Kod szkolenia: **HACGAM**

Tytuł szkolenia: **Metody i narzędzia weryfikacji bezpieczeństwa sieciowego**

Dni: 1

Opis:

Cel gry szkoleniowej

Celem gry szkoleniowej jest 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. W ramach zajęć zostaną omówione przykładowe narzędzia umożliwiające 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, rozpoczynając od nazwy domenowej pewnej fikcyjnej organizacji słuchacze uzyskają dostęp do konsoli podatnej maszyny. Po zakończeniu szkolenia uczestnik będzie w stanie dokonać przeglądu sieci własnej organizacji w celu wykrycia potencjalnych słabych stron wdrożonych mechanizmów bezpieczeństwa. Takie działanie można traktować jako wykonanie wewnętrznego audytu bezpieczeństwa. Dodatkowo zdobyta w trakcie zajęć wiedza pozwoli lepiej zabezpieczyć powierzone sieci.

Mocne strony

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.

Wymagania

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

Program szkolenia:

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