Certified Network Defender version 2

Kód kurzu: CNDv2

CNDv2 je pokročilý bezpečnostný kurz s veľkým množstvom praktických ukážok a cvičení, kde sa účastníci formou praktického nasadenia zoznámia so všetkými základnými komponentami obrany IT prostredia nevyhnutných pre efektivnu obranu IT prostredia proti hackingu. Ide o unikátne školenie, kde sa každý z účastníkov dozvie najčastejšie chyby v bezpečnosti enterprise prostredia a zoznámi sa s technikami zabezpečenia pre elimináciu bezpečnostných rizík a tieto techniky si vyskúša tiež prakticky. Je to teda ideálne školenie pre budúcich IT špecialistov v odbore bezpečnosti, ktorí chcú získať ucelený prehľad aj praktickú skúsenosť IT bezpečnostných opatrení. Dozvedia sa nielen nevyhnutnú teóriu bezpečnosti, ale absolventi pochopia dôvody pre zavedenie bezpečnostných opatrení pomocou praktických ukážok hackingu bežného IT prostredia a môžu vidieť elimináciu útokov po aplikovaní bezpečnostných opatrení vytváraných v priebehu kurzu. Tento kurz učia lektori etického hackingu vykonávajúci penetračné testy, a preto sa účastníci dozvedia najčastejšie chyby v zabezpečení IT z reálnej prevádzky a môžu sa lepšie zabezpečiť proti budúcim penetračným testom a reálným útokom.Absolventi pochopia princípy IDS/IPS systémov a sami si vytvoia funkčný IPS systém a detekčné pravidlá, pomocou ktorých majú za úlohu ubrániť napádaný systém v reálnom prostredí. Ďalej detekujú napadnuné systémy na úrovni siete prostredníctvom praktického zavedenia Honeypot siete, kde sa zoznámia nielen s nasadením a managementem honeypot systémov, ale taktiež sa naučia praktické postupy pre efektívne odklonenie útokov prostredníctvom honeypot systémov a naučia sa praktické pravidlá pre správne odtienenie napádaných systémov od zvyšku produkčného prostredia. V ďalšej časti sa zoznámia s obranou koncových systémov na Windowse, Linuxe aj mobilnej platforme.Naučia sa efektívne eliminovať hrozby malware a kryptovania dát ransomwarom prostredníctvom efektívnej analýzy aplikácií a makier v produkčnom prostredí a aplikovaním správnych pravidiel application whitelistingu, makro whitelistingu a sandboxingu. Ďalej sa naučia minimalizovať riziká a dopad útoku exploitácie pomocou skenovania zraniteľností a patch managementu a aplikovaním správnych baseline politík.Minimalizujeme riziko krádeže identity prostredníctvom praktického nasadenia viacfaktorového overovania MFA, kedy si účastníci prakticky vyskúšajú zavedenie overovania pomocou asymetrickej kryptografie - prakticky si vykonáme implementáciu overovania pomocou SSH kľúčov, klientskych certifikátov, Smart Card overovanie pomocou virtuálnych a fyzických kariet a s tým súvisiace PKI Enterprise Deployment. Naučíme sa tiež nielen praktickú segmentáciu siete pomocou 802.1x a WPA-Eterprise bezdrôtových sietí a obranu proti najčastejším sieťovým útokom ako je DHCP Snooping, Dynamic ARP Inspection, IP Source Guard, ale taktiež odporúčanie pre správne vykonanie analýzy prostredia pred ich zavedením pre minimalizáciu dopadov zmien v konfigurácii siete a najčastejšie chyby, ktorým správcovia v praxi čelí a ako im predchádzať.Naučíme sa sledovať bezpečnostné udalosti pomocou sledovania udalostí v systémoch a zberu logov v SIEMe.

Pre koho je kurz určený

Kurz je veľmi vhodný pre správcov bezpečnosti počítačových sietí, systémových administrátorov, absolventov kurzov etického hackingu GOC3 – Hacking v Praxi a CEH – Certified Ethical Hacker a každého, kto hľadá relevantnú obranu proti etickému i neetickému hackingu.

Čo Vás naučíme

Zabezpečiť sieť proti najčastejším hacking útokom

Implementovať segmentáciu siete a zabezpečiť prístup do siete pomocou 802.1x a WPA Enterprise vrátane správnej konfigurácie klientov

Implementovať Smart Card pre bezpečné overovanie vo Windows prostredí

Ochrániť koncové systémy proti malware hrozbám

Implementovať IDS/IPS pre sledovanie sieťovej komunikácie

Implementovať Honeypot systémy a správne zabezpečiť ich prevádzku

Sledovať bezpečnostné udalosti

Požadované vstupné znalosti

Odporúčame predchádzajúce absolvovanie kurzu CompTIA Security+. Dobrá znalosť správy operačných systémov a znalosť sieťových protokolov na úrovni kurzov GOC2 a GOC3 sú nevyhnutnou podmienkou.

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

- Princíp pravidiel sledovania sieťovej komunikácie
- Správa a vytváranie vlastných pravidiel
- Konfigurácia systému pre sledovanie prevádzky
- Konfigurácia SPAN portu
- Inline režim
- Zmeny v TCP prevádzke

HoneyPots

- Role honeypotu v sieťovej bezpečnosti
- Lightweight vs. full honeypot
- Praktická implementácia honeypot systémov
- Sledovanie systémov
- Správna implementácia siete pre minimalizáciu dopadu honeypot napadnutia

EndPoint Security

- Windows Endpoint security
- Linux Endpoint security
- Mobile Endpoint security
- OS Hardening
- Šifrovanie diskov
- HIPS

Effective Malware protection - Application Whitelisting a Macro whitelisting

- Analýza prostredia z pohľadu spúšťaného kódu
- Analýza prostredia z pohľadu procesov
- Sledovanie logov a doplňovanie nových pravidiel
- Vynútenie pravidiel
- Analýza office dokumentov v bezpečnom prostredí
- Správa CodeSigning certifikátov
- Správa trusted publishers

Passwordless environment and Multifactor authentication

- Overovanie pomoco kľúčov v SSH
- Overovanie pomocou SmartCard vo Windows prostredí
- Virtual Smart Card
- PKI management a Deployment certifikátov

802.1x a WPA Enterprise a zabezpečenie sieťových segmentov

- Analýza prostredia pred nasadením opatrení
- RADIUS, NAC - Network Access Controller
- Radius server konfigurácia
- Odporúčania pre certifikáty Radius serveru
- Konfigurácia supplicant riešení pre Microsoft a Linux
- Deployment certifikátov pre supplicanty
- Odporúčania pro Windows/Linux deployment
- Implementácia DHCP Snoopingu
- Implementácia ARP Inspection
- Implementácia 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

- Princíp sledovania udalostí vo Windows
- Princíp sledovania udalostí na Linuxu
- Princíp sledovania udalostí u sieťových prvkov
- Zber udalostí
- Analýza udalostí

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