



# Windows XP

Report generated by Nessus™

Mon, 29 Jan 2024 11:23:19 CET

---

## TABLE OF CONTENTS

---

### Vulnerabilities by Host

- 192.168.200.200.....4

Nessus Essentials

---

## **Vulnerabilities by Host**

---

192.168.200.200



## Vulnerabilities

Total: 30

| SEVERITY | CVSS V3.0 | VPR SCORE | PLUGIN | NAME  |
|----------|-----------|-----------|--------|---|
| CRITICAL | 9.8       | 9.2       | 34477  | MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (ECLIPSEDWING) (uncredentialed check)  |
| CRITICAL | 10.0      | -         | 73182  | Microsoft Windows XP Unsupported Installation Detection   |
| CRITICAL | 10.0      | -         | 108797 | Unsupported Windows OS (remote)   |
| CRITICAL | 10.0*     | 7.4       | 35362  | MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check)   |
| HIGH     | 8.1       | 9.7       | 97833  | MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check) |
| HIGH     | 7.3       | 6.6       | 26920  | SMB NULL Session Authentication   |
| MEDIUM   | 5.3       | -         | 57608  | SMB Signing not required  |
| INFO     | N/A       | -         | 10114  | ICMP Timestamp Request Remote Date Disclosure   |
| INFO     | N/A       | -         | 45590  | Common Platform Enumeration (CPE)   |
| INFO     | N/A       | -         | 54615  | Device Type   |
| INFO     | N/A       | -         | 35716  | Ethernet Card Manufacturer Detection  |
| INFO     | N/A       | -         | 86420  | Ethernet MAC Addresses  |
| INFO     | N/A       | -         | 10397  | Microsoft Windows SMB LanMan Pipe Server Listing Disclosure   |
| INFO     | N/A       | -         | 10785  | Microsoft Windows SMB NativeLanManager Remote System Information Disclosure   |

|      |     |   |                        |   |
|------|-----|---|------------------------|---|
| INFO | N/A | - | <a href="#">26917</a>  | Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry    |
| INFO | N/A | - | <a href="#">11011</a>  | Microsoft Windows SMB Service Detection                                       |
| INFO | N/A | - | <a href="#">100871</a> | Microsoft Windows SMB Versions Supported (remote check)                       |
| INFO | N/A | - | <a href="#">106716</a> | Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)             |
| INFO | N/A | - | <a href="#">11219</a>  | Nessus SYN scanner  |
| INFO | N/A | - | <a href="#">19506</a>  | Nessus Scan Information   |
| INFO | N/A | - | <a href="#">24786</a>  | Nessus Windows Scan Not Performed with Admin Privileges                       |
| INFO | N/A | - | <a href="#">10884</a>  | Network Time Protocol (NTP) Server Detection                                  |
| INFO | N/A | - | <a href="#">11936</a>  | OS Identification   |
| INFO | N/A | - | <a href="#">117886</a> | OS Security Patch Assessment Not Available                                    |
| INFO | N/A | - | <a href="#">96982</a>  | Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)  |
| INFO | N/A | - | <a href="#">25220</a>  | TCP/IP Timestamps Supported   |
| INFO | N/A | - | <a href="#">110723</a> | Target Credential Status by Authentication Protocol - No Credentials Provided |
| INFO | N/A | - | <a href="#">10287</a>  | Traceroute Information  |
| INFO | N/A | - | <a href="#">135860</a> | WMI Not Available   |
| INFO | N/A | - | <a href="#">10150</a>  | Windows NetBIOS / SMB Remote Host Information Disclosure                      |

\* indicates the v3.0 score was not available; the v2.0 score is shown