



SEKURAK.ACADEMY

CERTYFIKAT

UCZESTNICTWA W SZKOLENIU SEKURAK.ACADEMY 2024

ANALIZA POWŁAMANIOWA W LINUXSIE

DLA

Marcin Kołodziejczyk

DATA: 19.02.2024 R.

TRENER: Tomasz Turba

CZAS TRWANIA: 3 GODZINY

AGENDA

PRZYGOTOWANIE POLA BITWY – POKAZY PRAKTYCZNE

- Wykonanie ataków na infrastrukturę
- Wykonanie ataków na aplikację webową

WPROWADZENIE DO ANALIZY INCYDENTÓW BEZPIECZEŃSTWA

- Omówienie faz Cyber Kill Chain i zagrożenia APT
- Potencjalne architektury dla monitoringu i reagowania na incydenty
- Zabezpieczanie materiałów, normy, procedury, dokumentacja
- Monitoring ruchu sieciowego (logi i onelinery)

TECHNIKI ANALIZY POWŁAMANIOWEJ – POKAZY PRAKTYCZNE

- Analiza hosta i obrazu dysku twardego
- Analiza pamięci ulotnej RAM
- Analiza ruchu sieciowego na podstawie zrzutu PCAP
- Analiza dużych porcji danych – logów

DOBRE RADY ADMINISTRATORA W FORMIE SESJI Q&A

PUNKTY CPE/ECE: 3

SZKOLENIA.SECURITUM.PL