1. **SEC505.1: Learn PowerShell Scripting Why Is PowerShell So Important and Dangerous?**
    - The backbone of Windows and Azure automation
    - Graphical admin tools wrapped around PowerShell
    - Built-in remote script execution
    - Piping .NET and COM objects, not text
    - Using properties and methods of objects
    - PowerShell is like simplified C# Writing Your Own Scripts, Functions, and Modules
    - Writing your own functions
    - Passing arguments into your scripts
    - Function parameters and returning output
    - Flow control: if-then, do-while, foreach, switch
    - The .NET Framework class library: A vast playground
    - How to pipe data in/out of your scripts
    - How to create a PSM1 module script PowerShell Remoting
    - Remote command shells running PowerShell
    - Using TLS, SSH or IPsec to encrypt traffic
    - Remote command execution in scheduled tasks
    - File upload and download over the remoting port
    - Graphical apps can use PowerShell remoting too Getting Up and Running Quickly with PowerShell
    - Capturing the output of commands
    - Parsing text files and logs with regex patterns
    - Mounting the registry as a drive
    - Exporting data to CSV, HTML, and JSON files
    - Running scripts as scheduled jobs
    - Pushing out scripts through Group Policy
    - Importing modules and dot-sourcing functions

SEC5SEC505.2: Host Hardening and Active Directory Scripting

Continuous Secure Configuration Enforcement

- How to use Group Policy and PowerShell together
- Automating with INF security templates
- How to customize INF templates
- Microsoft Security Baselines and DoD STIGs
- SECEDIT.EXE scripting
- Building an in-house security repository for SecOps/DevOps
- NSA's Secure Host Baseline GPOs Remote PowerShell Script Execution with Group Policy
- Managing Group Policy Objects (GPOs) with PowerShell
- LSDOU, Block Inheritance, Enforced GPOs

- Group Policy permissions for targeting changes
- ADMX templates for mass registry editing
- Deploying PowerShell startup and logon scripts
- WMI item-level targeting of GPO preferences
- GPO scheduled tasks to run PowerShell scripts
- Remote command execution via GPO (not remoting)
- Empowering the Hunt Team to fight back! Server Hardening Automation
- Server Manager scripting with PowerShell
- Adding and removing roles and features
- Remotely gather an inventory of roles and features
- Why Server Nano or Server Core?
- Apply GPOs to stand-alones on-premises or in the cloud
- Running PowerShell automatically after service failure
- Service account identities, passwords, and risks
- Tools to reset service account passwords securely
- Desired State Configuration (DSC) PowerShell for Active Directory
- Query and manage Active Directory with PowerShell
- Create user accounts, reset passwords, manage groups
- Search organizational units using filter criteria
- The ADSI Edit Tool
- Active Directory Administrative Center (ADAC)

SEC505.3: Smart Tokens and Public Key Infrastructure (PKI)

Why Is a PKI Necessary?

- PKI is for strong authentication and encryption
- Passwords are obsolete, we need smart cards and YubiKeys
- Examples: VPNs, wireless, IPsec, SSL, S/MIME, etc.
- Certificates for mobile endpoints and BYOD
- Code signing certificates for AppLocker and PowerShell How to Install the Windows PKI
- PowerShell installation script for PKI
- PKI installation with Server Manager
- Root versus subordinate CAs
- Enterprise versus Stand-Alone CAs
- Should you be your own root CA?
- Custom certificate templates in Active Directory
- Controlling certificate auto-enrollment
- Setting up an Online Certificate Status Protocol (OCSP) responder web farm
- Configuring Certificate Revocation List (CRL) publication How to Manage Your PKI
- Where are private keys?
- Private key security best practices
- PowerShell script to audit trusted root CAs

- PowerShell script to delete hacker certificates
- Group Policy auto-deployment of certificates
- How to revoke compromised certificates
- Automatic private key backup and recovery
- Credential roaming of keys and passwords
- Delegation of PKI management to non-admins Deploying MFA Smart Tokens, Smart Cards, andTPMs
- Everything you need is built in!
- Smart tokens for Kerberos, BitLocker, EFS, etc.
- TPM virtual smart cards for multi-factor authentication (MFA)
- Smart tokens on a limited budget for the admins
- Safely enroll tokens and cards on behalf of other users
- Not just cards, but TPMs and USB YubiKeys too

SEC505.4: Protecting Admin Credentials and PowerShell JEA Restricting Unnecessary Admin Privileges

- What are the various "admin privileges" on Windows?
- How do we manage privileges on thousands of hosts?
- What privileges can be exploited to take over a machine?
- How to steal a password hash or Security Access Token (SAT)Compromise of Administrative Powers
- Limiting pass-the-hash/ticket and token abuse attacks
- Windows 10 Credential Guard
- Server 2019 Remote Credential Guard (RDP)
- Don't use Microsoft LAPS!
- Getting users out of the Administrators group (without a revolt)
- Limiting the power of administrative users
- Limiting privileges, logon rights, and permissions
- User Account Control (UAC) instead of RUNAS.EXE
- Enforcing different per-group password and lockout policies
- Using PowerShell to manage password resets
- Picture password and PIN logons on Windows 10
- Windows 10 biometric logons
- Password managers for administrators
- KeePass best practices and PowerShell script
- Windows 10 Credential Guard
- Server 2016 Remote Credential Guard PowerShell Just Enough Admin (JEA)
- JEA is Windows sudo, like on Linux
- JEA is Windows setuid root, like on Linux
- Restricting commands and arguments
- Verbose transcription logging
- How to set up and configure JEA
- Privileged Access Workstations (PAWs) Active Directory Permissions and Delegation

- Active Directory objects have permissions
- Active Directory objects have auditing
- Empty the Domain Admins group!
- Delegating authority at the OU level instead
- Granting limited powers to the Help Desk
- Designing Active Directory for the inevitable breach
- AD ACL Scanner and BloodHound

SEC505.5: Thwarting Hackers Inside The Network Anti-Exploitation and PowerShell

- Application whitelisting with AppLocker
- Scripting AppLocker with PowerShell
- PowerShell constrained language mode
- The Principle of (Endpoint) Least Privilege TCP/UDP Port Permissions for Role-Based Access Control
- IPsec for everything besides VPNs
- We don't discuss VPNs at all today!
- IPsec for blocking lateral post-exploitation
- Limiting access to ports based on global group membership
- IPsec-based encrypted VLANs
- Group Policy management of IPsec rules
- PowerShell and NETSH.EXE control of IPsec Windows Defender Firewall
- PowerShell scripting of Windows Firewall rules
- Group Policy management of Windows Firewall
- Blocking malware outbound connections
- Role-based access control at the network level
- What does "deep IPsec integration" mean?
- Using the firewall logs for network forensics PowerShell for Firewall and IPsec Rules
- PowerShell software-defined networking
- Scripting of Windows Firewall rules
- Scripting of IPsec port control rules
- Scheduled scripts to enforce desired rules
- Group Policy for networking scripts

SEC505.6: Blue Team PowerShell: WMI, DNS, RDP and SMB PowerShell and WMI

- Windows Admin Center (WAC) web browser interface
- Windows Management Instrumentation (WMI) service
- What is WMI and why do hackers abuse it so much?
- Using PowerShell to query WMI CIM classes
- WMI authentication and traffic encryption
- Inventory operating system versions and installed software

- WMI remote command execution versus PowerShell remoting
- WMI security best practices
- PowerShell security best practices
- PowerShell transcription logging to catch hackers Hardening DNS
- Why is DNS so easy to attack?
- Don't believe the haters, DNSSEC is fun!
- How to deploy DNSSEC step-by-step
- Kerberos for DNS secure dynamic updates
- DNS sinkholes for malware and threat detection
- Sinkholing unwanted DNS names with PowerShell
- DNS Distributed DoS attacks
- PowerShell management of all networking settings Dangerous Protocols We Can't Live Without
- Hackers want you to use RDP
- Remote Desktop Pwnage (RDP)
- SSL is dead, long live TLS
- TLS cipher suite optimization
- SMBv3 native encryption vs. Wireshark
- NTLM, NTLMv2, and Kerberos
- Kerberos Golden Tickets (Silver too)
- Kerberos double-encryption armoring
- What about IPv6 tunneling?