Tytuł szkolenia: Bezpieczeństwo sieci komputerowych (etap II)

Kod szkolenia: BEZP-SIECI-KOMP-II

Wprowadzenie

Jest to kolejny etap (drugi) szkolenia z bezpieczeństwa sieci komputerowych. Ten etap to przejście od małej sieci, do niewielkiej sieci firmowej. Podstawową różnicą tego etapu jest makieta, w której wprowadzony został podział na podsieci zgodnie z normą ISO27001. Na tym etapie zakładamy, że kursant zaczyna wdrażać dobre praktyki wymagane w sieciach firmowych ze względów cyberbezpieczeństwa. Kurs jest nastawiony na wprowadzenie kursanta do wdrożenia ISO27001.

Drugi etap to przede wszystkim bezpieczeństwo sieci - konfiguracja firewalla zarówno na styku z Internetem, jak i pomiędzy podsieciami. Aby uczynić szkolenie bardziej realistycznym, makieta symuluje dwie sieci firmowe, które z czasem zaczynają ze sobą współpracować w zakresie dostępu do zasobów. Kursanci uczą się jak konfigurować bezpieczeństwo takiej kooperacji na poziomie firewalla. Scenariusze ćwiczeń są tak dobrane, aby stanowić podbudowę pod ISO27001.

Na tym etapie kursanci pracują na makietach, wykonując przez trzy dni ćwiczenia związane z firewallem i ćwicząc realne scenariusze. Makieta posiada symulację Internetu, dla którego kursanci muszą skonfigurować odpowiedni poziom ochrony sieci prywatnych. Ćwiczone scenariusze oraz konfiguracje, które są pokazywane, mają przygotować kursantów do wdrożenia ISO27001 lub do audytu w tym kierunku.

Adresaci szkolenia

Cel szkolenia

Po zakończeniu kursu uczestnicy powinni:
1. Rozumieć ideę podziału na podsieci - VLAN-y, połączenia trunkowe
2. Potrafić zaprojektować adresację w firmie dla podziału na podsieci z uwzględnieniem dobrych praktyk
3. Rozumieć zasadę działania firewalli oraz zasady ruchu pakietów w sieciach
4. Potrafić wdrożyć na firewallu wytyczne polityki bezpieczeństwa z uwzględnieniem zaawansowanych rozwiązań i precyzyjnego filtrowania ruchu
5. Potrafić zastosować zaawansowaną translację adresów zarówno na styku sieci z Internetem jak i pomiędzy sieciami prywatnymi.

Do etapu drugiego przewidziany jest **etap 2b**, stanowiący ćwiczenia praktyczne do poznanego materiału. Podczas tego etapu kursanci realizują zadaną politykę bezpieczeństwa przy pomocy firewalla. Muszą również zaprojektować adresację dla dużej firmy z uwzględnieniem perspektywy bieżącej i przyszłej. **Ten etap nie jest obowiązkowy** ze względu na poznawany materiał.

Zobacz również:

- Szkolenie: **Bezpieczeństwo sieci komputerowych (etap I)**
- Szkolenie: **Bezpieczeństwo sieci komputerowych (etap III)**
- Szkolenie: **Bezpieczeństwo sieci komputerowych (etap IV)**

Czas i forma szkolenia

- 21 godzin (3 dni x 7 godzin), w tym wykłady i warsztaty praktyczne.

Plan szkolenia

1. Podstawy sieci firmowych z uwzględnieniem bezpieczeństwa
2. Podział na podsieci i techniki wykonania tego podziału
3. Podstawy działania firewalli
4. Firewalle stateless i stateful
5. Ograniczenia ruchu sieciowego pod kątem bezpieczeństwa