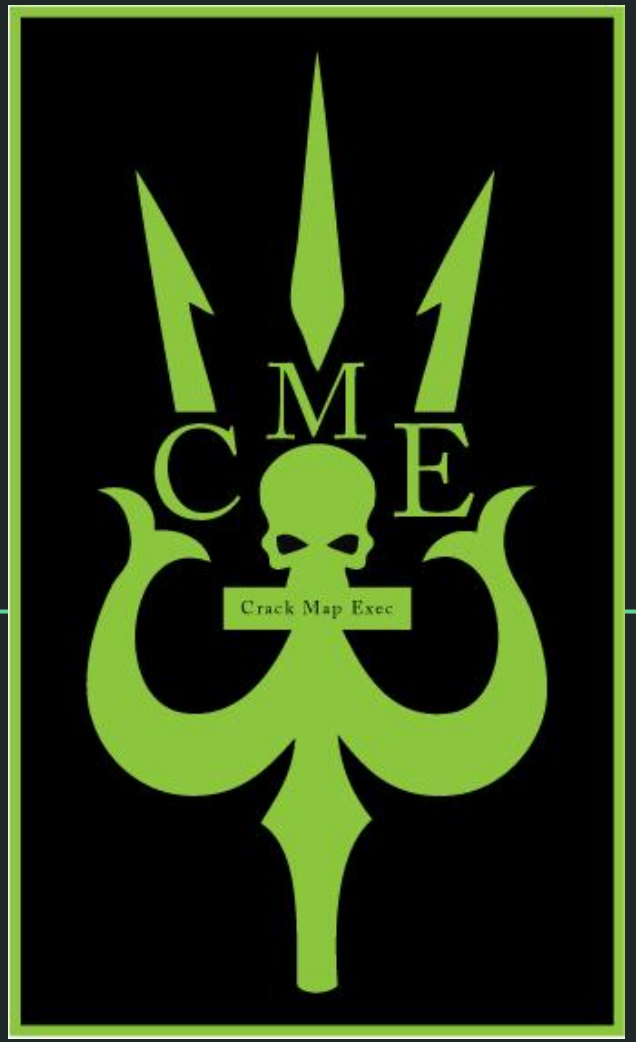
CrackMapExec

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)

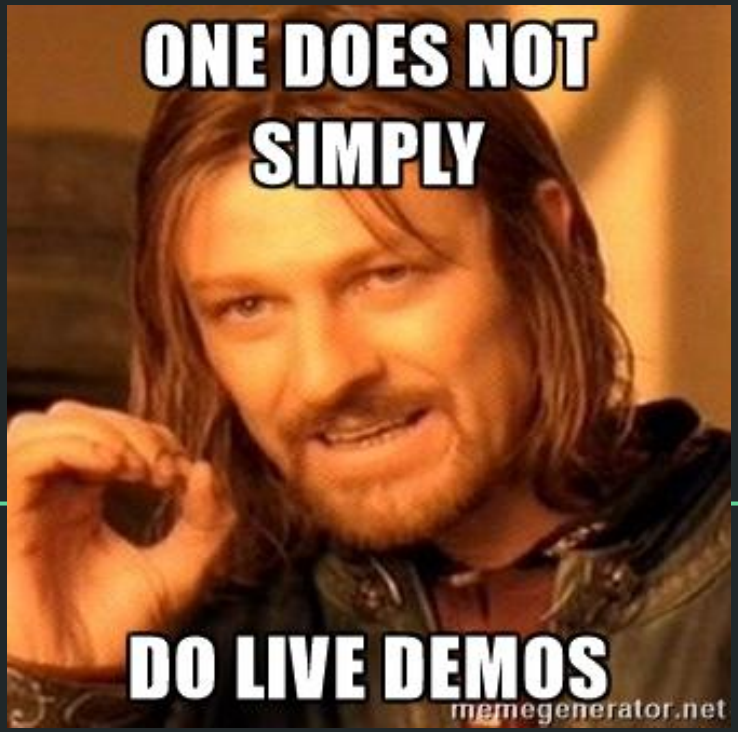
I got 99.. err.. 8 problems

- **Large Networks**
- **Credential Overload**
- **Situational Awareness**
- **AV Detection**
- **Stealth / “Living off the Land”**
- **External Tools (nope nope nooope)**
- **“Glue” between Metasploit and Empire**
- **Modularity**

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)



Demo Gods be nice plz

Module Chaining

Module Chaining Syntax (MCS) 101

Module1=>Module2=>Module3

Module1[OPTION=”value”]=>Module2[OPTION=”Value”]=>Module3

- “=>”: Chaining Operator
- “[OPTION=’Value1;;OPTION2=’Value2’]”: Module Options

Epic pwnage ahoy!

com_exec=>mimikatz

com_exec=>eventvwr_bypass=>met_inject

rundll32_exec=>com_exec=>empire_exec

DROPS MIC

Peering into the crystal ball...

- **User Tracking**
- **Kerberos Support**
- **BloodHound (OMFG)**
- **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?

In case you want to yell at me:

- Twitter (@byt3bl33d3r)
- IRC (@byt3bl33d3r)

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

People you should follow

- @agsolino
- @gentilkiwi
- @subTee
- @PyroTek3
- @Carlos_Perez
- @_wald0

@SquirrelsNaBrrl
(Thanks for the awesome logo!)

The PowerShell Mafia Gang
@harmj0y
@mattifestation
@enigma0x3