FORTINET Training Institute

FORTINET CERTIFIED SOLUTION SPECIALIST Security Operations

Security Operations Analyst

Attack Surface and Vectors

FortiAnalyzer 7.4

Last Modified: 22 January 2025

Lesson Overview

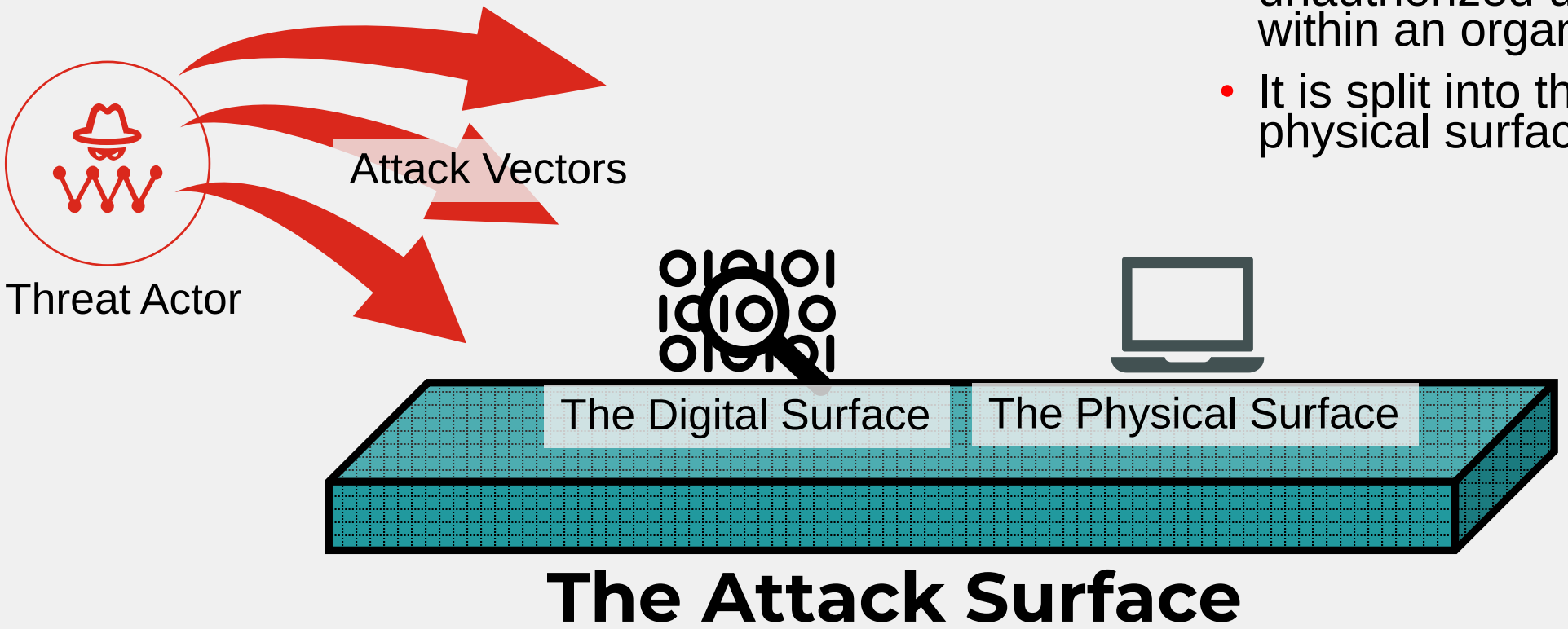
- The Attack Surface
- Attack Vectors
- Reviewing Traffic Flows

The Attack Surface

Objectives

- Describe the attack surface
- Describe how to identify the attack surface
- Describe how to reduce the attack surface

The Attack Surface—Introduction



- The attack surface encompasses all potential attack vectors that unauthorized users can exploit within an organization
- It is split into the digital and physical surfaces

Digital and Physical Attack Surfaces

Digital	Physical
Definition: • Encompasses all the hardware and software that connect to an organization's network	**Definition**: • Encompasses all devices that an attacker can gain physical access to
Applications and code	Desktop computers
IP addresses and ports	Laptops
Servers (such as web, database, email)	Hard drives
Websites	Mobile phones
Shadow IT	USB drives
VPN endpoints	Discarded hardware

Identifying the Attack Surface

- To determine your network's attack surface, you must have a complete picture of all the assets

- You can use an IT asset management software to track your assets, including:
  - Hardware
  - Software
  - IP addressing
  - Location
  - Licensing
  - Configurations
  - Patching
  - Lifecycle (end of support & end of life)
  - Inventory (asset tagging)

Reducing the Physical Attack Surface

- Restrict physical access to the building as much as possible
  - Limit employee access to only what they need
  - Employees should never hold open a door to a restricted area—prevents tailgating
- Do not allow visitors in working areas
  - Instead, have public areas and meeting spaces that are open to visitors
- Limit the use of removable media
  - USB drives, for example, can be used maliciously in many ways, such as exfiltrating data or installing malware
  - Employees may be baited into plugging in malicious devices
- Guard devices
  - Allow access to recycling areas only to authorized people
  - Thoroughly destroy discarded hard drives
  - Users should always lock their device before they leave their desk
  - Store unattended devices securely

Reducing the Digital Attack Surface

- Servers and network equipment are usually stored and racked in data centers with stricter access
  - They are *generally* more secure; they *should* be in a more secure location
  - As such, you can consider them part of the digital attack surface, since an attacker is less likely able to infiltrate data centers

- Remove unnecessary devices or services

- Segment the network
  - Macrosegmentation: Isolate different networks and VLANs from one another
  - Microsegmentation: Isolate the workloads of individual applications

- Fine-tune the level of access given to users and devices
  - Implement a zero-trust model

- Review logs and security events and incidents to find abnormal behavior

- Conduct SOC blue, red, and purple team exercises regularly

Knowledge Check

1. Which attack surface do USB drives belong to?
   - ✔ A. Physical
   - B. Digital

2. What is the definition of shadow IT?
   - ✔ A. Unauthorized devices and applications implemented by users.
   - B. Legacy devices and applications that are no longer actively managed.

Lesson Progress

- ✓ The Attack Surface
- Attack Vectors
- Reviewing Traffic Flows

Attack Vectors

Objectives

- Describe common attack vectors
- Describe security best practices against attack vectors
- Describe defenses against attack vectors

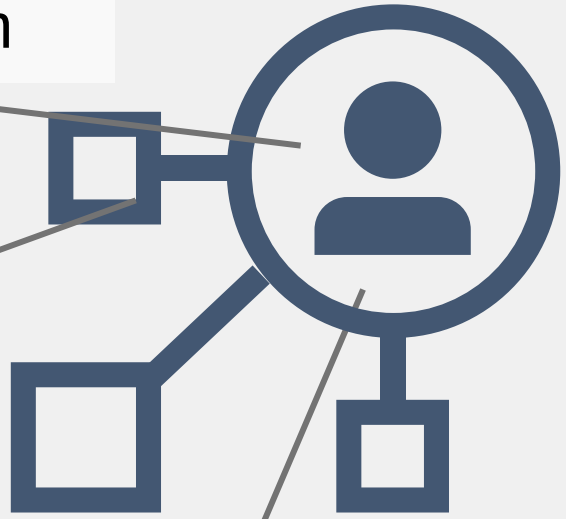
Attack Vectors Introduction

- As a SOC analyst, you should be able to identify attack vectors and formulate plans to defend them
- You can advise management with an action plan
- Attackers may follow a standard flow like the Cyber Kill Chain, or their steps can vary like the MITRE ATT&CK framework
- Attackers may have a specific goal in mind, which is dependent on the nature of the organization's business

Reconnaissance

- An attacker gathers information about a target **without directly interacting** with them

- Minor risk of detection

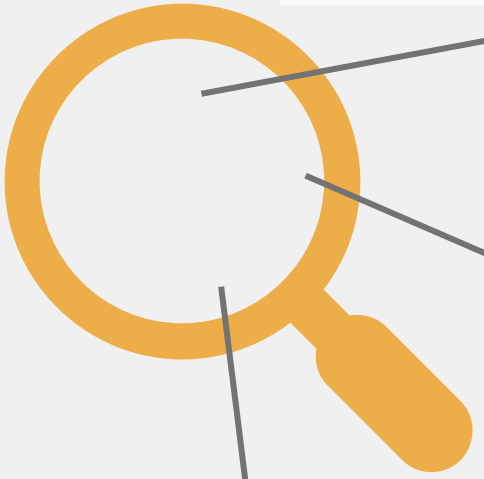


- Includes reading social platforms like Reddit, Facebook, Instagram, and LinkedIn

Passive

- An attacker gathers information about a target **by directly performing actions** on them

- Higher risk of detection

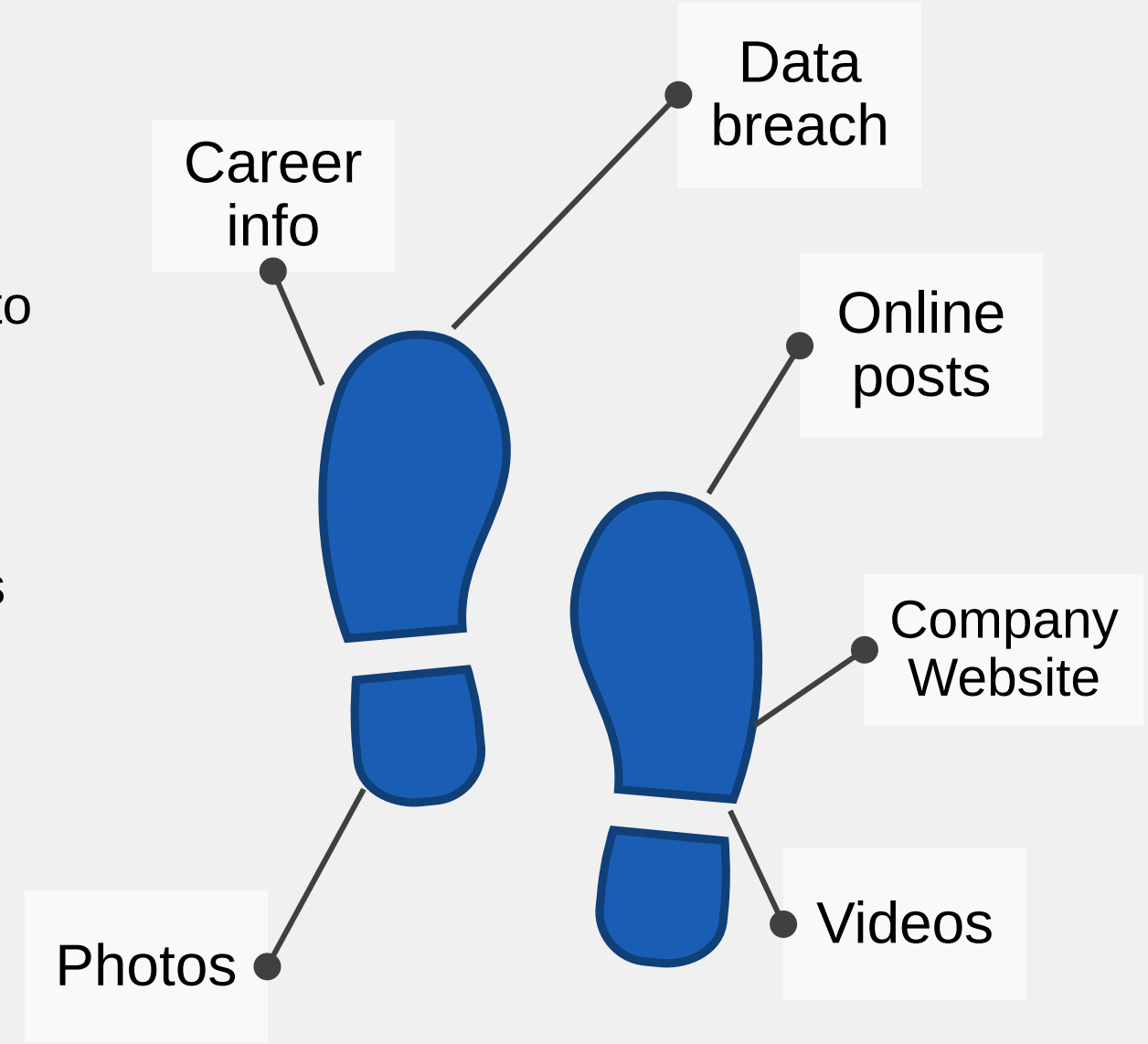


Active

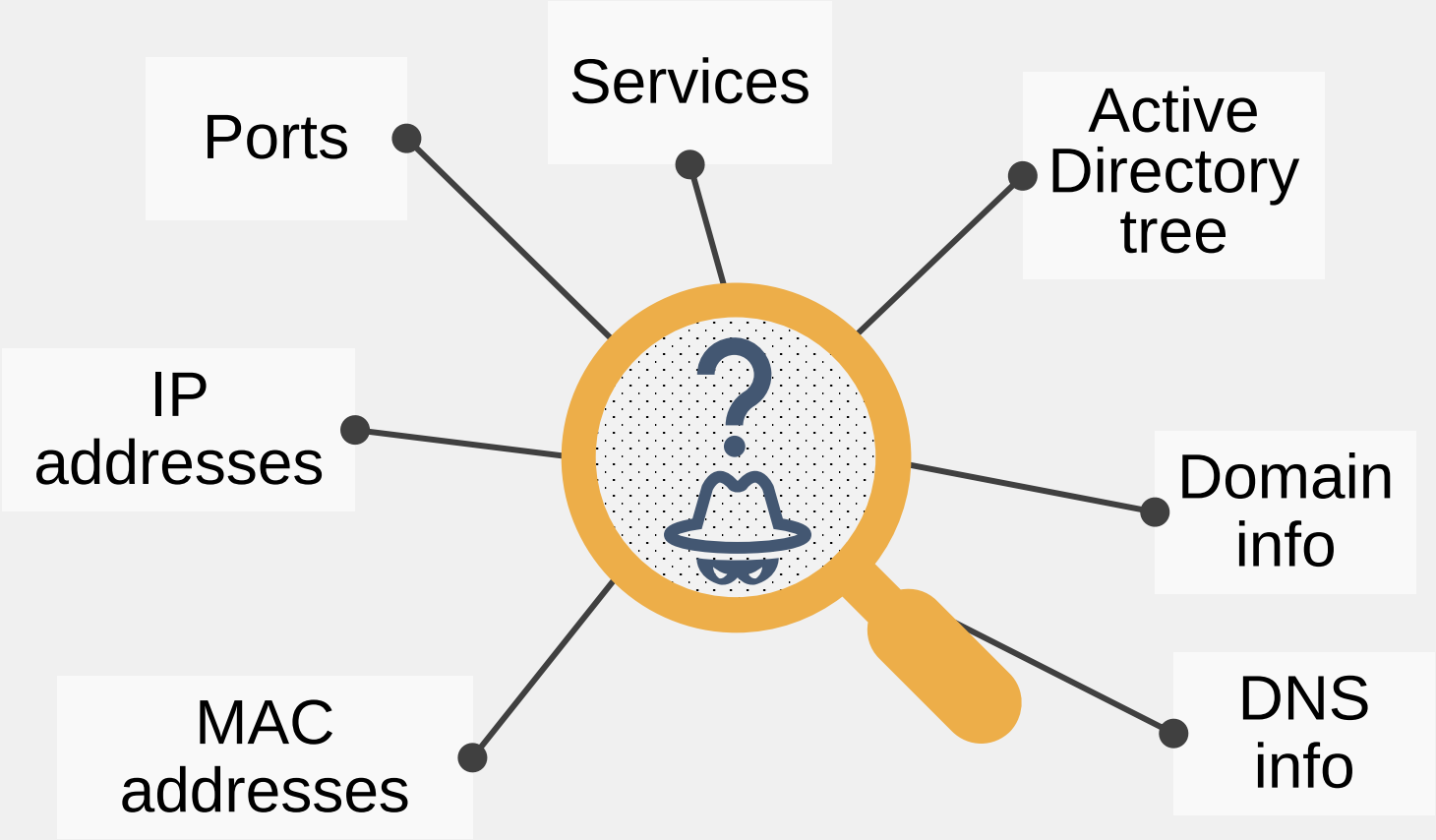
- Includes using tools like Nmap, Kali Linux, and DNS lookups

Passive Reconnaissance

- Your digital footprint is the trail of data you leave behind through your online activities
- Attackers can search through your profiles to gather information
- Your personal information can be used to spearphish or impersonate you, and access work resources



Active Reconnaissance



Review

- ✓ Describe the attack surface
- ✓ Describe how to identify the attack surface
- ✓ Describe how to reduce the attack surface
- ✓ Describe common attack vectors