CyberOps Modul 3: The Windows Operating System

3.1 Windows History

- DOS (Disk Operating System), MS-DOS
- NT (New Technologies)
- cmd-commands: `dir, cd, copy, del, find, mkdir, ren, help`
- Windows Versions: 7, Server 2008 R2, 8, Server 2012, 8.1, Server 2012 R2, 10, Server 2016
- Windows GUI: Desktop, Task Bar
- Operating System Vulnerabilities: Virus, malware, Windows Defender, unknown services, encryption, security policy, firewall, weak password, login as administrator

3.2 Windows Architecture and Operations

- Hardware Abstraction Layer (HAL), Kernel
- User Mode (driver crash → system crash), Kernel Mode (own restricted address space)
- Windows File Systems: exFAT, HFS+ (Mac OSX), ext (Linux), NTFS (Partition boot sector, Master file table, system files, file area)
- Alternate Data Streams: filename.txt:ADS
- Windows boot process: BIOS / UEFI → Bootmgr.exr → BCD → Winload.exe (Ntoskrnl.exe) / Winresume.exe (Hiberfil.sys)
- Windows Startup: Msconfig.exe
- Windows Shutdown: shutdown (ctrl+alt+del), restart, hibernate
- Processes, Threads, and Services: Task Manager
- Memory Allocation and Handles: RAMMap (sysinternals)
- The Windows Registry: HKCU, HKU, HKCR, HKLM, HKCC, regedit.exe (REG_BINARY, REG_DWORD, REG_SZ)
- Lab: sysinternals (procexp.exe), regedit.exe

3.3 Windows Configuration and Monitoring

- Run as Administrator
- Local Users and Domains (lusrmgr.msc)
- CLI (cmd.exe) and PowerShell
- WMI (Windows Management Instrumentation)
- The net Command: net accounts, net session, net share, net start, net stop, net use, net view
- Task Manager and Resource Monitor
- Networking: Network and Sharing Center, nslookup, netstat
- Accessing Network Resources: $\backslash\backslash servername\backslash sharename\backslash file$, RDP (Remote Desktop Connection)
- Windows Server: DNS, DHCP, SMB, NFS, DFS, FTP, HTTP, HTTPS, Group Policy, Active Directory

- Lab: Create User accounts
- Lab: Using Windows PowerShell
- Lab: Windows Task Manager
- Lab: Monitor and Manage System Resources in Windows

3.4 Windows Security

- The netstat Command
- Event Viewer
- Windows Update Management
- Local Security Policy
- Windows Defender
- Windows Defender Firewall