Windows Server - Active Directory SAE, Tiering and Red Forest

Kód kurzu: GOC159

Trojdňový kurz je určený správcom a architektom IT infraštruktúry postavenej na Active Directory a Azure Active Directory, ktorí sa chcú dozvedieť, ako funguje bezpečnosť používateľských účtov, ako správne nakladať s privilegovanými účtami správcov, ako bezpečne spravovať celé on-prem aj hybridné prostredie tak, aby nedochádzalo ku kompromitácii prihlasovacích údajov správcov, a tým sa buď úplne zamedzilo, prípadne sa aspoň izolovali incidenty ako je ransomware a ďalšie dnešné nákazy i napríklad sa zabránilo vstupu a prežitie APT.

Pre koho je kurz určený

Kurz je určený správcom a architektom bezpečnosti a IT infraštruktúry primárne postavené na Active Directory (AD DS) a Azure Active Directory (AAD)

Čo vás na kurze naučíme

- Pochopiť, proti akým druhom útokov sú princípy SAE, tiering a red forest vhodné
- Porozumieť základným bezpečnostným princípom Active Diretor a Azure Active Directory, bezpečnosti ich účtov a skupín/rolí, replikáciou a hesiel a riadenia prístupu vnútri týchto adresárov
- Porozumieť ich schopnosti izolovať alebo úplne obmedziť vstup malware všeobecne a obzvlášť ransomware, spyware, APT (advanced persistent threats) a ich ďalšie šírenie
- Pochopiť, ako fungujú bezpečnostné technické opatrenia ako je LDAPS, Kerberos armoring, Kerberos Compound ID, Protected Users skupina, ako minimalizovať použitie NTLM a ďalej zabezpečiť prihlasovacie údaje privilegovaných účtov
- Ako vybudovať SAE (secure adminitrative environment) pre správu AD DS, serverov a staníc, Azure AAD, Office 365 dodatočných a cudzích cloudových služieb aj ostatných systémov ako sú sieťové prvky, tlačiarne atď.
- Prečo je potrebný a ako zaviesť tiering a účinne separovať privilegované účty správcov, ako k tomu využívať čipové karty a ďalšie viac-faktorové prihlasovacie metódy (MFA - multi factor authentication)
- Ako v danom prostredí umožniť pohodlnú správu IT adminom aj dodávateľom
- Prečo je forest takzvane security boundary, ako sa kompromitujú všetky domény v nich a prečo je vhodné prevádzkovať viac oddelených forestov, napríklad pre DMZ a pod.
- Ako a prečo zaviesť red forest pre prostredie s viacerými forestmi

Predpokladané vstupné znalosti

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

Osnova kurzu

- Príklady útokov, proti ktorým sa chceme brániť
- Spyware, ransomware, keyloggery, riziká heslovníčkov (password managers)
- Riziká uložených prihlasovacích údajov, riziká slabých hesiel, riziká (ne)uzamykania účtov
- SSO injections (single sign on), riziká impersonácie, riziká Kerberos delegácií a Kerberos protocol transition
- Riziká spojené s Enteprise AD CS (certification services) a vydávaním prihlasovacích certifikátov do čipových kariet (smart card logon)
- Kompromitácie Domain Admins účtu vedie ku kompromitácii celého forestu
- Možnosti nasadenia viac-faktorového overovania (multifactor authentication), smart-card logon (PKINIT), TPM virtuálne čipové karty, tokeny, využitie Azure MFA
- Účty a skupiny s právami a prístupom na úrovni Domain Admins alebo možnosťou elevácie na túto úroveň
- Princípy synchronizácie účtov a hesiel AD DS a Azure AD, overovanie pomocou AD FS (federation services) pre Office365 a Kerberos pass through overovanie pre Azure
- Riadenie prístupu vnútri AD DS LDAP a Azure AD, AdminSDHolder, LDAP permissions
- Riadenie prístupu k správe Group Policy a Intune a riziká ochrany s tým spojené, plus Advanced GPM

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

- Bezpečnosť DNS a nebezpečnosť DHCP
- Viac-doménové prostredie, forest trust (vzťahy dôvery) a overovanie používateľských účtov a bezpečné použitie skupín medzi nimi
- Identifikácia tier0 (DC) zariadenia a privilegovaných účtov správcov
- Identifikácia tier1 (servers) zariadenia a privilegovaných účtov správcov
- Idnetifikácia tier2 (endpoint) zariadenia a privilegovaných účtov správcov
- Izolácia tier0-tier1-tier2 privilegovaných účtov správcov pomocou User Rights Assignment, Kerberos Authentication Policies, Selective Autentication
- Využitie Windows Firewall alebo Private VLAN technológií k rozbíjaniu jednotlivých bezpečnostných zón (tier)
- Budovanie bezpečného prostredia pre správu (SAE - secure administrative environment)
- Technológie a vhodné bezpečnostné opatrenia na jump servery (JS), privileged access workstation (PAW) a privileged access management servery (PAM)
- Prístup a jeho ochrana na JS, PAW a PAM, zabezpečenie prihlasovacích údajov správcov v takom prostredí, prístup cez VPN a dočasný alebo trvalý prístup cudzích dodávateľov
- Integrácia identity (IDM) a red-forest scenáre pre viac doménové prostredie, oddelené Foresty pre DMZ a ďalšie izolované siete, OT a výrobné siete postavené na Windows

Príprava k certifikačným skúškam

Pri certifikačných skúškach Microsoft platí, že okrem certifikácie MCM nie je účasť na oficiálnom MOC kurze nutnou podmienkou pre zloženie skúšky. Oficiálne kurzy MOC spoločnosti Microsoft, aj naše vlastné kurzy GOC sú vhodnou súčasťou prípravy na certifikačné skúšky pre zloženie skúšky Microsoft ako sú MTA, MCP, MCSA, MCSE alebo MCM.

Primárnym cieľom kurzu nie je priamo príprava na certifikačné skúšky, ale zvládnutie teoretických princípov a osvojenie si praktických schopností nutných k efektívnej práci s daným produktom.

MOC kurzy obvykle pokrývajú takmer všetky oblasti, ktoré sú požadované pri zodpovedajúcich certifikačných skúškach. Rozsah ich preberania na kurzoch však nie je taký, ako si vyžaduje certifikačná skúška.

Ako ďalšiu prípravu k certifikačným skúškam je možné využiť napríklad knihy od MS Press (tzv. Self-paced Training Kit) aj elektronický self-test software.

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