CYBER SECURITY LAB 03 – ANALYSIS OF DoS ATTACK CAPTURED IN SPLUNK

Denial of service Attack

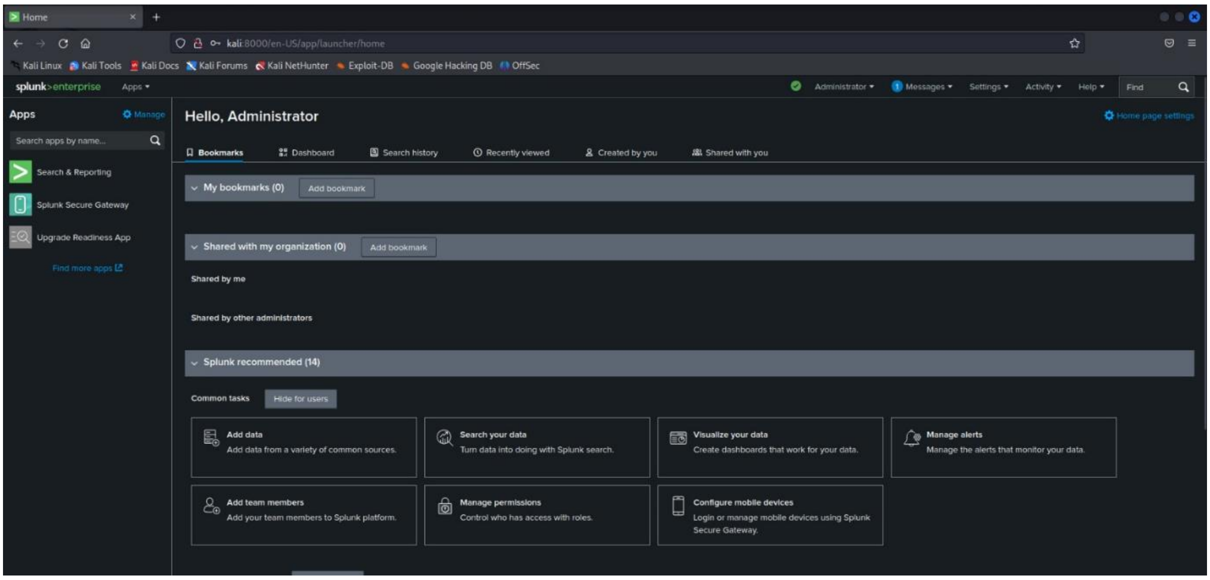
- DoS is cyber attack in which attacker makes a system unavailable to the intended user by interrupting its normal functioning.
- Excessive traffic overloads the network, causing delays and interruptions in legitimate communications.
- Bandwidth becomes saturated, preventing other devices from accessing the network.
- Critical server resources (CPU, RAM, storage) are consumed, leading to performance degradation or system crashes.

Simulating DoS attack

Attacker – Kali linux (172.17.128.130)

Target – Ubuntu (172.17.128.131)

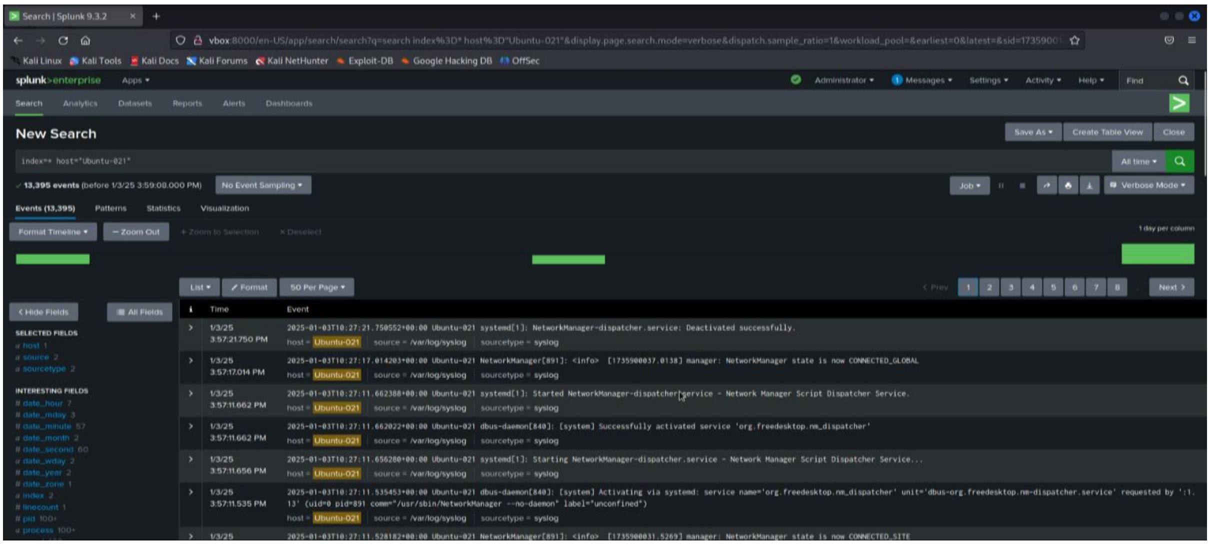
1. Start splunk enterprise in kali linux and access the admin interface.



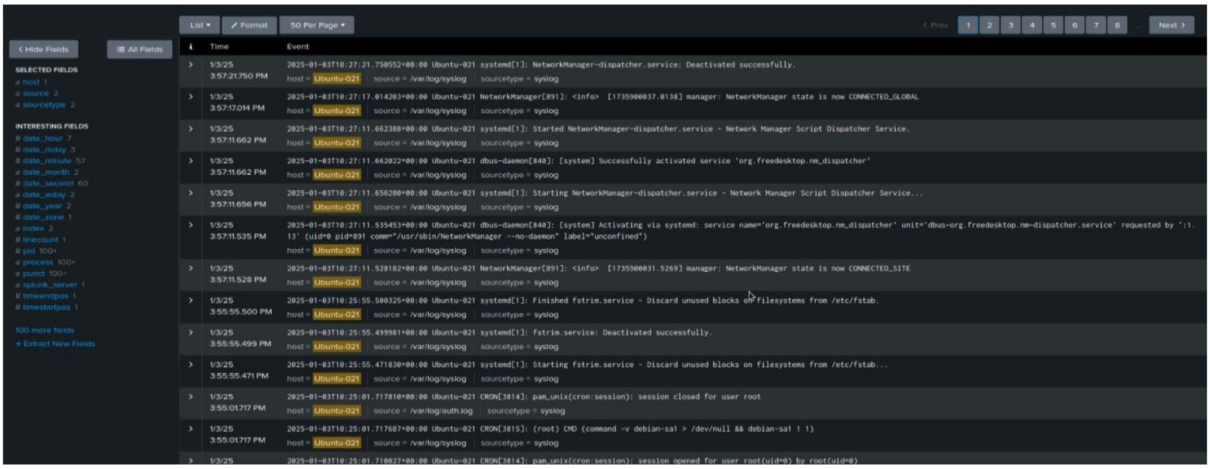
2. Start splunk forwarder in ubuntu.
3. In etter-cap scan for the hosts and add ubuntu as target 1.
4. Enable MITM -> ARP Poisoning.
5. Go to plugins -> Manage plugins -> DoS attack plugin.
6. Set victim's IP as ubuntu's IP and set any unused IP.
7. Now, the attack will happen.

Analysing splunk logs

1. Go to splunk interface.
2. Filter the logs with **index=* host=<host_name>**

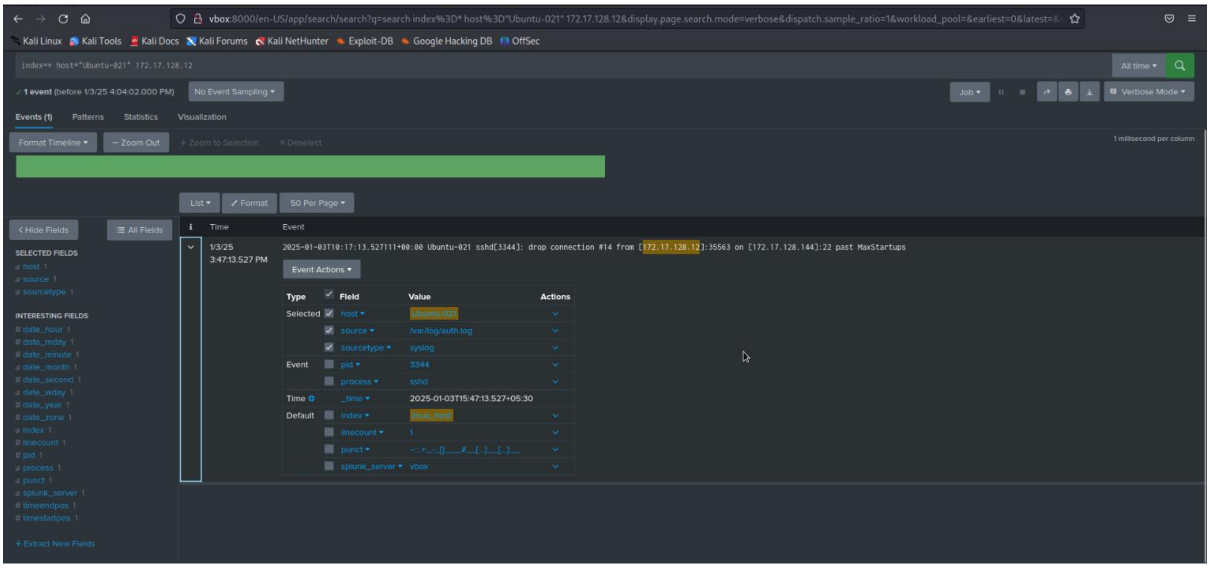


```
vbox:8000/en-US/app/search/search?q=search index%3D* host%3D"Ubuntu-021"&display.page.search.mode=verbose&dispatch.sample_ratio=1&workload_pool=&earliest=0&latest=&sid=1735900

New Search
index=* host="Ubuntu-021"
✓ 13,395 events (before 1/3/25 3:59:08.000 PM)    No Event Sampling
Events (13,395)   Patterns   Statistics   Visualization

Time                 Event
1/3/25 3:57:21.750 PM  2025-01-03T10:27:21.750552+00:00 Ubuntu-021 systemd[1]: NetworkManager-dispatcher.service: Deactivated successfully.
                       host = Ubuntu-021   source = /var/log/syslog   sourcetype = syslog
1/3/25 3:57:17.014 PM  2025-01-03T10:27:17.014203+00:00 Ubuntu-021 NetworkManager[891]: <info>  [1735900037.0138] manager: NetworkManager state is now CONNECTED_GLOBAL
                       host = Ubuntu-021   source = /var/log/syslog   sourcetype = syslog
1/3/25 3:57:11.662 PM  2025-01-03T10:27:11.662388+00:00 Ubuntu-021 systemd[1]: Started NetworkManager-dispatcher.service - Network Manager Script Dispatcher Service.
                       host = Ubuntu-021   source = /var/log/syslog   sourcetype = syslog
1/3/25 3:57:11.662 PM  2025-01-03T10:27:11.662022+00:00 Ubuntu-021 dbus-daemon[840]: [system] Successfully activated service 'org.freedesktop.nm_dispatcher'
                       host = Ubuntu-021   source = /var/log/syslog   sourcetype = syslog
1/3/25 3:57:11.656 PM  2025-01-03T10:27:11.656280+00:00 Ubuntu-021 systemd[1]: Starting NetworkManager-dispatcher.service - Network Manager Script Dispatcher Service...
                       host = Ubuntu-021   source = /var/log/syslog   sourcetype = syslog
1/3/25 3:57:11.535 PM  2025-01-03T10:27:11.535453+00:00 Ubuntu-021 dbus-daemon[840]: [system] Activating via systemd: service name='org.freedesktop.nm_dispatcher' unit='dbus-org.freedesktop.nm-dispatcher.service' requested by ':1.
                       13' (uid=0 pid=891 comm="/usr/sbin/NetworkManager --no-daemon" label="unconfined")
                       host = Ubuntu-021   source = /var/log/syslog   sourcetype = syslog
1/3/25                 2025-01-03T10:27:11.528182+00:00 Ubuntu-021 NetworkManager[891]: <info>  [1735900031.5269] manager: NetworkManager state is now CONNECTED_SITE
```



```
Time                 Event
1/3/25 3:57:21.750 PM  2025-01-03T10:27:21.750552+00:00 Ubuntu-021 systemd[1]: NetworkManager-dispatcher.service: Deactivated successfully.
                       host = Ubuntu-021   source = /var/log/syslog   sourcetype = syslog
1/3/25 3:57:17.014 PM  2025-01-03T10:27:17.014203+00:00 Ubuntu-021 NetworkManager[891]: <info>  [1735900037.0138] manager: NetworkManager state is now CONNECTED_GLOBAL
                       host = Ubuntu-021   source = /var/log/syslog   sourcetype = syslog
1/3/25 3:57:11.662 PM  2025-01-03T10:27:11.662388+00:00 Ubuntu-021 systemd[1]: Started NetworkManager-dispatcher.service - Network Manager Script Dispatcher Service.
                       host = Ubuntu-021   source = /var/log/syslog   sourcetype = syslog
1/3/25 3:57:11.662 PM  2025-01-03T10:27:11.662022+00:00 Ubuntu-021 dbus-daemon[840]: [system] Successfully activated service 'org.freedesktop.nm_dispatcher'
                       host = Ubuntu-021   source = /var/log/syslog   sourcetype = syslog
1/3/25 3:57:11.656 PM  2025-01-03T10:27:11.656280+00:00 Ubuntu-021 systemd[1]: Starting NetworkManager-dispatcher.service - Network Manager Script Dispatcher Service...
                       host = Ubuntu-021   source = /var/log/syslog   sourcetype = syslog
1/3/25 3:57:11.535 PM  2025-01-03T10:27:11.535453+00:00 Ubuntu-021 dbus-daemon[840]: [system] Activating via systemd: service name='org.freedesktop.nm_dispatcher' unit='dbus-org.freedesktop.nm-dispatcher.service' requested by ':1.
                       13' (uid=0 pid=891 comm="/usr/sbin/NetworkManager --no-daemon" label="unconfined")
                       host = Ubuntu-021   source = /var/log/syslog   sourcetype = syslog
1/3/25 3:57:11.528 PM  2025-01-03T10:27:11.528182+00:00 Ubuntu-021 NetworkManager[891]: <info>  [1735900031.5269] manager: NetworkManager state is now CONNECTED_SITE
                       host = Ubuntu-021   source = /var/log/syslog   sourcetype = syslog
1/3/25 3:55:55.500 PM  2025-01-03T10:25:55.500325+00:00 Ubuntu-021 systemd[1]: Finished fstrim.service - Discard unused blocks on filesystems from /etc/fstab.
                       host = Ubuntu-021   source = /var/log/syslog   sourcetype = syslog
1/3/25 3:55:55.499 PM  2025-01-03T10:25:55.499981+00:00 Ubuntu-021 systemd[1]: fstrim.service: Deactivated successfully.
                       host = Ubuntu-021   source = /var/log/syslog   sourcetype = syslog
1/3/25 3:55:55.471 PM  2025-01-03T10:25:55.471830+00:00 Ubuntu-021 systemd[1]: Starting fstrim.service - Discard unused blocks on filesystems from /etc/fstab...
                       host = Ubuntu-021   source = /var/log/syslog   sourcetype = syslog
1/3/25 3:55:01.717 PM  2025-01-03T10:25:01.717810+00:00 Ubuntu-021 CRON[3814]: pam_unix(cron:session): session closed for user root
                       host = Ubuntu-021   source = /var/log/auth.log   sourcetype = syslog
1/3/25 3:55:01.717 PM  2025-01-03T10:25:01.717687+00:00 Ubuntu-021 CRON[3815]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)
                       host = Ubuntu-021   source = /var/log/syslog   sourcetype = syslog
1/3/25                 2025-01-03T10:25:01.710827+00:00 Ubuntu-021 CRON[3814]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
```

3. Now, we can verify the DoS attack using the filter index=* host=”<host_name>” <Unused_IP>



```
vbox:8000/en-US/app/search/search?q=search index%3D* host%3D"Ubuntu-021" 172.17.128.12&display.page.search.mode=verbose&dispatch.sample_ratio=1&workload_pool=&earliest=0&latest=&

index=* host="Ubuntu-021" 172.17.128.12
✓ 1 event (before 1/3/25 4:04:02.000 PM)    No Event Sampling
Events (1)   Patterns   Statistics   Visualization

Time                 Event
1/3/25 3:47:13.527 PM  2025-01-03T10:17:13.527111+00:00 Ubuntu-021 sshd[3344]: drop connection #14 from [172.17.128.12]:35563 on [172.17.128.144]:22 past MaxStartups
```

Type		Field	Value
Selected	☑	host	Ubuntu-021
	☑	source	/var/log/auth.log
	☑	sourcetype	syslog
Event	☐	pid	3344
	☐	process	sshd
Time		_time	2025-01-03T15:47:13.527+05:30
Default	☐	index	linux_host
	☐	linecount	1
	☐	punct	--::+:_-_[]:___#__[..]:__[..]:__
	☐	splunk_server	vbox

The log shows an SSH connection dropped due to hitting the maximum limit. This might indicate multiple simultaneous SSH attempts, possibly from legitimate users or a brute-force attempt. Thus DoS attack is verified.