CrackMapExec 4.0

Owning ~~Active Directory using Active Directory~~
everything using all the things!

whoami

@byt3bl33d3r

https://github.com/byt3bl33d3r

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

How can we pwn things at scale?

How it all started…

Rewrite #6

Open **byt3bl33d3r** wants to merge 5 commits into `ShawnDEvans:master` from `byt3bl33d3r:rewrite_`

Conversation 13 | Commits 5 | Files changed 1

byt3bl33d3r commented on May 2, 2015

hey man,
I've been wanting to write something similar to smbmap for a long time, so I've been tweaking it the past day or so..
This is by no means finished, just wanted to submit this PR so you can kinda get a sense of the shape that it's taking.

So far there have been only a couple of major changes:

- Whole script is now fully asynchronous (with some exceptions)
- Added 'WMI' option for executing code using wmi

```
usage: smbmap.py [-h] [-u USERNAME] [-p PASSWORD] [-H HASH] [-d DOMAIN]
                 [-s SHARE] [-P {139,445}] [-t THREADS] [-S]
                 [-execm {wmi,smbexec}] [-x COMMAND]
                 target

SMBMap - Samba Share Enumerator | Shawn Evans - Shawn.Evans@gmail.com

positional arguments:
  target                The target range or CIDR identifier

optional arguments:
```

Standing on the shoulders...

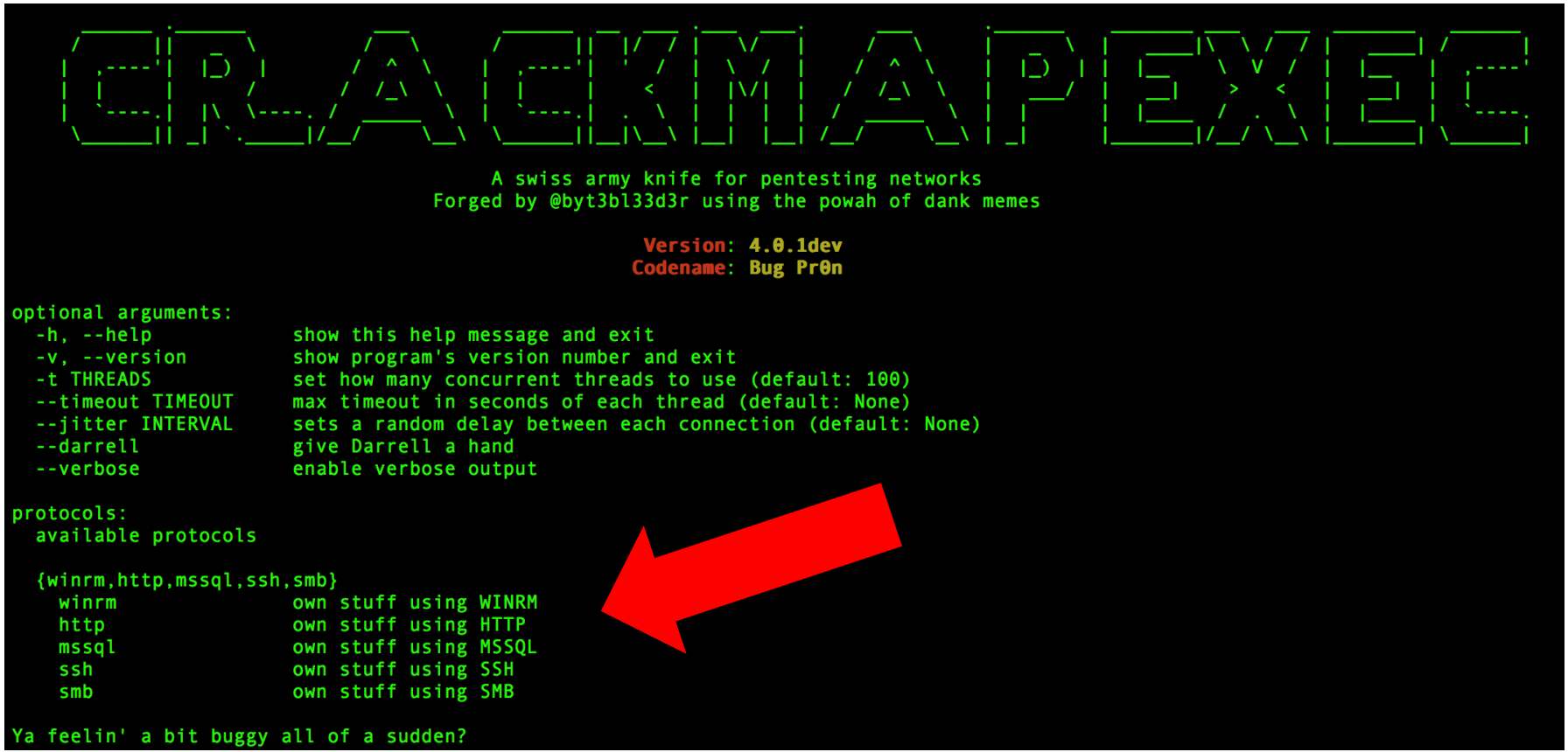
- Cred**Crack** (https://github.com/gojhonny/CredCrack)
- SMB**Map** (https://github.com/ShawnDEvans/smbmap)
- SMB**Exec** (https://github.com/pentestgeek/smbexec)

I got ~~99~~ 8 problems/features

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

But hang on… why just stop at AD?

New in v4: Modular protocols



Cause you don’t just see Windows on networks..

- **HTTP (Still in alpha…)**
- **MSSQL**
- **SSH**
- **SMB**

Fresh of the presses:

- **WinRM! (e.g. PS remoting)**

Putting the 0wn4ge puzzle together

These people did the hard stuff (Part 1)

Impacket - https://github.com/CoreSecurity/impacket

Pywinrm - https://github.com/diyan/pywinrm

Pywerview - https://github.com/the-useless-one/pywerview

PowerSploit - https://github.com/PowerShellMafia/PowerSploit

Invoke-Obfuscation - https://github.com/danielbohannon/Invoke-Obfuscation

These people did the hard stuff (Part 2)

Invoke-Vnc - https://github.com/artkond/Invoke-Vnc

Mimikittenz - https://github.com/putterpanda/mimikittenz

NetRipper - https://github.com/NytroRST/NetRipper

RandomPS-Scripts - https://github.com/xorrior/RandomPS-Scripts

SessionGopher - https://github.com/fireeye/SessionGopher

Mimipenguin - https://github.com/huntergregal/mimipenguin

I sacrificed this otter after taking this picture

Peering into the crystal ball…

- **WSH (Windows Script Host)**
- **Application Whitelisting Bypasses**
- **Module Chaining**

How do I stop this?

- **Account Lockout Policy**
- **Logging**
- **Segmentation**
- **Powershell Logging**
- **Microsoft ATA**
- **Microsoft LAPS**

Detecting CrackMapExec (CME) with Bro, Sysmon, and Powershell logs

https://www.n00py.io/2017/10/detecting-crackmapexec-cme-with-bro-sysmon-and-powershell-logs/

Questions? Insults?

In case you want to yell at me:
@byt3bl33d3r

#crackmapexec on bloodhoundhq.slack.com

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