

EVIL MAINFRAME

AT-A-GLANCE



INFO@EVILMAINFRAME.COM



[HTTPS://EVILMAINFRAME.COM](https://evilmainframe.com)



@EVILMAINFRAME

- TWO DAY CLASS
 - ON-SITE PRIVATE LPAR (MAINFRAME)
 - WORLDS ONLY MAINFRAME CTF
-

EVIL MAINFRAME – WORLDS ONLY HANDS ON MAINFRAME PENETRATION TESTING CLASS

Mainframes make up the lion's share of back-end systems at fortune 500s. Yet, pentesters know almost nothing about how to scope and conduct a penetration test against them. More and more we're seeing auditors and PCI QSA's no longer giving the mainframe a pass. When it's time for you to conduct a mainframe penetration test will you be ready?

This course exposes attendees to a live mainframe environment with over 12, hands on, lab experiences. The areas explored in this course include VTAM, CICS, TSO, and Unix. Students are given access to this z/OS mainframe environment for the duration of the course where they will learn to navigate the operating system, learn misconfiguration targets and privilege escalation techniques.

They will get introduced to the open source tools and libraries available for all the steps of a penetration test including Nmap, python, and Metasploit as well as writing their own tools using using REXX, JCL, and C. This class is outlined as a beginner class to mainframe hacking the attendee should have knowledge of IT security, penetration testing and very basic Python.

At the end of the class students will be able to put their skills to the test by forming teams and trying to win the worlds only mainframe CTF with challenges that range from easy to very difficult.

I HACKED THE MAINFRAME