# SEC546: **IPv6 Essentials**

| 2 Day Course | 12 CPEs | Laptop Required |
|---|---|---|

### Author Statement

The first time I heard about IPv6, I heard about things like "unlimited address space", and "all your traffic will be encrypted". However, I knew little about the meaning of these statements. As I delved deeper into IPv6 and started to deploy it in some of my networks, I found that much of what was said about IPv6 was more myth than reality. Implementing IPv6, and in particular securing IPv6, turned out to be a much larger challenge then I originally planned. While many networks are already "IPv6 ready", you as a network administrator are likely not. This course should make you "IPv6 ready" as well.

— Dr. Johannes Ullrich

**"I have a much better understanding of IPv6, what it offers when implemented properly, and how to analyze traffic generated."**

— Bradley Hoover, **ExxonMobil**

We are out of IPv4 addresses. ISPs worldwide will have to rapidly adopt IPv6 over the next years to grow, in particular as mobile devices require more and more address space. Already, modern operating systems implement IPv6 by default. Windows 7, for example, ships with Teredo enabled by default. This course is designed not just for implementers of IPv6, but also for those who just need to learn how to detect IPv6 and defend against threats unintentional IPv6 use may bring.

IPv6 is currently being implemented at a rapid pace in Asia in response to the exhaustion of IPv4 address space, which is most urgently felt in rapidly growing networks in China and India. Even if you do not feel the same urgency of IP address exhaustion, you may have to connect to these IPv6 resources as they become more and more important to global commerce.

### The Security Impact of IPv6

Implementing IPv6 should not happen without carefully considering the security impact of the new protocol. Even if you haven't implemented it yet, the ubiquitous IPv6 support in modern operating systems easily leads to unintentional IPv6 implementation, which may put your network at risk. In this course, we will start out by introducing the IPv6 protocol, explaining in detail many of its features like the IPv6 header, extension headers and auto configuration. Only by understanding the design of the protocols in depth will it be possible to appreciate the various attacks and mitigation techniques. The course will address how to take advantage of IPv6 to re-think how to assign addresses in your network and how to cope with what some suggest is the biggest security problem in IPv6: no more NAT! IPv6 doesn't stop at the network layer. Many application layer protocols change in order to support IPv6, and we will take a close look at protocols like DNS, DHCPv6 and more.

### What You Will Learn

The course covers various security technologies like firewalls and Intrusion Detection and Prevention Systems (IDS/IPS). It also addresses the challenges in adequately configuring these systems and makes suggestions as to how apply existing best practices to IPv6. Upcoming IPv6 attacks are discussed using tools like the THC IPv6 attack suite and others as an example.

This course will introduce network administrators and security professionals to the basic concepts of IPv6. While it is an introduction to IPv6, it is not an introduction to networking concepts. You should understand and be aware of the basic concepts of IPv4, and networking in general. It is an ideal refresher if you took SEC503 Intrusion Detection in Depth. However, you do not need to know IPv4 in the full detail in which it is presented in SEC503. The networking and IPv4 principles taught in SEC401 Security Essentials should prepare you for this course.

## Available Training Formats

### Live Training

**Live Events**
sans.org/information-security-training/by-location/all

**Summit Events**
sans.org/cyber-security-summit

**Private Training**
sans.org/private-training