Basic Vulnerability Scan Report

1. System Information

Property	Value
OS Name	Microsoft Windows 10 Pro
OS Version	10.0.26100.4061
IP Address	192.168.14.221

2. Method Used

- Manual scan conducted without third-party tools.
- Commands used:
  - `ipconfig` (for IP and network information)
  - `systeminfo` (for OS information)
  - `netstat -an | find "LISTEN"` (to identify open ports)
  - PowerShell (optional): `Get-NetTCPConnection`
- Identified open TCP ports and linked them with known vulnerabilities (CVEs) for assessment.

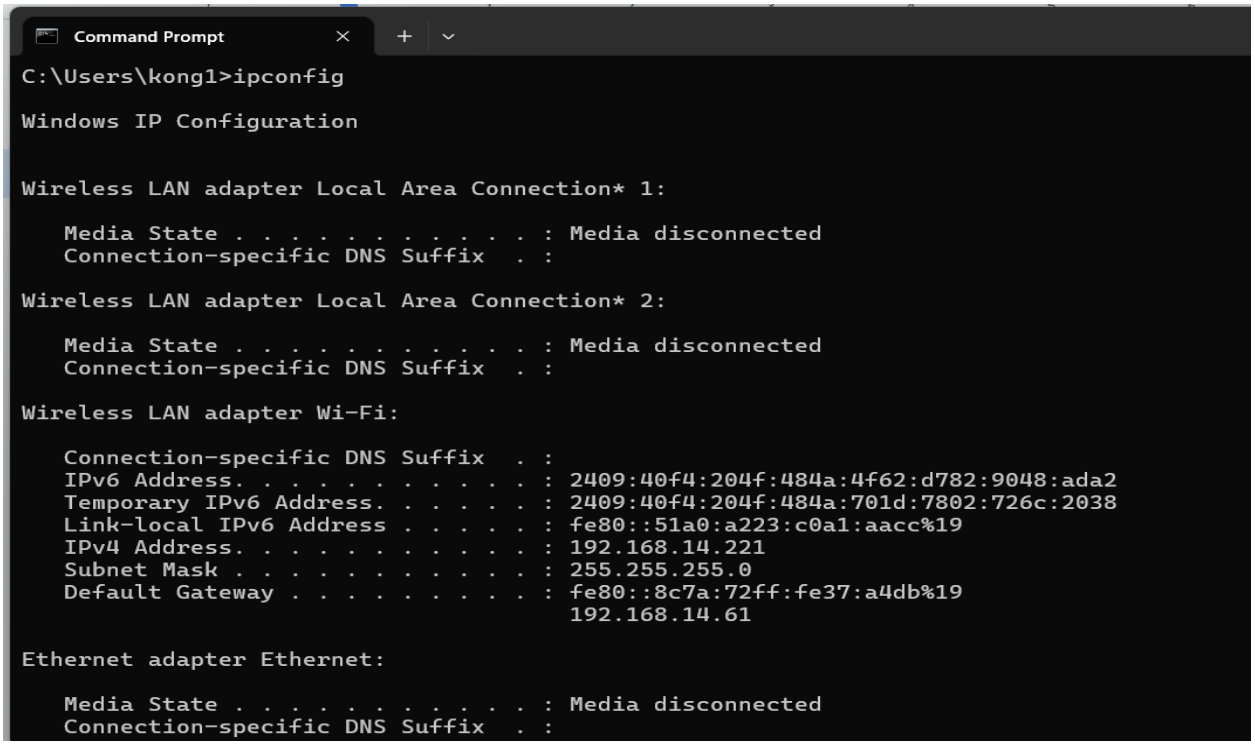
3. Findings

Port	Protocol	Description	Risk Level	Recommendation
135	TCP	Microsoft RPC	Medium	Block from public networks

139	TCP	NetBIOS Session Service	High	Disable if file sharing not required
445	TCP	SMB over TCP	High	Disable SMBv1, block externally
5040	TCP	DRM Media Sharing	Low	Disable if not used
6850	TCP	Unknown service	Medium	Investigate source and purpose
9012	TCP	Possibly custom app	Medium	Verify origin; restrict if unused
49664–49682	TCP	Dynamic RPC Ports	Medium	Restrict to local network if possible
1042, 1043, etc.	TCP	Loopback service ports	Low–Medium	Monitor for unexpected activity

4. Screenshots

`ipconfig` output



`netstat -an | find "LISTEN"` output

```
C:\Users\kong1>netstat -an | find "LISTEN"
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:6850           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:9012           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:9013           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:9014           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49673          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49674          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49675          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49676          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49677          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49678          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49679          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49680          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49681          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49682          0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1042         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1043         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:7778         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:11001        0.0.0.0:0              LISTENING
  TCP    127.0.0.1:13030        0.0.0.0:0              LISTENING
  TCP    127.0.0.1:13031        0.0.0.0:0              LISTENING
```

PowerShell output from `Get-NetTCPConnection`

```
LocalAddress                LocalPort RemoteAddress               RemotePort State       AppliedSetting
------------                --------- -------------               ---------- -----       --------------
::                          49675     ::                        0          Listen
::                          49668     ::                        0          Listen
::                          49667     ::                        0          Listen
::                          49666     ::                        0          Listen
::                          49665     ::                        0          Listen
::                          49664     ::                        0          Listen
::                          445       ::                        0          Listen
::                          135       ::                        0          Listen
127.0.0.1                   65001     0.0.0.0                   0          Listen
127.0.0.1                   61870     0.0.0.0                   0          Listen
127.0.0.1                   51100     0.0.0.0                   0          Listen
127.0.0.1                   50923     0.0.0.0                   0          Listen
127.0.0.1                   50100     0.0.0.0                   0          Listen
0.0.0.0                     49682     0.0.0.0                   0          Listen
0.0.0.0                     49681     0.0.0.0                   0          Listen
0.0.0.0                     49680     0.0.0.0                   0          Listen
0.0.0.0                     49679     0.0.0.0                   0          Listen
0.0.0.0                     49678     0.0.0.0                   0          Listen
0.0.0.0                     49677     0.0.0.0                   0          Listen
0.0.0.0                     49676     0.0.0.0                   0          Listen
0.0.0.0                     49675     0.0.0.0                   0          Listen
0.0.0.0                     49674     0.0.0.0                   0          Listen
0.0.0.0                     49673     0.0.0.0                   0          Listen
0.0.0.0                     49668     0.0.0.0                   0          Listen
```

5. References

- **CVE-2017-0144** – SMB Remote Code Execution (WannaCry):
  https://nvd.nist.gov/vuln/detail/CVE-2017-0144

- **NetBIOS/SMB Security Risks** – Microsoft Docs:

  https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-restrict-clients-allowed-to-make-remote-calls-to-sam

- **Hardening Windows Network Services** – OWASP Guide:
  https://owasp.org/www-project-wstg/

---

6. Conclusion

This basic vulnerability assessment using manual methods identified several open ports on the system, some of which are associated with known risks such as SMB (port 445) and NetBIOS (port 139). It is recommended to:

- Disable unused services,

- Block risky ports from external access,

- Regularly update the system,
- Use firewalls and endpoint protection tools.

This activity provided foundational experience in identifying network-related risks manually.