About Us

I am Rohan Vazarkar

Job: Pentester at Veris Group’s ATD
Tool creator/dev: EyeWitness, Python Empyre, etc.
Presenter: BSidesDC/LV/DE, Black Hat Arsenal, DefCon
Trainer: Black Hat USA 2016

Twitter: @CptJesus
About Us

I am Andy Robbins

Job: Pentester at Veris Group’s ATD
Speaker: BSidesLV/Seattle, ISC2 World Congress, ISSA International, DefCon
Trainer: Black Hat USA 2016
Other: Ask me about ACH

Twitter: @_wald0
About Us

I am Will Schroeder

Job: Researcher at Veris Group’s ATD
Tool creator/dev: Veil-Framework, PowerView, PowerUp, Empire/Empyre
Speaker: Ask me
Trainer: Black Hat USA 2014-2016
Other: Microsoft PowerShell/CDM MVP

Twitter: @harmj0y
The Current State of Active Directory Domain Privilege Escalation
“Defenders think in lists. Attackers think in graphs. As long as this is true, attackers win.”

John Lambert
GM, Microsoft Threat Intelligence Center
AD Domain Priv Esc

- Active Directory is everywhere
- Usage = Attention = Research time and $$$
- Sometimes we get easy buttons!
Derivative

Local Admin

“The chaining or linking of administrator rights through compromising other privileged accounts”

Justin Warner @sixdub
Challenges

- Extremely time consuming and tedious
- Not comprehensive
- Limited situational awareness
- Did you even need DA?
What do we need?

◇ Who is logged on where?
◇ Who has admin rights where?
◇ What users and groups belong to what groups?
Stealthy Data Collection with PowerView
“The best tool these days for understanding Windows networks is PowerView...”

Phineas Phisher
http://pastebin.com/raw/0SNSvyjJ
A pure PowerShell v2.0+ domain/network situational awareness tool

Collects the data that BloodHound is built on and doesn’t need elevated privileges for most collection methods!
Who’s Logged in Where?  
aka “user hunting”

INVOKED-UserHunter:
- **Get-NetSession** – sessions w/ a remote machine
- **Get-NetLoggedOn/Get-LoggedOnLocal** – who’s logged in on what machine

**-Stealth:**
- Enumerate commonly trafficked servers and query remote sessions for each
We can enumerate members of a local group on a remote machine, without admin privileges!

- The WinNT service provider or NetLocalGroupMembers()

PowerView:

- Get-NetLocalGroup -ComputerName IP [-API]
GPOs can set local administrators
GPOs are applied to OUs/Sites
- correlation == local admin information through communication with only a DC!

PowerView:
- Find-GPOLocation
Who’s in What Groups?

- Enumerate all groups and pull the members of each

- PowerShell:
  - `Get-NetGroup` | `Get-NetGroupMember`

- That’s it!
Invoke-BloodHound automates gathering PowerView data for a domain and spits out CSV files.

Give it a REST URI and a User/Pass to send it directly to the database!
Thanks!

@_wald0
@CptJesus
@harmj0y