

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

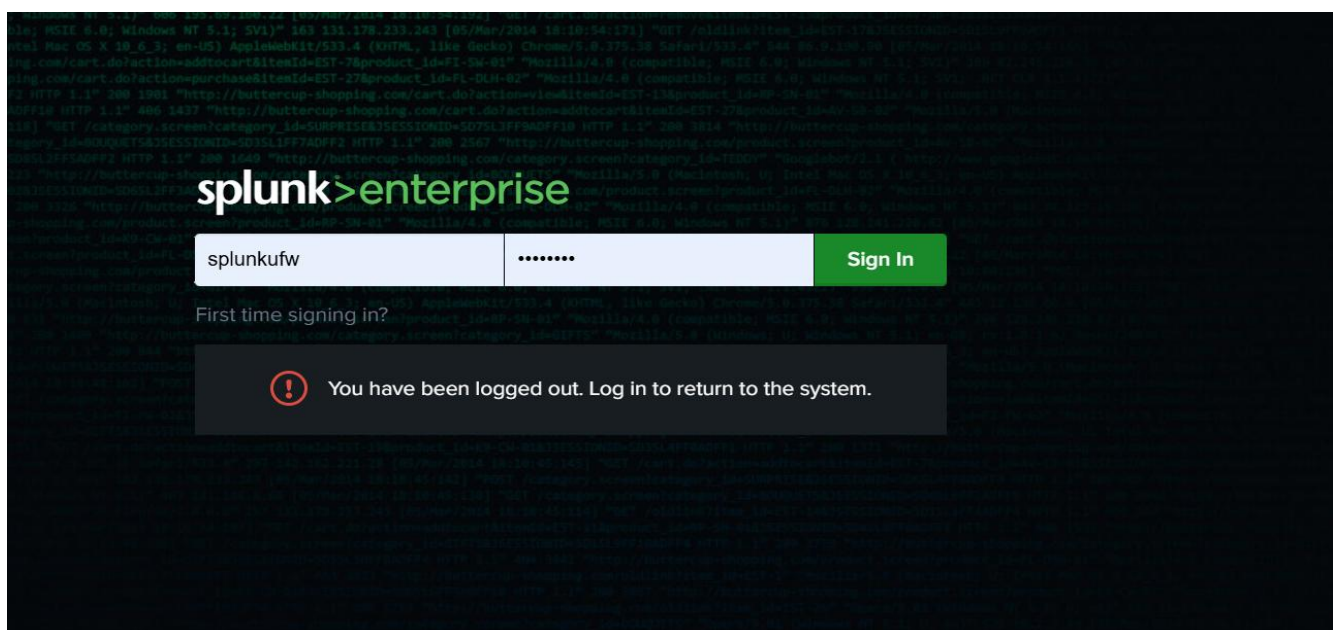
3] At this stage, it becomes necessary to determine the number and type of

```
tmNIDS - NIDS detection tester - @3CORESec
Project: https://github.com/3CORESec/testmynids.org

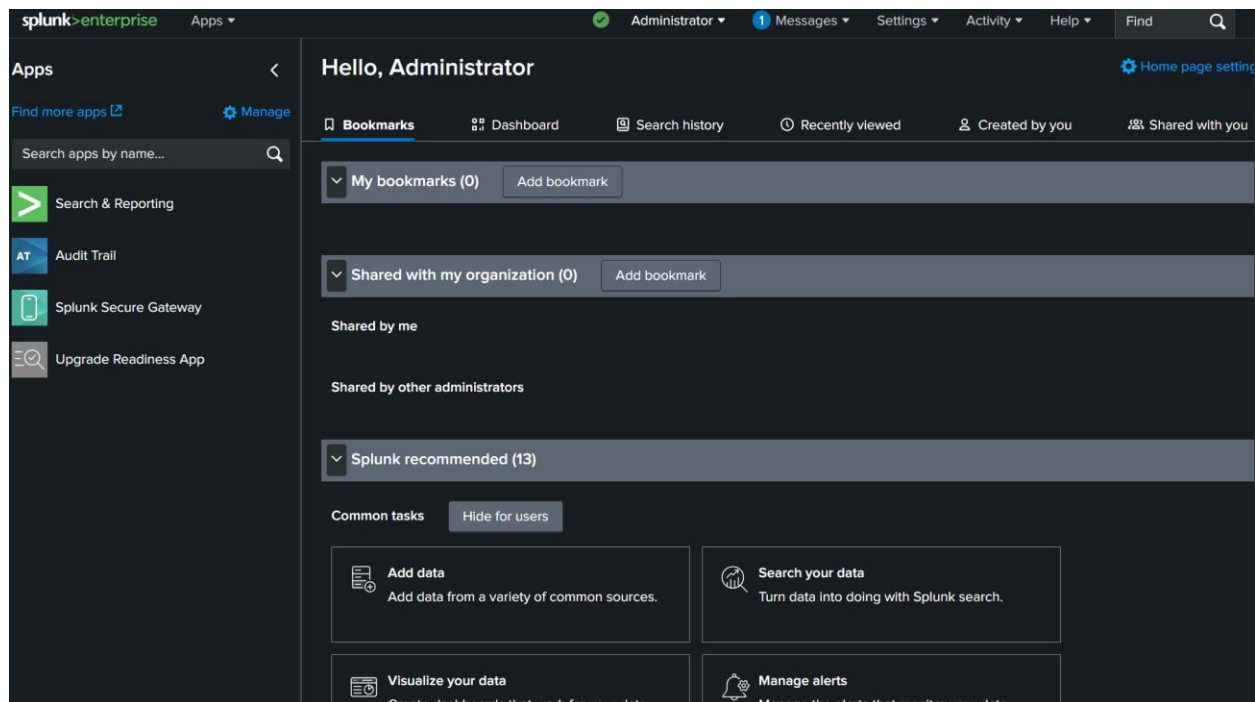
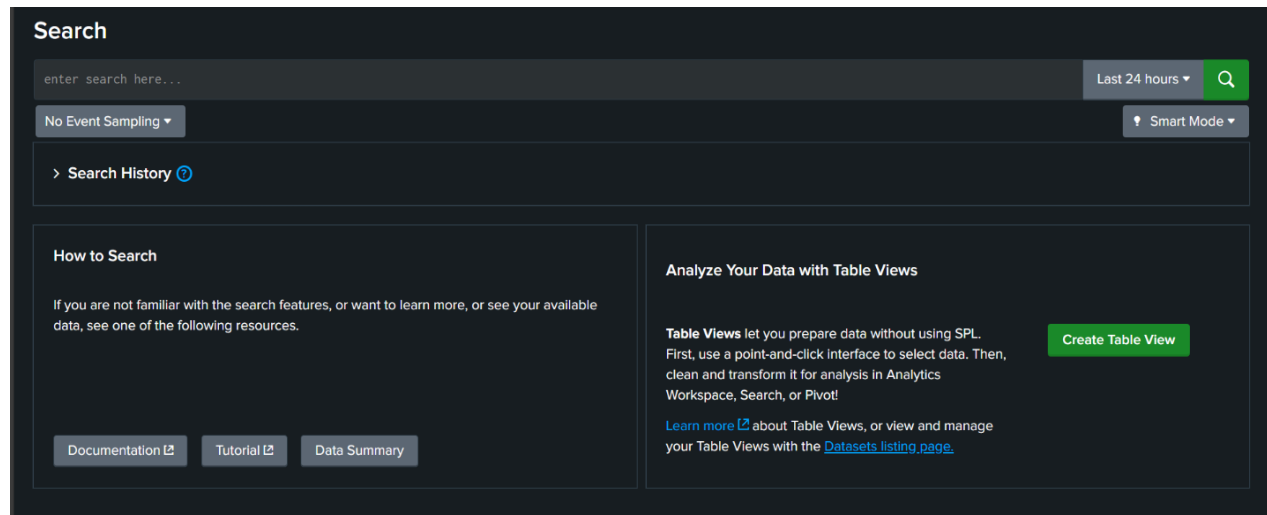
Choose which test you'd like to run:



1) Linux UID
2) HTTP Basic Authentication
3) HTTP Malware User-Agent
4) Bad Certificates & CAs
5) Tor .onion DNS response and known IPs connection
6) EXE or DLL download over HTTP
7) PDF download with Embedded File
8) Simulate SSH Outbound Scan
9) Miscellaneous domains (TLD's, Sinkhole, DDNS, etc)
10) Anonymous filesharing website
11) External IP Address Lookup
12) URL Shortener
13) Policy Violation - Gaming
14) Adware PUP
15) Malware - Command & Control - Beacon
16) CHAOS! RUN ALL!
17) Quit!
```

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.



Data Summary ×			
<div> <div>filter</div> <div>🔍</div> </div>			
Hosts (2)	Sources (83)	Sourcetypes (48)	
Host ↕		Count ↕	Last Update ↕
splunkufw		115,408	8/4/25 10:27:11.000 PM
ubuntu-server		5,625	7/25/25 9:10:17.000 PM

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

✓ 35 events (8/3/25 10:30:00.000 PM to 8/4/25 10:30:06.000 PM)

No Event Sampling ▾

Job ▾

⏏

🔍

📄

📁

🔔 Smart Mode ▾

Events (35)

Patterns

Statistics

Visualization

✓ Timeline format ▾

— Zoom Out

+ Zoom to Selection

× Deselect

1 hour per column

Format ▾

Show: 20 Per Page ▾

View: List ▾

< Prev

1

2

Next >

< Hide Fields

≡ All Fields

SELECTED FIELDS

a host 1

a source 3

a sourcetype 3

INTERESTING FIELDS

date_hour 1

date_mday 1

date_minute 5

a date_month 1

date_second 13

a date_wday 1

date_year 1

date_zone 2

a index 1

linecount 1

pid 5

a process 4

a punct 28

a splunk_server 1

timeendpos 2

timestartpos 1

i	Time	Event
>	8/4/25 10:28:56.374 PM	2025-08-04T16:58:56.374738+00:00 splunkufw systemd-resolved[9946]: Using degraded feature set UDP instead of UDP +EDNS0 for DNS server 10.124.161.111. host = splunkufw source = /var/log/syslog sourcetype = syslog
>	8/4/25 10:27:08.615 PM	08/04-16:57:08.615236 [**] [1:1882:10] ATTACK-RESPONSES id check returned userid [**] [Classification: Potentially Bad Traffic] [Priority: 2] [TCP] 2600:9000:237b:6a00:18:30b3:e400:93a1:80 -> 2402:3a80:43f0:8e01:20c:29ff:feb5:5d3d:47152 host = splunkufw source = /var/log/snort/snort.alert.fast sourcetype = fast-too_small
>	8/4/25 10:27:08.615 PM	08/04-16:57:08.615236 [**] [1:498:6] ATTACK-RESPONSES id check returned root [**] [Classification: Potentially Bad Traffic] [Priority: 2] [TCP] 2600:9000:237b:6a00:18:30b3:e400:93a1:80 -> 2402:3a80:43f0:8e01:20c:29ff:feb5:5d3d:47152 host = splunkufw source = /var/log/snort/snort.alert.fast sourcetype = fast-too_small
>	8/4/25 10:27:08.123 PM	2025-08-04T16:57:08.123876+00:00 splunkufw systemd-resolved[9946]: Using degraded feature set UDP instead of UDP +EDNS0 for DNS server 2402:3a80:43f0:8e01::cf. host = splunkufw source = /var/log/syslog sourcetype = syslog
>	8/4/25 10:27:03.032 PM	2025-08-04T16:57:03.032400+00:00 splunkufw systemd[1]: Finished systemd-tmpfiles-clean.service - Cleanup of Temporary Directories. host = splunkufw source = /var/log/syslog sourcetype = syslog
>	8/4/25 10:27:03.032 PM	2025-08-04T16:57:03.032156+00:00 splunkufw systemd[1]: systemd-tmpfiles-clean.service: Deactivated successfully. host = splunkufw source = /var/log/syslog sourcetype = syslog

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

< Hide Fields		All Fields	Format	Show: 20 Per Page	View: List	< Prev 1 2 Next >	
a splunk_server 1							
# timeendpos 2							
# timestartpos 1							
7 more fields							
+ Extract New Fields							
i	Time	Event					
>	8/4/25 10:27:03.032 PM	2025-08-04T16:57:03.032156+00:00 splunkufw systemd[1]: systemd-tmpfiles-clean.service: Deactivated successfully. host = splunkufw source = /var/log/syslog sourcetype = syslog					
>	8/4/25 10:27:02.996 PM	2025-08-04T16:57:02.996678+00:00 splunkufw systemd[1]: Starting systemd-tmpfiles-clean.service - Cleanup of Temporary Directories... host = splunkufw source = /var/log/syslog sourcetype = syslog					
>	8/4/25 10:27:02.984 PM	2025-08-04T16:57:02.984773+00:00 splunkufw systemd-resolved[9946]: Grace period over, resuming full feature set (UDP+EDNS0) for DNS server 10.124.161.111. host = splunkufw source = /var/log/syslog sourcetype = syslog					
>	8/4/25 10:25:01.977 PM	2025-08-04T16:55:01.977994+00:00 splunkufw CRON[12964]: pam_unix(cron:session): session closed for user root host = splunkufw source = /var/log/auth.log sourcetype = auth-too_small					
>	8/4/25 10:25:01.975 PM	2025-08-04T16:55:01.975822+00:00 splunkufw CRON[12965]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1) host = splunkufw source = /var/log/syslog sourcetype = syslog					
>	8/4/25 10:25:01.972 PM	2025-08-04T16:55:01.972132+00:00 splunkufw CRON[12964]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0) host = splunkufw source = /var/log/auth.log sourcetype = auth-too_small					
>	8/4/25 10:23:00.062 PM	2025-08-04T16:53:00.062874+00:00 splunkufw splunk[12859]: 2025-08-04 16:53:00.062 +0000 splunkd started (build 237ebbd22314) pid=12859 host = splunkufw source = /var/log/syslog sourcetype = syslog					
>	8/4/25 10:23:00.044 PM	2025-08-04T16:53:00.044891+00:00 splunkufw splunk[12859]: PYTHONHTTPSVERIFY is set to 0 in splunk-launch.conf disabling certificate validation for the httplib and urllib libraries shipped with the embedded Python interpreter; must be set to "1" for increased security host = splunkufw source = /var/log/syslog sourcetype = syslog					
>	8/4/25 10:22:59.846 PM	2025-08-04T16:52:59.846511+00:00 splunkufw splunk[12859]: #011Validating installed files against hashes from '/opt/splunkforwarder/splunkforwarder-9.4.3-237ebbd22314-linux-amd64-manifest' host = splunkufw source = /var/log/syslog sourcetype = syslog					

AUTHOR : SHAIKH SALMAN

384shaikhsalman@gmail.com

linkedIn : 384shaikhsalman