Module 01

Introduction to Ethical Hacking

Elements of Information Security

Information security is a state of well-being of information and infrastructure in which the possibility of theft, tampering, and disruption of information and services is low or tolerable

Confidentiality	Assurance that the information is accessible only to those authorized to have access
Integrity	The trustworthiness of data or resources in terms of preventing improper or unauthorized changes
Availability	Assurance that the systems responsible for delivering, storing, and processing information are accessible when required by the authorized users
Authenticity	Refers to the characteristic of a communication, document, or any data that ensures the quality of being genuine
Non-Repudiation	A guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message

Classification of Attacks

Passive Attacks	• Passive attacks do not tamper with the data and involve intercepting and monitoring network traffic and data flow on the target network • Examples include sniffing and eavesdropping
Active Attacks	• Active attacks tamper with the data in transit or disrupt the communication or services between the systems to bypass or break into secured systems • Examples include DoS, Man-in-the-Middle, session hijacking, and SQL injection
Close-in Attacks	• Close-in attacks are performed when the attacker is in close physical proximity with the target system or network in order to gather, modify, or disrupt access to information • Examples include social engineering such as eavesdropping, shoulder surfing, and dumpster diving
Insider Attacks	• Insider attacks involve using privileged access to violate rules or intentionally cause a threat to the organization's information or information systems • Examples include theft of physical devices and planting keyloggers, backdoors, and malware
Distribution Attacks	• Distribution attacks occur when attackers tamper with hardware or software prior to installation • Attackers tamper with the hardware or software at its source or in transit

Information Warfare

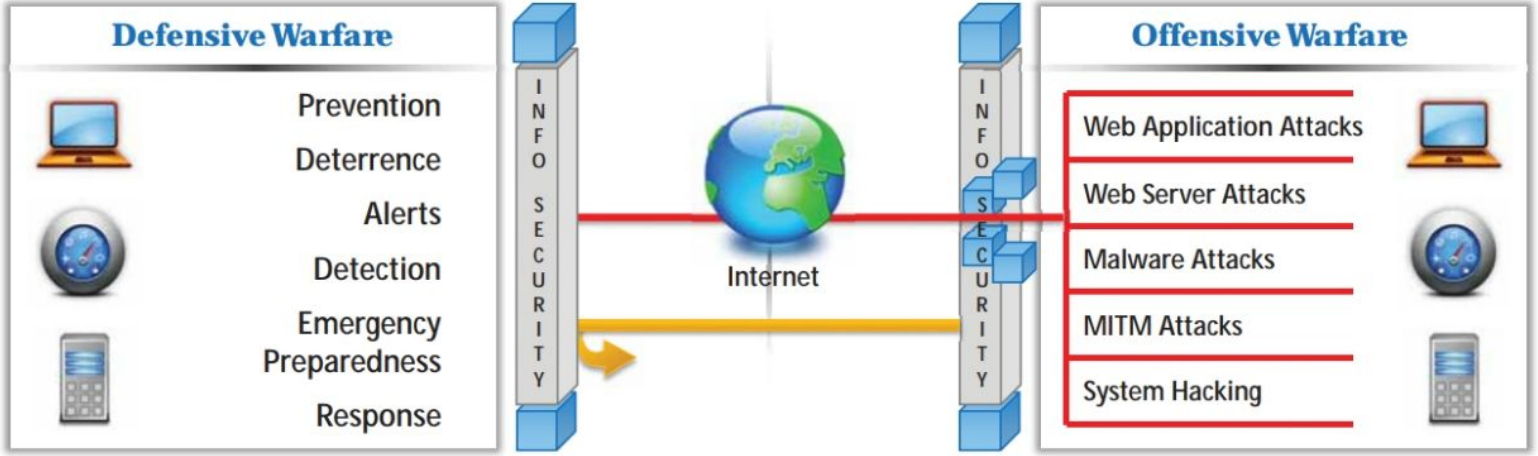
- The term information warfare or InfoWar refers to the use of information and communication technologies (ICT) to gain competitive advantages over an opponent

Defensive Information Warfare

Refers to all strategies and actions designed to defend against attacks on ICT assets

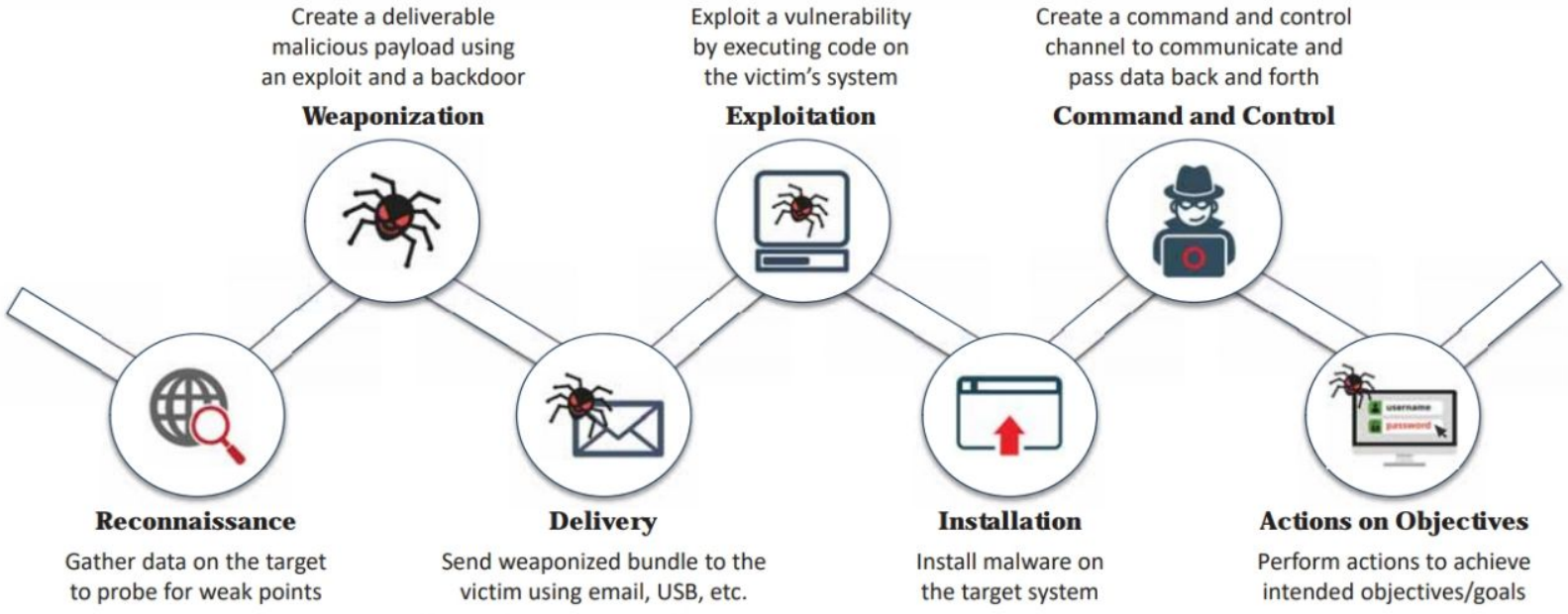
Offensive Information Warfare

Refers to information warfare that involves attacks against the ICT assets of an opponent



Cyber Kill Chain Methodology

- The cyber kill chain methodology is a component of intelligence-driven defense for the identification and prevention of malicious intrusion activities
- It provides greater insight into attack phases, which helps security professionals to understand the adversary's tactics, techniques, and procedures beforehand



Tactics, Techniques, and Procedures (TTPs)

The term Tactics, Techniques, and Procedures (TTPs) refers to the patterns of activities and methods associated with specific threat actors or groups of threat actors

Tactics

- "Tactics" are the guidelines that describe the way an attacker performs the attack from beginning to the end
- This guideline consists of the various tactics for information gathering to perform initial exploitation, privilege escalation, and lateral movement, and to deploy measures for persistent access to the system and other purposes

Techniques

- "Techniques" are the technical methods used by an attacker to achieve intermediate results during the attack
- These techniques include initial exploitation, setting up and maintaining command and control channels, accessing the target infrastructure, covering the tracks of data exfiltration, and others

Procedures

- "Procedures" are organizational approaches that threat actors follow to launch an attack
- The number of actions usually differs depending on the objectives of the procedure and threat actor group

Adversary Behavioral Identification

- Adversary behavioral identification involves the identification of the common methods or techniques followed by an adversary to launch attacks on or to penetrate an organization's network
- It gives the security professionals insight into upcoming threats and exploits

Adversary Behaviors

1 Internal Reconnaissance	4 Use of Command-Line Interface	7 Use of DNS Tunneling
2 Use of PowerShell	5 HTTP User Agent	8 Use of Web Shell
3 Unspecified Proxy Activities	6 Command and Control Server	9 Data Staging

Indicators of Compromise (IoCs)

- Indicators of Compromise (IoCs) are the clues, artifacts, and pieces of forensic data found on the network or operating system of an organization that indicate a potential intrusion or malicious activity in the organization's infrastructure

- IoCs are not intelligence, although they do act as a good source of information regarding the threats that serve as data points in the intelligence process

- Security professionals need to perform continuous monitoring of IoCs to effectively and efficiently detect and respond to evolving cyber threats

Categories of Indicators of Compromise

- Understanding IoCs helps security professionals to quickly detect the threats against the organization and protect the organization from evolving threats

For this purpose, IoCs are divided into four categories:

Email Indicators

- Email indicators are used to send malicious data to the target organization or individual
- Examples include the sender's email address, email subject, and attachments or links

Network Indicators

- Network indicators are useful for command and control, malware delivery, identifying the operating system, and other tasks
- Examples include URLs, domain names, and IP addresses

Host-Based Indicators

- Host-based indicators are found by performing an analysis of the infected system within the organizational network
- Examples include filenames, file hashes, registry keys, DLLs, and mutex

Behavioral Indicators

- Behavioral indicators of compromise are used to identify specific behavior related to malicious activities
- Examples of behavioral indicators include document executing PowerShell script, and remote command execution

Hacker Classes

01

Black Hats

Individuals with extraordinary computing skills; they resort to malicious or destructive activities and are also known as crackers

02

White Hats

Individuals who use their professed hacking skills for defensive purposes and are also known as security analysts. They have permission from the system owner

03

Gray Hats

Individuals who work both offensively and defensively at various times

04

Suicide Hackers

Individuals who aim to bring down the critical infrastructure for a "cause" and are not worried about facing jail terms or any other kind of punishment

05

ScriptKiddies

An unskilled hacker who compromises a system by running scripts, tools, and software that were developed by real hackers

06

CyberTerrorists

Individuals with wide range of skills who are motivated by religious or political beliefs to create fear through the large-scale disruption of computer networks

07

State-Sponsored Hackers

Individuals employed by the government to penetrate and gain top-secret information from and do damage to the information systems of other governments

08

Hacktivist

Individuals who promote a political agenda by hacking, especially by defacing or disabling websites

Hacking Phase: Reconnaissance

- Reconnaissance refers to the preparatory phase where an attacker seeks to gather information about a target prior to launching an attack
- This information could be the future point of return, noted for ease of entry for an attack, when more about the target is known on a broad scale
- The reconnaissance target range may include the target organization's clients, employees, operations, network, and systems

Reconnaissance Types

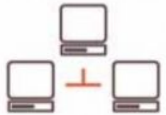
Passive Reconnaissance

- Passive reconnaissance involves acquiring information without directly interacting with the target
- For example, searching public records or news releases

Active Reconnaissance

- Active reconnaissance involves directly interacting with the target by any means
- For example, telephone calls to the target's help desk or technical department

Hacking Phase: Scanning

Pre-attack Phase	Scanning refers to the pre-attack phase when the attacker scans the network for specific information based on information gathered during reconnaissance 
Port Scanner	Scanning can include the use of dialers, port scanners, network mappers, ping tools, and vulnerability scanners 
Extract Information	Attackers extract information such as live machines, port, port status, OS details, device type, and system uptime to launch attack 

Hacking Phase: Gaining Access

1. Gaining access refers to the point where the attacker obtains access to the operating system or applications on the target computer or network

2. The attacker can gain access at the operating system, application, or network levels

3. The attacker can escalate privileges to obtain complete control of the system. In this process, the target's connected intermediate systems are also compromised

4. Examples include password cracking, buffer overflows, denial of service, and session hijacking

Hacking Phase: Maintaining Access

1. Maintaining access refers to the phase when the attacker tries to retain their ownership of the system

2. Attackers may prevent the system from being owned by other attackers by securing their exclusive access with backdoors, rootkits, or trojans

3. Attackers can upload, download, or manipulate data, applications, and configurations on the owned system

4. Attackers use the compromised system to launch further attacks

Hacking Phase: Clearing Tracks

1

Clearing tracks refers to the activities carried out by an attacker to hide malicious acts

2

The attacker's intentions include obtaining continuing access to the victim's system, remaining unnoticed and uncaught, and deleting evidence that might lead to their prosecution

3

The attacker overwrites the server, system, and application logs to avoid suspicion

Attackers always cover their tracks to hide their identity

What is Ethical Hacking?

- Ethical hacking involves the use of hacking tools, tricks, and techniques to identify vulnerabilities and ensure system security

- It focuses on simulating the techniques used by attackers to verify the existence of exploitable vulnerabilities in a system's security

- Ethical hackers perform security assessments for an organization with the permission of concerned authorities

Why Ethical Hacking is Necessary

To beata hacker, you need to think like one!

Ethical hacking is necessary as it allows for counter attacks against malicious hackers through anticipating the methods used to break into the system

Reasons why organizations recruitethical hackers

- To prevent hackers from gaining access to the organization's information systems
- To uncover vulnerabilities in systems and explore their potential as a security risk
- To analyze and strengthen an organization's security posture, including policies, network protection infrastructure, and end-user practices
- To provide adequate preventive measures in order to avoid security breaches
- To help safeguard customer data
- To enhance security awareness at all levels in a business

Why Ethical Hacking is Necessary (Cont'd)

Ethical Hackers Try to Answer the Following Questions

1. What can an intruder see on the target system? (Reconnaissance and Scanning phases)
2. What can an intruder do with that information? (Gaining Access and Maintaining Access phases)
3. Does anyone at the target organization notice the intruders' attempts or successes? (Reconnaissance and Covering Tracks phases)
4. Are all components of the information system adequately protected, updated, and patched?
5. How much time, effort, and money are required to obtain adequate protection?
6. Are the information security measures in compliance with legal and industry standards?

Skills of an Ethical Hacker

1 Technical Skills

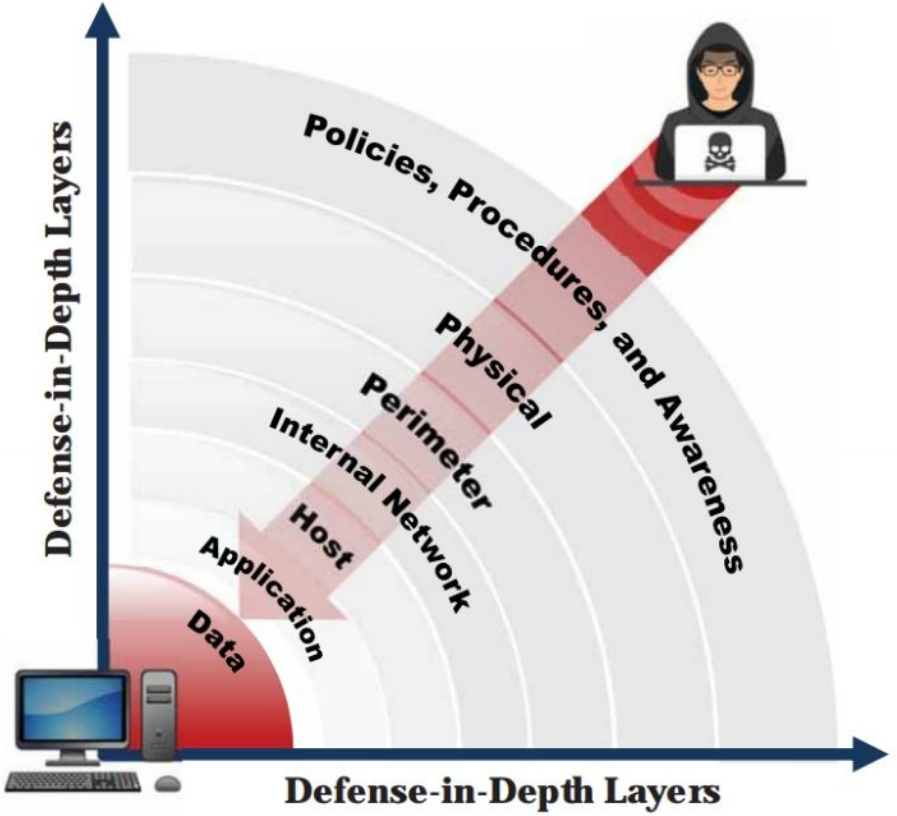
- In-depth knowledge of major operating environments such as Windows, Unix, Linux, and Macintosh
- In-depth knowledge of networking concepts, technologies, and related hardware and software
- A computer expert adept at technical domains
- Knowledgeable about security areas and related issues
- "High technical" knowledge for launching sophisticated attacks

2 Non-Technical Skills

- The ability to learn and adopt new technologies quickly
- Strong work ethics and good problem solving and communication skills
- Committed to the organization's security policies
- An awareness of local standards and laws

Defense-in-Depth

- Defense-in-depth is a security strategy in which several protection layers are placed throughout an information system
- It helps to prevent direct attacks against the system and its data because a break in one layer only leads the attacker to the next layer



What is Risk?

- Risk refers to the degree of uncertainty or expectation that an adverse event may cause damage to the system
- Risks are categorized into different levels according to their estimated impact on the system
- A risk matrix is used to scale risk by considering the probability, likelihood, and consequence or impact of the risk

Risk Levels

Risk Level	Action
Extreme or High	➢ Immediate measures should be taken to combat risk ➢ Identify and impose controls to reduce risk to a reasonably low level
Medium	➢ No urgent action is required ➢ Implement controls as soon as possible to reduce risk to a reasonably low level
Low	➢ Take preventive steps to mitigate the effects of risk

Risk Matrix

Probability			Consequences				
			Insignificant	Minor	Moderate	Major	Severe
81 - 100%	Likelihood	Very High Probability	Low	Medium	High	Extreme	Extreme
61 - 80%		High Probability	Low	Medium	High	High	Extreme
41 - 60%		Equal Probability	Low	Medium	Medium	High	High
21 - 40%		Low Probability	Low	Low	Medium	Medium	High
1 - 20%		Very Low Probability	Low	Low	Medium	Medium	High

Note: This is an example of a risk matrix. Organizations need to create their own risk matrix based on their business needs

Risk Management

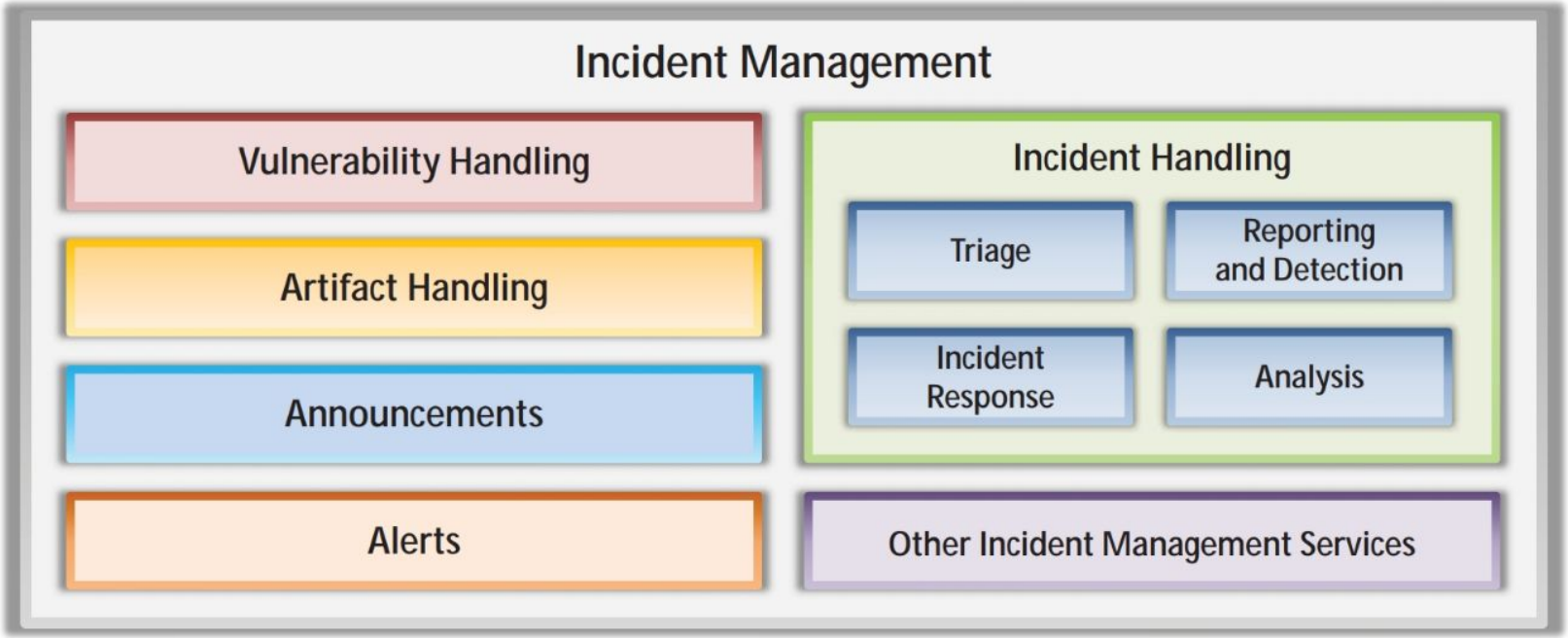
- Risk management is the process of reducing and maintaining risk at an acceptable level by means of a well-defined and actively employed security program

Risk Management Phases

Risk Identification	Identifies the sources, causes, consequences, and other details of the internal and external risks affecting the security of the organization
Risk Assessment	Assesses the organization's risk and provides an estimate of the likelihood and impact of the risk
Risk Treatment	Selects and implements appropriate controls for the identified risks
Risk Tracking	Ensures appropriate controls are implemented to handle known risks and calculates the chances of a new risk occurring
Risk Review	Evaluates the performance of the implemented risk management strategies

Incident Management

- Incident management is a set of defined processes to identify, analyze, prioritize, and resolve security incidents to restore normal service operations as quickly as possible and prevent future recurrence of the incident



Incident Handling and Response

- Incident handling and response (IH&R) is the process of taking organized and careful steps when reacting to a security incident or cyberattack

Steps involved in the IH&R process:

1. Preparation
2. Incident Recording and Assignment
3. Incident Triage
4. Notification
5. Containment
6. Evidence Gathering and Forensic Analysis
7. Eradication
8. Recovery
9. Post-Incident Activities
   - Incident Documentation
   - Incident Impact Assessment
   - Review and Revise Policies
   - Close the Investigation
   - Incident Disclosure

Payment Card Industry Data Security Standard (PCI DSS)

- The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle cardholder information for major debit, credit, prepaid, e-purse, ATM, and POS cards
- PCI DSS applies to all entities involved in payment card processing — including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process, or transmit cardholder data

PCI Data Security Standard — High Level Overview

Build and Maintain a Secure Network	Implement Strong Access Control Measures
Protect Cardholder Data	Regularly Monitor and Test Networks
Maintain a Vulnerability Management Program	Maintain an Information Security Policy

https://www.pcisecuritystandards.org

Failure to meet the PCI DSS requirements may result in fines or the termination of payment card processing privileges

Module Summary

- This module discussed elements of information security, information security attacks, and information warfare
- It discussed cyber kill chain methodology, TTPs, and IoCs in detail
- It also discussed hacking concepts, types, and phases
- This module also covered ethical hacking concepts such as the scope and limitations of ethical hacking, skills, and other pertinent information in detail
- It discussed information security controls such as defense-in-depth, risk management, cyber threat intelligence, threat modeling, incident management process, and AI and ML
- This module ended with a detailed discussion of various information security acts and laws from around the world
- The next module will go into detail about how attackers, as well as ethical hackers and pen testers, perform footprinting to collect information about the target of an evaluation before an attack or audit