Nmap Scan Report for 192.168.50.1

Scan Date: 2025-06-23
Tool Used: Zenmap (Nmap GUI)
Command Executed:

```
bash
CopyEdit
nmap -sS -p- 192.168.50.1
```

Host Information

- **IP Address:** 192.168.50.1
- **Status:** Host is up
- **Scan Duration:** 6.18 seconds

Open Ports and Services

Port	State	Service
135/tcp	Open	msrpc
137/tcp	Filtered	netbios-ns
139/tcp	Open	netbios-ssn
445/tcp	Open	microsoft-ds
903/tcp	Open	iss-console-mgr
913/tcp	Open	apex-edge
4622/tcp	Open	Unknown
4623/tcp	Open	Unknown
5040/tcp	Open	Unknown
7070/tcp	Open	realserver
49664/tcp	Open	Unknown
49665/tcp	Open	Unknown
49666/tcp	Open	Unknown
49669/tcp	Open	Unknown
49670/tcp	Open	Unknown
49676/tcp	Open	Unknown

- **Total Open Ports Detected:** 16
- **Note:** 65,519 ports were closed (reset responses).

Network Configuration (from ipconfig)

Adapter	IPv4 Address	Subnet Mask
VMware Network Adapter VMnet1	192.168.50.1	255.255.255.0
VMware Network Adapter VMnet8	192.168.138.1	255.255.255.0

- The target IP `192.168.50.1` matches the VMware VMnet1 adapter, indicating the scan was likely conducted on a virtual host or isolated virtual network.

Observations

- Common Windows ports (135, 139, 445) are open, suggesting a Windows-based service or OS.
- Many high numbered ports (e.g., 49664–49676) are open but unrecognized, often used for dynamic or ephemeral port allocations.
- Some ports like 7070 (RealServer streaming media) indicate multimedia or legacy server components may be present.
- NetBIOS and RPC services are active, which can be security-relevant in vulnerability assessments.