Teória sietí a TCP/IP - sledovanie komunikácií s WireShark a NMAP

Kód kurzu: GOC246

Trojdňový kurz preberá pokročilé techniky riešenia problémov so sieťovými komunikáciami za použitia nielen nástroja WireShark a NMAP, ale aj Fiddler a ďalších nástrojov zabudovaných vo Windows oparačných systémoch a PowerShellu. Súčasťou je aj skenovanie siete pomocou protokolov ARP a IP aj určenie otvorených TCP a UDP portov sieťových služieb v prostredí LAN a VLAN.

Predpokladané vstupné znalosti

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

Dobrá znalosť technológií TCP/IP a DNS

Osnova kurzu

Prieskum testovacieho prostredia na platforme Hyper-V, virtuálne siete a alokácia MAC adries virtuálnym počítačom

Úvod do Windows Firewall

Architektúra nástroja WireShark a jeho inštalácia na Windows

Architektúra nástroja nmap a jeho inštalácia na Windows

Základy odpočúvania sieťovej komunikácie nástrojom WireShark

Filtrovanie paketov v programe WireShark

Princípy protokolu ARP pomocou WireShark a jeho využitia na riešenie problémov, prieskumu siete a vyhľadávania okolitých počítačov pomocou NMAP

Opakovanie princípov DHCP pomocou WireShark a jeho využitie na riešenie problémov, prieskumu siete a riešenie problémov s DHCP samotným, DHCP Relay aj pomocou NMAP

Skenovanie UDP služieb a ich UDP portov pomocou NMAP na príkladoch služieb ako je DNS, RADIUS a NTP

Pripomenutie funkcií ICMP ako Destination Port Unreachable a Echo (Ping)

Opakovanie fungovania TCP pomocou WireShark, trojcestný dohovor komunikácie a skenovanie portov pomocou NMAP a Test-NetConnection v PowerShellu

Riešenie problémov s duplicitnými IP adresami a firewal prestupmi všeobecne aj konkrétne za použitia Windows Defender Firewall

Riešenie problémov s DNS prekladom mien na LAN pomocou NSLOOK, Resolve-DnsName, NMAP a WireShark

Základy HTTP protokolu, HTTP proxy, základy HTTPS a TLS

Využitie nástroja Fiddler k základnému prieskumu HTTP a HTTPS komunikácií

Intranetové komunikácie vo Windows LAN sieťach ako je LDAP, Kerberos, SMB, RPC, DCOM a WMI, RDP, WinRM a Enter-PSSession a riešenie problémov s nimi

Detaily o začatí komunikácií TLS protokolov TLS 1.0, TLS 1.1, TLS 1.2 a TLS 1.3 a riešenie ich problémov s Wireshark

Príprava na certifikačné skúšky

Pri certifikačných skúškach Microsoft platí, že okrem certifikácií MCM, nie je účasť na oficiálnom MOC kurze nutnou podmienkou pre zloženie skúšky

Oficiálne kurzy MOC firmy Microsoft aj naše vlastné kurzy GOC sú vhodnou súčasťou prípravy na certifikačné skúšky firmy Microsoft, ako sú MTA, MCP, MCSA, MCSE, alebo MCM

Primárnym cieľom kurzu však nie je priamo príprava na certifikačné skúšky, ale zvládnutie teoretických princípov a

GOPAS Praha
Na Strži 2097/63
140 00 Praha 4 - Krč
Tel.: +420 226 201 390
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 530 513 590
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 902 903 132
info@gopas.sk

osvojenie si praktických zručností potrebných na efektívnu prácu s daným produktom

MOC kurzy obvykle pokrývajú takmer všetky oblasti, požadované pri zodpovedajúcich 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) aj elektronický self-test software

GOPAS Praha
Na Strži 2097/63
140 00 Praha 4 - Krč
Tel.: +420 226 201 390
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 530 513 590
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 902 903 132
info@gopas.sk