

Re: Terminal Services Auditing not working

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2002-07/0090.html>

From: Bryan Ponnwitz (bponnwit@btboces.org)

Date: 07/19/02

Date: Fri, 19 Jul 2002 13:55:12 -0400

From: "Bryan Ponnwitz" <bponnwit@btboces.org>

To: <focus-ms@securityfocus.com>, <security-basics@securityfocus.com>

Noah:

I followed your steps for auditing logon events to the T and it seemed to work great. The following to events were logged to my Security log everytime I logged on:

Account Used for Logon by: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
Account Name:
 bponnwit
Workstation:
 EDTEC-WEBMASTER

---AND---

Successful Logon:

 User Name: bponnwit
 Domain: EDTEC-WEBMASTER
 Logon ID: (0x0,0x49BC7)
 Logon Type: 2
 Logon Process: User32
 Authentication Package: Negotiate
 Workstation Name: EDTEC-WEBMASTER

My terminal server is not part of a domain though, so any changes that I make to the local security policy can't be overridden. The only thing that I can think of that would cause you to not be auditing the events would be if you're terminal server is part of a domain and the local security policy is being overridden by the domain security policy.

Bryan Ponnwitz
Webmaster - Broome-Tioga Boces
bponnwit@btboces.org
(607) 763-3609

>>> Noah White <noah@baysystems.com> 07/19/02 10:01AM >>>

SecurityFocus Microsoft: Re: Terminal Services Auditing not working

Hello,

I'm running Win2K server SP2. Using the Local Security Policy tool I've

set the Audit Policy to audit the following (S – success; F – Failure):

Audit Account logon event – S/F

Audit logon events – S/F

Then using the Terminal Services Configuration tool I've right clicked

on the RDP–Tcp connection and selected Properties. From there selected

the Permissions tab and clicked on the Advanced button. From the next screen I've click the Auditing tab and added Administrator. I've selected Successful/Failed for all the Access options except Message and

Virtual channel and applied them.

I've rebooted the system and logged in through Terminal Services but the

security event log does not contain any Terminal Services specific event

IDs such as 682. I do see the normal system logon auditing events generated by the local security policy auditing settings but that's it.

Does TS auditing even work? What am I missing?

TIA,

–Noah

-
- **Previous message:** [Kolde, Jennifer E.: "RE: local security policy"](#)
 - **Maybe in reply to:** [Noah White: "Terminal Services Auditing not working"](#)
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)