black hat®
MIDDLE EAST AND AFRICA

14 - 16
NOVEMBER
2023

RIYADH EXHIBITION AND
CONVENTION CENTER,
MALHAM, SAUDI ARABIA

TRAININGS BROCHURE

POST- EVENT TRAINING: 18 - 22 NOV 2023

Organised by:

tahaluf
an informa company

In association with:

الاتحاد السعودي للأمن السيبراني والبرمجة والدرونز
SAUDI FEDERATION FOR CYBERSECURITY, PROGRAMMING & DRONES

black hat®

/ TITLE

EXP 401

ADVANCED WINDOWS EXPLOITATION (AWE)

USD 12,375

/ TRACK

Penetration Testing

/ SKILL LEVEL

Advanced

/ DURATION

5 Days

/ DATES

Sat 18 Nov - Wed 22 Nov

/ SUMMARY

- Modern exploits for Windows-based platforms require modern bypass methods to circumvent Microsoft's defenses. In Advanced Windows Exploitation (EXP-401), OffSec challenges learners to develop creative solutions that work in today's increasingly difficult exploitation environment.
- The case studies in AWE are large, well-known applications that are widely deployed in enterprise networks. The course dives deep into topics ranging from precision heap spraying to DEP and ASLR bypass techniques to 64-bit kernel exploitation.
- AWE is a particularly demanding penetration testing course. It requires a significant amount of student-instructor interaction. Therefore, we limit AWE courses to a live, hands-on environment at Black Hat USA in Las Vegas, NV.

/ DETAILED DESCRIPTION

- Advanced Windows Exploitation (AWE) is our most demanding Offensive Security Course, featuring a sophisticated hands-on computer lab environment challenging you to bring out your best penetration testing skills.
- Modern exploits for Windows-based platforms require modern bypass methods to circumvent Microsoft's defenses. In Advanced Windows Exploitation (EXP-401), OffSec challenges students to develop creative solutions that work in today's increasingly difficult exploitation environment.
- This is the hardest course we offer, and it requires a significant time investment. Learners need to commit to reading case studies and reviewing the provided reading material each evening.

/ DETAILED DESCRIPTION [contd.]

- The OSEE is the most difficult exploit development certification you can earn. We recommend completing the 300-level certifications before registering for this course.
- Students who complete EXP-401 and pass the exam will earn the Offensive Security Exploitation Expert (OSEE) certification. The OSEE exam assesses not only the course content, but also the ability to think laterally and adapt to new challenges.
- The virtual lab environment has a limited number of target systems. The software within contains specific, unknown vulnerabilities. Students have 72 hours to develop and document exploits. The exam requires a stable, high-speed internet connection.
- You must submit a comprehensive penetration test report as part of the exam. It should contain in-depth notes and screenshots detailing the steps taken and the exploit methods used.

/ BENEFITS

- Analyze vulnerable software
- Find problematic code
- Develop a functioning exploit for various modern Windows operating systems.

/ AGENDA / TOPICS

- Bypass and evasion of user mode security mitigations such as DEP, ASLR, CFG, ACG and CET
- Advanced heap manipulations to obtain code execution along with guest-to-host and sandbox escapes
- Disarming WDEG mitigations and creating version independence for weaponization
- 64-Bit Windows Kernel Driver reverse engineering and vulnerability discovery
- Bypass of kernel mode security mitigations such as kASLR, NX, SMEP, SMAP, kCFG and HVCI

/ STUDENT REQUIREMENTS

- Learners should be experienced in developing windows exploits and understand how to operate a debugger.
- Familiarity with WinDBG, x86_64 assembly, IDA Pro and basic C/C++ programming is highly recommended.
- A willingness to work and put in real effort will greatly help students succeed in this security training course.

/ WHAT STUDENTS SHOULD BRING TO THE CLASS

- Bring a serious laptop for this course. It should be able to run three VMs with ease. Please do not bring netbooks or other low-resolution systems. The only supported host operating system is Windows 10.
- VMware Workstation 15 or higher
- 64-bit CPU with a minimum of 4 cores along with support for NX, SMEP, VT-d/IOMMU and VT-x/EPT
- At least 160 GB HD free
- At least 16 GB of RAM

/ WHAT STUDENTS WILL BE PROVIDED WITH ONSITE

- Wi-Fi Internet

/ ABOUT THE EXAM

- This course may qualify you for 40 $(ISC)^2$ CPE Credits after you submit your documentation at the end of the training course or pass the certification challenge.
- 48-hour exam

/ TITLE

WEB 300

ADVANCE WEB ATTACKS AND EXPLOITATION (AWAE)

USD 10,725

/ TRACK

Penetration Testing

/ SKILL LEVEL

Advanced

/ DURATION

5 Days

/ DATES

Sat 18 Nov - Wed 22 Nov

/ SUMMARY

Advanced Web Attacks and exploitation (WEB-300) is an advanced web application security course that teaches the skills needed to conduct white box web app penetration tests. Learners who complete the course and pass the exam earn the OffSec Web Expert (OSWE) certification and will demonstrate mastery in exploiting front-facing web apps. The OSWE is one of three certifications making up the OSCE3 certification along with the OSEP for advanced pentesting and OSED for exploit development.

/ DETAILED DESCRIPTION

- Offensive Security is giving you more for the same price in the Advanced Web Attacks and Exploitation (AWAE) course update. We've added 50% more content with new modules, custom private machines, and practice labs to give your team an even deeper understanding of web application security practices.
- This challenging certification program will develop their skills in a white box and black box environment, with insight and instruction from top cybersecurity leaders. Students who complete the course and pass the exam earn the Offensive Security Web Expert (OSWE) certification, demonstrating mastery in exploiting front-facing web apps.
- With AWAE you can trust that your company's data, reputation, and financial stability are as secure as possible, because your employees are well-prepared to take on the latest challenges

/ BENEFITS

- 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

/ AGENDA / TOPICS

- Cross-Origin Resource Sharing (CORS) with CSRF and RCE
- JavaScript Prototype Pollution
- Advanced Server-Side Request Forgery (SSRF)
- Web security tools and methodologies
- Source code analysis
- Persistent cross-site scripting
- Session hijacking
- NET deserialization
- Remote code execution
- Blind SQL injection
- Data exfiltration
- Bypassing file upload restrictions and file extension filters
- PHP type juggling with loose comparisons
- PostgreSQL Extension and User Defined Functions
- Bypassing REGEX restrictions
- Magic hashes
- Bypassing character restrictions
- UDF reverse shells
- PostgreSQL large objects
- DOM-based cross site scripting (black box)
- Server-side template injection
- Weak random token generation
- XML external entity injection
- RCE via database functions
- OS command injection via WebSockets (black box)

/ TARGET AUDIENCE

- Experienced penetration testers who want to better understand white box web app pentesting
- Web application security specialists
- Web professionals working with the codebase and security infrastructure of a web application

/ STUDENT REQUIREMENTS

- Comfort reading and writing at least one coding language
- Familiarity with Linux
- Ability to write simple Python / Perl / PHP / Bash scripts
- Experience with web proxies
- General understanding of web app attack vectors, theory, and practice

/ WHAT STUDENTS SHOULD BRING TO THE CLASS

- Their laptop

/ WHAT STUDENTS WILL BE PROVIDED WITH ONSITE

- Wi-Fi Internet

/ ABOUT THE EXAM

- The WEB-300 web application security course and online lab prepares you for the OSWE certification
- 48-hour exam
- Proctored

/ TITLE

PEN 300

ADVANCED EVASION TECHNIQUES AND BREACHING DEFENSES (OSEP)

USD 8,500

/ TRACK

Penetration Testing

/ SKILL LEVEL

Advanced

/ DURATION

5 Days

/ DATES

Sat 18 Nov - Wed 22 Nov

/ SUMMARY

Evasion Techniques and Breaching Defenses (PEN-300) is an advanced penetration testing course. Learners who complete the course and pass the exam will earn the OffSec Experienced Pentester (OSEP) certification. This course builds on the knowledge and techniques taught in Penetration Testing with Kali Linux, teaching learners to perform advanced penetration tests against mature organizations with an established security function and focuses on bypassing security mechanisms that are designed to block attacks. The OSEP is one of three certifications making up the OSCE3 certification along with the OSWE for advanced web attacks and OSED for exploit development.

/ DETAILED DESCRIPTION

- Take penetration testing skills to new heights with Evasion Techniques and Breaching Defenses (PEN-300) from Offensive Security. We set a strong foundation with our industry-leading Penetration Testing with Kali Linux (PWK) course, and are bringing students to the next level with this advanced pentesting training course.

- PEN-300 teaches the skills necessary to bypass many different types of defenses while performing advanced attacks that avoid detection. Students who complete the course and pass the exam earn the Offensive Security Experienced Penetration Tester (OSEP) certification, demonstrating their ability to perform advanced penetration tests against mature organizations.

/ BENEFITS

- Preparation for more advanced Penetration Testing 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

/ Agenda / Topics

- Operating System and Programming Theory
- Client Side Code Execution With Office
- Client Side Code Execution With Jscript
- Process Injection and Migration
- Introduction to Antivirus Evasion
- Advanced Antivirus Evasion
- Application Whitelisting
- Bypassing Network Filters
- Linux Post-Exploitation
- Kiosk Breakouts
- Windows Credentials
- Windows Lateral Movement
- Linux Lateral Movement
- Microsoft SQL Attacks
- Active Directory Exploitation
- Combining the Pieces
- Trying Harder: The Labs

/ TARGET AUDIENCE

- PEN-300 is an advanced course designed for OSCP-level penetration testers who want to develop their skills against hardened systems
- Job roles like senior penetration tester, security researcher, application penetration tester, and any software developer working on security products could benefit from the course

/ STUDENT REQUIREMENTS

- Solid ability in enumerating targets to identify vulnerabilities
- The ability to identify and exploit vulnerabilities like SQL injection, file inclusion, and local privilege escalation
- A foundational understanding of Active Directory and knowledge of basic AD attacks

/ WHAT STUDENTS SHOULD BRING TO THE CLASS

- Their Laptop

/ WHAT STUDENTS WILL BE PROVIDED WITH ONSITE

- Wi-Fi Internet

/ ABOUT THE EXAM

- The PEN-300 course and online lab prepares you for the OSEP certification
- 48-hour exam
- Proctored

/ TITLE

SOC 200

SECURITY OPERATIONS AND DEFENSIVE ANALYSIS (OSDA)

USD 8,500

/ TRACK

Defense, Risk, Pentesting

/ SKILL LEVEL

Advanced

/ DURATION

5 Days

/ DATES

Sat 18 Nov - Wed 22 Nov

/ SUMMARY

Learn the foundations of cybersecurity defense with Foundational Security Operations and Defensive Analysis (SOC-200), a course designed for job roles such as Security Operations Center (SOC) Analysts and Threat Hunters. Learners gain hands-on experience with a SIEM, identifying and assessing a variety of live, end-to-end attacks against a number of different network architectures. Learners who complete the course and pass the exam earn the OffSec Defense Analyst (OSDA) certification, demonstrating their ability to detect and assess security incidents.

/ DETAILED DESCRIPTION

- Learn the foundations of cybersecurity defense with Offensive Security's new Security Operations and Defensive Analysis (SOC-200) course on security operations.
- OffSec set the industry standard with Penetration Testing with Kali Linux (PWK), teaching students how to perform practical attacks against networks and systems. Now with SOC-200 we reveal the consequences of common attacks from a defensive perspective.
- Students who complete the course and pass the associated exam earn the Offensive Security Defense Analyst (OSDA) certification, demonstrating their ability to detect and assess security incidents. A certified OSDA candidate is prepared to join and participate in a Security Operations Center (SOC) as a Junior Analyst.

/ BENEFITS

- Learn how attackers operate with the MITRE ATT&CK® framework
- Audit Windows and Linux endpoints
- Review common attacks
- Use a SIEM to track adversaries

/ AGENDA / TOPICS

- Attacker Methodology Introduction
- Windows Endpoint Introduction
- Windows Server Side Attacks
- Windows Client-Side Attacks
- Windows Privilege Escalation
- Windows Persistence
- Linux Endpoint Introduction
- Linux Server Side Attacks
- Network Detections
- Antivirus Alerts and Evasion
- Network Evasion and Tunneling
- Active Directory Enumeration
- Windows Lateral Movement
- Active Directory Persistence
- SIEM Part One: Intro to ELK
- SIEM Part Two: Combining the Logs
- Exam

/ TARGET AUDIENCE

- Job roles like: Security Operations Center (SOC) Tier 1, Tier 2 and Tier 3 Analysts, Jr. roles in Threat Hunting and Threat Intelligence Analysts, Jr. roles in Digital Forensics and Incident Response (DFIR)
- Anyone interested in detection and security operations, and/or committed to the defense or security of enterprise networks

/ STUDENT REQUIREMENTS

- All prerequisites for SOC-200 can be found within the Offsec Fundamentals Program, included with a Learn Subscription
- Prerequisite Topics include:
  - SOC-100: Linux Basics 1 & 2
  - SOC-100: Windows Basics 1 & 2
  - SOC-100: Networking Basics

/ WHAT STUDENTS SHOULD BRING TO THE CLASS

- Their Laptop

/ WHAT STUDENTS WILL BE PROVIDED WITH ONSITE

- Wi-Fi Internet

/ ABOUT THE EXAM

- The OSDA Exam Scheduling Open Now
- The SOC-200 course prepares you for the OSDA certification
- Proctored

/ TITLE

PEN 200

PENTESTING WITH KALI (PWK)

USD 8,500

/ TRACK

Penetration Testing

/ SKILL LEVEL

Advanced

/ DURATION

5 Days

/ DATES

Sat 18 Nov - Wed 22 Nov

/ SUMMARY

The industry-leading Penetration Testing with Kali Linux (PWK/PEN-200) course introduces penetration testing methodologies, tools and techniques via hands-on experience and is self-paced. Learners who complete the course and pass the exam will earn the OffSec Certified Professional (OSCP) certification which requires holders to successfully attack and penetrate various live machines in a safe lab environment. The OSCP is considered to be more technical than other ethical hacking certifications and is one of the few that requires evidence of practical penetration testing skills.

/ DETAILED DESCRIPTION

- Penetration Testing with Kali Linux (PWK) is an online pentesting course designed for security professionals and network administrators who want to take a serious and meaningful step into the world of professional penetration testing. This best-in-class training course introduces students to the latest ethical hacking tools and techniques, including remote, virtual penetration testing labs for practicing the course materials.
- PWK simulates a full penetration test from start to finish by immersing the student into a target-rich and vulnerable network environment. Students who pass the exam earn the industry-leading OSCP certification.

/ BENEFITS

- Learn how to become a penetration tester by 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

/ BENEFITS [cond.]

- Leveraging tunneling techniques to pivot between networks
- Creative problem-solving and lateral thinking skills

/ AGENDA / TOPICS

- Introduction to Cybersecurity
- Effective Learning Strategies
- Report Writing for Penetration Testers
- Information Gathering
- Vulnerability Scanning
- Introduction to Web Applications
- Common Web Application Attacks
- SQL Injection Attacks
- Client-Side Attacks
- Locating Public Exploits
- Fixing Exploits
- Antivirus Evasion
- Password Attacks
- Windows Privilege Escalation
- Linux Privilege Escalation
- Advanced Tunneling
- The Metasploit Framework
- Active Directory Introduction and Enumeration
- Attacking Active Directory Authentication
- Lateral Movement in Active Directory
- Assembling the Pieces
- Trying Harder: The Labs

/ TARGET AUDIENCE

- Infosec professionals transitioning into penetration testing
- Pentesters seeking one of the best pentesting certifications
- Those interested in pursuing a penetration tester career path Security professionals
- Network administrators
- Other technology professionals

/ STUDENT REQUIREMENTS

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

/ WHAT STUDENTS SHOULD BRING TO THE CLASS

- Their Laptop

/ WHAT STUDENTS WILL BE PROVIDED WITH ONSITE

- Wi-Fi Internet

/ ABOUT THE EXAM:

- The PEN-200 course and online lab prepares you for the OSCP penetration testing certification
- 24-hour exam
- Proctored

/ TITLE

WEB ATTACKS WITH KALI LINUX (OSWA)

USD 8,500

/ TRACK

Penetration Testing

/ SKILL LEVEL

Advanced

/ DURATION

5 Days

/ DATES

Sat 18 Nov - Wed 22 Nov

/ SUMMARY

Learn the foundations of web application assessments with Foundational Web Application Assessments with Kali Linux (WEB-200). Learners who complete the course and pass the exam will earn the OffSec Web Assessor (OSWA) certification and will demonstrate their ability to leverage web exploitation techniques on modern applications. This course teaches learners how to discover and exploit common web vulnerabilities and how to exfiltrate sensitive data from target web applications. Learners that complete the course will obtain a wide variety of skill sets and competencies for web app assessments.

/ DETAILED DESCRIPTION

- Learn the foundations of web application assessments with Offensive Security's new course, Web Attacks with Kali Linux (WEB-200).
- WEB-200 teaches students how to discover and exploit common web vulnerabilities, and how to exfiltrate sensitive data from target web applications. Students will obtain a wide variety of skill sets and competencies for web app assessments.
- Students who complete the course and pass the associated exam earn the Offensive Security Web Assessor (OSWA) certification, demonstrating their ability to leverage modern web exploitation techniques on modern applications. A certified
- OSWA candidate is prepared to take on the Advanced Web Attacks and Exploitation (WEB-300) course.

/ BENEFITS

- Perform stored and reflected XSS
- Attack four common database management systems with SQLi
- Exploit six different templating engines often leading to RCE with SSTI

/ AGENDA / TOPICS

- Tools for the Web Assessor
- Cross-Site Scripting (XSS) Introduction, Discovery, Exploitation and Case Study
- Cross-Site Request Forgery (CSRF)
- Exploiting CORS Misconfigurations
- Database Enumeration
- SQL Injection (SQLi)
- Directory Traversal
- XML External Entity (XXE) Processing
- Server-Side Template Injection (SSTI)
- Server-Side Request Forgery (SSRF)
- Command Injection
- Insecure Direct Object Referencing
- Assembling the Pieces: Web Application Assessment Breakdown

/ TARGET AUDIENCE

- Job roles like: Web Penetration Testers, Pentesters, Web Application Developers, Application Security Analysts, Application Security Architects, and SOC Analysts and other blue team members
- Anyone interested in expanding their understanding of Web Application Attacks, and/or Infra Pentesters looking to broaden their skill sets and Web App expertise

/ STUDENT REQUIREMENTS

- All prerequisites for WEB-200 can be found within the Offsec Fundamentals Program, included with a Learn subscription
- Prerequisite Topics include:
- WEB-100: Web Application Basics
- WEB-100: Linux Basics 1 & 2
- WEB-100: Networking Basics

/ WHAT STUDENTS SHOULD BRING TO THE CLASS

- Their Laptop

/ WHAT STUDENTS WILL BE PROVIDED WITH ONSITE

- Wi-Fi Internet

/ ABOUT THE EXAM

- The OSWA exam is a proctored exam
- The WEB-200 course and online lab prepares you for the OSWA certification