Capture the Flag - Hacking Windows Infrastructure 1

Course code: GLAB007

The two days interactive lab leads the students using lateral movement through a Windows enterprise environment in order to gain Domain Admins credentials.

Pro koho je kurz určen

GLAB kurzy jsou praktická adrenalinová cvičení na počítačích. Účastníci dostanou pouze seznam úkolů, které mají splnit a snaží se samostatně najít řešení předložených problémů. Lektor se účastní pouze jako průvodce, rádce a pomocník, který vás vytáhne z nejhoršího.

GLAB je tedy určen všem, kdo mají rádi výzvy, rádi se baví a chtějí si dokázat, že jsou schopni pracovat v časovém stresu a dozvědět se, kde mají mezery. Na své si přijdou i ti soutěživí z vás, protože po splnění úkolů dostáváte prestižní certifikát.

Standardní MOC a GOC kurzy účastníky připravují hlavně teoreticky a řeší problémy z jednoduchého implementačního pohledu. Zatímco GLABy jsou hlavně o útočení, řešení potíží, a také o implementaci komplexnějších scénářů, díky kterým vědomosti z běžného kurzu "zapadnou do sebe".

Ani certifikační zkoušky Microsoft ani EC-Council nezkouší praktickou stránku věci, naše GLABy jsou celosvětově výjimečnou příležitostí!

Lektor je na kurzu proto, aby vás vedl v samostatné práci, uváděl vás do jednotlivých kroků a scénářů a pomohl vám, pokud už nebudete moci dál.

Co vás na kurzu naučíme

Vyzkoušíte si samostatně řešit problémy, o kterých se na kurzech pouze mluví

Nebojte se, že bychom vás v tom nechali samotné, lektor vám vždy pomůže, když budete potřebovat

Užijete si napětí, adrenalin a práci pod časovým presem, můžete si zasoutěžit s kolegy

Dokážete si, že na to máte a že to umíte

Ukážete svoje schopnosti i svému okolí, protože po absolvování dostanete prestižní certifikát, který to jasně dokazuje

Dozvíte se, co ještě neznáte a kde máte mezery pro další studium, lektor vám krátce zdůvodní neúspěchy, případně po skončení prodiskutujete detaily

GLAB můžete díky standardní "garanci vědomostí" navštívit dvakrát, bez ohledu na to, jak úspěšní budete. Můžete ho absolvovat i vzdáleně a nemusíte kvůli tomu sedět v učebně.

Předpokládané vstupní znalosti

Znalosti v rozsahu kurzů uvedených v sekcích Předchozí kurzy a Související kurzy

Osnova kurzu

Rekognoskace sítě postavené na Windows Active Directory

Seznamy účtů a vyhledání zranitelností a cílů útoku

Obcházení Secure Boot a Credential Guard (Device Guard)

Vypnutí Credential Guard (Device Guard)

Metody SSO (single-sign-on) injection

Využití script injection

Offline útok na operační systém

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

Offline útok na BitLocker

Reinstalační útok na BitLocker

Útok na virtuální server z pozice správce Hyper-V virtualizaci

Software keylogger pod obyčejným uživatelem

Využití stejných hesel různých účtů

Hesla servisních účtů, IIS a naplánovaných úloh

Laterální pohyb prostředím Windows podnikové sítě

Obcházení UAC (User Account Control)

Útoky pass-the-hash a pass-the-ticket

Uložená hesla Windows

Získávání hesel z KeePass a dalších trezorů na hesla

Skrývání útočných skriptů a škodlivého kódu obecně

Zneužití Kerberos delegation a Kerberos delegation with protocol transition

Krádež certifikační autority

Získání forest admin oprávnění z podřízené domény

Přístup k podnikovým emailovým schránkám služby Office365

Příprava k certifikačním zkouškám

Kurz není přímo určen jako příprava na žádnou konkrétní certifikační zkoušku, ale výborně se hodí jako praktická příprava k čemukoliv, co se týká bezpečnosti, nebo 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

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