Kod szkolenia: **NDS**

Tytuł szkolenia: **Kompleksowa diagnostyka i zabezpieczanie sieci IT**

Dni: 4

Opis:

Adresaci szkolenia:

Szkolenie adresowane jest w szczególności do osób odpowiedzialnych za przeprowadzanie audytów bezpieczeństwa infrastruktury sieciowej oraz za wdrażanie systemów bezpieczeństwa. Dodatkowo prezentowana wiedza może być przydatna wszystkim osobom odpowiedzialnym oraz zainteresowanym wdrażaniem i monitorowaniem/weryfikowaniem działalności usług bezpieczeństwa w sieciach komputerowych w szczególności systemów zapór ogniowych i systemów wykrywania włamań.

Cel szkolenia:

Celem szkolenia jest przedstawienie różnych narzędzi diagnostycznych umożliwiających przeprowadzanie audytu bezpieczeństwa jak również zapoznanie się ideą działania, możliwościami oraz topologiami wykorzystującymi zapory ogniowe i systemy wykrywania włamań.

W szczególności:

Uczestnicy kursu zapoznają się między innymi z najpopularniejszym skanerem Nmap, umożliwiającym dokonanie inwentaryzacji działających maszyn, uruchomionych na nich usług a nawet ich wersji. W programie kursu omówione zostaną programy umożliwiające analizę ruchu sieciowego (tak zwane snifery) - Wireshark oraz tcpdump. Dodatkowo zostanie przedstawiony program hping2 umożliwiający wygenerowanie ruchu testującego systemy bezpieczeństwa takie jak zapory ogniowe czy systemy wykrywania włamań (ang. Intrusion Detection System, IDS).

Kurs koncentruje się na narzędziach dla sieci kablowych, jednak wspomniane są różnice i specyficzne cechy oprogramowania umożliwiającego audyt sieci WiFi na przykładzie skanera Kismet.

Podczas kursu zostanie przedstawiony sposób działania zapory ogniowej oraz topologie sieci wykorzystujące zapory ogniowe do budowy DMZ. W ramach kursu zostanie omówiona konfiguracji mechanizmów filtrowania ruchu wchodzącego i wychodzącego (ang. ingress and outgress filtering) Dodatkowo zostaną przedstawione mechanizmy takie jak translacja adresów (ang. network address translation, NAT) oraz przekierowanie portów.

W trakcie kursu zostanie omówiona idea działania systemów wykrywania włamań. Podczas kursu uczestniczy zapoznają się z jednym z najpopularniejszych systemów IDS – Snort. Podczas zajęć zostanie omówiona podstawowa konfiguracja a także bardziej zaawansowane strojenie systemy do potrzeb sieci, polegające na pisaniu własnych reguł. Uczestniczy zapoznają się z wynikami działania programu wraz z logami dla przykładowych ataków. Dodatkowo zostaną omówione modyfikacje oraz narzędzia pomocnicze: Snort Inline – system IPS (ang. intrusion prevention system) oraz konsola webowa Base (następca ACID).

Działanie wszystkich omawianych aspektów zostanie przetestowane w trakcie ćwiczeń.

Mocne strony szkolenia:

Program kursu obejmuję część teoretyczną oraz dużą liczbę ćwiczeń pozwalających praktycznie sprawdzić działanie omawianych programów.

Oprócz przedstawienia i dokładnego omówienie wybranych najpopularniejszych programów podczas kursu zostaną krótko przedstawione inne przydatne narzędzia.

W kursie oprócz nacisku na omówienie konfiguracji zapory ogniowej związanej z najczęściej wykorzystywanymi protokołami – TCP, UDP oraz ICMP zostaną przedstawione inne rzadziej spotykana a sprawiające problemy konfiguracyjne protokoły, na przykład różnego rodzaju protokoły tunelowe, VPN itp.

Program jest ciągle uaktualniany, tak, by uwzględniać nowe zagrożenia oraz funkcjonalności omawianego oprogramowania.

Wymagania:

Od uczestników szkolenia wymagana jest znajomość podstawowych zagadnień związanych z sieciami komputerowymi (podstawowe protokoły i mechanizmy sieciowe, adresacji itp.) oraz podstawowa znajomość konfiguracji aplikacji oraz systemu Linux.

Parametry szkolenia:

4*8 godzin (4*7 godzin netto) wykładów i warsztatów.

Wielkość grupy: maks. 8-10 osób.

Program szkolenia:

1. Wrowadzenie do zagrożeń sieciowych
    - Podatność/exploit/atak
    - Rodzaje ataków
    - Rekonesans
    - DoS/DDoS
    - Przejęcie kontroli

2. Skanowanie
    - Techniki skanowania
    - GoogleHack
    - Serwis Shodan
    - Wykorzystanie programu Nmap
    - Snifery - tcpdump/wireshark
3. Usługi ochrony informacji
    - Poufność
    - Uwierzytelnienie
    - Ochrona Integralności
    - Szyfry
    - Funkcje skrótu
    - Omówienie i konfiguracja PKI
4. Mechanizmy ochrony sieci
    - Zapory ogniowe
    - Topologie z DMZ
    - Konfiguracja zapory z w wykorzystaniem iptables
    - Konfiguracja NAT i zapory ogniowej
    - Systemy wykrywania włamań
    - Mechanizmy obrony warstwy drugiej
    - Systemy wykrywanie włamań
    - Konfiguracja systemu Snort
5. Bezpieczeństwo transmisji
    - VPN
    - Tunelowanie
    - Konfiguracja https
    - Konfiguracja OpenVPN
6. Błędy aplikacji a przejęcie kontroli nad maszyną
    - Podstawowe rodzaje błędów w aplikacjach
    - Omówienie buffer overflow
    - Wykorzystanie środowiska Metasploit do przejęcia kontroli