SEC661: **ARM Exploit Development**

2 Day Course	12 CPEs	Laptop Required

You Will Learn:

- Techniques for running ARM in an emulated environment
- The fundamentals of ARM assembly
- How to write ARM exploits to leverage stack-based buffer overflows
- Exploit mitigations and common workarounds
- How to work with ARM shellcode
- Return Oriented Programming (ROP)
- How to exploit IoT devices in ARM
- 64-bit ARM exploit development

Prerequisites:

- Familiarity with some type of assembly language is recommended. We will cover some of the basics in class, but any assembly experience would be a great head start.
- Working knowledge of the C programming language
- Familiarity with the Linux operating system, including navigating the file system and running basic commands, as well as using a console-based editor such as vim or nano.
- Ability to edit and run basic Python scripts

The Internet of Things (IoT) has taken over. Everywhere we look we see more systems coming online, from routers to refrigerators. But as these systems become more and more integrated into our home and business networks, how does their security posture keep up with their increasing popularity? The Advanced Reduced instruction set computing Machines architecture (ARM) introduced a new family of computer processors that provide a robust platform that is ideal for running a wide variety of small, specialized systems.

Unfortunately, the rapid expansion of new devices coming to market, along with accelerated development lifecycles, mean that security is often an afterthought. The security posture of many IoT devices is further restricted due to hardware limitations and the need to maintain low production costs.

Now more than ever, there is a demand for highly skilled security professionals who understand IoT vulnerabilities and ARM exploitation. However, the complexity of exploit development and the difficulty of acquiring and analyzing the software that runs on IoT systems can create intimidating barriers to those wanting to enter this field.

SEC661: ARM Exploit Development is designed to break down those barriers. It has been built from the ground up to give students a solid foundation in exploit development on the ARM platform. The course starts by going over the fundamentals of the architecture and some basic ARM assembly. Initial emphasis is placed on key data structures and how they work together so that students gain a better understanding of why certain vulnerabilities occur.

Students are provided with the tools they need to set up and work in an ARM environment. From there, we go through several hands-on labs that explore memory corruption vulnerabilities and show how to craft custom input in order to gain control of execution. We will also cover common exploit mitigations and techniques for bypassing them. Finally, students will demonstrate their understanding of the core concepts taught in this highly technical course by crafting their own exploits against two emulated ARM routers.

Author Statement

"If you have been looking to get into exploit development or are looking to grow and solidify your skills, this course was designed for you. ARM is taking the world by storm. With billions of new devices being introduced each year, understanding the fundamentals of security vulnerabilities in ARM and how they can be exploited is a valuable skill that will continue to be in high demand for years to come. My goal in writing this course is to ignite the passion within you and equip you with the skills you need to take you to the next level."

— John deGruyter

Section Descriptions

SECTION 1: ARM Exploit Fundamentals

Section 1 kicks off with an overview of ARM and how it differentiates itself from other architectures. Next, we dive into some common ARM assembly instructions and show how they interact with the system. With emulation, we are able to work directly in an environment where we can debug ARM programs and step through them one instruction at a time. We take an in-depth look at the stack and how it can be abused by vulnerabilities that allow an attacker to gain control of execution. We build upon this knowledge by writing our own ARM exploits for a couple of different scenarios. We close out section one by looking at different types of exploit mitigations and how they have changed the game for attackers.

TOPICS:

- Overview of the ARM architecture and how it affects us as both consumers and security professionals
- Cross-compiling ARM binaries and how the different steps of the build process are relevant to exploit development
- Format and common patterns in ARM assembly
- Tools and techniques for emulating ARM
- ARM analysis and debugging
- The Stack and how this important data structure is used and abused by exploit developers
- Stack Overflows, leveraging stack-based memory corruption in order to gain control of execution
- Exploit Mitigations and how they can be bypassed

SECTION 2: Exploiting IoT Devices

We begin Section 2 by looking at some ARM shellcode under the hood. We go over bad characters and different scenarios that might require modifying and reassembling shellcode. From there, we shift our focus to the Internet of Things (IoT) and start by extracting some firmware. We then analyze a Netgear exploit that was recently disclosed in 2020. Return-Oriented Programming (ROP) is covered in detail and we show how to find gadgets and build custom ROP chains. We then examine how this type of exploit can be used against an emulated Dlink router. Finally, we go over the differences between 32-bit and 64-bit ARM, stepping through some 64-bit ARM shellcode and using it to exploit a buffer overflow.

TOPICS:

- How shellcode works and how to modify it for custom exploits
- Common techniques for acquiring and analyzing firmware images
- In-depth analysis of a real world IoT exploit against Netgear devices
- How Return-Oriented Programming works, searching for gadgets and creating custom ROP chains
- In-depth breakdown of a vulnerability and exploit used to attack an emulated Dlink router.
- Similarities and differences of 64-bit ARM and leveraging what we ve learned on this platform

Who Should Attend

If you have wanted to get into ARM exploitation but didn t know where to start, this course was written for you. The course is a must for:

- Security researchers who are targeting IoT devices and other embedded systems.
- Software developers who are interested in building more secure systems and need a deeper understanding of security vulnerabilities.
- Former students of SANS SEC660: Advanced Penetration Testing and Exploit Writing who want to add ARM exploitation to their skillset.
- Penetration testers, red teamers, and other offensive operations professionals who want to learn how to weaponize discovered vulnerabilities on devices using ARM processors

SEC661 is designed to break down the complexity of exploit development and the difficulties with analyzing software that runs on IoT devices. Students will learn how to interact with software running in ARM environments and write custom exploits against known IoT vulnerabilities.