Certified Network Defender version 2

Course code: CNDv2

CND je pokročilý bezpečnostní kurz s velkým množstvím praktických ukázek a cvičení, kde si účastníci formou praktického nasazení seznámí se všemi základními komponentami obrany IT prostředí nezbytných pro efektivní obranu IT prostředí proti hackingu. Jedná se o unikátní školení, kde se každý z účastníků dozví nejčastější chyby v bezpečnosti enterprise prostředí a seznámí se s technikami zabezpečení pro eleminici bezpečnostních rizik a tyto techniky si vyzkouší také prakticky. Je to tedy ideální školení pro budoucí IT specialisty v oboru bezpečnosti, kteří chtějí získat ucelený přehled i praktickou zkušenost IT bezpečnostních opatření. Dozví se nejen nezbytnou teorii bezpečnosti, ale absolventi pochopí důvody pro zavádění bezpečnostních opatření pomocí praktických ukázek hackingu běžného IT prostředí a mohou vidět eliminaci útoků po aplikování bezpečnostních opatření vytvářených v průběhu kurzu. Tento kurz učí lektoři etického hackingu provádějící penetrační testy a proto se účastníci dozvědí nejčastější chyby v zabezpečení IT z reálného provozu a mohou se lépe zabezpečit proti budoucím penetračním testům a reálným útokům.Absolventi pochopí principy IDS/IPS systémů a sami si vytvoří funkční IPS systém a detekční pravidla, pomocí nichž mají za úkol ubránit napadaný systém v reálném prostředí. Dále detekují napadené systémy na úrovni sítě prostřednictvím praktického zavedení Honeypot sítě, kde se seznámí nejen s nasazením a managementem honeypot systémů, ale také se naučíme praktické postupy pro efektivní odklonění útoku prostřednictvím honeypot systémů a naučíme se prakticky pravidla pro správné odstínění napadaných systémů od zbytku produkčního prostředí. V další části se seznámí s obranou koncových systémů na Windows, Linux i mobilní platformě.Naučíte se efektivně eliminovat hrozby malware a kryptování dat ransomwarem prostřednictvím efektivní analýzy aplikací a maker v produkčním prostředí a aplikováním správných pravidel application whitelistingu, makro whitelistingu i sandboxingu. Dále se naučíme minimalizovat rizika a dopad útoku exploitace pomocí skenování zranitelností a patch managementu a aplikováním správných baseline politik.Minimalizujeme riziko krádeže identity prostřednictvím praktického nasazení vícefaktorového ověřování MFA, kdy si účastníci prakticky vyzkouší zavedení ověřování pomocí asymetrické kryptografie - prakticky si provedeme implementaci ověřování pomocí SSH klíčů, klientských certifikátů, Smart Card ověřování pomocí virtuálních i fyzických karet a s tím související PKI Enterprise Deployment. Naučíme se také nejen praktickou segmentaci sítě pomocí 802.1x a WPA-Eterprise bezdrátových sítí a obranu proti nejčastějším síťovým útokům jako je DHCP Snooping, Dynamic ARP Inspection, IP Source Guard, ale také doporučení pro správné provedení analýzy prostředí před jejich zavedením pro minimalizaci dopadů změn v konfiguraci sítě a nejčastější chyby, na kterým správci v praxi čelí a jak jim předcházet.Naučíme se sledovat bezpečnostní události pomocí sledování událostí v systémech a sběru logů v SIEMu.

Pro koho je kurz určen

Kurz je velmi vhodný pro správce bezpečnosti počítačových sítí, systémové administrátory, absolventy kurzů etického hackingu GOC3 – Hacking v Praxi a CEH – Certified Ethical Hacker a každého, kdo hledá relevantní obranu proti etickému i neetickému hackingu.

Co Vás naučíme

Zabezpečit síť proti nejčastějším hacking útokům

Implemetovat segmentaci sítě a zabezpečit přístup do sítě pomocí 802.1x a WPA Enterprise včetně správné konfigurace klientů

Implementovat Smart Card pro bezpečné ověřování ve Windows prostředí

Ochránit koncové systémy proti malware hrozbám

Implementovat IDS/IPS pro sledování síťové komunikace

Implementovat Honeypot systémy a správně zabezpečit jejich provoz

Sledovat bezpečnostní události

Požadované vstupní znalosti

Doporučujeme předchozí absolvování krutzů CompTIA Security+. Dobrá znalost správy operačních systémů a znalost síťových protokolů na úrovni kurzu GOC2 a GOC3 jsou nezbytnou podmínkou.

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

Osnova kurzu

IDS/IPS - intrusion detection system / intrusion preverntion system

- Princip pravidel sledování síťové komunikace
- Správa a vytváření vlastních pravidel
- Konfigurace systému pro sledování provozu
- Konfigurace SPAN portu
- Inline režim
- Změny v TCP provozu

HoneyPots

- Role honeypotu v síťové bezpečnosti
- Lightweight vs. full honeypot
- Praktická implementace honeypot systémů
- Sledování systémů
- Správná implementace sítě pro minimalizaci dopadu honeypot napadení

EndPoint Security

- Windows Endpoint security
- Linux Endpoint security
- Mobile Endpoint security
- OS Hardening
- Šifrování disků
- HIPS

Effective Malware protection - Application Whitelisting a Macro whitelisting

- Analýza prostředí z pohledu spouštěného kódu
- Analýza prostředí z pohledu procesů
- Sledování logů a doplňování nových pravidel
- Vynucení pravidel
- Analýza office dokumentů v bezpečném prostředí
- Správa CodeSigning certifikátů
- Správa trusted publishers1

Passwordless environment and Multifactor authentication

- Ověřování pomocí klíčů v SSH
- Ověřování pomocí SmartCard ve Windows Prostředí
- Virtual Smart Card
- PKI management a Deployment certifikátů

802.1x a WPA Enterprise a zabezpečení síťových segmentů

- Analýza prostředí před nasazením opatření
- RADIUS, NAC - Network Access Controller,
- Radius server konfigurace
- Doporučení pro certifikáty Radius serveru
- Konfigurace supplicant řešení pro Microsoft i Linux
- Deployment certifikátů pro supplicanty
- Doporučení pro Windows/Linux deployment
- Implementace DHCP Snoopingu
- Implementace ARP Inspection
- Implementace IP Source Guard

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

- MAC whitelisting
- Switchport port security maximum

SIEM

- Princip sledování událostí ve Windows
- Princip sledování událostí na Linuxu
- Princip sledování událostí u síťových prvků
- Sběr událostí
- Analýza událostí

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