CrackMapExec

Owning Active Directory using Active Directory

whoami

@byt3bl33d3r

https://github.com/byt3bl33d3r

https://keybase.io/byt3bl33d3r

What is this thing?
What’s up with the name?

Standing on the shoulders...

- Cred**Crack** (https://github.com/gojhonny/CredCrack)
- SMB**Map** (https://github.com/ShawnDEvans/smbmap)
- SMB**Exec** (https://github.com/pentestgeek/smbexec)

I got 99.. err.. 6 problems

- **Large Networks**
- **Credential Overload**
- **Situational Awareness**
- **AV Detection**
- **Stealth / “Living off the Land”**
- **No External Tools**

Designed to be the “glue” between Metasploit and Empire

Putting the 0wn4ge puzzle together

These people did most of the work

- **Impacket** (https://github.com/CoreSecurity/impacket)
- **Powersploit** (https://github.com/PowerShellMafia/PowerSploit)
- **Mimikatz** (https://github.com/gentilkiwi/mimikatz)

Enough talk!

Demo Gods be nice plz

Peering into the crystal ball...

- **Module Chaining**
- **User Tracking**
- **Kerberos Support**
- **Pywerview** (https://github.com/the-useless-one/pywerview)

How do I stop all of this Crack, Mapping and Exec'ing?

Get the basics down:

- **Account Lockout Policy**
- **Logging**
- **Segmentation**

Then step up your game:

- **Microsoft ATA**
- **Microsoft LAPS**

Questions? Insults? Rotten Tomatoes?

CME is fully Open Source and hosted here:
https://github.com/byt3bl33d3r/CrackMapExec

Special Thanks

- @agsolino
- @gentilkiwi
- @subTee
- @PyroTek3

- The PowerShell Mafia Gang
  - @harmj0y
  - @mattifestation
  - @enigma0x3