⚑ **Location: https://offensivesec.org**

📅 **Date: Saturday 17th & Sunday 18th October 2026**

🕓 **Time: 12 noon to 8pm UK (BST)**

🏆 PRIZE DRAW — WIN YOUR FULL COURSE FEE BACK

Every attendee is automatically entered. One student walks away with a complete refund.

https://offensivesec.org

Mainframe Offensive Security Testing Course

Instructor: Kev Milne

Course Overview

This unique two-day mainframe hacking course provides practical techniques for conducting effective mainframe penetration tests. Delivered over weekends only, the course takes place in a secure, remote-access lab environment where the instructor actively teaches and shadows students throughout.

The course is suitable for mainframers, penetration testers, and those pivoting into cyber security roles. As the only publicly available course of its kind, designed and priced to be accessible to both corporate clients and individual learners, it offers significant value and will give you or your team a distinct competitive edge.

The course covers the fundamentals of mainframes and penetration testing, with a strong emphasis on hands-on learning to ensure students can fully develop their skills. This latest run features **brand new scripts, tooling and techniques** developed since the last course, so newcomers and returning students alike will be working with the very latest mainframe offensive tradecraft. It also includes a Capture the Flag (CTF) challenge and provides a certificate of completion.

Early bird and student discounts are always available, and all participants are entered into a **prize draw where one student will win a full course refund.**

Early bird £450 until 16th September 2026, then £700 full price.

Student discounts also available – check for the latest offers.

Student Lab Checklist

Before attending this course, please ensure the following:

- ✔ Basic Linux skills or completion of pre-course materials
- ✔ Laptop with a modern web browser (Chrome, Firefox, or Edge)
- ✔ Second screen to view Zoom sessions comfortably
- ✔ Reliable internet connection

⚑ **Location: https://offensivesec.org**
📅 **Date: Saturday 17th & Sunday 18th October 2026**
🕓 **Time: 12 noon to 8pm UK (BST)**

2-Day Agenda

(Hands-on, Instructor-led, Remote Labs)
Featuring brand new scripts, tooling and techniques.

Day 1 — Foundations & Reconnaissance

Morning Session

- Course Introduction & Setup
- Overview of IBM zSeries
- Mainframe Architecture & Terminology
- x3270 Terminal Usage
- TSO & ISPF Basics
- RACF Overview
- UNIX System Services (USS) on z/OS
- NMAP Scanning and Mainframe Scripts
- Reconnaissance: Identifying Open Services & Entry Points

Afternoon Session

- Network Attacks (MITM, TN3270 sniffing)
- Brute Forcing: FTP, TSO, CICS logons
- OSINT Techniques for Mainframes
- Practical Lab: Scanning & Recon Exercises
- Practical Lab: Access Enumeration & Information Gathering

⚑ **Location: https://offensivesec.org**

📅 **Date: Saturday 17th & Sunday 18th October 2026**

🕛 **Time: 12 noon to 8pm UK (BST)**

Day 2 — Exploitation & Post-Exploitation

Morning Session

- Privilege Escalation Paths
- CICS Security Testing & Exploitation (DVCA, CICSPWN)
- Mainframe Application Flaws (KICKS, CICS Trans IDs)
- REXX & JCL for Post-Exploitation

Afternoon Session

- RACF Database Extraction & Analysis
- Cracking RACF Hashes (John The Ripper, DES/KDF)
- NMAP NSE Scripts (tn3270, cics-enum, tso-enum)
- CTF-Style Final Lab: Full Mainframe Attack Simulation
- Course Wrap-Up & Q&A
- Certification Exam (Multiple-choice) & CTF Results

Notes

- Maximum of 10 students per class to ensure the best possible learning experience
- Secure, remote-access lab with instructor support and shadowing
- Weekend-only delivery (Saturday 17th & Sunday 18th October 2026, 12 noon to 8pm UK / BST)
- Brand new scripts, tooling and techniques included in this run
- Includes CTF Challenge & Certificate of Completion
- **Early bird £450 until 16th September, then £700 – Check Eventbrite!**
- **Prize draw — one student will win a full course refund!**