Szkolenia Komputerowe

Program szkolenia certyfikowanego kursu CCNA Security

Szkolenie kończące się egzaminem, który umożliwi zdobycie ***certyfikatu Cisco*** poświadczającego posiadanie przez uczestnika wiedzy zdobytej podczas kursu ***Cisco CCNA Security***.

Czas trwania kursu **– 70 godzin dydaktycznych** (11 dni x 6 godzin + 1 dzień x 4 godziny) **oraz egzamin końcowy** w Lokalnej Akademii Cisco Fundacji ALTERnacja.

Szczegółowy opis kursu

Kurs Cisco CCNA Security prezentuje zagadnienia usystematyzowane w **11 modułach**.

1. Zagrożenia w nowoczesnych sieciach:

- Zabezpieczanie sieci,
- Przegląd zagrożeń sieciowych,
- Rodzaje i typy ataków,
- Rodzaje złośliwego oprogramowania (wirusy, robaki etc.),
- Metody ograniczenia zagrożeń sieciowych,
- Organizacje związane z bezpieczeństwem.

2. Zabezpieczanie urządzeń sieciowych:

- Zabezpieczenie dostępu do urządzeń sieciowych,
- Przypisywanie ról administracyjnych,
- Monitorowanie i zarządzenie urządzeniami sieciowymi,
- Zautomatyzowane funkcjonalności bezpieczeństwa,
- Zabezpieczenie płaszczyzny zarządzania urządzenia Cisco.

3. Uwierzytelnianie, autoryzacja i rozliczanie (AAA):

- Motywacja do stosowania metod AAA: uwierzytelniania, autoryzacji i rozliczenia,
- Protokoły TACACS+ i RADIUS,
- Lokalne uwierzytelnienie,
- Uwierzytelnienie AAA na serwerze zewnętrznym.

4. Implementacja technologii ścian ogniowych (firewall):

- Systemy zapobiegania intruzom – firewalle, rozdaje firewalli,
- Listy kontroli dostępu (ACL),
- Implementacja Zone-Based Firewall (ZBF).

5. Implementacja ochrony przed zagrożeniami (IPS):

- Implementacja IPS w systemie Cisco IOS,
- Typy sygnatur, rodzaje alarmów,
- Metody wdrożenia IDS/IPS oraz metody wykrywania ataków.

6. Zabezpieczanie lokalnej sieci:

- Port-security na przełącznikach L2,
- zabezpieczenie protokołu STP, storm control, zabezpieczenie trunków,
- Bezpieczeństwo L2 – ataki na CAM (MAC spoofing, MAC flooding),
- Network Admission Control (NAC).

7. Systemy kryptograficzne:

- Szyfrowanie symetryczne i asymetryczne,
- Integralność danych i uwierzytelnienie,
- Przegląd usług kryptograficznych,
- Infrastruktura klucza publicznego (PKI) – podpis cyfrowy.

8. Implementacja wirtualnych sieci prywatnych (VPN):

- Opis komponentów oraz mechanizmów VPN
- Charakterystyka rozwiązań VPN.
- Konfiguracja VPN site-to-site za pomocą CLI

9. Konfiguracja urządzeń typu Adaptive Security Appliance (ASA):

- Podstawowa konfiguracja Cisco ASA,
- Inspekcja ruchu,
- Translacja adresów sieciowych,
- Listy kontroli dostępu.

10. Zaawansowana konfiguracja (ASA):

- Konfiguracja Anyconnect SSL VPN,
- Konfiguracja Clientless SSL VP,N
- Narzędzie Adaptive Security Device Manager (ASDM),
- Zaawansowane konfiguracja funkcjonalności ASA.

11. Zarządzanie bezpieczną siecią:

- Zagrożenia bezpieczeństwa we współczesnych sieciach,
- Weryfikacja bezpieczeństwa sieci,
- Polityka bezpieczeństwa sieci.