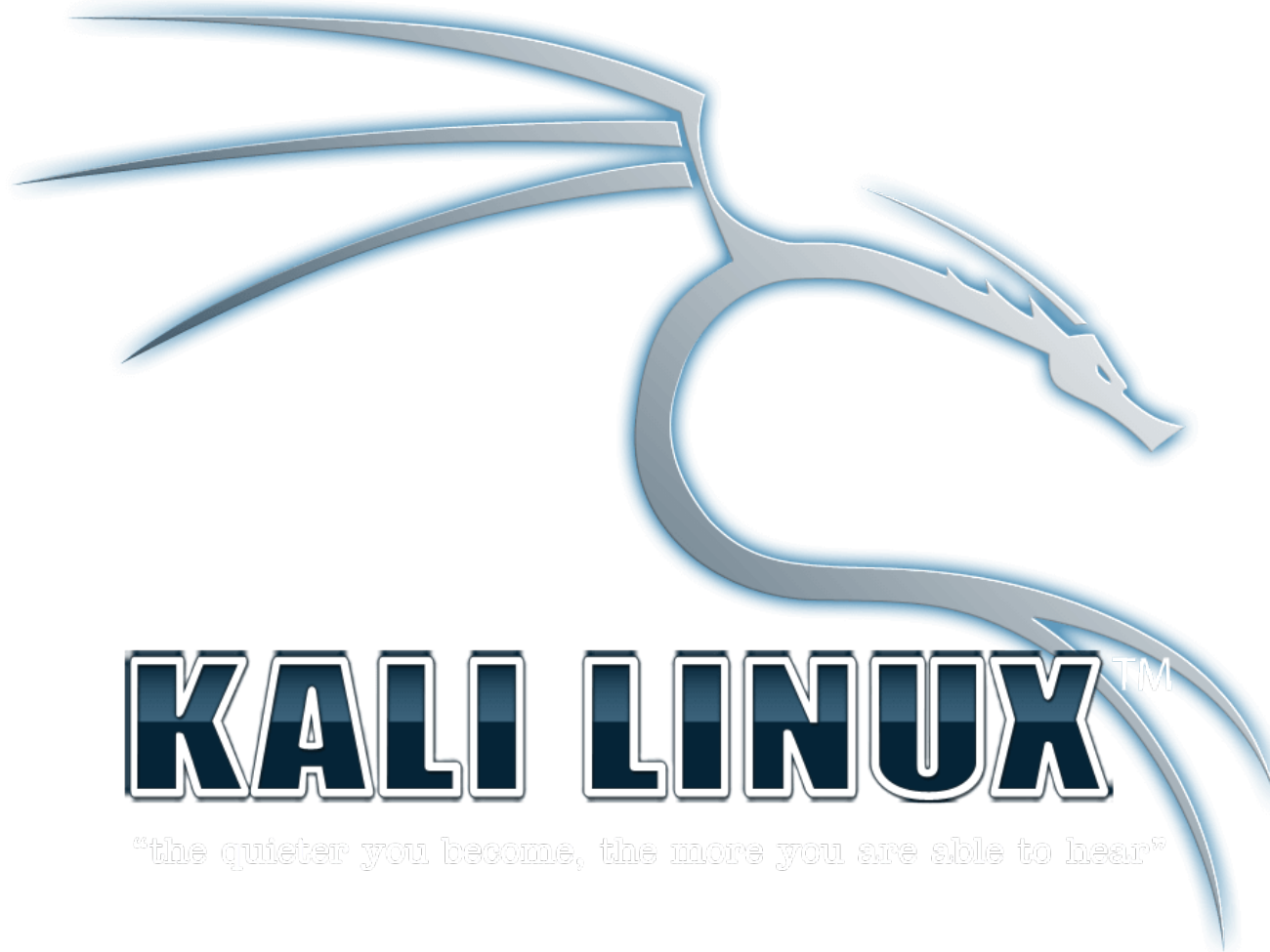


Pentest com Kali Linux





Instrutor: Vitor Mazuco

<http://facebook.com/vitormazuco>

Email: vitor.mazuco@gmail.com

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



Uma das etapas mais importantes de um ataque é o recolhimento de informações. Para ser capaz de lançar um ataque, é preciso reunir informações básicas sobre o nosso alvo. Assim, quanto mais informações temos, maior a probabilidade de um ataque bem sucedido.



Eu também quero enfatizar um aspecto importante desta fase, e é a documentação. O lançamento mais recente do Kali inclui algumas ferramentas para nos ajudar a reunir e organizar os dados do nosso alvo, o que nos permite obter um reconhecimento melhor. Ferramentas como Maltego CaseFile e KeepNote são exemplos disso.

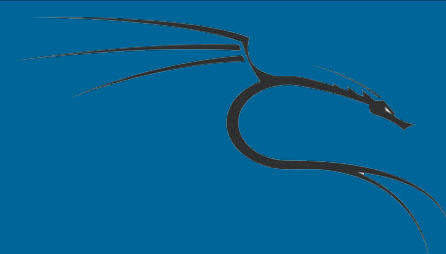


Enumeração do serviço

Nesta aula, vamos realizar alguns truques de enumeração de serviço. Enumeração é um processo que nos permite reunir informações de uma rede. O tráfego SNMP em uma rede.



Vamos examinar as técnicas de enumeração de SNMP e enumeração DNS. Enumeração de DNS é o processo de localizar todos os servidores DNS e entradas DNS para uma organização. Ele nos permitirá reunir informações críticas sobre a organização, como nomes de usuário, nomes de computadores, endereços IP, e assim por diante.



Para realizar esta tarefa, usaremos um DNSenum. Para a enumeração do SNMP, vamos usar uma ferramenta chamada *SnmpEnum*. Que é uma ferramenta de enumeração de SNMP poderoso que permite aos usuários para analisar as informações.