CyberDefense Pro - CySA+

Last updated: 5/13/2021

Course Outline

1. Introduction
2. Threat Intelligence
3. Risk Mitigation
4. Social and Physical Security
5. Reconnaissance
6. Enumeration
7. Vulnerability Management
8. Identity and Access Management Security (IAM)
9. Cybersecurity Threats
10. Infrastructure Security
11. Wireless and IoT Security
12. Infrastructure Analysis
13. Software Assurance
14. Data Analysis
15. Incident Response

Table of Contente

Contents

1. Introduction

2. Threat Intelligence

2.1 Penetration Testing and Threat Hunting

Penetration Test Process and Types

Penetration Test Process and Types Facts

This lesson covers the following topics:

- Penetration testing
- Types of penetration testing
- Penetration testing process

Penetration Testing

Cybersecurity professionals design and implement controls to secure resources. Once implemented, these controls should be considered a work in progress. Regular penetration testing (pen tests) can help ensure that the controls are working effectively and are continually updated. Key facts about penetration testing include:

- Penetration testing is the practice of finding vulnerabilities and risks with the purpose of securing the computer or network system.
- During pen testing, individuals attempt to break into a network or system using the same tools an attacker would use.
- To be most effective, pen tests are run by a security analyst or someone who is not involved in the security implementation processes.
- A penetration test helps to ensure a fresh look at potential weaknesses.
- If the pen tester can break into the system or find a way to cause damage, the appropriate security measures need to be taken to harden the system.

Types of Penetration Testing

The following table describes the three types of penetration testing.

Type	Description
Black box	The penetration tester has no information regarding the target or network. This type of test best simulates an outside attack and ignores the insider threats.
White box	The penetration tester is given full knowledge of the target or network. This test allows for a comprehensive and thorough test but is not very realistic.
Gray box	The penetration tester is given partial information about the target or network, such as IP configurations or emails lists. This test simulates an insider threat.

Penetration Testing Process

The following table describes steps in the penetration testing process

Step	Description
Planning	Before penetration testing begins, the test should be well planned and well documented. This helps to protect the organization and the tester. Document the following during the planning phase. • Timing - Determine when the penetration testing will occur. Consider whether it should be done during a time that would have less impact on daily operations. • Scope - Determine if the tester has full access to all systems. If not, specify the systems, networks, or accounts that the penetration tester does not have access to. • Authorization - Document the permission granted to the penetration tester to conduct the test. Ensure that authorization is documented before testing begins.
Information gathering	After planning is completed, the penetration testers start to collect information about the networks and systems that they are testing. Include the following sources to gather information from. • Organization's website or sales materials • Social engineering • Public records • Network scanning

	Include the following in the information gathered. • Users • Organizational hierarchy • Vendors • Operating systems • Hardware
Execution	Once the needed information is gathered, the pen tester can begin to execute the planned attack. The steps within this process can happen again and again in the same order or in a different order. The attack has the following four parts: • Access. • Privilege escalation. • System exploration. • Installation and use of pen testing tools.
Reporting	After any penetration test, a detailed report must be compiled. Documentation is an extremely important protection for the pen tester and the organization. The results of the test should be shared with network and system administrators so they can see the effectiveness of the current controls and where additional security measures need to be implemented.

Security Intelligence Cycle Facts

This lesson covers the topic of the security intelligence cycle.

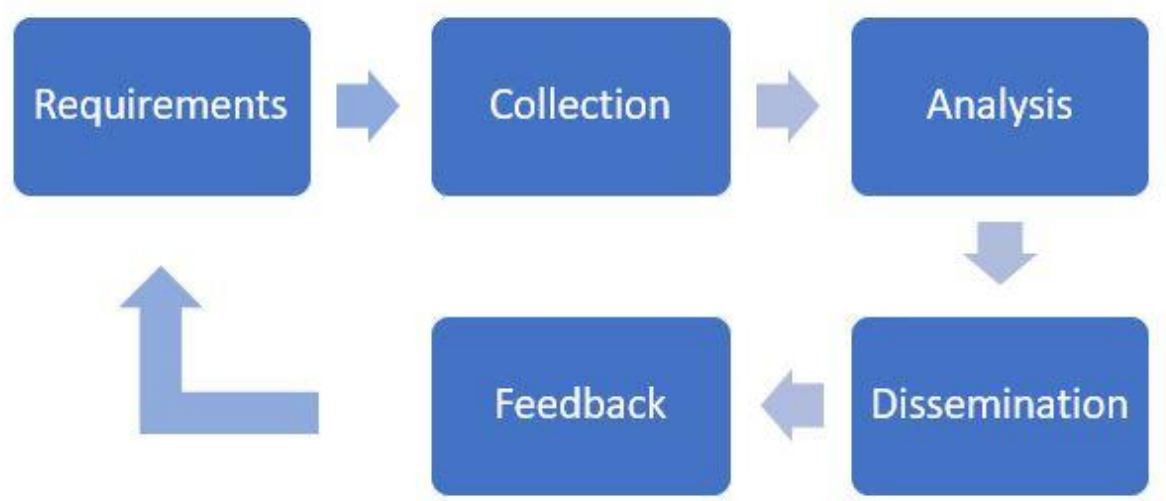
Security Intelligence Cycle

Knowing how and where to use threat intelligence can be challenging. Some organizations use the security intelligence cycle to provide a standard approach for managing their intelligence strategy. The following table describes the phases of the security intelligence cycle.

Phase	Description

Requirements	During the requirements phase, you determine what you need to obtain. These requirements can be driven by: • Recent attacks within your organization. • Risk assessment. • Current industry trends. During this phase you want to: • Verify that you have access to the data that you need. • Implement additional information gathering measures as needed. • Verify technical or regulatory restrictions.
Collection	Once you have determined the requirements, you move into the data collection phase. Data can be collected from: • System and application logs. • Open-source intelligence. • Closed-source intelligence. Because you are using multiple systems and sources, all data will be in different formats. To streamline the information into a form that can be analyzed, you must process it. This means organizing the data into a format that can be easily correlated, filtered, and searched.
Analysis	Once everything is in the same format, you are ready for the analysis phase. This phase requires much effort and attention to detail. Artificial intelligence and machine learning techniques have been improved and are being used in analytics software. Although some data can be normalized, filtered, and organized by software solutions, manual work is needed in most instances.
Dissemination	The next phase is to disseminate intelligence to members of your security team and members of your organization's leadership team. Dissemination can take place using status alerts, written reports, or other forms suitable to the intended audience. The same information should be presented differently depending on its intended use: • Strategic intelligence is information that impacts an organization's big picture objectives. These objectives could be driving business plans and priorities for the coming year.

	• Tactical intelligence helps security professionals to respond to incidents or to make security decisions. • Operational intelligence impacts the way managers plan day-to-day activities.
Feedback	Because you want to always improve your processes, feedback is essential. Always consider the feedback that you get from the reports that you sent out. This can help improve requirements in the next cycle. Feedback could include: • What was missed? Which incidents were not mitigated? • What was the quality of the intelligence sources? Which ones paid off and which ones should not be used again? • How can the life cycle can be improved next time?



Threat Actor Type Facts

Threat actors generally fall into categories based on their skills and motivations.

This lesson covers the following topics:

- Hacker types

- Threat actor types

Hacker Types

Hackers can be divided into three general categories:

Type	Description
White hat	This is a skilled hacker who uses skills and knowledge for defensive purposes only. A white hat hacker interacts only with a system to which explicit permission to access has been granted. These are ethical hackers.
Black hat	This hacker is also very skilled but uses knowledge and skills for illegal or malicious purposes. A black hat hacker is also known as a cracker. Black hat hackers are highly unethical.
Gray hat	The gray hat hacker falls in the middle of the white hat and black hat hackers. The gray hat may cross the line of what is ethical, but usually has good intentions and is not being malicious like a black hat hacker.

Threat Actor Types

Here are several types of threat actors:

Type	Description
Nation-state	A hacker who works for a government and attempts to gain top-secret information by hacking other governments.
Hacktivist	A hacker whose main purpose is to protest and express views and opinions. Hacktivists often deface websites or use denial-of-service attacks.
Criminal organization	Criminal organizations have transitioned many of their operations to a virtual setting. The internet provides a wider range of targets and provides additional options for obscuring their actions. Because criminals are often targeting individuals in multiple jurisdictions, prosecution can be difficult.

Internal – intentional	Internal intentional threats can include employees, vendors, or contractors who use their network access to access confidential information, or to hinder the availability of data or systems. The motivations for these insiders could include competitiveness, greed, or grievances against the organization. They could be acting on their own accord or recruited by someone on the outside.
Internal - unintentional	Internal unintentional threats are usually a result of a lack of training or laziness. Although these insiders don't intend to cause harm, their actions could result in unintentional weakened security points that could be used by intentional attackers. The best network security systems can be rendered useless if employees do not know how to use them effectively. Security training is critical for employees at all levels of an organization.

2.1 Section Quiz

2.1Section-quiz.pdf (wordpress.com)