Network Security – Etický hacking v praxi

Kód kurzu: GOC3

Toto školenie hackingu vás zoznámi so základnými nástrojmi a princípmi, ktoré sa používajú pre útoky a penetračné testovanie. Kurz vám umožní do detailu pochopiť a vyskúšať si metódy, pomocou ktorých sa vykonávajú útoky na naše počítačové siete a serverové systémy z vnútornej časti siete a pri útokoch Man-in-the-Middle proti klientom mimo vnútornú sieť. Účastníci si vyskúšajú radu techník ako na Windows platforme, tak aj na Linuxe. Účasť na tomto kurze alebo zodpovedajúce znalosti sú nutným predpokladom pre účasť na kurze CEH - Certified Ethical Hacker.

Pre koho je kurz určený

Kurz je určený správcom sietí, ktorí sú zodpovední za bezpečnosť počítačových sietí a chcú pomocou praktických ukážok porozumieť, prečo je nutné zavádzať opatrenia, ktoré štandardné bezpečnostné kurzy a oficiálne Whitepapery vysvetľujú len teoreticky. Kurz môžeme odporučiť aj správcom sieťovej infraštruktúry na hlbšie porozumenie princípom TCP/IP protokolu. Vďaka úvodnej časti opakovania TCP/IP sa na kurze môžu zúčastniť všetci, ktorí už majú znalosti a skúsenosti na úrovni kurzu GOC2 alebo aspoň ročnú skúsenosť s administráciou sieťových služieb. V priebehu kurzu používame nástroje pre Windows i ich ekvivalenty v Linux prostredí, avšak vďaka detailným vysvetleniam a inštrukciám v priebehu kurzu znalosť Linux systémov nie je potrebná.

Čo Vás naučíme

Náš výnimočný kurz Network Security - Hacking v praxi Vám umožní do detailu pochopiť a vyskúšať si metódy, pomocou ktorých sa vykonávajú útoky na naše počítačové siete a serverové systémy. V priebehu kurzu si postupne vysvetlíme a vyskúšame všetko, čo potrebujete poznať na obranu proti technikám na mapovanie prostredí napádaných firiem, skenovanie sieťového prostredia, ARP Poisioning, ukladanie a prenos hesiel v sieti a metódy na ich zachytávanie a prelamovanie pomocou CPU, GPU a distribuovaného útoku. V nasledujúcej časti kurzu preberáme slabiny bezdrôtových sietí, kde si vysvetlíme jednotlivé druhy prevádzky vo WiFi sieťach a máte možnosť prakticky si vyskúšať monitorovanie WiFi sietí i techniky generovania sieťovej prevádzky pomocou WiFi Injection, odpájanie klientov v sieti, zachytávanie prevádzky v monitorovacom móde a prelamovanie hesiel do WEP a WPA sietí. V záverečnej časti kurzu si precvičíme napádanie počítačových systémov pomocou obávanej exploitácie služieb a tiež si ukážeme hlavný cieľ dnešných hacking útokov, kde si vyskúšate ovládanie vlastného botnetu. Ukážeme si tiež pokročilé útoky Man in the Middle, ktoré sa dnes používajú na elimináciu zabezpečenia HTTPS a spôsoby skrývania informácií.

Osnova kurzu

Úvod

- Opakovanie TCP/IP
- Odchytávanie dát v sieťovom analyzéri
- Vyhľadávanie informácií z internetových zdrojov

Analýza prostredí a prvé útoky

- Analýza prostredí náchylných k sociálnemu inžinierstvu
- Skenovanie sieťových služieb pomocou skenovania otvorených portov a bannerov
- Analýza používaných operačných systémov
- Princíp a aplikovanie ARP Poisioning pomocou nástrojov pre MS Windows i Linux

Heslá a ich prelamovanie

- Princípy ukladania hesiel v operačných systémoch
- Prenos hesiel pri sieťovom overovaní
- Downgrade overovacích metód

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

- Útoky na heslá hrubou silou pomocou CPU, grafických kariet a distribuovaného útoku
- Rainbow Tables - princípy vyhľadávania, spôsob generovania pre konkrétne prostredie a druhy útokov, analýza
- Time/Memory Tradeoff efektu
- SMB rRlay a SMB Reflection Attack

Bezdrôtové siete

- Druhy rámcov používaných v bezdrôtových sieťach
- Analýza bezdrôtových sietí v dosahu
- Zneužitie neautorizovaných rámcov
- WiFi Injection a monitor mód WiFi kariet
- Útoky na WEP siete
- Útoky na WPA1 PSK a WPA2 PSK siete
- Prelamovanie EAPOL rámcov pomocou grafických kariet
- Votrelecká AP

Pokročilejšie útoky

- Možnosti Ettercap pre MitM
- Využitie Metasploit Framework pre exploitáciu sieťových služieb
- Vytváranie vlastnej Botnet siete
- Skrývanie prostriedkov pomocou steganografie a rootkitov
- MitM a obchádzanie HTTPS zabezpečení

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