Análise de banners

Análise de informações de banners é conhecido como Banner Grabbing.

Consiste na coleta de dados e informações do alvo usando como fonte os banners de servidores, serviços ou sistemas operacionais utilizados, como por exemplo, o servidor web Apache ou IIS, banco de dados MySQL ou SQL Server, proxy Squid entre outros.

Os banners são na realidade páginas avisos ou assinaturas com informações sobre o respectivo serviço, servidor (Figura 1) ou sistema operacional, como por exemplo uma página de erro de um servidor web ou proxy.

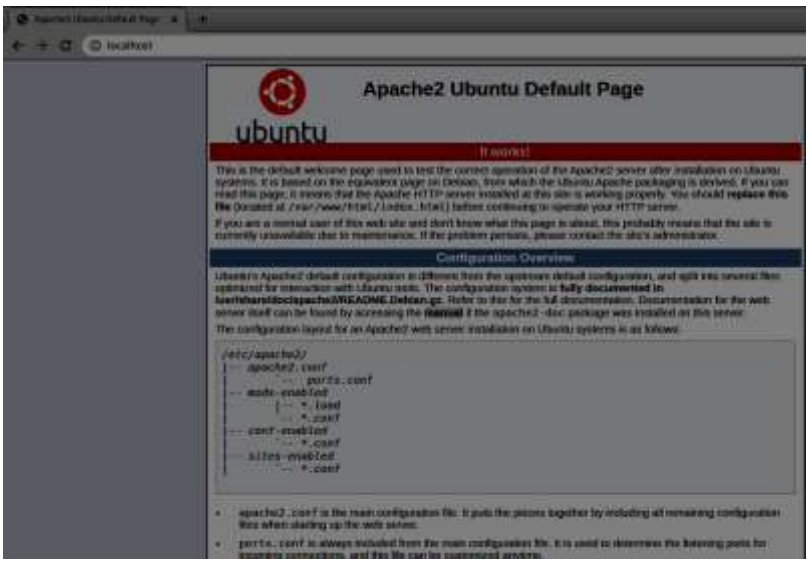

Figura 1. Banner do servidor http Apache.

netcat (nc)

Uma ferramenta muito importante na prática de capturas de banners de servidores e sistemas é o netcat. O netcat vem de net (rede) e cat (captura).

Dessa forma o netcat pode ser usado para fazer a captura do banner do http ou https em suas diversas portas utilizadas.

O comando a seguir faz a varredura do servidor web na porta 80 do domínio solicitado.

Caso após o comando a conexão seja estabelecida com o servidor deve-se inserir o parâmetro:

READ/HTTP/1.0

Que solicita ao servidor que o cabeçalho HTTP seja exibido contendo várias informações.

```
# nc -v www.ifms.edu.br 80
Connection to www.ifms.edu.br 80 port [tcp/http] succeeded!
```

READ/HTTP/1.0
HTTP/1.1 400 Bad Request
Date: Thu, 10 Dec 2020 23:38:47 GMT
Server: Apache/2.4.7 (Ubuntu)
Content-Length: 306
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
Your browser sent a request that this server could not understand.

<hr>
<address>Apache/2.4.7 (Ubuntu) Server at www.ifms.edu.br Port 80</address>
</body></html>

As informações exibidas são importantes, pois podemos determinar o tipo de sistema operacional (Linux Ubuntu), o tipo e versão do servidor web (Apache versão 2.4.7) e que a porta utilizada para o servico http é a 80.

Para conexões https (http + SSL), que geralmente usa a porta 443, podemos utilizar o openssl de acordo com o comando a seguir:

# openssl s_client -quiet -connect www.ifms.edu.br:443
depth=2 OU = GlobalSign Root CA - R3, O = GlobalSign, CN = GlobalSign
verify return:1
depth=1 C = BE, O = GlobalSign nv-sa, CN = GlobalSign RSA OV SSL CA 2018
verify return:1
depth=0 C = BR, ST = Mato Grosso do Sul, L = Campo Grande, O = "Inst Fed de Educ, Ciencia e Tec de Mato Grosso do Sul", CN = www.ifms.edu.br
verify return:1
READ/HTTP/1.0
HTTP/1.1 400 Bad Request
Date: Fri, 11 Dec 2020 00:15:14 GMT
Server: Apache/2.4.7 (Ubuntu)
Content-Length: 307
Connection: close
Content-Type: text/html; charset=iso-8859-1

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
</p>
<hr>
<address>Apache/2.4.7 (Ubuntu) Server at www.ifms.edu.br Port 443</address>
</body></html>
```

Novamente a consulta nos retorna que a porta o sistema operacional, o tipo e versão do servidor web e que a porta 443 está ativa.

Usando nmap para scanear banners

O nmap apresenta a flag -A que é utilizada para capturar banners deservidores. O comando pode ser utilizado como a seguir:

nmap -A www.ifms.edu.br -PO

```
Starting Nmap 7.60 ( https://nmap.org ) at 2020-12-10 21:34 -04
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000021s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE   VERSION
80/tcp   open  http      Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
631/tcp  open  ipp       CUPS 2.2
| http-methods:
|_  Potentially risky methods: PUT
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: CUPS/2.2 IPP/2.1
|_http-title: Home - CUPS 2.2.7
3306/tcp open  mysql     MySQL 5.7.32-0ubuntu0.18.04.1
| mysql-info:
|   Protocol: 10
|   Version: 5.7.32-0ubuntu0.18.04.1
|   Thread ID: 7
|   Capabilities flags: 65535
```

| Some Capabilities: Support41Auth, Speaks41ProtocolNew, Speaks41ProtocolOld, SupportsTransactions, LongPassword, FoundRows, LongColumnFlag, SwitchToSSLAfterHandshake, ODBCClient, IgnoreSpaceBeforeParenthesis, SupportsLoadDataLocal, InteractiveClient, ConnectWithDatabase, IgnoreSigpipes, SupportsCompression, DontAllowDatabaseTableColumn, SupportsAuthPlugins, SupportsMultipleResults, SupportsMultipleStatments
| Status: Autocommit
| Salt: \x0Bk\x04#k\x1E%i\x1B^R\x03\x12IV0ZP50
|_ Auth Plugin Name: 96
9050/tcp open tor-socks Tor SOCKS proxy
| socks-auth-info:
| Username and password
|_ No authentication
| socks-open-proxy:
| status: open
| versions:
| socks4
|_ socks5
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 0 hops
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.78 seconds