Hardening Linux a Windows serverov podľa CIS a STIG

Kód kurzu: LXHARD

V tomto štvordňovom kurze účastníci získajú teoretické aj praktické zručnosti pri aplikovaní CIS a STIG odporúčaní, audite a automatizácii hardeningu (Ansible, SCAP nástroje).

Pre koho je kurz určený

IT administrátori, bezpečnostní špecialisti, DevOps/SecOps inžinieri.

Čo Vás naučíme

- Pochopiť princípy CIS a STIG, rozdiely a použitie v praxi.
- Mať schopnosť manuálne i automatizovane hardenovať Linux a Windows servery.
- Mať zručnosť v používaní audit-nástrojov (OpenSCAP, CIS-CAT, STIG Viewer / SCAP).
- Budete mať hotový Ansible playbook pre hardening a reportovacie skripty.

Požadované vstupné znalosti

Základy správy Linuxu a Windows (práca s príkazovým riadkom, základné GPO/AD znalosti).

Študijné materiály

Prezentácie, PDF osnovy, VM obrazy/virtuálne stroje, ukážkové skripty a playbooky, certifikát účasti.

Osnova kurzu

- Úvod + CIS pre Linux &Windows
- Úvod do hardeningu: princípy (minimalizácia útočnej plochy, least privilege), bežné hrozby a regulácie (PCI DSS, NIST).
- Prehľad CIS Benchmarks: štruktúra, Level 1 vs Level 2, ako získať a čítať benchmark.
- Príklady odporúčaní CIS pre Linux aj Windows (účty, služby, logovanie, sieť).
- Praktické cvičenie: analýza CIS Benchmark (napr. Ubuntu a Windows Server) a demo skenovania (CIS-CAT Lite/Pro).
- STIG, porovnanie STIG vs CIS + pracovné nástroje
- Úvod do STIG (DISA, CAT I-III), SCAP, rozdiely oproti CIS a kedy použiť ktorý štandard.
- Práca so STIG Viewer a SCAP nástrojmi, demo SCAP/OSCAP skenovania.
- Skupinová aktivita: porovnanie konkrétneho pravidla (napr. politika hesiel) v CIS vs STIG.
- Hands-on: Hardening Linux
- Kernel &sysctl, systemd služieb, firewall (firewalld/ufw), správa súborových oprávnení, SELinux/AppArmor.
- Príklady CIS a STIG pravidiel pre Linux (vysvetlenie a vplyv).
- Praktický lab: manuálny hardening Ubuntu/RHEL podľa CIS Level 1; implementácia vybraných STIG CAT I pravidiel.
- Overenie shody: OpenSCAP / CIS-CAT skenovanie a interpretácia výsledkov.
- Hands-on: Hardening Windows + Ansible automatizácia
- Hardening Windows Server (Group Policy, registrácia, firewall, Windows Defender), CIS a STIG príklady (SMBv1, audit, ACL).
- Úvod do Ansible (inventory, playbooky) + prehľad CIS/ STIG role a WinRM pre Windows.
- Workshop: vytvorenie a spustenie Ansible playbookov — Linux aj Windows hardening.
- Záverečný projekt: nasadiť playbook a overiť compliance (CIS-CAT / OpenSCAP).

GOPAS Praha
Na Strži 2097/63
140 00 Praha 4 - Krč
Tel.: +420 226 201 390
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 530 513 590
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 902 903 132
info@gopas.sk