Enterprise Computing Solutions - Education Services

NABÍDKA ŠKOLENÍ

Prosím kontaktujte nás zde

Arrow ECS, a.s., 28. října 3390/111a, 702 00 Ostrava

Email: training.ecs.cz@arrow.com
Phone: +420 597 488 811

EC-Council Encryption Specialist

Kód:	DÉLKA:	CENA:
ECC_ECES	24 Hours (3 DENNÍ)	Kč bez DPH 33,000.00

Description

EC-Council Certified Encryption Specialist je nejnovější hard-core deepdive elitní školení této renomované firmy, které má za úkol seznámit bezpečnostní IT specialisty s principy a implementací šifrovacích metod. ECES školení je unikátní v tom, že se můžete dozvědět detaily o principech šifrování a hashů, ale i prakticky vyzkoušet jejich implementaci v reálných aplikacích a serverových řešeních. Toto školení vyučují naši specialisté s praktickou i odbornou znalostí principů kryptografie. Proto máte jedinečnou příležitost pro analýzu jednotlivých šifrovacích a podepisovacích rutin, která je pro naše odborné lektory oblíbeným tématem, které vám zpřístupní v maximálně srozumitelné i praktické formě. Pokud vás láká téma skrývání obsahu a odhalení jeho principu, je pro vás naše nové školení unikátní příležitostí pro konzultaci s opravdovými profesionály z oboru. V ceně kurzu je i celosvětově uznávaná zkouška EC-Council Encryption Specialist (E|CES), jejímž složením studenti dokládají praktickou znalost šifrování pevných disků, sestavení VPN a teorie šifer od cézarovy šifry po RSA či AES.

Toto školení pořádá společnost Gopas a.s.

Cíle

- Principy šifrování a podpisu
- Přehlednou analýzu různých rutin
- Praktickou implementaci šifrování v různých serverových i klientských ochranných technologiích

Určeno pro

Tento kurz je urcen pro administrátory bezpecnosti, správce sítí, správce firewallu, testery zabezpecení IT infrastruktury, systémové adminstrátory, pentestery, forenzní analytiky a pro každého, kdo se zajímá o možnosti skrývání obsahu na hlubší úrovni než je pouhé stažení aplikace pro šifrování a její spuštení klikáním myši.

Vstupní znalosti

Praktická správa MS Windows prostředí na úrovni kurzů uvedených v předchozích školeních

Program

Modul 1 - úvod do kryptografie a její vývoj

- Principy kryptografie
- Historický vývoj
- Monoalfabetická substituční šifra
- Cézarova šifra
- Atbaš
- ROT13
- Vigenerova šifra, příklad a prolomení
- ADFGVX šifra
- Playfairova šifra
- Enigma
- CrypTool

Modul 2 - symetrická kryptografie a hashe

- Symetrická kryptografie
- Teorie informace
- Kerckhoffsův princip
- Subsituce
- Transpozice
- Substituce a Transpozice
- Binární ano, or, xor
- Bloková šifra vs. Streamová šifra
- Feistelova šifra
- DES
- 3DES
- DESx
- AES
- Blowfish
- Serpent
- Twofish
- Skipjack
- IDEA
- ECB
- CBC
- RC4
- MD5, MD6

Modul 3 - teorie čísel a asymetrická kryptografie

- Asymetrická kryptografie
- Prvočísla
- Prvočísla
- Fibonacciho posloupnost
- Narozeninový paradox
- Generátory náhodných čísel
- Diffile-Hellman
- Rivest Shamir Adlemna (RSA)
- Jak funguje RSA
- Příklad RSA
- DSA
- Podepisování pomocí DSA
- Eliptické křivky
- Variace eliptických křivek
- Elgamal

Modul 4 – aplikace šifrování

- Digitální podpis
- Co je to digitální certifikát
- X.509
- Obsah certifikátu X.509
- Certifikační autorita
- Registrační autorita
- PKI – Infrastruktura veřejného klíče
- Digitální certifikáty
- Protokoly pro ověřování certifikátu serveru
- Správa certifikátů
- Důvěryhodnost certifikátů
- Používání certifikátů ve webových službách
- MS Certifikační služby
- Windows certifikáty a certmgr.msc
- Pretty Good Privady (PGP)
- Certifikáty PGP
- SSL
- TLS
- Šifrování souborů pomocí EFS
- Zálohování EFS klíčů
- Obnova EFS klíčů
- BitLocker, Truecrypt
- Steganografie – vývoj, implementace a analýza

Modul 5 – aplikace šifrování

- Lámání šifer
- Kryptoanalýza
- Frekvenční analýza
- Lámání moderních šifer
- Lineární kryptoanalýza
- Diferenční kryptoanalýza
- Integrální kryptoanalýza
- Rainbow Tables
- Lámání hesel
- Nástroje

Termíny školení

Termíny školení na vyžádání, kontaktujte nás prosím

Dodatečné informace

Školení je možné zajistit na míru. Kontaktujte nás pro bližší informace.