|  | | | | | |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  | | | | | |  |  |  |  |  |
|  | | | | | |  |  |  |  |  |
|  | | | | | |  |  |  |  |  |
|  | | | | | |  |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Address** | **Port** | **Service** | **Purpose** | **Risk Level** |
| 192.168.1.X | 135/tcp | msrpc (Microsoft RPC) | Windows RPC for remote management | Moderate (often exploited in malware) |
|  | 139/tcp | netbios-ssn (NetBIOS) | Windows file/printer sharing | High (old and vulnerable) |
|  | 445/tcp | microsoft-ds (SMB) | Windows file sharing (SMB) | High (ransomware target) |
|  | 16992/tcp | amt-soap-http (Intel AMT) | Intel remote management (if not used, disable it) | Moderate to High (remote access risk) |