

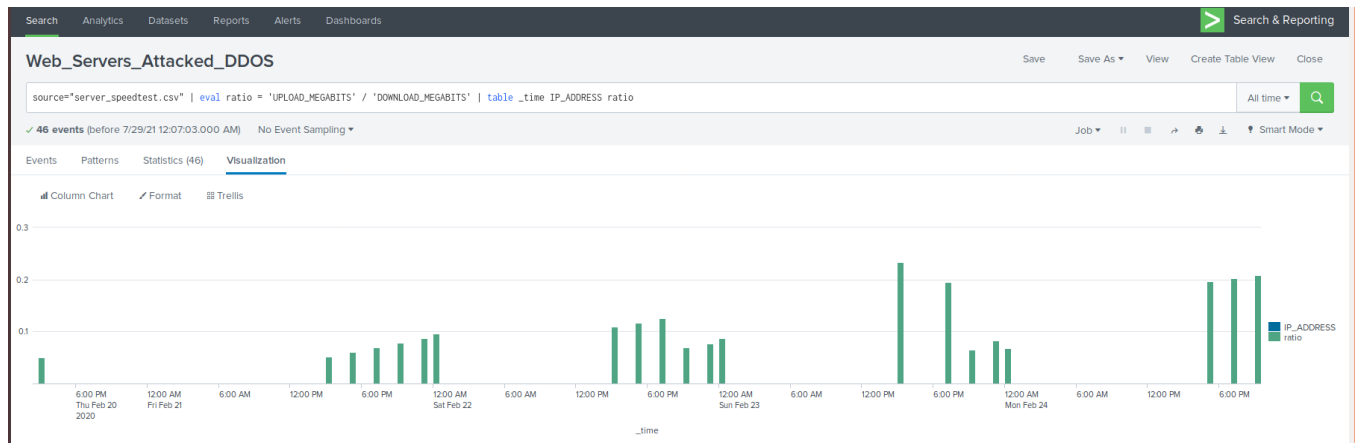
WEEK 18: Homework Lets Go Splunking

Step 1: DDOS Attack

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

02-23-2020 at 2:30pm

How long did it take your systems to recover? Full recovery after 9 hours



Step 2: Creating Critical Vulnerability Alert

New Search

source="nessus_logs.csv" host="9a4fc8dfabe7" sourcetype="csv" severity=critical dest_ip="10.11.36.23"

✓ 98 events (before 7/29/21 12:36:55.000 AM) No Event Sampling

Events (98) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect

1 hour per column

List Format 20 Per Page

< Hide Fields All Fields

SELECTED FIELDS

- # host 1
- # source 1
- # sourcetype 1

INTERESTING FIELDS

- # bid 15
- # cve 22
- # cvss 3
- # cvss_base_score 3
- # cvss_vector 3
- # date_hour 13
- # date_minute 2
- # date_second 31
- # date_wday 2
- # date_year 1
- # date_zone 1
- # dest 1
- # dest_dns 1
- # dest_ip 1
- # dest_is_expected 1
- # dest_mac 19
- # dest_nt_host 15
- # dest_pci_domain 1
- # dest_port 9
- # dest_port_proto 11
- # dest_requires_av 1
- # dest_should_timesync 1
- # dest_should_update 1
- # end_time 49
- # extracted_eventtype 4
- # extracted_host 1
- # extracted_index 1
- # extracted_incount 1
- # extracted_source 1

Event 1

Time: 2/20/20 5:33:01.000 PM

Event: ,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-vj7zgf1pcb88,,,,,Thu Feb 20 17:33:01 2020,,,,inventory os report Show all 13 lines host = 9a4fc8dfabe7 source = nessus_logs.csv sourcetype = csv

Event 2

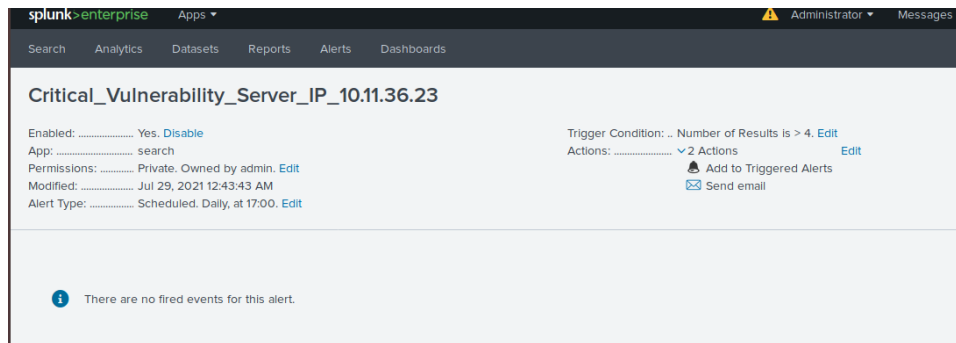
Time: 2/20/20 5:33:01.000 PM

Event: ,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-vj7zgf1pcb88,,,,,Thu Feb 20 17:33:01 2020,,,,inventory os report Show all 13 lines host = 9a4fc8dfabe7 source = nessus_logs.csv sourcetype = csv

Event 3

Time: 2/20/20 5:27:48.000 PM

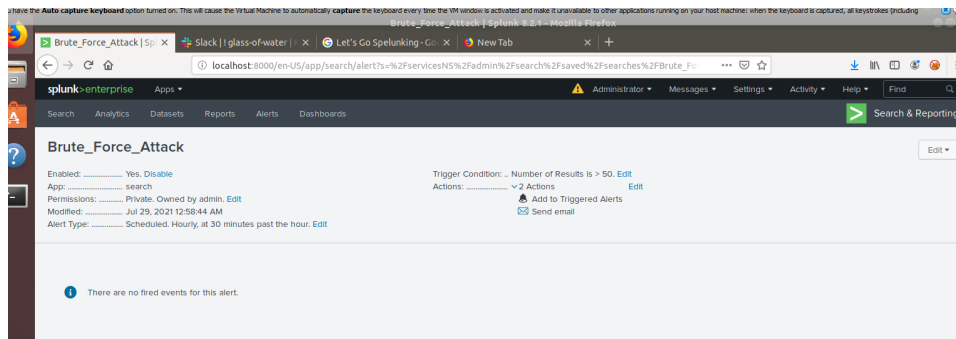
Event: ,start_time="Thu Feb 20 17:27:48 2020" end_time="Thu Feb 20 17:27:48 2020" dest_dns="HOST-003" dest_mac="0b:4a:fe:06:36:92" dest_ip="10.11.36.29" os="Microsoft Windows XP Service Pack 2" os="Microsoft Windows XP Service Pack 3" dest_port_proto="general" severity_id="4" signature_family="Service 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,e,,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 de tectio,12122,eventgen,nessus,prd-p-vj7zgf1pcb88,,,,,Thu Feb 20 17:27:48 2020,,,,inventory Show all 15 lines host = 9a4fc8dfabe7 source = nessus_logs.csv sourcetype = csv



Step 3: Brute Force, Failed Login Attempts Alert

Baseline is 10 Failed Logins

Brute Force trigger is 50+



New Search

Save AsCreate Table ViewClose

source=Administrator_logs.csv* host=9a4fc8dfabe7* sourcetype=csv* name=An account failed to log on*

All time

1,004 events (before 7/29/21 12:53:53.000 AM) No Event Sampling

Job

Smart Mode

Events (1,004)PatternsStatisticsVisualization

Format TimelineZoom OutZoom to SelectionDeselect

1 hour per column

12345678Next

Hide FieldsAll Fields

SELECTED FIELDS

a host 1

a source 1

a sourcetype 1

a src_ip 100+

INTERESTING FIELDS

a Account_Domain 2

a Account_Name 2

a action 1

a app 3

a Authentication_Package 3

a body 100+

a Caller_Process_ID 16

a Caller_Process_Name 1

a category 1

a ComputerName 50

a date_hour 24

a date_mday 2

a date_minute 60

a date_month 1

a date_second 60

a date_wday 2

a date_year 1

a date_zone 1

a dest 51

a dest_is_expected 1

a dest_nt_domain 1

a dest_nt_host 51

a dest_pcl_domain 1

a dest_requires_av 1

a dest_should_timesync 1

a dest_should_update 1

a dvc 50

a dvc_is_expected 1

a dvc_ntl_host 50

a dvc_pcl_domain 1

a dvc_requires_av 1

a dvc_should_timesync 1

2/21/202112:47:00 PM

8/21/2020 17:12:47, "WINDOWS
WINDOWS", "ADMINISTRATOR
ADMINISTRATOR",,NTLM,,0x4,-,,,,,,,,,ops-sys-003,,,0xf4e3ac39,4625,An account failed to log on,Information,Unknown User name or bad passwo
rd,,,,,,,,,0,,Audit Success,Security,,,0x4,f4e3ac39,0,,,An account failed to log on.
Subject:
Security ID:
abc\def
Show all 135 lines
host = 9a4fc8dfabe7 | source = Administrator_logs.csv | sourcetype = csv | src_ip = 133.213.121.158

2/21/20215:10:52:00 PM

8/21/2020 17:10:52, "WINDOWS
WINDOWS", "ADMINISTRATOR
ADMINISTRATOR",,MICROSOFT_AUTHENTICATION_PACKAGE_V1_0,,,0xb,-,,,,,,,,,HOST-005,,,0x508a3a43,4625,An account failed to log on,Information,,U
nknown User name or bad password,,,,,,,,,4,,Audit Success,Security,,,0x0,508a3a43,4,,,An account failed to log on.
Subject:
Security ID:
abc\def
Show all 136 lines
host = 9a4fc8dfabe7 | source = Administrator_logs.csv | sourcetype = csv | src_ip = 225.235.161.149

2/21/20215:10:48:00 PM

8/21/2020 17:10:48, "WINDOWS
WINDOWS", "ADMINISTRATOR
ADMINISTRATOR",,NTLM,,0x7,-,,,,,,,,,PROD-WFS-002,,,0x28528027,4625,An account failed to log on,Information,Unknown User name or bad passwo
rd,,,,,,,,,4,,Audit Success,Security,,,0x7,28528027,4,,,An account failed to log on.
Subject:
Security ID:
NT AUTHORITY\SYSTEM
Show all 136 lines
host = 9a4fc8dfabe7 | source = Administrator_logs.csv | sourcetype = csv | src_ip = 150.214.99.187

2/21/20215:10:30:00 PM

8/21/2020 17:10:30, "WINDOWS
WINDOWS", "ADMINISTRATOR
ADMINISTRATOR",,NTLM,,0x9,-,,,,,,,,,BUSDEV-006,,,0x9ABE7A08,4625,An account failed to log on,Information,Unknown User name or bad passwo
rd,,,,,,,,,20,,Audit Success,Security,,,0x9,9ABE7A08,20,,,An account failed to log on.
Subject:
Security ID:
abc\def
Show all 135 lines
host = 9a4fc8dfabe7 | source = Administrator_logs.csv | sourcetype = csv | src_ip = 27197111.225

2/21/20215:07:59:00 PM

8/21/2020 17:07:59, "WINDOWS
WINDOWS", "ADMINISTRATOR
ADMINISTRATOR",,Negotiate,,,0xb,-,,,,,,,,,ops-sys-006,,,0xbCD84A87,4625,An account failed to log on,Information,Unknown User name or bad p
assword,,,,,,,,,14,,Audit Success,Security,,,0xb,CD84A87,14,,,An account failed to log on.

Right Click

Reports created:

Reports

Reports are based on single searches and can include visualizations, statistics and/or events. Click the name to view the report. Open the report in Pivot or Search to refine the parameters or further explore the data.

11 Reports

AllYoursThis App's

filter

i	Title *	Actions	Next Scheduled Time ↕	Owner ↕	App ↕	Sharing ↕
>	DB SERVER ATTACK REPORT	Open in SearchEdit	2021-07-29 12:00:00 UTC	admin	search	Private
>	Errors in the last 24 hours	Open in SearchEdit	None	nobody	search	App
>	Errors in the last hour	Open in SearchEdit	None	nobody	search	App
>	Geographic Map - POST Request monitor by Source IP	Open in SearchEdit	None	admin	search	Private
>	License Usage Data Cube	Open in SearchEdit	None	nobody	search	App
>	Messages by minute last 3 hours	Open in SearchEdit	None	nobody	search	App
>	Orphaned scheduled searches	Open in SearchEdit	None	nobody	search	App
>	Pie Chart - Top 10 URL_PATH	Open in SearchEdit	None	admin	search	Private
>	Radial Gauge Post Request Monitor	Open in SearchEdit	None	admin	search	Private
>	Splunk errors last 24 hours	Open in SearchEdit	None	nobody	search	App
>	Web_Servers_Attacked_DDOS	Open in SearchEdit	None	admin	search	Private