

CYBER SECURITY

ASSIGNMENT - 1



Edit with WPS Office

WHAT IS FOOT PRINTING

- Footp Footprinting means gathering information about a target system that 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. m



TYPES OF FOOTPRINTING

- There are two types of footprinting as following below.
- Active Footprinting: Active footprinting means performing footprinting by getting in direct touch with the target machine.
- Passive Footprinting: Passive footprinting means collecting information about a system located at a remote distance from the attacker.



INFORMATION GATHERED BY THE FOOTPRINTING

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



ARCHITECTURE OF FOOTPRINTING



Edit with WPS Office

WHAT IS DNS FOOTPRINTING

- DNS Footprinting is a technique that is used by an attacker to gather DNS information about the target system. DNS Footprinting allows the attacker to obtain information about the DNS Zone Data, which includes:
 - DNS Domain Names
 - Computer Names
 - IP Addresses
 - Network related information



Record	Description
A	A record is an address mapping record, also known as a DNS host record.
MX	The mail server record specifies an SMTP email server
NS	It specifies the authoritative Name Server.
CNAME	Conical Name record, a ias record used to alias a hostname to another hostname
SOA	Start of Authority is the authoritative Name server for the current DNS zone.
PTR	Pointer records. It allows a DNS resolver to provide an IP address and receive a hostname
TXT	Text Record, It contains machine-readable data such as DKIM.
HINFO	Host information record includes CPU type and OS
SRV	Service Records



RECONNAISSANCE

- Information Gathering and getting to know the target systems is the first process in ethical hacking. Reconnaissance is a set of processes and techniques (Footprinting, Scanning & Enumeration) used to covertly discover and collect information about a target system.
- During reconnaissance, an ethical hacker attempts to gather as much information about a target system as possible



TYPES OF RECONNAISSANCE

- Reconnaissance takes place in two parts

- ☒ Active Reconnaissance

- ☒ Passive Reconnaissance.

- ☒ ACTIVE: In this process, you will directly interact with the computer system to

gain information. This information can be relevant and accurate. But there is a risk of getting detected if you are planning active reconnaissance without permission. If you are detected, then system admin can take severe action against you and trail your subsequent activities.

- ☒ PASSIVE: In this process, you will not be directly connected to a computer system. This process is used to gather essential information without ever interacting with the target systems.



ADVANTAGES OF FOOTPRINTING

- Gathering the basic security configurations of a target machine along with network route and data flow.
- Identifying vulnerabilities in the target machine.
- Identifying which attack is handier to hack the target system.
- Assessing an organization's security posture.
- Identifying any security weaknesses and gathering contact information for system administrators and other users who may access sensitive data.
- Determining the security postures of the target.
- Acquiring precious data, for example, network blocks, explicit IP addresses, representative subtleties, etc



UNDERSTANDING ETHICAL HACKING

- Ethical Hacking, also referred to as “white hat hacking,” “Pen Testing,” or simply “ethical hacking,” plays a critical role in maintaining the security and integrity of computer systems and networks. It involves cybersecurity practices that use hacking tools and techniques to identify vulnerabilities and weaknesses in computer systems and networks with the primary objective of preventing unauthorized access to systems and sensitive data, protecting against cyber-attacks, and ensuring the security of an organization’s assets.



TYPES OF ETHICAL HACKING

- Black-box Testing
- White-box Testing
- Gray-box Testing
- Web Application Hacking
- Hacking Wireless Networks
- Social engineering
- System hacking
- Web server hacking



DIFFERENCE BETWEEN FOOTPRINTING AND RECONNAISSANCE

Characteristic	Footprinting	Reconnaissance
Goal	Gather information about a target system or organization	Gather information about a target system or organization and identify potential attack vectors
Techniques	Passive techniques, such as searching for information online	Active and passive techniques
Risk	Low risk of detection	Medium to high risk of detection





Edit with WPS Office