HackTheBox
Valetine - Walkthrough
IP: 10.10.10.79

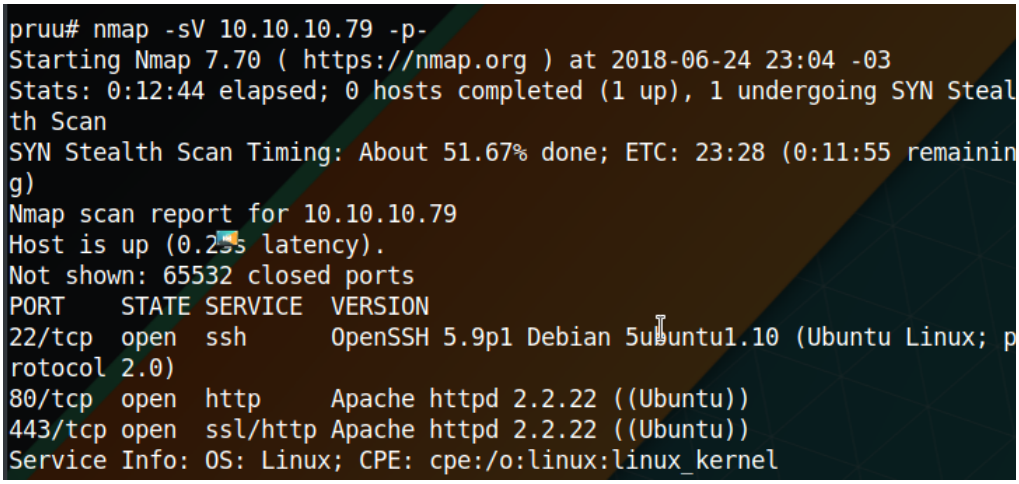
Escrito por: https://t.me/c4rloseduard0

- **Descrição**

Nome: Valentine
IP: 10.10.10.79
Dificuldade: Fácil
Localização: www.hackthebox.eu/home/machines/profile/127

- **Scanning**

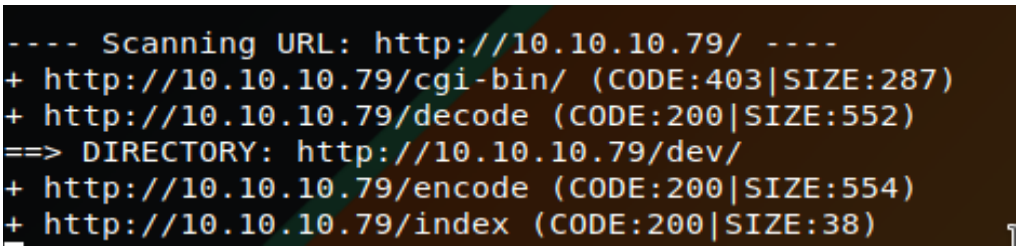
Para começar, foi feito um simples port scan usando nmap que revelou algumas portas abertas:



Por familiaridade começamos a exploração pelos serviços HTTP. Ao visitar página nos deparamos com uma imagem que remetia a uma vulnerabilidade conhecida, a Heartbleed.

- **Enumeração**

Antes de prosseguir com a vulnerabilidade em si, foi feito uma enumeração de diretórios e arquivos, usando o dirb:



- **Exploração**

O encode/decode era apenas um codificador de base64, não havia falha explorável nele, então entramos no diretório dev e encontramos dois arquivos, um deles continha notas com atividades que o administrador devia fazer, o outro era um hexadecimal que foi baixado para que vissemos em que resultava sua decodificação.

```
$ wget http://10.10.10.79/dev/hype_key
```

```
$ xxd -r -p hype_key > output.txt
```

O arquivo output.txt era uma chave privada, que posteriormente deve ser usada para se conectar via ssh, porém ainda precisamos da sua senha e um usuário.

- **A Falha**

Segundo o wikipédia, Heartbleed é um bug na biblioteca de software de criptografia open-source OpenSSL, que permite a um atacante ler a memória de um servidor ou de um cliente, permitindo a este recuperar chaves SSL privadas do servidor. E como tinhamos uma imagem com a “logo” da falha no site, começamos a explorá-la. Na internet existem diversos exploits capazes de nos mostrar o que queremos, mas por ser mais prático eu usei um exploit do metasploit.

```
msf > use auxiliary/scanner/ssl/openssl_heartbleed
msf auxiliary(scanner/ssl/openssl_heartbleed) > set RHOSTS 10.10.10.79
RHOSTS => 10.10.10.79
msf auxiliary(scanner/ssl/openssl_heartbleed) > set verbose true
verbose => true
msf auxiliary(scanner/ssl/openssl_heartbleed) > exploit
```

Depois de executar o comando algumas vezes, é retornado um base64 que quando decodificado nos dá a senha que precisavámos. Agora só nos falta o usuário para que possamos entrar via ssh, se observamos a palavra hype aparece várias vezes em nossa exploração, então podemos deduzir que este seja o usuário.

```
$ chmod 600 output.txt
$ ssh -i output.txt hype@10.10.10.79
```

Entrando via ssh já é possível conseguir a flag do user.

- **Escalação de Privilégios:**

Começamos procurando arquivos que fossem executados com permissão de root, em seguida tentamos enumerar possíveis lugares que pudessem ser explorados usando o LinEnum.sh, não houve muito sucesso. Depois de tentarmos um “procedimento padrão” para conseguirmos acesso como superusuário, procuramos ajuda no fórum do HackTheBox, e muitas pessoas recomendaram o cowroot, um famoso exploit que permite escalar privilégio usando uma falha no kernel Linux. Então compilamos em nosso computador, em seguida baixamos na máquina e executamos:

```
$ chmod +x cowroot
$ ./cowroot
```

Dessa forma conseguimos acessar como superusuário e conseguir a flag de root

```
# cat /root/root.txt
```