



Cybersecurity

Module 19 Challenge Submission File

Let's Go Splunking!

Make a copy of this document to work in, and then respond to each question below the prompt. Save and submit this completed file as your Challenge deliverable.

Step 1: The Need for Speed

1. Based on the report you created, what is the approximate date and time of the attack?

The attack began on 2020-02-23 at 14:30:00, the download speeds dropped from around 100 to ~7 and the Upload went from around 10 to ~1.

2. How long did it take your systems to recover?

It seems that the systems had recovered by 23:30:00 on the same day.

Provide a screenshot of your report:

source="server_speedtest (1).csv" | eval ratio = 'DOWNLOAD_MEGABITS' / 'UPLOAD_MEGABITS' | table _time IP_ADDRESS DOWNLOAD_MEGABITS UPLOAD_MEGABITS ratio

23 events (before 2/22/23 1:43:34.000 AM) No Event Sampling

Events Patterns **Statistics (23)** Visualization

20 Per Page Format Preview

	_time	IP_ADDRESS	DOWNLOAD_MEGABITS	UPLOAD_MEGABITS	ratio
1	2020-02-20 14:21:00	198.153.194.1	109.16	5.43	20.1
2	2020-02-21 14:30:00	198.153.194.1	105.91	5.51	19.2
3	2020-02-21 16:30:00	198.153.194.2	106.91	6.51	16.4
4	2020-02-21 18:30:00	198.153.194.2	107.91	7.51	14.4
5	2020-02-21 20:30:00	198.153.194.1	108.91	8.51	12.8
6	2020-02-21 22:30:00	198.153.194.1	109.91	9.51	11.6
7	2020-02-21 23:30:00	198.153.194.1	109.16	10.51	10.39
8	2020-02-22 14:30:00	198.153.194.1	105.91	11.51	9.202
9	2020-02-22 16:30:00	198.153.194.2	106.91	12.51	8.546
10	2020-02-22 18:30:00	198.153.194.2	107.91	13.51	7.987
11	2020-02-22 20:30:00	198.153.194.2	108.91	7.51	14.5
12	2020-02-22 22:30:00	198.153.194.2	109.91	8.51	12.9
13	2020-02-22 23:30:00	198.153.194.2	109.16	9.51	11.5
14	2020-02-23 14:30:00	198.153.194.1	7.87	1.83	4.30
15	2020-02-23 14:30:00	198.153.194.2	12.76	2.19	5.83
16	2020-02-23 18:30:00	198.153.194.2	17.56	3.43	5.12
17	2020-02-23 20:30:00	198.153.194.2	65.34	4.23	15.4
18	2020-02-23 22:30:00	198.153.194.1	78.34	6.51	12.0
19	2020-02-23 23:30:00	198.153.194.2	123.91	8.51	14.6
20	2020-02-23 23:30:00	198.153.194.1	122.91	7.51	16.4

Step 2: Are We Vulnerable?

Provide a screenshot of your report:

New Search

source="nessus_logs.csv" host="nessus_logs" sourcetype="csv" dest_ip="10.11.36.23" | stats count by severity

243 events (before 2/22/23 2:08:55.000 AM) No Event Sampling

Events Patterns **Statistics (5)** Visualization

20 Per Page Format Preview

	severity	count
1	critical	49
2	high	47
3	informational	52
4	low	50
5	medium	45

Provide a screenshot showing that the alert has been created:

source="nessus_logs.csv" host="nessus_logs" sourcetype="csv" dest_ip="10.11.36.23" severity=critical severity=critical

All time

49 events (before 2/22/23 2:12:46.000 AM) No Event Sampling

Job

Smart Mode

Events (49) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect

1 hour per column

List Format 20 Per Page

Prev 1 2 3 Next

< Hide Fields

All Fields

SELECTED FIELDS

a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS

bid 15
a cve 22
cvss 3
cvss_base_score 3
cvss_vector 3
date_hour 13
date_mday 2
date_minute 35
date_month 1
date_second 31
date_wday 2
date_year 1
date_zone 1
a dest 1
a dest_dns 1
a dest_ip 1
a dest_is_expected 1
a dest_mac 19
a dest_nt_host 15
a dest_pci_domain 1

Time Event

2/20/20 5:33:01.000 PM

,"start_time""Thu Feb 20 17:33:01 2020" end_time""Thu Feb 20 17:33:01 2020" dest_dns""HOST-003" dest_nt_host""ops-sys-006" dest_mac""ad:7b:3d:db:49:8b" dest_ip""10.11.36.13" os""Cisco Router" dest_port_proto""el-random(827/tcp)" severity_id""4" signature_id""12258" signature""Additional DNS Hostnames"
---splunk-ta-nessus-end-of-event---
",2020-02-20T18:03:12.000+0000,,,,,,,,,HOST-003,,,,,HOST-003,10.11.36.23,false,,ad:7b:3d:db:49:8b,ops-sys-006,,untrust,827,el-random(827/tcp),false,,false,false,,Thu Feb 20 17:33:01 2020,nessus_nessus_misconfigured_wireless_device nessus_plugin_avail nessus_system_version,127.0.0.1,,main,,,4,,,Cisco Router,12258,,,Cisco Router,,,,,Nessus,,,Err:509,,,critical,4,,,Additional DNS Hostnames,12258,eventgen,nessus,prd-p-vj7zgflpcb88,,,,,,Thu Feb 20 17:33:01 2020,,,,,"inventory
os
report
Show all 13 lines
host = nessus_logs | source = nessus_logs.csv | sourcetype = csv

2/20/20 5:27:48.000 PM

,"start_time""Thu Feb 20 17:27:48 2020" end_time""Thu Feb 20 17:27:48 2020" dest_dns""HOST-003" dest_mac""0b:4a:fe:06:36:92" dest_ip""10.11.36.29" os""Microsoft Windows XP Service Pack 2" os""Microsoft Windows XP Service Pack 3" dest_port_proto""general" severity_id""4" signature_family""Service detection" signature_id""12122" signature""Terminal Services Encryption Level is not FIPS-140 Compliant"
---splunk-ta-nessus-end-of-event---
",2020-02-20T17:39:19.000+0000,,,,,,,,,HOST-003,,,,,HOST-003,10.11.36.23,false,,0b:4a:fe:06:36:92,,untrust,,general,,false,,false,false,,Thu Feb 20 17:27:48 2020,nessus_nessus_misconfigured_device nessus_plugin_avail nessus_system_version,127.0.0.1,,main,,,4,,,Microsoft Windows XP Service Pack 2 Microsoft Windows XP Service Pack 3",12122,,,Microsoft Windows XP Service Pack 2 Microsoft Windows XP Service Pack 3",,,,Nessus,,,Err:509,,,critical,4,,,Terminal Services Encryption Level is not FIPS-140 Compliant,Service detection,12122,eventgen,nessus,prd-p-vj7zgflpcb88,,,,,,Thu Feb 20 17:27:48 2020,,,,,"inventory
Show all 15 lines
host = nessus_logs | source = nessus_logs.csv | sourcetype = csv

2/20/20 5:19:58.000 PM

,"start_time""Thu Feb 20 17:19:58 2020" end_time""Thu Feb 20 17:19:58 2020" dest_dns""HOST-003" dest_nt_host""HOST-003" dest_mac""fb:69:33:d1:44:a4" dest_ip""10.11.36.29" os""Microsoft Windows XP Service Pack 2" os""Microsoft Windows XP Service Pack 3" dest_port_proto""el-random(2426/tcp)" sev

Critical Database Vulnerabilities

detection of critical database vulnerabilities.

Enabled: Yes. Disable

App: search

Permissions: Private. Owned by admin. Edit

Modified: Feb 22, 2023 2:16:19 AM

Alert Type: Scheduled. Daily, at 0:00. Edit

Trigger Condition: .. Number of Results is > 0. Edit

Actions: 1 Action Edit

Send email

Step 3: Drawing the (Base)line

1. When did the brute force attack occur?

The brute force attack started at 8am on Feb 21st 2020 and ended around 2pm on the same day.

2. Determine a baseline of normal activity and a threshold that would alert if a brute force attack is occurring:

The baseline of activity would be from 5-28 failed login attempts, and the threshold would be 35 failed login attempts

3. Provide a screenshot showing that the alert has been created:

Brute Force Attack Threshold

Enabled: Yes. [Disable](#)

App: search

Permissions: Private. Owned by admin. [Edit](#)

Modified: Feb 22, 2023 2:33:37 AM

Alert Type: Scheduled. Hourly, at 0 minutes past the hour. [Edit](#)

Trigger Condition: .. Number of Results is > 35. [Edit](#)

Actions: [▼](#) 1 Action [Edit](#)

[✉](#) Send email