Forensics w systemie Linux

Poziom ekspercki

Agenda:

- Biały wywiad na podstawie narzędzi w systemach Linux
- Linux jako narzędzie wykonywania kopii binarnych - lokalnych i sieciowych
- SED, GREP, AWK
- Narzędzia do analizy tablicy MFT
- Analiza osi czasu systemu Windows
- Analizy binarnych plików - pagefile.sys, hiberfile, SPL, SHD, RAM,
- Zaawansowana analiza pamięci operacyjnej
- Odzyskiwanie plików z wykorzystaniem systemu Linux
- Steganografia w systemie Linux
- Analiza logów w systemie Linux
- Analiza strategicznych miejsc w systemie Linux
- Analiza ruchu sieciowego na podstawie darmowych narzędzi
- Gotowe platformy analityczne - przedstawienie i omówienie
- Kali Linux USB z trybem zapisywania zmian

Gdzie: **ForSec SA**
ul. 73 Pułku Piechoty 7A
40-496 Katowice
lub szkolenie on-line

Czas: **3 dni (9:00 - 15:30)**

FORSEC
Forensics&Security