SANS SEC505 – Securing Windows and Resisting Malware

Topics

Windows OS & Apps Hardening

1) Sec Templates & Group Policy 505.1–15-74
2) Anti-Malware Strategies 505.1–75-118
3) Hardening Vulnerable Apps 505.1–119-170

HVT & Restricting Admin Compromise

1) Securing HVT 505.2–9-96
2) AD Permissions & Auditing 505.2–98-139
3) Patch Management 505.2–141-176

PKI, BitLocker, and Secure Boot

1) What Is A Public Key Infra ? 505.3–8-47
2) Installing Certificate Services 505.3–49-85
3) Securing Private Keys 505.3–87-105
4) Managing PKI and Smart Cards 505.3–107-152
5) BitLocker and Secure Boot 505.3–154-181

IPSec, Firewall, DNS, and Wireless

1) Windows Firewall 505.4–8-34
2) IPSec Encryption and Port Control 505.4–36-83
3) Enterprise Testing and Deployment 505.4–85-95
4) DNS Security 505.4–97-139
5) Wireless/Wired Network Access . 505.4–141-203

Server Hardening & Dynamic Access Ctl

1) Windows Server Hardening 505.5–9-137
2) Dynamic Access Control 505.5–139-237

Windows Powershell Scripting

1) Overview, Installation & Security ... 505.6–8-31
2) Getting Around Inside The Shell .. 505.6–33-57
3) Running Cmdlets, Func & Scripts 505.6–59-115
4) Ex: AD, Event Logs & Nmap ... 505.6–117-139
5) writing Own Functions & Scripts 505.6–141-185
6) Windows Mgt Instrumentation .. 505.6–187-201

Categories

Appendix

802.11 Wireless Concepts Refresher 505.4–205
Accounting = Logging 505.4–211
ADM/ADMX Templates 505.1–192
Becoming A Domain Controller 505.1–172
Editing Security Templates By Hand ... 505.1–186
Network Unlock 505.3–183
NTLMv2 Authentication 505.5–239
RADIUS Account Lockout 505.4–215
Restricting Anonymous Access 505.5–249
Social Engineering 505.1–180

Best Practices & Tips

Anti-Malware Training 505.1–102
Application Whitelisting 505.1–82
AppLocker Default Rules Creation 505.1–94
Auditing 505.2–139
BitLocker, TPM, Secure Boot 505.3–177-181
CA Hierarchy Design 505.3–57-58
Certificate Template Permissions 505.3–84-85
DAC – Upgrade Servers & Clients First 505.5–141
Debug Program Privilege 505.2–32
Delegation Of Authority 505.2–117-118
Deny NTFS Exec Permission on Paths .. 505.1–94
Desktop Management 505.1–114
Disable NetBIOS And LLMNR 505.4–97-103
DNS Security 505.4–133-139
EMET Configuration 505.1–127, 128, 129
Get AppLocker Warning Messages 505.1–96
Good-to-have Security Features 505.1–79-80
GPO Scripts 505.1–71, 73
Import/Change DNS Records 505.4–108
Java Security Recommendations 505.1–165
Load Balancing 505.2–160
Local Accounts And Passwords 505.2–92-95
Local Administrators Group 505.2–47
Logon Restrictions 505.2–19
Password Managers 505.2–88-90
Patch Management Update Cycle .. 505.2–142-143
Permieter Firewall Policies 505.4–9
Picture Password And PIN 505.2–82-84
Principle of Least Privileges 505.2–42
Private Keys Protection 505.3–98-105
Privileges List 505.2–23
RDP 505.5–112-113
Scheduled Tasks 505.5–55-57
Service Account Identities 505.4–36
SMB 3.0 .... 505.5–98
Software Inventory 505.1–120
Token Abuse/Pass-the-hash 505.2–33-39
Two-Account Strategy 505.2–49-50
User Rights List 505.2–17
Virtual Desktop Infrastructure 505.1–114
Wireless Security 505.4–197-203
WPAD Hardening 505.1–148

Group Policy Configurables

801.X Configuration 505.4–193
Account Policies 505.2–64-68
AppLocker 505.1–90-93
Audit Policies 505.5–68, 215
  Advanced Configuration 505.5–72
Auto-Enrollment Settings 505.3–108
AutoPlay 505.1–101
BitLocker Drive Encryption 505.1–106
  .... 505.3–162, 164
  AD Backup 505.3–175
  Data Recovery Agent (Add) 505.3–176
  Passphrase (Enable) 505.3–165
  PIN/USB Option (Show) 505.3–165
  Unique Identifiers 505.3–176
Certificate Path Validation Settings 505.3–121
Console Logon Authentication 505.2–93
Credential Roaming 505.3–115
Credentials Caching 505.2–39
  .... 505.5–106

Credentials Delegation 505.5–111-112
Credentials Storage 505.2–87
 505.5–55
CredSSP Credentials Sharing 505.2–37
Custom Tech Support Link 505.1–95
DCHP Audit Logging (Enable) 505.4–113
EMET 505.1–126
Event Log Settings 505.5–73
Global Groups 505.2–43
Google Chrome 505.1–151
IE Browing History 505.5–81
Integrity Checking (Re-Enable) 505.3–162, 164
Internet Connection Sharing (Limit) 505.4–182
Internet Explorer Hardening 505.1–130, 136, 137
IPSec Policies 505.4–90
Java APPLET Element Support 505.1–161
Java Configuration Files 505.1–161
LLMNR (Disable) 505.4–102
Local Accounts 505.2–93
Local Groups 505.2–45
Local Passwords 505.2–93-94
Make Desktops Like Appliances 505.1–85-88
Name Resolution Policy 505.4–126
Network Authentication 505.2–93
Network Bridging (Disable) 505.4–182
Network Profiles 505.4–25
NTLM Restriction 505.5–117
NTP Settings 505.5–77
Password Complexity Filtering 505.2–70
Prevent Ignoring Certificate Errors 505.5–103
Privileges 505.2–22
Proxy Settings 505.1–146
RDP Restricted Admin Mode 505.2–37
Removable Devices Control 505.1–104
Require Smart Card Authentication 505.2–21
Scheduled Jobs 505.2–92
Scheduled Tasks 505.5–53
Scripts 505.1–70, 72-73
 505.2–91
Server Manager Default Source Path 505.5–17
Services Settings 505.5–32
SMB Signing 505.5–97
System Restore Setting 505.5–80
Turn Off Root CA Updates 505.3–119
User Account Control 505.2–54, 60
User Rights Assignment 505.2–17, 22
Windows Firewall 505.4–89-90
Windows Updates 505.2–159
Wireless Network Policy 505.4–179

Tools

Active Directory

`ACLDIAG.EXE` 505.2–100, ? 112-113
`ADPREP.EXE` 505.2–101
 505.3–49
`ADRESTORE.EXE` 505.2–102
`CSVDE.EXE` 505.2–101
`DCDIAG.EXE` 505.2–101
`DNSCMD.EXE` 505.2–101
`DS*.EXE` 505.2–100-101
`DSACLS.EXE` 505.2–? 110-112
`DSREVOKE.EXE` 505.2–113
`ENUMPROP.EXE` 505.2–100
`LDIFDE.EXE` 505.2–101
`MOVETREE.EXE` 505.2–101
`NETDIAG.EXE` 505.2–101
`NETDOM.EXE` 505.2–100
`NLTEST.EXE` 505.2–100
`NTDSUTIL.EXE` 505.2–101
`REPADMIN.EXE` 505.2–101
`SDCHECK.EXE` 505.2–100, 113
ADMT 505.2–101
CLONEPRINCIPAL (VBS) 505.2–101
FastLane ActiveRoles 505.2–118
JoeWare Tools 505.2–101
NetIQ Directory Security Admin 505.2–118
Quest Software 505.2–118

MSI Package Editors

Advanced Installer 505.2–163
CapaInstaller 505.2–163
EMCO MSI Package Builder 505.2–163
Flexera InstallShield & AdminStudio 505.2–163
ITNinja 505.2–163
ScriptLogic/Quest MSI Studio 505.2–163
WinINSTALL 505.2–163

Network

`DIG.EXE` 505.4–105, 129
`DNSCMD.EXE` 505.4–103, 105
`DNSDIAG.EXE` 505.4–106
`DNSLINT.EXE` 505.4–106
`Dot11WLogoTests.exe` 505.4–197
`IASPARSE.EXE` 505.4–213
`IPCONFIG.EXE` 505.4–105
`IPSECCMD.EXE` 505.4–19, 39, 92
`IPSECPOL.EXE` 505.4–20, 39, 92-93
`NBTSTAT.EXE` 505.4–98
 505.5–84
`NETDIAG.EXE` 505.4–19
`NETSH.EXE` 505.4–16, 39, 65, 92-95, 127, 183, 185, 194
`NSLOOKUP.EXE` 505.4–105, 135
`RASUSERS.EXE` 505.4–135
EMCO MAC Address Scanner 505.4–185
McAfee ePolicy Orchestrator 505.4–185
Vanilla DH 505.4–54

Password Filters

Dictionary Password Filter 505.2–73
DictionaryFilter 505.2–73
Hitachi ID 505.2–73
NFront Password Filter 505.2–73
PASSFILT 505.2–72
Password Policy Enforcer 505.2–73
PasswordFilter 505.2–73
Specops Password Policy 505.2–73

Password Managers

AutoCipher 505.2–96

Cyber-Ark 505.2–88, 95
IronKey 505.2–88
Kapersky Password Manager 505.2–88
KeePass 505.2–88
LastPass Pocket 505.2–88
Lieberman Software 505.2–88, 95
ManageEngine 505.2–95
NetWrix Privileged Account Manager 505.2–96
Password Safe 505.2–88
PasswordCourier 505.2–96
RoboForm 505.2–88
SplashID 505.2–88
Thycotic Secret Server 505.2–96

Patch Managers

MBSACLI.EXE 505.2–169-171
Altiris 505.2–171
Citrix GoToManage 505.2–162
Ecora 505.2–171
FileHippo Update Checker 505.2–168
Gravity Storm 505.2–171
IBM Endpoint Manager 505.2–171
Lumension Patch 505.2–172
Ninite 505.2–168
Secunia PSI/OSI 505.2–167-168
Shavlik Technologies 505.2–172
SolarWinds Patch Manager 505.2–162
System Center Config Manager 505.2–172
TechTracker 505.2–168

Public Key Infrastructure

CERTREQ.EXE 505.3–19
CERTSRV.EXE 505.3–13, 18
CERTUTIL.EXE 505.3–17-18, 67, 71, 74, 107, ? 113, 124
CMGETCER.DLL 505.3–20
DSSTORE.EXE 505.3–17
MSCEP.DLL 505.3–20
WINHTTPCERTCFG.EXE 505.3–18
ADSI 505.3–19
CA/Cert/Templates MMC Snap-ins 505.3–13
Certificate Services Websites 505.3–15-16
Enterprise PKI MMC Snap-in 505.3–14-15
Forefront Identity Manager 505.3–140
Group Policy Settings For PKI 505.3–13
Key Recovery Tool 505.3–16
MSDN CryptoAPI Tools 505.3–20
Powershell Certificates Provider 505.3–15
Quest Software's Powershell Cmdlets 505.3–19
Versatile Security 505.3–139

Products ●

Bit9 Security Platform 505.1–82, 107
CoreTrace Bouncer 505.1–82
CoSoSys Endpoint Protector 505.1–107
DeviceLock 505.1–107
Kapersky Device Control 505.1–107
Lumension Application Control 505.1–82
Lumension Device Control 505.1–107
McAfee Application Control 505.1–82
McAfee Device Control 505.1–107
Microsoft AppLocker 505.1–82
SignaCert Entreprise Trust 505.1–82
Sophos SafeGuard 505.1–107
Symantec Endpoint Protection 505.1–107
VMWare Workstation 505.1–110

Proxy Servers

Blue Coat ProxySG 505.4–10
Squid 505.4–10
Websense Gateway 505.4–10

System

ADDIAG.EXE 505.1–36
AUDITPOL.EXE 505.2–137-139
505.5–70, 215
AUTO2EXE.EXE 505.2–50
AUTOIT.EXE 505.2–50
CMD.EXE 505.1–70, 84, 88
505.2–60-62
CMDKEY.EXE 505.2–87
CONSENT.EXE 505.2–57
CONTROL.EXE 505.2–87
CPAU.EXE 505.2–50
CSCRIPT.EXE 505.1–70, 96
DCGPOFIX.EXE 505.1–36
DCPROMO.EXE 505.2–100
DISKPART.EXE 505.3–155
DISM.EXE 505.5–46
DNSCMD.EXE 505.1–147
DSAC.EXE 505.5–146
EPAL.EXE 505.2–50
EXPLORER.EXE 505.1–84, 88
505.2–57
FC.EXE 505.5–66
FINDSTR.EXE 505.1–27
FSUTIL.EXE 505.5–79
GPOTOOL.EXE 505.1–36
GPRESULT.EXE 505.1–36
GPUPDATE.EXE 505.1–31, 35
505.2–44
GREP.EXE 505.1–27
ICACLS.EXE 505.2–58-60
IEXPLORE.EXE 505.1–135, 142
KLIST.EXE 505.5–145
LDIFDE.EXE 505.2–77-79
LDP.EXE 505.2–100, 103
LSASS.EXE 505.2–31, 34
505.3–90
MMC.EXE 505.1–15, 32
505.2–99
MSTSC.EXE 505.2–36
505.5–105, 111
NET.EXE 505.2–52, 87
NOTEPAD.EXE 505.1–84
POWERSHELL.EXE 505.1–96
PSEXEC.EXE 505.2–30, 36, 50, 57
505.5–53
RECIMG.EXE 505.1–112
REG.EXE 505.5–176
REGEDIT.EXE 505.1–18, 27

505.2–52
505.3–71, 95, 118
REGSVR32.EXE 505.2–100
RUNAS.EXE 505.2–30, 32, 49, 50, 54, 57
RUNDLL32.EXE 505.2–87
SC.EXE 505.5–29, 32-36, 39
SCHTASKS.EXE 505.2–35, 505.5–53, 57
SCW.EXE 505.5–18
SCWCMD.EXE 505.5–19-21
SECEDIT.EXE 505.1–27, 29-30, 36
505.5–23
SETSPN.EXE 505.3–17
SYSKEY.EXE 505.3–91, 95, 99-102
SYSPREP.EXE 505.1–118
TPMVSCMGR.EXE 505.3–144
TQCRUNAS.EXE 505.2–50
VAULTCMD.EXE 505.2–87
W32TM.EXE 505.3–52
505.5–77
WHOAMI.EXE 505.2–22, 53, 54, 57
505.5–145, 169
WMIC.EXE 505.2–36
WSCRIPT.EXE 505.1–70, 96
WSUSUTIL.EXE 505.2–160
WUAUCLT.EXE 505.2–160
ADMX Migrator 505.1–36, 61
Performance Monitor 505.4–106, 135
Sysinternals 505.2–102

Tool
CEPSETUP.EXE 505.4–40
CHML.EXE 505.2–58-60, 90
CSDIFF.EXE 505.5–66
KERBTRAY.EXE 505.2–38
LSADUMP2.EXE 505.3–96
REGIL.EXE 505.2–58
RUNASIL.EXE 505.2–58
SHA256DEEP.EXE 505.5–66-67
STREAMS.EXE 505.5–175
WINDIFF.EXE 505.5–66
gpprefdecrypt.py 505.2–94
Cain 505.2–31
505.3–96
EMET 505.1–123
Incognito 505.2–29
Manage-BDE 505.3–142, 155, 158-159, 175-177
Metasploit 505.1–77
505.2–32
Network Password Recovery 505.2–86
NirSoft's LSA Secrets View 505.5–35
OllyDbg 505.2–31
Process Explorer 505.2–54, 57
Process Hacker 505.1–127, 128
505.2–57, 58
Process Monitor 505.2–48
Runhash 505.2–32
Windows Credentials Editor 505.2–32

Wireless Network
Aircrack-ng 505.4–143
Airpwn 505.4–187
Cain & Abel 505.4–144
505.5–109
CloudCracker 505.4–143
CoWPAtty 505.4–143
Elcomsoft Wireless Security Auditor 505.4–143
Fluke AirMagnet 505.4–185
Metageek Chanalyzer 505.4–184
Metageek inSSIDer 505.4–184
Metageek Wi-Spy 505.4–184
NirSoft's Wireless Key View 505.4–144
Pyrit 505.4–143

PowerShell Cmdlets

Account Policy
get-addefaultdomainpasswordpolicy 505.2–75
get-addomain 505.2–75
get-adfinegrainedpasswordpolicy 505.2–76
new-adfinegrainedpasswordpolicy 505.2–76
set-addefaultdomainpasswordpolicy 505.2–75
set-adfinegrainedpasswordpolicy 505.2–76
add-adfinegrainedpasswordpolicysubject 505.2–76

Active Directory
Get-ADClaimType 505.5–165
Get-ADComputer 505.5–167
Get-ADResourcePropertyList 505.5–181-182
Get-ADResourceProperty 505.5–179
Get-ADUser 505.5–169
Set-ADObject 505.5–167

AppLocker
get-applockerfileinformation 505.1–96
get-applockerpolicy 505.1–96
new-applockerpolicy 505.1–95
set-applockerpolicy 505.1–96
test-applockerpolicy 505.1–96

Classification
Update-FSRMClassificationpropertyDefinition 505.5–176

Installation & Configuration
Get-WindowsImage 505.5–45
Install-WindowsFeature 505.5–16-17, 46, 146
Remove-WindowsFeature 505.5–45
Set-ItemProperty 505.5–96
Uninstall-WindowsFeature 505.5–17

Inventory
get-wmiobject 505.1–120
505.2–28, 92

Network
Add-DnsServerTrustAnchor 505.4–121
Get-DnsClientNrptPolicy 505.4–127
Get-DnsServerDnsSecZoneSetting 505.4–123
Get-DnsServerTrustAnchor 505.4–124
Get-SmbConnection 505.5–93
Get-SmbShare 505.5–94
Resolve-DnsName 505.4–119, 129
Set-DnsServerGlobalNameZone 505.4–103
Set-SmbServerConfiguration 505.5–94, 96
Set-SmbShare 505.5–94

Permissions
 Get-Acl 505.5–145
 Set-Acl 505.5–145
PowerShell
 Format-Table 505.5–169
 Set-ExecutionPolicy 505.1–13
 dir 505.3–15
 export-csv 505.1–120
 get-content 505.1–121
 505.2–170-171
 get-executionpolicy 505.1–97
 get-help 505.1–35, 98, 165
 505.2–100
 505.3–15, 156
 505.4–16, 93, 127
 505.5–16, 37-38, 145, 170
 get-service 505.5–34-36
 import-module 505.1–35
 505.2–100
 505.5–16
 select-object 505.1–121
 505.5–182
 set-executionpolicy 97

Locations
C:\Users\username\Documents\
 Security\Templates 505.1–15
%AllUsersAppData%\Microsoft\
 Crypto 505.3–95
%AppData%\Microsoft\
 Crypto 505.3–88-89
 System Certificates 505.3–89
%PrgFiles%\
 Gpmc\Scripts 505.1–34
 Update Services\Tools 505.2–160
%SysRoot%\
 CAPOLICY.INF 505.3–50-51
 Inf 505.1–57-59
 505.2–159
 PolicyDefinitions\en-US 505.1–59
 PolicyDefinitions 505.1–59
 SYSVOL 505.1–57
 ServiceProfiles 505.3–95
 System32\Certsrv\Certenroll 505.3–124
 System32\Drivers\Etc\hosts 505.4–131
 System32\dns 505.4–124, 138
 System32 505.2–108, 123
 System32\CertLog 505.3–65
%UserProfile%\Application Data\Microsoft\
 Protect\CREDHIST 505.3–92
\\controller\SYSVOL*domain*\Policies\
 PolicyDefinitions\en-US 505.1–59
 PolicyDefinitions 505.1–59
\\server\SYSVOL*domain*\Policies\ 505.1–39
 PolicyDefinitions 505.2–159
 GPO-GUID\Adm 505.1–57, 59
http://*server*/certsrv/ 505.3–27-28, 60, 67, 149

SANS SEC505 – Securing Windows and Resisting Malware

A

- Access-Denied Assistance → FSRM
- Account Policies 505.2–? 63-69
- Accounts Inventory 505.2–92
- ACE 505.2–106
- ACL 505.2–26, 109 505.3–83
  - Discretionary (DACL) 505.2–106, 135 505.5–152
  - System (SACL) 505.2–106, 134-135
  - Tools 505.2–? 111-114
- Acronis 505.1–112 505.2–148
- ACT 505.1–122, 127 505.2–48
- Active Directory 505.2–43, 77 66-67, 71
  - Auditing 505.2–134-139
  - Central Access Rules & Policy → CAR
  - Certificate Services 505.3–22, 27-28
    - Best Practices Analyzer 505.3–76
    - Install 505.3–59-68
    - Policy Module 505.3–? 65-67, 71
    - Post-Install 505.3–69-76
    - Pre-Install 505.3–49-52
    - Website 505.3–27-28, 67, 124, 149-152
  - Command-Line Tools 505.2–100-101
  - Delegation Of Control 505.1–48 505.2–115-118 505.5–174
  - DNS 505.4–107-108
  - `DSSEC.DAT` 505.2–108, 123
  - Functional Level 505.5–128
  - Generic Auditing 505.2–135
  - Global Catalog 505.3–52
  - Groups
    - Cert Publishers 505.3–? 73
    - DNSUpdateProxy 505.4–111-113
    - Everyone 505.4–110
    - Protected Users 505.5–119
    - RAS And IAS Servers 505.4–148, 174-175
    - Wireless Users 175
  - Inventory 505.1–121
  - Permissions 505.2–104-110, 127
    - Fix Procedure 505.2–112
    - Proposed 505.5–214-216
  - PKI 505.3–9
  - Properties Visibility 505.2–108
  - Provided Scripts 505.2–127
  - Tools 505.2–98-103, 118
    - → ACL Tools
- Active Directory → Resource Properties
- ActiveX 505.1–130, 133, 136, 141-142, 167
- ADAC 505.2–75, 98 505.5–145-146
- ADM/ADMX Templates 505.1–21, 31, ? 57-61, 122, 125
  - Central Store 505.1–58-60
  - Convert 505.1–61
  - Create 505.1–61
  - Custom 505.1–? 192-197
  - Hardening 505.1–151, 154, 167, 170
  - Import 505.1–57
  - Migration 505.1–61
- Administrative Templates
  - Control Panel 505.1–85-86
  - Desktop 505.1–85
  - Network 505.1–86
  - Start Menu 505.1–85
  - System 505.1–86
  - Windows Components 505.1–85
  - WSUS 505.2–159
- Administrators 505.2–29, 31, 40, 41, 44, 92-93, 130-131
- AdminSDHolder 505.2–109
- ADML File 505.1–58-59
- ADMT 505.2–101
- Adobe Reader/Acrobat 505.1–152
  - Alternatives 505.1–156-157
- ADS 505.5–140, 175
- ADSI 505.2–77, 79, 96, 99, 111, 114 505.3–22, 175 505.4–110
  - Scripting Support 505.2–102, 114
- AES 505.2–39, 94, 148 505.3–21, 32, 90, 112, 157-159, 180-181 505.4–38-39, 67
- AGPM 505.1–35
- AH 505.4–32, 47-48, 52, ? 56-61, 66
- AIA 505.3–45, 50, 71
- AIK 505.2–148
- Amazon 505.1–115
- Anonymous Access Restriction 505.5–249-253
- Anti-Malware 505.1–114
- Antivirus 505.1–79-81
- App-V 505.1–112
- AppContainer Sandbox 505.1–133
- Application Control 505.2–47
- Application Whitelisting 505.1–82-88
- AppLocker 505.1–88, 89-98
  - Conditional Expressions 505.5–150
  - Default Rules 505.1–91
  - Import/Export XML Files 505.1–95
  - Rules Precedence 505.1–? 95
- ARP Poisoning 505.4–187
- ASLR 505.1–125, 127, 133, 153
- Audit Policies 505.2–? 136-137
- Audit Policies → Active Directory
- Audit Policy 505.5–68-70
  - Advanced Configuration 505.5–70-72
  - DNS Logging 505.5–78
  - NTFS Last Access Timestamps 505.5–79
  - Process Creation/Termination 505.5–78
  - Windows Firewall 505.5–78
- Authenticated Users 505.2–126
- Authentication 505.3–29
  - Precedence 505.4–68

- AuthIP 505.4–54-55, 64, 71
- AuthZ API 505.5–150
- Auto-Unlock 505.3–? 169
- AutoIt 505.2–50, 144
- AutoPlay & AutoRun 505.1–101-103
- `AutoRun.inf` 505.1–101
- Avecto Privilege Guard 505.1–37

B

- Backdoor 505.2–25
  505.4–13
- Backtrack 505.4–142
- BAP 505.4–170
- BDC 505.2–152
- BeyondTrust PowerBroker Desktops 505.1–37
- Biba Model 505.2–56
- Bit9 Security Platform 505.1–82, 88, 99-100
- BitLocker 505.1–106, 110, 124, 127
  505.2–90
  505.3–64, 142, 154-160, 183
  - Data Recovery Agent 505.3–175-176
  - Emergency Recovery 505.3–? 172-176
  - On USB Drives 505.3–167-171
  - Password Recovery Viewer 505.3–? 156
  - Tools 505.3–155-156
  - TPM Options 505.3–? 163-166
- BitLocker To Go 505.1–111
  505.3–154-155, 167-169, 171, 176
  - Enable 505.3–168
- BITS 505.2–152, 157, 166
- BSOD crash 505.1–111
  505.5–75
- Bulletins 505.2–146
  505.5–10
- BYOD 505.1–110, 115
  - Tethering 505.4–181-183

C

- CA 505.3–49-52, 53-58
  505.4–69, 174-175
  - `CAMONITOR.VBS` 505.3–75
  - `CAPICOM.DLL` 505.3–75
  - `CAPOLICY.INF` 505.3–50-51, 124
  - Enterprise 505.3–? 65-66, 83, 107, 124, 146, 151
    505.4–69, 163
    - Certificates (Template) → PKI
  - Monitoring Events 505.3–75
  - Permissions 505.3–81
  - Roles 505.3–74
  - Stand-Alone 505.3–65-66, 71, 84, 124, 146
  - Trusted 505.3–117
- Cached Credentials 505.2–38
- Cain 505.2–31
- CAP 505.5–190-191, 197-198
  - Publication Through GPO 505.5–200-202
  - Staging 505.5–215
- CAR 505.5–? 190, 192-195
- CCITSE 505.3–74
- CDP 505.3–44, 50, 71, 123-125
- CEnroll 505.3–19
- Centrify DirectControl 505.1–37
- Certificate → Cryptography, PKI
- CHAP 505.2–65
  505.4–39
- Choke Points 505.4–9
- Chrome Frame 505.1–150
- CIS 505.1–19
- Claims → DAC
- Class User/Machine 505.1–? 193
- Classification Rules → FSRM
- Classification Tags → DAC
- Cloud 505.1–115
  505.4–188
- CMGetCer 505.3–20
- CNAME 505.4–103
- CNG 505.3–89-90, 505.3–95
- Cold Boot Attack 505.3–179
- Conditional Expressions
  - Strings 505.5–151
  - With Claims 505.5–172-174
  - With Resource Tags 505.5–186-187
  - Without Claims 505.5–148-153
- Conficker 505.1–77, 101
  505.2–16
  505.4–13
- Confidentiality 505.3–30
- Connection Sharing 505.4–182
- Control Points 505.1–7
- Core Impact 505.1–77
- Credential Roaming 114-116
- Credentials Manager 505.2–85
- CredSSP 505.2–36, 39
  505.5–110
- CRL 505.3–22, 44, 50, 52, 67-68, 71, ? 123-125
  505.4–164
- Cross-Forest Trusts 505.5–? 126-130
- CryptoAPI/CNG 505.3–9, 19-23, 89, 117, 133
  - Definition 505.3–12
  - Documentation 505.3–38
  - MSDN Tools 505.3–? 20
  - Path Validation Procedure 505.3–46
- Cryptography 505.3–29-40
  - Acronyms And Abbreviations 505.3–38-39
  - Certification Authority 505.3–37, 41-47
  - Definitions 505.3–31-33
  - Security Benefits 505.3–29
  - X.509v3 Certificate Structure 505.3–? 43-45
    505.4–162
- CSE 505.1–64
  505.2–45, 92
  505.5–32
- CSP 505.3–21-23, 62, 94, 133
- CTL 505.3–22, 54, 119-121

D

- DAC 505.2–122
  505.5–115
  - Overview 505.5–? 139-144
  - Access-Denied Assistance → FSRM
  - Big Picture 505.5–190-191
  - Central Access Rules & Policy 505.5–192-209
  - Claims 505.2–63
    505.5–157-158
    - Types 505.5–164-165
    - Valid 505.5–162
  - Classification Tags 505.5–175
    - Automatic Application 505.5–217-220
    - Products Using Tags 505.5–236-237
  - Components 505.5–140
  - Glossary 505.5–143-144
  - Kerberos Compound Auth → Kerberos
  - Requirements 505.5–? 141-142
  - Resource 505.5–178
  - Test Permissions → Proposed Permissions
  - Third-Party Additions 505.5–230
  - Tools 505.5–145-146
- Data Integrity 505.3–30
- Data Loss Prevention 505.1–107
- Data Segregation 505.1–115
- Debug Programs Privilege 505.2–31-32
  505.5–34, 37
- Debugger 505.2–31
- Deep Freeze 505.1–113
- Delegation Of Control Wizard 505.2–? 119-121
- `DELEGWIZ.INF` 505.2–119
- DEP 505.1–125, 126, 153
- DES 505.2–39, 65
  505.3–90, 112
  505.4–67
- Desktop IE 505.1–132
- Desktop Management 505.1–114
- Device Control 505.1–107
- DHCP 505.4–110, 505.1–144
- Diffie-Hellman 505.3–35
  505.4–52, 54, 63-65, 71
  - Types & Groups 505.4–64
- Digest 505.2–39
- Digital Certificate 505.3–43-45
- DirectAccess 505.2–165-166
  505.3–11, 143
  505.4–11-12
- DISA 505.1–21
- DLL Injection 505.2–25, 31, 34, 47
- DLP 505.1–107
  505.2–122
- DNS 505.1–144
  - Active Directory 505.4–107-108
  - AD-Integrated 505.4–108-109, 115, 134-135
  - Authoritative Server 505.4–128
  - Cache Poisoning Attack 505.4–102, 113, 138
  - DNS Name Resolution Only 505.5–83
  - DNSSEC 505.4–115-120
    - Management 505.4–121-130
  - GlobalNames Zone 505.4–103
  - Internal/External 505.4–133-135
  - Key Master 505.4–125
  - Logging 505.5–78
  - Records Permissions 505.4–110
  - Secure Dynamic Updates 505.4–109-114
  - Single-Label Name Resolution 505.4–103
  - Sinkhole 505.4–131
  - Tools 505.4–104-106
  - Zone 505.4–107, 123
    - Signing 505.4–116
    - Stub 505.4–136
- DoD Protocol Model 505.4–? 36
- DOI 505.4–49
- Domain Admin 505.2–14, 505.2–132-133
- Domain Controller 505.1–172-179
- Domain Join 505.2–126, 129
- DoS Attack 505.4–115, 141, 215
  505.5–76, 110-111
- DPAPI 505.2–81-82, 89
  505.3–89-90, 102

E

- EAP 505.4–162, 208
- ECDSA 505.4–73
- Effective Permissions 505.5–152-155
  - NTFS & CAP 505.5–204-207
- EMET 505.1–122-129
- EMS 505.1–120, 150
  505.2–92, 142
- Enclave 505.4–8
- Enterprise Trust 505.3–119
- Enterprise-Scale Registry Editor 505.1–55
- EPM 505.1–132-134
- ESP 505.4–32, 47-48, 52, 56-61, 63, 66
  505.5–121
- Ethernet Switches 505.4–190-192
  - Requirements 505.4–191
  - Wired AutoConfig Service 505.4–191
- Event Viewer 505.1–90
  505.2–134
  505.4–20, 106, 211
  505.5–58, 68
  - ID 1001, 1005 (SMB) 505.5–95-96
  - ID 4688, 4689 (Process) 505.5–78
  - ID 4817, 4818 (GOAA) 505.5–? 214, 233

F

- FAST 505.5–114
- FCI 505.5–140, 218, 221
  - Third-Party Additions 505.5–230
- FDCC 505.1–20
- File System Encryption 505.3–11
- Firefox 505.3–117

- 505.5–51
- Firewire Port Attack 505.3–179
- Flame 505.1–77
- Flamer 505.1–145
- FSRM 505.5–140, 176, 191, 218, 221
  - Access-Denied Assistance .... 505.5–? 210-213
  - Automatic Classification Rules .... 505.5–? 221
  - Installation 505.5–146
- Full Control Delegation 505.2–130
- FullArmor 505.1–36
- FVEK 505.3–157-158, 175

G

- `Generic.inf` 505.1–15-16
- Ghost 505.1–112
- Global Catalog 505.3–67
- GMSA 505.5–38
- GOAA .... 505.5–191, ? 231-235
  - Compatibility Issues 505.5–232
- Google Chrome 505.1–149-151
- 505.5–51
- GPMC 505.1–32
- 505.2–99
  - Replacements 505.1–37
- GPO 505.1–21
  - Acces Control Lists 505.1–47
  - Applicability (which, when) 505.1–39
  - Apply Changes 505.2–44
  - Audit Policy 505.2–135-137
  - Backup/Restore 505.1–33
  - Configurations 505.1–41
  - Creation 505.1–40
  - Delegation of Control 505.1–48
  - Enforced 505.1–46
  - HTML/XML reports 505.1–32
  - Inheritance 505.1–45
  - IPSec & Firewall Policies 505.4–89-91
  - Links 505.1–42
  - Loopback Mode 505.1–50-52
  - Options visibility 505.1–57
  - Passwords 505.1–65
  - Precedence 505.1–44
  - 505.4–90
  - Preferences 505.1–63-68
  - 505.2–45, 92, 93-94
  - Refresh 505.1–31-32, 50
  - Scheduled Jobs 505.2–94-95
  - Scripts 505.1–69-74
  - 505.2–94-95
  - 505.4–93
  - Slow Link Detection 505.1–49
  - Tech Support Link 505.1–95
  - WMI Filtering 505.1–50
- Group Policy 505.1–31, 124-126
  - Capabilities 505.1–31
  - Enhancements 505.1–36-37
  - Tools 505.1–31

H

- Hardening
  - Base Principle 505.5–13
  - Cross-Forest Trusts → Cross-Forest Trusts ....
  - Dangerous Files 505.5–49-51
  - Disable Unnecessary Services 505.5–29-32
  - Extranet Forest For Exposed Servers 505.5–131-134
  - Extranet Forest FW Design Issues . 505.5–135-137
  - IPSec & Windows Firewall 505.5–121-123
  - IPv6 → IPv6 ....
  - Kerberos Armoring → Kerberos ....
  - NTLM Auth Restriction → NTLM ....
  - Pre-Forensics 505.5–60-81
    - Logging & Audit 505.5–68-76
    - Miscellaneous Settings 505.5–77-81
    - System Snapshots 505.5–60-67
  - Provided Scripts 505.5–62-65
  - RDP → RDP ....
  - Scheduled/Immediate Tasks 505.5–52-59
  - Server Installation 505.5–41-48
  - Servers Exposure To Internal Forest 505.5–124-125
  - Service Account Identities 505.5–33-40
  - SMB → SMB ....
  - SSL/TLS → SSL/TLS ....
  - Start 505.5–12-15
  - Unnecessary Networking Components 505.5–82-88
- Hardware Identifier Strings 505.1–105
- Hash 505.2–32
- 505.3–35-36
- 505.4–38, 51-52, 158
- Health Certificate 505.4–70
- Hibernation 505.3–170, 179
- High-Value Target 505.2–9, 132-133
- 505.4–85
- HIPS 505.2–34
- HSM 505.3–49, 62, 99
- Hyper-V 505.1–117

I

- I8 .... 505.2–78-79
- IAS 505.4–175-177
- ICA 505.1–109, 110
- iDRAC 505.2–35
- IDS/IPS 505.2–13
- IETF 505.3–9, 43
- IFilter 505.5–218-219
- IIS 505.3–11, 16, 18, 127
- 505.5–38-39
  - Services Not Required 505.5–29-30
  - Services Required 505.5–31
- IKE .... 505.4–42, 47, ? 49-55, 71
- ILM 505.5–134
- iLO 505.2–35
- ILT 505.1–67
- Immunity Canvas 505.1–77
- Incognito 505.2–29
- INF 505.1–15, 105

- 505.5–22-24
- Initial Soft Target 505.2–11
- Installation Disk Image 505.2–149
- Integrity Control Tools 505.2–58
- Integrity Labels 505.2–54
- Interactive Logon 505.2–30, 35, 38
- Internet Explorer 505.1–85
  - 505.5–51
  - Certificates 505.3–108
  - Enhanced Protected Mode 505.1–132-134
  - Hardening 505.1–130-131
  - Protected Mode 505.1–134
  - SmartScreen Filter 505.1–135
  - XSS Filter 505.1–135
  - Zones 505.1–136-140
- IPSec 505.1–31
  - 505.2–17, 51, 90
  - 505.3–35
  - Definition 505.3–10
  - Overview 505.4–36-42
  - Advanced Options – Phase I & II 505.4–64-67
  - AH/ESP Differences 505.4–? 59
  - Authentication Options 505.4–68-74
  - Benefits 505.4–38-41
  - Channel 505.4–71
  - Command-Line Tools 505.4–92
    - Dynamic/Static Mode 505.4–93
  - Connection Security Rules 505.4–75-83
    - Precedence 505.4–81
  - Default Settings 505.4–62-63
  - DNSSEC 505.4–128
  - Drawbacks 505.4–41
  - Encapsulating Security Payload 505.4–56-59
  - Flooding 505.4–42
  - Hardening 505.5–121-123
  - Internet Key Exchange 505.4–? 49-55
  - Modes (AH/ESP) 505.4–56-59
  - Modes (Phases) 505.4–52
  - Negociation 505.4–51-52
  - Null Encapsulation 505.4–60-61
  - Order Of Specificity 505.4–82
  - Policy 505.4–81, 90
    - Rules → Connection Security Rules
    - Rules Priority 505.4–? 81
    - Scripting 505.4–92-95
  - Port Permissions 505.2–19-20
  - Protocols 505.4–47-48
  - Requiring 505.4–45
  - Scenarios And Uses 505.4–43-46
  - Tools 505.4–15-20
  - Tunneling 505.4–? 80-81
  - Windows Firewall 505.4–39
  - Wireless 505.4–44
- IPv6 505.5–89-92
- IronKey 505.2–88
- ISAKMP 505.4–50-53
- IT Authority Delegation 505.2–132

J

- Java 505.1–158-166
  - Configuration Files 505.1–164
  - Control Panel 505.1–160
  - Deployment Rule Sets 505.1–165
  - Editions 505.1–159
  - Security Levels 505.1–162
- Javascript 505.1–130, 144, 153, 154
- JScript 505.1–69, 96
  - 505.2–102

K

- KB
  - List Article Numbers (PowerShell) 505.2–170
- KeePass 505.2–88-90
- Kerberos 505.2–28, 32, 37, 39, 96, 126
  - 505.3–10, 134, 136-137
  - 505.4–38, 64, 68-70, 109
  - Armoring 505.5–114-116, 142, 158, 160
  - Compound Authentication 505.5–158-162, 172
    - Enable 505.5–160
    - Restrictions 505.5–161
  - Hardening 505.5–114-116
  - Ticket 505.5–158
  - Vs NTLM 505.5–110-111
- Kernel Mode 505.2–33
- Key 505.3–31-35
  - 505.5–? 102
  - Master 505.3–91
    - 505.4–64, 71
  - Preshared 505.4–71-72
  - Private 505.3–33, 87-90, 94-95, 98, 111
  - Protection 505.3–112
  - Recovery Procedure 505.3–113
  - Session 505.3–33, ? 91, 104
  - System 505.3–91, 100
- KVMoIP 505.2–35
  - 505.3–101

L

- LDAP 505.1–39
  - 505.2–72, 100, 103
  - 505.3–11
  - 505.4–24
- LDF 505.2–77, 79
  - Provided File 505.2–77
- LLMNR 505.4–101-103, 130, 188
- Local Policies 505.1–17
- Lockout Policies 505.2–? 66-69, 74
  - 505.3–67, 138
  - Screensaver Password 505.2–? 68
- Logon/Logoff Scripts 505.1–72
- Low Integrity Level 505.1–133, 150, 153, 168
- LSA 505.5–191, 204
  - Secrets 505.2–14, 17, 34

505.3–95, 104
505.5–34

M

Malware Analysis Lab 505.4–9
Malware Automation Tools 505.1–77
Man-In-The-Middle Attack 505.4–54, 71, 102, 119
505.5–97, 103, 105, 109-110, 114
Master Key → Key
Maximum Wait Time 505.1–? 73
MBSA 505.2–169-170
MDOP 505.1–35
505.3–156
MDT 505.2–148
Metasploit 505.1–77, 145
505.2–30, 32
Metro IE 505.1–? 132
MIC 505.1–134
505.2–53, 56-61, 90
  Labels 505.2–56-58
Microsoft Critical Patches 505.2–142
Microsoft Office 505.1–167-170
Migration Tools 505.2–101
MKPK 505.3–91-92
MMC 505.1–24, 85
505.2–35
  AD Domains & Trusts Snap-in 505.5–128
  AD Snap-ins 505.2–98
  Certificate Templates Snap-in 505.3–77, 128
  Certificates Snap-in 505.3–13, 25, 28, 113, 117, 148
505.4–163
  Certification Authority Snap-in 505.3–13, 123, 128
  DHCP Snap-in 505.4–110
  DNS Snap-in 505.4–104, 136
505.5–78
  File Server Resource Manager Snap-in 505.5–145
  Internet Authentication Service Snap-in 505.4–175
  IP Security Monitor Snap-in 505.4–16, 81
  IP Security Policies Snap-in 505.4–17, 89
  Network Policy Server Snap-in 505.4–148, 211
  Online Responder Snap-in 505.3–129, 132
  RDS Host Config Snap-in 505.5–108-110
  Register Snap-in DLL 505.2–100
  Security Config & Analysis Snap-in 505.1–? 24
505.5–23
  Security Templates Snap-in 505.1–15
505.5–23
  Services Snap-in 505.4–192
  Task Scheduler Snap-in 505.5–57
  TPM Management Snap-in 505.3–142
  Windows Firewall Snap-in 505.4–15, 33, 76, 81
Model → Biba, DoD, Web-of-Trust
MPPE 505.4–167-168
MSA 505.5–37-38
MSDE 505.2–152, 157
MSI 505.1–31, 122, 149, 152, 170
505.2–47, 103, 152, 163-164, 171
Multilink 505.4–170

N

NAC 505.2–175-176
NAP 505.2–175
505.4–70, 150
NAT 505.4–40, 47-48
NDS 505.2–72
NetBIOS 505.1–144
505.4–188
  Disable 505.4–97-103
505.5–83-86
NetBT 505.4–98-99
505.5–83-85
Netcat 505.4–33
Network Access Control 505.2–175-176
Network Bridging 505.4–182-183
Network Logon 505.2–30, 34, 126
Network Unlock 505.3–183-185
NIST 505.1–20
505.3–9
NLA 505.4–24-25
505.5–110
Nmap 505.2–174
505.4–185
No Read/Write/Execute 505.2–59
Non-Repudiation 505.3–30
NPS 505.4–147-150, 505.4–173
  Certificates 505.4–163
  Client 505.4–149
  Clients 505.4–196
  Configuration 505.4–173-177
  Network Policies 505.4–151-156
    Constraints 505.4–157-158, 165-168
    Settings 505.4–169-172
NRPT 505.4–102, 126, 128
NTFS 505.1–94, 134
505.2–22, 26, 48, 58
505.3–11
  File System Permissions 505.1–? 18
  Last Access Timestamps 505.5–79
NTLM 505.2–32, 39, 96, 126
505.4–55, 64, 68
  Auth Restriction (Hardening) 505.5–117-120
  Authentication (v2) 505.5–239-248
  Vs Kerberos 505.5–110-111
NTP 505.3–51
505.5–77
Nuke From Orbit 505.1–115
Null Session 505.5–58, 249

O

OAKLEY 505.4–53
OCSP 505.3–50, 60, 127-132
OllyDbg 505.2–31

Opera 505.5–51
OU Admins 505.2–130, 132-133
Outlook 505.1–61

P

PAC 505.5–158-162
Pass-the-hash 505.2–31-32, 47, 133
  Mitigation 505.2–33-39
Password Managers 505.2–88
Password Safe 505.2–88
Password/Passphrase Policy 505.2–63, 65, 74, 81, 83
  505.3–67, 179
  Filters 505.2–72-73
  Length VS Complexity 505.2–70-73
Passwords Management 505.1–65
Patch Management 505.2–141
  Tools 505.2–149, 160, 163, 168, 171
Patch Manager 505.2–162
PCoIP 505.1–110
PCR 505.3–156
PDC Emulator 505.2–109
  505.3–51
PE 505.2–54
PE Header 505.1–128
PEAP 505.3–11
Perfect Forward Secrecy → PFS
Performance Monitor 505.4–106, 135
Perl 505.1–96
  505.2–102, 114
PFS 505.4–? 65
  505.5–? 102
PFX 505.3–18
PGP 505.3–43, 54
  505.4–? 36-37
Picture Password 505.2–80-84
PIN 505.2–80-84
  505.3–10
PK 505.3–157-158
PKCS 505.3–19, 22, 68, 70, 91-92, 113
  Message Types 505.3–40
PKI 505.1–31
  505.3–37, 43, 49, 87
  Auto-Enrollment 505.3–107-110
  505.4–163
  Certificate Enrollment 505.3–81-85
  Certificate Renewal 505.3–? 28
  Certificate Services → Active Directory
  Certificate Stores 505.3–22-23, 117
  Certificate Structure 505.3–43-45
  Certificate Templates 505.3–77-80
    Built-in 505.3–83
    Cross-Forest Replication 505.3–80
  Certificate Wizards 505.3–26
  Custom Applications 505.3–12, 19
  Definition And Characteristics 505.3–8-9
  Enrollment Agent 505.3–146-152
  Hierarchy Design 505.3–? 53-58
  Policy Module → Active Directory
  Private Key Archival 505.3–78, 111-113
  Protected Stores 505.3–23
  Standards 505.3–9
  Tools 505.3–13-24
  Web Enrollment Support 505.3–15
PolicyPak 505.1–37
Pooled VM 505.1–118
Port Numbers 505.2–? 103
  505.5–48
  IPSec 505.4–74
  LDAP 505.2–103
  LLMNR 505.4–101
  NetBIOS 505.4–100
  Querying Group Memberships On DC 505.4–74
  RADIUS 505.4–171
  RDP 505.5–105, 107-108
  SMB 505.5–93
Power 505.2–13, 133
PowerShell 505.1–13, 35, 69, 88, 95, 97, 120, 164
  505.2–28, 75, 92, 100, 160, 170
  505.3–19, 505.3–177
  505.4–15, 92, 106, 185
  Provided Scripts 505.2–35, 94-95
  505.4–106, 132
  505.5–32
PPTP 505.4–167-168
Privileges 505.2–22-24
  Maleficent Seven 505.2–25-26
Process Explorer 505.2–54, 57
Process Hacker 505.1–127, 128
  505.2–22, 57
Process Monitor 505.2–48
Proposed Permissions 505.5–? 214-216
Protected Users 505.2–39
Protected View 505.1–155, 167
Protocol Transition 505.5–142, 160
PSK 505.4–143
Python 505.1–96

R

RADIUS 505.2–13, 19, 65-66
  505.4–145, 505.4–173
  Account Lockout 505.4–215
  Benefits 505.4–145-146
  Clients 505.4–196
  NPS 505.4–147-150
  Policies 505.4–151-156
RDP 505.1–109, 110, 117
  505.2–20, 26, 30, 32, 33, 35, 51
  Description 505.5–105-113
  Hardening 505.5–105-113
  Thin Client 505.5–111
  With TLS 505.5–103
RDS 505.5–105-107
RDS Server 505.1–109, 117, 118
Removable Devices 505.1–102, 104-105, 106-107

- Requested Execution Level 505.2–54
- Resource Kit 505.1–58
  505.3–16-18, 20
  505.4–40, 106, 155
  505.5–51
- Resource Properties 505.5–178-182
  - Lists 505.5–? 181
  - Reference 505.5–180
  - Suggested Values 505.5–? 179
- RMS 505.5–236
- Roaming 505.1–111, 118, 148, 152
  505.2–85-86, 88
  505.3–9, ? 87, 93, 100, 111, 114
  505.4–24, 46, 77, 131-132
- Rogue Computer 505.2–173-174
- Rootkit 505.2–25, 47
  505.3–178
- RPC 505.2–126
- RRAS 505.3–11
- RSA 505.3–32-33, 62, 158
  505.4–73
- RSAT 505.1–32, 63
  505.2–100
- Runhash 505.2–32
- Running As ... 505.2–53

S

- S/MIME 505.3–10
- S4U2Self 505.5–160
- SA 505.4–? 49-52
- SAM 505.2–32
  505.4–173
- Sandbox 505.1–112, 150
- SAT 505.1–150, 153, 168
  505.2–15, 16, 22, 53, 57, 63, 136
  505.5–204
  - Definition 505.2–27-28
  - Delegation 505.2–28, 34
  - Exposure 505.2–25-26, 34, 94
  - Impersonation 505.2–28
  - Labels 505.2–57
- SCA databases 505.1–? 24
- SCADA 505.2–10
- SCCM 505.1–152
  505.2–149, 171
- SCEP 505.3–20, 60
- SCM 505.1–21
- Script Center 505.2–160
  505.3–75
- SCW 505.5–18-19, 23
- SDK 505.5–51
- SDN 505.4–8
- Secunia PSI 505.2–165, 505.2–167-168
- Secure Boot 505.2–34, 82
  505.3–98, 505.3–160
- Secure E-Mail 505.3–10
- Securing The Human 505.1–103
- Security Association → SA
- Security Awareness 505.1–102-103
- Security Guide 505.1–131, 167, 170
- Security Templates 505.1–15-23
  505.5–22-24
  - Available 505.1–20-21
  - By Hand 505.1–186-191
  - Incremental 505.1–25
  - Permissions 505.1–18-19
- Security Websites 505.5–10
- Security Zone 505.4–85-88
  - IP Addressing Scheme 505.4–86-87
- SEHOP 505.1–125, 128-129, 153
- Server Installation 505.5–41-48
  - Core 505.5–41-48
  - Full 505.5–45-46
  - Minimal 505.5–45-46
- Server Manager 505.5–12-14
  - Roles & Features 505.1–117
    505.2–98, 150, 153, 157
    505.3–59-60, 76
  - Scripting 505.5–16-17
  - Services 505.5–94
- Service 505.5–33
  - Account 505.5–33-40
    - Global 505.5–34
    - Step-By-Step Guide 505.5–37
  - Compromission 505.5–35
  - Identity Preference List 505.5–33
  - Recovery 505.5–31-32
- SharePoint 505.5–236
- Shatter Attack 505.2–59
- SID 505.2–18, 27, 53, 57, 81
  505.3–88
  - Well-Known 505.1–190-191
- SIEM 505.5–76
- SKEME 505.4–53
- Smart Card/Token 505.2–51
  505.3–87, 133-137
  - Overview 505.2–21
  - Certificate Templates 505.3–? 146
  - Kerberos Combined 505.3–? 136-137
  - PIN Management & Crypto HW 505.3–138-140
  - Removal 505.3–? 147
  - Smart Cards Deployment 505.3–146-152
  - Support 505.3–10
  - TPM Virtual Smart Card 505.3–141-145
- SMB 505.2–16, 27, 90, 95
  505.4–? 97-98, 100
  - Description 505.5–93
  - Encryption 505.5–94, 96
  - Hardening 505.5–93-98
  - Message Signing 505.5–97
- Social Engineering 505.1–180-185
  505.2–11, 68
- SoftGrid 505.1–112
- Software Restriction → AppLocker
- Solution Accelerator 505.2–149

Specops 505.1–37
SplashID 505.2–88
SSH 505.4–37
SSL/TLS 505.3–11-12
505.4–36-37
505.5–99-100
Cipher Suite Order 505.5–101-103
Hardening 505.5–99-104
SSPI 505.3–9
Startup/Shutdown Scripts 505.1–73
505.2–94
Station Hop 505.3–147
SteadyState 505.1–112
Streaming 505.1–109, 113
Stunnel 505.4–37
Stuxnet 505.1–77, 101
Suggested Values → Resource Properties
System Restore/Protection 505.5–80
SYSVOL 505.1–57, 59, 65, 73, 164
505.2–94, 159

T

Task Manager 505.1–88
Task Scheduler 505.1–85
TBS 505.3–142
TDSS Rootkit 505.4–132
TGT 505.2–37, 39
505.5–114, 505.3–136-137
Thin-Client 505.4–11
Thumbprint 505.3–? 45
TMG 505.3–11
Token Abuse/Stealing 505.2–29, 133
Mitigation 505.2–33-39
TPM 505.2–82
505.3–98, 141, 154-158
Trust Anchor 505.4–117
Trust Level 505.2–54
Trusted Signing Certificate 505.1–165
TTL 505.3–64

U

UAC 505.1–134
505.2–32, 49, 50, 52-55, 90
505.3–178
UAG 505.3–11
UIPI 505.2–59
Ultimate Goal 505.2–10
UPD 505.1–118
Update Cycle 505.2–142-143
USB Boot 505.1–111
User Profile 505.3–88
User Profile Disk 505.1–118
User Rights 505.2–16-18, 22

V

VBScript 505.1–69, 96
505.2–101-102, 114, 160
505.3–75
VDI 505.1–109, 114, 117
505.2–51, 505.5–106
VerySign 505.3–41-42, 57, 117
505.4–69
VHDX 505.1–118
505.3–180
Virtual Desktop Infrastructure 505.1–109-113
Advantages/Disadvantages 505.1–114-116
Deployment 505.1–117-118
VMK 505.3–? 157-158
VMWare 505.1–110
VNC 505.2–35
Volume Shadow Copy 505.5–80
VPN 505.2–13, 19, 505.2–165-166
505.3–11
505.4–11-12, 37, 41, 57, 149, 188-189
VSA 505.5–35, 38-40

W

WDS 505.2–? 148-150
Web Proxy 505.1–143
Web-of-Trust Model 505.3–54
WEP 505.4–207
Whois Lookup 505.4–136
WinAPI 505.2–99
Windows Credentials Editor 505.2–32
Windows Explorer 505.1–85
505.3–168-169
505.5–145
Windows Firewall 505.4–21-22, 25, 100
505.5–58
Connection Security Rules 505.4–75-83
Default Settings 505.4–? 27-29
Hardening 505.5–121-123
Logging 505.5–78
Network Profiles 505.4–23-26
Policy Scripting 505.4–92-95
Rule Precedence 505.4–34
Tools 505.4–? 15-20
Windows Recovery Environment 505.1–111
Windows Script Host 505.1–70, 96
Windows To Go 505.1–110
505.3–170
Windows Update Catalog 505.2–153
WinRT 505.2–15, 98
505.4–31
WINS Server 505.1–144
505.4–97
Wireless
802.11 505.4–205
Access Points – Rogue & Public 505.4–183-189
Client Configuration 505.4–178-180
DoS Attack Vulnerabilities 505.4–141-142
EAP 505.4–159-160, 162

- EAP-TLS & Smart Card Support ..505.4–162-164
- Infrastructure/Ad Hoc Mode 505.4–206
- PEAP 505.4–160-161, 163, 171-177
- Pre-Shared Key Issues 505.4–143-144
- Tunneled TLS 505.4–192

WLBS 505.2–160

WMI 505.1–52, 121, 164
- 505.2–36, 173-174
- 505.3–164
- 505.4–106

WPA/WPA2 ....505.4–? 208

WPAD 505.4–11, 505.1–143
- Attack 505.1–145
- Hardening 505.1–146-148

WQL 505.1–53

WSUS 505.2–151-156
- API 505.2–160
- Client Administration ....505.2–? 159-161
- Console 505.2–157-158
- Disappointments 505.2–162-164
- Requirements 505.2–157
- Tools 505.2–160

`WUAU.ADM` 505.2–159

X

XML 505.1–122
- 505.5–22-24

XMLLite 505.2–45, 92

Z

ZAP 505.1–31