CompTIA Security+

Kód kurzu: CTSEC

Tento unikátny päťdňový kurz je základnou prípravou pre celosvetovo uznávanú certifikačnú skúšku CompTIA Security+ SY0-701, ktorá je dnes štandardom pre IT certifikáciu v oblasti bezpečnosti. Účastníci získajú súhrnný prehľad IT bezpečnostných riešeniach a získajú možnosť si prakticky vyskúšať implementáciu rôznych bezpečnostných opatrení. Vďaka vedúcej úlohe bezpečnosti v IT prostrediach všetkých firiem a dlhoročnej tradícii tejto certifikačnej skúšky, je CompTIA Security + kurz jednoznačne zásadnou výhodou pre IT pracovníkov na všetkých pozíciách.

Pre koho je kurz určený

Kurz je určený pokročilým užívateľom počítačov a začínajúcim bezpečnostným administrátorom.

Čo vás naučíme

- Porozumieť základným konceptom identifikácie a riešeniu bezpečnostných rizík
- Porozumieť základným konceptom kryptografie a správne ich využívať – symetrické kľúče, certifikáty
- Získate prehľad najzraniteľnejších častí sieťovej infraštruktúry TCP/IP a ich riešení
- Porozumiete princípom ochrany e-mailovej komunikácie, vzdialených pripojení VPN, bezdrôtových sietí a ďalších metód komunikácie
- Porozumiete princípom overovania identity
- Ako nastavovať užívateľské skupiny, ich práva a prístupové oprávnenia
- Implementovať bezpečnostné opatrenia a updaty
- Porozumiete základným konceptom bezpečnostných politík od zaistenia fyzickej bezpečnosti po zachovanie chodu firmy
- Vytváranie bezpečnostnej dokumentácie a Security Incident Handling

Požadované vstupné znalosti

Účastníci by mali mať znalosti na úrovni certifikácie CompTIA A+, Network+ alebo ekvivalentné praktické skúsenosti v oblasti administrácie sietí a operačných systémov Microsoft. Účastníci by mali mať veľmi dobré skúsenosti v oblasti konfigurácie siete.

Osnova kurzu

1. Základy bezpečnosti
   - Cyklus informačnej bezpečnosti
   - Základy bezpečnostných politík
   - Overovacie metódy
   - Základy kryptografie
2. Bezpečnostné hrozby a zraniteľnosti
   - Sociálne inžinierstvo
   - Hrozby fyzického prístupu
   - Hrozby v sieťovom prostredí
   - Riziká a zraniteľnosti bezdrôtových sietí
   - Riziká chybne naprogramovaných aplikácií
3. Sieťová bezpečnosť
   - Prehľad sieťových zariadení z pohľadu bezpečnosti
   - Koncept sieťové bezpečnosti
   - Ukážky sieťových útokov
   - Zabezpečenie bežnej sieťovej prevádzky
   - Zabezpečenie infraštruktúry bezdrôtových sietí
4. Zabezpečenie aplikácií, dát a prvkov

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk

- Základné pravidlá zabezpečenia staníc
- Základné pravidlá zabezpečenia serverov
- Zabezpečenie dát
- Zabezpečenie mobilných zariadení
- Možnosť zabezpečenia aplikácií

5. Správa identít a prístupu
   - Typy autentizácií
   - Smart karty a tokeny
   - Stratégie skupín
   - Správa prístupu pomocou ACL
   - RADIUS Server a 802.1x
   - VLAN Management
   - Správa prístupu do VPN
   - WPA1/2 Enterprise
6. Správa PKI a certifikátov
   - Koncept PKI
   - Možnosť využitia certifikátov
   - Inštalácia Enterprise certifikačnej autority a správa šablón
   - Zálohovanie a obnova certifikačnej autority
   - Automatické vs. ručné vydávanie certifikátov
   - Správa a zálohovanie privátnych kľúčov
7. Monitoring bezpečnosti
   - Auditovanie v OS
   - Auditovanie siete
   - IDS/IPS
   - Honeypots
   - Antivírusy
8. Zaistenie dostupnosti, zachovanie chodu firmy a Incident Response
   - Základné koncepty zaistenia funkčnosti firmy
   - SLA
   - Vysoká dostupnosť
   - Zálohovanie a obnova
   - Čo robiť, keď príde k napadnutiu firmy

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk