Network Security – Etický hacking v praxi

Kód kurzu: GOC3

Toto školení vás seznámí se základními nástroji a principy, které se používají pro útoky a penetrační testování. Náš ojedinělý pětidenní kurz vám umožní do detailu pochopit i vyzkoušet metody, pomocí kterých se provádí útoky na počítačové sítě a serverové systémy z vnitřní části sítě a při útocích Man-in-the-Middle proti klientům mimo vnitřní síť. Účastníci si vyzkouší řadu technik jak na Windows platformě, tak i na Linuxu. Účast na tomto kurzu nebo odpovídající znalosti jsou nutným předpokladem pro účast na kurzu CEH - Certified Ethical Hacker.

Pro koho je kurz určen

Kurz je určen správcům sítí, kteří jsou zodpovědní za bezpečnost počítačových sítí a chtějí pomocí praktických ukázek porozumět, proč je nutné zavádět opatření, které standardní bezpečnostní kurzy a oficiální whitepapery vysvětlují pouze teoreticky. Kurz můžeme doporučit i správcům síťové infrastruktury pro hlubší porozumění principům TCP/IP protokolu. Díky úvodní části opakování TCP/IP se kurzu mohou účastnit všichni, kdo již mají znalosti a zkušenosti na úrovni kurzu GOC2 nebo alespoň roční zkušenosti s administrací síťových služeb a znalosti základní správy serverových operačních systémů. V průběhu kurzu používáme nástroje pro Windows i jejich ekvivalenty v Linux prostředí, avšak díky detailním vysvětlením i instrukcím v průběhu kurzu znalost linux systémů není zapotřebí.

Co vás na kurzu naučíme

Náš ojedinělý kurz GOC3 Hacking v praxi Vám umožní do detailu pochopit i vyzkoušet metody, pomocí kterých se provádí útoky na naše počítačové sítě a serverové systémy. V průběhu kurzu si postupně vysvětlíme i vyzkoušíme vše, co potřebujete znát pro obranu proti technikám pro mapování prostředí napadaných firem, skenování síťového prostředí, ARP poisioning, ukládání a přenos hesel v síti a metody pro jejich zachytávání a prolamování pomocí CPU, GPU a distribuovaného útoku. V následující části kurzu probíráme slabiny bezdrátových sítí, kde si vysvětlíme jednotlivé druhy provozu ve WiFi sítích a máte možnost si prakticky vyzkoušet monitorování WiFi sítí i techniky generování síťového provozu pomocí WiFi injection, odpojování klientů v síti, zachytávání provozu v monitorovacím módu a prolamování hesel do WEP a WPA sítí. V závěrečné části kurzu si ukážeme také pokročilé útoky Man in the Middle, které se dnes používají pro eliminaci zabezpečení HTTPS, co hrozí na nezáplatovaných systémech - napadání počítačových systémů pomocí obávané exploitace služeb a metody skrývání v napadeném systému.

Osnova kurzu

Úvod

- Opakování TCP/IP
- Odchytávání dat v síťovém analyzéru
- Vyhledávání informací z Internetových zdrojů
- Spouštění procesů pod službami a plánovanými úlohami

Analýza prostředí a první útoky

- Analýza prostředí náchylných k sociálnímu inženýrství
- Skenování síťových služeb pomocí skenování otevřených portů a bannerů
- Analýza používaných operačních systémů
- Princip a aplikování ARP poisioningu pomocí nástrojů pro Microsoft Windows i Linux

Hesla a jejich prolamování

- Principy ukládání hesel v operačních systémech
- Přenos hesel při síťovém ověřování
- Downgrade ověřovacích metod

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

Copyright © 2020 GOPAS, a.s.,
All rights reserved

- Útoky na hesla hrubou silou pomocí CPU, grafických karet a distribuovaného útoku
- Rainbow Tables - principy vyhledávání, způsob generování pro konkrétní prostředí a druhy útoků, analýza time/memory tradeoff efektu

Bezdrátové sítě

- Druhy rámců používaných v bezdrátových sítích
- Analýza bezdrátových sítí v dosahu
- Zneužití neautorizovaných rámců
- WiFi Injection a monitor mód WiFi karet
- Útoky na WEP sítě
- Útoky na WPA1 PSK a WPA2 PSK sítě
- Prolamování EAPOL rámců pomocí grafických karet
- Vetřelecká AP
- WPS

Pokročilejší útoky

- Zasílání falešných certifikátů, importování kořenových certifikačních autorit a vytváření legitimních falešných certifikátů obcházení HTTPS zabezpečení
- Využití Metasploit Frameworku pro exploitaci síťových služeb
- Skrývání prostředků pomocí rootkitů

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

Copyright © 2020 GOPAS, a.s.,
All rights reserved