**Nmap Scan Report – 192.168.1.114**

**Scan Date:** June 15, 2025  
**Nmap Version:** 7.97  
**Target IP Address:** 192.168.1.114  
**Command Used:** nmap 192.168.1.114

**🖥️ Host Information**

* **Host Status:** Up
* **Latency:** 0.00020 seconds
* **Total Ports Scanned:** 65535
* **Closed Ports:** 65521 (reset)
* **Open/Filtered Ports:** 14 listed below

**📊 Open and Filtered Ports**

| **Port** | **State** | **Service** | **Description** |
| --- | --- | --- | --- |
| **135/tcp** | open | msrpc | Microsoft RPC (Remote Procedure Call) – used for DCOM services |
| **137/tcp** | filtered | netbios-ns | NetBIOS Name Service – filtered by firewall or not responding |
| **139/tcp** | open | netbios-ssn | NetBIOS Session Service – used for file/printer sharing |
| **445/tcp** | open | microsoft-ds | SMB over TCP – Windows file sharing (CIFS) |
| **5040/tcp** | open | unknown | Unidentified service – requires further investigation |
| **6850/tcp** | open | iccrushmore | Possibly a custom or non-standard application |
| **9012/tcp** | open | unknown | Unknown – non-standard or proprietary service |
| **9013/tcp** | open | unknown | Unknown – non-standard or proprietary service |
| **49664/tcp** | open | unknown | High port – likely dynamic or RPC-related |
| **49665/tcp** | open | unknown | High port – possibly part of RPC service range |
| **49668/tcp** | open | unknown | High port – typical of Windows dynamic RPC ports |
| **49669/tcp** | open | unknown | High port – dynamic or custom application |
| **49670/tcp** | open | unknown | High port – likely ephemeral |
| **49683/tcp** | open | unknown | High port – likely dynamic |

**🧠 Interpretation & Insights**

* **Windows Host Detected:**  
  The presence of ports 135, 139, 445, and dynamic RPC ports suggests the host is likely running **Microsoft Windows**.
* **NetBIOS/SMB Services Enabled:**  
  These are often used for **file sharing** and **remote management**, but can be security risks if exposed to untrusted networks.
* **Filtered Port (137):**  
  Indicates that the port is being **actively filtered** by a firewall or not responding to probes.
* **Unidentified Ports (5040, 9012–9013, 4966x+):**  
  These may be **custom services**, **ephemeral ports**, or **part of remote procedure call (RPC)** services. Further investigation or a version scan (nmap -sV) is recommended.

**🛡️ Recommendations**

1. **Restrict access** to SMB/NetBIOS ports (135, 139, 445) unless absolutely necessary.
2. Perform a **service/version detection scan** for unknown ports: nmap -sV 192.168.1.114
3. Use nmap -A or nmap -O to identify the **OS** and enable more detailed analysis.
4. Verify with the system administrator which services are expected, especially for ports like 5040, 9012, 49664, etc.
5. Ensure firewall rules are appropriately configured to block unnecessary access from external networks.

**📘 Further Steps**

* Run this command for detailed info: nmap -sV -p135,139,445,5040,6850,9012,9013,49664-49670 192.168.1.114
* Consider vulnerability scanning tools (e.g., **OpenVAS**, **Nessus**) if security auditing is required.