Infosec Overview

Information security (infosec) is a vast field. The field has grown and evolved greatly in the last few years. It offers many specializations, including but not limited to:

- `Network and infrastructure security`
- `Application security`
- `Security testing`
- `Systems auditing`
- `Business continuity planning`
- `Digital forensics`
- `Incident detection and response`

In a nutshell, infosec is the practice of protecting data from unauthorized access, changes, unlawful use, disruption, etc. Infosec professionals also take actions to reduce the overall impact of any such incident.

Data can be electronic or physical and tangible (e.g., design blueprints) or intangible (knowledge). A common phrase that will come up many times in our infosec career is protecting the "confidentiality, integrity, and availability of data," or the `CIA triad`.

Risk Management Process

Data protection must focus on efficient yet effective policy implementation without negatively affecting an organization's business operations and productivity. To achieve this, organizations must follow a process called the `risk management process`. This process involves the following five steps:

Step	Explanation
`Identifying the Risk`	Identifying risks the business is exposed to, such as legal, environmental, market, regulatory, and other types of risks.
`Analyze the Risk`	Analyzing the risks to determine their impact and probability. The risks should be mapped to the organization's various policies, procedures, and business processes.
`Evaluate the Risk`	Evaluating, ranking, and prioritizing risks. Then, the organization must decide to accept (unavoidable), avoid (change plans), control (mitigate), or transfer risk (insure).
`Dealing with Risk`	Eliminating or containing the risks as best as possible. This is handled by interfacing directly with the stakeholders for the system or process that the risk is associated with.
`Monitoring Risk`	All risks must be constantly monitored. Risks should be constantly monitored for any situational changes that could change their impact score, `i.e., from low to medium or high impact`.

As mentioned previously, the core tenet of infosec is information assurance, or maintaining the `CIA` of data and making sure that it is not compromised in any way, shape, or form when an incident occurs. An incident could be a natural disaster, system malfunction, or security incident.

Red Team vs. Blue Team

In infosec, we usually hear the terms `red team` and `blue team`. In the simplest terms, the `red team` plays the attackers' role, while the `blue team` plays the defenders' part.

Red teamers usually play an adversary role in breaking into the organization to identify any potential weaknesses real attackers may utilize to break the organization's defenses. The most common task on the red teaming side is penetration testing, social engineering, and other similar offensive techniques.

On the other hand, the blue team makes up the majority of infosec jobs. It is responsible for strengthening the organization's defenses by analyzing the risks, coming up with policies, responding to threats and incidents, and effectively using security tools and other similar tasks.

Role of Penetration Testers

A security assessor (network penetration tester, web application penetration tester, red teamer, etc.) helps an organization identify risks in its external and internal networks. These risks may include network or web application vulnerabilities, sensitive data exposure, misconfigurations, or issues that could lead to reputational harm. A good tester can work with a client to identify risks to their organization, provide information on how to reproduce these risks, and guidance on either mitigating or remediating the issues identified during testing.

Assessments can take many forms, from a white-box penetration test against all in-scope systems and applications to identify as many vulnerabilities as possible, to a phishing assessment to assess the risk or employee's security awareness, to a targeted red team assessment built around a scenario to emulate a real-world threat actor.

We must understand the bigger picture of the risks an organization faces and its environment to evaluate and rate vulnerabilities discovered during testing accurately. A deep understanding of the risk management process is critical for anyone starting in information security.

This module will focus on how to get started in infosec and penetration testing from a hands-on perspective, specifically selecting and navigating a pentest distro, learning about common technologies and essential tools, learning the levels and the basics of penetration testing, cracking our first box on HTB, how to find and ask for help most effectively, common potential issues, and how to navigate the Hack the Box platform.

While this module uses the Hack The Box platform and purposefully vulnerable machines as examples, the fundamental skills showcased apply to any environment.

Next ➜

Mark Complete & Next

Cheat Sheet

Table of Contents

Types of Shells

Privilege Escalation

Transferring Files

Getting Started with Hack The Box (HTB)

Starting Out

Navigating HTB

Attacking Your First Box

Nibbles - Enumeration

Nibbles - Web Footprinting

Nibbles - Initial Foothold

Nibbles - Privilege Escalation

Nibbles - Alternate User Method - Metasploit

Problem Solving

Common Pitfalls

Getting Help

What's Next?

Next Steps

Knowledge Check

My Workstation

OFFLINE

Start Instance

1 / 1 spawns left