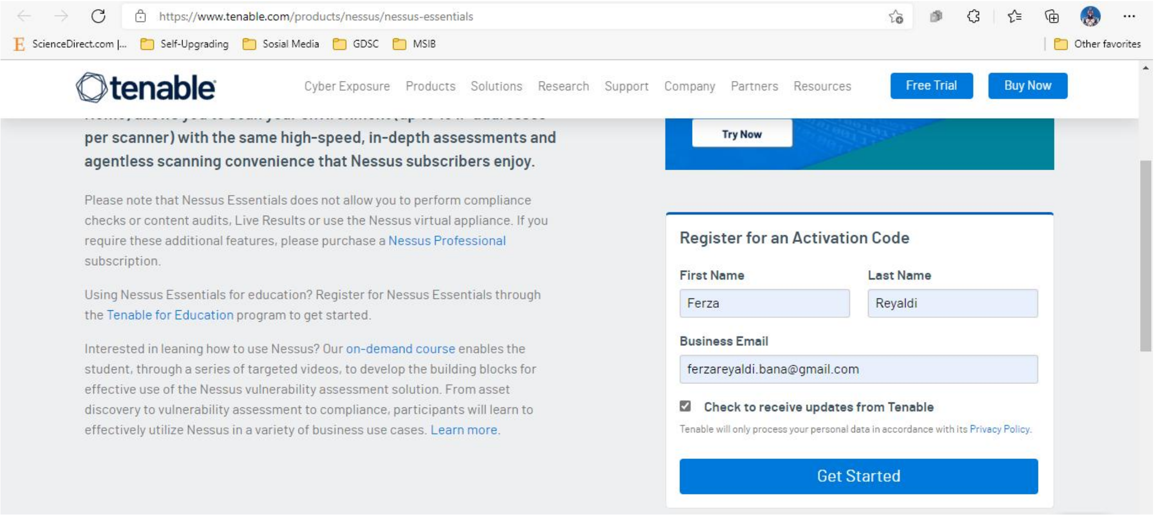
Nama : Ferza Reyaldi
NIM : 09021281924060
Mata Kuliah : Keamanan Jaringan Komputer

Ujian Tengah Semester
Laporan TryHackMe: Nessus

Task 2: Installation

1. Lakukan Registrasi akun untuk mendapatkan *activation code*.



per scanner) with the same high-speed, in-depth assessments and agentless scanning convenience that Nessus subscribers enjoy.

Please note that Nessus Essentials does not allow you to perform compliance checks or content audits, Live Results or use the Nessus virtual appliance. If you require these additional features, please purchase a Nessus Professional subscription.

Using Nessus Essentials for education? Register for Nessus Essentials through the Tenable for Education program to get started.

Interested in leaning how to use Nessus? Our on-demand course enables the student, through a series of targeted videos, to develop the building blocks for effective use of the Nessus vulnerability assessment solution. From asset discovery to vulnerability assessment to compliance, participants will learn to effectively utilize Nessus in a variety of business use cases. Learn more.

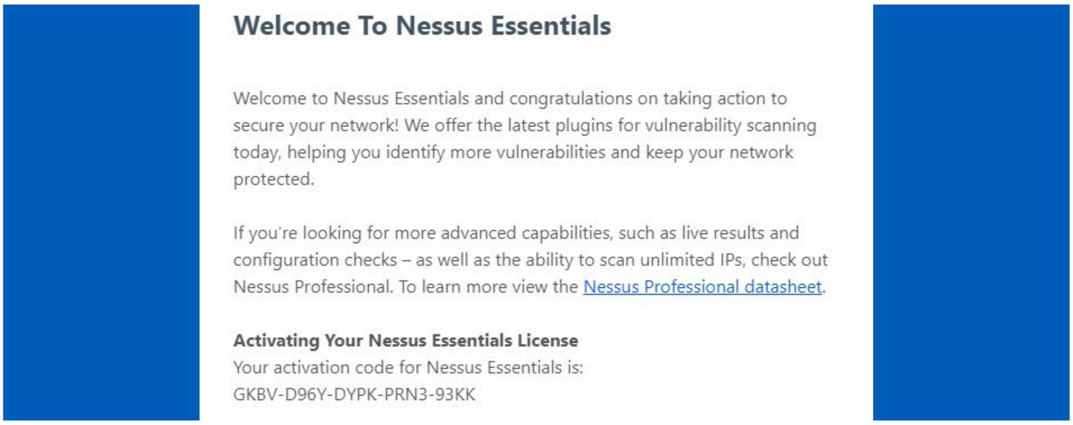
Register for an Activation Code

First Name: Ferza
Last Name: Reyaldi
Business Email: ferzareyaldi.bana@gmail.com

☑ Check to receive updates from Tenable

Tenable will only process your personal data in accordance with its Privacy Policy.

Get Started



Welcome To Nessus Essentials

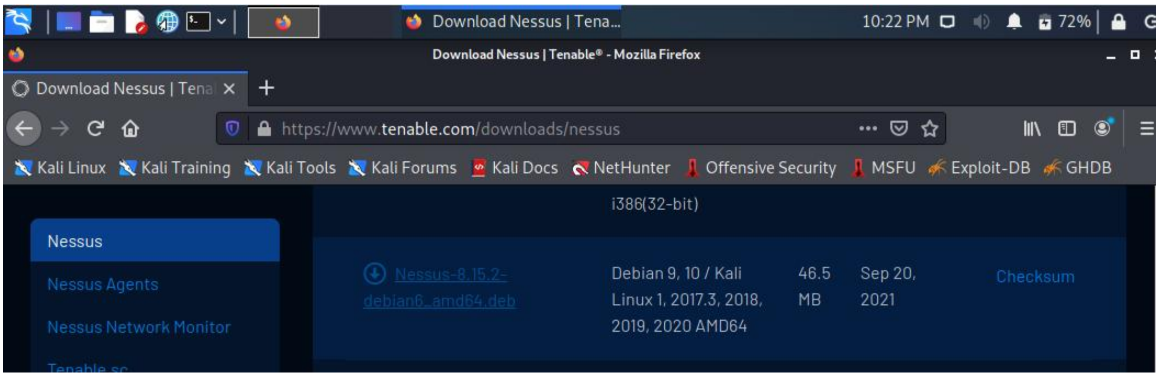
Welcome to Nessus Essentials and congratulations on taking action to secure your network! We offer the latest plugins for vulnerability scanning today, helping you identify more vulnerabilities and keep your network protected.

If you're looking for more advanced capabilities, such as live results and configuration checks – as well as the ability to scan unlimited IPs, check out Nessus Professional. To learn more view the Nessus Professional datasheet.

Activating Your Nessus Essentials License

Your activation code for Nessus Essentials is:
GKBV-D96Y-DYPK-PRN3-93KK

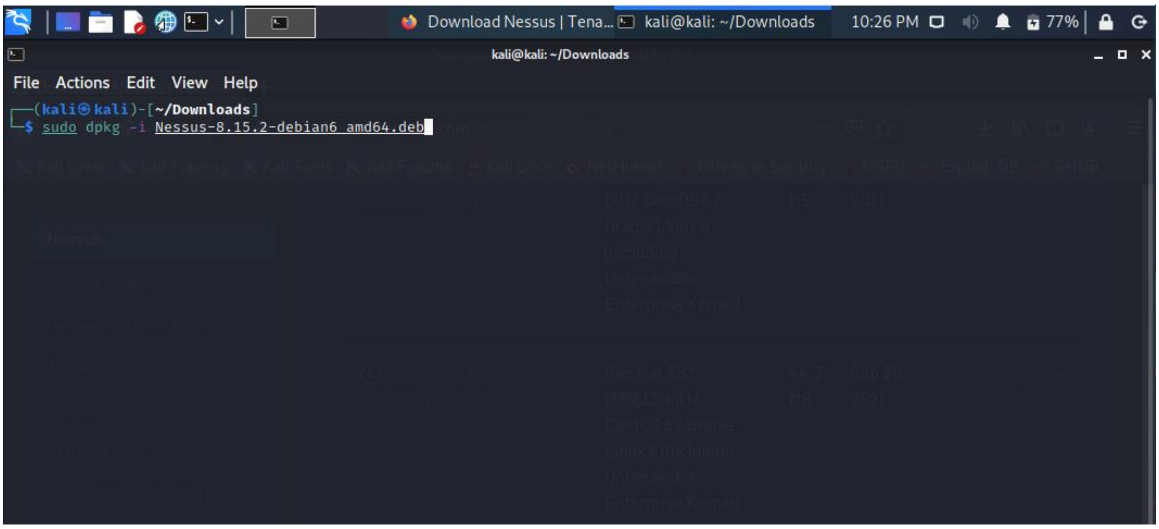
2. Unduh file **Nessus-#.##.#-debian6_amd64.deb.**



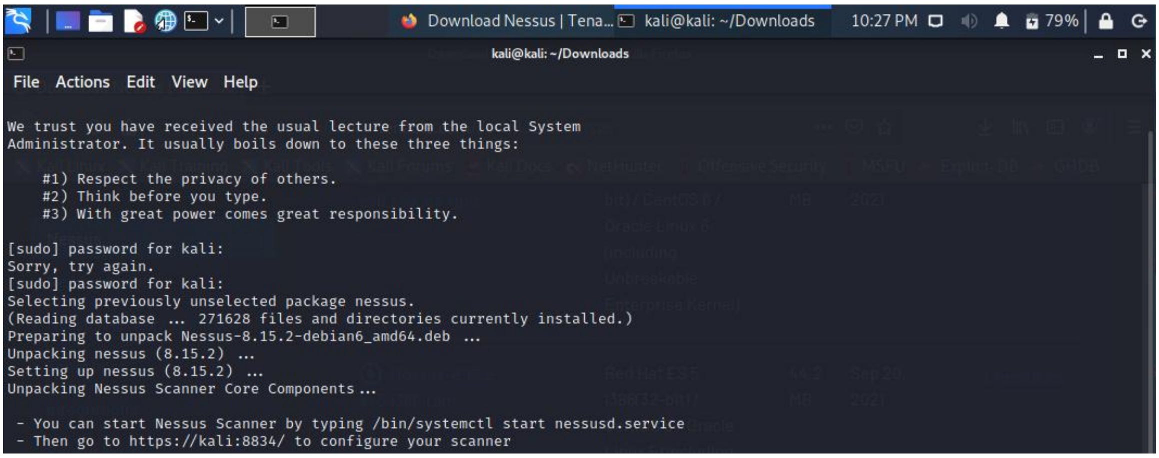
i386(32-bit)

Nessus-8.15.2-debian6_amd64.deb | Debian 9, 10 / Kali Linux 1, 2017.3, 2018, 2019, 2020 AMD64 | 46.5 MB | Sep 20, 2021 | Checksum

3. Buka terminal, jalankan perintah **sudo dpkg -i [Nama File Package].deb** untuk menginstal Nessus.

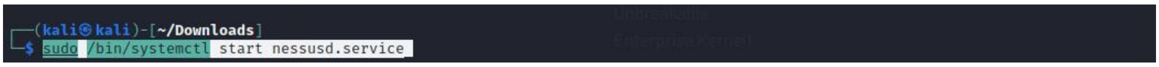


```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo dpkg -i Nessus-8.15.2-debian6_amd64.deb
```



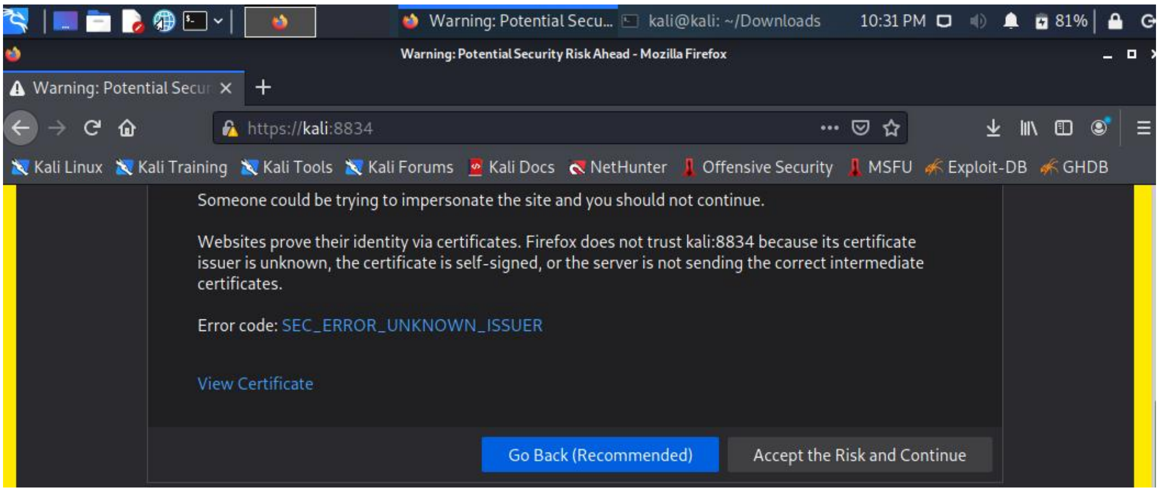
```
We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
Selecting previously unselected package nessus.
(Reading database ... 271628 files and directories currently installed.)
Preparing to unpack Nessus-8.15.2-debian6_amd64.deb ...
Unpacking nessus (8.15.2) ...
Setting up nessus (8.15.2) ...
Unpacking Nessus Scanner Core Components...

 - You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
 - Then go to https://kali:8834/ to configure your scanner
```

4. Mulai Nessus Service dengan perintah **sudo /bin/systemctl start nessusd.service**



```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo /bin/systemctl start nessusd.service
```

5. Buka https://kali:8834/. Jika ada *prompted* dengan *security risk alert*, klik **Advanced -> Accept the Risk and Continue**.



Someone could be trying to impersonate the site and you should not continue.

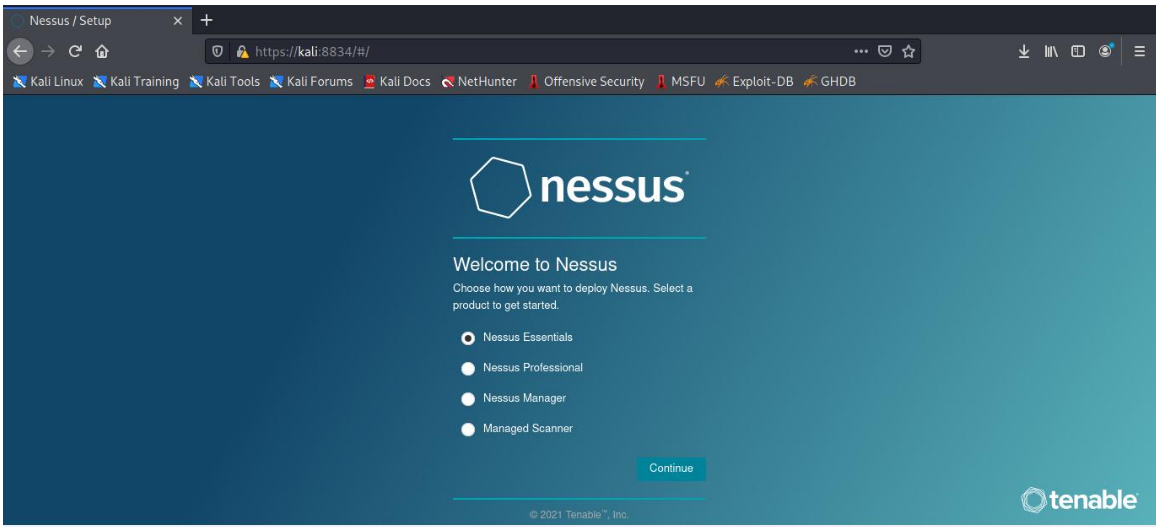
Websites prove their identity via certificates. Firefox does not trust kali:8834 because its certificate issuer is unknown, the certificate is self-signed, or the server is not sending the correct intermediate certificates.

Error code: SEC_ERROR_UNKNOWN_ISSUER

View Certificate

Melakukan *set up* Scanner

6. Pilih **Nessus Essentials**, klik **Continue**.



Welcome to Nessus

Choose how you want to deploy Nessus. Select a product to get started.

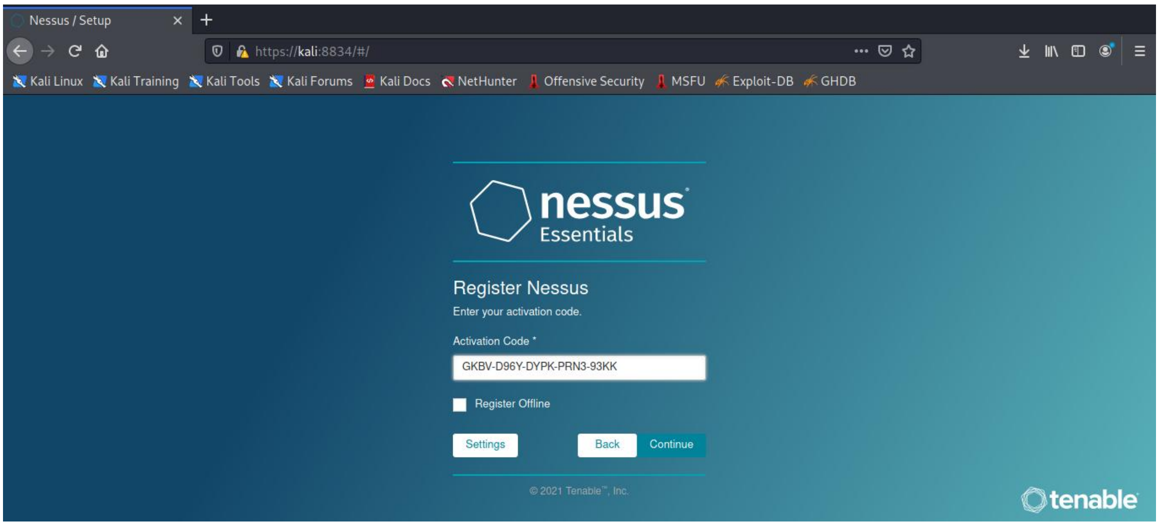
● Nessus Essentials

○ Nessus Professional

○ Nessus Manager

○ Managed Scanner

7. Klik **skip**, kemudian masukan *activation code*.



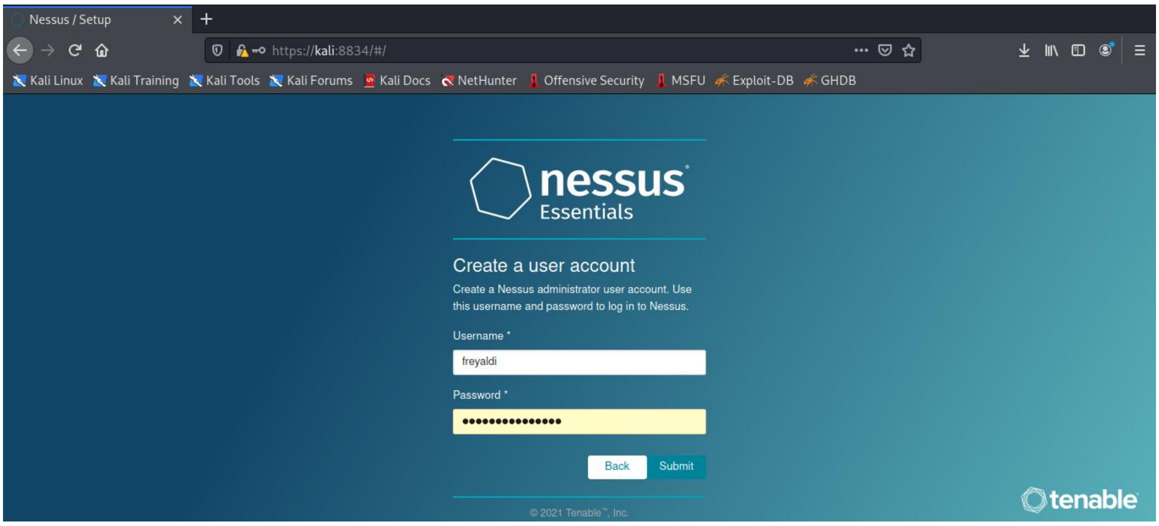
Register Nessus

Enter your activation code.

Activation Code *: GKBV-D96Y-DYPK-PRN3-93KK

□ Register Offline

8. Buat username dan password.



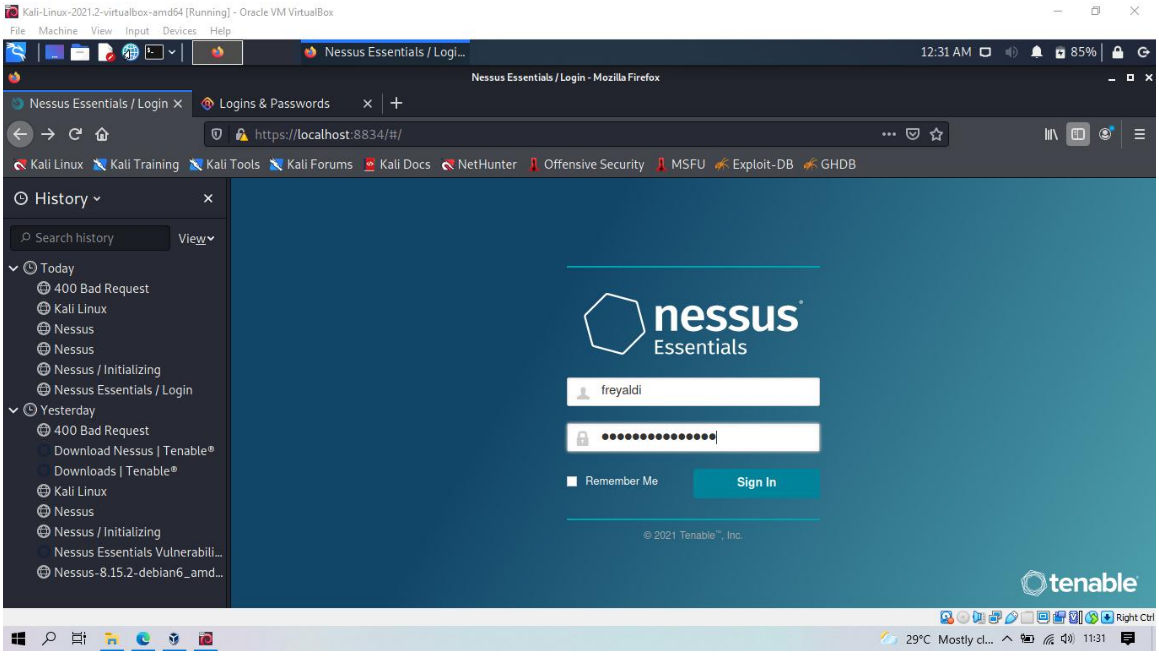
Create a user account

Create a Nessus administrator user account. Use this username and password to log in to Nessus.

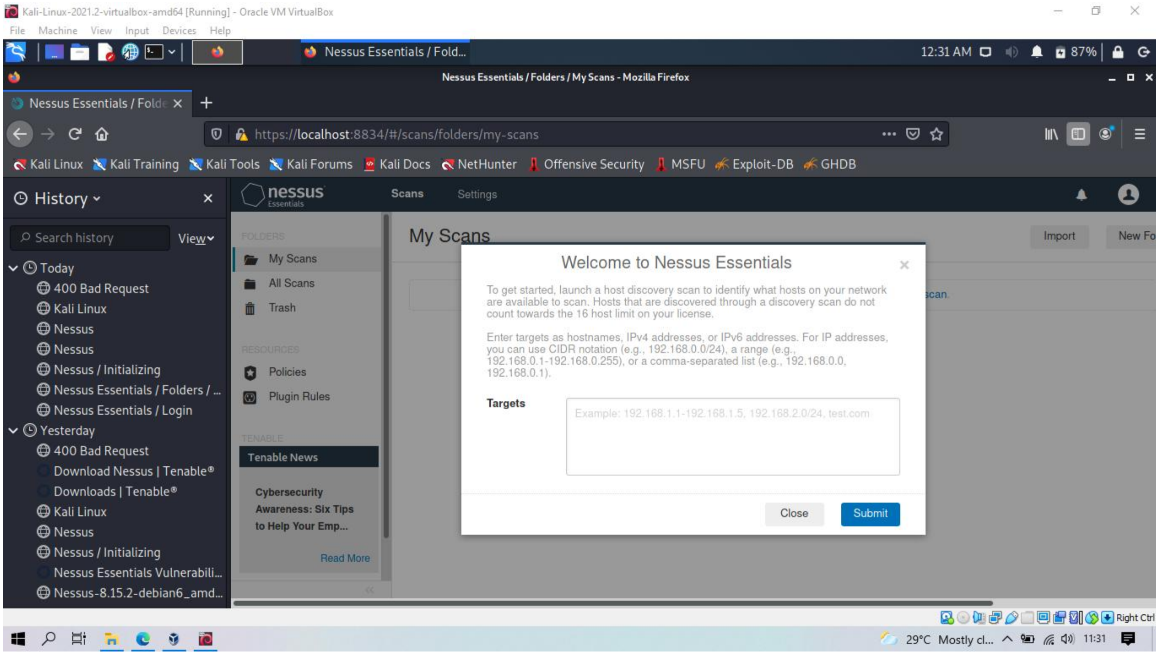
Username *: freyaldi

Password *: •••••••••••••••

9. Log in dengan kredensial akun yang telah dibuat


Kali-Linux-2021.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
Nessus Essentials / Login - Mozilla Firefox
https://localhost:8834/#/
History
nessus Essentials
freyaldi
Remember Me
Sign In
© 2021 Tenable™, Inc.
tenable

10. Nessus berhasil diinstal.


Nessus Essentials / Folders / My Scans - Mozilla Firefox
https://localhost:8834/#/scans/folders/my-scans
Scans
Settings
My Scans
All Scans
Trash
Policies
Plugin Rules
Tenable News
Cybersecurity Awareness: Six Tips to Help Your Emp...
Read More
Import
Close
Submit

Welcome to Nessus Essentials

To get started, launch a host discovery scan to identify what hosts on your network are available to scan. Hosts that are discovered through a discovery scan do not count towards the 16 host limit on your license.

Enter targets as hostnames, IPv4 addresses, or IPv6 addresses. For IP addresses, you can use CIDR notation (e.g., 192.168.0.0/24), a range (e.g., 192.168.0.1-192.168.0.255), or a comma-separated list (e.g., 192.168.0.0, 192.168.0.1).

Targets: Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com

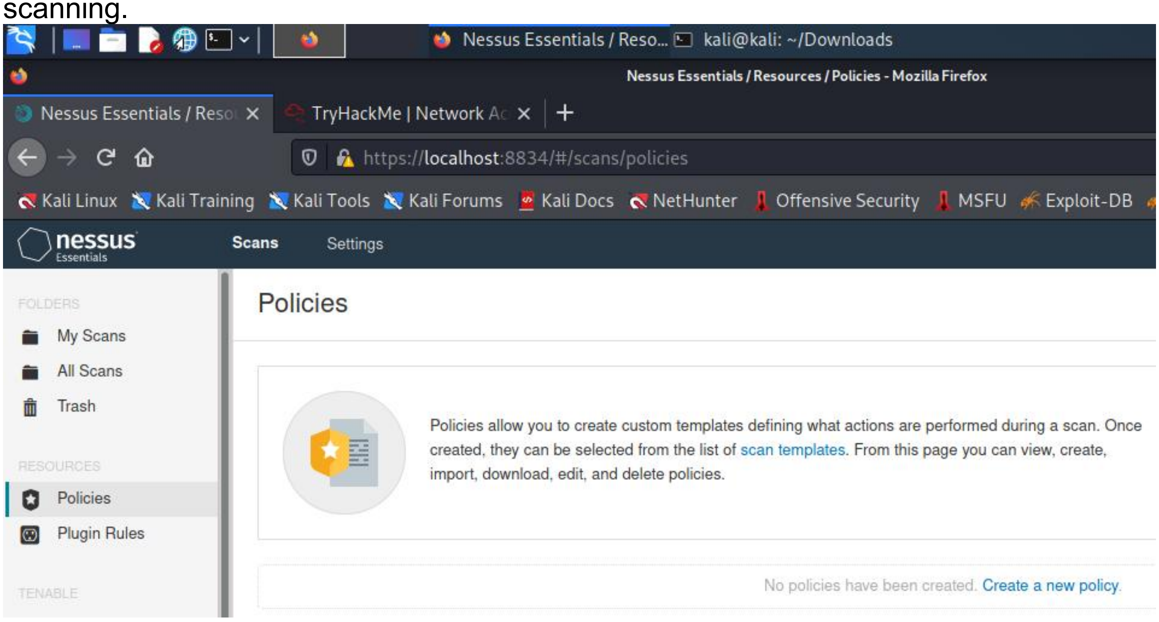
Task 3: Navigation & Scans

What is the name of the **button** which is used to launch a scan?

Jawab: new scan
digunakan untuk menjalankan/membuat suatu scanning apapun pada Nessus.

What side menu option allows us to create **custom templates**?

Jawab: policies
terletak pada bagian **resources**, memungkinkan untuk membuat *custom template* dalam scanning.

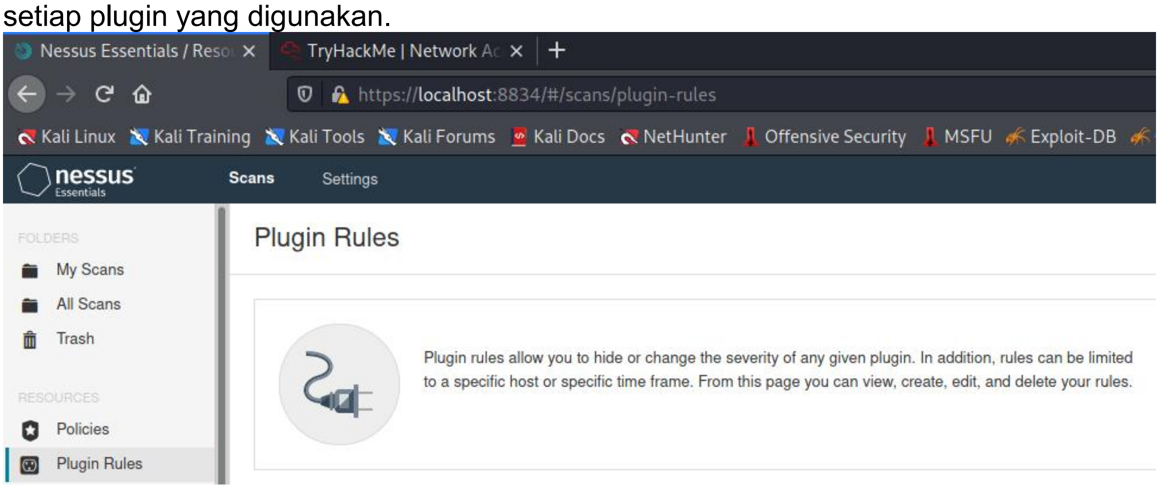


Policies allow you to create custom templates defining what actions are performed during a scan. Once created, they can be selected from the list of scan templates. From this page you can view, create, import, download, edit, and delete policies.

No policies have been created. Create a new policy.

What menu allows us to change **plugin** properties such as hiding them or changing their severity?

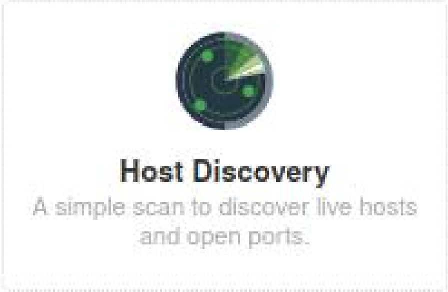
Jawab: plugin rules
terletak pada bagian **resources**, memungkinkan untuk menyembunyikan *severity* dari setiap plugin yang digunakan.



Plugin rules allow you to hide or change the severity of any given plugin. In addition, rules can be limited to a specific host or specific time frame. From this page you can view, create, edit, and delete your rules.

In the '**Scan Templates**' section after clicking on '**New Scan**', what scan allows us to see simply what hosts are alive?

Jawab: host discovery
memungkinkan melakukan scanning untuk melihat/menemukan host yang hidup dan port-port yang terbuka.

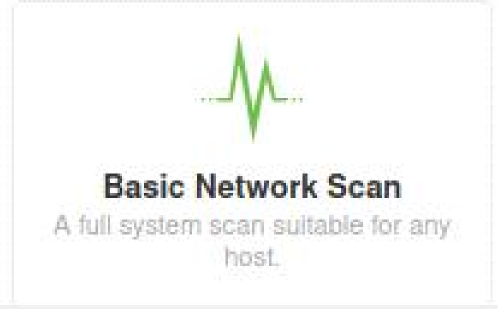


Host Discovery

A simple scan to discover live hosts and open ports.

One of the most useful scan types, which is considered to be '**suitable for any host**'?

Jawab: basic network scan
tipe scan yang paling fleksibel dan sangat berguna karena cocok untuk semua jenis host.

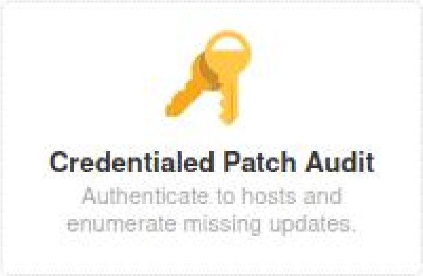


Basic Network Scan

A full system scan suitable for any host.

What scan allows you to '**Authenticate to hosts and enumerate missing updates**'?

Jawab: credentialed patch audit
Tipe scan yang memungkinkan untuk melakukan autentikasi pada host dan melakukan enumerasi terhadap perubahan yang hilang.



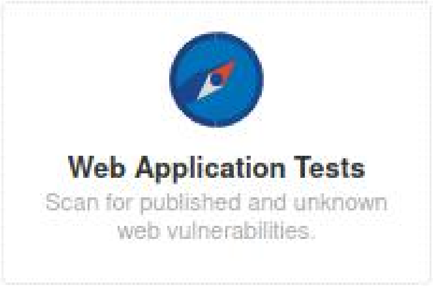
Credentialed Patch Audit

Authenticate to hosts and enumerate missing updates.

What scan is specifically used for scanning **Web Applications**?

Jawab: web applications tests

Tipe scan khusus dilakukan pada web applications vulnerabilities, baik yang bersifat publik ataupun tidak diketahui.



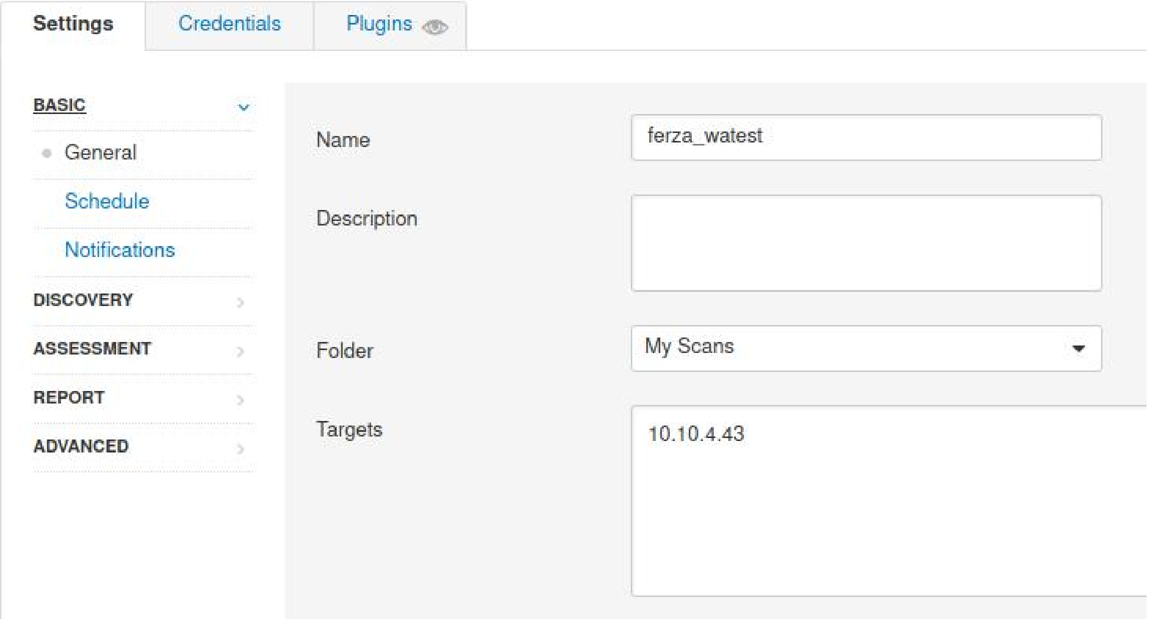
Web Application Tests

Scan for published and unknown web vulnerabilities.

Task 4: Scanning

Create a new '**Basic Network Scan**' targeting the deployed VM. What option can we set under '**BASIC**' (on the left) to set a time for this scan to run? This can be very useful when network congestion is an issue.

Jawab: schedule
Salah satu menu yang berada pada bagian BASIC, sesuai namanya berguna untuk mengatur waktu untuk menjalankan scan.



Name: ferza_watest

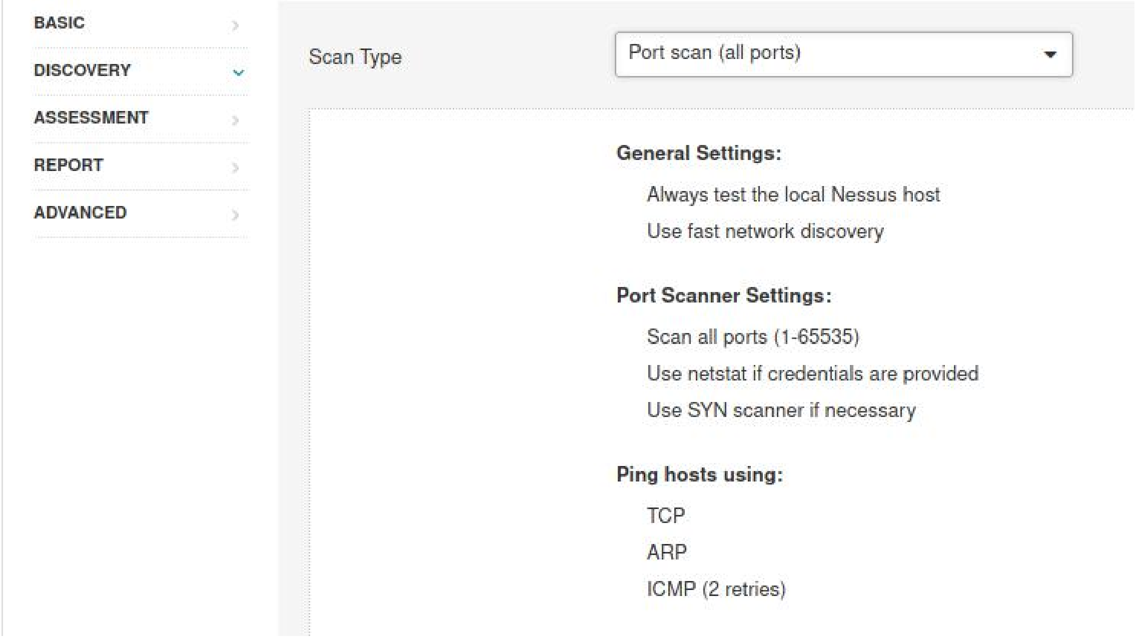
Description:

Folder: My Scans

Targets: 10.10.4.43

Under '**DISCOVERY**' (on the left) set the '**Scan Type**' to cover ports 1-65535. What is this type called?

Jawab: port scan (all ports)
Pada bagian DISCOVERY, tepatnya menu Scan Type, pilih **port scan (all ports)** dengan tujuan agar semua port diperiksa.



Scan Type: Port scan (all ports)

General Settings:

Always test the local Nessus host

Use fast network discovery

Port Scanner Settings:

Scan all ports (1-65535)

Use netstat if credentials are provided

Use SYN scanner if necessary

Ping hosts using:

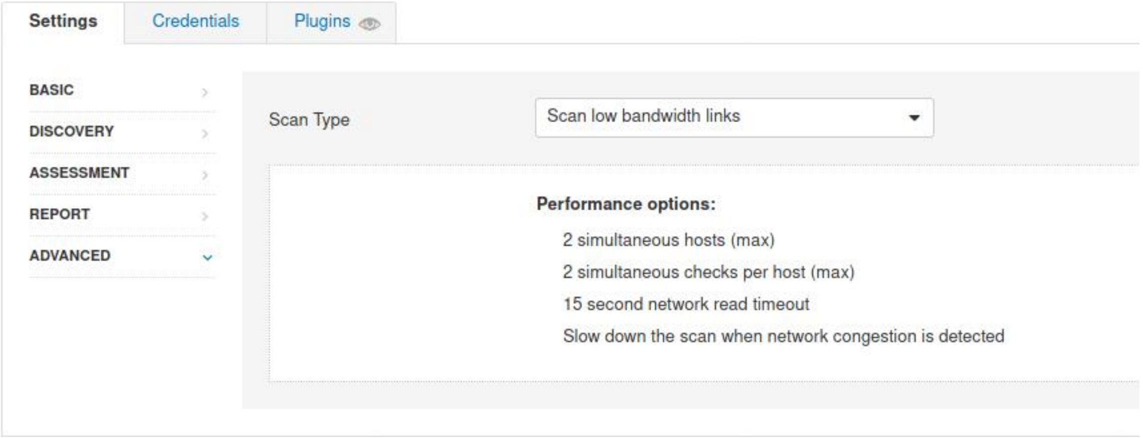
TCP

ARP

ICMP (2 retries)

What '**Scan Type**' can we change to under '**ADVANCED**' for lower bandwidth connection?

Jawab: scan low bandwidth links
Pada bagian ADVANCED, pilih **Scan low bandwidth links** dengan tujuan agar dapat dilakukan scanning dengan koneksi bandwidth yang lebih kecil/rendah.



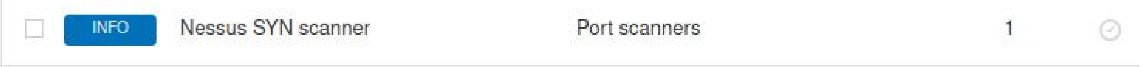
Scan Type: Scan low bandwidth links

Performance options:

2 simultaneous hosts (max)
2 simultaneous checks per host (max)
15 second network read timeout
Slow down the scan when network congestion is detected

After the scan completes, which '**Vulnerability**' in the '**Port scanners**' family can we view the details of to see the open ports on this host?

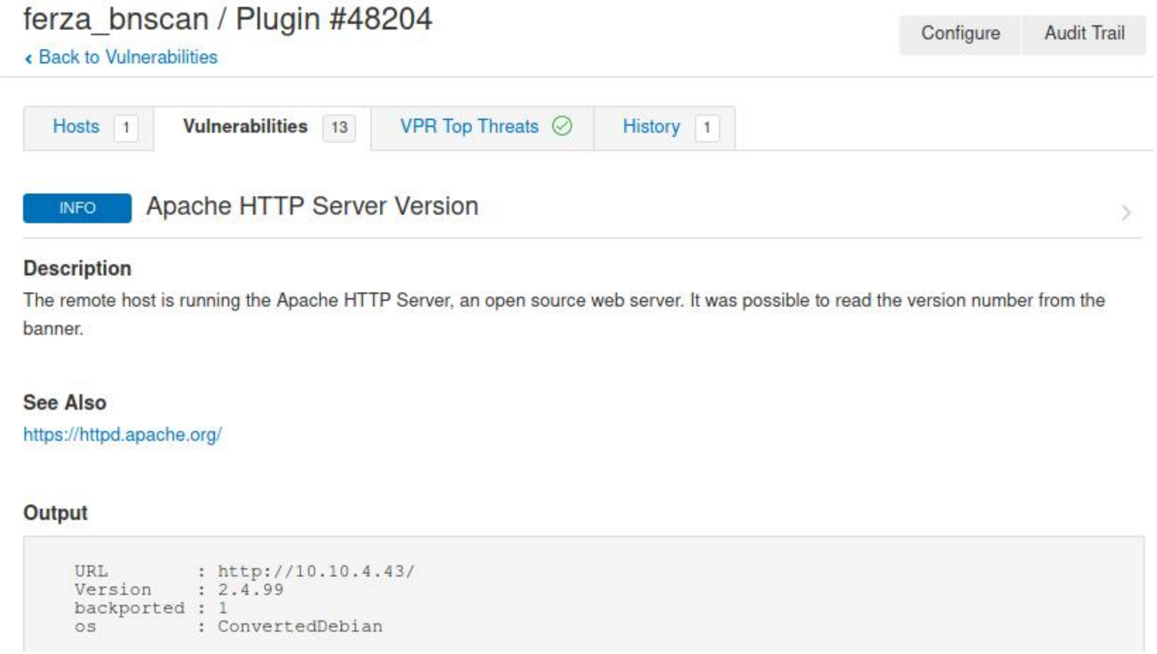
Jawab: nessus SYN scanner
Satu-satunya **vulnerability** yang termasuk **port scanners** dari hasil scan adalah **nessus SYN scanner**.



□ INFO	Nessus SYN scanner	Port scanners	1

What **Apache HTTP Server Version** is reported by Nessus?

Jawab: 2.4.99
Pada plugin #48204, berisi tentang **Apache HTTP Server Version**, berdasarkan keluarkan yang ditampilkan, versi dari Apache HTTP Server adalah 2.4.99.



ferza_bnscan / Plugin #48204

Apache HTTP Server Version

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

See Also

https://httpd.apache.org/

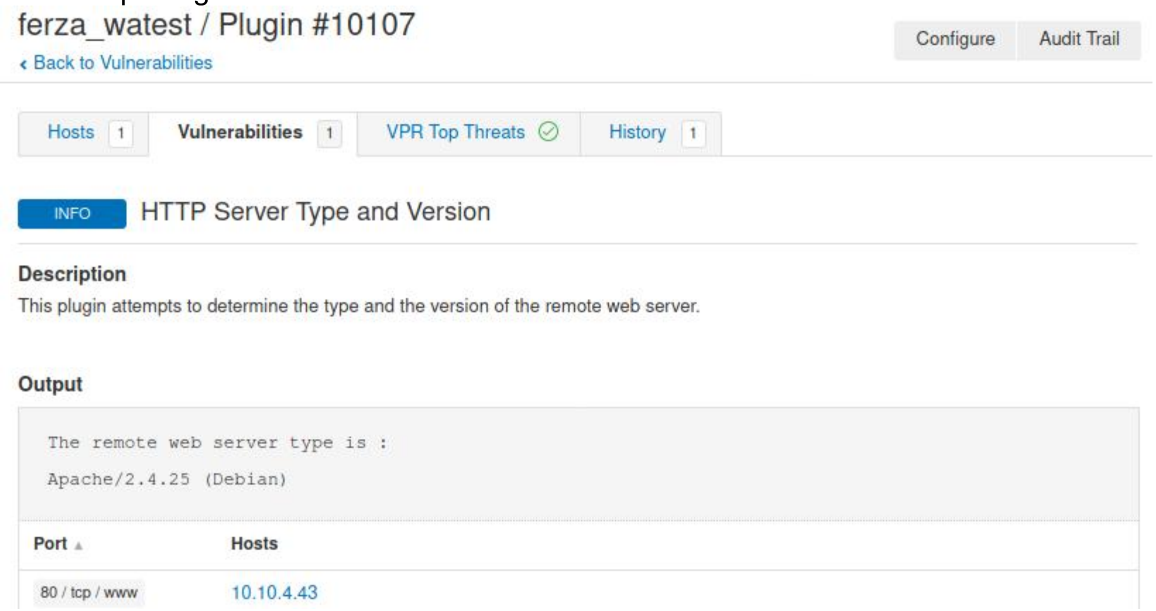
Output

```
  URL        : http://10.10.4.43/
  Version    : 2.4.99
  backported : 1
  os         : ConvertedDebian
```

Task 5: Scanning a Web Application

What is the plugin id of the plugin that determines the HTTP server type and version?

Jawab: 10107
Plugin#10107 berisi mengenai tipe dan versi HTTP server, seperti pada deskripsi dan keluaran pada gambar berikut.



ferza_watest / Plugin #10107

‹ Back to Vulnerabilities

HTTP Server Type and Version

Description

This plugin attempts to determine the type and the version of the remote web server.

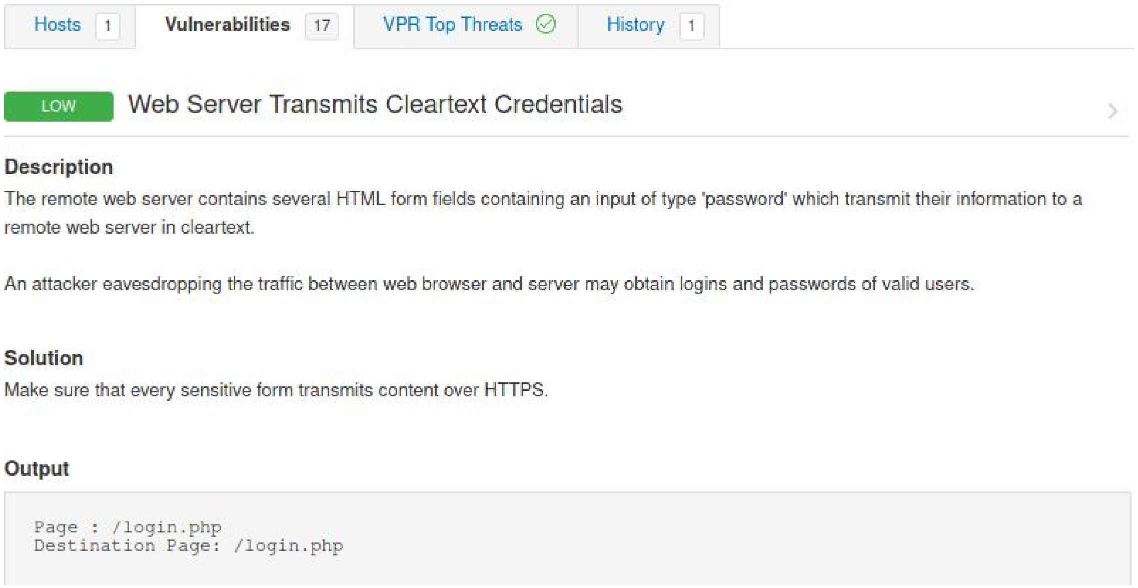
Output

```
The remote web server type is :

Apache/2.4.25 (Debian)
```

Port ▲	Hosts
80 / tcp / www	10.10.4.43

What authentication page is discovered by the scanner that transmits credentials in cleartext?

Jawab: login.php
Login.php adalah halaman autentikasi yang melakukan transmisi kredensial dalam bentuk *cleartext*.



Web Server Transmits Cleartext Credentials

Description

The remote web server contains several HTML form fields containing an input of type 'password' which transmit their information to a remote web server in cleartext.

An attacker eavesdropping the traffic between web browser and server may obtain logins and passwords of valid users.

Solution

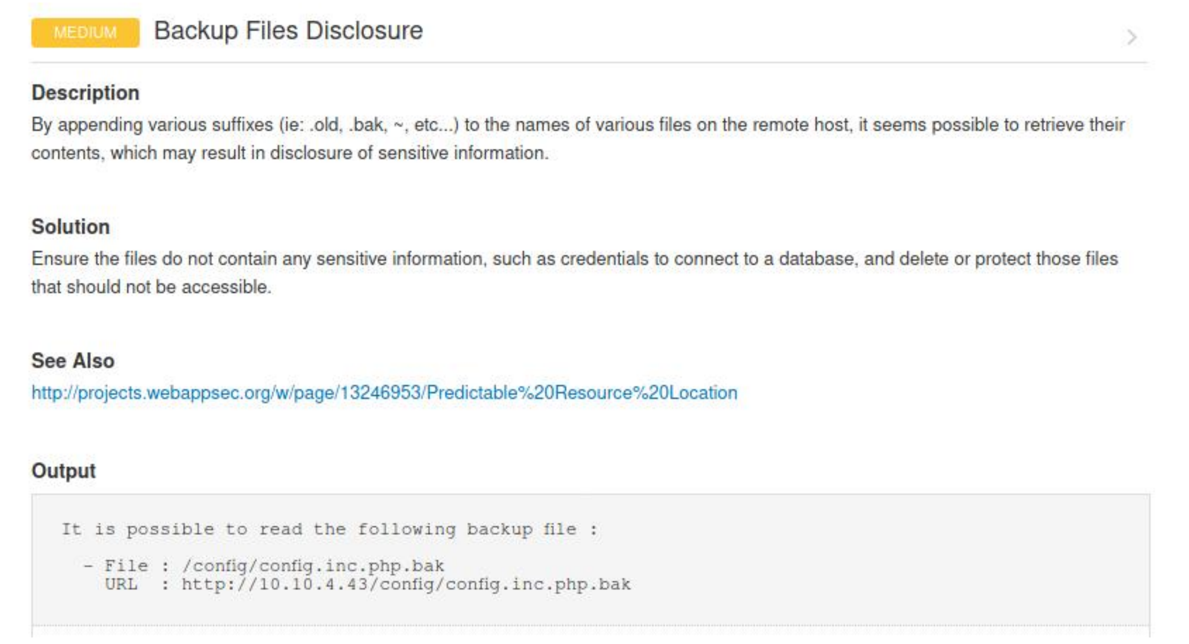
Make sure that every sensitive form transmits content over HTTPS.

Output

```
Page : /login.php
Destination Page: /login.php
```

What is the file extension of the config backup?

Jawab: .bak



MEDIUM Backup Files Disclosure

Description

By appending various suffixes (ie: .old, .bak, ~, etc...) to the names of various files on the remote host, it seems possible to retrieve their contents, which may result in disclosure of sensitive information.

Solution

Ensure the files do not contain any sensitive information, such as credentials to connect to a database, and delete or protect those files that should not be accessible.

See Also

http://projects.webappsec.org/w/page/13246953/Predictable%20Resource%20Location

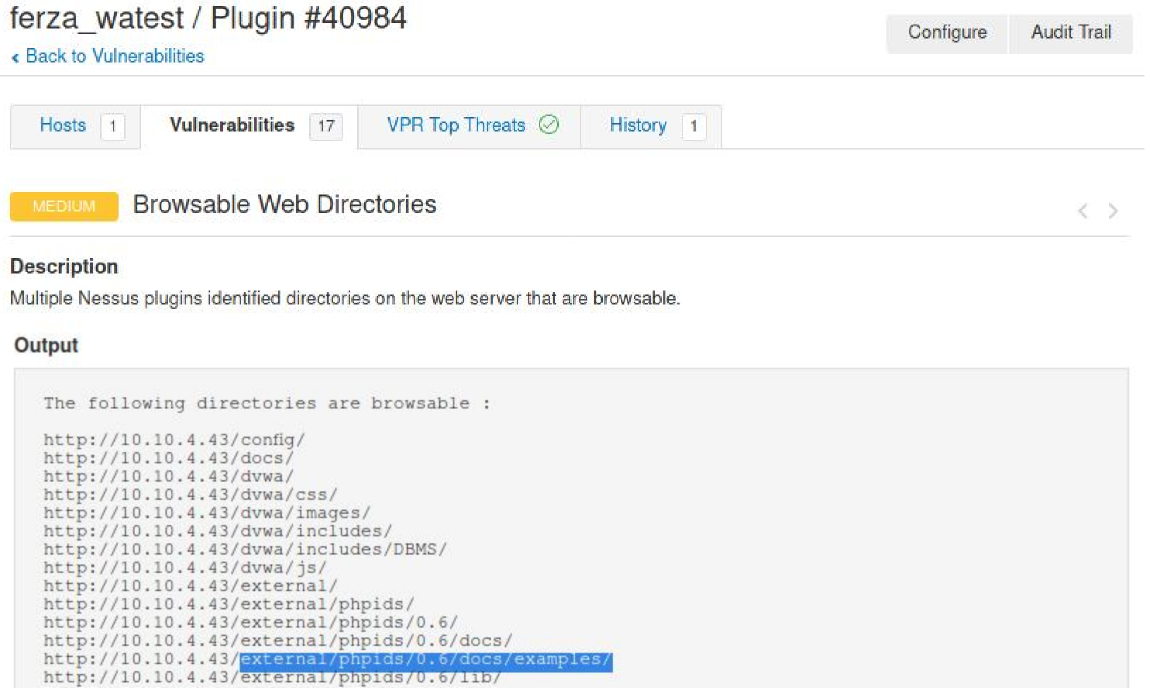
Output

```
It is possible to read the following backup file :

  - File : /config/config.inc.php.bak
    URL  : http://10.10.4.43/config/config.inc.php.bak
```

Which directory contains example documents? (This will be in a php directory)

Jawab: /external/phpids/0.6/docs/examples/

Pada plugin #40984 berisi tentang direktori web yang bisa ditelusuri, salah satunya adalah direktori yang berisi dokumen contoh seperti pada teks yang dipilih di gambar berikut.



ferza_watest / Plugin #40984

‹ Back to Vulnerabilities

MEDIUM Browsable Web Directories

Description

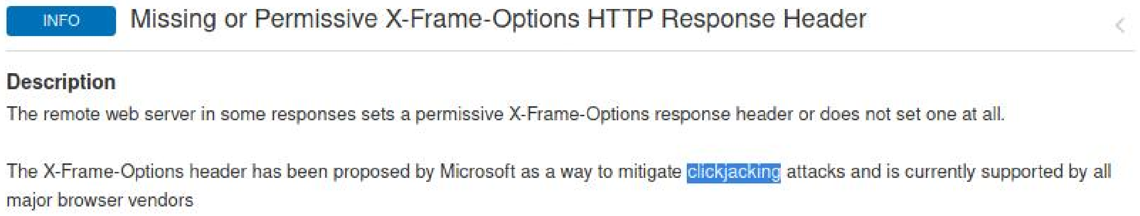
Multiple Nessus plugins identified directories on the web server that are browsable.

Output

```
The following directories are browsable :

http://10.10.4.43/config/
http://10.10.4.43/docs/
http://10.10.4.43/dvwa/
http://10.10.4.43/dvwa/css/
http://10.10.4.43/dvwa/images/
http://10.10.4.43/dvwa/includes/
http://10.10.4.43/dvwa/includes/DBMS/
http://10.10.4.43/dvwa/js/
http://10.10.4.43/external/
http://10.10.4.43/external/phpids/
http://10.10.4.43/external/phpids/0.6/
http://10.10.4.43/external/phpids/0.6/docs/
http://10.10.4.43/external/phpids/0.6/docs/examples/
http://10.10.4.43/external/phpids/0.6/lib/
```

What vulnerability is this application susceptible to that is associated with X-Frame-Options?

Jawab: clickjacking
X-Frame-Options rentan terkena serangan *clickjacking* sehingga Microsoft memberikan Header sebagai langkah untuk mitigasi dari serangan tersebut.



INFO Missing or Permissive X-Frame-Options HTTP Response Header

Description

The remote web server in some responses sets a permissive X-Frame-Options response header or does not set one at all.

The X-Frame-Options header has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors