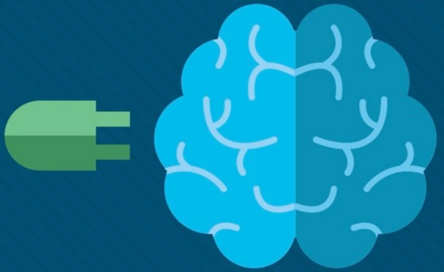


Chapter 8: Protecting the Network

Information Security

Dr. Ayman Aljarbouh

8.1 Understanding Defense

Module Objectives

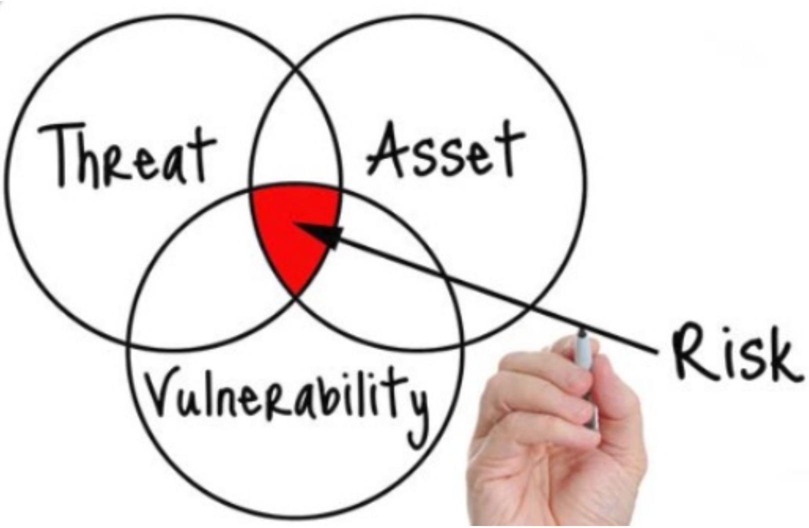
Module Title: Understanding Defense

Module Objective: Explain approaches to network security defense.

Topic Title	Topic Objective
Defense-in-Depth	Explain how the defense-in-depth strategy is used to protect networks.
Security Policies, Regulations, and Standards	Explain security policies, regulations, and standards.

Assets, Vulnerabilities, Threats

- Cybersecurity risk consists of the following:
  - **Assets** - Anything of value to an organization that must be protected including servers, infrastructure devices, end devices, and the greatest asset, data.
  - **Vulnerabilities** - A weakness in a system or its design that could be exploited by a threat.
  - **Threats** - Any potential danger to an asset.



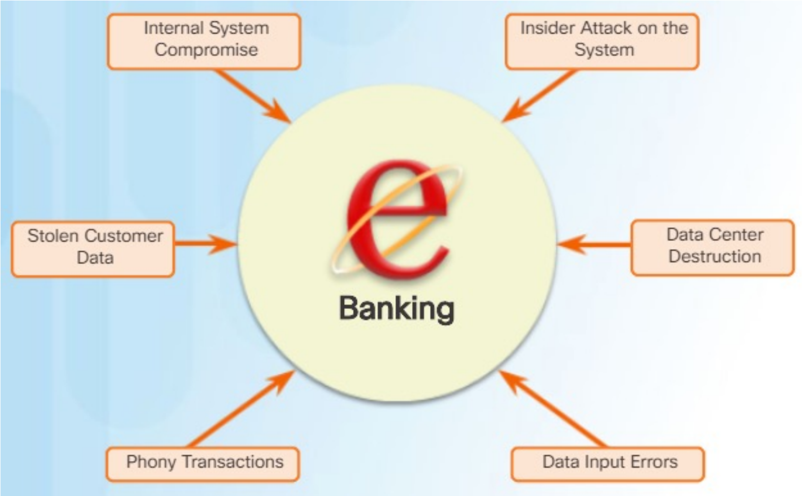
Identify Assets

- Many organizations only have a general idea of the assets that need to be protected.
- All the devices and information owned or managed by the organization are the assets.
- Assets constitute the attack surface that threat actors could target.
- Asset management consists of:
  - Inventorying all assets.
  - Developing and implementing policies and procedures to protect them.
- Identify where critical information assets are stored, and how access is gained to that information.

Defense-in-Depth

Identify Vulnerabilities

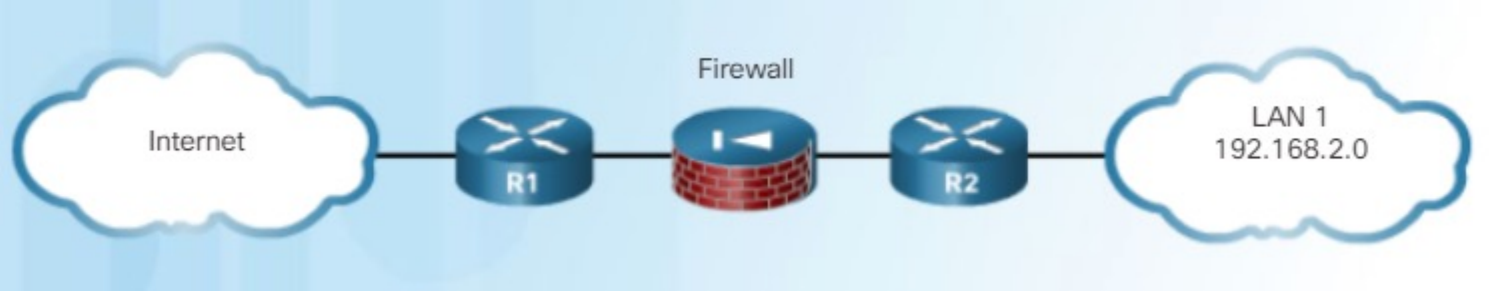
- Identifying vulnerabilities includes answering the following questions:
  - What are the vulnerabilities?
  - Who might exploit the vulnerabilities?
  - What are the consequences if the vulnerability is exploited?
- For example, an e-banking system might have the following threats:
  - Internal system compromise
  - Stolen customer data
  - Phony transactions
  - Insider attack on the system
  - Data input errors
  - Data center destruction



Defense-in-Depth

Identify Threats

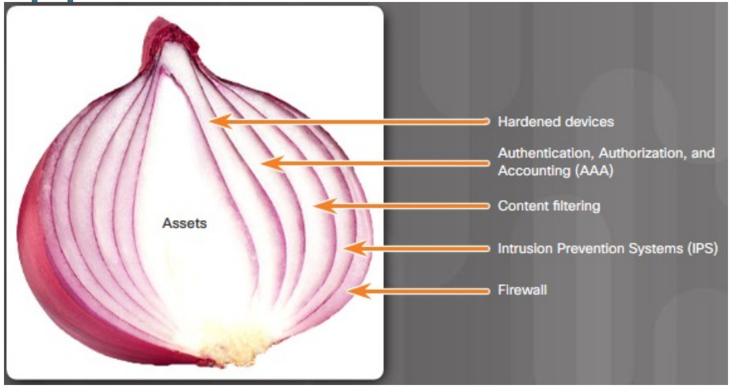
- Using a defense-in-depth approach to identify assets might include a topology with the following devices:
  - **Edge router** – first line of defense; configured with a set of rules specifying which traffic it allows or denies.
  - **Firewall** – A second line of defense; performs additional filtering, user authentication, and tracks the state of the connections.
  - **Internal router** – a third line of defense; applies final filtering rules on the traffic before it is forwarded to its destination.

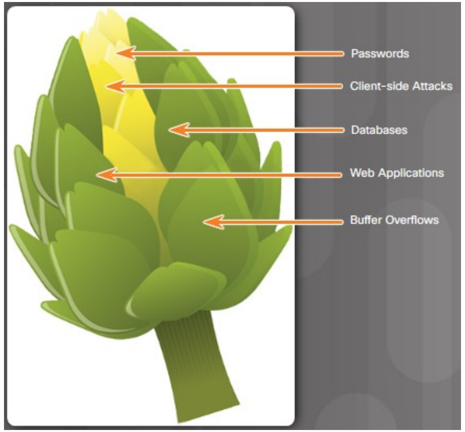


Defense-in-Depth

Security Onion and Security Artichoke Approaches

- The security onion analogy illustrates a layered approach to security.
- A threat actor would have to peel away at a network's defense mechanisms one layer at a time.
- However, with the evolution of borderless networks, a security artichoke is a better analogy.
- Threat actors may only need to remove certain "artichoke leaves" to access sensitive data.
- For example, a mobile device is a leaf that, when compromised, may give the threat actor access to sensitive information such as corporate email.
- The key difference between security onion and security artichoke is that not every leaf needs to be removed in order to get at the data.


Assets
Hardened devices
Authentication, Authorization, and Accounting (AAA)
Content filtering
Intrusion Prevention Systems (IPS)
Firewall



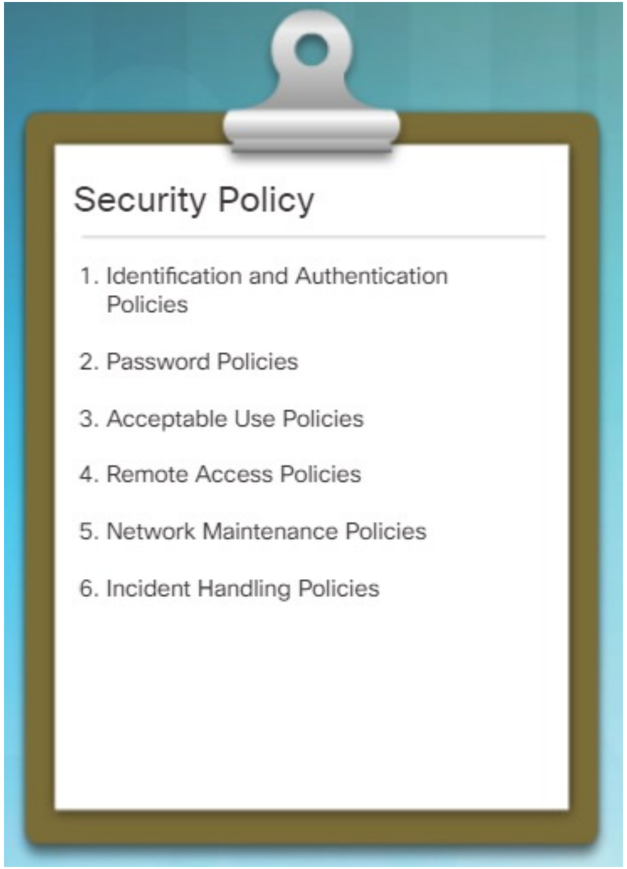
Business Policy

- Policies provide the foundation for network security by defining what is acceptable.
- Business policies are the guidelines developed by an organization that govern its actions and the actions of its employees.
- An organization may have several guiding policies:
  - **Company policies** - establish the rules of conduct and the responsibilities of both employees and employers.
  - **Employee policies** - identify employee salary, pay schedule, employee benefits, work schedule, vacations, and more.
  - **Security policies** - identify a set of security objectives for a company, define the rules of behavior for users and administrators, and specify system requirements.

Security Policies

Security Policy

- A comprehensive security policy has a number of benefits:
  - Demonstrates an organization’s commitment to security.
  - Sets the rules for expected behavior.
  - Ensures consistency in system operations, software and hardware acquisition and use, and maintenance.
  - Defines the legal consequences of violations.
  - Gives security staff the backing of management.
- A security policy may include one or more of the items shown in the figure.
- An Acceptable Use Policy (AUP) is one of the most common policies and covers what users are allowed and not allowed to do on the various system components.



Security Policy

1. Identification and Authentication Policies
2. Password Policies
3. Acceptable Use Policies
4. Remote Access Policies
5. Network Maintenance Policies
6. Incident Handling Policies

Security Policy (Contd.)

The following table lists the policies that may be included in a security policy:

Policy	Description
Identification and authentication policy	It specifies authorized persons that can have access to network resources and identity verification procedures.
Password policies	These ensure passwords meet minimum requirements and are changed regularly.
Acceptable use policy (AUP)	It identifies network applications and uses that are acceptable to the organization. It may also identify ramifications if this policy is violated.
Remote access policy	It identifies how remote users can access a network and what is accessible via remote connectivity.
Network maintenance policy	It specifies network device operating systems and end user application update procedures.
Incident handling procedures	These describe how security incidents are handled.

Security Policies

BYOD Policies

- Many organizations support Bring Your Own Device (BYOD), which enables employees to use their own mobile devices to access company resources.
- A BYOD policy should include:
  - Specify the goals of the BYOD program.
  - Identify which employees can bring their own devices.
  - Identify which devices will be supported.
  - Identify the level of access employees are granted when using personal devices.
  - Describe the rights to access and activities permitted to security personnel on the device.
  - Identify which regulations must be adhered to when using employee devices.
  - Identify safeguards to put in place if a device is compromised.

Security Policies

BYOD Policies (Cont.)

- The following BYOD security best practices help mitigate BYOD risks:
  - Password protected access for each device and account.
  - Manually controlled wireless connectivity so the device only connects to trusted networks.
  - Keep software updated to mitigate against the latest threats.
  - Back up data in case device is lost or stolen.
  - Enable “Find my Device” locator services that can remotely wipe a lost device.
  - Provide antivirus software.
  - Use Mobile Device Management (MDM) software to enable IT teams to implement security settings and software configurations on all devices that connect to company networks.

Regulatory and Standard Compliance

- Compliance regulations and standards define what organizations are responsible for providing, and the liability if they fail to comply.
- The compliance regulations that an organization is obligated to follow depend on the type of organization and the data that the organization handles.
- Specific compliance regulations will be discussed later in the course.

Protecting the Network

New Terms and Commands

- Assets
- Vulnerabilities
- Threats
- Edge router
- Internal router
- Security Onion
- Security Artichoke

- Defense-in-Depth
- Acceptable Use Policy (AUP)
- Mobile Device Management (MDM)
- Bring Your Own Device (BYOD)
- Security policies
- Company policies
- Employee policies

Lab 30 - Examining Telnet and SSH in Wireshark

In this lab, you will complete the following objectives:

- Examine a Telnet Session with Wireshark
- Examine an SSH Session with Wireshark