securitum

Netsecurity **Master** od sekuraka

Naucz się, jak skutecznie zabezpieczać infrastrukturę IT, poznając techniki stosowane przez atakujących!

11 4-godzinnych sesji szkoleniowych na żywo w przystępnej formule

MODUŁ 1

SZEŚĆ SESJI NA ŻYWO

2800 ZŁ NETTO

MODUŁ 2

PIĘĆ SESJI NA ŻYWO

2200 ZŁ NETTO

POŁĄCZ I ZYSKAJ

MODUŁ 1 i MODUŁ 2

~~5000~~ ZŁ NETTO

3990 ZŁ NETTO

DLACZEGO TEN KURS JEST TAK DOBRY

- Łącznie ponad 40 godzin praktycznej, warsztatowej wiedzy
- Minimum niezbędnej teorii, realne przykłady luk w zabezpieczeniach sieci, skuteczne sposoby ich eliminacji
- Wiedza zdobywana od doświadczonych administratorów/audytorów systemów IT
- Dostęp do dedykowanej platformy szkoleniowej i laboratorium sieciowego
- Dostęp do nagrań sesji szkoleniowych

KORZYŚCI DLA FIRMY I ZESPOŁU

- Skuteczniejsza identyfikacja potencjalnych ataków na infrastrukturę sieciową firmy
- Możliwość zastosowania poznanych metod ochrony przed atakami
- Umiejętność samodzielnego przeprowadzenia testów penetracyjnych
- Wzrost świadomości zespołu w zakresie skutków cyberprzestępstw
- Zwiększenie bezpieczeństwa w firmie

netsec.sekurak.pl

securITum

AGENDA

MODUŁ 1

Sesja nr 1: Rekonesans sieciowy i wyszukiwanie podatności:

- Skanowanie portów. Jak funkcjonują skanery portów? Na jakich portach działają poszczególne usługi? Wykorzystanie zaawansowanych filtrów oraz technik skanowania sieci (również bardzo dużych).
- Praktyczna metodologia związana z zarządzaniem wynikami skanów. Jak skutecznie skanować olbrzymie sieci i się nie pogubić?
- Fuzzing katalogów aplikacji webowych.
- Wstęp do OSINT-u. Wyszukiwanie domen, subdomen, adresów IP organizacji, jej zasobów chmurowych, zbieranie dodatkowych treści na podstawie nazwy organizacji i szczątkowych danych.
- Laboratorium do samodzielnej realizacji.

Sesja nr 2: Eksploitacja usług sieciowych. Bezpieczeństwo poczty:

- Sposoby wyszukiwania eksploitów w sieci. Samodzielna modyfikacja i tworzenie eksploitów. Wyszukiwanie tzw. *low-hanging fruits*.
- Metasploit: narzędzie do eksploitacji, ale również zarządzania procesem skanowania rozległych sieci.
- Sposoby na zdobycie i utrzymanie kontroli nad atakowanym urządzeniem (*persistence*). Wyjaśnienie pojęć: *reverse shell, bind shell, web shell, shell* typu *staged, stageless*.
- Typowe problemy związane z bezpieczeństwem usług SMTP.
- Laboratorium do samodzielnej realizacji.

Sesja nr 3: Poruszanie się w lokalnej sieci:

- Analiza lokalnego urządzenia – po uzyskaniu dostępu do niego. Zbieranie istotnych informacji o sieci LAN oraz samym urządzeniu.
- *Port forwarding, network pivoting*. Jak przeskakiwać pomiędzy kolejnymi podsieciami?
- Jak w sposób niewykrywalny skanować wewnętrzną sieć LAN, bez dostępu do skanera portów na przejętym urządzeniu?
- Laboratorium do samodzielnej realizacji.

Sesja nr 4: Bezpieczeństwo Wi-Fi. Techniki omijania antywirusów:

- WPA2-PSK, WPA2-MGT, WPA3, a może WEP? Uporządkowanie teorii.
- Rekonesans lokalnych sieci Wi-Fi.
- Praktyczne ataki na nowoczesne sieci Wi-Fi: od ataków na WPA2-PSK, przez Evil Twin, do downgrade'u połączenia WPA3.
- Schemat działania sposobów analizy statycznej oraz dynamicznej.
- Przykładowe techniki omijania antywirusów/EDR.
- Wprowadzenie do tematyki Command and Control.
- Wyszukiwanie serwerów C&C w Internecie.

Sesja nr 5: IDS/IPS:

- Podstawy działania systemów IDS/IPS.
- Wprowadzenie do konfiguracji oprogramowania Snort i Wazuh.
- Wykrywanie specyficznych sygnatur ruchu w lokalnej sieci z użyciem oprogramowania Snort.
- Laboratorium do samodzielnej realizacji.

Sesja nr 6: Wieloetapowe zadanie praktyczne podsumowujące moduł szkoleniowy

MODUŁ 2

Sesja nr 1: Problemy związane z bezpieczeństwem systemu Linux:

- Zbieranie informacji o lokalnym systemie i usługach w sieci.
- Typowe sposoby na zwiększenie uprawnień na urządzeniu.
- Ukrywanie backdoorów.
- Hardening i obrona przed atakami (SELinux, AppArmor, *sandboxing*, zasada najniższych uprawnień, minimalizacja powierzchni ataku, *hardening* kernela, szyfrowanie danych w spoczynku).
- Laboratorium do samodzielnej realizacji.

Sesja nr 2: Problemy bezpieczeństwa systemu Windows:

- Zbieranie informacji o lokalnym systemie i usługach w sieci.
- Ataki na konta i hasła użytkowników.
- Typowe sposoby na zwiększenie uprawnień na urządzeniu.
- Ukrywanie backdoorów. Obfuskacja i unikanie detekcji.
- *Hardening* i obrona przed atakami (*hardening* protokołów Windows, bezpieczeństwo kont lokalnych, minimalizacja powierzchni ataku, szyfrowanie danych w spoczynku).

Sesja nr 3: Podstawy Active Directory z perspektywy pentestera:

- Techniki pozwalające na łatwe zdobywanie poświadczeń kolejnych urządzeń po zdobyciu dostępu do sieci LAN.
- Enumeracja Active Directory i wyszukiwanie typowych podatności.
- Sprawdzone sposoby na proste przejęcie poświadczeń istotnych użytkowników i kontrolera domeny.

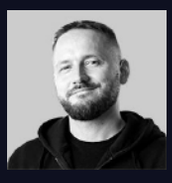
Sesja nr 4: Podstawy bezpieczeństwa Dockera i Kubernetesa:

- Ataki na kontenery/demon Docker/Kubernetes.
- Podstawowe zasady bezpiecznej konfiguracji Dockera/Kubernetesa.
- Laboratorium do samodzielnej realizacji.

Sesja nr 5: Wieloetapowe zadanie praktyczne podsumowujące moduł szkoleniowy

PROWADZĄCY

Marek Rzepecki



Tomasz Turba

Kamil Jarosiński

securITum

DLA KOGO

- Administratorzy IT
- Pracownicy SOC
- Pracownicy działów bezpieczeństwa
- Pentesterzy
- Osoby odpowiedzialne za wdrożenia zabezpieczeń w firmach

ZAPISY I SZCZEGÓŁY

netsec.sekurak.pl

Dodatkowe pytania: e-mail: szkolenia@securitum.pl
tel. +48 (12) 352 33 82