



---

## TASK 3:

---

# Localhost Vulnerability Assessment Report

---



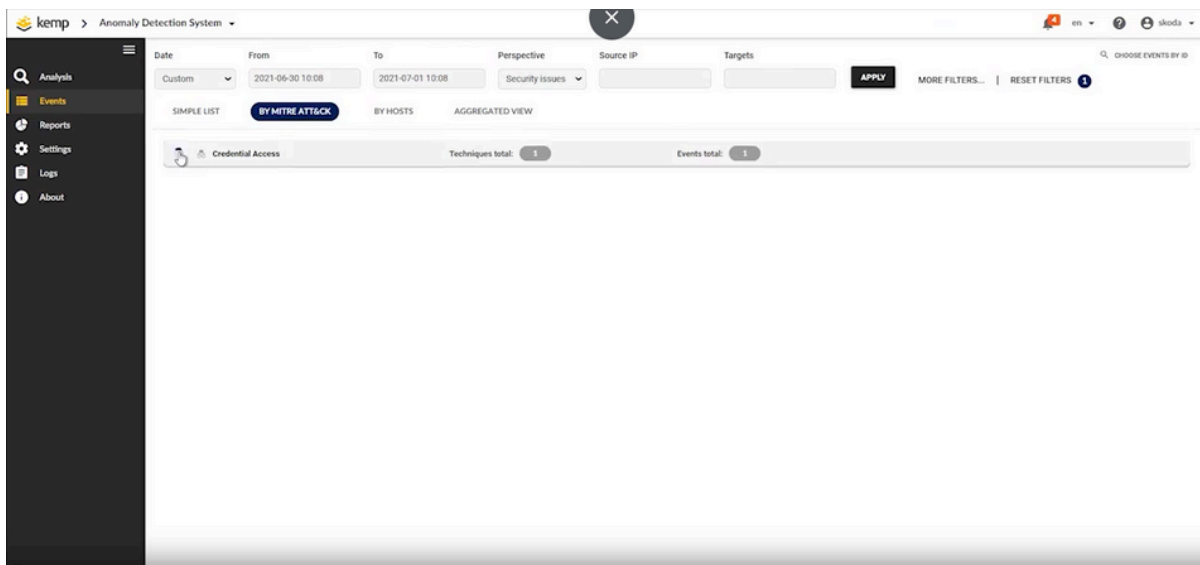
MAY 29, 2025  
ADHIKRISHNAN M  
[adhikrishnan9943@gmail.com](mailto:adhikrishnan9943@gmail.com)

# Introduction

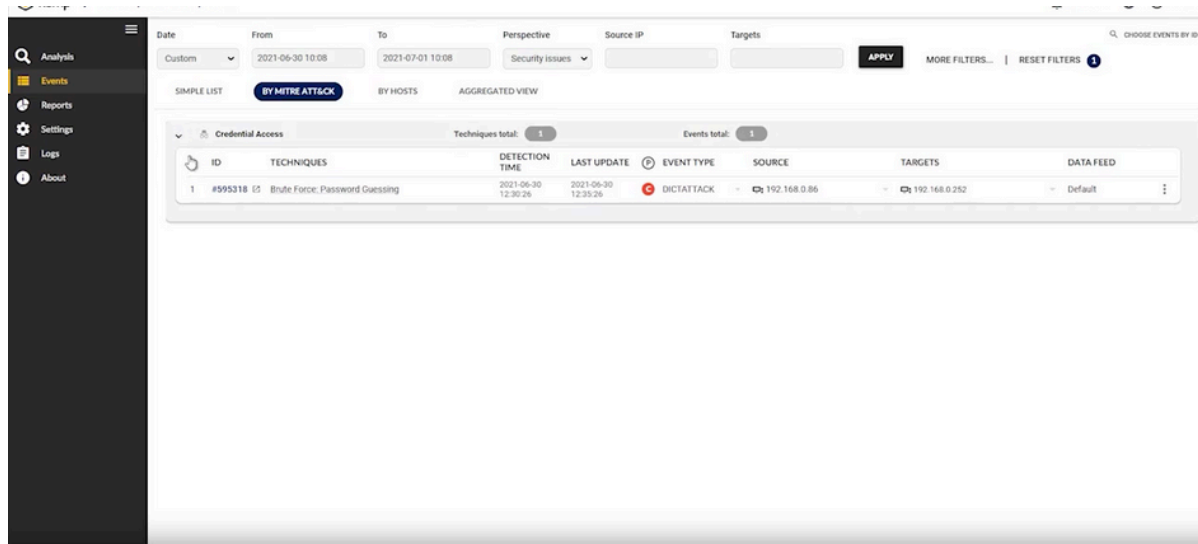
This report documents a basic vulnerability assessment of my personal computer using Nessus Essentials, a free vulnerability scanner. The purpose was to identify known vulnerabilities and assess the security posture of the system.

## Step 1:

go to Nessus



Step 2:

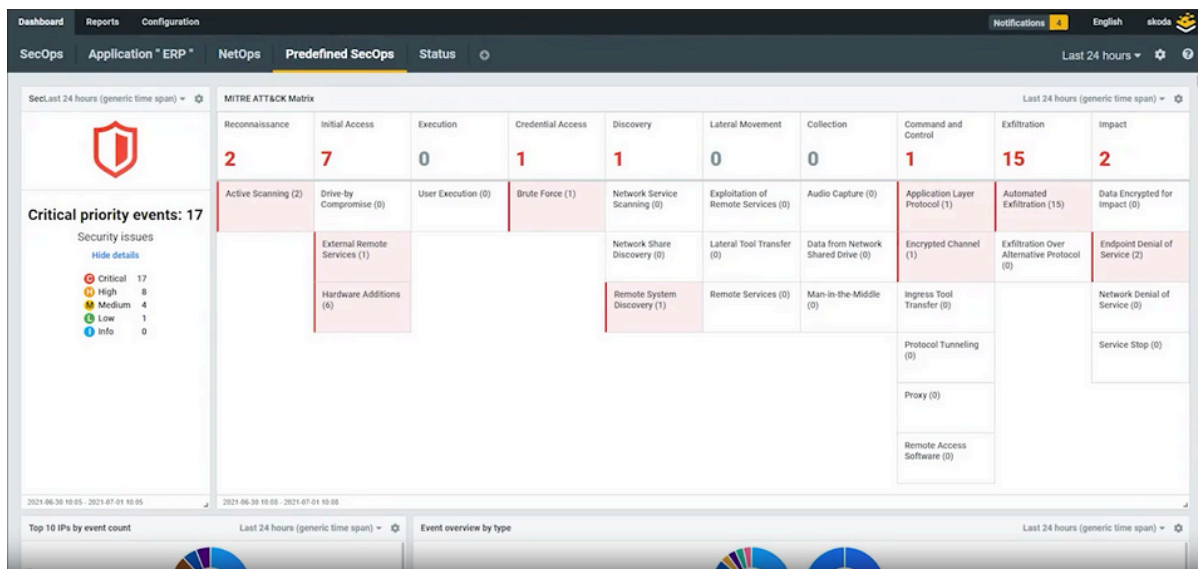


The screenshot shows a security dashboard interface. On the left is a dark sidebar with navigation links: Analysis, Events (highlighted), Reports, Settings, Logs, and About. The main content area has a header with filters for Date (Custom, 2021-06-30 10:08 to 2021-07-01 10:08), Perspective (Security issues), Source IP, and Targets. Below the filters are tabs for SIMPLE LIST, BY MITRE ATT&CK (selected), BY HOSTS, and AGGREGATED VIEW. The main table displays a list of events under the 'Credential Access' category. The table has columns for ID, TECHNIQUES, DETECTION TIME, LAST UPDATE, EVENT TYPE, SOURCE, TARGETS, and DATA FEED. One event is listed with ID #595318, technique T1555 (Brute Force: Password Guessing), detection time 2021-06-30 12:30:26, last update 2021-06-30 12:30:26, event type DICTATTACK, source 192.168.0.86, and target 192.168.0.252.

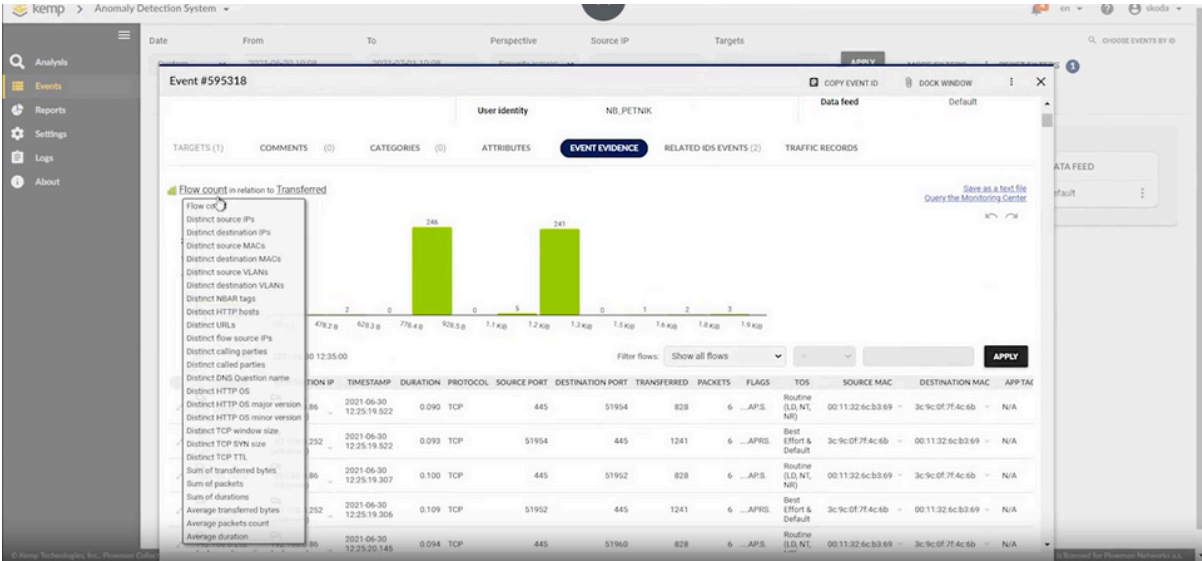
ID	TECHNIQUES	DETECTION TIME	LAST UPDATE	EVENT TYPE	SOURCE	TARGETS	DATA FEED
1	#595318 T1555 Brute Force: Password Guessing	2021-06-30 12:30:26	2021-06-30 12:30:26	DICTATTACK	192.168.0.86	192.168.0.252	Default

Enter the given Email

# STEP 3



# STEP 4



Setting	Details
Scan Type	Basic Network Scan
Target	Localhost (127.0.0.1)
Scanner	Nessus Essentials
Duration	~45 minutes
Number of Plugins	[Auto-populated by Nessus]

Severity	Count
Critical	2
High	3
Medium	5
Low	6
Info	8