Desist with Demanding Domain

(aka, Stop Skipping the Strays)

Introduction

- Killian Ditch – killianditch@gmail.com
- Penetration Tester for Coalfire Systems, Inc.
- Toiled through 8 years of IT and software support – helpdesk, sysadmin, etc.
- Moved to a offensive security consulting role 2.5 years ago

Agenda

- ~~Introduction~~
- Briefing
- Example penetration test
- Examples of valuable non-AD assets
- Consequences of a compromised host
- Q&A

What & Why?

- Discussion Presentation
  - Commentary on the status quo from the perspective of a relative newbie to the industry

What & Why?

- Rationale
  - NOT disparaging the importance of Active Directory/Windows Domain testing
  - Initiate a conversation about too much focus on the goal of Domain Admin creating a tunnel-vision effect resulting in dismissal of risk to business-critical assets

Common Penetration Test

- Example Payment Card Industry Data Security Standard (PCI DSS) pen test
- Target: Cardholder Data Environment (CDE)
  - Network location with servers/databases/credit cards defined as in scope for the test
- Tester is placed in a non-CDE network segment
  - Remote device or on-site test
- Goal is to gain access to the CDE and compromise customer data

Reconnaissance

- Vulnerability scan
  - Nessus, Nexpose, OpenVAS
- Port scan/service identification
  - Nmap, masscan
- Less than covert, but scheduling demands quick work

Initial Foothold

- Direct exploitation of a CDE server/service
  - The result of poor segmentation
- Leveraging network traffic
  - Cleartext credentials
    - FTP, Telnet, HTTP
  - Server Message Block (SMB)
    - NTLMRelayx, Responder, etc.
- Direct exploitation of a surrounding host
  - Missing patches/exposed services
  - If it could lead to pivoting into the CDE, it’s in scope!

Credential Compromise

- Password cracking
  - Hashes captured from network traffic
    - Responder
- Mimikatz
  - Retrieve cleartext credentials stored in memory
- Pass-the-Hash
  - Re-use local Administrator or user password hashes

Status Recap

- Working set of domain credentials
- Potentially shelled a compromised host

Diverging Strategies

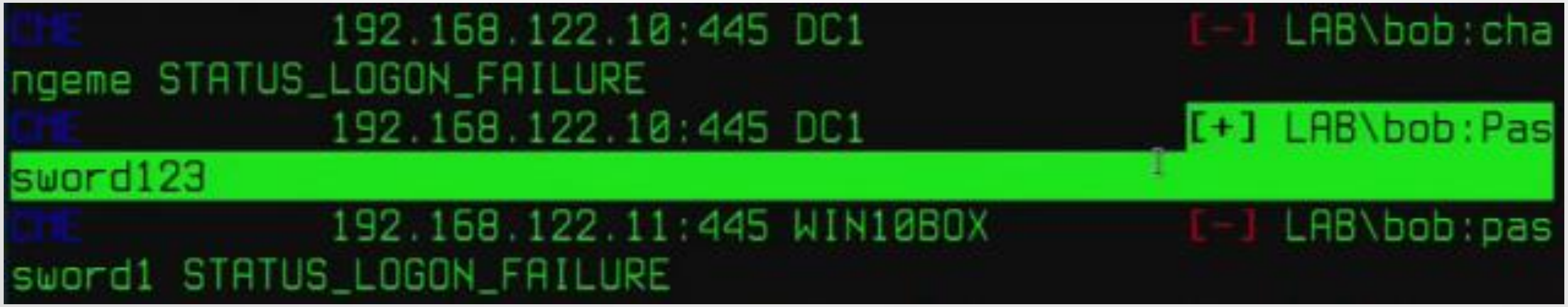
- Escalate privileges to Domain Admin (DA)
  - Use domain rights to look for data
- Use current privileges to harvest available data
  - Escalate as needed

Traditional Privilege Escalation

1. Connect to targets
   - RDP, PsExec
2. Dump credentials
   - Mimikatz, Hashdump
3. Assess new accounts’ privileges/group memberships
   - ‘net user kditch /domain’
4. GOTO 1

Newfangled Priv Esc

- CrackMapExec (CME)
  - Connect to Targets
  - Dump Credentials
  - Assess new accounts’ privileges



```
CME          192.168.122.10:445 DC1                 [-] LAB\bob:cha
ngeme STATUS_LOGON_FAILURE
CME          192.168.122.10:445 DC1                 [+] LAB\bob:Pas
sword123
CME          192.168.122.11:445 WIN10BOX            [-] LAB\bob:pas
sword1 STATUS_LOGON_FAILURE
```

Priv Esc

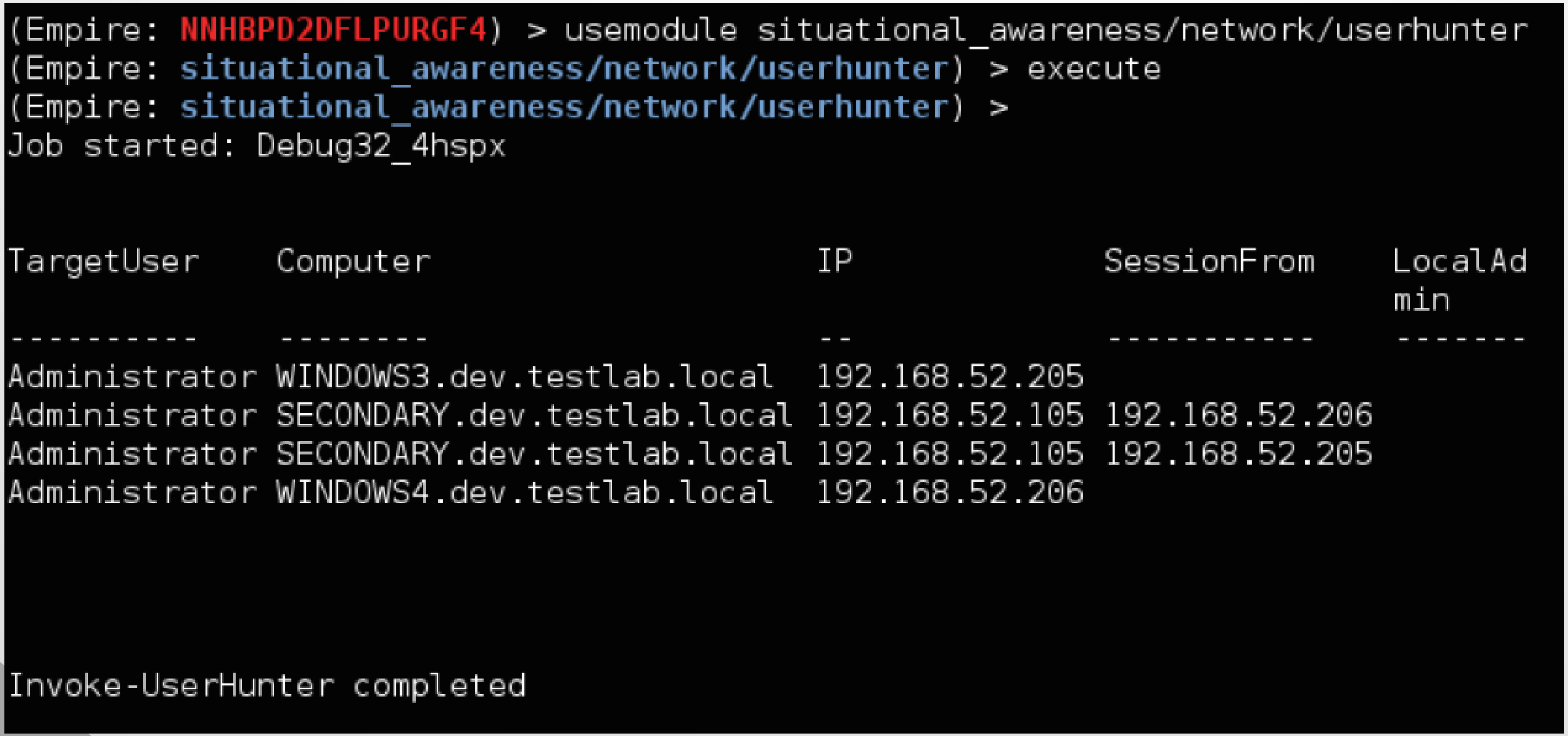
- Issue at hand
  - How to find computers with DA sessions?

Priv Esc

- Issue at hand
  - How to find computers with DA sessions?
- PowerShell

Newfangled Priv Esc

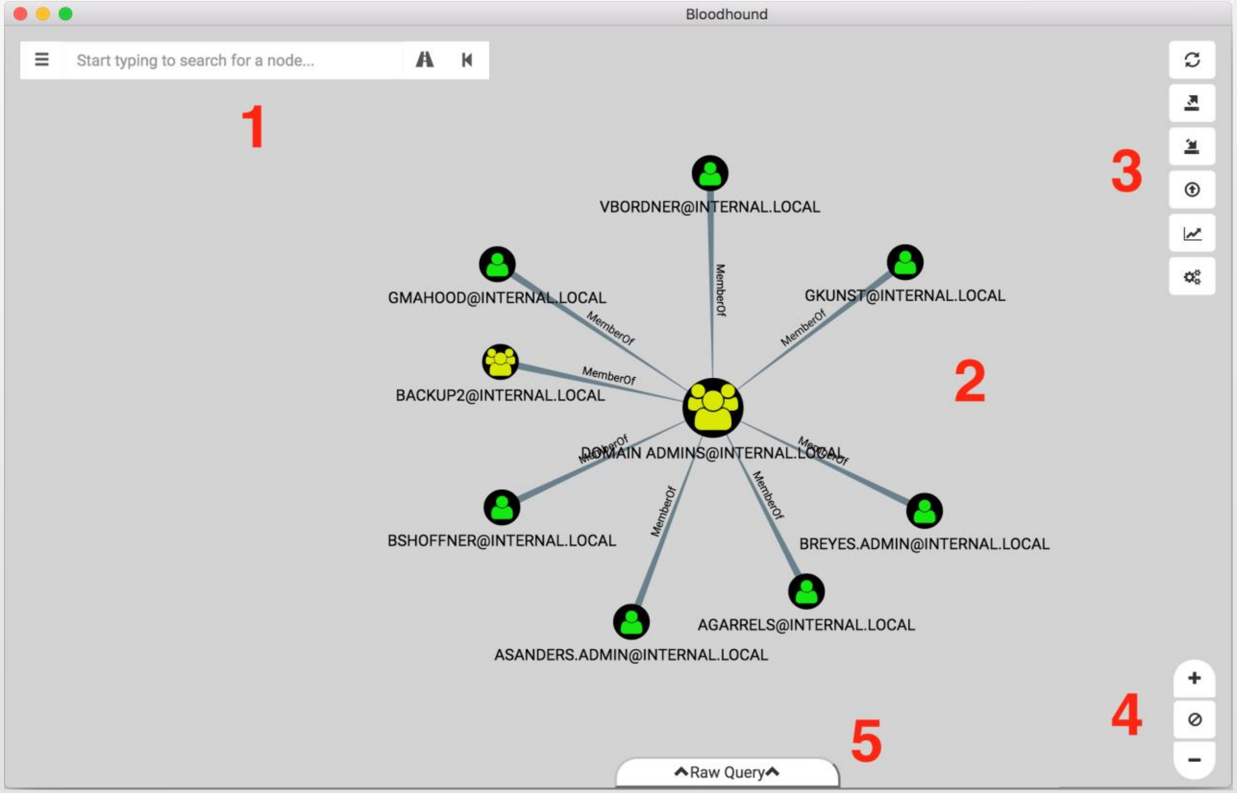
- PowerShell Empire
  - Invoke-UserHunter/Invoke-StealthUserHunter
    - Determine where DAs have active sessions



```
(Empire: NNHBPD2DFLPURGF4) > usemodule situational_awareness/network/userhunter
(Empire: situational_awareness/network/userhunter) > execute
(Empire: situational_awareness/network/userhunter) >
Job started: Debug32_4hspx


TargetUser    Computer                    IP             SessionFrom    LocalAd
                                                                        min
----------    --------                    --             -----------    -------
Administrator WINDOWS3.dev.testlab.local  192.168.52.205
Administrator SECONDARY.dev.testlab.local 192.168.52.105 192.168.52.206
Administrator SECONDARY.dev.testlab.local 192.168.52.105 192.168.52.205
Administrator WINDOWS4.dev.testlab.local  192.168.52.206




Invoke-UserHunter completed
```

Newfangled Priv Esc

- Bloodhound
  - BloodHound uses graph theory to reveal the hidden and often unintended relationships within an Active Directory environment.



Results

- Escalating to DA is faster and more efficient than ever.
  - Can even be automated!
    - See DeathStar

Results

- Some testers end up focusing exclusively on getting to that step and forget the purpose of a pen test.
  - Prove business risk of a compromise, not just prove a compromise is possible.

Results

- AD members naturally get prioritized, which comes at the expense of non-AD members.
  - Can’t run domain queries on a machine that doesn’t communicate to a domain controller.
    - Invoke-UserHunter & Bloodhound can’t make use of the host.

Results/Incoming Rant

- Initial footholds have been discarded as soon as AD status was determined.
  - No assessment of host’s value after “systeminfo | findstr Domain”
    - Not even a file system search for “password”
    - No netstat for listening services or network connections
    - No quick packet capture of network traffic the compromised host can see

- Disclosure: This conversation inspired my talk.

The Flip Side

- Why aren’t machines members of a domain?

Reasons to Pay Attention

- The obvious: Linux environment
  - Less common than Windows networks, but not uncommon.
  - Too much focus on Windows/Active Directory reduces the flexibility required to attack Linux systems.

Reasons to Pay Attention

- Infrastructure
  - Routers/Switches/Phones
    - If compromised, all network traffic can be diverted, spied upon, etc.
    - Eavesdropping on a VoIP call merely requires capturing the packets.
      - Cain and Abel & Wireshark
  - Badge/Door control & surveillance cameras

Reasons to Pay Attention

- Forgotten servers
  - Legacy machines
    - Remnants of previous network configurations, databases, file servers, etc.
  - Acquisitions
    - Security policies and system hardening not applied yet.
  - Affiliates/Vendors
    - Potentially avenues into other organizations

Reasons to Pay Attention

- Rogue hosts/“Shadow IT”
  - Developer computers/environments
    - Copies of intellectual property/source code
    - Insecure credential storage
  - “Temporary” Virtual Machines

One machine - so what?

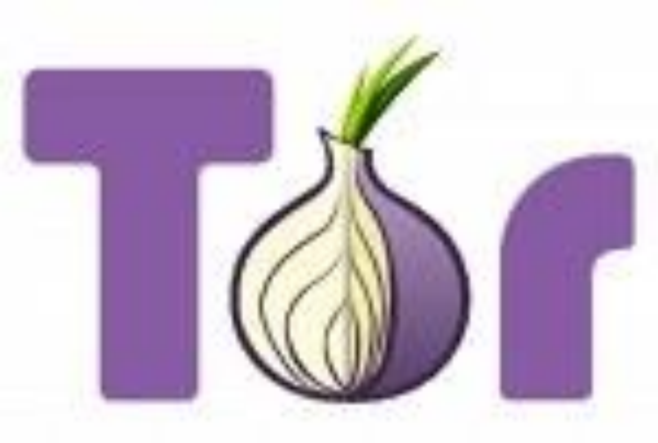
- What can be done with an Internet-connected computer?

Consequences of Compromise

- Attack Proxy
  - Pivot malicious traffic against a secondary target through the company’s network.
  - Attribution credits the company with the attack.
    - Legal repercussions and reputational damage
    - Hacking back

Consequences of Compromise

- Tor Node
  - Create an endpoint that would allow anyone to use the company’s network as their gateway to the Internet.
  - The company takes the blame.



Consequences of Compromise

- File Storage
  - Stashed and shared warez, illegal content, and other files on printers, FTP servers, etc.
  - If reported, the company would have to prove that the content was maliciously placed.

Consequences of Compromise

- Crypto Currency
  - Mining
  - Ransomware

Summary

- A host’s value can’t be known until assessed.
- DA should be a means to an end, not the end itself.
  - Unless specified by the client
- Defenders should be looking out for non-AD members, too.

Questions/Comments/Discussion?