



VAST
VIPER Assessment Security Tools

VAST Course Outline



VAST Course Outline
Lasted updated: July 2010
© Copyright 2010 Siper Systems
PROPRIETARY AND CONFIDENTIAL

Introduction

UC promises new and exciting technologies. It provides benefits such as cost savings, increased productivity and efficiency. With these advantages will also come the risk of introducing new vulnerabilities into the existing corporate data network. Designed by the Siperia VIPER Lab, the VAST (VIPER Assessment Security Tools) training class addresses the need to properly understand VoIP / UC risks, perform a VoIP security assessment, and properly provide countermeasures and suggestions in order to remediate the VoIP and UC vulnerabilities found in a customer or partner network.

Course Objectives

The goals and objectives of the VAST class are as follows:

- ▶ Provide training for the student on how to use existing, open source IP Video and VoIP security tools in order to identify and validate vulnerabilities in a UC network.
- ▶ Training and education on UC vulnerabilities, their business impact, and how each vulnerability impacts the CIA (Confidentiality, Integrity, Availability) triad
- ▶ Education and knowledge on what types of security defenses and features are commonly found in UC deployments
- ▶ Training on how each UC vulnerability can be remediated, or otherwise protected against
- ▶ Provide a framework and technical methods for building a UC Security assessment methodology into existing data security practices
- ▶ The confidence and hands-on, technical experience to independently run a UC security assessment
- ▶ Learn tips and tricks for UC security analysis that VIPER team members have learned from running UC security assessments against production, enterprise networks.

How the class is organized

The VAST class is organized into “Modules.” Each VAST Module will cover a key concept, theory, or principle around UC Security. For a given module, the student will first receive a lecture by the instructor covering a specific security issue or protection measure found in production networks. Next, the student will receive an overview covering how the VoIP security tool can be used in order to defeat a specific feature, or how that tool can be used to validate and identify a specific security issue that is prevalent in production networks. In addition, the business impact of that finding will be explored. Finally, the student will end the module with being able to practice hands-on with the security tool against a production simulated UC deployment, thus uniting theory with practical methods. Each module is flexibly designed to allow the student additional lab time in order to practice the VoIP / UC specific attack, until they are comfortable and ready to move on to the next module.

The class is designed around the VIPER VAST (<http://vipervast.sf.net>) live DVD, a collection of open source security tools that are useful to a security assessment. Each student will have their own running instance of VAST on their laptop, and the instructor will lead the students on how to run each UC security tool. This method of combining theory with hands-on, practical experience against a real production deployment will give the student a security assessment methodology for running a successful UC security assessment. It will also give the students the confidence to have hands-on, technical experience in how to run a UC Security assessment. The design and objective behind this class is to quickly and comprehensively immerse the student in a UC Security Assessment Methodology: UC Security from a high-level, and down to the practical, hands-on. This will allow the students to create their own UC Security practice or run a very successful VoIP or IP Video security assessment independently.

Module Course Description: The information described below is a short description of the VAST (VIPER Assessment Security Tools) assessment modules, a loose, informal framework and description of test methods for penetration testing against a VoIP or IP Video network. The VAST Modules are based on the VAST Live DVD: <http://vipervast.sourceforge.net>. The information is developed by Siper Systems VIPER Lab, and is subject to change without notice.

Module 1: Voice VLANs

The first module will introduce students to VoIP and the Voice VLAN. Students will learn about the VLAN Hop vulnerability and how to run the "VoIP Hopper" tool in order to gain unauthorized access into the IP Phone network.

Module 2: Protecting with Port Security

In this module, students will be exposed to a common network security feature that Network Administrators have implemented in order to protect the VoIP network. The concept of MAC address filtering in the context of VoIP will be explored, and a tool for security testing will be demonstrated and tested in the lab.

Module 3: Protecting with 802.1x

After discussion of how to test for Port Security, students will learn about the 802.1x security feature of wired Ethernet networks, and how the feature is used with IP Phones in order to help provide strong network authentication in environments with low physical security. Students will learn about the XTest VIPER Lab tool, and how this tool can be used to enumerate vulnerabilities in 802.1x.

Module 4: Theft of VoIP Corporate Directory

This module will explore the concept of accessing potentially sensitive corporate data elements through VoIP. Students will learn how to run the "ACE" security assessment tool, and see how the VoIP corporate directory can be downloaded from the IP Phone in a corporate lobby,

and also leveraged for UC attacks against users in Active Directory or an LDAP server.

Module 5: VoIP Eavesdropping

Students will learn the business impact of classic VoIP Eavesdropping, and will get training on how to use the UCSniff tool in order to enumerate Eavesdropping vulnerabilities.

Module 6: UC Keystroke Logging

The UC Keystroke Logging module will demonstrate how DTMF digits in IP Phones can carry potentially sensitive information, such as voice mail passwords, and banking account information used in IVR applications. Students will learn about how this data can be carried over SIP trunks and line side control plane traffic. Students will learn how to use the UCSniff tool in order to demonstrate this vulnerability.

Module 7: IP Video Eavesdropping

This module will include lab time for how to intercept and playback Video conversations used with IP video applications such as those used by IP Phones and TelePresence.

Module 8: IP Video Interception, Recording, and Replay

This module will introduce students to the "VideoJak" IP video DoS and interception tool. Students will learn how to use this tool to test for targeted IP Video DoS against an IP video stream, including the ability to defeat an IP video surveillance camera solution.

Module 9: RealTime Audio and Video Monitoring

VoIP and IP Video are RealTime communications and extremely sensitive to degraded QoS. This module will introduce the concept of RealTime monitoring – a RealTime loss of confidentiality in IP Video conversations. UCSniff is the first security tool to be able to intercept and play both audio and video. Students will learn how to run this new

and exciting, practical UC attack vector, which was publicly demonstrated for the first time at the ToorCon security conference.

Module 10: Manually Verify Encryption

As a security professional, one cannot always rely on automated tools. This module addresses the need for security professionals to manually analyze a pcap network trace file, and know what to look for in order to verify that proper encryption is in place.

Module 11: Reconnaissance

Reconnaissance is the introductory module to the external modules. It will show the student how to remotely discover VoIP services over a public network. Additional techniques for service fingerprinting will be demonstrated in the lab portion of this module.

Module 12: User Enumeration

The "User Enumeration" module will show students the importance of identifying VoIP users, what tools can be used to achieve this goal, and why this goal is important to demonstrate to customers.

Module 13: DoS with Flooding and Fuzzing

The DoS module will explain the importance of high availability to UC, and how the business can be impacted by loss of available UC services. The lab portion of this module will provide the opportunity to use tools in order to enumerate DoS vulnerabilities.

Module 14: Toll Fraud

In the Toll Fraud module, the student will learn how toll fraud can take place against VoIP, including some lessons learned and experience from VIPER conducting security assessments related to toll fraud and financial breaches through VoIP. The students will be immersed in toll fraud technical methods and techniques. The last VAST module will conclude with the student being able to simulate a toll fraud attack over the public Internet, using combined tools and methods from previous modules.

Prerequisites

The VAST class requires each student to have the following:

- ✓ Exposure to the Linux Operating System or other Unix-based OS.
- ✓ Grasp of the TCP/IP protocol suite.
- ✓ Each student must bring to the training a laptop capable of running the VAST suite of tools.
- ✓ A minimum of one year experience performing network or application security assessments is strongly recommended.

Contact Us

Website: www.viperlab.net

Phone: +1.214.206.3210

Email: info@viperlab.net

