Files

main

Go to file t

.github
2023
0ByteCTF 2023
0xL4ugh CTF 2023
1337UP LIVE CTF
24h@CTF 2023
ASC Cyber Wargames Qualificat...
AmateursCTF 2023
BDSec CTF 2023
BYUCTF 2023
BlueHens CTF 2023

ctf-writeup / 2023 / niteCTF 2023 / conqueror /

Add file

daffainfo feat: grouped the challs ✕ e6c48e5 · last month History

Name	Last commit message	Last commit date
..		
images	feat: grouped the challs	last month
README.md	feat: grouped the challs	last month

README.md

conqueror

> Our company is dealing with a possible case of corporate espionage. The credentials of one of our systems were changed and it was used to gain access to our internal network.
> Our company is dealing with a possible case of corporate espionage. The credentials of one of our systems were changed and it was used to gain access to our internal network.

> Help us gain access to the system before its too late.

> Memory Dump Link: https://drive.google.com/file/d/14MWp-UtVPAcu1hEyv1_xBhpdO3nIrEBo/view?usp=sharing

> Flag Format: nite{user_password}

> coup de réseau will be visible after solving this challenge.

About the Challenge

We were given a memory dump file and we need to get the user and password

How to Solve?

To solve this challenge, we can use `volatility3` and then run this command to dump the user and the MD5 hash.

```
vol -f dump1.mem windows.hashdump.Hashdump
```

```
Volatility 3 Framework 2.5.2
Progress:  100.00               PDB scanning finished
User    rid     lmhash  nthash

Administrator   500     aad3b435b51404eeaad3b435b51404ee        31d6cfe0d16ae931b73c59d7e0c089c0
Guest   501     aad3b435b51404eeaad3b435b51404ee        31d6cfe0d16ae931b73c59d7e0c089c0
DefaultAccount  503     aad3b435b51404eeaad3b435b51404ee        31d6cfe0d16ae931b73c59d7e0c089c0
WDAGUtilityAccount      504     aad3b435b51404eeaad3b435b51404ee        9cc8759ba5c1750aaa38ea34618d559b
napoleon        1001    aad3b435b51404eeaad3b435b51404ee        89000a8b49f1a83c11b40fcdcd332135
sshd    1002    aad3b435b51404eeaad3b435b51404ee        8592797289d524686d08ab5493493656
root@ubuntu-s-1vcpu-2gb-sgp1-01:~/dump1#
```

Crack the MD5 hash using bruteforce attack, or you can try to put these hashes into cracker online like https://crackstation.net

Hash	Type	Result
89000a8b49f1a83c11b40fcdcd332135	NTLM	shorty

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

```
nite{napoleon_shorty}
```