

Microsoft Azure - hacking a penetračné testovanie

Kód kurzu: GOC238

Päťdňový kurz predstavuje svet Microsoft cloudu z pohľadu etického hackera, penetračného testera, ale aj špinavého útočníka. Na praktických cvičeniach si účastník vyskúša, ako do prostredia Azure/Azure AD reálni útočníci prenikajú (initial access), ako potom napádajú ďalšie zdroje organizácie (privilege escalation, lateral movement), a tiež ako sa nepozorovane skrývajú pred obrancami (Defense evasion, persistence). Neskôr v druhej časti rozoberieme, ako sa proti útočným taktikám v jednotlivých fázach účinne brániť, alebo „Ak poznáš nepriateľa aj sám seba, môžeš bez obáv zviest sto bitiek. Ak poznáš seba, ale nie nepriateľa, raz vyhráš a druhýkrát prehráš. Ak nepoznáš ani seba ani nepriateľa, prehráš v každej bitke.“ Sun Tzu – Umenie vojny.

Pre koho je kurz určený

Kurz je vhodný ako pre obrancov, ktorí majú na starosti zabezpečenie cloudových služieb Azure/Microsoft 365 (blue team), tak aj pre penetračných testerov (red team).

Predpokladané vstupné znalosti

- Znalosti v rozsahu kurzov uvedených v sekciách
- **Predchádzajúce kurzy**
- a
- **Súvisiace kurzy**
- Dobrá znalosť technológií TCP/IP a DNS

Osnova kurzu

- Attack strategy na Azure a Azure AD (AAD)
- Pentesting nástroje
- Vyhľadávanie Azure zdrojov (public facing services) a ich zraniteľností
- Initial access útoky, exploitácia
- Prístupové tokeny a ich krádež
- Authenticated Enumeration
- Privilege Escalation
- Metódy persistence
- Data exfiltration
- Bypassing Defenses
- Security strategy na ochranu identít a zdrojov v Azure
- Ochrana identít (Password protection, MFA, Passwordless, Conditional access, PIM)
- Konfigurácia oprávnení pre skupiny a aplikačné identity
- Multi-layered approach ochrana pre jednotlivé komponenty IaaS, PaaS
- Defender for cloud - assess, detect and respond pre zdroje v Azure

Príprava na certifikačné skúšky

Pri certifikačných skúškach Microsoft platí, že okrem certifikácie MCM nie je účasť na oficiálnom MOC kurze nevyhnutnou podmienkou pre zloženie skúšky. Oficiálne kurzy MOC spoločnosti Microsoft a aj naše vlastné kurzy GOC sú vhodnou súčasťou prípravy na certifikačné skúšky spoločnosti Microsoft, ako sú MTA, MCP, MCSA, MCSE, alebo MCM. Primárnym cieľom kurzu však nie je priamo príprava na certifikačnú skúšku, ale zvládnutie teoretických princípov a osvojenie si praktických zručností potrebných na efektívnu prácu s daným produktom. MOC kurzy zvyčajne pokrývajú takmer všetky oblasti požadované pri príslušných certifikačných skúškach. Ich prebratie na kurze ale nebýva daný vždy presne rovnaký čas a dôraz, ako vyžaduje certifikačná skúška. Ako ďalšiu prípravu na certifikačné skúšky je možné využiť napríklad knihy od MS Press (tzv. Self-paced Training Kit) alebo elektronický self-test softvér.

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