



# Enumeração

Marcos Flávio Araújo Assunção  
Fundamentos de Ethical Hacking

# Enumeração



The screenshot shows a Mozilla Firefox browser window with the address bar displaying `http://www.baq`. The page title is "Index of /img/banners/exemplos". The page content is a directory listing with columns for Name, Last modified, Size, and Desc. The listing includes various banner files and directories, such as "Parent Directory", "banner-vertical.jpg", "banner mega.gif", "botao site.gif", "botao site news.gif", "full banner news.gif", "full banner site.gif", "half banner news.gif", "half banner site.gif", "hiper banner.gif", "informes-empresarial...", "ins junto as noticia...", and "popup.gif". The status bar at the bottom indicates "Concluído".

Name	Last modified	Size	Desc
[DIR] <a href="#">Parent Directory</a>	07-Feb-2005 09:59	-	
[IMG] <a href="#">banner-vertical.jpg</a>	17-Mar-2005 11:16	103k	
[IMG] <a href="#">banner mega.gif</a>	17-Jan-2006 15:29	35k	
[IMG] <a href="#">botao site.gif</a>	14-Oct-2004 09:47	26k	
[IMG] <a href="#">botao site news.gif</a>	14-Oct-2004 09:47	24k	
[IMG] <a href="#">full banner news.gif</a>	14-Oct-2004 09:47	47k	
[IMG] <a href="#">full banner site.gif</a>	14-Oct-2004 09:47	41k	
[IMG] <a href="#">half banner news.gif</a>	14-Oct-2004 09:47	48k	
[IMG] <a href="#">half banner site.gif</a>	14-Oct-2004 09:47	42k	
[IMG] <a href="#">hiper banner.gif</a>	17-Jan-2006 15:59	103k	
[IMG] <a href="#">informes-empresarial...&gt;</a>	17-Mar-2005 11:19	155k	
[IMG] <a href="#">ins junto as noticia...&gt;</a>	14-Oct-2004 09:47	40k	
[IMG] <a href="#">popup.gif</a>	14-Oct-2004 09:47	40k	

Apache/1.3.33 Server at www.baguete.com.br Port 80

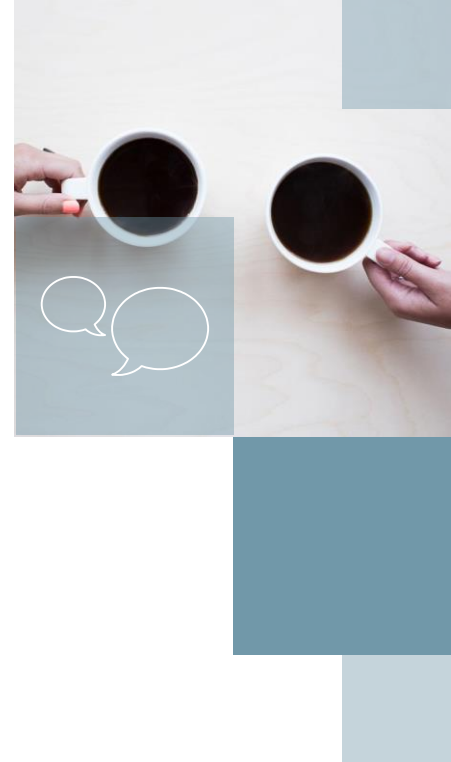
- Tem como objetivo identificar os serviços rodando nas portas, o Sistema Operacional e outros elementos
- Captura de banners
- Fingerprint
- Usuários / E-mails
- Regras de Firewall



## Captura de Banners

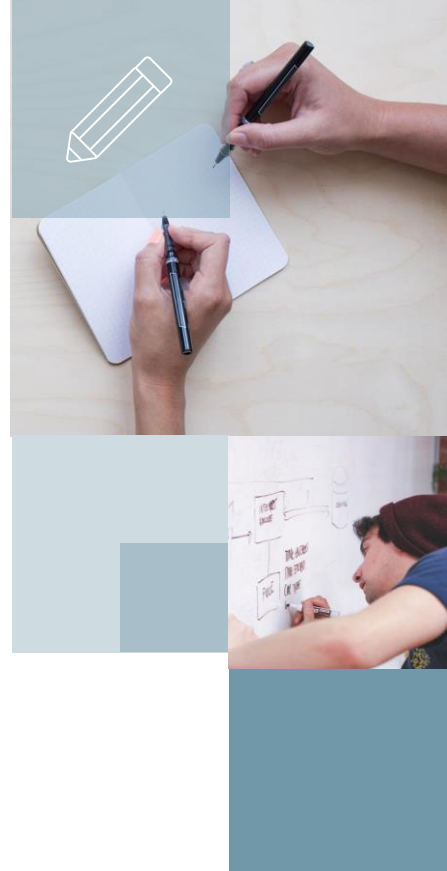
```
C:\>ftp 192.168.10.3
Conectado a 192.168.10.3.
220 (vsFTPd 2.3.4)
Usuário (192.168.10.3:(none)):
```

- Basta se conectar ao serviço usando telnet
- Muitos serviços não são configurados para alterar o banner padrão
- Mostra o nome e a versão do software
- Informação pouco confiável



# Fingerprint

- Usa um banco de dados de “impressões digitais” para identificar o serviço
- Baseia-se na análise do comportamento de pacotes



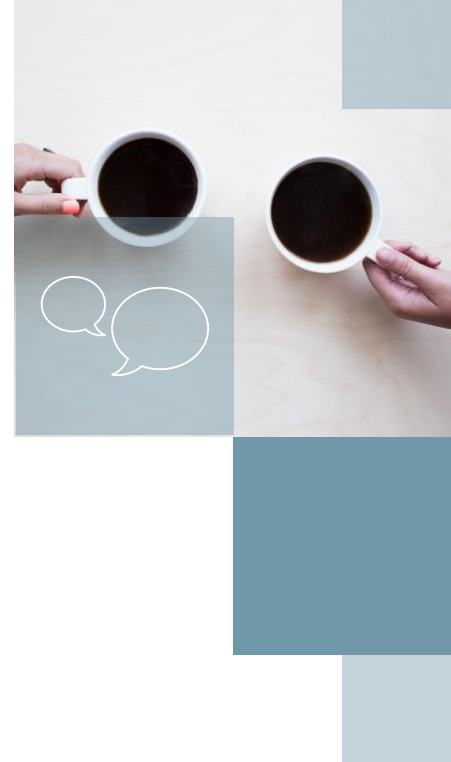
## Fingerprint com o NMAP

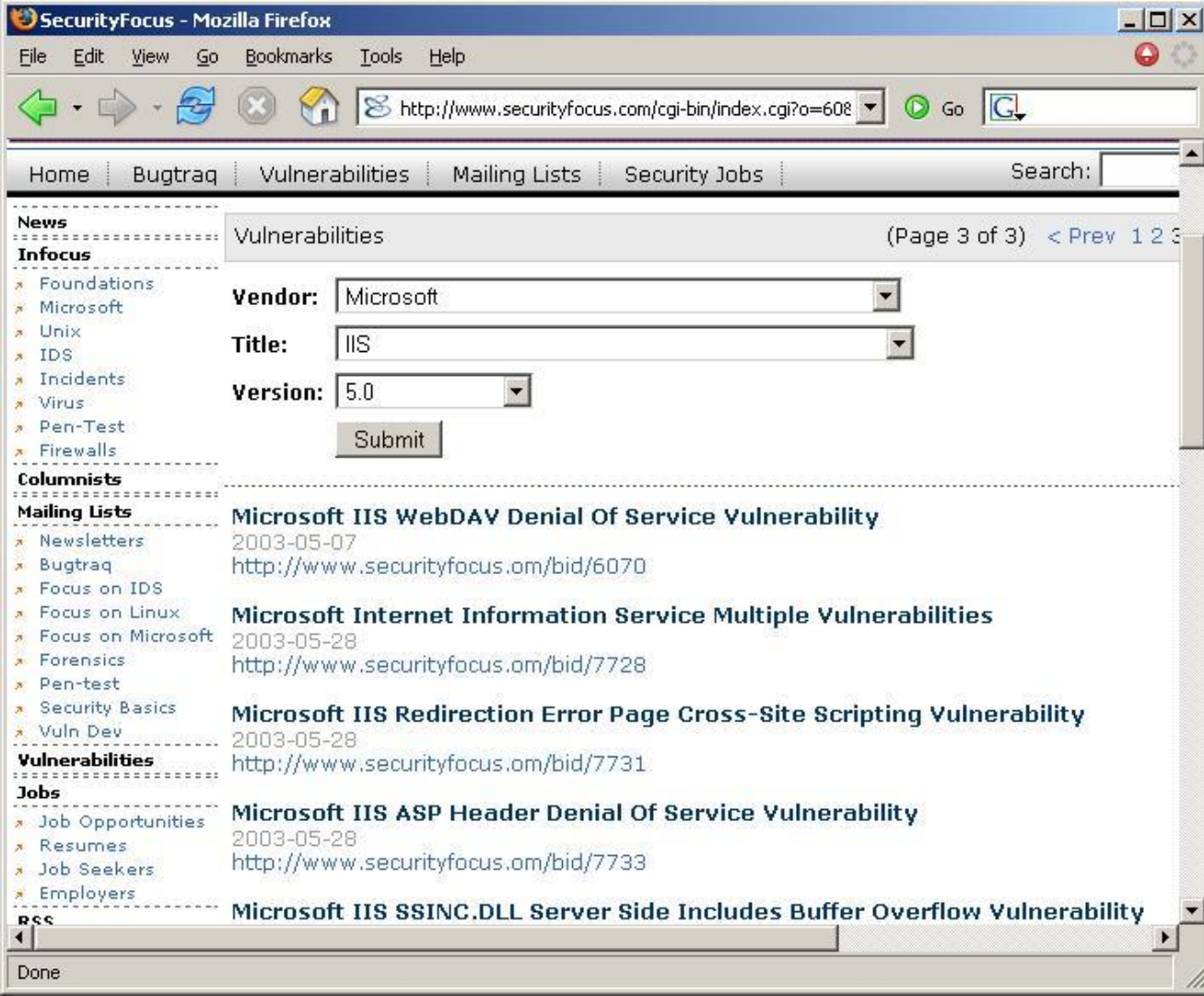
Sistema Operacional: **opção -O**

```
Device type: general purpose  
Running: Microsoft Windows 2003  
OS details: Microsoft Windows Server 2003 SP1  
Network Distance: 1 hop
```

Serviços das portas: **opção -A**

```
1524/tcp open  ingreslock?  
2049/tcp open  rpcbind  
2121/tcp open  ftp          ProFTPD 1.3.1  
3306/tcp open  mysql        MySQL 5.0.51a-  
! mysql-info: Protocol: 10
```



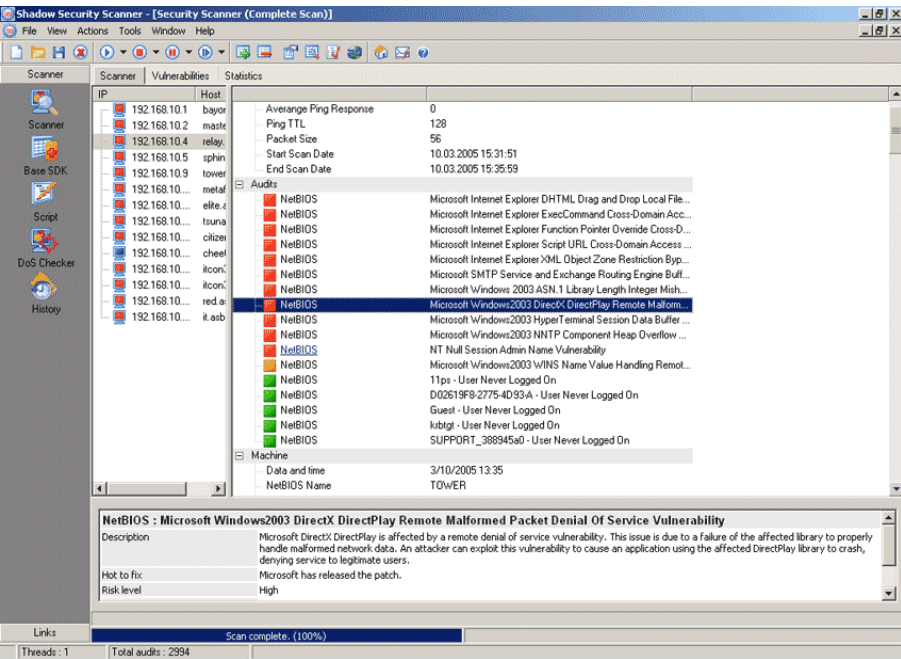


Pesquisa manual  
por Falhas

SecurityFocus



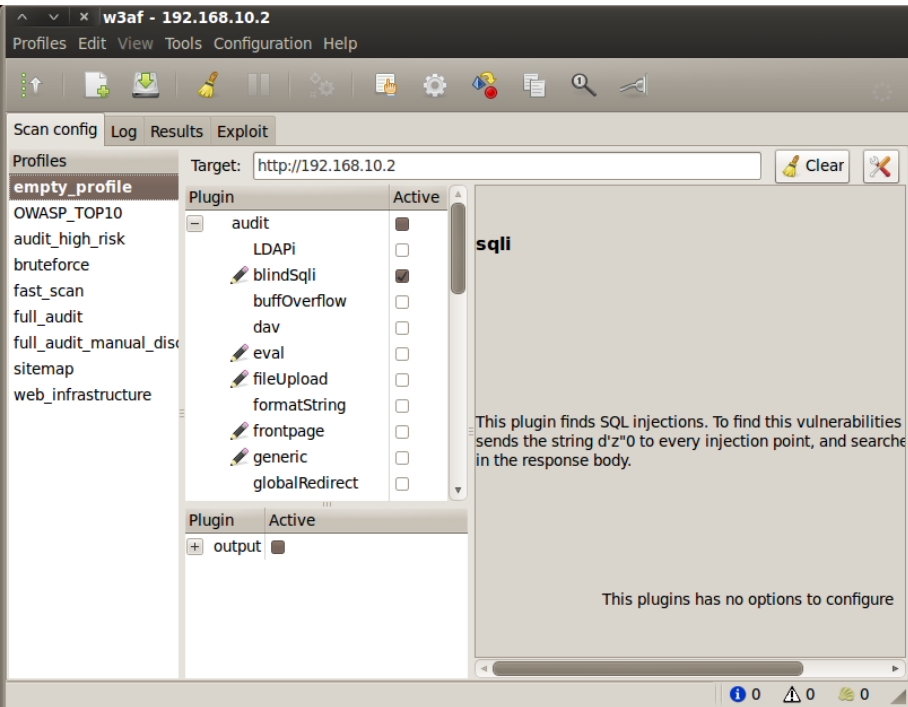
# Scanners “genéricos” de vulnerabilidades



- Não se focam em um serviço específico.
- São como um médico generalista, detectam “superficialmente” problemas em vários protocolos.
- Exemplos de softwares: Nessus, Retina, Languard, Shadow Security Scanner
- Boa opção para uma grande rede corporativa



# Scanners “específicos” de vulnerabilidades



- Focam em poucos protocolos e serviços (**normalmente apenas um**), por isso fazem uma análise mais apurada.
- Há muitos scanners destes para http, sql, etc.
- Exemplos de softwares: **Nikto, SQLMap, SQL Ninja, Acunetix, W3AF, Burp Scanner, etc.**

