Windows: Log User Logins

With a focus on admin logins and use of privilege

Type of Systems: Windows AD Domain Controller
Necessary Skills: Use of the Group Policy and Event Viewer tools.

Complete Goal: To log every time a user logs in and when a user uses admin privileges.

Steps:

1. Login to the AD domain controller as the domain admin.
2. Open the Group Policy Management Console (CMD: `gpmc`).
3. In the directory pane on the left, navigate: *Forest: (domainName)* > *Domains* > *(domainName)*
   When *(domainName)* is the AD domain name.
4. Right click on “Default Domain Policy” and select “Edit.”
5. Navigate to *Computer Configuration* > *Policies* > *Windows Settings* > *Security Settings* > *Local Policies* > *Security Options*
6. Open “Audit: Force audit policy subcategory settings” and enable it.
7. Navigate to *Security Settings* > *Advanced Audit Policy Configuration* > *Logon/Logoff*
8. Open “Audit Logon” and enable “Success.” This will log when a user logs on to their machine.
9. In the same directory, open “Audit Special Logon” and enable “Success” and “Failure.” This will log when a user succeeds or fails to login as an admin user (or any time they request admin privileges).
10. After changing the group policy, you must refresh the policy on the domain. Use CMD: `gpupdate /force`
11. To ensure that our configuration is correct, open event viewer (CMD: `eventvwr`) to check the logs. Navigate to *Windows Logs* > *Security*. You should see multiple events with IDs 4624 (Logon), and 4672 (Special Logon). These are the instances of logons/access listed in chronological order.

Relevant Info:

- If user logins need to be added to the **centralized logging server**, you need to add the security log to your forwarder. The log is located at: *C:\Windows\System32\winevt\Logs\Security.evtx*
- The logs will be swamped with hundreds or thousands of user logins and admin logins. The reason for this is because it is not just recording the typical “type user

and password" logins, but it also records when a user **accesses** something. For example, if I open something like Windows Firewall that requires admin privilege to access, Windows calls this a login as a batch job and so it will add user and admin login events to the security log. There are also logins as a system service, so when a service starts, that service will login as the user that is running the service.

Appendix:

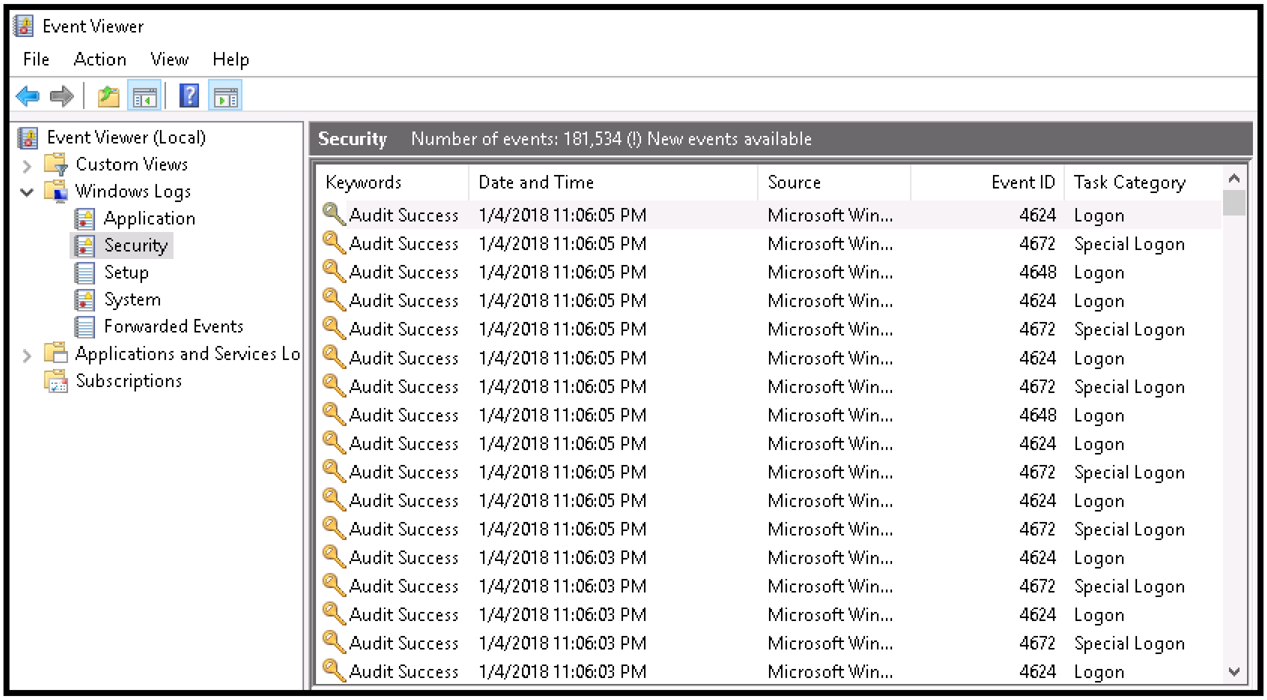
Basic Audits VS Advanced Audit Policy: http://bit.ly/2E8cjCM

Advanced Security Audit Policies: http://bit.ly/2CVCWf4

Windows Event Log IDs: http://bit.ly/2CFdfS9

Windows Event 4672 Description: http://bit.ly/2lUwsVF

Step 11: Event Viewer with a ton of Logon and Admin Logon events.



Security Number of events: 181,534 (!) New events available

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	1/4/2018 11:06:05 PM	Microsoft Win...	4624	Logon
Audit Success	1/4/2018 11:06:05 PM	Microsoft Win...	4672	Special Logon
Audit Success	1/4/2018 11:06:05 PM	Microsoft Win...	4648	Logon
Audit Success	1/4/2018 11:06:05 PM	Microsoft Win...	4624	Logon
Audit Success	1/4/2018 11:06:05 PM	Microsoft Win...	4672	Special Logon
Audit Success	1/4/2018 11:06:05 PM	Microsoft Win...	4624	Logon
Audit Success	1/4/2018 11:06:05 PM	Microsoft Win...	4672	Special Logon
Audit Success	1/4/2018 11:06:05 PM	Microsoft Win...	4648	Logon
Audit Success	1/4/2018 11:06:05 PM	Microsoft Win...	4624	Logon
Audit Success	1/4/2018 11:06:05 PM	Microsoft Win...	4672	Special Logon
Audit Success	1/4/2018 11:06:05 PM	Microsoft Win...	4624	Logon
Audit Success	1/4/2018 11:06:05 PM	Microsoft Win...	4672	Special Logon
Audit Success	1/4/2018 11:06:03 PM	Microsoft Win...	4624	Logon
Audit Success	1/4/2018 11:06:03 PM	Microsoft Win...	4672	Special Logon
Audit Success	1/4/2018 11:06:03 PM	Microsoft Win...	4624	Logon
Audit Success	1/4/2018 11:06:03 PM	Microsoft Win...	4672	Special Logon
Audit Success	1/4/2018 11:06:03 PM	Microsoft Win...	4624	Logon