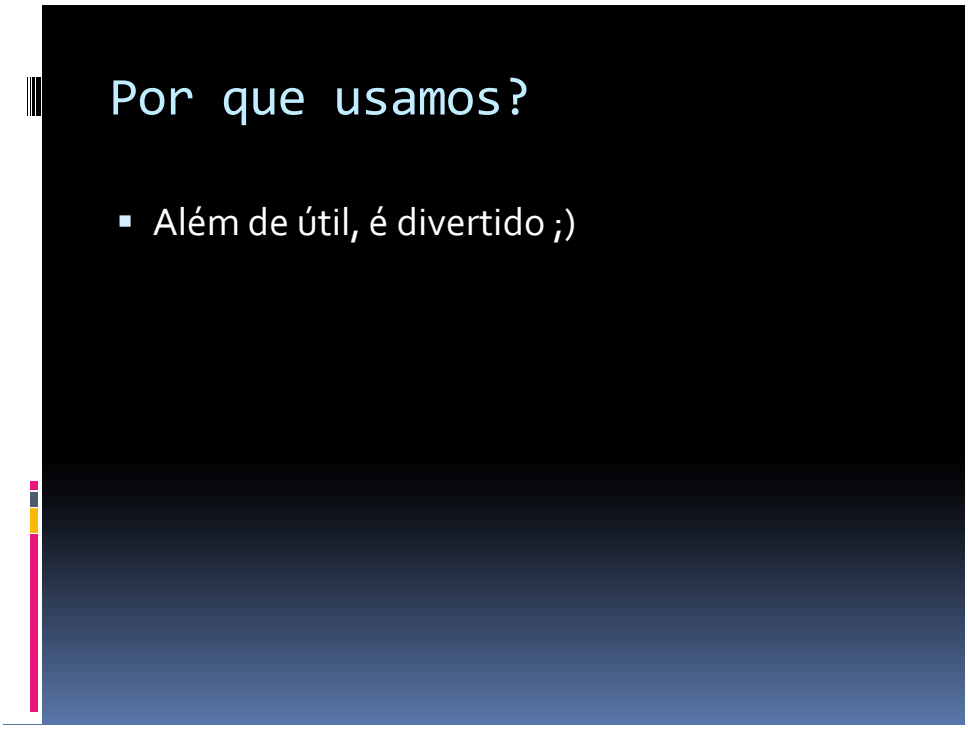
Testes de Intrusão em Redes Corporativas

407

17 Google Hacking

17.1 Objetivo

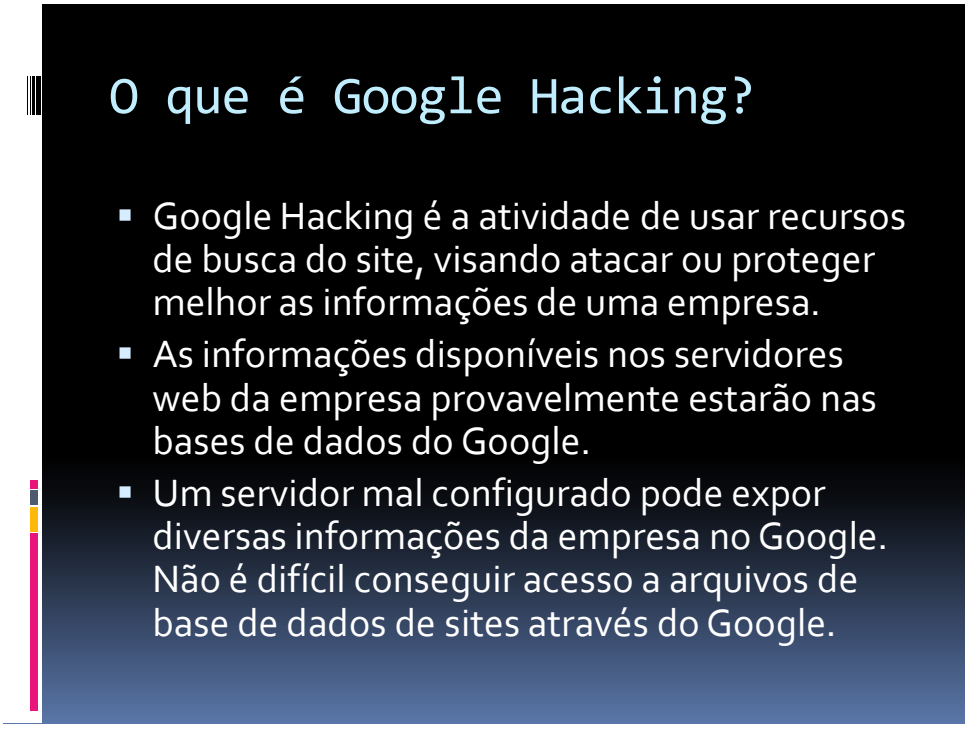
- Entender o que é Google Hacking
- Conhecer os riscos que o Google traz
- Aprender como usar o Google como ferramenta auxiliar para um pentest



17.2 O que é Google Hacking?

Google Hacking é a atividade de usar recursos de busca do site, visando atacar ou proteger melhor as informações de uma empresa. As informações disponíveis nos servidores web da empresa provavelmente estarão nas bases de dados do Google.

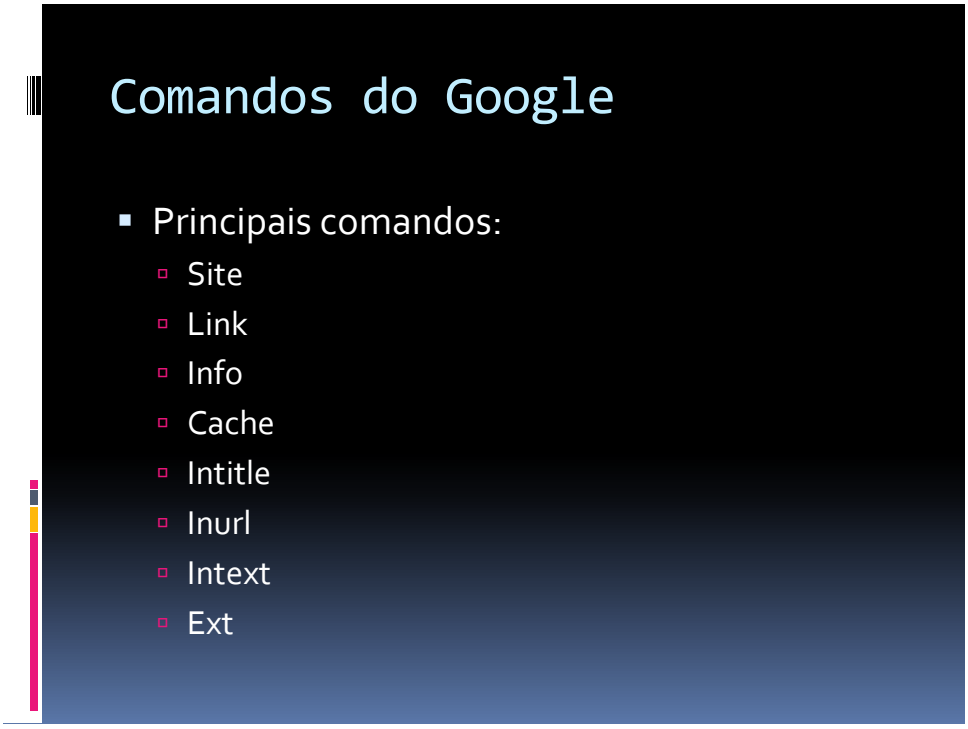
Um servidor mal configurado pode expor diversas informações da empresa no Google. Não é difícil conseguir acesso a arquivos de base de dados de sites através do Google.



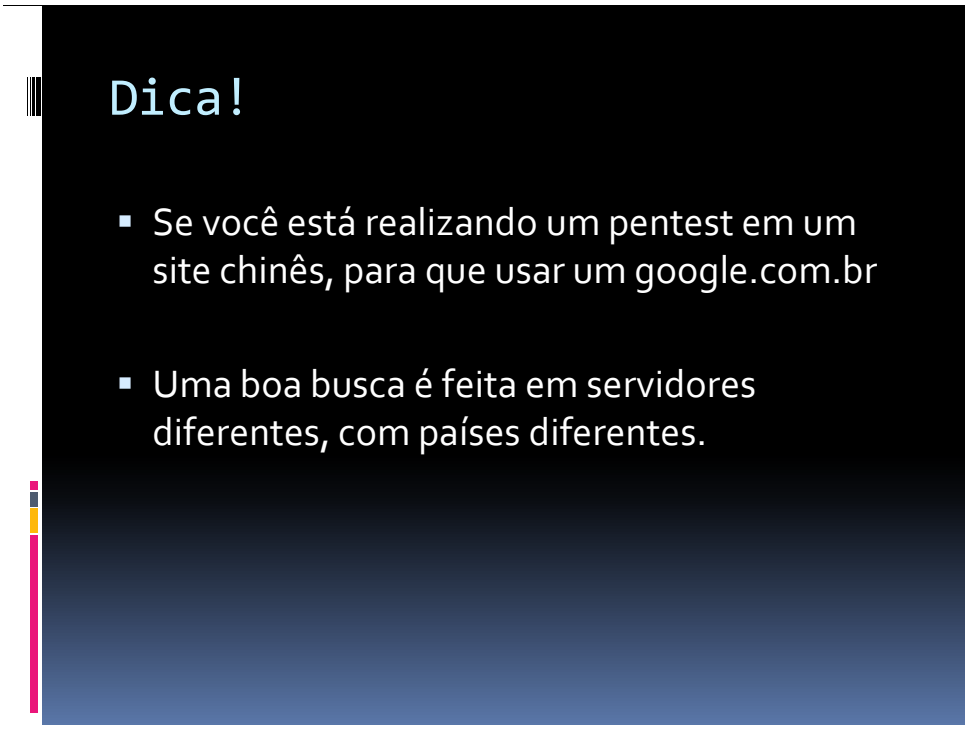
17.3 Comandos

- site: = Sua busca ficará restrita ao domínio especificado. [site:.br/.us/.mx(restringe sua busca nos domínios com os finais mencionados) ou você utiliza um domínio específico site:4linux.com.br]
- link: = Faz uma busca em apontamentos de domínio (link:4linux.com.br)
- info: = Mostra informações sobre a página especificada (info:4linux.com.br)
- cache: = Mostra a Última versão em cache da página (cache:4linux.com.br)
- intitle: = Faz uma busca no título do site (intitle:Hacker)
- allintitle: = Uma variação do intitle procura SOMENTE no título das páginas (allintitle:hacking)
- inurl: = Procura o termo na URL do site (inurl:hacker)

- allinurl: = Uma variação do inurl: procura SOMENTE na url das páginas (allinurl:4linux)
- intext: = Procura termos dentro da página(intext:4linux)
- allintext: = Variação ao intext procura SOMENTE no corpo da mensagem (allintext:4linux)
- allinanchor: = Procura o termo somente no texto do link (allinanchor:Security Officer)
- " " = Utilizado para busca Refinada em definição de termos (Gosto do google) COm isso você esta fazendo busca com 3 palavras distintas gosto, do, google utilizando o caracter "" voce refina sua busca "gosto do google"
- ext: = Procura arquivos com uma extensão pré definida (ext:doc busca)
- filetype: mesma função do ext:
- phonebook: = Busca de telefones por nome (phonebook:bill gates) Infelizmente não disponível para muitos países. Algumas variações (rphonebook; bphonebook)
- daterange: = Limita sua pesquisa em uma data particular ou variação de datas em que uma página foi indexada. ("George Bush" daterange:2452389-2452389)



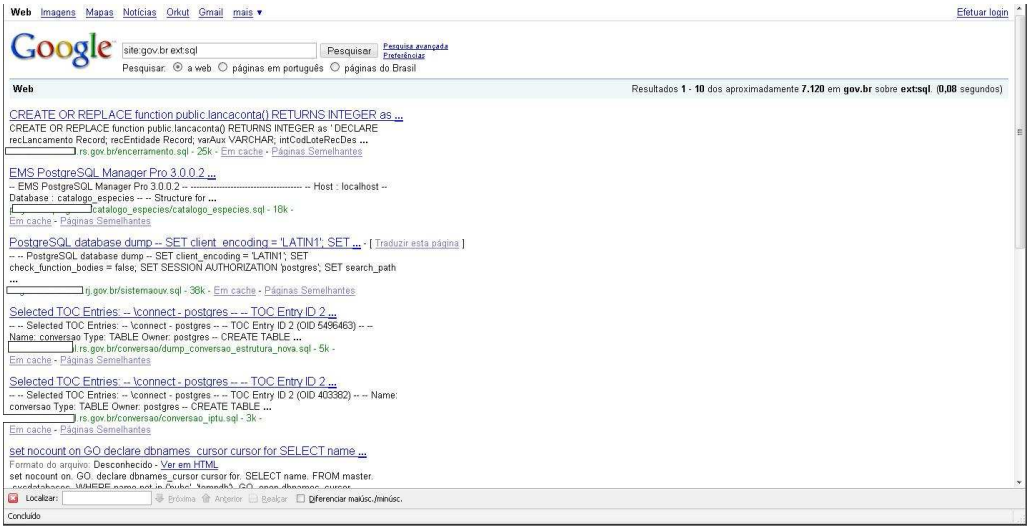
*Dica: Se você está realizando um pentest em um site chinês, para que usar um google.com.br? O Google prioriza os resultados para determinados websites. Raramente você vê páginas escritas em japonês, chinês, árabe e outros quando usa o google.com.br, não? Uma boa busca é feita em servidores diferentes, com países diferentes.



17.4 Prática Dirigida

Busca por arquivos de base de dados em sites do governo:

site:gov.br ext:sql



Busca por um servidor específico

- inurl:"powered by" site:sistema.com.br

A pesquisa busca arquivos de e-mail em formato .mdb

- inurl:e-mail filetype:mdb

Essa pesquisa busca telefones disponíveis em intranet encontradas pelo Google

- inurl:intranet + intext:"telefone"

Realizando uma pesquisa dessa maneira é possível identificar muitos dos subdomínios da Oracle

- site:oracle.com -site:www.oracle.com

Detectando sistemas que usando a porta 8080

- inurl:8080 -intext:8080

Encontrando VNC

- intitle:VNC inurl:5800 intitle:VNC

Encontrando VNC

- intitle:"VNC Viewer for Java"

Encontrando Webcam ativa

- "Active Webcam Page" inurl:8080

Encontrando Webcam da toshiba:

- intitle:"toshiba network camera - User Login"

Encontrando Apache 1.3.20:

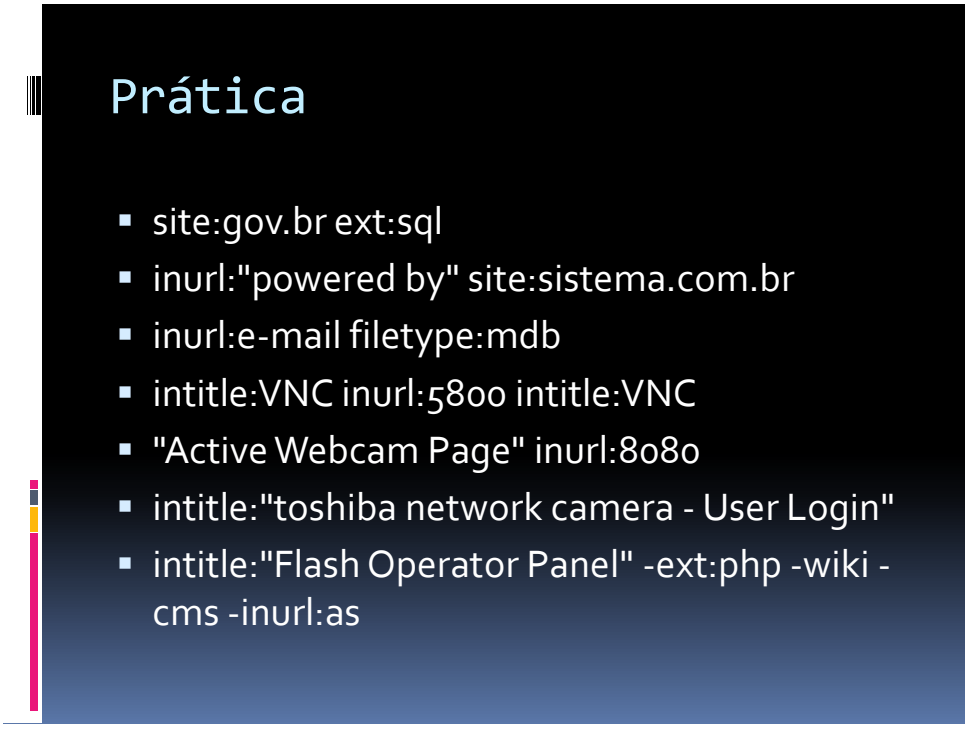
- "Apache/1.3.20 server at" intitle:index.of

Asterisk VOIP Flash Interface

- intitle:"Flash Operator Panel" -ext:php -wiki -cms -inurl:as

Possíveis falhas em aplicações web:

- allinurl:".php?site="
- allinurl:".php?do="
- allinurl:".php?content="
- allinurl:".php?meio="
- allinurl:".php?produto="
- allinurl:".php?cat="



17.5 Contramedidas

- Possuir uma boa política referente à publicações de informações na internet.
- Não deixar configurações padrão em servidores web, para que os mesmos não consigam ser identificados facilmente.
- Sempre analisar as informações disponíveis sobre a empresa em sites de busca.
- Alertar e treinar os funcionários da empresa com relação a maneira com que um ataque de engenharia social pode acontecer, e as possíveis informações que o atacante poderá usar nesse ataque.

17.6 Laboratório

1. Identifique servidores vulneráveis através do sistema de busca do Google.
2. Identifique arquivos SQL e senhas através do Google.