Courses Agenda and Details

Vulnerability Manager Training

(HT101) Network Vulnerability Assessment

Proactive vulnerability assessment training is the key to any organization's security posture. Constant assessment for potential weakness is required to maintain a security edge as new vulnerabilities in operating systems, software, hardware, and even human elements are identified and exploited every day. This course is designed to provide the fundamental knowledge necessary to comprehend the overall **host & network security** posture and the basic **practices in vulnerability assessment** course.

Course Agenda:

- System Fundamentals
- Network Fundamentals
- Common Perimeter Protections
- Wireless Assessment & Weakness
- Basic of Bash Scripting
- Infrastructure Information Gathering
- O.S. Fingerprinting
- System & Network Services
- Active System & Network Vulnerability Scanning
- User Credential Gathering
- Identify False Positive and Noise
- Vulnerability Impact Evaluation
- References & Tools

(HT102) Application Vulnerability Assessment

This course is designed to train participants to perform threat and vulnerability assessment, understanding the fundamental technical skills required to identify and prevent **application vulnerabilities**. You will also discuss about **methods to support secure software development**. This course is useful for security personnel and others who may be responsible for assessing and **managing the risk of threats to process** facilities.

Course Agenda:

- Application Fundamentals
- Basic of PHP, Perl and Python Scripting
- App Information Gathering
- App Protocols & Integrations
- App Services & Functions
- App Flow Charting
- Secure Software Development
- WEB Application Scanning
- Session Hijacking & Identity Theft
- Mobile Devices Vulnerabilities
- Application Vulnerability Scanning
- Vulnerability Analysis
- Vulnerability Impact Evaluation
- Risk Management, Incident Handling & Remediation Planning
- References & Tools

Code Engineer Training

(HT103) Vulnerability Detection and Exploitation

You will learn how to apply the theory and practice of **code auditing**, how to **dissect an application**, how to discover security vulnerabilities and assess the danger each vulnerability presents. You will **run vulnerability scans and observe exploits** to better secure networks, servers and workstations. This course is valuable for those involved in securing enterprise systems: network and system administrators, computer security personnel, officers with direct involvement in security and those involved in cybersecurity measures and implementation.

Course Agenda:

- Exploitation Techniques Fundamentals
- Public Vulnerabilities & 0-Days
- OWASP top 10
- Enterprise Defensive Security Solutions
- Think out of the box
- Set-Up the Lab
- Source Code Auditing
- Writing a simple Fuzzer
- Client Side VS Server Side Attacks
- Mobile Vulnerabilities & Weakness
- Execute Organized Attacks
- Remote Exploiting
- Modifying Exploit Code
- Web App Exploit Development
- Inject & Execute your code
- Mantaining Access
- References & Tools

(HT104) Reverse Engineering

The course builds a strong foundation for **reverse-engineering software using** a variety of system and network monitoring utilities, **a disassembler, a debugger** and other tools for turning software inside-out. You also learn how to **understand key characteristics of malware** discovered during the examination.

Course Agenda:

- Reverse Engineering Fundamentals
- Forensics Methods and Techniques
- Static vs. Dynamic Analysis
- Dealing with code Obfuscation & Encryption
- Building an analysis environment
- Network Traffic Analysis
- Memory Analysis
- Charting malware redirection
- Carving executables out of RAM
- Differences in Behaviors in Relation to the Environment
- Code Obfuscation & Encryption
- Disassembly & Debug
- References & Tools

Offensive Expert Training

(HT105) Network Penetration Test

You will learn proper planning, scoping and recon, and then **dive deep into scanning, target exploitation, password attacks, and wireless and web ap**ps with detailed **hands-on exercises** and practical tips for doing the job safely and effectively. You will finish up with an intensive, hands-on exercise in which **you'll conduct a penetration test** against a sample target organization, demonstrating the knowledge you mastered in this course.

Course Agenda:

- Preliminary skills
- Exploitation Fundamentals
- Wireless Cracking
- How to use pentester tools
- Information Gathering
- Initial Target Scanning
- Vulnerability Scanning
- Host Intrusion
- Web Application Attacks
- Wireless Crypto and Client Attacks
- Password based Attacks
- Advanced Bash Scripting
- References & Tools

(HT106) Application Penetration Test

Through detailed, **hands-on exercises** and training, you will be taught the **four-step process for Web application penetration t**esting. You will **inject SQL** into back-end databases, **learning how attackers exfiltrate sensitive data**. You will **utilize cross-site scripting** attacks to dominate a target infrastructure in our unique hands-on laboratory environment. And you will **explore various other Web app vulnerabilities** in-depth with tried-and-true techniques for finding them using a structured testing regimen.

Course Agenda:

- General Web Application Probing
- Enumeration, Vulnerability Assessment and Exploitation phases
- Input Validation
- Access Control
- Authentication and Session Management
- SQL Injections
- Cross-Site Scripting (XSS)
- Buffer Overflows
- Injecting Flaws
- Error Handling
- Insecure Storage
- Denial of Service
- Configuration Management
- Application Hacking
- Advanced Attack Vectors
- Advanced PHP, Perl and Python Scripting
- References & Tools