissance
- Footprinting through Search Engines, Web Services, and Social Networking Sites
- Website Footprinting
- Email Footprinting
- Competitive Intelligence
- Whois, DNS, and Network Footprinting
- Footprinting through Social Engineering
- Footprinting Tools
- Countermeasures
- Footprinting Pen Testing

Introduction to Ethical Hacking

PURPOSE OF ETHICAL HACKING:

- Ethical hacking is the practice of systematically probing systems, networks, and applications to uncover security vulnerabilities that could be exploited by malicious hackers. The key goal is **proactive defense**, identifying and fixing weaknesses before attackers can exploit them.
- Ethical hackers simulate real attacks to discover loopholes, including weak authentication, configuration flaws, unpatched vulnerabilities, or insecure data transmission.

DIFFERENT TYPES OF HACKER

WHITE HAT

White hat hackers are who work to keep data safe from other hacker by finding vulnerabilities in system that can be mitigated. They are usually employed by the target system's owner and are typically paid for their work. They just do legal work and use their knowledge for legal work, this type of hackers are also called as ethical hackers.

BLACK HAT

Black hat hackers are who steal data by exploiting vulnerabilities. They do illegal activities. They steal data and sell it their motives are to personal gain. They just want to make their own profit or benefit.

GREY HAT

A gray hat hacker is someone who may engage in hacking activities without malicious intent but without explicit authorization. Gray hat hackers operate in a morally ambiguous area between black hat and white hat hacking, and their actions can vary depending on the situation.

Information Security Overview

CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY (CIA TRIAD):

- **Confidentiality**: Ensures that sensitive information is only accessible to authorized individuals. Techniques like encryption and access controls protect confidentiality.
- **Integrity**: Guarantees that data remains accurate, complete, and unaltered during storage or transmission. Hashing and checksums are used to verify data integrity.
- **Availability**: Ensures that information and resources are available to authorized users when needed. Measures like redundancy, load balancing, and backups ensure availability.

The **CIA Triad** is the foundation of information security. Balancing these three principles helps protect systems from threats and ensures smooth business operations.

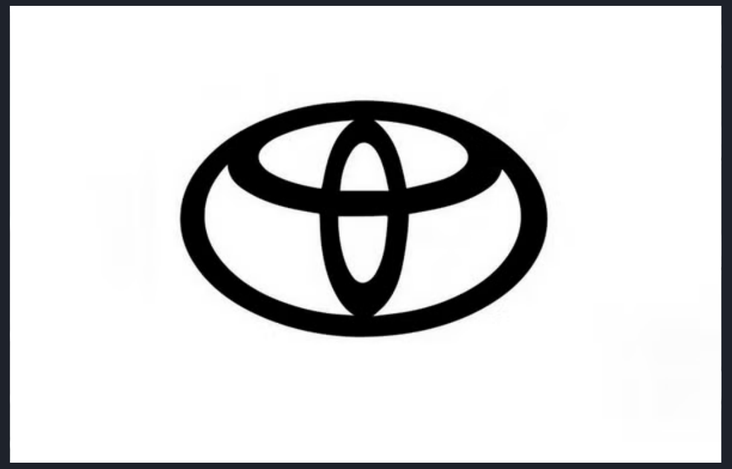
Importance of Information Security

- **Protects Sensitive Data**: Safeguards personal, financial, and business information.
- **Prevents Financial Loss**: Reduces costs associated with data breaches and cyber incidents.
- **Ensures Business Continuity**: Minimizes disruption and keeps operations running smoothly.
- **Maintains Compliance**: Helps meet legal standards and avoid fines (e.g., GDPR, HIPAA).
- **Builds Customer Trust**: Strengthens brand reputation by protecting client data.
- **Defends Against Cyber Threats**: Mitigates risks from malware, phishing, and hacking attempts.

CASE STUDIES OF RECENT BREACHES

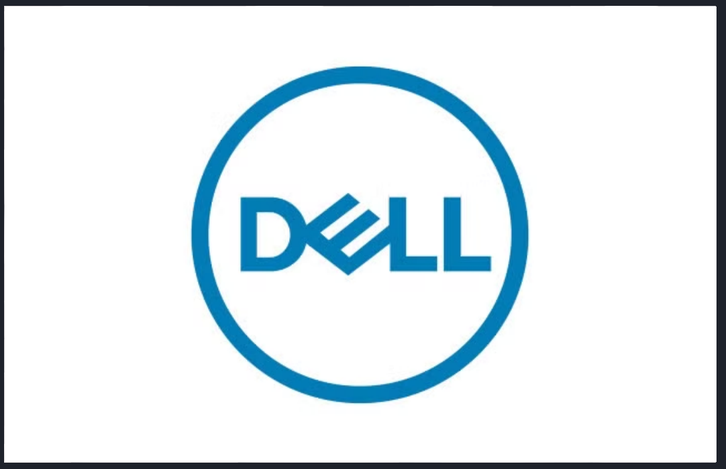
Wazirx

Indian cryptocurrency exchange WazirX has reported a substantial security breach leading to the loss of over $230 million in digital assets.



Toyota

Toyota has acknowledged a significant data breach of 240GB of customer information. The leaked data may include personal details such as names, addresses, contact information, and potentially sensitive financial data.



Dell

In May 2024, Dell was hit with a massive cyberattack that could affect their 49 million customers.

Information Security Threats and Attack Vectors

COMMON THREATS

- **Malware**: Malicious software that damages or disrupts systems.
- **Phishing**: Deceptive attempts to steal sensitive information.
- **Ransomware**: Blocks access to data until a ransom is paid.
- **DoS Attacks**: Overloads systems to disrupt services.

ATTACK VECTORS

- **Social Engineering**: Manipulating people to gain unauthorized access.
- **Software Vulnerabilities**: Exploiting weaknesses in applications.
- **Weak Passwords**: Easily guessed credentials leading to unauthorized access.

Wireshark Demonstration: Capturing and Analyzing Network Traffic

APPLYING FILTERS

- **Basic Filters**: Use Wireshark's filters to focus on specific types of traffic, such as:
  - http for HTTP traffic (e.g., browsing)
  - dns for DNS queries and responses
  - tcp.port == 80 or tcp.port == 443 for web traffic
- **Advanced Filtering**: Apply more complex filters to narrow down packets, such as ip.addr == [specific IP] to see all traffic associated with a specific IP address.

Tasks for Practice

1. **Capture** network traffic while browsing a website.
2. **Filter** for HTTP and DNS packets to observe the request-response cycle.
3. **Analyze** the packet details, identifying source and destination IPs and any unexpected responses.

Ethical Hacking Concepts

HACKING PHASES:

- **Reconnaissance**: Gathering information about the target.
- **Scanning**: Identifying open ports and services.
- **Gaining Access**: Exploiting vulnerabilities to access systems.
- **Maintaining Access**: Ensuring continued access to the system.
- **Covering Tracks**: Removing evidence of the attack to avoid detection.

Task: Vulnerability Scanning with Nmap (Practical Task)

> **Basic Nmap Scan**: Run the following command to scan a target machine's IP for open ports and services:
> `$ nmap -sV -O 192.168.1.1`

-sV: Detects version information of services running on open ports.

-O: Attempts to identify the operating system of the target.

Expected Output:

A list of open ports, services running on them, and possible OS detection. This information is crucial for determining which vulnerabilities could be exploited.

Task Goals:

- Understand how ethical hackers perform network reconnaissance.
- Learn how to interpret scan results to identify potential vulnerabilities for further testing.

Information Security Controls

Key Controls:

- **Preventive Controls**: Stop attacks before they happen (e.g., firewalls, strong passwords).
- **Detective Controls**: Identify and alert on attacks in progress (e.g., IDS/IPS).
- **Corrective Controls**: Respond to and fix issues after an attack (e.g., backups, patching).

Examples:

- **Firewall**: Blocks unauthorized access.
- **IDS/IPS (Intrusion Detection/Prevention Systems)**: Monitors and blocks suspicious activities.
- **Encryption**: Secures data from unauthorized access.

Configuring a Firewall Rule with iptables :

```
$ sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
```

This command allows incoming TCP connections on port 80 (HTTP traffic), effectively opening up access for web requests to the server on that port. It’s a basic rule commonly used to permit HTTP traffic on a web server

- **sudo**: Runs the command with superuser privileges, necessary for modifying firewall settings.
- **iptables**: The command-line utility for managing firewall rules on Linux.
- **-A INPUT**: Appends (-A) a rule to the INPUT chain, which applies to incoming network traffic.
- **-p tcp**: Specifies the protocol type, in this case, TCP (Transmission Control Protocol), which is commonly used for web traffic and other reliable connections.
- **--dport 80**: Defines the destination port to match, here port 80, which is used for HTTP (web traffic).
- **-j ACCEPT**: Specifies the action to "jump" (-j) to. ACCEPT allows the matching traffic to pass through the firewall.

Penetration Testing Concepts

TYPES OF PENETRATION TESTS:

- **Black-box**: Tester has no prior knowledge of the target environment.
- **White-box**: Tester has full knowledge, including network and system details.
- **Gray-box**: Tester has partial knowledge, simulating an internal threat.

PHASES OF PENETRATION TESTING:

- **Planning**: Defining scope, objectives, and legal permissions.
- **Discovery**: Gathering information and scanning for vulnerabilities.
- **Attack**: Attempting to exploit vulnerabilities identified in discovery.
- **Reporting**: Documenting findings, vulnerabilities, and recommended fixes.

INFORMATION SECURITY LAWS AND STANDARDS

GDPR (General Data Protection Regulation)

- Applies to EU member states.
- Aims to protect the privacy and data rights of individuals, controlling how personal data is collected, stored, and used.
- Penalties for non-compliance are significant, incentivizing strict data security measures.

HIPAA (Health Insurance Portability and Accountability Act):

- U.S. legislation focused on protecting health information.
- Regulates the handling, storage, and transmission of Protected Health Information (PHI).
- Compliance includes implementing both physical and technical safeguards.

PCI-DSS (Payment Card Industry Data Security Standard):

- Developed by credit card companies to secure cardholder data.
- Requires regular security assessments and penetration testing for systems involved in processing payment card data.
- Non-compliance risks include financial penalties and damage to reputation.

ISO 27001 (International Organization for Standardization 27001):

- A global standard outlining the best practices for information security management systems (ISMS).
- Includes policies, procedures, and controls to mitigate information security risks.
- Certification is a recognized benchmark for information security practices across industries.

Footprinting and Reconnaissance

Footprinting is the process of gathering extensive information about a target's infrastructure to identify potential weaknesses, entry points, and attack surfaces. This initial phase in ethical hacking or penetration testing helps create a comprehensive profile of the target.

PURPOSE OF FOOTPRINTING:

- **Identify Vulnerabilities**: Discover weak points in security, such as exposed services, open ports, and misconfigurations.
- **Understand the Network Structure**: Learn about IP ranges, network infrastructure, firewall configurations, and the location of servers.
- **Map External Resources**: Gather information on web servers, domains, subdomains, DNS servers, and associated IP addresses.
- **Gather Key Details on Technology Stack**: Identify operating systems, application versions, and other tech stacks, which could be vulnerable to known exploits.

Types:

PASSIVE FOOTPRINTING:

Gathering data without direct interaction with the target, thus avoiding detection.

- Searching for publicly available information on search engines, social media, and public databases.
- Checking DNS records, performing Whois lookups, and reviewing archived versions of the target’s website.

ACTIVE FOOTPRINTING:

Interacting directly with the target to obtain information, which can raise the risk of detection. Examples include:

- Using tools like ping, traceroute, nmap for network scanning.
- Performing DNS queries using dig or nslookup to identify subdomains and IP addresses.

DNS Lookups Using Dig or Nslookup:

```
$ dig example.com
```

This command queries the DNS records for the target domain, revealing IP addresses and potential subdomains.

```
$ nslookup example.com
```

This command retrieves DNS information that can help understand the target's DNS infrastructure and related network details.

Footprinting is critical for building a strategic approach to penetration testing, as it reveals publicly accessible data that attackers could leverage for malicious purposes.

Footprinting through Search Engines, Web Services, and Social Networking Sites

SEARCH ENGINES:

Google Dorking: Leveraging advanced Google search operators to locate specific information.

- **Example**: intitle:"index of" "admin" to find exposed directories containing sensitive information.
- **Purpose**: Uncover exposed files, login pages, or vulnerable systems.

WEB SERVICES:

Shodan: A search engine for internet-connected devices.

- **Example**: Querying port:80 or country:"IN" on Shodan to locate publicly accessible devices.
- **Purpose**: Identify vulnerable IoT devices, web servers, and open ports in the target’s environment.

Practical Time

Google Dorking to Find Login Portals:

```
inurl:"admin" OR inurl:"login" -site:example.com
```

This query locates login pages across multiple websites, excluding a specific site, to demonstrate locating access points.

Web Services (Shodan):

```
product:"Apache" port:80
```

This query finds devices running the Apache web server on port 80. It can help identify vulnerable servers that may be misconfigured or outdated.

Website Footprinting

The process of gathering detailed information about a target website's technologies, content management systems (CMS), and subdomains to identify potential vulnerabilities.

KEY INFORMATION EXTRACTED:

- **Technologies**: Identify the web server, programming languages, and frameworks used.
- **Content Management Systems (CMS)**: Detect platforms like WordPress, Joomla, or Drupal.
- **Subdomains**: Discover additional domains associated with the target, which may expose other attack vectors.

Practical Time

WhatWeb: A command-line tool for identifying various web technologies.

```
$ whatweb example.com
```

Wappalyzer:

A browser extension that identifies technologies used on websites by analyzing HTTP headers and HTML.

- Install the Wappalyzer extension in a browser and navigate to the target website to see a summary of detected technologies.

Competitive Intelligence

The practice of gathering publicly available information about competitors to gain insights into their strategies, strengths, weaknesses, and potential vulnerabilities.

KEY AREAS OF FOCUS:

- **Market Positioning**: Understanding how competitors position themselves in the market.
- **Product Offerings**: Analyzing competitors' products and services, including pricing and features.
- **Marketing Strategies**: Examining competitors' marketing campaigns, social media presence, and customer engagement.

Whois, DNS, and Network Footprinting:

WHOIS LOOKUP:

A query that retrieves information about the registered owner of a domain name, including contact details and registration dates.

Command-line tool or web-based service to check domain ownership.

```
$ whois example.com
```

Displays registrant information, domain status, and expiration dates.

DNS Footprinting:

WHOIS LOOKUP:

The process of querying DNS servers to obtain information about a domain's structure and associated records.

A DNS enumeration tool that helps gather DNS records and perform zone transfers.

```
$ dnsrecon -d example.com
```

To identify subdomains, A records, MX records, and more.

Footprinting through Social Engineering

The art of manipulating individuals to obtain confidential information or influence their actions. It relies on exploiting human psychology rather than technical hacking techniques.

KEY TECHNIQUES:

- **Pretexting**: Creating a fabricated scenario to obtain information from the target.
- **Phishing**: Sending fraudulent communications that appear to come from a reputable source, typically via email, to trick individuals into revealing sensitive information.
- **Baiting**: Offering something enticing to lure victims into providing information or access.

Phishing Email Attack:

A user receives an email that appears to be from their bank, asking them to verify their account information due to suspicious activity.

KEY CHARACTERISTICS OF THE PHISHING EMAIL:

- **Urgency**: The email creates a sense of urgency, prompting the recipient to act quickly without thinking.
- **Generic Greetings**: Instead of using the recipient's name, it may start with "Dear Customer."
- **Suspicious Links**: The email contains links that lead to a fake website designed to look like the bank's official site.
- **Grammar Errors**: Many phishing emails contain spelling and grammatical errors.

How to Recognize a Phishing Email:

- **Check the Sender's Email Address**: Verify the sender's domain. Official communications will come from a company domain (e.g., @bank.com), not a generic email provider (e.g., @gmail.com).
- **Hover Over Links**: Before clicking, hover over any links to see the actual URL. If it looks suspicious or doesn’t match the intended website, do not click.
- **Look for Urgency and Threats**: Be wary of emails that insist on immediate action or threaten account suspension.
- **Contact the Company Directly**: If in doubt, contact the company directly using a known, official phone number or email address to verify the message's legitimacy.

Footprinting Tools

These tools assist security professionals in gathering information about a target organization, its network infrastructure, and potential vulnerabilities. They automate the process of information gathering and provide valuable insights.

SHODAN :

- A search engine for internet-connected devices. Shodan allows users to find devices based on specific search criteria, revealing their vulnerabilities and configurations.

  Use Case:

  Useful for identifying exposed devices and services in a target's network.

Countermeasures

Countermeasures are defensive techniques and strategies implemented to protect systems and networks from potential threats and attacks. These measures help to minimize vulnerabilities and enhance the overall security posture of an organization.

DEFENSIVE TECHNIQUES:

Using VPNs (Virtual Private Networks):

- **Purpose**: VPNs encrypt your internet connection, masking your IP address and making it difficult for attackers to intercept your data.
- **Benefit**: Provides anonymity and secures data transmission over public networks.

Removing Metadata:

- **Purpose**: Metadata in files (e.g., documents, images) can reveal sensitive information about the file's origin, creator, and editing history.
- **Benefit**: By stripping metadata, you reduce the risk of unintentionally leaking personal or sensitive information.

Footprinting Pentesting

The primary objective of footprinting penetration testing is to assess an organization’s exposure to potential threats and vulnerabilities. This involves gathering detailed information about the target's systems, networks, and applications to identify weaknesses that could be exploited by attackers. By understanding these vulnerabilities, organizations can implement appropriate security measures to mitigate risks and enhance their overall security posture.

KEY OBJECTIVES

- Identify publicly accessible information that could be used for an attack.
- Assess the organization’s digital footprint to understand the level of exposure.
- Recommend strategies to minimize risks associated with discovered vulnerabilities.

Performing a Shodan Search to Find Exposed Services:

In the search bar, enter specific queries to find exposed services.

```
"port:80"  # Finds devices with HTTP services
"port:22"  # Finds devices with SSH services
"default password"  # Searches for devices with default credentials
"Apache/2.4.7"  # Finds devices running this version of Apache
```

Review the results to identify devices and services that are publicly accessible and may be vulnerable. Pay attention to:

- IP addresses
- Open ports
- Device types
- Any banner information that may reveal software versions.

</>

Any Doubts ?

</>

Hope you Enjoyed the Session

THANK YOU FOR JOINING

Pitch

Want to make a presentation like this one?

Start with a fully customizable template, create a beautiful deck in minutes, then easily share it with anyone.

Create a presentation (It's free)