Kod szkolenia: **IDS**

Tytuł szkolenia: **Systemy wykrywania włamań**

Dni: 1

Opis:

Adresaci Szkolenia:

Szkolenie adresowane jest do administratorów sieci oraz osób odpowiedzialnych za wdrażania polityki bezpieczeństwa w oparciu o mechanizmy sieciowe. Prezentowana wiedza może być także przydatna dla osób odpowiedzialnych za tworzenie oraz weryfikowanie wdrożenia polityki bezpieczeństwa.

Cel szkolenia:

Celem szkolenia jest przedstawienie idei działania systemów wykrywania włamań (ang. Intrusion Detection Systems, IDS) oraz poznanie konfiguracji przykładowego, jednego z najpopularniejszych systemów rozwiązania – systemy Snort dla platformy Linux.

W szczególności:

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).

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.

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:

8 godzin (7 godzin netto) wykładów i ćwiczeń.

Wielkość grupy: maks. 8-10 osób.

Program szkolenia:

1. Wprowadzenie do zagrożeń sieciowych
    - Podatność/exploit/atak
    - Rodzaje ataków
    - Rekonesans
    - DoS/DDoS
    - Przejęcie kontroli
2. Systemy wykrywania włamań
    - Historia rozwoju systemów wykrywania włamań
    - Omówienie różnego typu zapór ogniowych
    - Porównanie zalet i wad systemów NIDS i HIDS
3. Konfiguracja systemu wykrywania włamań Snort
    - Omówienie podstawowej konfiguracji
    - Zapoznanie się z mechanizmem logowania
    - Wstępny tuning reguł i systemu
    - Mechanizm zmiennych konfiguracyjnych
4. Konfiguracje zaawansowane
    - Omówienie języka reguł systemu Snort
    - Przygotowanie własnych reguł
    - Konfiguracja mechanizmu rozłączenia niebezpiecznych połączeń