BEZPIECZEŃSTWO SYSTEMÓW IT
SECURITUM

SZKOLENIE

Powłamaniowa analiza incydentów bezpieczeństwa IT

Grupa docelowa

Administratorzy systemów | Administratorzy sieci | Pracownicy SOC

Poziom zaawansowania

★ ★ ★

O SZKOLENIU

- Umożliwia poznanie metod analizy oraz szukania anomalii w dużych porcjach informacji związanych z incydentem bezpieczeństwa IT.
- Prowadzone jest w formie „hands-on" – uczestnicy samodzielnie analizują realne incydenty bezpieczeństwa w infrastrukturze IT firmy.
- Część praktyczną poprzedza wprowadzenie teoretyczne, przedstawiające m.in. sposoby szeregowania faz oraz możliwości analizy incydentów bezpieczeństwa
- Jest kierunkowane na techniki analizy oraz szukania anomalii w dużych zbiorach danych, zarówno w plikach tekstowych, jak i zrzutach ruchu sieciowego.

Dodatkowe informacje
https://goo.gl/vFWBen

Zamówienie szkolenia
https://goo.gl/RkSVR1

UCZESTNICY O SZKOLENIU

- *Konkretne, techniczne podejście, jasno wyjaśnione narzędzia, komendy.*
- *Tematyka, bardzo dobra agenda, ciekawe ćwiczenia.*
- *Bardzo dobre przygotowanie prowadzącego.*
- *Bardzo dobrze skonfigurowane i przygotowane środowisko.*
- *Dużo konkretnej i praktycznej wiedzy.*
- *Angażowało szare komórki.*
- *Nacisk na ćwiczenia i zrozumienie mechanizmów.*

RAMOWY PROGRAM SZKOLENIA

Wprowadzenie do KillChain

- Czym jest KillChain?
- Omówienie KillChain oraz metod detekcji i prewencji dla każdej z faz
- Studium przypadku KillChain

Omówienie metod detekcji oraz analizy ataków cybernetycznych

- Monitoring ruchu sieciowego (logi)
- Omówienie źródeł logowania (np. FW, Proxy, DNS, AV, (H)IPS/IDS)
- Omówienie retencji danych
- Monitoring ruchu sieciowego (przechwytywanie ruchu, full packet capture)
- Omówienie źródeł logowania oraz wykluczeń
- Omówienie retencji danych
- Analiza hosta (krótkie omówienie jej możliwości i narzędzi wykonania)
- Analiza pamięci oraz obrazu dysku twardego
- Analiza podstawowych informacji systemowych
- Obróbka plików pcap w command line: tshark, tcpdump, bro

Analiza przypadku – atak prosty z wykorzystaniem złośliwego oprogramowania

- Identyfikacja pracowników oraz infrastruktury informatycznej przedsiębiorstwa – praca w grupie
- Przeglądanie oraz obróbka dużych ilości logów w systemie Linux – praca w grupie
- Przeglądanie oraz obróbka plików pcap – praca w grupie
- Analiza incydentu z rozpisaniem na fazy KillChain – praca w grupie
- Prezentacja rozwiązania
- Możliwości zabezpieczenia przed incydentem z punktu widzenia KillChain – dyskusja

Analiza przypadku – atak złożony z wykorzystaniem złośliwego oprogramowania

- Przeglądanie oraz obróbka dużych ilości logów w systemie Linux – praca w grupie
- Przeglądanie oraz obróbka plików pcap – praca w grupie
- Analiza incydentu ze szczątkowych danych z rozpisaniem na fazy KillChain – praca w grupie
- Porównanie wyników analizy – prezentacja
- Możliwości zabezpieczenia przed incydentem z punktu widzenia KillChain – dyskusja

SZKOLENIE POLECAJĄ

ROSWALTO
sekurak.pl
programista

TRENER

Marcin Szymankiewicz

- Lider zespołu Cyber Security w globalnej korporacji
- Ponad 3 lata doświadczenia w monitoringu, budowaniu detekcji oraz analizie incydentów bezpieczeństwa z wykorzystaniem różnych narzędzi i technik
- Ponad 10 lat doświadczenia w projektowaniu i utrzymaniu sieci komputerowych oraz konfiguracji usług i serwerów systemu Linux
- Członek polskiego zespołu The Honeynet Project, aktywny szkoleniowiec w ramach projektu na międzynarodowych warsztatach
- Autor serii artykułów na portalu oraz w zinie sekurak.pl

PUBLIKACJE

- *Deobfuskacja JavaScript* goo.gl/KE1921
- *Deobfuskacja JavaScript – część druga. JSDetox na przykładzie realnego malware* goo.gl/qxr1ET
- *Deobfuskacja JavaScript – część trzecia* goo.gl/Em6Zgb

ZAPISZ SIĘ

Zamówienie szkolenia
https://goo.gl/RkSVR1

Dodatkowe informacje
https://goo.gl/vFWBen

< SZKOLENIA@SECURITUM.PL >