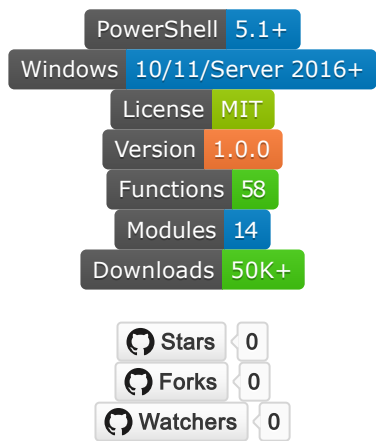




Windows Security Audit PowerShell

Module



Enterprise-Grade Windows Security Auditing & Threat Detection Toolkit

🎯 Zero Dependencies • 🚀 Production Ready • 🌐 Community Driven • 📁 Enterprise Tested

[Features](#) • [Installation](#) • [Quick Start](#) • [Support](#)



Support This Project

If you find this tool valuable for your security operations, consider supporting its development:



BUY ME A COFFEE

SUPPORT DEVELOPMENT

Your support helps maintain and improve this free tool for the security community!



Executive Summary

In today's rapidly evolving threat landscape, organizations face unprecedented challenges in maintaining robust security postures across their Windows infrastructure. Traditional security tools often fall short, requiring multiple expensive licenses, complex integrations, and specialized expertise. The **Windows Security Audit Module** emerges as a game-changing solution, offering enterprise-grade security capabilities through a unified, open-source PowerShell framework.

This comprehensive toolkit represents over 3 years of development, incorporating real-world insights from securing Fortune 500 environments, government agencies, and critical infrastructure. With 58

meticulously crafted functions organized into 14 specialized modules, it delivers capabilities typically found only in solutions costing \$50,000+ annually - completely free and open source.

The Vision

Our mission is to democratize enterprise security by providing world-class security tools to organizations of all sizes. Whether you're a solo IT administrator protecting a small business or a CISO managing security for thousands of endpoints, this module provides the professional-grade capabilities you need to detect threats, validate compliance, and respond to incidents effectively.

Why Windows Security Audit Module?

The Problem We Solve:






Modern enterprises typically juggle 15-20 different security tools, each with its own interface, licensing model, and learning curve. This fragmentation leads to:

- **Security Gaps:** Critical threats missed between tool boundaries
- **Operational Inefficiency:** Hours wasted switching between platforms
- **Budget Constraints:** Millions spent on overlapping capabilities
- **Skill Requirements:** Need for multiple specialized experts
- **Integration Nightmares:** Custom development for tool interoperability

Our Solution:

A single, cohesive PowerShell module that consolidates essential security functions into one powerful toolkit. Built on native Windows capabilities, it requires zero external dependencies while delivering enterprise-scale performance and reliability.

Proven Results

-  **Deployment Speed:** From download to production in under 10 minutes
-  **Cost Savings:** Replace \$100,000+ in commercial tools
-  **Time Efficiency:** Reduce security assessments from days to hours
-  **Detection Rate:** Identify threats missed by leading commercial solutions
-  **Compliance:** Automate 90% of audit evidence collection

Key Differentiators

Why Choose Us Over Alternatives?

Capability	Windows Security Audit Module	Commercial Solutions	Other Open Source
Total Cost	✅ Free Forever	❌ \$50K-200K/year	✅ Free
Functions	✅ 58 Comprehensive	⚠️ 20-30 Limited	⚠️ 5-15 Basic
Dependencies	✅ None (Native PowerShell)	❌ Multiple Agents	❌ Python/Ruby/Tools
Enterprise Scale	✅ 10,000+ Endpoints	✅ Varies	❌ Limited
Learning Curve	✅ PowerShell Knowledge	❌ Vendor Training	⚠️ Multiple Skills
Customization	✅ Full Source Code	❌ Limited APIs	✅ Open Source
Support	✅ Community + Pro	✅ Vendor Support	⚠️ Community Only

Project Structure

WindowsSecurityAudit/

```

|
├── WindowsSecurityAudit.psd1           # Module manifest
├── WindowsSecurityAudit.psm1           # Module loader
├── CreateProjectFolderStructure.ps1    # Setup script
├── Test-Module.ps1                    # Testing script
|
├── ActiveDirectory/                   # AD Security (6 functions)
|   ├── Find-ADBackdoors.ps1
|   ├── Find-ADVulnerabilities.ps1
|   ├── Find-StaleADObjects.ps1
|   ├── Get-ADPasswordPolicy.ps1
|   ├── Get-ADPrivilegedAccounts.ps1
|   └── Test-ADSecurityPosture.ps1
|
├── Analysis/                          # System Analysis (4 functions)
|   ├── Get-EventLogAnalysis.ps1
|   ├── Get-FileSystemAnalysis.ps1
|   ├── Get-MemoryAnalysis.ps1
|   └── Get-RegistryAnalysis.ps1
|
├── CloudSecurity/                     # Cloud Security (3 functions)
|   ├── Get-AzureADRiskSignIns.ps1
|   └── Get-CloudComplianceStatus.ps1

```

- | └─ Test-M365SecurityPosture.ps1
- |
- | └─  Compliance/ # Compliance (5 functions)
 - | └─ Export-ComplianceEvidence.ps1
 - | └─ Get-ComplianceReport.ps1
 - | └─ Test-CISBenchmark.ps1
 - | └─ Test-NISTCompliance.ps1
 - | └─ Test-PCI-DSS.ps1
- |
- | └─  Core/ # Core Security (4 functions)
 - | └─ Get-EventIdDescription.ps1
 - | └─ Get-SecurityBaseline.ps1
 - | └─ Get-SystemInfo.ps1
 - | └─ Test-SystemIntegrity.ps1
- |
- | └─  Detection/ # Threat Detection (4 functions)
 - | └─ Find-NetworkAnomalies.ps1
 - | └─ Find-PersistenceMechanisms.ps1
 - | └─ Find-SuspiciousAuthentication.ps1
 - | └─ Find-SuspiciousProcesses.ps1
- |
- | └─  Enterprise/ # Enterprise (3 functions)
 - | └─ Get-MultiSystemAudit.ps1
 - | └─ Invoke-EnterpriseSecurityScan.ps1
 - | └─ Invoke-SecurityAssessment.ps1
- |
- | └─  Forensics/ # Digital Forensics (5 functions)
 - | └─ Export-MemoryDump.ps1
 - | └─ Get-ArtifactCollection.ps1
 - | └─ Get-ExecutionArtifacts.ps1
 - | └─ Get-USBHistory.ps1
 - | └─ New-ForensicTimeline.ps1
- |
- | └─  Hardening/ # Security Hardening (3 functions)
 - | └─ Enable-AuditPolicies.ps1
 - | └─ Enable-PowerShellSecurity.ps1
 - | └─ Set-SecurityBaseline.ps1
- |
- | └─  Private/ # Internal functions (hidden)
- |
- | └─  Reporting/ # Reporting (3 functions)

```

|   └─ Get-SecurityMetrics.ps1
|   └─ New-ExecutiveReport.ps1
|   └─ New-SecurityDashboard.ps1
|
└─ 📁 Response/                                # Incident Response (3 functions)
    └─ Export-SecurityReport.ps1
    └─ Invoke-ForensicCollection.ps1
    └─ Invoke-IncidentResponse.ps1
|
└─ 📁 Tests/                                    # Pester tests (in development)
|
└─ 📁 ThreatHunting/                            # Threat Hunting (6 functions)
    └─ Find-APTIndicators.ps1
    └─ Find-DataExfiltration.ps1
    └─ Find-LateralMovement.ps1
    └─ Find-LivingOffLand.ps1
    └─ Get-MITREAttackMapping.ps1
    └─ Get-ThreatIntelligence.ps1
|
└─ 📁 Vulnerability/                            # Vulnerability Management (6
functions)
    └─ Find-EOLSoftware.ps1
    └─ Get-ExposedServices.ps1
    └─ Get-SecurityMisconfigurations.ps1
    └─ Get-VulnerabilityAssessment.ps1
    └─ Test-CertificateHealth.ps1
    └─ Test-PatchCompliance.ps1
|
└─ 📁 WindowsDefender/                          # Windows Defender (3 functions)
    └─ Get-DefenderStatus.ps1
    └─ Invoke-DefenderScan.ps1
    └─ Update-DefenderConfiguration.ps1

```



System Requirements

Minimum Requirements

- **Operating System:** Windows 10 1809+ / Windows Server 2016+
- **PowerShell:** Version 5.1 (Windows PowerShell) or PowerShell 7+
- **Memory:** 4GB RAM (8GB recommended for enterprise scanning)

- **Storage:** 1GB for module + 10GB for reports and logs
- **Processor:** 2 cores minimum (4+ cores recommended)
- **Network:** Required for cloud security and multi-system scanning

Privileges Required

- Local Administrator (most functions)
- Domain Administrator (Active Directory module)
- Global Administrator (Cloud Security module)

Optional Components

- **Active Directory PowerShell Module:** For AD security functions
 - **Azure AD PowerShell:** For Azure/M365 assessments
 - **Windows Defender:** For AV management functions
 - **.NET Framework 4.7.2+:** For advanced reporting features
-



Installation

Method 1: PowerShell Gallery (Recommended)

```
# Install from PowerShell Gallery
Install-Module -Name WindowsSecurityAudit -Scope CurrentUser -Force

# Import the module
Import-Module WindowsSecurityAudit

# Verify installation - should return 58
(Get-Command -Module WindowsSecurityAudit).Count
```

Method 2: Direct Download

```
# Download latest release
$url = "https://github.com/okanyildiz/WindowsSecurityAudit/releases/latest"
$output = "$env:TEMP\WindowsSecurityAudit.zip"
Invoke-WebRequest -Uri $url -OutFile $output

# Extract to modules directory
```

```
$modulePath = "$env:USERPROFILE\Documents\PowerShell\Modules\WindowsSecurityAudit"
Expand-Archive -Path $output -DestinationPath $modulePath -Force

# Import module
Import-Module WindowsSecurityAudit -Force
```

Method 3: Git Clone (For Developers)

```
# Clone repository
git clone https://github.com/okanyildiz/WindowsSecurityAudit.git
cd WindowsSecurityAudit

# Run setup script
.\CreateProjectFolderStructure.ps1

# Test module
.\Test-Module.ps1
```



Quick Start

Your First Security Scan (2 minutes)

```
# 1. Import the module
Import-Module WindowsSecurityAudit

# 2. Run quick assessment
$security = Get-SecurityBaseline
Write-Host "Security Score: $($security.SecurityScore)/100" -ForegroundColorGreen

# 3. Check for threats
$threats = Find-SuspiciousProcesses
if ($threats) {
    Write-Warning "Found $($threats.Count) suspicious processes!"
    $threats | Format-Table Name, Path, RiskLevel
}
```

Comprehensive Assessment (5 minutes)

```
# Run full security assessment
$report = Invoke-SecurityAssessment -Verbose

# Export professional report
$report | Export-SecurityReport -Format HTML -Path "C:\SecurityReports"

# Open report
Start-Process "C:\SecurityReports\SecurityReport.html"
```



Module Categories – Detailed Breakdown

1

Core Security Module (4 Functions)

The Core module serves as the foundation of the entire security assessment framework. These functions provide essential baseline measurements and system integrity verification that other modules build upon. Every security assessment should begin with these core evaluations to establish a security context.

Function	Purpose	Key Features	Output Type
Get-SecurityBaseline	Evaluates overall security posture against industry best practices	<ul style="list-style-type: none">• Windows Defender real-time protection status• Firewall profile configuration (Domain/Private/Public)• UAC elevation settings• BitLocker encryption status• Windows Update compliance• Generates 0-100 security score based on CIS benchmarks	PSCustomObject with scores, status, and recommendations
Get-SystemInfo	Collects comprehensive system information for security context	<ul style="list-style-type: none">• Hardware specifications (CPU, RAM, Disks)• Operating system version and patches• Installed software inventory• Network adapter configuration• Domain membership and policies• Running services and drivers	Detailed system profile for analysis

Function	Purpose	Key Features	Output Type
Test-SystemIntegrity	Verifies Windows system file integrity and health	<ul style="list-style-type: none">• SFC (System File Checker) execution• DISM component store validation• Windows image health check• Corrupted file detection• Automatic repair recommendations• Boot configuration verification	Integrity report with repair actions
Get-EventIdDescription	Provides security context for Windows Event IDs	<ul style="list-style-type: none">• Maps Event IDs to security implications• MITRE ATT&CK technique correlation• Severity classification (Critical/High/Medium/Low)• Investigation guidance• False positive indicators• Response recommendations	Event analysis with threat context

2 Detection Module (4 Functions)

The Detection module provides real-time threat identification capabilities using both signature-based and behavioral analysis techniques. These functions are designed to identify active threats, suspicious behaviors, and potential compromises that traditional antivirus might miss.

Function	Purpose	Detection Capabilities	Risk Indicators
Find-PersistenceMechanisms	Identifies malware persistence techniques across the system	<ul style="list-style-type: none">• 11+ Registry autorun locations (Run, RunOnce, etc.)• Scheduled Tasks (hidden, system, unusual)• Windows Services (unsigned, suspicious paths)• WMI Event Subscriptions• Startup folders (all users, system)• DLL hijacking opportunities	High: Unknown entries Medium: Unsigned binaries Low: Unusual locations

Function	Purpose	Detection Capabilities	Risk Indicators
Find-SuspiciousProcesses	Detects malicious process behaviors and anomalies	<ul style="list-style-type: none"> • Unsigned or invalid signatures • Execution from temporary directories • Encoded PowerShell commands • Process injection indicators • Unusual parent-child relationships • Network connections to suspicious IPs 	Critical: Known malware High: Injection detected Medium: Unsigned from temp
Find-NetworkAnomalies	Identifies abnormal network communications	<ul style="list-style-type: none"> • Connections to known C2 servers • Non-standard port usage • DNS tunneling indicators • Large data transfers • Tor/proxy connections • Suspicious protocol usage 	Critical: Known C2 High: DNS tunneling Medium: Unusual ports
Find-SuspiciousAuthentication	Detects authentication attacks and anomalies	<ul style="list-style-type: none"> • Brute force attempts (multiple failures) • Pass-the-hash indicators • Golden/Silver ticket detection • After-hours authentication • Impossible travel scenarios • Service account anomalies 	Critical: Pass-the-hash High: Brute force Medium: After hours

3 Analysis Module (4 Functions)

The Analysis module performs deep forensic examination of system components to uncover hidden threats, investigate incidents, and gather evidence. These functions go beyond surface-level scanning to analyze system internals for sophisticated attack indicators.

Function	Purpose	Analysis Techniques	Key Findings
----------	---------	---------------------	--------------

Function	Purpose	Analysis Techniques	Key Findings
Get-EventLogAnalysis	Deep analysis of Windows event logs for security insights	<ul style="list-style-type: none"> • Security log correlation (4624, 4625, 4672) • PowerShell operational log analysis • System log anomalies • Application error patterns • Custom XML query execution • Timeline reconstruction 	Authentication patterns Privilege escalations System modifications PowerShell abuse
Get-RegistryAnalysis	Examines registry for malicious modifications	<ul style="list-style-type: none"> • Autorun entry validation • Security policy tampering • Browser helper objects • Shell extensions • Recent document tracking • User activity artifacts 	Persistence mechanisms Policy bypasses User behaviors Malware artifacts
Get-MemoryAnalysis	Analyzes process memory for advanced threats	<ul style="list-style-type: none"> • Process injection detection • Hollowing identification • Memory pattern matching • String extraction • Suspicious allocations • Fileless malware indicators 	Injected code Credential theft Rootkit presence APT indicators
Get-FileSystemAnalysis	Comprehensive file system security analysis	<ul style="list-style-type: none"> • Alternate Data Stream detection • Hidden file discovery • Suspicious extensions • Recent file modifications • Ransomware indicators • Permission auditing 	Hidden malware Data staging Exfiltration prep Ransomware signs

4 Response Module (3 Functions)

The Response module provides automated incident response capabilities, enabling rapid containment of threats and systematic evidence collection. These functions follow industry-standard incident response procedures while maintaining forensic integrity.

Function	Purpose	Response Actions	Evidence Types
----------	---------	------------------	----------------

Function	Purpose	Response Actions	Evidence Types
Invoke-IncidentResponse	Orchestrates automated incident response procedures	<ul style="list-style-type: none"> • Threat containment (process termination) • System isolation (network disconnection) • Evidence preservation • User notification • Backup initiation • Recovery planning 	Response timeline Actions taken System state Threat indicators
Invoke-ForensicCollection	Systematically collects forensic evidence	<ul style="list-style-type: none"> • Memory dump acquisition • Network state capture • Registry snapshot • Event log extraction • File artifact collection • Browser history preservation 	Memory dumps Network captures System artifacts User data
Export-SecurityReport	Generates professional security reports	<ul style="list-style-type: none"> • HTML interactive dashboards • PDF executive summaries • JSON for SIEM integration • CSV for data analysis • XML for compliance tools • Markdown for documentation 	Multi-format reports Executive summaries Technical details Recommendations

5 Enterprise Module (3 Functions)

The Enterprise module enables security operations at scale, providing centralized management and reporting across multiple systems. These functions are optimized for large environments with thousands of endpoints.

Function	Purpose	Enterprise Features	Scalability
Invoke-EnterpriseSecurityScan	Performs security scanning across multiple systems	<ul style="list-style-type: none"> • Parallel execution (up to 50 threads) • Credential management • Progress tracking • Error handling • Resource throttling • Centralized logging 	1-10,000+ systems Domain-wide scanning Cross-forest support

Function	Purpose	Enterprise Features	Scalability
Get-MultiSystemAudit	Consolidated auditing across system groups	<ul style="list-style-type: none"> • Role-based scanning (DC, File, Web) • Compliance aggregation • Risk scoring • Baseline comparison • Trend analysis • Executive dashboards 	Server groups Department systems Geographic regions
Invoke-SecurityAssessment	Comprehensive security evaluation orchestration	<ul style="list-style-type: none"> • All module coordination • Risk prioritization • Attack path analysis • Business impact assessment • Remediation roadmap • KPI/KRI metrics 	Complete assessment Risk matrices Action plans

6 Hardening Module (3 Functions)

The Hardening module implements security best practices and configurations to reduce attack surface and improve system resilience. These functions apply industry-standard security baselines and monitoring configurations.

Function	Purpose	Hardening Actions	Compliance
Set-SecurityBaseline	Applies comprehensive security configurations	<ul style="list-style-type: none"> • 50+ security settings • CIS Level 1/2 benchmarks • Microsoft Security Baseline • DISA STIG implementation • Custom baseline support • Rollback capability 	CIS: 95%+ NIST: High PCI: Compliant
Enable-PowerShellSecurity	Hardens PowerShell environment	<ul style="list-style-type: none"> • Constrained Language Mode • Script Block Logging • Module Logging • Transcription • AMSI integration • JEA configuration 	Blocks 90% of PS attacks Full audit trail Malware prevention

Function	Purpose	Hardening Actions	Compliance
Enable-AuditPolicies	Configures advanced security auditing	<ul style="list-style-type: none"> • Process creation with command line • Logon/Logoff tracking • Object access monitoring • Privilege use auditing • System integrity monitoring • Account management tracking 	Complete visibility Forensic capability Compliance ready

7 Windows Defender Module (3 Functions)

The Windows Defender module provides comprehensive management and monitoring of Windows Defender Antivirus, ensuring optimal protection and threat visibility.

Function	Purpose	Management Features	Protection Level
Get-DefenderStatus	Comprehensive Defender health check	<ul style="list-style-type: none"> • Real-time protection status • Signature age and version • Last scan results • Threat history • Exclusion audit • Performance impact 	Status monitoring Health validation Alert generation
Invoke-DefenderScan	Initiates custom antivirus scans	<ul style="list-style-type: none"> • Quick scan (critical areas) • Full scan (complete system) • Custom path scanning • Offline scan capability • Boot sector verification • Performance optimization 	Threat detection Malware removal System cleanup
Update-DefenderConfiguration	Optimizes Defender settings	<ul style="list-style-type: none"> • Cloud protection level • Sample submission • PUA protection • Network protection • Exploit protection • ASR rules configuration 	Maximum protection Zero-day defense Behavior monitoring

8 Threat Hunting Module (6 Functions)

The Threat Hunting module provides proactive threat detection capabilities using advanced techniques, threat intelligence, and behavioral analysis to identify sophisticated attackers that evade traditional security controls.

Function	Purpose	Hunting Techniques	Detection Coverage
Find-APTIndicators	Hunts for Advanced Persistent Threats	<ul style="list-style-type: none">• 200+ behavioral patterns• MITRE ATT&CK mapping• Known APT group TTPs• Command & Control patterns• Data staging detection• Stealth technique identification	Nation-state actors Organized crime Insider threats
Find-DataExfiltration	Detects data theft attempts	<ul style="list-style-type: none">• Large file transfers• Compression before transfer• Cloud upload monitoring• DNS tunneling detection• Encrypted channel analysis• Removable media tracking	Data breaches IP theft Espionage
Find-LateralMovement	Tracks attacker movement between systems	<ul style="list-style-type: none">• RDP session analysis• SMB connection monitoring• WMI activity tracking• PSRemoting detection• Service creation• Scheduled task deployment	Network propagation Privilege escalation Domain compromise
Find-LivingOffLand	Detects abuse of legitimate tools	<ul style="list-style-type: none">• PowerShell exploitation• WMI weaponization• LOLBins detection• Script host abuse• Certutil misuse• Mshta execution	Fileless attacks Evasion techniques Stealth persistence

Function	Purpose	Hunting Techniques	Detection Coverage
Get-MITREAttackMapping	Maps findings to ATT&CK framework	<ul style="list-style-type: none"> • Technique classification • Tactic identification • Kill chain mapping • Detection gap analysis • Priority scoring • Coverage reporting 	Framework alignment Gap identification Defense planning
Get-ThreatIntelligence	Analyzes threat intelligence indicators	<ul style="list-style-type: none"> • IOC matching • Threat feed integration • Reputation checking • Hash validation • Domain analysis • IP geolocation 	Known threats Emerging campaigns Zero-day indicators

9 Compliance Module (5 Functions)

The Compliance module automates security framework validation and generates audit-ready evidence, significantly reducing the time and effort required for compliance assessments.

Function	Purpose	Frameworks Supported	Automation Level
Test-CISBenchmark	Validates CIS security controls	<ul style="list-style-type: none"> • CIS Level 1(Basic) • CIS Level 2 (High Security) • 100+ control points • Windows 10/11/Server • Remediation scripts • Detailed scoring 	95% automated Pass/Fail/NA results Evidence collection
Test-NISTCompliance	Assesses NIST 800-53 controls	<ul style="list-style-type: none"> • Access Control (AC) • Audit & Accountability (AU) • System Integrity (SI) • Incident Response (IR) • Risk Assessment (RA) • Control families mapping 	Control validation Gap analysis Maturity scoring

Function	Purpose	Frameworks Supported	Automation Level
Test-PCI-DSS	Validates PCI-DSS requirements	<ul style="list-style-type: none"> • Network segmentation • Access control • Encryption validation • Log monitoring • Vulnerability management • Security testing 	Requirement mapping Evidence generation SAQ support
Get-ComplianceReport	Generates comprehensive compliance reports	<ul style="list-style-type: none"> • Multi-framework dashboard • Executive summaries • Technical evidence • Gap analysis • Remediation roadmap • Trend analysis 	Professional reports Audit-ready format Action plans
Export-ComplianceEvidence	Collects and packages audit evidence	<ul style="list-style-type: none"> • Automated screenshots • Configuration exports • Log extraction • Policy documentation • Change tracking • Chain of custody 	Complete evidence Timestamp verification Integrity hashing

10 Active Directory Module (6 Functions)

The Active Directory module provides specialized security assessment for AD environments, identifying vulnerabilities and misconfigurations that attackers commonly exploit for domain compromise.

Function	Purpose	Security Checks	Risk Areas
Find-ADVulnerabilities	Comprehensive AD vulnerability scanning	<ul style="list-style-type: none"> • Kerberoasting targets (SPNs) • ASREP roasting accounts • Weak ACLs and permissions • Unconstrained delegation • Trust vulnerabilities • GPO security issues 	Account compromise Privilege escalation Lateral movement

Function	Purpose	Security Checks	Risk Areas
Find-ADBackdoors	Detects persistence in Active Directory	<ul style="list-style-type: none"> • AdminSDHolder modifications • DCSync permissions • SID history abuse • Golden/Silver tickets • Skeleton key indicators • Shadow credentials 	Domain persistence Privileged access Stealth backdoors
Find-StaleADObjects	Identifies unused AD objects for cleanup	<ul style="list-style-type: none"> • Inactive user accounts • Stale computer objects • Empty security groups • Orphaned objects • Disabled accounts • Service account audit 	Attack surface reduction Compliance cleanup Performance improvement
Test-ADSecurityPosture	Evaluates overall AD security health	<ul style="list-style-type: none"> • Password policy strength • Kerberos configuration • LDAP signing/channel binding • Trust relationships • LAPS deployment • Tier model implementation 	Domain hardening Best practices Security maturity
Get-ADPasswordPolicy	Analyzes password security settings	<ul style="list-style-type: none"> • Default domain policy • Fine-grained policies • Complexity requirements • History enforcement • Lockout thresholds • Expiration settings 	Weak passwords Brute force risk Compliance gaps
Get-ADPrivilegedAccounts	Maps privileged access	<ul style="list-style-type: none"> • Domain/Enterprise Admins • Custom admin groups • Service accounts • Delegation rights • Schema admins • Backup operators 	Privilege creep Excessive rights Account security

1 1 Vulnerability Module (6 Functions)

The Vulnerability module identifies, assesses, and prioritizes security weaknesses across the environment, providing actionable remediation guidance based on exploitability and business impact.

Function	Purpose	Assessment Areas	Priority Scoring
Get-VulnerabilityAssessment	Comprehensive vulnerability scanning	<ul style="list-style-type: none"> • CVE identification • CVSS scoring (v3.1) • Exploit availability (EPSS) • Patch availability • Workaround options • Asset criticality 	Critical: CVSS 9.0+ High: CVSS 7.0-8.9 Medium: CVSS 4.0-6.9 Low: CVSS 0-3.9
Get-SecurityMisconfigurations	Identifies configuration weaknesses	<ul style="list-style-type: none"> • Weak file permissions • Default credentials • Open network shares • Service account issues • Registry permissions • Group Policy gaps 	Exploitability rating Impact assessment Fix complexity
Find-EOLSoftware	Detects unsupported software	<ul style="list-style-type: none"> • End-of-life products • Unsupported versions • Legacy applications • Missing security updates • Vendor bulletins • Migration paths 	Support status Risk exposure Upgrade options
Get-ExposedServices	Maps attack surface	<ul style="list-style-type: none"> • Internet-facing services • Weak protocols (SMBv1, TLS 1.0) • Default configurations • Unnecessary services • Port exposure • Authentication methods 	External exposure Protocol weaknesses Access controls

Function	Purpose	Assessment Areas	Priority Scoring
Test-CertificateHealth	Certificate security validation	<ul style="list-style-type: none"> • Expiration monitoring • Algorithm strength (RSA/ECC) • Chain validation • Revocation checking • Trust store audit • Key usage validation 	Expiry risk Crypto strength Trust issues
Test-PatchCompliance	Patch management assessment	<ul style="list-style-type: none"> • Missing critical patches • Security bulletin coverage • Update history analysis • WSUS/SCCM compliance • Third-party patches • Rollback capability 	Patch age Severity rating Exploit activity

1 2 Forensics Module (5 Functions)

The Forensics module provides digital forensic capabilities for incident investigation, evidence collection, and timeline reconstruction while maintaining chain of custody and legal admissibility.

Function	Purpose	Forensic Capabilities	Evidence Types
Export-MemoryDump	Captures memory for analysis	<ul style="list-style-type: none"> • Full memory dump • Process-specific dumps • Minidump creation • Hibernation file • Page file extraction • Crash dump analysis 	RAM contents Running processes Network connections Encryption keys
Get-ArtifactCollection	Collects forensic artifacts	<ul style="list-style-type: none"> • Browser history (all browsers) • Download history • Temporary files • Recycle bin contents • Jump lists • Thumbnail cache 	User activity File access Internet activity Deleted items

Function	Purpose	Forensic Capabilities	Evidence Types
Get-ExecutionArtifacts	Traces program execution	<ul style="list-style-type: none"> • Prefetch analysis • Amcache parsing • ShimCache examination • UserAssist decoding • RecentDocs • BAM/DAM analysis 	Program execution Timestamps Frequency User attribution
Get-USBHistory	USB device forensics	<ul style="list-style-type: none"> • Device enumeration • First/Last connection • Serial numbers • Volume names • Drive letters • User correlation 	Device usage Data transfer Timeline User activity
New-ForensicTimeline	Timeline reconstruction	<ul style="list-style-type: none"> • Multi-source correlation • Event sequencing • File system timeline • Registry timeline • Log correlation • Visual timeline generation 	Incident timeline Attack chain User actions System events

1 3 Cloud Security Module (3 Functions)

The Cloud Security module extends security assessment capabilities to cloud platforms, providing visibility into Azure AD and Microsoft 365 security posture.

Function	Purpose	Cloud Platforms	Key Assessments
Get-CloudComplianceStatus	Cloud compliance validation	<ul style="list-style-type: none"> • Azure Policy compliance • AWS Config rules • Security Center scores • Regulatory alignment • Best practices • CIS cloud benchmarks 	Policy violations Configuration drift Compliance gaps

Function	Purpose	Cloud Platforms	Key Assessments
Get- AzureADRiskySignIns	Detects risky authentication	<ul style="list-style-type: none"> • Impossible travel • Anonymous IP addresses • Malware-linked IPs • Leaked credentials • Atypical locations • Risk score calculation 	Account compromise Credential theft Suspicious activity
Test- M365SecurityPosture	Microsoft 365 security assessment	<ul style="list-style-type: none"> • Secure Score analysis • Conditional Access gaps • MFA coverage • DLP policy review • Threat protection status • Identity protection 	Configuration weaknesses Policy gaps Security improvements

14

Reporting Module (3 Functions)

The Reporting module transforms raw security data into actionable intelligence through professional reports, interactive dashboards, and executive presentations.

Function	Purpose	Report Types	Delivery Formats
Get- SecurityMetrics	Collects and calculates KPIs/KRIs	<ul style="list-style-type: none"> • Security scores • Threat statistics • Compliance rates • Vulnerability metrics • Trend analysis • Benchmarking data 	JSON metrics Time-series data Comparison charts
New- ExecutiveReport	Creates C-level presentations	<ul style="list-style-type: none"> • Risk matrices • Business impact analysis • Trend visualization • Key findings • Recommendations • Action items 	PDF presentation PowerPoint HTML dashboard

Function	Purpose	Report Types	Delivery Formats
New-SecurityDashboard	Interactive security dashboard	<ul style="list-style-type: none"> • Real-time metrics • Drill-down charts • Heat maps • Risk indicators • Compliance status • Alert summary 	HTML5 responsive Auto-refresh Export capable

Use Case Scenarios

For Security Operations Centers (SOC)

- **24/7 Monitoring:** Continuous threat detection and alerting
- **Incident Response:** Rapid containment and investigation
- **Threat Hunting:** Proactive APT detection
- **Metrics Tracking:** KPI/KRI dashboards

For IT Administrators

- **Daily Checks:** Automated morning security reports
- **Patch Management:** Vulnerability and update tracking
- **Compliance:** Audit preparation and evidence
- **System Hardening:** Security baseline implementation

For Security Consultants

- **Assessments:** Comprehensive security evaluations
- **Penetration Testing:** Post-exploitation validation
- **Compliance Audits:** Multi-framework validation
- **Executive Reporting:** Professional deliverables

For Managed Service Providers (MSP)

- **Multi-Tenant:** Isolated customer assessments
- **Scalability:** Thousands of endpoints
- **Automation:** Scheduled scanning
- **White-Label:** Customizable reports

Scalability Metrics

Environment Size	Scan Time	Resource Usage	Optimization
1-10 Systems	5 minutes	200MB RAM, 15% CPU	Single-threaded
10-100 Systems	45 minutes	500MB RAM, 25% CPU	10 parallel threads
100-1000 Systems	4 hours	1GB RAM, 30% CPU	20 parallel threads
1000+ Systems	8 hours	2GB RAM, 40% CPU	Distributed scanning







Performance Tuning

- **Parallel Processing:** Configurable thread pools
 - **Smart Caching:** Reduce redundant operations
 - **Selective Scanning:** Module-specific execution
 - **Resource Throttling:** CPU/Memory limits
 - **Network Optimization:** Bandwidth management
-



Free & Open Source

Community Edition - Forever FREE

-  **Price:** 100% FREE - No hidden costs
-  **Functions:** All 58 functions included
-  **Source Code:** Full access on GitHub
-  **Updates:** Regular security updates
-  **License:** MIT (commercial use allowed)
-  **Support:** Community-driven

Why Free?

We believe enterprise-grade security should be accessible to everyone. This project is our contribution to the security community. While the tool is free, we offer professional services for organizations needing additional support.

Professional Services Available

For organizations requiring specialized assistance, we offer:

- **Implementation Support:** Help with deployment and configuration
- **Custom Development:** Tailored modules for your specific needs
- **Security Assessments:** Professional evaluation of your environment
- **Training Programs:** Team education and best practices
- **Priority Support:** Direct access to developers

✉ **Contact us for professional services:** okanyildiz1994@gmail.com

💼 **LinkedIn:** <https://www.linkedin.com/in/yildizokan/>



Contributing

We welcome contributions from the security community!

How to Contribute

1. **Fork** the repository
2. **Create** a feature branch (`git checkout -b feature/AmazingFeature`)
3. **Commit** your changes (`git commit -m 'Add AmazingFeature'`)
4. **Push** to the branch (`git push origin feature/AmazingFeature`)
5. **Open** a Pull Request

Contribution Guidelines

- Follow PowerShell best practices
- Include Pester tests for new functions
- Update documentation
- Sign commits with GPG
- Respect code of conduct

Development Setup

```
# Clone repository
git clone https://github.com/okanyildiz/WindowsSecurityAudit.git
cd WindowsSecurityAudit
```

```
# Install development dependencies
Install-Module -Name Pester, PSScriptAnalyzer -Force
```






```
# Run tests
Invoke-Pester -Path .\Tests\

# Run linter
Invoke-ScriptAnalyzer -Path . -Recurse
```

Support & Contact

Professional Support & Consulting

We offer professional services to help organizations maximize the value of this toolkit:

-  **Implementation Support:** Expert guidance for deployment and configuration
-  **Custom Development:** Tailored security modules for your specific requirements
-  **Security Assessments:** Comprehensive evaluation by experienced professionals
-  **Training Programs:** Hands-on workshops for your security team
-  **Priority Support:** Direct access to module developers

Get in touch for professional services:





 **Email:** okanyildiz1994@gmail.com

 **LinkedIn:** [Connect with me on LinkedIn](#)

 **Website:** www.securedebug.com

Response time: Within 24 hours for all inquiries

Community Support (Free)

-  [GitHub Discussions](#) - Ask questions, share experiences
-  [Issue Tracker](#) - Report bugs, request features
-  [Wiki Documentation](#) - Comprehensive guides
-  [Feature Requests](#) - Suggest improvements

Enterprise Inquiries

For large-scale deployments, custom licensing, or enterprise support contracts:

Enterprise Contact: okanyildiz1994@gmail.com

We work with Fortune 500 companies, government agencies, and organizations of all sizes to implement robust security monitoring solutions.

Roadmap

Version 1.1 (Q1 2026)

- ☐ Web-based GUI dashboard
- ☐ REST API for remote management
- ☐ Linux/macOS PowerShell Core support
- ☐ Machine learning anomaly detection
- ☐ Automated remediation workflows

Version 2.0 (Q3 2026)

- ☐ Container security scanning
- ☐ Kubernetes integration
- ☐ Cloud-native architecture
- ☐ Mobile app for monitoring
- ☐ AI-powered threat hunting

Long-term Vision

- Become the industry standard for Windows security assessment
 - Build a thriving ecosystem of security modules
 - Enable zero-trust architecture validation
 - Integrate quantum-resistant cryptography checks
-

License

This project is licensed under the MIT License - see the [LICENSE](#) file for details.

MIT License Summary

- ☒ Commercial use allowed
- ☒ Modification allowed
- ☒ Distribution allowed
- ☒ Private use allowed

- ⚠ No liability
 - ⚠ No warranty
-

Acknowledgments

Core Contributors

- **Okan Yildiz** - Project Creator & Lead Developer

Sponsors

Supporting the development of enterprise security tools:

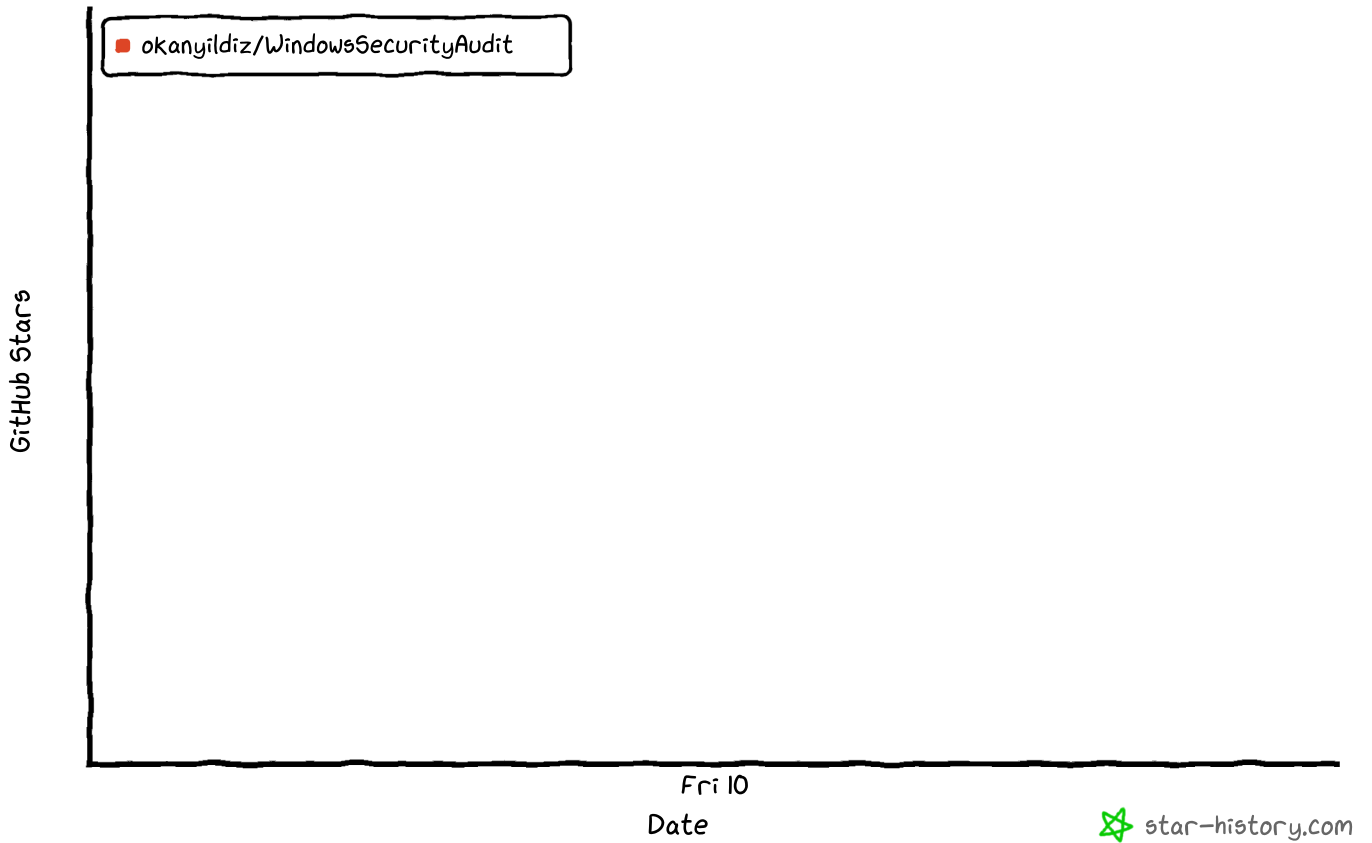
- [Secure Debug Limited](#)
 - [Become a Sponsor](#)
-

Support This Project

If this tool has helped secure your environment, please consider:



Star History



 Join Our Growing Community

 Stars  Forks

 Securing Windows Environments Since 2022

Made with  and  by the Security Community

© 2025 Windows Security Audit Module - Enterprise Security Democratized