

RE: scan of domain logon reveals unknown port

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2003-08/0135.html>

From: Bell, Stephen (*SBell_at_sla.com*)

Date: 08/18/03

Date: Mon, 18 Aug 2003 10:21:48 -0700

To: "Dan Larsen" <drlarsen77@hotmail.com>, <focus-ms@securityfocus.com>

The following information was extracted from MSKB 280132.

It explains what ports must be open in order for a member server to operate correctly.

In this scenario it is giving the ports thru a firewall, but that is basically what you are trying to achieve by locking down the ports on the server.

Port 1026 is used for AD logon and directory replication.

Cheers

Steve

Enable Windows 2000 Server-based computers to log on to the domain through the firewall by opening the following ports for inbound traffic:

53 (Transmission Control Protocol [TCP], User Datagram Protocol [UDP]) – Domain Name System (DNS).

80 (TCP) – Required for Outlook Web Access 5.5 access for communication between Exchange front-end and back-end servers.

88 (Transmission Control Protocol [TCP], UDP) – Kerberos authentication.

123 (TCP) – Windows Time Synchronization Protocol (NTP). Note that this is not necessary for Windows 2000 logon capability, but may be configured or required by the network administrator.

135 (TCP) – EndPointMapper.

389 (TCP, UDP) – Lightweight Directory Access Protocol (LDAP).

445 (TCP) – Server message block (SMB) for Netlogon, LDAP conversion and distributed file system (Dfs) discovery.

3268 (TCP) – LDAP to global catalog servers.

One port for the Active Directory logon and directory replication interface (universally unique identifiers [UUIDs]

12345678-1234-abcd-ef00-01234567cfff and

e3514235-4b06-11d1-ab04-00c04fc2dcd2), which is typically assigned port

1025 or 1026 during startup. This value is not set in the DSProxy or

System attendant (MAD) source code, so you must map the port in the

registry on any domain controllers that the Exchange 2000 computer must

SecurityFocus Microsoft: RE: scan of domain logon reveals unknown port

contact through the firewall to process logons, and then open the port on the firewall.

To map the port in the registry:

Start Registry Editor (Regedt32.exe).

Locate the following key in the registry:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NTDS\Parameters

On the Edit menu, click Add Value, and then add the following registry value:

Value Name: TCP/IP Port

Data Type: REG_DWORD

Radix: Decimal

Value: greater than 1024

Quit Registry Editor.

Make sure that the slash in "TCP/IP" is a forward slash, and that the value that you assign is greater than 1024, in decimal format. That number is the extra port that you need to open (TCP, UDP) on the firewall. Setting this registry value on every domain controller inside the firewall does not impact performance, and covers any logon request redirects that occur as a result of servers that are down, roles that change, or bandwidth needs.

NOTE: For the server inside the firewall to communicate back through the firewall to the external server, you also need to have ports 1024 through 65535 configured for outbound communications. Computers that initiate the communication through the firewall use a client-side port that is dynamically assigned and cannot be configured.

@hotmail.com]

Sent: Friday, August 15, 2003 3:22 PM

To: focus-ms@securityfocus.com

Subject: scan of domain logon reveals unknown port

Hello,

After having one of my fully patched Win2k/IIS5 web servers hacked, I had decided to enable Routing and Remote Access restricting only traffic to ports I determined were necessary.

After spending much time researching, I configured Routing and Remote Access only to find that when logging in using my Domain Administrator account, I was now greeted with a lengthy (approx 15 minute) delay at the "Loading your personal settings" window.

Rechecking my settings revealed no missed entries, so I decided to install

RE: scan of domain logon reveals unknown port

SecurityFocus Microsoft: RE: scan of domain logon reveals unknown port

Ethereal to find out exactly what was going on. Interestingly enough, I discovered that during the logon process there was some TCP communication between the Win2k DC / DNS server and the IIS web server on port 1026.

I enabled incoming and outgoing traffic for all packets originating from, or going to, port 1026 and my login delay is gone. However, I wasn't able to find anything anywhere explaining what this communication on port 1026 is for. Also, I would have expected it to be below the 1024 range.

Can anybody shed some light on what is going on here? I'd like to move ahead and lock down all my servers in a similar fashion, however I'd like to know what port 1026 is and if I can rely on that traffic always being on the same port. If not, I'm hoping to find out how I can configure Routing and Remote Access to allow proper communication with the DC.

Below is a list of the ports I have opened and what I believe their function is. I have configured the routing for all traffic to/from the ports listed.

Thanks for any help you can provide.

Regards,
Dan

21 TCP FTP
25 TCP SMTP
53 TCP UDP DNS
80 TCP HTTP
88 TCP UDP Kerberos Secure Authentication
135 TCP MS Networking
137 UDP MS Networking
138 UDP MS Networking
139 TCP MS Networking
389 TCP LDAP
443 TCP SSL
445 TCP NetBIOS over TCP/IP
464 TCP UDP Kerberos Password
3268 TCP MS Global Catalog
3269 TCP MS Global Catalog w/ LDAP/SSL
3389 TCP RDP
1026 TCP Unknown?

SecurityFocus Microsoft: RE: scan of domain logon reveals unknown port

Your network firewall and IDS products do not prevent Web application attacks - the most common form of online exploitation- resulting in Web defacement, data theft, sabotage and fraud.

KaVaDo is the only company that provides a complete suite of Web application security products.

Download a FREE whitepaper on "Security Policy Automation for Web Applications":<http://www.securityfocus.com/Kavado-focus-ms>

KaVaDo provides the first and only integrated Web application scanner and firewall security suite that prevent Web applications attacks, the most common form of online exploitation. Download a FREE whitepaper on Security Policy Automation for http://www.securityfocus.com/sponsor/KaVaDo_focus-ms_030818
