securITum

CERTYFIKAT

UCZESTNICTWA W SZKOLENIU

WPROWADZENIE DO BEZPIECZEŃSTWA LINUX, CZĘŚĆ I (LOGI, PODSTAWY ANALIZY POWŁAMANIOWEJ)

DLA:

Andrii Kartashov

DATA	TRENER	CZAS TRWANIA
5.02.2024 R.	Karol Szafrański	3.5 GODZINY

AGENDA

Logi i więcej: wszystkie możliwe źródła zapisanych zdarzeń

- ✓ Syslog, journald i dmesg – co, gdzie i dlaczego jest logowane (lub nie)
- ✓ Gdzie i jak poza /var/log szukać logów usług i aplikacji
- ✓ Nie tylko historia Basha – przydatne ślady po użyciu narzędzi administracyjnych/programistycznych
- ✓ Auditd/SELinux – czego ciekawego można się dowiedzieć z ich logów
- ✓ Co się dzieje w kontenerach
- ✓ Metryki wydajności (CPU/RAM/IO) a włamania i analiza powłamaniowa
- ✓ O prewencji – jak sensownie zbierać logi, jak silnie monitorować najważniejsze dla nas procesy i pliki

Analiza i wizualizacja aktywności sieciowej

- ✓ Czy można zauważyć nietypowy ruch (eksfiltracja danych, komunikacja z C2), nie mając dużego i ciężkiego IDS-a
- ✓ Nie tylko tcpdump i Wireshark – garść mniej znanych narzędzi, które warto mieć pod ręką

Przegląd technik ukrywania się stosowanych przez włamywaczy oraz sposoby ich wykrywania

- ✓ Fałszywe nazwy procesów, pozornie nieistniejące/ukryte pliki i inne triki
- ✓ Nieoczywiste lokalizacje złośliwych plików i ustawień, persystencja

PUNKTY CPE/ECE: 3.5