Szkolenie HoneyINT: OSINT + Honeypoty w praktyce obronnej

Opis szkolenia: HoneyINT to szkolenie, które łączy OSINT i honeypoty w jeden spójny system wczesnego wykrywania aktywności ofensywnej w infrastrukturze IT. Zamiast reagować na incydenty, uczysz się wykrywać rekonesans i próby ataku zanim dojdzie do włamania. To szkolenie o analizie danych, korelacji sygnałów i podejmowaniu decyzji operacyjnych - nie o instalacji narzędzi.

Kod szkolenia: OSI-HoneyINT-01

Kategoria: OSINT / BLUE TEAM

Trenerka: Beata Zalewa

Czas trwania: 2 dni / 16 godzin (9:00 – 17:00)

Poziom zaawansowania: Podstawowy

Język wykładowy: język polski

Forma szkolenia: zdalne. Po wcześniejszym uzgodnieniu możliwe szkolenie w siedzibie klienta.

Materiały: w języku polskim. Na życzenie klienta materiały w języku angielskim.

Wymagania wstępne:

- do udziału w szkoleniu wymagany jest komputer, na którym można uruchomić maszynę wirtualną lub dostęp do serwera VPS, na którym będzie można przygotować środowiska wg instrukcji i zainstalować honeypoty i narzędzia OSINT
- instancja WordPress (testowa)
- dostęp do wygenerowanych przez honeypoty i aplikacje logów (web / systemowych)

Grupa decelowa:

Szkolenie jest przeznaczone dla osób, które:

- zarządzają serwerami i infrastrukturą (Linux / Windows / infrastruktura webowa / WordPress / chmura)
- analizują logi
- pracują jako DevSecOps / SysAdmin / specjalista Security
- odpowiadają za bezpieczeństwo aplikacji lub sieci
- chcą przejść z podejścia reaktywnego na wyprzedzające
- chcą zrozumieć realne techniki rekonesansu i wykrywania ataków

Cel szkolenia: Głównym celem tego szkolenia jest wyposażenie uczestników w zaawansowane umiejętności z zakresu białego wywiadu (OSINT) oraz aktywnej obrony z wykorzystaniem technologii honeypotów (HoneyINT). Uczestnicy nauczą się projektować, wdrażać i monitorować pułapki sieciowe, aby skutecznie wykrywać, analizować i opóźniać ataki cybernetyczne. Ważnym aspektem kursu jest również integracja informacji o atakujących z danymi z otwartych źródeł w celu precyzyjnego profilowania zagrożeń i zrozumienia taktyk przestępców. Szkolenie ma na celu przekształcenie biernej ochrony infrastruktury IT w

proaktywną strategię defensywną, która znacząco zwiększy bezpieczeństwo organizacji. Ponadto kursanci zdobędą praktyczną wiedzę o tym, jak bezpiecznie wyciągać cenne wnioski wywiadowcze (Threat Intelligence) z interakcji intruzów z fałszywymi zasobami.

Efekty szkolenia:

- Uczestnik potrafi zbudować mapę powierzchni ataku, która później będzie determinowała rozmieszczenie honeypotów.
- Uczestbik rozumie, co honeypot realnie wykrywa i potrafił(a) zaprojektować honeypoty na podstawie zebranych danych z OSINT, dopasowanie rozwiązanie do realnych wymagań infrastruktury i minimalizować szum i fałszywie pozytywne sygnały.
- Uczestnik potrafi rozpoznać automatyczne skanowanie i oddzielić je od realnego targetowania.
- Uczestnik potrafi korelować dane z OSINT i honeypotów w celu identyfikacji wzorców ataków, rozróżniać przypadkowy ruch od ukierunkowanej aktywności oraz określać moment wymagający reakcji operacyjnej.

Co otrzymasz?

- Materiały szkoleniowe.
- Szkolenie kończy się certyfikatem uczestnictwa.

Agenda szkolenia

Godzina	Czas trwania	Moduł	Forma
Dzień 1			
9:00 – 9:15	15 minut	**Moduł 1: Powitanie i omówienie**	Powitanie
9:15 – 10:30	75 minut	**Moduł 2: Identyfikacja powierzchni ataku i analiza rekonesansu**	Teoria, przykłady
10:30 – 10:45	15 minut	Przerwa	-
10:45 – 12:30	105 minut	**Moduł 2: Identyfikacja powierzchni ataku i analiza rekonesansu**	Laboratorium praktyczne, analiza wyników
12:30 – 13:00	30 minut	Przerwa obiadowa	-

Godzina	Czas trwania	Moduł	Forma
13:00 – 15:00	120 minut	**Moduł 3: Projektowanie honeypotów w oparciu o dane OSINT**	Teoria, przykłady
15:00 – 15:15	15 minut	Przerwa	-
15:15 – 16:45	90 minut	**Moduł 3: Projektowanie honeypotów w oparciu o dane OSINT**	Laboratorium praktyczne, analiza wyników
16:45 – 17:00	15 minut	**Sesja Q&A**	Pytania
Dzień 2			
9:00 – 9:15	15 minut	**Podsumowanie dnia pierwszego**	Podsumowanie
9:15 – 10:30	75 minut	**Moduł 4: Wykrywanie botów, skanowania i prób exploitacji**	Warsztaty
10:30 – 10:45	15 minut	Przerwa	-
10:45 – 12:30	105 minut	**Moduł 4: Wykrywanie botów, skanowania i prób exploitacji**	Warsztaty
12:30 – 13:00	30 minut	Przerwa obiadowa	-
13:00 – 15:00	120 minut	**Moduł 5: Łączenie sygnałów i identyfikacja wzorców ataków**	Warsztaty
15:00 – 15:15	15 minut	Przerwa	-
15:15 – 16:45	90 minut	**Moduł 5: Łączenie sygnałów i identyfikacja wzorców ataków**	Warsztaty

Godzina	Czas trwania	Moduł	Forma
16:45 – 17:00	15 minut	**Moduł 6: Podsumowanie, pytania i dalsze kroki**	Dyskusja, Q&A, materiały końcowe

Szczegółowy program szkolenia

Moduł 1: Wprowadzenie i cele szkolenia

Przedstawienie programu, celów i wartości szkolenia.

Moduł 2: Identyfikacja powierzchni ataku i analiza rekonesansu

Jak realnie wygląda rekonesans widziany „z zewnątrz", jak go wykrywać oraz jak mapować powierzchnię ataku (*attack surface*) organizacji na podstawie danych publicznych.

Zakres:

- identyfikacja subdomen, usług i ekspozycji infrastruktury
- analiza technologii backend / CMS / frameworków
- wykrywanie śladów automatycznego skanowania

Przykładowe narzędzia:

- **amass** – enumeracja subdomen i relacji DNS
- **theHarvester** – email, domeny, metadane
- **Shodan** – ekspozycja usług i portów
- **SpiderFoot** – integruje wiele źródeł (Shodan, WHOIS, DNS, wycieki danych (*leaks*))
- **Recon-ng** – automatyzacja OSINT
- **Photon** – crawler aplikacji web, pasuje pod WordPress + honeypoty HTTP

Moduł 3: Projektowanie honeypotów w oparciu o dane OSINT

Ten moduł skupia się na budowie warstwy obserwacyjnej opartej na rzeczywistej powierzchni ataku, a nie losowych usługach.

- typy honeypotów i ich zastosowanie
- gdzie i jak je umieszczać w infrastrukturze
- jak nie ujawnić honeypota

- jakie dane są wartościowe, a jakie są szumem
- wzorce zachowań atakujących
- kiedy użycie honeypota traci sens

Typy honeypotów omawiane na szkoleniu:

- SSH / Telnet honeypoty
- HTTP/HTTPS honeypoty (fake login panels)
- API honeypoty (REST endpoints)
- Honeypoty na WordPressa
- Honeypoty typu credential harvesting traps

Przykładowe narzędzia:

- Cowrie – symulacja SSH i logowanie ataków brute-force
- Dionaea – przechwytywanie exploitów i malware
- Honeytrap - nasłuchuje na portach i loguje próby połączeń
- Wordpot - symuluje WordPressa i zbiera próby logowania i exploitów
- OpenCanary – służy do wczesnego wykrywania intruzów i cyberataków wewnątrz sieci firmowej

Moduł 4: Wykrywanie botów, skanowania i prób exploitacji

Moduł skupia się na jednym z najczęstszych wektorów ataku w internecie: WordPressie, a także na aplikacjach internetowych.

- najczęstsze ataki na WordPress
- honeypoty jako fałszywe punkty wejścia
- wykrywanie brute-force i botów
- analiza prób exploitacji pluginów i wersji CMS (RCE, upload plików, LFI)
- fingerprinting narzędzi atakujących
- których honeypotów na Wordpresie osobiście, a z których zrezygnowałam i dlaczego

Przykładowe narzędzia:

- Wordfence – detekcja i firewall aplikacyjny
- WPScan – analiza podatności WordPress

- Fail2ban – blokowanie brute-force
- ModSecurity – reguły WAF dla HTTP
- Nginx – analiza logów i reverse proxy security

Przykładowe testy honeypotów na WordPressie:

- fałszywe panele logowania /wp-admin
- fałszywe plugin endpoints
- atrapy endpointów REST API i stron uploadu plików

Moduł 5: Łączenie sygnałów i identyfikacja wzorców ataków

Najważniejszy moduł operacyjny.

Zakres:

- przejście od danych do działania
- korelacja IP, user-agentów i fingerprintów
- połączenie OSINT + honeypoty + logi
- identyfikacja botnetów i narzędzi skanujących
- analiza timingów i sekwencji ataków
- budowa reguł detekcji
- priorytetyzacja zagrożeń, co ignorować, co eskalować
- wprowadzenie do automatyzacji reakcji

Przykładowe narzędzia:

- Elastic Stack (Elasticsearch, Kibana, Logstash) – korelacja logów
- Wazuh – SIEM + HIDS
- Grafana Loki – dashboardy metryk
- Graylog (wersja Open Source) – scentralizowany system zarządzania logami z wbudowanymi mechanizmami alertów i korelacji
- Zeek – analiza ruchu sieciowego

Moduł 6: Podsumowanie, pytania i dalsze kroki

Zebranie kluczowych wniosków, sesja Q&A oraz przekazanie materiałów dodatkowych i rekomendacji do dalszego rozwoju kompetencji w zakresie OSINT i honeypotów.

- Podsumowanie kluczowych zagadnień i wnioski.
- Sesja Q&A.
- Materiały dodatkowe i rekomendacje.

Zarejestruj się na szkolenie: szkolenia@zalnet.pl

https://zalnet.pl/edu/honeyint-honeypoty-osint-jako-system-wczesnego-wykrywania-atakow/

Szukasz szkolenia w godzinach wieczornych: https://zalnet.pl/slodka-promocja-na-dzien-ojca-kup-szkolenie-honeyint-i-zabierz-druga-osobe-gratis-tate-mame-lub-kolege-z-pracy/

Kup szkolenie w trybie wieczorowym: https://cart.easy.tools/checkout/zalnet/honeyint-osint-honeypoty-w-praktyce-obronnej