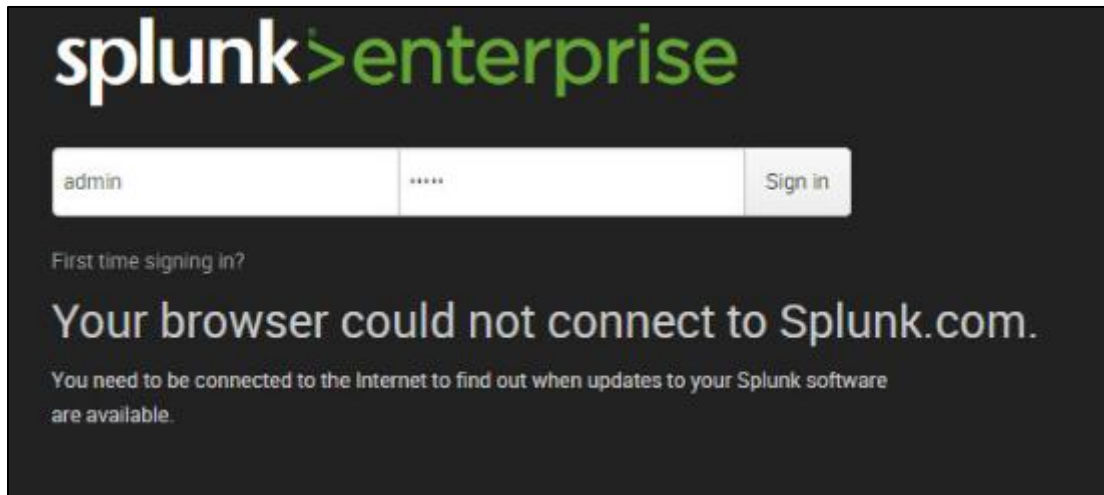


Splunk

Splunk is a SIEM (Security Information and Event Management) solution that uses big data from websites, applications, servers, networks, sensors, and mobile devices for more efficient analysis. It is particularly useful for event correlation and supports a wide variety of environments.

Splunk setup :



License selection Screen (Free License)

Change license group

The type of license group determines what sorts of licenses can be used in the pools on this license server.
[Learn more](#)

☐

Enterprise license

This license adds support for multi-user and distributed deployments, alerting, role-based security, single sign-on, scheduled PDF delivery, and unlimited data volumes.

There are no valid Splunk *Enterprise licenses* installed. You will be prompted to install a license if you choose this option.

☐

Forwarder license

Use this group when configuring Splunk as a forwarder. [Learn more](#)

☒

Free license

Use this group when you are running Splunk Free. This license has a 500MB/day daily indexing volume.
[Learn more](#)

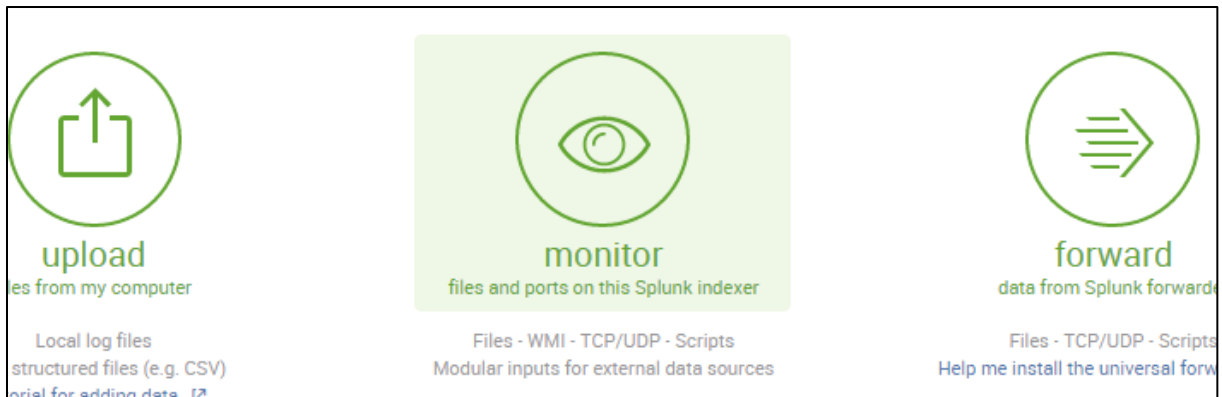
Change successful

The licensing group has been set to **Free license**. You must restart Splunk in order for changes to take effect.

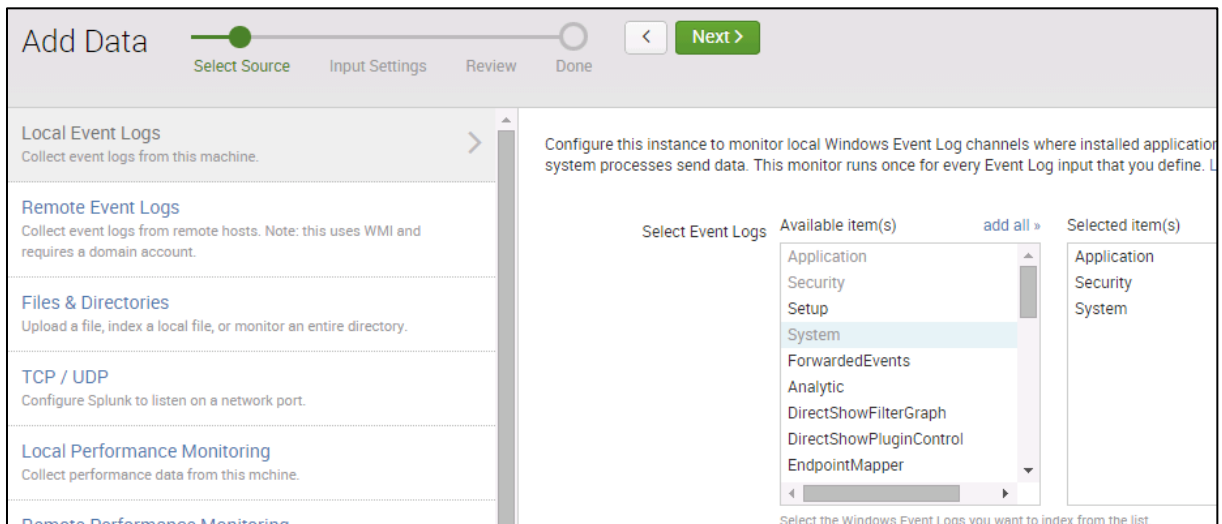
Restart later

Restart now

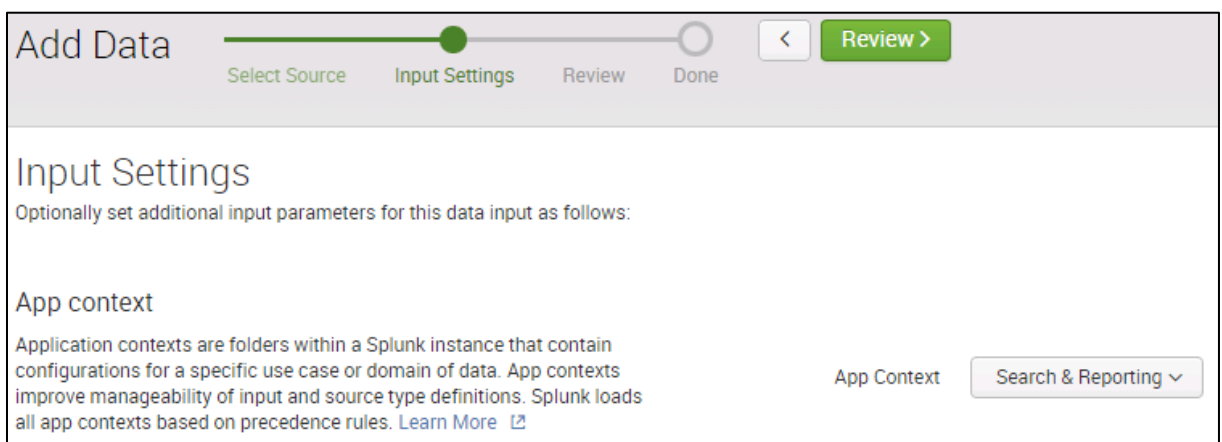
Adding data > Monitor



On the **Input Settings**, Selecting the following items : Application, Security, System.



No changes here



New Search

source="WinEventLog:*" host="WIN7-LAN"

✓ 6,562 events (before 4/1/20 1:13:12.000 PM)

Events (6,562) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect

List Format 20 Per Page < Prev 1 2 3 4 5 6 7 8

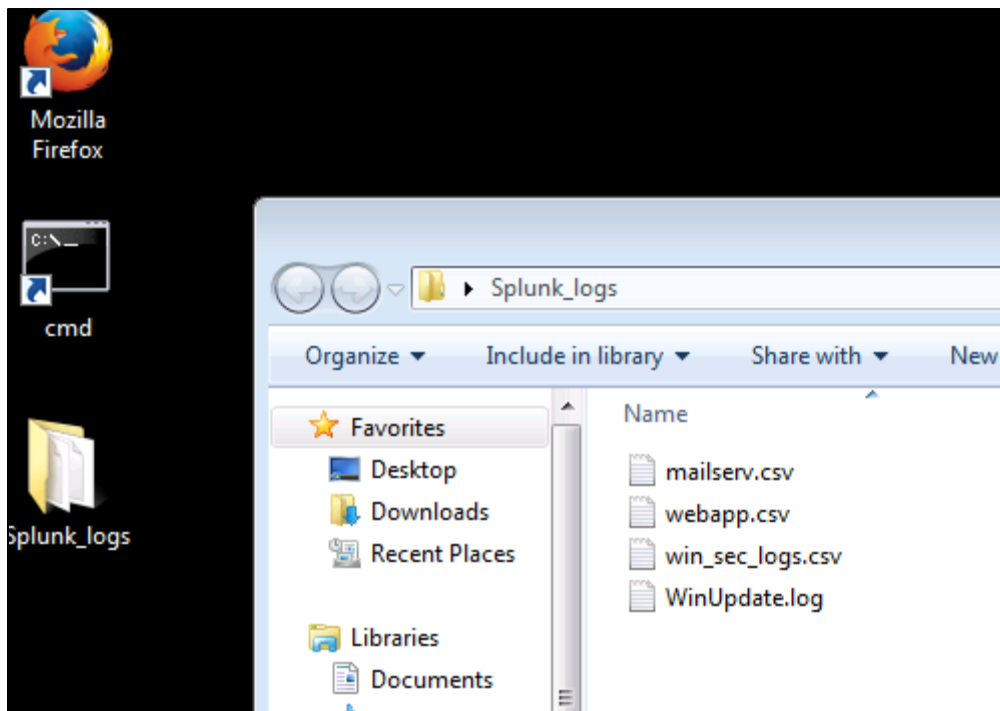
< Hide Fields All Fields		i	Time	Event
Selected Fields		>	4/1/20 12:50:58.000 PM	04/01/2020 12:50:58 PM LogName=Security SourceName=Microsoft Windows security auditing. EventCode=4672 EventType=0 Show all 27 lines
a host 1				
a source 3				
a sourcetype 3				

host = WIN7-LAN | source = WinEventLog:Security | sourcetype = WinEventLog:Security

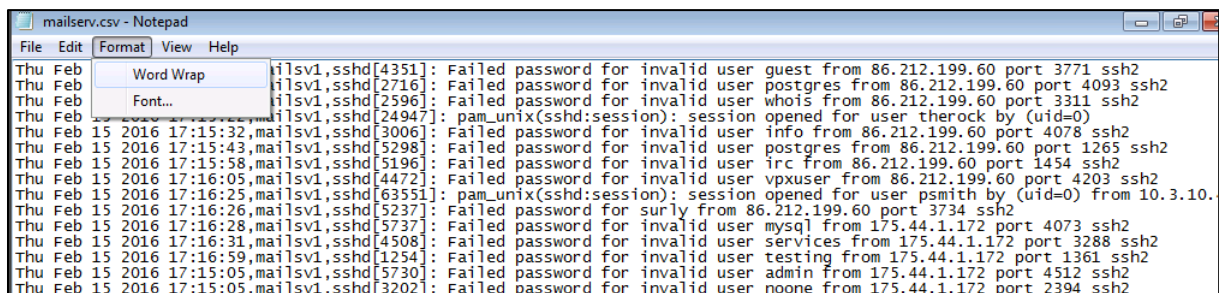
You are exploring log file correlation and analysis using the Splunk platform to test your ability to identify indicators of compromise. You have several different types of log files to ingest into the Splunk engine for analysis. Your task is to correlate information from the various logs together in order to determine what level of unauthorized system access was obtained and what application provided the access.

OS: Windows 7, Splunk version 6.2.3

I open up the Splunk-logs folder and check the data (raw form)



I open the “mailserv.csv” file and checked the “Word Wrap” to make all data lines visible without having to scroll sideways.



While checking the other files log, I see some suspicious entries:

- File downloads (someone is downloading the web folders to analyze it offline)
- High number of invalid login attempts (seems like an automatic password attack with a script or tool against the mail server via SSH)

```

hu Feb 15 2016 17:15:05,mailsv1,sshd[4351]: Failed password for invalid user guest from
86.212.199.60 port 3771 ssh2
hu Feb 15 2016 17:15:08,mailsv1,sshd[2716]: Failed password for invalid user postgres from
86.212.199.60 port 4093 ssh2
hu Feb 15 2016 17:15:15,mailsv1,sshd[2596]: Failed password for invalid user whois from
86.212.199.60 port 3311 ssh2
hu Feb 15 2016 17:15:22,mailsv1,sshd[24947]: pam_unix(sshd:session): session opened for
user therock by (uid=0)
hu Feb 15 2016 17:15:32,mailsv1,sshd[3006]: Failed password for invalid user info from
86.212.199.60 port 4078 ssh2
hu Feb 15 2016 17:15:43,mailsv1,sshd[5298]: Failed password for invalid user postgres from
86.212.199.60 port 1265 ssh2
hu Feb 15 2016 17:15:58,mailsv1,sshd[5196]: Failed password for invalid user irc from
86.212.199.60 port 1454 ssh2
hu Feb 15 2016 17:16:05,mailsv1,sshd[4472]: Failed password for invalid user vpxuser from
86.212.199.60 port 4203 ssh2
hu Feb 15 2016 17:16:25,mailsv1,sshd[63551]: pam_unix(sshd:session): session opened for
user psmith by (uid=0) from 10.3.10.46
hu Feb 15 2016 17:16:26,mailsv1,sshd[5237]: Failed password for surly from 86.212.199.60
port 3734 ssh2
hu Feb 15 2016 17:16:28,mailsv1,sshd[5737]: Failed password for invalid user mysql from
75.44.1.172 port 4073 ssh2
hu Feb 15 2016 17:16:31,mailsv1,sshd[4508]: Failed password for invalid user services from
75.44.1.172 port 3288 ssh2
hu Feb 15 2016 17:16:59,mailsv1,sshd[1254]: Failed password for invalid user testing from
75.44.1.172 port 1361 ssh2
hu Feb 15 2016 17:15:05,mailsv1,sshd[5730]: Failed password for invalid user admin from
75.44.1.172 port 4512 ssh2

```

webapp.csv - Notepad

File Edit Format View Help

```

Source IP,Time,Web Activity
24.12.76.129,[15/Feb/2016:21:40:16],""GET / HTTP/1.1"" 200 2343 ""-"" ""Mozilla/5.0
(Windows NT 6.3; WOW64; rv:30.0) Gecko/20100101 Firefox/30.0""
24.12.76.129,[15/Feb/2016:21:40:20],""GET /stylesheets/sytle.css HTTP/1.1"" 200 3012
""http://www.churchcampfire.com"" ""Mozilla/5.0 (Windows NT 6.3; WOW64; rv:20.0)
Gecko/20100101 Firefox 30.0""
24.12.76.129,[15/Feb/2016:21:40:26],""GET /wp-content/uploads/wp-id-
clefdtpiomnaropopwmjo.jpg HTTP/1.1"" 200 441
""http://www.churchcampfire.com/stylesheets/style.css"" Mozilla/5.0 (Windows NT 6.3; WOW64;
rv:20.0) Gecko/20100101 Firefox 30.0""
24.12.76.129,[15/Feb/2016:21:40:29],""GET /webstatic/mktg/Logos/paypal-logo.svg HTTP/1.1""
200 2184

```

Webapp.csv Each line shows:

- The **IP address** of the webserver visited
- **When the site was visited** (local system time-stamped)
- **GET request for item/page** (with path to item/page)
- **Server status code** (200 == OK)
- **User-agent/browser** used to request item/page (Firefox, Opera)

```

24.12.76.129,[15/Feb/2016:21:40:16],""GET / HTTP/1.1"" 200 2343 ""-"" ""Mozilla/5.0 (Windows NT 6.3; WOW64; rv:30.0)
Gecko/20100101 Firefox/30.0""
24.12.76.129,[15/Feb/2016:21:40:20],""GET /stylesheets/sytle.css HTTP/1.1"" 200 3012 ""http://www.churchcampfire.com""
""Mozilla/5.0 (Windows NT 6.3; WOW64; rv:20.0) Gecko/20100101 Firefox 30.0""
24.12.76.129,[15/Feb/2016:21:40:26],""GET /wp-content/uploads/wp-id-clefdtpiomnaropopwmjo.jpg HTTP/1.1"" 200 441
""http://www.churchcampfire.com/stylesheets/style.css"" Mozilla/5.0 (Windows NT 6.3; WOW64; rv:20.0) Gecko/20100101 Firefo
x 30.0""

```

Mailserv.csv Each line shows:

- **Time/date stamp** from the mail server for each item
- **Server "name"** (mailsv1)
- **Daemon used for sending logged item in** (sshd)
- **Error alert verbiage** (Failed...)
- **IP address of the attacking machine** (86.212.199.60)

```

86.212.199.60 port 4093 ssh2
Thu Feb 15 2016 17:15:15,mailsv1,sshd[2596]: Failed password for invalid user whois from
86.212.199.60 port 3311 ssh2
Thu Feb 15 2016 17:15:22,mailsv1,sshd[24947]: pam_unix(sshd:session): session opened for
user therock by (uid=0)
Thu Feb 15 2016 17:15:32,mailsv1,sshd[3006]: Failed password for invalid user info from
86.212.199.60 port 4078 ssh2

```

Win_sec_logs are security event log dumps from the Windows 2008 Server on the Fortan network and **WinUpdate** provides information on any missing or failed patches

The image shows two Notepad windows. The top window, titled 'win_sec_logs.csv', contains a Windows security event log entry. The entry details a successful login for the user 'dglover' from 'win2k8.fortan.local'. It lists various privileges assigned to the session, including SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeSystemEnvironmentPrivilege, and SeImpersonatePrivilege. The bottom window, titled 'WinUpdate.log', shows the initialization and startup of the Windows Update service. It includes timestamps, process IDs (920), and session IDs (31c) for various steps, such as logging initialization, process and module loading, service startup, and agent configuration.

```

win_sec_logs.csv - Notepad
File Edit Format View Help
Time,Message,Id,Task,RecordId,ProviderName,ProviderId,LogName,ProcessId,ThreadId,Machine
e,UserId,LevelDisplayName,OpcodeDisplayName,TaskDisplayName
2/16/2016 17:27,"Special privileges assigned to new logon.
Subject:
    Security ID:          S-1-5-21-2505584053-1088085678-451726313-1000
    Account Name:         dglover
    Account Domain:       win2k8.fortan.local
    Logon ID:             0x28768
Privileges:
    SeSecurityPrivilege
    SeTakeOwnershipPrivilege
    SeLoadDriverPrivilege
    SeBackupPrivilege
    SeRestorePrivilege
    SeDebugPrivilege
    SeSystemEnvironmentPrivilege
    SeImpersonatePrivilege",4672,12548,7557,Microsoft-windows-
Security-Auditing,54849625-5478-4994-a5ba-
3e3b0328c30d,Security,480,1348,win2k8.fortan.local,,Information,Info,Special Logon
2/16/2016 17:27,"An account was successfully logged on.
Subject:
    Security ID:          S-1-5-18
    Account Name:         dglover
    Account Domain:       win2k8.fortan.local
    Logon ID:             0x28768

WinUpdate.log - Notepad
File Edit Format View Help
2015-05-21 11:05:18:070 920 31c Misc ===== Logging initialized
(build: 7.5.7601.17514, tz: -0400) =====
2015-05-21 11:05:18:133 920 31c Misc = Process: C:\windows
\system32\svchost.exe
2015-05-21 11:05:18:195 920 31c Misc = Module: c:\windows
\system32\wuaueng.dll
2015-05-21 11:05:18:055 920 31c Service *****
2015-05-21 11:05:18:320 920 31c Service ** START ** Service: Service
startup
2015-05-21 11:05:18:383 920 31c Service *****
2015-05-21 11:05:18:633 920 31c Agent * WU client version
7.5.7601.17514
2015-05-21 11:05:18:695 920 31c Agent * Base directory: C:\windows
\SoftwareDistribution
2015-05-21 11:05:18:695 920 31c Agent * Access type: No proxy
2015-05-21 11:05:18:695 920 31c Agent * Network state: Connected
2015-05-21 11:05:19:289 920 31c DtaStor Default service for AU is
{00000000-0000-0000-0000-000000000000}

```

It can also get obtained with Powershell using these commands

```

Select Windows PowerShell
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Users\student> get-hotfix

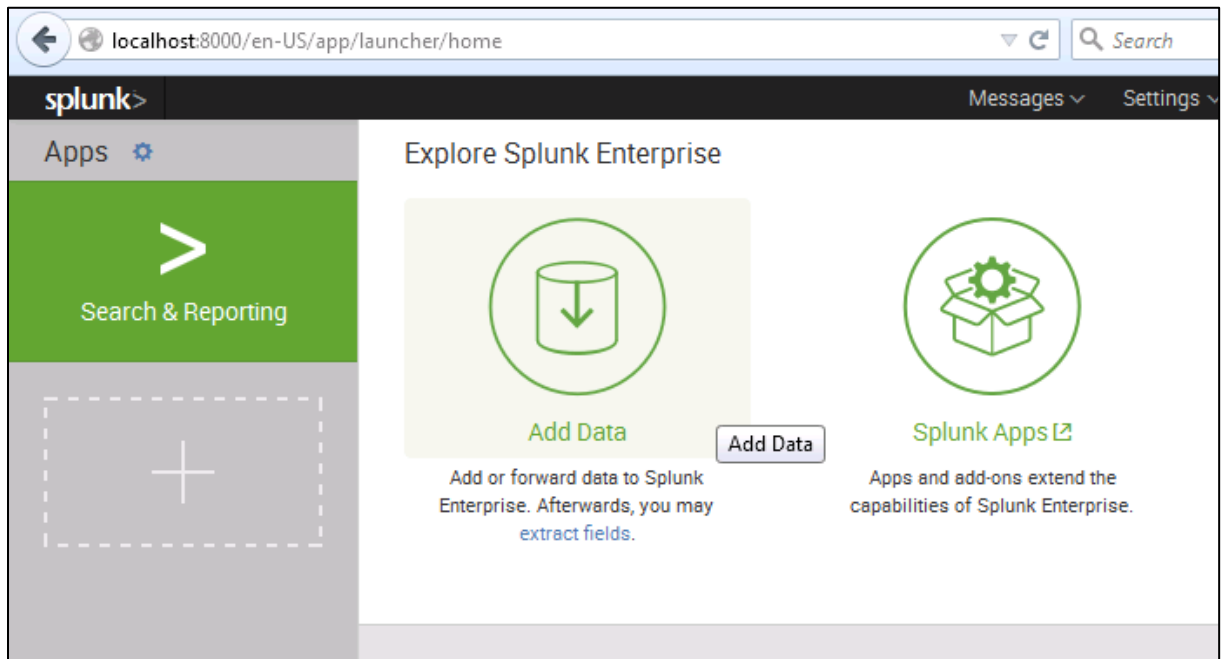
Source          Description          HotFixID          InstalledBy          InstalledOn
-----
WIN7-LAN        Update               KB955484          WIN7-LAN\student    5/21/2015 12:00:00 AM
WIN7-LAN        Hotfix              KB2534111         WIN7-LAN\student    5/21/2015 12:00:00 AM
WIN7-LAN        Security Update     KB2621440         NT AUTHORITY\SYSTEM 6/2/2015 12:00:00 AM
WIN7-LAN        Update              KB958488          WIN7-LAN\student    5/28/2015 12:00:00 AM
WIN7-LAN        Update              KB976902          WIN7-LAN\Administ... 11/21/2010 12:00:00 AM

PS C:\Users\student> wmic qfe

Caption          InstalledOn  Name  ServicePackInEffect  CSName  Description  FixComments  HotFixID
-----
dent            5/21/2015
http://support.microsoft.com/?kbid=2534111  WIN7-LAN  Update              KB955484
5/21/2015
http://support.microsoft.com/?kbid=2621440  WIN7-LAN  Security Update     KB2621440
6/2/2015
http://support.microsoft.com               WIN7-LAN  Update              KB958488
dent            5/28/2015
http://support.microsoft.com/?kbid=976902   WIN7-LAN  Update              KB976902
inistrator     11/21/2010

```

Back to the topic and Launching Splunk to add the data logs.



Adding WinUpdate

At the **Input Settings Screen**, I change the Host Field Value

Add Data

Select Source Set Sourcetype **Input Settings** Review Done

Input Settings

Optionally set additional input parameters for this data input as follows:

Host

When Splunk indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates, and can be defined based either on the path to the source data, a regular expression, or a number that represents a segment of a file path. [Learn More](#)

Constant value Regular expression on path Segment in path

Host field value:

Add Data

Select Source Set Sourcetype Input Settings Review **Done**

✓ File has been uploaded successfully.

Configure your inputs by going to Settings > [Data Inputs](#)

[Start Searching](#) Search your data now or see [examples and tutorials](#)

Once it is done I do the same process with **Webapp.csv** file. Unlike the previous log file, I leave it to csv Sourcetype.

splunk> Apps Messages Settings

Add Data

Select Source Set Sourcetype Input Settings Review Done

Set Sourcetype

Data preview lets you see how Splunk sees your data before indexing. If the events look correct and have the right timestamps, click the options below to define proper event breaks and timestamps. If you cannot find an appropriate source type for your data, create a new source type.

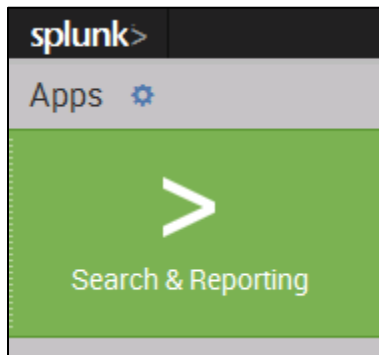
Source: **webapp.csv**

Sourcetype: csv Save As

Table Format 20 Per Page

	_time	Source IP	Time
--	-------	-----------	------

Once the four log files uploaded I click on the **Search and Reporting** tab



I searched for the Mailserv log file: there was a large amount of login failures in the mailserv log

New Search

source=mailserv.csv All time

27 events (before 4/1/20 8:24:44.000 AM)

Job Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 hour per column

	i	Time	Event
>	2/16/16 6:15:07.000 PM	Thu Feb 16 2016 18:15:07,mailsv1,sshd[21881]: pam_unix(sshd:session): session closed for user dglover by (uid=0)	host = mailserv source = mailserv.csv sourcetype = csv
>	2/16/16 6:15:05.000 PM	Thu Feb 16 2016 18:15:05,mailsv1,sshd[46748]: Received disconnect from 10.3.10.135: disconnected by user	host = mailserv source = mailserv.csv sourcetype = csv
>	2/16/16 5:27:11.000 PM	Thu Feb 16 2016 17:27:11,mailsv1,sshd[12190]: pam_unix(sshd:session): session opened for user dglover by (uid=0) from 10.3.10.135	host = mailserv source = mailserv.csv sourcetype = csv

Selected Fields: host, source, sourcetype

Interesting Fields: date_hour, date_mday

Webapp log : some suspicious files being downloaded followed by a POST activity from the Windows system to a remote page

< Hide Fields

All Fields

List

Format

20 Per Page

< Prev 1 2 Next >

a date_zone 1	i	Time	Event
a index 1	>	2/15/16 9:40:30.000 PM	24.12.76.129,[15/Feb/2016:21:40:30],""GET /xmlrpc.php HTTP/1.1"" 200 54 ""-"" ""Opera\\9.64"" host = webapp source = webapp.csv sourcetype = csv
# linecount 1	>	2/15/16 9:40:33.000 PM	72.111.89.104,[15/Feb/2016:21:40:33],""GET /wp-content/plugins/cforms/js/include/fil esforyou.exe HTTP/1.1"" 404 8816 ""-"" ""Opera\\9.64"" host = webapp source = webapp.csv sourcetype = csv
a punct 16	>	2/15/16 9:40:38.000 PM	72.111.89.104,[15/Feb/2016:21:40:38],""GET /wp-content/plugins/cforms/js/include/you rresume.exe HTTP/1.1"" 404 8816 ""-"" ""Opera\\9.64"" host = webapp source = webapp.csv sourcetype = csv
a Source IP 4	>	2/15/16 9:40:41.000 PM	72.111.89.104,[15/Feb/2016:21:40:41],""GET /wp-content/plugins/cforms/js/include/fil esforyou.exe HTTP/1.1"" 404 8816 ""-"" ""Opera\\9.64"" host = webapp source = webapp.csv sourcetype = csv
a splunk_server 1	>	2/15/16 9:40:44.000 PM	72.111.89.104,[15/Feb/2016:21:40:44],""GET /wp-content/plugins/cforms/js/include/you rresume.exe HTTP/1.1"" 404 8816 ""-"" ""Opera\\9.64"" host = webapp source = webapp.csv sourcetype = csv
a Time 23	>	2/15/16 9:40:49.000 PM	72.111.89.104,[15/Feb/2016:21:40:49],""GET /xmlrpc.php HTTP/1.1"" 200 54 ""-"" ""Ope ra\\9.64"" host = webapp source = webapp.csv sourcetype = csv
# timeendpos 2	>	2/15/16 9:40:51.000 PM	72.111.89.104,[15/Feb/2016:21:40:51],""GET /xmlrpc.php HTTP/1.1"" 200 54 ""-"" ""Ope ra\\9.64"" host = webapp source = webapp.csv sourcetype = csv
# timestartpos 2	>	2/15/16 9:41:26.000 PM	72.111.89.104,[15/Feb/2016:21:41:26],""POST /wp-content/plugins/cforms/js/include/in stalled.php HTTP/1.1"" 200 5269 ""http://churchcampfire.com/installed.php"" host = webapp source = webapp.csv sourcetype = csv
a Web Activity 19			
Extract New Fields			

win_sec_logs.csv: a user account called **gam3r** was created at 9:57 pm on 2/15/16.

2/15/16 2/15/2016 21:57, "A user account was created."
9:57:00.000 PM
Subject:
Security ID: S-1-5-21-2505584053-1088085678-451726313-1001
Account Name: gam3r
Account Domain: win2k8.fortan.local
Logon ID: 0x651cd

New Account:
Security ID: S-1-5-21-2505584053-1088085678-451726313-1002
Account Name: admin
Account Domain: win2k8.fortan.local

The **gam3r** account was added to the Admin group obtaining privileges.

New Search

Save As

source=win_sec_logs.csv security-enabled

All time

3 events (before 5/4/17 1:49:00.000 PM)

Job

||

→

↓

🖨

💡 Smart

Events (3)

Patterns

Statistics

Visualization

Format Timeline

Zoom Out

Zoom to Selection

Deselect

1 millisecond

List

Format

20 Per Page

Hide Fields

All Fields

i

Time

Event

Selected Fields

host 1

source 1

sourcetype 1

2/15/16

2/15/2016 21:57, "A member was added to a security-enabled global group.

9:57:00.000 PM

Subject:

Security ID: S-1-5-21-2505584053-1088085678-451726313-1001

Account Name: gam3r

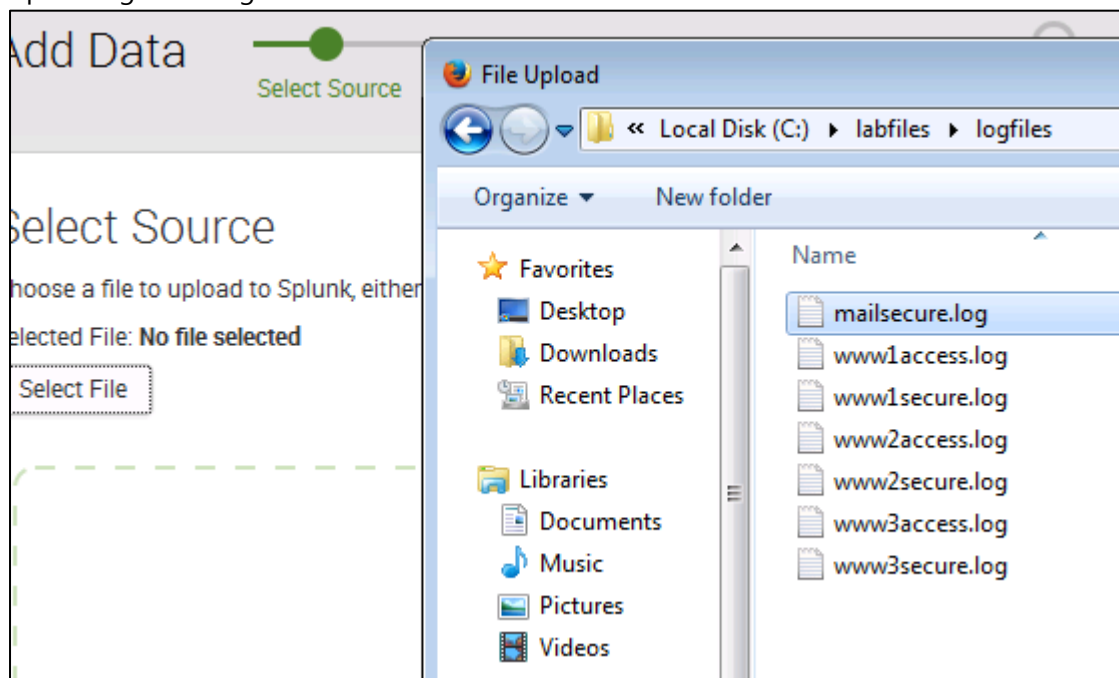
Account Domain: win2k8.fortan.local

Show all 15 lines

host = win_sec : source = win_sec_logs.csv : sourcetype = csv

numerous attempts to gain ssh access to the mail server. We then noticed a user had clicked on a link that downloaded an application onto his computer - this happened on the same system that was reported to have suffered from erratic system behavior. Once the application was downloaded, it attempted to create a user called **gam3r** and then add it to the administrator group. After the user was added to the administrator group, the attacker would have full access to the machine. However, thanks to your sharp eye in catching the activity the application will be removed from the system and mitigations will be put into place in order to stop future breaches via this same program.

Uploading more log files



Those logs look complicated to read

```
mailsecure.log - Notepad
File Edit Format View Help

Thu Nov 17 2014 00:15:05 mailsrv1 sshd[4351]: Failed password for invalid user guest from
86.212.199.60 port 3771 ssh2Thu Nov 17 2014 00:15:05 mailsrv1 sshd[2716]: Failed password
for invalid user postgres from 86.212.199.60 port 4093 ssh2Thu Nov 17 2014 00:15:05 mailsrv1
sshd[2596]: Failed password for invalid user whois from 86.212.199.60 port 3311 ssh2Thu Nov
17 2014 00:15:05 mailsrv1 sshd[24947]: pam_unix(sshd:session): session opened for user
djohnson by (uid=0)Thu Nov 17 2014 00:15:05 mailsrv1 sshd[3006]: Failed password for invalid
user info from 86.212.199.60 port 4078 ssh2Thu Nov 17 2014 00:15:05 mailsrv1 sshd[5298]:
Failed password for invalid user postgres from 86.212.199.60 port 1265 ssh2Thu Nov 17 2014
00:15:05 mailsrv1 sshd[5196]: Failed password for invalid user irc from 86.212.199.60 port
1454 ssh2Thu Nov 17 2014 00:15:05 mailsrv1 sshd[4472]: Failed password for invalid user
vpxuser from 86.212.199.60 port 4203 ssh2Thu Nov 17 2014 00:15:05 mailsrv1 sshd[63551]:
pam_unix(sshd:session): session opened for user djohnson by (uid=0)Thu Nov 17 2014 00:15:05
mailsv1 sshd[5237]: Failed password for surly from 86.212.199.60 port 3734 ssh2Thu Nov 17
2014 00:15:05 mailsrv1 sshd[5737]: Failed password for invalid user mysql from 175.44.1.172
port 4073 ssh2Thu Nov 17 2014 00:15:05 mailsrv1 sshd[4508]: Failed password for invalid user
services from 175.44.1.172 port 3288 ssh2Thu Nov 17 2014 00:15:05 mailsrv1 sshd[1254]:
Failed password for invalid user testing from 175.44.1.172 port 1361 ssh2Thu Nov 17 2014
00:15:05 mailsrv1 sshd[46748]: Received disconnect from 10.3.10.46 11: disconnected by user
Thu Nov 17 2014 00:15:05 mailsrv1 sshd[5730]: Failed password for invalid user admin from
175.44.1.172 port 4512 ssh2Thu Nov 17 2014 00:15:05 mailsrv1 sshd[3202]: Failed password for
invalid user noone from 175.44.1.172 port 2394 ssh2Thu Nov 17 2014 00:15:05 mailsrv1 sshd
[5555]: Failed password for invalid user noone from 175.44.1.172 port 2326 ssh2Thu Nov 17
2014 00:15:05 mailsrv1 sshd[1258]: Failed password for invalid user web002 from 175.44.1.172
port 4851 ssh2Thu Nov 17 2014 00:15:05 mailsrv1 sshd[12190]: pam_unix(sshd:session): session
opened for user djohnson by (uid=0)Thu Nov 17 2014 00:15:05 mailsrv1 sshd[5240]: Failed
password for invalid user sys from 175.44.1.172 port 1317 ssh2Thu Nov 17 2014 00:15:05
mailsv1 sshd[4814]: Failed password for backup from 175.44.1.172 port 2985 ssh2Thu Nov 17

www1access.log - Notepad
File Edit Format View Help

209.160.24.63 - - [17/Nov/2014:18:22:16] "GET /product.screen?productId=WC-SH-
A02&JSESSIONID=SD0SL6FF7ADFF4953 HTTP 1.1" 200 3878 "http://www.google.com" "Mozilla/5.0
(Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46
Safari/536.5" 349209.160.24.63 - - [17/Nov/2014:18:22:16] "GET /oldlink?itemId=EST-
6&JSESSIONID=SD0SL6FF7ADFF4953 HTTP 1.1" 200 1748 "http://www.buttercupgames.com/oldlink?
itemId=EST-6" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko)
Chrome/19.0.1084.46 Safari/536.5" 731209.160.24.63 - - [17/Nov/2014:18:22:17] "GET
/product.screen?productId=BS-AG-G09&JSESSIONID=SD0SL6FF7ADFF4953 HTTP 1.1" 200 2550
"http://www.buttercupgames.com/product.screen?productId=BS-AG-G09" "Mozilla/5.0 (Windows NT
6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 422
209.160.24.63 - - [17/Nov/2014:18:22:19] "POST /category.screen?
categoryId=STRATEGY&JSESSIONID=SD0SL6FF7ADFF4953 HTTP 1.1" 200 407
```

Add Data

Select Source

Set Sourcetype

Input Settings

Review

Done

<Review >

Input Settings

Optionally set additional input parameters for this data input as follows:

Host

When Splunk indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates, and can be defined based either on the path to the source data, a regular expression, or a number that represents a segment of a file path. [Learn More](#)

Constant value

Regular expression on path

Segment in path


Host field value

mailserver

In order to get syslog data from a remote system into Splunk. I used the monitor option instead of uploading. I have to authorize TCP/UDP input. I use TCP since its is more reliable on port 20000.

Add Data


How do you want to add data?



upload

files from my computer

Local log files
Local structured files (e.g. CSV)
[Tutorial for adding data](#)



monitor

files and ports on this Splunk indexer

Files - WMI - TCP/UDP - Scripts
Modular inputs for external data sources

Add Data Progress: Select Source (1/4) Next >

Local Event Logs
Collect event logs from this machine.

Remote Event Logs
Collect event logs from remote hosts. Note: this uses WMI and requires a domain account.

Files & Directories
Upload a file, index a local file, or monitor an entire directory.

TCP / UDP
Configure Splunk to listen on a network port. >

Local Performance Monitoring

Configure this instance to listen on any TCP or UDP port to capture data sent over the network (such as syslog). [Learn More](#)

☒ TCP ☐ UDP

Port ?
Example: 139

Source name override ?
host:port

Only accept connection from ?

On the next page I modify the Sourcetype to “syslog” and Host to “IP”

Add Data Progress: Input Settings (2/4) Review >

Input Settings
Optionally set additional input parameters for this data input as follows:

Sourcetype
The source type is one of the default fields that Splunk assigns to all incoming data. It tells Splunk what kind of data you've got, so that Splunk can format the data intelligently during indexing. And it's a way to categorize your data, so that you can search it easily.

Select Manual

App context
Application contexts are folders within a Splunk instance that contain configurations for a specific use case or domain of data. App contexts improve manageability of input and source type definitions. Splunk loads all app contexts based on precedence rules. [Learn More](#)

App Context

Host
When Splunk indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates, and can be defined based either on the path to the source data, a regular

Method ? ☒ IP ☐ DNS ☐ Custom

Once it is done, I switch to a Kali linux machine and modifying the “rsyslog.conf” which logs system messages on unix systems


```
File Edit View Search Terminal Help
root@kali-lan:~# locate rsyslog.conf
/etc/rsyslog.conf
/usr/share/man/man5/rsyslog.conf.5.gz
/var/lib/dpkg/info/rsyslog.conf.files
root@kali-lan:~#
```

```
root@kali-lan: ~
File Edit View Search Terminal Help
GNU nano 2.2.6 File: /etc/rsyslog.conf

# /etc/rsyslog.conf Configuration file for rsyslog.
#
# For more information see
# /usr/share/doc/rsyslog-doc/html/rsyslog_conf.html

#####
#### MODULES ####
#####

$ModLoad imuxsock # provides support for local system logging
$ModLoad imklog    # provides kernel logging support
#$ModLoad immark   # provides --MARK-- message capability
```

I had some issue with nano so I used another file editor and added these line at the end of the document

```
$ModLoad imfile
$InputFileName /var/log/nginx/error.log
$InputFileTag nginx:
$InputFileStateFile stat-nginx-error
$InputFileSeverity error
$InputRunFileMonitor

$InputFilePollingInterval 10

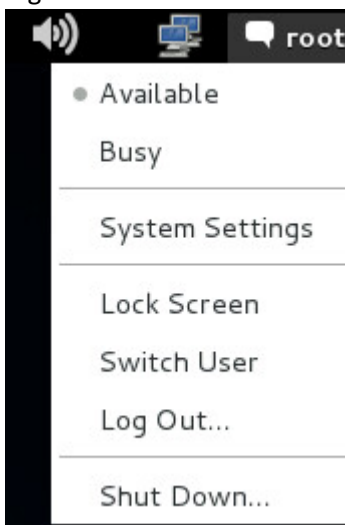
*.* @@192.168.0.30:20000
```

```
*rsyslog.conf
File Edit Search Options Help
#       busy site..
#
daemon.*;mail.*;\
        news.err;\
        *.*=debug;*.*=info;\
        *.*=notice;*.*=warn      | /dev/xconsole
#To send data to splunk server
$ModLoad imfile
$InputFileName /var/log/nginx/error.log
$InputFileTab nginx:
$InputFileStateFile stat-nginx-error
$InputRunFileMonitor

$InputFilePollingInterval 10

*.* @@192.168.0.30:20000
```

Right after that I rebooted the linux machine



Once it rebooted it typed the following command:

```
root@kali-lan: ~
File Edit View Search Terminal Help
root@kali-lan:~# logger -t test "this is a test of splunk forwarding"
root@kali-lan:~#
```

Once back in the Splunk search interface I checked if I could forward logs across a network to splunk interface. It works.

SearchPivotReportsAlertsDashboards

Search & Rep

New Search

Save As

"this is a test"

All time

✓ 1 event (before 3/16/15 11:24:08.000 AM)

JobPauseRefreshDownloadPrintSmart

Events (1)PatternsStatisticsVisualization

Format TimelineZoom OutZoom to SelectionDeselect1 millisecond per

ListFormat50 Per Page

< Hide Fields

All Fields

i	Time	Event
>	3/16/15 11:23:56.000 AM	<13>Mar 16 11:23:56 kali-lan test: this is a test of splunk forwarding host = kali-lan source = tcp:20000 sourcetype = syslog

Selected Fields