Troubleshooting network communications with Wireshark

Course code: GOC246

This three-day course covers advanced techniques for troubleshooting network communications using WireShark and NMAP, Fiddler, and other tools built into Windows operating systems and PowerShell. It also includes network scanning using ARP and IP protocols, as well as determining open TCP and UDP ports for network services in LAN and VLAN environments.

Assumed entry knowledge

Knowledge within the scope of the courses listed in the Previous courses and Related courses sections>

Good knowledge of TCP/IP and DNS technologies

Course outline

Research of the test environment on the Hyper-V platform, virtual networks and allocation of MAC addresses to virtual computers

Introduction to Windows Firewall

Architecture of WireShark and its installation on Windows

Architecture of nmap and its installation on Windows

Basics of wireshark network interception

Filtering packets in WireShark

Principles of ARP protocol using WireShark and its use for troubleshooting, network exploration and searching for nearby computers using NMAP

Review of DHCP principles using WireShark and its use for troubleshooting, network exploration and troubleshooting DHCP itself, DHCP Relay and using NMAP

Scanning UDP services and their UDP ports using NMAP on examples of services such as DNS, RADIUS and NTP

Reminding of ICMP functions such as Destination Port Unreachable and Echo (Ping)

Review of TCP operation using WireShark, three-way communication negotiation and port scanning using NMAP and Test-NetConnection in PowerShell

Solution problems with duplicate IP addresses and firewall penetrations in general and specifically using Windows Defender Firewall

Troubleshooting DNS name resolution on LAN using NSLOOK, Resolve-DnsName, NMAP and WireShark

Basics of HTTP protocol, HTTP proxy, basics of HTTPS and TLS

Using the Fiddler tool for basic exploration of HTTP and HTTPS communications

Intranet communications in Windows LAN networks such as LDAP, Kerberos, SMB, RPC, DCOM and WMI, RDP, WinRM and Enter-PSSession and troubleshooting them

Details of initiating TLS communications of TLS 1.0, TLS 1.1, TLS 1.2 and TLS 1.3 protocols and troubleshooting them with Wireshark

Preparation for certification exams

For Microsoft certification exams, except for MCM certifications, participation in the official MOC course is not required a condition for passing the exam

Official Microsoft MOC courses and our own GOC courses are a suitable part of preparing for Microsoft certification

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

exams, such as MTA, MCP, MCSA, MCSE, or MCM

However, the primary goal of the course is not directly preparing for certification exams, but mastering theoretical principles and acquiring practical skills necessary to work effectively with a given product

MOC courses usually cover almost all areas required for the corresponding certification exams. However, their discussion in the course is not always given exactly the same time and emphasis as the certification exam requires

As additional preparation for certification exams, you can use, for example, books from MS Press (so-called Self-paced Training Kit) and electronic 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