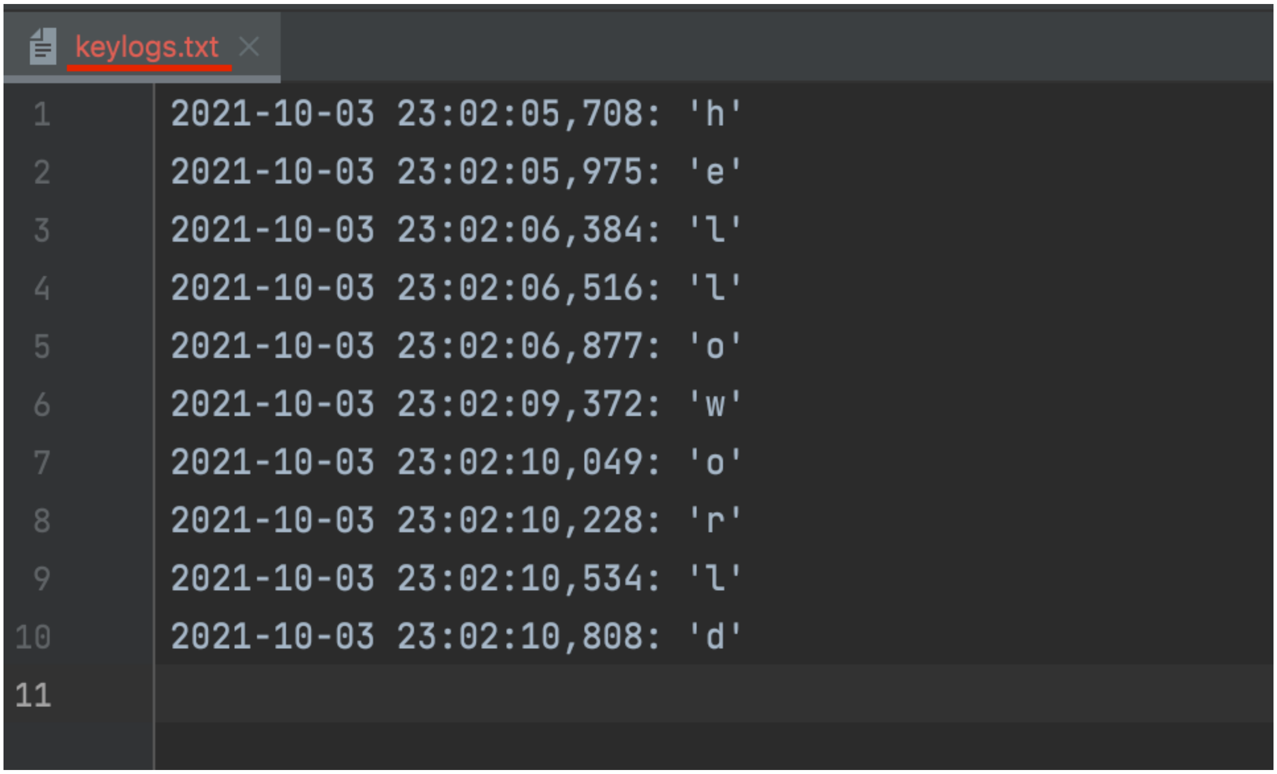
Output:

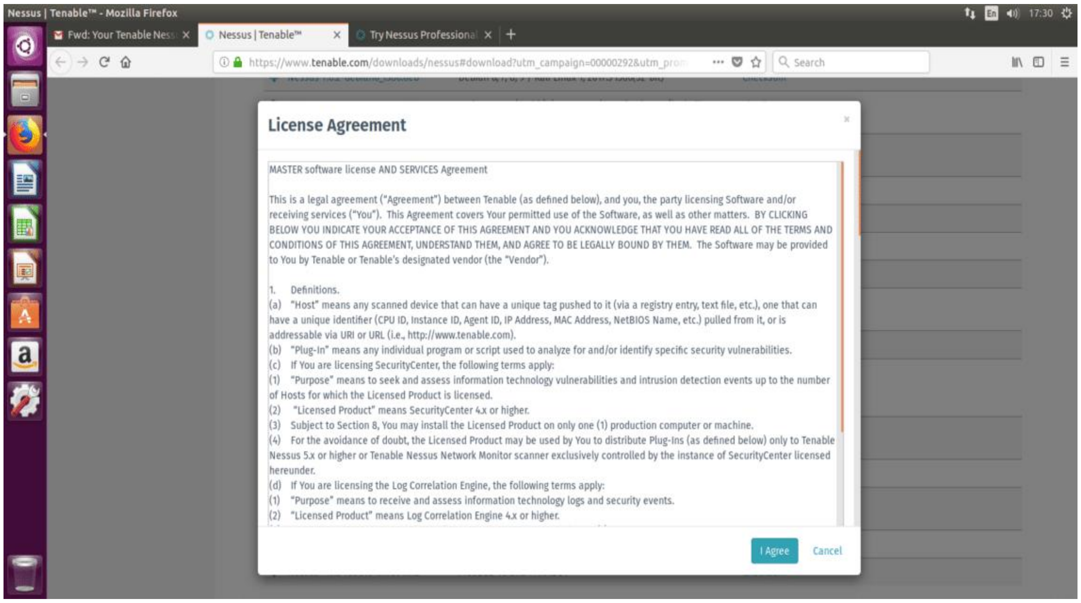
- **We get a keylogs file containing all the key we pressed on our keyboard along with the date and time.**



```
2021-10-03 23:02:05,708: 'h'
2021-10-03 23:02:05,975: 'e'
2021-10-03 23:02:06,384: 'l'
2021-10-03 23:02:06,516: 'l'
2021-10-03 23:02:06,877: 'o'
2021-10-03 23:02:09,372: 'w'
2021-10-03 23:02:10,049: 'o'
2021-10-03 23:02:10,228: 'r'
2021-10-03 23:02:10,534: 'l'
2021-10-03 23:02:10,808: 'd'
```

- **We can view the background process through task manager.**

Fill the form to get your trial code by email, click on the “Download and install” link.


Nessus | Tenable™ - Mozilla Firefox
Fwd: Your Tenable Ness
Nessus | Tenable™
Try Nessus Professional
https://www.tenable.com/downloads/nessus#download?utm_campaign=00000292&utm_pro
Search
17:30

License Agreement

MASTER software license AND SERVICES Agreement

This is a legal agreement (“Agreement”) between Tenable (as defined below), and you, the party licensing Software and/or receiving services (“You”). This Agreement covers Your permitted use of the Software, as well as other matters. BY CLICKING BELOW YOU INDICATE YOUR ACCEPTANCE OF THIS AGREEMENT AND YOU ACKNOWLEDGE THAT YOU HAVE READ ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT, UNDERSTAND THEM, AND AGREE TO BE LEGALLY BOUND BY THEM. The Software may be provided to You by Tenable or Tenable’s designated vendor (the “Vendor”).

1. Definitions.
(a) “Host” means any scanned device that can have a unique tag pushed to it (via a registry entry, text file, etc.), one that can have a unique identifier (CPU ID, Instance ID, Agent ID, IP Address, MAC Address, NetBIOS Name, etc.) pulled from it, or is addressable via URI or URL (i.e., http://www.tenable.com).
(b) “Plug-In” means any individual program or script used to analyze for and/or identify specific security vulnerabilities.
(c) If You are licensing SecurityCenter, the following terms apply:
(1) “Purpose” means to seek and assess information technology vulnerabilities and intrusion detection events up to the number of Hosts for which the Licensed Product is licensed.
(2) “Licensed Product” means SecurityCenter 4.x or higher.
(3) Subject to Section 8, You may install the Licensed Product on only one (1) production computer or machine.
(4) For the avoidance of doubt, the Licensed Product may be used by You to distribute Plug-Ins (as defined below) only to Tenable Nessus 5.x or higher or Tenable Nessus Network Monitor scanner exclusively controlled by the instance of SecurityCenter licensed hereunder.
(d) If You are licensing the Log Correlation Engine, the following terms apply:
(1) “Purpose” means to receive and assess information technology logs and security events.
(2) “Licensed Product” means Log Correlation Engine 4.x or higher.

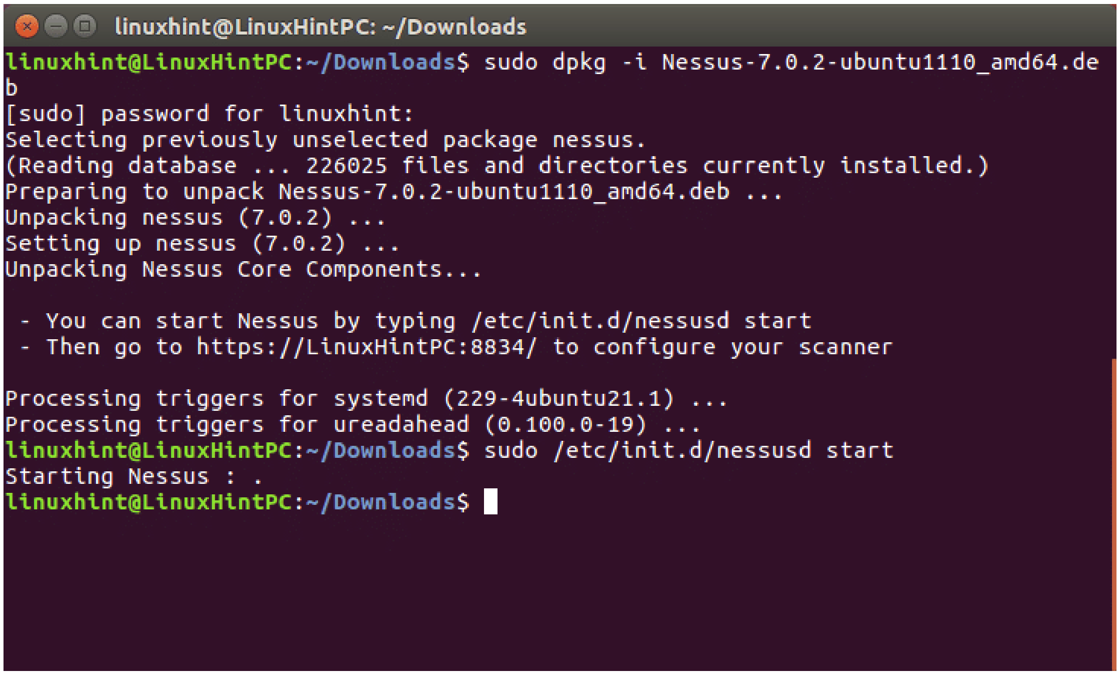
Installing Nessus:

Installing Nessus is very easy, especially if you have read our tutorial on DPKG packages manager.

Run: **sudo dpkg -i**

And after the installation is done follow the instructions by running:
sudo /etc/init.d/nessusd start

Your terminal should show very similar results to the following:



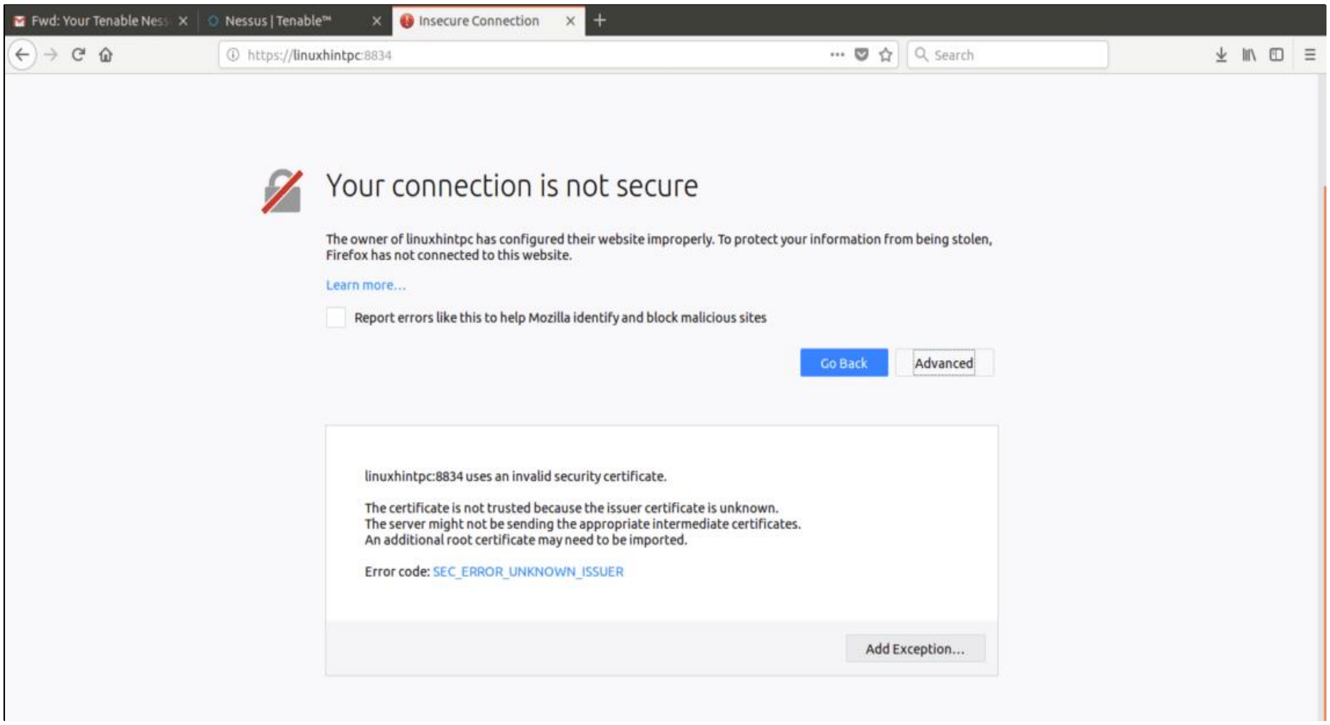
```
linuxhint@LinuxHintPC:~/Downloads$ sudo dpkg -i Nessus-7.0.2-ubuntu1110_amd64.de
b
[sudo] password for linuxhint:
Selecting previously unselected package nessus.
(Reading database ... 226025 files and directories currently installed.)
Preparing to unpack Nessus-7.0.2-ubuntu1110_amd64.deb ...
Unpacking nessus (7.0.2) ...
Setting up nessus (7.0.2) ...
Unpacking Nessus Core Components...

 - You can start Nessus by typing /etc/init.d/nessusd start
 - Then go to https://LinuxHintPC:8834/ to configure your scanner

Processing triggers for systemd (229-4ubuntu21.1) ...
Processing triggers for ureadahead (0.100.0-19) ...
linuxhint@LinuxHintPC:~/Downloads$ sudo /etc/init.d/nessusd start
Starting Nessus : .
linuxhint@LinuxHintPC:~/Downloads$ 
```

Following Nessus' installation instructions lets go to: https:// YOURPCNAME:8443 (change YOURPCNOW for your computer's name, works with localhost too).

When opening the Web interface, a SSL error may appear.



Your connection is not secure

The owner of linuxhintpc has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.

Learn more…

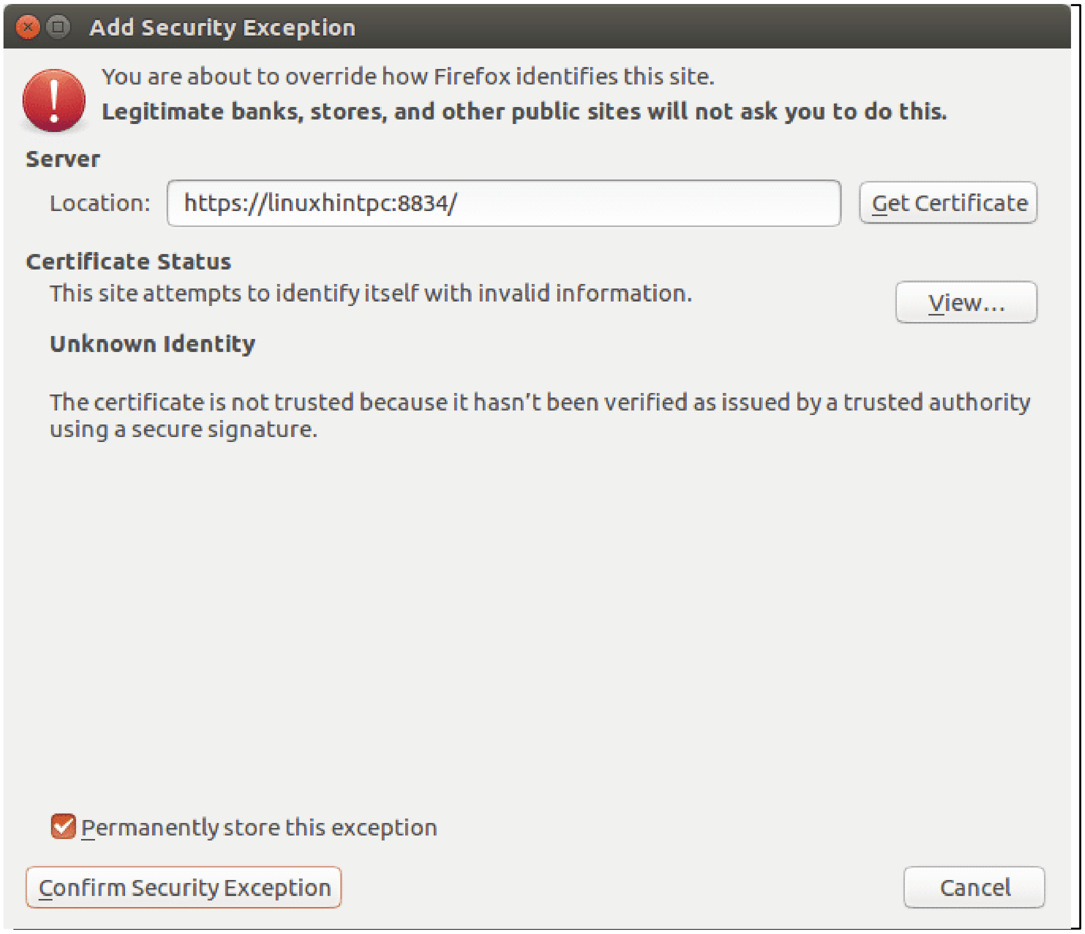
□ Report errors like this to help Mozilla identify and block malicious sites

linuxhintpc:8834 uses an invalid security certificate.

The certificate is not trusted because the issuer certificate is unknown.
The server might not be sending the appropriate intermediate certificates.
An additional root certificate may need to be imported.

Error code: SEC_ERROR_UNKNOWN_ISSUER

Just add an exception and continue accessing:



Add Security Exception

You are about to override how Firefox identifies this site.

Legitimate banks, stores, and other public sites will not ask you to do this.

Server

Location: https://linuxhintpc:8834/

Certificate Status

This site attempts to identify itself with invalid information.

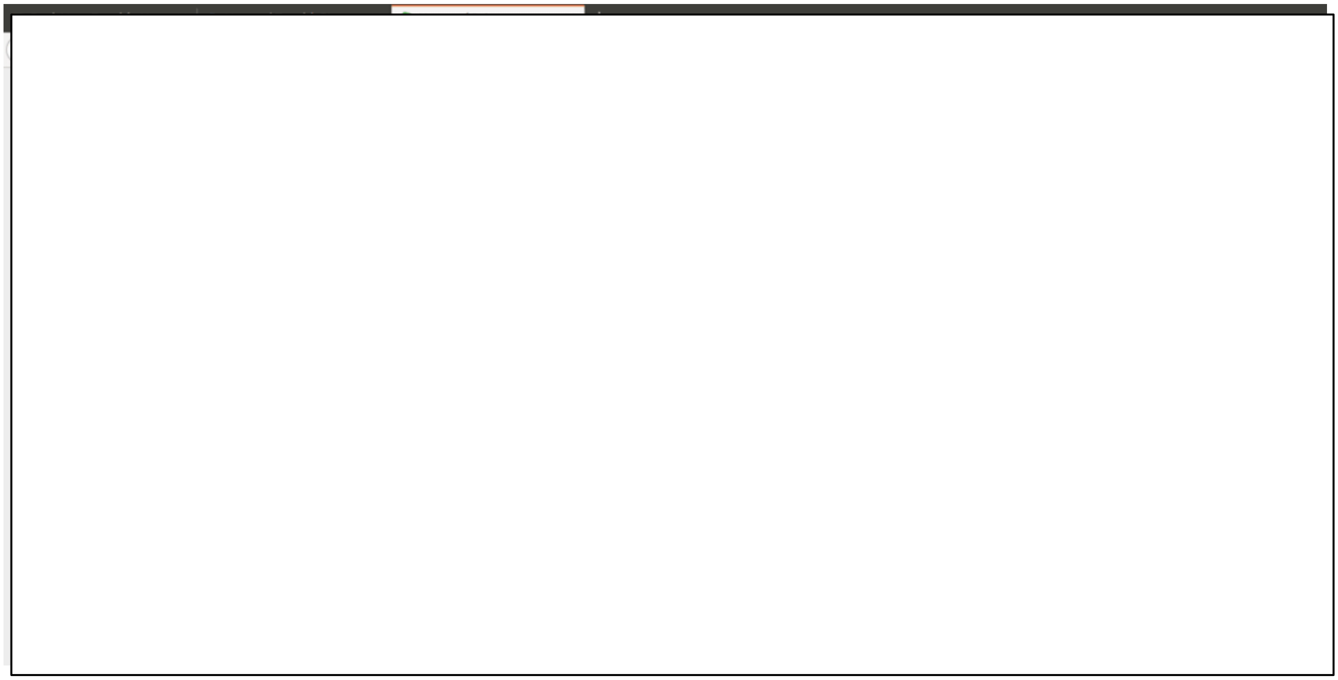
Unknown Identity

The certificate is not trusted because it hasn't been verified as issued by a trusted authority using a secure signature.

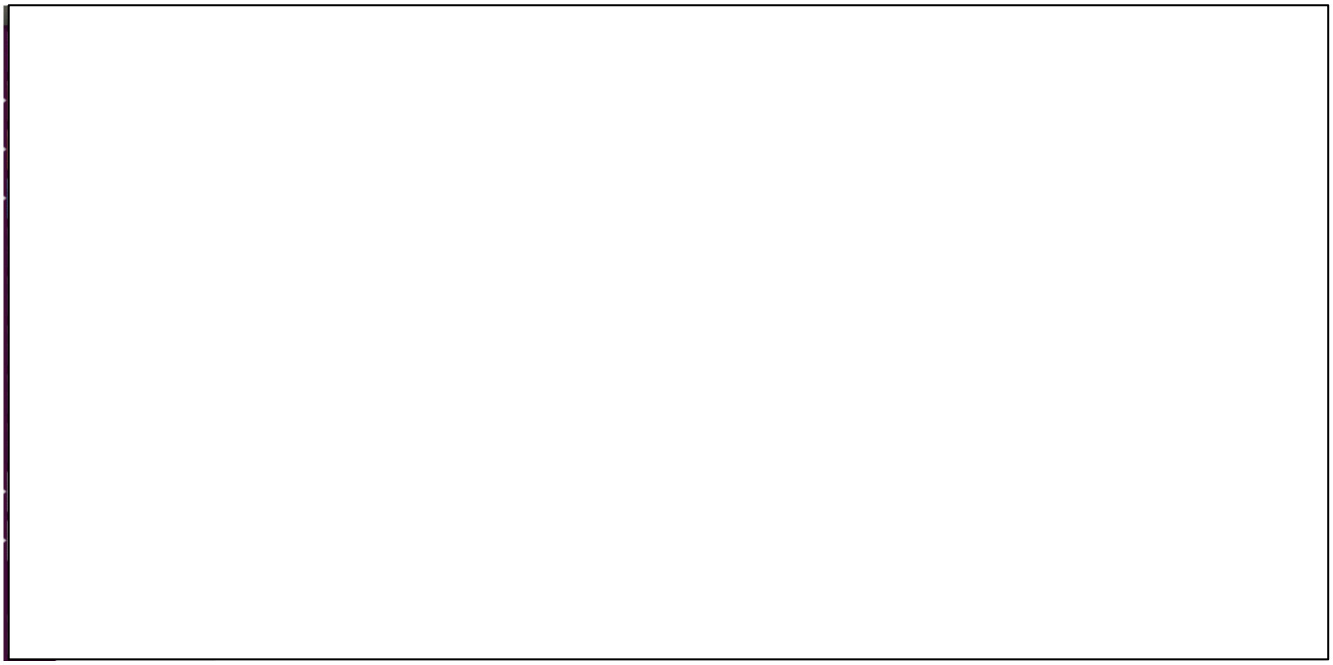
☑ Permanently store this exception

Finally we'll meet Nessus' screen, login using "admin" both as user and password.

In the next screen select the use you’ll give to Nessus and put the trial code you got by e-mail.

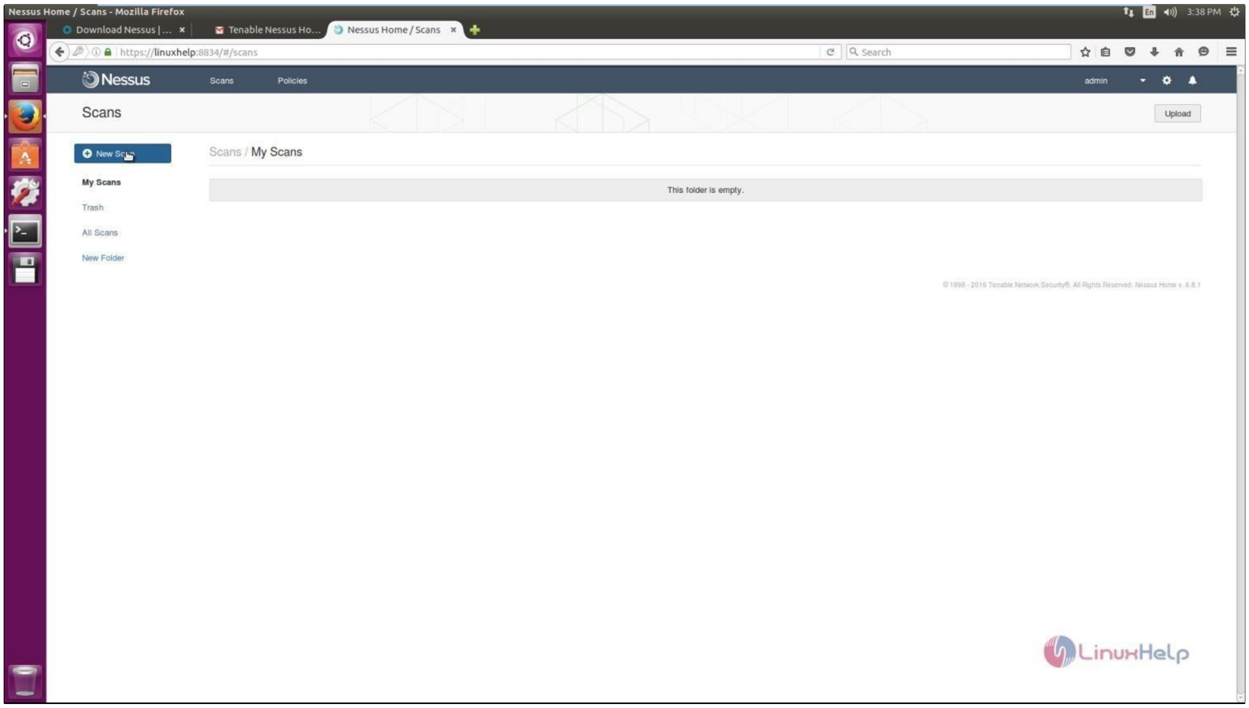


After filling everything Nessus will start initializing as shown in the next image, this step may take about 20 or 30 minutes, after finishing the next screen will be:

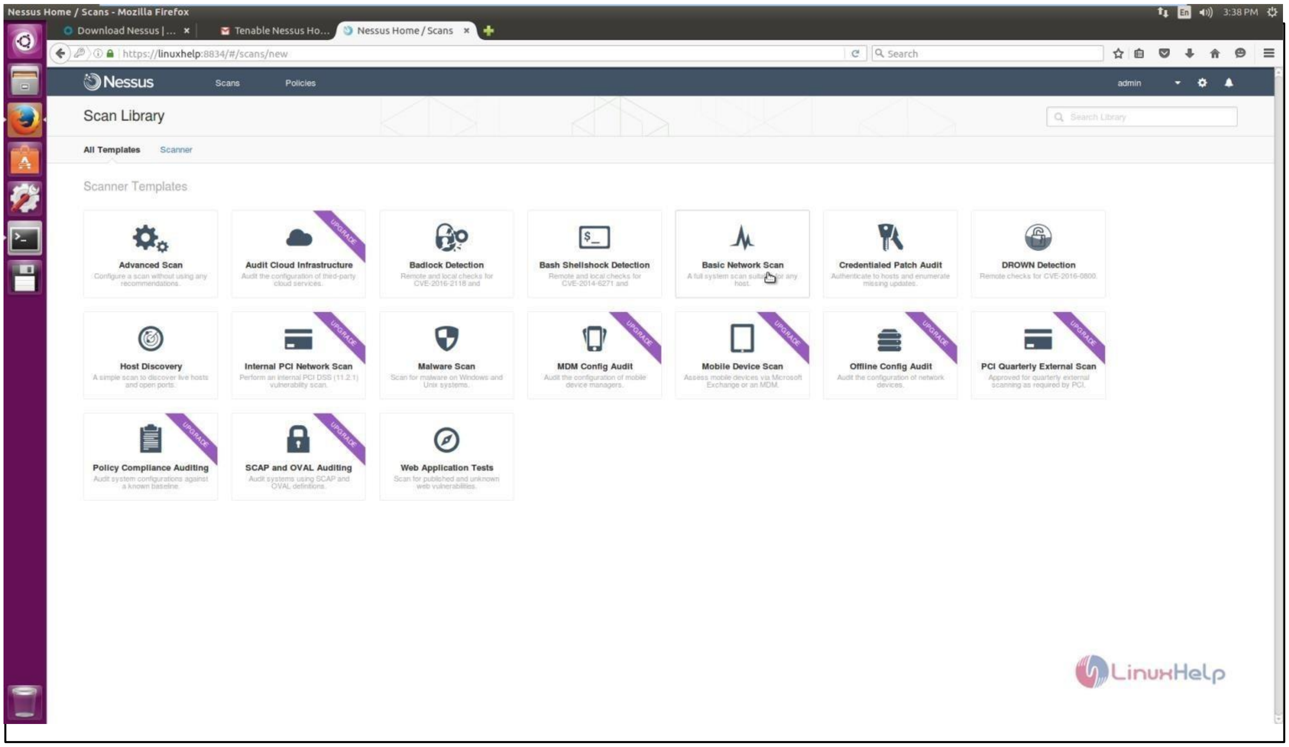


Scanning using Nessus:

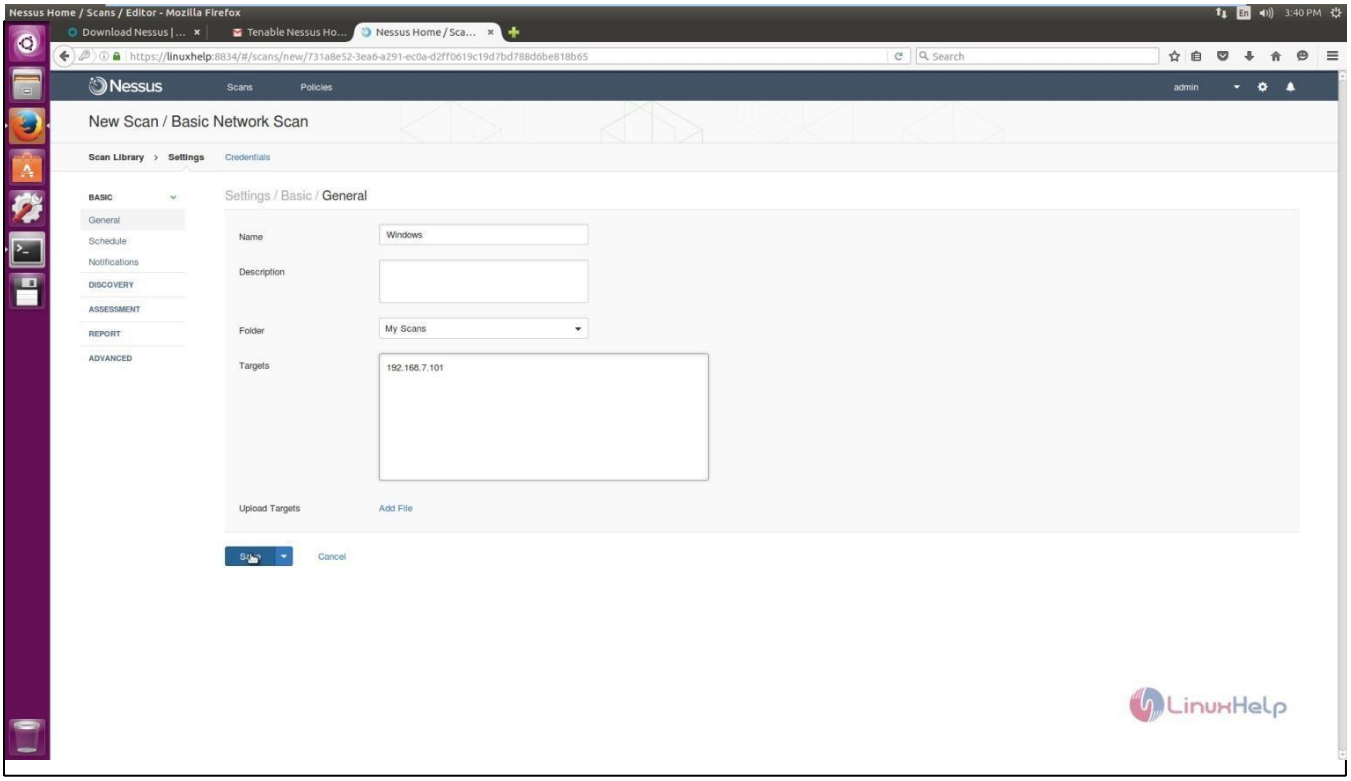
To create a new scan, click New Scan icon.



Select the type of scan.


Nessus Home / Scans - Mozilla Firefox
Download Nessus | ...
Tenable Nessus Ho...
Nessus Home / Scans
https://linuxhelp:8834/#/scans/new
Search
Nessus
Scans
Policies
admin
Scan Library
Search Library
All Templates
Scanner
Scanner Templates
Advanced Scan
Configure a scan without using any recommendations.
Audit Cloud Infrastructure
Audit the configuration of third-party cloud services.
UPGRADE
Badlock Detection
Remote and local checks for CVE-2016-2118 and
Bash Shellshock Detection
Remote and local checks for CVE-2014-6271 and
Basic Network Scan
A full system scan suitable for any host.
Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.
DROWN Detection
Remote checks for CVE-2016-0800.
Host Discovery
A simple scan to discover live hosts and open ports.
Internal PCI Network Scan
Perform an internal PCI DSS (11.2.1) vulnerability scan.
UPGRADE
Malware Scan
Scan for malware on Windows and Unix systems.
MDM Config Audit
Audit the configuration of mobile device managers.
UPGRADE
Mobile Device Scan
Assess mobile devices via Microsoft Exchange or an MDM.
UPGRADE
Offline Config Audit
Audit the configuration of network devices.
UPGRADE
PCI Quarterly External Scan
Approved for quarterly external scanning as required by PCI.
UPGRADE
Policy Compliance Auditing
Audit system configurations against a known baseline.
UPGRADE
SCAP and OVAL Auditing
Audit systems using SCAP and OVAL definitions.
UPGRADE
Web Application Tests
Scan for published and unknown web vulnerabilities.
LinuxHelp

Enter the details of the system where the scan is to be performed.



New Scan / Basic Network Scan

Settings / Basic / General

Name: Windows

Description:

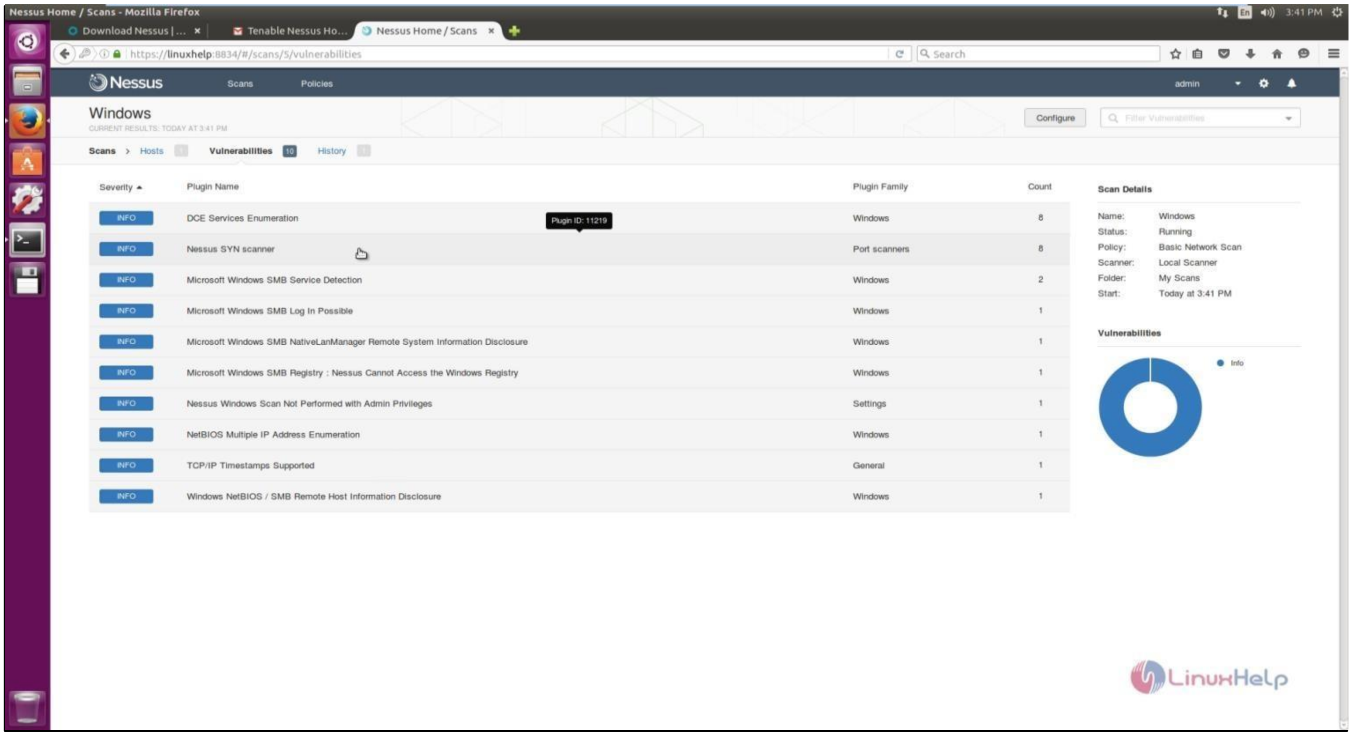
Folder: My Scans

Targets: 192.168.7.101

Upload Targets: Add File

Select the scan and click the drop-down more and then launch the scan.

Select the scan to see the vulnerabilities in the target system.



Windows
CURRENT RESULTS: TODAY AT 3:41 PM

Scans > Hosts 1 Vulnerabilities 10 History 1

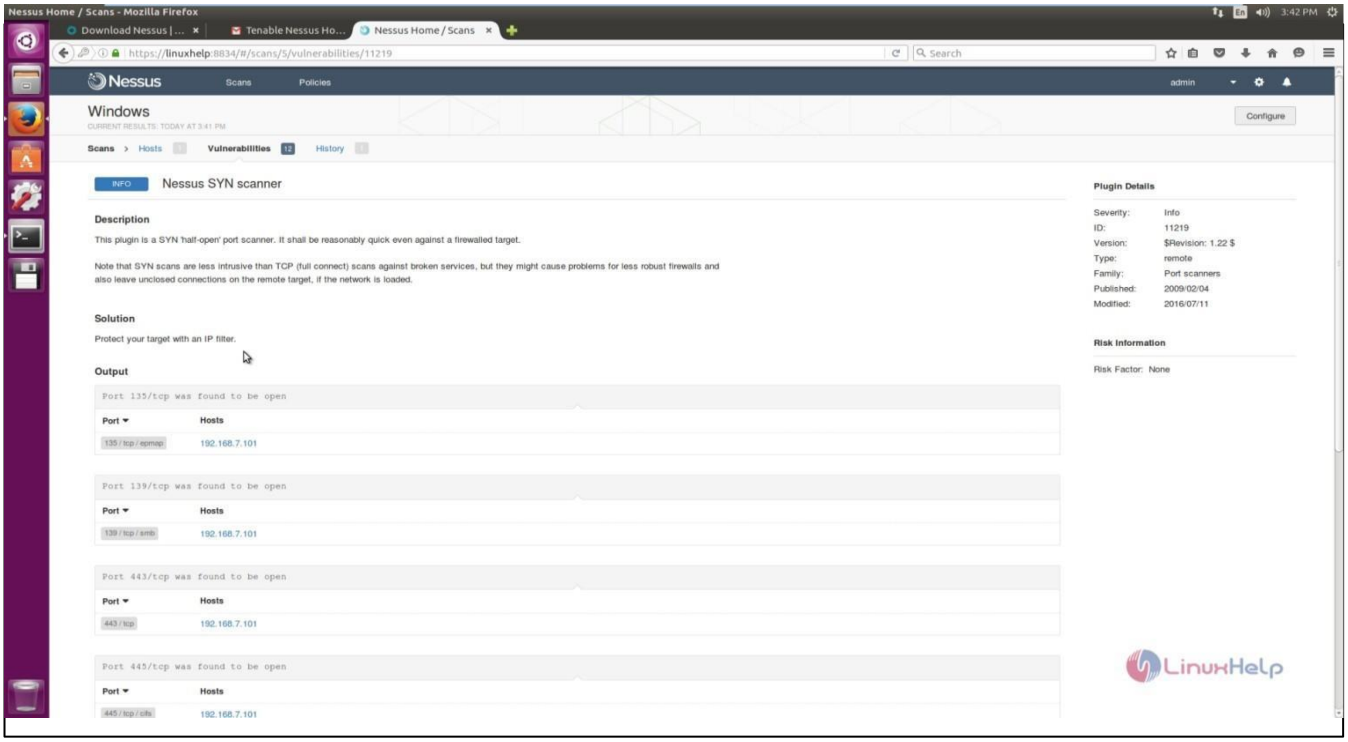
Severity	Plugin Name	Plugin Family	Count
INFO	DCE Services Enumeration	Windows	8
INFO	Nessus SYN scanner	Port scanners	8
INFO	Microsoft Windows SMB Service Detection	Windows	2
INFO	Microsoft Windows SMB Log In Possible	Windows	1
INFO	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure	Windows	1
INFO	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry	Windows	1
INFO	Nessus Windows Scan Not Performed with Admin Privileges	Settings	1
INFO	NetBIOS Multiple IP Address Enumeration	Windows	1
INFO	TCP/IP Timestamps Supported	General	1
INFO	Windows NetBIOS / SMB Remote Host Information Disclosure	Windows	1

Scan Details

Name:	Windows
Status:	Running
Policy:	Basic Network Scan
Scanner:	Local Scanner
Folder:	My Scans
Start:	Today at 3:41 PM

Vulnerabilities

Click the vulnerability to see the description and solution for the vulnerabilities.



Windows
CURRENT RESULTS: TODAY AT 3:41 PM

Scans > Hosts 1 Vulnerabilities 12 History 1

INFO Nessus SYN scanner

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Output

```
Port 135/tcp was found to be open
```

Port	Hosts
135 / tcp / epmap	192.168.7.101

```
Port 139/tcp was found to be open
```

Port	Hosts
139 / tcp / smb	192.168.7.101

```
Port 443/tcp was found to be open
```

Port	Hosts
443 / tcp	192.168.7.101

```
Port 445/tcp was found to be open
```

Port	Hosts
445 / tcp / cifs	192.168.7.101

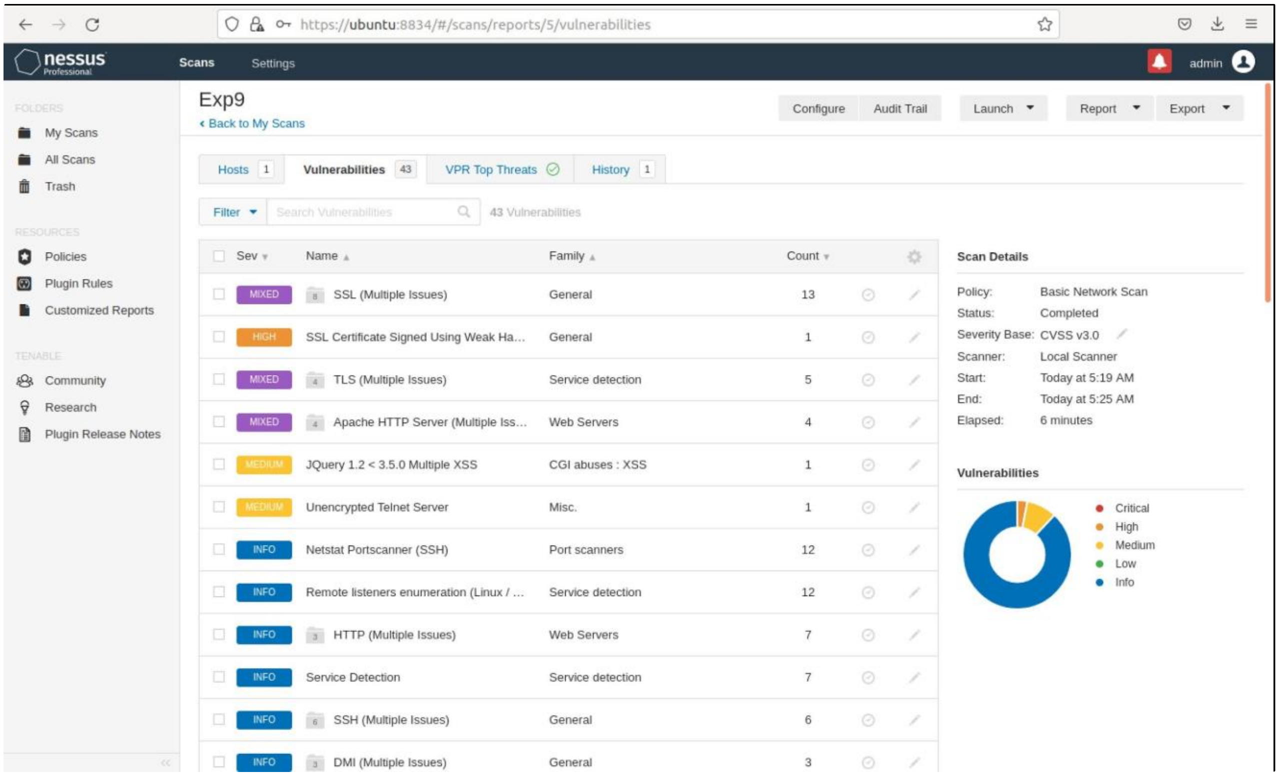
Plugin Details

Severity:	Info
ID:	11219
Version:	$Revision: 1.22 $
Type:	remote
Family:	Port scanners
Published:	2009/02/04
Modified:	2016/07/11

Risk Information

Risk Factor: None

Output :



Exp9

43 Vulnerabilities

Sev	Name	Family	Count
MIXED	SSL (Multiple Issues)	General	13
HIGH	SSL Certificate Signed Using Weak Ha...	General	1
MIXED	TLS (Multiple Issues)	Service detection	5
MIXED	Apache HTTP Server (Multiple Iss...	Web Servers	4
MEDIUM	JQuery 1.2 < 3.5.0 Multiple XSS	CGI abuses : XSS	1
MEDIUM	Unencrypted Telnet Server	Misc.	1
INFO	Netstat Portscanner (SSH)	Port scanners	12
INFO	Remote listeners enumeration (Linux / ...	Service detection	12
INFO	HTTP (Multiple Issues)	Web Servers	7
INFO	Service Detection	Service detection	7
INFO	SSH (Multiple Issues)	General	6
INFO	DMI (Multiple Issues)	General	3

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 5:19 AM
End:	Today at 5:25 AM
Elapsed:	6 minutes

Vulnerabilities