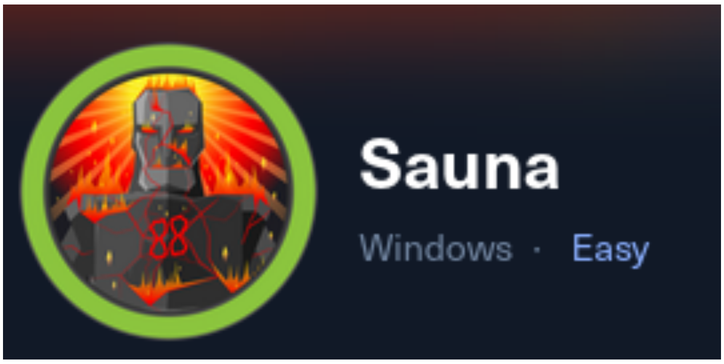
Sauna



Enumeration

Trying null and anonymous login fail for SMB and RPC

Website:

On the about page, we see multiple full names which can be used to create a wordlist of potential users

I used the following article to generate such a wordlist:
https://dzmitry-savitski.github.io/2020/04/generate-a-user-name-list-for-brute-force-from-first-and-last-name

With this wordlist, we can use kerbrute to find valid users on the box.
-> Yields fsmith as a valid user

with this username, we can conduct a ASRep Roasting attack

Foothold

ASRep Roasting

impacket-GetNPUsers -dc-ip 10.10.10.175 -usersfile valid.lst -format hashcat -outputfile hashes.txt -dc-host EGOTISTICAL-BANK.LOCAL EGOTISTICAL-BANK.LOCAL/fsmith
-> Get hash

hashcat -m 18200 -a 0 hash.txt /usr/share/wordlists/rockyou.txt
→ Crack hash

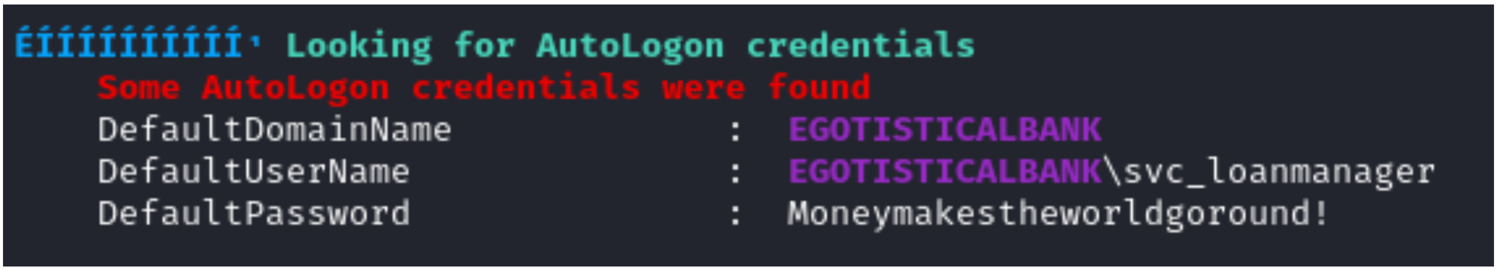
creds (allows us to winrm in):

fsmith:Thestrokes23

Priv Esc

----- LATERAL MOVEMENT -----

From WINPEAS:



```
ÉÍÍÍÍÍÍÍÍÍÍ¹ Looking for AutoLogon credentials
    Some AutoLogon credentials were found
    DefaultDomainName             :  EGOTISTICALBANK
    DefaultUserName               :  EGOTISTICALBANK\svc_loanmanager
    DefaultPassword               :  Moneymakestheworldgoround!
```

This data can also be retrieved using a registry query:
reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon"

AutoLogon allows anyone with physical access to the computer to get logged on without authentication. The credentials, however, are stored in plaintext in the Windows Registry, allowing remote attackers to gain access to the account from a lower privileged one.

Oddly, there is no user called svc_loanmanager, but there is one called svc_loanmgr, and the password works!

Creds:

svc_loanmgr:Moneymakestheworldgoround!

----- PRIVILEGE ESCALATION -----

With the new creds, bloodhound tells us we can perform a DCSync attack to dump NTLM hashes of other users.

After getting the Administrator's NTLM hash, we can use a Pass the Hash attack to gain administrative access over the box.