SZKOLENIE ŚREDNIO ZAAWANSOWANE

Metody i narzędzia weryfikacji bezpieczeństwa sieciowego

HACGAM

Czas trwania: 1 dni (8h)

Cele szkolenia

- Zapoznanie słuchaczy z podstawami bezpieczeństwa sieciowego oraz narzędziami wykorzystywanymi przez osoby przeprowadzające audyty bezpieczeństwa sieci jak również w złej wierze przez atakujących maszyny podłączone do sieci
- Omówienie przykładowych narzędzi umożliwiających pobranie szczegółowych danych z DNS i zmapowanie struktury sieci, przeskanowanie zakresu adresów IP lub usług działających na wybranej maszynie oraz narzędzie Metasploit, umożliwiające wykorzystanie podatności w aplikacji w celu uzyskania dostępu do maszyny
- Zapoznanie z poszczególnymi technikami wykorzystywanymi w czasie audytu bezpieczeństwa i odpowiednimi narzędziami pozwalającymi uzyskać wartościowe informacje zrealizowane jest w ramach gry szkoleniowej
- W kolejnych zadaniach, uzyskanie dostępu do konsoli podatnej maszyny rozpoczynając od nazwy domenowej pewnej fikcyjnej organizacji
- Nabycie umiejętności dokonania przeglądu sieci własnej organizacji w celu wykrycia potencjalnych słabych stron wdrożonych mechanizmów bezpieczeństwa
- Wykonanie wewnętrznego audytu bezpieczeństwa
- Możliwość lepszego zabezpieczenia powierzonej sieci dzięki zdobytej wiedzy

Zalety

- Najważniejszą zaletą gry szkoleniowej jest skupienie się na części praktycznej - pracy z wybranymi narzędziami umożliwiającymi sprawdzenie różnych aspektów bezpieczeństwa sieciowego
- Zajęcia zrealizowane są w formie gry szkoleniowej gdzie rozpoczynając od adresu domenowego fikcyjnej organizacji uczestnik uzyskać dostęp do powłoki systemowej podatnej maszyny
- Kolejność omawianych tematów odpowiada poszczególnym etapom procesu zdobywania wiedzy o interesującej sieci, lokalizowanie potencjalnych słabych punktów i ich wykorzystanie
- Uczestnicy kursu otrzymają materiały, które można traktować jako przewodnik umożliwiający dokonanie prostego audytu sieci oraz próby uzyskania dostępu do potencjalnie podatnych maszyn
- Dodatkowo materiały zawierają ściągawkę" najważniejszych komend i przełączników narzędzi wykorzystywanych podczas zajęć

- Praktyka przed teorią - wszystkie szkolenia technologiczne prowadzone są w formie warsztatowej. Konieczna teoria jest wyjaśniana na przykładzie praktycznych zadań
- Konkretne umiejętności - w ramach każdego szkolenia rozwijamy praktyczne umiejętności związane z daną technologią i tematyką
- Nauka z praktykami - wszyscy trenerzy na co dzień pracują w projektach, gwarantuje to dostęp do eksperckiej wiedzy i praktycznego know-how

Wymagania

- Od uczestników szkolenia wymagana jest znajomość podstawowych zagadnień związanych z sieciami komputerowymi (podstawowe protokoły i mechanizmy sieciowe, adresacji itp.)

Program

1. Wprowadzenie do zagadnień sieciowych
    a. Topologia sieci Internet
    b. Adresacja w sieciach IPv4
    c. Urządzenie łączące elementy sieciowe
    d. Omówienie podstawowych narzędzi mapowania sieci: ping i traceroute/tracert
2. Wprowadzenie do usługi DNS
    a. Adresy domenowe a adresy sieciowe
    b. Omówienie architektury systemu DNS
    c. Rodzaje rekordów w systemie DNS
    d. Możliwość wykorzystanie informacji DNS na potrzeby audyty bezpieczeństwa
    e. Narzędzie umożliwiające pobranie informacji z systemu DNS: nslookup, dig
3. Narzędzia umożliwiające skanowanie sieci
    a. Wprowadzenie do protokołów sieciowych IP, ICMP, TCP i UDP
    b. Omówienie możliwość zdalnego rozpoznania działających maszyn i uruchomionych usług
    c. Wprowadzenie do programu Nmap - skanera sieciowego
4. Wprowadzenie do podatności w aplikacjach
    a. Rodzaje podatności i możliwości ich wykorzystania
    b. Omówienie pojęć exploit, shellcode, backdoor
5. Narzędzia umożliwiające wykorzystanie podatności
    a. Wprowadzenie do programu Metasploit
    b. Wykorzystanie programu Metasploit do uzyskania dostępu do podatnej maszyny