**Spotting the Adversary with Windows Event Log Monitoring**

**Events to Monitor in a Windows Environment**

Part I.  
  
[Update: Part 2 can be found here.](http://www.redblue.team/2015/09/spotting-adversary-with-windows-event_21.html)

O.K. you have purchased a SIEM, added your Windows servers and you're ready to create your use-cases. You draw a blank. The amazing part about a SIEM is that you can build use-cases for literally thousands of scenarios. Unfortunately, however, the problem with a SIEM is that you have to create literally tens of thousands of alerts to monitor said use-cases. Monitoring for five failed logins followed by a successful login is great, but what good is the alert if the account locks after three failed attempts? Or if you have 10,000 users to monitor? To add to this, according to [Verizon's 2013 Data Breach Report](http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf), 76% of breaches involved stolen or weak credentials. So what to monitor for?

I find that it is often best to start with the basics-to report and/or alert on basic system functionality at the start, and to build more advanced use-cases based on abnormal behaviour outside of your companies policies.  
  
Fortunately, the friendly folks at the NSA have written [Spotting the Adversary with Windows Event Log Monitoring](https://www.nsa.gov/ia/_files/app/spotting_the_adversary_with_windows_event_log_monitoring.pdf), a great guide that walks you through what they have determined are the 16 primary categories to focus on within Windows event logs to ensure system security. We will be going through the first eight in part I, and the second eight in [part II](http://www.redblue.team/2015/09/spotting-adversary-with-windows-event_21.html).

1. Clearing Event Logs
2. Account Usage
3. Remote Desktop Logon Detection
4. Windows Defender Activities
5. Application Crashes
6. Software and Service Installation
7. External Media Detection
8. Pass the Hash Detection
9. AppLocker
10. System or Service Failures
11. Windows Update Errors
12. Kernel Driver Signing
13. Group Policy Errors
14. Mobile Device Activities
15. Printing Services
16. Windows Firewall

Before I start I want to clarify a not-so-obvious gotcha about Windows event logs for newcomers--Windows NT to Windows 2003 event IDs are identified via three digits; however, Windows Vista/Windows 2008 and beyond event IDs are identified by a four-digit ID. Therefore, any event ID with three digits is only applicable to Windows 2003 and before (and four digits beyond 2003.) Another useful tip is [Randy's Ultimate Windows Security](https://www.ultimatewindowssecurity.com/), which provides detailed information on nearly every Windows security event.

**1. Clearing Event Logs**

This is often the first alert I will install in a client's environment. There are very few reasons to clear the audit log directly, if the audit log is too large the event log's maximum size should be [set](https://technet.microsoft.com/en-us/library/cc759052(v=ws.10).aspx)to a smaller size. As such, outside of an improperly configured device an event log would only be cleared to hide malicious activities. As such, a simple alert looking for the following events is usually sufficient.

|  |
| --- |
| <http://3.bp.blogspot.com/-zONsz1fjYVI/Vfdzg_pXtCI/AAAAAAAAQXE/LMjq_JbhK3U/s1600/4.6%2BClearing%2BEvent%2BLogs.png> |
| Table-1: Event Log Cleared |

**2. Account Usage**

A proper set of alerts and reports for improper account activity is key to a useful SIEM. Setting an alert for X failed logins may drive your SOC crazy every Monday morning after a long weekend, but setting this threshold to alert when it occurs after-hours or on non-user systems could indicate malicious behaviour.  
  
The size of your environment and your companies security policies will weigh heavily on the value of certain actions being an alert or a report--a team of 200 may have a weekly report on created users, whereas a team of 20,000 may have a daily report. As such I will make my recommendations based on generalizations of a business with 1,000 users:

* A weekly report for created users and users added to privileged groups;
* An alert for Security-enabled group modifications;
* An alert for service account failed logins or account lockouts, although this is prone to alert-spamming in the case of an incorrectly configured script or service continually trying to log in;
* An alert for three non-service failed logins to a non-user system after-hours;
* Interactive logins by a service account; and
* A successful user login from a non-whitelisted country

|  |
| --- |
| <http://4.bp.blogspot.com/-ZtyCNFwBnw4/VfdzhKqnBFI/AAAAAAAAQXc/WnTLvAO3fSE/s1600/4.8%2BAccount%2BUsage.png> |
| Table-2: Account Usage |

Of course this is not a complete list of recommended alerts or reports, rather a couple of examples to get you started.

**3. Remote Desktop Logon Detection**

Remote desktop alerts and reports are tricky. Datacenter jumpboxes are the most used machines--they are the most heavily used, store endless amounts of 'temporary' data, and are often the most sought after machine by a hacker. Typically once a hacker gains access to a jumpbox they have access to your most valuable resources, so tracking access is very important.  
  
But how do you identify when access is malicious? In a 24h SOC access will be made 24 hours a day, so after-hour logins are not useful. This is something that I usually need to discuss in length with a client to really understand their environment before making remote desktop alerts. Some general concepts are:

* If your jumpbox is accessed from a specific subnet, alert when the connection is made from a different subnet, such as the DMZ.
* Alert when a service account attempts to connect to a jumpbox
* Alert or report for after-hour connections during non-change-window hours

|  |
| --- |
| <http://2.bp.blogspot.com/-2ZbAxefxmkw/Vfdzf8WcreI/AAAAAAAAQX0/BaU14btWpR8/s1600/4.16%2BRemote%2BDesktop%2BLogon%2BDetection.png> |
| Table-3: Remote Desktop Logins |

A remote desktop login is a standard login with a Logon Type of 10. Logon types are indicators of the login methodology used during the login--interactive, network, batch service, etc. They are essential for understanding how someone accessed a system. There is a large difference between a user logging in after hours via an RDP session and a new scheduled task.

**4. Windows Defender Activities**

This is pretty straight forward--a windows defender event shows detected malware/failed scan/failed update, etc. Essentially all events should be an alert.

|  |
| --- |
| <http://2.bp.blogspot.com/-Ygq_JjPlBIU/VfdzeQCbcuI/AAAAAAAAQWU/OksMxqYMe1c/s1600/4.11%2BWindows%2BDefender%2BActivities.png> |
| Table-4: Windows Defender |

**5. Application Crashes**

Application crashes are difficult to judge whether they will be effective alerts or reports in a client's environment. I tend to try to determine if the company has the resources available to perform an active investigation as towards why the application crashed. In the least a report or alert should be made for your high-value assets. That said, application crashes can be an indication of malicious code interfacing with an application to exploit it or replace it.

|  |
| --- |
| <http://1.bp.blogspot.com/-g_ilz_z8S5w/VfdzgE1LnXI/AAAAAAAAQW8/0pnJyas2jk8/s1600/4.2%2BApplication%2BCrashes.png> |
| Table-5: Application Crashes |

**6. Software and Service Installation**

Installed software and services should be at the least a report, and an alert for high priority assets (although change-window time frames can be excluded to avoid false-positives.)

|  |
| --- |
| <http://1.bp.blogspot.com/-8rP56LJX2sk/VfdzhOVPwQI/AAAAAAAAQXg/dqusv1Rxw9M/s1600/4.7%2BSoftware%2Band%2BService%2BInstallation.png> |
| Table-5: Software and Service Installation |

**7. External Media Detection**

There should always be a legitimate reason for plugging an external device into a high-value asset. An alert is recommended for medium to high severity events, and it is good to monitor external devices that are plugged in a new service is run within a few minutes on the system as this often indicates that something has executed off of the external media.

|  |
| --- |
| <http://2.bp.blogspot.com/-sYRavQiSxuQ/Vfdze6dahBI/AAAAAAAAQWg/2hePNu71ZeQ/s1600/4.13%2BExternal%2BMedia%2BDetection.png> |
| Table-6: External Media Detection |

**8. Pass the Hash Detection**

Tracking user accounts for detecting Pass the Hash (PtH) requires creating a custom view with XML to configure more advanced filtering options. The event query language is based on XPath, a query language for selecting [nodes](https://en.wikipedia.org/wiki/Node_(computer_science)) from an [XML](https://en.wikipedia.org/wiki/XML) document.   
  
Spotting the Adversary has defined a QueryList described below that is limited in detecting PtH attacks. These queries focus on discovering lateral movement by an attacker using local accounts that are not part of the domain. The QueryList captures events that show a local account attempting to connect remotely to another machine not part of the domain. This event is a rarity so any occurrence should be treated as suspicious.  
  
In the QueryList below, substitute the <DOMAIN NAME> section with the desired domain name.  
<QueryList>  
 <Query Id="0" Path="ForwardedEvents">  
 <Select Path="ForwardedEvents">  
 \*[System[(Level=4 or Level=0) and (EventID=4624)]]  
 and  
 \*[EventData[Data[@Name='LogonType'] and (Data='3')]]  
 and  
 \*[EventData[Data[@Name='AuthenticationPackageName'] = 'NTLM']]  
 and  
 \*[EventData[Data[@Name='TargetUserName'] != 'ANONYMOUS LOGON']]  
 and  
 \*[EventData[Data[@Name='TargetDomainName'] != '<DOMAIN NAME>']]  
 </Select>  
 </Query>  
  
</QueryList>  
  
These XPath queries are used for the Event Viewer’s Custom Views, and are not applicable to a SIEM itself.  
  
The successful use of PtH for lateral movement between workstations would trigger the following:  
   - Event ID **4624**  
   - Event level **Information**  
   - LogonType of **3**  
   - Logon method is **NTLM** authentication   
   - A **not-domain** logon and not **ANONYMOUS** account.

|  |
| --- |
| <http://1.bp.blogspot.com/-RlG87NcvtWM/Vfdzfrj3m9I/AAAAAAAAQXw/eSQoWI1IWnc/s1600/4.15%2BPass%2Bthe%2BHash%2BDetection.png> |
| Table-8: Pass the Hash Successful Logon Properties |

A failed PtH logon attempt would have all of the above properties except Event ID **4625** indicating a failed logon:

|  |
| --- |
| <http://2.bp.blogspot.com/-2IXj3WzxNSs/VfdzfbpyZVI/AAAAAAAAQX4/VsumBl9UEZg/s1600/4.15%2BPass%2Bthe%2BHash%2BDetection-2.png> |
| Table-9: Pass the Hash Failed Logon Properties |

**Conclusion**

The NSA's [Spotting the Adversary with Windows Event Log Monitoring](https://www.nsa.gov/ia/_files/app/spotting_the_adversary_with_windows_event_log_monitoring.pdf) provides an excellent breakdown of key Windows events when creating an initial set of alerts and reports for key windows assets. Part two will break down the second half of the event categories