

RE: Logging admin access to workstations

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2002-03/0744.html>

From: Demitrious S. Kelly (apokalyptik@apokalyptik.com)

Date: 03/14/02

From: "Demitrious S. Kelly" <apokalyptik@apokalyptik.com>
To: "'Alan Cooper'" <imalcooper@yahoo.com>, <security-basics@securityfocus.com>
Date: Thu, 14 Mar 2002 10:27:40 -0800

Use a packet sniffer to keep track of her network activities would be my suggestion... you could track by IP address.

If you have a problem with DHCP handing out random addresses, just assign a reservation on the DHCP server... that way it appears that nothing out of the norm is occurring...

Then again if she's using a static IP which she deigns to change from time to time (whether you allow the change or not) things could get tricky...

if you are using login scripts consider adding (to her login) a ping to a server which could log the ICMP requests and you could then match her per login... but make sure to redirect the output, and limit the number of requests to one so that it does not look suspicious, or take a good deal of extra time... :) However if she uses a firewall that's intrusive (like zone alarm) it might set off an alarm and have her wondering why ping needs access on startup...

And I would suggest logs... logs up the WAZOO... log everything... log the logging processes, and log the processes logging the logging – if you catch my drift...

But alas I'm no security expert, and I probably give my advice far too freely where it isn't needed nor wanted...

Those are just my \$.02

Cheers, and good luck!

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

From: Alan Cooper [mailto:imalcooper@yahoo.com]
Sent: Wednesday, March 13, 2002 10:22 AM
To: security-basics@securityfocus.com
Subject: Logging admin access to workstations

RE: Logging admin access to workstations

SecurityFocus BASICS: RE: Logging admin access to workstations

I have a potential hacker on our corporate LAN who has network-wide administration rights and may be copying confidential files from several executive workstations. This is a Windows environment and the workstations involved are Windows 2000 Pro and NT. The person suspected is extremely sharp and I need to do this without her knowledge. It is unlikely that we could use a keyboard-logging program since she is using a laptop (asking for the laptop may arise her suspicions). She also VPN's from home and I have no access to her home systems.

Is there a program that we can run on Win 2000 and NT workstations that will log all access attempts, tell me what they are doing if access is granted, their IP address, time of day, etc? Is there a better way approach this problem?

Thanks for your help.

Do You Yahoo!?

Try FREE Yahoo! Mail – the world's greatest free email!

<http://mail.yahoo.com/>

- ***Previous message:*** [Mike Craik: "Re: How to know when was root passwd changed"](#)
- ***In reply to:*** [Alan Cooper: "Logging admin access to workstations"](#)
- ***Next in thread:*** [Michael Perez: "RE: Logging admin access to workstations"](#)
- ***Messages sorted by:*** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)