**FUNDAMENTOS DE ETHICAL HACKING –**

**ANOTAÇÕES E OBSERVAÇÕES PRÁTICAS**

**2021**

**Seção 2:**

**Ethical Hacking – Fundamentos e Metodologia**

**Pentest/*Teste de Invasão:***

*Tipos:*

* *Black Box: Teste "cego", realizado em um sistema remoto. Não há conhecimento prévio da estrutura da empresa.*
* *Gray Box: Com conhecimento* parcial da estrutura empresarial.
* White Box: Teste realizado com total conhecimento da estrutura do alvo. Ou seja, quão longe alguém que possui acesso interno total à empresa chegaria, e qual o escopo do dano?

*Fases:*

* Reconhecimento: identificação de dados da empresa;
* Varredura: com as info. obtidas anteriormente, realiza um trabalho de "verificação" de acordo com a necessidade. Um exemplo seria uma varredura de IPs, após a obtenção da range de IPs da empresa.
* Ganho de acesso: com a obtenção das informações anteriores, utiliza-se técnicas de invasão no serviço;
* Mantendo o acesso: após a invasão, o pentester vai utilizar métodos - como um backdoor - para que, se necesssário futuramente, realize outro acesso no sistema antes invadido.
* Cobrindo rastros: Usando mecanismos específicos, o pentester cobre seus rastros.

**Seção 4:**

**Fundamentos de Protocolos de Redes e Linux**

**Modelo OSI x Modelo TCP/IP:**

O Modelo TCP/IP possui 4 camadas:

* Aplicação
* Transporte
* Internet
* Acesso à rede

*Protocolos:*

* DNS - Tradução de nomes para endereços (cisco.com >> 198.133.219.25, ou vice-versa). Devido à sua importânica, é alvo constante de ataques como, por exemplo, o spoofing.
* HTTP e HTTPS - protocolo de transferência de hipertexto, onde o cliente efetua uma requisição em uma página web. Usa-se os métodos GET ("Pega" a página, depois da requisição) e POST ("posta" dados colocados, por exemplo, em um formulário.) HTTP não possui criptografia, HTTPS sim.
* Acesso Remoto - operação de acesso remoto a um computador.

*Camada de transporte:*

* TCP - Protocolo CONFIÁVEL, porém lento, que oferece mecanismos de retransmissão de pacotes e controle de fluxo de conexão. Também permite estabelecimento de conexões.
* UDP - Protocolo NÃO CONFIÁVEL, porém rápido, que é utilizado para, por exemplo, streaming de vídeos, comunicação de protocolos de roteamento, entre outros.

*Endereço de aplicações por porta:*

* Em um servidor, é possível se ter várias portas, cada uma associada a um serviço. Serviços como o DNS podem utilizar mais de uma porta (DNS utiliza duas portas, TCP e UDP).

*Faixas de portas TCP/UDP:*

* 0 a 1023: Portas conhecidas (contato);
* 1024 a 49151: Portas Registradas (portas que seu computador abre para se conectar a algum local, e são aleatórias);
* 49152 a 65535: Portas Privadas e/ou Dinâmicas;

**Endereçamento IP:**

* IP: Endereço lógico que a máquina utiliza para navegar na internet/rede local. Pode ser obtido automaticamente, por DHCP, ou colocado manualmente. Um IP tem 32 bits, e é dividido em "pedaços" de 8 bits cada. 24 bits são dedicados à porção de rede, enquanto os outros 8 bits restantes são dedicados à porção de host.

Abaixo, tabela que indica classes de IP:



*Endereços IP: Uni, multi e broadcast:*

* Unicast: endereço lógico em uma máquina, único à esta.
* Broadcast: endereço que, quando recebe uma informação, replica a rede toda.
* Multicast: replica informações a um pedaço limitado da rede, não a todos como o broadcast.

*Endereços públicos e privados:*

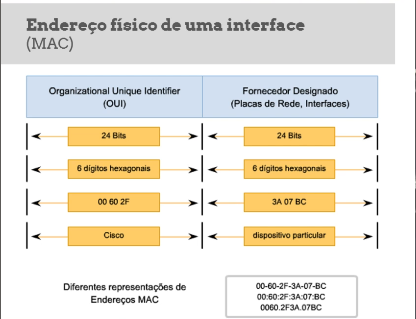
* Público: endereço usado na internet, dado pelo provedor de internet. Pode ser acessado por qualquer um.
* Privadas: Podem ser usadas em rede interna, não é acessível.

*Endereço físico de uma interface (Endereço MAC):*

O End. Lógico é configurado, já o MAC é fixo ao hardware. É um endereço hexadecimal, notações de 0 - 9 e A – F.

Endereços MAC são compostos de 12 dígitos. Os primeiros 6 dígitos representam o fabricante, enquanto os últimos 6 dígitos identificam o dispositivo.

Abaixo, figura que apresenta informações mais detalhadas sobre Endereços MAC:



*Protocolo ARP:*

Protocolo que mapeia endereços IP para endereços MAC. Caso deseje realizar uma comunicação com um IP qualquer (nesse caso, 10.10.10.3), o protocolo ARP, então, realiza um broadcast com a informação de que “alguém está procurando esse IP e seu endereço MAC”. A máquina dona do IP, após receber este broadcast, responde à maquina que realizou o pedido, e compartilha seu endereço MAC físico.

**Linux Cheat Sheet**

clear: limpa a tela de comandos;

pwd: indica a pasta atual;

ls: lista o conteúdo da pasta atual;

ls -l: mostra conteúdo extra;

ls -l (arquivo): lista apenas o arquivo alvo;

rm (alvo) : apaga o arquivo/pasta alvo;

mkdir (nome) : cria um novo diretório;

cd .. : volta um “caminho” para trás;

cd / : volta para a raíz;

vim (arquivo) **ou** vi (arquivo) **ou** nano (arquivo) : abre o editor de texto Vim/Vi/Nano;

cat (arquivo) : apresenta o conteúdo do arquivo diretamente no terminal, sem a necessidade de abrí-lo;

cat (arquivo) | more : “pausa” a tela, enquanto apresenta o conteúdo do arquivo. Ao apertar espaço, ele passa para a próxima página. Para sair, basta apertar **Q**;

cat (arquivo) | less : possui a mesma função que o more, mas apresenta o arquivo de uma forma mais flexível, que permite que você desça e suba a tela, no estilo de um editor de textos;

cat (arquivo) | grep (filtro) : filtra o conteúdo do arquivo, para apresentar apenas as linhas que possuam o parâmetro do filtro;

head -(número de linhas) (arquivo) : mostra o conteúdo do arquivo diretamente no terminal, limitado pelo número de linhas escolhido previamente;

tail -(número de linhas) (arquivo) : mostra o conteúdo do arquivo diretamente no terminal, limitado pelo número de linhas escolhido previamente;

* **Exemplo**: head -4 arquivo apresentará as quatro **primeiras linhas** do arquivo, enquanto tail -4 arquivo apresentará as quatro **últimas linhas** do arquivo;

echo (texto) >> (arquivo) : **ADICIONA** uma nova linha ao arquivo, com o texto desejado;

echo (texto) > (arquivo) : **SUBSTITUI** todo o conteúdo do arquivo pelo texto desejado;

ifconfig : apresenta as configurações de endereço IP da(s) sua(s) placa(s) de rede;

ifconfig (interface, como por exemplo **eth0**) (IP desejado) netmask (máscara do IP desejado) : configura o endereço IP;

ifconfig (interface) down: desliga a interface especificada no comando;

ifconfig (interface) up: liga a interface especificada no comando;

who : mostra todos os logados no sistema;

whoami : mostra qual seu usuário;

ps : mostra os processos do usuário.

ps -e : mostra todos os processos do sistema.

(comando) –help : mostra todas as opções possíveis com um determinado comando;

man (comando) : abre um documento detalhado, que apresenta informações e opções disponíveis para um determinado comando;

useradd (usuário) : cria um novo usuário;

adduser (usuário) : cria um usuário, pasta root, grupo e senha. É mais prático;

cat /etc/passwd : mostra todos os usuários;

cat /etc/shadow : mostra todos os usuários, mais suas senhas criptografadas

chown (usuário):(grupo) : muda o dono do diretório atual para o indicado no comando.

chmod (parâmetro) **ou** chmod (parâmetro 1) + (parâmetro 2) : muda as permissões, de acordo com o(s) parâmetro(s) indicados no comando. Alguns dos parâmetros:

* rwx (read, write, execution – leitura, escrita e execução);
* ugo (user, group, others – usuário, grupo, outros);
* a (all - todos);

Exemplo:

chmod g+x (arquivo) : modifica as permissões para que o grupo especificado seja capaz de executar o arquivo indicado. O grupo ao qual a permissão está sendo dada é indicado ao escrever-se o comando ls -l (arquivo alvo). O símbolo + adiciona a permissão de execução à lista de permissões desse usuário em relação a esse comando.

chmod g-x (arquivo) : modifica as permissões para que o grupo especificado não seja mais capaz de executar o arquivo indicado. O grupo de qual a permissão está sendo revogada é indicado ao escrever-se o comando ls -l (arquivo alvo). O símbolo - remove a permissão de execução da lista de permissões desse usuário em relação a esse comando.

chmod a+w (arquivo) : modifica as permissões para que **todos** (all) sejam capazes de executar o arquivo indicado.

**Seção 5: Reconhecimento**

**WHOIS e Lookup de DNS:**

O WhoIs, utilizando um domínio e/ou endereço IP pré-conhecidos, é capaz de extrair informações antes desconhecidas sobre o alvo do pentest.

Utilizando como exemplo o site *defhack.com*, obtemos as seguintes informações:

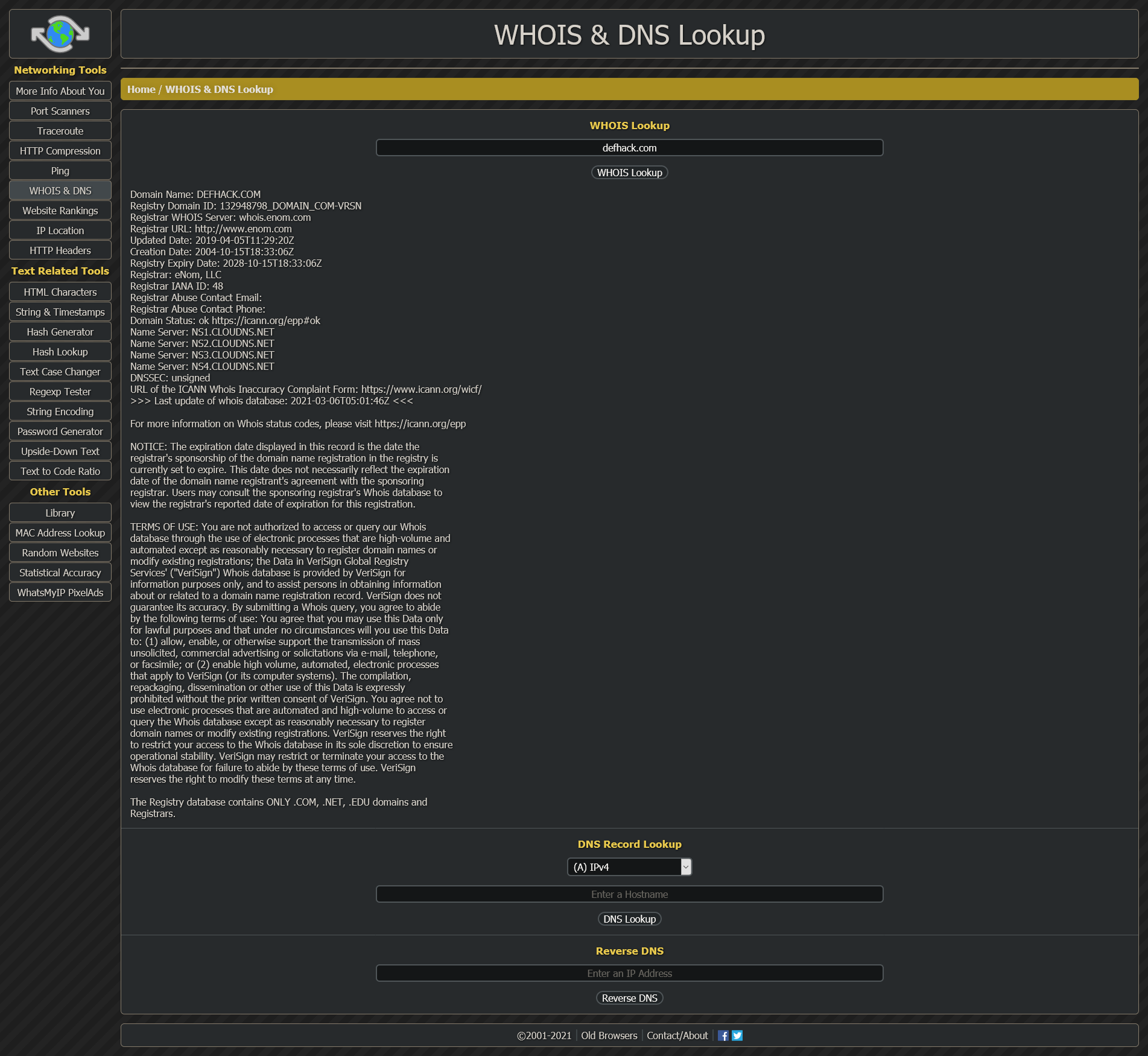
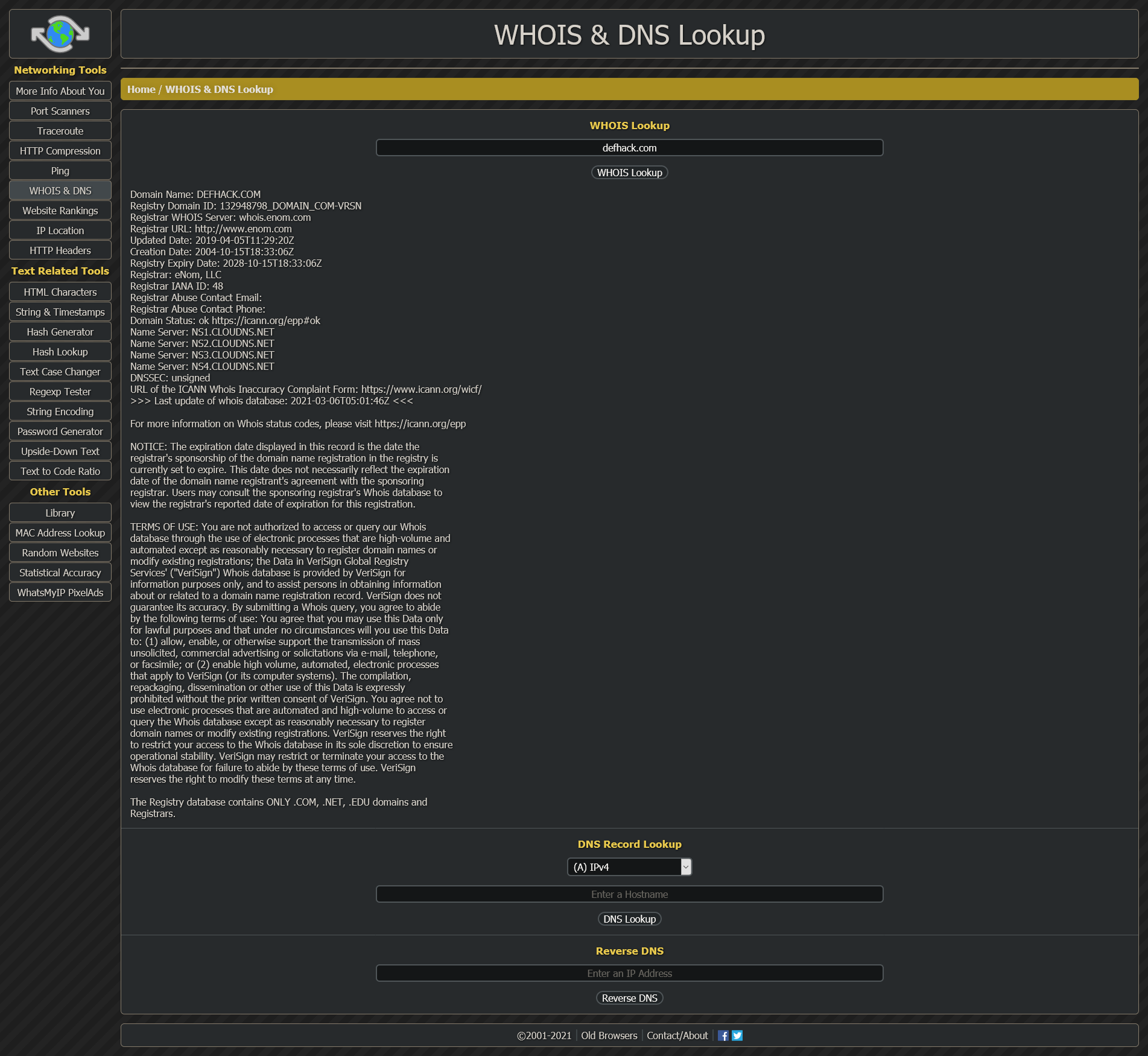


Imagem com zoom:



Abaixo, explicação de alguns dos termos vistos:

* **Domain Name:** Nome do domínio pesquisado;
* **Registrar:** A empresa utilizada para fazer o registro do domínio;
* **Name Server:** Servidores DNS do domínio;
* **Updated Date:** data de atualização;
* **Creation Date:** data de criação;
* **Expiration Date:** data de vencimento do domínio;

Muitos ataques de engenharia social se aproveitam de dados obtidos por meio de uma consulta de IP em um site com serviço Whois, como o ***whatsmyip.org*** ou ***registro.br***.

O site ***registro.br*** conta com um modo “avançado” de pesquisa, onde apresenta diversas informações com um certo grau de confidencialidade, informações que poderiam ser usadas para ataques com cunho malicioso, baseados, por exemplo, em Engenharia Social.

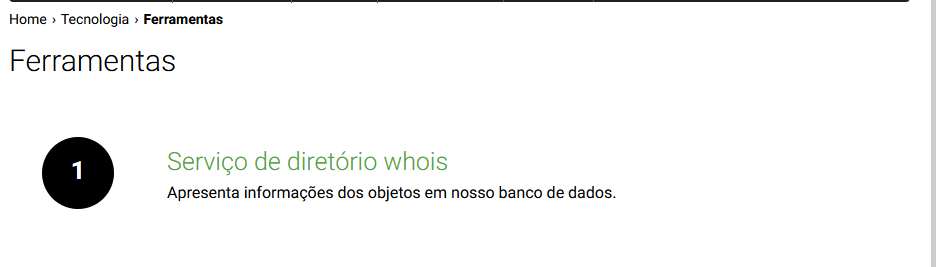
Abaixo, um passo-a-passo para a realização de uma consulta com detalhes avançados no site ***registro.br***.

1 - Entre no site **registro.br**;

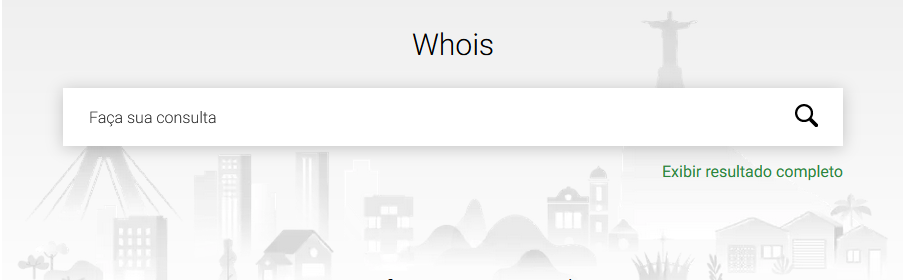
2 – Na aba **Tecnologia**, clique em **Ferramentas**;



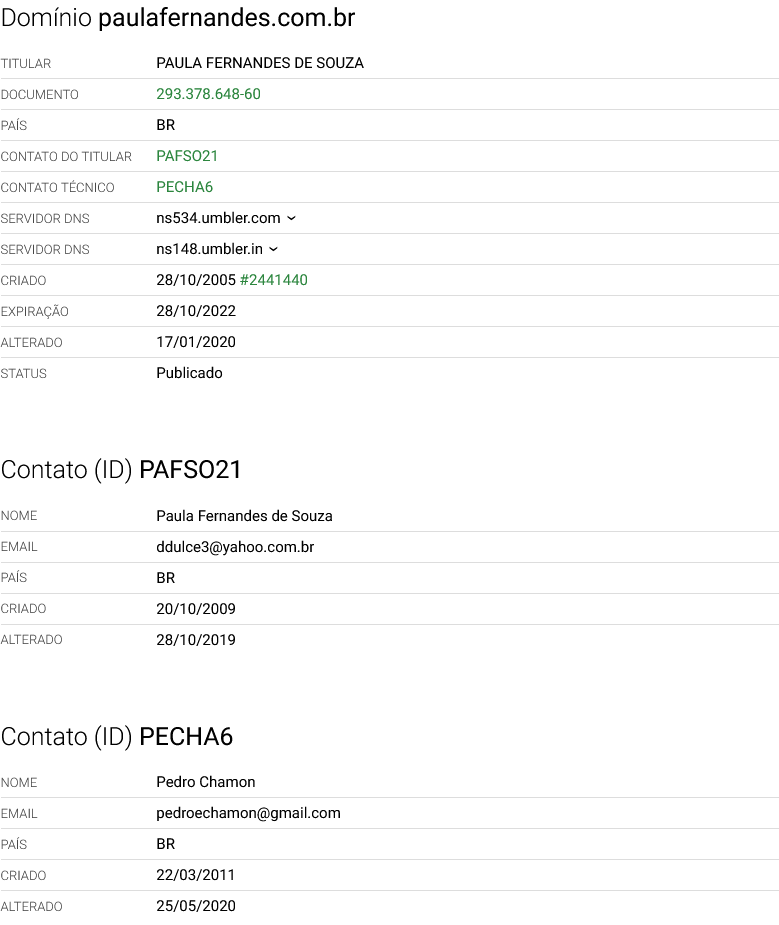
3 – Em **Ferramentas**, clique em **Serviço de Diretório Whois**;



4 – Na barra de pesquisa, escreva o IP/domínio desejado. Após concluir, clique em **Exibir Resultado Completo**. No exemplo das fotos, usaremos o domínio da cantora Paula Fernandes, **paulafernandes.com.br**;



Estes são os resultados:



Repare nos resultados: o site apresenta o CPF com o qual o domínio foi registrado, além de informações como o nome do registrante, país, e endereço de e-mail. Em outros casos, é possível obter até mesmo o endereço do registrante.

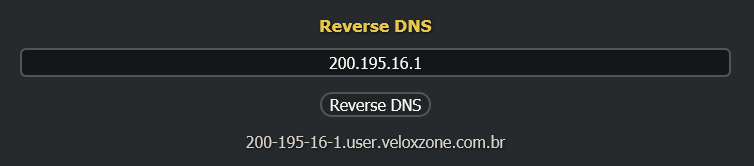
No caso de um lookup com o IP **200.195.16.1**, recebe-se os seguintes resultados:



Pontos importantes:

* **NetRange**: Apresenta a faixa de endereçamento IP onde este endereço está incluído;
* **NetName**: LACNIC-200. Bloco 200 é o bloco de IPs da América Latina, e LACNIC é o Registro de Endereços da Internet para a América Latina e o Caribe. Já é possível saber que este IP está na América Latina.

Como obter mais informações relacionadas a este IP? Basta realizar uma busca de DNS reverso:



Essa busca retornará o domínio correspondente ao endereço IP que, no caso acima, é **200-195-16-1.user.veloxzone.com.br**.

Para saber a localização aproximada de um endereço IP, pode se utilizar a função de **IP Location** do site.

Utilizando o IP **200.131.250.5**:

