

Pentest com Kali Linux





Instrutor: Vitor Mazuco

<http://facebook.com/vitormazuco>

Email: vitor.mazuco@gmail.com

WebSite: <http://vmzsolutions.com.br>



Encontrando Vulnerabilidades locais com o OpenVAS

O OpenVAS nos permite atacar uma ampla gama de vulnerabilidades, e vamos avaliar as vulnerabilidades de nossa rede específicas para o tipo de informação que procuramos após o término da avaliação. Nesta aula, usaremos o OpenVAS para fazer a varredura de vulnerabilidades em uma máquina que está na rede local.



Encontrando Vulnerabilidades locais com o OpenVAS

Vá para > **Configuration** > **Scan Configs**:

Digite o nome do scan que quer fazer. Para esta aula, vamos escrever as *Vulnerabilidades Locais*.

Escolha as opções:

Empty, static and fast

E salve



Encontrando Vulnerabilidades locais com o OpenVAS

New Scan Config ?

Name

Local Vulnerabilities

Comment (optional)

Base

☒ Empty, static and fast

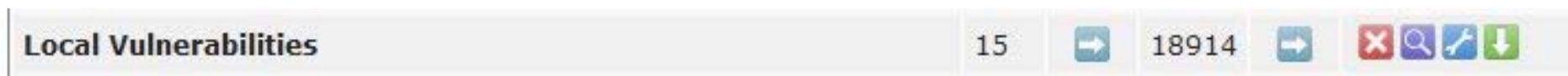
☐ Full and fast

Create Scan Config



Encontrando Vulnerabilidades locais com o OpenVAS

Agora, clique no ícone de ferramenta ao lado de Local Vulnerabilities:





Encontrando Vulnerabilidades locais com o OpenVAS

- Criar um novo alvo(new target) e realizar as seguintes tarefas:
- Digite o nome do alvo.
- Digite os hosts usando uma das seguintes formas:
- Digite apenas um endereço: 192.168.0.10
- Digite vários endereços, separados por uma vírgula:
192.168.0.10,192.168.0.115
- Ou então, digite um intervalo de endereços: 192.168.0.1-20

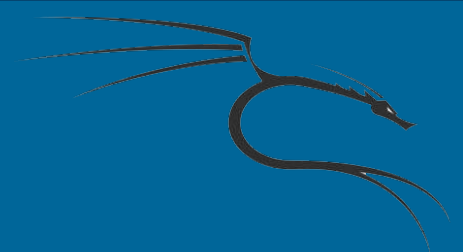


Encontrando Vulnerabilidades locais com o OpenVAS

Para cada família local encontrado, coloque uma marca de verificação na caixa **Select all NVT's**. Uma família é um grupo de vulnerabilidades. As vulnerabilidades são:

- Compliance
- Credentials
- Default Accounts
- Denial of Service
- FTP
- Ubuntu Local Security Checks

Encontrando Vulnerabilidades locais com o OpenVAS



Navigation

- Scan Management
 - Tasks
 - New Task
 - Notes
 - Overrides
 - Performance
- Configuration
 - Scan Configs
 - Targets
 - Credentials
 - Agents
 - Escalators
 - Schedules
 - Report Formats
 - Slaves
- Administration
 - Users
 - NVT Feed
 - Settings
- Help
 - Contents
 - About

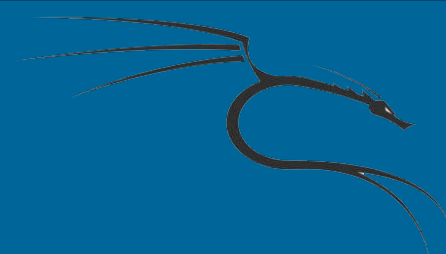
Edit Scan Config Details ?

[Back to Configs](#)

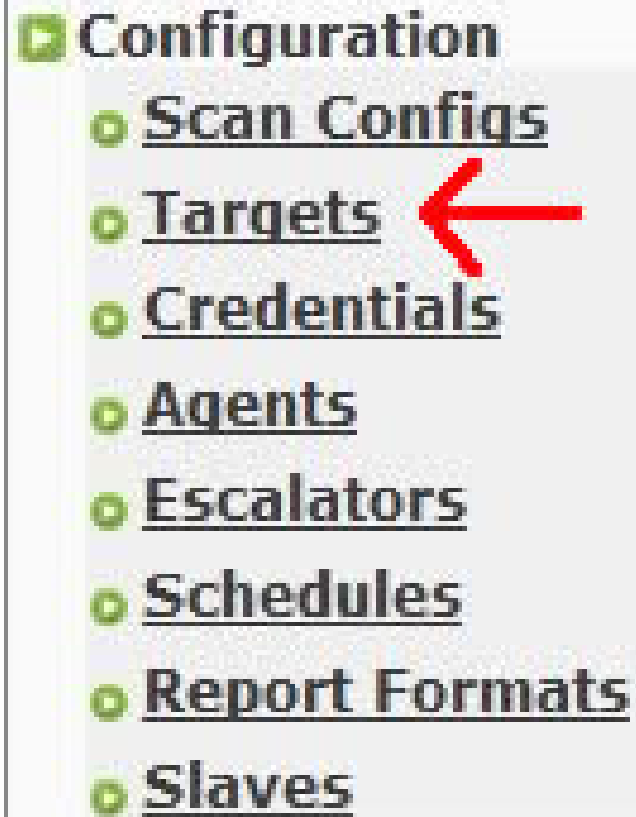
Name: Local Vulnerabilities
Comment:

Edit Network Vulnerability Test Families

Family	NVT's selected	Trend	Select all NVT's	Action
AIX Local Security Checks	1 of 1		<input checked="" type="checkbox"/>	
Brute force attacks	0 of 11		<input type="checkbox"/>	
Buffer overflow	0 of 434		<input type="checkbox"/>	
CISCO	0 of 4		<input type="checkbox"/>	
CentOS Local Security Checks	1243 of 1243		<input checked="" type="checkbox"/>	
Compliance	0 of 3		<input type="checkbox"/>	
Credentials	0 of 2		<input type="checkbox"/>	
Databases	0 of 71		<input type="checkbox"/>	
Debian Local Security Checks	2476 of 2476		<input checked="" type="checkbox"/>	
Default Accounts	0 of 28		<input type="checkbox"/>	
Denial of Service	0 of 777		<input type="checkbox"/>	
FTP	0 of 159		<input type="checkbox"/>	



Vá para > **Configuration** > **Targets**:

- 
- A screenshot of the OpenVAS web interface showing the 'Configuration' menu. The menu is expanded, displaying a list of sub-items. A red arrow points to the 'Targets' item.
- Configuration
 - Scan Configs
 - Targets
 - Credentials
 - Agents
 - Escalators
 - Schedules
 - Report Formats
 - Slaves



Crie um novo Target em **Create Target** e realizar as seguintes tarefas:

- Insira o nome da tarefa.
- Insira um comentário (opcional).
- Escolha a sua configuração de *scan*. Neste caso **Local Vulnerabilities**.
- Selecione os destinos de digitalização. Neste caso **Local Network**.



Encontrando Vulnerabilidades locais com o OpenVAS

- Deixe todas as outras opções como estão.
- Clique em **Create Task**.



Encontrando Vulnerabilidades locais com o OpenVAS

New Task ?

Name	<input type="text" value="Local Vulnerabilities"/>
Comment (optional)	<input type="text"/>
Scan Config	<input type="text" value="Local Vulnerabilities"/> ▼
Scan Targets	<input type="text" value="Local Network"/> ▼
Escalator (optional)	-- ▼
Schedule (optional)	-- ▼
Slave (optional)	-- ▼

Create Task



Encontrando Vulnerabilidades locais com o OpenVAS

Agora vá para **Scan Management | Tasks**.

Clique no botão ***play*** ao lado de nossa análise. Neste caso, **Local Vulnerability Scan**:



Encontrando Vulnerabilidades locais com o OpenVAS

Results of last operation

Operation: Delete Task
Status code: 200
Status message: OK

Tasks ? ★
No auto-refresh Apply overrides ↻

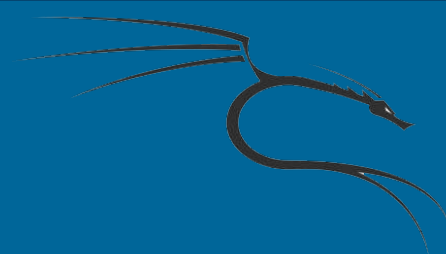
Task	Status	Reports			Threat	Trend	Actions
		Total	First	Last			
Local Vulnerabilities Scan	Done	1	Aug 8 2012		None		▶ ⏸ ⏹ ✖ 🔍 🔧



Encontrando Vulnerabilidades locais com o OpenVAS

Nesta aula, usamos o OpenVAS para procurar um conjunto de vulnerabilidades locais, e finalmente, selecionamos o nosso alvo que completou a varredura. O OpenVAS fez a varredura e listou as vulnerabilidades conhecidas incluídos da nossa NVT.

Extra!



Task Summary ? ↺

Name: Local Vulnerabilities Scan

Comment:

Config: [Full and fast](#)

Escalator:

Schedule: (Next due: over)

Target: [Localhost](#)

Slave:

Status: Done

Reports: 1 (Finished: 1)

[Back to Tasks](#)

Reports for "Local Vulnerabilities Scan" ? ↺ √Apply overrides ↺

Report	Threat	Scan Results					Actions
		High	Medium	Low	Log	False Pos.	
Thu Aug 9 11:46:07 2012 Done	Medium	0	1	1	13	0	

Notes on Results of "Local Vulnerabilities Scan" ? ↺

NVT	Text	Actions

Overrides on Results of "Local Vulnerabilities Scan" ? ↺

NVT	From	To	Text	Actions