Szkolenie

Od zera do hackera

czyli jak rozpocząć praktykę w cyberbezpieczeństwie

Kurs przeznaczony jest dla osób pragnących rozpocząć swoją karierę w cyberbezpieczeństwie. które chcą poznać praktyczne podstawy i nie wiedzą, jak i od czego zacząć. W ramach pierwszej części szkolenia zostaną omówione niezbędne podstawy wymagane w pracy każdego „bezpiecznika", takie jak sieci komputerowe, administracja systemami operacyjnymi, praktyczna kryptografia oraz podstawy programowania skryptowego. W dalszych etapach poruszone zostaną zagadnienia dotyczące testów penetracyjnych infrastruktury sieciowej i aplikacji webowych, ataki na aplikacje desktopowe, pisanie własnych *exploitów* i dostosowywanie gotowych narzędzi, a także zagadnienia związane z systemami zabezpieczeń, analizą powłamaniową i proceduralnymi oraz prawnymi aspektami pracy w bezpieczeństwie IT.

Szkolenie w prezentowanej formie jest polecane zarówno dla osób, które dopiero rozpoczynają swoją przygodę z cyberbezpieczeństwem, jak i tych, które posiadają już pewne podstawy – pozwoli ono wtedy na odświeżenie i usystematyzowanie wiedzy zdobytej wcześniej.

Każde zagadnienie poruszane w ramach kursu jest przedstawiane praktycznie, a uczestnicy będą mieli możliwość samodzielnego wykonania zadania na rzeczywistym środowisku udostępnionym do zajęć. Zagadnienia omawiane będą w formie problemowej, na przykładach z życia, spotkanych w trakcie wielu lat pracy dla prywatnych i publicznych organizacji i dbania o ich bezpieczeństwo. Dla chętnych pojawią się także dodatkowe zadania, rozszerzające materiał szkolenia, nie pozwalające nudzić się na znajomych już tematach.

1. Wprowadzenie do sieci komputerowych (24 godziny)
    a. Warstwa fizyczna i infrastruktura sieciowa, standardy Ethernet, 802.11
    b. Urządzenia sieciowe warstwy L1 i L2
    c. Sieci VLAN i łącza trunk
    d. Protokół STP
    e. Warstwa sieci: IPv4, ICMP, ARP, routing statyczny i dynamiczny
    f. Warstwa transportowa: TCP, UDP
    g. Usługi sieciowe: DHCP, DNS, NAT, HTTP
2. Wprowadzenie do systemów operacyjnych – Linux (40 godzin)
    a. Podstawowa konfiguracja systemu
    b. Środowisko CLI i Bash
    c. Automatyzacja zadań w Bash
    d. Konfiguracja sieci w systemie Linux
    e. Użytkownicy, grupy i zarządzanie uprawnieniami
    f. Uprawnienia w systemie plików
    g. Zadania administracyjne (zarządzanie dyskami, zarządzanie zadaniami, logowanie, zarządzanie procesami i usługami)
    h. Zdalny dostęp do systemu (SSH, VNC)
    i. Usługi sieciowe (DNS, NFS, HTTP)

    j. Zapora sieciowa
    k. Systemy i modele zabezpieczeń (SELinux)
    l. Wirtualizacja i konteneryzacja
3. Kryptografia (16 godzin)
    a. Wprowadzenie do zagadnień kryptografii i kryptoanalizy
    b. Integralność – sumy kontrolne, ochrona przed atakami Man in the Middle
    c. Przechowywanie i łamanie haseł
    d. Podpis cyfrowy i certyfikaty
    e. Infrastruktura klucza publicznego
    f. Bezpieczeństwo danych – szyfrowanie
    g. Systemy TPM i HSM – wprowadzenie
4. Systemy bezpieczeństwa (12 godzin)
    a. Zapory sieciowe (firewall)
    b. Systemy IPS/IDS
    c. Systemy Data Leakage Prevention
    d. Systemy ochrony stacji roboczych
    e. Konfiguracja i testowanie przykładowych systemów bezpieczeństwa (Snort, OSSEC)
    f. Projektowanie bezpiecznej sieci komputerowej
5. Sieciowe usługi bezpieczeństwa i zdalnego dostępu (12 godzin)
    a. Tunele VPN i przykładowa konfiguracja rozwiązania (OpenVPN)
    b. Uwierzytelnianie i szyfrowanie protokołów sieciowych
    c. DNSSEC i DoH
6. Zagrożenia (8 godzin)
    a. Źródła zagrożeń
    b. Modelowanie, klasyfikacja i ocena zagrożeń
    c. Metodyki ataków
    d. Socjotechnika
    e. Kradzieże tożsamości
7. Testy penetracyjne – Ethical Hacking (32 godziny)
    a. Pasywne i aktywne gromadzenie informacji
    b. Wykrywanie systemów komputerowych ofiary
    c. Wykrywanie i ocena podatności
    d. Atak
    e. Eskalacja uprawnień i utrzymanie dostępu
    f. Zacieranie śladów
    g. Raport z przeprowadzonego testu
    h. Aspekty prawne i organizacyjne
    i. Case study – własny test penetracyjny
8. Bezpieczeństwo aplikacji webowych (24 godziny)
    a. Typowe problemy aplikacji webowych
    b. Skanowanie aplikacji webowych
    c. Zarządzanie sesją użytkownika
    d. Wstrzykiwanie kodu (command injection, HTTP injection)
    e. XSS i CSRF
    f. Mechanizmy ochrony (CSP, prepared statements)
9. Atakowanie infrastruktury sieciowej (16 godzin)

    a. Błędy w sprzęcie i firmware na urządzeniach
    b. Bezpieczeństwo i podatności w sieciach bezprzewodowych (WPA, WPS, WPA-Enterprise)
10. Błędy w oprogramowaniu i pisanie własnych exploitów (24 godziny)
    a. Wprowadzenie do architektury x86
    b. Język C/C++ i zarządzanie pamięcią
    c. Wprowadzenie do języka Python
    d. Podstawy asemblera x86
    e. Typowe błędy programistyczne (m.in. buffer overflow i format string)
    f. Tworzenie exploitów
    g. Dostosowywanie gotowych rozwiązań
11. Prawne i organizacyjne aspekty bezpieczeństwa (8 godzin)
    a. Polityka i procedury bezpieczeństwa
    b. Systemy zarządzania bezpieczeństwem informacji – ISO 27000
    c. RODO i inne regulacje prawne ważne w pracy IT
12. Reagowanie na incydenty i analiza śledcza (24 godziny)
    a. Jak przygotować się przed incydentem
    b. Wykrywanie i reagowanie na incydenty
    c. Metodyki reagowania
    d. Analiza śledcza i powłamaniowa
    e. Procedury i raporty poincydentalne