ZESTAWIENIE SZKOLEŃ E-LEARNINGOWYCH

L. P.	NAZWA SZKOLENIA	ZAGADNIENIA SZKOLENIOWE	ILOŚĆ GODZIN
1	**Akademia bezpieczeństwa**	**Wprowadzenie do OSSTMM i Hakowania** • Hakowanie złośliwego oprogramowania o Techniki hakowania w badaniu ataków złośliwym oprogramowaniem. o Jak malware dostaje się do sieci, jak się porusza, jak działa. o Korzystanie z narzędzi sieciowych. • Analiza ataku (wprowadzenie do OSSTMM) o Strategie postępowania a taktyki stosowane w celu jej realizacji. o Manewrowanie po polu bitwy poprzez użycie narzędzi sieciowych oraz hackerskich. o Jak zarządzać trwającymi atakami, jak przygotować się na nadchodzące, mimo że nie znamy i nie spodziewamy się konkretnego typu ataku. • Podstawy informatyki śledczej o Omówienie sposobów jak zagrożenia omijają kontrolki operacyjne, powierzchnie ataku i zaufanie do osiągnięcia dostępu do aktywów. o Narzędzia i techniki w badaniu konkretnych systemów i urządzeń. **OSSTMM i Hakowanie** • Podstawy Hakingu w modelu OSSTMM o OSSTMM w hakowaniu jako szybsza i bardziej bezpośrednia metoda prowadzenia badań. o Przedstawienie metody OSSTMM w praktycznych podstawach hakowania sieci i systemów. o Ogólna metodyka hakowania • Technologie sieciowe w modelu OSSTMM: Email i Web o Omówienie najpopularniejszych wektorów ataku o Przedstawienie różnorodności ataków o Przyjmowanie właściwej postawy obronnej w zadanych kanałach komunikacji. • Hakowanie Haseł o Omówienie uwierzytelniania w modelu OSSTMM. o Omówienie szyfrowania w modelu OSSTMM.	20 x 45 min
2	**Ekspert bezpieczeństwa OSSTMM**	**Zarządzanie i wdrożenie modelu OSSTMM w cyberbezpieczeństwie organizacji** • Definicje i słownictwo: Spojrzenie na bezpieczeństwo z perspektywy OSSTMM poprzez ustandaryzowanie słownictwa • Strategie bezpieczeństwa OSSTMM o Elementy planu o Co chcemy osiągnąć o Dotarcie do celu o Jak mają wyglądać nasze działania operacyjne o Co jest możliwe do osiągnięcia • Testowanie bezpieczeństwa OSSTMM - taktyka i metryki o OSSTMM jako nowoczesna pętla OODA w cyberbezpieczeństwie o Strategia kontra działalność operacyjna • Kontrolki interakcji o Zarządzanie interakcjami z nami i aktywami o Kontrola operacyjna w różnych środowiskach cybernetycznych o Badanie dowolnej interakcji • Zasady testowania o Zasady patrolowania cyberprzestrzeni o Obserwacja, inspekcja, gotowość narzędzi, komunikacja, właściwe reagowanie o Zasady i umiejętności potrzebne do przeprowadzenia testów bezpieczeństwa	8 x 45 min
3	**Bezpieczeństwo systemu Linux**	**o Analiza środowiskowa:** □ Zrozumienie typów systemów Linux □ Zrozumienie BIOS-u □ Zrozumienie Bootloadera □ Analizowanie systemu operacyjnego □ Analizowanie dysku twardego □ Shells □ Rodzaje złośliwego oprogramowania **o Hardening Interakcji:** □ Konta użytkowników i uprawnienia □ Analiza hasła □ Przywileje dotyczące plików □ Porty i usługi □ Host Firewalls **o Analizowanie emanacji:** □ Networking □ DNS / Hosts □ Logowanie □ Instalacje oprogramowania □ Czas **o Analizowanie zasobów:** □ Routing □ Service Manager □ Kernel □ Containers □ Wirtualizacja	20 x 45 min
4	**Bezpieczeństwo systemu Windows**	**o Uwierzytelnianie i autoryzacja** □ Proces uwierzytelniania i autoryzacji □ Uwierzytelnianie biometryczne □ Wirtualne karty inteligentne w procesie uwierzytelniania **o Zarządzanie bezpieczeństwem systemu** □ Szyfrowanie BItLocker □ UAC □ Polityki GPO □ Zarządzanie plikiem Host **o Zarządzanie kontrolą dostępu w systemach Windows** □ Uprawnienia użytkowników, □ Pojęcie dziedziczenia □ UAC □ Ograniczenia praw aplikacji □ Ustawienia zasad domenowych **o Narzędzia wspierające bezpieczeństwo i monitorujące** □ Windows Deffender □ Microsoft update □ SCM, SCT. ASA □ Konfiguracja FIrewall □ Zarządzanie zbieraniem logów oraz ich analiza.	20 x 45 min