Enumeração

Marcos Flávio Araújo Assunção

Fundamentos de Ethical Hacking

Enumeração

- 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

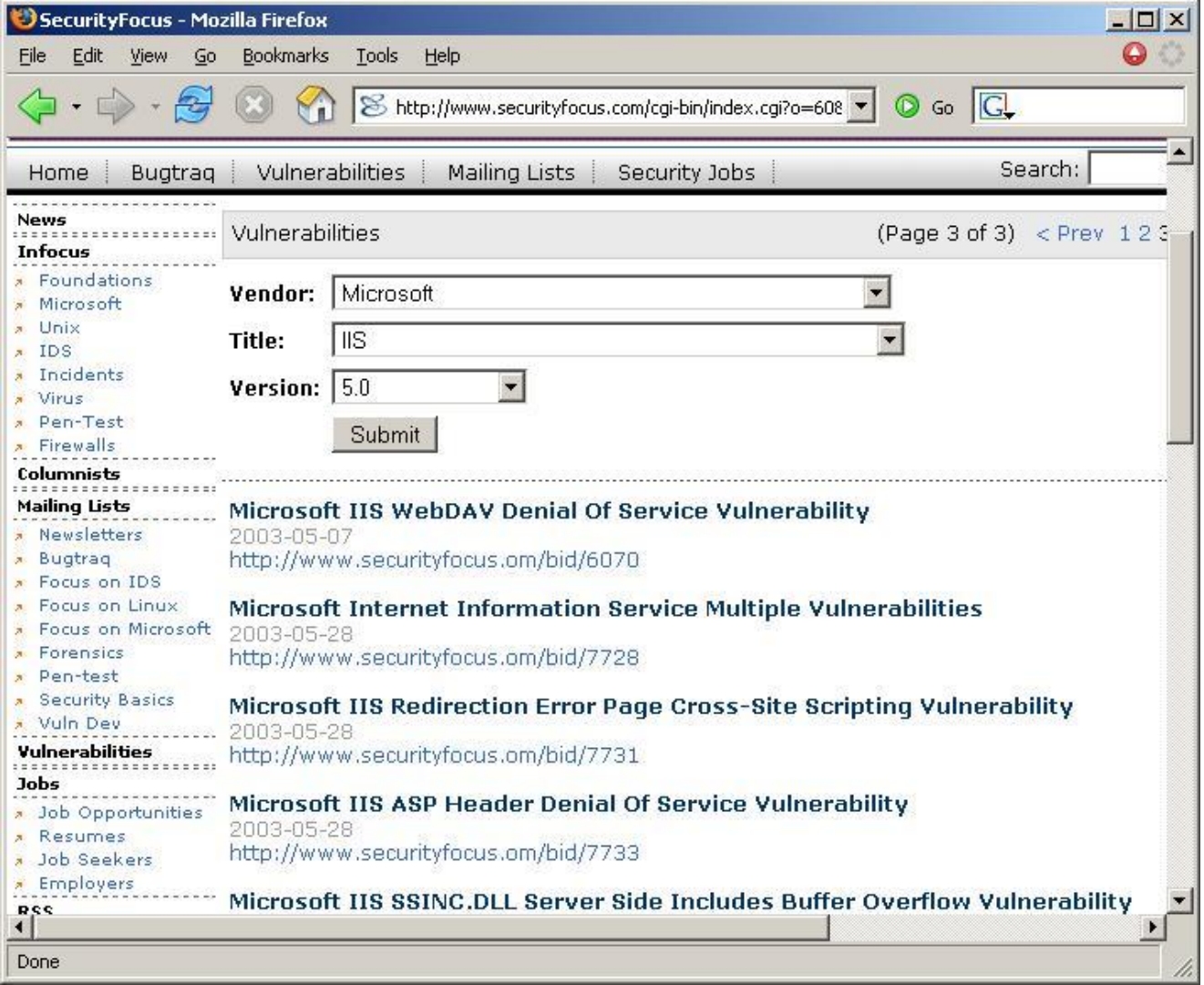
Fingerprint com o **NMAP**

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**

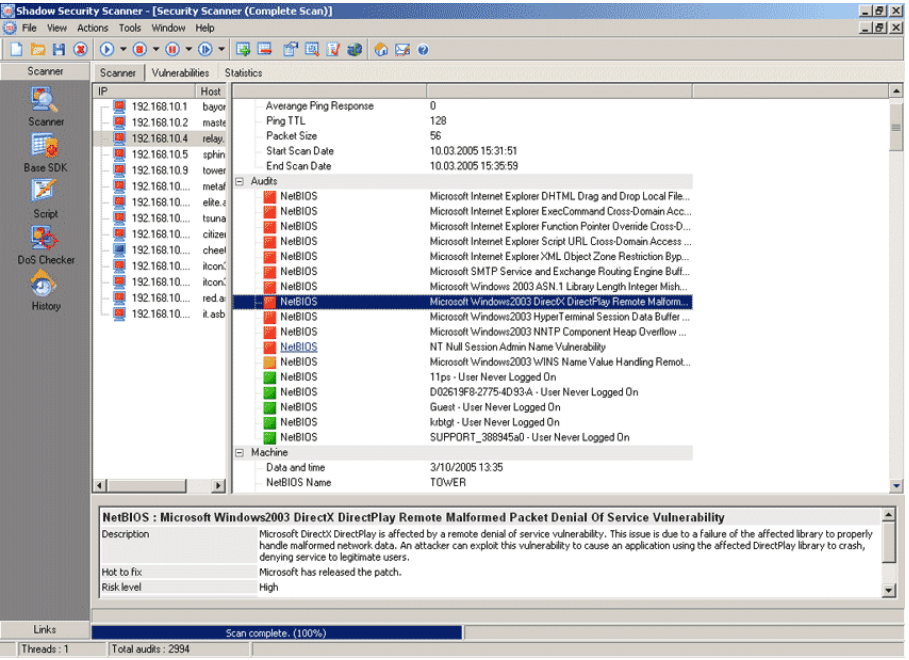
```
1524/tcp open   ingreslock?
2049/tcp open   rpcbind
2121/tcp open   ftp          ProFTPD 1.3.1
3306/tcp open   mysql        MySQL 5.0.51a-
|  mysql-info: Protocol: 10
```



Pesquisa manual por Falhas

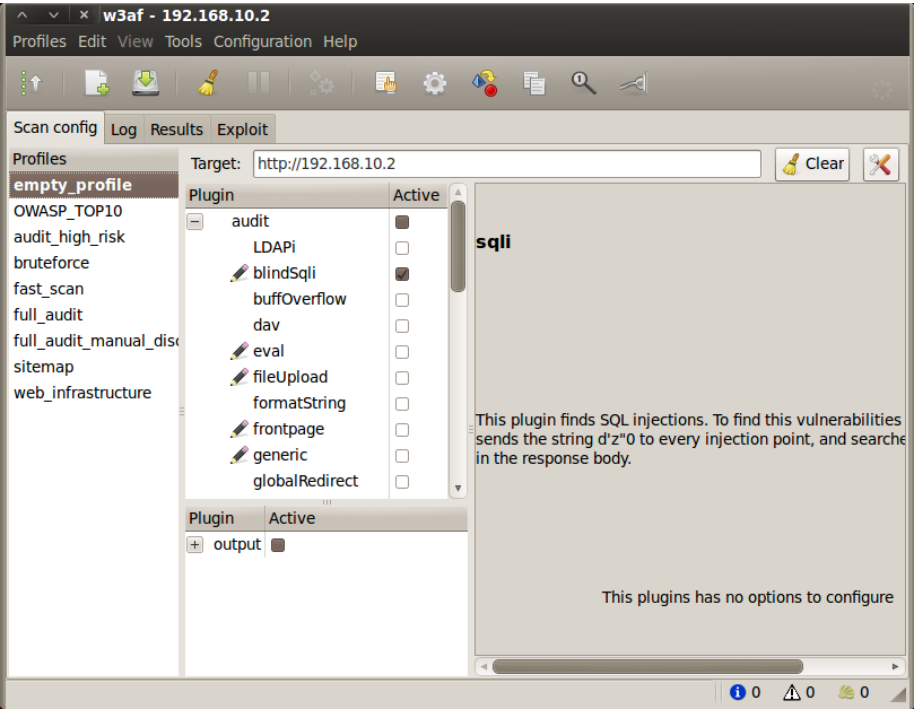
SecurityFocus

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.