Microsoft http://www.iss.net/security\_center/advice/Exploits/Ports/groups/Microsof...

**advICE :Exploits :Ports :groups :**Microsoft



When you look at an installation of Windows (especially server-versions of Windows), you will find a number of ports open. Several of these are well-known ports, while others are dynamically assigned.

The dynamically assigned ports start at port 1024 and usually range up through roughly port 1100. The exact meaning of these can be obtained through the "endpoint mapper" at port 135.

**Basic Windows ports**

135 The "end-point mapper". RPC services are assigned other ports dynamically. When trying to connect to a service, you go throug this mapper to discover where it is located. The process works the same as on the UNIX RPC portmapper. A big difference is that a lot of services run on top of named pipes, which don't have a specific port.

137 NetBIOS name service. This is how NetBIOS-based services find each other. On a NetBIOS network, these names uniquely identify the machine and services running on the machine (and the IP address doesn't matter). Machines find each other either using broadcasts or looking them up in a centralized NetBIOS naming server (called a WINS server).

138 NetBIOS datagram service. This is primarily used for broadcasting information. It is primarily used by the SMB browser service that fills the information within the "Network Neighborhood" icon.

**Basic Services**

This section describes the ports that you would encounter when installing the basic services on WinNT Server. Note that virtually all Microsoft services require port 135 for remote administration.

|  |  |  |
| --- | --- | --- |
| 42 | For WINS replication. Remember that normal access to the WINS service is through port 137; this | |
|  | port is used for database replication. | |
| 1723 | PPTP (Microsoft's VPN solution). Note that this will also use IP protocol 47. | |

138 NetBIOS datagram service. This is primarily used for broadcasting information. It is primarily used by the SMB browser service that fills the information within the "Network Neighborhood" icon.

**Exchange Server**

This section describes the type of ports you might see in Micorosft's Exchange server. This is a huge e-mail server package.

Again note the heavy reliance upon port 135 for remote administration and RPC communication between server components.

102 X.400 MTA

110 POP3

119 NNTP

8/23/2009 2:40 PM1 of 3

Microsoft http://www.iss.net/security\_center/advice/Exploits/Ports/groups/Microsof...

143 IMAP4 389 LDAP 563 POP3 over SSL. 636 LDAP over SSL. 993 IMAP4 over SSL. 995 POP3 over SSL.

**NetMeeting**

Microsoft's NetMeeting is video-conferencing style software.

389 Internet Locator Server (ILS) using LDAP. 522 ULP (User Location Server), obsoleted by LDAP. ULP is only used by older version of

NetMeeting. 636 Secure LDAP over SSL 1503 T.120 teleconferencing protocol 1720 H.323 call setup 1731 Audio call control protocol

Dynamically assigned ports for call control and RTP transport of the data.

**Windows Media**

The Windows Media Server streams content over the web. This was formerly known as "NetShow" and uses the .asf file extension.

80 Can stream content over HTTP. 1755 Uses a TCP control connection on this port, as well as some UDP traffic. 7007 Encoder-to-server traffic. This allows an encoder (such as a system encoding live radio) to stream

content to the server, which then streams it out to clients.

Note that the UDP traffic may be carried over IP multicast.

**Terminal Server**

Microsoft's Terminal Server is a special version of WinNT Server that allows remote GUI access. It is essentially Microsoft's version of X Windows, but since the Win32 API isn't geared toward remote viewing, its bandwith requirements are higher. Clients are available for WinCE devices allow NC-style access.

|  |  |  |
| --- | --- | --- |
| 3389 1494 636 1503 1720 1731 | RDP client Citrix (ICA) client Secure LDAP over SSL T.120 teleconferencing protocol H.323 call setup Audio call control |  |
|  |  | 8/23/2009 2:40 PM |

2 of 3

Microsoft http://www.iss.net/security\_center/advice/Exploits/Ports/groups/Microsof...

Privacy Policy | Copyright Info

Dynamically assigned ports for call control and RTP transport of the data.

**Cluster Server**

Clustering is where multiple servers coordindate themselves into providing the same service so that if any server goes down, clients get uninterupted operation.

1717 Convoy

2504 WLBS

**Other**

593 Encapsulates the RPC 'end-point mapping' services within HTTP.

1477 MS SNA server

1478 MS SNA server

1. **q150543**
2. **q176466**
3. **q158623**
4. **q155831**

8/23/2009 2:40 PM3 of 3