



## windows 10 single host

---

Report generated by Nessus™

Thu, 19 May 2022 13:24:42 India Standard Time

---

---

TABLE OF CONTENTS

---

**Vulnerabilities by Host**

- 192.168.1.101.....4

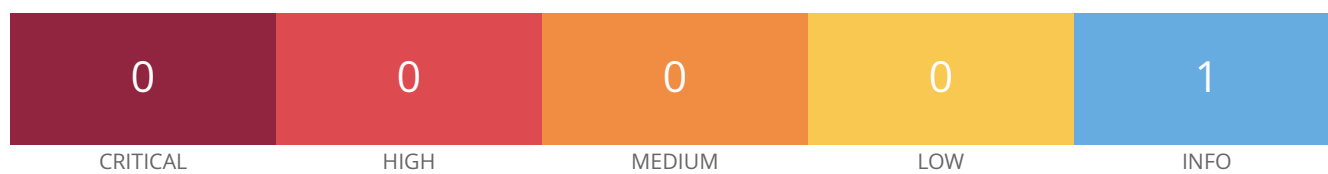
---

## **Vulnerabilities by Host**

---

---

**192.168.1.101**



---

## Scan Information

Start time: Thu May 19 13:17:12 2022  
End time: Thu May 19 13:24:41 2022

---

## Host Information

Netbios Name: DESKTOP-0N46D3D  
IP: 192.168.1.101  
MAC Address: 80:2B:F9:8C:E6:2F 00:0C:29:07:AC:A3  
OS: Microsoft Windows 10 Pro

---

## Vulnerabilities

**110723 - Target Credential Status by Authentication Protocol - No Credentials Provided**

---

### Synopsis

Nessus was able to find common ports used for local checks, however, no credentials were provided in the scan policy.

---

### Description

Nessus was not able to successfully authenticate directly to the remote target on an available authentication protocol. Nessus was able to connect to the remote port and identify that the service running on the port supports an authentication protocol, but Nessus failed to authenticate to the remote service using the provided credentials. There may have been a protocol failure that prevented authentication from being attempted or all of the provided credentials for the authentication protocol may be invalid. See plugin output for error details.

Please note the following :

- This plugin reports per protocol, so it is possible for valid credentials to be provided for one protocol and not another. For example, authentication may succeed via SSH but fail via SMB, while no credentials were provided for an available SNMP service.
- Providing valid credentials for all available authentication protocols may improve scan coverage, but the value of successful authentication for a given protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol. For example, successful authentication via SSH is more valuable for Linux targets than for Windows targets, and likewise successful authentication via SMB is more valuable for Windows targets than for Linux targets.

## Solution

---

n/a

## Risk Factor

---

None

## References

---

XREF IAVB:0001-B-0504

## Plugin Information

---

Published: 2018/06/27, Modified: 2021/11/19

## Plugin Output

---

tcp/0

```
SMB was detected on port 445 but no credentials were provided.  
SMB local checks were not enabled.
```