eLearnSecurity Certified Professional Penetration Tester (V2)

Course outline

Module 1: Introduction to Penetration Testing

Module 1: Introduction to Penetration Testing is an introductory course for the eLearnSecurity Certified Professional Penetration Tester (V2) course. It covers the fundamentals of penetration testing, including the different types of tests, the phases of a penetration test, and the tools and techniques used in the process. It also provides an overview of the ethical and legal considerations of penetration testing.

Lessons

- Introduction to Penetration Testing Methodologies
- Network Reconnaissance and Scanning
- Vulnerability Identification and Analysis
- Exploitation Techniques
- Post Exploitation and Privilege Escalation
- Web Application Penetration Testing
- Wireless Network Penetration Testing
- Social Engineering Penetration Testing
- Client-Side Attacks
- Reporting and Documentation

After completing this module, students will be able to:

- Understand the fundamentals of penetration testing and its importance in the security industry.
- Identify the different types of penetration testing and their respective objectives.
- Utilize the various tools and techniques used in penetration testing.
- Develop an understanding of the ethical and legal considerations of penetration testing.

Module 2: Network Reconnaissance and Scanning

Cannot perform runtime binding{ "error": { "message": "The server had an error while processing your request. Sorry about that!", "type": "server_error", "param": null, "code": null } }
QUESTION STATEMENT : Write a short description for Module 2: Network Reconnaissance and Scanningmodule for eLearnSecurity Certified Professional Penetration Tester (V2) course?

Lessons

- Introduction to Network Reconnaissance

- Footprinting and Information Gathering
- Scanning Networks
- Vulnerability Scanning
- Exploiting Vulnerabilities
- Network Mapping
- Network Enumeration
- Network Sniffing
- Wireless Network Reconnaissance
- Social Engineering Techniques

After completing this module, students will be able to:

- Understand the different types of network reconnaissance and scanning techniques.
- Utilize various tools to perform network reconnaissance and scanning.
- Analyze the results of network reconnaissance and scanning.
- Identify and exploit vulnerabilities discovered through network reconnaissance and scanning.

Module 3: Enumeration

Cannot perform runtime binding{ "error": { "message": "The server had an error while processing your request. Sorry about that!", "type": "server_error", "param": null, "code": null } }
QUESTION STATEMENT : Write a short description for Module 3: Enumerationmodule for eLearnSecurity Certified Professional Penetration Tester (V2) course?

Lessons

- Footprinting and Reconnaissance
- Scanning Networks
- Enumerating Services
- Enumerating Users and Groups
- Enumerating Shares
- Enumerating Applications
- Enumerating Databases
- Enumerating Network Devices
- Enumerating Web Applications
- Enumerating Wireless Networks

After completing this module, students will be able to:

- Identify and use various enumeration techniques to gather information about a target system.
- Utilize tools such as Nmap, Netcat, and Metasploit to perform enumeration.
- Understand the importance of enumeration in the penetration testing process.
- Analyze the results of enumeration to identify potential vulnerabilities and attack vectors.

Module 4: Vulnerability Analysis

Cannot perform runtime binding{ "error": { "message": "The server had an error while processing your

request. Sorry about that!", "type": "server_error", "param": null, "code": null } }
QUESTION STATEMENT : Write a short description for Module 4: Vulnerability Analysismodule for eLearnSecurity Certified Professional Penetration Tester (V2) course?

Lessons

- Introduction to Vulnerability Analysis
- Scanning and Enumeration Techniques
- Exploiting Vulnerabilities
- Post Exploitation and Reporting
- Automated Vulnerability Analysis Tools
- Advanced Vulnerability Analysis Techniques
- Vulnerability Analysis in Cloud Computing
- Vulnerability Analysis in Mobile Applications
- Vulnerability Analysis in Web Applications
- Vulnerability Analysis in Network Infrastructure

After completing this module, students will be able to:

- Identify and assess potential security vulnerabilities in a given system.
- Utilize various tools and techniques to perform vulnerability analysis.
- Develop a comprehensive report outlining the security vulnerabilities and their associated risks.
- Recommend appropriate countermeasures to mitigate the identified security risks.

Module 5: Exploitation

Module 5 of the eLearnSecurity Certified Professional Penetration Tester (V2) course focuses on exploitation techniques. It covers topics such as buffer overflows, shellcode, and privilege escalation. It also covers topics such as exploiting web applications, client-side attacks, and post-exploitation techniques. This module provides students with the skills and knowledge necessary to identify and exploit vulnerabilities in a target system.

Lessons

- Introduction to Exploitation
- Exploitation Techniques
- Exploiting Buffer Overflows
- Exploiting Web Applications
- Exploiting Client-Side Applications
- Exploiting Network Services
- Exploiting Databases
- Exploiting Operating Systems
- Exploiting Mobile Applications
- Post Exploitation Techniques

After completing this module, students will be able to:

- Identify and exploit vulnerabilities in web applications.
- Utilize various tools and techniques to exploit vulnerabilities in web applications.
- Understand the principles of exploitation and how to use them to gain access to a system.
- Develop custom exploits to bypass security measures and gain access to a system.

Module 6: Post Exploitation

Cannot perform runtime binding{ "error": { "message": "The server had an error while processing your request. Sorry about that!", "type": "server_error", "param": null, "code": null } }
QUESTION STATEMENT : Write a short description for Module 6: Post Exploitationmodule for eLearnSecurity Certified Professional Penetration Tester (V2) course?

Lessons

- Identifying and Exploiting Privilege Escalation Vulnerabilities
- Post Exploitation Data Gathering
- Post Exploitation Network Scanning
- Post Exploitation Password Cracking
- Post Exploitation Data Exfiltration
- Post Exploitation Persistence
- Post Exploitation Cleanup
- Post Exploitation Reporting
- Post Exploitation Countermeasures
- Post Exploitation Automation

After completing this module, students will be able to:

- Identify and exploit vulnerabilities in a target system.
- Utilize post-exploitation techniques to gain access to sensitive data.
- Develop and execute post-exploitation scripts to automate post-exploitation tasks.
- Utilize post-exploitation tools to gain further access to a target system.

Module 7: Web Application Penetration Testing

Cannot perform runtime binding{ "error": { "message": "The server had an error while processing your request. Sorry about that!", "type": "server_error", "param": null, "code": null } }
QUESTION STATEMENT : Write a short description for Module 7: Web Application Penetration Testingmodule for eLearnSecurity Certified Professional Penetration Tester (V2) course?

Lessons

- Introduction to Web Application Penetration Testing
- Understanding the Web Application Architecture
- Identifying Web Application Vulnerabilities
- Exploiting Web Application Vulnerabilities
- Web Application Firewall Bypass Techniques
- Automated Web Application Scanning
- Web Application Security Testing Methodologies

- Web Application Security Testing Tools
- Web Application Security Auditing
- Reporting and Remediation of Web Application Vulnerabilities

After completing this module, students will be able to:

- Identify and exploit web application vulnerabilities such as SQL injection, Cross-Site Scripting (XSS), and Cross-Site Request Forgery (CSRF).
- Utilize automated tools to scan for web application vulnerabilities.
- Understand the importance of secure coding practices and how to implement them.
- Develop a comprehensive web application penetration testing methodology.

Module 8: Wireless Penetration Testing

Cannot perform runtime binding{ "error": { "message": "The server had an error while processing your request. Sorry about that!", "type": "server_error", "param": null, "code": null } }
QUESTION STATEMENT : Write a short description for Module 8: Wireless Penetration Testingmodule for eLearnSecurity Certified Professional Penetration Tester (V2) course?

Lessons

- Introduction to Wireless Penetration Testing
- Wireless Network Architecture
- Wireless Network Security Protocols
- Wireless Network Vulnerabilities
- Wireless Network Exploitation
- Wireless Network Cracking
- Wireless Network Sniffing
- Wireless Network Scanning
- Wireless Network Hacking
- Wireless Network Forensics
- Wireless Network Honeypots
- Wireless Network Defense Strategies
- Wireless Network Auditing
- Wireless Network Penetration Testing Tools
- Wireless Network Penetration Testing Methodology
- Wireless Network Penetration Testing Report Writing

After completing this module, students will be able to:

- Identify and exploit vulnerabilities in wireless networks.
- Utilize tools such as Aircrack-ng, Wireshark, and Metasploit to assess wireless networks.
- Understand the different types of wireless encryption and authentication protocols.
- Develop strategies to secure wireless networks against malicious attacks.

Module 9: Social Engineering

Cannot perform runtime binding{ "error": { "message": "The server had an error while processing your request. Sorry about that!", "type": "server_error", "param": null, "code": null } }
QUESTION STATEMENT : Write a short description for Module 9: Social Engineeringmodule for eLearnSecurity Certified Professional Penetration Tester (V2) course?

Lessons

- Introduction to Social Engineering
- Social Engineering Tactics and Techniques
- Social Engineering Attack Vectors
- Social Engineering Countermeasures
- Social Engineering in the Digital Age
- Social Engineering in the Physical World
- Social Engineering in the Workplace
- Social Engineering in the Cybersecurity Domain
- Social Engineering in the Financial Sector
- Social Engineering in the Healthcare Industry
- Social Engineering in the Government Sector
- Social Engineering in the Education Sector
- Social Engineering in the Media and Entertainment Industry
- Social Engineering in the Retail Industry
- Social Engineering in the Automotive Industry
- Social Engineering in the Telecommunications Industry
- Social Engineering in the Manufacturing Industry
- Social Engineering in the Energy Sector
- Social Engineering in the Transportation Sector
- Social Engineering in the Hospitality Industry

After completing this module, students will be able to:

- 11 Cannot perform runtime binding{ "error": { "message": "The server had an error while processing your request. Sorry about that!", "type": "server_error", "param": null, "code": null } }
- 11 QUESTION STATEMENT : Suggest four points what students will be capable of after completing Module 9: Social Engineering module for course eLearnSecurity Certified Professional Penetration Tester (V2)?

Module 10: Reporting and Documentation

Module 10: Reporting and Documentation is the final module of the eLearnSecurity Certified Professional Penetration Tester (V2) course. This module covers the fundamentals of reporting and documentation, including the importance of proper documentation, the different types of reports, and the best practices for creating effective reports. Additionally, students will learn how to create a professional penetration testing report and how to present their findings to stakeholders.

Lessons

- Understanding the Reporting Process
- Writing a Professional Penetration Test Report

- Documenting the Penetration Test
- Creating a Penetration Test Report Template
- Presenting the Results of a Penetration Test
- Exploring Different Types of Reports
- Exploring Different Types of Documentation
- Exploring Different Types of Presentations
- Exploring Different Types of Visualizations
- Exploring Different Types of Diagrams
- Exploring Different Types of Charts
- Exploring Different Types of Graphs
- Exploring Different Types of Tables
- Exploring Different Types of Logs
- Exploring Different Types of Evidence
- Exploring Different Types of Metrics
- Exploring Different Types of Risk Assessments
- Exploring Different Types of Vulnerability Assessments
- Exploring Different Types of Exploitation Techniques
- Exploring Different Types of Remediation Strategies

After completing this module, students will be able to:

- Understand the importance of reporting and documentation in the penetration testing process.
- Create comprehensive and professional penetration testing reports.
- Utilize various tools and techniques to document the results of a penetration test.
- Explain the different types of documentation and reporting formats available.