

Hack Attempt on Windows 2003 AD Native

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2004-11/1580.html

From: JJ (jj_at_stokes.net)

Date: 11/24/04

Date: Wed, 24 Nov 2004 10:45:08 -0600

Source IPs of machines trying to hack my servers...

80.108.107.98
216.104.175.22
216.60.115.194
65.92.174.189

My servers on the Internet are: 1 DC/Exchange 2003, Sharepoint Portal 2003, and File Server

Question to you guys...I have a network which I maintain...I review the logs every other day and noticed that those IPs above were attempting to hack into my servers which are on the Internet...

All my machines are Windows 2003.

The funny thing is that when I changed the PASSWORD and renamed the Administrator account (Domain Admin) – next day, from those source address they were attempting to connect again but using the NEW Admin account I created!

How are they finding out or enumerating the Admin account username – because I renamed it?!

Unfortunately...we do not have a firewall...getting it this weekend...but my question is not about this (I know I need to PUSH for a firewall ASAP).