

RE: Trace of 139 attack?

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2001-07/0182.html>

From: Nick Ferguson (N Ferguson@peregrineinc.com)

Date: 07/26/01

Message-ID: <43BEC9994C6AD411A3A50090277DE4F517F895@TCLNRAID>
From: Nick Ferguson <N Ferguson@peregrineinc.com>
To: "'stephen.pinto@paladion.net'" <stephen.pinto@paladion.net>
Subject: RE: Trace of 139 attack?
Date: Thu, 26 Jul 2001 10:44:46 -0700

info on locking admin account with passprop in ntreskit

http://support.microsoft.com/support/kb/articles/Q158/3/88.asp?LN=EN-US&FR=0&qry=q158388&rnk=1&src=DHCS_MSPSS_gn_SRCH&SPR=IIS

Passprop.exe Provides functionality not available in User Manager. Allows policies to force complex passwords that contain a mix of upper and lowercase letters and numbers or symbols, and the ability to lock out an administrator's account over the network, but still allowing an administrator to log on interactively on domain controllers.

Nick Ferguson

-----Original Message-----

From: Stephen Pinto [<mailto:stephen.pinto@paladion.net>]
Sent: Monday, July 23, 2001 3:54 PM
To: FOCUS-MS
Subject: FW: Trace of 139 attack?

Oh how idiot of me!!! it can be locked out but not " Disabled "

-----Original Message-----

From: Todd Schubert [<mailto:tschubert@jorycapital.com>]
Sent: Thursday, July 26, 2001 2:47 AM
To: 'stephen.pinto@paladion.net'; Patrik Birgersson
Cc: FOCUS-MS
Subject: RE: Trace of 139 attack?

This is not true. The Administrator account can be locked out if too many incorrect passwords are entered for it.

Todd Schubert
Information Technology Specialist

RE: Trace of 139 attack?

SecurityFocus Microsoft: RE: Trace of 139 attack?

Jory Capital Inc.
phone: 204.925.5215
fax: 204.942.0047
email: tschubert@jorycapital.com

-----Original Message-----

From: Stephen Pinto [mailto:stephen.pinto@paladion.net]
Sent: Monday, July 23, 2001 5:07 PM
To: Patrik Birgersson
Cc: FOCUS-MS
Subject: RE: Trace of 139 attack?

To add to Patrick

- 1) administrator account cannot be locked
- 2) Enable Auditing in your policies
- 3) Use some software(scheduler) to export your logs to some other machine or tape after a particular period of time.so that even if the hacker plans of deleting the logs he cannot do it. Best practice is to use a Dot Matrix printer to print the logs which is a bit expensive.

Usually if a attacker is doing a brute force on ur Server ur logs will get full. best solution is to use an IDS (snort which is free)
Try Firewall like checkpoint which has some authentication mechanism.
Better go to www.sans.org you will get lots of info.

Regards
Stephen Pinto
Security Consultant
Paladion Networks,
E-217, Tower-3, International InfoTech Park,
Vashi, Navi Mumbai,400703
Ph: +91 22 7812446 / 7812450/ 7892890
FAX: +91 22 7812140

-----Original Message-----

From: Patrik Birgersson [mailto:pbirgersson@telia.com]
Sent: Wednesday, July 25, 2001 12:34 AM
To: Eagle; focus-ms@securityfocus.com
Subject: SV: Trace of 139 attack?

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

You would like to use the Event Log.

There's an HOWTO at:

<http://support.microsoft.com/support/kb/articles/Q300/5/49.ASP>
(URL might be wrapped).

If this box of yours is a web server to the world, you should not use it as file server with NetBIOS shares 'n stuff. Use another box on a private network for that

RE: Trace of 139 attack?

SecurityFocus Microsoft: RE: Trace of 139 attack?

If your shares must be accessed from outside your office (like from another office or employees on the road) you should use some VPN solution that tunnels your NetBIOS traffic.

NetBIOS is inherently insecure and shall not be allowed from untrusted networks (you know – like the Internet).

If the server you're talking about is an Intranet server, then you might have a harder time disabling NetBIOS, especially if you got *old* clients (like Win95/98/ME/NTW) that doesn't utilize Kerberos for authentication.

However, regardless of the server is "inside" or "outside" and whether you restricted NetBIOS or not, your Security Log would fill up quickly if someone's bruteforcing an account. You should configure your machine so that it'll shut down if the security log fills up (this can be "dangerous" – you must of course maintain your logs carefully, otherwise your computer will shutdown "out of the blue" on day). You should also apply timed account lockouts if more than 5 (3 attempts with manual unlock if you're strict) failed login attempts has been made.

Patrik Birgersson

Security is not a product – it is a process

-----BEGIN PGP SIGNATURE-----

Version: PGP 7.0

iQA/AwUBO13GkB+A7LF3JdzkEQKcWgCg6x++IGX8tIRbjQOxyYL0n/e2q7Y AoJ3V
qpTAJ7IBSFICAoHKct3C+Axm

=qvIn

-----END PGP SIGNATURE-----

This e-mail and any attachments may contain confidential, privileged or proprietary information. If you are not the intended recipient, please notify the sender immediately by return e-mail, delete this e-mail (with any attachments) and destroy any copies. Any dissemination or use of this information by a person other than the intended recipient is unauthorized and may be illegal.

This email and any files transmitted with it are confidential and are intended solely for the use of the individual or entity to whom they are addressed. This communication represents the originator's personal views and opinions, which do not necessarily reflect those of the company. If you are not the original recipient or the person responsible for delivering the email to the intended recipient, be advised that you have received this email in error, and that any use, dissemination, forwarding, printing or copying of this email is strictly prohibited. If you received this email in error, please immediately notify the sender.

SecurityFocus Microsoft: RE: Trace of 139 attack?

- *Previous message:* Paul L Schmehl: "RE: Microsoft SMTP Service"
- *Maybe in reply to:* Eagle: "Trace of 139 attack?"
- *Next in thread:* Thor@HammerofGod.com: "Re: Trace of 139 attack?"
- *Messages sorted by:* [date] [thread] [subject] [author] [attachment]