SOAPHound — tool to collect Active Directory data via ADWS

Nikos Karouzos · Follow

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 $/month

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

directly communicating to the LDAP server. Instead, LDAP queries are wrapped within a series of SOAP messages, which are sent to the ADWS server using a NetTCPBinding communication channel. Next, the ADWS server unwraps the LDAP queries and forwards them to the LDAP server running on the same domain controller. As a result, LDAP traffic is not sent via the wire and therefore would not be easily detected by common monitoring tools.

Of course, this blog also contains some custom detections to alert you in case of SOAPHound(-like) behavior in your environment ;-)

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

. . .

Introduction

Adversaries commonly use the LDAP protocol to perform Active Directory (AD) enumeration via Active Directory Lightweight Directory Services (AD LDS). They extract information on the AD schema, such as domain users, devices, groups and their underlying access rights; providing a quick overview of the organization and significantly helping in the identification of potential attack paths. The AD schema also contains information about

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Membership

✓ Read member-only stories

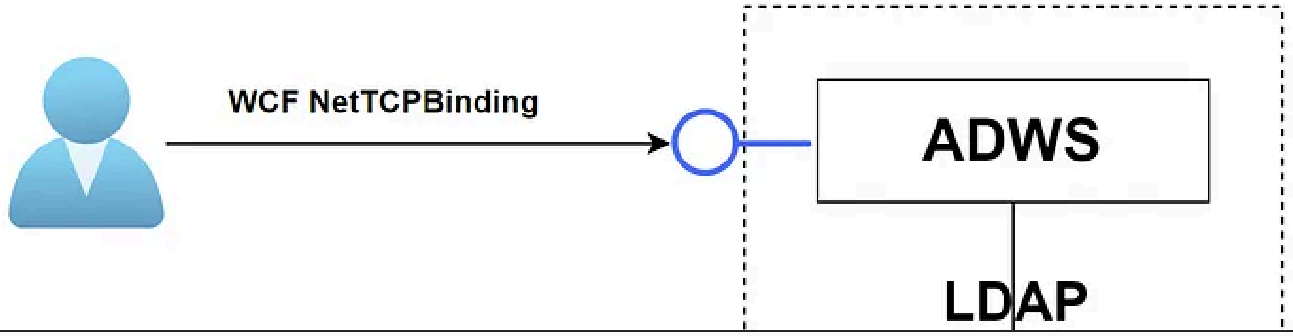
✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

legitimate tools, most notably the Active Directory module for Windows PowerShell, and provides a much faster interface to retrieve LDAP data.



Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.
✓ Organize your knowledge with lists and highlights.
✓ Tell your story. Find your audience.

Membership

✓ Read member-only stories
✓ Support writers you read most
✓ Earn money for your writing
✓ Listen to audio narrations
✓ Read offline with the Medium app

The ADWS server is listening on TCP port 9389 of domain controllers and facilitates SOAP-based search operations against directory services. It is compatible with LDAP filters, so it is possible to perform specific search queries and retrieve only the required properties. In fact, when ADWS is used, the DC performs LDAP requests internally to retrieve the results, in the context of the user sending the SOAP messages. For more information, please refer to the relevant Microsoft documentation.

ADWS clients (e.g., via the Active Directory PowerShell module) establish a NetTCPBinding session with the server, generating a run-time

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

- MS-WSMAN (Web services management protocol)

For the full list of Web Services protocols used by Active Directory systems, please refer to the MS-ADSO (Active Directory System Overview).

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

✦ Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

protocol to use. Eventually, and depending on the ADWS endpoint, SOAP messages are sent using different authentication mechanisms, as shown in the below table:

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

potential of the protocol, as well as developing the initial versions of SOAPHound.

Challenge #1 — Debugging

Our first challenge when playing around with the ADWS protocol was to debug the actual traffic sent to the ADWS server. Initially, we used the PowerShell AD module as our client, which is the most common tool using this protocol.

Running a simple Get-ADUser command within a Windows Domain context

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

✦ Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

We parsed only the fields required for ingestion from the results using LINQ. Most properties are simple strings that can be easily parsed. Some are more complex and are encoded as a list of strings; for example, group members, byte arrays, etc. All data was parsed into a generic class called ADObject that has the appropriate definitions.

Challenge #3 — nTSecurityDescriptor attribute

The nTSecurityDescriptor is one of the most crucial LDAP attributes to enumerate, since it contains the Access Control Entries (ACEs), owner information, and inheritance assigned to the object. If parsed properly, it

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- Distraction-free reading. No ads.
- Organize your knowledge with lists and highlights.
- Tell your story. Find your audience.

Membership

- Read member-only stories
- Support writers you read most
- Earn money for your writing
- Listen to audio narrations
- Read offline with the Medium app

Initially, our attempts to retrieve the nTSecurityDescriptor attributes of objects failed due to permission errors. The reason was explained in this blog post. The nTSecurityDescriptor attribute contains 4 separate pieces of information: DACL (Discretionary ACL), SACL (System ACL), Owner, and Primary Group. When you query Active Directory it will attempt by default to retrieve all parts of the security descriptor. However, your account may not have access to all parts (most notably, the SACL). When this happens, AD decides to simply not return anything. To get around the limitation above and still query the nTSecurityDescriptor, you need to use an LDAP control to specify you do not want the SACL. The control is

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- Distraction-free reading. No ads.
- Organize your knowledge with lists and highlights.
- Tell your story. Find your audience.

Membership

- Read member-only stories
- Support writers you read most
- Earn money for your writing
- Listen to audio narrations
- Read offline with the Medium app

- ACE type (allow/deny/audit)
- ACE flags (inheritance and audit settings)
- Permissions (list of incremental permissions)
- **ObjectType (GUID)**
- **Inherited Object Type (GUID)**
- **Trustee (SID)**

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

LDAP query, which is run before collecting the actual data and retrieves the “ObjectSID”, “ObjectGUID”, “DistinguishedName” and “ObjectClass” attributes of all objects within the Active Directory. Refer to the “ — buildcache” mode of the SOAPHound tool below.

Challenge #4 — Optimize size and stealthiness

Another point of interest was to stay under the radar of monitoring tools. Not only regarding the network traffic (which was more or less sorted by design, by using ADWS protocol), but also in the actual LDAP queries being sent by the tool. We did not want to trigger detections by using known LDAP

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

At this point, we had created a working and stable version of SOAPHound, which has been thoroughly tested in our lab. However, when we tried to actually run it in a client Active Directory environment, we ran into a timeout issue. More specifically, our LDAP request to retrieve all AD objects was failing after 30 minutes, which is the default expiration interval for EnumerationContext requests. After some additional research, we realized that the 30 minute timeout was set by default by the ADWS server and we could not renew the EnumerationContext at the client side without losing the previously obtained data. The only solution was to save the data that we have already obtained and reconnect with a new EnumerationContext request

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

SOAPHound supports the following authentication methods:

- Using the existing authentication token of the current user. This is the default option, if no username and password are supplied.
- Supplying a username and password on the command-line (--*user* and --*password* arguments, respectively).

Connection options

When SOAPHound runs in a domain-joined machine, it will automatically

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

is used when crafting the trust relationships between objects via the relevant Access Control Entries (ACEs).

An example command to build the cache file is:

```
SOAPHound.exe --buildcache -c c:\temp\cache.txt
```

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Showstats runs locally and does not send any network traffic.

Method 2: collecting BloodHound Data (--bhdump)

After the cache file has been generated, you can use the --*bhdump* collection method to collect data from the domain that can be imported into BloodHound.

An example command to collect BloodHound data is below. Do note that this

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- Distraction-free reading. No ads.
- Organize your knowledge with lists and highlights.
- Tell your story. Find your audience.

✦ Membership

- Read member-only stories
- Support writers you read most
- Earn money for your writing
- Listen to audio narrations
- Read offline with the Medium app

The JSON files contain the collected Users, Groups, Computers, Domains, GPOs and Containers, including their relationships.

LDAP queries being sent:

```
LDAP base: defaultNamingContext of domain
LDAP filter: "(!soaphound=*)"
LDAP properties: "name", "sAMAccountName", "cn", "dNSHostName", "objectSid", "object
```

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- Distraction-free reading. No ads.
- Organize your knowledge with lists and highlights.
- Tell your story. Find your audience.

Membership

- Read member-only stories
- Support writers you read most
- Earn money for your writing
- Listen to audio narrations
- Read offline with the Medium app

```
SOAPHound.exe -c c:\temp\cache.txt --bhdump -o c:\temp\bloodhound-output
--autosplit --threshold 1000
```

This will generate the output in batches of a maximum of 1000 objects per starting letter. If there are more than 1000 objects for a single starting letter, SOAPHound will use two depth levels to retrieve the objects. This will result in larger number of queries, each one returning a maximum of 1000 objects.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Method 3: collecting ADCS Data (--certdump)

After the cache file has been generated, you can use the --*certdump* collection method to collect ADCS data from the domain that can be imported into BloodHound. ADCS output data is classified as GPOs in BloodHound.

This collection method does not support the --*autosplit* and --*threshold* command-line arguments. An example command to collect ADCS data is below. Note that this references the cache file generated in a previous step.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Method 4: collecting AD-integrated DNS data (--dnsdump)

Besides BloodHound data, SOAPHound can also be used to collect AD-integrated DNS data. This does not require a cache file and does not support the --*autosplit* and --*threshold* command-line arguments.

An example command to collect AD Integrated DNS data is:

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

which information gathering attempts using SOAPHound can be detected.

Revisiting previous FalconFriday detections in the context of ADWS

We previously released a FalconFriday blog post about detecting Active Directory data collection in 2021: https://falconforce.nl/falconfriday-detecting-active-directory-data-collection-0xff21/.

This 2021 blog post described three methods to detect the collection:

1. Client-side LDAP query logging using Microsoft Defender for Endpoint

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

queries per day, this would lead to a very large amount of telemetry being collected and stored.

We discovered that for LDAP queries the following capping is applied by the MDE agent:

- Within a 24 hour period only one entry is logged if the SearchFilter, DistinguishedName and Initiating process are the same.
- A maximum of 1000 LDAP queries are logged per machine per day,

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

agent. The downside of this detection method is that it only records LDAP queries that it finds suspicious. It is possible for an attacker to modify the exact LDAP queries used; to make them appear as benign. For example, by avoiding the usage of *ObjectClass=**. Since most queries performed by SOAPHound at this time are not considered to be suspicious by MDI, it is hard to use this method to detect collection. Unfortunately, the identification of which queries are considered to be suspicious in MDI cannot be configured by using a method similar to custom detections.

3. Domain controller object access logging via SACLs and audit policies

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

include IPs where the *microsoft.activedirectory.webservices.exe* binary is running. This only works when the target machine is also enrolled in MDE.

In a typical environment there are only a handful of programs that are making connections to the ADWS service:

- Active Directory Administrative Center (dsac.exe)
- Microsoft Monitoring Agent
- PowerShell

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Conclusion

Information gathering methods in Active Directory were already challenging to detect. The release of this new tool that targets ADWS instead of directly targeting LDAP further increases the need for custom detections in this area. The existing method based on the number of AD Objects being accessed by a user is still the most reliable way to detect data collection, but it does require a custom SACL to be configured and has a high log volume. Existing telemetry can be used to specifically detect the ADWS-based collection, by

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

✦ Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

--

Written by Nikos Karouzos

Follow

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app