LAB - SEM 05 - Info Gathering Web - VPN

LAB01: Microsoft-IIS/7.5

Usamos a dica do Longatão das massas:

> Quando você faz um http request para o servidor informando um arquivo de um determinado tipo (php, aspx, jsp) o servidor vai ver se compreende aquele tipo de solicitação.
> Por exemplo, no caso de chegar um request para aspx ele vai verificar:
> - Eu entendo aspx? não.. retorna erro default..
> - Eu entendo aspx? sim.. responde com a tecnologia que ele tem.
> E com isso acabamos descobrindo a tecnologia utilizada. (By Longatto)
>
> Revisar o módulo "Information Gathering - WEB", aula "Conhecendo o Curl"

Então executamos um curl direcionado ao host 172.16.1.60

```
curl -v 172.16.1.60
```

A resposta trouxe o seguinte:

```
└─# curl -v 172.16.1.60/arquivo.html
*   Trying 172.16.1.60:80 ...
* Connected to 172.16.1.60 (172.16.1.60) port 80
> GET /arquivo.html HTTP/1.1
> Host: 172.16.1.60
> User-Agent: curl/8.4.0
> Accept: */*
>
< HTTP/1.1 404 Not Found
< Content-Type: text/html
< Server: Microsoft-IIS/7.5
< X-Powered-By: ASP.NET
< Date: Sun, 21 Jan 2024 00:50:46 GMT
< Content-Length: 1245
<
```

LAB02: ASP.NET

Respondido no lab passado

LAB03: 2.0.50727

Para encontrar essa informação, continuamos mudando a extensão do arquivo aleatório solicitado.
Quando solicitamos aspx, a key chegou: