CCNA Security

Komerčný názov kurzu: Implementing Cisco IOS Network Security (IINS)
ID certifikačnej skúšky: 640-553
Rozsah: 5 x 8 hod. praktických stretnutí

Podmienky kurzu:
Od uchádzačov o kurz požadujeme splnenie aspoň jednej z nasledujúcich podmienok:

- absolvované prvé štyri semestre CCNA v jednej zo sieťových akadémií CISCO
- držiteľ platného certifikátu CCNA
- vedomosti na úrovni CCNA (samoštúdium alebo absolvovanie sieťarských predmetov. Študenti FIIT nadobudnú potrebné vedomosti absolvovaním predmetu Počítačové siete II, resp. Prepínanie a smerovanie v IP sieťach)

Obsah kurzu:
V CCNA Security sa študenti oboznámia so základmi problematiky bezpečnosti v sieťach založených na protokole IP.

CCNA Security je najnovší prírastok do rodiny kurzov v rámci projektu Cisco Networking Academy a predstavuje úvodný kurz do bezpečnosti vo svete Cisco sietí. Pomocou nadstavby nad vedomosťami nadobudnutými počas CCNA štúdia, umožňuje jednotlivcovi splniť stále sa zvyšujúce požiadavky na bezpečnostnú rozhľadenosť v sieťovom zameraní.

Informácie v CCNA Security dajú absolventovi jadro teoretických a praktických zručností pre potreby inštalácie, monitorovania a odlaďovania. Tieto vedomosti a certifikácia si kladú za cieľ umožniť vstup absolventovi do junior pozície v rámci sieťového odvetvia.

Kurz je organizovaný ako kombinácia e-vzdelávania (e-learning) v systéme NetAcad v kombinácii s praktickými stretnutiami. Na praktických stretnutiach si budú môcť účastníci kurzu vyskúšať konfigurácie na reálnych zariadeniach spoločnosti Cisco.

Kurz je ukončený simulovanou certifikačnou skúškou, ktorej cieľom je lepšie pripraviť študentov na reálnu certifikačnú skúšku CCNA Security – Implementing Cisco IOS Network Security (IINS) s číslom 640-553. Študenti obdržia osvedčenie o úspešnom absolvovaní tohto kurzu.

Osnova kurzu (predbežné rozdelenie)

Kurz je rozdelený do piatich dní po 8 hodín. Kurz ma dokopy 40 hodín praktických stretnutí. RCNA FIIT STU si vyhradzuje právo rozloženie praktických cvičení bez predbežného upozornenia pozmeniť.

Deň 1:

- Úvod do kurzu
- Blok prednášok (úvod do bezpečnosti a základné zabezpečenie Cisco zariadení)
- Praktické cvičenia na prvotné zabezpečenie prepínačov a smerovačov Cisco

Deň 2:

- Blok prednášok (Autentifikácia, Autorizácia, Monitorovanie – AAA, RADIUS, TACACS+, ACS Server, 802.1x, úvod do filtrovania a firewallu)
- Praktické cvičenia (AAA, ACS Server, opakovanie ACL)

Deň 3:

- Blok prednášok (Pokračovanie Firewall z predošlého dňa, IDS a IPS systémy)
- Praktické cvičenia (Firewall a IPS)

Deň 4:

- Blok prednášok (Zabezpečenie layer 2 RM OSI, útoky na STP, MAC flooding, storm control)
- Praktické cvičenia (Zabezpečenie layer 2 RM OSI, útoky na STP, BPDU spoofing útok)

Deň 5:

- Blok prednášok (kryptografické systémy, VPN technológia/IPSec)
- Praktické cvičenia (VPN, IPSec, Cisco Easy VPN, opakovanie)

Certifikácia

Na úspešné získanie certifikátu CCNA Security je nutné mať platný certifikát CCNA alebo hociktorý CCIE (CCDE) certifikát a absolvovanú skúšku, ktorá vedie k získaniu tohto certifikátu. Certifikát CCNA je následne možné získať absolvovaním skúšky s číslom 640-553.