OT/SCADA Penetration Testing Methodology

55 Minutes Remaining

Instructions Resources Help  100%

# Module 11: OT/SCADA Penetration Testing Methodology

## **Objective**

The process of penetrating testing with ICS and SCADA is not the same as that of a normal IT pen test. With ICS/SCADA, penetration testers must determine the attack surface largely without sending data into the target, which results in a different type of process to follow for testing ICS and SCADA systems and, consequently, OT networks.

With this type of testing, penetration testers must ensure that they have accurate asset inventory and identification, this can be obtained from the client in the initial data call or from Open Source Intelligence gathering. SCADA penetration testing should be limited to test-bed or development systems and executed in a passive manner to avoid disrupting operations.

## **Scenario**

Industrial protocols have evolved over time from simplistic networks that collect information from remote devices to complicated networks of systems that have redundancy built into the devices. Protocols utilized inside industrial control systems are occasionally very specific to the application.

Over the years, many efforts have been made by standards organizations such as IEC, ISO, and ANSI to standardize protocols. There is an abundance of proprietary protocols as well. In most cases, these protocols are built by vendors to require specific software and hardware to create vendor-centric systems. Irrespective of the origin of the protocol, most industrial protocols have one aspect in common: they were not designed with security in mind and are inherently insecure.

This has become a significant problem since their convergence with IT networks and the now-dominant Transmission Control Protocol (TCP)/Internet Protocol (IP)-based protocols. Understanding these security flaws and how they are exploited is crucial for penetration testing and threat modeling in industrial control system (ICS) environments.