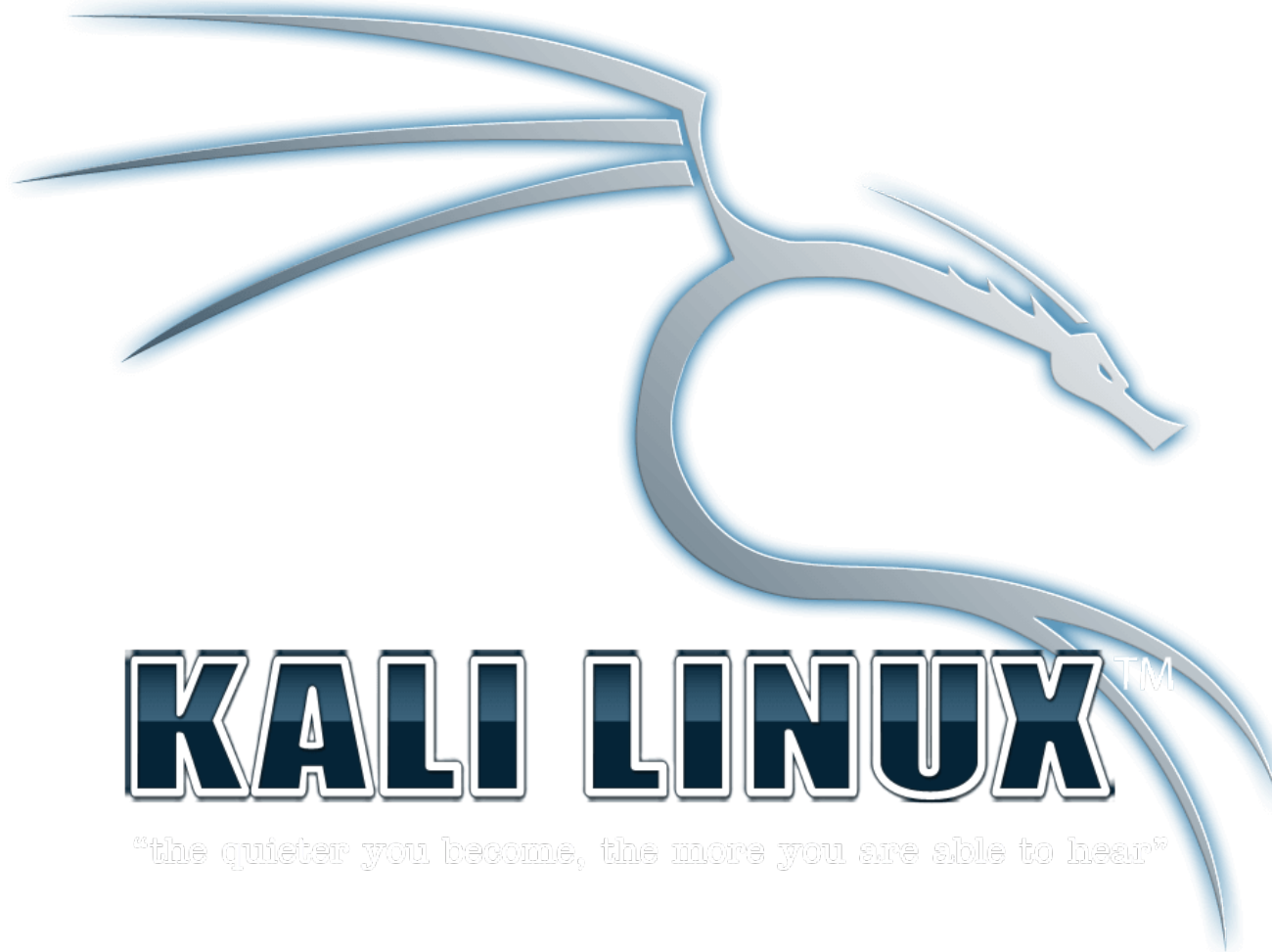


Pentest com Kali Linux





Instrutor: Vitor Mazuco

<http://facebook.com/vitormazuco>

Email: vitor.mazuco@gmail.com

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



Encontrar vulnerabilidades na rede com o Nessus

O Nessus nos permite atacar uma ampla gama de vulnerabilidades dependendo da nossa configuração, e vamos limitar a nossa lista para avaliar as vulnerabilidades de para um tipo de informação específica que nós procuramos a fim de ganhar conteúdo a respeito de nossos alvos. Nesta aula, vamos configurar o Nessus para encontrar vulnerabilidades na rede em nossos pentest. Estes são vulnerabilidades específicas em máquinas ou em protocolos sobre nossa rede local.



Encontrar vulnerabilidades na rede com o Nessus

Para completar esta aula, é recomendável o uso de máquina virtual para testar contra:

- Windows XP, 7, 8, 8.1 ou 10
- Metasploitable 2.0
- Firewall ou um roteador
- Uma distribuição Linux de sua preferência




Encontrar vulnerabilidades na rede com o Nessus

Na guia de Plugins, clique em Desativar tudo e selecione as seguintes vulnerabilidades:

- ✓ CISCO
- ✓ DNS
- ✓ Default Unix Accounts
- ✓ FTP
- ✓ Firewalls
- ✓ Gain a shell remotely
- ✓ General
- ✓ Netware
- ✓ Peer-To-Peer File Sharing
- ✓ Policy Compliance
- ✓ SMTP Problems
- ✓ SNMP
- ✓ Service Detection
- ✓ Settings
- ✓ Windows
- ✓ Windows : Microsoft Bulletins
- ✓ Windows : User management

Encontrar vulnerabilidades na rede com o Nessus



Scans Policies vitormazuco

Rede

Disable All Enable All Filter Plugin Families

Policies > Settings Credentials Compliance **Plugins**

Show Enabled | Show A

Status	Plugin Family ▼	Total
ENABLED	CISCO	753
ENABLED	Default Unix Accounts	106
ENABLED	DNS	145
ENABLED	Firewalls	176
ENABLED	FTP	247
ENABLED	Gain a shell remotely	279
ENABLED	General	224

Status	Plugin Name	Plugin ID
ENABLED	Microsoft Windows 'Account Operators' Group User List	10901
ENABLED	Microsoft Windows 'Administrators' Group User List	10902
ENABLED	Microsoft Windows 'Backup Operators' Group User List	10904
ENABLED	Microsoft Windows 'Domain Administrators' Group User List	10908
ENABLED	Microsoft Windows 'Print Operators' Group User List	10905
ENABLED	Microsoft Windows 'Replicator' Group User List	10906
ENABLED	Microsoft Windows 'Server Operators' Group User List	10903

Save Cancel



Encontrar vulnerabilidades na rede com o Nessus

Agora defina os endereços IP das máquinas que você quer que seja executado o pentest, e depois execute a verificação. Após concluído a tarefa, saia o report para futuras análises.