Capture the Flag - Hacking Windows Infrastructure 2

Course code: GLAB008

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

Pro koho je LAB 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. Postupy řešení nejsou k dispozici, je znám pouze žádaný výsledek, který lektor zkontroluje.

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 **70%** 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 řešení potíží, a také o implementaci komplexnějších scénářů, díky kterým vědomosti z běžného kurzu "zapadnou do sebe". Ani certifikační zkoušky **Microsoft** a **EC-Council** nezkouší praktickou stránku věci, naše GLABy jsou celosvětově výjimečnou příležitostí!

Ke kurzu GLAB nedostanete postup řešení, ale lektor, který je celou dobu cvičení účasten, má právo vám celkem 3x napovědět. Po skončení vám lektor v krátkosti zdůvodní vaše špatné řešení, případně s ním můžete probrat další detaily.

Co vás na kurzu naučíme

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

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

Dokážete si, že na to máte a že to umíte

Ukážete svoje schopnosti i svému okolí, protože po absolvování alespoň **70%** úkolů 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

Předpokládané vstupní znalosti

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

Dobrá znalost technologií TCP/IP a DNS

Metody výuky

Vlastní samostatná cvičení na virtuálních počítačích na platformě Hyper-V podle zadání úkolů

Lektor má právo vám během kurzu celkem 3x napovědět, nikoliv však kompletní řešení daného úkolu

Studijní materiály

Autorizované **GOPAS** zadání úkolů podle **GLAB** kurzu, v elektronické, nebo tištěné formě

Témata cvičení a úkolů, která se vyskytují buď na GLAB007 nebo GLAB008

Rekognoskace sítě postavené na Windows Active Directory

Seznamy účtů a vyhledání zranitelností a cílů útoku

Obcházení Secure Boot a Credential Guard (Device 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

Vypnutí Credential Guard (Device Guard)

Metody SSO (single-sign-on) injection

Využití script injection

Offline útok na operační systém

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

Zneužití špatného použití RDP přístupů správců

Injekce kódu do služeb a webových aplikací

Zneužití účtu správce AD FS (Active Directory Federation Services, ADFS) pro přístup do Office365 a Azure

Sociální inženýrství a využití fake-GUI

Krádeže software certifikátů uživatelů a počítačů k získání přístupu

Získávání šifrovacích klíčů databázím SQL Serveru

Obcházení MFA (multi-factor authentication) technologií

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