

1. INTRODUÇÃO

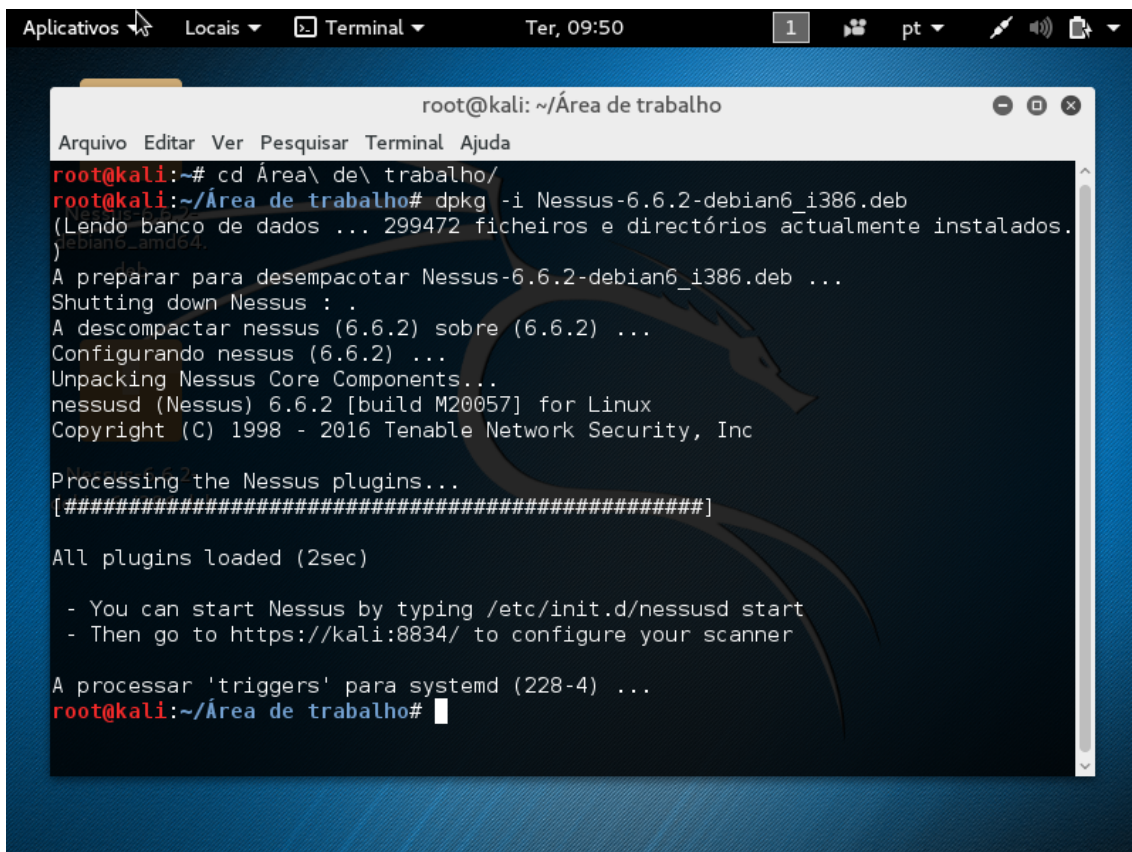
Nessus é um *scanner* de vulnerabilidade desenvolvido pela Tenable Network Security. De acordo com pesquisas feitas em 2009 por sectools.org, Nessus é *scanner* de vulnerabilidade mais popular do mundo. Tenable Network Security estimou no ano de 2005 que foi usado por mais de 75.000 organizações em todo o mundo.

Ele é composto por um cliente e servidor, sendo que o *scan* propriamente dito é feito pelo servidor. O servidor Nessus faz um *port scan* ao computador alvo, depois disso vários *scripts* ligam-se a cada porta aberta para verificar problemas de segurança.

O Projeto "Nessus" foi iniciado por Renaud Deraison em 1998 para fornecer a comunidade um *scanner* de segurança remoto livre. Em 5 de outubro de 2005, Tenable Network Security, a empresa Renaud Deraison co-fundou, mudou Nessus 3 para *software* privado. Ele ainda pode ser adquirido gratuitamente para uso pessoal em um ambiente não-empresarial, sendo compatível com as plataformas Windows, Mac e Linux.

A documentação com especificações e manuais pode ser encontrado no endereço: https://docs.tenable.com/nessus/6_7/index.htm.

1.1 Arquivo de instalação do Nessus sendo descompactado.



A screenshot of a terminal window on a Kali Linux desktop. The window title is "root@kali: ~/Área de trabalho". The terminal shows the command `dpkg -i Nessus-6.6.2-debian6_i386.deb` being executed. The output indicates that the package is being installed, including unpacking core components and processing plugins. The terminal text is as follows:

```
root@kali:~# cd Área\ de\ trabalho/
root@kali:~/Área de trabalho# dpkg -i Nessus-6.6.2-debian6_i386.deb
(Lendo banco de dados ... 299472 ficheiros e directórios actualmente instalados.
)
A preparar para descompactar Nessus-6.6.2-debian6_i386.deb ...
Shutting down Nessus : .
A descompactar nessus (6.6.2) sobre (6.6.2) ...
Configurando nessus (6.6.2) ...
Unpacking Nessus Core Components...
nessusd (Nessus) 6.6.2 [build M20057] for Linux
Copyright (C) 1998 - 2016 Tenable Network Security, Inc

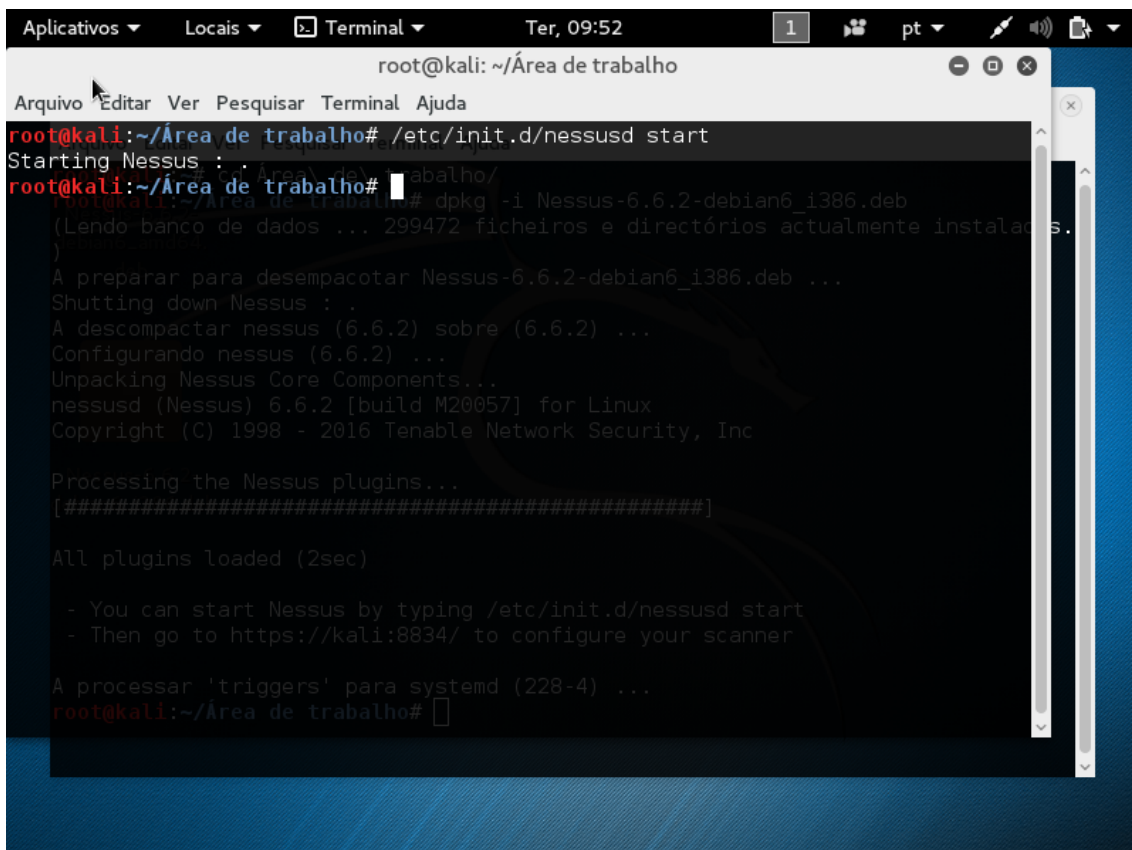
Processing the Nessus plugins...
[#####]

All plugins loaded (2sec)

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

A processar 'triggers' para systemd (228-4) ...
root@kali:~/Área de trabalho#
```

1.2 Iniciando o serviço com o comando: "nessusd start".

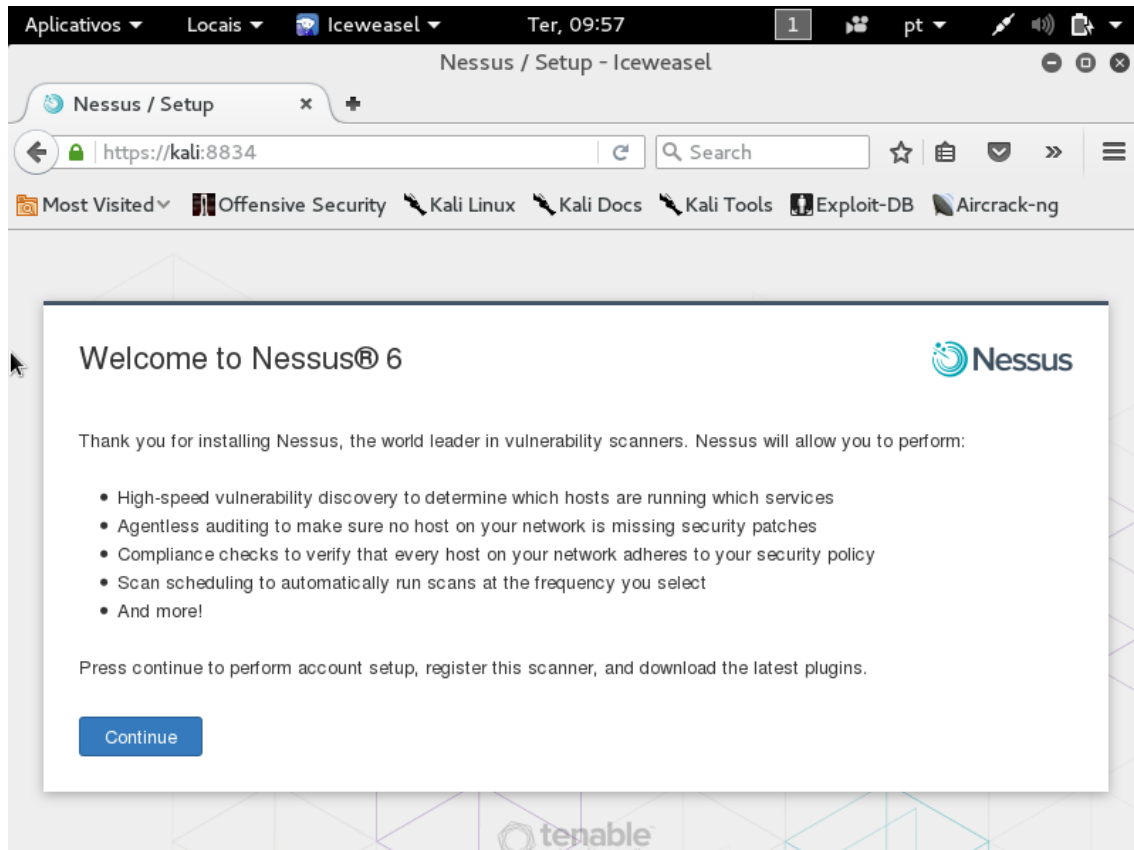


A screenshot of a terminal window on a Kali Linux desktop, showing the start of the Nessus service. The window title is "root@kali: ~/Área de trabalho". The terminal shows the command `/etc/init.d/nessusd start` being executed. The output indicates that the service is starting. The terminal text is as follows:

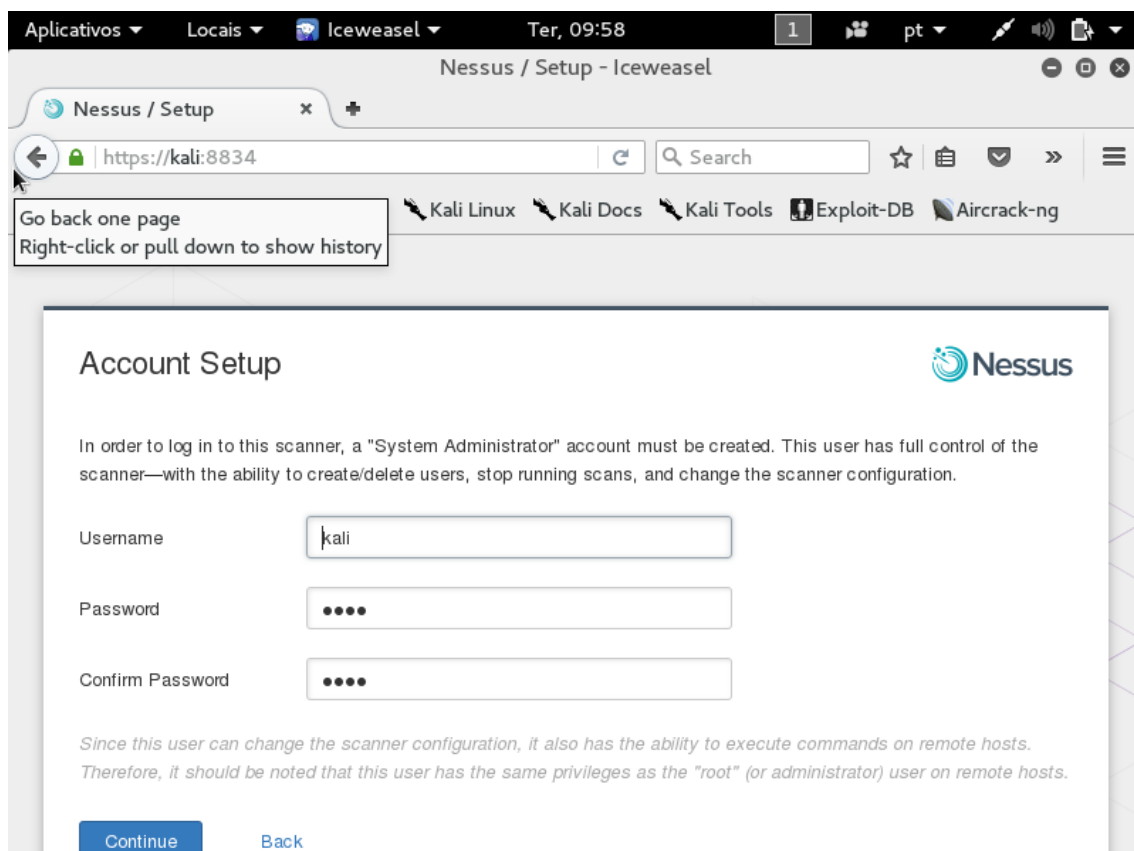
```
root@kali:~/Área de trabalho# /etc/init.d/nessusd start
Starting Nessus : .
root@kali:~/Área de trabalho#
```

The terminal also shows the installation output from the previous step, including the unpacking of core components and the processing of plugins.

1.3 Tela inicial Nessus



2. Criando a conta



3. Ativação

The screenshot shows a web browser window with the title "Nessus / Setup - Iceweasel". The address bar shows "https://kali:8834". The page is titled "Product Registration" and features the Nessus logo. A paragraph explains that Tenable's research staff releases plugins to detect vulnerabilities. Below the text, there are two input fields: "Registration" with a dropdown menu showing "Nessus (Home, Professional or Manager)" and "Activation Code" with the text "C2D2-7F0E-28AC-9141-9D10". At the bottom, there are three buttons: "Continue" (highlighted with a mouse cursor), "Back", and "Custom Settings". A loading spinner is visible in the bottom left corner of the registration box.

Product Registration

As information about new vulnerabilities is discovered and released into the public domain, Tenable's research staff releases plugins that enable Nessus to detect their presence. These plugins contain vulnerability information, algorithms to test for the presence of the issue, and a set of remediation actions. [Registering this scanner](#) will grant you access to download these plugins.

Registration: Nessus (Home, Professional or Manager)

Activation Code: C2D2-7F0E-28AC-9141-9D10

Continue Back Custom Settings

4. Fazendo o Login:

The screenshot shows a web browser window with the title "Nessus / Login - Iceweasel". The address bar shows "https://kali:8834/#/". The page is titled "Nessus home" and features the Nessus logo. There are two input fields: a username field with the text "kali" and a password field with four dots. Below the password field, there is a checkbox labeled "Remember Me" and a "Sign In" button. The Tenable logo is visible in the bottom right corner of the page.

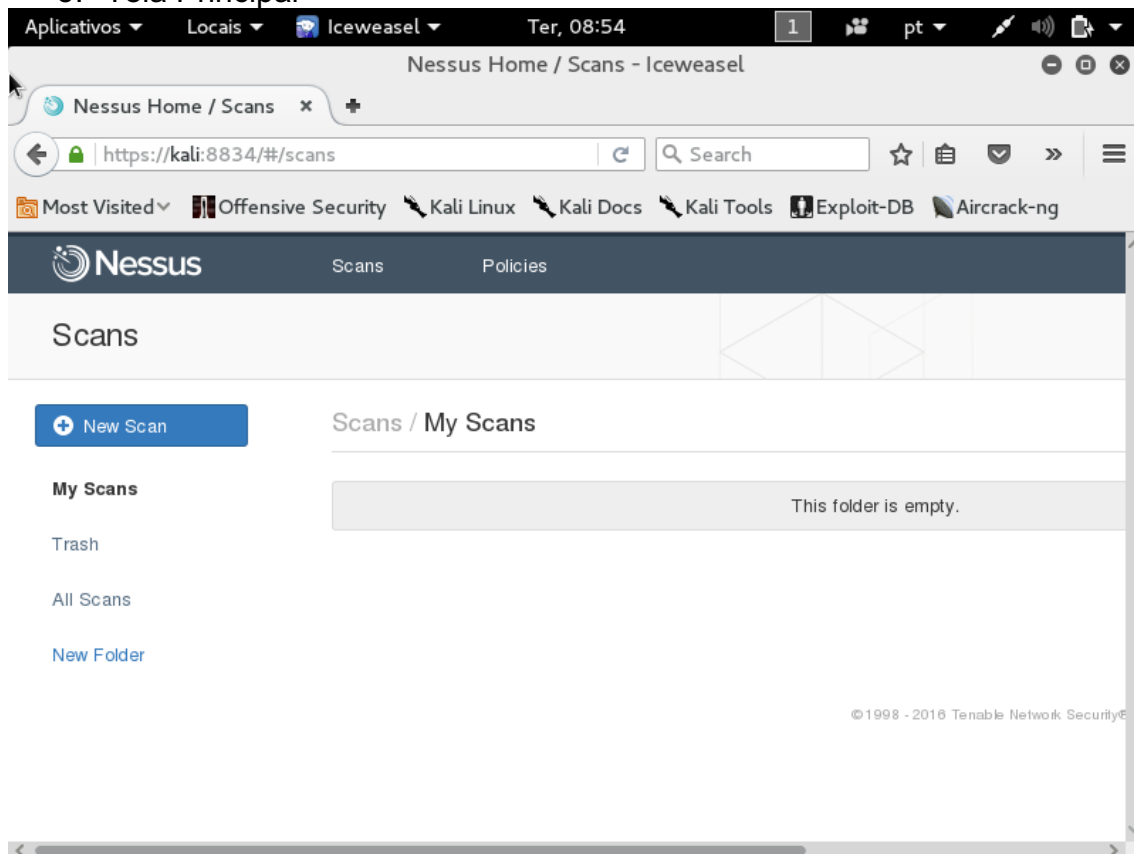
Nessus home

Username: kali

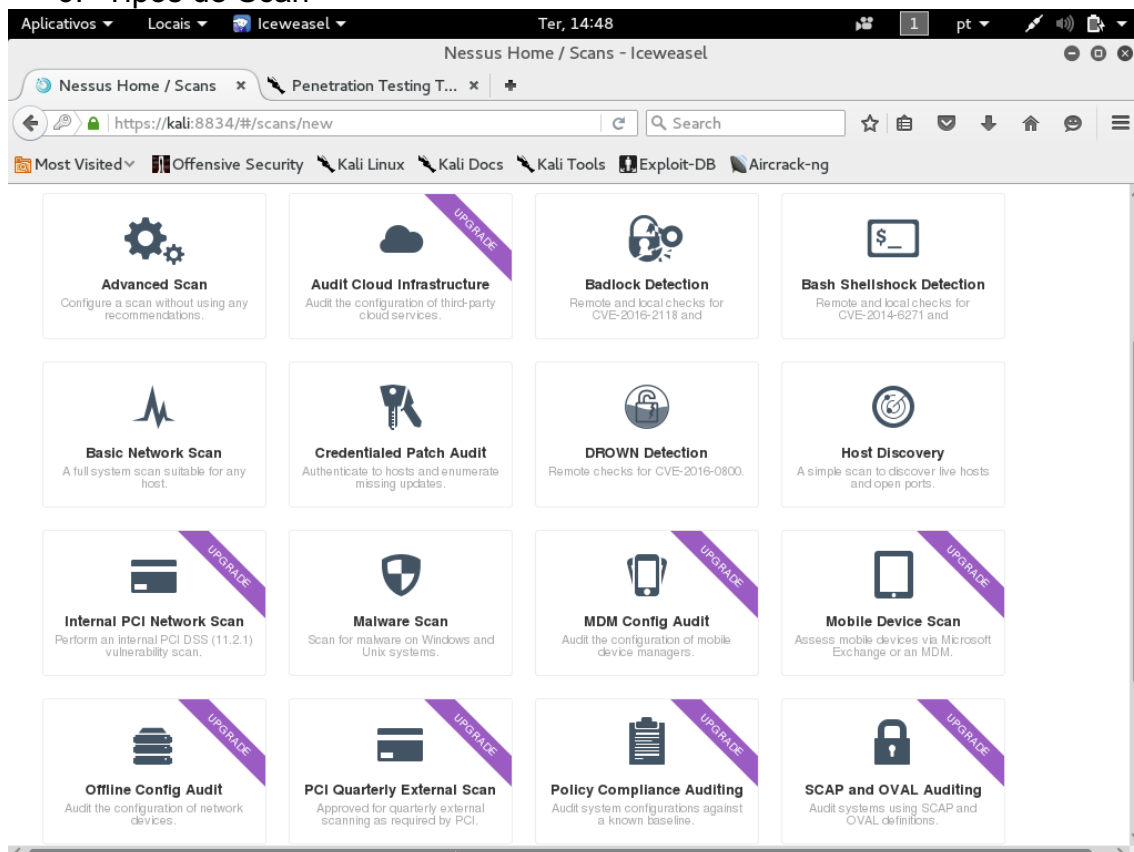
Password:

☐ Remember Me Sign In

5. Tela Principal



6. Tipos de Scan



7. Seleccionamos Basic Scan Network.

The screenshot shows the Nessus Editor interface in a web browser. The browser's address bar displays the URL `https://kali:8834/#/scans/new/731a8e52-3ea6-a291-ec0a-d2ff`. The page title is "Nessus Home / Scans / Editor - Iceweasel". The left sidebar contains a menu with sections: "BASIC" (with a green checkmark), "General", "Schedule", "Notifications", "DISCOVERY", "ASSESSMENT", "REPORT", and "ADVANCED". The main content area is titled "Settings / Basic / General" and contains the following fields:

- Name:** A text input field containing "BasicScan".
- Description:** A text input field containing "Basic Scan".
- Folder:** A dropdown menu currently showing "My Scans".
- Targets:** A large text area containing the IP range "192.168.0.1-192.168.0.5".

Below the targets field, there are links for "Upload Targets" and "Add File". At the bottom of the form, there are "Save" and "Cancel" buttons.

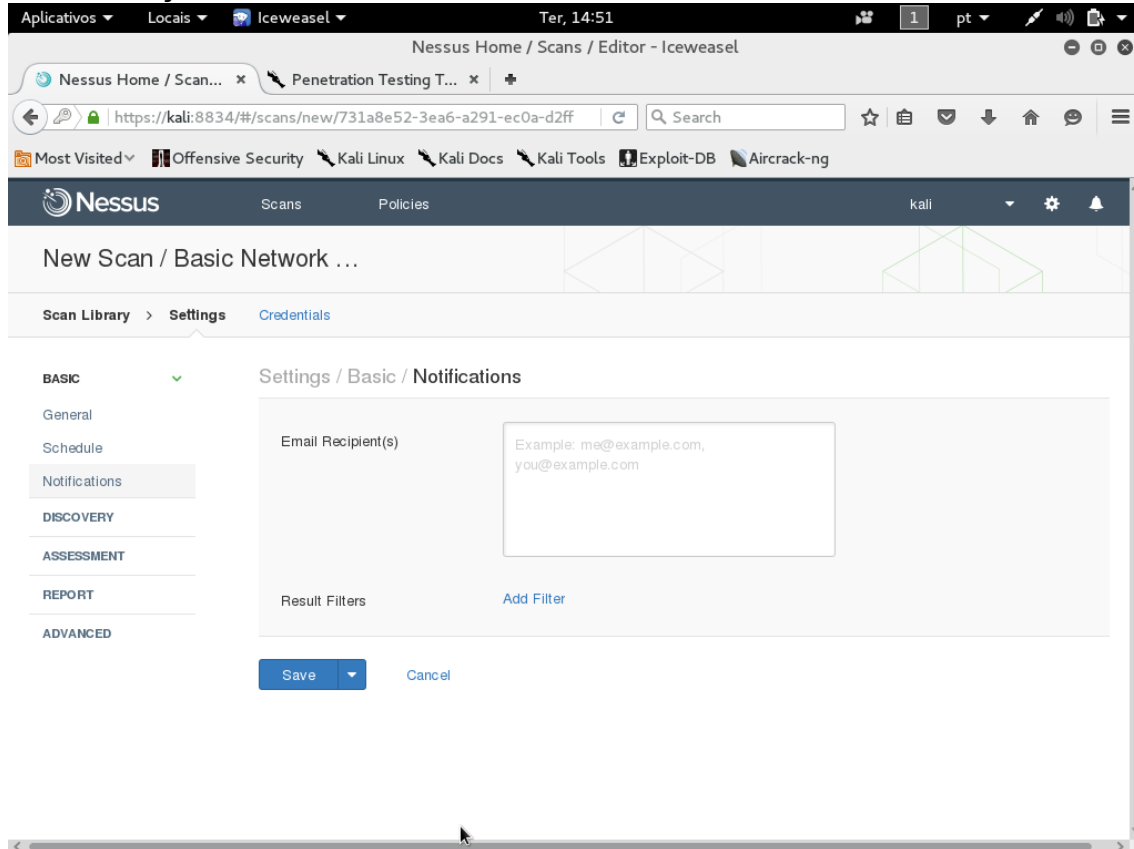
8. Cronograma.

The screenshot shows the Nessus Editor interface in a web browser. The browser's address bar displays the URL `https://kali:8834/#/scans/new/731a8e52-3ea6-a291-ec0a-d2ff`. The page title is "Nessus Home / Scans / Editor - Iceweasel". The left sidebar contains a menu with sections: "BASIC" (with a green checkmark), "General", "Schedule", "Notifications", "DISCOVERY", "ASSESSMENT", "REPORT", and "ADVANCED". The main content area is titled "Settings / Basic / Schedule" and contains the following field:

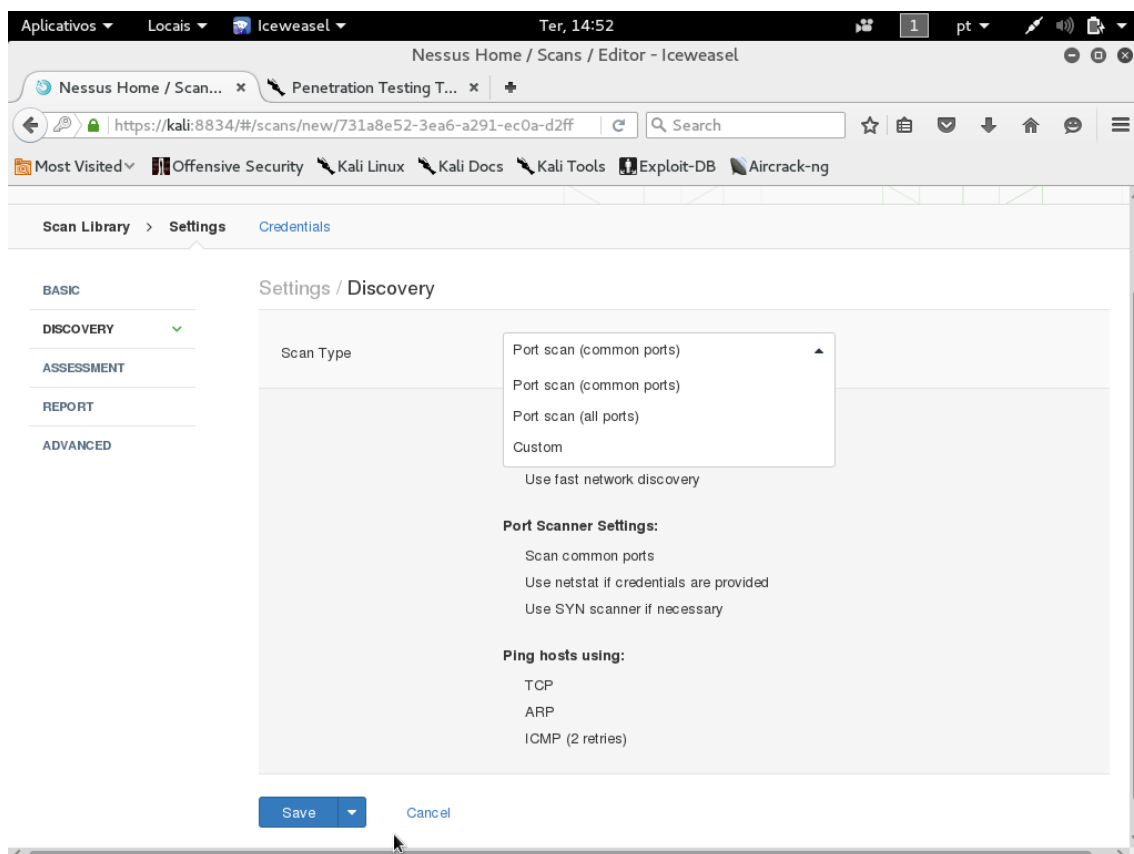
- Enable Schedule:** A toggle switch currently set to "Off".

Below the toggle switch, there are "Save" and "Cancel" buttons.

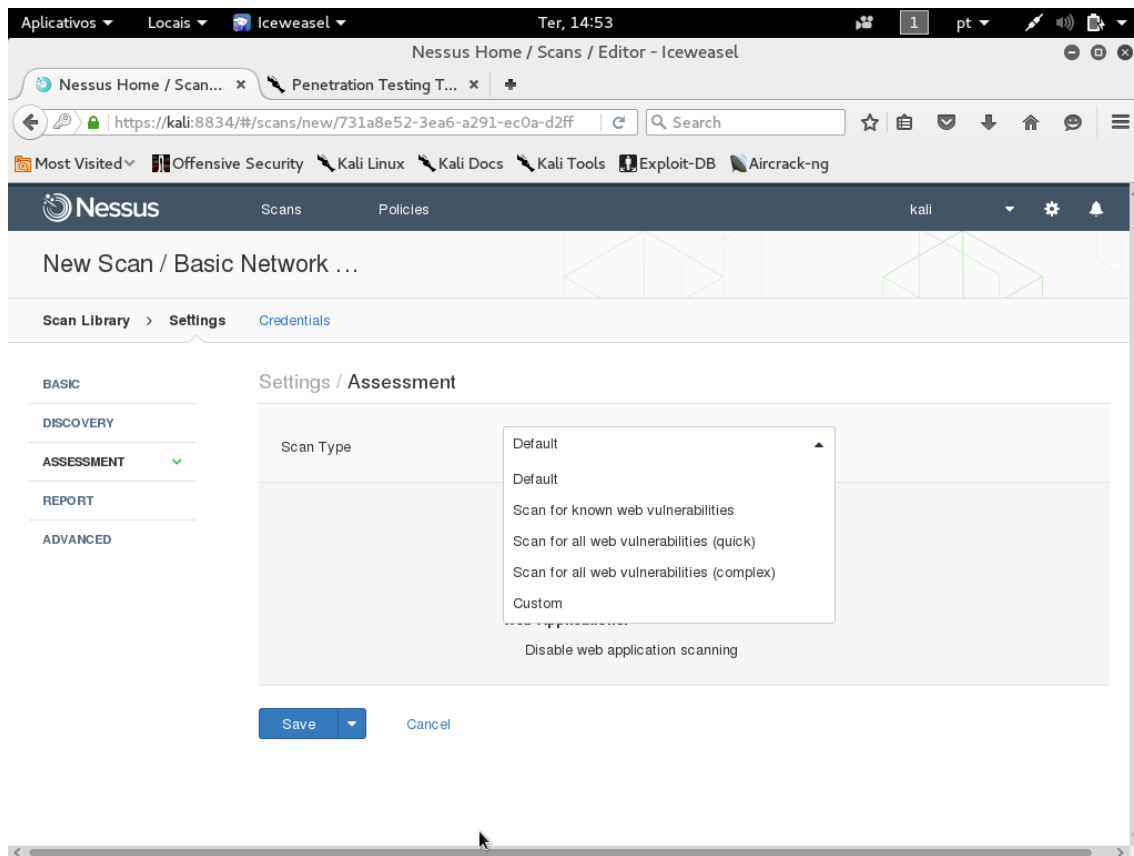
9. Função enviar resultados via email



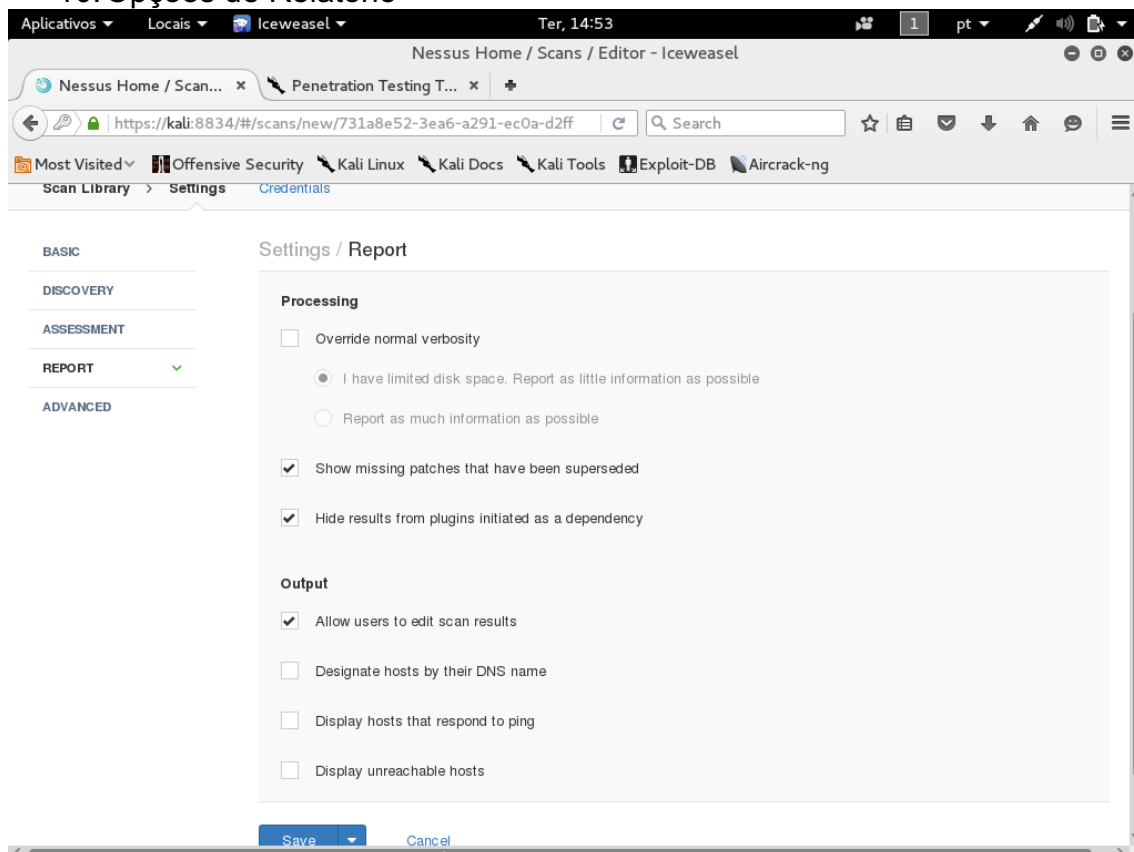
9.1 Formas de scanear básico



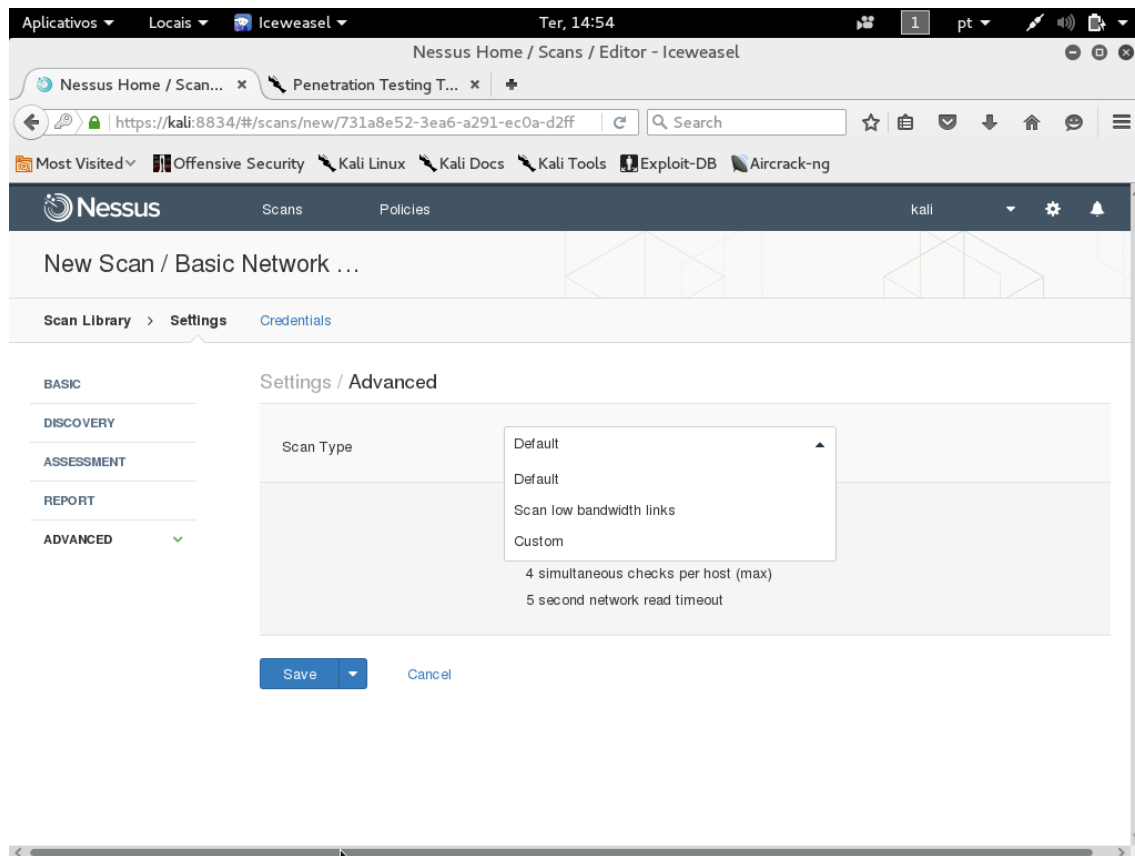
9.2 Scan tipo básico



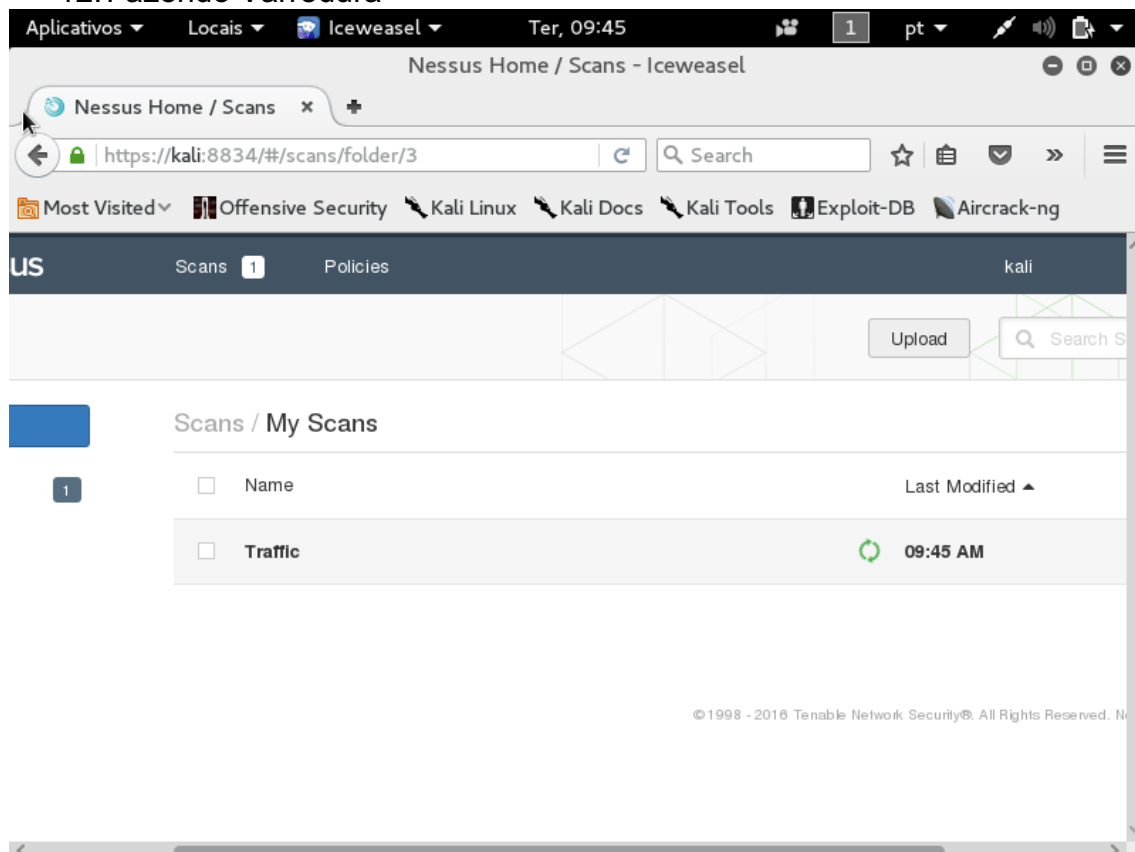
10. Opções de Relatório



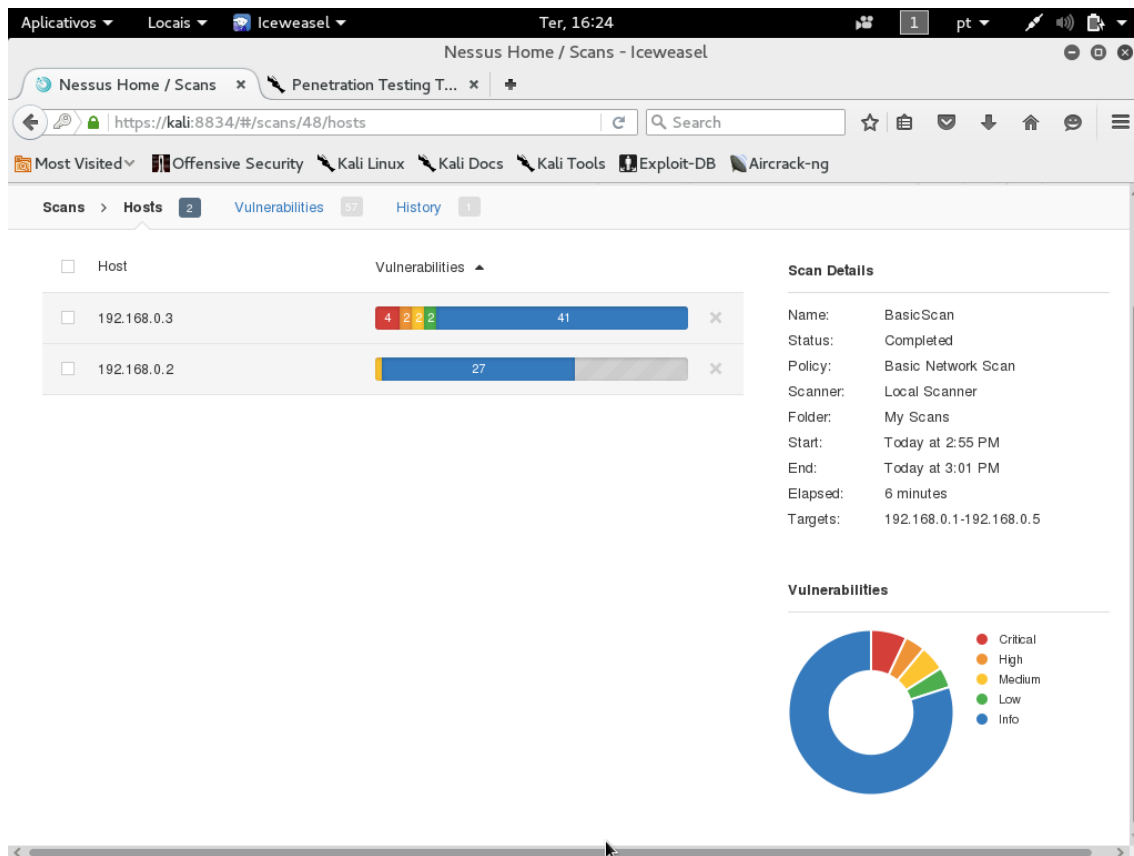
11. Opções avançadas



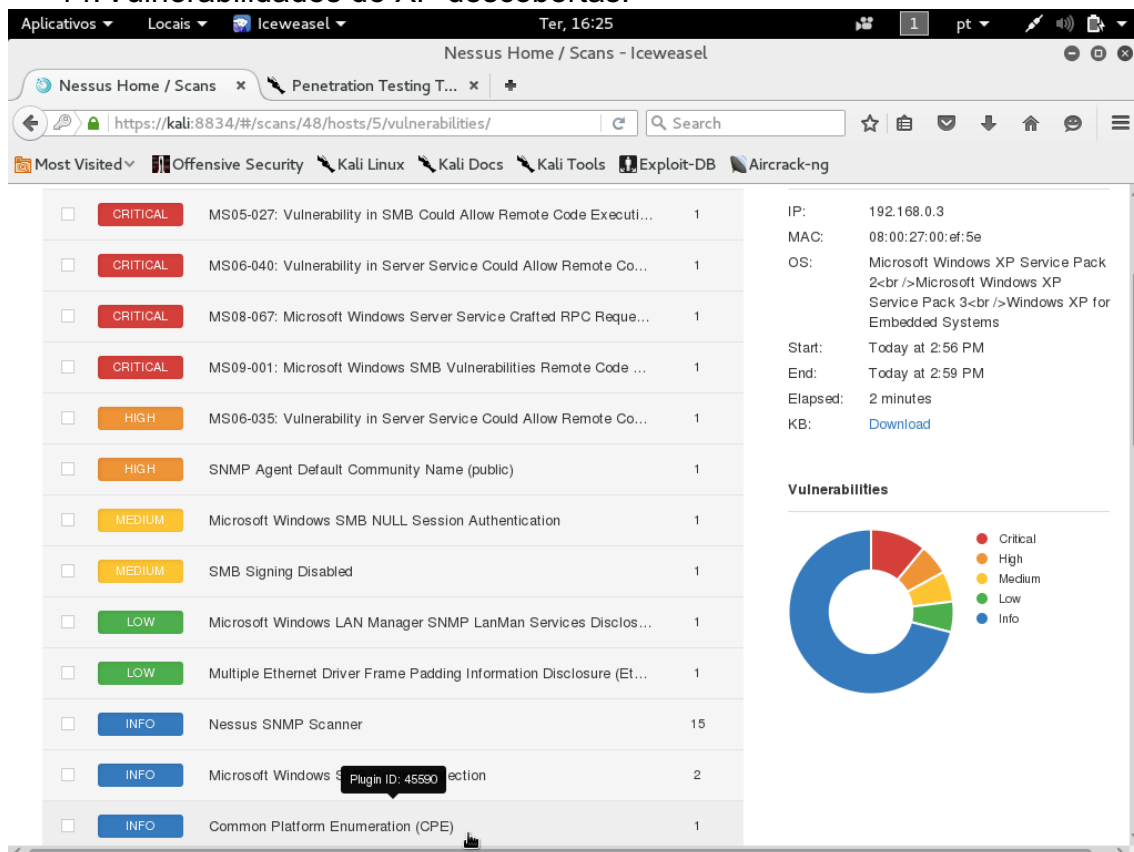
12. Fazendo Varredura



13. Visualizando os Resultados.



14. Vulnerabilidades do XP descobertas.



15. Vulnerabilidades do Kali Linux

