18.1 Defense-in-Depth

Understanding Defense

Assets, Vulnerabilities, Threats

- Cybersecurity analysts must prepare for any type of attack. It is their job to secure the assets of the organization's network.
- To do this, cybersecurity analysts must first identify:
  - **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 actor.
  - **Threats** - Any potential danger to an asset.

Understanding Defense

Identify Assets

- The collection of all the devices and information owned or managed by the organization are the assets.
- These assets must be inventoried and assessed for the level of protection needed to thwart potential attacks.
- Asset management consists of inventorying all assets, and then developing and implementing policies and procedures to protect them.
- This task can be daunting considering many organizations must protect internal users and resources, mobile workers, and cloud-based and virtual services.
- Further, organizations need to identify where critical information assets are stored, and how access is gained to that information.
- Information assets vary, as do the threats against them. Each of these assets can attract different threat actors who have different skill levels and motivations.

Understanding Defense

Identify Vulnerabilities

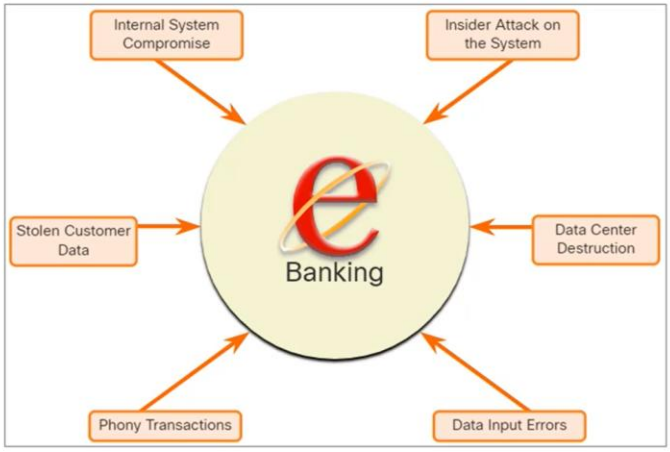
- Threat identification provides an organization with a list of likely threats for a particular environment.
- When identifying threats, it is important to ask several questions:
  - What are the possible vulnerabilities of a system?
  - Who may want to exploit those vulnerabilities to access specific information assets?
  - What are the consequences if system vulnerabilities are exploited and assets are lost?

Understanding Defense

Identify Vulnerabilities (Contd.)

The threat identification for an e-banking system would include:

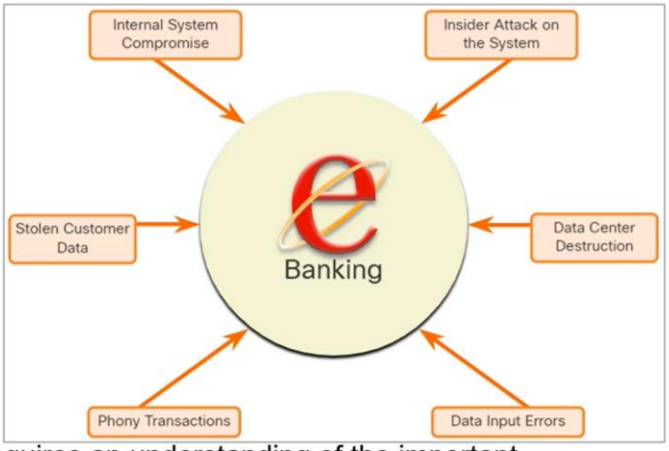
- **Internal system compromise** - The attacker uses the exposed e-banking servers to break into an internal bank system.
- **Stolen customer data** - An attacker steals the personal and financial data of bank customers from the customer database.
- **Phony transactions from an external server** - An attacker alters the code of the e-banking application and makes transactions by impersonating a legitimate user.



Understanding Defense

Identify Vulnerabilities (Contd.)

- **Phony transactions using a stolen customer PIN or smart card** - An attacker steals the identity of a customer and completes malicious transactions from the compromised account.
- **Data input errors** - A user inputs incorrect data or makes incorrect transaction requests.
- **Data center destruction** - A cataclysmic event severely damages or destroys the data center.



- Identifying vulnerabilities on a network requires an understanding of the important applications used as well as the different vulnerabilities of that application and hardware. This requires a significant amount of research on the part of the network administrator.

Understanding Defense

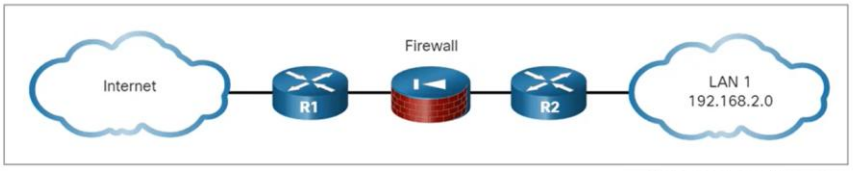
Identify Threats

- Organizations must use a defense-in-depth approach to identify threats and secure vulnerable assets.
- This approach uses multiple layers of security at the network edge, within the network, and on network endpoints.
- In this approach, a router first screens the traffic before forwarding it to a dedicated firewall appliance, for example, the Cisco ASA.
- Routers and firewalls are not the only devices that are used in a defense-in-depth approach.
- Other security devices include Intrusion Prevention Systems (IPS), advanced malware protection (AMP), web and email content security systems, identity services, network access controls and more.
- In the layered defense-in-depth security approach, the different layers work together to create a security architecture in which the failure of one safeguard does not affect the effectiveness of the other safeguards.

Understanding Defense

Identify Threats (Contd.)

- The figure displays a simple topology of a defense-in-depth approach:
  - **Edge router -** The first line of defense is known as an edge router (R1 in the figure). The edge router has a set of rules specifying which traffic it allows or denies. It passes all connections that are intended for the internal LAN to the firewall.
  - **Firewall -** A second line of defense is the firewall. The firewall is a checkpoint device that performs additional filtering and tracks the state of the connections. It denies the initiation of connections from the untrusted networks to the trusted network while enabling internal users to establish two-way connections to the untrusted networks.
  - **Internal router -** Another line of defense is the internal router (R2 in the figure). It can apply final filtering rules on the traffic before it is forwarded to its destination.



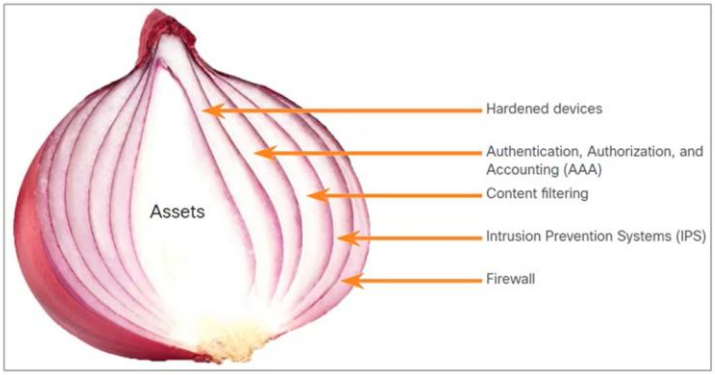
Understanding Defense

The Security Onion and The Security Artichoke

There are two common analogies that are used to describe a defense-in-depth approach.

Security Onion

- A common analogy used to describe a defense-in-depth approach is called "the security onion."
- As illustrated in figure, a threat actor would have to peel away at a network's defenses layer by layer in a manner similar to peeling an onion.
- Only after penetrating each layer would the threat actor reach the target data or system.



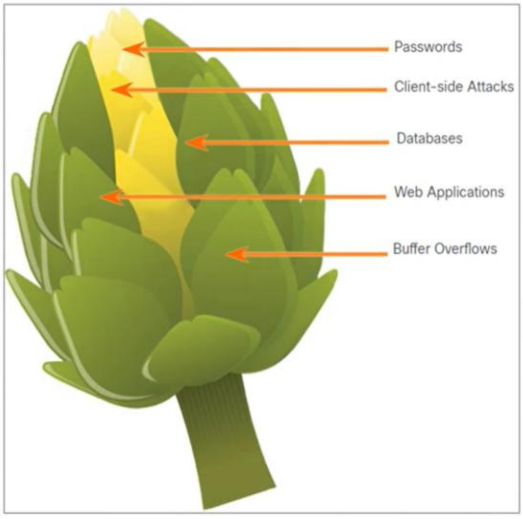
Note: *The security onion described on this page is a way of visualizing defense-in-depth. This is not to be confused with the Security Onion suite of network security tools.*

Understanding Defense

The Security Onion and The Security Artichoke (Contd.)

Security Artichoke

- The evolution of borderless networks has changed the analogy to the "security artichoke", which benefits the threat actor.
- As illustrated in the figure, threat actors no longer have to peel away each layer. They only need to remove certain "artichoke leaves."
- The bonus is that each "leaf" of the network may reveal sensitive data that is not well secured.
- In order to get at the heart of the artichoke, the hacker chips away at the security armor along the perimeter.
- While internet-facing systems are very well protected, persistent hackers do find a gap in that hard-core exterior through which they can enter.



18.2 Security Policies, Regulations, and Standards

Security Policies, Regulations, and Standards

Business Policies

- Business policies are the guidelines that are developed by an organization to govern its actions.
- The policies define standards of correct behavior for the business and its employees.
- In networking, policies define the activities that are allowed on the network.
- This sets a baseline of acceptable use. If behavior that violates business policy is detected on the network, it is possible that a security breach has occurred.

Security Policies, Regulations, and Standards

Business Policies (Contd.)

An organization may have several guiding policies, as listed in the table.

Policy	Description
Company policies	• It establishes the rules of conduct and the responsibilities of both employees and employers. • It protect the rights of workers as well as the business interests of employers. • Depending on the needs of the organization, various policies and procedures establish rules regarding employee conduct, attendance, dress code, privacy and other areas related to the terms and conditions of employment.
Employee policies	• These policies are created and maintained by human resources staff to identify employee salary, pay schedule, employee benefits, work schedule, vacations, and more. • They are often provided to new employees to review and sign.
Security policies	• These policies identify a set of security objectives for a company, define the rules of behavior for users and administrators, and specify system requirements. • These objectives, rules, and requirements collectively ensure the security of a network and the computer systems in an organization. • It is a constantly evolving document based on changes in the threat landscape, vulnerabilities, and business and employee requirements.

Security Policies, Regulations, and Standards

Security Policy

- Security policies are used to inform users, staff, and managers of an organization's requirements for protecting technology and information assets.
- A comprehensive security policy has a number of benefits, including the following:
  - 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 also specifies the mechanisms that are needed to meet security requirements and provides a baseline from which to acquire, configure, and audit computer systems and networks for compliance.

Security Policies, Regulations, and Standards

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, Regulations, and Standards

BYOD Policies

- Bring Your Own Device (BYOD) enables employees to use their own mobile devices to access company systems, software, networks, or information.
- It provides key benefits to enterprises, including increased productivity, reduced costs, better mobility for employees, and so on. These benefits also bring an increased security risk as BYOD can lead to data breaches and greater liability for the organization.
- Therefore, a BYOD security policy should be developed to accomplish the following:
  - 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, Regulations, and Standards

BYOD Policies (Contd.)

The following table lists the BYOD security best practices to help mitigate BYOD vulnerabilities:

Best Practice	Description
Password protect access	Use unique passwords for each device and account.
Manually control wireless connectivity	Turn off Wi-Fi and Bluetooth connectivity when not in use. Connect only to trusted networks.
Keep updated	Always keep the device OS and other software updated. Updated software often contains security patches to mitigate against the latest threats or exploits.
Back up data	Enable backup of the device in case it is lost or stolen.
Enable "Find my Device"	Subscribe to a device locator service with remote wipe feature.
Provide antivirus software	Provide antivirus software for approved BYOD devices.
Use Mobile Device Management (MDM) software	MDM software enables IT teams to implement security settings and software configurations on all devices that connect to company networks.

Regulatory and Standards Compliance

- There are also external regulations regarding network security.
- Network security professionals must be familiar with the laws and codes of ethics that are binding on Information Systems Security (INFOSEC) professionals.
- Many organizations are mandated to develop and implement security policies.
- Compliance regulations 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.

18.3 Understanding Defense Summary

What Did I Learn in this Module?

- The starting point for network defense is the identification of assets, vulnerabilities, and threats.
- Assets are anything of value to an organization that must be protected including servers, infrastructure devices, end devices, and the greatest asset, data.
- Vulnerabilities are weaknesses in a system or its design that could be exploited by a threat actor.
- Threats are any potential danger to an asset.
- Organizations must use a defense-in-depth approach to identify threats and secure vulnerable assets.
- Organizations must have a set of policies that define the activities that are allowed on the network.
- Business policies define standards of correct behavior for the business and its employees.
- Security policies are used to inform users, staff, and managers of an organization's requirements for protecting technology and information assets.
- The purpose of a BYOD (Bring Your Own Device) policy is to enable employees to use their own mobile devices to access company systems, software, networks, or information.
- The compliance regulations that an organization is obligated to follow depend on the type of organization and the data that the organization handles.