In this course you will learn how to:

- Write PowerShell scripts for Windows and Active Directory security automation
- Safely run PowerShell scripts on thousands of hosts over the network
- Defend against PowerShell malware such as ransomware
- Harden Windows Server and Windows 10 against skilled attackers

In particular, we will use PowerShell to secure Windows against many of the attacks described in the MITRE ATT&CK matrix, especially stolen administrative credentials, ransomware, hacker lateral movement inside the LAN, and insecure Windows protocols, like RDP and SMB.

You will leave this course ready to start writing your own PowerShell scripts to help secure your Windows environment. It’s easy to find Windows security checklists, but how do you automate those changes across thousands of machines? How do you safely run scripts on many remote boxes? In this course you will learn not just Windows and Active Directory security, but how to manage security using PowerShell.

DON’T JUST LEARN POWERSHELL SYNTAX, LEARN HOW TO LEVERAGE POWERSHELL AS A FORCE MULTIPLIER FOR WINDOWS SECURITY

There is another reason why PowerShell has become popular: PowerShell is just plain fun! You will be surprised at how much you can accomplish with PowerShell in a short period of time – it’s much more than just a scripting language, and you don’t have to be a coding guru to get going.

Learning PowerShell is also useful for another kind of security: job security. Employers are looking for IT people with PowerShell skills. You don’t have to know any PowerShell to attend this course, we will learn it together during the labs.

You can learn basic PowerShell syntax on YouTube for free, but this course goes far beyond syntax. In this course we will learn how to use PowerShell as a platform for managing security, as a “force multiplier” for the Blue Team, and as a rocket booster for your Windows IT career.

WE WILL WRITE A POWERSHELL RANSOMWARE SCRIPT AND DEFEND AGAINST IT

Unfortunately, PowerShell is being abused by hackers and malware authors, so in the last section of the course, we will write our own ransomware script to see how to defend against scripts like it.

This is a fun course and a real eye-opener, even for Windows administrators with years of experience. Come have fun learning PowerShell and Windows security at the same time.

The course author, Jason Fossen, is a SANS Institute Fellow and has been writing and teaching for SANS since 1998. In fact, SEC505 has had at least one day of PowerShell for more than 10 years, and now PowerShell is the centerpiece of the course.
### Section Descriptions

#### SECTION 1: Learn PowerShell Scripting for Security
This course section covers what you need to know to get started using PowerShell. You do not need to have any prior scripting or programming experience. We have PowerShell labs throughout the course, so this section is not the only PowerShell material. We start with the essentials, then go more in depth as the course progresses. Do not worry, you will not be left behind, the PowerShell labs walk you through every step. If you already have PowerShell experience, then there will be intermediate topics for you too.

**TOPICS:** PowerShell IS Dangerous (and Fun); Writing Your Own Scripts, Functions, and Modules; Up and Running Quickly with PowerShell; Piping Objects Instead of Text

---

#### SECTION 2: You Don’t Know the POWER!
How can we run PowerShell scripts on thousands of systems with just a few lines of code? This section is about remote command execution using PowerShell Remoting, the SSH service on Windows, the Task Scheduler service, and boot up scripts assigned through Group Policy.

**TOPICS:** PowerShell Remoting; OpenSSH on Windows; PowerShell Just Enough Admin (JEA); PowerShell, Group Policy, and the Task Scheduler

---

#### SECTION 3: WMI and Active Directory Scripting
PowerShell is deeply integrated into the Windows Management Instrumentation (WMI) service. Many PowerShell commands are just wrappers for WMI functions. Hackers love the WMI service too, but for the wrong reasons. The WMI service is enabled by default and accessible over the network. With our PowerShell WMI scripts we can remotely execute commands, reboot machines, forcibly log users off, kill processes, and much more. Today, we will see how to do all this. WMI scripting is a bit difficult, but we'll go through all the strange namespaces and classes together. In this section we will also use PowerShell to search, manage, and secure Active Directory. With PowerShell we can find abandoned user accounts and disable them. We can enforce our desired group memberships with scheduled scripts. We can reset passwords on thousands of user accounts. And when hackers are brute-forcing passwords, our PowerShell scripts can find the accounts being targeted. Of course, malicious insiders can do much of the same, such as with the Bloodhound tool, so we’ll examine how we can restrict what users can see or change.

**TOPICS:** PowerShell for WMI; PowerShell for Active Directory; Active Directory Permissions and Auditing

---

#### SECTION 4: Hardening Network Services with PowerShell
In this course section, we will use PowerShell and Group Policy to automate the hardening of many exploitable services and protocols, such as Kerberos, Domain Name System (DNS), Remote Desktop Protocol (RDP), and File and Printer Sharing (SMB). Think of Kerberos Golden Tickets, DNS response spoofing, the BlueKeep RDP attack, the EternalBlue/WannaCry SMB worm, and other attacks.

**TOPICS:** Server Hardening Automation for DevOps; Windows Firewall Scripting; Share Permissions for TCP/UDP Listening Ports with IPsec; Exploitable Protocols and Services

---

#### SECTION 5: Certificates and Multifactor Authentication
Smart cards and smart tokens, such as YubiKeys, are the gold standard for multi-factor authentication (MFA). In this course section, we will use PowerShell to install a certificate server that can be used to deploy smart cards and smart USB tokens. Smart cards and tokens can be used for PowerShell Remoting, signing PowerShell scripts, Remote Desktop Protocol (RDP) logons, User Account Control (UAC), ASP.NET web application logons, and more.

**TOPICS:** Certificate Authentication and TLS Encryption for PowerShell; Installing a Windows Certificate Server with PowerShell; Deploying Smart Cards, Smart Tokens, and TPM Virtual Smart Cards; Security Best Practices

---

#### SECTION 6: PowerShell Security, Ransomware, and DevOps
In this course section, we will write a PowerShell ransomware script and unleash it inside our training VM (don’t release it into the wild, you’ll go to federal prison). The purpose of this ethical hacking is to discuss defenses against this kind of PowerShell abuse. How can we secure PowerShell itself? PowerShell is not a single tool. There is no one registry value or patch to magically make PowerShell "secure," but there is a lot we can do. In this section we will cover many defensive techniques to prevent future compromises, reduce the harm we suffer after a compromise, and gain visibility into PowerShell malicious activity for the sake of forensics, incident response, and threat hunting.

**TOPICS:** PowerShell Ransomware; Anti-Exploitation Defenses for PowerShell; PowerShell Visibility and Detection; Capstone: DevOps Automation with PowerShell

---

### Who Should Attend
- Anyone who wants to learn PowerShell automation
- “Ops” personnel in SecOps/DevOps
- Blue Team players who were terrified by SECS04
- Windows endpoint and server administrators
- Anyone implementing the CIS Critical Security Controls
- Anyone implementing the MITRE ATT&CK mitigations

“`This class provided real-world examples and sample scripts to make a Windows-centric environment fundamentally more secure.``”

— Nick Boardman, HRSD

---

**GIAC Certified Windows Security Administrator**

The GIAC Certified Windows System Administrator (GCWN) certification validates a practitioner’s ability to secure Microsoft Windows clients and servers. GCWN certification holders have the knowledge and skills needed to configure and manage the security of Microsoft operating systems and applications, including: PKI, IPsec, Group Policy, AppLocker, DNSSEC, PowerShell, and hardening Windows against malware and persistent adversaries.

- Defensible networking
- Endpoint protection
- Operating system and application hardening
- PKI management
- Restricting administrative compromise
- Securing PowerShell

---

**GIAC Certified Windows Security Administrator**

The GIAC Certified Windows System Administrator (GCWN) certification validates a practitioner’s ability to secure Microsoft Windows clients and servers. GCWN certification holders have the knowledge and skills needed to configure and manage the security of Microsoft operating systems and applications, including: PKI, IPsec, Group Policy, AppLocker, DNSSEC, PowerShell, and hardening Windows against malware and persistent adversaries.

- Defensible networking
- Endpoint protection
- Operating system and application hardening
- PKI management
- Restricting administrative compromise
- Securing PowerShell

---

**GIAC Certified Windows Security Administrator**

The GIAC Certified Windows System Administrator (GCWN) certification validates a practitioner’s ability to secure Microsoft Windows clients and servers. GCWN certification holders have the knowledge and skills needed to configure and manage the security of Microsoft operating systems and applications, including: PKI, IPsec, Group Policy, AppLocker, DNSSEC, PowerShell, and hardening Windows against malware and persistent adversaries.

- Defensible networking
- Endpoint protection
- Operating system and application hardening
- PKI management
- Restricting administrative compromise
- Securing PowerShell