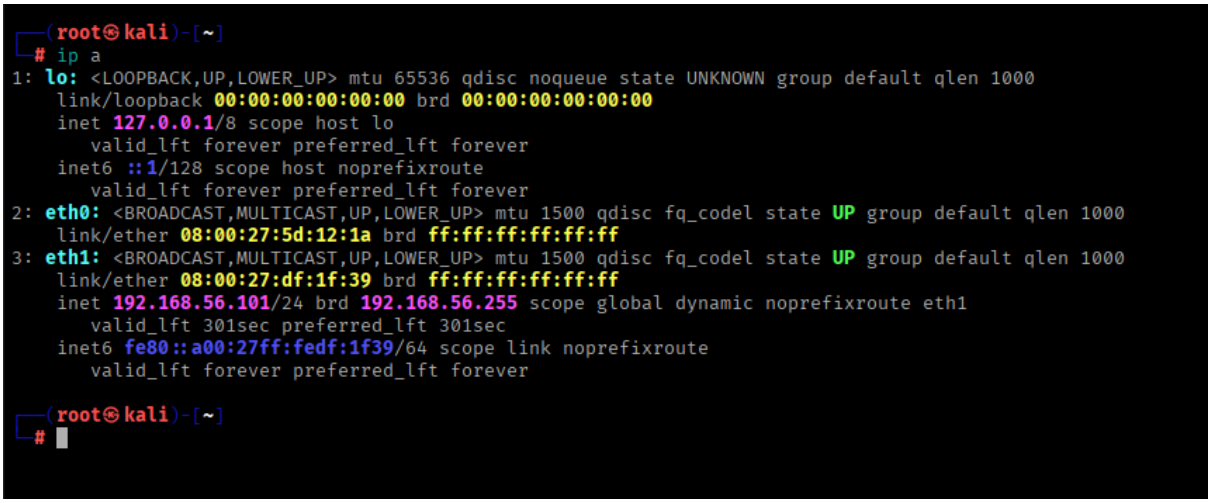
Relatório de Evidências Técnicas: Operação Deathstar

Analista: Leonardo Pereira Pinheiro **Alvo:** 192.168.56.105 **Resumo:** Documentação cronológica da exploração, desde o reconhecimento inicial até o comprometimento total do sistema (Root).

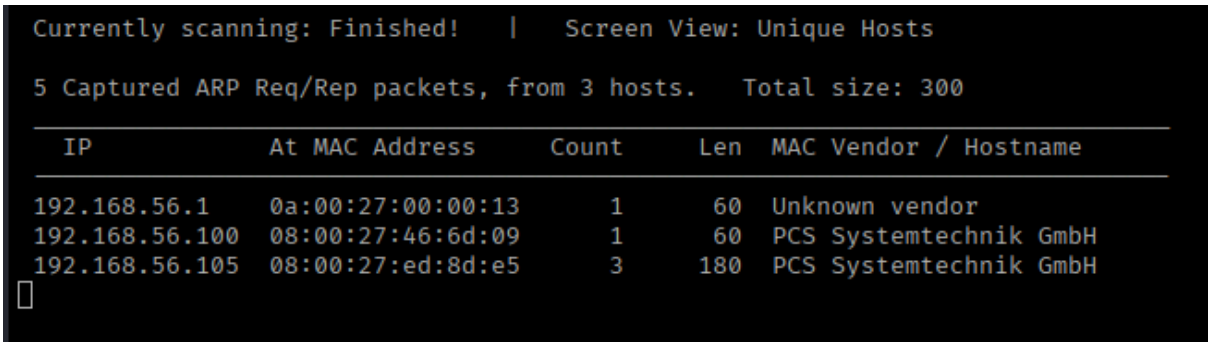
Configuração e Descoberta de Rede

Esta página mostra o início do reconhecimento da rede.

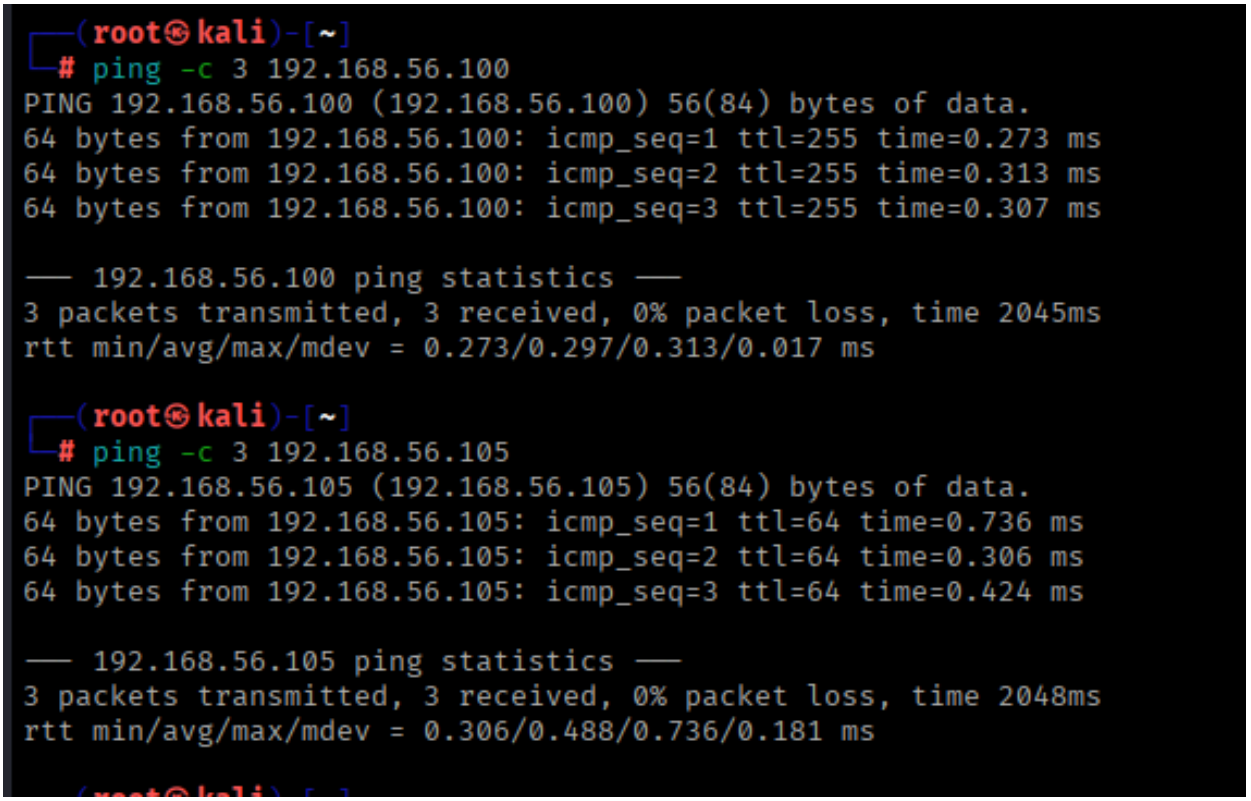
- **Verificação de IP:** O comando `#ip a` é usado para verificar o endereço IP da máquina atacante (Kali Linux).



- **Varredura ARP:** Uma tabela ARP é exibida, identificando os hosts ativos na rede. O alvo foi identificado como **192.168.56.105** (PCS Systemtechnik GmbH).



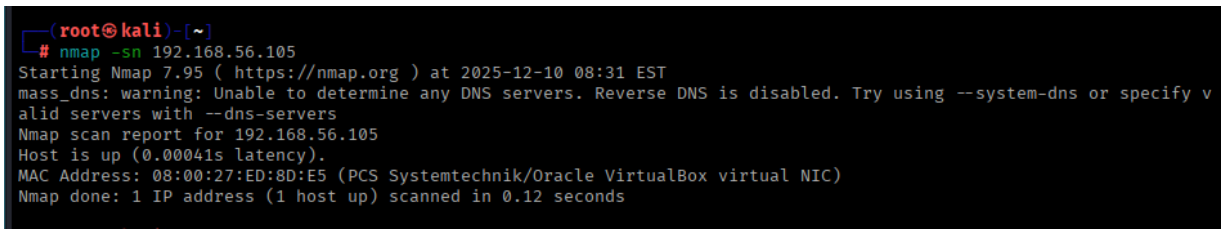
- **Teste de Conectividade:** O comando `ping` confirma que a máquina alvo (192.168.56.105) está respondendo e acessível.



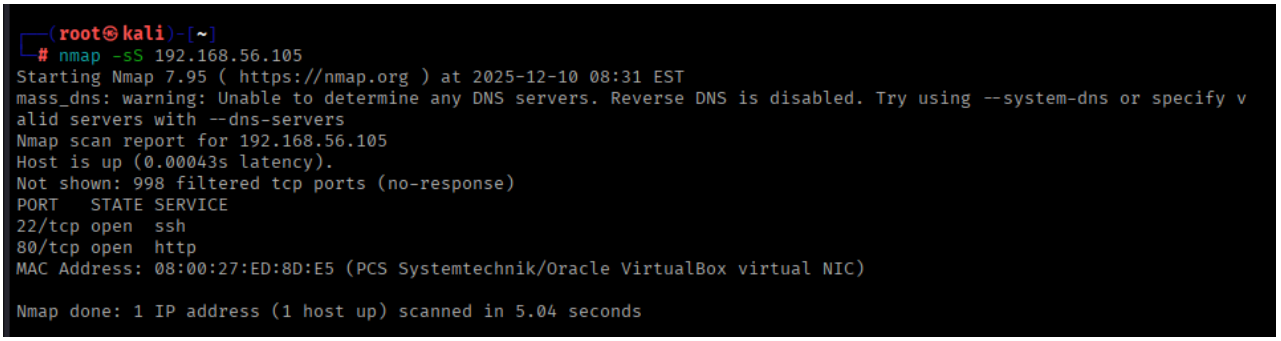
Escaneamento de Portas (Nmap)

Aqui ocorre a enumeração dos serviços rodando no alvo.

- **Varredura Simples:** O comando `nmap -sn` verifica se o host está "vivo".



- **Varredura de Portas:** O comando `nmap -sS` identifica as portas abertas. Foram encontradas a **22 (SSH)** e a **80 (HTTP)**.

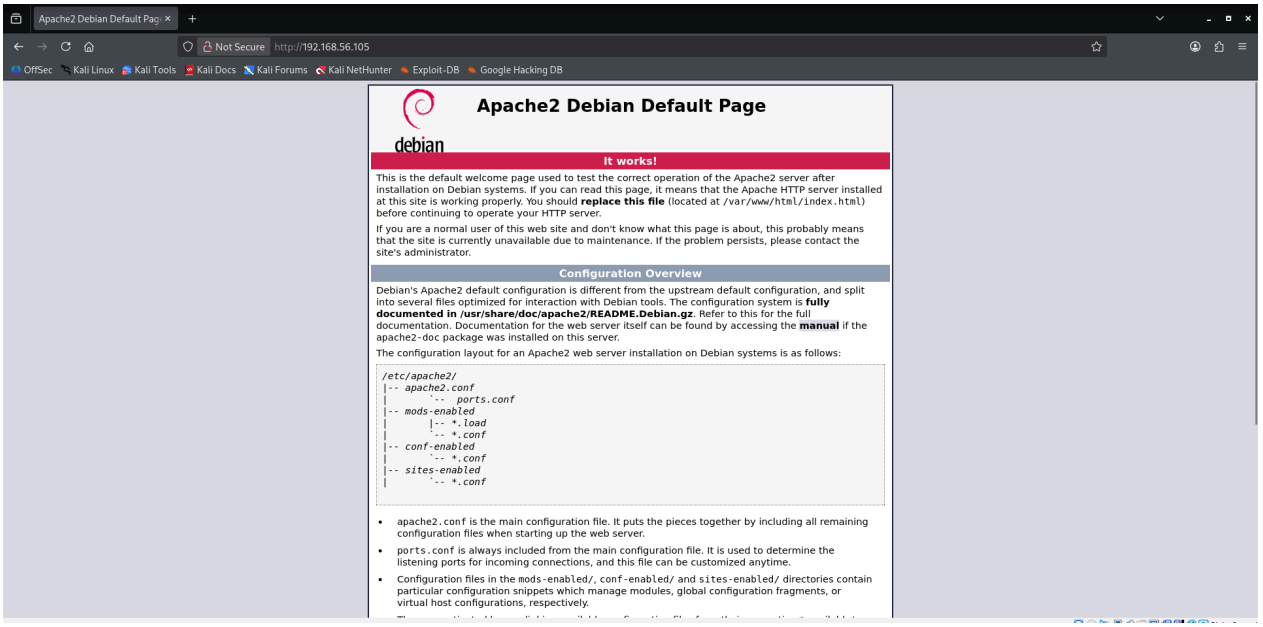


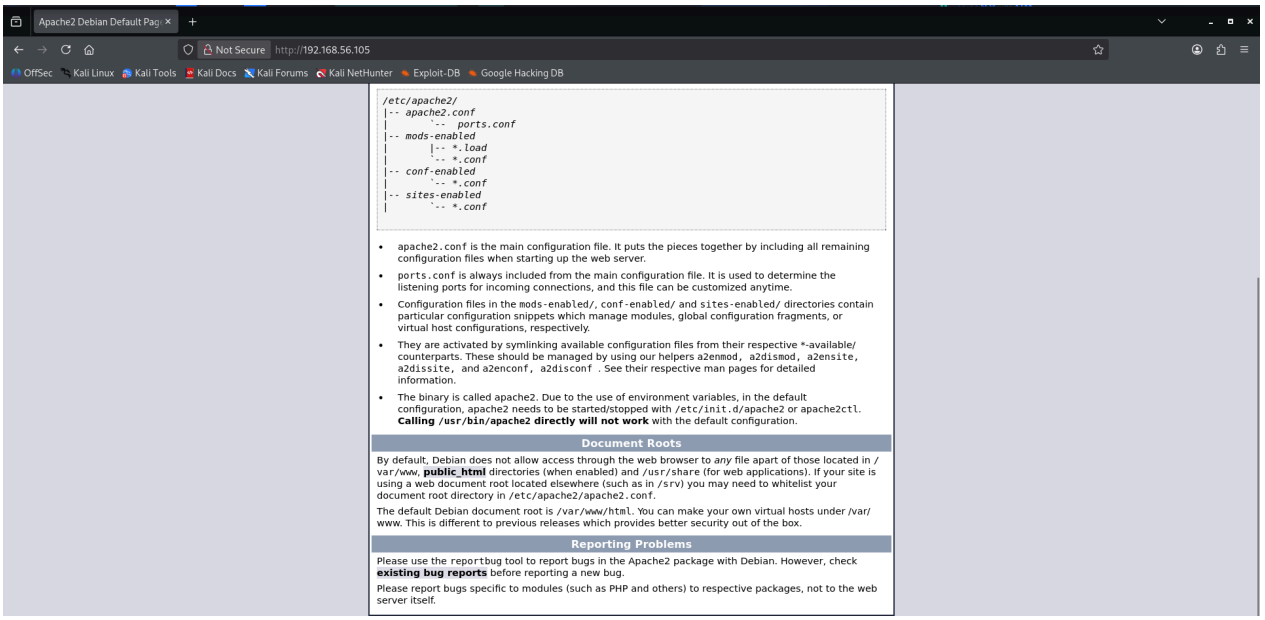
- **Detecção de Versão e Vulnerabilidades:** O comando `nmap -sV --script vuln` detalha as versões: OpenSSH 8.4p1 e Apache 2.4.56. O script também encontrou o arquivo `/robots.txt`.

Enumeração Web (Feroxbuster)

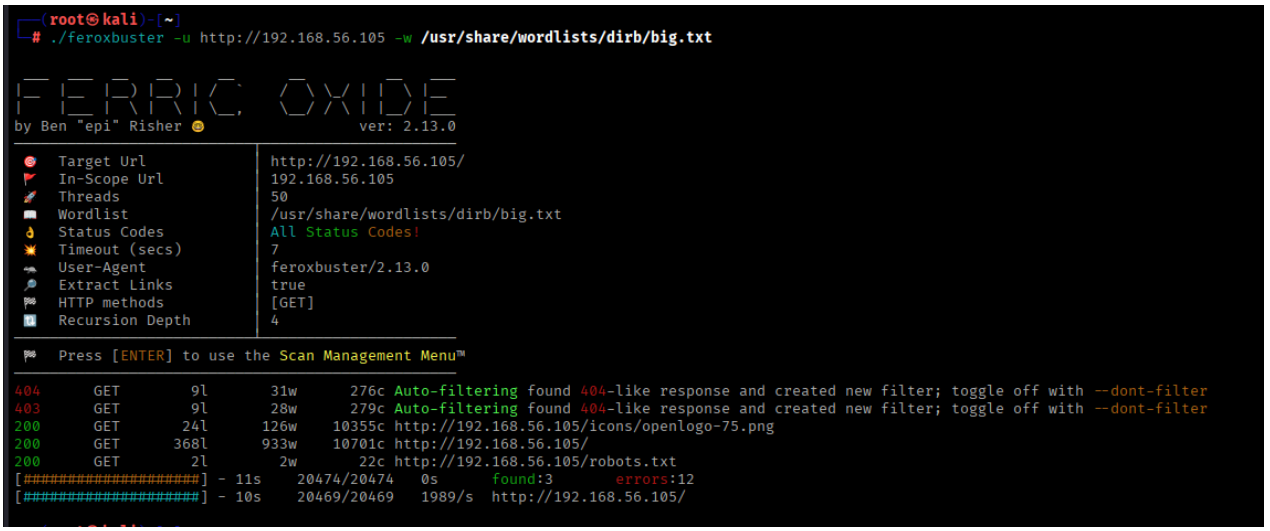
O atacante começa a investigar o servidor web na porta 80.

- **Página Padrão:** O navegador mostra a página padrão do Apache "It works!", confirmando que o servidor web está ativo.





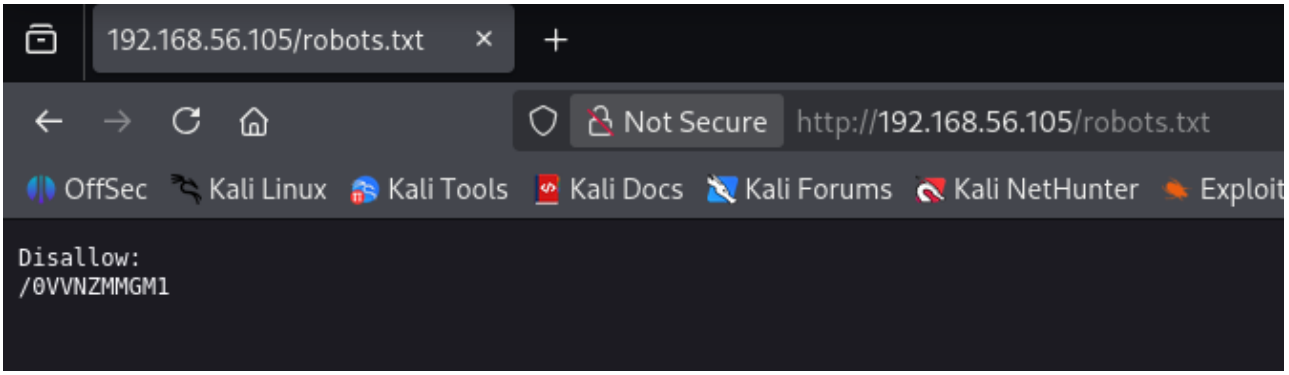
- **Brute-Force de Diretórios:** A ferramenta `feroxbuster` (ou similar visualizada no log) começa a testar diretórios usando uma wordlist (`big.txt`) para encontrar pastas ocultas.



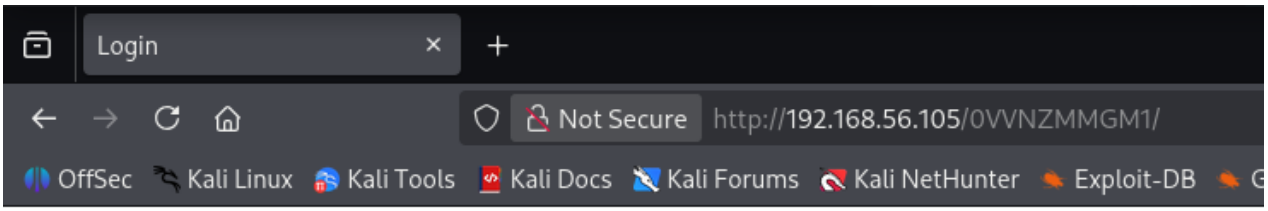
Robots.txt e Login Oculto

Descoberta de caminhos sensíveis.

- **Robots.txt:** O navegador acessa `robots.txt`, que revela uma entrada "Disallow" para o diretório `/0VVNZMMGM1`.



- **Página de Login:** Ao acessar esse diretório oculto, é encontrado um formulário de login.



Login

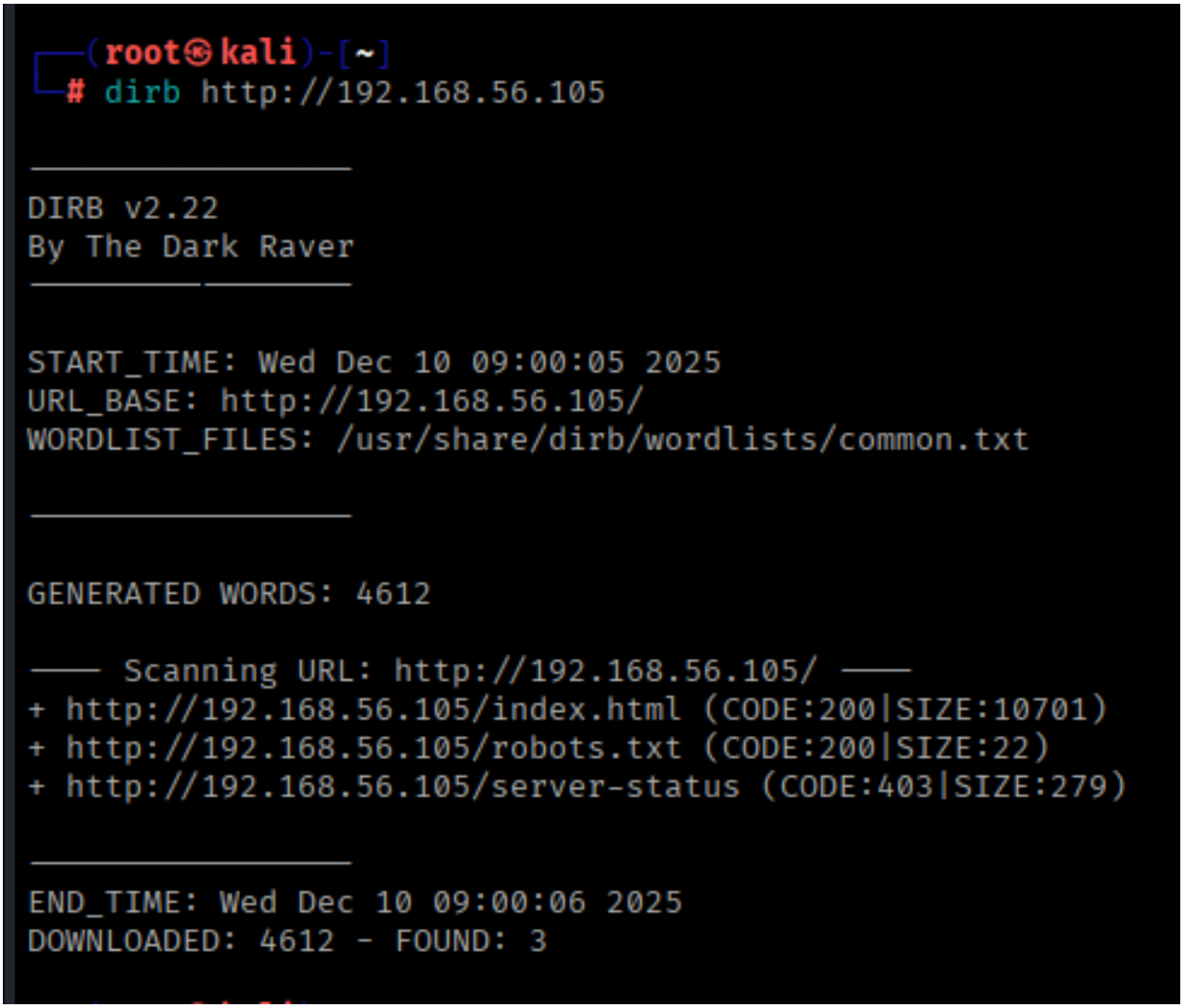
Nome de Usuário: Senha: Entrar

- **Gobuster:** O comando `gobuster` confirma a existência dos diretórios, retornando status 200 (OK) para `robots.txt` e 403 (Forbidden) para outros arquivos.

```
┌──(root㉿kali)-[~]
└─# gobuster dir -u http://192.168.56.105 -w /usr/share/wordlists/dirb/big.txt
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.56.105
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htpasswd            (Status: 403) [Size: 279]
/.htaccess            (Status: 403) [Size: 279]
/robots.txt           (Status: 200) [Size: 22]
/server-status        (Status: 403) [Size: 279]
Progress: 20469 / 20469 (100.00%)
===============================================================
Finished
===============================================================
```

Varredura Dirb

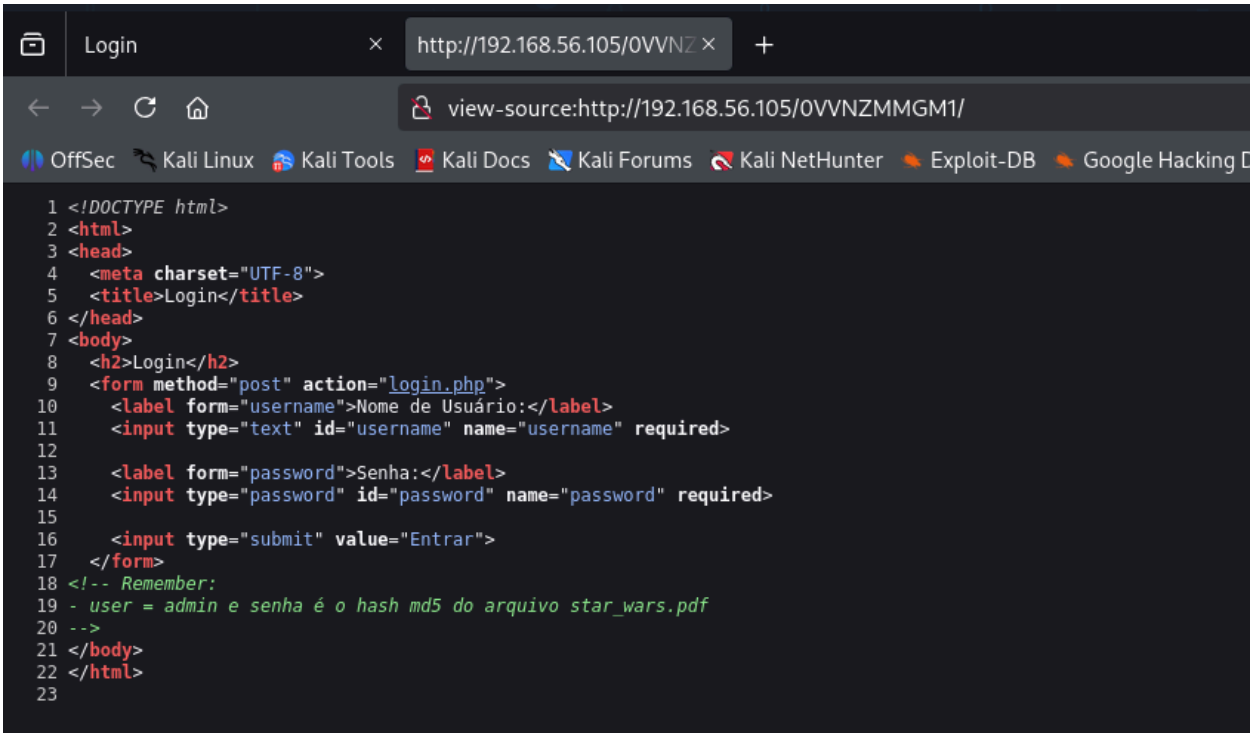
- **Confirmação:** A ferramenta `dirb` é executada para confirmar a enumeração de diretórios, encontrando `index.html` e `robots.txt`.



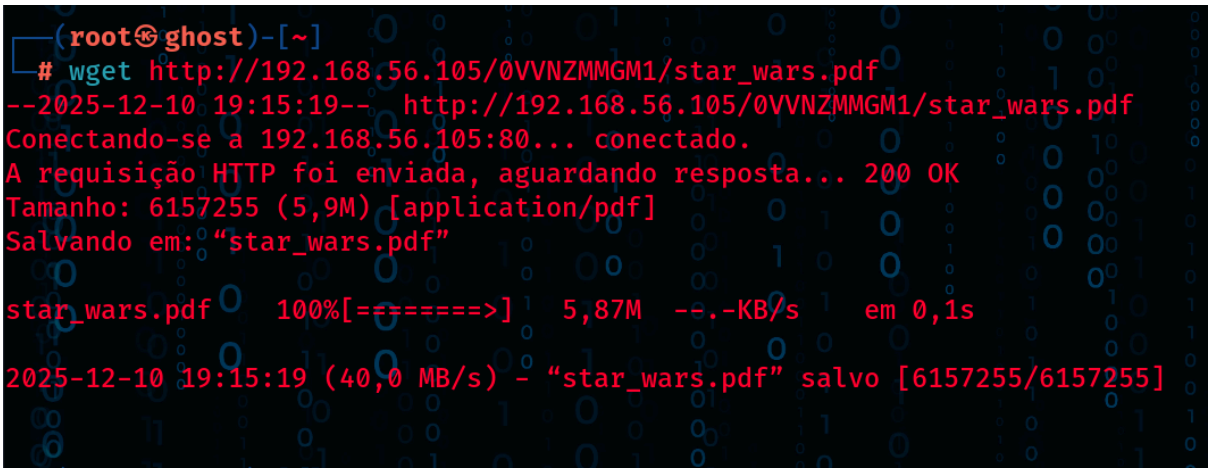
Código Fonte e Download de PDF

O primeiro grande achado (Information Disclosure).

- **Código Fonte (View Source):** Ao inspecionar o HTML da página de login (`/0VVNZMMGM1/`), um comentário revela a credencial: usuário `admin` e a senha é o hash MD5 do arquivo `star_wars.pdf`.



- **Wget:** O comando `wget` é usado para baixar esse arquivo PDF do servidor para a máquina do atacante.



Análise do PDF e Cálculo do Hash

Obtenção da primeira senha.

- **Conteúdo do PDF:** As imagens mostram o conteúdo do arquivo baixado, um trabalho acadêmico sobre Star Wars.

UNIVERSIDADE FEDERAL DE SÃO CARLOS – UFSCAR

CENTRO DE EDUCAÇÃO E CIÊNCIAS HUMANAS – CECH

PROGRAMA DE PÓS-GRADUAÇÃO EM IMAGEM E SOM

DEPARTAMENTO DE ARTES E COMUNICAÇÃO – DAC

Uma Análise do Story World de Star Wars: A New Hope e Star Wars: The Force Awakens

ANTONIO HENRIQUE GARCIA VIEIRA

São Carlos – SP
2017

Introdução

Devido a constante atualização dos meios de comunicação e das formas de comunicar, o conteúdo do que é expresso acaba sofrendo modificação ou mesmo tornando-se um conteúdo completamente novo. Podemos encontrar na própria tradição oral[1], que acompanha a humanidade desde os primórdios, as várias versões de uma mesma história, contada com nuances, transforma-se em outroconto, completamente diferente.

Com o passar do tempo e a evolução da sociedade temos a criação da escrita, um reflexo da necessidade da organização do tempo e do espaço proporcionado por novas relações sociais (MCLUHAN; 2003), a escrita representou também uma forma de se registrar a memória e colocar aquilo que a tradição oral carregava em uma mídia duradoura. A transição da oralidade para a escrita acarretou também mudanças nas maneiras com que as histórias eram contadas, tanto na forma em que era contada, com o propósito de cativar um leitor ou sujeitas aos caprichos de estilo do meio em que estivessem publicadas (SANTAELA; 2004), algo que com o passar dos anos podemos encontrar nas adaptações de diferentes mídias. .

Um caso de adaptação que podemos citar é o conto de H.P. Lovecraft chamado Nas Montanhas da Loucura (1936), que através de releituras acabou por influenciar inúmeras outras obras, até chegar ao cinema como O Enigma de Outro Mundo (1982) de John Carpenter. Ryan Lambie do site Den of Geek[2], aponta:

> *It's a well-known fact in geek circles that The Thing is an adaptation of sci-fi author John W Campbell's 1938 novella, Who Goes There. Already adapted once by Howard Hawks and Christian Nyby in 1951, it was Carpenter's rendition that hewed closer to the original story, wisely dumping the alien carrot of the Hawks' picture and reinstating Campbell's protean monster. But in his take on The Thing, Carpenter also brought something else to this chilly tale: a sense of apocalyptic doom, emphatically underlined by a conclusion that, unlike Campbell's*

[1] Segundo o dicionário Webster: as histórias, crenças, etc., que um grupo de pessoas compartilha por contar histórias e falar uns com os outros. (MERRIAN-WEBSTER, ***Definition of Tradition***; 2016. Disponível em: <http://www.merriam-webster.com/dictionary/oral%20tradition>. Acesso em 12 de nov. 2016. Tradução nossa.)

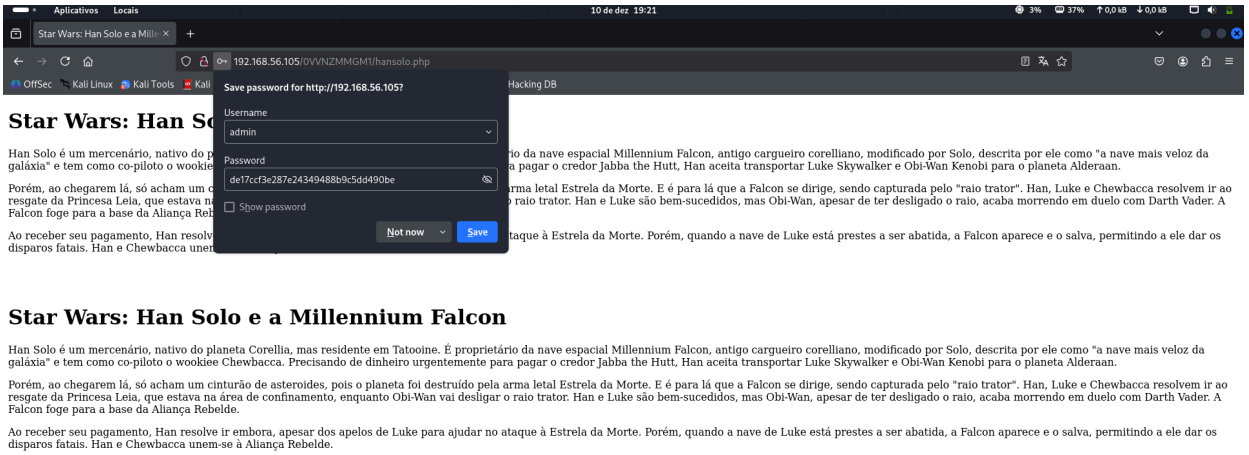
[2] LAMBIE, Ryan; **HP Lovecraft and his lasting impact on cinema**; 2011. Disponível em: <http://www.denofgeek.com/movies/18189/hp-lovecraft-and-his-lasting-impact-on-cinema#ixzz4HTDRq1Gp> Acesso em Acesso em 12 de nov. 2016.

- **MD5Sum:** O comando `md5sum star_wars.pdf` é executado no terminal. O hash gerado (`de17ccf...`) é a senha do usuário admin.

Área Admin (Han Solo) e Nova Dica

Acesso inicial e movimentação lateral.

- **Página Han Solo:** Após logar como admin, o atacante vê um texto sobre Han Solo.



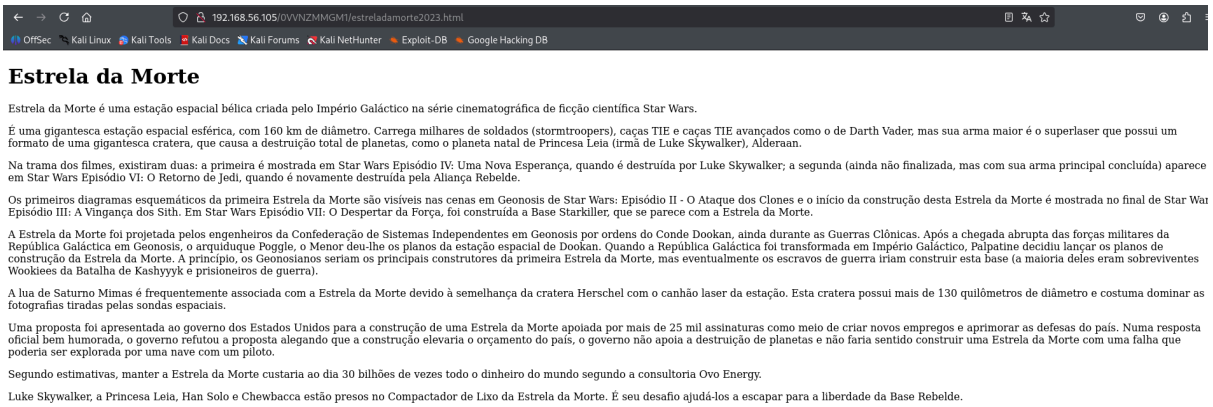
- **Nova dica no HTML:** O código fonte desta página (`hansolo.php`) revela o próximo passo: usuário `darth` para o diretório `/restrict98712`, com a senha escondida na página `estreladamorte2023.html`.

```
<!DOCTYPE html>
<html>

<head>
  <title>Star Wars: Han Solo e a Millennium Falcon</title>
</head>
<body>
  <h1>Star Wars: Han Solo e a Millennium Falcon</h1>

  <p>Han Solo é um mercenário, nativo do planeta Corellia, mas residente em Tatooine. É proprietário da nave espacial Millennium Falcon, antig

  <p>Porém, ao chegarem lá, só acham um cinturão de asteroides, pois o planeta foi destruído pela arma letal Estrela da Morte. E é para lá que

  <p>Ao receber seu pagamento, Han resolve ir embora, apesar dos apelos de Luke para ajudar no ataque à Estrela da Morte. Porém, quando a nave
</body>
<!--
- Remember:
- deixei a senha de "darth" para logar em 'restrict98712' na página "estreladamorte2023.html". Boa sorte!
-->
</html>

```

Wordlist Contextual (CeWL)

Preparação para o ataque ao usuário Darth.

- **Texto Alvo:** Mostra a página `estreladamorte2023.html` cheia de texto sobre a Estrela da Morte.



- **CeWL:** O comando `cewl` varre essa URL e cria um arquivo de texto (`palavras_estrela.txt`) contendo todas as palavras da página para usar como dicionário de senhas.

```
┌──(root㉿ghost)-[~]
└─# cewl -w palavras_estrela.txt http://192.168.56.105/0VVNZMMGM1/estreladamorte2023.html
CeWL 6.2.1 (More Fixes) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
```

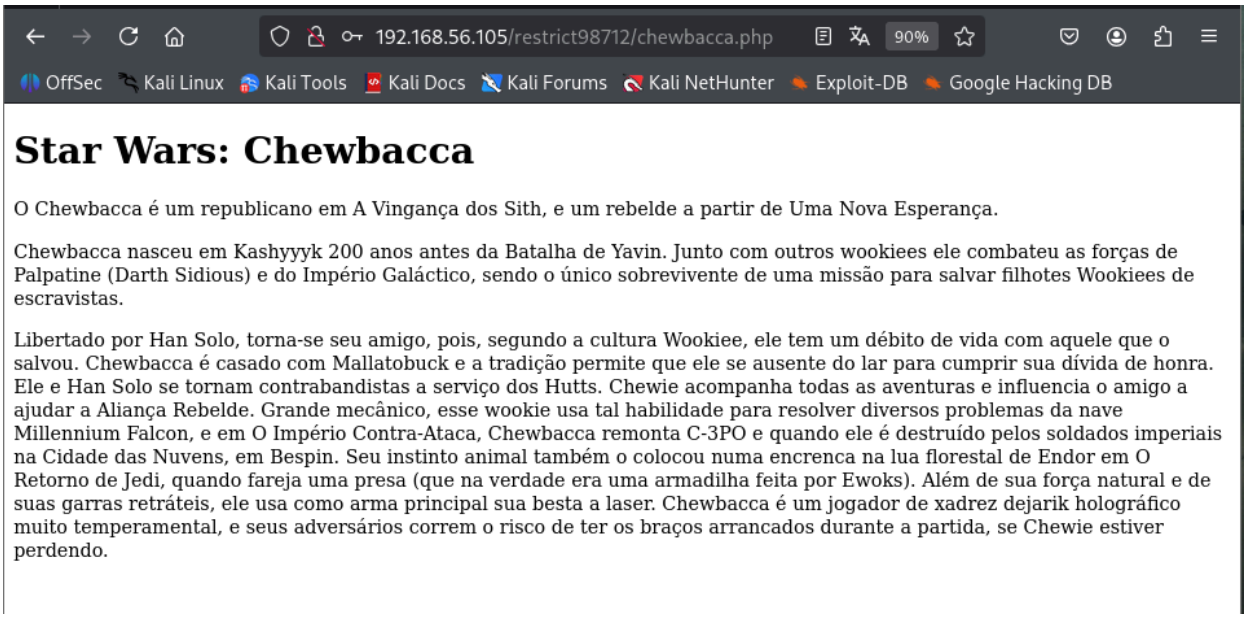
Hydra (Darth) e Página Chewbacca

Quebra da segunda senha.

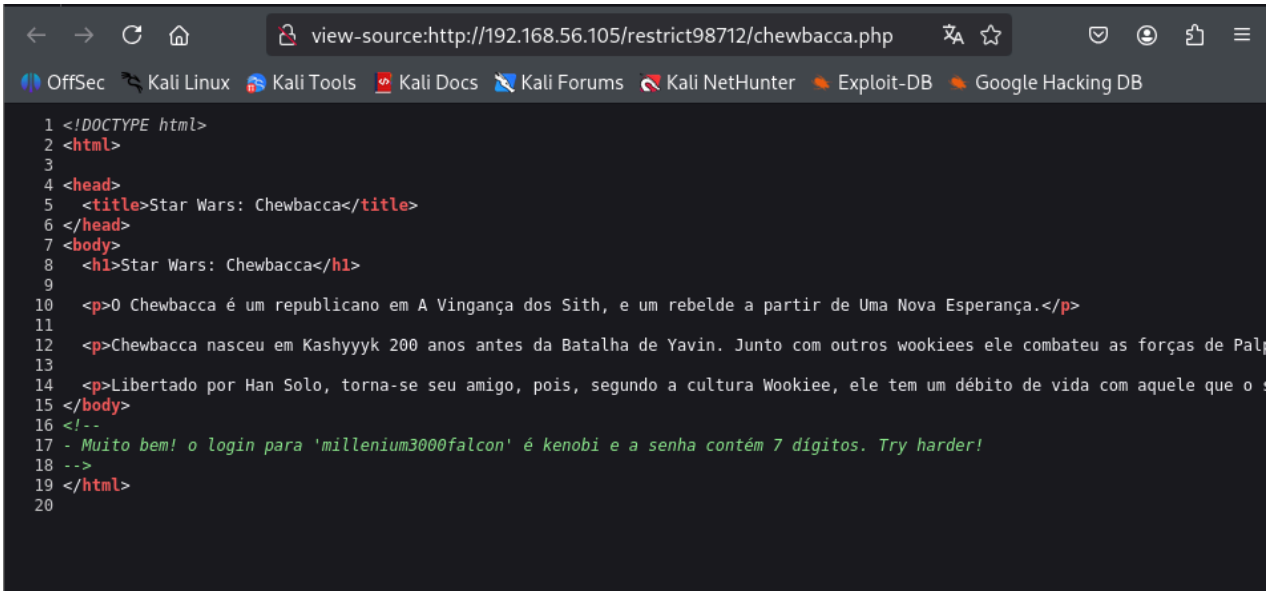
- **Ataque Hydra:** A ferramenta `hydra` usa a lista gerada pelo CeWL e descobre que a senha do usuário `darth` é **Chewbacca**.

```
┌──(root㉿ghost)-[~]
└─# hydra -l darth -P palavras_estrela.txt 192.168.56.105 http-post-form "/restrict98712/login.php:username=^USER^&password=^PASS^:F=Dad
os estão incorretos"
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal p
urposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-12-10 20:01:50
[DATA] max 16 tasks per 1 server, overall 16 tasks, 235 login tries (l:1/p:235), ~15 tries per task
[DATA] attacking http-post-form://192.168.56.105:80/restrict98712/login.php:username=^USER^&password=^PASS^:F=Dados estão incorretos
[80][http-post-form] host: 192.168.56.105   login: darth   password: Chewbacca
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-12-10 20:01:54
```

- **Página Chewbacca:** Após logar como Darth, acessa-se a página sobre o Chewbacca.



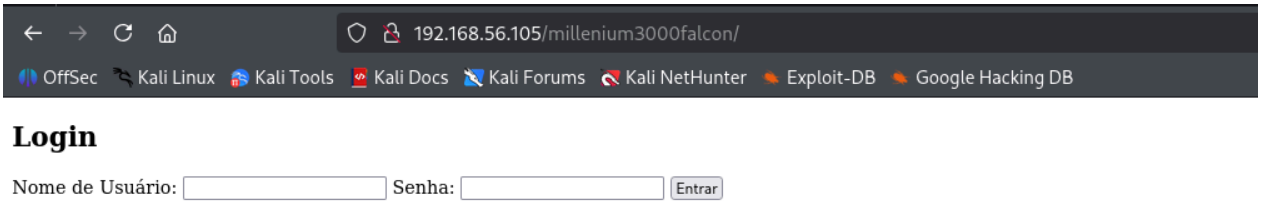
- **Dica Numérica:** O código fonte (`chewbacca.php`) dá a instrução para o próximo nível: usuário `kenobi`, diretório `/millenium3000falcon` e a senha tem **7 dígitos**.

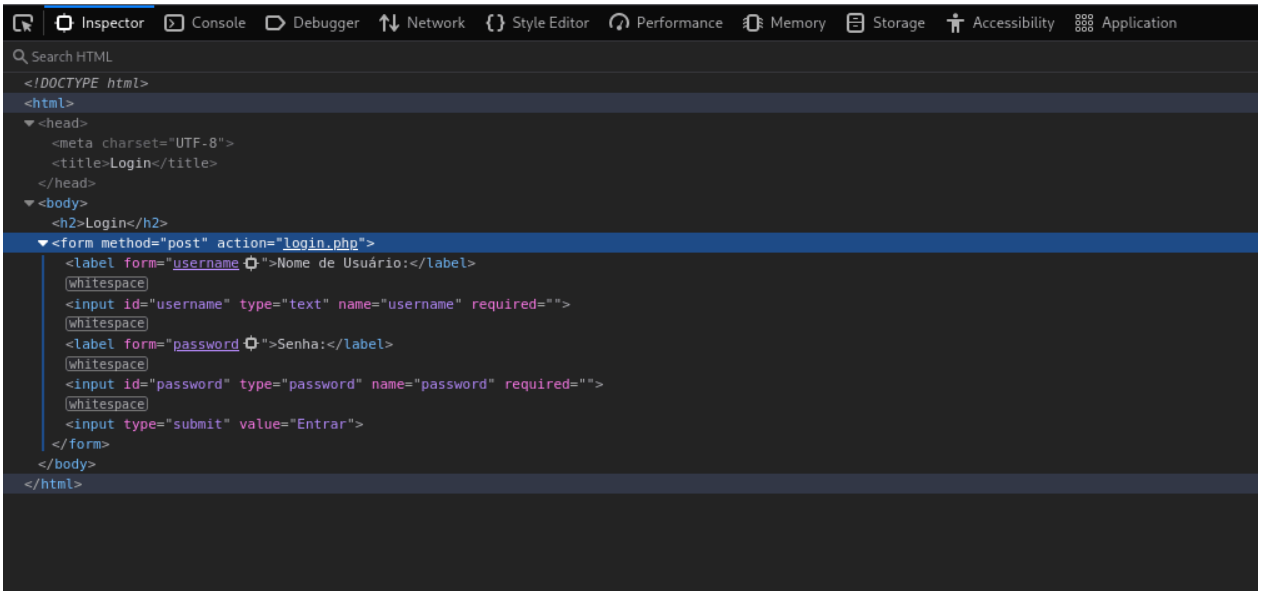


Geração de Wordlist Numérica (Crunch)

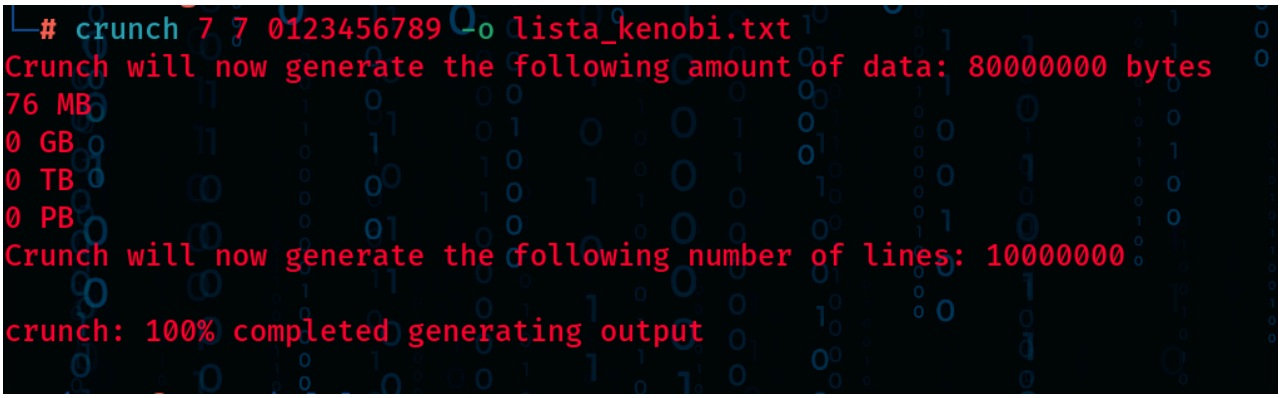
Preparação para o ataque ao usuário Kenobi.

- **Login Kenobi:** Mostra o formulário de login no novo diretório.





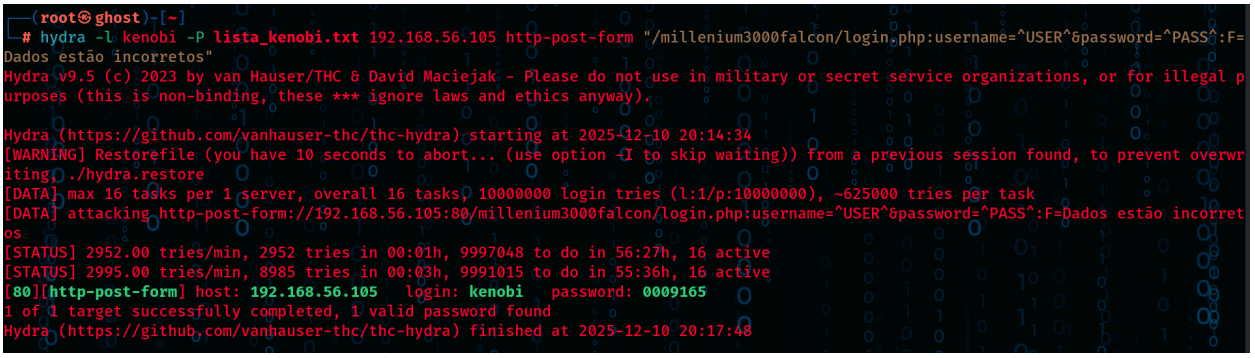
- **Crunch:** O comando `crunch 7 7 0123456789` gera um arquivo (`lista_kenobi.txt`) contendo todas as combinações possíveis de números com 7 dígitos.



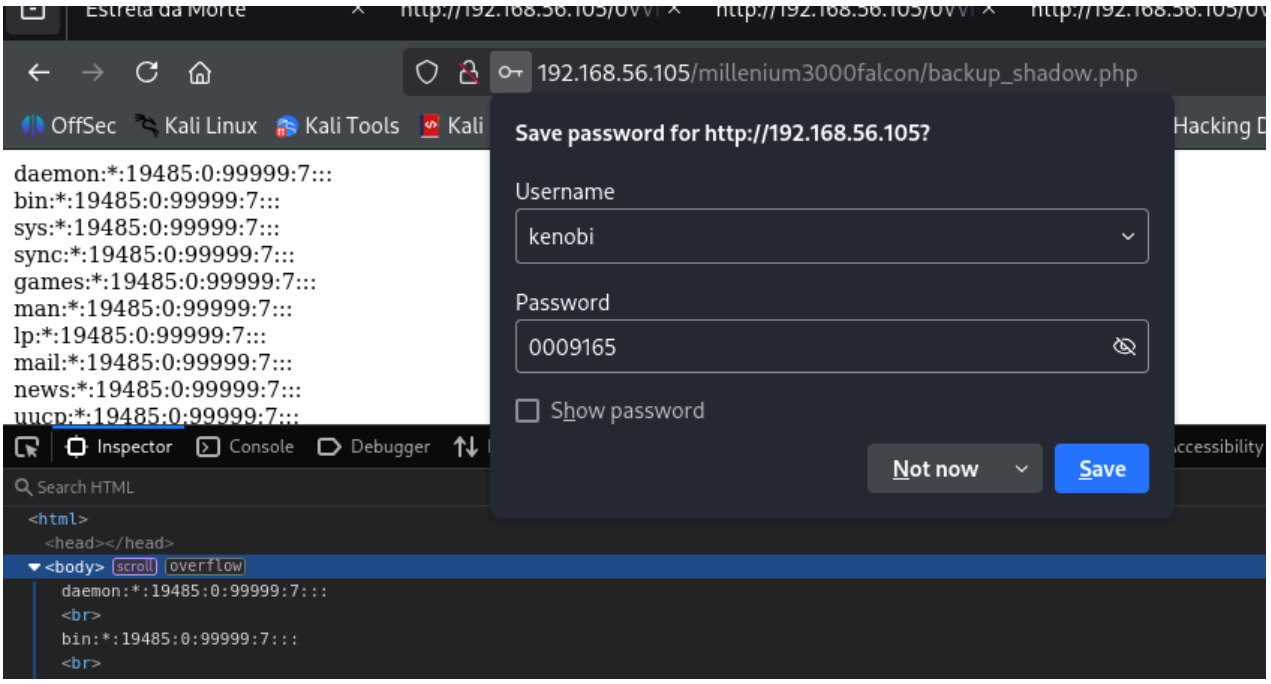
Hydra (Kenobi) e Vazamento Crítico

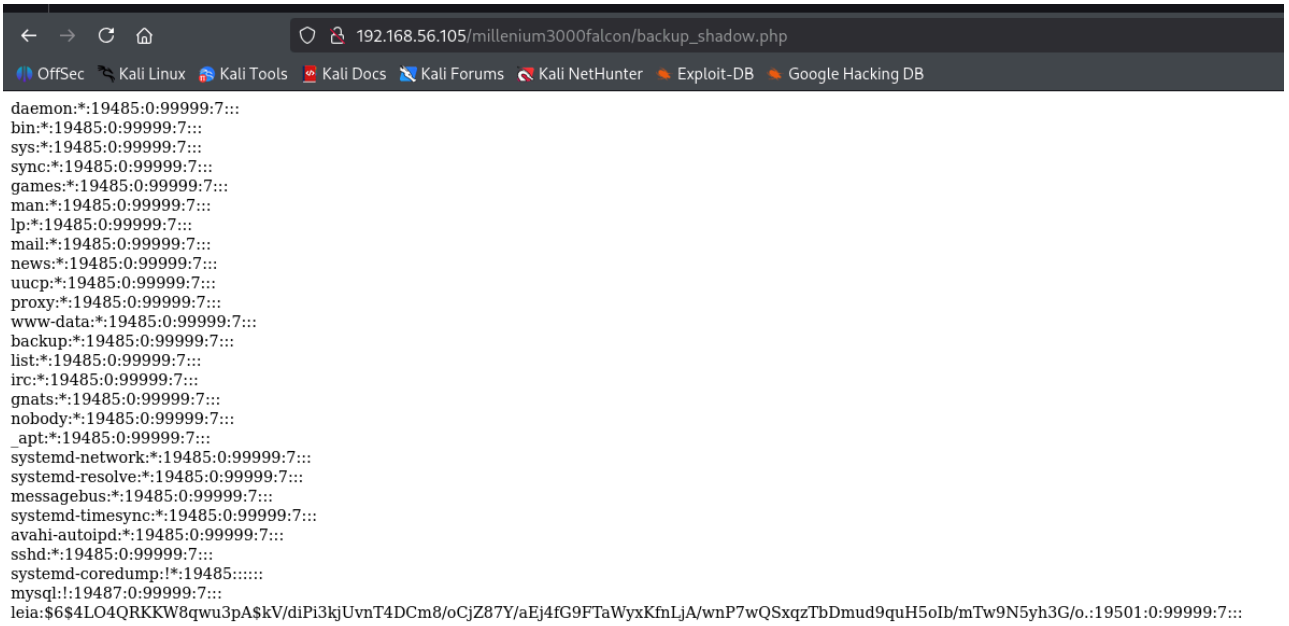
Quebra da terceira senha e exposição do sistema.

- **Ataque Hydra:** O `hydra` descobre a senha numérica de Kenobi: **0009165**.

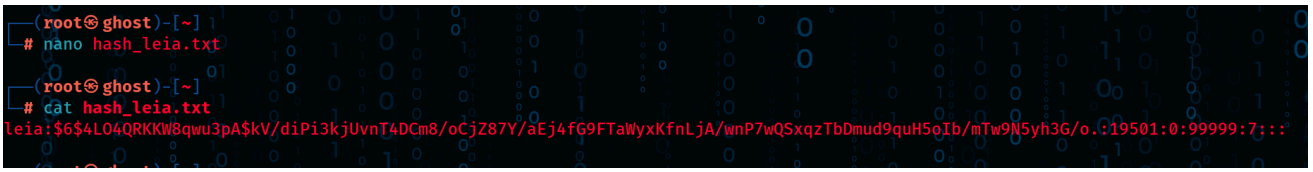


- **Vazamento do /etc/shadow:** Ao logar como Kenobi, a página `backup_shadow.php` exibe o conteúdo do arquivo `/etc/shadow` do Linux, que contém os hashes das senhas dos usuários do sistema. O hash da usuária **leia** é exposto.





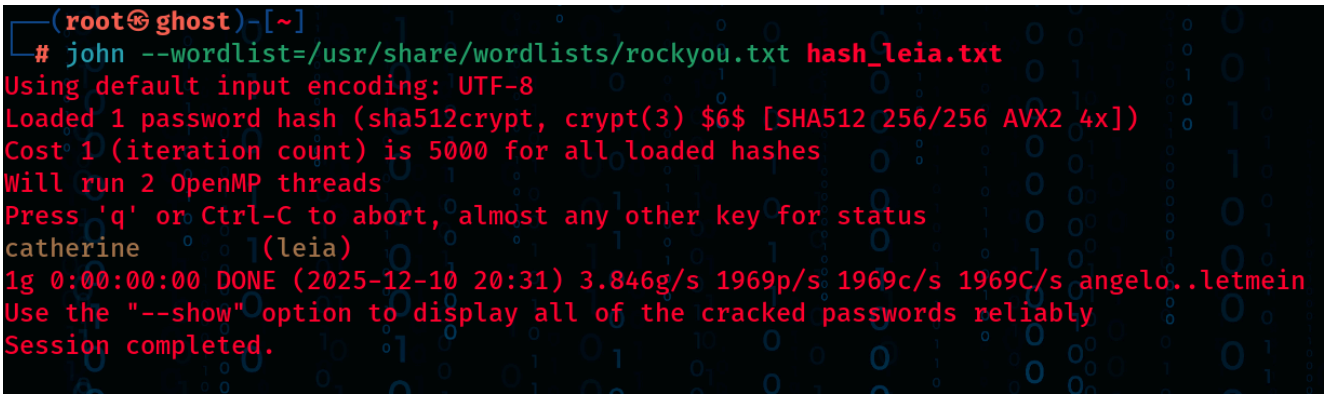
- **Salvando o Hash:** O atacante copia o hash da Leia para um arquivo chamado `hash_leia.txt`.



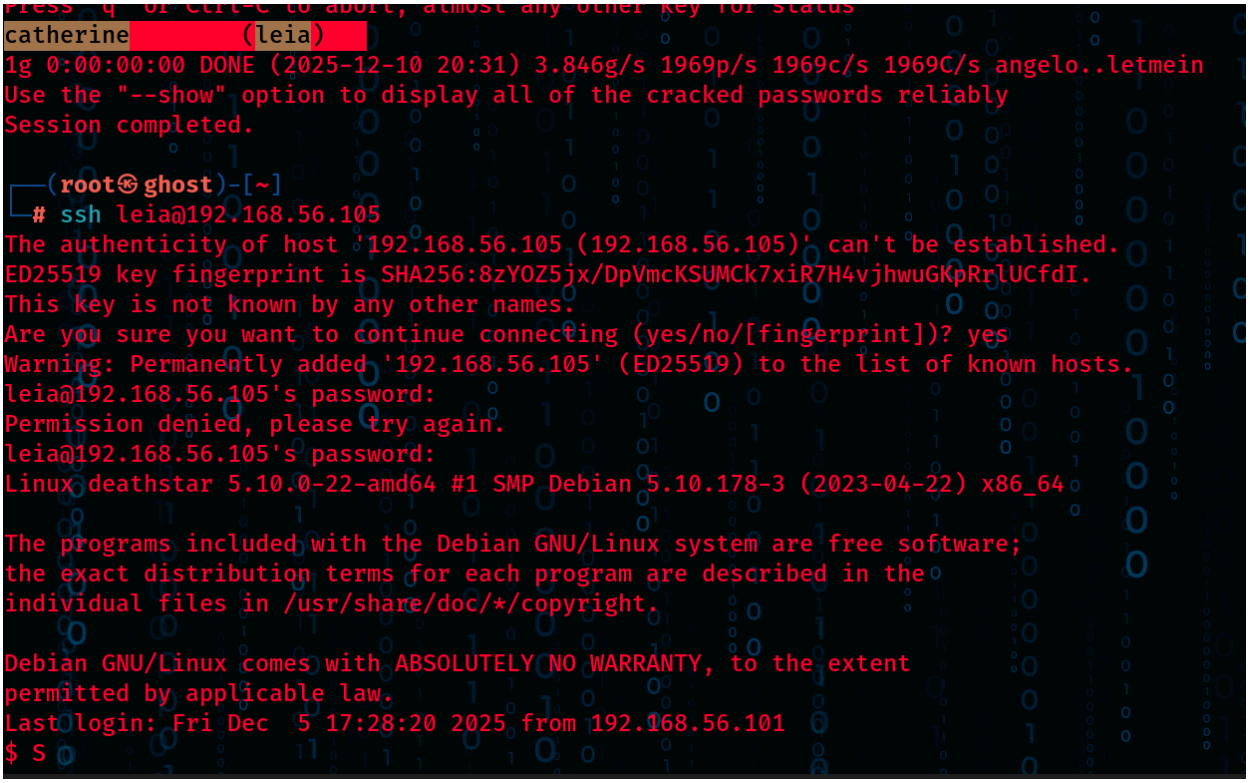
Quebra de Hash (John) e Acesso Root

Comprometimento total.

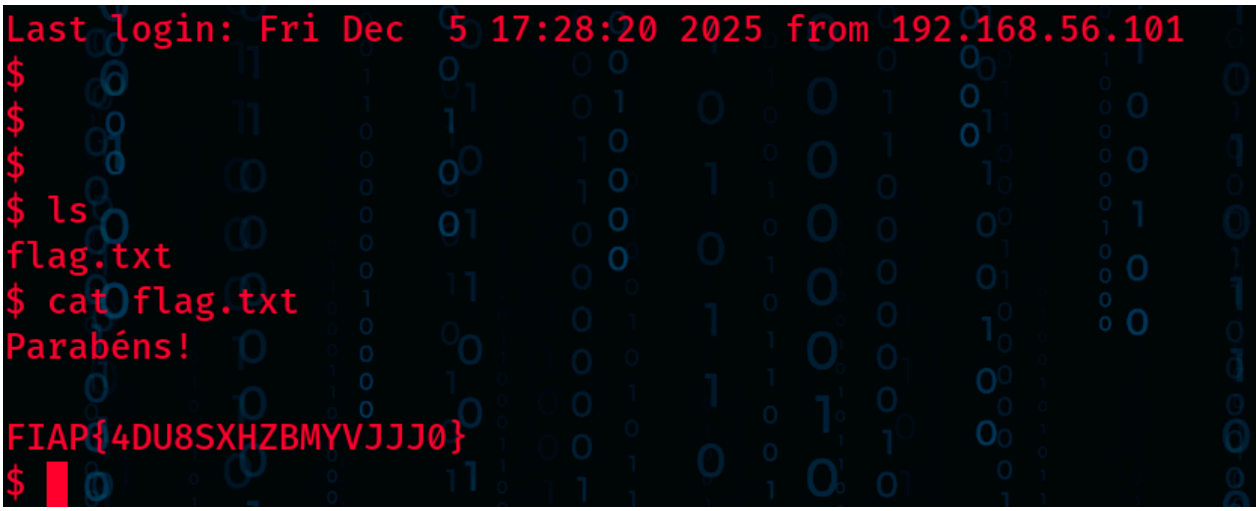
- **John the Ripper:** A ferramenta `john` quebra o hash da Leia e revela a senha: **catherine**.



- **Acesso SSH:** O atacante usa `ssh leia@192.168.56.105` e a senha descoberta para entrar no servidor via terminal.



- **Captura da Flag:** O comando `cat flag.txt` exibe a prova final da invasão: `FIAP{...}`.



Conclusão Técnica: As evidências coletadas demonstram que o servidor Deathstar possuía múltiplas falhas de configuração e desenvolvimento, permitindo que um atacante externo escalasse privilégios desde um acesso web não autenticado até o controle do sistema operacional através de técnicas de enumeração e força bruta