2.4.2 Vulnerability Concerns Facts

A knowledgeable attacker can exploit network device vulnerabilities to gain access to network resources.

This lesson covers the following topics:

- Network Vulnerabilities
- Adversarial Artificial Intelligence

Network Vulnerabilities

The following table describes common network vulnerabilities.

Vulnerability	Description
Default accounts and passwords	Default accounts and passwords are factory defaults that are pre-configured for a new network device. Default account names and passwords should be changed immediately when hardware or software is turned on for the first time.
Weak passwords	Weak passwords are passwords that are blank, too short, dictionary words, or simple. In other words, they are passwords that can be quickly identified using password cracking tools. *Password cracking* is the process of recovering secret passwords from data that has been stored in or transmitted by a computer system. To avoid this vulnerability enforce complex password requirements. Complex passwords are typically over eight characters and a mix of character types (letters, numbers and symbols). Also require that the passwords are not words, variations of words, or derivatives of the user name.
Privilege escalation	Privilege escalation allows a user to take advantage of a software bug or design flaw in an application to gain access to system resources or additional privileges that aren't typically available to that user. Examples of privilege escalation include: ▪ A user who accesses a system with a standard user account but is able to access functions reserved for higher-level user accounts such as administrative features. ▪ A user who is able to access content that should be accessible only by a different user. ▪ A user with administrative access who can access content that should be available only to a regular user. Privilege escalation does *not* occur when a user is able to steal or hack administrator credentials and is therefore able to access administrative functions. Privilege escalation refers to accessing features with an account that normally should not have access to those features.
Backdoor	A *backdoor* is an unprotected access method or pathway. Backdoors: ▪ Include hard-coded passwords and hidden service accounts. ▪ Are often added during development as a shortcut to circumvent security. If they are not removed, they present a security problem. ▪ Can be added by attackers who have gained unauthorized access to a device. When added, the backdoor can be used at a future time to easily bypass security

	controls. ▪ Can be used to remotely control the device at a later date. ▪ Rely on secrecy to maintain security. To protect against backdoors, do not allow programmers to bypass security during development. Carefully examine the code before release to remove any traces of backdoors that might have been included.
Cloud-based and third-party systems	When dealing with cloud-based or other third-party systems, you need to make special provisions. If an organization is using a cloud-based system, that means the organization doesn't own the system and cannot legally provide permission for a penetration test to be carried out on that system. The penetration tester must make sure to get the explicit permission of the cloud provider before performing any tests. Other third-party systems can cause issues for the penetration tester. If systems are interconnected, such as in a supply chain, the penetration tester needs to ensure they do not accidentally access the third party's systems. The penetration tester can also discover vulnerabilities that affect the third party. In this scenario, the penetration tester should report findings to the client and let the client handle the reporting. As you identify threats and evaluate vulnerabilities, consider risks that can occur at any point in the company's supply chain. The chain typically includes those supplying raw materials; manufacturing products; and selling and distributing the products to end customers.
Inherent vulnerabilities	Identify inherent vulnerabilities or systems that lack proper security controls. For example, if your organization needs to use an older version of Windows for a particular application, then you should identify that system as a vulnerability. IoT and SCADA devices are both systems that lack proper security controls and must be dealt with appropriately.
Application flaws	Flaws in the validation and authorization of users present the greatest threat to security in transactional applications. When you assess this type of vulnerability, evaluate deployment and communication between the server and client. It is imperative to develop tight security through user authorization and validation. You can use both open-source and commercial tools for this assessment.
Misconfigurations	The primary cause of misconfiguration is human error. Web servers, application platforms, databases, and networks are all at risk for unauthorized access. Areas to check include outdated software, unnecessary services, incorrectly authenticated external systems, security settings that have been disabled, and debug enabled on a running application.
Root account	The root account has all system privileges and no barriers. It is also referred to as superuser. To prevent accidental damage to the system, an administrator using root must precisely and expertly perform tasks on the system. Also, the administrator should be the only one using the root account. Because there's no safety net when using root, it's important to make backups of any files or directories you're working with. Another danger of using root frequently is that most apps and programs have several programming errors (because of the amount of code required and its complexity). An

	attacker can find and exploit these errors to gain control of a system when a program runs with root privileges instead of an ordinary user account, which has very limited privileges. To avoid unnecessary risk, use the root account only when absolutely necessary. This includes experienced administrators. Have administrators log in with the admin account and use the su command. This command gives root privileges only as needed, without requiring a new login.

Adversarial Artificial Intelligence (AI)

Artificial intelligence (AI) refers is the simulation of human intelligence in machines that are programmed to think like humans and mimic their actions. AI also refers to any machine that exhibits traits associated with a human mind, such as learning and solving problems.

Be aware of the following about Artificial intelligence (AI):

- Refers to the simulation of human intelligence in machines.
- Goals include learning, reasoning, and perception.
- AI is used across different industries, including government and the private sector.
- Weak AI tends to be simple and single-task oriented, while strong AI carries on tasks that are more complex and human-like.

Adversarial Artificial Intelligence (AI) can be divided into two categories. weak and strong.

Depending on the source, some of the examples may be listed as weak, strong, or both.

Category	Description
Weak Artificial Intelligence	Weak artificial intelligence is usually designed to perform one particular job. It is also sometimes referred to as Narrow AI. Examples include: ▪ Simple video games (chess or checkers) ▪ Smart speakers ▪ Spam and web filtering ▪ Search engines ▪ Automated chats ▪ Image (facial) recognition ▪ Speech recognition
Strong Artificial Intelligence	Strong artificial intelligence systems are systems that carry out human-like tasks, which are typically complex. Strong AI include the ability to reason, make judgments, solve puzzles, learn, plan, and communicate. It is also sometimes referred to as Full AI. Examples include: ▪ Advanced video games ▪ Software that assists doctors in surgery ▪ Self-driving cars ▪ Disease diagnosis

Artificial intelligence includes many risks.

Risk	Description
Data	Data could be retracted from some data, but not others. For example, a patient's medical records may have the patient record retracted in one part of the record, but their name could be listed in another.
Technology	Issues with technology can cause AI to fail. For example, if not all data is looked at by AI, the results could have a negative feedback.
Interaction with humans	Accidents and injuries can occur when humans fail to take action or recognize when AI fails. For example, humans can rely on self-driving cars only to be involved in accidents for situations that AI is not able to deal with.
Security	Hackers can exploit the data that companies collect for AI. This can cause issues such as identity fraud.
Models	AI can unintentionally discriminate against a protected class of people. AI can be used for facial recognition and mistake the gender or race or misidentify people.