Lab 6

Systems Updates, Patching and Compliance

Develop, maintain and test secure systems and applications:

Summary:

Many security vulnerabilities are fixed by patches issued by software vendors. Organizations should establish a process to identify security vulnerabilities and rank them according to their level of risk. Relevant security patches should be installed within a month of their release to protect against cardholder data compromise. All software applications developed internally or externally, should be developed securely in accordance with the PCI DSS. They should also be based on industry standards and/or best practices, and incorporate information security throughout their entire development lifecycle.

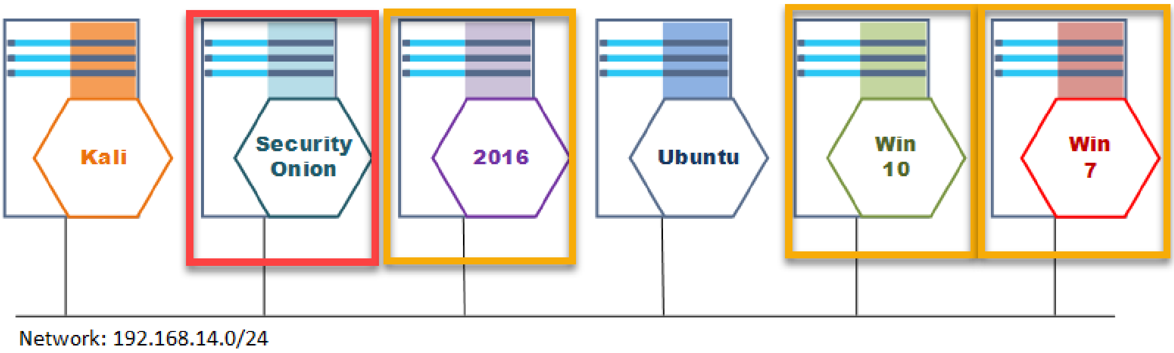
Contents:

Lab Setup:

Security onion is collecting log data from all of the systems on the network. In this exercise we will be filtering these logs to confirm compliance with standard windows updates. We can build filters to search for the installation of specific high risk updates or search for a more general “Best Practices” policy of installing updates in a timely manner. For this particular lab we are looking specifically for Windows Update compliance however with some tuning almost any log file can be imported and parsed by Kibana. This lab is a more general version of Lab 5. In Lab 5 we were looking specifically for Windows Defender Definition updates whereas we are now looking for all required updates. The same techniques we used in Lab 5 are also useful here.

PCI_DSS Mapping:

> 6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.
>
> Note: Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1.



Windows Logs:

Common update events:

There are many Event IDs that are related to windows update. For our purposes we really only need to worry about event_id:19.

[event_id:]

event_id	data.EventChannel.System.Message
19	Installation Successful: Windows successfully installed the following update: <update>.
20	Installation Failure: Windows failed to install the following update with error <error code>: <update>.
25	Windows Update failed to check for updates with error 0x********.
26	Windows Update successfully found # updates.
31	Windows Update failed to download an update. (see “updateTitle” for failed update KB******* number.
41	An update was downloaded. (see “updateTitle” for update KB******* number.)
43	Installation Started: Windows has started….
44	Windows update started downloading an update

In Kibana:

Key Fields for Parsing Updates:

Field	Description
data.EventChannel.System.ProviderName	The Windows Event Viewer log source **[Microsoft-Windows-WindowsUpdateClient/Operational]**
event_id	The Windows Event ID
data.EventChannel.EventData.updateTitle	This is the Windows Update Name (search for specific update KB#)
data.EventChannel.System.SystemTime	The Time an Event was logged to the windows machine (Remember all times on Sec Onion are UTC) vs likely timezone setting on Windows machine. To set timezone: Management -> Advanced Settings.
agent.ip	IP address of the Wazuh agent generating the log entry.

Basic Search strings:

To find all Windows Update Events:

```
>_ data.EventChannel.System.ProviderName:WindowsUpdateClient
```

To find a specific event_id:

```
>_ event_id:<id number.>
```

To search for a specific KB# for a required update

```
>_ data.EventChannel.EventData.updateTitle:KB#
```

Audit HowTo:

Filtering (Type it in):

Find all Successful updates:(Quick way the find successful updates)
Note: Updates requiring a reboot will not show up until after reboot.

```
>_ event_id:19
```

To remove Windows Defender Definition updates so we can see standard updates.

```
>_ event_id:19 AND NOT data.EventChannel.EventData.updateTitle:KB2267602
```

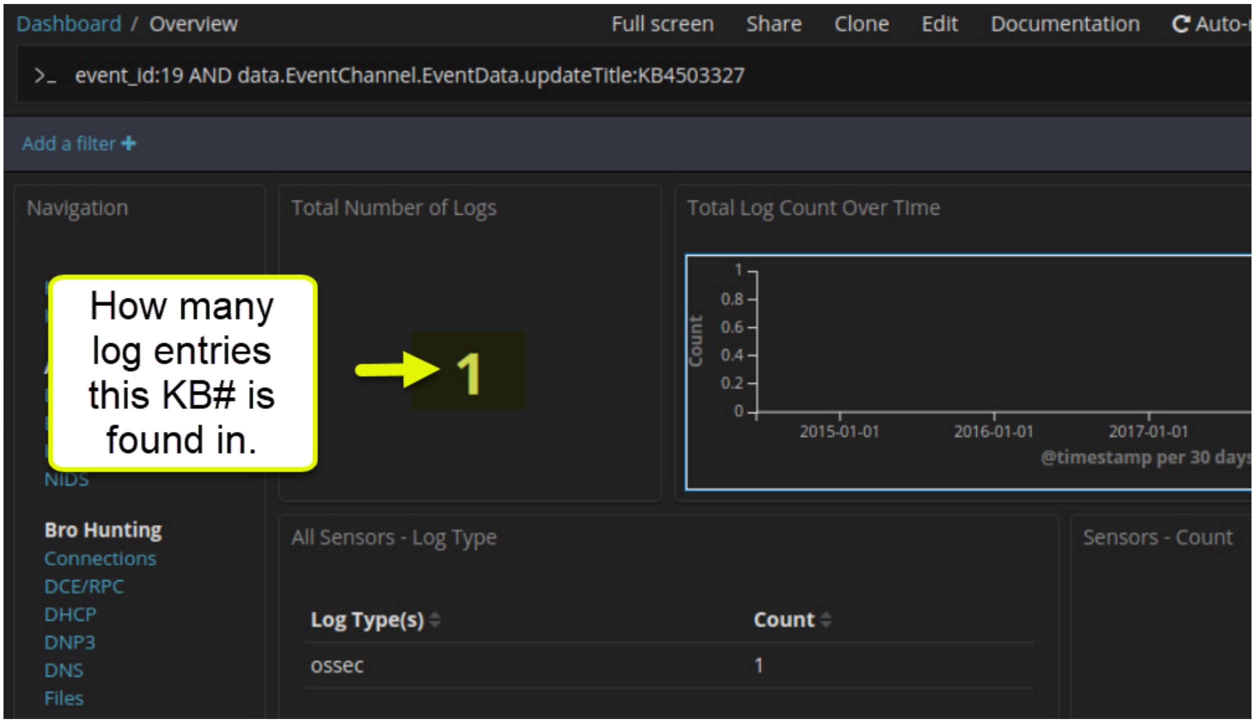
To audit a specific machine by its ip address:

```
>_ event_id:19 AND NOT data.EventChannel.EventData.updateTitle:KB2267602 AND
agent.ip:192.168.14.105
```

We want to confirm that Windows Updates are being installed within one week of initial release.

Filtering (Use the Wizard):

1. Search for a KB# that you want to audit in Kibana (Note: Total Number of Logs).

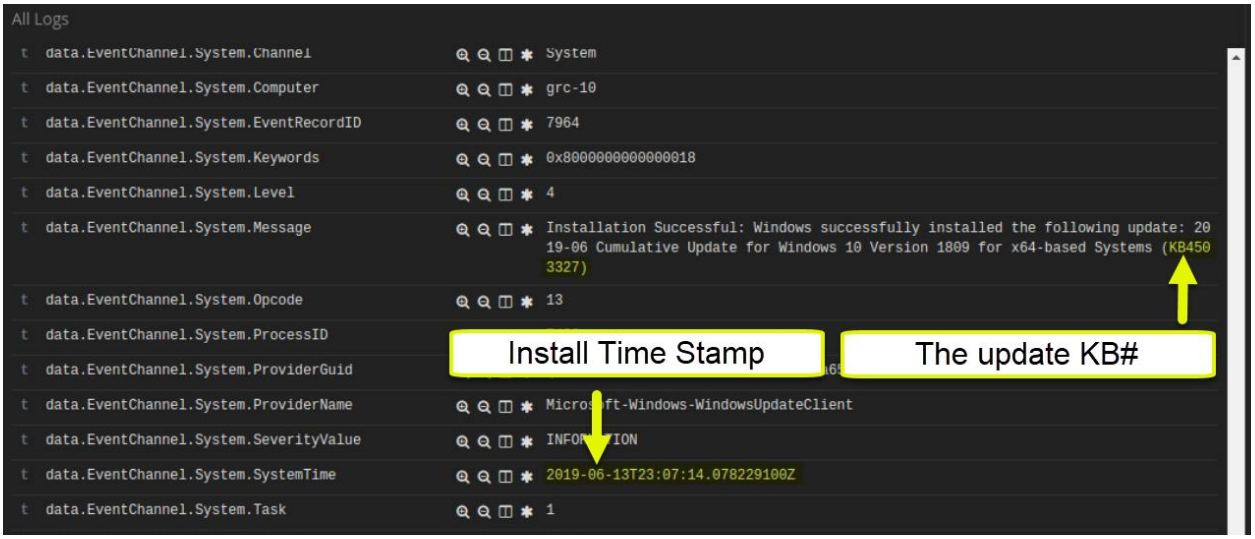


```
>_ event_id:19 AND data.EventChannel.EventData.updateTitle:KB4503327
```

How many log entries this KB# is found in.

Log Type(s)	Count
ossec	1

2. Scroll down to the “All Logs” area and expand the first entry. We are looking for two pieces of information.



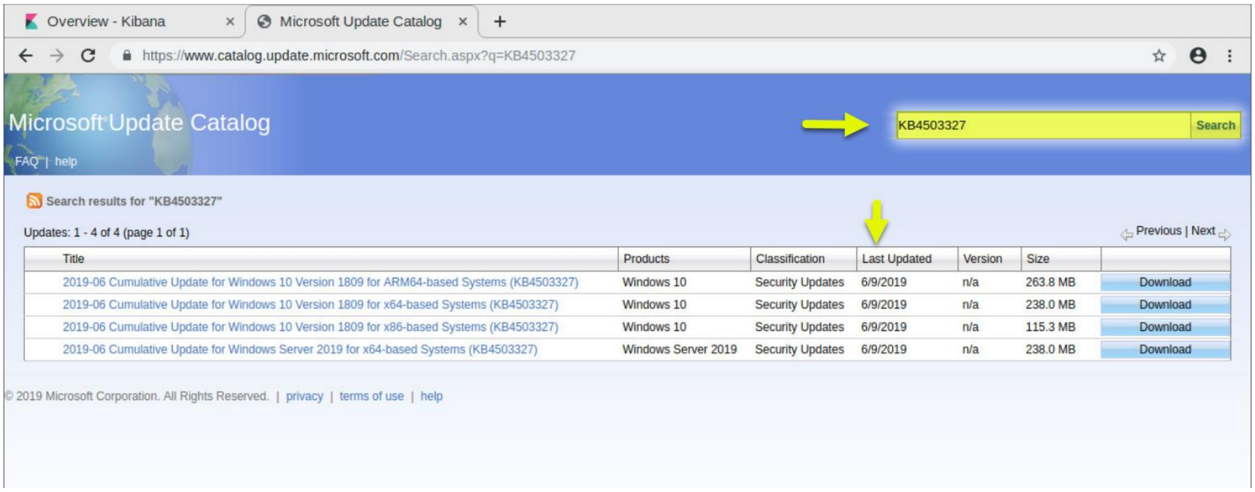
```
t  data.EventChannel.System.Channel          System
t  data.EventChannel.System.Computer         grc-10
t  data.EventChannel.System.EventRecordID    7964
t  data.EventChannel.System.Keywords         0x8000000000000018
t  data.EventChannel.System.Level            4
t  data.EventChannel.System.Message          Installation Successful: Windows successfully installed the following update: 20
                                             19-06 Cumulative Update for Windows 10 Version 1809 for x64-based Systems (KB450
                                             3327)
t  data.EventChannel.System.Opcode           13
t  data.EventChannel.System.ProcessID
t  data.EventChannel.System.ProviderGuid
t  data.EventChannel.System.ProviderName     Microsoft-Windows-WindowsUpdateClient
t  data.EventChannel.System.SeverityValue    INFORMATION
t  data.EventChannel.System.SystemTime       2019-06-13T23:07:14.078229100Z
t  data.EventChannel.System.Task             1
```

Install Time Stamp

The update KB#

3. We can check the initial release date for an update using the Microsoft Update Catalog and the KB# for the update:

   https://www.catalog.update.microsoft.com



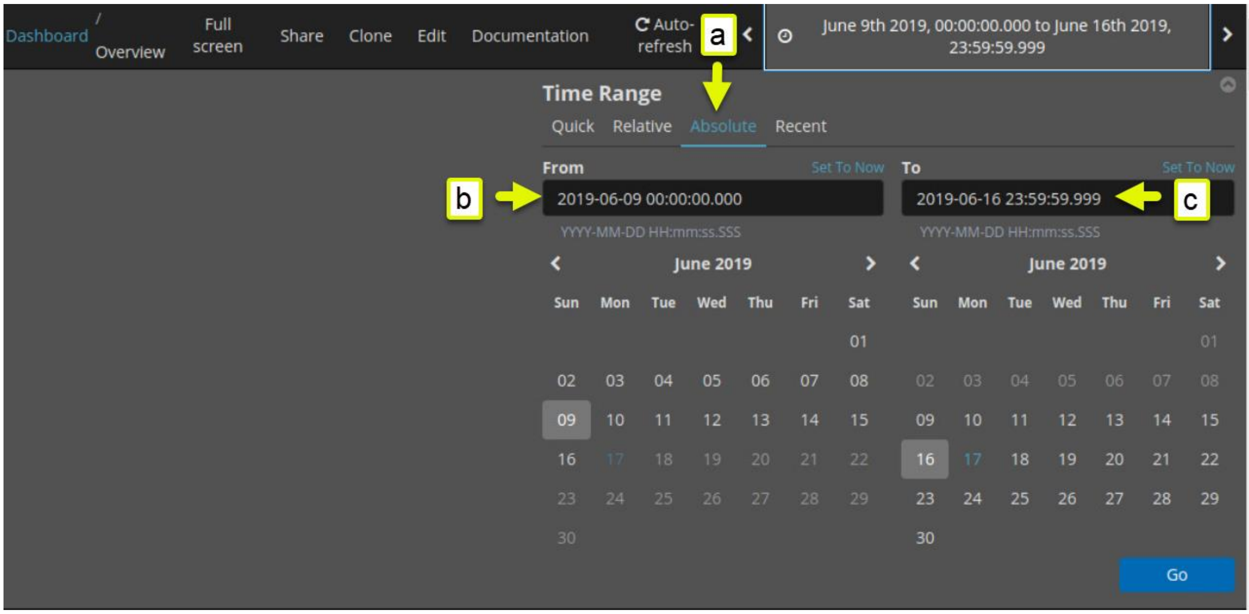
Search results for "KB4503327"

Updates: 1 - 4 of 4 (page 1 of 1)

Title	Products	Classification	Last Updated	Version	Size	
2019-06 Cumulative Update for Windows 10 Version 1809 for ARM64-based Systems (KB4503327)	Windows 10	Security Updates	6/9/2019	n/a	263.8 MB	Download
2019-06 Cumulative Update for Windows 10 Version 1809 for x64-based Systems (KB4503327)	Windows 10	Security Updates	6/9/2019	n/a	238.0 MB	Download
2019-06 Cumulative Update for Windows 10 Version 1809 for x86-based Systems (KB4503327)	Windows 10	Security Updates	6/9/2019	n/a	115.3 MB	Download
2019-06 Cumulative Update for Windows Server 2019 for x64-based Systems (KB4503327)	Windows Server 2019	Security Updates	6/9/2019	n/a	238.0 MB	Download

© 2019 Microsoft Corporation. All Rights Reserved. | privacy | terms of use | help

4. Go to the upper right corner to select the date range you are looking for.
   a. Select “Absolute”
   b. The first date will be the “Last Updated” date from the website.
   c. The second date will be how many days from release the install should take place according to your policy (Let's assume 1 week here).



June 9th 2019, 00:00:00.000 to June 16th 2019, 23:59:59.999

Time Range

From: 2019-06-09 00:00:00.000

To: 2019-06-16 23:59:59.999

5. If the “Total Number of Logs” stays the same all updates of that KB# were installed within the policy time span. If the number changes, that many updates were done after the policy time span expires.

For the most part we can check a few updates as a sample and if all are within the required specification we can assume that the configurations are correct.

ToDo:

1. List the 4 most recently installed updates in the logs and the machine they were installed on (Make sure to remove Windows Defender Definition updates).
   ____

2. What was the initial release date of KB4499177? ________________________

3. Check if update KB4499177 Was installed within one week of its release date as corporate policy dictates.
   ____