# Experiment 7

**7.1 Aim:-** Study of malicious software using different tools: a) Keylogger attack using a keylogger tool. b) Simulate DOS attack using Hping or other tools c) Use the NESSUS/ISO Kali Linux tool to scan the network for vulnerabilities

**7.2Course Outcome:-**

Explain the need of network management security, illustrate the need for NAC and identify the function of an IDS and firewall for the system security.

**7.3 Lab Objective:-**

To familiarize students to different malware and attacks on networks and infer the use of firewalls and security protocols.

**7.4 Requirement:-**

Keylogger tool (e.g., Revealer Keylogger, KidLogger, Spyrix Free Keylogger)
Windows/Linux machine to execute the attack
Hping3 (available in Kali Linux)
Nessus (Tenable Nessus Scanner) – for network vulnerability assessment

**7.5 Theory:**

**Keylogger Tool**

**Introduction**

A keylogger (keystroke logger) is a type of surveillance software that records all keystrokes made on a computer or mobile device. It can be used for both ethical purposes (such as monitoring employee or child activity) and malicious activities (such as stealing passwords and sensitive data).

**Working Principle**

- Keyloggers operate by intercepting and recording keystrokes before they reach the operating system or application.
- They store captured data in log files, which may be sent to an attacker via email or a remote server.
- Some advanced keyloggers can also capture clipboard data, take screenshots, and monitor applications.

**Examples of Keylogger Tools**

- Revealer Keylogger – Monitors and records keystrokes in real time.
- KidLogger – Logs keystrokes and provides parental monitoring features.
- Spyrix Free Keylogger – Captures keystrokes and allows remote monitoring.

**Execution Environment**

- Windows/Linux machine – Keyloggers can be installed on either operating system, depending on the tool used.

**Hping3 (Available in Kali Linux)**

**Introduction**

Hping3 is a command-line network security tool used for packet crafting, network testing, and penetration testing. It is commonly used to simulate attacks like Denial-of-Service (DoS), network mapping, and firewall testing.

**Working Principle**

- Hping3 can send custom TCP, UDP, and ICMP packets to analyze network responses.
- It helps in testing firewall rules, detecting open ports, and performing DoS attacks by flooding a target with packets.
- It can operate in raw mode, allowing security researchers to modify packet headers.

**Common Uses of Hping3**

- Simulating DoS Attacks – By sending a high volume of packets, Hping3 can flood a system, making it unresponsive.
- Firewall Testing – Hping3 can check how firewalls handle different types of network traffic.
- Network Scanning – It can detect open ports and active hosts.

**Nessus (Tenable Nessus Scanner) – For Network Vulnerability Assessment**

**Introduction**

Nessus is a widely used vulnerability scanner developed by Tenable Inc. It is used to detect security vulnerabilities, misconfigurations, and compliance issues in a networked environment.

**Working Principle**

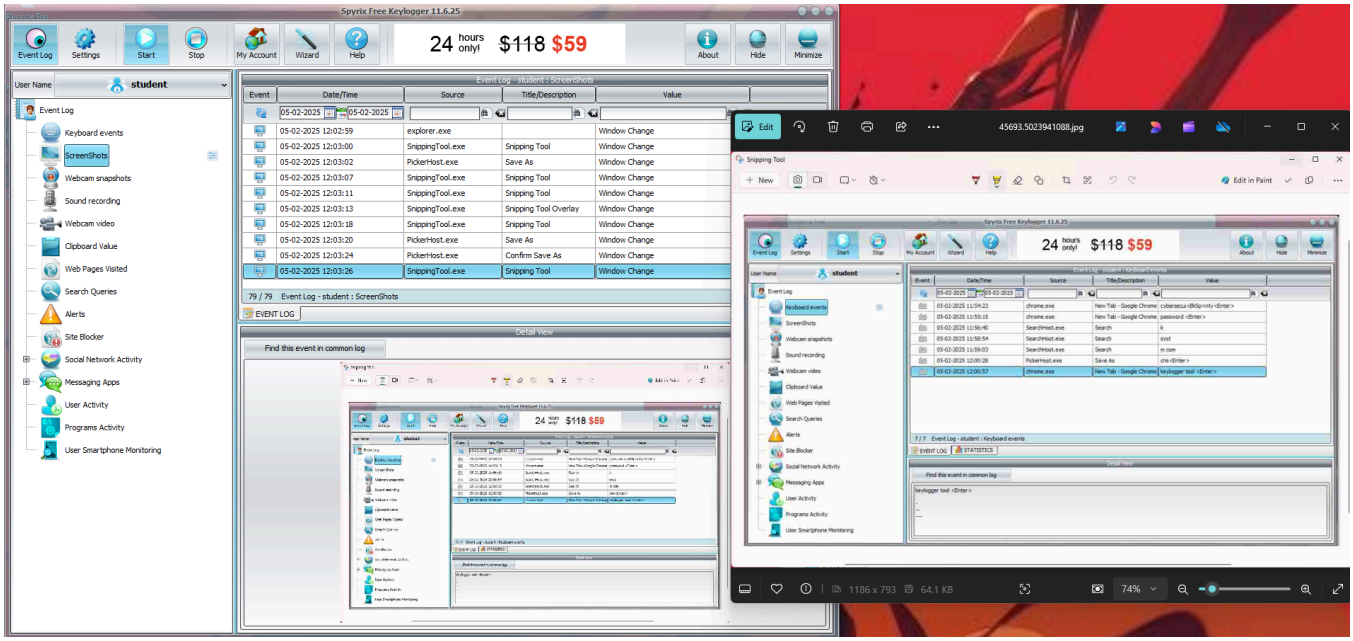
- Nessus scans a network and identifies vulnerabilities in operating systems, applications, and network services.
- It checks for outdated software, misconfigurations, and potential security exploits.
- The tool generates a detailed vulnerability report, ranking issues by severity level.

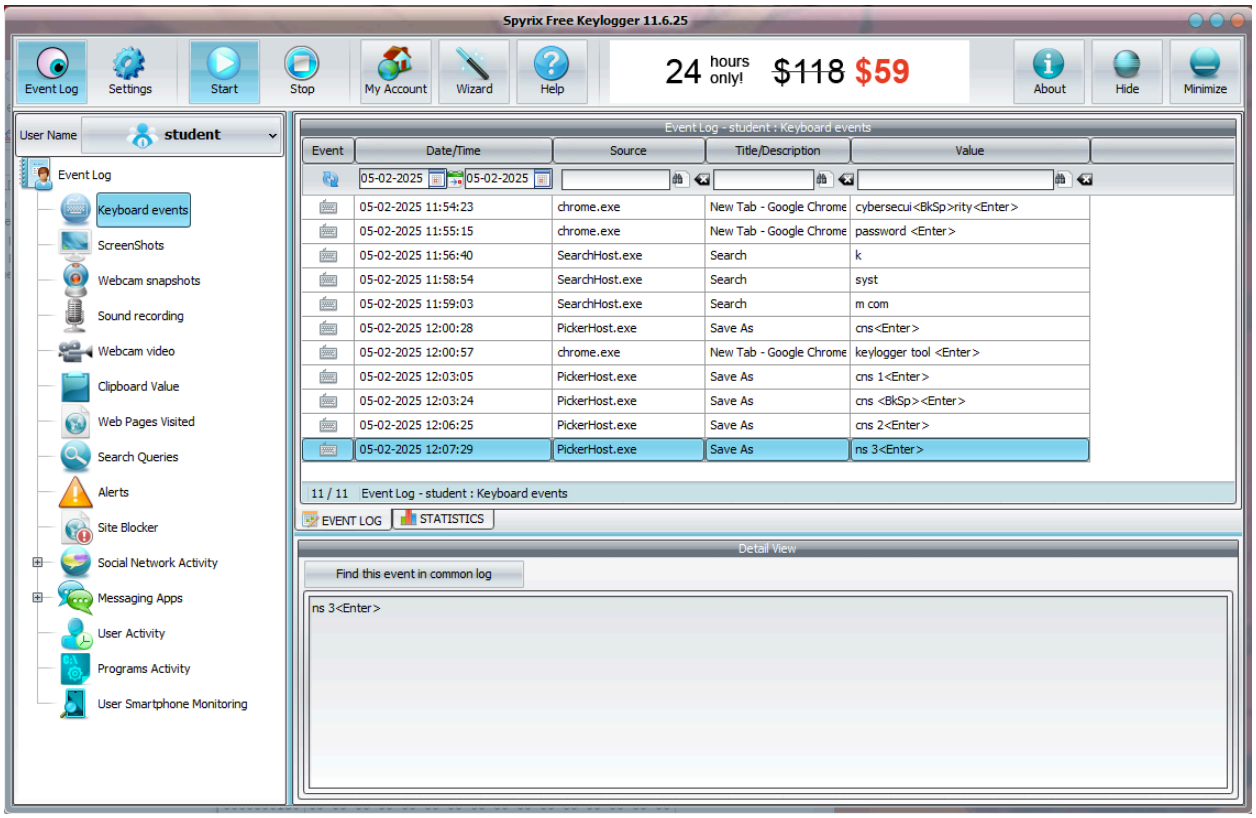
**Common Uses of Nessus**

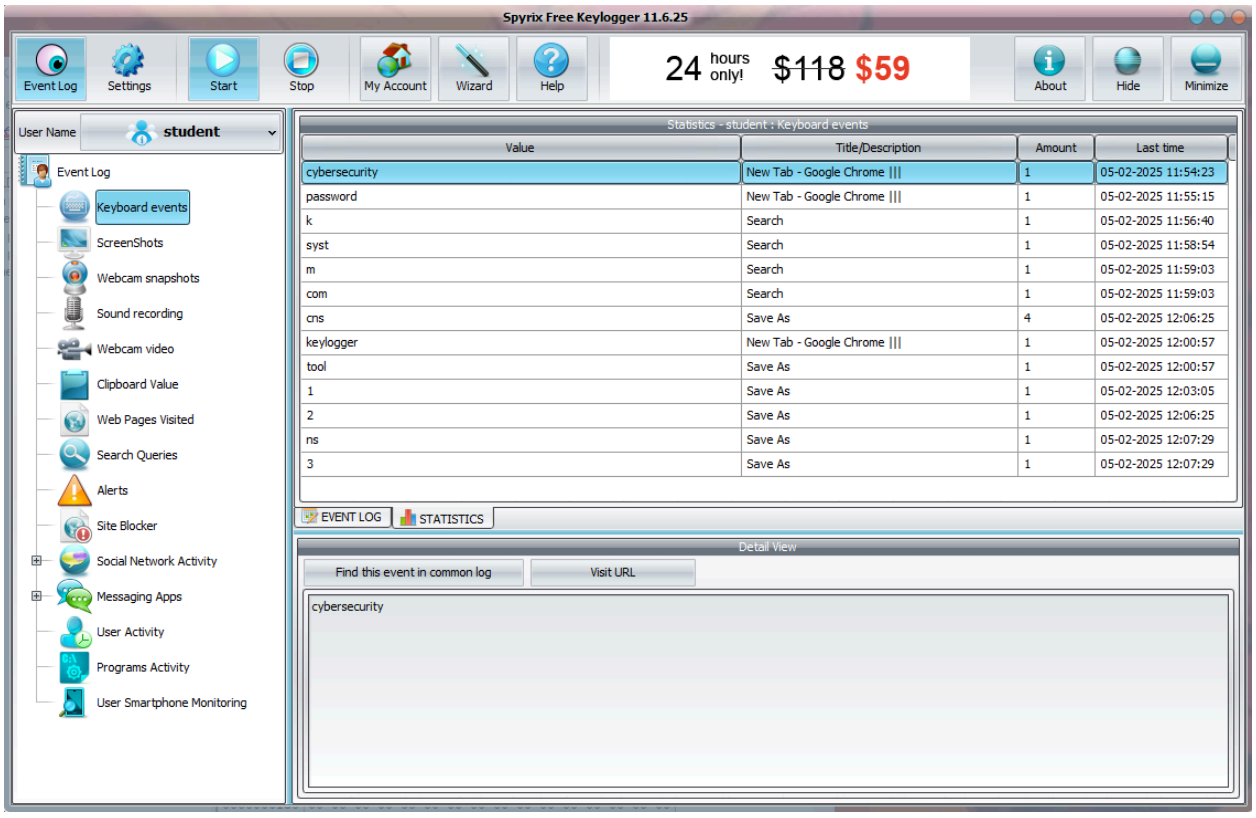
- Network Security Audits – Identifies weaknesses in system configurations and services.
- Compliance Scanning – Helps organizations meet security standards such as ISO 27001, PCI-DSS, and HIPAA.
- Penetration Testing – Used by ethical hackers to find and patch vulnerabilities before attackers exploit them.

**7.7 Result/Output :-**

a) **Keylogger attack:**




Spyrix Free Keylogger 11.6.25
Event Log
Settings
Start
Stop
My Account
Wizard
Help
24 hours only!
$118 $59
About
Hide
Minimize
User Name
student
Event Log
Keyboard events
ScreenShots
Webcam snapshots
Sound recording
Webcam video
Clipboard Value
Web Pages Visited
Search Queries
Alerts
Site Blocker
Social Network Activity
Messaging Apps
User Activity
Programs Activity
User Smartphone Monitoring
Event Log - student : Keyboard events
Event
Date/Time
Source
Title/Description
Value
05-02-2025
05-02-2025
05-02-2025 11:54:23 chrome.exe New Tab - Google Chrome cybersecui<BkSp>rity<Enter>
05-02-2025 11:55:15 chrome.exe New Tab - Google Chrome password <Enter>
05-02-2025 11:56:40 SearchHost.exe Search k
05-02-2025 11:58:54 SearchHost.exe Search syst
05-02-2025 11:59:03 SearchHost.exe Search m com
05-02-2025 12:00:28 PickerHost.exe Save As cns<Enter>
05-02-2025 12:00:57 chrome.exe New Tab - Google Chrome keylogger tool <Enter>
05-02-2025 12:03:05 PickerHost.exe Save As cns 1<Enter>
05-02-2025 12:03:24 PickerHost.exe Save As cns <BkSp><Enter>
05-02-2025 12:06:25 PickerHost.exe Save As cns 2<Enter>
05-02-2025 12:07:29 PickerHost.exe Save As ns 3<Enter>
11 / 11 Event Log - student : Keyboard events
EVENT LOG
STATISTICS
Detail View
Find this event in common log
ns 3<Enter>


Spyrix Free Keylogger 11.6.25
Event Log
Settings
Start
Stop
My Account
Wizard
Help
24 hours only!
$118 $59
About
Hide
Minimize
User Name
student
Event Log
Keyboard events
ScreenShots
Webcam snapshots
Sound recording
Webcam video
Clipboard Value
Web Pages Visited
Search Queries
Alerts
Site Blocker
Social Network Activity
Messaging Apps
User Activity
Programs Activity
User Smartphone Monitoring
Statistics - student : Keyboard events
Value
Title/Description
Amount
Last time
cybersecurity New Tab - Google Chrome ||| 1 05-02-2025 11:54:23
password New Tab - Google Chrome ||| 1 05-02-2025 11:55:15
k Search 1 05-02-2025 11:56:40
syst Search 1 05-02-2025 11:58:54
m Search 1 05-02-2025 11:59:03
com Search 1 05-02-2025 11:59:03
cns Save As 4 05-02-2025 12:06:25
keylogger New Tab - Google Chrome ||| 1 05-02-2025 12:00:57
tool Save As 1 05-02-2025 12:00:57
1 Save As 1 05-02-2025 12:03:05
2 Save As 1 05-02-2025 12:06:25
ns Save As 1 05-02-2025 12:07:29
3 Save As 1 05-02-2025 12:07:29
EVENT LOG
STATISTICS
Detail View
Find this event in common log
Visit URL
cybersecurity

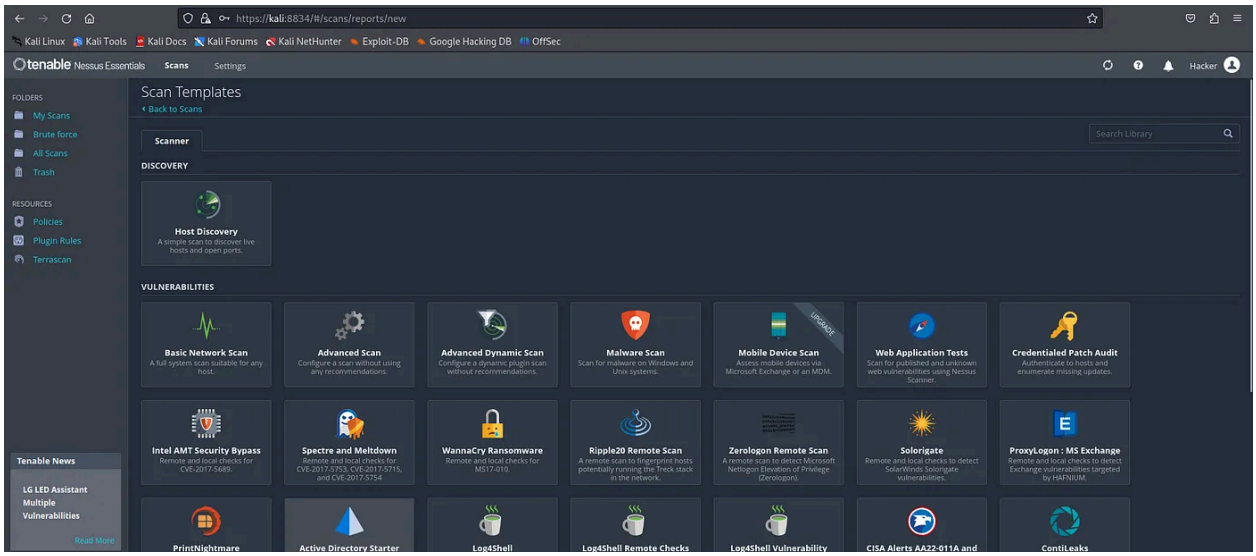
**b) DOS attack:**

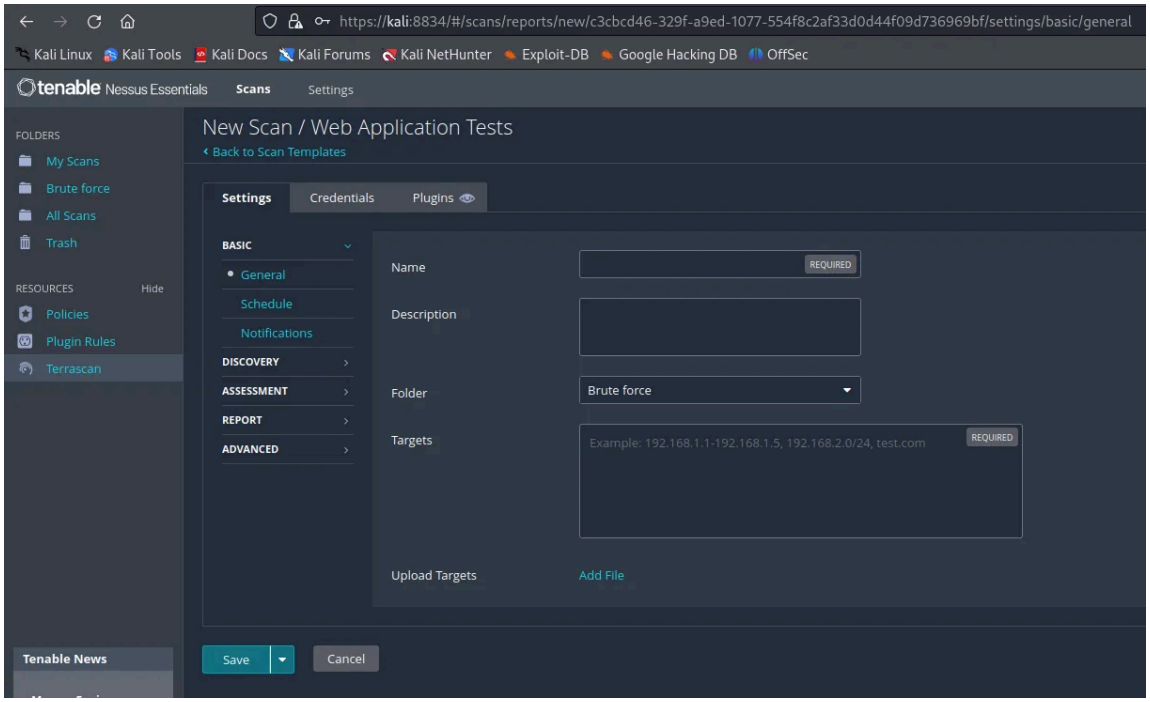
```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 -S --flood -p 80 192.168.236.128
HPING 192.168.236.128 (eth0 192.168.236.128): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.236.128 hping statistic ---
72127449 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

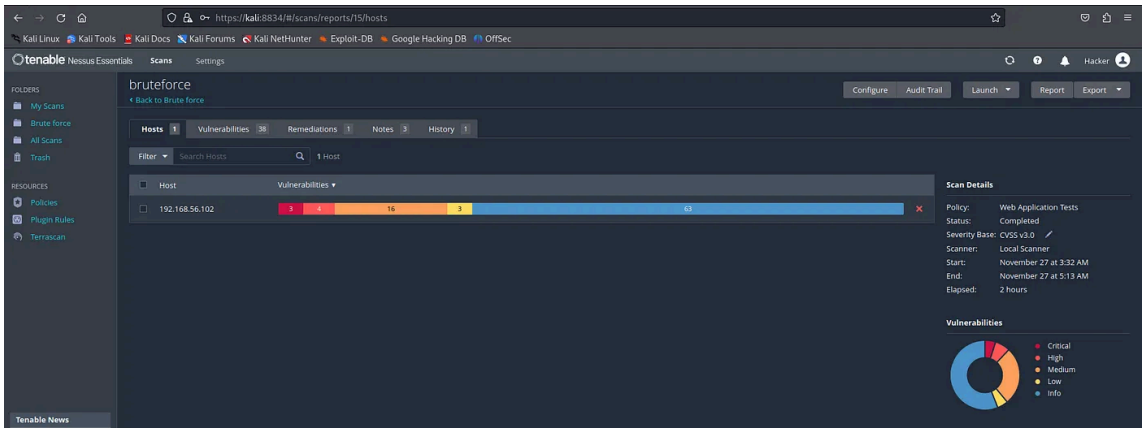
```
top - 19:16:12 up 18 min,  2 users,  load average: 1.38, 1.33, 0.94
Tasks: 263 total,   2 running, 261 sleeping,   0 stopped,   0 zombie
%Cpu(s): 12.8 us, 26.4 sy,  0.0 ni, 46.3 id,  0.0 wa,  0.0 hi, 14.6 si,  0.0 st
MiB Mem :   3884.3 total,   1655.3 free,   1073.4 used,   1449.3 buff/cache
MiB Swap:   2135.0 total,   2135.0 free,      0.0 used.   2810.9 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
   7087 root      20   0    9516   5120   4864 R  96.7   0.1  11:30.83 hping3
   1078 root      20   0  431392 142100  64136 S   2.7   3.6   0:31.02 Xorg
     26 root      20   0       0      0      0 S   2.3   0.0   0:03.99 ksoftirqd/1
   2154 kali      20   0  286420  46172  19532 S   1.7   1.2   0:13.56 panel-13-cpugra
     17 root      20   0       0      0      0 I   0.3   0.0   0:01.94 rcu_preempt
     25 root      rt   0       0      0      0 S   0.3   0.0   0:01.10 migration/1
    704 root      20   0  243992   9424   8016 S   0.3   0.2   0:02.83 vmtoolsd
   2275 kali      20   0  213092  38724  29840 S   0.3   1.0   0:03.01 vmtoolsd
  10024 kali      20   0  617028 109004  88616 S   0.3   2.7   0:02.40 qterminal
  10644 kali      20   0   10524   5572   3524 R   0.3   0.1   0:00.97 top
      1 root      20   0   23208  14036  10392 S   0.0   0.4   0:02.06 systemd
      2 root      20   0       0      0      0 S   0.0   0.0   0:00.03 kthreadd
      3 root      20   0       0      0      0 S   0.0   0.0   0:00.00 pool_workqueue_release
      4 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/R-rcu_gp
      5 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/R-sync_wq
      6 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/R-slub_flushwq
      7 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/R-netns
      8 root      20   0       0      0      0 I   0.0   0.0   0:00.21 kworker/0:0-events
      9 root       0 -20       0      0      0 I   0.0   0.0   0:00.28 kworker/0:0H-kblockd
     11 root      20   0       0      0      0 I   0.0   0.0   0:00.00 kworker/u512:0-ipv6_addrconf
     12 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/R-mm_percpu_wq
     13 root      20   0       0      0      0 I   0.0   0.0   0:00.00 rcu_tasks_kthread
     14 root      20   0       0      0      0 I   0.0   0.0   0:00.00 rcu_tasks_rude_kthread
     15 root      20   0       0      0      0 I   0.0   0.0   0:00.00 rcu_tasks_trace_kthread
     16 root      20   0       0      0      0 S   0.0   0.0   0:04.08 ksoftirqd/0
     18 root      20   0       0      0      0 S   0.0   0.0   0:00.00 rcu_exp_par_gp_kthread_worker/1
     19 root      20   0       0      0      0 S   0.0   0.0   0:00.00 rcu_exp_gp_kthread_worker
     20 root      rt   0       0      0      0 S   0.0   0.0   0:00.01 migration/0
     21 root     -51   0       0      0      0 S   0.0   0.0   0:00.00 idle_inject/0
     22 root      20   0       0      0      0 S   0.0   0.0   0:00.00 cpuhp/0
     23 root      20   0       0      0      0 S   0.0   0.0   0:00.00 cpuhp/1
     24 root     -51   0       0      0      0 S   0.0   0.0   0:00.00 idle_inject/1
     32 root      20   0       0      0      0 I   0.0   0.0   0:00.49 kworker/u514:1-events_unbound
     33 root      20   0       0      0      0 S   0.0   0.0   0:00.00 kdevtmpfs
     34 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/R-inet_frag_wq
     36 root      20   0       0      0      0 S   0.0   0.0   0:00.00 kauditd
```

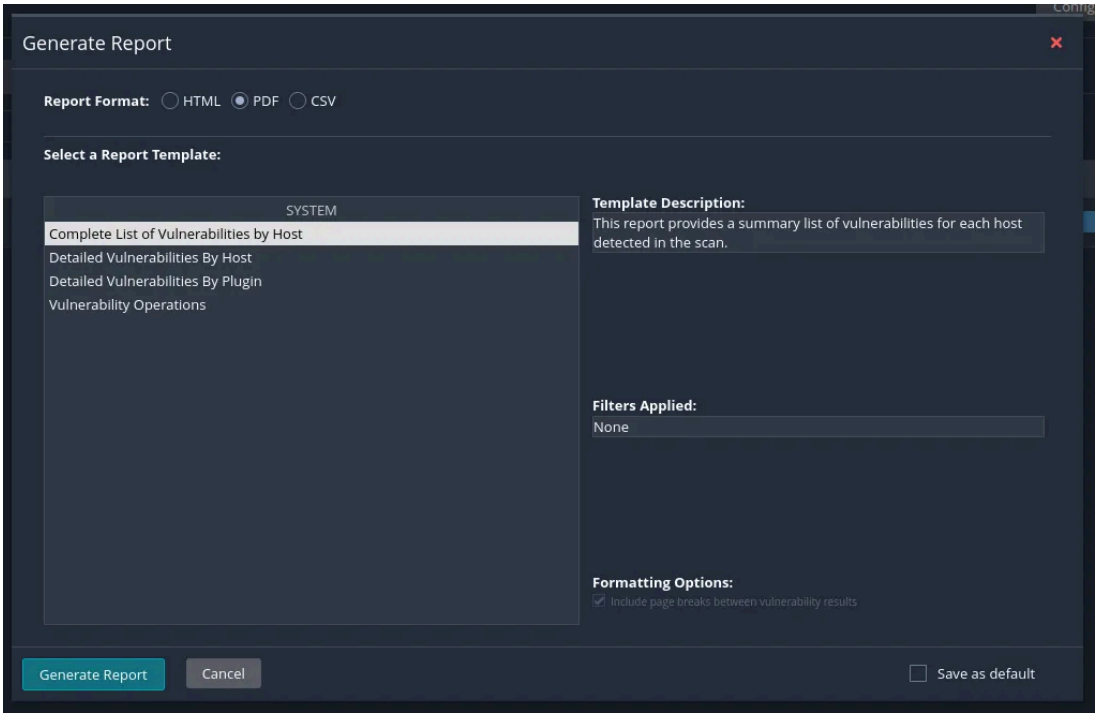
## c) Nessus/iso kali linux:

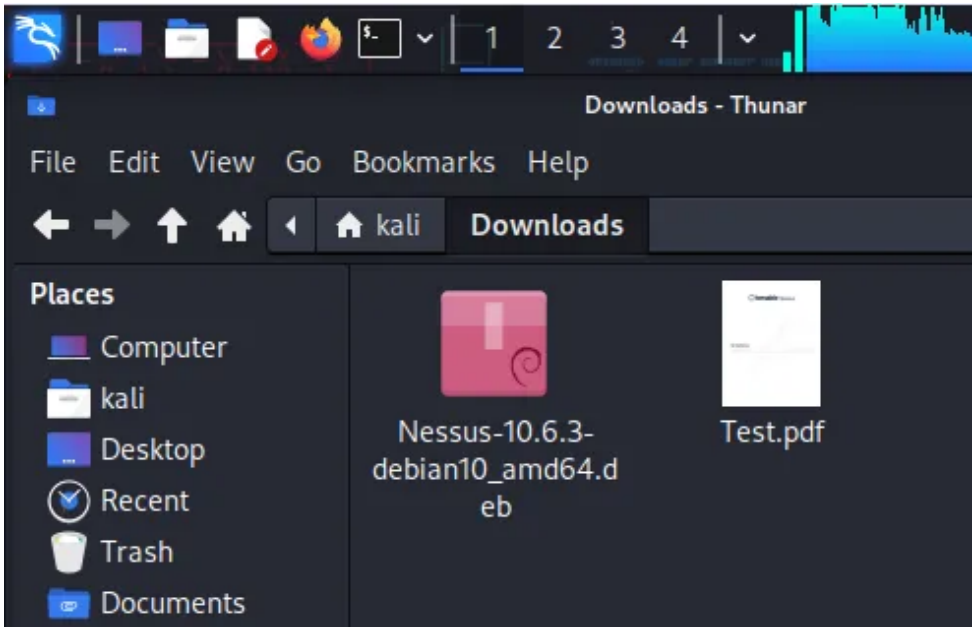
```
┌──(kali㉿kali)-[~]
└─$ wget https://www.tenable.com/downloads/api/v2/pages/nessus/files/Nessus-10.6.1-ubuntu_amd64.deb
--2025-02-26 19:35:04--  https://www.tenable.com/downloads/api/v2/pages/nessus/files/Nessus-10.6.1-ubuntu_amd64.deb
Resolving www.tenable.com (www.tenable.com)... 104.16.48.5, 104.16.49.5, 2606:4700::6810:3105, ...
Connecting to www.tenable.com (www.tenable.com)|104.16.48.5|:443... connected.
HTTP request sent, awaiting response... 404 Not Found
2025-02-26 19:35:05 ERROR 404: Not Found.

┌──(kali㉿kali)-[~]
└─$ cd ~/Downloads

┌──(kali㉿kali)-[~/Downloads]
└─$ ls
Nessus-10.8.3-ubuntu1604_amd64.deb

┌──(kali㉿kali)-[~/Downloads]
└─$ sudo dpkg -i Nessus-10.6.1-ubuntu_amd64.deb
dpkg: error: cannot access archive 'Nessus-10.6.1-ubuntu_amd64.deb': No such file or directory

┌──(kali㉿kali)-[~/Downloads]
└─$ sudo dpkg -i Nessus-*.deb
Selecting previously unselected package nessus.
(Reading database ... 469827 files and directories currently installed.)
Preparing to unpack Nessus-10.8.3-ubuntu1604_amd64.deb ...
Unpacking nessus (10.8.3) ...
Setting up nessus (10.8.3) ...
HMAC : (Module_Integrity) : Pass
SHA1 : (KAT_Digest) : Pass
SHA2 : (KAT_Digest) : Pass
SHA3 : (KAT_Digest) : Pass
TDES : (KAT_Cipher) : Pass
AES_GCM : (KAT_Cipher) : Pass
AES_ECB_Decrypt : (KAT_Cipher) : Pass
RSA : (KAT_Signature) : RNG : (Continuous_RNG_Test) : Pass
Pass
ECDSA : (PCT_Signature) : Pass
ECDSA : (PCT_Signature) : Pass
DSA : (PCT_Signature) : Pass
TLS13_KDF_EXTRACT : (KAT_KDF) : Pass
```




https://kali:8834/#/scans/reports/new/c3cbcd46-329f-a9ed-1077-554f8c2af33d0d44f09d736969bf/settings/basic/general
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
tenable Nessus Essentials
Scans
Settings
FOLDERS
My Scans
Brute force
All Scans
Trash
RESOURCES
Hide
Policies
Plugin Rules
Terrascan
Tenable News
New Scan / Web Application Tests
Back to Scan Templates
Settings
Credentials
Plugins
BASIC
General
Schedule
Notifications
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Name
REQUIRED
Description
Folder
Brute force
Targets
Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com
REQUIRED
Upload Targets
Add File
Save
Cancel


bruteforce
Back to Brute force
Configure
Audit Trail
Launch
Report
Export
Hosts
Vulnerabilities
Remediations
Notes
History
Filter
Search Hosts
1 Host
Host
Vulnerabilities
192.168.56.102
Scan Details
Policy: Web Application Tests
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: November 27 at 3:32 AM
End: November 27 at 5:13 AM
Elapsed: 2 hours
Vulnerabilities
Critical
High
Medium
Low
Info


Generate Report
Report Format: HTML PDF CSV
Select a Report Template:
SYSTEM
Complete List of Vulnerabilities by Host
Detailed Vulnerabilities By Host
Detailed Vulnerabilities By Plugin
Vulnerability Operations
Template Description:
This report provides a summary list of vulnerabilities for each host detected in the scan.
Filters Applied:
None
Formatting Options:
Include page breaks between vulnerability results
Generate Report
Cancel
Save as default




**7.8 Conclusion:-**

In this experiment, we explored different cybersecurity threats and defense mechanisms through three key exercises. First, we performed a keylogger attack using Spyrix, which captured every keystroke and took screenshots of the system, showcasing how attackers can secretly monitor user activity. Second, we performed a Denial of Service (DoS) attack using Hping3, demonstrating how an attacker can flood a target system with excessive packets, leading to service disruption. Lastly, we conducted a network vulnerability scan using Nessus, identifying security weaknesses that could potentially be exploited by attackers. These exercises highlight the critical need for strong security measures such as firewalls, intrusion detection systems (IDS), endpoint protection, and awareness training to prevent and mitigate such cyber threats.