Capture the Flag - hackni si Windows podnikovú sieť 1

Kód kurzu: GLAB007

Dvojdňové praktické cvičenia o tom, ako sa pomocou účtu obyčajného užívateľa postupne vypracovať na vládcu celej podnikovej počítačovej siete, postavenej na Microsoft technológiách. Krok za krokom boj o jednotlivé vlajky vo forme účtov, hesiel alebo utajovaných informácií, skrytých na chránených serveroch alebo v emailových schránkach. Zažite pocit, že to dokážete. A pochopte, ako sa máte správať, aby sa to nestalo vo vašej vlastnej sieti.

Pre koho je kurz určený

GLAB kurzy sú praktické adrenalínové cvičenia na počítačoch. Účastníci dostanú iba zoznam úloh, ktoré majú splniť a snažia sa samostatne nájsť riešenia predložených problémov. Lektor sa zúčastňuje iba ako sprievodca, radca a pomocník, ktorý vás vytiahne z najhoršieho.

GLAB je teda určený všetkým, ktorí majú radi výzvy, radi sa bavia a chcú si dokázať, že sú schopní pracovať v časovom strese a dozvedieť sa, kde majú medzery. Na svoje si prídu aj tí súťaživí z vás, pretože po splnení úloh dostávate prestížny certifikát.

Štandardné MOC a GOC kurzy účastníkov pripravujú hlavne teoreticky a riešia problémy z jednoduchého implementačného pohľadu, kým GLABy sú hlavne o útočení, riešení problémov a tiež o implementácii komplexnejších scenárov, vďaka ktorým vedomosti z bežného kurzu "zapadnú do seba".

Ani certifikačné skúšky Microsoft ani EC-Council neskúšajú praktickú stránku veci, naše GLABy sú celosvetovo výnimočnou príležitosťou!

Lektor je na kurze preto, aby vás viedol v samostatnej práci, uvádzal vás do jednotlivých krokov a scenárov a pomohol vám, ak už nebudete môcť ďalej.

Čo vás na kurze naučíme

- Vyskúšate
- si samostatne riešiť problémy, o ktorých sa na kurzoch iba hovorí
- Nebojte
- sa, že by sme vás v tom nechali samotných, lektor vám vždy pomôže, keď budete potrebovať
- Užijete
- si napätie, adrenalín a prácu pod časovým stresom, môžete si zasúťažiť s kolegami
- Dokážete
- si, že na to máte a že to viete
- Ukážete
- svoje schopnosti aj svojmu okoliu, pretože po absolvovaní dostanete prestížny certifikát, ktorý to jasne dokazuje
- Dozviete
- sa, čo ešte nepoznáte a kde máte medzery pre ďalšie štúdium, lektor vám krátko zdôvodní neúspechy, prípadne po skončení prediskutujete detaily
- GLAB
- môžete vďaka štandardnej "garancii vedomostí" navštíviť dvakrát, bez ohľadu na to, akí úspešní budete. Môžete ho absolvovať aj vzdialene a nemusíte kvôli tomu sedieť v učebni.

Predpokladané vstupné znalosti

Znalosti v rozsahu kurzov uvedených v sekciách Predchádzajúce kurzy a Súvisiace kurzy

Osnova kurzu

- Rekognoskácia siete postavenej na Windows Active Directory
- Zoznamy účtov a vyhľadanie zraniteľností a cieľov útoku

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

- Obchádzanie Secure Boot a Credential Guard (Device Guard)
- Vypnutie Credential Guard (Device Guard)
- Metódy SSO (single-sign-on) injection
- Využitie script injection
- Offline útok na operačný systém
- Offline útok na BitLocker
- Reinstalačný útok na BitLocker
- Útok na virtuálny server z pozície správcu Hyper-V virtualizáciu
- Softvér keylogger pod obyčajným užívateľom
- Využitie rovnakých hesiel rôznych účtov
- Heslá servisných účtov, IIS a naplánovaných úloh
- Laterálny pohyb prostredím Windows podnikovej siete
- Obchádzanie UAC (User Account Control)
- Útoky pass-the-hash a pass-the-ticket
- Uložené heslá Windows
- Získavanie hesiel z KeePass a ďalších trezorov na heslá
- Skrývanie útočných skriptov a škodlivého kódu všeobecne
- Zneužitie Kerberos delegation a Kerberos delegation with protocol transition
- Krádež certifikačnej autority
- Získanie forest admin oprávnenia z podriadenej domény Prístup k podnikovým emailovým schránkam služby Office365

Príprava k certifikačným skúškam

Kurz nie je priamo určený ako príprava na žiadnu konkrétnu certifikačnú skúšku, ale výborne sa hodí ako praktická príprava k čomukoľvek, čo sa týka bezpečnosti, alebo etického hackingu

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