# Advanced Scan (Policy) - Win 7

## Vulnerabilities by Host

# Vulnerabilities by Host

# 10.0.2.245

| | | | | |
|---|---|---|---|---|
| **3** | **5** | **9** | **1** | **36** |
| CRITICAL | HIGH | MEDIUM | LOW | INFO |

Vulnerabilities                                                                 Total: 54

| SEVERITY | CVSS V3.0 | PLUGIN | NAME |
|---|---|---|---|
| CRITICAL | 9.8 | 125313 | Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check) |
| CRITICAL | 9.8 | 108797 | Unsupported Windows OS (remote) |
| CRITICAL | N/A | 53514 | MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check) |
| HIGH | 8.8 | 79638 | MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check) |
| HIGH | 8.1 | 97833 | MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check) |
| HIGH | 7.5 | 35291 | SSL Certificate Signed Using Weak Hashing Algorithm |
| HIGH | 7.5 | 42873 | SSL Medium Strength Cipher Suites Supported (SWEET32) |
| HIGH | N/A | 58435 | MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check) |
| MEDIUM | 6.8 | 90510 | MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check) |
| MEDIUM | 6.5 | 51192 | SSL Certificate Cannot Be Trusted |
| MEDIUM | 6.5 | 104743 | TLS Version 1.0 Protocol Detection |
| MEDIUM | 5.9 | 65821 | SSL RC4 Cipher Suites Supported (Bar Mitzvah) |
| MEDIUM | 5.3 | 57608 | SMB Signing not required |
| MEDIUM | 4.0 | 58453 | Terminal Services Doesn't Use Network Level Authentication (NLA) Only |

| | | | |
|---|---|---|---|
| MEDIUM | N/A | 18405 | Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness |
| MEDIUM | N/A | 57582 | SSL Self-Signed Certificate |
| MEDIUM | N/A | 57690 | Terminal Services Encryption Level is Medium or Low |
| LOW | N/A | 30218 | Terminal Services Encryption Level is not FIPS-140 Compliant |
| INFO | N/A | 10114 | ICMP Timestamp Request Remote Date Disclosure |
| INFO | N/A | 45590 | Common Platform Enumeration (CPE) |
| INFO | N/A | 10736 | DCE Services Enumeration |
| INFO | N/A | 54615 | Device Type |
| INFO | N/A | 35716 | Ethernet Card Manufacturer Detection |
| INFO | N/A | 86420 | Ethernet MAC Addresses |
| INFO | N/A | 53513 | Link-Local Multicast Name Resolution (LLMNR) Detection |
| INFO | N/A | 10785 | Microsoft Windows SMB NativeLanManager Remote System Information Disclosure |
| INFO | N/A | 26917 | Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry |
| INFO | N/A | 11011 | Microsoft Windows SMB Service Detection |
| INFO | N/A | 100871 | Microsoft Windows SMB Versions Supported (remote check) |
| INFO | N/A | 106716 | Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check) |
| INFO | N/A | 11219 | Nessus SYN scanner |
| INFO | N/A | 19506 | Nessus Scan Information |
| INFO | N/A | 24786 | Nessus Windows Scan Not Performed with Admin Privileges |
| INFO | N/A | 11936 | OS Identification |
| INFO | N/A | 117886 | OS Security Patch Assessment Not Available |
| INFO | N/A | 66334 | Patch Report |
| INFO | N/A | 66173 | RDP Screenshot |
| INFO | N/A | 56984 | SSL / TLS Versions Supported |

| INFO | N/A | 10863 | SSL Certificate Information |
|------|-----|-------|---------------------------|
| INFO | N/A | 70544 | SSL Cipher Block Chaining Cipher Suites Supported |
| INFO | N/A | 21643 | SSL Cipher Suites Supported |
| INFO | N/A | 57041 | SSL Perfect Forward Secrecy Cipher Suites Supported |
| INFO | N/A | 51891 | SSL Session Resume Supported |
| INFO | N/A | 96982 | Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check) |
| INFO | N/A | 11153 | Service Detection (HELP Request) |
| INFO | N/A | 25220 | TCP/IP Timestamps Supported |
| INFO | N/A | 110723 | Target Credential Status by Authentication Protocol - No Credentials Provided |
| INFO | N/A | 64814 | Terminal Services Use SSL/TLS |
| INFO | N/A | 10287 | Traceroute Information |
| INFO | N/A | 35711 | Universal Plug and Play (UPnP) Protocol Detection |
| INFO | N/A | 135860 | WMI Not Available |
| INFO | N/A | 35712 | Web Server UPnP Detection |
| INFO | N/A | 10150 | Windows NetBIOS / SMB Remote Host Information Disclosure |
| INFO | N/A | 10940 | Windows Terminal Services Enabled |