

#JonSecOps

End-to-End Brute-Force Attack Simulation and Monitoring in an AD Environment

FIGURE 1: LOGICAL DIAGRAM

SIEM / Active Directory / Brute Force Attack Project

Network: 192.168.10/24

Splunk Server VM: 192.168.10.10

Windows Server / Active Directory VM: 192.168.10.7

Kali / Attacker Machine VM: 192.168.10.250

Windows 10 / Target PC VM: 192.168.10.100

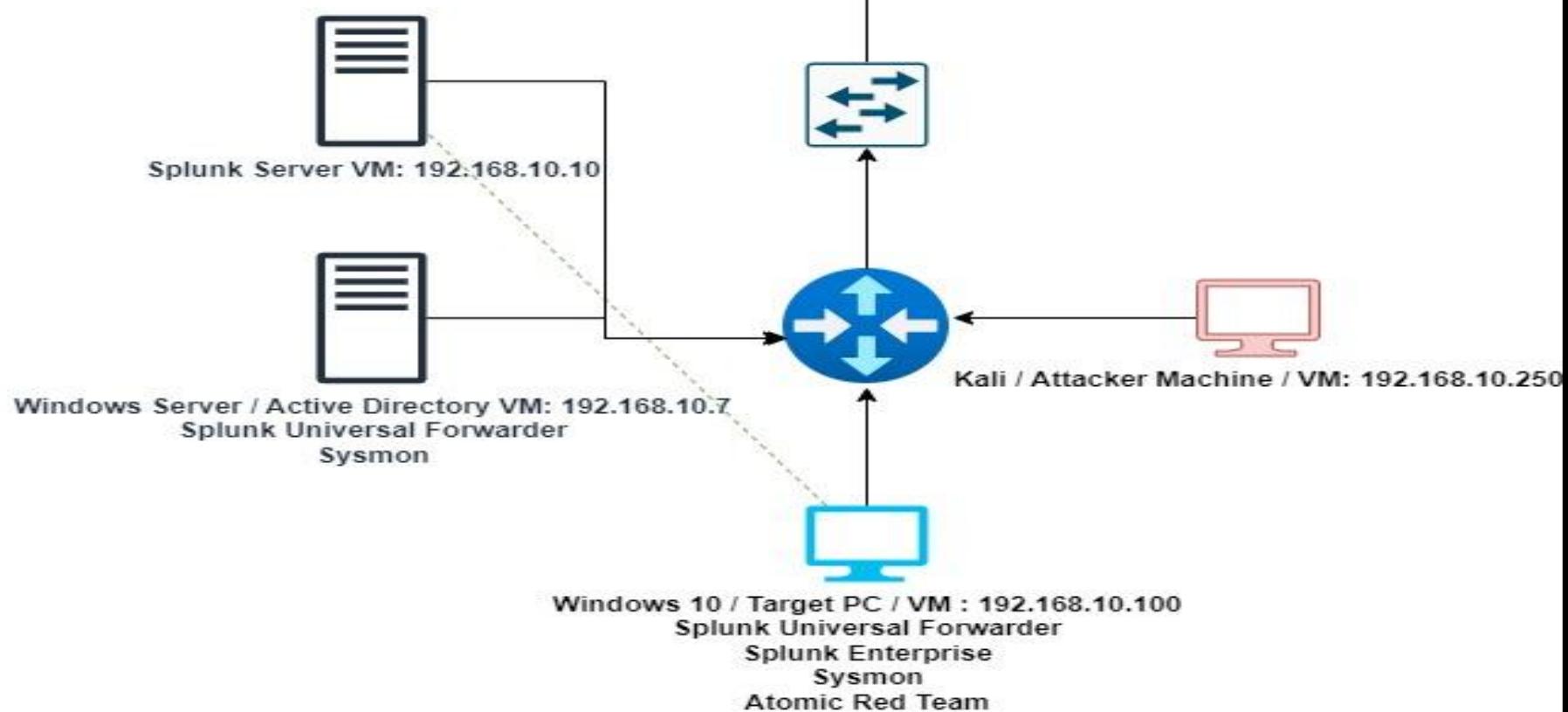


FIGURE 2: SYSTEM CONFIGURATIONS



Splunk Server: 192.168.10.10

- Installed Splunk on an Ubuntu server.
- Upgraded the server using sudo apt-get upgrade.
- Configured the Splunk server's IP address as a static IP to match the logical design.
- Added a user after installing Splunk on the Ubuntu server.



Windows Server / Active Directory: 192.168.10.7
Splunk Universal Forwarder
Sysmon

- Configured the computer name to ACTDIRSERVER.
- Assigned a static IP address to align with the logical design.
- Installed the Splunk Universal Forwarder and configured the inputs.conf file by copying it from the etc/system/default directory to the local folder. This defined the data to forward to the Splunk server.
- Installed Sysmon.
- Configured receiving settings and set the port to 9997 to ensure the Splunk server can receive data.
- Configured Server Manager to add roles and features, including the Active Directory Domain Services role.
- Promoted the server to a domain controller and created a new forest.
- Created users in Active Directory for a brute-force attack simulation using a Kali/attacker machine.



Windows 10 / Target PC : 192.168.10.100
Splunk Universal Forwarder
Splunk Enterprise
Sysmon
Atomic Red Team

- Renamed the computer to TARGET-PC.
- Configured a static IP address to align with the logical design.
- Installed the Splunk Universal Forwarder, created a copy of the inputs.conf file from the etc/system/default directory, and pasted it into the local folder to define the data to forward to the Splunk server.
- Installed Sysmon.
- Created an index called endpoint in Splunk Enterprise to collect telemetry from the configured input file in Splunk Universal Forwarder.
- Configured Splunk Enterprise receiving settings to use port 9997, ensuring the Splunk server can receive data.
- Connected the Windows target machine to the ACTDIRSERVER domain controller (LAB.local) and authenticated using the Jenny Smith account.
- Configured the Active Directory server with two users.
- Installed Atomic Red Team to simulate attacks and generate telemetry visible in Splunk.
- Enabled Remote Desktop access for Active Directory users jsmith and tsmith.

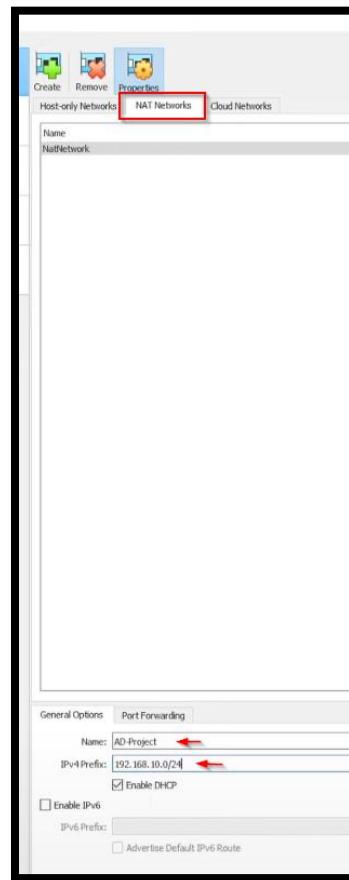


Kali / Attacker Machine: 192.168.10.250

- Configured a static IP address to match the logical design.
- Installed the Crowbar tool.
- Created a directory named Lab-project.
- Located the rockyou wordlist pre-installed in Kali Linux under the usr/share/wordlists directory.
- Unzipped the rockyou.txt file and copied it to the Lab-project directory.
- Extracted the first 20 lines from the rockyou.txt file and saved them in a new file named passwords.txt.
- Edited the passwords.txt file to include the Active Directory users' passwords, used for the brute-force password attack.
- Conducted a successful brute-force password attack against the Active Directory users.
- Captured the telemetry in Splunk, including EventCode 4625, indicating failed login attempts for the accounts.

Kali Linux, Windows 10, Windows Server 2022 and Splunk Server software was installed. Once the virtual machines for these systems were created, the NAT Network settings within VirtualBox was changed so that all created virtual machines will be on the same network called AD-Project. The IPv4 address was changed to 192.168.10.0/24 which coincides with the IP address within the logical diagram.

FIGURE 3: NAT NETWORK SETTINGS CONFIGURATION

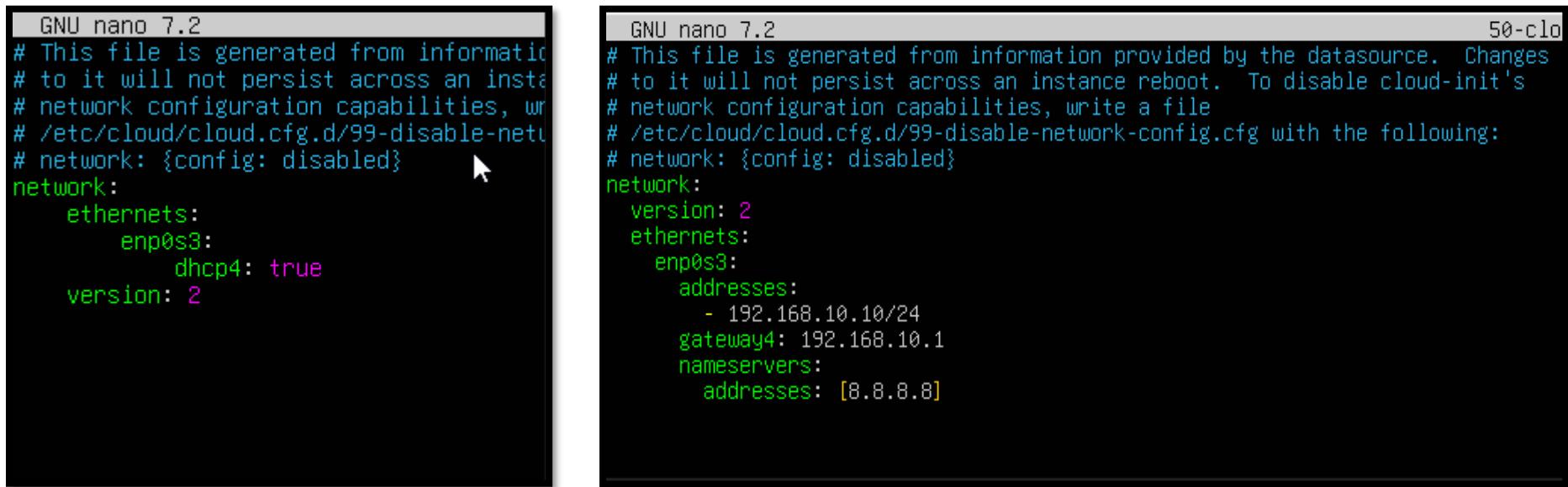


The splunk servers IP address was changed to match the IP address within the logical diagram which is 192.168.10.10. The '**`sudo nano /etc/netplan/50-cloud-init.yaml`**' command was used to change this.

```
jm@splunk:~$ sudo nano /etc/netplan/50-cloud-init.yaml
```

Once entered, the following network configurations were made within the yaml file. Displayed is the original configurations next to the changed configurations. Once completed the ‘**sudo netplan apply**’ command was used to allow the configuration changes. The ‘**ip a**’ command was used to display the newly created IP address of 192.168.10.10.

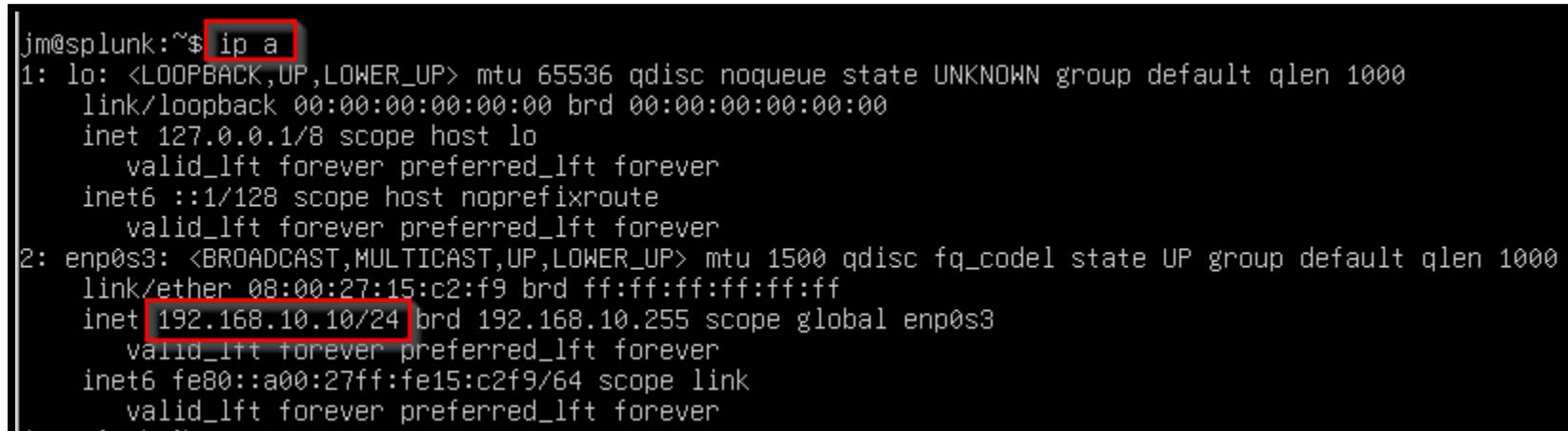
FIGURE 4: SPLUNK SERVER NETWORK ADDRESS CONFIGURATIONS



The figure consists of two side-by-side terminal windows. Both windows have a black background and white text. The left window is titled "GNU nano 7.2" and shows the original network configuration. The right window is also titled "GNU nano 7.2" and shows the modified configuration after changes were made. The right window has a small "50-clo" label in the top right corner.

```
GNU nano 7.2
# This file is generated from information
# to it will not persist across an instance
# network configuration capabilities, write a file
# /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg with the following:
# network: {config: disabled}
network:
  ethernets:
    enp0s3:
      dhcp4: true
version: 2

50-clo
GNU nano 7.2
# This file is generated from information provided by the datasource. Changes
# to it will not persist across an instance reboot. To disable cloud-init's
# network configuration capabilities, write a file
# /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg with the following:
# network: {config: disabled}
network:
  version: 2
  ethernets:
    enp0s3:
      addresses:
        - 192.168.10.10/24
      gateway4: 192.168.10.1
      nameservers:
        addresses: [8.8.8.8]
```



The figure shows a single terminal window with a black background and white text. The command 'ip a' is entered at the prompt. The output lists network interfaces: 'lo' (loopback) and 'enp0s3' (ethernet). The 'enp0s3' interface has an IP address of 192.168.10.10/24, which is highlighted with a red box. Other details like MTU, queueing discipline (qdisc), broadcast range (brd), and link layer information are also listed.

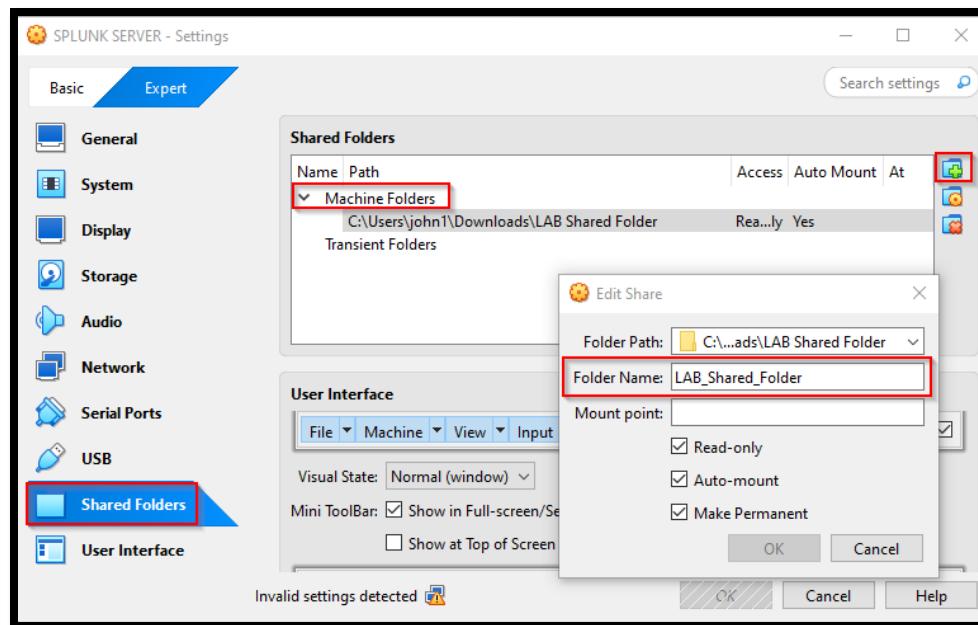
```
jm@splunk:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
  link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
  inet 127.0.0.1/8 scope host lo
    valid_lft forever preferred_lft forever
  inet6 ::1/128 scope host noprefixroute
    valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
  link/ether 08:00:27:15:c2:f9 brd ff:ff:ff:ff:ff:ff
  inet 192.168.10.10/24 brd 192.168.10.255 scope global enp0s3
    valid_lft forever preferred_lft forever
  inet6 fe80::a00:27ff:fe15:c2f9/64 scope link
    valid_lft forever preferred_lft forever
```

Splunk Enterprise for Linux was then downloaded on the host machine. Within the Splunk Server the guest add-ons for Virtual Box needed to be installed so the ‘**sudo apt-get install virtualbox-guest-additions-iso**’ command was entered.

```
jm@splunk:~$ sudo apt-get install virtualbox-guest-additions-iso
```

To share folders from the host machine to the Splunk Server machine, the Splunk Server Vms shared folder settings was configured and a folder named LAB_Shared_Folder was created. The downloaded Splunk Enterprise file was then copied to the LAB_Shared_Folder folder on the host system.

FIGURE 5: ALLOWING HOST COMPUTER TO SHARE FILES WITH SPLUNK SERVER VM



To add a user to the vboxsf group in the Splunk Server the ‘**sudo apt-get install virtualbox-guest-utils**’ command was entered followed by the ‘**sudo adduser jm vboxsf**’ command.

```
jm@splunk:~$ sudo apt-get install virtualbox-guest-utils
```

```
jm@splunk:~$ sudo adduser jm vboxsf
```

To make a directory called *share*, the ‘**mkdir share**’ command was entered followed by the ‘ls -la’ command to display the created directory.

```
jm@splunk:~$ ls -la
total 40
drwxr-x--- 5 jm jm 4096 Feb 10 16:30 .
drwxr-xr-x 3 root root 4096 Dec 12 01:24 ..
-rw----- 1 jm jm 1394 Dec 16 16:16 .bash_history
-rw-r--r-- 1 jm jm 220 Mar 31 2024 .bash_logout
-rw-r--r-- 1 jm jm 3771 Mar 31 2024 .bashrc
drwx----- 2 jm jm 4096 Dec 12 01:25 .cache
-rw----- 1 jm jm 20 Feb 10 16:30 .lesshist
-rw-r--r-- 1 jm jm 807 Mar 31 2024 .profile
drwxrwxr-x 2 jm jm 4096 Dec 12 02:04 share
drwx----- 2 jm jm 4096 Dec 12 01:25 .ssh
-rw-r--r-- 1 jm jm 0 Dec 12 01:25 .sudo_as_admin_successful
```

To mount the created LAB_Shared_Folder on our host machine to our created directory named *share* within the Splunk Server, the ‘**sudo mount -t vboxsf -o uid=1000, gid=1000 LAB_Shared_Folder share/**’ was entered. To install the Splunk Enterprise file from the host system to the Splunk server the ‘**cd share**’ command was used followed by the ‘**sudo dpkg -i splunk-9.2.0.1-d8ae995bf219-linux-2.6-amd.64.deb**’ command.

(add image)

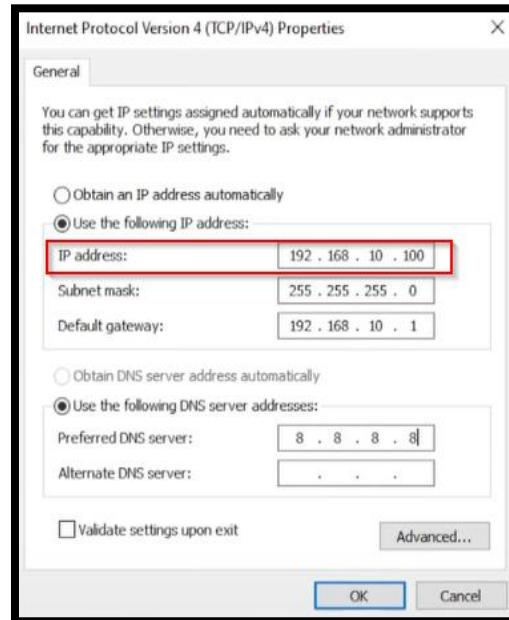
After installation the ‘**sudo -u splunk bash**’ command was entered to change to the user *splunk*. The ‘**cd bin**’ command was entered to get into splunk’s binary files and the ‘**./splunk start**’ command was entered to run the installer.

```
jm@splunk:/opt/splunk$ sudo -u splunk bash
splunk@splunk:~$ cd bin
splunk@splunk:~/bin$ ./splunk start
```

After the administrator and username creation for splunk, the ‘exit’ command was entered to switch back to the user jm. The ‘cd bin’ command was used to get into the binary files, and the ‘sudo ./splunk enable boot-start -user splunk’ to allow splunk to run with the user splunk after the vm reboots.

```
splunk@splunk:~/bin$ exit  
exit  
jm@splunk:/opt/splunk$ cd bin  
jm@splunk:/opt/splunk/bin$ sudo ./splunk enable boot-start -user splunk
```

The Windows 10 machine name was changed to Target PC and its IP address was changed to 192.168.10.100 within the network settings.



On the Windows 10 Target PC machine, Spunk Universal Forwarder was installed/configured and Sysmon with installed with olaf configuration (sysmonconfig.xml) from github.

If you intend to use a Splunk receiving indexer to configure this UniversalForwarder, please specify the host or IP, and port (default port is 9997). This is an optional step. However, UniversalForwarder needs either a deployment server or receiving indexer in order to do anything.

Receiving Indexer

Hostname or IP
192.168.10.10 : 9997
Enter the hostname or IP of your receiving indexer, e.g. ds.splunk.com

Cancel Back Next

olafhartong / sysmon-modular Public

Code Issues 27 Pull requests 14 Discussions Actions Projects Wiki Security

sysmon-modular / sysmonconfig.xml

Azure Pipeline Updated after successful CI/CD run ... a9ff298 · 5 months ago History

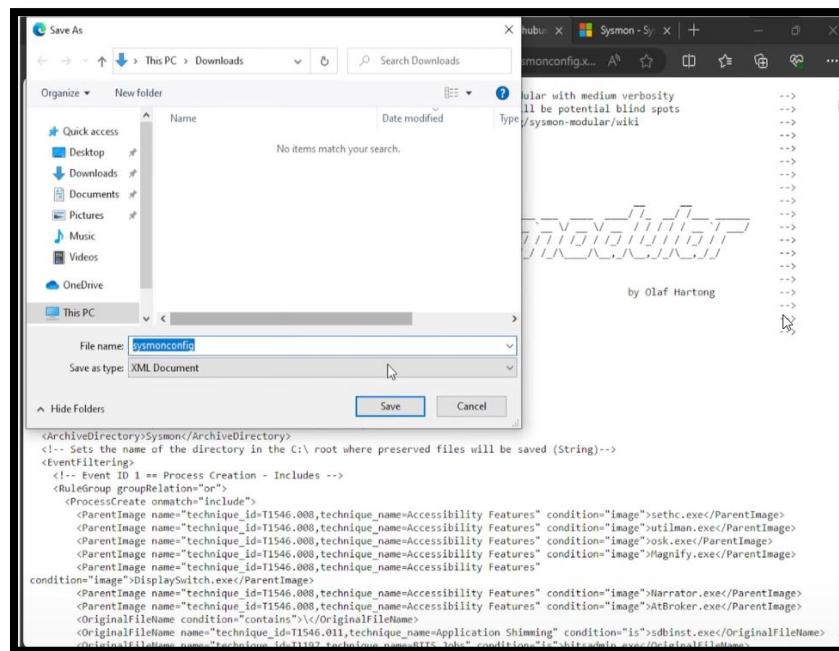
Code Blame 2704 lines (2704 loc) · 247 KB Raw

```

1 <!-- NOTICE : This is a balanced generated output of Sysmon-->
2 <!-- due to the balanced nature of this configuration there w-->
3 <!-- for more information go to https://github.com/olafharton-->
4 <!--
5 <!-- /**
6 <!-- //** */
7 <!-- ((&&&*+
8 <!-- ,(((((((((. **&&(
9 <!-- (((&&(((((((((((//**&&(
10 <!-- (&&(((((((((((((((//&(
11 <!-- &///(((((((((((//&(
12 <!-- ((/ ((((((/(((/
13 <!-- &(((#./((((((( #((((&(
14 <!-- &&(((#./(((((((#(&&(

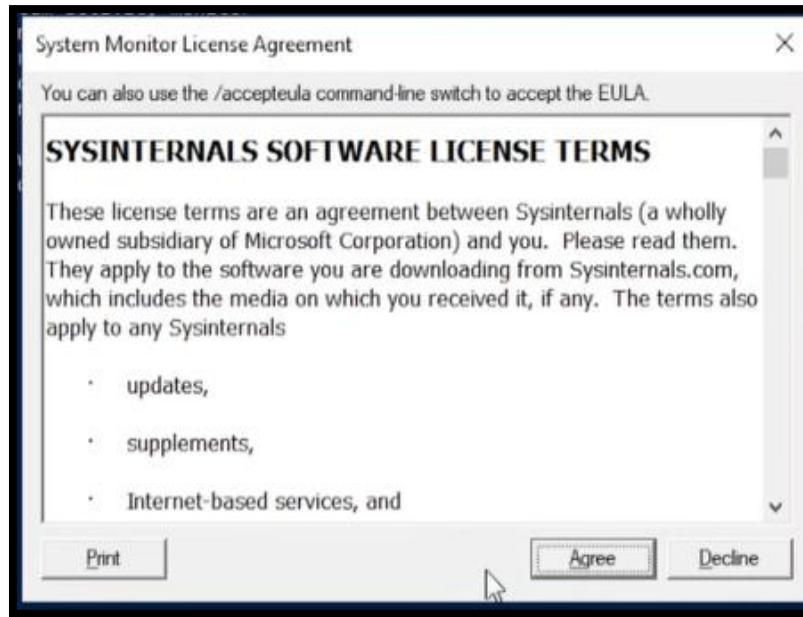
```

The sysmon configuration file was then saved to the Target PC.

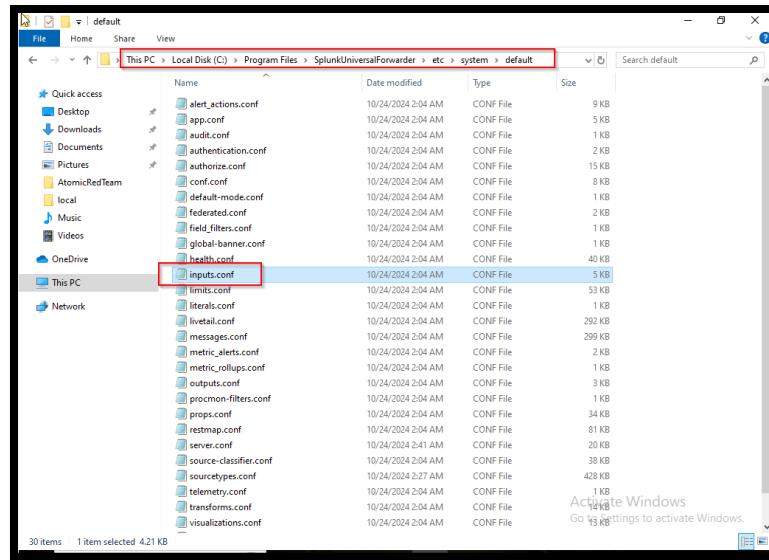


Sysmon was installed using the following command

```
PS C:\Users\TARGET PC\Downloads\Sysmon> .\Sysmon64.exe -i ..\sysmonconfig.xml
```



To instruct our installed splunk forwarder on what we want to send over to our splunk server the inputs.conf in the SplunkUniversalForwarder default folder needs to be copied and configured in the SplunkUniversalForwarders local folder.



The copied inputs.conf is first opened and configured in notepad as an administrator and saved in the local folder.

The image contains two side-by-side screenshots. The left screenshot shows a Notepad window titled 'inputs.conf - Notepad'. The content of the file is as follows:

```
[WinEventLog://Application]
index = endpoint
disabled = false

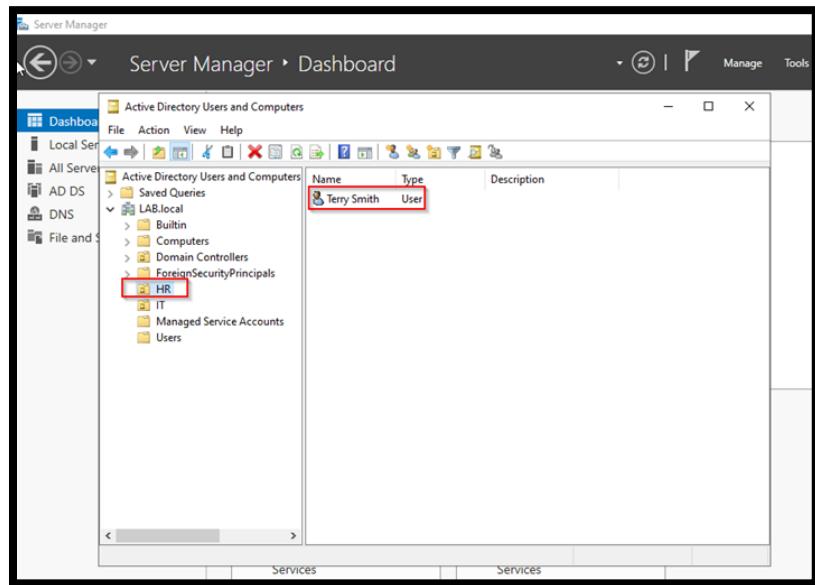
[WinEventLog://Security]
index = endpoint
disabled = false

[WinEventLog://System]
index = endpoint
disabled = false

[WinEventLog://Microsoft-Windows-Sysmon/Operational]
index = endpoint
disabled = false
renderXml = true
source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational
```

The right screenshot shows a Windows File Explorer window. The path is 'This PC > etc > system > local'. The 'inputs.conf' file is selected and highlighted with a red box. The file is a CONF File, modified on 2/15/2024 at 5:10 PM, and is 1 KB in size. Other files in the folder include 'authentication.conf', 'outputs.conf', 'README', and 'server.conf'. A status bar at the bottom shows '5 items'.

FIGURE 3: ADDED USERS IN ACTIVE DIRECTORY SERVER



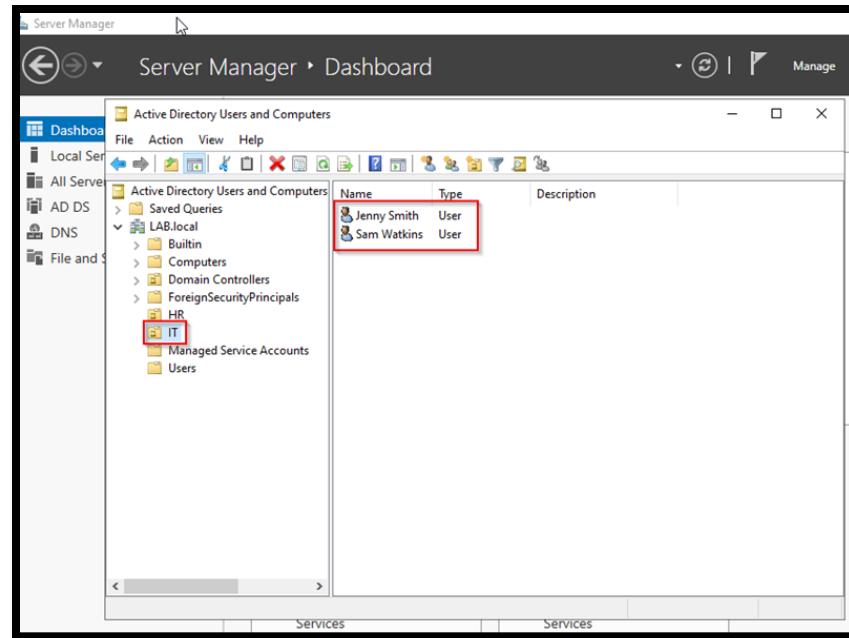


FIGURE 4: KALI / ATTACKER MACHINE COMMANDS

```
(kali㉿kali)-[~]
$ cd /usr/share/wordlists
(kali㉿kali)-[/usr/share/wordlists]
$ ls
amass dirb dirbuster dnsmap.txt fasttrack.txt fern-wifi john.lst legion metasploit nmap.lst rockyou.txt.gz
(kali㉿kali)-[/usr/share/wordlists]
$ sudo gunzip rockyou.txt.gz
(kali㉿kali)-[/usr/share/wordlists]
$ ls
amass dirb dirbuster dnsmap.txt fasttrack.txt fern-wifi john.lst legion metasploit nmap.lst rockyou.txt sc
(kali㉿kali)-[/usr/share/wordlists]
$ cp rockyou.txt ~/Desktop/lab-project
```

(kali㉿kali)-[~/Desktop/lab-project]

```
$ ls -lh
total 134M
-rw-r--r-- 1 kali kali 134M Dec 12 17:56 rockyou.txt
```

(kali㉿kali)-[~/Desktop/lab-project]

```
$ head -n 20 rockyou.txt > passwords.txt
```

(kali㉿kali)-[~/Desktop/lab-project]

```
$ cat passwords.txt
```

```
123456
12345
123456789
password
iloveyou
princess
1234567
rockyou
12345678
abc123
nicole
daniel
babygirl
monkey
lovely
jessica
654321
michael
ashley
qwerty
superdummy@4
superduper@4
baller2024@4
```

(kali㉿kali)-[~/Desktop/lab-project]

```
File Actions Edit View Help
GNU nano 8.2
```

```
123456
12345
123456789
password
iloveyou
princess
1234567
rockyou
12345678
abc123
nicole
daniel
babygirl
monkey
lovely
jessica
654321
michael
ashley
qwerty
superdummy@4
superduper@4
baller2024@4
```

(kali㉿kali)-[~/Desktop/lab-project]

```
$ cat passwords.txt
```

```
123456
12345
123456789
password
iloveyou
princess
1234567
rockyou
12345678
abc123
nicole
daniel
babygirl
monkey
lovely
jessica
654321
michael
ashley
qwerty
superdummy@4 → Jenny Smiths Password
superduper@4 → Terry Smiths Password
baller2024@4 → Sam Watkins Password
```

FIGURE 5: SUCCESSFUL BRUTE FORCE ATTACK

(kali㉿kali)-[~/Desktop/lab-project]

```
$ crowbar -b rdp -u tsmith -C passwords.txt -s 192.168.10.100/32
```

2024-12-12 18:03:19 START

2024-12-12 18:03:19 Crowbar v0.4.2

2024-12-12 18:03:19 Trying 192.168.10.100:3389

2024-12-12 18:03:24 RDP-SUCCESS : 192.168.10.100:3389 - tsmith:superduper@4

2024-12-12 18:03:24 STOP

FIGURE 6: SPLUNK TELEMETRY OF BRUTE FORCE ATTACK ON TARGET MACHINE

index="endpoint" tsmith EventCode=4625

✓ 148 events (12/12/24 9:00:00.000 PM to 12/13/24 9:38:11.000 PM)

No Event Sampling ▾

Events (148) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect 1 hour per column

List ▾ ✓ Format 20 Per Page ▾ < Prev 1 2 3 4 5 6 7 8 Next >

i	Time	Event
>	12/13/24 12:34:48.000 AM	12/12/2024 07:34:48 PM ... 20 lines omitted ... Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: tsmith Account Domain: Show all 61 lines

< Hide Fields

SELECTED FIELDS

- # EventCode 1
- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS

- a Account_Domain 1
- a Account_Name 2

EventCode = 4625 host = TARGET5PC source = WinEventLog:Security sourcetype = WinEventLog:Security

Search | Splunk 9.3.1

Windows Security Log Event ID 4625

Not secure | 192.168.10.10:8000/en-US/app/search/search?q=search%20index%204625

< Hide Fields All Fields List Format 20 Per Page < Prev 1 2 3 4 5 6 7 8 Next >

	i	Time	Event
# LineCount 1			<p>Account For Which Logon Failed:</p> <p>Security ID: S-1-0-0</p> <p>Account Name: tsmith</p> <p>Account Domain:</p>
a LogName 1			<p>Failure Information:</p> <p>Failure Reason: Unknown user name or bad password.</p> <p>Status: 0xC000006D</p> <p>Sub Status: 0xC000006A</p>
a Logon_ID 1			<p>Process Information:</p> <p>Caller Process ID: 0x0</p> <p>Caller Process Name: -</p>
a Logon_Process 1			<p>Network Information:</p> <p>Workstation Name: kali</p> <p>Source Network Address: 192.168.10.250</p> <p>Source Port: 0</p>
# Logon_Type 1			<p>Detailed Authentication Information:</p> <p>Logon Process: NtLmSsp</p> <p>Authentication Package: NTLM</p> <p>Transited Services: -</p> <p>Package Name (NTLM only): -</p> <p>Key Length: 0</p>
a Message 1			
a OpCode 1			
a Package_Name__NTLM_only_ 1			
a punct 1			
# RecordNumber 100+			
a Security_ID 1			
a Source_Network_Address 1			
# Source_Port 1			
a SourceName 1			
a splunk_server 1			
a Status 1			
a Sub_Status 1			
a TaskCategory 1			
a Transited_Services 1			
a Type 1			
a Workstation_Name 1			
+ Extract New Fields			

Activate Windows



Ultimate IT
SECURITY

December 2024
Patch Tuesday

sponsored by LOGbinder

User name:

Password:

/ [Forgot?](#)

[Register](#)

Security Log Windows SharePoint SQL Server Exchange | Training Tools Newsletter Webinars Blog

Webinars Training Encyclopedia Quick Reference Book

Encyclopedia

- Event IDs
- All Event IDs
- Audit Policy

Go To Event ID:

Security Log
Quick Reference
Chart



⇒ Windows Security Log Event ID 4625 ⇒

4625: An account failed to log on

On this page

- Description of this event
- Field level details
- Examples

This is a useful event because it documents each and every failed attempt to logon to the local computer regardless of logon type, location of the user or type of account.

Free Security Log Resources by Randy

Operating Systems	Windows 2008 R2 and 7 Windows 2012 R2 and 8.1 Windows 2016 and 10 Windows Server 2019 and 2022
Category	Logon/Logoff
Subcategory	Logon
Type	Failure
Corresponding events in Windows 2003 and before	529 , 530 , 531 , 532 , 533 , 534 , 535 , 536 , 537 , 539

index="endpoint" tsmith EventCode=4624

Last 24 hours 

✓ 5 events (12/12/24 10:00:00.000 PM to 12/13/24 10:00:34.000 PM)

No Event Sampling ▾

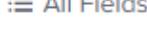
Events (5) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect 1 hour per column



List ▾ Format 20 Per Page ▾

Time	Event
12/13/24 12:34:47.000 AM	... 26 lines omitted ... New Logon: Security ID: S-1-5-21-3968765168-2457327897-4288992809-1 106 Account Name: tsmith Account Domain: LAB
Show all 70 lines	
EventCode = 4624 host = TARGET5PC source = WinEventLog:Security sourcetype = WinEventLog:Security	

< Hide Fields  All Fields i Time Event

SELECTED FIELDS # EventCode 1 a host 1 a source 1 a sourcetype 1

INTERESTING FIELDS a Account_Domain 2 a Account_Name 2 a Authentication_Package 1

Event			
		Message=An account was successfully logged on.	
Subject:			
		Security ID:	S-1-0-0
		Account Name:	-
		Account Domain:	-
		Logon ID:	0x0
Logon Information:			
		Logon Type:	3
		Restricted Admin Mode:	-
		Virtual Account:	No
		Elevated Token:	No
Impersonation Level:			Impersonation
New Logon:			
106		Security ID:	S-1-5-21-3968765168-2457327897-4288992809-1
		Account Name:	tsmith
		Account Domain:	LAB
		Logon ID:	0x19B002F
		Linked Logon ID:	0x0
		Network Account Name:	-
		Network Account Domain:	-
		Logon GUID:	{00000000-0000-0000-0000-000000000000}

Search | Splunk 9.3.1

Windows Security Log Event ID 4624

https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event....

Click to go back (Alt+Left arrow), hold to see history

December 2024 Patch Tuesday

"Pat

User name:
Password:
[Login](#) / [Forgot?](#)
[Register](#)

Ultimate IT SECURITY

Security Log Windows SharePoint SQL Server Exchange | Training Tools Newsletter Webinars Blog

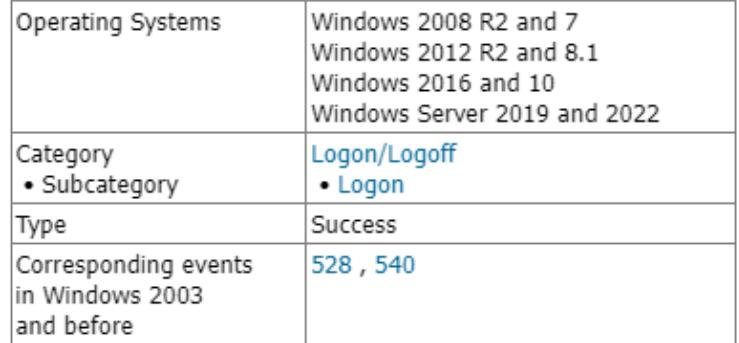
Webinars Training Encyclopedia Quick Reference Book

Encyclopedia

- Event IDs
- All Event IDs
- Audit Policy

Go To Event ID: Go

Security Log Quick Reference Chart



Windows Security Log Event ID 4624

4624: An account was successfully logged on

On this page

- Description of this event
- [Field level details](#)
- [Examples](#)

This is a highly valuable event since it documents each and every successful attempt to logon to the local computer regardless of logon type, location of the user or type of account. You can tie this event to logoff events [4634](#) and [4647](#) using Logon ID.

Win2012 adds the Impersonation Level field as shown in the example.
Win2016/10 add further fields explained below.

Search | Splunk 9.3.1 Windows Security Log Event ID 4648

← ⌛ Not secure | 192.168.10.10:8000/en-US/app/search/search?q=search%20index%204648

No Event Sampling

Events (20,250) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection × Deselect 1 h

EventCode

>100 Values, 33.995% of events

Selected Yes No

Reports

Average over time Maximum value over time Minimum value over time

Top values Top values by time Rare values

Events with this field

Avg: 5009.49128413713 Min: 0 Max: 51057 Std Dev: 3034.6035876147666

Top 10 Values Count %

Value	Count	%
4624	1,774	25.77%
4672	1,639	23.809%
4634	1,554	22.574%
7036	490	7.118%
4625	301	4.372%
5379	254	3.69%
4799	101	1.467%
566	63	0.915%
16394	51	0.741%
16384	50	0.726%

Activate Windows
Go to Settings to activate

SELECTED FIELDS

- # EventCode 100+
- a host 2
- a source 4
- a sourcetype 4

INTERESTING FIELDS

- a Account_Domain 7
- a Account_Name 22
- a ComputerName 2
- # EventType 4
- a Guid 1
- a index 1
- a Keywords 8
- # linecount 31
- a LogName 3
- a Logon_ID 100+
- a Message 100+
- a Name 2