Microsoft

Reconnaissance actions

Threats targeting the hybrid & cloud identity platforms

External resources disclaimer

This material includes links to external publicly available articles, projects, and research papers which are provided to you as a convenience and for informational purposes only.

Microsoft bears no responsibility for the accuracy, legality, content or any other aspect of the external site. Use of external hyperlinks does not constitute an endorsement by Microsoft of the linked content.

The external content referenced in this document belongs exclusively to their respective author(s). Inclusion in this presentation does not grant you with any right on the external content. You must comply with the original source's applicable policies.

How to use this document

Why this document?

This document is provided as a companion of the video lessons. Additional information is included here which would not fit the video format or would exaggeratedly lengthen the videos. As you are watching the videos, the instructor will point you to additional content in this document.

Structure

The structure of this slide deck follows the structure of the lessons. One slide deck is provided for each module. The slide deck has the same structure (naming of chapters and sections) as the associated video so that you can quickly jump to the slides of the lesson you are currently watching.

Foreword

This deck contains some design artefacts which all have their importance…

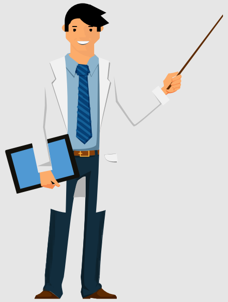
Abbr.

This sticky note icon is used to introduce the **abbreviation** of a concept or a technical word. Once the abbreviation has been introduced, the full version is no longer mentioned.

You will also find a list of all abbreviations at the end of the deck.

We were all young once. A section with this icon will tell you the **history** you might have missed by not working with the technology for the last 20 years.

Just because you are new does not mean you do not have to know how we got here!



Professor Useful will introduce some **tricky technical details** which might not seem relevant at first but could end up being really useful if you want to dig deeper in the technology.

This frame contains…

- Takeaways so important that we framed them

How to know the slide level

This deck contains 3 different content levels:

1. Regular level, the common slide
2. Advanced level, a slide with this indicator at the top left Adv.
3. Additional content, all hidden slides

Sequence

2

Reconnaissance actions

Learning Objectives

Protect an environment from reconnaissance actions.

Agenda

1. Information collection using Lightweight Directory Access Protocol (LDAP)
2. Account enumeration through SAM-R interface
3. Network mapping using DNS
4. Mapping users and machines using SMB enumeration

Chapter

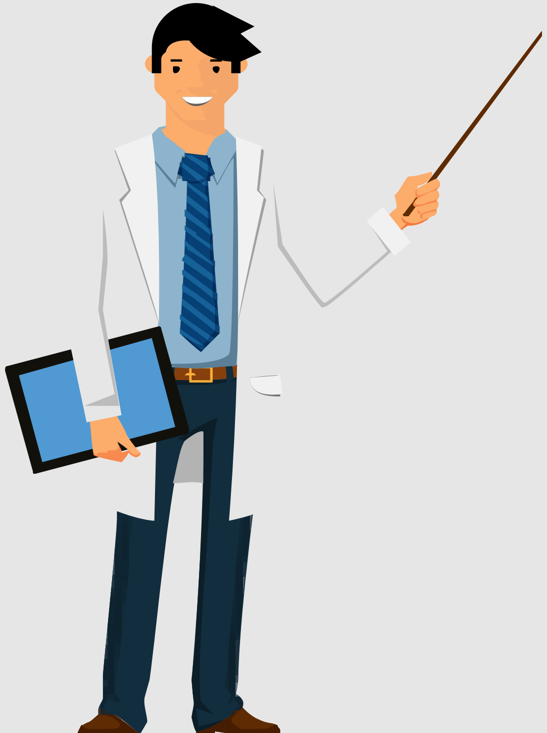
2.2.1

Information collection using LDAP

🎯 List the types of LDAP filters used during recognition

Why use LDAP?

- Easy, standard protocol
- Requires DC connectivity (TCP 389/636 and/or 3268/3269)
- Authenticated users can read (almost) everything



Except Secrets (nobody can read them) and
Confidential attributes (only designated users can)

Adv.

🤫 Confidential attributes

- Schema admins can mark attributes as confidential
- Restrict who can read them
  - By default, only the admin
  - But can be delegated with the CONTROL_ACCESS permission
- Examples
  - Roaming secret keys
  - Computer passwords (Local Administrator Password Solution)

LAPS

Useful LDAP queries

- List all group members
  - Privileged groups
  - Protected objects

- List users’ security settings
  - Password change dates
  - User options

- List the OUs and the linked GPO

The userAccountControl attribute

- Attribute that stores various information about the account
- Binary flags
  - Examples:

Value	Flags	Meaning
514	512 + 2	Normal Account + Account disabled
66048	512 + 65536	Normal Account + Password never expires
546	512 + 32 + 2	Normal Account + Password not required + Account disabled

  - Sensitive flags to look for:
    PASSWD_NOTREQD
    ENCRYPTED_TEXT_PWD_ALLOWED
    DONT_EXPIRE_PASSWORD
    TRUSTED_FOR_DELEGATION
    USE_DES_KEY_ONLY
    DONT_REQ_PREAUTH

Adv.

The PASSWD_NOTREQD flag

- Flag of the userAccountControl attribute
- The account does not require a password **BUT** it does not mean that it does not have a password
- Only an operator with **Password Reset** permission can set a blank password on an account with that flag on

- It should be removed after user account creation if the account is created by a script
- It should be removed after a manual computer account creation

LDAP GUI builtin tools

- Remote Server Administration Tools

RSAT

- Active Directory Users and Computers console
  - List all domain objects and their attributes
  - Search wizards
  - Shortcut: `dsa.msc`
- Administrative Center
  - Newer console, more options than its predecessor
  - Multi forests management, new search options, GUI for newest features such as Authentication Policies or Fine Grained Password Policies
  - Shortcut: `dsac.exe`
- Group Policy Management console
  - List all group policies and visualize settings in HTML
  - Shortcut: `gpmc.msc`

Adv.

LDAP GUI builtin tools

- Active Directory Sites and Services console
  - List all configuration related to forest applications, such as Exchange configuration, AD replication configuration, certificate services configuration…
  - Shortcut: `dssite.msc`
- Windows Admin Center
  - Web-based tool replacing the Windows Server Manager
  - More about it later in this course
- “Find users, contacts and groups” wizard
  - Available on all Windows versions
  - Command line: `%SystemRoot%\SYSTEM32\rundll32.exe dsquery,OpenQueryWindow`

Adv.

LDAP CLI builtin tools

- dsquery.exe
  - Example: `dsquery user -samid Administrator`
- dsget.exe
  - Example: `dsquery user -samid Administrator | dsget user -sid`
- repadmin.exe
  - To manage replication related matters
  - Can also be used to query metadata and attributes
- PowerShell
  - Active Directory Module
  - [ADSI] object class
  - [System.DirectoryServices] classes

LDAP filter examples

All enabled users

```
(&(objectCategory=person)(objectClass=user)
(!(userAccountControl:1.2.840.113556.1.4.803:=2)))
```

Domain Admins direct members

```
(memberOf=CN=Domain Admins,CN=Users,DC=contoso,DC=com)
```

Domain Admins members (including nested group members) [1]

```
(memberOf:1.2.840.113556.1.4.1941:=CN=Domain Admins,CN=Users,DC=piesec,DC=ca)
```

Enabled users who have not logged in for the last 90 days [2]

```
(&(objectCategory=person)(objectClass=user)(!userAccountControl:1.2.840.113556.1
.4.803:=2)(|(lastLogonTimestamp<=132977628000000000)(!lastLogonTimestamp=*)))
```

LDAP back in the day…

- Back in Windows 2000 Server
  DCs accepted anonymous LDAP calls

- There is still a setting to allow them but it's off by default since 2003

- Anonymous binds always work, but you don't get to list anything

Adv.

List Object Access Mode

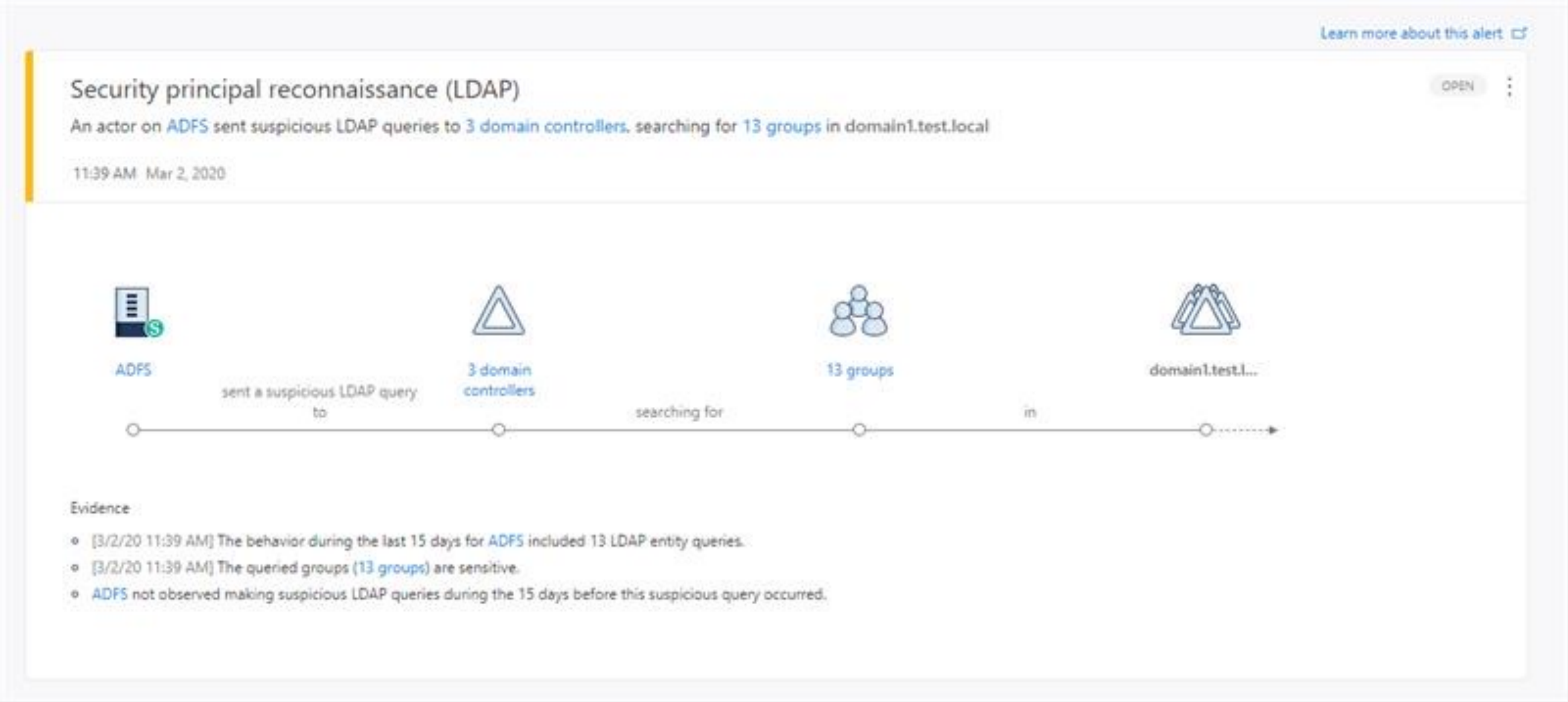
- Rare configuration

🛑 **Not recommended**

- Change the default permissions of authenticated users
  - Users must be granted the permission to list containers
  - Can break a lot of applications if not well understood/deployed

Detection

- Example of alerts from Microsoft Defender for Identity



Security principal reconnaissance (LDAP)

An actor on ADFS sent suspicious LDAP queries to 3 domain controllers, searching for 13 groups in domain1.test.local

11:39 AM Mar 2, 2020

Evidence

- [3/2/20 11:39 AM] The behavior during the last 15 days for ADFS included 13 LDAP entity queries.
- [3/2/20 11:39 AM] The queried groups (13 groups) are sensitive.
- ADFS not observed making suspicious LDAP queries during the 15 days before this suspicious query occurred.

LDAP search logging

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Diagnostics]
"15 Field Engineering"=dword:00000005

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters]
"Expensive Search Results Threshold"=dword:00000001
"Inefficient Search Results Threshold"=dword:00000001
"Search Time Threshold (msecs)"=dword:00000001
```

- Generate events 1644 in the Directory Service
- Very, very verbose
- May impact DCs’ performance

LDAP enumeration attack summary

Attack's pre-requisites

- A regular account (or just network connectivity if anonymous access is enabled)

Protection

- Make sure anonymous access for LDAP is disabled
- Enable logging[1]

Chapter

2.2.2

Account enumeration through Security Account Manager Remote protocol (SAM-R) interface

🎯 Develop a plan to reduce the risk of information exposure through SAM-R

User and Group membership reconnaissance (SAM-R)

- Security account manager remote protocol (SAM-R) is a protocol that allows the remote management of users, groups and other security principals

- An attacker can exploit this protocol to enumerate accounts and groups for a server, workstation or a Domain Controller

SAM-R on domain members

- Only for members of the local administrator group can use it
  - Before Windows Server 2016/Windows 10 any authenticated user
- Governed by security settings
  - ⚙ Network access: Restrict clients allowed to make remote calls to SAM
  - Backported to Windows Server 2008 R2/Windows 7 and higher

Recommended to restrict SAM-R to all versions of Windows on **member server**

Adv.

Anonymous SAM on domain members

- Disabled by default
- Governed by security settings

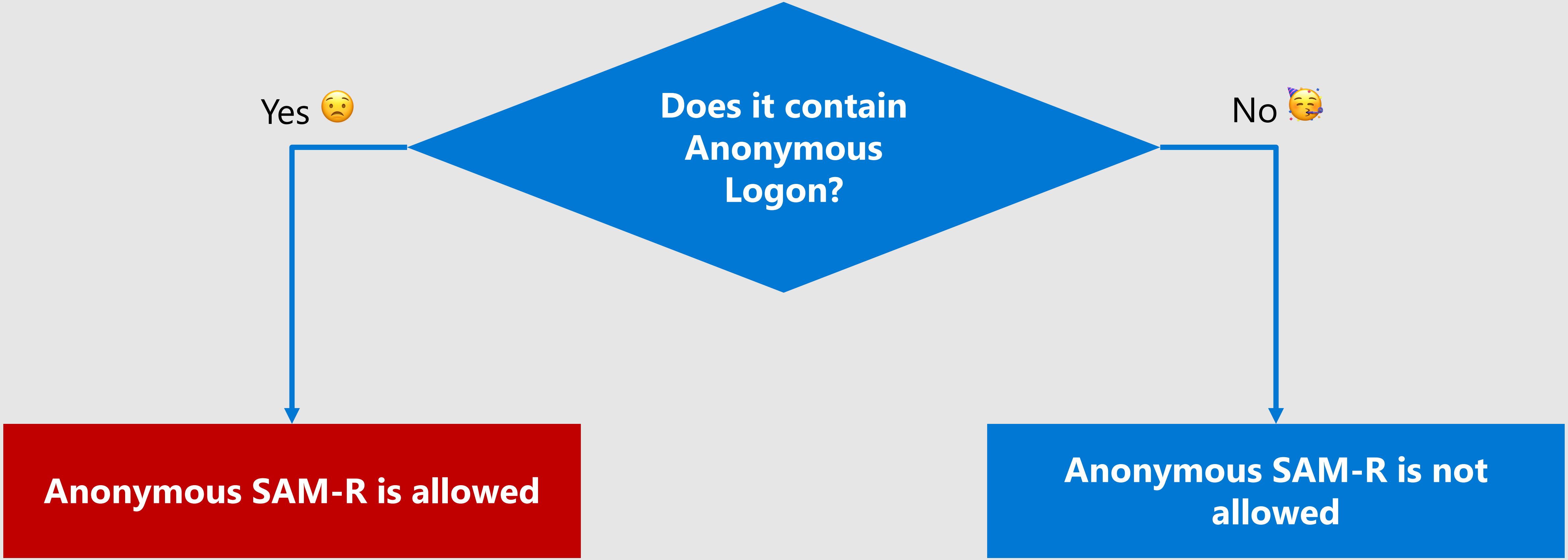
  ⚙ Network access: Do not allow anonymous enumeration of SAM accounts

  ⚙ Network access: Do not allow anonymous enumeration of SAM accounts and shares

- Those settings do not apply to domain controllers

Anonymous SAM on domain controllers

- Pre-Windows 2000 Compatible Access group


Does it contain Anonymous Logon?
Yes 😟
No 🥳
Anonymous SAM-R is allowed
Anonymous SAM-R is not allowed

Anonymous SAM on domain controllers

- Pre-Windows 2000 Compatible Access group

Remove the **Anonymous Logon** security principal from the **Pre-Windows 2000 Compatible Access group**

- Although possible, restricting **Authenticated Users** from performing SAM-R queries on domain controllers will impact systems and applications compatibility

SAM enumeration examples

Using net.exe

```
net.exe users /domain
net.exe groups /domain
```

Anonymous SAM-R enumeration with nmap.exe

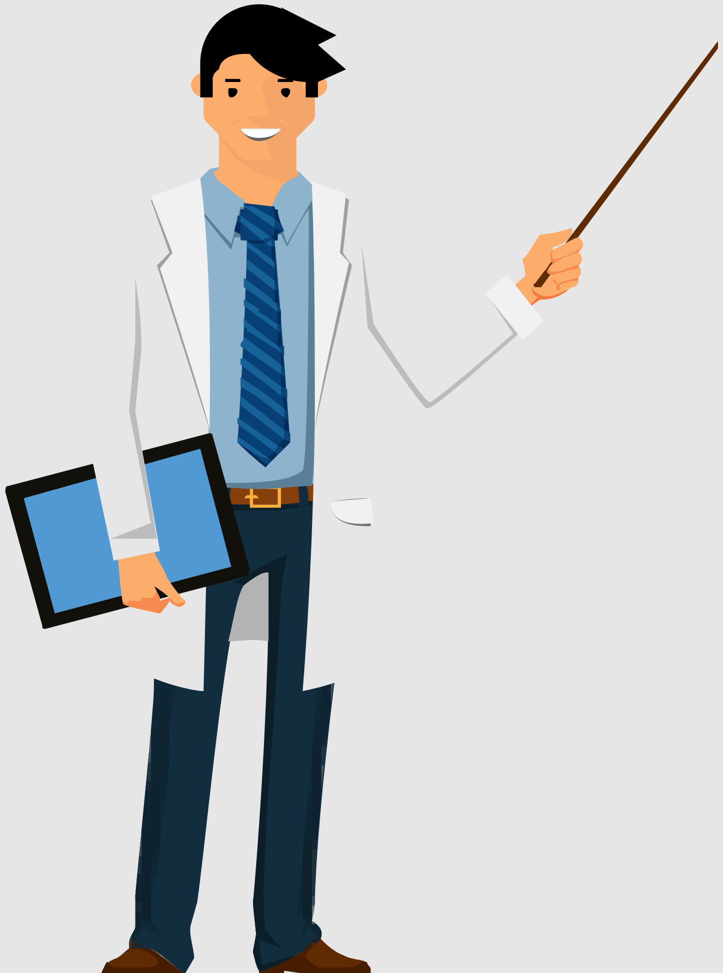
```
nmap.exe --script smb-enum-users.nse -p 445 10.0.0.10
```

SAM-R enumeration with nmap.exe

```
nmap.exe --script smb-enum-users.nse --script-args
smbuser=normaluser,smbpass=password -p 445 10.0.0.10
```

Adv.

SAM database on domain controllers



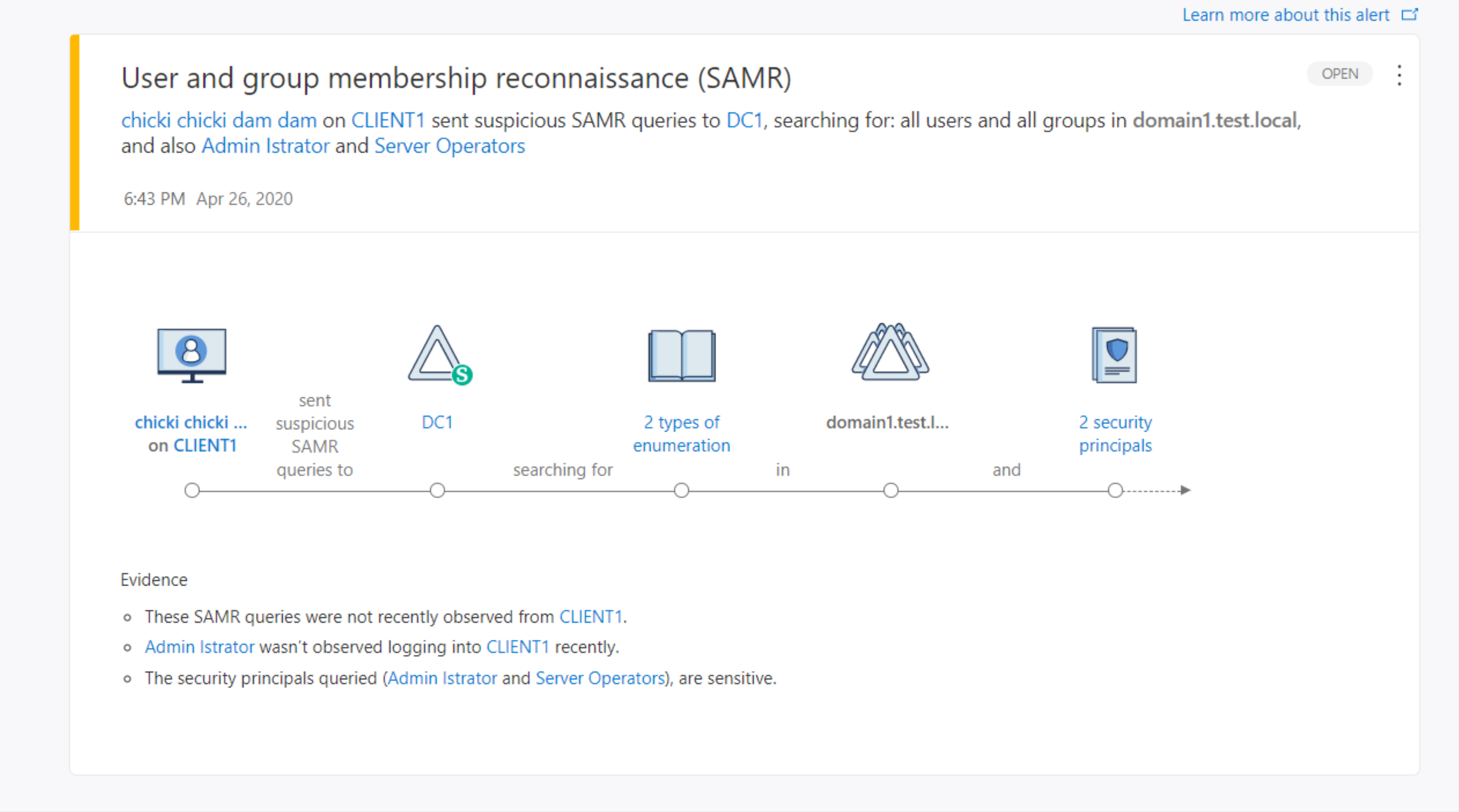
DCs also have a SAM database used when the DC restarts in recovery mode

It contains the admin account you can use to log in to the console

⚠ But can be used at any time if the registry value DsrmAdminLogonBehavior is set to 2

Detection on domain controllers

- Example of alerts from Microsoft Defender for Identity



Learn more about this alert

User and group membership reconnaissance (SAMR)

OPEN

chicki chicki dam dam on CLIENT1 sent suspicious SAMR queries to DC1, searching for: all users and all groups in **domain1.test.local**, and also Admin Istrator and Server Operators

6:43 PM Apr 26, 2020

Evidence

- These SAMR queries were not recently observed from CLIENT1.
- Admin Istrator wasn't observed logging into CLIENT1 recently.
- The security principals queried (Admin Istrator and Server Operators), are sensitive.

SAMR enumeration attack summary

Attack’s pre-requisites

- A regular account (or just network connectivity if anonymous access is enabled)

Protection

- Limit SAMR enumeration to local admins only on member servers
- Make sure anonymous SAMR is disable on domain controllers

Chapter

2.2.3

Network mapping using Domain Name System (DNS)

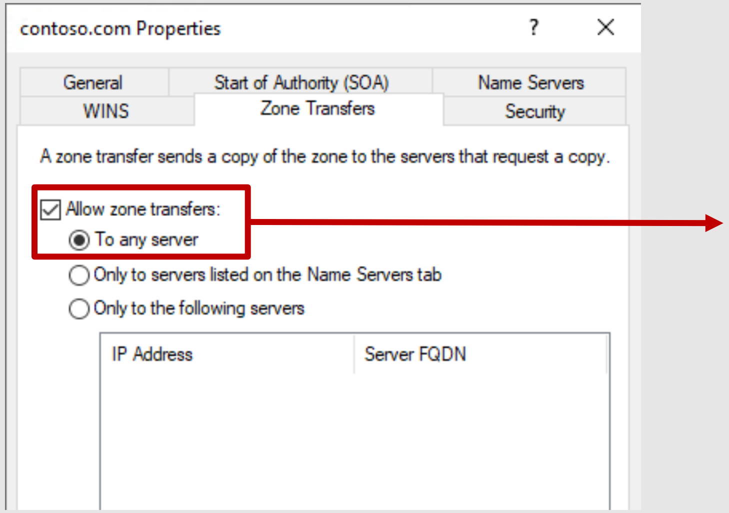
🎯 Limit recognition actions using DNS

Network mapping reconnaissance using DNS

- Ubiquitous protocol
- Does not require authentication
  - Only network connectivity UDP/TCP 53
- “Brute forcing” DNS
  - Trying all or many DNS requests to discover names and services
- List all domain controllers
  - By listing SRV records used for the DC location process

Abuse of zone transfers

- Sometimes misconfigured
  - Zone transfer is not required to replicate DNS data when the zone is integrated in AD DS
  - Can be done with tools such as nslookup
  - Should be either disabled or restricted to specific servers



contoso.com Properties

A zone transfer sends a copy of the zone to the servers that request a copy.

☑ Allow zone transfers:

● To any server

○ Only to servers listed on the Name Servers tab

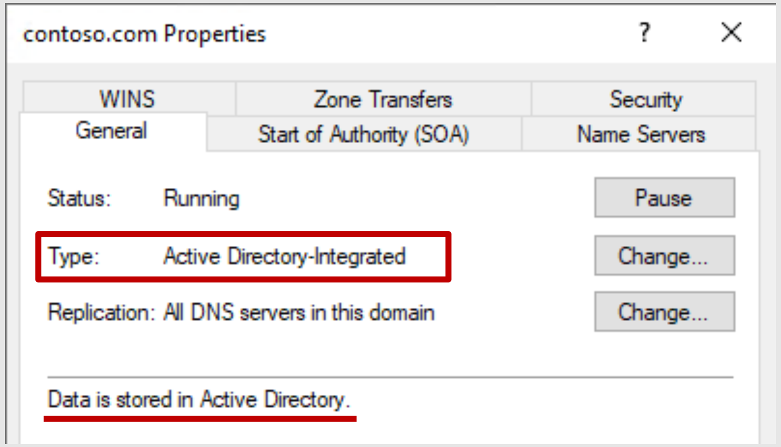
○ Only to the following servers

IP Address	Server FQDN

misconfiguration

Abuse of zone transfers

- Integrated zones
  - Turn DNS into a multi-master model
  - Allow authenticated dynamic updates
  - Records are stored in the AD DS database



contoso.com Properties

Status: Running

Type: Active Directory-Integrated

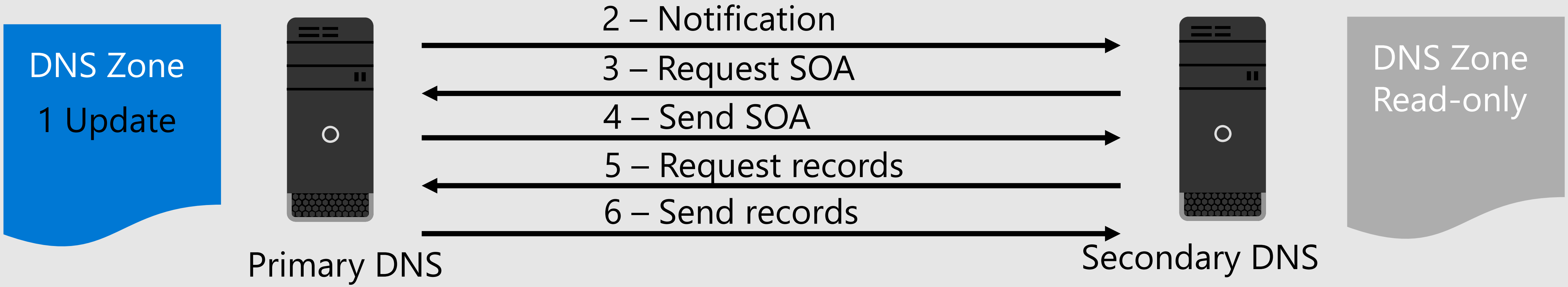
Replication: All DNS servers in this domain

Data is stored in Active Directory.

Adv.

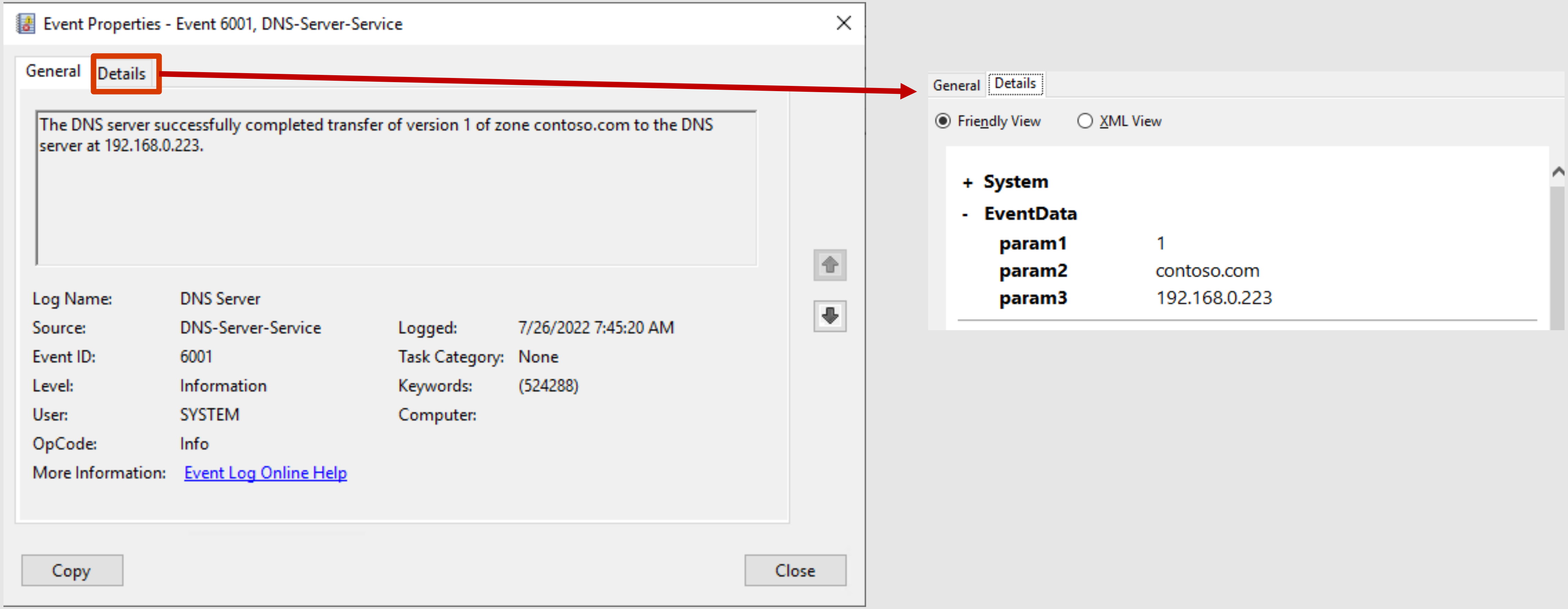
Zone transfers

- Offer a way to maintain DNS secondary servers up to date
  - Full transfer: AXFR
  - Incremental transfer: IXFR
  - Can also use notifications



Detection on DNS servers

- Zone transfers generate an event on the DNS server



Event Properties - Event 6001, DNS-Server-Service

The DNS server successfully completed transfer of version 1 of zone contoso.com to the DNS server at 192.168.0.223.

Log Name: DNS Server

Source: DNS-Server-Service

Logged: 7/26/2022 7:45:20 AM

Event ID: 6001

Task Category: None

Level: Information

Keywords: (524288)

User: SYSTEM

Computer:

OpCode: Info

More Information: Event Log Online Help

● Friendly View ○ XML View

+ System
- EventData

param1	1
param2	contoso.com
param3	192.168.0.223

DNS reconnaissance

Brute force DNS

```
nmap.exe --script dns-brute --script-args dns-brute.domain=contoso.com,dns-
brute.srv 10.0.0.10
```

Enumerate DCs

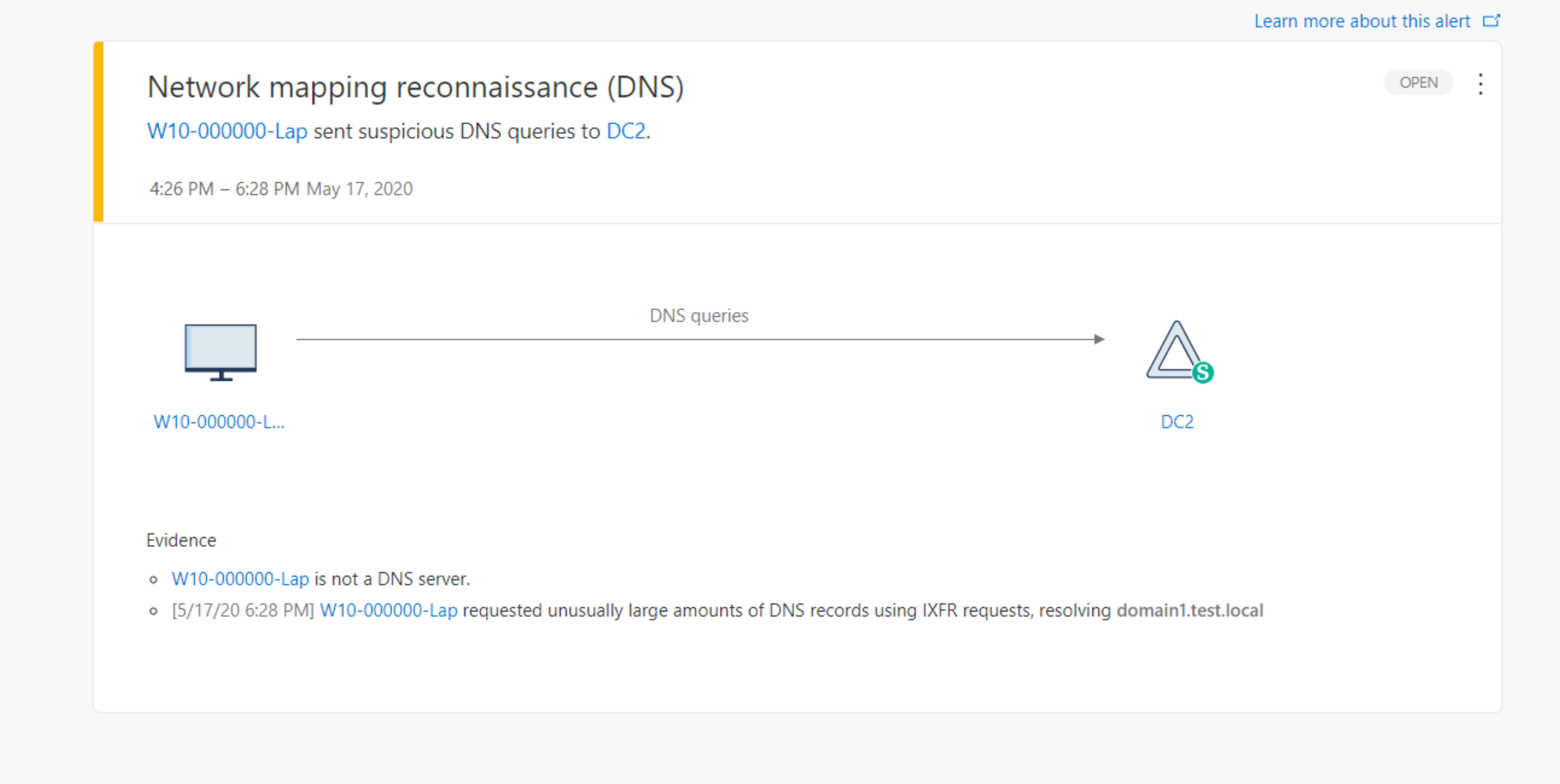
```
nltest.exe /DCLIST:contoso.com
```

Trigger zone tranfer

```
nslookup.exe
set d
ls –t ALL contoso.com.
```

Detection on DNS servers

- Example of alerts from Microsoft Defender for Identity



Learn more about this alert

Network mapping reconnaissance (DNS)

OPEN

W10-000000-Lap sent suspicious DNS queries to DC2.

4:26 PM – 6:28 PM May 17, 2020

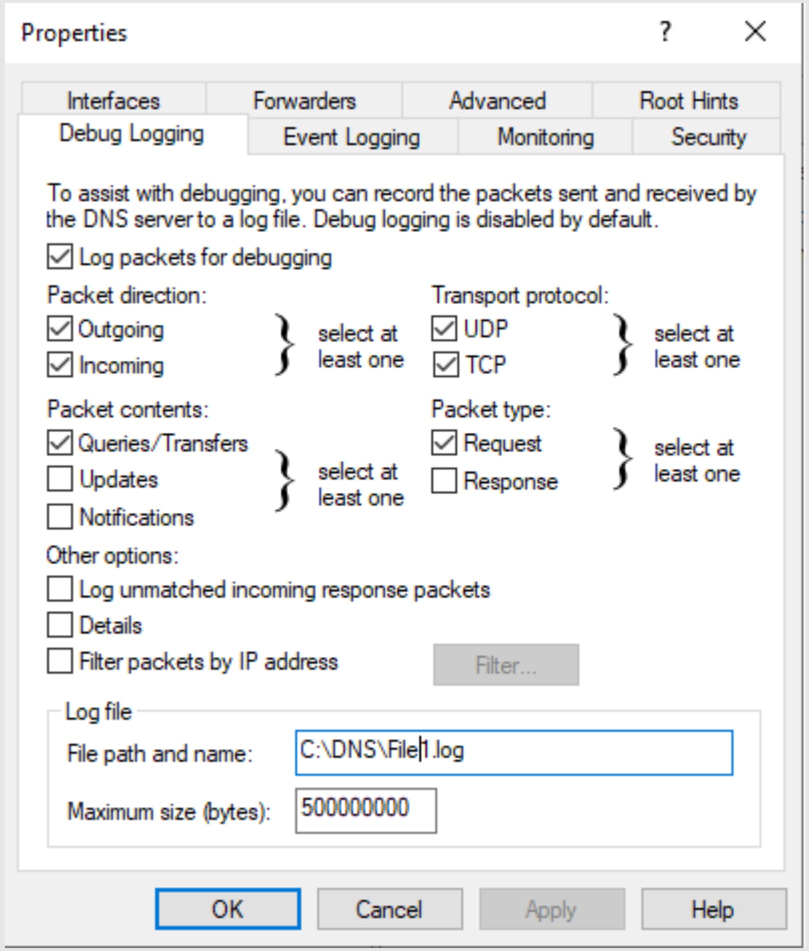
Evidence

- W10-000000-Lap is not a DNS server.
- [5/17/20 6:28 PM] W10-000000-Lap requested unusually large amounts of DNS records using IXFR requests, resolving domain1.test.local

Adv.

Detection on DNS servers

- Debug logs on DNS servers
  - Can log everything
  - Very, very verbose
  - Hard to automate collection (text file)



To assist with debugging, you can record the packets sent and received by the DNS server to a log file. Debug logging is disabled by default.

☑ Log packets for debugging

Packet direction:
☑ Outgoing
☑ Incoming
} select at least one

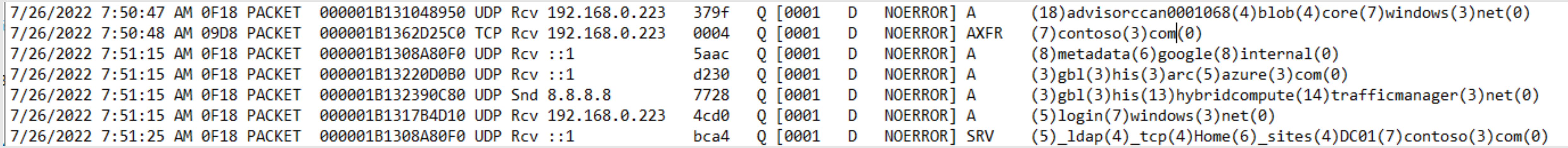
Transport protocol:
☑ UDP
☑ TCP
} select at least one

Packet contents:
☑ Queries/Transfers
☐ Updates
☐ Notifications
} select at least one

Packet type:
☑ Request
☐ Response
} select at least one

Other options:
☐ Log unmatched incoming response packets
☐ Details
☐ Filter packets by IP address

Log file
File path and name: C:\DNS\File1.log
Maximum size (bytes): 500000000



```
7/26/2022 7:50:47 AM 0F18 PACKET  000001B131048950 UDP Rcv 192.168.0.223   379f   Q [0001   D   NOERROR] A      (18)advisorccan0001068(4)blob(4)core(7)windows(3)net(0)
7/26/2022 7:50:48 AM 09D8 PACKET  000001B1362D25C0 TCP Rcv 192.168.0.223   0004   Q [0001   D   NOERROR] AXFR   (7)contoso(3)com(0)
7/26/2022 7:51:15 AM 0F18 PACKET  000001B1308A80F0 UDP Rcv ::1             5aac   Q [0001   D   NOERROR] A      (8)metadata(6)google(8)internal(0)
7/26/2022 7:51:15 AM 0F18 PACKET  000001B13220D0B0 UDP Rcv ::1             d230   Q [0001   D   NOERROR] A      (3)gbl(3)his(3)arc(5)azure(3)com(0)
7/26/2022 7:51:15 AM 0F18 PACKET  000001B132390C80 UDP Snd 8.8.8.8         7728   Q [0001   D   NOERROR] A      (3)gbl(3)his(13)hybridcompute(14)trafficmanager(3)net(0)
7/26/2022 7:51:15 AM 0F18 PACKET  000001B1317B4D10 UDP Rcv 192.168.0.223   4cd0   Q [0001   D   NOERROR] A      (5)login(7)windows(3)net(0)
7/26/2022 7:51:25 AM 0F18 PACKET  000001B1308A80F0 UDP Rcv ::1             bca4   Q [0001   D   NOERROR] SRV    (5)_ldap(4)_tcp(4)Home(6)_sites(4)DC01(7)contoso(3)com(0)
```

Abuse of the zone integration

- When DNS is integrated in AD, all the DNS data is available through LDAP

- Using LDAP to extract DNS might evade some detection tools

- Results must be parsed
  - Some records are stored in binary format

- LDAP search logging can be used to detect enumerations

DNS enumeration attack summary

Attack's pre-requisites

- Network connectivity

Protection

- Disable zone transfer
- Enable logging[1]

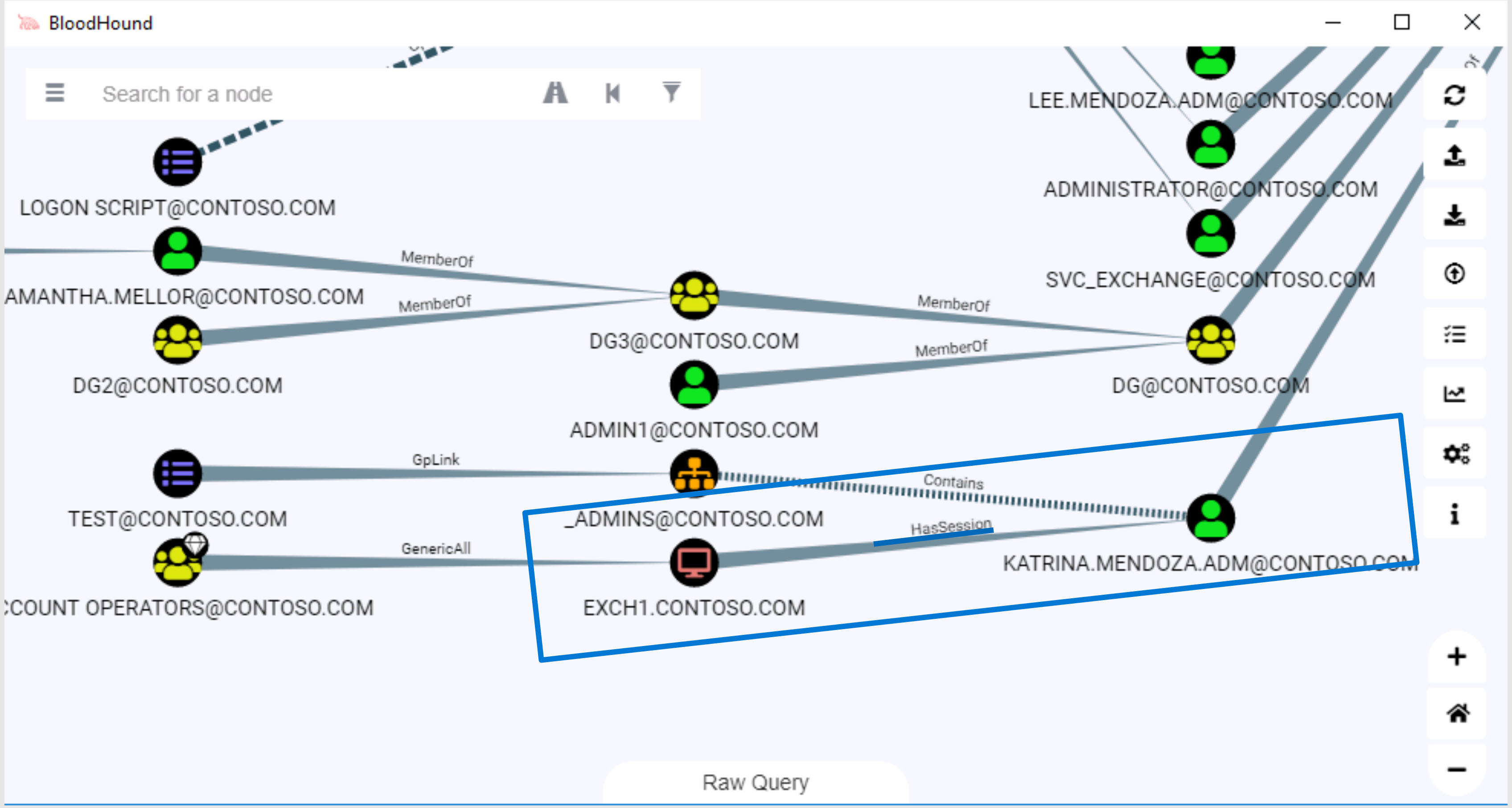
Chapter

2.2.4

Mapping users and machines using SMB enumeration

🎯 Protect AD from SMB enumeration

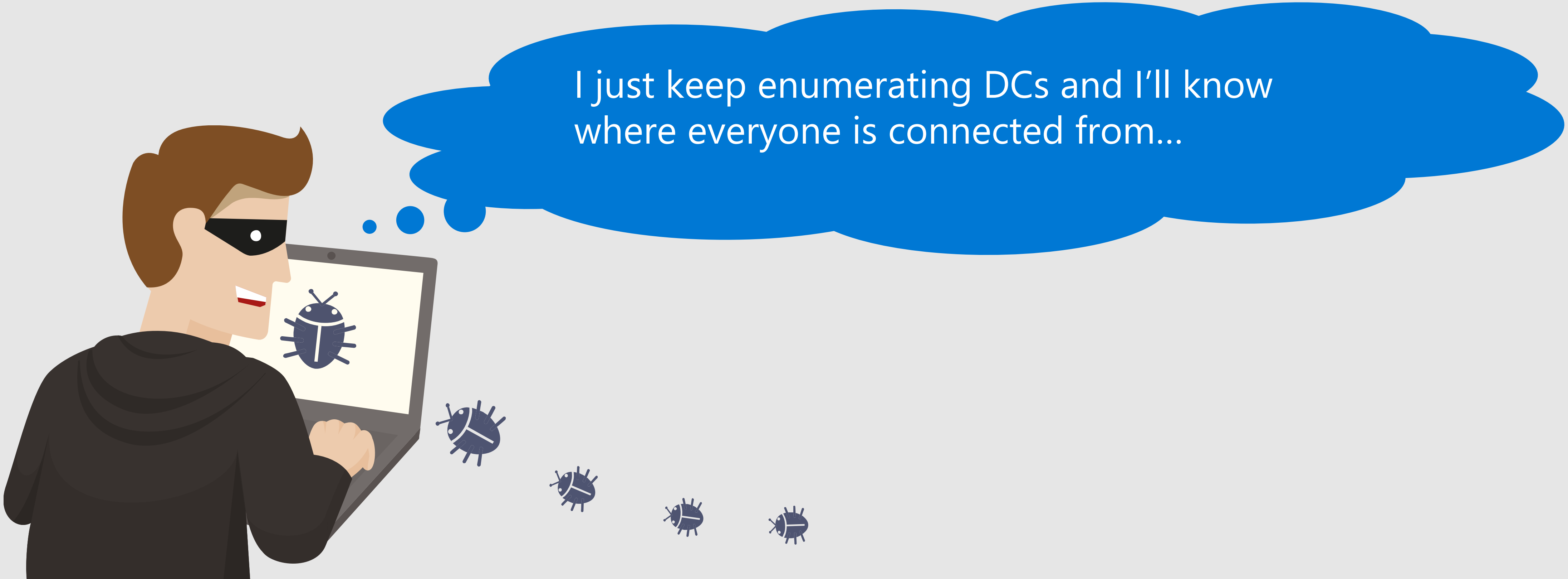
SMB enumeration



SMB session enumerations help attackers to detect where users are connected from

Why are attackers having a blast with SMB?

- Domain Controllers are always SMB servers (because of SYSVOL)
- All domain joined clients will connect to it at some point
- Not always monitored


I just keep enumerating DCs and I’ll know where everyone is connected from…

SMB enumeration tools

Using SMBv1

```
nmap.exe -p 445 --script smb-enum-sessions.nse --script-args
smbuser=nomraluser,smbpass=password DC01
```

Using NetSess.exe

```
NetSess.exe DC01
```

Using PowerShell

```
Invoke-NetSessionEnum -HostName DC01
```

Restrict SMB enumeration

- Permissions are governed by a registry value

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\DefaultSecurity]
"SrvsvcSessionInfo"
```

- Binary structure
- Can be modified with **Net-Cease** PowerShell module
  - Only administrator should be granted the permission to enumerate sessions

✅ Restrict it on Domain Controllers and other SMB servers

Restrict SMB enumeration with Net-Cease

List permissions

```
Get-NetSessionEnumPermission
```

Disable enumeration for Authenticated Users

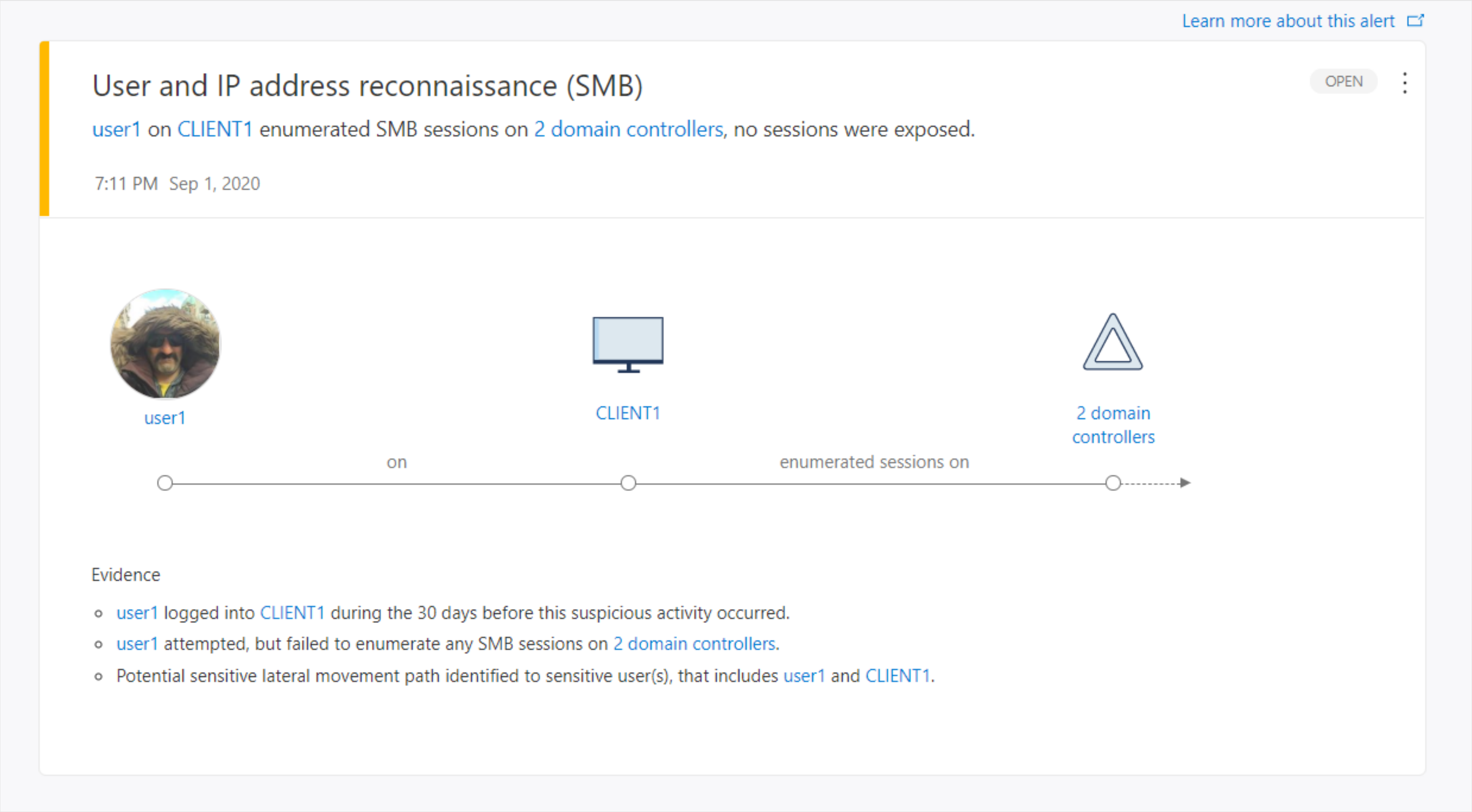
```
Set-NetSessionEnumPermission
```

Restore enumeration for Authenticated Users

```
Restore-NetSessionEnumPermission
```

Detection on domain controllers

- Example of alerts from Microsoft Defender for Identity



Learn more about this alert

User and IP address reconnaissance (SMB)

OPEN

user1 on CLIENT1 enumerated SMB sessions on 2 domain controllers, no sessions were exposed.

7:11 PM Sep 1, 2020

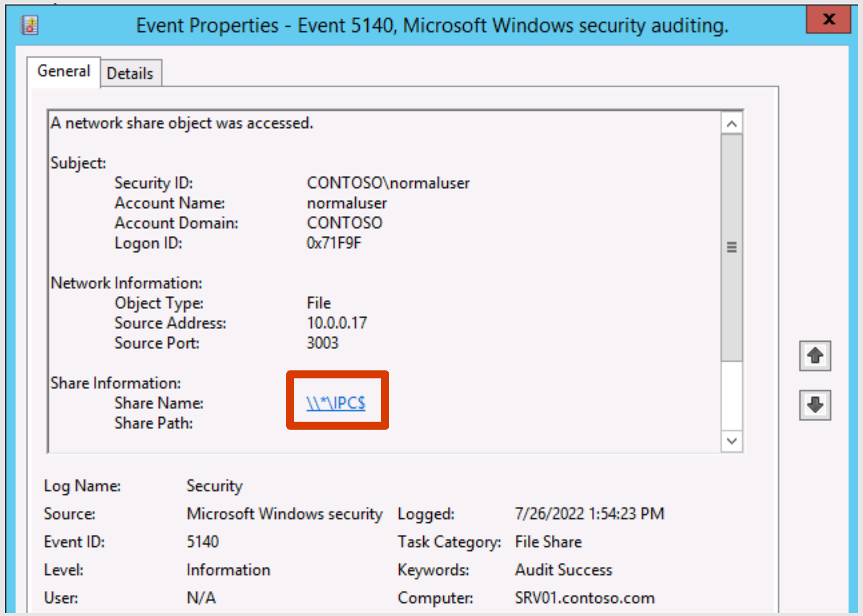
Evidence

- user1 logged into CLIENT1 during the 30 days before this suspicious activity occurred.
- user1 attempted, but failed to enumerate any SMB sessions on 2 domain controllers.
- Potential sensitive lateral movement path identified to sensitive user(s), that includes user1 and CLIENT1.

Adv.

Detection on servers

- Potentially detected in the security event logs if **File Share** and/or **Detailed File Share** audit subcategories are enabled
- Generates events **5140** and/or **5145** for the IPC$ share but those are not specific to SMB enumeration



Event Properties - Event 5140, Microsoft Windows security auditing.
General
Details

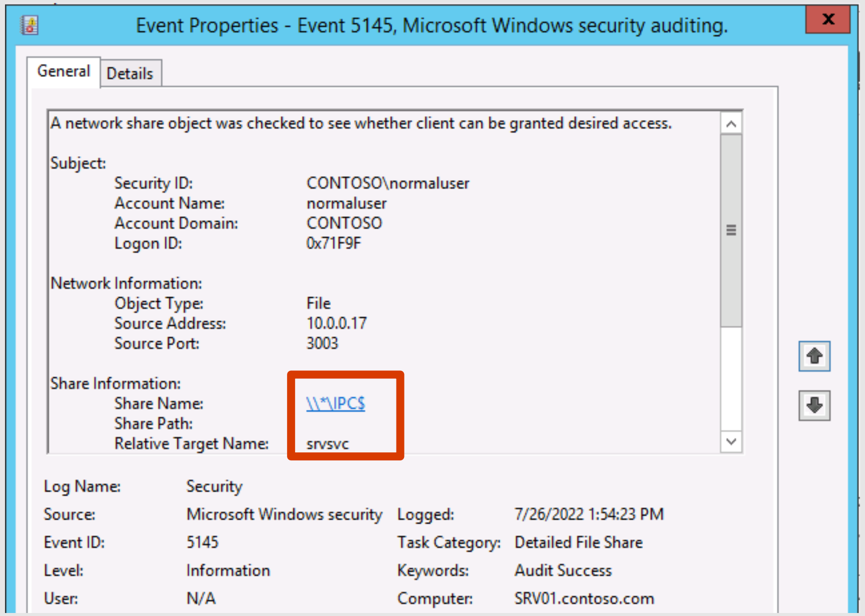
```
A network share object was accessed.

Subject:
        Security ID:            CONTOSO\normaluser
        Account Name:           normaluser
        Account Domain:         CONTOSO
        Logon ID:               0x71F9F

Network Information:
        Object Type:            File
        Source Address:         10.0.0.17
        Source Port:            3003

Share Information:
        Share Name:             \\*\IPC$
        Share Path:
```

```
Log Name:     Security
Source:       Microsoft Windows security    Logged:         7/26/2022 1:54:23 PM
Event ID:     5140                          Task Category:  File Share
Level:        Information                   Keywords:       Audit Success
User:         N/A                           Computer:       SRV01.contoso.com
```



Event Properties - Event 5145, Microsoft Windows security auditing.
General
Details

```
A network share object was checked to see whether client can be granted desired access.

Subject:
        Security ID:            CONTOSO\normaluser
        Account Name:           normaluser
        Account Domain:         CONTOSO
        Logon ID:               0x71F9F

Network Information:
        Object Type:            File
        Source Address:         10.0.0.17
        Source Port:            3003

Share Information:
        Share Name:             \\*\IPC$
        Share Path:
        Relative Target Name:   srvsvc
```

```
Log Name:     Security
Source:       Microsoft Windows security    Logged:         7/26/2022 1:54:23 PM
Event ID:     5145                          Task Category:  Detailed File Share
Level:        Information                   Keywords:       Audit Success
User:         N/A                           Computer:       SRV01.contoso.com
```

SMB enumeration attack summary

Attack's pre-requisites

- A regular account

Protection

- Limit SMB enumeration to local admins on member servers
- Limit SMB enumeration to domain admins on domain controllers

Microsoft

List of abbreviations

LAPS – Local Administrator Password Solution

RSAT – Remote Server Administration Tools