SPECTEROPS

Manually Enumerating AD Attack Paths with BOFHound

Matt Creel

Adam Brown

Matt Creel

- Senior Consultant at SpecterOps
- Previous experience as a red teamer & pentester
- Impacket fanboy and producer of buggy Python tools

@Tw1sm

tw1sm.substack.com

github.com/Tw1sm

medium.com/@mcreel31

Adam Brown

- Chief of Offensive Cyber Capabilities
- Previous focus on Offensive R&D and Red Teaming
- Currently solutioning offensive management at scale

@coffeegist

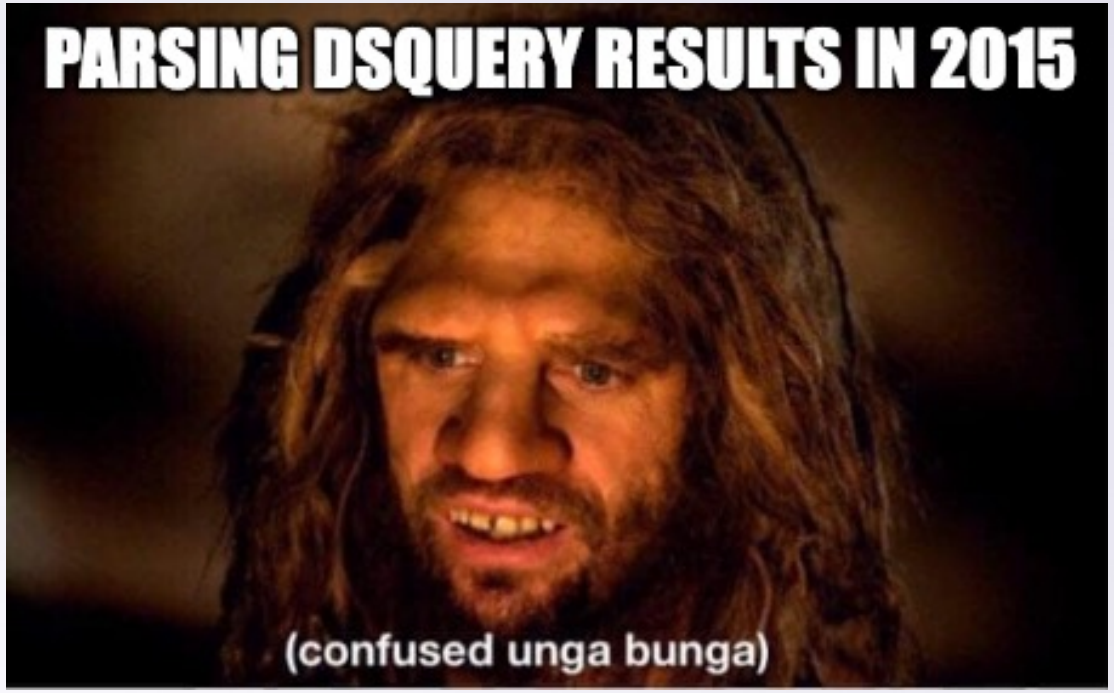
github.com/coffeegist

Agenda

- Background
- LDAP reconnaissance detection strategies
- Our approach – BOFHound
- LDAP query efficiency
- Manual session & local group data collection
- Pitfalls and TODOs
- Questions!

In the beginning...

We were all "living off the land" using built-in tooling with crude manual parsing to piece together the bigger picture called Active Directory...



“Old-School” Tools

Built-ins

Tools like net.exe and dsquery.exe have existed as LOLBins for a long time

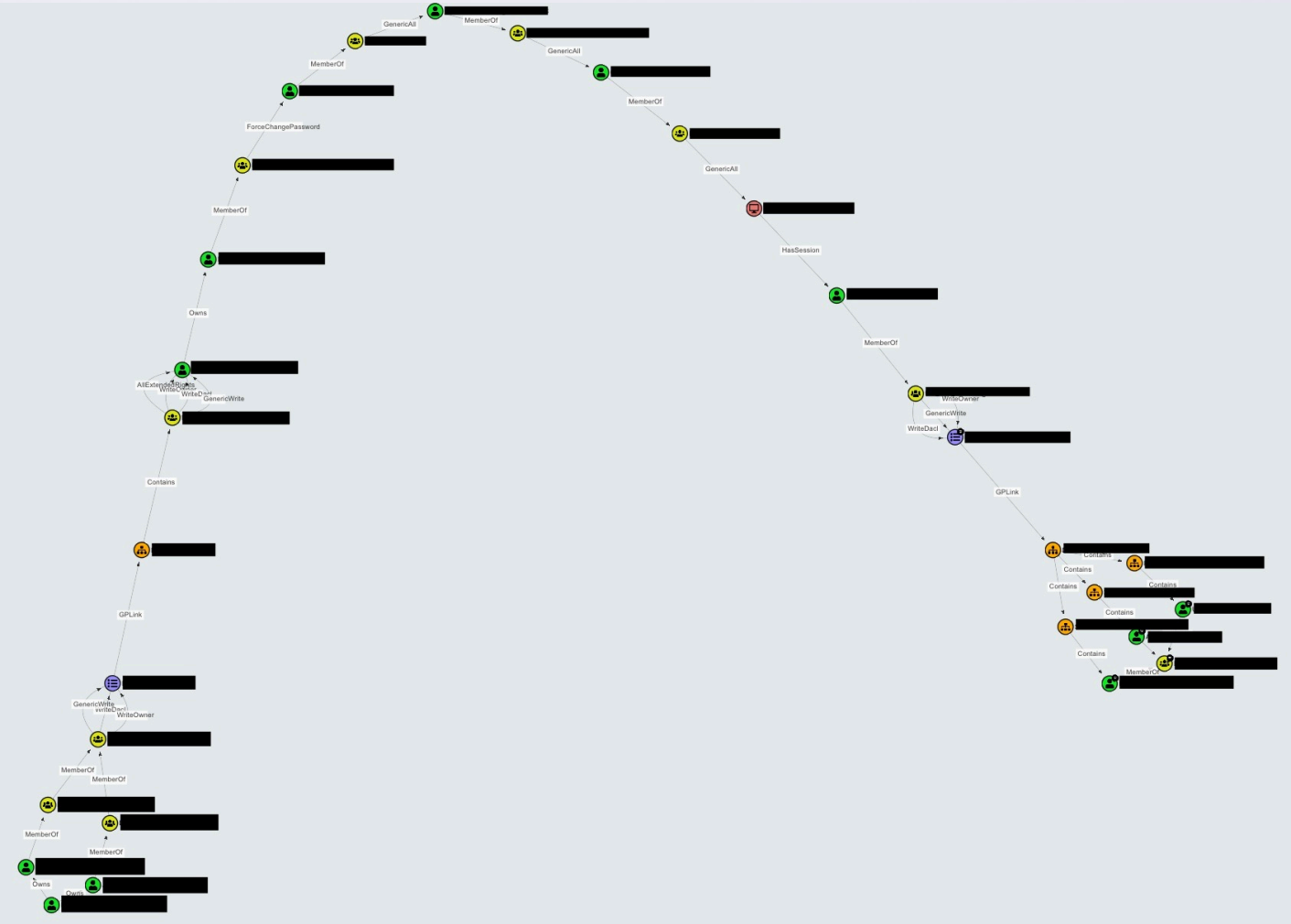
ADExplorer

Sysinternals tool that provides an ADUC-like GUI to browse objects.

PowerView

Original PowerShell tooling to mimic net.exe functionality via WinAPIs and provide targeted domain reconnaissance functions

Enlightenment



But It’s Not Always Possible

What methods of LDAP enumeration (and record keeping) do we have to fall back on?

“Modern Fallback” Tools

ADExplorer Snapshot.py

AdExplorerSnapshot.py allows for AdExplorer snapshots to be converted to BloodHound compatible JSON

SharpView, EDD, StandIn

C# tools based off PowerView, providing templated functions for domain enumeration and situational awareness

Manual Tools

The ldapsearch BOF, Linux ldapsearch utility, dsquery.exe, etc… through which the operator manually supplies query parameters

Disclaimer

If you can run SharpHound, you should run SharpHound

The Problem

As a red teamer, I want to…

- To collect data on Active Directory objects
- Collect session, logged on and local group data
- Control the speed and footprint of data collection
- Map attack paths using BloodHound's interface and Cypher queries

As a red teamer, I don't want to…

- Be required to load .NET tooling
- Create excess numbers of SMB connections to remote hosts
- Query all Active Directory objects at once
- Trip a detection or burn the operation

Detection Strategies

What are some approaches defenders take to detect malicious LDAP reconnaissance?

Client-Side vs. Server-Side Detections

Client Side

- Query Logging
  - API Hooks
  - ETW Providers
- Baselining Source Processes

Server Side

- Query Logging
- Baselining Volume
- SACLs and Audit Policies
- Expensive LDAP Queries

Client-Side Logging

Data Source

Monitor LDAP query events initiated on Windows hosts

- MDE automatically collects these via ETW
- Outside of MDE, subscribing to the *Microsoft-Windows-LDAP-Client* ETW provider can provide access to query filter strings
- API Hooking

Detection Strategy[1]

- Cross-reference logged LDAP search filters with known/unique filter components used in tooling leveraged by attackers
- Detect anomalous LDAP activity based on source process and environmental baselines

[1]https://falconforce.nl/falconfriday-detecting-active-directory-data-collection-0xff21/

Client-Side Logging – Event Tracing for Windows

```
PS C:\Tools\SilkETW> .\SilkETW.exe -pn Microsoft-Windows-Ldap-Client -t user -ot eventlog

SILKETW
[v0.8 - Ruben Boonen => @FuzzySec]

[+] Collector parameter validation success..
[>] Starting trace collector (Ctrl-c to stop)..
[?] Events captured: 97
```

Event Properties - Event 3, SilkETW Collector

General | Details

hostserviceaccount;unixuserpassword;msSFU30Password;unicodepwd;ntsecuritydescriptor;certificatetemplates;flags;cacertificate;n
flag;mspki-enrollment-flag;mspki-template-schema-version;mspki-cert-template-oid;pkioverlapperiod;pkiexpirationperiod;pkiexte
ra-signature;mspki-certificate-application-policy;mspki-ra-policies;crosscertificatepair;mspki-ra-application-policies;mspki-private
flag;gplink","ProviderName":"Microsoft-Windows-LDAP-Client","ScopeOfSearch":"2","ProcessId":"6,696","EventName":"EventID
30)","PID":"6696","SearchFilter":"(|(objectClass=container)(objectClass=configuration)(objectclass=pKICertificateTemplate)(|
(objectClass=certificationAuthority)(objectClass=pkiEnrollmentService))
(objectCategory=pKIEnrollmentService))","TID":"7416","DistinguishedName":"CN=Configuration,DC=redania,DC=local","MSec":"51615.1528","PName":""}}

Log Name:	SilkETW-Log		
Source:	SilkETW Collector	Logged:	1/24/2024 7:17:10 AM
Event ID:	3	Task Category:	None
Level:	Information	Keywords:	Classic
User:	N/A	Computer:	CINTRA.redania.local

Client ETW Telemetry[1] Logging Filter Used by SharpHound for ADCS Enumeration

```
let timeframe = 1h;
let suspect_search_filter=dynamic([
    "objectGUID=*", // AD Explorer IOC
    "(schemaIDGUID=*)", // Sharphound IOC
    "(&(objectclass=computer)(userAccountControl:1.2.840.113556.1.4.803:=8192))" // Sharphound IOC
    "(|(samAccountType=805306368)(samAccountType=805306369)(objectclass=organizationalUnit))", // Sharphound IOC
    "(|(samaccounttype=268435456)(samaccounttype=268435457)(samaccounttype=536870912)(samaccounttype=536870913))", // Sharphoun
    "(samAccountType=805306368)(samAccountType=805306369)" // Sharphound IOC
]);
DeviceEvents
| where ingestion_time() >= ago(timeframe)
| where ActionType =~ "LdapSearch"
| where not(InitiatingProcessFolderPath startswith @"c:\program files\azure advanced threat protection sensor\" and InitiatingP
| extend AdditionalFields=parse_json(AdditionalFields)
| extend SearchFilter=tostring(AdditionalFields.SearchFilter)
| where SearchFilter has_any(suspect_search_filter)
| project-reorder DeviceName, InitiatingProcessFolderPath, SearchFilter, InitiatingProcessCommandLine
```

FalconForce Example Client-Side Kusto Query[2] (MDE)

[1]https://github.com/mandiant/SilkETW
[2]https://github.com/FalconForceTeam/FalconFriday/tree/master/Discovery

Server-Side Logging

Data Source

Monitor LDAP query events on domain controllers

- MDE automatically logs these
- Outside of MDE, can use the same ETW provider discussed during client-side logging
- EventID 1644 also provides LDAP filters

Detection Strategy[1]

- Cross-reference logged LDAP search filters with known/unique filter components used in tooling leveraged by attackers

[1]https://falconforce.nl/falconfriday-detecting-active-directory-data-collection-0xff21/

Server-Side Logging

Event Properties - Event 1644, ActiveDirectory_DomainService

General | Details

Internal event: A client issued a search operation with the following options.

Client:
192.168.0.102:55244
Starting node:
DC=redania,DC=local
Filter:
(& (| (userAccountControl&16777216) (userAccountControl&524288) (msDS-AllowedToDelegateTo=*) (msDS-AllowedToActOnBehalfOfOtherIdentity=*)) (! (userAccountControl&2)) (! (userAccountControl&8192)))
Search scope:
subtree
Attribute selection:
[all_with_list]nTSecurityDescriptor
Server controls:
SDflags:0x7;
Visited entries:
3754
Returned entries:
1
Used indexes:
DNT_index:2604:N;

Event ID 1644[1,2] Logging Filter Used in Impacket's *findDelegation.py*

```
let timeframe = 1h;
let suspect_search_filter=dynamic([
    "objectGUID=*", // AD Explorer IOC
    "(schemaIDGUID=*)", // Sharphound IOC
    "(&(objectclass=computer)(userAccountControl&8192))" // Sharphound IOC
    "(|(samAccountType=805306368)(samAccountType=805306369)(objectclass=organizationalUnit))", // Sharphound IOC
    "(|(samaccounttype=268435456)(samaccounttype=268435457)(samaccounttype=536870912)(samaccounttype=536870913))", // Sharphoun
    "(samAccountType=805306368)(samAccountType=805306369)" // Sharphound IOC
]);
IdentityQueryEvents
| where ingestion_time() >= ago(timeframe)
| where ActionType =~ "LDAP query"
| extend Query=replace_string(Query," ","")
| where Query has_any (suspect_search_filter)
```

FalconForce Example Server-Side Kusto Query (MDE)

[1] https://learn.microsoft.com/en-us/troubleshoot/windows-server/identity/event1644reader-analyze-ldap-query-performance
[2] https://directoryadmin.blogspot.com/2019/10/hunting-bad-ldap-queries-on-your-dc.html

SACLs and Audit Policies

Data Source

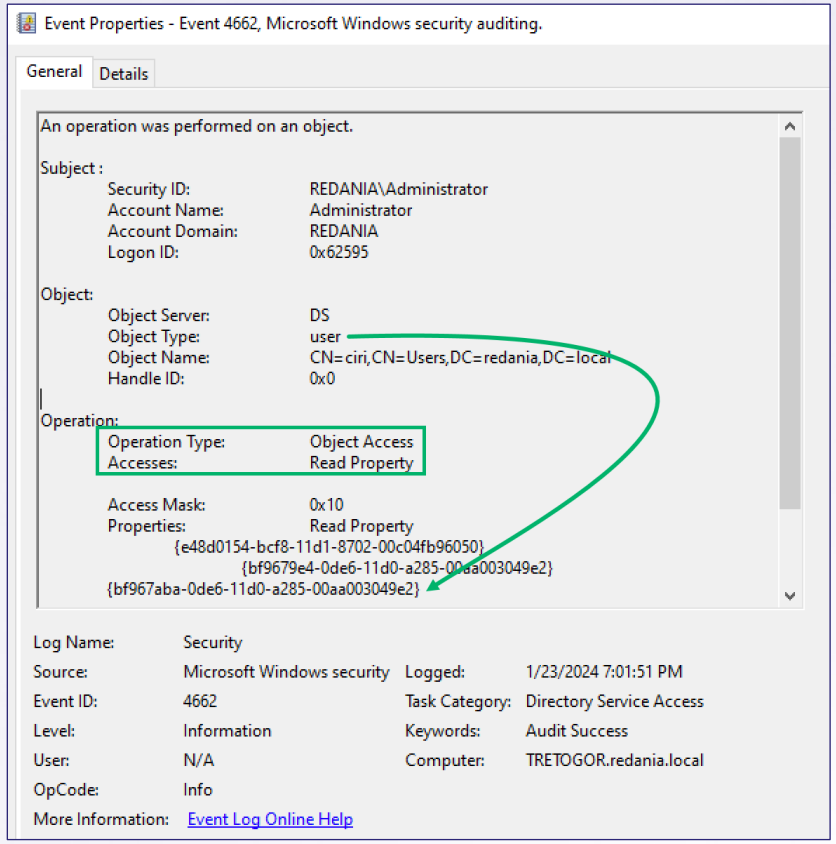
Set SACLs on the domain's descendant user, group and computer objects to create log entries (event 4662) each time anyone reads the properties of these objects

Detection Strategy[1]

1. Baseline the amount of user, group, and computer objects queried over a timeframe (e.g., 14 days) per user
2. Raise an alert if daily object query volume becomes greater than the max baseline by a factor (e.g., 20x) and over a minimum threshold (e.g., 20,000 objects)

[1] https://falconforce.nl/falconfriday-detecting-active-directory-data-collection-0xff21/

SACLs and Audit Policies



Event ID 4662 Logging Read Access to a User Object

```
let timeframe = 1d;
let lookback_days=14d; // Look back this many days to calculate baseline for maximum number of objects accessed per day.
let min_suspicious_count = 20000; // Only consider users looking up at least this many objects during the timeframe.
let suspicious_factor = 50; // Consider as suspicious if requesting more than suspicious_factor*daily maximum in lookback perio
let ADObjectAccess=(
    SecurityEvent
    | where EventID == 4662
    | where ObjectType in~ (
        "%{bf967aba-0de6-11d0-a285-00aa003049e2}", // User.
        "%{bf967a9c-0de6-11d0-a285-00aa003049e2}" //  Group.
        "%{bf967a86-0de6-11d0-a285-00aa003049e2}" //  Computer.
    )
);
let AccessBaseline=(
    ADObjectAccess
    | where TimeGenerated between (ago(timeframe + lookback_days)..ago(timeframe))
    | summarize BaselineObjectCount=count() by Account, bin(TimeGenerated,1d)
    | summarize PreviousMaxObjectPerDay=max(BaselineObjectCount) by Account
);
ADObjectAccess
| where ingestion_time() >= ago(timeframe)
| summarize ObjectCount=count(),TimeGenerated=min(TimeGenerated) by Account
| where ObjectCount > min_suspicious_count
| join kind=leftouter AccessBaseline on Account
| extend PreviousMaxObjectPerDay=coalesce(PreviousMaxObjectPerDay,0)
// Calculate what is considered a suspicious number for the given user.
| extend SuspiciousThreshold=max_of(PreviousMaxObjectPerDay*suspicious_factor,min_suspicious_count)
| where ObjectCount > SuspiciousThreshold
| project TimeGenerated, Account, ObjectCount, PreviousMaxObjectPerDay, SuspiciousThreshold
```

FalconForce Example Kusto Query (MDE)

[1] https://falconforce.nl/falconfriday-detecting-active-directory-data-collection-0xff21/

Expensive LDAP Query Logging

Data Source

Set registry values to enable logging of LDAP queries that are:

- Long running (search time over N milliseconds)
- Inefficient (Visit > N objects AND return < 10%)
- Expensive (return > N entries)

Detection Strategy

1. Baseline the returned entries, visited entries, and/or time it takes current LDAP queries to run
2. Raise an alert if these baselines are exceeded by a factor which will vary based on which metric you are measuring

[1] https://directoryadmin.blogspot.com/2019/10/hunting-bad-ldap-queries-on-your-dc.html

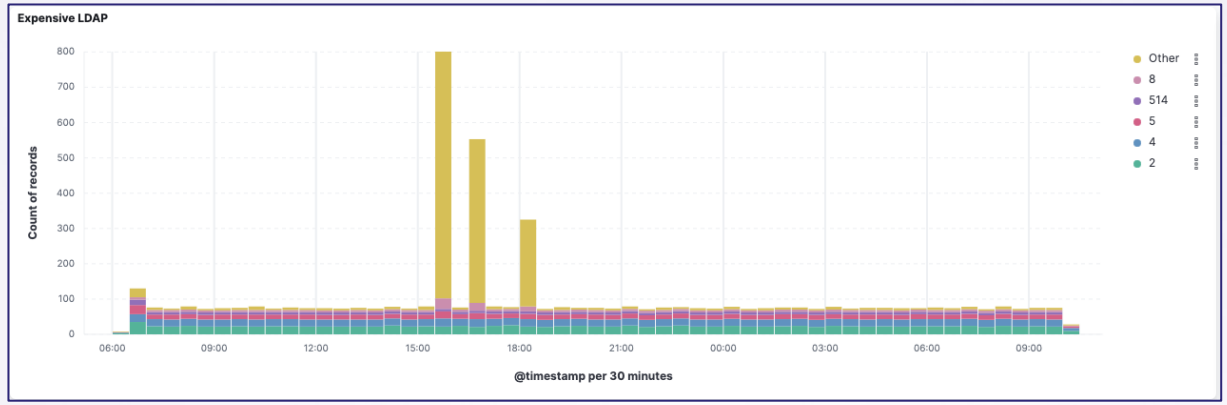
Expensive LDAP Queries

Default SharpHound DCOnly Collection

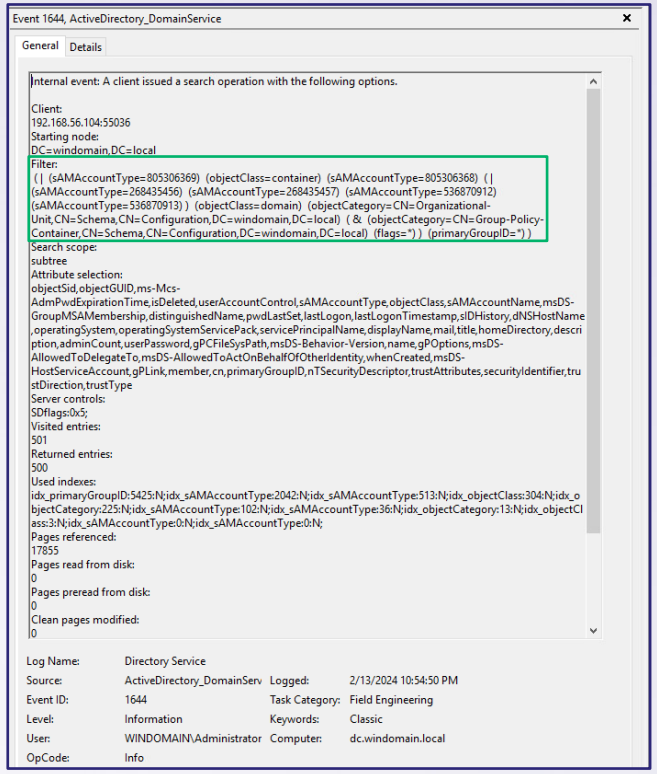
- Tunable using elements under

  HKLM/System/CurrentControlSet/Services/NTDS/Parameters

  - *Expensive Search Results Threshold*
  - *Inefficient Search Results Threshold*
  - *Search Time Threshold (msecs)*



LDAP Requests Grouped by Visited Entries



Event 1644, ActiveDirectory_DomainService

General Details

Internal event: A client issued a search operation with the following options.

Client:
192.168.56.104:55036
Starting node:
DC=windomain,DC=local
Filter:
(| (sAMAccountType=805306369) (objectClass=container) (sAMAccountType=805306368) (| (sAMAccountType=268435456) (sAMAccountType=268435457) (sAMAccountType=536870912) (sAMAccountType=536870913)) (objectClass=domain) (objectCategory=CN=Organizational-Unit,CN=Schema,CN=Configuration,DC=windomain,DC=local) (& (objectCategory=CN=Group-Policy-Container,CN=Schema,CN=Configuration,DC=windomain,DC=local) (flags=*)) (primaryGroupID=*))
Search scope:
subtree
Attribute selection:
objectSid,objectGUID,ms-Mcs-AdmPwdExpirationTime,isDeleted,userAccountControl,sAMAccountType,objectClass,sAMAccountName,msDS-GroupMSAMembership,distinguishedName,pwdLastSet,lastLogon,lastLogonTimestamp,sIDHistory,dNSHostName,operatingSystem,operatingSystemServicePack,servicePrincipalName,displayName,mail,title,homeDirectory,description,adminCount,userPassword,gPCFileSysPath,msDS-Behavior-Version,name,gPOptions,msDS-AllowedToDelegateTo,msDS-AllowedToActOnBehalfOfOtherIdentity,whenCreated,msDS-HostServiceAccount,gPLink,member,cn,primaryGroupID,nTSecurityDescriptor,trustAttributes,securityIdentifier,trustDirection,trustType
Server controls:
SDflags:0x5;
Visited entries:
501
Returned entries:
500
Used indexes:
idx_primaryGroupID:5425:N;idx_sAMAccountType:2042:N;idx_sAMAccountType:513:N;idx_objectClass:304:N;idx_objectCategory:225:N;idx_sAMAccountType:102:N;idx_sAMAccountType:36:N;idx_objectCategory:13:N;idx_objectClass:3:N;idx_sAMAccountType:0:N;idx_sAMAccountType:0:N;
Pages referenced:
17855
Pages read from disk:
0
Pages preread from disk:
0
Clean pages modified:
0

Log Name:	Directory Service		
Source:	ActiveDirectory_DomainServ	Logged:	2/13/2024 10:54:50 PM
Event ID:	1644	Task Category:	Field Engineering
Level:	Information	Keywords:	Classic
User:	WINDOMAIN\Administrator	Computer:	dc.windomain.local
OpCode:	Info		

Event 1644 Showing Filters from BloodHound –c DCOnly

[1] https://learn.microsoft.com/en-us/troubleshoot/windows-server/identity/event1644reader-analyze-ldap-query-performance

Our Approach

How can we leverage this information to perform LDAP reconnaissance, maintain BloodHound usability, and minimize our risk of detection?

ldapsearch BOF

Situational Awareness BOF Collection

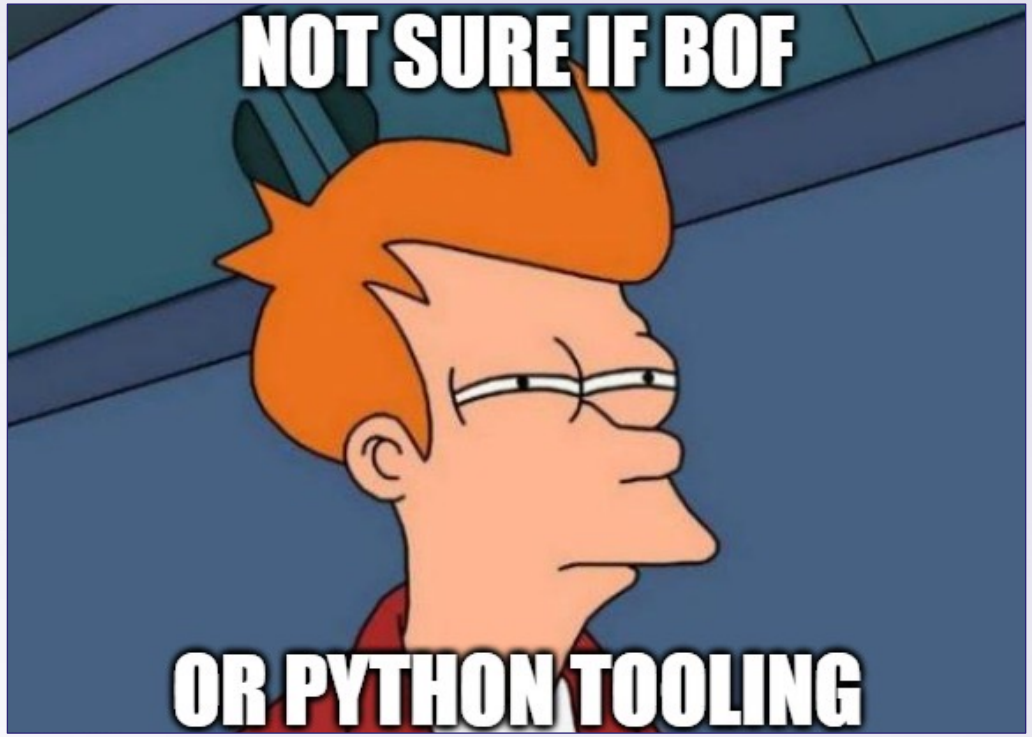
```
beacon> help ldapsearch
ldapsearch <query> [comma_separated_attributes] [result_count] [scope_of_search] [DC hostname or IP] [Distingished Name to use]
        "" works as a default for attributes (get all) DC hostname / IP (use Primary DC) and distingished name (use Base domain Level)
        0 works as default for result_count (get all). For scope_of_search, use 1 [LDAP_SCOPE_BASE], 2 [LDAP_SCOPE_ONELEVEL] or 3 [LDAP_SCOPE_SUBTREE] (3 is used by default)
```

```
[02/14 22:11:12] beacon> ldapsearch (samaccountname=geralt) *,ntsecuritydescriptor
[02/14 22:11:12] [+] Running ldapsearch (T1018, T1069.002, T1087.002, T1087.003, T1087.004, T1482)
[02/14 22:11:12] [*] Running ldapsearch (T1018, T1069.002, T1087.002, T1087.003, T1087.004, T1482)
[02/14 22:11:30] [+] host called home, sent: 11631 bytes
[02/14 22:11:31] [+] received output:
Binding to 192.168.0.235
[02/14 22:11:31] [+] received output:
[*] Distinguished name: DC=redania,DC=local
[*] targeting DC: \\TRETOGOR.redania.local
[*] Filter: (samaccountname=geralt)
[*] Scope of search value: 3
[*] Returning specific attribute(s): *,ntsecuritydescriptor

--------------------
objectClass: top, person, organizationalPerson, user
cn: Geralt
givenName: Geralt
distinguishedName: CN=Geralt,CN=Users,DC=redania,DC=local
instanceType: 4
whenCreated: 20230220011053.0Z
whenChanged: 20240129164653.0Z
displayName: Geralt
uSNCreated: 13022
memberOf: CN=BO-san-distlist1,OU=Shadow,DC=redania,DC=local, CN=EV-vie-admingroup1,OU=Domain Controllers,DC=redania,DC=local,
uSNChanged: 100735
nTSecurityDescriptor:
AQAEnIgEAACkBAAAAAAAABQAAAAEAHQEGAAAAAUAPAAQAAAAAwAAAABCFkzAINARp2gAqgBuBSkUzChINxS8RZsHrW8BXl8oAQIAAAAAAAUgAAAAKgIAAAUAPAAQA
name: Geralt
objectGUID: aba5ca7b-d893-4ea8-b93a-e7f27847da95
userAccountControl: 66048
badPwdCount: 0
codePage: 0
countryCode: 0
badPasswordTime: 0
lastLogoff: 0
lastLogon: 133511292011973597
pwdLastSet: 133213290537482634
primaryGroupID: 513
objectSid: S-1-5-21-1308756548-3893869957-2915408613-1103
adminCount: 1
accountExpires: 9223372036854775807
logonCount: 9
sAMAccountName: geralt
sAMAccountType: 805306368
```

BOFHound

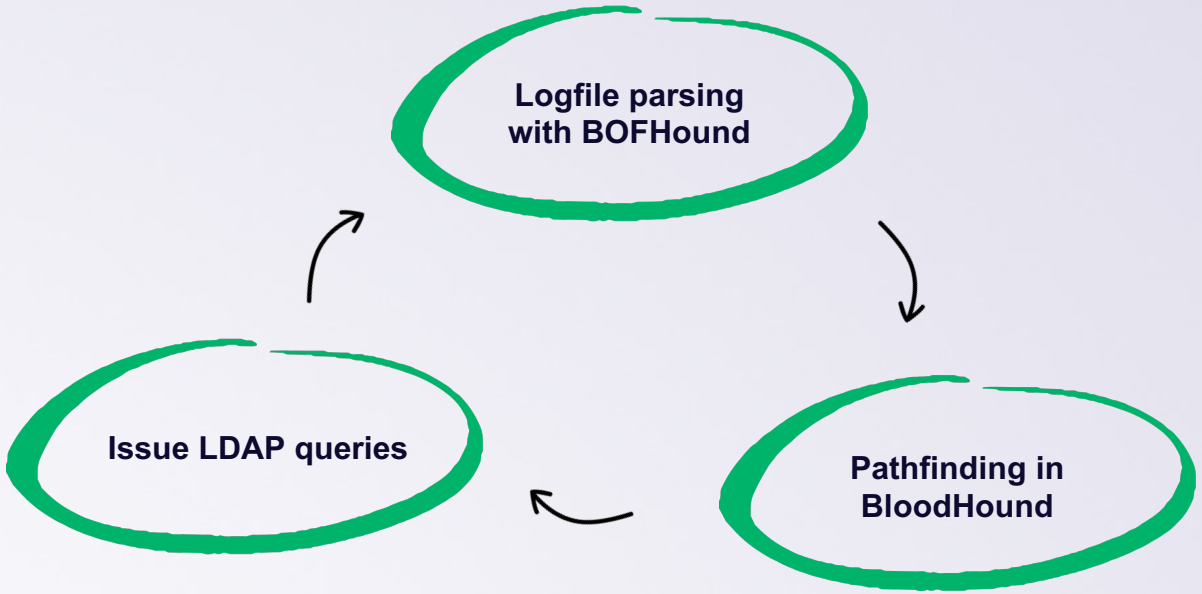
- Parses raw text LDAP objects from [C2] logfiles
- Outputs BloodHound compatible JSON files
- Is in fact, not a BOF
  - Written in Python, used offline
  - Originally built to support the SA ldapsearch[1] BOF
- Conceptualized to help avoid detections in place for expensive LDAP queries



[1]https://github.com/trustedsec/CS-Situational-Awareness-BOF/blob/master/src/SA/ldapsearch/entry.c

BOFHound Workflow

- Cyclical workflow
  - Path mapping with incomplete data in BH reveals additional SIDs/DNs to query
- Granular control of enumeration speed/depth
  - Supports LDAP and session/local group data
  - Can be performed over days/weeks
  - Can choose to not approximate a “full” SharpHound collection



Demo

Activities Applications aggressor-Aggressor Jan 24 19:34

Cobalt Strike

Cobalt Strike View Payloads Attacks Site Management Reporting Help

external	internal	listener	user	computer	note	process	pid	arch	last	sleep
192.168.0.146	192.168.0.146	https	ciri	CINTRA		beacon_x64.exe	6208	x64	2s	2 seconds

Event Log X | Beacon 192.168.0.146@6208 X

```
[CINTRA] - x64 |  ciri | 6208 - x64                                  last:2s
beacon>
```

Terminal | BloodHound — Mozilla Firefox | Cobalt Strike | 1/2

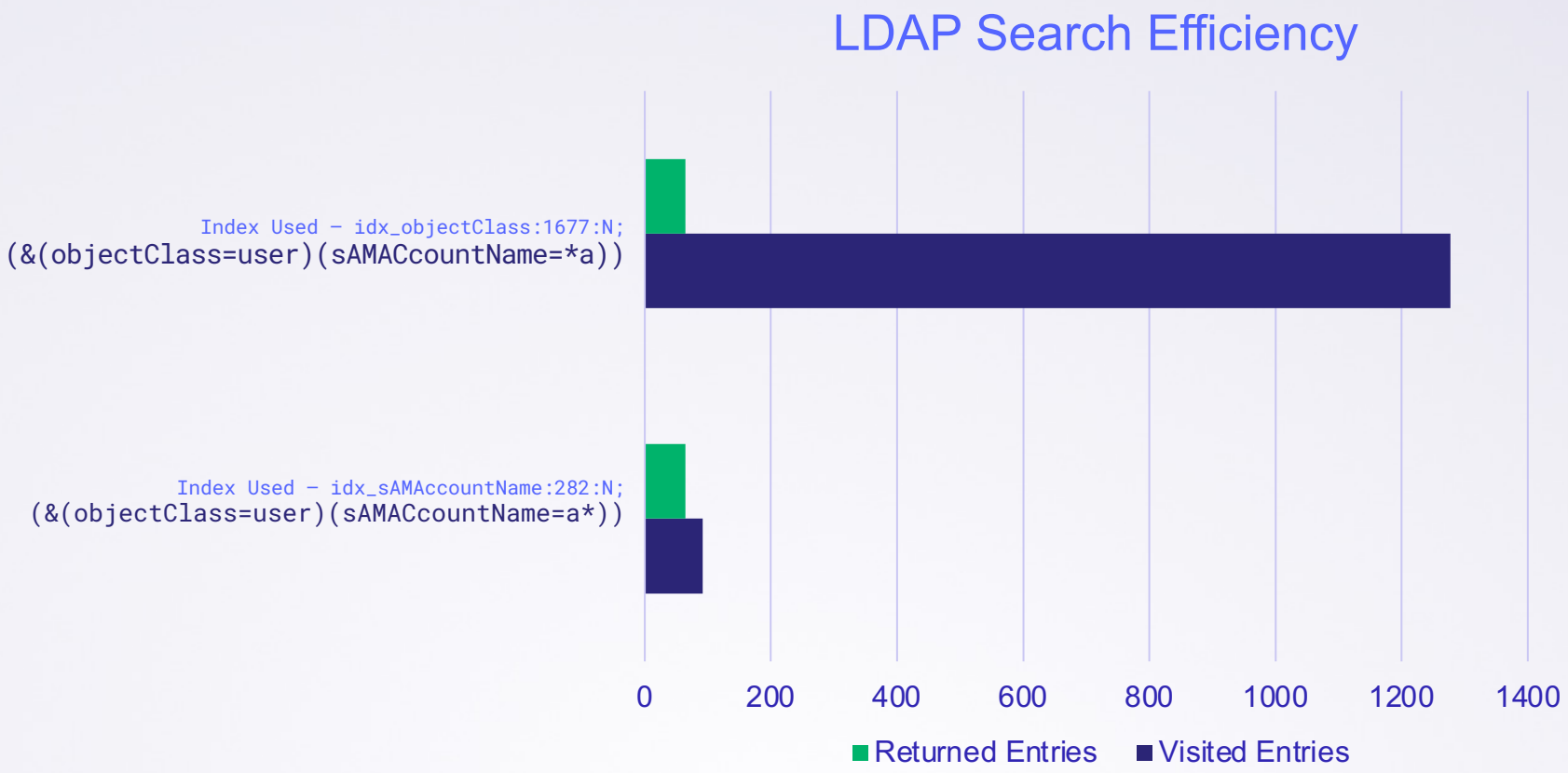
Efficient Queries

Being Mindful of Visited Entries

- Optimize search scopes and base names
- Use wildcards carefully
- Attribute presence filters make efficient use of indices
- Use indexed attributes where possible
  - https://learn.microsoft.com/en-us/windows/win32/adschema/attributes-indexed

Impacts of Wildcards

Filter on sAMAccountName



Reading Indices – idx_objectClass:1677:N;

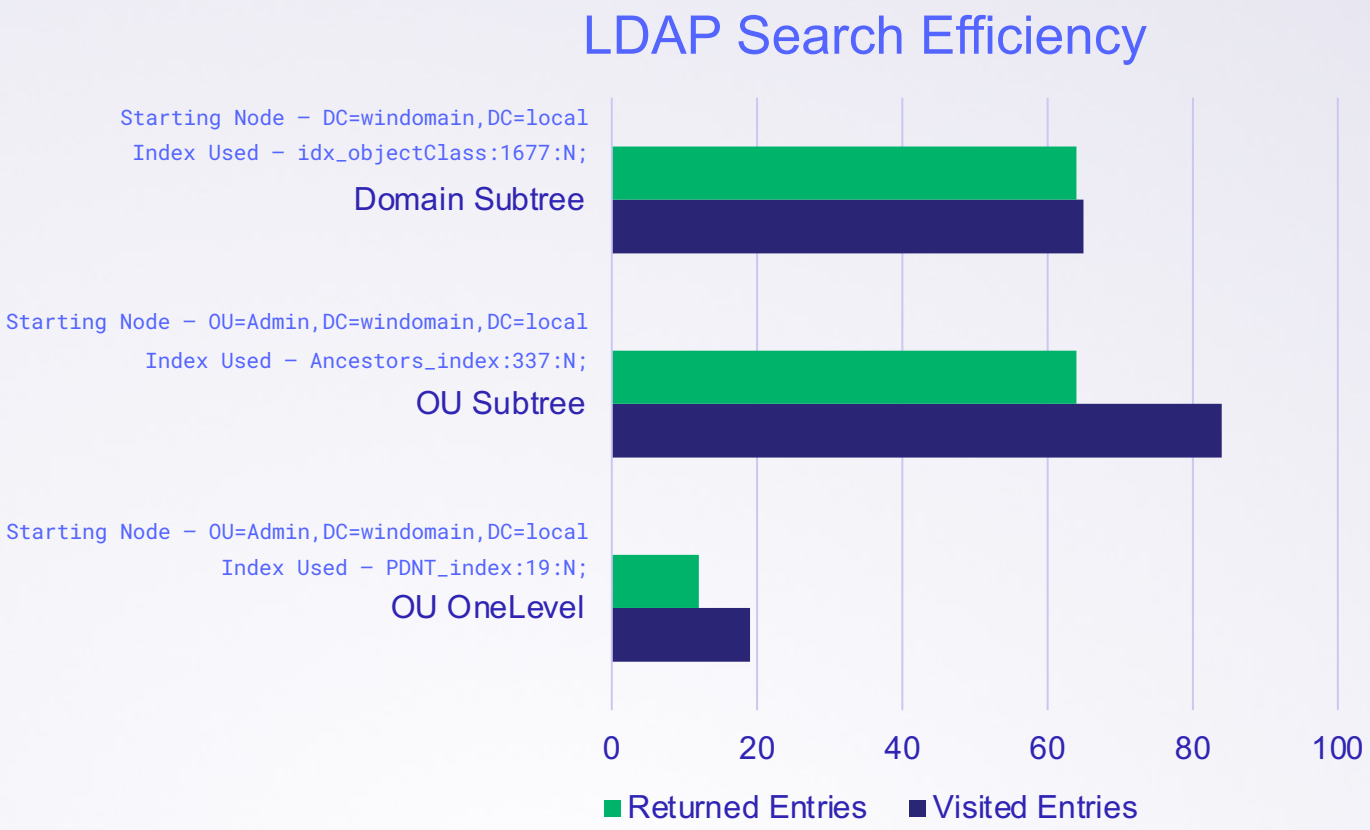
idx_objectClass– Name of the index

1677 – Represents the size or number of entries indexed by this index.

N – Type of index (Normal)

Impacts of Search Scope, Base, and Indices

(objectclass=user)



Helpful Queries/Filters

- Use ***,ntsecuritydescriptor** to return all attributes and the base64 security descriptor
- OU Walking[1]
  - `ldapsearch “(&(objectclass=organizationalunit)(name=KEYWORD*))”`
- Using Search Bases
  - `ldapsearch <filter> “” 0 “” OU=KEYWORD-OU,DC=domain,DC=local”`
- Unrolling Group Membership
  - `ldapsearch “(&(memberOf:1.2.840.113556.1.4.1941:=CN=GroupName,DC=domain,DC=local))”`
- Querying Accounts with TRUSTED_FOR_DELEGATION
  - `ldapsearch “(&(userAccountControl:1.2.840.113556.1.4.803:=524288))”`
- Pulling LAPS Information
  - `ldapsearch (name=ms-mcs-admpwd) name,schemaidguid 1 "" CN=Schema,CN=Configuration,DC=domain,DC=local`

[1]https://www.mdsec.co.uk/2024/02/active-directory-enumeration-for-red-teams/

Demo

Session Collection

Activities Applications aggressor-Aggressor Jan 24 21:41

Cobalt Strike

Cobalt Strike View Payloads Attacks Site Management Reporting Help

external	internal	listener	user	computer	note	process	pid	arch	last	sleep
192.168.0.146	192.168.0.146	https	ciri	CINTRA		beacon_x64.exe	6208	x64	668ms	2 seconds

Event Log X | Beacon 192.168.0.146@6208 X | Downloads X

```
2024-01-24T13:36:44.7260963-08:00|INFORMATION|Beginning LDAP search for redania.local
2024-01-24T13:36:44.7260963-08:00|INFORMATION|Testing ldap connection to redania.local

[01/24 21:37:16] [+] received output:
2024-01-24T13:37:14.9520766-08:00|INFORMATION|Status: 0 objects finished (+0 0)/s -- Using 59 MB RAM

[01/24 21:37:28] [+] received output:
2024-01-24T13:37:26.8670924-08:00|INFORMATION|Beginning LDAP search for redania.local Configuration NC

[01/24 21:37:30] [+] received output:
2024-01-24T13:37:28.1863361-08:00|INFORMATION|Producer has finished, closing LDAP channel
2024-01-24T13:37:28.1863361-08:00|INFORMATION|LDAP channel closed, waiting for consumers
2024-01-24T13:37:29.0186699-08:00|INFORMATION|Consumers finished, closing output channel
2024-01-24T13:37:29.0339572-08:00|INFORMATION|Output channel closed, waiting for output task to complete
Closing writers
2024-01-24T13:37:29.1302289-08:00|INFORMATION|Status: 2023 objects finished (+2023 45.97727)/s -- Using 66 MB RAM
2024-01-24T13:37:29.1302289-08:00|INFORMATION|Enumeration finished in 00:00:44.4042459
2024-01-24T13:37:29.3904934-08:00|INFORMATION|Saving cache with stats: 1984 ID to type mappings.
 1985 name to SID mappings.
 0 machine sid mappings.
 2 sid to domain mappings.
 0 global catalog mappings.
2024-01-24T13:37:29.4190786-08:00|INFORMATION|SharpHound Enumeration Completed at 1:37 PM on 1/24/2024! Happy Graphing!

[01/24 21:37:36] beacon> ls
[01/24 21:37:36] [*] Tasked beacon to list files in .
[01/24 21:37:38] [+] host called home, sent: 19 bytes
[01/24 21:37:38] [*] Listing: C:\Users\ciri\Desktop\

 Size     Type    Last Modified         Name
 ----     ----    -------------         ----
 236kb    fil     01/24/2024 13:37:29   20240124133725_BloodHound.zip
 321kb    fil     01/24/2024 06:43:26   beacon_x64.exe
 282b     fil     12/26/2023 07:07:13   desktop.ini
 328kb    fil     01/24/2024 13:37:29   NzNkODQyZDktMWNhMy00NjZmLWExZTEtYWJjMTRhNzA4NTA2.bin

[01/24 21:37:49] beacon> download 20240124133725_BloodHound.zip
[01/24 21:37:49] [*] Tasked beacon to download 20240124133725_BloodHound.zip
[01/24 21:37:51] [+] host called home, sent: 37 bytes
[01/24 21:37:51] [*] started download of C:\Users\ciri\Desktop\20240124133725_BloodHound.zip (241853 bytes)
[01/24 21:37:51] [*] download of 20240124133725_BloodHound.zip is complete
```

[CINTRA] - x64 | ciri | 6208 - x64 last:668ms

beacon>

Terminal | BloodHound — Mozilla Firefox | Cobalt Strike 1/2

Tool Support (What can we Parse)

LDAP Objects

- ldapsearch BOF
- pyldapsearch
- Brute Ratel’s LDAP Sentinel
- Aced

Session & Local Group Objects

BOFs

- netsession2
- regsession
- netloggedon2
- netLocalGroupListMembers2

Pitfalls

- Fairly niche use-case
- Time/labor intensity
- Memory consumption
  - Logs with hundreds of thousands of unique objects will probably cause Python to run out of memory during ACL parsing

TODO

Potential Future Features

- ADCS data parsing and edges
- Reduce memory consumption using an on-disk database or BHCE API
- Near real-time log monitoring
  - BHCE API integration could allow seamless C2 LDAP queries → UI updates

References

Tooling Mentioned

- https://github.com/PowerShellMafia/PowerSploit
- https://github.com/tevora-threat/SharpView
- https://github.com/RedSiege/EDD
- https://github.com/dirkjanm/BloodHound.py
- https://github.com/dirkjanm/ldapdomaindump
- https://learn.microsoft.com/en-us/sysinternals/downloads/adexplorer
- https://github.com/c3c/ADExplorerSnapshot.py
- https://github.com/FuzzySecurity/StandIn
- https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/cc732952(v=ws.11)
- https://github.com/trustedsec/CS-Situational-Awareness-BOF

SPECTEROPS

Thank you

Q/A Time!

Matt Creel | mcreel@specterops.io

Adam Brown | adam.m.brown@protonmail.com