Kod szkolenia: **FW**

Tytuł szkolenia: **Zapory ogniowe**

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 zapoznanie się możliwościami oraz topologiami wykorzystującymi zapory ogniowe na przykładzie zapory ogniowej w systemie Linux, konfigurowanej za pomocą programu iptables.

W szczególności:

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. Działanie wszystkie 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:

1*8 godzin (1*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. Mechanizmy ochrony sieci z wykorzystaniem zapory ogniowej
    - Historia rozwoju zapór ogniowych
    - Omówienie różnego typu zapór ogniowych
    - Topologie sieci z DMZ
    - Wykorzystanie zapory ogniowej do eliminacji zagrożeń
3. Konfiguracja zapory ogniowej z wykorzystaniem iptables
    - Podstawy mechanizmu iptables
    - Łańcuchu i tablice
    - Dodawanie, usuwanie i podgląd reguł
    - Podstawowa konfiguracja zapory - zezwolenie i zabronienie ruchu
4. Konfiguracje zaawansowane
    - Konfiguracja mechanizmu NAT
    - Konfiguracja przekierowania portów
    - Ingres/egress filtering