



## Who is Accessing Your Server ?

### Authentication Event Analyzer

Do you have remote access to your Windows based networks and do you know who and when employees or hackers are trying to access your data. This easy to use report tool may be of great use to the Practice Manager who wants to keep on top of there network security.

Organizations have been providing access to company networks to mobile personal as well as those in your office for the past decade. While trusted company employees experience the convenience of being able to access company data and sensitive records at the touch of a button from virtually anywhere in the world, so to does everybody else on the internet. Now having said this, IT personnel have made a living designing VPN solutions and password protecting access to make sure that only the right people have can access the right information, yes?

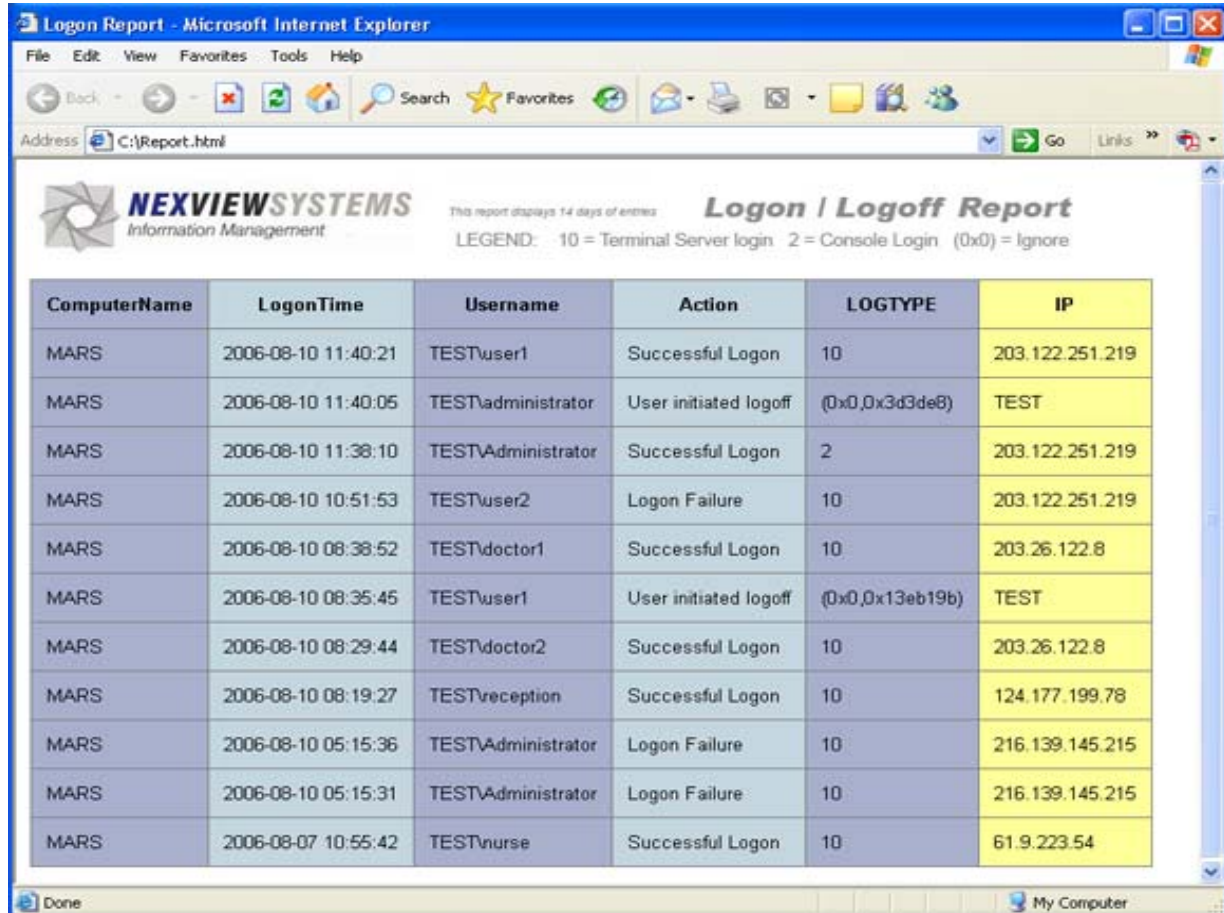
It's nice to think you have your firewall, antivirus, acceptable use policy and SOE policy. Everything should be covered right? But how do you know if it's really working?

Well there is no real silver bullet answer but you should at least be able to keep an eye on some of the basic things; like who has been logging on from home, when staff logged on, for how long staff logged on as well as weather anybody is attempting to gain access to your system, by guessing user names and passwords (Brute force attack).

To combat these issue NEXview Systems has developed an inexpensive way for supervisors and managers, to proactively self manage access to there network. The Authentication Event Analyzer can generate a simple to understand audit report of log on / log off activity. With a simple click the user can see who has logged in and out of there corporate network? Say Tom Brown tried to log in 200 times at midnight last night, this could be a potential attacker trying to guess Tom's password! Tom might also have logged on for 3 hours last night when he is supposed to be on holidays. These are just some of the valuable information that can be obtained with The Authentication Event Analyzer. This tool works best for organizations with a single Active Directory Domain Controller running Microsoft Terminal Services. However it can be easily adapted to various kinds of Network Topology on discussion with our Engineers.

If you are interested in this reporting tool please give us a call at NEXVIEW Systems on 08 8376 9972 or email [tmoyle@nexviewsystems.com](mailto:tmoyle@nexviewsystems.com) and will explain in details how this audit tools works.

## Screenshot of HTML Report



The screenshot shows a Microsoft Internet Explorer browser window displaying an HTML report. The browser's address bar shows 'C:\Report.html'. The report header includes the NEXVIEWSYSTEMS logo and the title 'Logon / Logoff Report'. A legend indicates that '10' represents Terminal Server login and '2' represents Console Login, with '(0x0)' representing Ignore. The main content is a table with the following data:

ComputerName	LogonTime	Username	Action	LOGTYPE	IP
MARS	2006-08-10 11:40:21	TESTuser1	Successful Logon	10	203.122.251.219
MARS	2006-08-10 11:40:05	TESTadministrator	User initiated logoff	(0x0,0x3d3de8)	TEST
MARS	2006-08-10 11:38:10	TESTAdministrator	Successful Logon	2	203.122.251.219
MARS	2006-08-10 10:51:53	TESTuser2	Logon Failure	10	203.122.251.219
MARS	2006-08-10 08:38:52	TESTdoctor1	Successful Logon	10	203.26.122.8
MARS	2006-08-10 08:35:45	TESTuser1	User initiated logoff	(0x0,0x13eb19b)	TEST
MARS	2006-08-10 08:29:44	TESTdoctor2	Successful Logon	10	203.26.122.8
MARS	2006-08-10 08:19:27	TESTreception	Successful Logon	10	124.177.199.78
MARS	2006-08-10 05:15:36	TESTAdministrator	Logon Failure	10	216.139.145.215
MARS	2006-08-10 05:15:31	TESTAdministrator	Logon Failure	10	216.139.145.215
MARS	2006-08-07 10:55:42	TESTnurse	Successful Logon	10	61.9.223.54