

CompTIA.

CompTIA PenTest+

Exam PT0-002

CompTIA PenTest+ Exam PT0-002

Lesson 12



Attacking Specialized Systems

Objectives

- Explain common attacks and vulnerabilities against specialized systems.

Lesson 12

Topic 12A

Identify Attacks on the IoT

Understanding the IoT

- IoT devices are appliances with integrated computer functionality that includes apps, storage, and networking.
- Devices can be vulnerable to many of the standard attacks associated with web applications and network functions.
- Most have external connectivity to the wider world, along with many more "things" in between, which broadens the attack surface
 - Attacks can include buffer overflows, SQL injection, SYN flood, and privilege escalation.

Understanding Component Weaknesses

- Many IoT devices are an amalgamation of components from a variety of vendors, and can have several vulnerabilities
- Vulnerabilities can include:
 - Vendor patches and update processes can be inadequate.
 - Components could have preloaded malware or even backdoor access
 - The device might have insecure or even outdated components
 - Configurations that are hard-coded may be difficult or impossible to remove.

Vulnerable Targets

- Many IoT devices do not natively use encryption. As a result, any communication is transmitted in cleartext.
 - This can allow anyone to intercept and read or modify the contents.
- Devices lack physical security. Most are small, such as IP cameras, and can be placed in several areas, many in plain sight.
 - Unless access is restricted, these devices can be damaged or stolen.
- As a result, IoT devices must not be allowed on the network without a *process* in place to validate, manage, and monitor them.

Leaking Sensitive Data

- Many IoT devices use Bluetooth Low Energy (BLE), which can leak sensitive data.
- Malicious actors can capture data that is in cleartext and result in data leakage and expose the following:
 - The device model, software, and version, smart home activities
 - Gather e-mail addresses and phone numbers, and eavesdrop voice assistant commands

Triggering an Attack

- **Weaponizing an IoT Device**

- If a device is vulnerable, a malicious actor can infect a vulnerable IoT device with malware and then turn the device into a zombie.
- Once infected, the device will wait for instructions from the C&C server to launch a DDoS attack on a target.

- **Denial of Sleep attack**

- Continuously sends signals to the device preventing the rest cycle, which drains the battery.
- This leaves the device vulnerable to an attack.

Leveraging CoAP and MQTT


- **CoAP** works within a constrained network to transfer data in several different devices.
 - It doesn't have a way to provide security for group communication.
 - Some attacks to include coercive parsing, spoofing and packet amplification
- **MQTT** carries authenticated messages between devices
 - The data is not encrypted and can be vulnerable to an attack.
 - Some of the threats include sniffing, data modification, joining a botnet

Review Activity: Identify Attacks on the IoT

- Outline some reasons IoT devices represent a vulnerable target
- List some of the component weaknesses in IoT devices
- Explain why IoT devices should be tested prior to deployment
- Discuss how using BLE can lead to data leakage
- Describe some attacks on IoT devices
- Review how IoT protocols can represent a vulnerability

Lab Activity

Assisted Lab: Discovering IoT devices with Shodan

- Lab types
 - Assisted labs guide you step-by-step through tasks
 - Applied labs set goals with limited guidance
- Complete lab
 - Submit all items for grading and check each progress box
 - Select “Grade Lab” from final page
- Save lab 
 - Select the hamburger menu and select “Save”
 - Save up to two labs in progress for up to 7 days
- Cancel lab without grading
 - Select the hamburger menu and select “End”

Lesson 12

Topic 12B

Recognize Other Vulnerable Systems

Understanding Data Storage Systems

- In addition to cloud storage, an organization might have on-premises storage systems within a data center. Examples include:
 - **DAS** - is storage attached to a system, such as a hard drive
 - **NAS** - is a group of file servers attached to the network
 - **SAN** - is a separate subnetwork that houses a large amount of data.
- Because of the wide variety of options, it's essential to inventory and test storage systems during the PenTest.

Controlling Infrastructure

- An industrial control system (ICS) is any system that enables users to control industrial and critical infrastructure assets over a network.
- Many ICSs were established years before security standards were developed, and as a result, can be outdated and vulnerable.
 - If critical infrastructure resources are damaged or destroyed, this can result in a significant negative impact.
 - Additionally, as more systems are incorporated into an organization's network, there is greater chance for exploitation.

Securing Control Systems

- A SCADA system is a type of ICS that manages large-scale, multiple-site devices and equipment over large geographic areas
- The Industrial Internet of Things (IIoT), can optimize the way SCADA handles data.
 - IIoT is a complement to a SCADA system as it merges the control functionality with the data collecting ability of an IoT device.

Leaving Data Exposed

- In some cases, vulnerabilities exist as a result of human error along with improper or missing configurations.
 - For example, leaving the username and password as the default or blank
- Another issue that can expose a system to an attack is management interface vulnerabilities.
 - If the management interface is not correctly configured, this can expose the network, and provide the ability to have direct access to the data.

Handling Errors

- Error messages can help during the troubleshooting process.
- If there is too much detail in the message, this can expose user credentials, software version, and configuration settings.
- For example, the following provides the full pathname, which could lead to a Directory Traversal attack:
 - `warning.setText("WARNING: Could not connect to management server at " + fullpathname)`

Fuzzing the System

- Fuzzing sends a running application random and unusual input and monitor how the app responds.
- When setting up the fuzzer, the team can select what objects are to be tested, such as configuration files, source code, logs and archives
- Once activated, the fuzzer will search for objects and report the findings, such as the following:
 - `/example/login.php` - Admin login page/section found

Review Activity: Recognize Other Vulnerable Systems

- Review the different types of data storage systems
- Describe the significance of an industrial control system (ICS)
- Compare SCADA with and IIoT system
- Review ways misconfiguration can lead to data exposure
- Explain how error messages can be a vulnerability
- Outline why the team would use a fuzzer

Lesson 12

Topic 12C

Explain Virtual Machine Vulnerabilities

Using Virtualization

- Virtualization enables multiple operating systems to run simultaneously on a single computer.
- A virtual platform requires at least three components:
 - **Host hardware**—represents the platform that will host the virtual environment.
 - **Hypervisor/Virtual Machine Monitor (VMM)**—manages the virtual machine environment and facilitates interaction with the hardware and network.
 - **Guest operating systems** (Virtual Machines or instances)—represent the operating systems installed under the virtual environment.

Comparing Host-Based versus Bare Metal

- **Host-based** (Type II hypervisor) is installed onto a host OS
 - Any VMs are a guest and ride on top of the native operating system
 - Examples include VMware Workstation, Oracle Virtual Box, and Parallels
- **Bare metal** (Type I hypervisor) is installed directly onto the hardware and manages access without going through a host OS
 - Commonly used in an enterprise network.
 - Examples include VMware ESXi Server, MS Hyper-V, and Citrix's XEN Server.

Securing the VM Environment

- Managing a virtual environment takes place at two levels:
 - *Within the hypervisor*, which is the software or firmware that creates and manages virtual machines on the host hardware.
 - *Within the virtual machine*, which is a guest operating system installed on a host computer using a hypervisor, such as Microsoft Hyper-V or VMware.
- Each level introduces additional considerations:
 - Procedures include using security configuration templates, patch management, and inclusion in intrusion detection and audit regimes.

Avoid VM Sprawl and Protect the Repositories

- When VMs are poorly configured for security, they're exposed to many of the same threats as a physical machine.
- Situations that can make security issues more complex:
 - **VM sprawl** refers to creating VMs without proper change control procedures, which can create a vulnerable environment.
 - A **VM repository** stores VM templates or images. VM repositories that are compromised are called bad repositories.

Monitoring the Containers

- Containers provide an agile method of provisioning resources.
- Vulnerabilities commonly are related to misconfiguration issues
 - For example, improperly constructed images that contain non-essential software that can put the container at risk.
 - Any liberal configuration might allow a malicious actor to move laterally through a container environment.
- Any network policies should restrict access only to what is required for essential communication.

Attacking a Virtual Environment

- Virtual environments are designed to provide full isolation between guest and host operating systems.
- However, they can fall victim to an attack which can range in the type of attack and what environment is affected, as follows:
 - **Class 1** – the attack happens outside of the VM.
 - **Class 2** – the attack directly affects a VM.
 - **Class 3** – the attack originates within the VM and is the attack source.

Escaping a Virtual Environment

- **VM escape** is an attack where malware running in a VM can interact directly with the hypervisor or host kernel.
- For this attack to take place, the malicious actor must detect the presence of a virtualized environment.
 - The next step in is for the attacker to compromise the hypervisor.
- Preventing a VM escape attack is dependent on vendor identifying and patching security vulnerabilities in the hypervisor.
 - The impact of VM escaping can be reduced by using effective service design and network placement when deploying VMs.

Hyperjacking the Hypervisor

- Hypervisors are generally regarded as well-protected and robust. However, they can suffer from vulnerabilities as well.
- **Hyperjacking** is when a malicious actor takes control of the hypervisor that manages a virtual environment.
 - Once the malicious actor has taken control of the hypervisor, they will have all the required privileges and can take full control of the environment.
 - In addition, they will be able to access every VM along with the data and can then use any guest OS as a staging ground to attack other guests.

Review Activity: Explain Virtual Machine Vulnerabilities

- Describe the elements of a virtual platform
- Discuss the two levels securing a VM environment takes place
- Explain why it's essential to avoid VM sprawl
- Review reasons why it's important to protect the repositories
monitor the containers
- List the different classes of virtualized environment attacks
- Outline how VM escape can occur and the danger of Hyperjacking

Lesson 12



Summary