Reverse engineering is a vital skill for those in the field of information security to properly safeguard organizations from external threats. Participant will learn to recognize high level language constructs by performing binary analysis and discover the underlying nature of any Windows binary. This Bootcamp will familiarize participants with all aspects of reverse engineering (reversing) Linux 32-bit & Windows 32-bit applications for the purposes of locating flaws and exploiting them.

This real-time immersive virtual-lead workshop uses a combination of lecture, real-world experiences, and hands-on exercises to teach you the techniques to test the security of tried-and-true internal enterprise web technologies, as well as cutting-edge Internet-facing application.

By the end of this Workshop, Participants will be able to:

- Understand, locate & exploit all of the common flaws in 32-bit Linux & Windows based binaries - flaws include, but are not limited to, buffer overflow, heap overflows, format string flaws, section overflows, and kernel flaws.
- Perform dissection of binaries to locate overflow based vulnerabilities, play with branching and control of the program and exploit vulnerable functionalities left by developers
- Gauge and able to understand and infer the control flow of the programs to assist them in further course of reverse engineering
- Will be able to automate flaw discovery
- Access & experience the state-of-art real world training lab setup

Supported by: ENCIPHERS

Exclusive by: THOMVELL international