



# Segurança de Redes

3º Semestre



## Google Hacking

**Prof. Nataniel Vieira**  
**[nataniel.vieira@gmail.com](mailto:nataniel.vieira@gmail.com)**



# O que é Google Hacking?

**Google Hacking é a atividade de utilizar os mecanismos de busca do google, visando proteger as informações de uma empresa ou para realização de ataques.**

**Considerada a melhor ferramenta para os hackers, pois o Google possui diversos recursos que podem ser utilizados durante um teste de invasão.**



# **Google Hacking Database**

**É um banco de dados virtual, previamente criado, com tags de busca no Google, Com intuito de conseguir informações específicas.**

**Deve-se ter em mente a possibilidade de adaptar tais tags de busca para um necessidade específica.**



# Google Hacking Database

**Google Hacking Database disponível em:**

**<http://johnny.ihackstuff.com/ghdb/>**



# Google Hacking

**Por se tratar de um sistema público para busca de informações sobre qualquer coisa, é possível levantar informações de sites, propagandas, documentos, redes sociais, grupos e etc.**

**Exemplo: e-mail + cpf**



# Operadores avançados

**O mecanismo de busca do google além de permitir encontrar informações de sites/URLs específicas, possui um mecanismo de operadores avançados que permitem uma busca através de filtros poderosos que resultam em buscas exatas sobre algo que se esteja buscando.**



# Operadores avançados

**intitle, allintitle**

**Busca conteúdo no título (tag title) da página.**

**Allintext**

**Localiza uma string dentro do texto de uma página.**

**inurl, allinurl**

**Encontra texto em uma URL.**



# Operadores avançados

**site**

**Direciona a pesquisa para o conteúdo de um determinado site.**

**filetype**

**Busca por um arquivo de determinado tipo.**

**link**

**Busca por links para uma determinada página.**





# Operadores avançados

**cache**

**Mostra a versão em cache de uma determinada página.**

**daterange**

**Busca por páginas publicadas dentro de um “range” de datas.**

**Phonebook, Rphonebook, /Bphonebook**

**Mostra listas de telefones residencias ou comerciais**



# **Operadores avançados**

## **Autor**

**Procura o autor de uma postagem**

## **Group**

**Pesquisas nomes de grupos, seleciona grupos individuais**

## **Insubject**

**Localiza uma sequência no assunto de um grupo de postagem**



# Reconhecimento (\*)

**Detectando sistemas que usando a porta 3389**

**inurl:3389 -intext:3389**

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

**site:gov.br ext:sql**

**busca telefones disponíveis em intranet encontradas pelo Google**

**inurl:intranet + intext:"telefone"**

**\*Metodologia de pentest**



# **Reconhecimento (\*)**

**Encontrando paginas de administração de roteadores  
intitle:"colocar o nome de gerência do router"**

**Encontrando Apache (versão)**

**"Apache/versão server at"intitle:index.of**

**Detectando sistemas que usando a porta 8080**

**inurl:3389 -intext:3389**

**\*Metodologia de pentest**



# Falhas em aplicações web

**allinurl:".php?site="**

**allinurl:".php?do="**

**allinurl:".php?produto="**

**allinurl:".php?content="**

**allinurl:".php?cat="**



# Contra medidas

**Não manter configurações padrão em servidores web, de forma que os mesmos não possam ser identificados facilmente.**

**Definir uma boa política referente às publicações de informações na internet.**



# **Contra medidas**

**Estar sempre analisando informações disponíveis sobre a empresa em sites de busca.**

**Trabalhar a cultura de 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.**

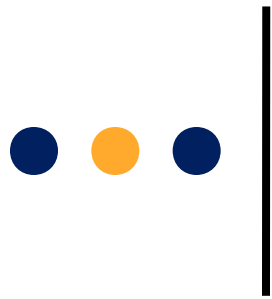


# **Exercício 01**

**1.1 – Usando o Recurso Google Hacking, vasculhe a internet e encontre algum arquivo com a extensão PDF e um XLS, que contenham telefones.**

**1.2 - Usando o Recurso Google Hacking, vasculhe a internet e encontre algum roteador da marca TPLINK e sua página de gerência.**





## **Exercício 02**

**2.1 - Procure e encontre seus dados na internet (utilizando o Google). Consiga o maior número de dados a seu respeito.**

**2.2 – Exercícios 01 e 02 devem ser resolvidos em sala de aula.**



## Exercício 03

**3.1) Para servir como cliente para as buscas, ativar uma máquina virtual Windows XP, disponível em:**

[ftp://192.168.200.3/VM\\_Windows\\_XP\\_Professional.zip](ftp://192.168.200.3/VM_Windows_XP_Professional.zip)

**3.2) Acessar os sites:**

<http://www.exploit-db.com/google-dorks/>

<http://johnny.ihackstuff.com/ghdb/>

**3.3) Utilizar 08 buscas, preferencialmente, de categorias diferentes e explorar os resultados encontrados.**



## Exercício 03

3.4) Analisar e documentar os resultados, em formato **PDF** com o nome de **GH3**, e enviar por e-mail para: **nataniel.vieira@gmail.com**

3.5) Entrega do exercício 03 deverá ser realizada até dia **21/05/2016** às **23:59hs**.



# Referências

**Hackers for Charity**

<http://www.hackersforcharity.org/ghdb/>

**Exploit DB – GHDB**

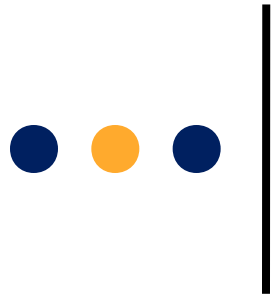
<http://www.exploit-db.com/google-dorks/>

**Google Hacking DataBase**

<http://johnny.ihackstuff.com/ghdb/>

**Buscas em cache**

<https://web.archive.org>



# Contato



**nataniel.vieira**



**nataniel.vieira@gmail.com**