Title	Windows Administration
Long Title	Windows Administration
Credits	5
NFQ Level	8
Module Author	George D O'Mahony

Module Description:

The Microsoft Windows Operating System, colloquially known as Windows, is a family of several proprietary graphical operating systems developed by Microsoft Corporation. Each family caters to a certain sector of the computing industry. For example, Windows is ubiquitous in the personal computer space and is often deployed on an enterprise scale as both a desktop and a server-side OS (Operating System). Understanding the inner workings of Windows is essential for anyone interested in defending or evaluating the security of computer systems and networks. As a result, there is a high demand for qualified Windows professionals. This module covers topics such as Windows Logging, file management and manipulation, advanced PowerShell use, Active Directory, performance evaluation, Windows Registry, Sysinternals, windows networking and more. At the end of the module the learner should have acquired the skills and knowledge to successfully configure, manage, troubleshoot, and administer a Windows system. This module was developed under the CyberSkills HCI (Human Capital Initiative) Pillar 3 Project. Please refer to consortium agreement for ownership.

Learning Outcomes

On successful completion of this module the learner will be able to:

LO1	Assess the underlying system architecture of Windows including, processes, threads, dynamic link libraries and APIs (Application Programming Interfaces).
LO2	Evaluate and apply utilities, including Sysinternals, to manage, diagnose, troubleshoot and monitor a Windows environment.
LO3	Securely configure and administer essential windows networking, monitoring, task scheduling, logging and system services.
LO4	Design sophisticated PowerShell scripting capabilities to perform complex system administrative tasks.
LO5	Deploy Active Directory and implement associated administration, security and authentication tasks.

Indicative Content

Windows System Architecture

The underlying system architecture of Windows. Processes and services, how to view them, and how to interact with them. Critical components of a process and their purpose. Core processes within a Windows system. Definition of a thread and how it relates to a process. Dynamic link libraries (DLLs) and their significance in the Windows environment. Windows APIs and how they provide native functionality to interact with key components of the Windows operating system.

System Monitoring and Sysinternals

Discretionary access control and Windows security principles (agent or entity): automated accounts, threads, processes, groups of users, etc. Security identifiers (SIDs). Windows User and Group Permissions (net command), User Account Control (UAC): runas command, NTFS (New Technology File System) Permissions (icacls). Dynamic Link Libraries. Windows Registry. Windows Registry Values. Windows Disk Utilities and Alternate Data Streams. Sysinternals Installation and setup: File and Disk Utilities, Networking Utilities, Process Utilities, Security Utilities, System Information, Windows Registry Utilities and Miscellaneous. Apply Sysinternals utilities to manage, troubleshoot and diagnose Windows systems and applications.

Networking, Performance, Scheduling, Logging and Services

Monitor performance in memory; CPU (Central Processing Unit) utilization, tuning, processor speed, fixing bottlenecks. Look at scheduled jobs and auto-start programs. Task Scheduler, schtasks, Task manager, Windows File Transfers, interacting with files, Device Performance & Health, environment variables, searching for files and text, retrieving system information. What are Windows Event logs and what data do they contain? What type of information regarding the wellbeing and efficiency of the system do they contain? Extracting diagnostic data and capabilities from log data. What is Windows event viewer and how to read log files using PowerShell cmdlets. Working with processes and services: List/start/stop/restart processes and services and associated permissions. Client-server protocols native to the Windows environment. Service Control Manager (SCM), Service Applications Enumeration and Remote operation. Networking utilities to gather information and/or interact with the network settings of a Windows device: ping, tracert, arp, netstat, socat, nbtstat, nslookup, ipconfig, route, and more. Active Connections and Neighbors, Network Interface Controllers (NICs), Network troubleshooting, check DNS (Domain Name System) settings and host files, routing, network shares, remote administration, Windows Defender.

PowerShell Scripting

What is PowerShell and how is it used? Determine system administration and automation tasks where scripting may be of assistance. Script design to automate repetitive tasks and assist troubleshooting. Script development to automate system tasks, Cmdlets, variables, arrays, regular expressions, I/O redirection, remoting, pipes, function complexities, aliases, operators, looping, conditions, hashtables, debugging and integrated scripting environment. Adding and removing users; handling permissions; getting help; files and folders operations; automating Active Directory tasks; setting password policies; system administration cmdlets; advanced cmdlets; WMIC; Managing processes, services, events and network connections.

Active Directory

Active Directory's concepts and services along with how organizations implement and use Active Directory to provide a scalable and centralized IT (Information Technology) management, authentication, and authorization framework. Active Directory top domain (forest) and sub-domains, Domain Controller (DC), Kerberos, managing access permissions centrally and dynamically, naming conventions, structure layout, service usage, Active Directory Users, Active Directory Groups, Group Policy objects and permissions.

Course Work

Assessment Type	*Assessment Description*	*Outcome Addressed*	*% of Total*	*Assessment Date*
Project	In this project, the student will access and evaluate an enterprise network to determine where scripting may be of assistance in monitoring, logging, and troubleshooting and design a number of PowerShell scripts that utilize Sysinternals.	1, 2, 3, 4	50	Week 6
Project	In this project, the student will deploy a network topology and deploy Active Directory and all required networking and services according to an assigned enterprise profile.	1, 3, 5	50	Sem End

Assessment Breakdown	%
Coursework	100

Re-Assessment Requirement

Coursework Only

This module is reassessed solely on the basis of re-submitted coursework. There is no repeat written examination.

Workload – Full Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Leaner Workload*
Lecture	Lecture underpinning the learning outcomes.	2.00	Every Week	2.00
Lab	Lab to support content delivered.	2.00	Every Week	2.00
Independent & Directed Learning (Non-contact)	Independent learning by the student.	3.00	Every Week	3.00
		Total Hours		7.00
		Total Weekly Learner Workload		7.00
		Total Weekly Contact Hours		4.00

Workload – Part Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Leaner Workload*
Lecture	Lecture underpinning the learning outcomes.	2.00	Every Week	2.00
Lab	Lab to support content delivered.	2.00	Every Week	2.00
Independent & Directed Learning (Non-contact)	Independent learning by the student.	3.00	Every Week	3.00
		Total Hours		7.00
		Total Weekly Learner Workload		7.00
		Total Weekly Contact Hours		4.00

Recommended Book Resources

Yosifovich, Pavel and Ionescu, Alex, Russinovich, Mark E, Solomon, David A, Ionescu, Alex. (2017), Windows internals. Part 1 : system architecture, processes, threads, memory management, and more, 7th Ed. Washington: Microsoft Press, [ISBN: 9780735684188].

Supplementary Book Resources

Remzi H Arpaci-Dusseau, Andrea C Arpaci-Dusseau. (2018), Operating Systems: Three Easy Pieces, 1st Ed. CreateSpace Independent Publishing Platform, [ISBN: 978198508659].

St., Cyr, Ken, and Laura E. Hunter. (2011), Automating Active Directory Administration with Windows PowerShell 2. 0, John Wiley & Sons, Incorporated, [ISBN: 9781118027318].

Anton Chuvakin, Kevin Schmidt, and Chris Phillips. (2012), Logging and Log Management : The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management, [ISBN: 9781597496360].

Dauti, Bekiam. (2022), Windows Server 2022 Administration Fundamentals: A beginner's guide to managing and administering Windows Server environments, Packt Publishing, [ISBN: 978-180323215].

Berkouwer, Sander. (2022), Active Directory Administration Cookbook, 2nd Ed. Packt Publishing, [ISBN: 9781803242507].

Other Resources

Website, Windows Technical Documentation for Developers and IT Pros,

https://learn.microsoft.com/en-us/window s/

Website, Sysinternals,

https://learn.microsoft.com/en-us/sysint ernals/

Website, Event Logging,

https://learn.microsoft.com/en-us/window s/win32/eventlog/event-logging

Website, Cmdlet Overview,

https://learn.microsoft.com/en-us/powers hell/scripting/developer/cmdlet/cmdlet-o verview?view=powershell-7.3&viewFall backFrom=powershell-7.1

Website, Active Directory Domain Services Overview,

https://learn.microsoft.com/en-us/window s-server/identity/ad-ds/get-started/virt ual-dc/active-directory-domain-services- overview

Website, Microsoft Kerberos,

https://learn.microsoft.com/en-us/window s/win32/secauthn/microsoft-kerberos

Website, Selecting the Forest Root Domain,

https://learn.microsoft.com/en-us/window s-server/identity/ad-ds/plan/selecting-t he-forest-root-domain