CONTINUOUS ATTACK DETECTION USING tmNIDS

1] First and foremost, it is essential to thoroughly locate and examine the tmNIDS

```
splunkufw@splunkufw:~$ ls
splunkforwarder-9.4.2-e9664af3d956-linux-amd64.deb  testmynids.org  wazuh-
splunkufw@splunkufw:~$
```

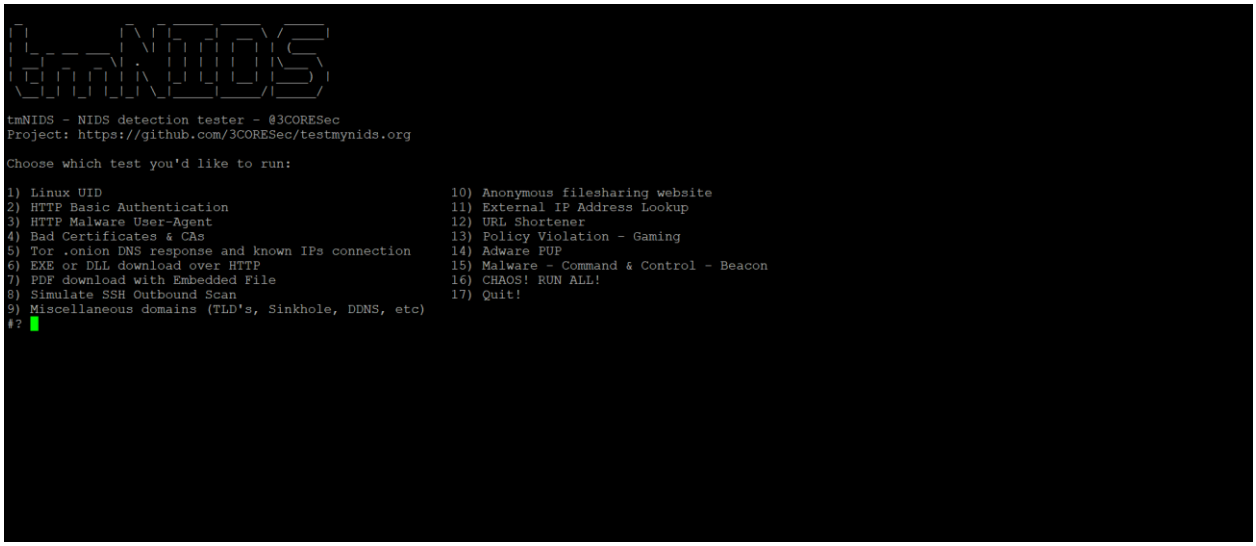
(Traffic Monitoring Network Intrusion Detection System) directory in order to ensure its proper configuration and availability. This preparatory step is necessary to effectively simulate and monitor continuous attack scenarios during practical exercises involving Splunk, thereby facilitating comprehensive analysis and accurate detection of persistent network threats.

```
splunkufw@splunkufw:~/testmynids.org$ ls
assets  helpers  pcaps  README.md  tmNIDS
splunkufw@splunkufw:~/testmynids.org$ ./tmNIDs
```

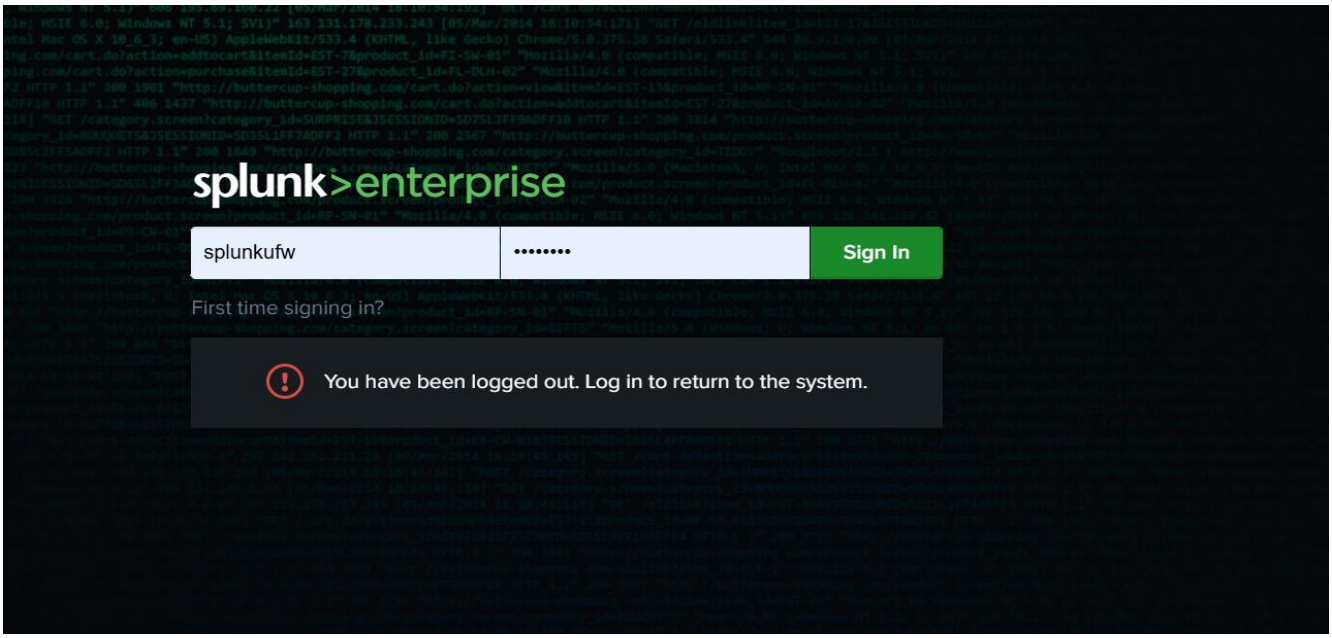
2] Subsequently, navigate to the tmNIDS (Traffic Monitoring Network Intrusion Detection System) environment or directory to initiate the configured attack simulation on the target system. This step is crucial for generating real-time network traffic anomalies, allowing for effective testing, detection, and correlation of malicious activities using Splunk or other security monitoring tools.

START THE ATTACKS

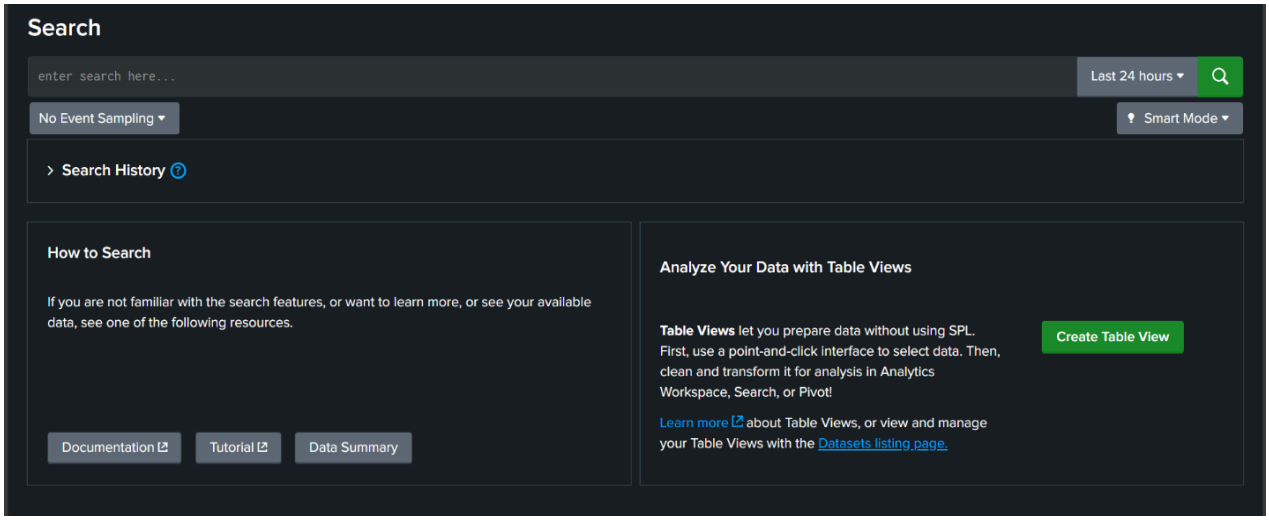
3] At this stage, it becomes necessary to determine the number and type of

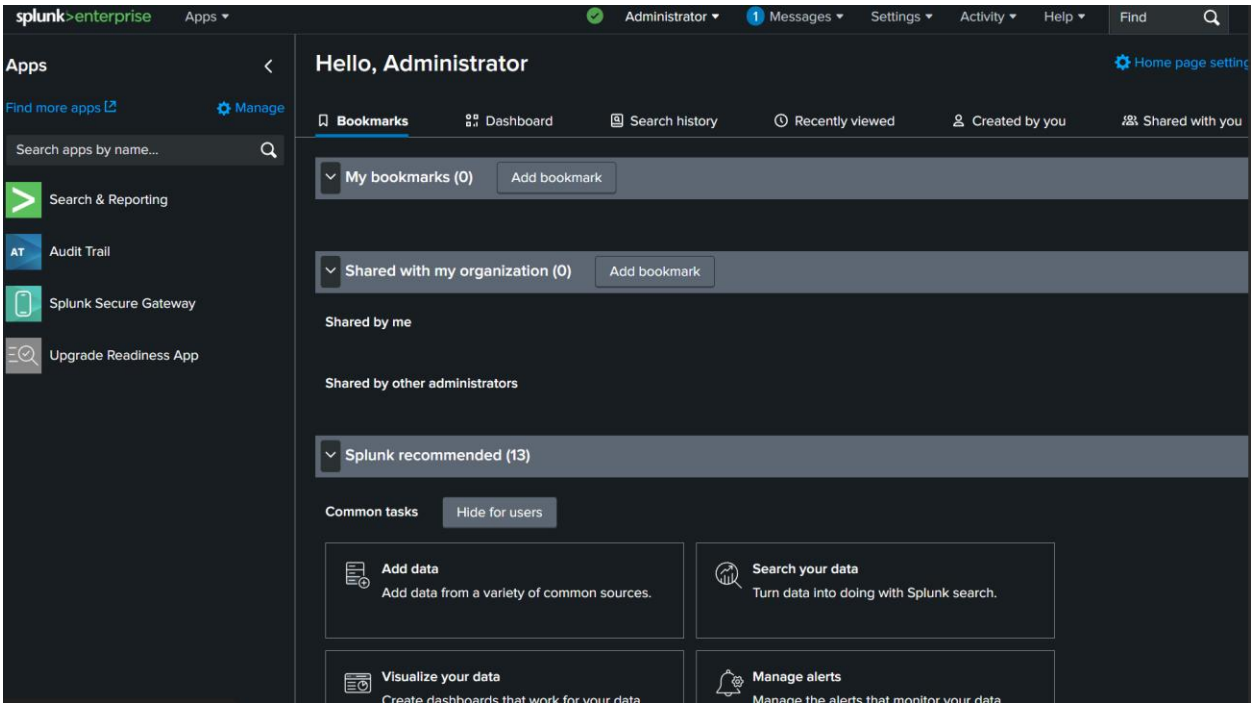


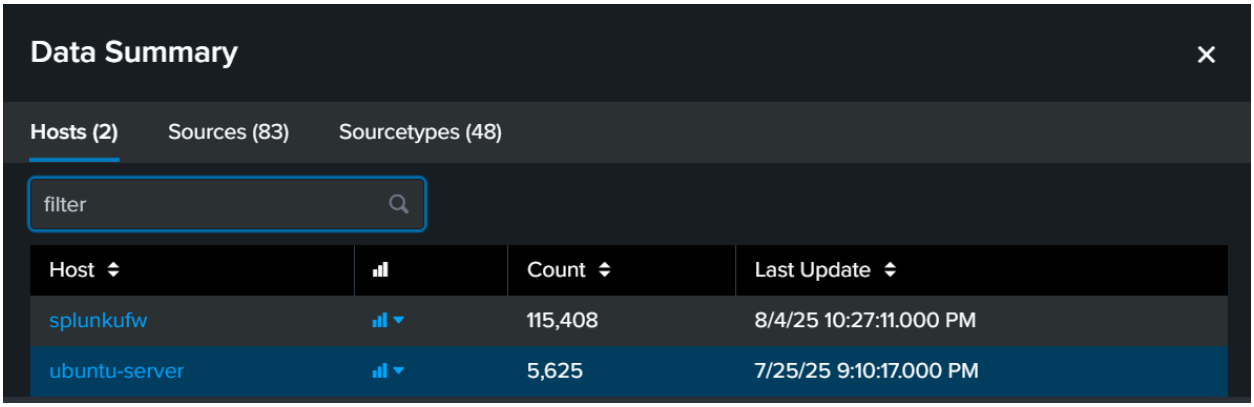
attacks to be executed as part of the simulation. A specific numerical identifier is typically selected to initiate a chosen attack pattern. However, for the purpose of comprehensive testing and evaluation, we will be executing all available attack types. In this context, the identifier corresponding to the execution of all attacks is ‘16’, which will be used to trigger a full-scale simulation of multiple threat scenarios across the network environment.



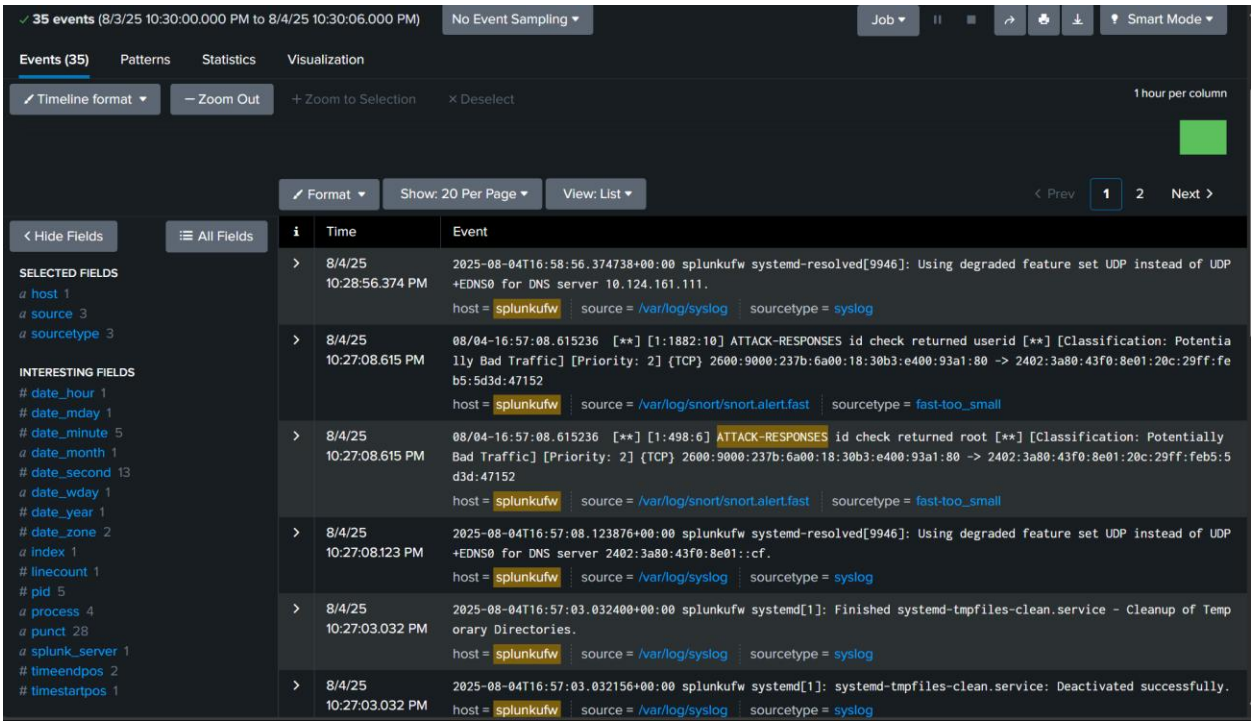
4] It is now appropriate to initiate the enterprise server in order to begin monitoring and analyzing the generated logs. This step is essential for observing real-time data flow, detecting anomalies, and verifying the effectiveness of the simulated attack scenarios within the network infrastructure.



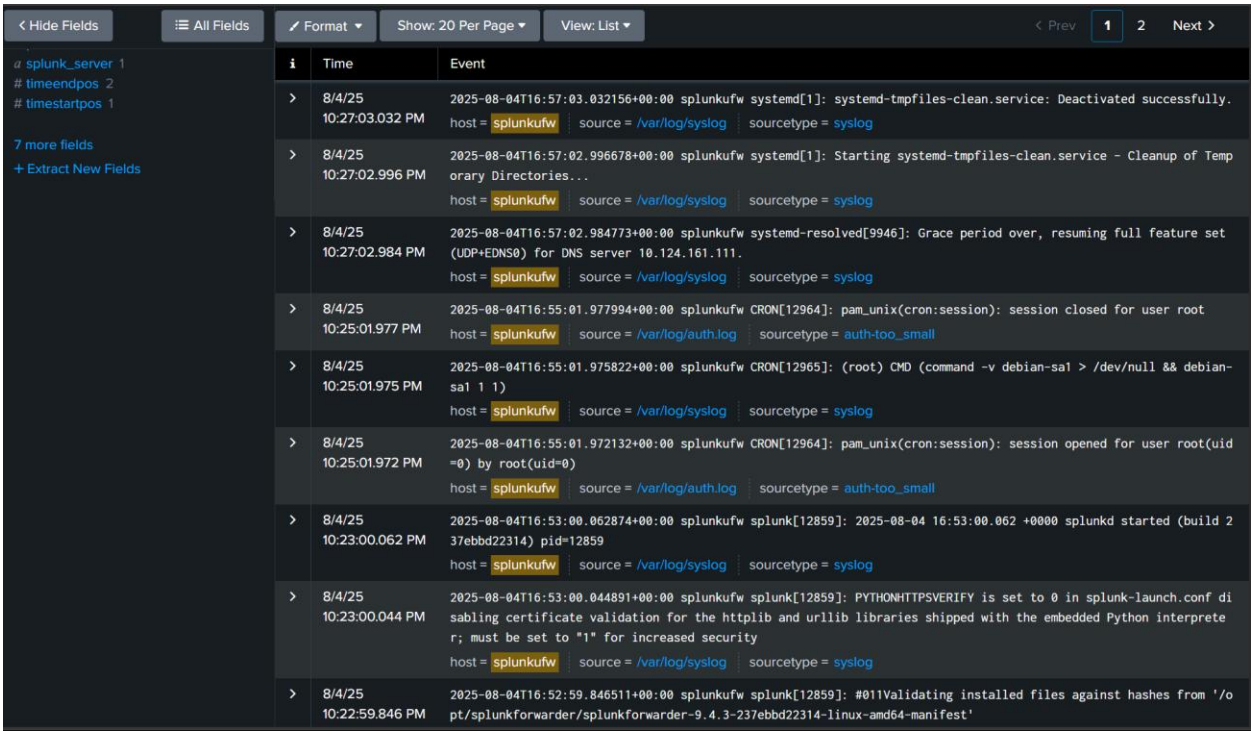




5] At this point, observe the current system time and review the real-time logs being generated. The continuous attack simulation is actively in progress, and the intrusion detection system is capturing live data, providing valuable insights into



the behavior, source, and pattern of the ongoing network threats.



AUTHOR : SHAIKH SALMAN

384shaikhsalman@gmail.com

linkedIn : 384shaikhsalman