EC-Council

CAST 611v3

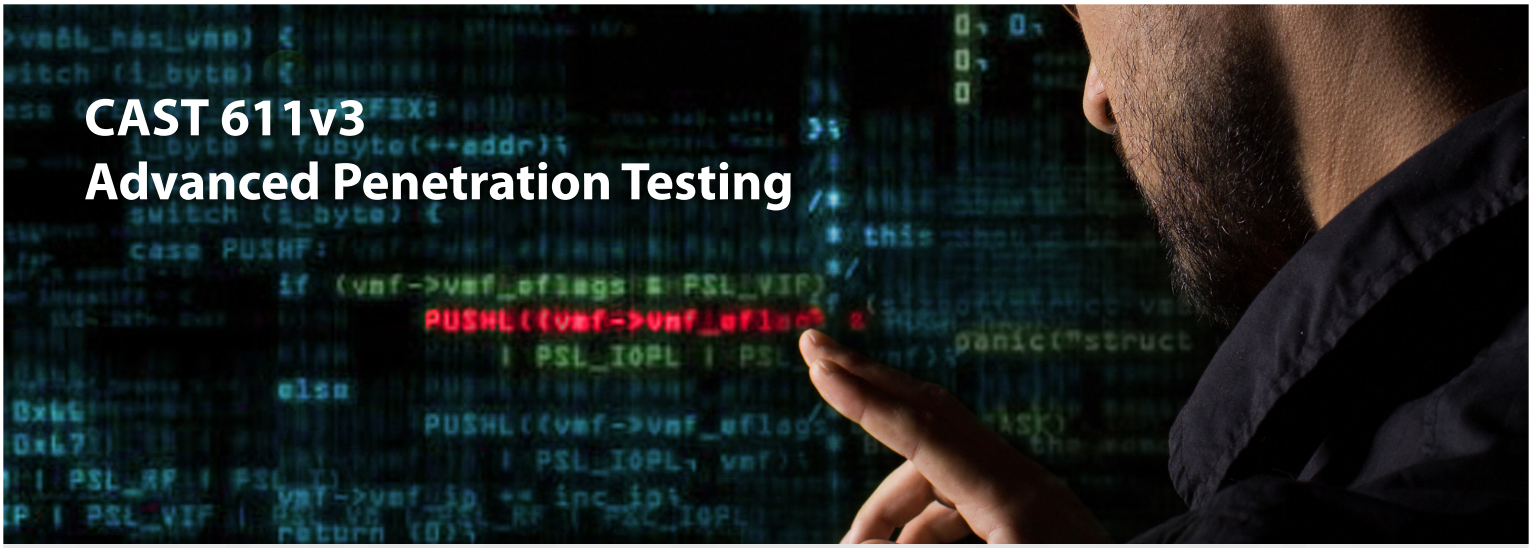
Advanced Penetration Testing

CAST

CENTER FOR ADVANCED SECURITY TRAINING

What is CAST (Center for Advanced Security Training)?

With the speed at which the information security landscape evolves; professionals must stay up-to-date on the latest security techniques, threats and remediation strategies. In response, EC-Council created CAST to meet these challenges head-on. The Center for Advanced Security Training addresses the direct needs of those professionals who must retain the necessary skills required for their positions within the information security industry. CAST provides very specialized training programs governing key information security domains, at an advanced level. EC-Council co-developed CAST with well-respected industry practitioners, ensuring you receive the most important learning experiences and everything needed to conquer any Challenge.



CAST 611v3
Advanced Penetration Testing

Course Description

This course covers everything you need to know for a professional security test as well as how to produce the two most important items; the findings and report!

The practical environment ranges progress in difficulty and reflect enterprise network architecture. This environment includes defenses and challenges which you must defeat and overcome. This is not your typical FLAT network! As you progress through the range levels, each encounter will present the top defenses of today and you will learn the best and latest evasion techniques.

This training format has helped thousands of penetration testers globally and is proven to be effective!

The CAST 611v3 course is 100% hands-on. No course materials, or slides to weigh you down. Everything presented in the course is through an enterprise network environment, which must be attacked, exploited, evaded, defended, etc.

The CAST 611v3 consists of the following lab modules:

- Information Gathering and OSINT
- Scanning
- Enumeration
- Vulnerability Analysis
- Exploitation
- Post Exploitation
- Advanced Techniques
- Data Analysis and Reporting

Once you have practiced this then you will go against a "live" range.

The process is as follows:

- **Access the range:** Four Ranges
  - You will be provided a scope of work
  - Have 2-3 hours on the range and then be provided a debrief

The ranges are progressive and increase in difficulty at each level. There are 3-4 levels to complete then you are ready for the challenge range practical!

- **Practical:** Two phases
  - Scope of work for each phase
  - 3 hours to complete the practical
  - Save all of the data and build a target database of your findings. At completion of the range section
  - 75 minutes for written exam base on ranges – Pass exam
  - Receive CAST Advanced Penetration Tester Certification

Motto:

- So you think you can pen test? PROVE IT!

How Will This Course Benefit You?

01 Understand what it takes to break into a highly secured organization from the outside

02 Review proven methods on how to avoid detection by IDS/IPS and how to move around the network freely

03 How to apply the best practices for mitigating or circumventing security implementations such as locked desktops, GPOs, IDS/IPS, WAFs and several others

04 Professional understanding and skills on Pen Testing high security environments covering areas such as government, financial and other key industry installations

What Will You Learn?

Students completing this course will gain in-depth knowledge in the following areas:

01 Advanced scanning methods

02 Attacking from the Web

03 Client side pen-testing

04 Attacking from the LAN

05 Breaking out of restricted environments

06 Bypassing network-based IDS/IPS

07 Privilege escalation

08 Post-exploitation

Who Should Attend

- Information Security Professionals
- Penetration Testers
- IT Managers
- IT Auditors
- Government and Intelligence Agencies interested in real world attack and defense in today's complex and highly secure IT environments

Training Information

Title of the Course: **Advanced Penetration Testing**

Training Duration: **4 Days**

Training Timing: **9:00 AM to 5:00 PM**

Exam Details

Exam Title: **CAST 611 - Advanced Penetration Testing**

Number of Questions: **60 (Based on practical results)**

Exam Duration: **75 minutes**

Passing Score: **70%**

Test Delivery: **ECC Exam Portal**

Note: Open book, note, and access to a range is allowed during the test

Course Outline

Day 1

Module 01: Information Gathering and OSINT

- Information Gathering with NSLOOKUP and Dig
- DNS Enumeration with dnsenum and dnsrecon
- Enumeration with fierce
- Registrars and Whois
- Google Hacking Database
- Enumeration with Metagoofil
- Cloud Scanning with Shodan

Module 02: Scanning

- Scanning with Nmap
- Scanning with the Tool DMitry
- Scanning with the Tool Netdiscover
- Scanning with the Tool sslscan
- Scanning and Scripting with the Tool hping3
- Scanning and Building a Target Database

Range One: Live Target Range Challenge Level One

Day 2

Module 03: Enumeration

- Enumerating Targets
- Enumerating SMB
- OS Fingerprinting with Nmap

Module 04: Vulnerability Analysis

- Vulnerability Sites
  - Review the National Vulnerability Database Website
  - Review Secunia Website
  - Review Security Focus Website
  - Review Zero Day Initiative Website
- Vulnerability Analysis with OpenVAS
- WebGoat Tutorial
- Vulnerability Scanning with W3AF Console
- Vulnerability Scanning with Skipfish
- Vulnerability Scanning with Vega
- Vulnerability Scanning with Owasp-zap

Module 05: Exploitation

- Exploit Sites
  - Review the Security Focus Website
  - Review GNU Citizen Website
  - Review TopSite Website
  - Review Exploit Database Website
- Manual Exploitation
  - Scan the Target
  - Identify Vulnerabilities
  - Search for an Exploit for the Vulnerability
  - Prepare the Exploit
  - Attempt to Exploit the Target Machine
- Exploitation with Metasploit
  - Scan the Target
  - Identify Vulnerabilities
  - Find Exploit for the Vulnerability
  - Exploit the Targets
- Exploitation with Armitage
  - Scan from within Armitage
  - Manage Targets in Armitage
  - Exploit Targets with Armitage

Range Two: Live Target Range Challenge Level Two

Day 3

Module 06: Post Exploitation

- Local Assessment
  - Conduct the Scanning Methodology against the Machine
  - Identify Vulnerabilities
  - Search for an Exploit
  - Compile the Exploit
  - Attempt to Exploit the Machine
  - Harvest Information from an Exploited Machine
  - Grab the Password Files
  - Crack Passwords
  - Transfer Files or Copy Files to and from an Exploited Machine

Module 07: Advanced Techniques

- Scanning with Nmap against Defenses
  - Scan for Live Systems
  - Scan for Open Ports
  - Observe and Troubleshoot the Scan
  - Attempt Advanced Options to Try to Get the Scan through a Filter
- Detecting Load Balancing with Command Line Tools and Firefox
- Detecting Load Balancing with lbd
- Detecting Web Application Firewall Using WAFW00F
- Evasion Using Social-Engineer Toolkit (SET)
  - Configure the SET Tool
  - Build the Payload (Create the Powershell Script)
  - Send the Powershell Code File to the Target Machine
  - Attempt to Exploit the Machine

Range Three: Live Target Range Challenge Level Three

Range Four: Live Target Range Challenge Level Four (Range Four is optional)

Day 4

Module 08: Data Analysis and Reporting

- Compiling Data in MagicTree
- Developing a Report
  - Identify the Components of a Report
  - Review the Findings and Create Report Information
  - Review Sample Reports
  - Create a Custom Report
- Developing a Report Using KeepNote

Practical Phase One

- External Penetration Testing

Practical Phase Two

- External and Internal Testing

Written Exam

- 60 questions
- 75 minutes

Master Trainer: Kevin Cardwell

Kevin Cardwell served as the leader of a 5 person Red Team that achieved a 100% success rate at compromising systems and networks for six straight years. He has conducted over 500 security assessments across the globe. His expertise is in finding weaknesses and determining ways clients can mitigate or limit the impact of these weaknesses.

He currently works as a free-lance consultant and provides consulting services for companies throughout the world, and as an advisor to numerous government entities within the US, Middle East, Africa, Asia and the UK. He is an Instructor, Technical Editor and Author for Computer Forensics, and Hacking courses. He is the author of the Center for Advanced Security and Training (CAST) Advanced Network Defense course. He is technical editor of the Learning Tree Course Penetration Testing Techniques and Computer Forensics. He has presented at the Blackhat USA, Hacker Halted, ISSA and TakeDownCon conferences. He has chaired the Cybercrime and Cyberdefense Summit in Oman. He is author of Bactrack: Testing Wireless Network Security. Kevin holds a BS in Computer Science from National University in California and a MS in Software Engineering from the Southern Methodist University (SMU) in Texas. He developed the Strategy and Training Development Plan for the first Government CERT in the country of Oman that recently was rated as the top CERT for the Middle East. He serves as a professional training consultant to the Oman Information Technology Authority, and developed the team to man the first Commercial Security Operations Center in the country of Oman. He has worked extensively with banks and financial institutions throughout the Middle East, Europe and the UK in the planning of a robust and secure architecture and implementing requirements to meet compliance. He currently provides consultancy to Commercial companies, governments, major banks and financial institutions in the Gulf region to include the Muscat Securities Market (MSM) and the Central Bank of Oman. Additionally, he provides training and consultancy to the Oman CERT and the SOC team in the monitoring and incident identification of intrusions and incidents within the Gulf region.

EC-Council