

SPLUNK

Splunk is a strong tool used for analyzing data, especially in cybersecurity. It helps organizations gather, organize, and analyze log data from different sources. With its powerful features, it lets users quickly solve problems by providing complete insights and analytics.

/opt/splunk/bin/splunk start

```
root@Ubuntu:/home/vboxuser# /opt/splunk/bin/splunk start
The splunk daemon (splunkd) is already running.

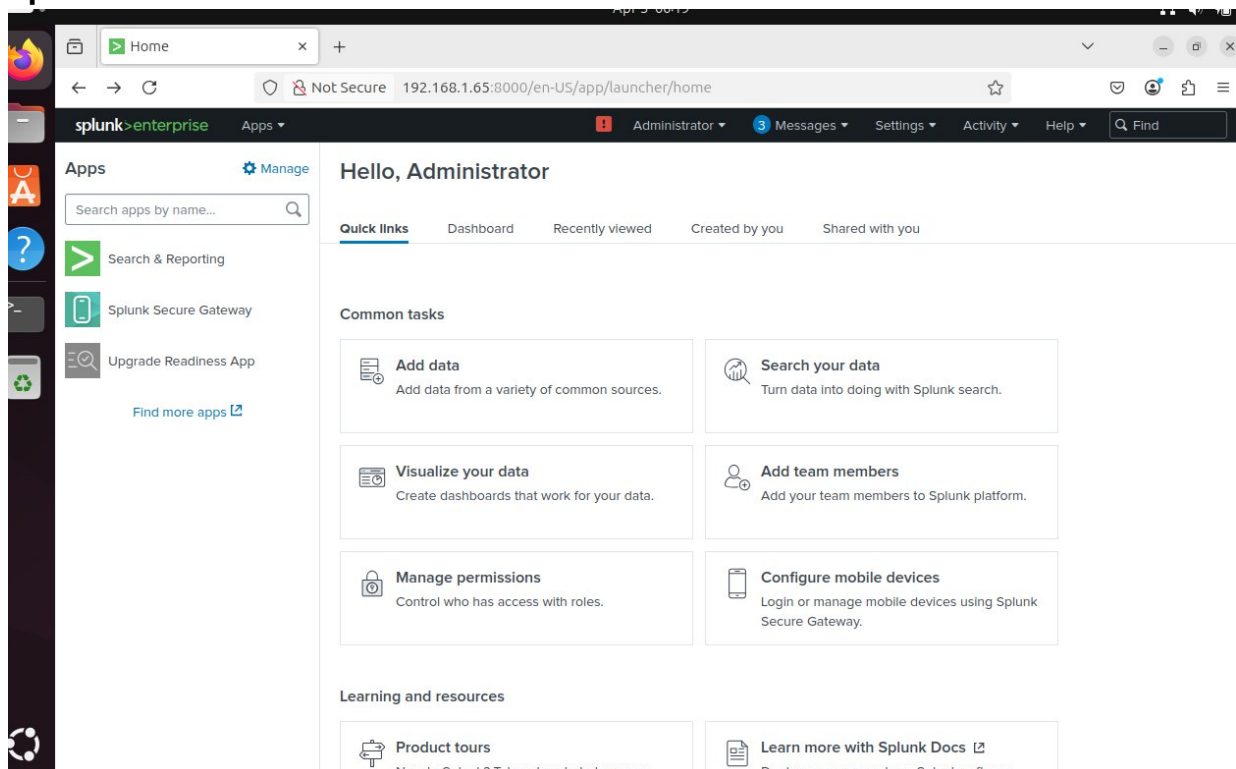
Waiting for web server at http://127.0.0.1:8000 to be available..... Done

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

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

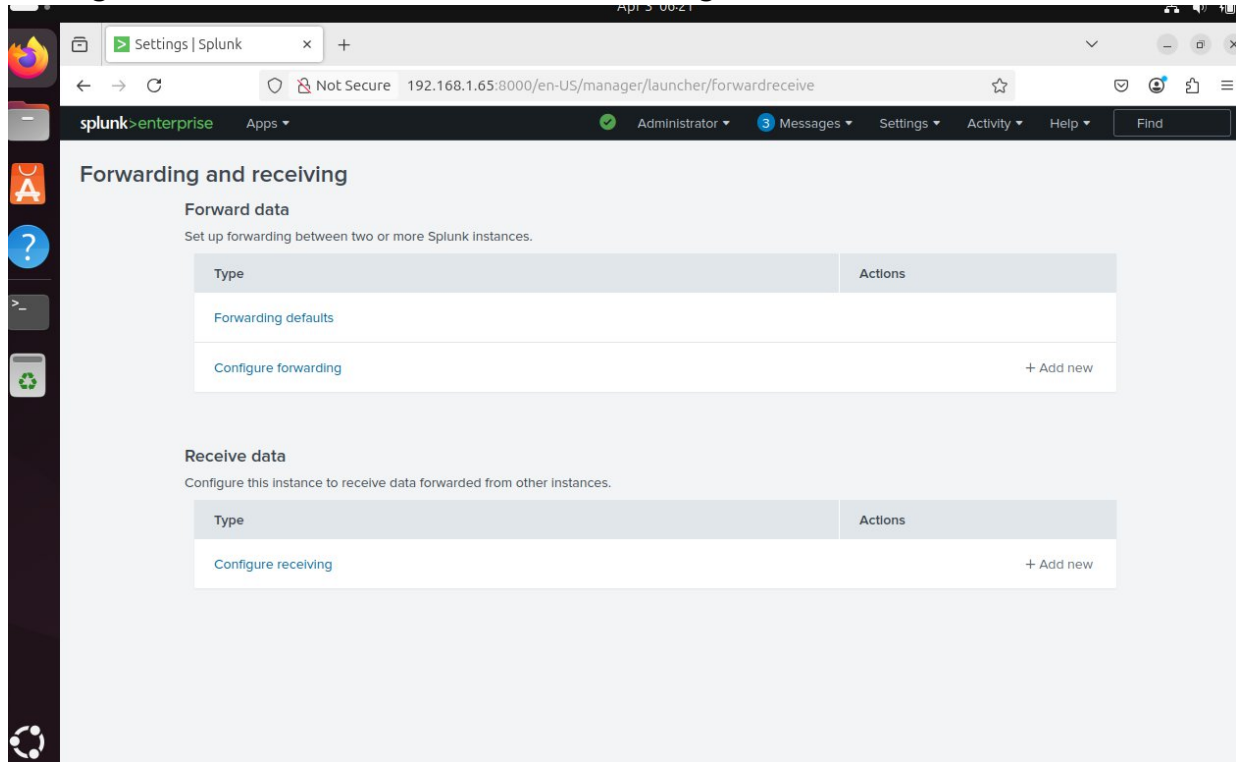
root@Ubuntu:/home/vboxuser#
```

Splunk overview and dashboard



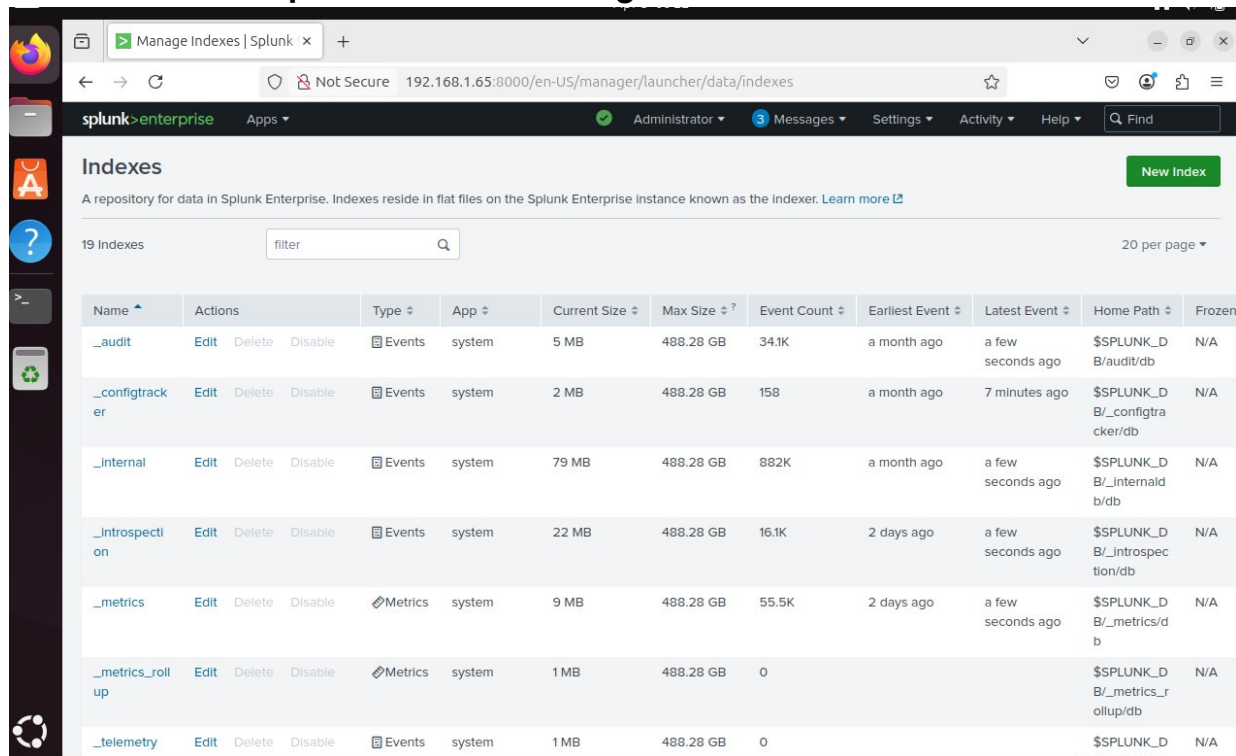
Splunk offers a robust platform for data visualization and monitoring through its dashboard features. Users can create and customize dashboards to display real-time metrics, visualizations, and alerts, enabling quick insights into system performance and security events.

Configure forwarder and receiver from settings



Configuring a Splunk Forwarder and Receiver involves setting up a Splunk Universal Forwarder (for data collection) and a Splunk instance (for data receiving and indexing). Below are the steps to configure both components.

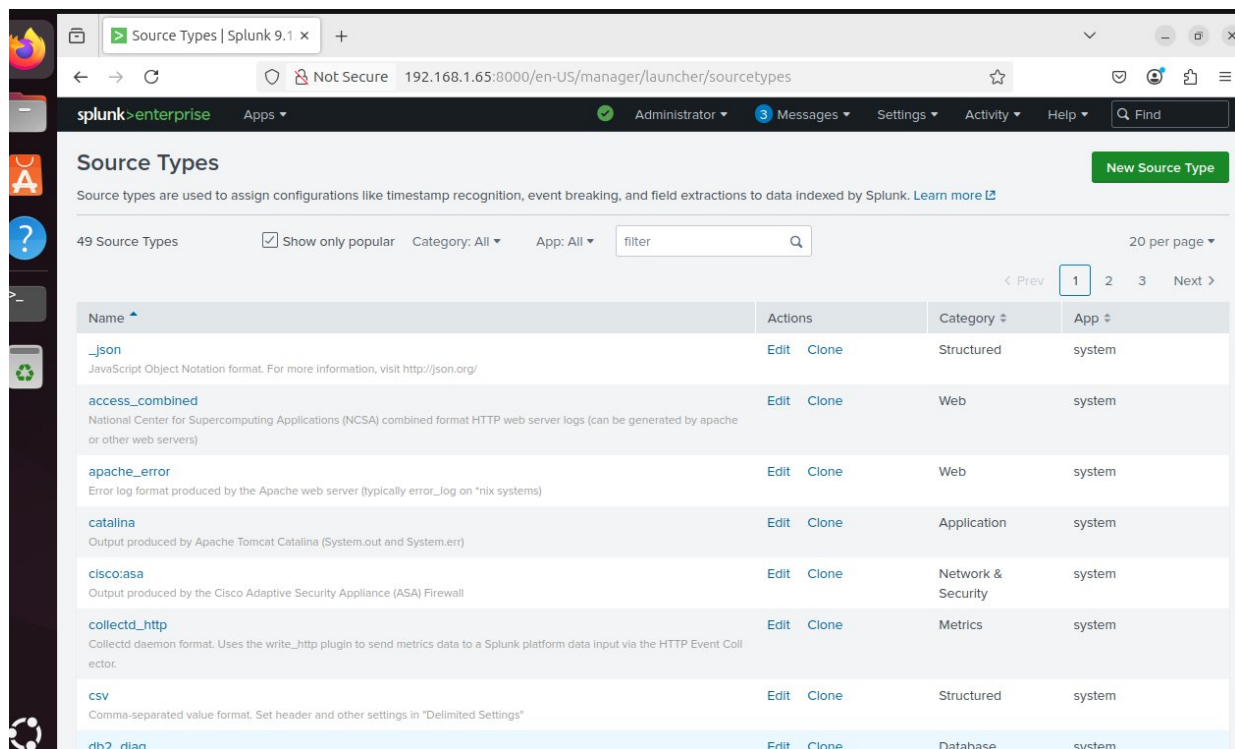
Create Indexes as per choice from setting > indexes > new index



Creating a new index in Splunk is essential for organizing and managing your data effectively. Whether you choose to use the Splunk Web interface or edit configuration files directly, both methods are valid and will allow you to set up a new index for your data.

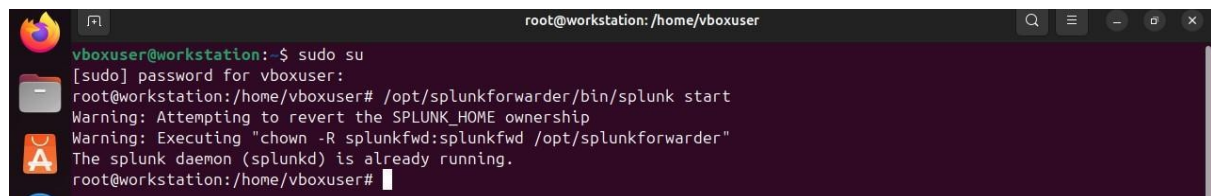
Create source type as per choice from setting > source types > new source type

Creating a new sourcetype in Splunk is essential for ensuring that your data is indexed and interpreted correctly. Whether you choose to use the Splunk Web interface or edit configuration files directly, both methods are valid and will allow you to set up a new sourcetype for your data.



Open Workstation

`/opt/splunkforwarder/bin/splunk start`



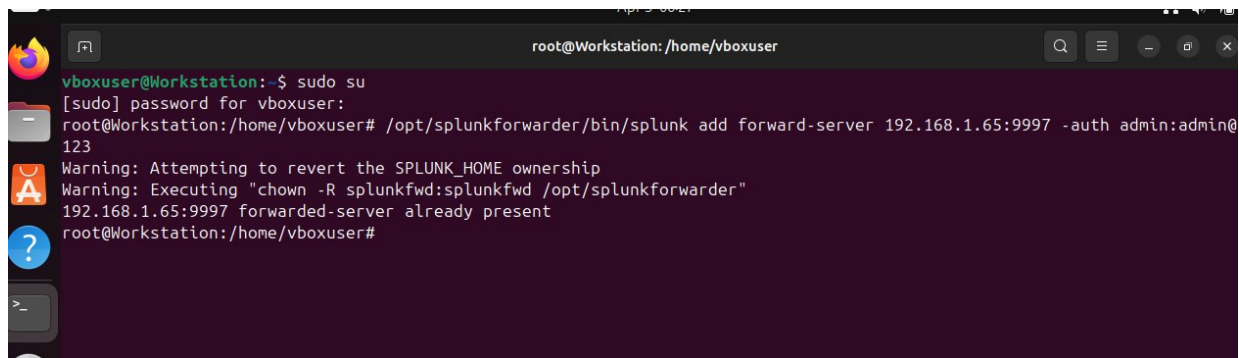
`nano /opt/splunkforwarder/etc/system/local/inputs.conf`



This configuration is likely used in a Linux environment where Splunk is collecting logs for monitoring and analysis.

The specified logs are crucial for system administration and security, providing insights into both general system events (syslog) and security-related events (auth.log).

/opt/splunkforwarder/bin/splunk add forwarder-server 192.168.1.65:9997 -auth admin:admin@123



```
root@Workstation: /home/vboxuser
vboxuser@Workstation:~$ sudo su
[sudo] password for vboxuser:
root@Workstation:/home/vboxuser# /opt/splunkforwarder/bin/splunk add forwarder-server 192.168.1.65:9997 -auth admin:admin@123
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
192.168.1.65:9997 forwarded-server already present
root@Workstation:/home/vboxuser#
```

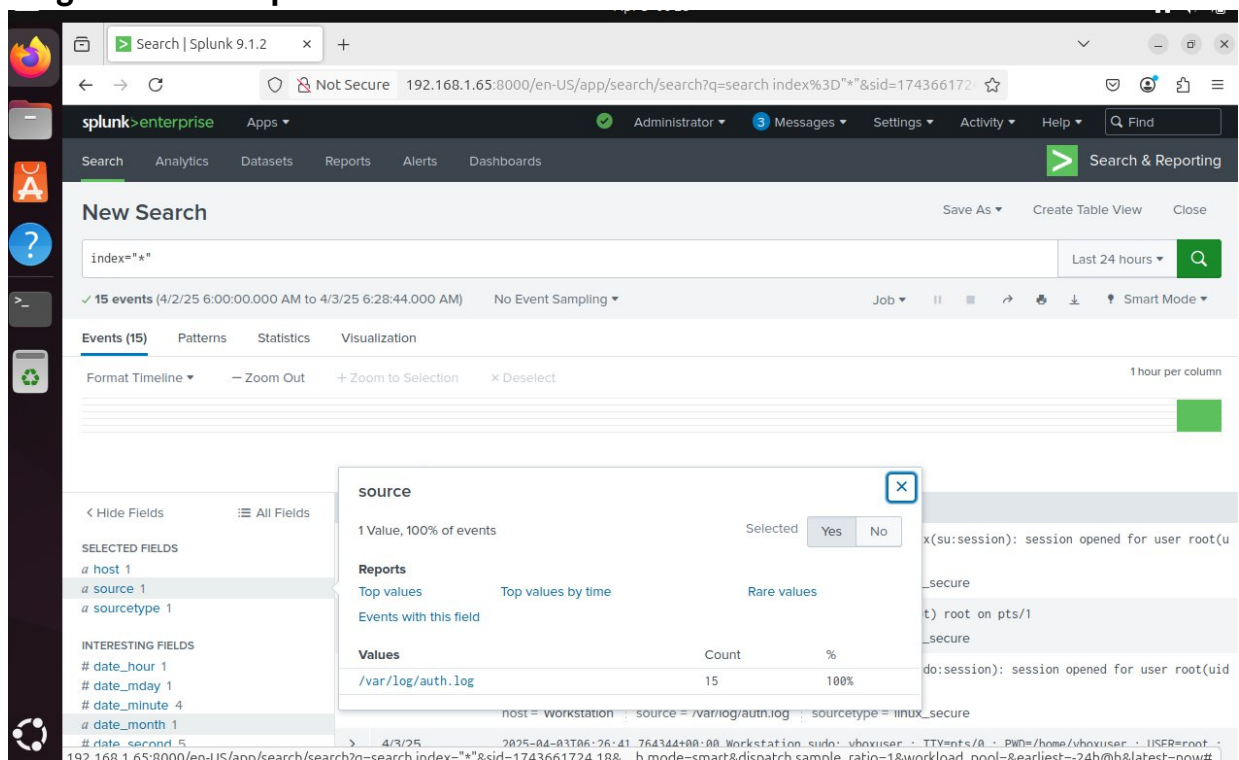
In short, this command is meant to set up the Splunk Universal Forwarder to monitor a specific data source, but the address format looks like it might be wrong for a file or folder. The command also includes login details to connect to the Splunk system. If you want to monitor a specific file or folder, you should replace 192.168.1.65:9997 with the actual file or folder path you want to track.

/opt/splunkforwarder/bin/splunk add monitor /var/log/auth.log

/opt/splunkforwarder/bin/splunk add monitor /var/log/syslog

These commands configure Splunk to actively monitor two critical log files (auth.log for authentication events and syslog for system events), ensuring that important security and operational data is collected for analysis.

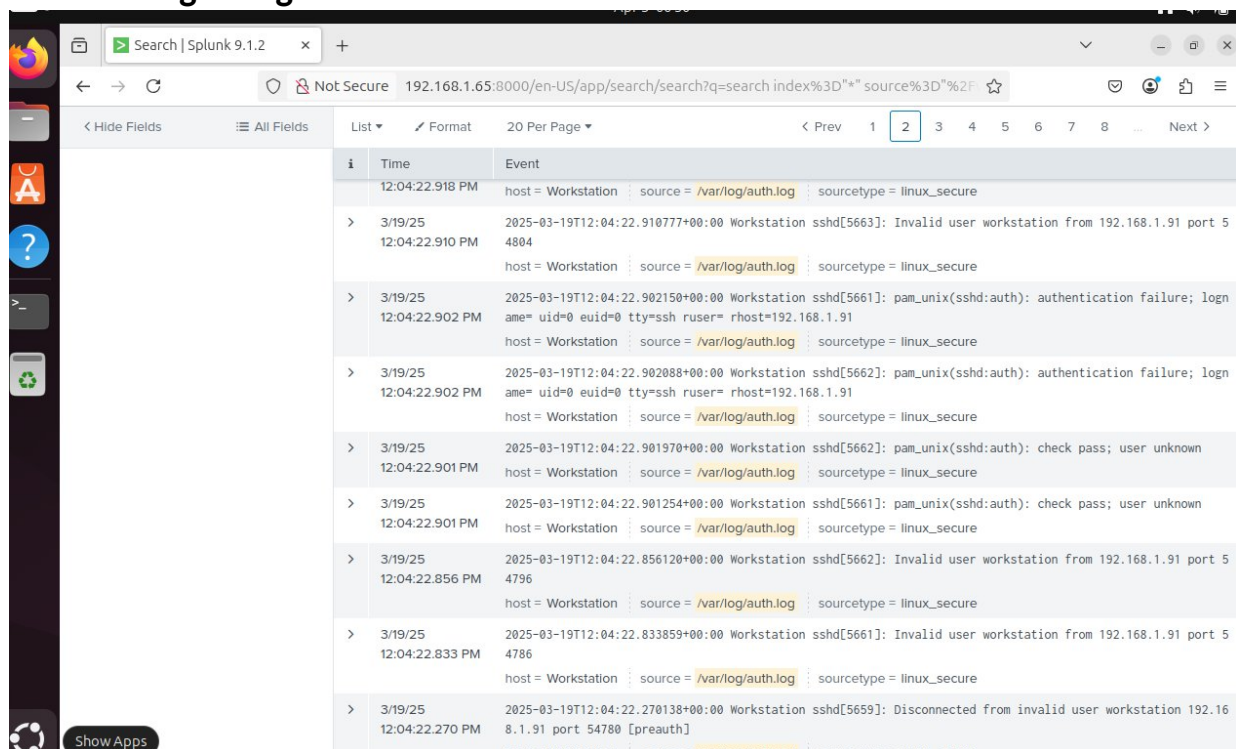
Logs shown on splunk server



The screenshot shows the Splunk web interface with a search for 'index=*'. The search results show 15 events. A modal window is open showing the 'source' field with 1 value, 100% of events. The modal also shows a table of values for the 'source' field.

| Values | Count | % |
|-------------------|-------|------|
| /var/log/auth.log | 15 | 100% |

Attacker logs are generated



The screenshot shows a Splunk search interface with the following details:

- Search bar: Search | Splunk 9.1.2
- URL: 192.168.1.65:8000/en-US/app/search/search?q=search index%3D"*" source%3D"/var/log/auth.log"
- Results table with columns: i, Time, Event
- Page 2 of 2, 20 Per Page

| i | Time | Event |
|---|-------------------------|---|
| | 12:04:22.918 PM | host = Workstation source = /var/log/auth.log sourcetype = linux_secure |
| > | 3/19/25 12:04:22.910 PM | 2025-03-19T12:04:22.910777+00:00 Workstation sshd[5663]: Invalid user workstation from 192.168.1.91 port 54804 host = Workstation source = /var/log/auth.log sourcetype = linux_secure |
| > | 3/19/25 12:04:22.902 PM | 2025-03-19T12:04:22.902150+00:00 Workstation sshd[5661]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.91 host = Workstation source = /var/log/auth.log sourcetype = linux_secure |
| > | 3/19/25 12:04:22.902 PM | 2025-03-19T12:04:22.902088+00:00 Workstation sshd[5662]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.91 host = Workstation source = /var/log/auth.log sourcetype = linux_secure |
| > | 3/19/25 12:04:22.901 PM | 2025-03-19T12:04:22.901970+00:00 Workstation sshd[5662]: pam_unix(sshd:auth): check pass; user unknown host = Workstation source = /var/log/auth.log sourcetype = linux_secure |
| > | 3/19/25 12:04:22.901 PM | 2025-03-19T12:04:22.901254+00:00 Workstation sshd[5661]: pam_unix(sshd:auth): check pass; user unknown host = Workstation source = /var/log/auth.log sourcetype = linux_secure |
| > | 3/19/25 12:04:22.856 PM | 2025-03-19T12:04:22.856120+00:00 Workstation sshd[5662]: Invalid user workstation from 192.168.1.91 port 54796 host = Workstation source = /var/log/auth.log sourcetype = linux_secure |
| > | 3/19/25 12:04:22.833 PM | 2025-03-19T12:04:22.833859+00:00 Workstation sshd[5661]: Invalid user workstation from 192.168.1.91 port 54786 host = Workstation source = /var/log/auth.log sourcetype = linux_secure |
| > | 3/19/25 12:04:22.270 PM | 2025-03-19T12:04:22.270138+00:00 Workstation sshd[5659]: Disconnected from invalid user workstation 192.168.1.91 port 54780 [preauth] host = Workstation source = /var/log/auth.log sourcetype = linux_secure |

Nmap -sV 192.168.1.65

```
(root@kali)~# nmap -sV 192.168.1.65
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-03 12:17 IST
Nmap scan report for 192.168.1.65
Host is up (0.0044s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
25/tcp    open  smtp    Postfix smtpd
8000/tcp  open  http    Splunkd httpd
8089/tcp  open  ssl/http Splunkd httpd
MAC Address: DC:97:BA:5E:02:59 (Intel Corporate)
Service Info: Host: UBuntu

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 36.31 seconds
```

This command helps you learn more about what software is running on a specific device in your local network.

Hydra -L user.txt -P user.txt ssh://192.168.1.65

```
(root@kali)-[~]
└─# hydra -L user.txt -P user.txt ssh://192.168.1.65
Hydra v9.5 (c) 2023 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 2025-04-03 12:22:16
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 9 tasks per 1 server, overall 9 tasks, 9 login tries (1:3/p:3), -1 try per task
[DATA] attacking ssh://192.168.1.65:22/
[ERROR] could not connect to ssh://192.168.1.65:22 - Connection refused
```

This command is trying to log into the SSH service on the specified device by testing all combinations of usernames and passwords from the provided files