



# OpenVAS: Open Vulnerability Assessment Scanner

**Davi Augusto Neves Leite**

**Giovani Candido**

**Luis Henrique Morelli**

**Luiz Fernando Merli de Oliveira Sementille**

**191027383**

**191021601**

**181027097**

**191021032**

**Prof. Dr. Kelton Pontara da Costa**

**Segurança de Sistemas da Informação**

# Sumário da Apresentação

01

## Sobre o OpenVAS

Um pouco sobre sua história, arquitetura e serviços

Como instalar a ferramenta para Kali Linux e problemas que podem ser encontrados

## Instalação

02

03

## Testes

Testes realizados utilizando as máquinas virtuais

Sites usados para aprender como instalar e utilizar corretamente a ferramenta

## Referências

04

# 01

## Sobre o OpenVAS

O que é o “Open Vulnerability Assessment Scanner”?



# Linha do tempo



# OpenVAS Scanner

## O que é?

Um mecanismo de varredura completo de vulnerabilidades

## Como ele faz?

Utiliza feeds abrangentes e atualizados diariamente de coleções de NVTs



# Greenbone

## O que ele faz?

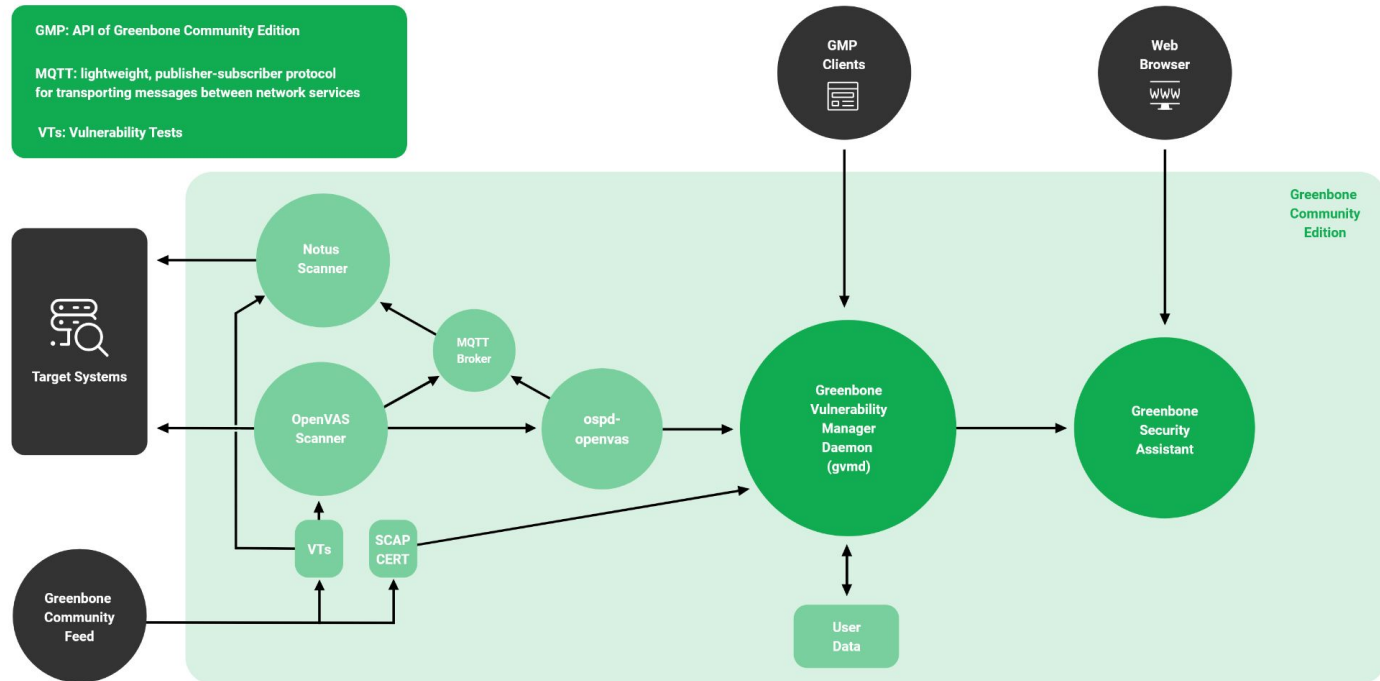
Executa Testes de Vulnerabilidade de Rede (NVTs) nos sistemas de destino

## Qual a vantagem?

Garante integridade e segurança, com coleções em constante crescimento e sincronizadas aos servidores

# OpenVAS Scanner: Arquitetura do GVM

## Greenbone Community Edition 22.04 Architecture



# Componentes do OpenVAS Scanner



## **ospd-openvas**

Implementação em servidor utilizando o protocolo OSP para controle remoto da ferramenta OpenVAS Scanner

## **openvas-scanner**

Executa rotinas que verificam a presença de um problema de segurança específico, conhecidos ou em potencial



# Open Server Protocol





# Opções da Interface Gráfica

## Scan Management

Permite criar novas tarefas de verificação, modificar as que foram criadas anteriormente, revisar as notas ou substituir

## Asset Management

Lista os hosts analisados, junto com o número de vulnerabilidades identificadas

## Configuration

Permite configurar os alvos, atribuir credenciais de acesso para revisões de segurança locais, configurar e agendar verificações, configurar a geração de relatórios

## Extras

Mostra informações sobre as opções de configuração, desempenho ou gerenciamento de segurança de informações do OpenVAS

# Serviços



## OpenVAS Manager

O OpenVAS Manager é o serviço que executa tarefas como filtragem ou classificação dos resultados da análise



## OpenVAS Scanner

O OpenVAS Scanner é o responsável por executar os Testes de Vulnerabilidade de Rede

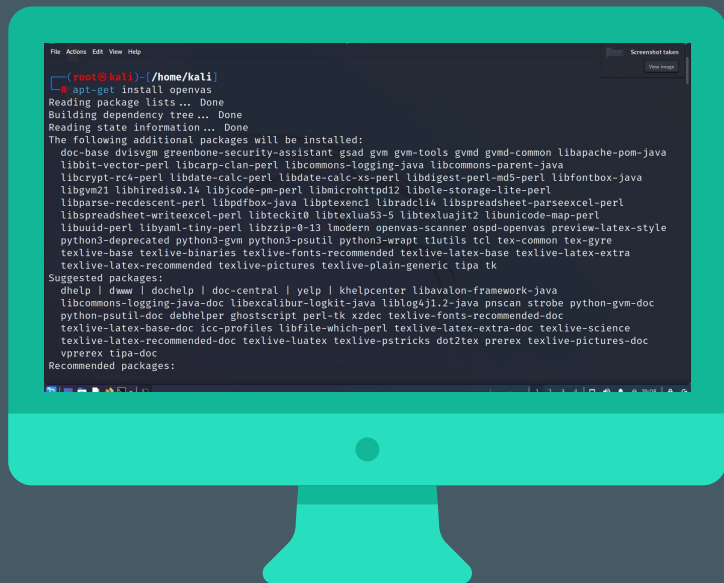


# 02 Instalação e Desafios

Problemas enfrentados na  
instalação da ferramenta

# Kali-Linux

## Comandos

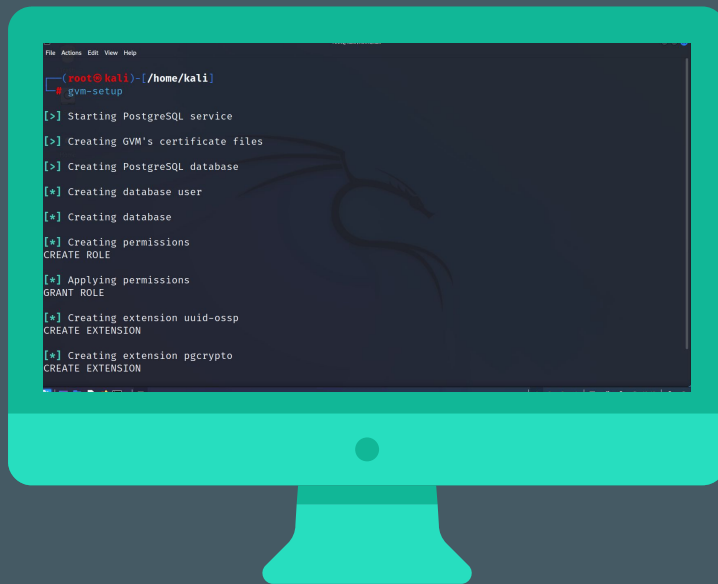


- **sudo su** (ou use **sudo** para cada comando a seguir): entrar no modo root
- Após entrar no modo **root**:
  - **apt-get update && apt-get upgrade -y && apt-get autoremove -y**: atualizar todos os repositórios e pacotes do sistema
  - **apt-get install openvas**: instalação da base do OpenVAS, mas não da ferramenta em si

# Kali-Linux

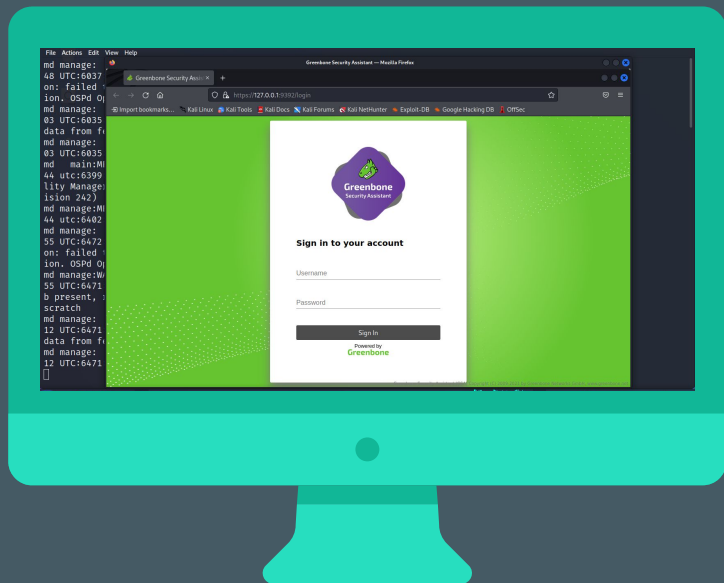
## Comandos

- Por fim, execute o **gvm-setup**, o qual instala o OpenVAS e suas dependências, configurando o scanner
- Após a instalação, **salve a senha** mostrada no terminal. O usuário associado é **"admin"**.
- Necessário realizar a sincronização com o banco de dados da ferramenta, por meio de:
  - `greenbone-feed-sync --type GVMMD_DATA`
  - `greenbone-feed-sync --type SCAP`
  - `greenbone-feed-sync --type CERT`



# Kali-Linux

## Comandos

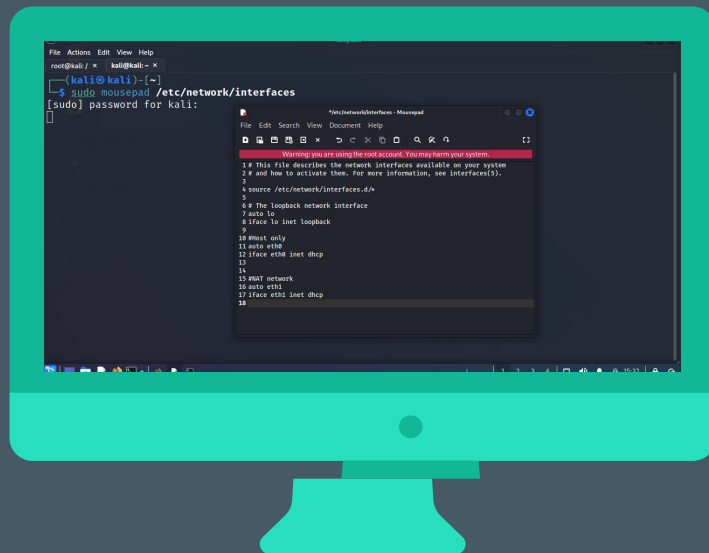


- Após isso, reinicie a ferramenta por meio dos comandos:
  - `gvm-stop`
  - `gvm-start`
- Acesse o endereço “**127.0.0.1:9392**” pelo navegador e entre no sistema da GVM
- O arquivo de log de execução do GVM pode ser visto com os comandos:
  - `tail -f /var/log/gvm/gvmd.log`

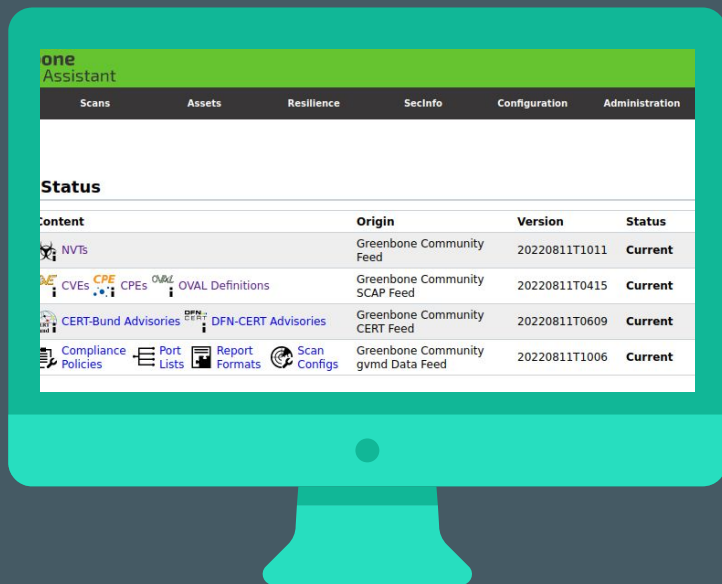
# Kali-Linux

## Alguns problemas encontrados

- Configuração das interfaces de redes da VirtualBox
  - O que é?
    - O Kali-Linux não consegue se conectar nas duas interfaces “Ethernet” simultaneamente.
  - Como resolver?
    - Aplique o comando “`sudo mousepad /etc/network/interfaces`” e acrescente as seguintes linhas (sem a numeração):
      1. `#Host only`
      2. `auto eth0`
      3. `iface eth0 inet dhcp`
      - 4.
      5. `#NAT network`
      6. `auto eth1`
      7. `iface eth1 inet dhcp`
    - Reinicie a máquina virtual. Caso ainda não funcione, retire as linhas que adicionou acima e reinicie novamente.



# Kali-Linux



## Alguns problemas encontrados

- Falha ao iniciar ou executar tarefa de "Scan" (ou qualquer outra)
  - O que é?
    - Basicamente, o GVM não consegue executar quaisquer de seus módulos.
  - Como resolver?
    - Execute os comandos de sincronização por meio de `sudo gvm-feed-update` e verifique seus status em: <https://127.0.0.1:9392/feedstatus> e com o comando `tail -f /var/log/gvm/gvmd.log`.
    - É necessário que estejam com status de "Current".



# 03

## Testes

Analizando as vulnerabilidades de  
um Windows 7 por meio da  
VirtualBox



# Pré-Requisitos

- Configurar duas máquinas virtuais, sendo uma com Kali-Linux e a outra com Windows 7, utilizando as seguintes configurações de rede:

Adaptador 1	Adaptador 2	Adaptador 3	Adaptador 4
✓ Habilitar Placa de Rede			
Conectado a: Rede Interna			
Nome: intnet			
▼ Avançado (D)			
Tipo de Placa: Intel PRO/1000 MT Desktop (82540EM)			
Modo Promíscuo: Recusar			
Endereço MAC: 08002700B4A1			
✓ Cabo conectado			

Adaptador 1	Adaptador 2	Adaptador 3	Adaptador 4
✓ Habilitar Placa de Rede			
Conectado a: Placa em modo Bridge			
Nome: wlp3s0			
▼ Avançado (D)			
Tipo de Placa: Intel PRO/1000 MT Desktop (82540EM)			
Modo Promíscuo: Recusar			
Endereço MAC: 0800270E8AB7			
✓ Cabo conectado			

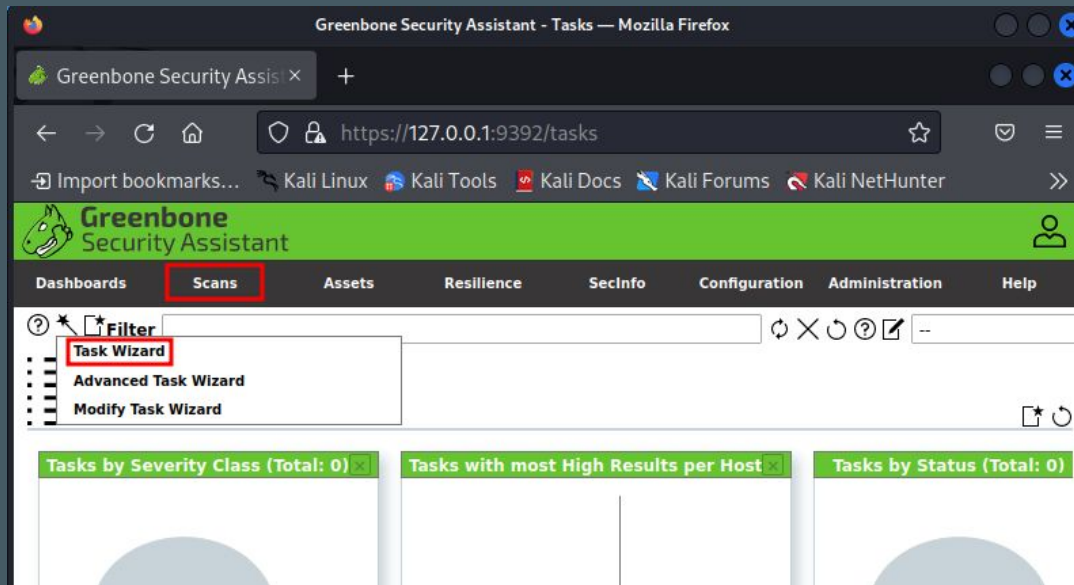
## Pré-Requisitos

- Realizar as configurações de **IP** e **Gateway** do “Ethernet 1” (relativo ao adaptador de Rede Interna “*intnet*” do VirtualBox) para ambos os sistemas operacionais, como mostradas na tabela abaixo:

Sistema Operacional	IP	Gateway
Linux	192.168.10.1	255.255.255.0
Windows	192.168.10.2	255.255.255.0

# Criar nova tarefa de “Scan”

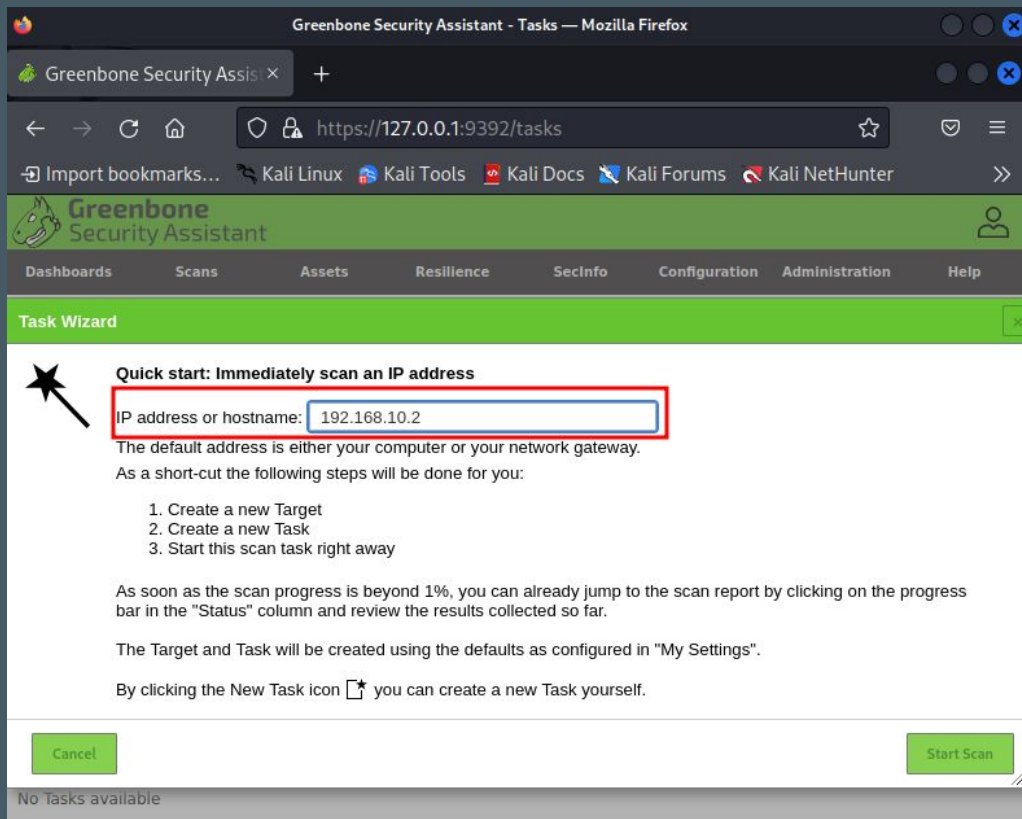
- Seguindo os passos do capítulo 2, aperte na aba de “Scans” no segundo botão da barra superior de tarefas do GVM



## Criar nova tarefa de “Scan”

- Com a tela de “Scans” aberta, crie uma nova tarefa por meio do segundo botão na aba “Task Wizard” ou na aba “Advanced Task Wizard”.
- Com a máquina virtual do Windows 7 aberta, coloque o seu respectivo IP no campo de entrada de texto, ou seja, “192.168.10.2” e deixe os outros campos padrões.
  - Caso esteja na “Advanced Task Wizard”, coloque o endereço IP em “Target Host”.

# Criar nova tarefa de "Scan"



The screenshot shows the Greenbone Security Assistant web interface in a Mozilla Firefox browser. The address bar shows the URL `https://127.0.0.1:9392/tasks`. The interface has a green header with the Greenbone logo and a navigation menu with items: Dashboards, Scans, Assets, Resilience, Secinfo, Configuration, Administration, and Help. Below the header is a green bar labeled 'Task Wizard'. The main content area is titled 'Quick start: Immediately scan an IP address' and features a star icon. A red box highlights the 'IP address or hostname:' input field, which contains the value '192.168.10.2'. Below this, text explains that the default address is either the user's computer or network gateway and lists three steps: 1. Create a new Target, 2. Create a new Task, and 3. Start this scan task right away. Further text states that once the scan progress is beyond 1%, users can jump to the scan report. It also mentions that the Target and Task will be created using defaults from 'My Settings'. At the bottom, it says that clicking the New Task icon (a square with a star) allows users to create a new Task themselves. At the bottom of the wizard, there are two green buttons: 'Cancel' and 'Start Scan'. A status bar at the very bottom indicates 'No Tasks available'.

Greenbone Security Assistant - Tasks — Mozilla Firefox

Greenbone Security Assis x +


https://127.0.0.1:9392/tasks

Import bookmarks... Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter

Greenbone Security Assistant

Dashboards Scans Assets Resilience Secinfo Configuration Administration Help

Task Wizard

 **Quick start: Immediately scan an IP address**

IP address or hostname: 192.168.10.2


The default address is either your computer or your network gateway.

As a short-cut the following steps will be done for you:

1. Create a new Target
2. Create a new Task
3. Start this scan task right away

As soon as the scan progress is beyond 1%, you can already jump to the scan report by clicking on the progress bar in the "Status" column and review the results collected so far.

The Target and Task will be created using the defaults as configured in "My Settings".


By clicking the New Task icon  you can create a new Task yourself.

Cancel Start Scan

No Tasks available

# Criar nova tarefa de "Scan"

Advanced Task Wizard



**Quick start: Create a new task**

This wizard can help you by creating a new scan task and automatically starting it.

All you need to do is enter a name for the new task and the IP address or host name of the target, and select a scan configuration.

You can choose, whether you want to run the scan immediately, schedule the task for a later date and time, or just create the task so you can run it manually later.

In order to run an authenticated scan, you have to select SSH and/or SMB credentials, but you can also run an unauthenticated scan by not selecting any credentials. If you enter an email address in the "Email report to" field, a report of the scan will be sent to this address once it is finished.

For any other setting the defaults from "My Settings" will be applied.

**Task Name**

Windows 7

**Scan Config**

daba56c8-73ec-11df-a47! ▼

**Target Host(s)**

192.168.10.2

☒ Start immediately

☐ Create Schedule:

08/10/2022 ...

at 17 h 20 m

Coordinated Universal Time/UTC ▼

☐ Do not start automatically

**SSH Credential**

-- ▼ on port 22

**SMB Credential**

-- ▼

**ESXi Credential**

-- ▼

**Email report to**

Cancel

Create

# Modos de Operação do Scan

- O **Scan** possui os seguintes modos de operação (ou configuração):

<b>Base</b>	Apenas VTs que coletam informações sobre o sistema de destino, não analisando nenhuma vulnerabilidade. Utiliza a porta <i>Ping Host</i> , a qual detecta se um host está ativo.
<b>Discovery</b>	Obtém informações sobre portas abertas, hardware usado, firewalls, serviços usados, software instalado e certificados. Assim como o <i>Base</i> , não analisa vulnerabilidade.
<b>Empty</b>	Não contém VTs. Utilizado para criar uma configuração personalizável de análise.
<b>Full and Fast</b>	Opção principal que utiliza quase todos os VTs para analisar as vulnerabilidades possíveis do sistema de destino.
<b>Host Discovery</b>	Utilizada para detectar sistemas de destino. Não analisa vulnerabilidades.
<b>Log4Shell</b>	Utilizado para detectar aplicações com a vulnerabilidade do tipo <i>Log4j</i> .
<b>System Discovery</b>	Utilizada para detectar sistemas de destino, com a inclusão de sistemas operacionais instalados e hardware utilizado. Não analisa vulnerabilidades.



# Criar nova tarefa de “Scan”: modo de configuração

Task Name: Windows 7

Scan Config: Full and fast ▲

Target Host(s):

Start Time:  m

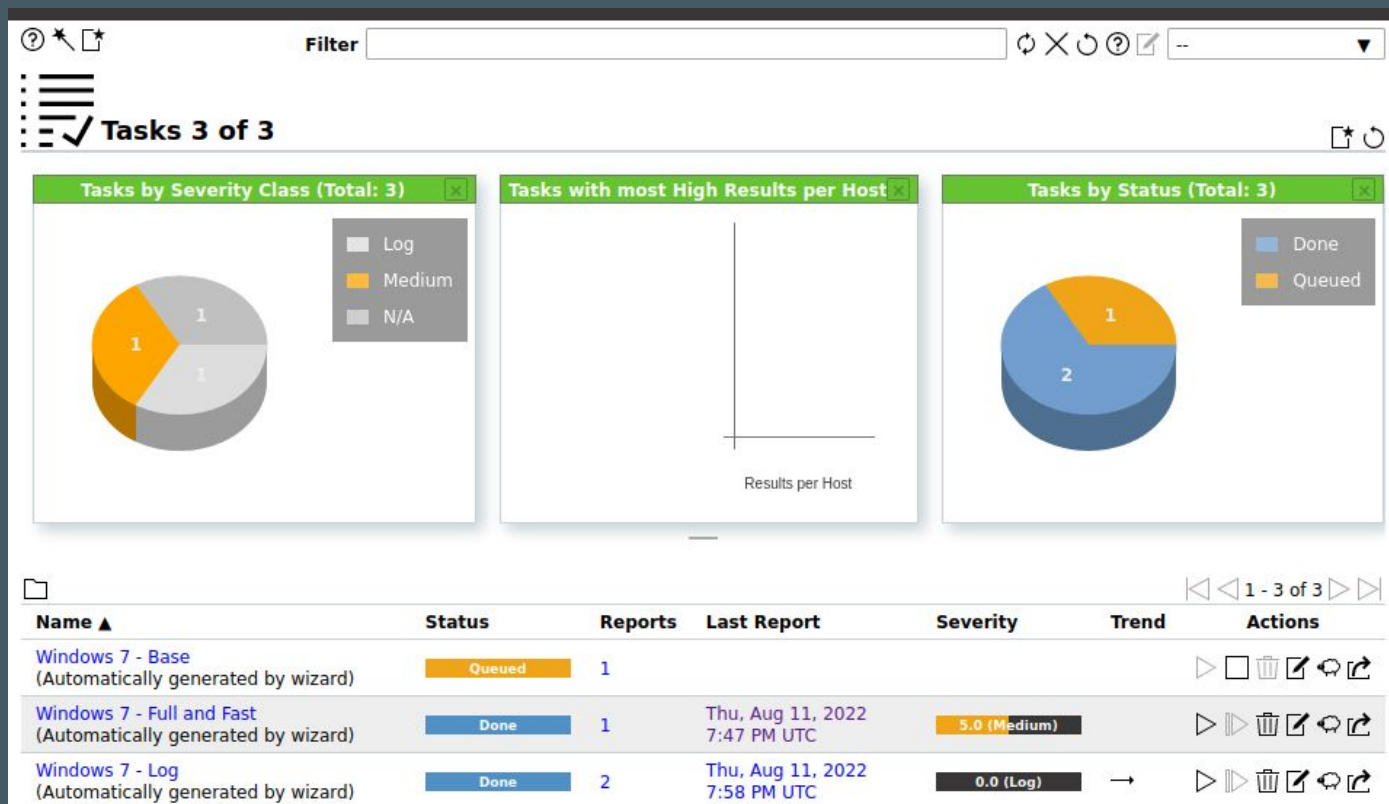
Coordinated Universal Time/UTC ▼

☐ Do not start automatically

## Verificar as tarefas de Scan e seus estados

- Assim que a criação da tarefa for feita, é possível visualizar seu estado na “**Dashboard**” do Scan.
  - Em outras palavras, é possível verificar as tarefas em andamento e realizar um conjunto de opções sobre elas, como mudar parâmetros, deletar, exportar como XML, dentre outras opções.


# Verificar as tarefas de Scan e seus estados



## Verificar os resultados e detalhes da tarefa

- Ao apertar sobre uma tarefa concluída (ou em andamento), é possível acessar todos os seus detalhes de operação e sobre a ocorrência de vulnerabilidades, dependendo da configuração do Scan.

# Verificar os resultados e detalhes da tarefa

**Rep Thu, Aug 11, 20**  
**ort: 22 7:51 PM UTC**

[Done](#)

b906a77e-  
ID: eb54-4779-a96a-  
be07613b9f31



Thu, Aug 11,  
Created: 2022 7:51 PM  
UTC

Thu, Aug 11,  
Modified: 2022 7:57 PM  
UTC

Owner: admin

[Information](#) [Results \(7 of 7\)](#) [Hosts \(1 of 1\)](#) [Ports \(4 of 4\)](#) [Applications \(0 of 0\)](#) [Operating Systems \(1 of 1\)](#) [CVEs \(0 of 0\)](#) [Closed CVEs \(0 of 0\)](#) [TLS Certificates \(0 of 0\)](#) [Error Messages \(0 of 0\)](#) [User Tags \(0\)](#)

◀◀ 1 - 7 of 7 ▶▶

Vulnerability		Severity ▼	QoD	Host		Location	Created
				IP	Name		
Services		0.0 (Log)	80 %	192.168.10.2		5357/tcp	Thu, Aug 11, 2022 7:52 PM UTC
DCE/RPC and MSRPC Services Enumeration		0.0 (Log)	80 %	192.168.10.2		135/tcp	Thu, Aug 11, 2022 7:53 PM UTC
SMB/CIFS Server Detection		0.0 (Log)	80 %	192.168.10.2		445/tcp	Thu, Aug 11, 2022 7:53 PM UTC
SMB/CIFS Server Detection		0.0 (Log)	80 %	192.168.10.2		139/tcp	Thu, Aug 11, 2022 7:53 PM UTC
SMB NativeLanMan		0.0 (Log)	95 %	192.168.10.2		445/tcp	Thu, Aug 11, 2022 7:53 PM UTC
OS Detection Consolidation and Reporting		0.0 (Log)	80 %	192.168.10.2		general/tcp	Thu, Aug 11, 2022 7:55 PM UTC



# 04 Referências

Sites de apoio

# Referências

**Documentação do Greenbone Vulnerability Manager (OpenVAS):**  
<https://greenbone.github.io/docs/latest/index.html>  
<https://docs.greenbone.net/GSM-Manual/gos-22.04/en/scanning.html>

**Repositório Oficial:**  
<https://github.com/greenbone/openvas-scanner>

**Instalação, Configuração e Execução em Kali-Linux:**  
<https://www.ceos3c.com/security/install-openvas-kali-linux/>  
<https://linuxhint.com/install-openvas-kali-linux/>

**Instalação, Configuração e Execução em Ubuntu:**  
<https://tiagotavares.io/2021/12/gestao-de-vulnerabilidades-com-greenbone-openvas-ubuntu-20.04-updated-dez-2021/>

# Obrigado pela atenção!

Ficou alguma dúvida?  
Se ficou, o **Kelton** responde!