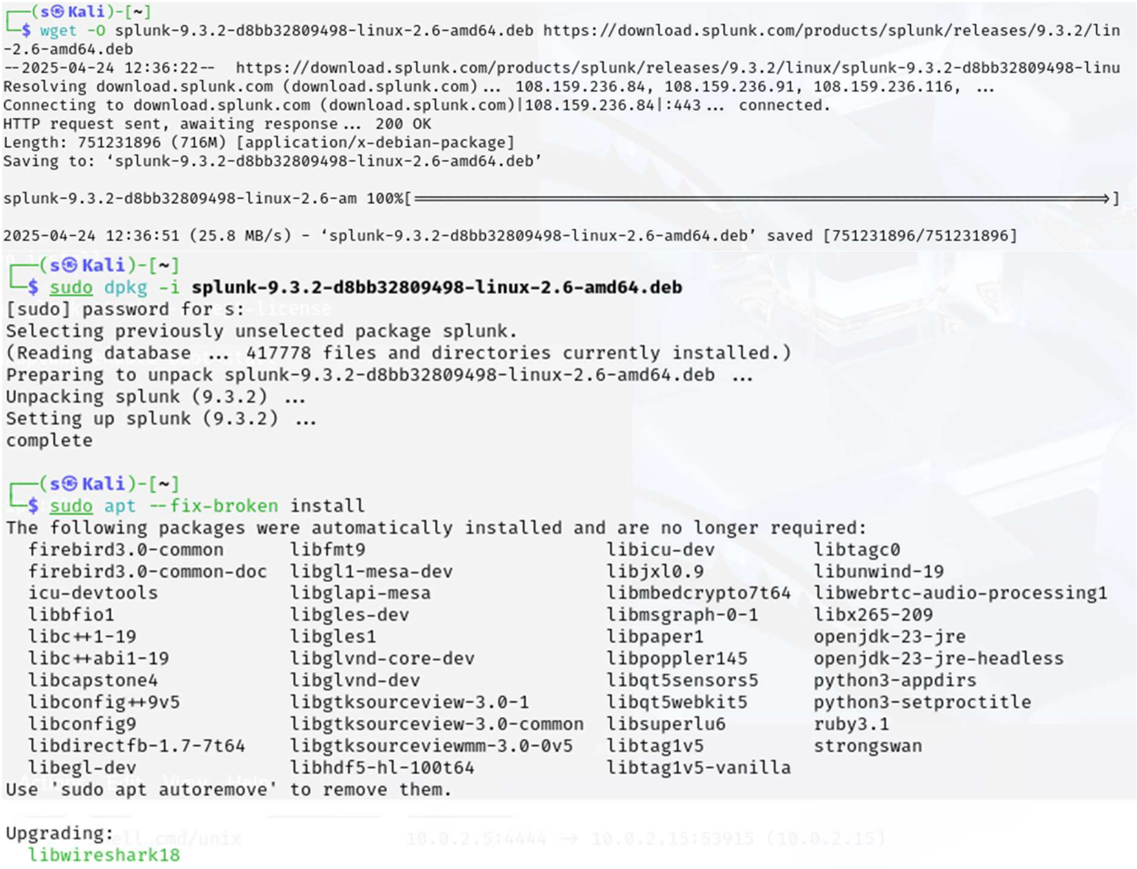
Phase Two:

In this phase, we will download splunk, which is a software for analyzing and monitoring data, in both devices, with victim machine having splunkforwarder to forward data to the attacker machine, which will work as a server here. Since we gained access to the victim device in phase one, this phase will focus on collecting data and analyzing it to our advantage.

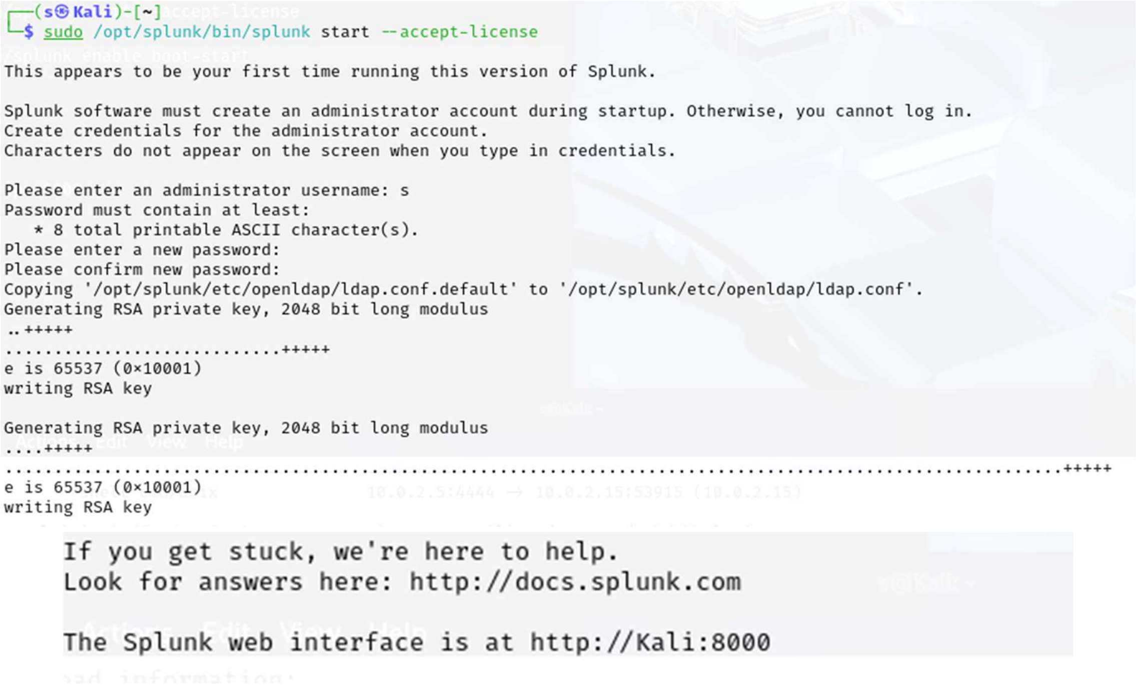
Setting up Attacker device with Splunk:

Figure 6: Downloading Splunk



```
┌──(s㉿Kali)-[~]
└─$ wget -O splunk-9.3.2-d8bb32809498-linux-2.6-amd64.deb https://download.splunk.com/products/splunk/releases/9.3.2/lin
-2.6-amd64.deb
--2025-04-24 12:36:22--  https://download.splunk.com/products/splunk/releases/9.3.2/linux/splunk-9.3.2-d8bb32809498-linu
Resolving download.splunk.com (download.splunk.com)... 108.159.236.84, 108.159.236.91, 108.159.236.116, ...
Connecting to download.splunk.com (download.splunk.com)|108.159.236.84|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 751231896 (716M) [application/x-debian-package]
Saving to: ‘splunk-9.3.2-d8bb32809498-linux-2.6-amd64.deb’

splunk-9.3.2-d8bb32809498-linux-2.6-am 100%[=================================================================>]

2025-04-24 12:36:51 (25.8 MB/s) - ‘splunk-9.3.2-d8bb32809498-linux-2.6-amd64.deb’ saved [751231896/751231896]
┌──(s㉿Kali)-[~]
└─$ sudo dpkg -i splunk-9.3.2-d8bb32809498-linux-2.6-amd64.deb
[sudo] password for s:
Selecting previously unselected package splunk.
(Reading database ... 417778 files and directories currently installed.)
Preparing to unpack splunk-9.3.2-d8bb32809498-linux-2.6-amd64.deb ...
Unpacking splunk (9.3.2) ...
Setting up splunk (9.3.2) ...
complete

┌──(s㉿Kali)-[~]
└─$ sudo apt --fix-broken install
The following packages were automatically installed and are no longer required:
  firebird3.0-common      libfmt9                        libicu-dev          libtagc0
  firebird3.0-common-doc  libgl1-mesa-dev                libjxl0.9           libunwind-19
  icu-devtools            libglapi-mesa                  libmbedcrypto7t64   libwebrtc-audio-processing1
  libbfio1                libgles-dev                    libmsgraph-0-1      libx265-209
  libc++1-19              libgles1                       libpaper1           openjdk-23-jre
  libc++abi1-19           libglvnd-core-dev              libpoppler145       openjdk-23-jre-headless
  libcapstone4            libglvnd-dev                   libqt5sensors5      python3-appdirs
  libconfig++9v5          libgtksourceview-3.0-1         libqt5webkit5       python3-setproctitle
  libconfig9              libgtksourceview-3.0-common    libsuperlu6         ruby3.1
  libdirectfb-1.7-7t64    libgtksourceviewmm-3.0-0v5     libtag1v5           strongswan
  libegl-dev              libhdf5-hl-100t64              libtag1v5-vanilla
Use 'sudo apt autoremove' to remove them.

Upgrading:
  libwireshark18
```

Figure 7: Accepting splunk and running it in port 8000

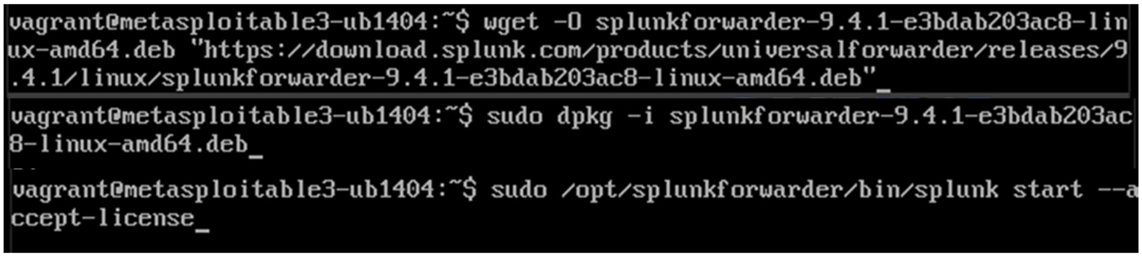


```
┌──(s㉿Kali)-[~]
└─$ sudo /opt/splunk/bin/splunk start --accept-license

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: s
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'.
Generating RSA private key, 2048 bit long modulus
..+++++
............................+++++
e is 65537 (0×10001)
writing RSA key

Generating RSA private key, 2048 bit long modulus
....+++++
.............................................................................................................+++++
e is 65537 (0×10001)
writing RSA key
```

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

The Splunk web interface is at http://Kali:8000
```

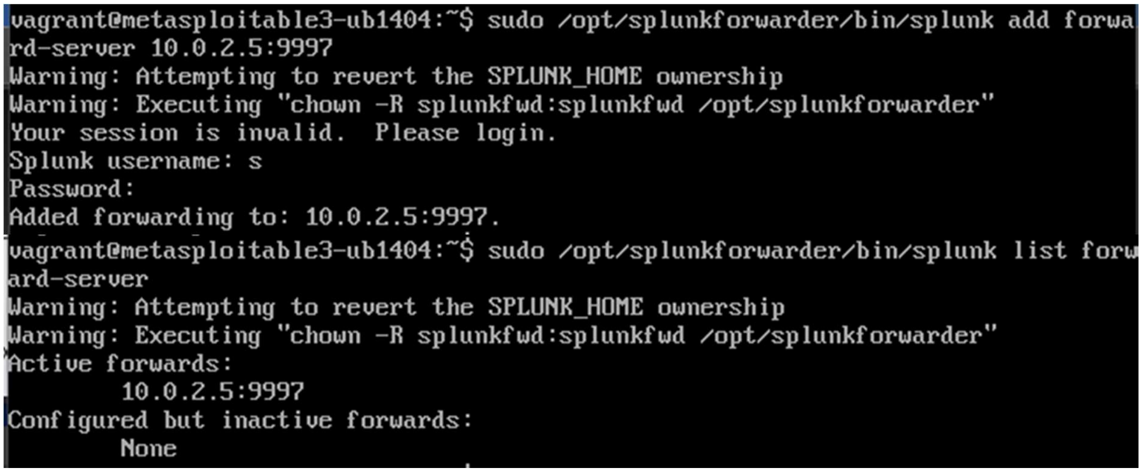
Setting up Victim device with Splunk/SplunkForwarder:

Figure 8: Getting splunkForwarder ready



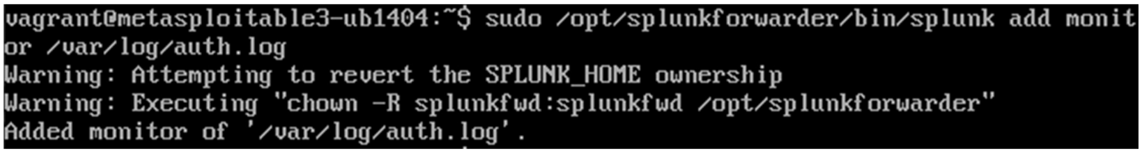
```
vagrant@metasploitable3-ub1404:~$ wget -O splunkforwarder-9.4.1-e3bdab203ac8-lin
ux-amd64.deb "https://download.splunk.com/products/universalforwarder/releases/9
.4.1/linux/splunkforwarder-9.4.1-e3bdab203ac8-linux-amd64.deb"_
vagrant@metasploitable3-ub1404:~$ sudo dpkg -i splunkforwarder-9.4.1-e3bdab203ac
8-linux-amd64.deb_
vagrant@metasploitable3-ub1404:~$ sudo /opt/splunkforwarder/bin/splunk start --a
ccept-license_
```

Figure 9: Making it forward the data to our server, and checking its reachability



```
vagrant@metasploitable3-ub1404:~$ sudo /opt/splunkforwarder/bin/splunk add forwa
rd-server 10.0.2.5:9997
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Your session is invalid.  Please login.
Splunk username: s
Password:
Added forwarding to: 10.0.2.5:9997.
vagrant@metasploitable3-ub1404:~$ sudo /opt/splunkforwarder/bin/splunk list forw
ard-server
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Active forwards:
        10.0.2.5:9997
Configured but inactive forwards:
        None
```

Figure 10: Making /var/log/auth.log as a monitored data



```
vagrant@metasploitable3-ub1404:~$ sudo /opt/splunkforwarder/bin/splunk add monit
or /var/log/auth.log
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Added monitor of '/var/log/auth.log'.
```

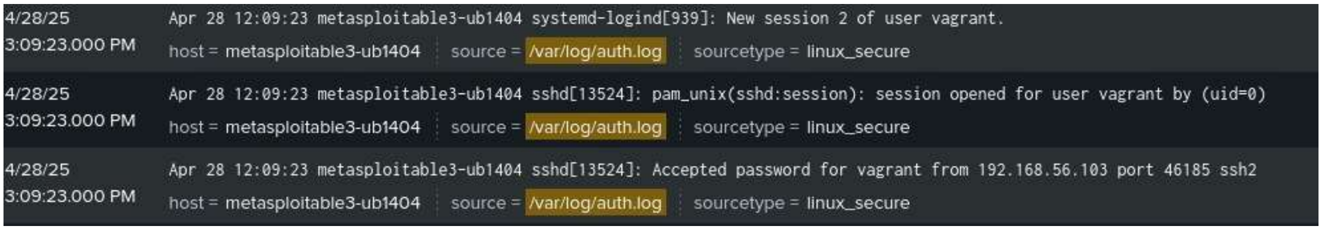
After getting Splunk and SplunkForwarder ready:

We decided to continue using SSH attack, and to show the visualization of its logs in the following part of this phase.

Attack logs and Visualization:

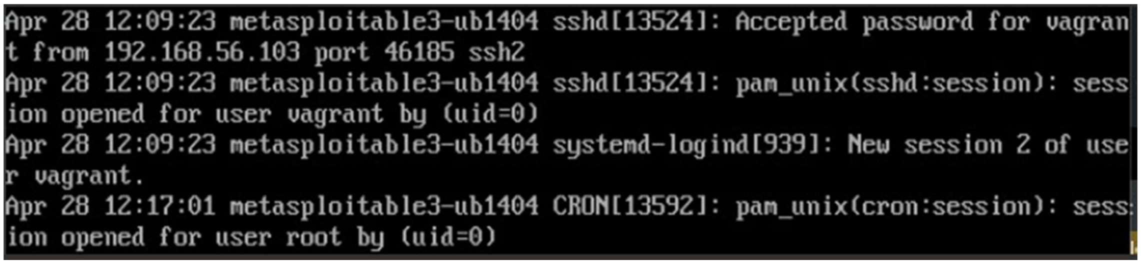
After setting up both devices, and choosing which vulnerability to continue with, we sent the log data from metasploitable 3 to kali machine, and we were able to capture the logs and visualize it as follows:

Figure 11: Events from attacker



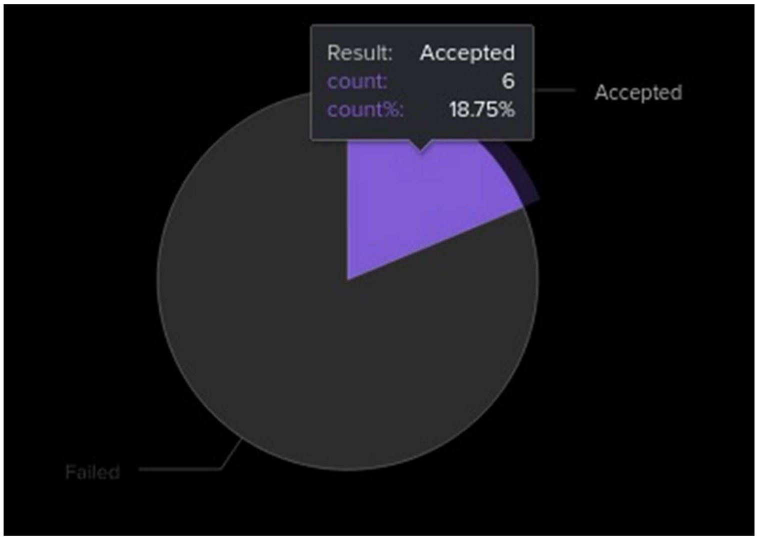
```
4/28/25          Apr 28 12:09:23 metasploitable3-ub1404 systemd-logind[939]: New session 2 of user vagrant.
3:09:23.000 PM   host = metasploitable3-ub1404   source = /var/log/auth.log   sourcetype = linux_secure
4/28/25          Apr 28 12:09:23 metasploitable3-ub1404 sshd[13524]: pam_unix(sshd:session): session opened for user vagrant by (uid=0)
3:09:23.000 PM   host = metasploitable3-ub1404   source = /var/log/auth.log   sourcetype = linux_secure
4/28/25          Apr 28 12:09:23 metasploitable3-ub1404 sshd[13524]: Accepted password for vagrant from 192.168.56.103 port 46185 ssh2
3:09:23.000 PM   host = metasploitable3-ub1404   source = /var/log/auth.log   sourcetype = linux_secure
```

Figure 12: Events from victim



```
Apr 28 12:09:23 metasploitable3-ub1404 sshd[13524]: Accepted password for vagran
t from 192.168.56.103 port 46185 ssh2
Apr 28 12:09:23 metasploitable3-ub1404 sshd[13524]: pam_unix(sshd:session): sess
ion opened for user vagrant by (uid=0)
Apr 28 12:09:23 metasploitable3-ub1404 systemd-logind[939]: New session 2 of use
r vagrant.
Apr 28 12:17:01 metasploitable3-ub1404 CRON[13592]: pam_unix(cron:session): sess
ion opened for user root by (uid=0)
```

Figure 13: Brute Force Graph



Explaining the Figures above:

Figure 11 and Figure 12 show logs in both devices, with Figure 11 being the attacker device. Meanwhile, Figure 12 shows it in the victim device.

Figure 13 is our attack visualization, as our SSH attack is based on Brute Force. The attack was able to crack the victim's password in six tries, which means that it only needed six passwords to try in order to exploit the vulnerability. Figure 13 uses pie graph to visualize the percentage of correct passwords to wrong ones, which resulted in 18.75%.