Project Overview

This project simulates a Security Operations Center (SOC) environment using VMware Player 17. It includes a Splunk Enterprise SIEM server, a Snort IDS, Kali and a Windows endpoint, and Window server(Active Directory) all connected within a VMnet8(NAT) network. The lab is designed to replicate Tier 1 SOC analyst workflows such as log ingestion, threat detection, investigation, and incident response

Lab Topology & IP Plan

VMnet8(NAT): **192.168.15.0/24**

Assigned IPs:

- VM1 (Splunk:Ubuntu server): **192.168.15.11**

- VM2 (Snort: Ubuntu Desktop server): **192.168.15.10**

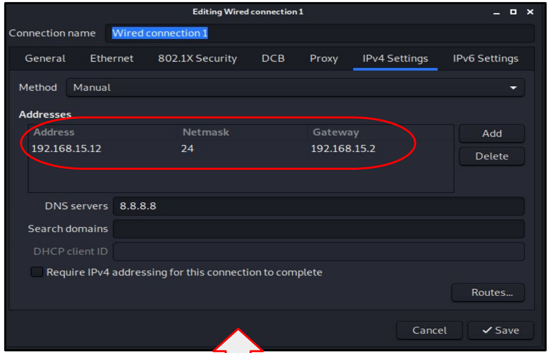
- VM3 (Kali): **192.168.15.12**

- VM3 (Windows Endpoint): **192.168.15.13**

- VM4 Windows server (Active Directory): **192.168.15.14**

- Ubuntu Server: https://ubuntu.com/download/server
- Ubuntu Server; https://ubuntu.com/download/desktop
- Kali: https://www.kali.org/get-kali/#kali-installer-images
- Windows11: https://www.microsoft.com/en-gb/software-download/windows1
- Windows Server: https://info.microsoft.com/ww-landing-evaluate-windows-server-2025.html?lcid=en-us&culture=en-us&country=us

Network Adapter configuration



Connection name: Wired connection 1

Method: Manual

Addresses

Address	Netmask	Gateway
192.168.15.12	24	192.168.15.2

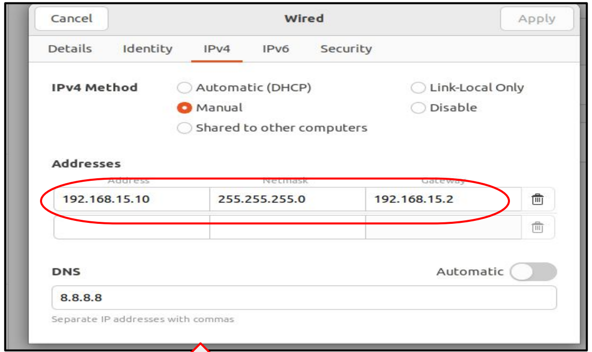
DNS servers: 8.8.8.8

Search domains:

DHCP client ID:

□ Require IPv4 addressing for this connection to complete

- Inside the **Kali** vm locate the network adapter in the top right corner
- Right click →Edit connections→wired connection1→select gear icon→IPV4 settings→Manual→Add
- Enter the IP address, Netmask, Gateway and DNS and click save



IPv4 Method

○ Automatic (DHCP)
● Manual
○ Shared to other computers
○ Link-Local Only
○ Disable

Addresses

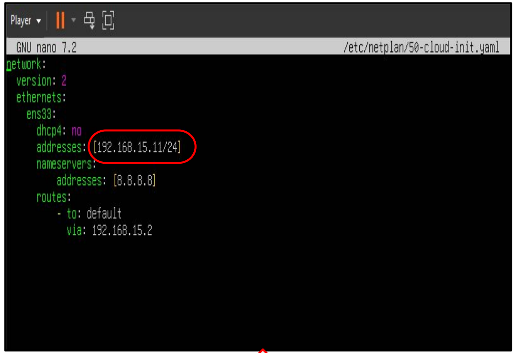
Address	Netmask	Gateway
192.168.15.10	255.255.255.0	192.168.15.2

DNS — Automatic: off

8.8.8.8

Separate IP addresses with commas

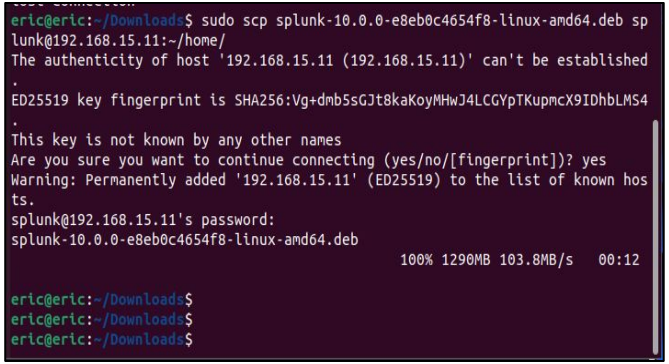
- Inside the **Ubuntu** vm locate the network adapter in the top right corner and right click
- Then select→Settings→gear icon→IPV4 settings→Manual→Add
- Enter the IP address, Netmask, Gateway and DNS and click save



```
GNU nano 7.2                                   /etc/netplan/50-cloud-init.yaml
network:
  version: 2
  ethernets:
    ens33:
      dhcp4: no
      addresses: [192.168.15.11/24]
      nameservers:
          addresses: [8.8.8.8]
      routes:
          - to: default
            via: 192.168.15.2
```

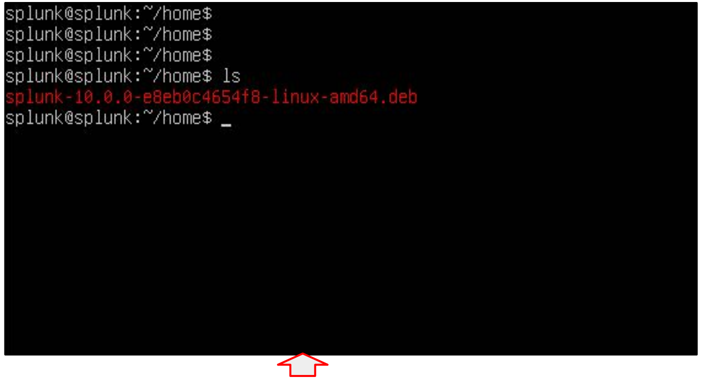
- Inside the Ubuntu live server vm**(splunk)**
- Enter the command *“sudo nano /etc/netplan/50-cloud-init.yaml”* to edit the file
- Enter the configurations and save file
- Then run the command “sudo netplan apply” in the terminal

Splunk file transfer



```
eric@eric:~/Downloads$ sudo scp splunk-10.0.0-e8eb0c4654f8-linux-amd64.deb sp
lunk@192.168.15.11:~/home/
The authenticity of host '192.168.15.11 (192.168.15.11)' can't be established
.
ED25519 key fingerprint is SHA256:Vg+dmb5sGJt8kaKoyMHwJ4LCGYpTKupmcX9IDhbLMS4
.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.15.11' (ED25519) to the list of known hos
ts.
splunk@192.168.15.11's password:
splunk-10.0.0-e8eb0c4654f8-linux-amd64.deb
                                            100% 1290MB 103.8MB/s   00:12

eric@eric:~/Downloads$
eric@eric:~/Downloads$
eric@eric:~/Downloads$
```

- In the “ubuntu desktop” vm go to “ “splunk.com” create an account and download splunk enterprise for linux(deb)
- In the terminal navigate to “Download” directory
- Copy the “splunk file” to the “ubuntu server” vm ***“scp splunkfile user@192.168.**.*:~/home/***



```
splunk@splunk:~/home$
splunk@splunk:~/home$
splunk@splunk:~/home$
splunk@splunk:~/home$ ls
splunk-10.0.0-e8eb0c4654f8-linux-amd64.deb
splunk@splunk:~/home$ _
```

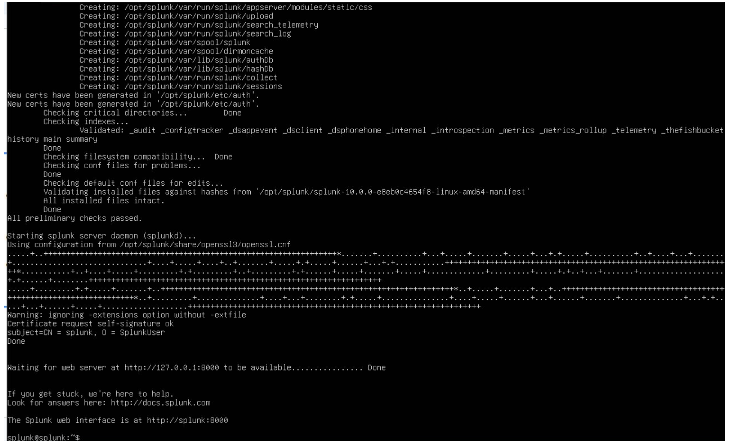
- In to Ubuntu server navigate to home directory and run “*ls*” command to list the content in the directory
- Splunk file was successfully copy to the vm machine

Before copying the file

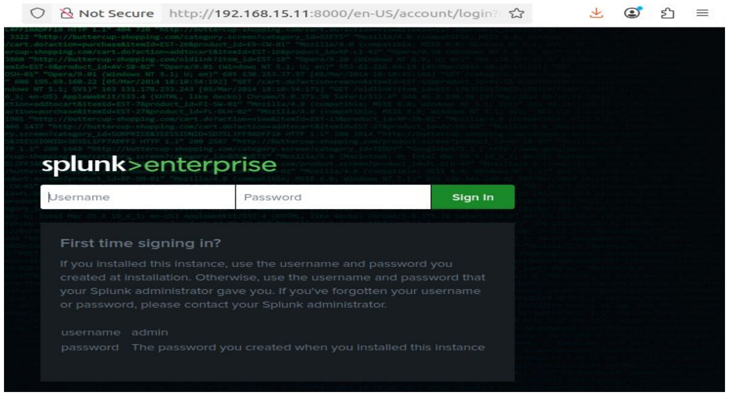
- **in ubuntu server**
- **Create a directory, home *“mkdir home”***
- **install ssh server *“sudo install openssh-server -y”***
- **Update firewall *“sudo ufw allow 22/tcp”***

Install the splunk package

- In the “home” directory run ***“sudo dpkg -i splunk-10.0.deb***
- Splunk will install into: ***/opt/splunk***
- Then run ***“sudo /opt/splunk/bin/splunk start -- accept-license”*** to accept license and set admin username and password, re-enter password to confirm
- In the firewall allow splunk web(port 8000) and forwarding(port 9997): ***sudo ufw allow 8000/tcp, sudo allow 9997/tcp, sudo ufw reload***
- Navigate to browser to access splunk web at ***http://192.168.15.11:8000***



```
                Creating: /opt/splunk/var/run/splunk/appserver/modules/static/css
                Creating: /opt/splunk/var/run/splunk/upload
                Creating: /opt/splunk/var/run/splunk/search_telemetry
                Creating: /opt/splunk/var/run/splunk/search_log
                Creating: /opt/splunk/var/spool/splunk
                Creating: /opt/splunk/var/spool/dirmoncache
                Creating: /opt/splunk/var/lib/splunk/authDb
                Creating: /opt/splunk/var/lib/splunk/hashDb
                Creating: /opt/splunk/var/run/splunk/collect
                Creating: /opt/splunk/var/run/splunk/sessions
New certs have been generated in '/opt/splunk/etc/auth'.
New certs have been generated in '/opt/splunk/etc/auth'.
        Checking critical directories...        Done
        Checking indexes...
                Validated: _audit _configtracker _dsappevent _dsclient _dsphonehome _internal _introspection _metrics _metrics_rollup _telemetry _thefishbucket
history main summary
        Done
        Checking filesystem compatibility...  Done
        Checking conf files for problems...
        Done
        Checking default conf files for edits...
        Validating installed files against hashes from '/opt/splunk/splunk-10.0.0-e8eb0c4654f8-linux-amd64-manifest'
        All installed files intact.
        Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
Using configuration from /opt/splunk/share/openssl3/openssl.cnf
.....+..+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*.......+.........+...+.....+.......+.....+...+.+.....+.........+..+....+...+.......
+............................+....+.....+....+..+.......+.....+.+.....+......+...+.+..........+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++*..........+..+....+.....+.........+.+.........+..+.........+.+.....+.....+.......+.....+.............+.........+.....+.+..+...+.......+................
+.+......+........++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
.....+.........+.+.....+.......+..+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*..+.....+.......+...+..+++++++++++++++++++++++++++++++++
+++++++++++++++++++++++++++*..+.........+..............+....+...+........+.+.....+...............+....+.....+......+...+......+.......+.............+...+.+..
...+...+......+.....+..................+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
Warning: ignoring -extensions option without -extfile
Certificate request self-signature ok
subject=CN = splunk, O = SplunkUser
Done


Waiting for web server at http://127.0.0.1:8000 to be available............... Done


If you get stuck, we're here to help.
Look for answers here: http://docs.splunk.com

The Splunk web interface is at http://splunk:8000

splunk@splunk:~$
```



First time signing in?

If you installed this instance, use the username and password you created at installation. Otherwise, use the username and password that your Splunk administrator gave you. If you've forgotten your username or password, please contact your Splunk administrator.

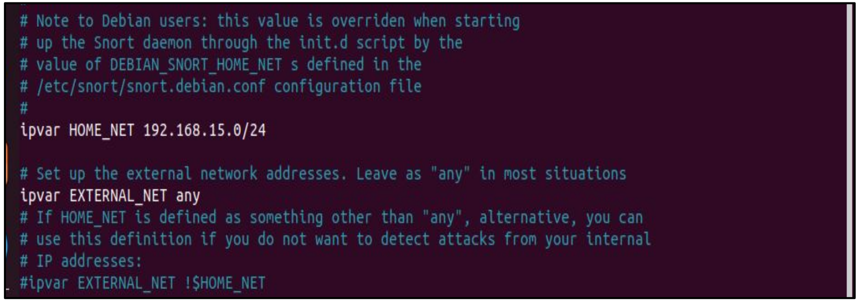
username admin
password The password you created when you installed this instance

Splunk universal forwarder installation

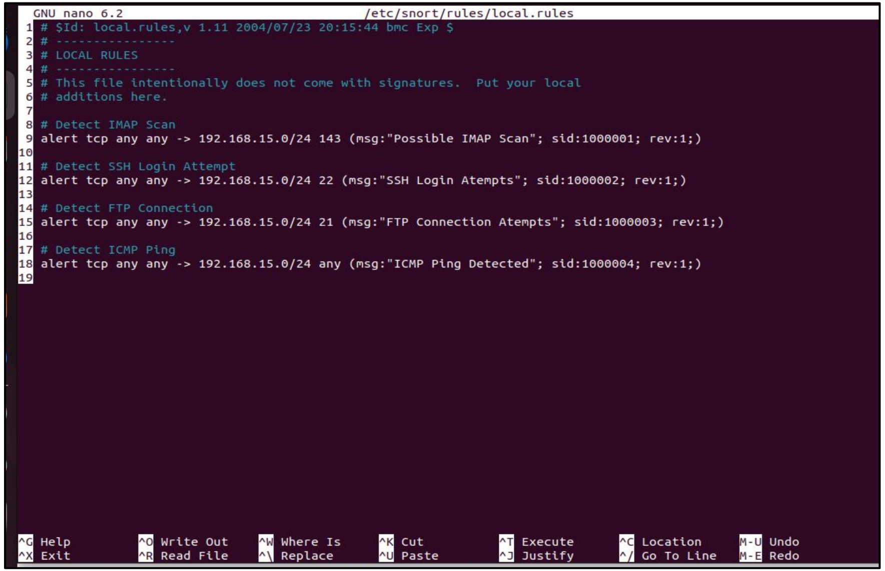
Next step is to install snort(IDS) and splunk universal forwarder in ubuntu desktop machine and configure to forward snort logs to the splunk server @192.168.15.11

Snort installation

- In the terminal run ***"sudo apt install snort -y"***
- Navigate to the snort.conf to configure($HOME_NET any) ***"sudo nano /etc/snort/snort.conf"*** change "any" to 192.168.15.0/24 and save
- Navigate to "local.rules" to write snort rules to detect icmp ping, IMAP scan, ssh login attempts and ftp connection, ***"sudo nano /etc/snort/rules/local.rules"*** and save
- Run ***"sudo snort -q -A console -i <interface> -T -c /etc/snort/rules/local.rules"*** to text the rules in terminal.



```
# Note to Debian users: this value is overriden when starting
# up the Snort daemon through the init.d script by the
# value of DEBIAN_SNORT_HOME_NET s defined in the
# /etc/snort/snort.debian.conf configuration file
#
ipvar HOME_NET 192.168.15.0/24

# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any
# If HOME_NET is defined as something other than "any", alternative, you can
# use this definition if you do not want to detect attacks from your internal
# IP addresses:
#ipvar EXTERNAL_NET !$HOME_NET
```



```
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# ----------------
# LOCAL RULES
# ----------------
# This file intentionally does not come with signatures.  Put your local
# additions here.

# Detect IMAP Scan
alert tcp any any -> 192.168.15.0/24 143 (msg:"Possible IMAP Scan"; sid:1000001; rev:1;)

# Detect SSH Login Attempt
alert tcp any any -> 192.168.15.0/24 22 (msg:"SSH Login Atempts"; sid:1000002; rev:1;)

# Detect FTP Connection
alert tcp any any -> 192.168.15.0/24 21 (msg:"FTP Connection Atempts"; sid:1000003; rev:1;)

# Detect ICMP Ping
alert tcp any any -> 192.168.15.0/24 any (msg:"ICMP Ping Detected"; sid:1000004; rev:1;)
```

Splunk Universal Forwarder installation

In the Ubuntu desktop vm, go the splunk.com in browser create an account and download splunk forwarder for linux

- Open terminal, navigate to “Download” directory and run ***“sudo dpkg -i splunkforwarder-10.0.deb”***

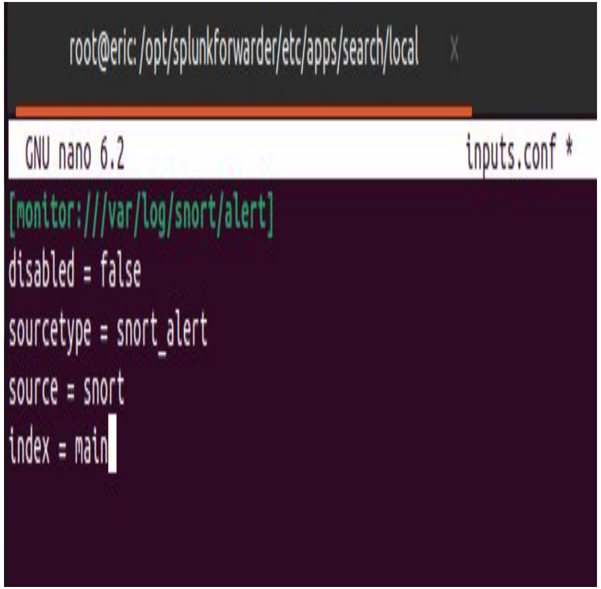
- Then run ***“sudo /opt/splunk/bin/splunk start -- accept-license”*** to accept license, set admin username and password, re-enter password to confirm

- Add the splunk server to the Universal Forwarder: ***“sudo /opt/splunkforwarder/bin/splunk add forward-server 192.168.15.11:9997”***, enter username and password to confirm

- Tell Universal Forwarder to monitor snort logs; snort logs are usually found at ***/var/log/snort***, “ ***“sudo /opt/splunkforwarder/bin/splunk add monitor /var/log/snort/alert***

- Next, configure “inputs.conf” @ ***“sudo nano /opt/splunkforwarder/etc/system/apps/search/local/inputs.conf”*** access the local directory as a **“root user”** input the script and save file

- Next, restart the uinversal forwarder “***sudo /opt/splunkforwarder/bin/splunk restart”***

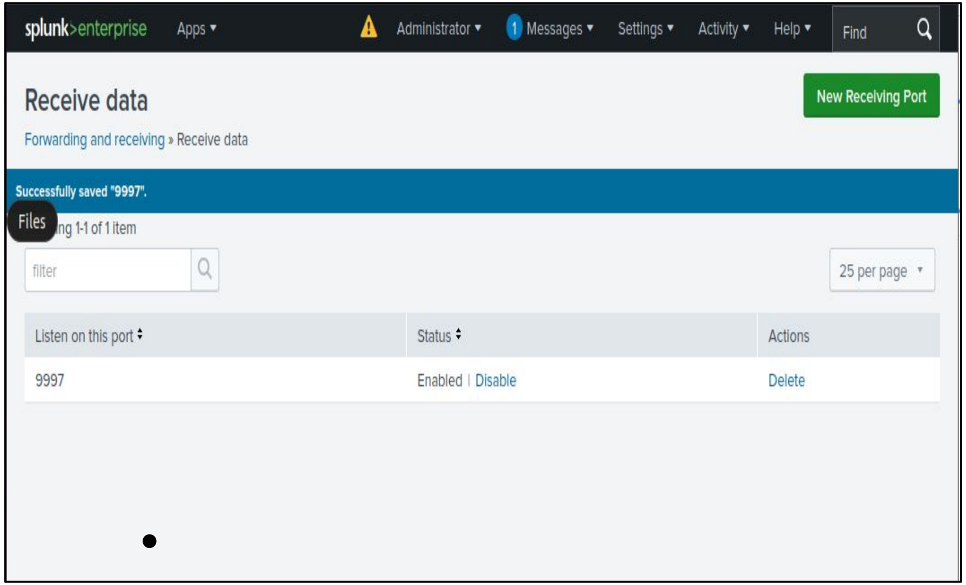


```
root@eric: /opt/splunkforwarder/etc/apps/search/local
GNU nano 6.2                                   inputs.conf *
[monitor:///var/log/snort/alert]
disabled = false
sourcetype = snort_alert
source = snort
index = main
```

Configure receiving port in splunk server

- In your browser sign into splunk server at http://192.168.15.11:8000

- In splunk user interface select **Settings→ forwarding and receiving→ configure receiving→ New Receiving Port** and enter the default receiving port number **“9997”** and hit save



Receive data

Forwarding and receiving » Receive data

Successfully saved "9997".

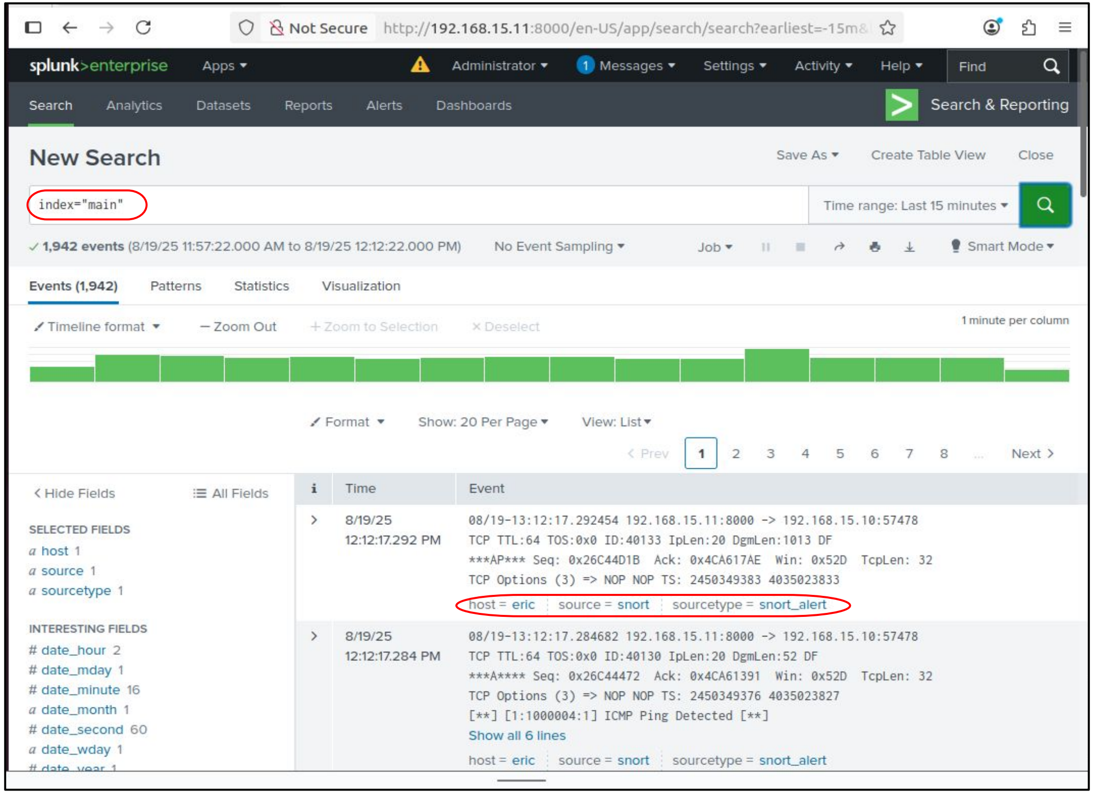
ng 1-1 of 1 item

Listen on this port ⇕	Status ⇕	Actions
9997	Enabled | Disable	Delete

Search for index

- Next, let’s navigate to search and reporting and search for snort log using the index we created “main

- **GREAT!!** The Universal forwarder is successfully ingesting logs into our splunk server.



```
index="main"
```

✓ 1,942 events (8/19/25 11:57:22.000 AM to 8/19/25 12:12:22.000 PM)

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
# date_hour 2
# date_mday 1
# date_minute 16
a date_month 1
# date_second 60
a date_wday 1
# date_year 1

i	Time	Event
>	8/19/25 12:12:17.292 PM	08/19-13:12:17.292454 192.168.15.11:8000 -> 192.168.15.10:57478 TCP TTL:64 TOS:0x0 ID:40133 IpLen:20 DgmLen:1013 DF ***AP*** Seq: 0x26C44D1B Ack: 0x4CA617AE Win: 0x52D TcpLen: 32 TCP Options (3) => NOP NOP TS: 2450349383 4035023833 host = eric source = snort sourcetype = snort_alert
>	8/19/25 12:12:17.284 PM	08/19-13:12:17.284682 192.168.15.11:8000 -> 192.168.15.10:57478 TCP TTL:64 TOS:0x0 ID:40130 IpLen:20 DgmLen:52 DF ***A**** Seq: 0x26C44472 Ack: 0x4CA61391 Win: 0x52D TcpLen: 32 TCP Options (3) => NOP NOP TS: 2450349376 4035023827 [**] [1:1000004:1] ICMP Ping Detected [**] Show all 6 lines host = eric source = snort sourcetype = snort_alert

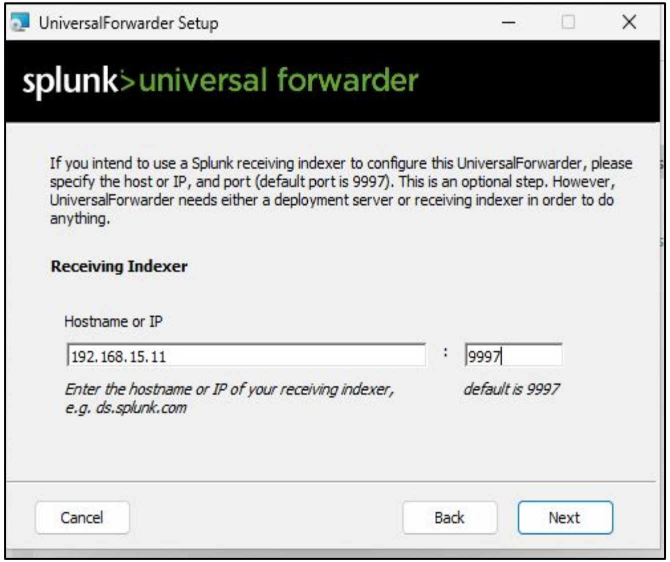
Configure windows(Domain accounts)to forward log to splunk

- In the window machine**(Target-PC)** open browser,go to splunk.com and download splunk universal forwarder for windows

- Open file explorer and install splunk forwarder in the download folder

- Click the check box to accept the license, then enter username select "generate random password" continue to hit next until you get to "receiving indexer prompt".

- Enter the splunk server IP and the default receiving port and select next, then wait for the full installation and click finish



UniversalForwarder Setup

splunk>universal forwarder

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.

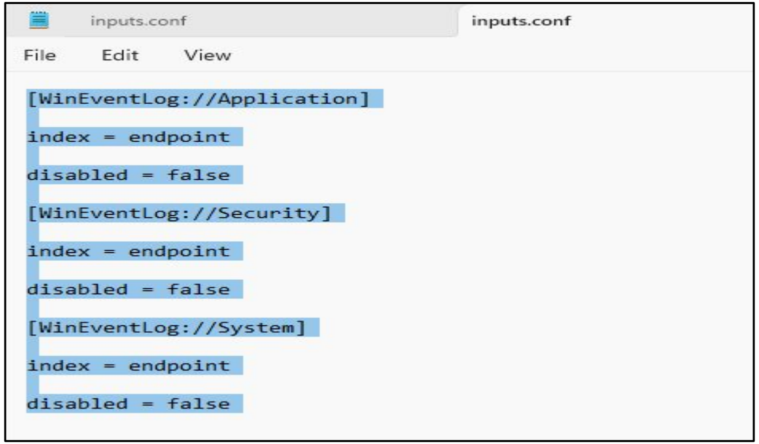
Receiving Indexer

Hostname or IP: 192.168.15.11 : 9997

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

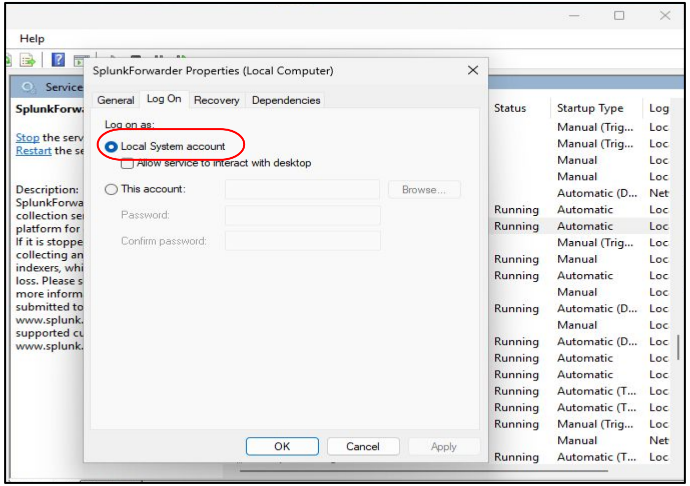
default is 9997

Configure input.conf and save in the “local folder”



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

- Locate Notepad in the window vm**(Target-PC)** run as administrator and input the following script and save as “input.conf” under **“C:Program Files\SplunkUniversalForwarder\etc\system\local*/”*** folder, ensure to save file type as “All file”



SplunkForwarder Properties (Local Computer)

Log on as:

● Local System account

□ Allow service to interact with desktop

○ This account:

Password:

Confirm password:

SplunkForw

Stop the serv
Restart the se

Description:
SplunkForwa
collection se
platform for
If it is stoppe
collecting an
indexers, whi
loss. Please s
more inform
submitted to
www.splunk.
supported cu
www.splunk.

Status	Startup Type	Log
	Manual (Trig...	Loc
	Manual (Trig...	Loc
	Manual	Loc
	Manual	Loc
	Automatic (D...	Net
Running	Automatic	Loc
Running	Automatic	Loc
	Manual (Trig...	Loc
Running	Manual	Loc
Running	Automatic	Loc
	Manual	Loc
Running	Automatic (D...	Loc
	Manual	Loc
Running	Automatic (D...	Loc
Running	Automatic	Loc
Running	Automatic	Loc
Running	Automatic (T...	Loc
Running	Automatic (T...	Loc
Running	Manual (Trig...	Loc
	Manual	Net
Running	Automatic (T...	Loc

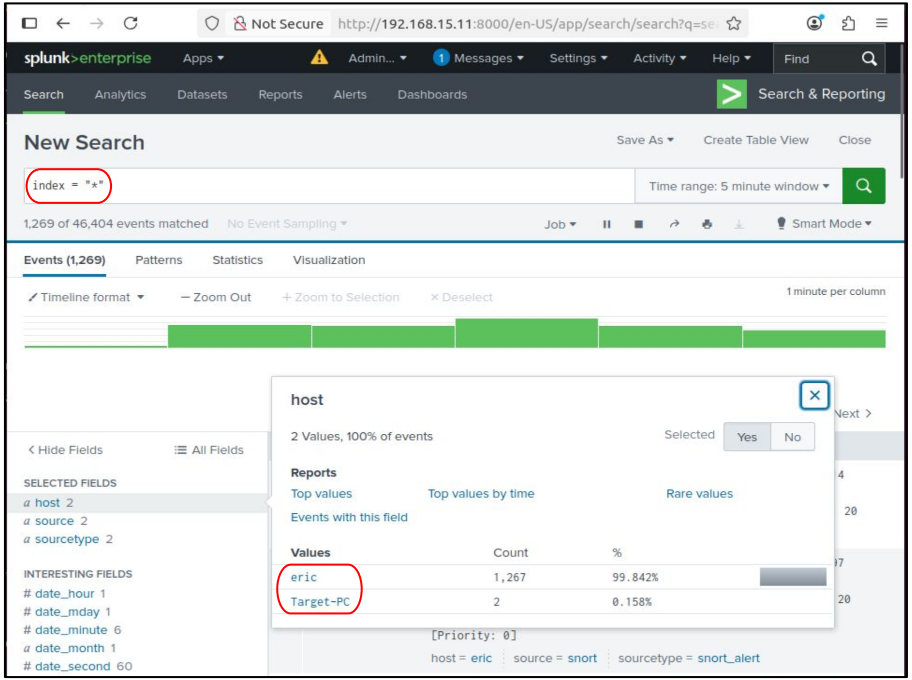
- Next, search “Services” in the window search bar run as administrator, navigate to SplunkForwarder make sure its Log On as “Local System account” and restart the service

Splunk Investigation

- Navigate to splunk user interface, create a new index call “endpoint” and save

- Go to search and reporting in the search bar set the index to wild card for general search [index = “*”] set time to 5mins and hit search and wait parse and return search results

- Under field select “host” to view result and you should see all the vm’s that are forwarding logs to the splunk server



New Search

```
index = "*"
```

Time range: 5 minute window

1,269 of 46,404 events matched   No Event Sampling

SELECTED FIELDS
- a host 2
- a source 2
- a sourcetype 2

INTERESTING FIELDS
- # date_hour 1
- # date_mday 1
- # date_minute 6
- a date_month 1
- # date_second 60

host

2 Values, 100% of events

Selected: Yes No

Values	Count	%
eric	1,267	99.842%
Target-PC	2	0.158%

```
[Priority: 0]
```

host = eric   source = snort   sourcetype = snort_alert

Attack simulations

In the next slides, we will conduct

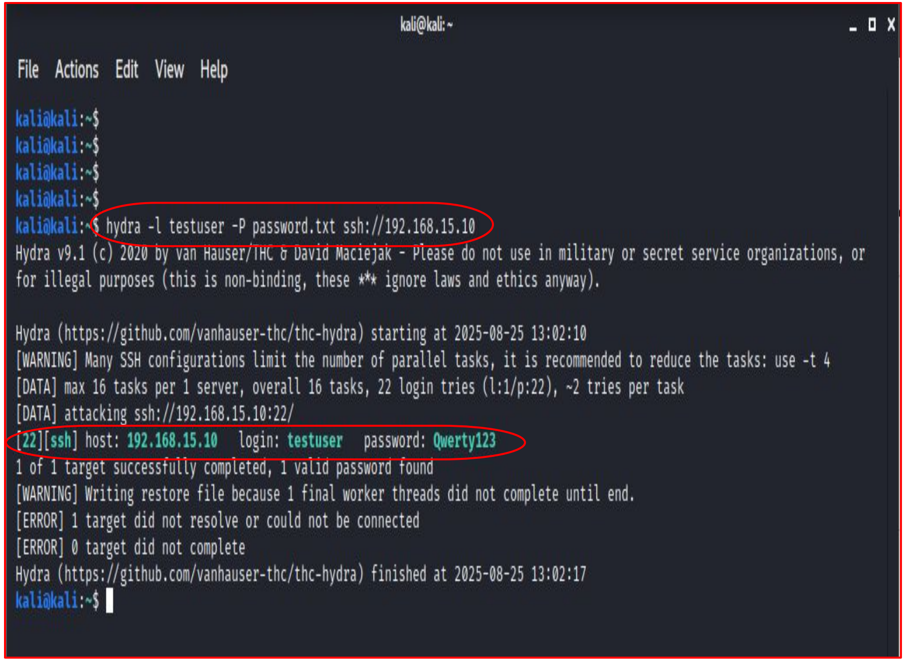
- **SSH Brute-Force Attack** on Ubuntu machine
- **RDP Brute-Force Attack** on Windows (Target-PC) joined to *eric.local* domain
- Attacks executed using **Hydra** from Kali Linux
- **Visualize logs results** in Splunk User Interface
- **Firstly,** we are going to switch our network to host only adapter, to enable us have a more control traffic

SSH Brute-force Attack

- In the ubuntu vm, install ssh server **“sudo apt install openssh-server -y”** and create a weak test user **“sudo adduser [testuser]”** and set password**[Qwerty123]**

- From the kali Linux vm run hydra **“hydra -l testuser -P password.txt ssh://192.168.15.10”**.

- This will simulate a repeated logins attempts against the testuser and return the correct password if attack is successful



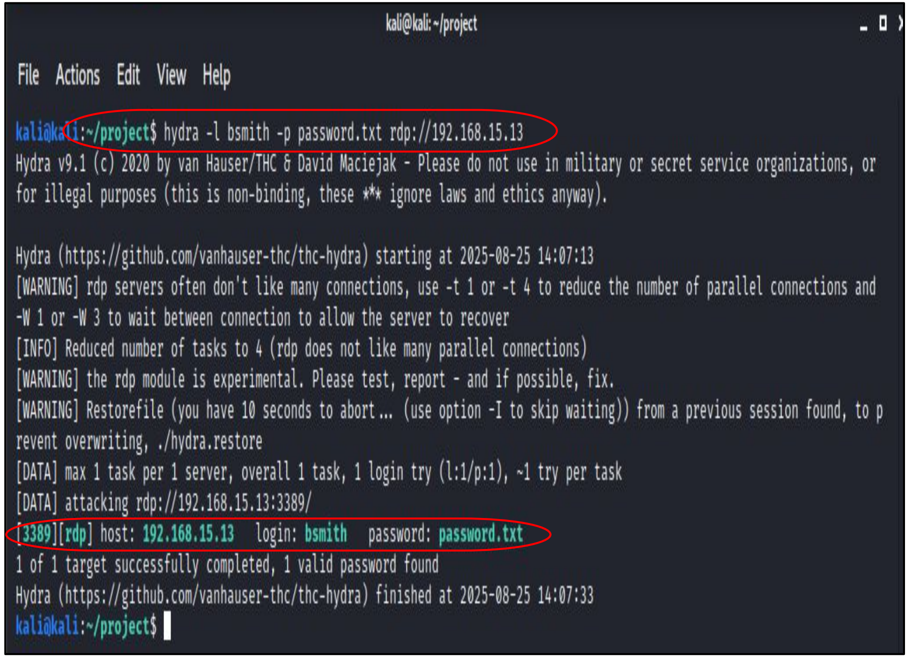
```
kali@kali:~$
kali@kali:~$
kali@kali:~$
kali@kali:~$
kali@kali:~$ hydra -l testuser -P password.txt ssh://192.168.15.10
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or
for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-08-25 13:02:10
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 22 login tries (l:1/p:22), ~2 tries per task
[DATA] attacking ssh://192.168.15.10:22/
[22][ssh] host: 192.168.15.10   login: testuser   password: Qwerty123
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-08-25 13:02:17
kali@kali:~$
```

RDP Brute-Force Attack

- **On the Windows (Target-PC) VM:**
  In the search bar, type **"Rename PC"** and press **Enter**, select **Advanced system settings**, go to the **Remote** tab,the check the box to **Enable Remote Desktop** (allow remote connections), click **Apply** and then **OK**

- From the kali Linux vm run hydra **"hydra -l bsmith -P password.txt rdp://192.168.15.13"**.

- This will simulate a repeated logins attempts against the user "bsmith" and return the correct password if attack is successful

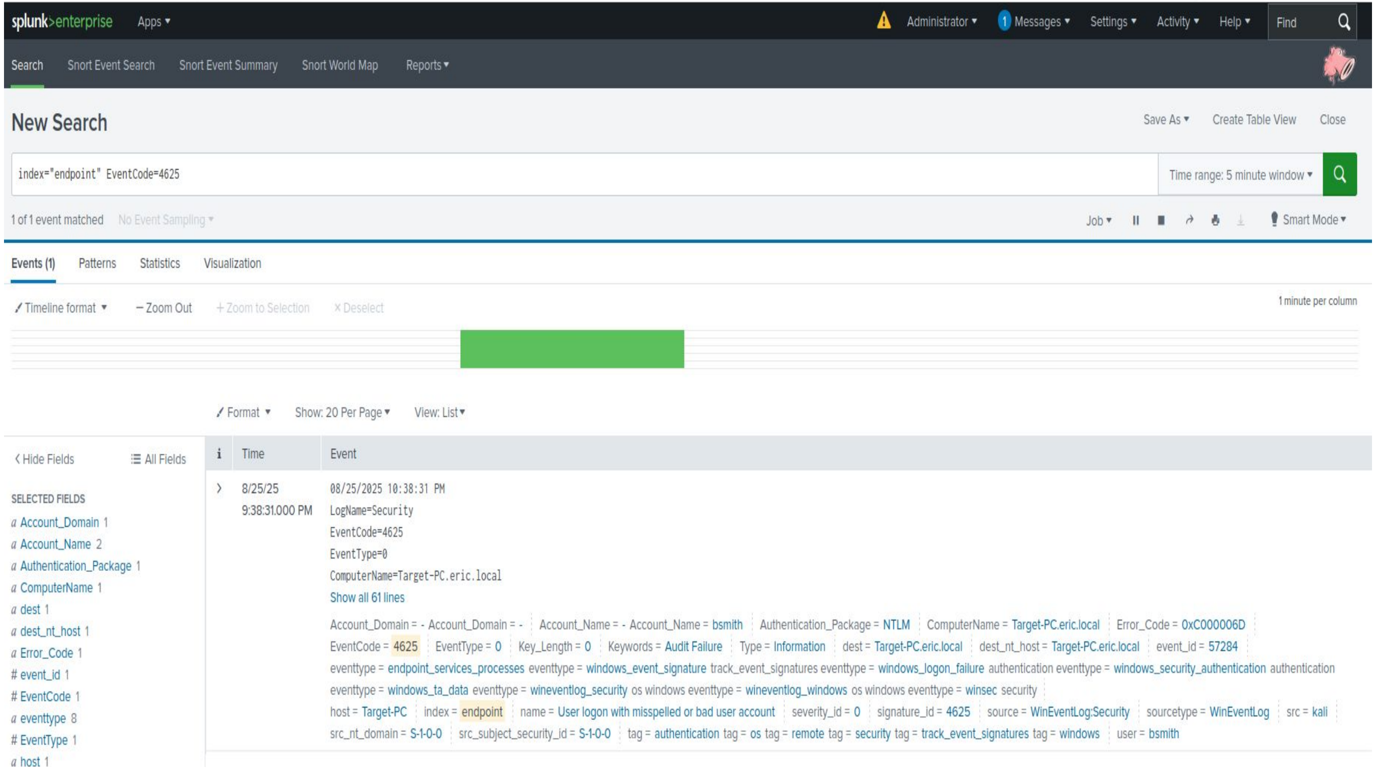


```
kali@kali:~/project$ hydra -l bsmith -p password.txt rdp://192.168.15.13
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or
for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-08-25 14:07:13
[WARNING] rdp servers often don't like many connections, use -t 1 or -t 4 to reduce the number of parallel connections and
-W 1 or -W 3 to wait between connection to allow the server to recover
[INFO] Reduced number of tasks to 4 (rdp does not like many parallel connections)
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to p
revent overwriting, ./hydra.restore
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking rdp://192.168.15.13:3389/
[3389][rdp] host: 192.168.15.13   login: bsmith   password: password.txt
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-08-25 14:07:33
kali@kali:~/project$
```

Brute-force analysis

- In our splunk search **index="endpoint"** to search for the endpoint logs.

- Then search for **EventCode=4625** to filters for failed Windows logon attempts.



New Search

```
index="endpoint" EventCode=4625
```

Time range: 5 minute window ▾

1 of 1 event matched No Event Sampling ▾

Show: 20 Per Page ▾ View: List ▾

SELECTED FIELDS
- a Account_Domain 1
- a Account_Name 2
- a Authentication_Package 1
- a ComputerName 1
- a dest 1
- a dest_nt_host 1
- a Error_Code 1
- # event_id 1
- # EventCode 1
- a eventtype 8
- # EventType 1
- a host 1

i	Time	Event

›	8/25/25
	9:38:31.000 PM
		08/25/2025 10:38:31 PM
		LogName=Security
		EventCode=4625
		EventType=0
		ComputerName=Target-PC.eric.local
		Show all 61 lines

Account_Domain = - Account_Domain = - | Account_Name = - Account_Name = bsmith | Authentication_Package = NTLM | ComputerName = Target-PC.eric.local | Error_Code = 0xC000006D
EventCode = 4625 | EventType = 0 | Key_Length = 0 | Keywords = Audit Failure | Type = Information | dest = Target-PC.eric.local | dest_nt_host = Target-PC.eric.local | event_id = 57284
eventtype = endpoint_services_processes eventtype = windows_event_signature track_event_signatures eventtype = windows_logon_failure authentication eventtype = windows_security_authentication authentication
eventtype = windows_ta_data eventtype = wineventlog_security os windows eventtype = wineventlog_windows os windows eventtype = winsec security
host = Target-PC | index = endpoint | name = User logon with misspelled or bad user account | severity_id = 0 | signature_id = 4625 | source = WinEventLog:Security | sourcetype = WinEventLog | src = kali
src_nt_domain = S-1-0-0 | src_subject_security_id = S-1-0-0 | tag = authentication tag = os tag = remote tag = security tag = track_event_signatures tag = windows | user = bsmith

Conclusion

Conclusion

This project simulate a SOC environment to practice Tier 1 analyst workflows. By integrating Splunk, Snort, Kali, and Windows systems in a virtual network, it demonstrated log ingestion, threat detection, and incident response, showcasing how centralized SIEM visibility enhances security operations