SEC568: Combating Supply Chain Attacks with Product Security TestingEmulation

5 Day Program	30 CPEs	Laptop Required

You Will Be Able To

- Conduct a product security test
- Reduce the impact of supply chain attacks on your organization
- Evaluate a Windows, Linux, or Android product for threats
- Perform basic static firmware analysis to understand what is running on a device
- Determine how a system changes because of installing new software
- Use Exploratory Data Analysis (EDA) techniques to analyze and present a large amount of data
- Dissect propriety protocols
- Build a threat model to articulate the biggest risks and mitigations
- Construct attack trees and use a risk scoring methodology to determine the risk of each threat discovered in previous phases

Prerequisites

- Basic Python coding skills
- Basic OS fundamentals
- Basic networking knowledge
- Understanding of core security principals
- Experience using VMware and virtual machines

Supply chain attacks go unnoticed on average for 235 days and do more damage as a result of us not having a deep understanding of the products being used on a network. Product security tests help obtain a comprehensive understanding of how choosing to use a particular product in your organization can increase your attack surface and affect your threat model and risk posture. This makes product security testing vital in preparing your organization to defend and recover from software supply chain attacks.

SEC568 is a practical on-ramp into the world of product security testing and risk analysis through more than 20 hands-on exercises designed to be challenging to both beginners and more advanced students. By utilizing offensive tactics with a defensive mindset, students will learn how to analyze the risk of introducing desktop, mobile, proprietary protocols, and hardware devices into your environment. You will use a wide variety of technical skills to gain a deep understanding of how a target operates.

Each section of the class will be accompanied by flow diagrams that provide each student a roadmap on how to navigate these complex topics with documented processes and clearly defined goals. As the class progresses, sections will increase in technical depth and difficulty. The number of hands-on exercises and the duration of them also increases proportionally as you gain new knowledge and develop new skills.

You will notice the class also gains a larger focus on networking as we dive deeper into product security testing. This networking focus is critical for a complete risk assessment in almost all organizations, as this threat vector has the highest likelihood to cause the most damage.

In the last section, the class culminates with a capstone event, a fully guided 5-hour exercise in which students will apply the entire product security testing process, starting with a closed-box analysis on a popular commercial application.

You Will Learn How To:

- Windows OS basics
- Linux OS basics
- Android OS basics
- Conduct efficient internet searching
- Networking fundamental concepts
- Decrypt networking traffic
- Build custom Scapy networking layers
- Collect, prepare, and analyze data with Python, Pandas DataFrame, and Jupyter Notebooks
- Know when to continue or stop a product security assessment
- Perform a variety of threat modeling concepts
- Identify different methods for determining risk
- Perform the basics of network fuzzing
- Analyze decompiled code

Section Descriptions

SECTION 1: Combating Supply Chain Attacks with Product Security Testing

The first section of this course describes the principles associated with both supply chain attacks and product security testing. We start to navigate the "why" and the "what" to product security testing, followed by which skills are important for success. We introduce our main methodology, our toolbox included in the supplied virtual machines, and the name of our fictious company you will be working for during the class, "Think Red, Act Blue." The main technical emphasis for section one will be to explore the basic, yet critical concept, of online product research followed by our first sections of basic enumeration and threat modeling. Through lectures and three hands-on exercises we will explore how to use simple tools such as binwalk, Corellium, APKLab, APKLeaks and associated product security methodologies to begin to understand how your target accomplishes its main goals. Students will be provided with access to a cloud-based mobile emulation platform (Corellium) to complete the last lab of this section.

TOPICS: Course Overview and Methodology; General and Software Supply Chain Application; Online Product Research; Basic Enumeration on Hardware Devices, Linux, and Android

SECTION 2: Basic Enumeration, Threat Modeling, and Intro to Deep Enumeration

The second section of the course will close out our study of basic enumeration by looking at the Windows platform and networking concepts that fit within the basic enumeration methodology. This will include using tools such as Microsoft Attack Surface Analyzer (ASA), Microsoft Sysinternal Suite, ProcDOT and more. This will allow for an in-depth conversation around the important role threat modeling plays in product security assessments and is a crucial first step to reducing the impact of supply chain attacks. Doing threat modeling and answering questions related to product security testing requires sifting through a large amount of data. In this section, we will introduce Exploratory Data Analysis (EDA), a common workflow to conduct analysis used to try to make sense of the data and present the results. Through lectures, demos, and hands-on exercises we will learn how to explore this data using data science tools like Python, Jupyter Notebooks, Pandas DataFrame, and graphical libraries like Matplotlib, among others. Lastly, this section will start segue into the course's deeper technical concepts by introducing deep enumeration.

TOPICS: Basic Enumeration on Windows; Basic Networking Analysis; Threat Modeling; Deep Enumeration

SECTION 3: Binary Code Analysis and Intro to Network Analysis

This section is all about deep enumeration, the process of deeper technical analysis to answer critical questions from a threat model. We will focus on two deep enumeration skills: binary code analysis and network analysis of unknown protocols. In the first half of Section 3, we will learn how to use decompiler tools to access the underlying code of an application and unpack archives when needed. This will culminate in a hands-on lab using JetBrain's dotPeek to answer critical questions related to supply chain attacks regarding how an application is being updated. Network traffic is often a key input to a system and a common entry point for attackers. To dive deeper into network analysis, this section will also take a pause to provide a primer into Scapy, a Python framework designed to manipulate networking packets. Armed with the knowledge and skills covered in this section, you will be better prepared to start dissecting proprietary or unknown protocols later in the course.

TOPICS: Binary Code Analysis; Scapy Primer; Understanding Proprietary Protocols

SECTION 4: Deep Network Analysis and Risk Analysis

This section will conclude our exploration of deep enumeration and work toward finalizing a product security test project. We begin with a continuation and finalization of dissecting proprietary protocols using Scapy to create custom layers and explain the basics of networking fuzzing. This will bring us to our final risk analysis section where we will focus on creating attack trees and applying risk scoring methods to assess the risk of supply chain attacks, among other risks to the Think Red, Act Blue organization. The section will conclude with important final topics that will allow us to wrap up our product security assessment, such as reporting and vulnerability disclosure.

TOPICS: Dissecting Proprietary Protocols; Fuzzing, Risk Analysis; Reporting; Vulnerability Disclosure

SECTION 5: Capstone Event

The course culminates in an all-day hands-on lab designed to give each student the experience of completing a product security test from start to finish. Students will be given a real application to test during this course section, which will apply the most crucial concepts learned throughout each previous section using the toolbox included in the supplied virtual machines and cloud-based labs.

TOPICS: Introduction to Target; Hands-on Product Security Testing Event; Instructor-led Discussion

Who Should Attend

- Network and systems penetration testers
- Application developers
- Security auditors
- SOC analysts, incident responders, and security engineers

NICE Framework Work Roles

- Cyber Defense Infrastructure Support Specialist (OPM 521)
- System Testing and Evaluation Specialist (OPM 671)

Author Statement

In our many years of experience conducting security assessments, we have observed the importance of being able to develop a holistic picture of the major areas of risk of an organization, while at the same time being prepared to zero-in on the risks introduced by a particular device or a specific product. However, the reality is that many organizations lack the knowledge and skills required to do a proper product security assessment. Some of these often rely on vulnerability scans that offer minimal information, with a focus on patching the systems evaluated and implementing generic security controls. Many others simply choose to ignore these threats altogether, closing their eyes to the reality and hoping for the best, while silently transferring the risk to their users, customers, and other stakeholders.

While it is true that threat actors still use unpatched vulnerabilities to obtain initial access into their victims, we are now seeing how attackers are more commonly using new methods of compromising software supply chains, undermining trust in the patching process by inserting malicious code into legitimate products. Think about it this way: Each time your organization deploys and installs new software on desktop, mobile, and cloud platforms, you can be creating new "holes" in your cyber defenses, from which sensitive data can leak.

We have designed this course to address this gap. Throughout five sections filled up with case studies, techniques, instructor-led demos and over 20 hands-on labs in realistic lab settings (including a final end-to-end capstone exercise), we will provide you with the knowledge and skills required to "Think Red, Act Blue" and combat these supply chain attacks employing product security testing. Our goal as authors is to make this class as practical and valuable to you and your organization as possible. To fulfil this promise, all the exercises we have created can be repeated at your own pace, both during and after class, and are thoroughly documented to maximize your learning experience.

Armed with the knowledge and skills we teach you in this class, you will obtain deep technical understanding of how product security testing works and how it can help mitigate the risks that any organization faces when it comes to supply chain attacks.

—Douglas McKee and Ismael Valenzuela