# skillsoft<sup>₽</sup> global knowledge<sub>™</sub>

# **Masterclass: Windows Security and Infrastructure Management**

Duration: 5 Days Course Code: WSI Delivery Method: Virtual Learning

#### **Overview:**

This is an international Live Virtual Class, which means you will share the learning experience in a group of IT pros from around the world! The class is taught in English by Cybersecurity Experts! Remember that this course is limited to 12 participants total to ensure the highest quality and unique learning experience.

During this course you will have an opportunity to interact with the instructor and get their help with any problems you might encounter, just as if it was a regular class. About the course The secure infrastructure configuration should be the most important line of defense in every organization. Unfortunately, people, the most valuable resource, are not always aware of the level of security in their companies, possible points of entry, how operating systems are attacked, and how to protect the infrastructure from successful attacks which are sometimes caused by configuration mistakes.

Understanding internal OS protection mechanisms and services/roles completely provides a huge impact on the whole infrastructure security level. Unfortunately, the problem is... rarely anyone has this impact! Advanced access rights, password mechanisms, windows internals, PowerShell usage for security purposes, gaining unauthorized access, advanced DNS configuration and common configuration mistakes, Active Directory security, IIS Security, debugging, advanced monitoring and troubleshooting and much more! Topics covered during this training will help you to walk in hackers' shoes and evaluate your infrastructure from their point of view.

#### Virtual Learning

This interactive training can be taken from any location, your office or home and is delivered by a trainer. This training does not have any delegates in the class with the instructor, since all delegates are virtually connected. Virtual delegates do not travel to this course, Global Knowledge will send you all the information needed before the start of the course and you can test the logins.

## **Target Audience:**

Enterprise administrators, infrastructure architects, security professionals, systems engineers, network administrators, IT professionals, security consultants and other people responsible for implementing network and perimeter security.

## **Testing and Certification**

What is wonderful about our certification is that it is lifetime valid with no renewal fees – the technology changes, but fundamentals and attitude remain mostly the same. Our Virtual Certificates, which entitle you to collect CPE Points, are issued via Accredible.

# Content:

Mediat 1: Windows Instants: System9: Non-invoce debugging9: Windows Saver 20193: Non-out-out-out-out-out-out-out-out-out-out	Contont		
a) International to the Windows 10 and Windows 2019 security concepts b) Architecture overview and terms     a) Setting up kerned debugging with a vitual machine as the target     c) Advanced BLC.ckr implementation scenarios       b) Architecture overview and terms     b) Debugging the boot process     c) Advanced BLC.ckr implementation techniques (provisioning, Standard User Rights and Network Unlock?       c) Key System Components I: Processes, Threads and Jobs I: Services, Functions and Routines II: Secsions in Objects and Handles;     c) Orach dump analysis     d) Advanced BCC.chr implementation Wizard Routines II: Secsions in Objects and Handles;       a) Advanced Local Procedure Call     a) Direct Kernel Object Manipulation     a) IPSec       a) Information gathering techniques I: Window Debugging II: Performance Monitor II: Window Debugging II: Performance Monitor II: Performance Monitoring and Performance Monitoring and Performance Monitor III: Pe		e) Kernel-mode debugging	
1 b) Architecture overview and terms2) Seming upkenel debugging with a vitual anchine as the target.2) Advanced BitLocker implementation christicaster (provision). Standard User standard User 	,	f) User-mode debugging	b) AppLocker implementation scenarios
() (by System Components I: Processes Process and Jobs II. Services, Functions and Routines III. Sessions iV. Objects and Handle v. Registry() Crash dump analysis() Advanced Security Configuration Wizard a) Proces () Direct Kernel Object Manipulation () Direct Kernel Object Manipulation () Processes () Processes () Processes () Processes () Processes () Processes () Processes () Processes () Processes () Process and Thread Management () Finding hidden processes () Rodule 5: Memory Analysis() Advanced GPO Management () Advanced GPO Management () Processes and Thread Management () Process priority management () Process priority management () Step-by-step memory analysis techniques () Process priority management () Step-by-step memory analysis techniques () Process priority management () Step-by-step memory analysis techniques () Process and thread nontioning and process ind thread monitoring and process indicate and techniques 			techniques (provisioning, Standard User
Routings III. Sessions IV. Objects and Handles       i) Crash dump analysis       e) Information gathering techniques i. Windows         a) Advanced Local Procedure Call       i) Direct Kernel Object Manipulation       e) IPSec         a) Information gathering techniques I. Windows       i) Rotkit Detection       a) Processes         b) Protecting Deformance Monitoriii. Windows       i) Rotkit Detection       a) Practicing Diagnostic and Recovery Toolkit         a) Process and Thread Management       Module 5: Memory Analysis       module 9: Layered Network Services         a) Process and thread internals       a) Memory acquisition techniques       module 9: Layered Network Services         b) Protected processes       b) Finding data and activities in memory       i) Fingerprinting techniques         c) Process priority management       c) Step-by-step memory analysis techniques       i) Enumeration techniques         d) Examining Thread Activity       a) Tools and techniques to perform memory roreacia       i) Networking Services Security (DNS, DFCP, SNMP, SMTP and other)         roubles Sciptorer, Process Monitor, and other processes       motioning Files and Folders by Using Sharder Cales       i) Network Load Balancing         a) Integrity Lavels       b) Protecting Sharder Files and Folders by Using Sharder Cales       i) Session Zero       i) Implementing Storage Spaces       i) Windows Dagnostic Infrastructure         d) Passwords security (techniques for getting       a	c) Key System Components i. Processes.	h) Debugging the boot process	Rights and Network Unlock?
() Direct Kernel Object Manipulation           () Advanced Local Procedure Call           () Advanced ADP Receiver Call         () Advanced ADP Receiver Call         () Advanced ADP Receiver Call             () Information gathering techniques i. Window 5           () Rotation 20 Diagnostic and Receiver Y could it              Andule 2: Process and Thread Management           Andule 5: Memory Analysis           hodule 9: Layered Network Services             A) Process and thread internals           a) Amony acquisition techniques               A) Process and thread internals           a) Amony acquisition techniques           a) Retwork services             A) Process and thread internals           b) Finding data and activities in memory           b) Finding data and activities in memory           b) Finding techniques             A) Process priority management           A) Call Process           b) Finding data and activities in memory           b) Finding data and activities in memory           b) Finding techniques             A) Process and thread nontoning and         tronspice (advanced usage         f) Call Process Explore (Process Keyling Memory         a) Scaring and monitoring Files and Folders by              Andule 3: System Se	Routines iii. Sessions iv. Objects and Handles	i) Crash dump analysis	d) Advanced Security Configuration Wizard
a) Information gethering techniques i. Windows Debugging ii. Performance Monitor ii. Windows Driver Kit iv. Other useful tools() Finding hidden processes(a) Practicing Diagnostic and Recovery Toolkit Driver Kit iv. Other useful toolsModule 2: Process and Thread ManagementModule 5: Memory Analysish) Toolsa) Process and thread internalsa) Memory acquisition techniquesModule 9: Layered Network Servicesb) Protected processesb) Finding data and activities in memoryb) Fingerprinting techniquesc) Process priority managementc) Step-by-step memory analysis techniquesc) Fungerprinting techniquesd) Examining Thread Activityc) Tools and techniques to perform memory forensicc) Enumeration techniquese) Process and thread monitoring and troubleshooting techniques (advanced usaged Process Explorer, Process Monitor, and other toolsModule 6: Storage Management a) Securing and monitoring Files and Folders by Using Shadow Copiesi) High Availability features: cluster improvements and SMB 7Scale – Out File Servera) Integrity Levelsc) Implementing Storage Spacesg) Network Load Balancingb) Session Zeroc) Implementing FSRM, managing Quotas File Screens, and Storage Reports (a) cauciting and troicing and techniques files activityg) Network Load Balancingc) Provideges, permissions and rightsc) Implementing FSRM, managing Quotas (p) Implementing FSRM, managing Quotas (p) Implementing Classification and Fileg) Windows Diagnostic Infrastructure	d) Advanced Local Procedure Call	j) Direct Kernel Object Manipulation	e) IPSec
Debuging ii. Performance Monitor iii. Windows Driver Kit iv. Other useful tools         i) Rootkit Detection         g) Practicing Diagnostic and Recovery Toolkit           Module 2: Process and Thread Management         Module 5: Memory Analysis         h) Tools           a) Process and thread internals         a) Memory acquisition techniques         Module 9: Layered Network Services           b) Protected processes         b) Finding data and activities in memory         a) Network sniffing techniques           c) Process priority management         c) Step-by-step memory analysis techniques         b) Fingerprinting techniques           d) Examining Thread Activity         d) Tools and techniques to perform memory forensic         c) Enumeration techniques           e) Process and thread monitoring and troubleshooting techniques (advanced usage of Process Explorer, Process Monitor, and other bols         Module 6: Storage Management         c) Enter Access           module 3: System Security Mechanisms         b) Protecting Shared Files and Folders by Using Shadow Copies         t) High Availability features: cluster improvements and SMB ?Scale – Out File Server?           a) Integrity Levels         c) Implementing ISCSI         Module 10: Monitoring and Event Tracing inplementing FSRM, managing Quotas, File Screams, and Storage Reports         g) Windows Diagnostic Infrastructure inplementing Classification and File           a) Prostecting passwords security (techniques for getting and cracking passwords)         i) Implementing ISSMI managing Quotas, File Screams, and Stora	e) Information gathering techniques i. Windows	k) Finding hidden processes	f) Advanced GPO Management
Module 2: Process and Thread Management       Module 5: Memory Analysis       Module 9: Layered Network Services         a) Process and thread internals       a) Memory acquisition techniques       Module 9: Layered Network Services         b) Protected processes       b) Finding data and activities in memory       a) Network sniffing techniques         c) Process priority management       c) Step-by-step memory analysis techniques       b) Finding techniques techniques         d) Examining Thread Activity       a) Tools and techniques to perform memory       c) Enumeration techniques         p) Process and thread innoitoring and process Explorer, Process Monitor, and other       Module 6: Storage Management       a) Network ing Services Security (DNS, DHCP, SNMP, SMTP and other)         module 3: System Security Mechanisms       a) Securing and monitoring Files and Folders by       p) Frotecting Sharder Files and Folders by       p) High Availability features: cluster improvements and SMB ?Scale – Out File Server)         a) Integrity Levels       c) Implementing Storage Spaces       g) Network Load Balancing       g) Network Load Balancing         b) Protecting Sharder Files and Folders by       p) Endernoit infigurage Spaces       g) Network Load Balancing       g) Network Load Balancing         b) Protecting Storage Spaces       g) Implementing Storage Reports       g) Nichows Diagnostic Infrastructure         c) Provideges, permissions and rights       g) Implementing Storage Reports       g) Nichows	Debugging ii. Performance Monitor iii. Windows		g) Practicing Diagnostic and Recovery Toolkit
a) Process and thread internalsa) Memory acquisition techniquesa) Network sniffing techniquesb) Protected processesb) Finding data and activities in memorya) Network sniffing techniquesc) Process priority managementc) Step-by-step memory analysis techniquesb) Fingerprinting techniquesd) Examining Thread Activityd) Tools and techniques to perform memory forensicc) Enumeration techniquese) Process and thread monitoring and troolsModule 6: Storage Management a) Securing and monitoring Files and Folders by Using Shadow Copiesc) Direct AccessModule 3: System Security Mechanisms b) Session Zeroc) Inplementing Storage Spacesc) Network Load Balancingc) Privileges, permissions and rightsc) Implementing FSRM, managing Quotas, File Screens, and Storage Reportsg) Windows Diagnostic Infrastructure File Screens, and Filesd) Passwords security (techniques for getting and cracking passwords)c) Implementing FSRM, managing Quotas, File Screens, and Filea) Windows Diagnostic Infrastructure b) Building auditing	Module 2: Process and Thread Management	Module 5: Memory Analysis	h) Tools
b) Protected processes b) Finding data and activities in memory b) Finderprinting techniques b) Finderprinting techniques c) Step-by-step memory analysis techniques c) Finderprinting techniques c) Funderation techniques for getting field Screens, and Storage Reports for getting for advitting funderation	a) Process and thread internals	a) Memory acquisition techniques	Module 9: Layered Network Services
c) Process priority managementc) Step-by-step memory analysis techniquesc) Fundamentiquesd) Examining Thread Activitya) Tools and techniques to perform memory forensicc) Enumeration techniquese) Process and thread monitoring and troubleshooting techniques (advanced usage of Process Explorer, Process Monitor, and other tools)Module 6: Storage Management a) Securing and monitoring Files and Foldersc) Direct AccessModule 3: System Security Mechanisms a) Integrity Levelsb) Protecting Shared Files and Folders by Using Shadow Copiesf) High Availability features: cluster improvements and SMB ?Scale – Out File Server)b) Session Zeroc) Implementing Storage Spaces 	b) Protected processes	b) Finding data and activities in memory	a) Network sniffing techniques
d) Examining Thread Activityd) Tools and techniques to perform memory forensicd) Networking Services Security (DNS, DHCP, SNMP, SMTP and other)e) Process and thread monitoring and troubleshooting techniques (advanced usage of Process Explorer, Process Monitor, and other)Module 6: Storage Management a) Securing and monitoring Files and Foldersd) Networking Services Security (DNS, DHCP, SNMP, SMTP and other)Module 3: System Security Mechanisms a) Integrity Levelsb) Protecting Shared Files and Folders by Using Shadow Copiesf) High Availability features: cluster improvements and SMB ?Scale – Out File Server)b) Session Zeroc) Implementing Storage Spacesg) Network Load Balancingc) Privileges, permissions and rightse) Implementing FSRM, managing Quotas, File Screens, and Storage Reportsa) Windows Diagnostic Infrastructure b) Building auditingd) Passwords security (techniques for getting and cracking passwords)f) Implementing Classification and Filea) Windows Diagnostic Infrastructure	c) Process priority management	c) Step-by-step memory analysis techniques	b) Fingerprinting techniques
Process and thread monitoring and trooles booting techniques (advanced usage of Process Explorer, Process Monitor, and other)Module 6: Storage Managementd) Networking Services Security (DNS, DHCP, SNMP, SMTP and other)Module 3: System Security Mechanisms a) Integrity Levelsa) Securing and monitoring Files and Folders by Using Shadow Copiesf) High Availability features: cluster improvements and SMB ?Scale – Out File Server)b) Session Zeroc) Implementing Storage Spacesg) Network Load Balancingc) Privileges, permissions and rightse) Implementing FSRM, managing Quotas, File Screens, and Storage Reportsa) Windows Diagnostic Infrastructure b) Building auditingd) Passwords security (techniques for getting and cracking passwords)e) Implementing Classification and Filea) Windows Diagnostic Infrastructure b) Building auditing	d) Examining Thread Activity		c) Enumeration techniques
Process Explorer, Process Monitor, and other tools)a) Securing and monitoring Files and Folderse) Direct AccessModule 3: System Security Mechanisms a) Integrity Levelsb) Protecting Shared Files and Folders by Using Shadow Copiesf) High Availability features: cluster improvements and SMB ?Scale – Out File Server)a) Integrity Levelsc) Implementing Storage Spacesg) Network Load Balancingb) Session Zerod) Implementing iSCSIModule 10: Monitoring and Event Tracingc) Privileges, permissions and rightse) Implementing FSRM, managing Quotas, File Screens, and Storage Reportsa) Windows Diagnostic Infrastructuref) Implementing Classification and Fileb) Building auditing			
Module 3: System Security Mechanismsb) Protecting Shared Files and Folders by Using Shadow Copiesf) High Availability features: cluster improvements and SMB ?Scale – Out File Server)a) Integrity Levelsc) Implementing Storage Spacesg) Network Load Balancingb) Session Zerod) Implementing iSCSIModule 10: Monitoring and Event Tracingc) Privileges, permissions and rightse) Implementing FSRM, managing Quotas, File Screens, and Storage Reportsa) Windows Diagnostic Infrastructuref) Implementing Classification and Fileb) Building auditing	Process Explorer, Process Monitor, and other	Module 6: Storage Management	e) Direct Access
b) Protecting Shared Files and Folders by Using Shadow Copiesimprovements and SMB ?Scale – Out File Server)a) Integrity Levelsc) Implementing Storage Spacesg) Network Load Balancingb) Session Zerod) Implementing iSCSIModule 10: Monitoring and Event Tracingc) Privileges, permissions and rightse) Implementing FSRM, managing Quotas, File Screens, and Storage Reportsa) Windows Diagnostic Infrastructured) Passwords security (techniques for getting and cracking passwords)f) Implementing Classification and Fileb) Building auditing		a) Securing and monitoring Files and Folders	
a) Integrity Levelsc) Implementing Storage Spacesg) Network Load Balancingb) Session Zeroc) Implementing iSCSIg) Network Load Balancingc) Privileges, permissions and rightsd) Implementing iSCSIModule 10: Monitoring and Event Tracingd) Passwords security (techniques for getting and cracking passwords)e) Implementing FSRM, managing Quotas, File Screens, and Storage Reportsa) Windows Diagnostic Infrastructure b) Building auditing	Module 3: System Security Mechanisms		improvements and SMB ?Scale - Out File
b) Session Zerod) Implementing iSCSIModule 10: Monitoring and Event Tracingc) Privileges, permissions and rightsd) Implementing iSCSIModule 10: Monitoring and Event Tracingd) Passwords security (techniques for getting and cracking passwords)e) Implementing FSRM, managing Quotas, File Screens, and Storage Reportsa) Windows Diagnostic Infrastructuref) Implementing Classification and Fileb) Building auditing	a) Integrity Levels		
c) Privileges, permissions and rights d) Passwords security (techniques for getting and cracking passwords) f) Implementing Classification and File a) Windows Diagnostic Infrastructure b) Building auditing	b) Session Zero	c) Implementing Storage Spaces	g) Network Load Balancing
d) Passwords security (techniques for getting and cracking passwords) File Screens, and Storage Reports b) Building auditing f) Implementing Classification and File	c) Privileges, permissions and rights	d) Implementing iSCSI	Module 10: Monitoring and Event Tracing
b) Building auditing f) Implementing Classification and File			a) Windows Diagnostic Infrastructure
			b) Building auditing

		c) Expression-based audit policies
f) Monitoring Registry Activity	g) Configuring and troubleshooting Distributed File System	d) Logging Activity for Accounts and processes
g) Driver signing (Windows Driver Foundation)	Module 7: Startup and Shutdown	
h) User Account Control Virtualization	a) Boot Process overview	<ul> <li>e) Auditing tools, techniques and improvements</li> </ul>
i) System Accounts and their functions	b) BIOS Boot Sector and Bootmgr vs. the	f) Auditing removable storage devices
j) Boot configuration	UEFI Boot Process	Module 11: Points of Entry Analysis
k) Services architecture	c) Booting from iSCSI	a) Offline access
I) Access tokens	d) Smss, Csrss, and Wininit	b) Kali Linux /other tools vs. Windows Security
m) Biometric framework for user authentication	e) Last Known Good configuration	
Module 4: Debugging ; Auditing	f) Safe Mode capabilities	c) Unpatched Windows and assigned attacks
a) Available debuggers	g) Windows Recovery Environment (WinRE)	d) Domain Controller attacks
	h) Troubleshooting Boot and Startup	e) Man-in-the Middle attacks
b) Working with symbols	Problems	f) Services security
c) Windows Global Flags	Module 8: Infrastructure Security Solutions	
d) Process debugging		

c) Expression based audit policies

# Additional Information:

#### Loads of Knowledge

The course is an intense workshop! During these 4 days we recommend a good cup of coffee – this course is really intense and in order not to miss a thing you MUST stay awake! Exercises All exercises are based on Windows Server 2016 and 2019, Windows 10 and Kali Linux. This course is based on practical knowledge from tons of successful projects, many years of real world experience and no mercy for misconfigurations or insecure solutions! Remember that the hybrid identity lab environment will stay online for an extra three weeks so you may practice even more after the training is completed!

## **Further Information:**

For More information, or to book your course, please call us on 00 971 4 446 4987

### training@globalknowledge.ae

www.globalknowledge.com/en-ae/

Global Knowledge, Dubai Knowledge Village, Block 2A, First Floor, Office F68, Dubai, UAE