OFFENSIVE SECURITY

PRODUCT OVERVIEW

OFFENSIVE® security

ATA APPLIED TECHNOLOGY ACADEMY

All trademarks and trade names are the property of their respective owners.

AN OFFENSIVE APPROACH

Well-designed mitigation strategies need routine security tests. The best tests simulate the techniques and methods of an intruder. By encouraging students to use the same tools, techniques, and mindset as a hacker, we level the playing field for defenders. At Offensive Security, we teach that offense is the best defense.

YOU DON’T BUY AN OFFSEC CERTIFICATION. YOU EARN IT.

The course material for OffSec exams and certifications is based on real-world situations, presented with hands-on training and practiced in a virtual lab. Exams are proctored and certification status is verifiable via digital badging.

Certificate holders have tried and tested their abilities and mindset. That means employers can hire OffSec alumni with confidence, knowing they have practical skills and the right attitude.

ATA APPLIED TECHNOLOGY ACADEMY

OFFENSIVE® security

OFFENSIVE SECURITY FEDERAL TRAINING & CERTIFICATION PROGRAMS

WHO

Offensive Security Services, LLC
230 Park Ave; 3rd Floor West
New York, NY 10169
CAGE: 8AVS9
federal@offensive-security.com
www.offensive-security.com

POC: Keith Peer, Head of Federal
k.peer@offensive-security.com
609-808-2900

Offensive Security's courses offer the most rigorous penetration testing training in the industry. An OffSec certification is a clear sign of a skilled and experienced penetration tester.

FROM THE CREATORS OF KALI LINUX
Offensive Security have defined the standard of excellence in penetration testing training. Elite security instructors teach our intense training scenarios and exceptional course material.

The same expert security professionals that designed Kali Linux developed our courses. These professionals leverage their own real-world penetration testing experience to ensure an unwavering focus on the practical applicability of course materials.

WHAT

Operational Need and Improvement

- The pipeline of skilled cyber personnel is limited.
- Training to high levels of proficiency is time-consuming and costly.
- Most university-based training is regarded as insufficient.
- Oversaturation of certification credentials from unknown, unverified, and untrusted sources
- Concerns remain about cost and return on investment.

Training Requirements

The individual will have the training, knowledge, skills and abilities required to demonstrate penetration testing activities and emulate offensive cyber actions and objectives, resulting in a practical certification exam.

- **General** – Demonstrates an overall understanding of the purpose and objectives of the process/topic to discuss the subject or process with individuals of greater knowledge.
- **Functional** – Demonstrates an understanding of the individual parts of the process/topic and the knowledge needed to conduct offensive cyber actions, assess operations/activities, apply acceptable performance standards, and recognize the need to seek and obtain appropriate expert advice or to consult appropriate reference materials.
- **Detailed** – Demonstrates an understanding of the inner workings of individual parts of the process/topic and comprehensive, intensive knowledge of the subject or process sufficient to provide advice in the absence of procedural guidance.

HOW

CONTENT				DELIVERY				
BOOK	VIDEO	LAB	EXAM	ONLINE	LIVE	ACADEMY		
●			● 72 hr		●		**EXP-401 | OSEE** Advanced Windows Exploitation (AWE)	EXPERT
●	●	●	● 48 hr	●	●		**EXP-301 | OSED** Windows Usermode Exploit Development (WUMED)	ADVANCED
●	●	●	● 48 hr	●	●		**WEB-300 | OSWE** Advanced Web Attacks and Exploitation (AWAE)	
●	●	●	● 48 hr	●	●		**PEN-300 | OSEP** Evasion Techniques and Breaching Defenses (ETBD)	
●	●	instructions to create lab	● 4 hr	●			**PEN-210 | OSWP** Wireless Attacks (WiFu)	FOUNDATION
●	●	●	● 24 hr	●	●	●	**PEN-200 | OSCP** Penetration Testing with Kali Linux (PWK)	

WHY

Utilizing Offensive Security's readymade Commercial Off The Shelf (COTS) training can quickly fill cyber training gaps and enhance existing knowledge, skills, and abilities with hands-on practical training labs, exams, and certifications.

Short term objectives

To cost-effectively and efficiently fill Offensive Cyber Operations (OCO) and Defensive Cyber Operations (DCO) training gaps with demonstrable performance testing and creditable certification from a well-known and highly regarding cyber training organization.

Long term objectives

To develop and measurably improve Cyber Mission Force (CMF) readiness, resiliency, and capability by training the OCO teams nation-state Tactics, Techniques and Procedures (TTP), and functionally cross-training the DCO on cyber adversaries TTP.

Combined Overall Objectives

To improve CMF OCO/DCO training outcomes by cost-effectively leveraging creditable private sector COTS training and certification from Offensive Security.

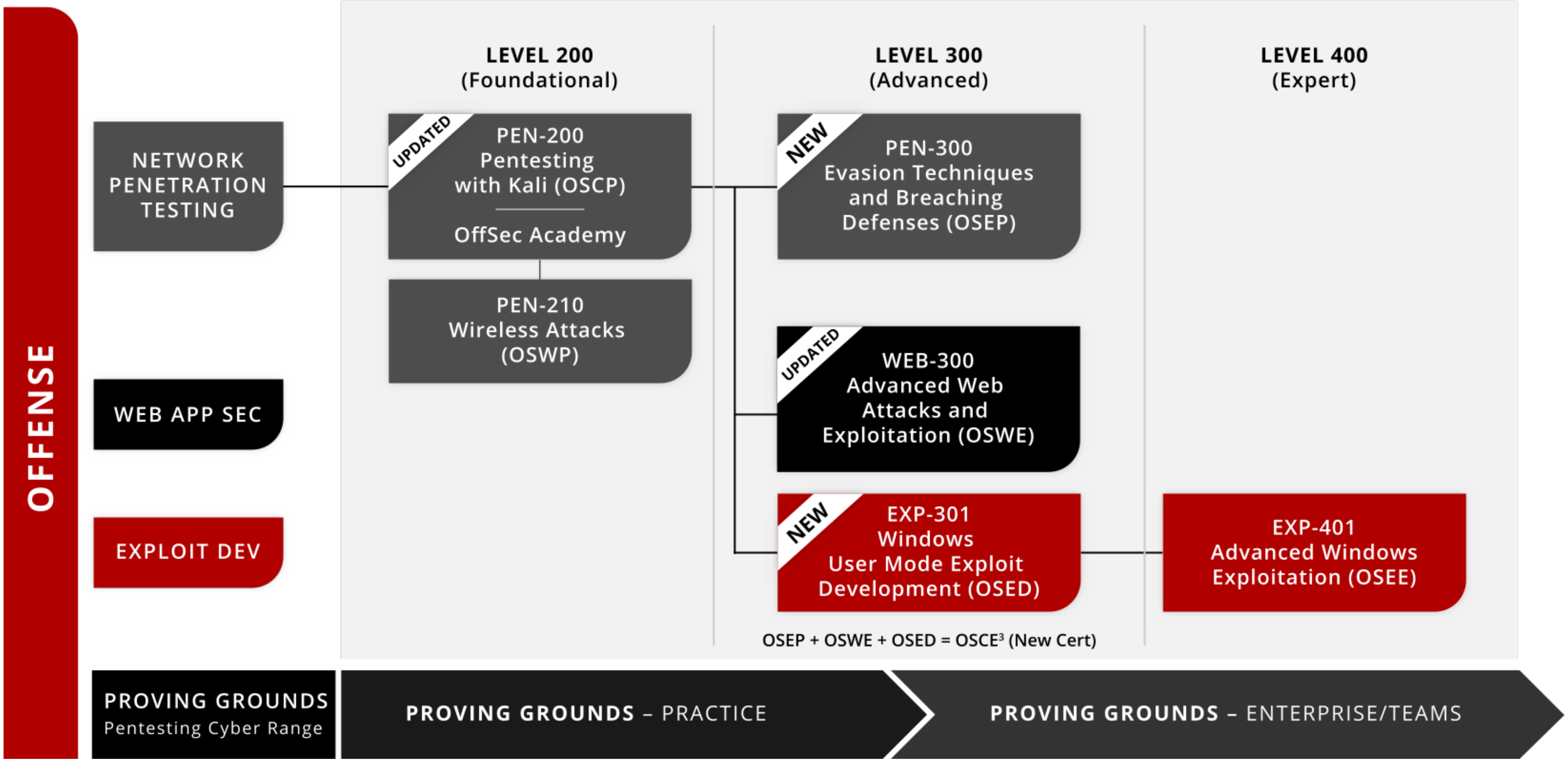
APPLIED TECHNOLOGY ACADEMY

OFFENSIVE SECURITY
COURSE ROADMAP

Course Syntax

PEN-301
Track ┘ Level ┘ └ OS

Track	Course Level	Operating System
PENtesting	100 - Beginner	0 - Multiple OS
WEB App Security	200 - Foundational	1 - Windows
EXPloit Dev	300 - Advanced	2 - macOS
	400 - Expert	3 - Linux



OFFENSE

LEVEL 200 (Foundational)

LEVEL 300 (Advanced)

LEVEL 400 (Expert)

NETWORK PENETRATION TESTING

UPDATED PEN-200 Pentesting with Kali (OSCP)

OffSec Academy

PEN-210 Wireless Attacks (OSWP)

NEW PEN-300 Evasion Techniques and Breaching Defenses (OSEP)

WEB APP SEC

UPDATED WEB-300 Advanced Web Attacks and Exploitation (OSWE)

EXPLOIT DEV

NEW EXP-301 Windows User Mode Exploit Development (OSED)

EXP-401 Advanced Windows Exploitation (OSEE)

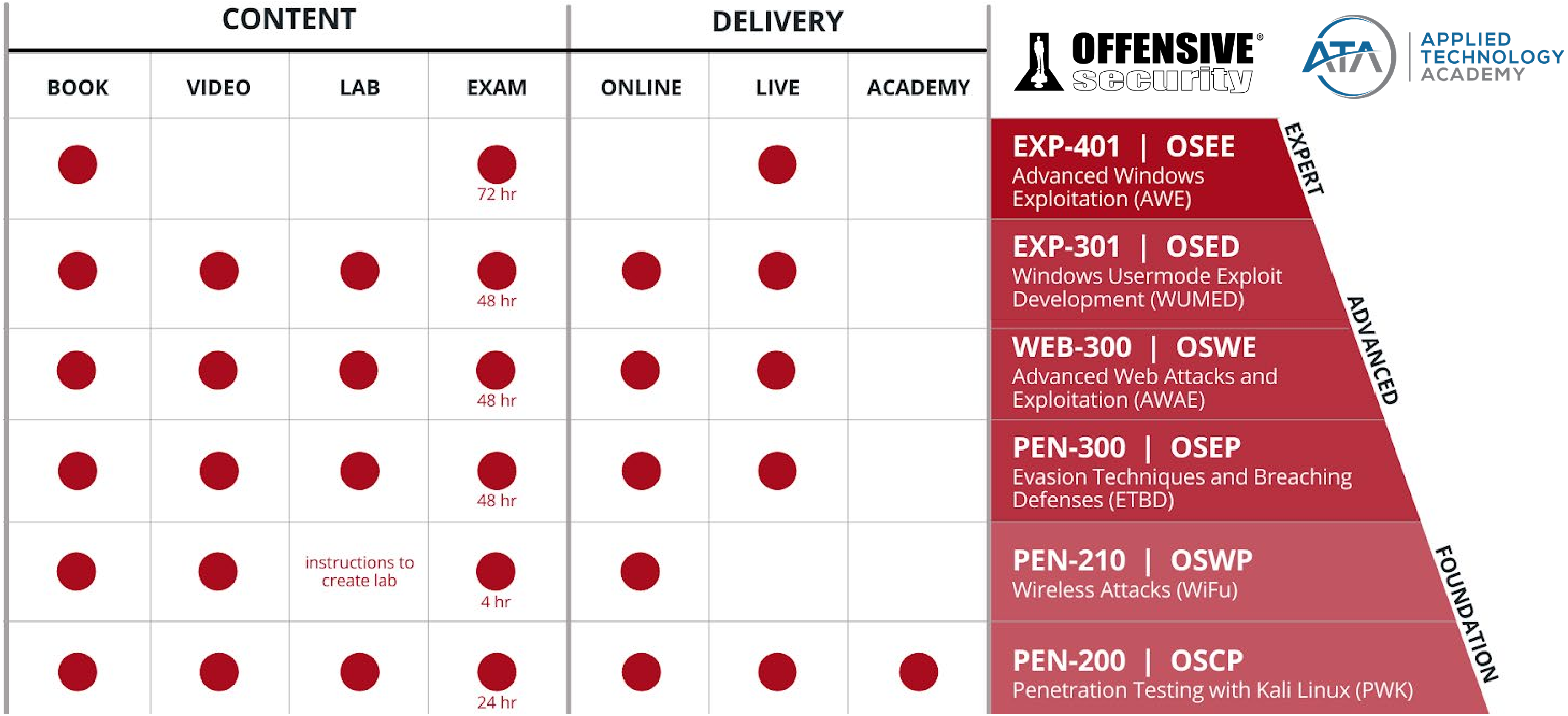
OSEP + OSWE + OSED = OSCE^3 (New Cert)

PROVING GROUNDS
Pentesting Cyber Range

PROVING GROUNDS – PRACTICE

PROVING GROUNDS – ENTERPRISE/TEAMS

COURSE OVERVIEW



CONTENT				DELIVERY				
BOOK	VIDEO	LAB	EXAM	ONLINE	LIVE	ACADEMY		
●			● 72 hr		●		**EXP-401 | OSEE** Advanced Windows Exploitation (AWE)	EXPERT
●	●	●	● 48 hr	●	●		**EXP-301 | OSED** Windows Usermode Exploit Development (WUMED)	ADVANCED
●	●	●	● 48 hr	●	●		**WEB-300 | OSWE** Advanced Web Attacks and Exploitation (AWAE)	
●	●	●	● 48 hr	●	●		**PEN-300 | OSEP** Evasion Techniques and Breaching Defenses (ETBD)	
●	●	instructions to create lab	● 4 hr	●			**PEN-210 | OSWP** Wireless Attacks (WiFu)	FOUNDATION
●	●	●	● 24 hr	●	●	●	**PEN-200 | OSCP** Penetration Testing with Kali Linux (PWK)	

OFFENSIVE® security

ATA APPLIED TECHNOLOGY ACADEMY

PEN-200

●●●○○

The official OSCP certification course.

MATERIALS

- 17+ hours of video
- 850-page PDF course guide
- Virtual lab environment 70 machines
- Active student forums

24H **EXAM**

Proctored, hands-on penetration test exam that requires students to submit a comprehensive report that should contain in-depth notes and screenshots detailing the findings.

Earn **OSCP**

PENETRATION TESTING WITH KALI LINUX (PWK)

Designed for information security professionals who want to take a serious and meaningful step into the world of professional penetration testing.

COMPETENCIES

- Using information gathering techniques to identify and enumerate targets running various operating systems and services
- Writing basic scripts and tools to aid in the penetration testing process
- Analyzing, correcting, modifying, cross-compiling, and porting public exploit code
- Conducting remote, local privilege escalation, and client-side attacks
- Identifying and exploiting XSS, SQL injection, and file inclusion vulnerabilities in web applications
- Leveraging tunneling techniques to pivot between networks
- Creative problem solving and lateral thinking skills

PREREQUISITES

- Solid understanding of TCP/IP networking
- Reasonable Windows and Linux administration experience
- Familiarity of Bash scripting with basic Python or Perl a plus

GET READY FOR OSCP

- Proving Grounds Prepare
- Kali Linux Revealed
- Proving Grounds Play & Practice

ATA APPLIED TECHNOLOGY ACADEMY

OFFENSIVE® security

PEN-210

●●●○○

The official OSWP certification course.

MATERIALS

- 3.5+ hours of video
- 380-page PDF course guide
- Access to home lab setup
- Active student forums

4H **EXAM**

Proctored, hands-on penetration test exam that requires students to submit a comprehensive report that should contain in-depth notes and screenshots detailing the findings.

Earn **OSWP**

WIRELESS ATTACKS (WiFu)

Introduces students to the skills needed to identify vulnerabilities in 802.11 networks and execute organized attacks. Each student will set up a home lab to practice the techniques learned in this online, self-paced course.

COMPETENCIES

- Greater insight into wireless offensive security and expanded awareness of the need for real-world security solutions
- Implementing attacks against WEP and WPA encrypted network
- Executing advanced attacks such as PRGA key extraction and one-way packet injection
- Using alternate WEP and WPA cracking techniques
- Using various wireless reconnaissance tools
- Understanding of how to implement different rogue access point attacks
- Familiarity with the BackTrack wireless tools

PREREQUISITES

- All students must have a solid understanding of TCP/IP and the OSI model, as well as familiarity with Linux.
- A modern laptop or desktop that can boot and run BackTrack and specific hardware is required to complete course exercises. You can use Kali Linux to take the course, but the exam uses BackTrack.

GET READY FOR OSWP

- Proving Grounds Prepare
- Kali Linux Revealed

APPLIED TECHNOLOGY ACADEMY

OFFENSIVE® security

PEN-300

●●●●○

The official OSEP certification course.

MATERIALS

- 19 hours of video
- 700-page PDF course guide
- Access to virtual lab environment
- Active student forums

48H **EXAM**

Proctored, hands-on penetration test exam that requires students to submit a comprehensive report that should contain in-depth notes and screenshots detailing the findings

Earn **OSEP**

EVASION TECHNIQUES AND BREACHING DEFENSES (ETBD)

An advanced penetration testing course that teaches students to perform advanced penetration tests against mature organizations with an established security function.

COMPETENCIES

- Preparation for more advanced field work
- Knowledge of breaching network perimeter defenses through client-side attacks, evading antivirus and allow-listing technologies
- How to customize advanced attacks and chain them together

PREREQUISITES

- Working familiarity with Kali Linux and Linux command line
- Solid ability in enumerating targets to identify vulnerabilities
- Basic scripting abilities in Bash, Python, and PowerShell
- Identifying and exploiting vulnerabilities like SQL injection, file inclusion, and local privilege escalation
- Foundational understanding of Active Directory and knowledge of basic AD attacks
- Familiarity with C# programming is a plus

GET READY FOR OSEP

- Penetration Testing with Kali Linux (PWK)

ATA APPLIED TECHNOLOGY ACADEMY

OFFENSIVE® security

WEB-300

●●●●○

The official OSWE certification course.

MATERIALS

- 10 hours of video
- 410-page PDF course guide
- Access to virtual lab environment and private lab
- Active student forums

48H **EXAM**

Proctored, hands-on penetration test exam that requires students to submit a comprehensive report that should contain in-depth notes and screenshots detailing the findings

Earn **OSWE**

ADVANCED WEB ATTACKS AND EXPLOITATION (AWAE)

An advanced web application security review course that teaches the skills needed to conduct white box web app penetration tests.

COMPETENCIES

- Performing advanced web app source code auditing
- Analyzing code, writing scripts, and exploiting web vulnerabilities
- Implementing multi-step, chained attacks using multiple vulnerabilities
- Using creative and lateral thinking to determine innovative ways of exploiting web vulnerabilities

PREREQUISITES

- Comfort reading and writing at least one coding language (Java, .NET, JavaScript, Python, etc)
- Familiarity with Linux: file permissions, navigation, editing, and running scripts
- Ability to write simple Python / Perl / PHP / Bash scripts
- Experience with web proxies, such as Burp Suite and similar tools
- General understanding of web app attack vectors, theory, and practice

GET READY FOR OSWP

- Penetration Testing with Kali Linux (PWK)

ATA APPLIED TECHNOLOGY ACADEMY

OFFENSIVE® security

EXP-301

●●●●○

The official OSED certification course.

MATERIALS

- 15 hours of video
- 600-page PDF course guide
- Access to virtual lab environment
- Active student forums

48H **EXAM**

Proctored, hands-on penetration test exam that requires students to submit a comprehensive report that should contain in-depth notes and screenshots detailing the findings

Earn **OSED**

WINDOWS USER MODE EXPLOIT DEVELOPMENT (WUMED)

An intermediate-level course which teaches students the fundamentals of modern exploit development and the skills needed to crack the critical security mitigations protecting enterprises.

COMPETENCIES

- Using WinDbgWriting your own shellcode
- Bypassing basic security mitigations, including DEP and ASLR
- Exploiting format string specifiers
- The necessary foundations for finding bugs in binary applications to create custom exploits

PREREQUISITES

- Familiarity with debuggers (ImmunityDBG, OllyDBG)
- Familiarity with basic exploitation concepts on 32-Bit
- Familiarity with writing Python 3 code
- (optional) Ability to read and understand C code at a basic level
- (optional) Ability to read and understand 32-Bit Assembly code at a basic level

GET READY FOR OSED

- Penetration Testing with Kali Linux (PWK)

APPLIED TECHNOLOGY ACADEMY

OFFENSIVE® security

WEB-401

●●●●●

The official OSEE certification course.

LIVE COURSE

72H **EXAM**
Proctored, hands-on penetration test exam that requires students to submit a comprehensive report that should contain in-depth notes and screenshots detailing the findings

Earn **OSEE** & **40 (ISC)^2 CPE CREDITS**

ADVANCED WINDOWS EXPLOITATION (AWE)

This is the hardest course that challenges students to develop creative solutions that work in today’s increasingly difficult exploitation environment.

COMPETENCIES

- NX/ASLR Bypass – Using different techniques to bypass Data Execution
- Prevention and Address Space Layout
- Randomization protection mechanisms on modern operating systems.
- Function pointer overwrites – Overwriting a function pointer in order to get code execution.
- Precision Heap Spraying – Spraying the heap for reliable code execution.
- Disarming EMET Mitigations to gain reliable code execution
- 32-Bit and 64-Bit Windows Kernel Driver Exploitation
- Kernel Pool Exploitation

PREREQUISITES

- Students should be experienced in developing windows exploits and understand how to operate a debugger.
- Familiarity with WinDbg, Immunity Debugger, and Python scripting is highly recommended.

GET READY FOR OSEE

- Windows User Mode Exploit Development (WUMED)
- Advanced Web Attacks and Exploitation (AWAE)
- Evasion Techniques and Breaching Defenses (ETBD)

ATA APPLIED TECHNOLOGY ACADEMY

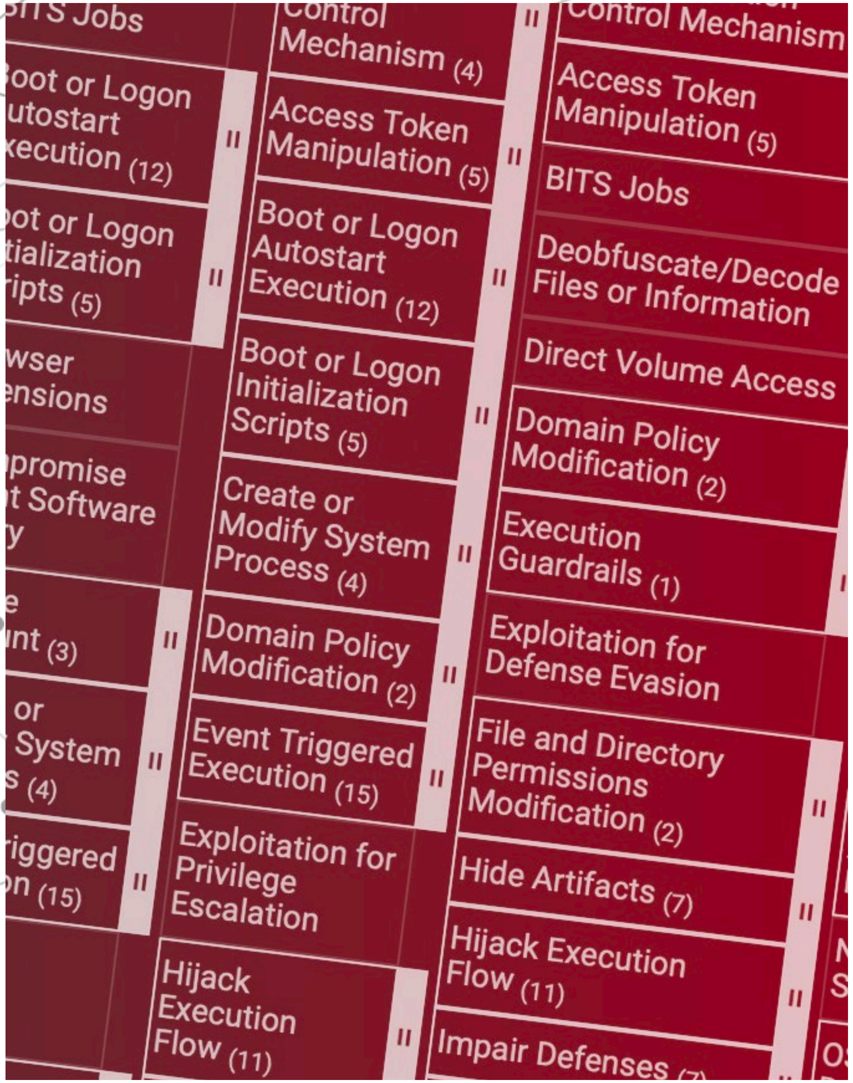
OFFENSIVE® security

PROVING GROUNDS **ENTERPRISE**

- Purpose-built, realistic, modern network of vulnerable machines
- Designed to test, train and challenge Penetration Testers of all levels
- Built to simulate a sophisticated corporate network
- Both web and non-web-based attack vectors
- Over 45 Windows and Linux machines and three unique subnetworks
- Perfect for honing skills, experimenting with new techniques, and for hiring pentesting candidates
- Drives Penetration Testers to perform at higher levels of creativity, cunning and lateral thinking

APPLIED TECHNOLOGY ACADEMY

OFFENSIVE® security



ITS Jobs

oot or Logon utostart xecution (12)

ot or Logon tialization ripts (5)

wser ensions

npromise t Software y

e int (3)

or System s (4)

riggered on (15)

Control Mechanism (4)

Access Token Manipulation (5)

Boot or Logon Autostart Execution (12)

Boot or Logon Initialization Scripts (5)

Create or Modify System Process (4)

Domain Policy Modification (2)

Event Triggered Execution (15)

Exploitation for Privilege Escalation

Hijack Execution Flow (11)

Control Mechanism

Access Token Manipulation (5)

BITS Jobs

Deobfuscate/Decode Files or Information

Direct Volume Access

Domain Policy Modification (2)

Execution Guardrails (1)

Exploitation for Defense Evasion

File and Directory Permissions Modification (2)

Hide Artifacts (7)

Hijack Execution Flow (11)

Impair Defenses (7)

MITRE ATT&CK ® FRAMEWORK

>80% COVERAGE

PROVING GROUNDS

APPLIED TECHNOLOGY ACADEMY

OFFENSIVE® security

WHY PROVING GROUNDS?

PROVING GROUNDS **ENTERPRISE**

REALISM

- Interesting pivots and expanding possibilities
- Recreates corporate network environment
- Difficulty ranges from easy to expert

DYNAMIC UPDATES

- Our labs grow as we discover new exploits
- New exploits added quarterly
- Real-world scenarios

DIVERSITY

- Multiple OS & Attack Vectors
- Built with a broad range of security and IT roles in mind

OFFENSIVE SECURITY

PROVING GROUNDS

THE **MOST** REALISTIC PENTESTING LABS

ATTACK SIMULATIONS INCLUDE:

- Man-in-the-middle attacks (MITM)
- Server message blocking (SMB)
- Phishing emails
- Web and mobile apps
- File server attacks
- Pivoting / lateral movement
- Custom exploits
- Reverse engineering apps
- Buffer overflow, injection, and password attacks
- Privilege escalation
- Information gathering
- Metasploit ® framework
- WhatsApp® (coming soon)

ENTERPRISE REALISM

- Modern Microsoft Windows domain infrastructure
- Windows Defender AV bypass
- Linux production environments
- Active Directory ®
- MITRE ATT&CK® Framework

APPLIED TECHNOLOGY ACADEMY

OFFENSIVE® security

OFFENSIVE SECURITY

PROVING GROUNDS

THE **MOST** REALISTIC PENTESTING LABS

APPLIED TECHNOLOGY ACADEMY

	COMMUNITY		PROFESSIONAL	
	PLAY	PRACTICE	TEAMS	ENTERPRISE
Session Environment	Standalone Machine	Standalone Machine	**Fully Networked**	**Fully Networked**
Lab Author	Community	Community + OffSec	**OffSec**	**OffSec**
Operating Systems	Linux	Linux, Windows	**Windows, Linux, Active Directory**	**Windows, Linux, Active Directory**
Session Time Limit	3 hours		**Unlimited**	**Unlimited**
Type of Environment	Shared	Shared	**Shared**	**Private**
Domain Authentication Attacks	X	X	✓	✓
Multi-System Attack Chains	X	X	✓	✓
MITRE ATT&CK Framework	X	Limited	✓	✓
Administrative Control	X	X	✓	✓
Unlimited User Access	X	X	**X**	✓

LEARN MORE

APPLIED TECHNOLOGY ACADEMY
1992 Lewis Turner Blvd., Ste. 131
Fort Walton Beach, FL 32547

Fort Walton / Tampa / Mobile Classrooms

CAGE: 8EBX7

info@appliedtechac.com

AppliedTechnologyAcademy.com

ATA APPLIED TECHNOLOGY ACADEMY

POCs:
Liz Pernaselci
Director of Sales
liz@appliedtechac.com
p: 800.674.3550 x3

Collin Vandersommen
Federal Program Manager
collin@appliedtechac.com
p: 800.674.3550 x4

OFFENSIVE® security