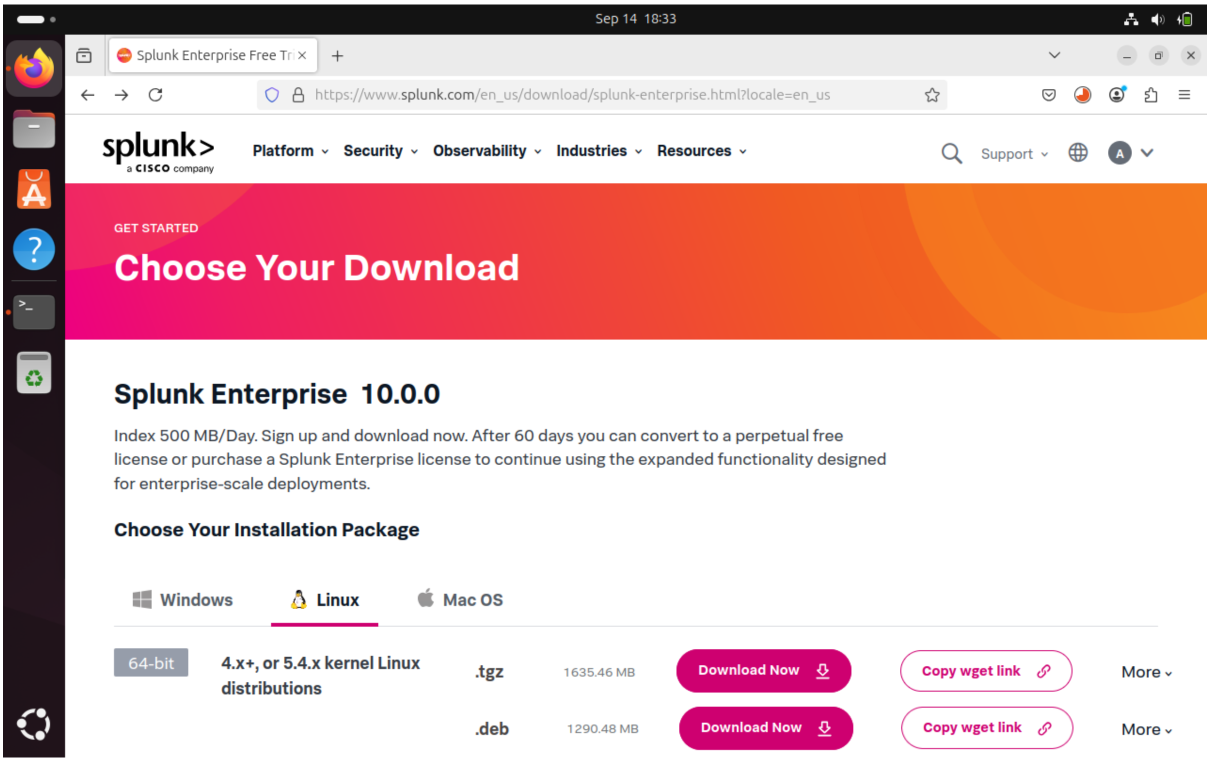
Network security monitoring using snort and splunk

1. Lab Environment & Topology

- Host platform: VMware Workstation / VMware Player.
- Attacker VM: Linux (Kali/Other) — tools: nmap, nping, curl, hping3, gobuster.
- Victim VM: Ubuntu (server/desktop) — tools installed: Snort IDS, Splunk (Enterprise or indexer) and Splunk Universal Forwarder (UF).
- Networking: Host-only / NAT internal network inside VMware NAT network 1. Example IPs used in lab:
  - Victim IP: 10.0.2.15
  - Attacker IP: 10.0.2.4
  - Splunk Indexer: 127.0.0.1:8000

2. Open ubuntu virtual machine

- Go to firefox and download splunk from splunk enterprise.
- Go to linux and download .deb file.



Choose Your Download

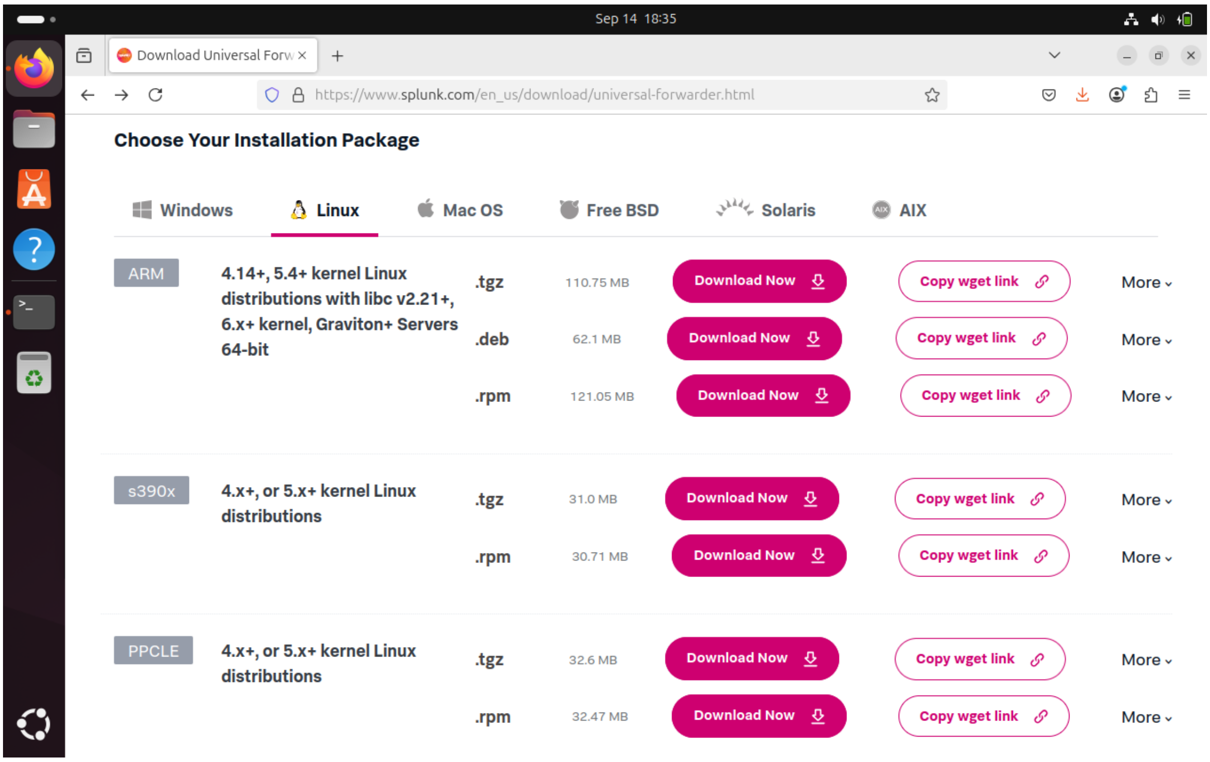
Splunk Enterprise 10.0.0

Index 500 MB/Day. Sign up and download now. After 60 days you can convert to a perpetual free license or purchase a Splunk Enterprise license to continue using the expanded functionality designed for enterprise-scale deployments.

Choose Your Installation Package

64-bit	4.x+, or 5.4.x kernel Linux distributions	.tgz	1635.46 MB	Download Now	Copy wget link	More
		.deb	1290.48 MB	Download Now	Copy wget link	More

- Download Universal Forwarder from Linux PPCLE .tgz file.

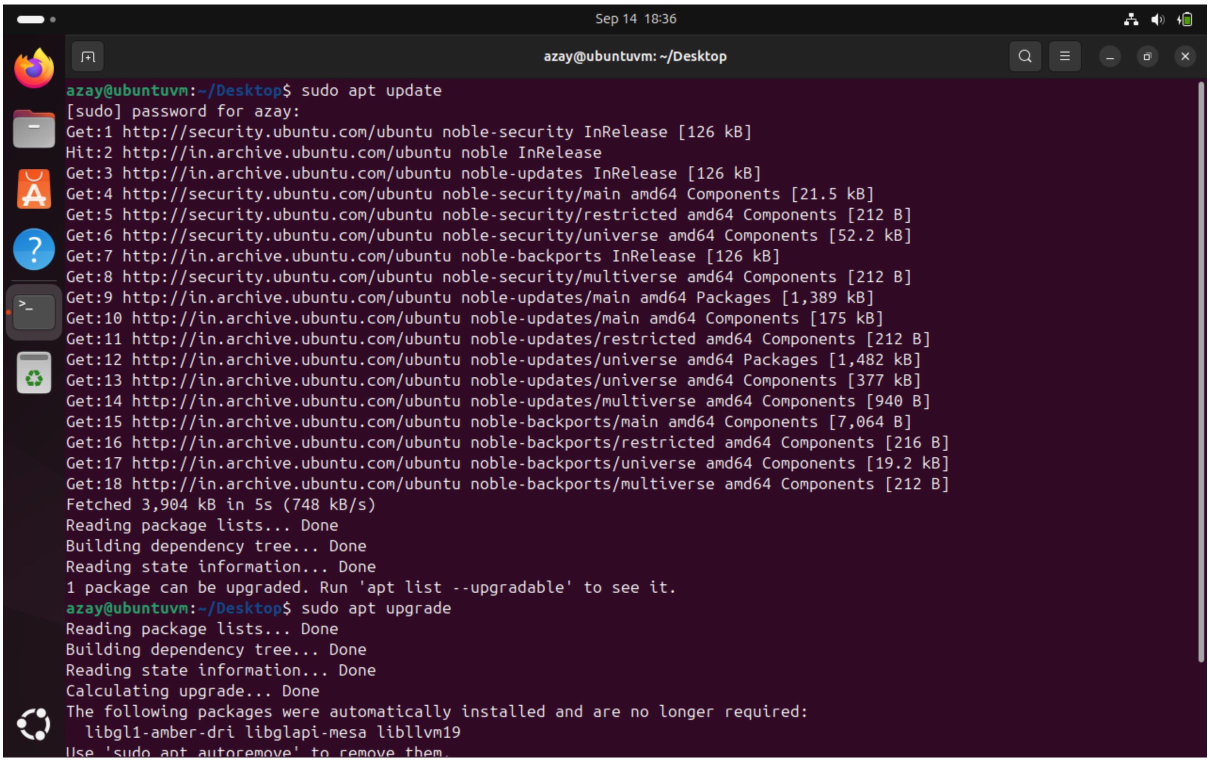

Sep 14 18:35
Download Universal Forw ×
https://www.splunk.com/en_us/download/universal-forwarder.html

Choose Your Installation Package

Windows
Linux
Mac OS
Free BSD
Solaris
AIX

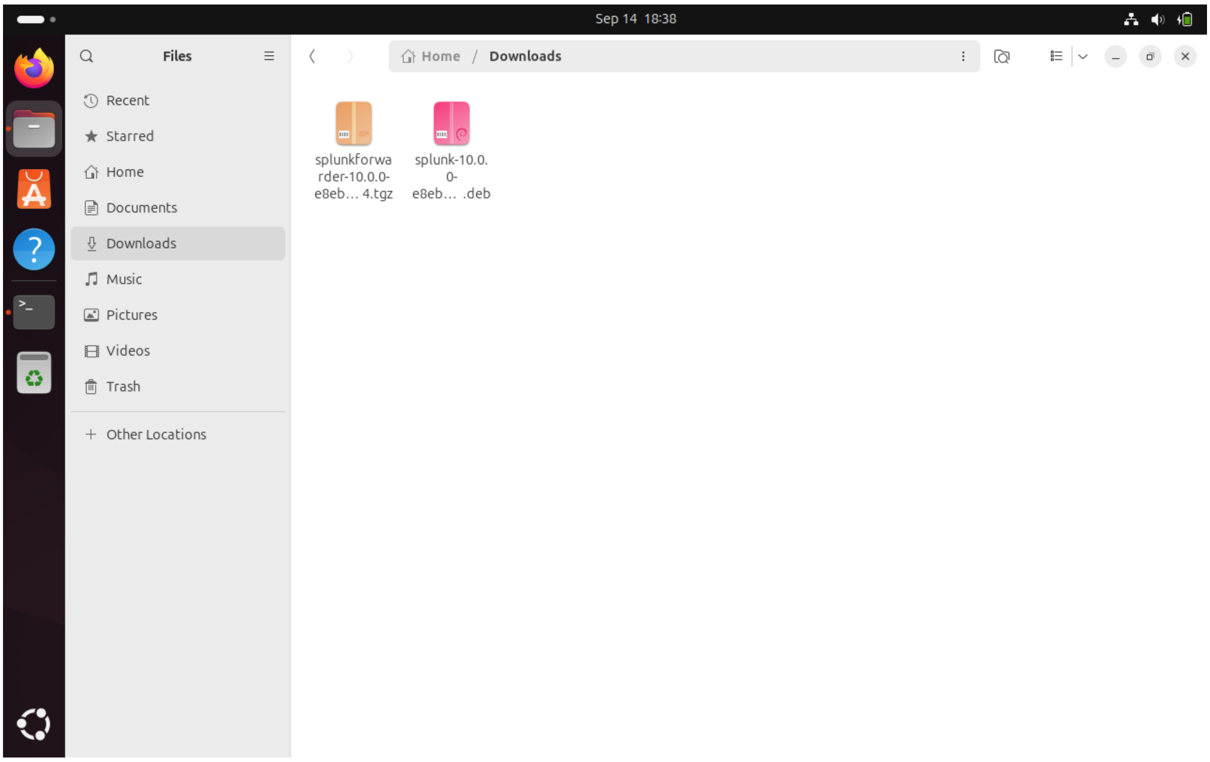
ARM	4.14+, 5.4+ kernel Linux distributions with libc v2.21+, 6.x+ kernel, Graviton+ Servers 64-bit	.tgz	110.75 MB	Download Now	Copy wget link	More
		.deb	62.1 MB	Download Now	Copy wget link	More
		.rpm	121.05 MB	Download Now	Copy wget link	More
s390x	4.x+, or 5.x+ kernel Linux distributions	.tgz	31.0 MB	Download Now	Copy wget link	More
		.rpm	30.71 MB	Download Now	Copy wget link	More
PPCLE	4.x+, or 5.x+ kernel Linux distributions	.tgz	32.6 MB	Download Now	Copy wget link	More
		.rpm	32.47 MB	Download Now	Copy wget link	More

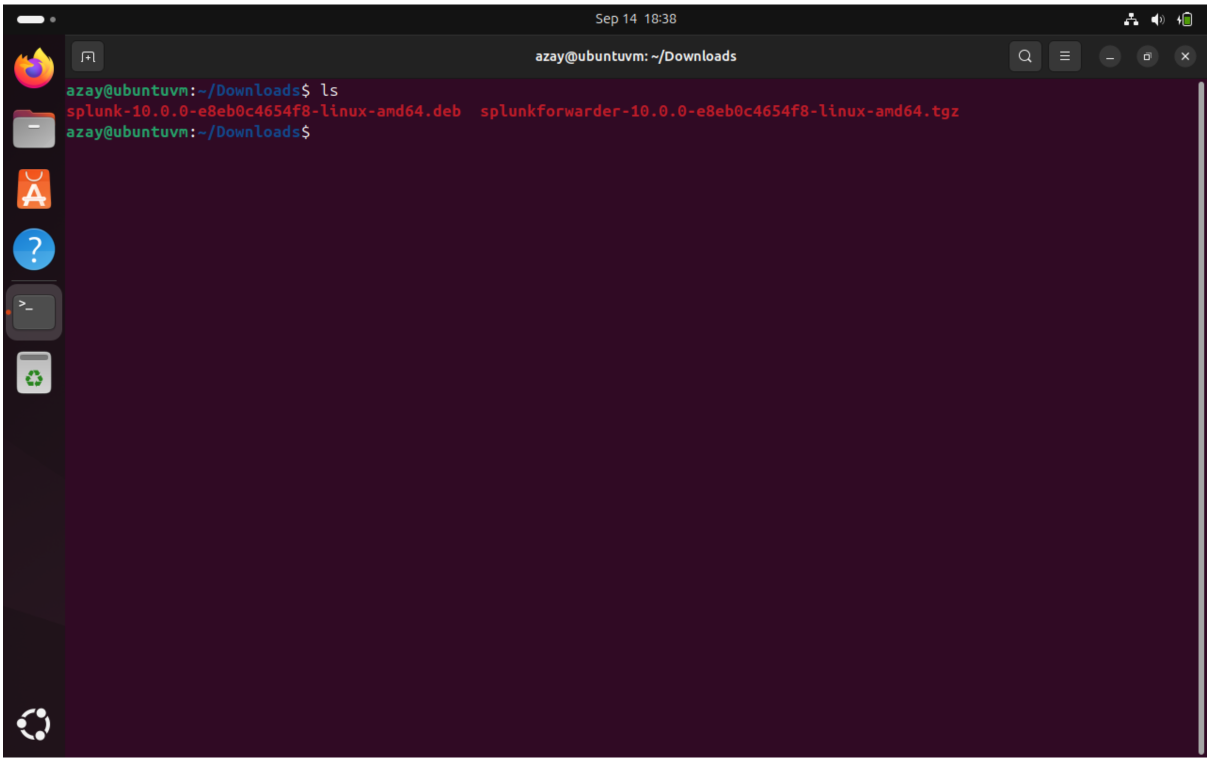
- Open terminal and make update and upgrade system



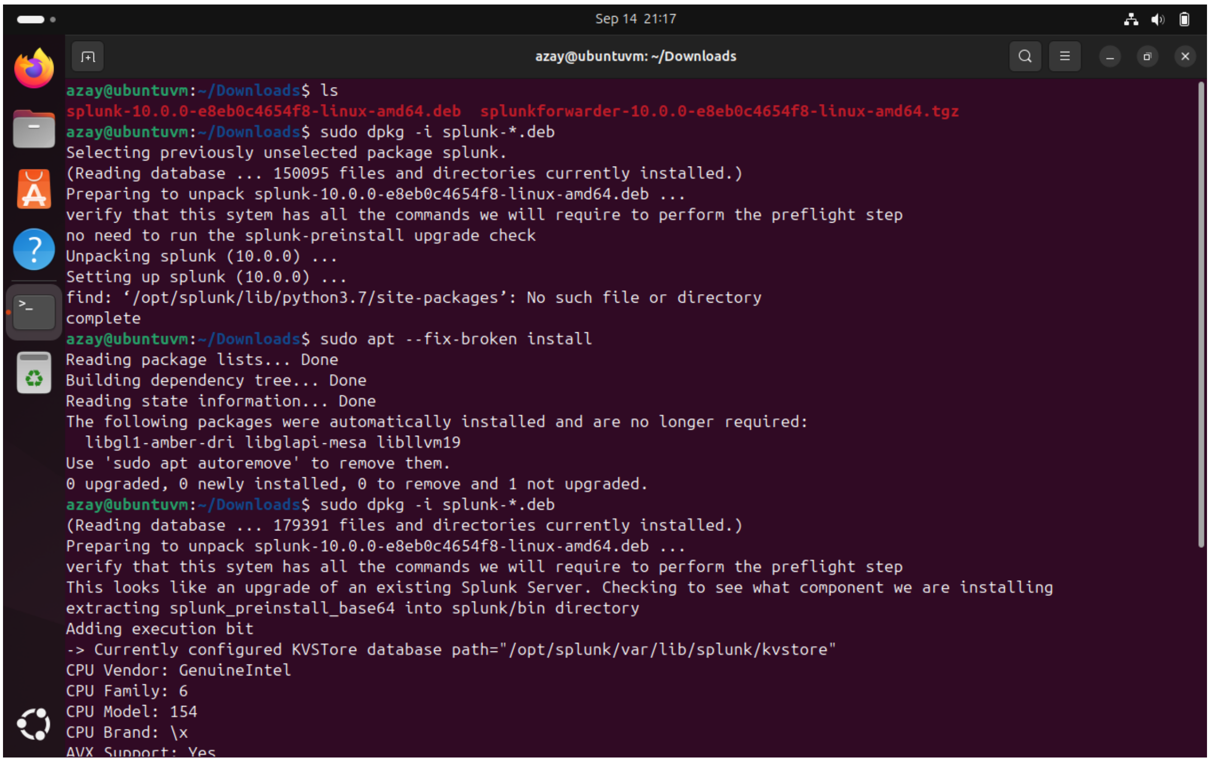
```
azay@ubuntuvm:~/Desktop$ sudo apt update
[sudo] password for azay:
Get:1 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Hit:2 http://in.archive.ubuntu.com/ubuntu noble InRelease
Get:3 http://in.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:4 http://security.ubuntu.com/ubuntu noble-security/main amd64 Components [21.5 kB]
Get:5 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Components [212 B]
Get:6 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Components [52.2 kB]
Get:7 http://in.archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Get:8 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Components [212 B]
Get:9 http://in.archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [1,389 kB]
Get:10 http://in.archive.ubuntu.com/ubuntu noble-updates/main amd64 Components [175 kB]
Get:11 http://in.archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Components [212 B]
Get:12 http://in.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Packages [1,482 kB]
Get:13 http://in.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Components [377 kB]
Get:14 http://in.archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Components [940 B]
Get:15 http://in.archive.ubuntu.com/ubuntu noble-backports/main amd64 Components [7,064 B]
Get:16 http://in.archive.ubuntu.com/ubuntu noble-backports/restricted amd64 Components [216 B]
Get:17 http://in.archive.ubuntu.com/ubuntu noble-backports/universe amd64 Components [19.2 kB]
Get:18 http://in.archive.ubuntu.com/ubuntu noble-backports/multiverse amd64 Components [212 B]
Fetched 3,904 kB in 5s (748 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
1 package can be upgraded. Run 'apt list --upgradable' to see it.
azay@ubuntuvm:~/Desktop$ sudo apt upgrade
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following packages were automatically installed and are no longer required:
  libgl1-amber-dri libglapi-mesa libllvm19
Use 'sudo apt autoremove' to remove them.
```

- Go to Downloads folder and extract and initialize Splunk and Universal Forwarder

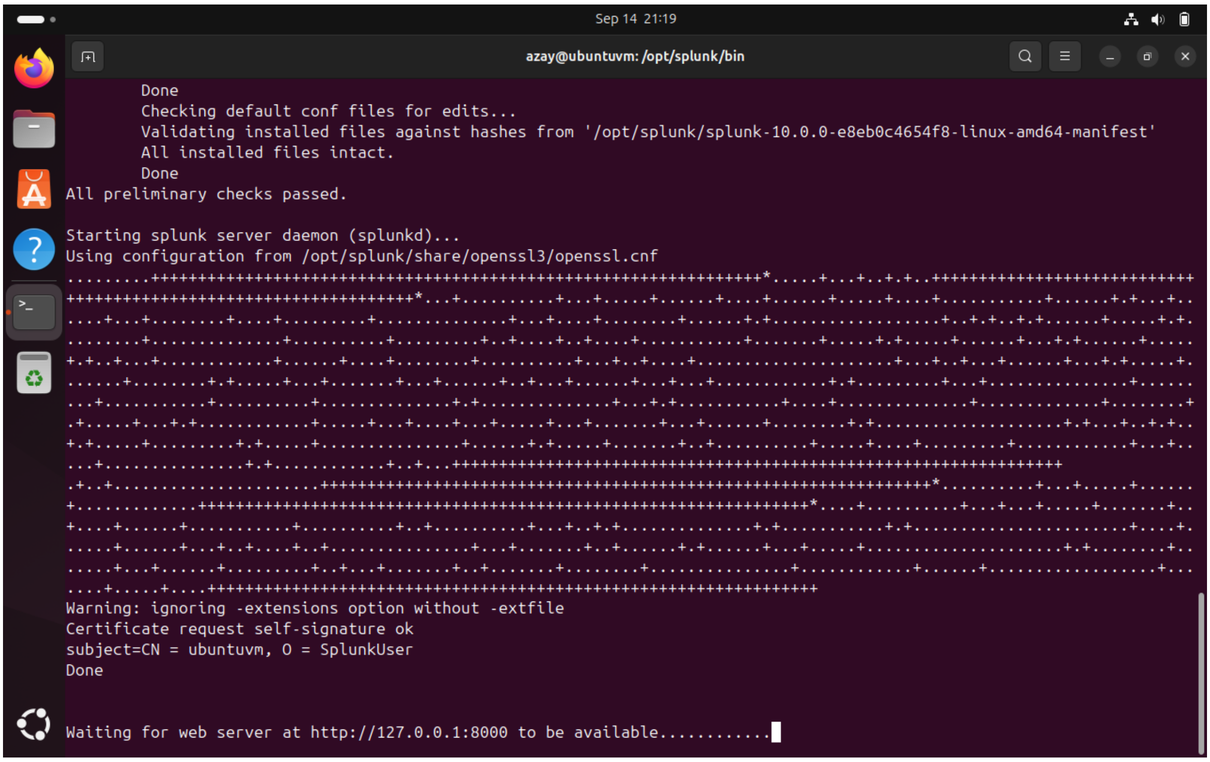




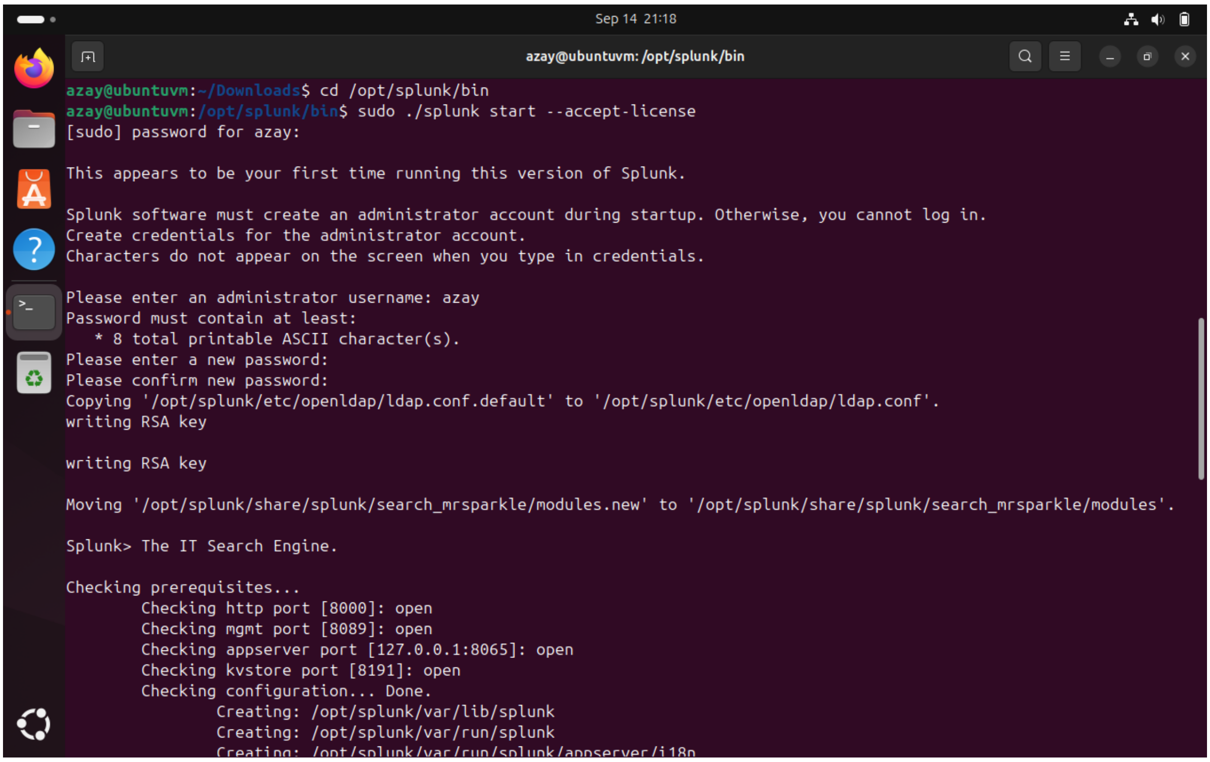
```
azay@ubuntuvm:~/Downloads$ ls
splunk-10.0.0-e8eb0c4654f8-linux-amd64.deb  splunkforwarder-10.0.0-e8eb0c4654f8-linux-amd64.tgz
azay@ubuntuvm:~/Downloads$
```



```
azay@ubuntuvm:~/Downloads$ ls
splunk-10.0.0-e8eb0c4654f8-linux-amd64.deb  splunkforwarder-10.0.0-e8eb0c4654f8-linux-amd64.tgz
azay@ubuntuvm:~/Downloads$ sudo dpkg -i splunk-*.deb
Selecting previously unselected package splunk.
(Reading database ... 150095 files and directories currently installed.)
Preparing to unpack splunk-10.0.0-e8eb0c4654f8-linux-amd64.deb ...
verify that this sytem has all the commands we will require to perform the preflight step
no need to run the splunk-preinstall upgrade check
Unpacking splunk (10.0.0) ...
Setting up splunk (10.0.0) ...
find: '/opt/splunk/lib/python3.7/site-packages': No such file or directory
complete
azay@ubuntuvm:~/Downloads$ sudo apt --fix-broken install
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libgl1-amber-dri libglapi-mesa libllvm19
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 1 not upgraded.
azay@ubuntuvm:~/Downloads$ sudo dpkg -i splunk-*.deb
(Reading database ... 179391 files and directories currently installed.)
Preparing to unpack splunk-10.0.0-e8eb0c4654f8-linux-amd64.deb ...
verify that this sytem has all the commands we will require to perform the preflight step
This looks like an upgrade of an existing Splunk Server. Checking to see what component we are installing
extracting splunk_preinstall_base64 into splunk/bin directory
Adding execution bit
-> Currently configured KVSTore database path="/opt/splunk/var/lib/splunk/kvstore"
CPU Vendor: GenuineIntel
CPU Family: 6
CPU Model: 154
CPU Brand: \x
AVX Support: Yes
```

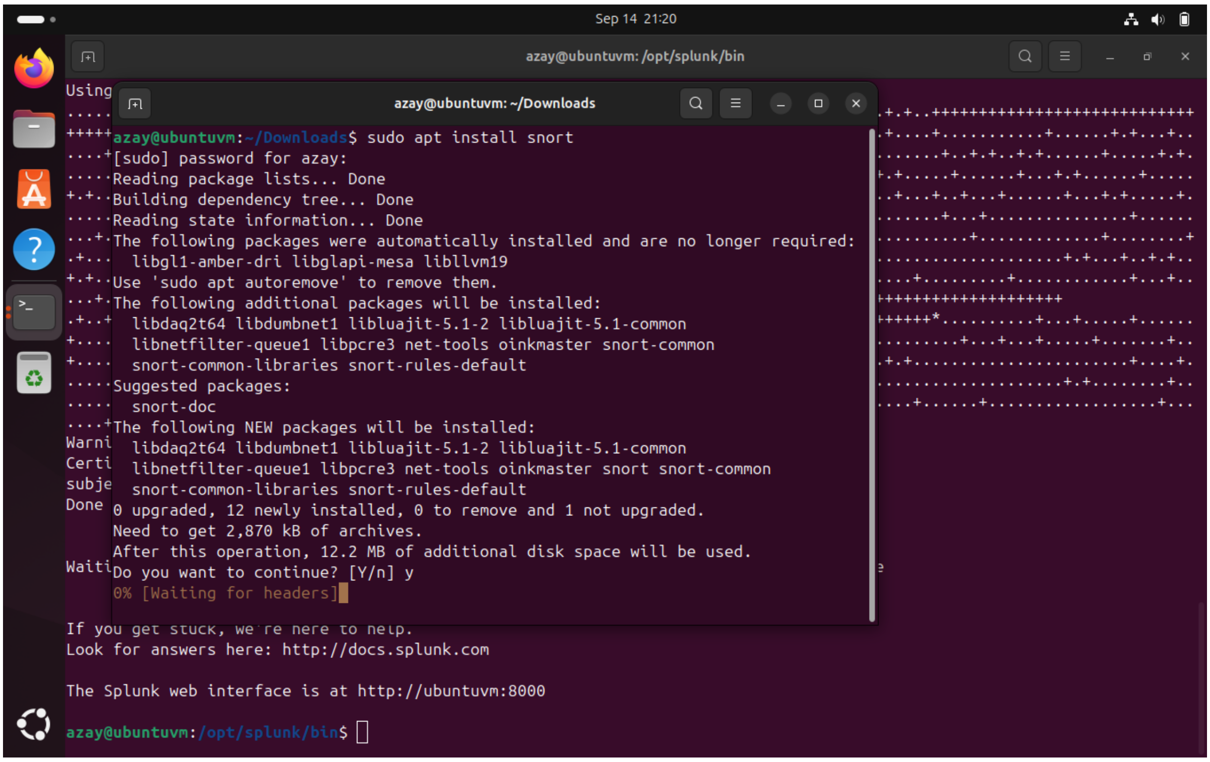


```
        Done
        Checking default conf files for edits...
        Validating installed files against hashes from '/opt/splunk/splunk-10.0.0-e8eb0c4654f8-linux-amd64-manifest'
        All installed files intact.
        Done
All preliminary checks passed.

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 = ubuntuvm, O = SplunkUser
Done


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



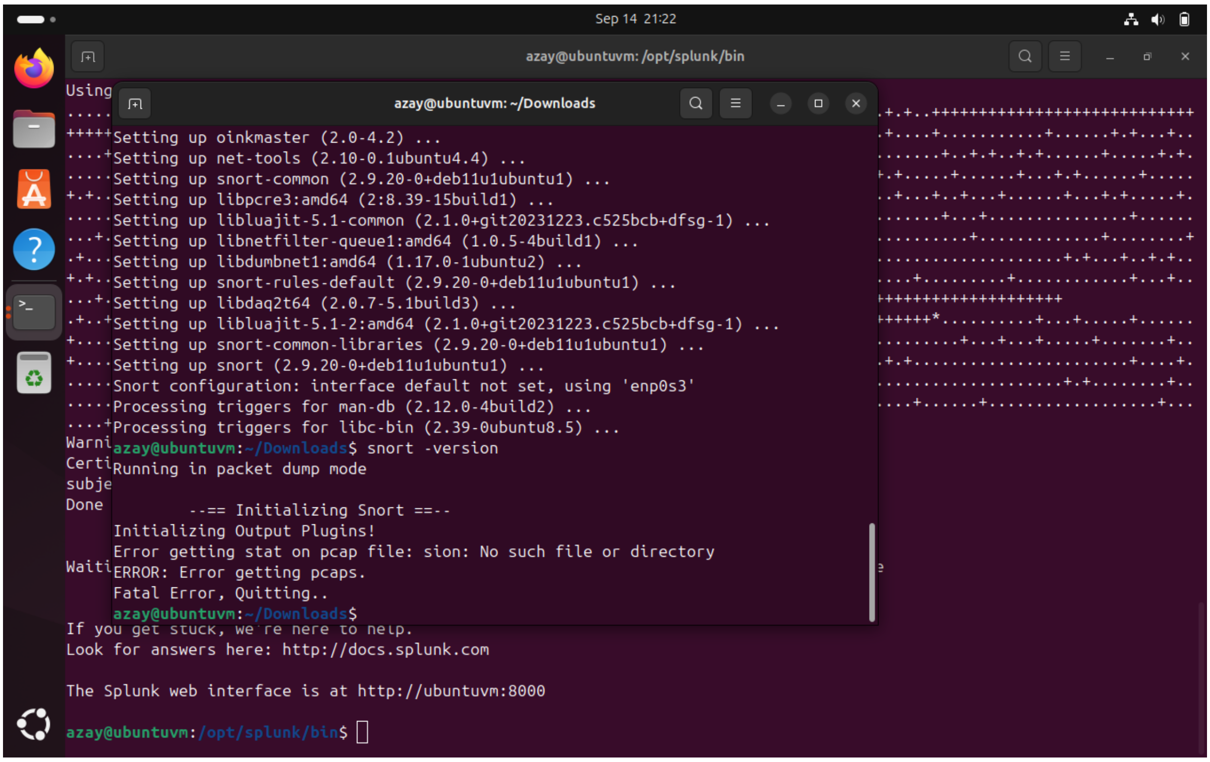
```
azay@ubuntuvm:~/Downloads$ cd /opt/splunk/bin
azay@ubuntuvm:/opt/splunk/bin$ sudo ./splunk start --accept-license
[sudo] password for azay:

This appears to be your first time running this version of Splunk.

Splunk software must create an administrator account during startup. Otherwise, you cannot log in.
Create credentials for the administrator account.
Characters do not appear on the screen when you type in credentials.

Please enter an administrator username: azay
Password must contain at least:
   * 8 total printable ASCII character(s).
Please enter a new password:
Please confirm new password:
Copying '/opt/splunk/etc/openldap/ldap.conf.default' to '/opt/splunk/etc/openldap/ldap.conf'.
writing RSA key

writing RSA key

Moving '/opt/splunk/share/splunk/search_mrsparkle/modules.new' to '/opt/splunk/share/splunk/search_mrsparkle/modules'.

Splunk> The IT Search Engine.

Checking prerequisites...
        Checking http port [8000]: open
        Checking mgmt port [8089]: open
        Checking appserver port [127.0.0.1:8065]: open
        Checking kvstore port [8191]: open
        Checking configuration... Done.
                Creating: /opt/splunk/var/lib/splunk
                Creating: /opt/splunk/var/run/splunk
                Creating: /opt/splunk/var/run/splunk/appserver/i18n
```

- Now Install and Initialize the Snort IDS



```
azay@ubuntuvm:~/Downloads$ sudo apt install snort
[sudo] password for azay:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libgl1-amber-dri libglapi-mesa libllvm19
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libdaq2t64 libdumbnet1 libluajit-5.1-2 libluajit-5.1-common
  libnetfilter-queue1 libpcre3 net-tools oinkmaster snort-common
  snort-common-libraries snort-rules-default
Suggested packages:
  snort-doc
The following NEW packages will be installed:
  libdaq2t64 libdumbnet1 libluajit-5.1-2 libluajit-5.1-common
  libnetfilter-queue1 libpcre3 net-tools oinkmaster snort snort-common
  snort-common-libraries snort-rules-default
0 upgraded, 12 newly installed, 0 to remove and 1 not upgraded.
Need to get 2,870 kB of archives.
After this operation, 12.2 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
0% [Waiting for headers]
```

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

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

azay@ubuntuvm:/opt/splunk/bin$
```



Sep 14 21:22

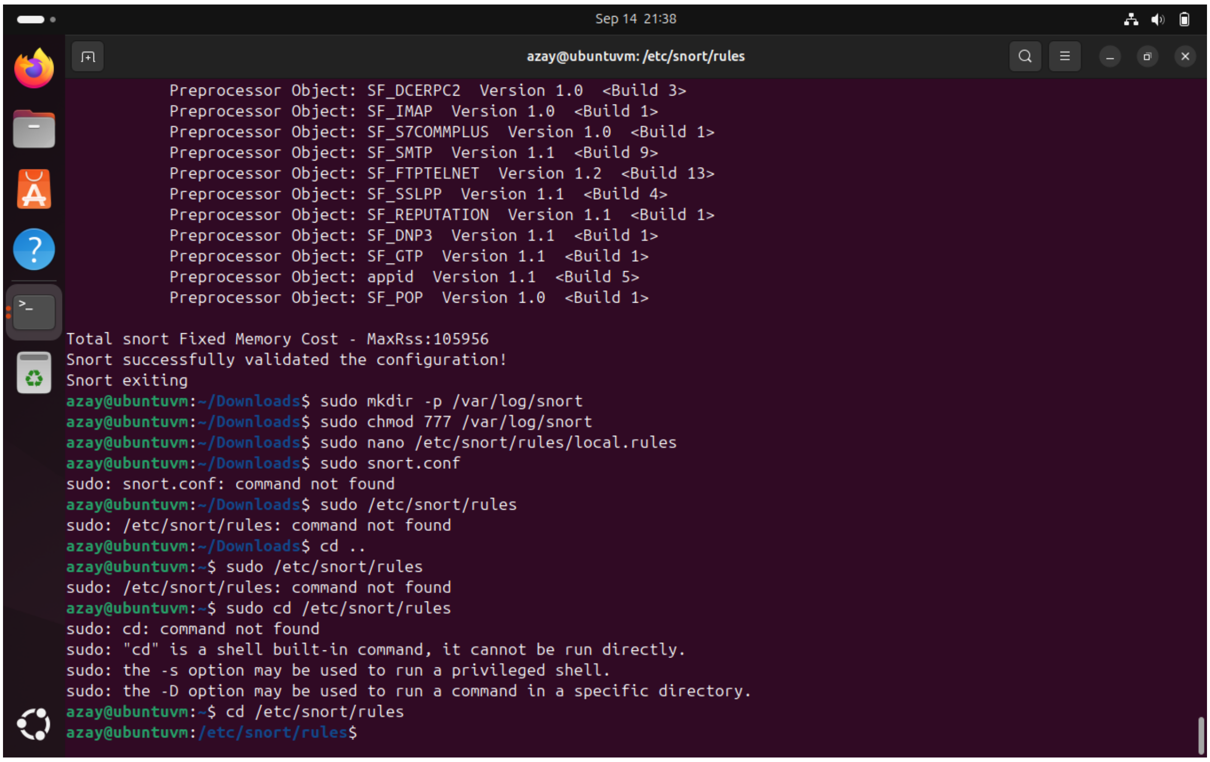
azay@ubuntuvm: /opt/splunk/bin

azay@ubuntuvm: ~/Downloads

```
Setting up oinkmaster (2.0-4.2) ...
Setting up net-tools (2.10-0.1ubuntu4.4) ...
Setting up snort-common (2.9.20-0+deb11u1ubuntu1) ...
Setting up libpcre3:amd64 (2:8.39-15build1) ...
Setting up libluajit-5.1-common (2.1.0+git20231223.c525bcb+dfsg-1) ...
Setting up libnetfilter-queue1:amd64 (1.0.5-4build1) ...
Setting up libdumbnet1:amd64 (1.17.0-1ubuntu2) ...
Setting up snort-rules-default (2.9.20-0+deb11u1ubuntu1) ...
Setting up libdaq2t64 (2.0.7-5.1build3) ...
Setting up libluajit-5.1-2:amd64 (2.1.0+git20231223.c525bcb+dfsg-1) ...
Setting up snort-common-libraries (2.9.20-0+deb11u1ubuntu1) ...
Setting up snort (2.9.20-0+deb11u1ubuntu1) ...
Snort configuration: interface default not set, using 'enp0s3'
Processing triggers for man-db (2.12.0-4build2) ...
Processing triggers for libc-bin (2.39-0ubuntu8.5) ...
azay@ubuntuvm:~/Downloads$ snort -version
Running in packet dump mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Error getting stat on pcap file: sion: No such file or directory
ERROR: Error getting pcaps.
Fatal Error, Quitting..
azay@ubuntuvm:~/Downloads$
```

```
Using
Warni
Certi
subje
Done

Waiti

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

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

azay@ubuntuvm:/opt/splunk/bin$
```

- Now create a folder to save log alerts

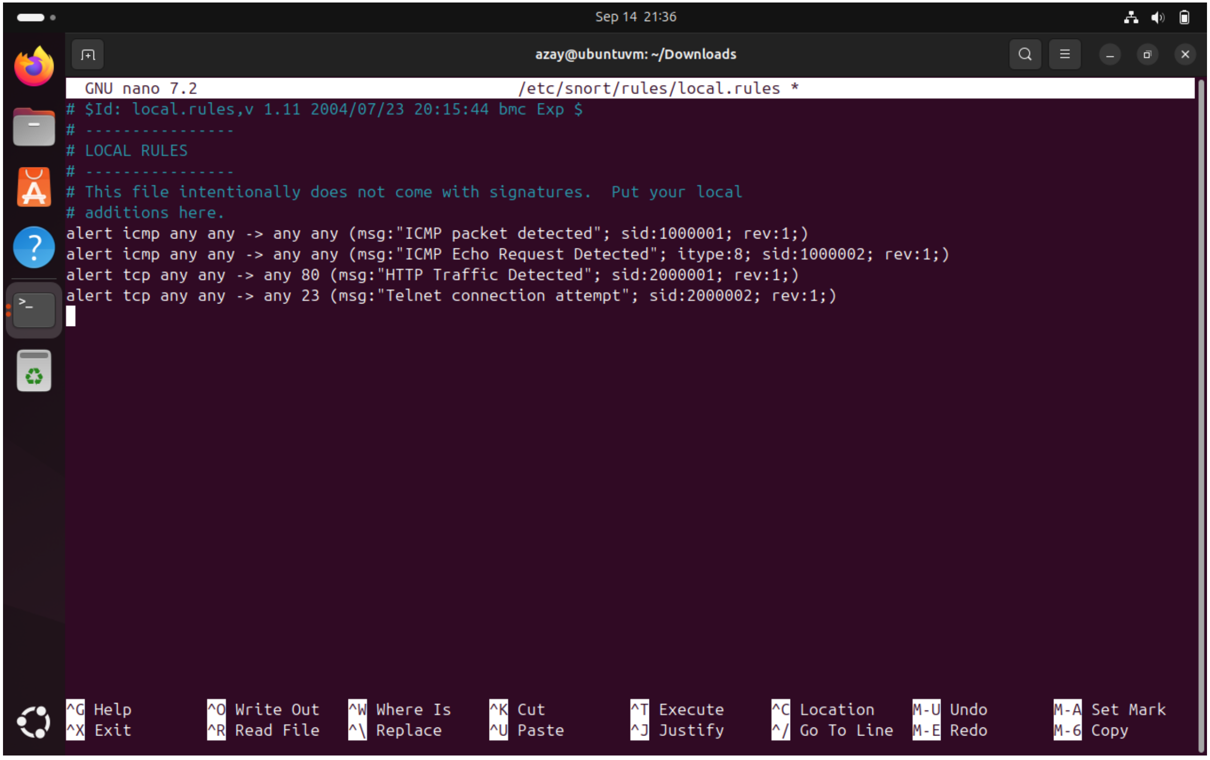


Sep 14 21:38

azay@ubuntuvm: /etc/snort/rules

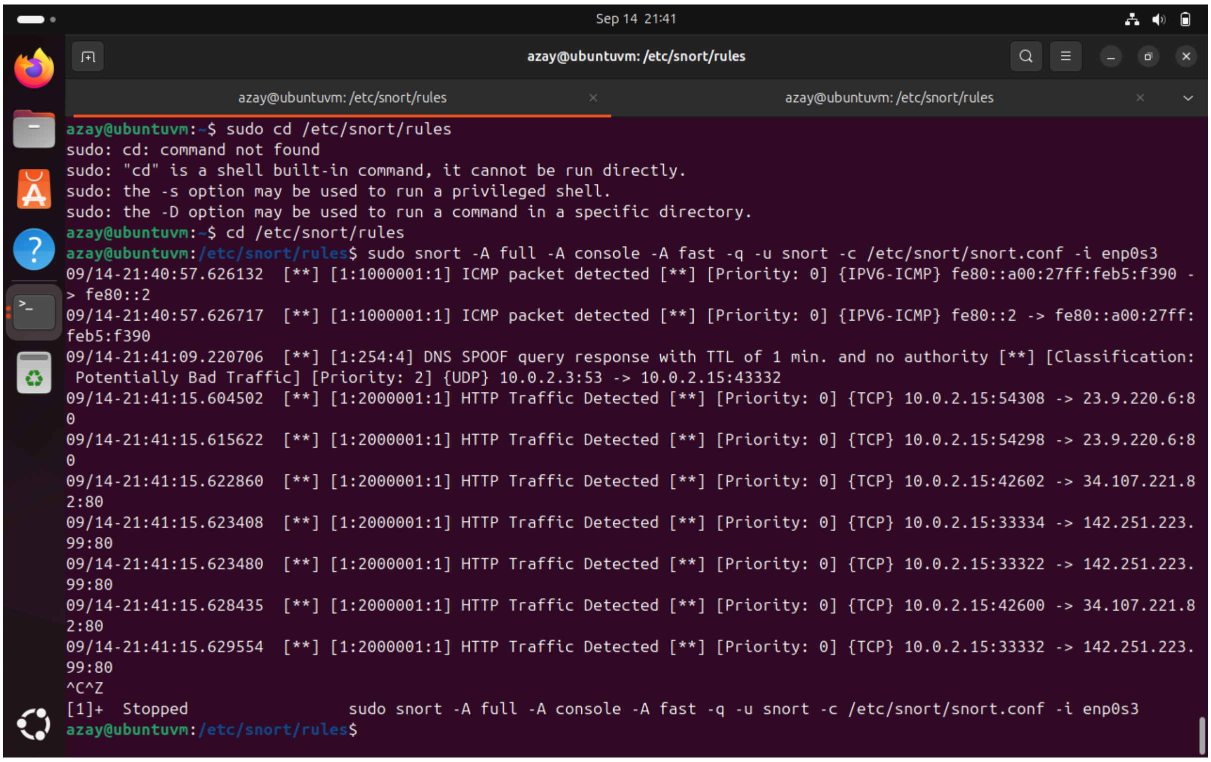
```
          Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
          Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
          Preprocessor Object: SF_S7COMMPLUS  Version 1.0  <Build 1>
          Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
          Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
          Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
          Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
          Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
          Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
          Preprocessor Object: appid  Version 1.1  <Build 5>
          Preprocessor Object: SF_POP  Version 1.0  <Build 1>

Total snort Fixed Memory Cost - MaxRss:105956
Snort successfully validated the configuration!
Snort exiting
azay@ubuntuvm:~/Downloads$ sudo mkdir -p /var/log/snort
azay@ubuntuvm:~/Downloads$ sudo chmod 777 /var/log/snort
azay@ubuntuvm:~/Downloads$ sudo nano /etc/snort/rules/local.rules
azay@ubuntuvm:~/Downloads$ sudo snort.conf
sudo: snort.conf: command not found
azay@ubuntuvm:~/Downloads$ sudo /etc/snort/rules
sudo: /etc/snort/rules: command not found
azay@ubuntuvm:~/Downloads$ cd ..
azay@ubuntuvm:~$ sudo /etc/snort/rules
sudo: /etc/snort/rules: command not found
azay@ubuntuvm:~$ sudo cd /etc/snort/rules
sudo: cd: command not found
sudo: "cd" is a shell built-in command, it cannot be run directly.
sudo: the -s option may be used to run a privileged shell.
sudo: the -D option may be used to run a command in a specific directory.
azay@ubuntuvm:~$ cd /etc/snort/rules
azay@ubuntuvm:/etc/snort/rules$
```

- Now add rules in to local.rules files to get alerts.



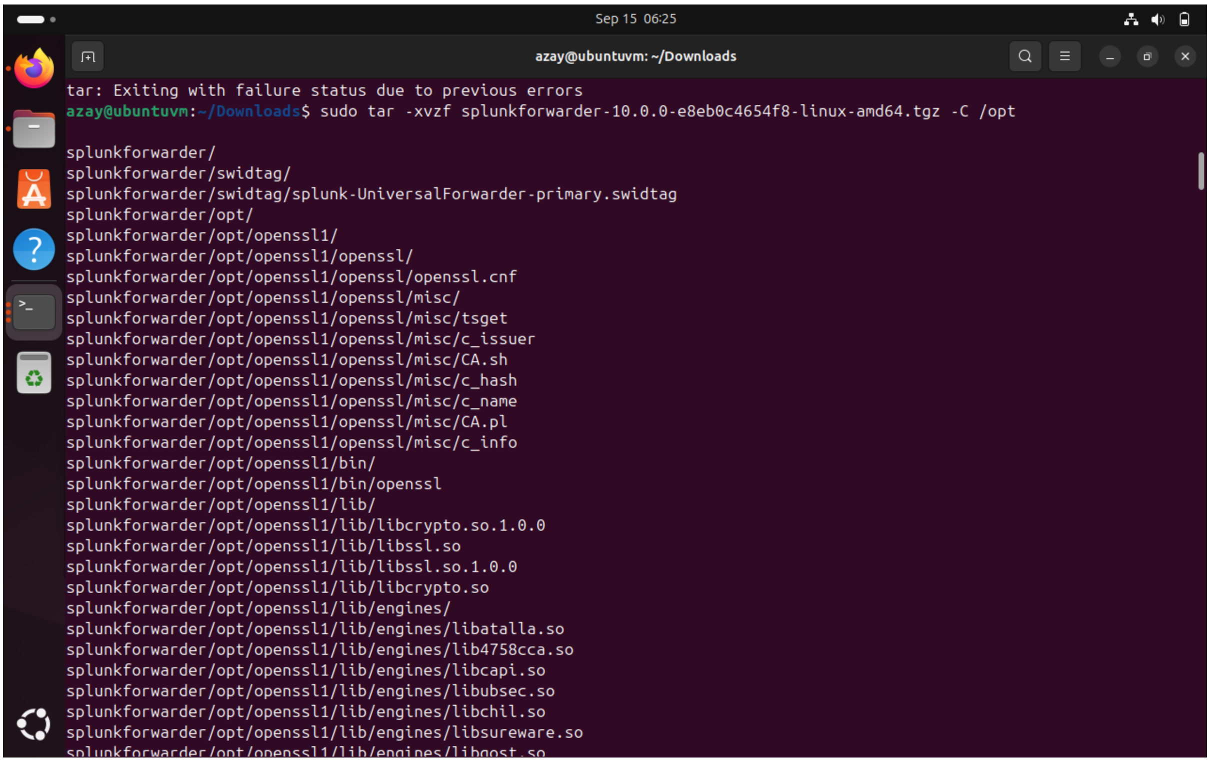
```
  GNU nano 7.2                          /etc/snort/rules/local.rules *
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# ----------------
# LOCAL RULES
# ----------------
# This file intentionally does not come with signatures.  Put your local
# additions here.
alert icmp any any -> any any (msg:"ICMP packet detected"; sid:1000001; rev:1;)
alert icmp any any -> any any (msg:"ICMP Echo Request Detected"; itype:8; sid:1000002; rev:1;)
alert tcp any any -> any 80 (msg:"HTTP Traffic Detected"; sid:2000001; rev:1;)
alert tcp any any -> any 23 (msg:"Telnet connection attempt"; sid:2000002; rev:1;)

^G Help       ^O Write Out   ^W Where Is    ^K Cut         ^T Execute     ^C Location    M-U Undo       M-A Set Mark
^X Exit       ^R Read File   ^\ Replace     ^U Paste       ^J Justify     ^/ Go To Line  M-E Redo       M-6 Copy
```

- Then Run command to get logs on console mode and to save in a file

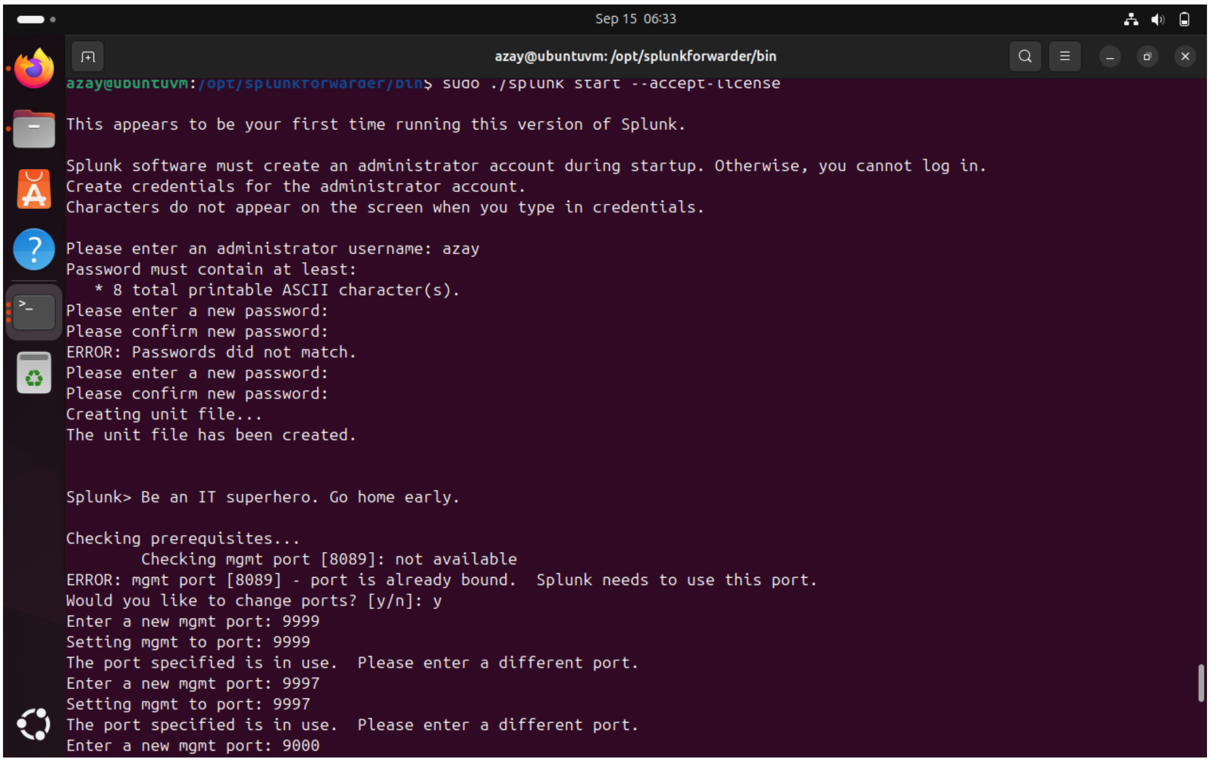

Sep 14 21:41
azay@ubuntuvm: /etc/snort/rules
azay@ubuntuvm: /etc/snort/rules
azay@ubuntuvm: /etc/snort/rules

```
azay@ubuntuvm:~$ sudo cd /etc/snort/rules
sudo: cd: command not found
sudo: "cd" is a shell built-in command, it cannot be run directly.
sudo: the -s option may be used to run a privileged shell.
sudo: the -D option may be used to run a command in a specific directory.
azay@ubuntuvm:~$ cd /etc/snort/rules
azay@ubuntuvm:/etc/snort/rules$ sudo snort -A full -A console -A fast -q -u snort -c /etc/snort/snort.conf -i enp0s3
09/14-21:40:57.626132  [**] [1:1000001:1] ICMP packet detected [**] [Priority: 0] {IPV6-ICMP} fe80::a00:27ff:feb5:f390 -
> fe80::2
09/14-21:40:57.626717  [**] [1:1000001:1] ICMP packet detected [**] [Priority: 0] {IPV6-ICMP} fe80::2 -> fe80::a00:27ff:
feb5:f390
09/14-21:41:09.220706  [**] [1:254:4] DNS SPOOF query response with TTL of 1 min. and no authority [**] [Classification:
 Potentially Bad Traffic] [Priority: 2] {UDP} 10.0.2.3:53 -> 10.0.2.15:43332
09/14-21:41:15.604502  [**] [1:2000001:1] HTTP Traffic Detected [**] [Priority: 0] {TCP} 10.0.2.15:54308 -> 23.9.220.6:8
0
09/14-21:41:15.615622  [**] [1:2000001:1] HTTP Traffic Detected [**] [Priority: 0] {TCP} 10.0.2.15:54298 -> 23.9.220.6:8
0
09/14-21:41:15.622860  [**] [1:2000001:1] HTTP Traffic Detected [**] [Priority: 0] {TCP} 10.0.2.15:42602 -> 34.107.221.8
2:80
09/14-21:41:15.623408  [**] [1:2000001:1] HTTP Traffic Detected [**] [Priority: 0] {TCP} 10.0.2.15:33334 -> 142.251.223.
99:80
09/14-21:41:15.623480  [**] [1:2000001:1] HTTP Traffic Detected [**] [Priority: 0] {TCP} 10.0.2.15:33322 -> 142.251.223.
99:80
09/14-21:41:15.628435  [**] [1:2000001:1] HTTP Traffic Detected [**] [Priority: 0] {TCP} 10.0.2.15:42600 -> 34.107.221.8
2:80
09/14-21:41:15.629554  [**] [1:2000001:1] HTTP Traffic Detected [**] [Priority: 0] {TCP} 10.0.2.15:33332 -> 142.251.223.
99:80
^C^Z
[1]+  Stopped                 sudo snort -A full -A console -A fast -q -u snort -c /etc/snort/snort.conf -i enp0s3
azay@ubuntuvm:/etc/snort/rules$
```

- Now initialize and start Universal Forwarder go to downloads and extract universal forwarder and go to bin then open terminal from bin to initialize and start Universal Forwarder

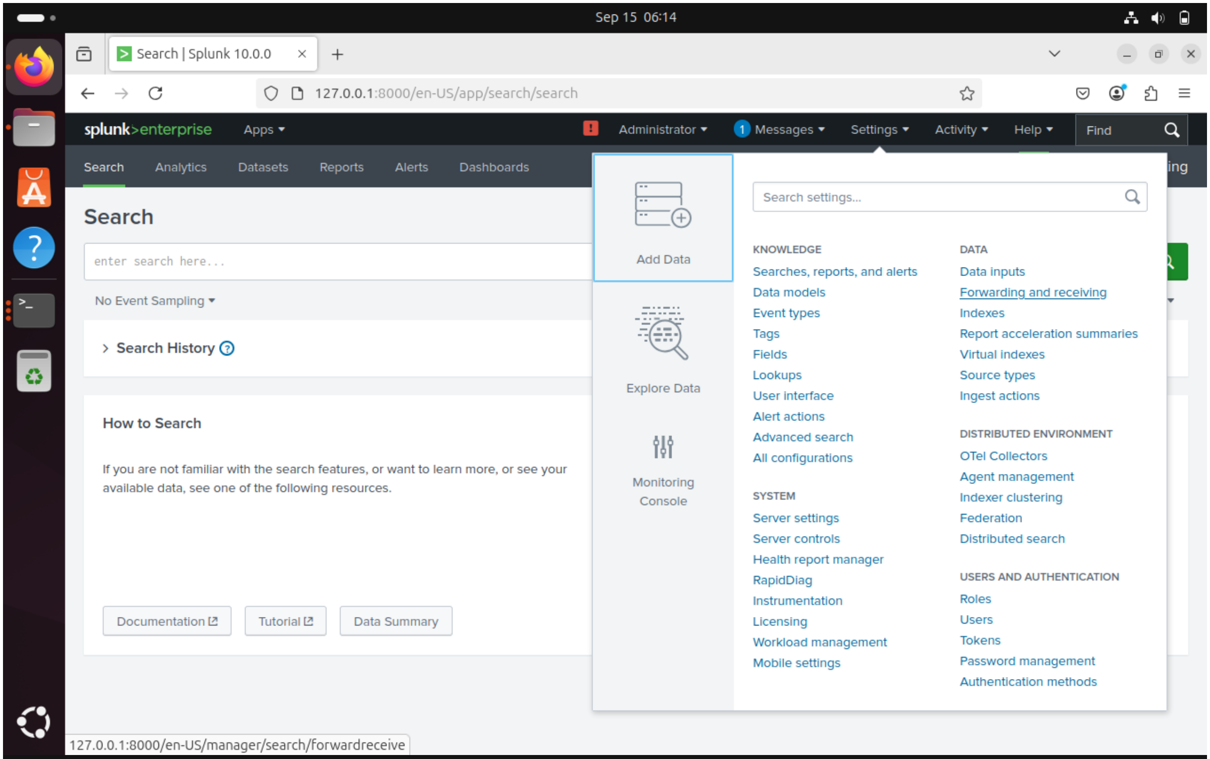


```
tar: Exiting with failure status due to previous errors
azay@ubuntuvm:~/Downloads$ sudo tar -xvzf splunkforwarder-10.0.0-e8eb0c4654f8-linux-amd64.tgz -C /opt

splunkforwarder/
splunkforwarder/swidtag/
splunkforwarder/swidtag/splunk-UniversalForwarder-primary.swidtag
splunkforwarder/opt/
splunkforwarder/opt/openssl1/
splunkforwarder/opt/openssl1/openssl/
splunkforwarder/opt/openssl1/openssl/openssl.cnf
splunkforwarder/opt/openssl1/openssl/misc/
splunkforwarder/opt/openssl1/openssl/misc/tsget
splunkforwarder/opt/openssl1/openssl/misc/c_issuer
splunkforwarder/opt/openssl1/openssl/misc/CA.sh
splunkforwarder/opt/openssl1/openssl/misc/c_hash
splunkforwarder/opt/openssl1/openssl/misc/c_name
splunkforwarder/opt/openssl1/openssl/misc/CA.pl
splunkforwarder/opt/openssl1/openssl/misc/c_info
splunkforwarder/opt/openssl1/bin/
splunkforwarder/opt/openssl1/bin/openssl
splunkforwarder/opt/openssl1/lib/
splunkforwarder/opt/openssl1/lib/libcrypto.so.1.0.0
splunkforwarder/opt/openssl1/lib/libssl.so
splunkforwarder/opt/openssl1/lib/libssl.so.1.0.0
splunkforwarder/opt/openssl1/lib/libcrypto.so
splunkforwarder/opt/openssl1/lib/engines/
splunkforwarder/opt/openssl1/lib/engines/libatalla.so
splunkforwarder/opt/openssl1/lib/engines/lib4758cca.so
splunkforwarder/opt/openssl1/lib/engines/libcapi.so
splunkforwarder/opt/openssl1/lib/engines/libubsec.so
splunkforwarder/opt/openssl1/lib/engines/libchil.so
splunkforwarder/opt/openssl1/lib/engines/libsureware.so
splunkforwarder/opt/openssl1/lib/engines/libgost.so
```



```
azay@ubuntuvm:/opt/splunkforwarder/bin$ sudo ./splunk start --accept-license

This appears to be your first time running this version of Splunk.

Splunk software must create an administrator account during startup. Otherwise, you cannot log in.
Create credentials for the administrator account.
Characters do not appear on the screen when you type in credentials.

Please enter an administrator username: azay
Password must contain at least:
   * 8 total printable ASCII character(s).
Please enter a new password:
Please confirm new password:
ERROR: Passwords did not match.
Please enter a new password:
Please confirm new password:
Creating unit file...
The unit file has been created.


Splunk> Be an IT superhero. Go home early.

Checking prerequisites...
        Checking mgmt port [8089]: not available
ERROR: mgmt port [8089] - port is already bound.  Splunk needs to use this port.
Would you like to change ports? [y/n]: y
Enter a new mgmt port: 9999
Setting mgmt to port: 9999
The port specified is in use.  Please enter a different port.
Enter a new mgmt port: 9997
Setting mgmt to port: 9997
The port specified is in use.  Please enter a different port.
Enter a new mgmt port: 9000
```

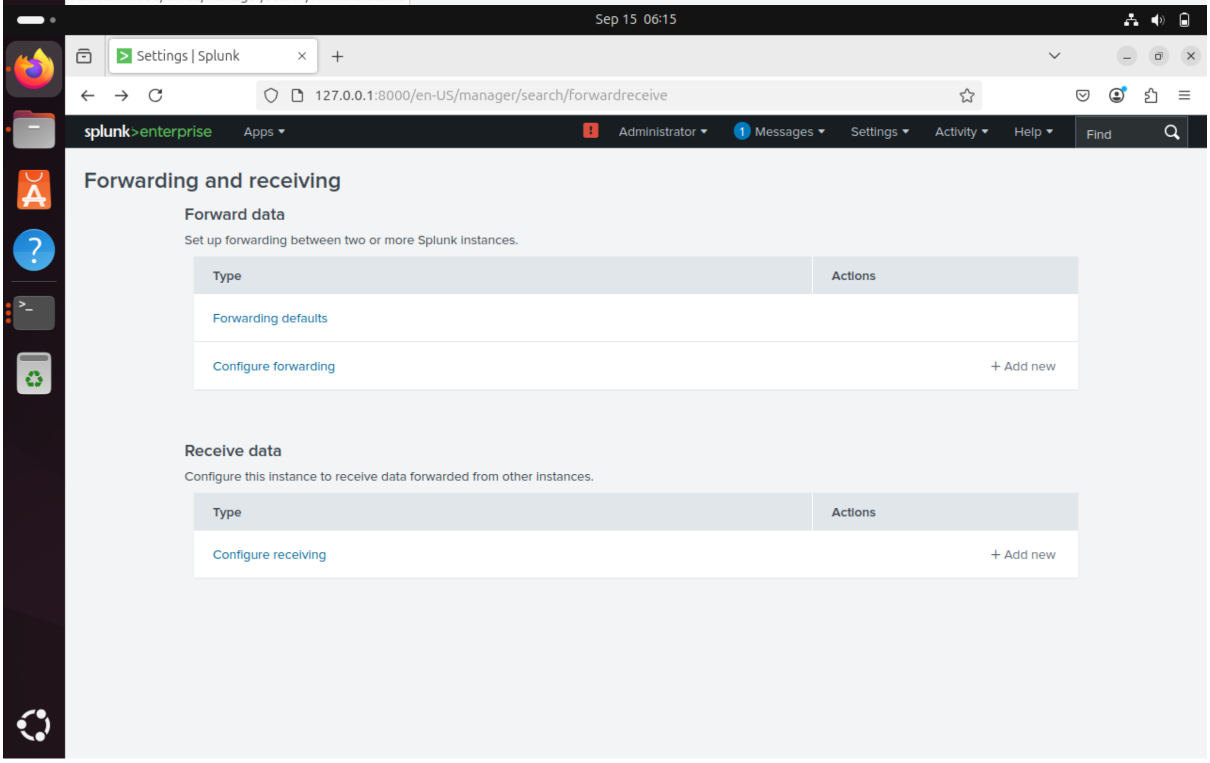
- Open browser and open Splunk using the server IP above
- Add port number in Splunk by clicking on forward and recieving



Search

How to Search

If you are not familiar with the search features, or want to learn more, or see your available data, see one of the following resources.



Forwarding and receiving

Forward data

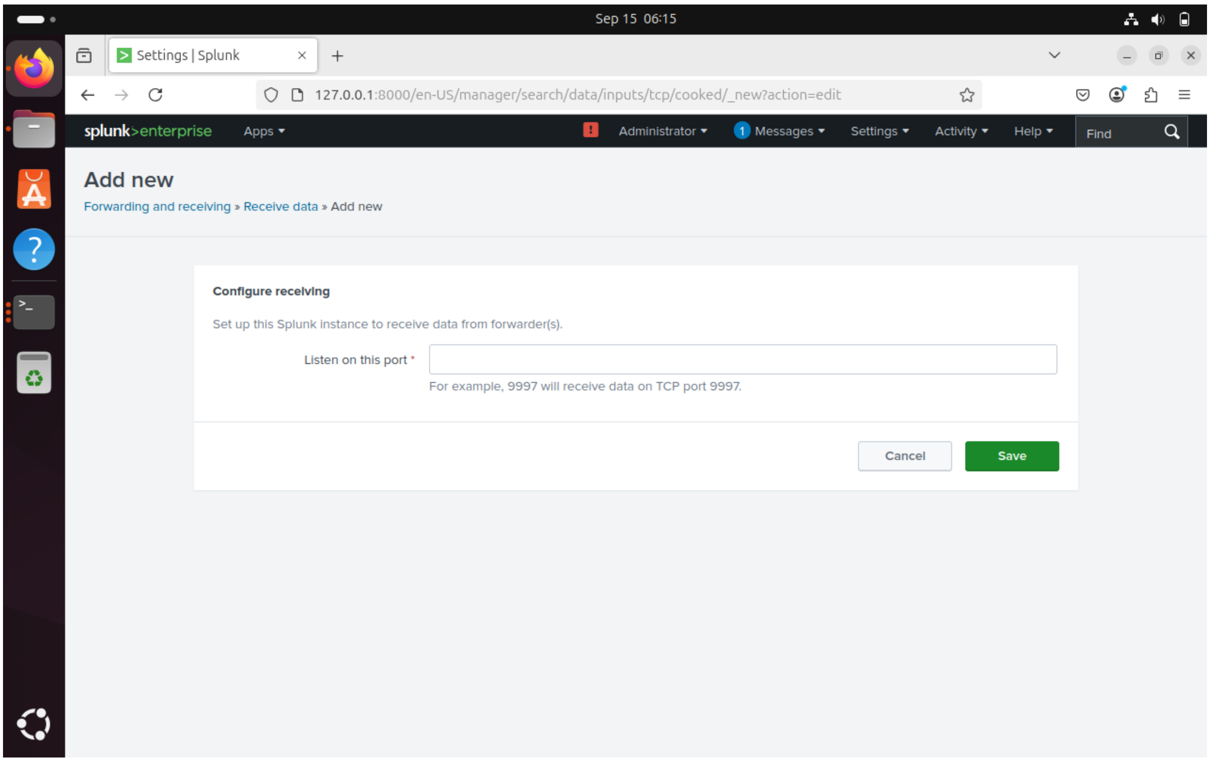
Set up forwarding between two or more Splunk instances.

Type	Actions
Forwarding defaults	
Configure forwarding	+ Add new

Receive data

Configure this instance to receive data forwarded from other instances.

Type	Actions
Configure receiving	+ Add new



Add new

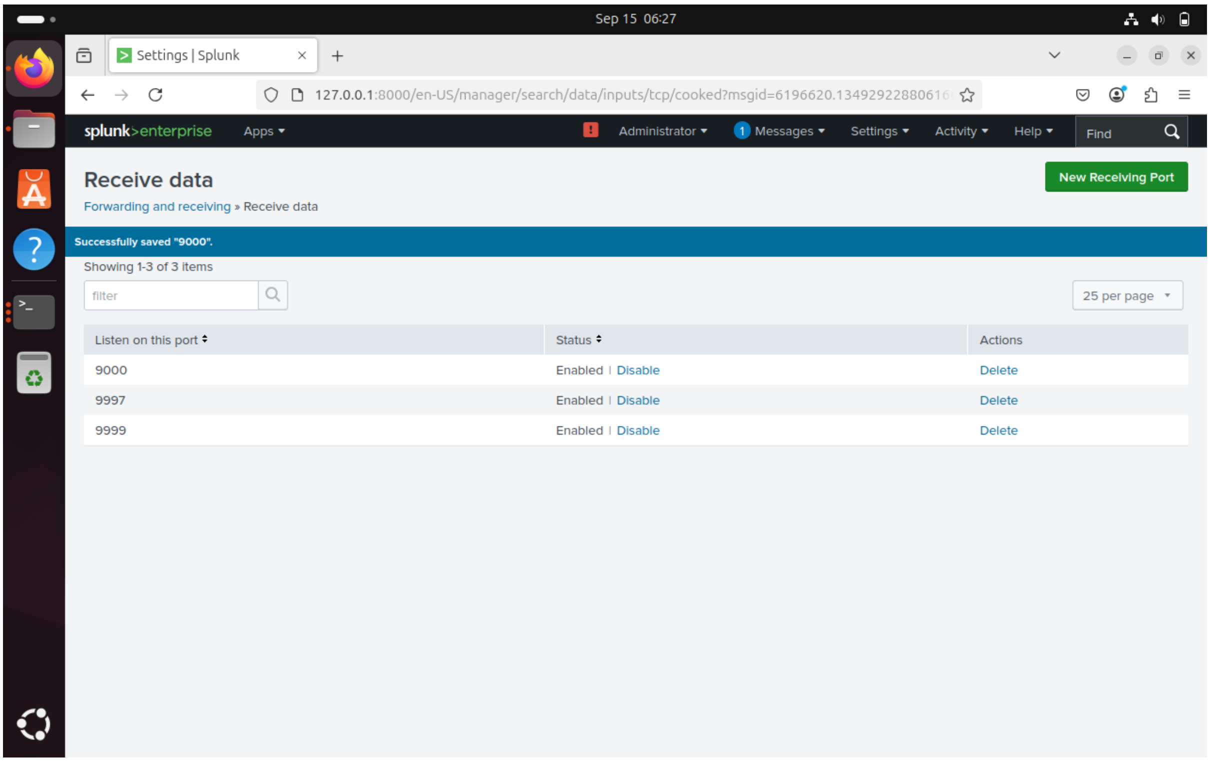
Forwarding and receiving » Receive data » Add new

Configure receiving

Set up this Splunk instance to receive data from forwarder(s).

Listen on this port *

For example, 9997 will receive data on TCP port 9997.



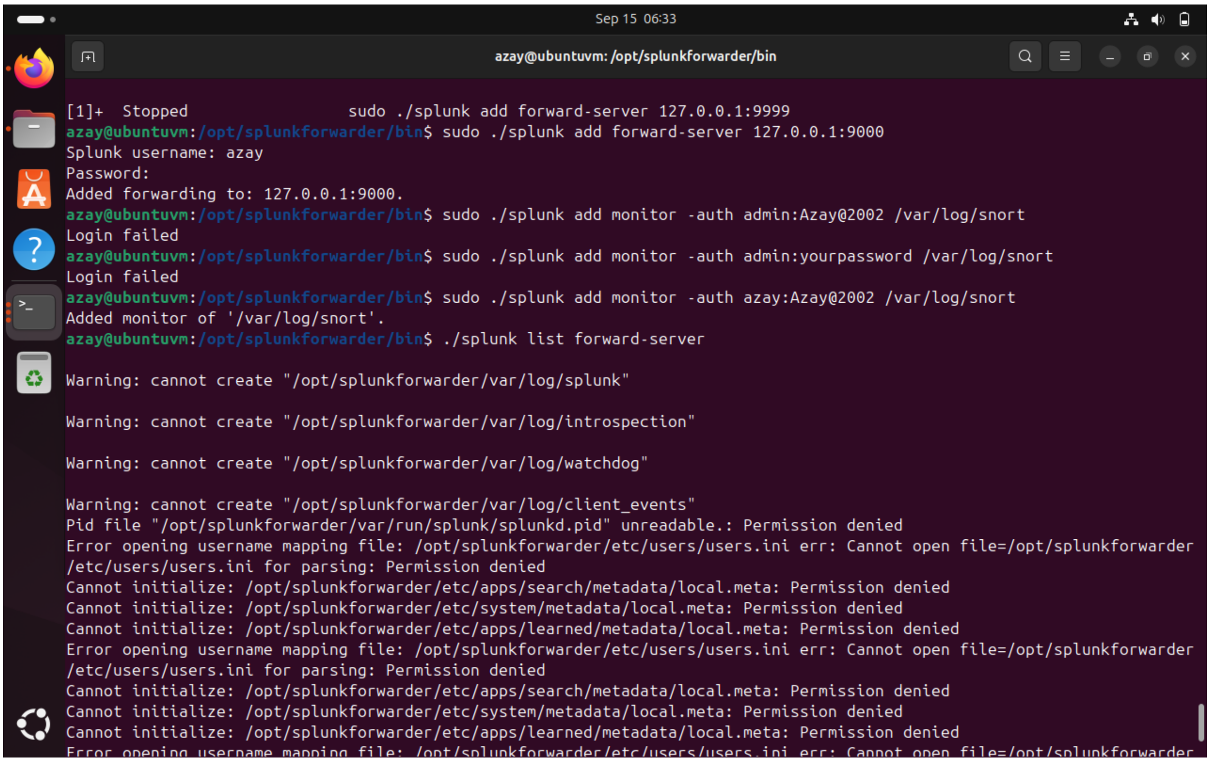
Receive data

Forwarding and receiving » Receive data

Successfully saved "9000".

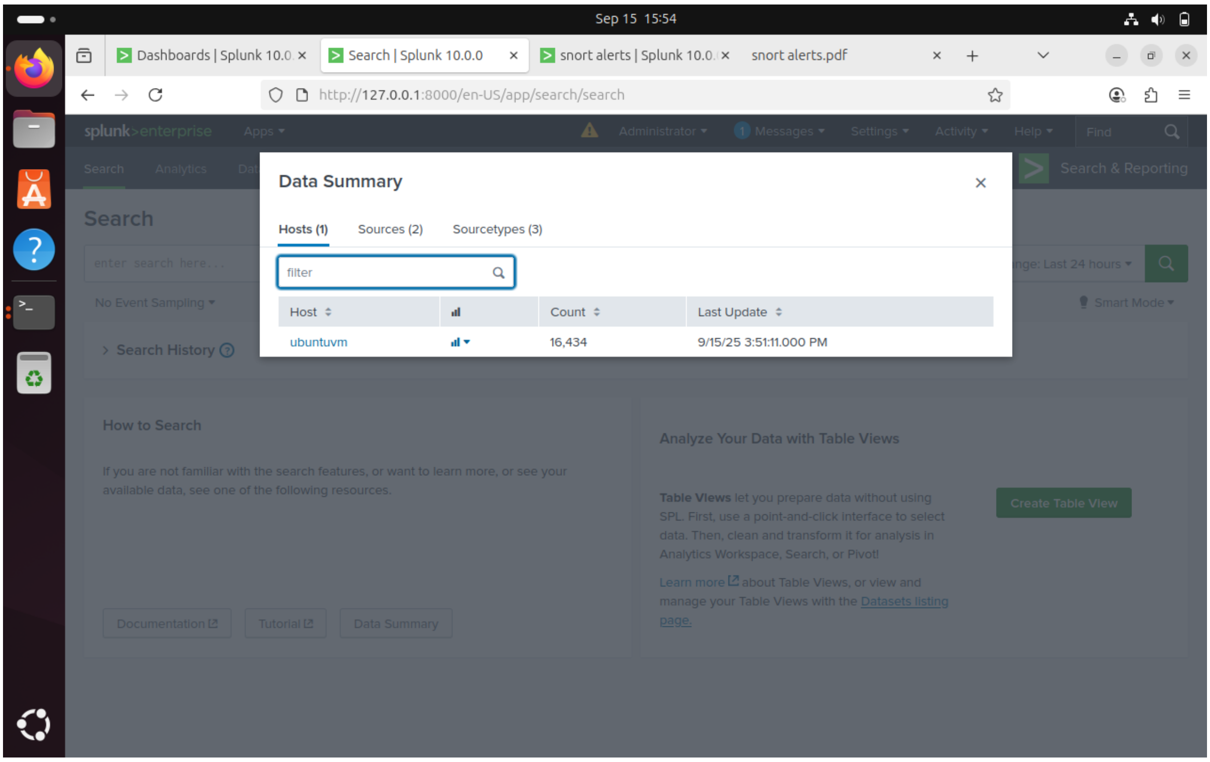
Showing 1-3 of 3 items

Listen on this port	Status	Actions
9000	Enabled | Disable	Delete
9997	Enabled | Disable	Delete
9999	Enabled | Disable	Delete



```
[1]+  Stopped                 sudo ./splunk add forward-server 127.0.0.1:9999
azay@ubuntuvm:/opt/splunkforwarder/bin$ sudo ./splunk add forward-server 127.0.0.1:9000
Splunk username: azay
Password:
Added forwarding to: 127.0.0.1:9000.
azay@ubuntuvm:/opt/splunkforwarder/bin$ sudo ./splunk add monitor -auth admin:Azay@2002 /var/log/snort
Login failed
azay@ubuntuvm:/opt/splunkforwarder/bin$ sudo ./splunk add monitor -auth admin:yourpassword /var/log/snort
Login failed
azay@ubuntuvm:/opt/splunkforwarder/bin$ sudo ./splunk add monitor -auth azay:Azay@2002 /var/log/snort
Added monitor of '/var/log/snort'.
azay@ubuntuvm:/opt/splunkforwarder/bin$ ./splunk list forward-server

Warning: cannot create "/opt/splunkforwarder/var/log/splunk"

Warning: cannot create "/opt/splunkforwarder/var/log/introspection"

Warning: cannot create "/opt/splunkforwarder/var/log/watchdog"

Warning: cannot create "/opt/splunkforwarder/var/log/client_events"
Pid file "/opt/splunkforwarder/var/run/splunk/splunkd.pid" unreadable.: Permission denied
Error opening username mapping file: /opt/splunkforwarder/etc/users/users.ini err: Cannot open file=/opt/splunkforwarder
/etc/users/users.ini for parsing: Permission denied
Cannot initialize: /opt/splunkforwarder/etc/apps/search/metadata/local.meta: Permission denied
Cannot initialize: /opt/splunkforwarder/etc/system/metadata/local.meta: Permission denied
Cannot initialize: /opt/splunkforwarder/etc/apps/learned/metadata/local.meta: Permission denied
Error opening username mapping file: /opt/splunkforwarder/etc/users/users.ini err: Cannot open file=/opt/splunkforwarder
/etc/users/users.ini for parsing: Permission denied
Cannot initialize: /opt/splunkforwarder/etc/apps/search/metadata/local.meta: Permission denied
Cannot initialize: /opt/splunkforwarder/etc/system/metadata/local.meta: Permission denied
Cannot initialize: /opt/splunkforwarder/etc/apps/learned/metadata/local.meta: Permission denied
Error opening username mapping file: /opt/splunkforwarder/etc/users/users.ini err: Cannot open file=/opt/splunkforwarder
```

- Click on search and reporting app and then click on data summary button given below



Data Summary

Host		Count	Last Update
ubuntuvm		16,434	9/15/25 3:51:11.000 PM

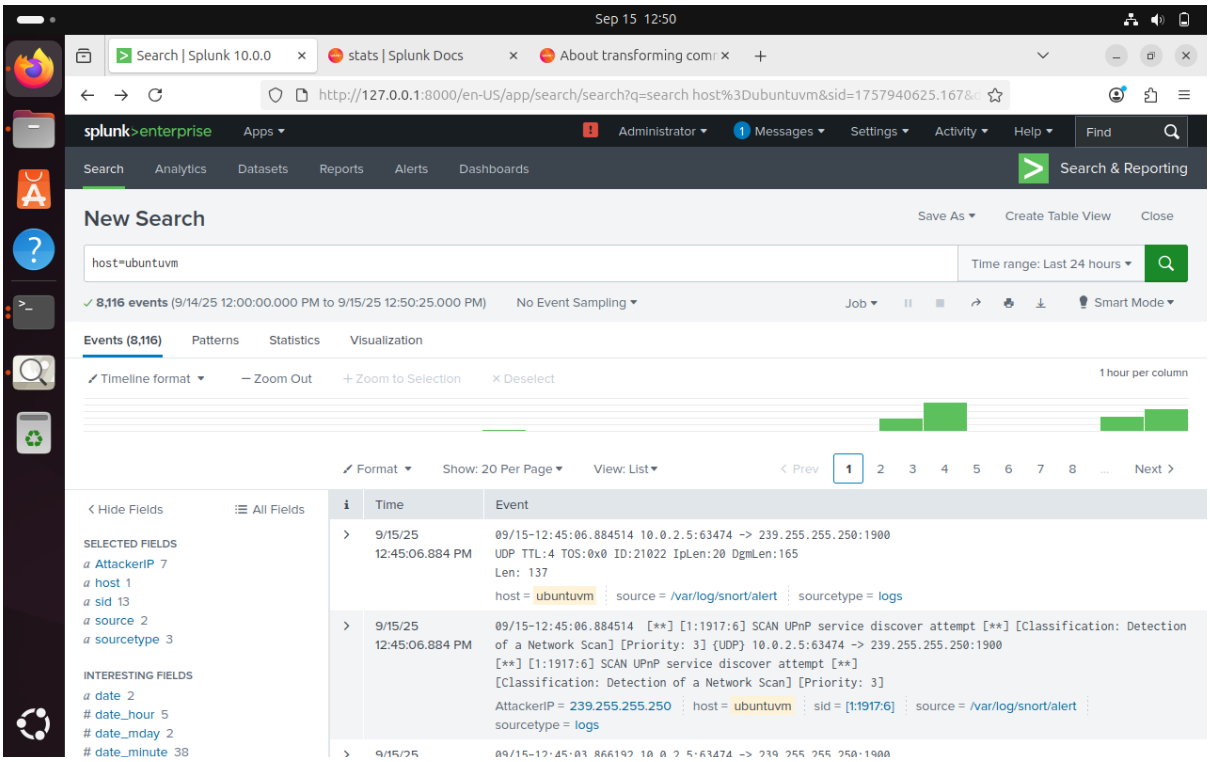
If you are not familiar with the search features, or want to learn more, or see your available data, see one of the following resources.

Table Views let you prepare data without using SPL. First, use a point-and-click interface to select data. Then, clean and transform it for analysis in Analytics Workspace, Search, or Pivot!

Learn more about Table Views, or view and manage your Table Views with the Datasets listing page.

You can see that your system is connencted through universal forwarder and the count will increase while getting logs

Real time logs monitorings



```
host=ubuntuvm
```

Time range: Last 24 hours

✓ 8,116 events (9/14/25 12:00:00.000 PM to 9/15/25 12:50:25.000 PM)   No Event Sampling

< Hide Fields   All Fields

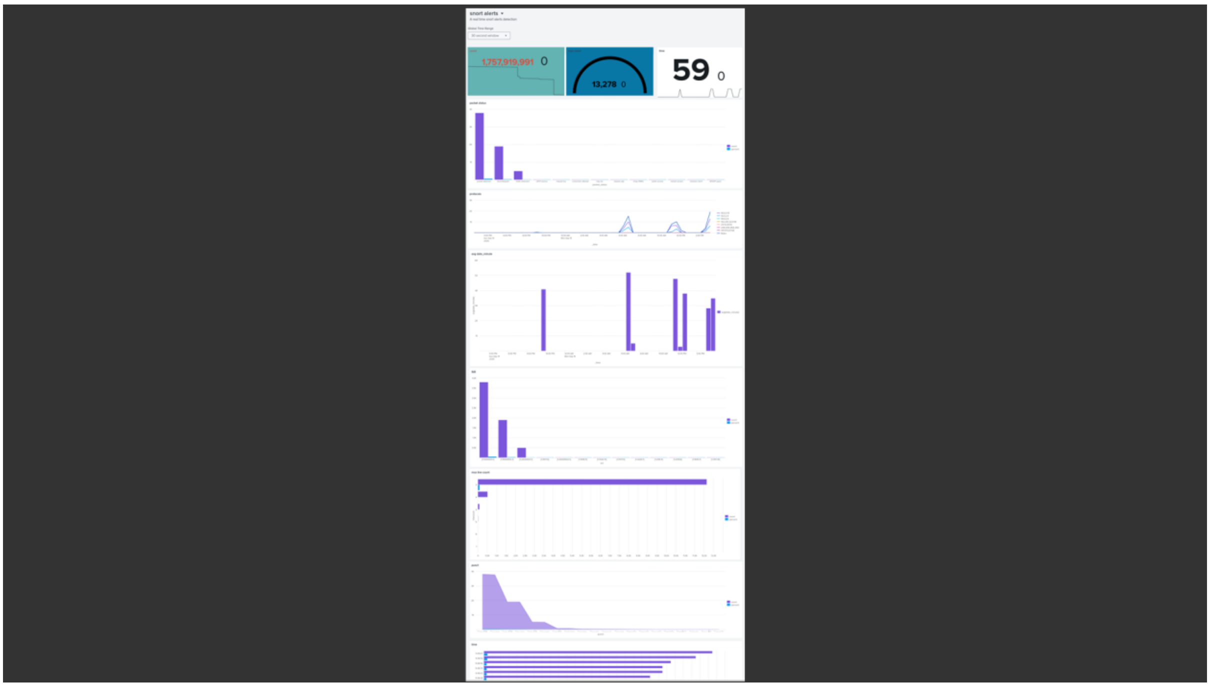
SELECTED FIELDS
a AttackerIP 7
a host 1
a sid 13
a source 2
a sourcetype 3

INTERESTING FIELDS
a date 2
# date_hour 5
# date_mday 2
# date_minute 38

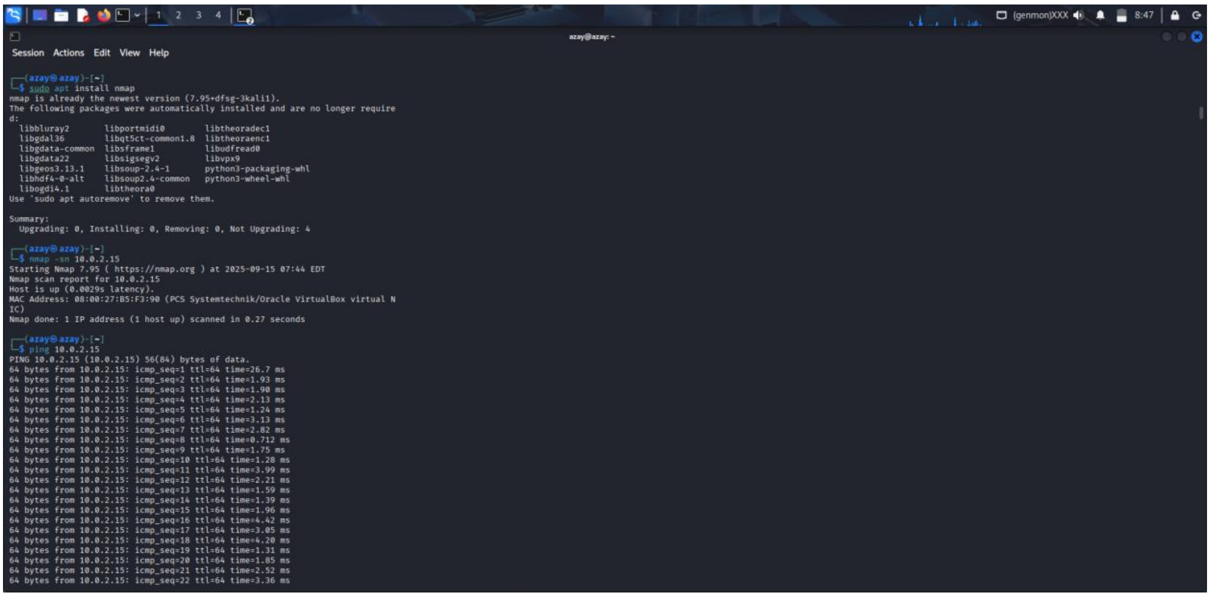
i	Time	Event
>	9/15/25 12:45:06.884 PM	09/15-12:45:06.884514 10.0.2.5:63474 -> 239.255.255.250:1900 UDP TTL:4 TOS:0x0 ID:21022 IpLen:20 DgmLen:165 Len: 137 host = ubuntuvm source = /var/log/snort/alert sourcetype = logs
>	9/15/25 12:45:06.884 PM	09/15-12:45:06.884514 [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 10.0.2.5:63474 -> 239.255.255.250:1900 [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] AttackerIP = 239.255.255.250 host = ubuntuvm sid = [1:1917:6] source = /var/log/snort/alert sourcetype = logs
>	9/15/25	09/15-12:45:03.866192 10.0.2.5:63474 -> 239.255.255.250:1900

Now we can create dashboards based on our requirements

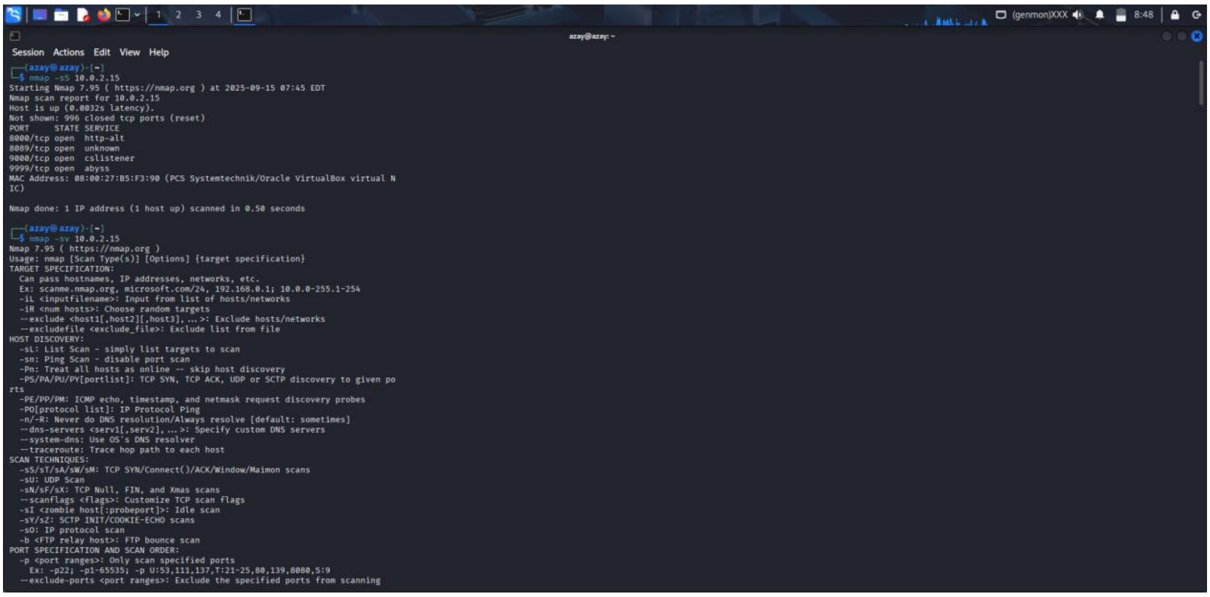
Dashboard



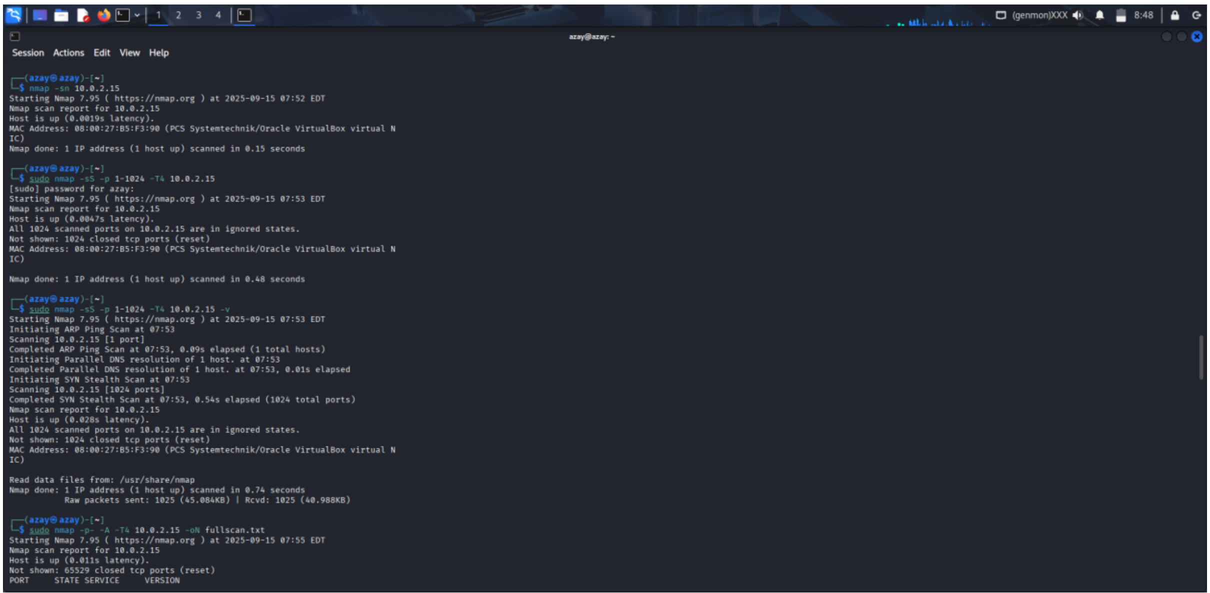
3. Linux attacks



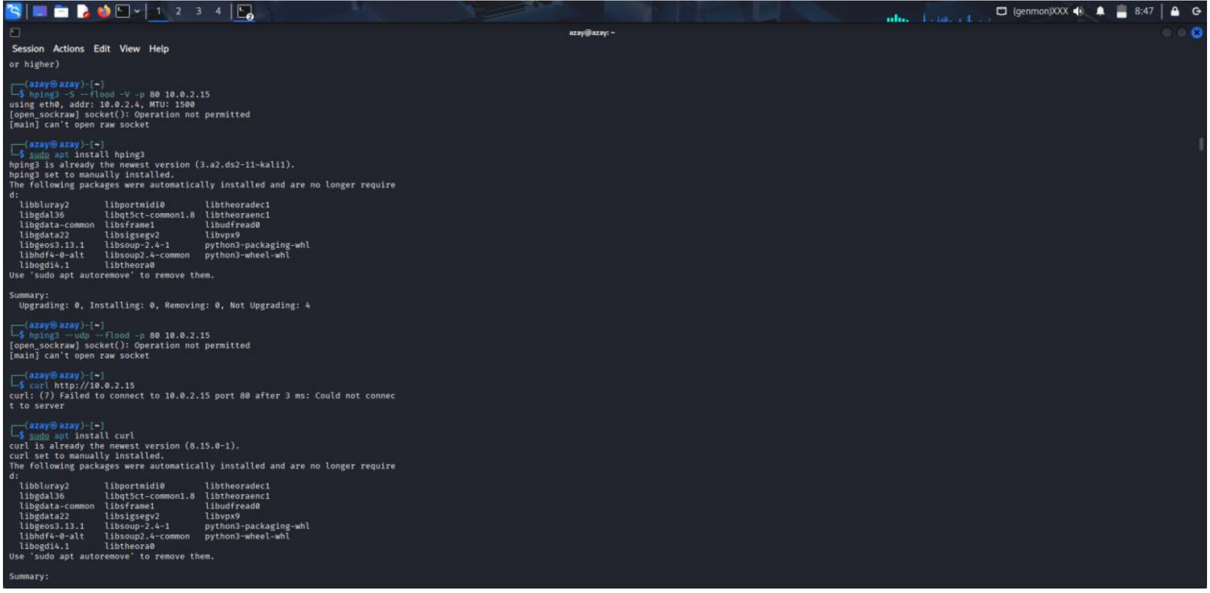
```
┌──(azay㉿azay)-[~]
└─$ sudo apt install nmap
nmap is already the newest version (7.95+dfsg-3kali1).
The following packages were automatically installed and are no longer require
d:
  libbluray2       libportmidi0         libtheoradec1
  libgdal36        libqt5ct-common1.8   libtheoraenc1
  libgdata-common  libsframe1           libudfread0
  libgdata22       libsigsegv2          libvpx9
  libgeos3.13.1    libsoup-2.4-1        python3-packaging-whl
  libhdf4-0-alt    libsoup2.4-common    python3-wheel-whl
  libogdi4.1       libtheora0
Use 'sudo apt autoremove' to remove them.

Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 4

┌──(azay㉿azay)-[~]
└─$ nmap -sn 10.0.2.15
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-15 07:44 EDT
Nmap scan report for 10.0.2.15
Host is up (0.0029s latency).
MAC Address: 08:00:27:B5:F3:90 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds

┌──(azay㉿azay)-[~]
└─$ ping 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=26.7 ms
64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=1.93 ms
64 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=1.90 ms
64 bytes from 10.0.2.15: icmp_seq=4 ttl=64 time=2.13 ms
64 bytes from 10.0.2.15: icmp_seq=5 ttl=64 time=1.24 ms
64 bytes from 10.0.2.15: icmp_seq=6 ttl=64 time=3.13 ms
64 bytes from 10.0.2.15: icmp_seq=7 ttl=64 time=2.82 ms
64 bytes from 10.0.2.15: icmp_seq=8 ttl=64 time=0.712 ms
64 bytes from 10.0.2.15: icmp_seq=9 ttl=64 time=1.75 ms
64 bytes from 10.0.2.15: icmp_seq=10 ttl=64 time=1.28 ms
64 bytes from 10.0.2.15: icmp_seq=11 ttl=64 time=3.99 ms
64 bytes from 10.0.2.15: icmp_seq=12 ttl=64 time=2.21 ms
64 bytes from 10.0.2.15: icmp_seq=13 ttl=64 time=1.59 ms
64 bytes from 10.0.2.15: icmp_seq=14 ttl=64 time=1.39 ms
64 bytes from 10.0.2.15: icmp_seq=15 ttl=64 time=1.96 ms
64 bytes from 10.0.2.15: icmp_seq=16 ttl=64 time=4.42 ms
64 bytes from 10.0.2.15: icmp_seq=17 ttl=64 time=3.05 ms
64 bytes from 10.0.2.15: icmp_seq=18 ttl=64 time=4.20 ms
64 bytes from 10.0.2.15: icmp_seq=19 ttl=64 time=1.31 ms
64 bytes from 10.0.2.15: icmp_seq=20 ttl=64 time=1.85 ms
64 bytes from 10.0.2.15: icmp_seq=21 ttl=64 time=2.52 ms
64 bytes from 10.0.2.15: icmp_seq=22 ttl=64 time=3.36 ms
```



```
┌──(azay㉿azay)-[~]
└─$ nmap -sS 10.0.2.15
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-15 07:45 EDT
Nmap scan report for 10.0.2.15
Host is up (0.0032s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
8000/tcp open  http-alt
8089/tcp open  unknown
9000/tcp open  cslistener
9999/tcp open  abyss
MAC Address: 08:00:27:B5:F3:90 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)

Nmap done: 1 IP address (1 host up) scanned in 0.50 seconds

┌──(azay㉿azay)-[~]
└─$ nmap -sv 10.0.2.15
Nmap 7.95 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN, TCP ACK, UDP or SCTP discovery to given po
rts
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
```



```
┌──(azay㉿azay)-[~]
└─$ nmap -sn 10.0.2.15
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-15 07:52 EDT
Nmap scan report for 10.0.2.15
Host is up (0.0019s latency).
MAC Address: 08:00:27:B5:F3:90 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds

┌──(azay㉿azay)-[~]
└─$ sudo nmap -sS -p 1-1024 -T4 10.0.2.15
[sudo] password for azay:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-15 07:53 EDT
Nmap scan report for 10.0.2.15
Host is up (0.0047s latency).
All 1024 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1024 closed tcp ports (reset)
MAC Address: 08:00:27:B5:F3:90 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)

Nmap done: 1 IP address (1 host up) scanned in 0.48 seconds

┌──(azay㉿azay)-[~]
└─$ sudo nmap -sS -p 1-1024 -T4 10.0.2.15 -v
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-15 07:53 EDT
Initiating ARP Ping Scan at 07:53
Scanning 10.0.2.15 [1 port]
Completed ARP Ping Scan at 07:53, 0.09s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 07:53
Completed Parallel DNS resolution of 1 host. at 07:53, 0.01s elapsed
Initiating SYN Stealth Scan at 07:53
Scanning 10.0.2.15 [1024 ports]
Completed SYN Stealth Scan at 07:53, 0.54s elapsed (1024 total ports)
Nmap scan report for 10.0.2.15
Host is up (0.028s latency).
All 1024 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1024 closed tcp ports (reset)
MAC Address: 08:00:27:B5:F3:90 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.74 seconds
           Raw packets sent: 1025 (45.084KB) | Rcvd: 1025 (40.988KB)

┌──(azay㉿azay)-[~]
└─$ sudo nmap -p- -A -T4 10.0.2.15 -oN fullscan.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-15 07:55 EDT
Nmap scan report for 10.0.2.15
Host is up (0.011s latency).
Not shown: 65529 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
```



```
or higher)

┌──(azay㉿azay)-[~]
└─$ hping3 -S --flood -V -p 80 10.0.2.15
using eth0, addr: 10.0.2.4, MTU: 1500
[open_sockraw] socket(): Operation not permitted
[main] can't open raw socket

┌──(azay㉿azay)-[~]
└─$ sudo apt install hping3
hping3 is already the newest version (3.a2.ds2-11-kali1).
hping3 set to manually installed.
The following packages were automatically installed and are no longer require
d:
  libbluray2       libportmidi0        libtheoradec1
  libgdal36        libqt5ct-common1.8  libtheoraenc1
  libgdata-common  libsframe1          libudfread0
  libgdata22       libsigsegv2         libvpx9
  libgeos3.13.1    libsoup-2.4-1       python3-packaging-whl
  libhdf4-0-alt    libsoup2.4-common   python3-wheel-whl
  libogdi4.1       libtheora0
Use 'sudo apt autoremove' to remove them.

Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 4

┌──(azay㉿azay)-[~]
└─$ hping3 --udp --flood -p 80 10.0.2.15
[open_sockraw] socket(): Operation not permitted
[main] can't open raw socket

┌──(azay㉿azay)-[~]
└─$ curl http://10.0.2.15
curl: (7) Failed to connect to 10.0.2.15 port 80 after 3 ms: Could not connec
t to server

┌──(azay㉿azay)-[~]
└─$ sudo apt install curl
curl is already the newest version (8.15.0-1).
curl set to manually installed.
The following packages were automatically installed and are no longer require
d:
  libbluray2       libportmidi0        libtheoradec1
  libgdal36        libqt5ct-common1.8  libtheoraenc1
  libgdata-common  libsframe1          libudfread0
  libgdata22       libsigsegv2         libvpx9
  libgeos3.13.1    libsoup-2.4-1       python3-packaging-whl
  libhdf4-0-alt    libsoup2.4-common   python3-wheel-whl
  libogdi4.1       libtheora0
Use 'sudo apt autoremove' to remove them.

Summary:
```