Windows: Identify Suspicious Logins

Type of Systems: Windows AD Domain Controller
Necessary Skills: Use of the Event Viewer tool, XML code

Complete Goal: To identify suspicious logins. We will attempt to sort through all of our logins and find logins by malicious users. The trick is that you probably don't know the times you and everyone else on the team logged in, so it will be difficult to know if it was a team member or a malicious actor logged in. Luckily, the event details include the remote IP and hostname of the computer that logged in, so we should be able to use these attributes to determine the legitimacy of our logins.

Prerequisite: Before searching for suspicious logins, you must be logging logins. If you have not done this yet, there is another playbook guide for it. See the guide: "Log User Logins."

Steps:

1. Login to the AD domain controller as the domain admin.
2. Open event viewer (CMD: `eventvwr`) and navigate: *Windows Logs* > *Security*.
3. In the "Actions" pane on the right, click "Filter Current Log."
4. Switch tabs to "XML."
5. In the bottom-left, select "Edit query manually."
6. Add the following text after *<Select Path="Security">**

   *[System[EventID=4624] and EventData[Data[@Name='TargetUserName'] = '**exampleUser**']]*

   When ***exampleUser*** is replaced by the username you're looking for. See the screenshot of example XML code in the appendix. If the filter is successful, there should only be a few dozen to a few hundred events, not thousands.
7. Once you've filtered the results, you need to sort through them and find suspicious logins. We will do this based on IPs and hostnames. For each event, click on it. In the general information pane, scroll down until you see "Network Information." It will show the hostname and IP address of the remote computer that logged in. If it appears that someone logged in from an IP outside of our subnets, that is probably a suspicious login.

Relevant Info:

- In step 7, note that there are typically three login events for each actual login. Look at the timestamps and find the earliest event for that particular series of events. That earliest event will have the correct hostname and IP address. The other events seem to be some other part of the authentication process and can be dismissed.
- To search for something other than a username in the XML code, you can reference the XML view of an event to figure out how to write the code. Specifically, in an event, switch to the “Details” tab and change to “XML View.” This will show the XML attribute name for each value. Take this and substitute it into the user search code above.

Appendix:

Example XML code to filter event logs: http://bit.ly/2E7plAz

Step 6: My XML code to filter events