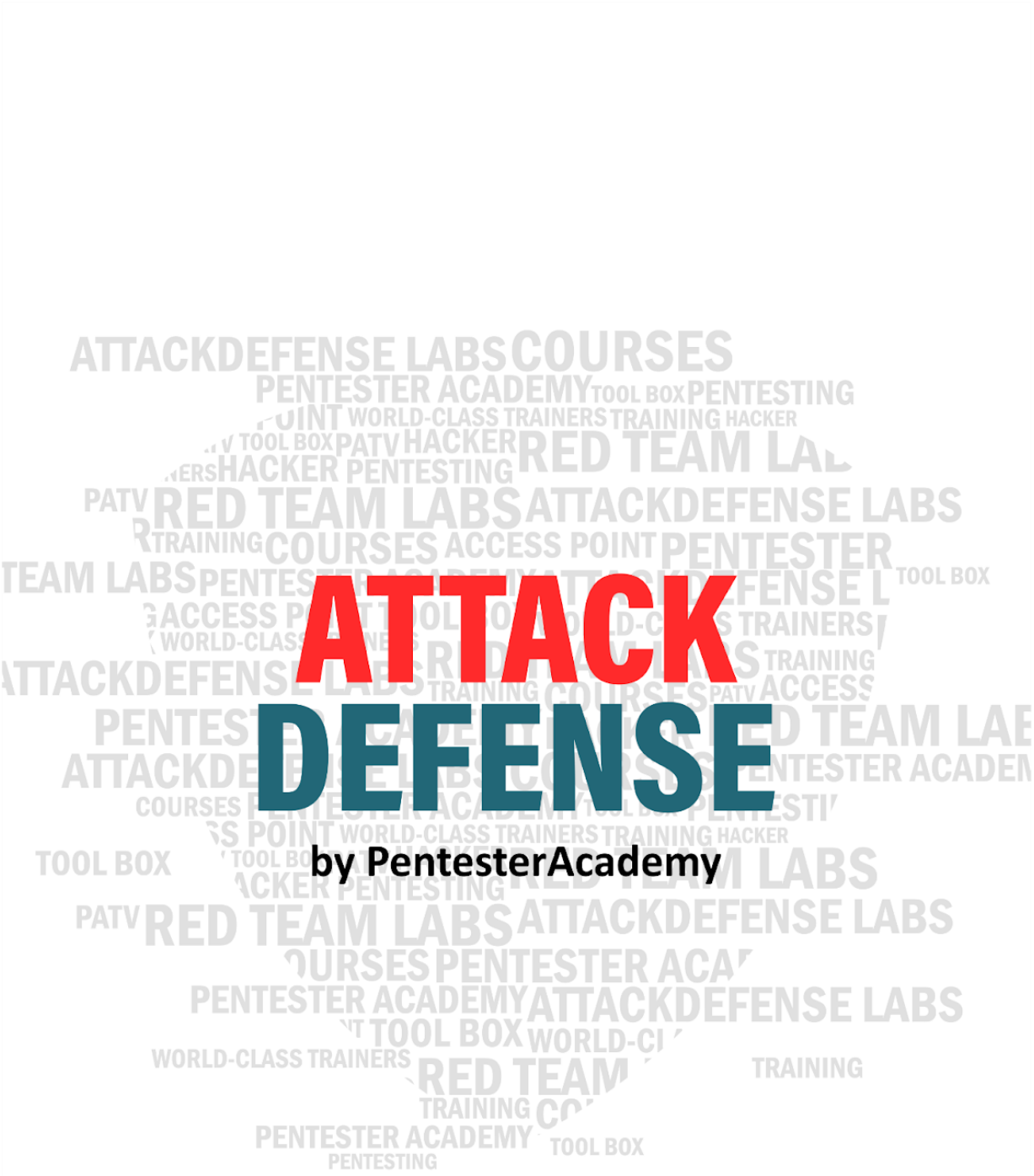
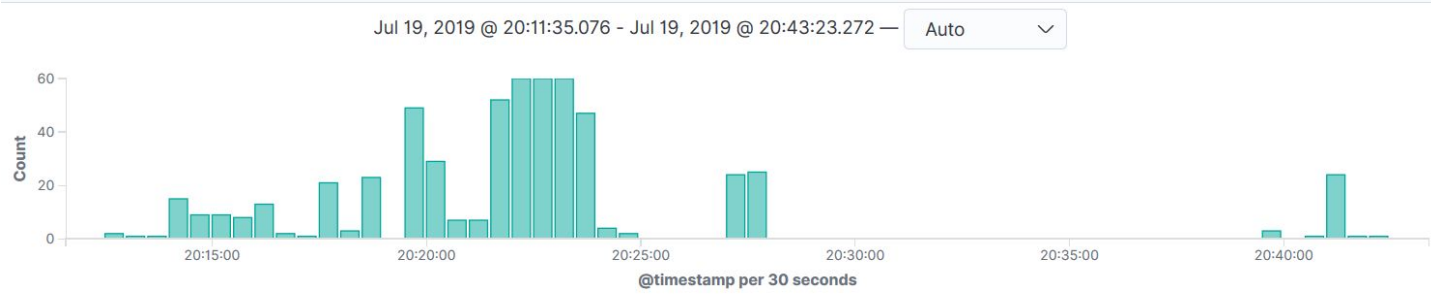

ATTACK
DEFENSE
by PentesterAcademy

Name	Kibana : Windows Event Logs I
URL	https://attackdefense.com/challengedetails?cid=1182
Type	Log Analysis : Windows Event Logs

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Kibana Dashboard:



Time	EventData.CommandLine
Jul 19, 2019 @ 20:12:51.000	consent.exe 4516 288 0000023C0CA21C70
Jul 19, 2019 @ 20:12:53.000	'C:\Windows\system32\cmd.exe'
Jul 19, 2019 @ 20:13:03.000	powershell
Jul 19, 2019 @ 20:13:46.000	-
Jul 19, 2019 @ 20:14:08.000	'C:\Windows\system32\cmd.exe' /c 'sc.exe create AtomicTestService binPath= C:\AtomicRedTeam\atomics\T1050\bin\AtomicService.exe'
Jul 19, 2019 @ 20:14:08.000	sc.exe create AtomicTestService binPath= C:\AtomicRedTeam\atomics\T1050\bin\AtomicService.exe
Jul 19, 2019 @ 20:14:08.000	-
Jul 19, 2019 @ 20:14:08.000	-
Jul 19, 2019 @ 20:14:08.000	'C:\Windows\system32\cmd.exe' /c 'sc.exe start AtomicTestService'
Jul 19, 2019 @ 20:14:08.000	sc.exe start AtomicTestService

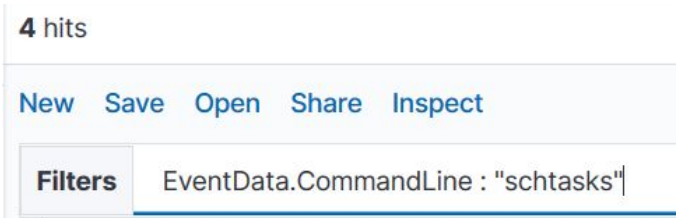
Q1. A task was scheduled to run daily at a specific time. Provide the password of the user running that task.

Ans: At0micStrong

Solution:

Step 1: Apply the following filter to list all the event logs where a scheduled task was created.

Filter: EventData.CommandLine : "schtasks"



4 event logs matched the filter.

Time	EventData.CommandLine
Jul 19, 2019 @ 20:27:4	'C:\Windows\system32\cmd.exe' /c 'SCHTASKS /Create /SC ONCE /TN spawn /TR C:\windows\system32\cmd.exe /ST 20:10'
Jul 19, 2019 @ 20:27:46.000	SCHTASKS /Create /SC ONCE /TN spawn /TR C:\windows\system32\cmd.exe /ST 20:10
Jul 19, 2019 @ 20:27:46.000	'C:\Windows\system32\cmd.exe' /c 'SCHTASKS /Create /S localhost /RU DOMAIN\user /RP At0micStrong /TN ' Atomic 'task /TR C:\windows\system32\cmd.exe /SC daily /ST 20:10'
Jul 19, 2019 @ 20:27:46.000	SCHTASKS /Create /S localhost /RU DOMAIN\user /RP At0micStrong /TN ' Atomic 'task /TR C:\windows\system32\cmd.exe /SC daily /ST 20:10

One of the processes creates a task that was scheduled to run daily.

```
SCHTASKS  /Create /S localhost /RU DOMAIN\user /RP At0micStrong /TN ' Atomic 'task /TR
C:\windows\system32\cmd.exe /SC daily /ST 20:10
```

The value of the /RP flag is the password for the user running the task, which was "At0micStrong" in this case.

Q2. A .txt file had been deleted securely using the 'sdelete' utility. Provide the full path of that file.

Ans: C:\some\file.txt

Solution:

Step 1: Apply the following filter to list all the event logs in which "sdelete" utility was used.

Filter: EventData.CommandLine : sdelete*

Time	EventData.CommandLine
Jul 19, 2019 @ 20:17:57.000	'C:\Windows\system32\cmd.exe' /c 'sdelete.exe C:\some\file.txt'

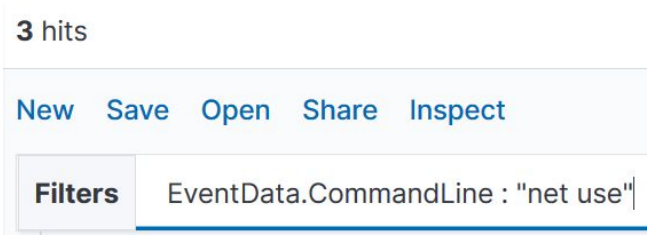
sdelete had been used to delete "C:\some\file.txt".

Q3. The host machine connected to a shared resource on a remote machine, as Administrator user using the 'net use' command. Provide the password used to connect to that remote machine.

Ans: P@ssw0rd1

Solution:

Step 1: Apply the following filter to list all the event logs in which "net use" command was used.



3 event logs matched the filter.

Time	EventData.CommandLine
Jul 19, 2019 @ 20:18:41.000	'C:\Windows\system32\cmd.exe' /c 'cmd.exe /c ' net use \\Target\C$ P@ssw0rd1 /u:DOMAIN\Administrator
Jul 19, 2019 @ 20:18:41.000	cmd.exe /c net use \\Target\C$ P@ssw0rd1 /u:DOMAIN\Administrator
Jul 19, 2019 @ 20:18:41.000	net use \\Target\C$ P@ssw0rd1 /u:DOMAIN\Administrator

```
cmd.exe  /c  net use \\Target\C$ P@ssw0rd1 /u:DOMAIN\Administrator
```

The password used to connect to the shared resource on the remote machine was "P@ssw0rd1".

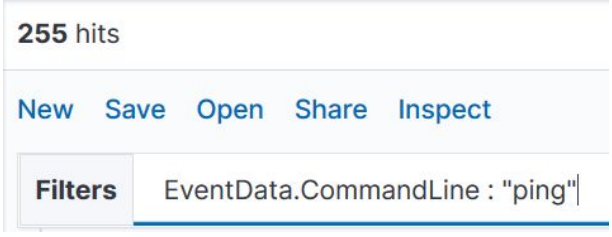
Q4. A ping sweep attack had been launched by the host machine against a network. What was the subnet address of that network? Provide the answer in CIDR notation.

Ans: 192.168.1.0/24

Solution:

Step 1: Apply the following filter to list all the event logs in which "ping" command was used.

Filter: EventData.CommandLine : "ping"



Time	EventData.CommandLine
Jul 19, 2019 @ 20:21:35.000	'C:\Windows\system32\cmd.exe' /c 'for /l %%i in (1,1,254) do ping -n 1 -w 100 192.168.1.%%i'

The matched event logs indicate that a ping sweep attack was launched on the subnet "192.168.1.0/24".

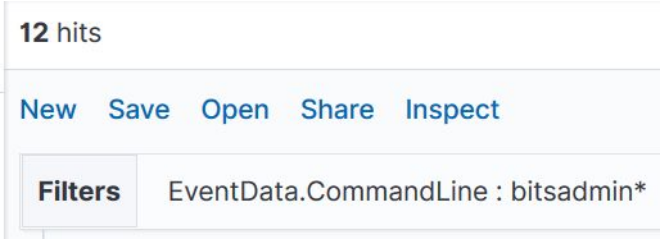
Q5. Bitsadmin tool was used to download a file from a remote server. Provide the full path of the downloaded file on the host machine.

Ans: C:\Windows\Temp\bitsadmin_flag.ps1

Solution:

Step 1: Apply the following filter to list all the event logs in which "bitsadmin" tool was used.

Filter: EventData.CommandLine : bitsadmin*



Jul 19, 2019 @ 20:18:0	bitsadmin.exe /transfer /Download /priority Foreground https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/atomics/T1197/T1197.md C:\Windows\Temp\bitsadmin_flag.ps1

The downloaded file was stored at "C:\Windows\Temp\bitsadmin_flag.ps1".

References:

1. ELK Stack (https://www.elastic.co/elk-stack)