Enumerando HTTP

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

O que buscamos?

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

+ Versões do Web Server (IIS, Apache, Nginx, etc)
+ Tecnologias utilizadas (PHP. ASP, JSP, etc)
+ Métodos aceitos (PUT, POST, DELETE, etc)

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

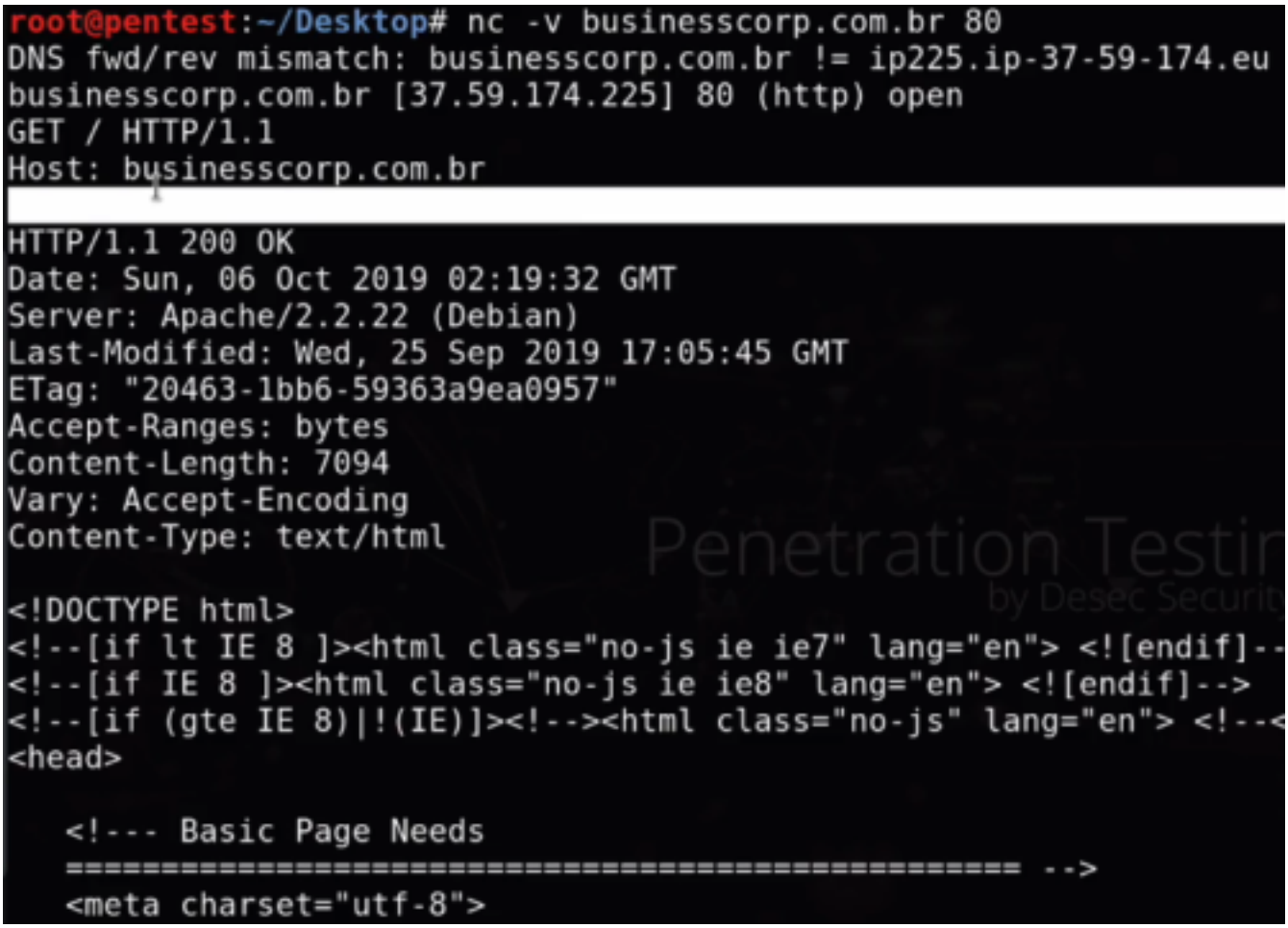
Como fazer?

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

+ Portas comuns: 80,8080,81,8081 (podemos ter um servidor web rodando em qualquer porta TCP)
+ Versões do protocolo: HTTP/1.0 | HTTP/1.1 (usar o Host:)
+ Requisições: GET | HEAD | OPTIONS
+ Utilitários: nc | curl | telnet

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

+ Importância de passar o host quando for usar o HTTP/1.1:
→ as vezes o mesmo endereço de IP pode ser usado para diferentes host, por ser compartilhado (isso também pode acontecer quando for usado um proxy)



+ OBS: As vezes a versão da tecnologia não é evindenciada de cara numa requisição do tipo GET.
Para resolver isso, devemos fazer uma busca por arquivos que usem
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

essa tecnologia, mesmo que eles não existam.
+ Exemplo: Identifiquei que é usada a tecnologia ASP. Pra que eu saiba qual a versão, devo fazer uma requisição por arquivos dessa extensão:
GET /index.aspx HTTP/1.0