# TG-III PENTESTING

EXAMPLE CORPO

Date: April 9th, 2025

Penetration Testing Findings Report

Business Confidential

## Table of Contents

# Confidentiality Statement

This document is the exclusive property of Example Corpo and TG-III Pentesting (TG3PT). This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent

of both Example Corpo and TG-III Pentesting.

Example Corpo may share this document with auditors under non-disclosure agreements to demonstrate penetration test requirement compliance.

# Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

Time-limited engagements do not allow for a full evaluation of all security controls. TG3PT prioritized the assessment to identify the weakest security controls an attacker would exploit. TG3PT recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

# Contact Information

| Name | Title | Contact Info |
|---|---|---|
| **TG-III Pentesting** | | |
| Navkaran Randhawa | Penetration Tester | randhawanavkaran@gmail.com |
| **Example Corpo** | | |
| Bob Bobson | Chief Information Security Officer | Email: bob@xmplcorp.com |

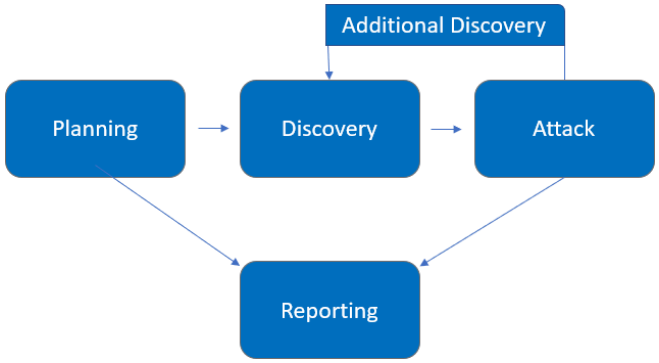
# Assessment Overview

From March 25th, 2023, to April 5th, 2023, Example Corpo engaged TG3PT to evaluate the security posture of its infrastructure compared to current industry best practices that included an active directory penetration test.

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 discovery upon new access.
- Reporting – Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.




# Assessment Components

## Internal Penetration Test

An internal penetration test emulates the role of an attacker from inside the network. An engineer will scan the network to identify potential host vulnerabilities and perform common and advanced internal AD attacks, such as: pass-the hash attack, AS-REP Roasting, Keberoasting attack, Silver Ticket Attack, and Golden Ticket Attack

# Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

| Severity | CVSS V3 Score Range | Definition |
|---|---|---|

| | | |
|---|---|---|
| Critical | 9.0-10.0 | Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately. |
| 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. |
| Moderate | 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 | Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window. |
| Informational | N/A | No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation. |

# Risk Factors

Risk is measured by two factors: Likelihood and Impact:

### Likelihood

Likelihood measures the potential of a vulnerability being exploited. Ratings are given based on the difficulty of the attack, the available tools, attacker skill level, and client environment.

### Impact

Impact measures the potential vulnerability's effect on operations, including confidentiality, integrity, and availability of client systems and/or data, reputational harm, and financial loss.

# Scope

| Assessment | Details |
|---|---|

| | |
|---|---|
| Internal Penetration Test | 172.16.0.0/24 |

## Scope Exclusions

Per client request, TG3PT did not perform any of the following attacks during testing:

- Denial of Service (DoS)
- Phishing/Social Engineering

All other attacks not specified above were permitted by Example Corpo.

## Client Allowances

Example Corpo provided TG3PT the following allowances:

- Internal access to the network via physical workstation within the facility.

# Executive Summary

TG3PT evaluated Example Corpo's internal security posture through penetration testing from March 25th, 2023, to April 5th, 2023. The following sections provide a high-level overview of vulnerabilities discovered, successful and unsuccessful attempts, and strengths and weaknesses.

## Scoping and Time Limitations

Scoping during the engagement did not permit denial of service or social engineering across all testing components.

Time limitations were in place for testing. Internal network penetration testing was permitted for twelve (12) business days.

## Testing Summary

To initiate the assessment, a reverse shell was successfully executed on a domain-joined Windows system, providing internal access. This foothold enabled enumeration and subsequent exploitation of Active Directory misconfigurations and authentication mechanisms.

Initial access was achieved by exploiting a vulnerable user through a malicious Word document containing a macro payload that initiated a reverse shell to the attacker's machine. Upon execution, this granted command-line access to the Windows 10 host, which was leveraged to escalate privileges and extract credentials. The team executed a series of attacks commonly used against corporate Windows domains:

- **Pass-the-Hash attacks** were performed to demonstrate how NTLM hashes could be used for unauthorized authentication without knowing the user's password.
- **AS-REP Roasting** was carried out to target accounts that lacked Kerberos pre-authentication requirements.
- **Kerberoasting** attacks were used to extract service account credentials by requesting service tickets tied to SPNs.
- **Golden Ticket attacks** were carried out by forging a Ticket Granting Ticket (TGT) after compromising the krbtgt account hash, leading to full domain compromise.

The TG3PT team discovered that Active Directory was vulnerable to several critical attack paths. Notably, the ability to leverage Pass-the-Hash and Kerberoasting led to escalated privileges within the domain. Additionally, weak password policies allowed cracked credentials during AS-REP Roasting and Kerberoasting attacks.

The assessment found no evidence of network-level patching vulnerabilities (e.g., MS17-010/EternalBlue) or missing system updates. However, misconfigurations at the domain level created critical risks. For further details, refer to the Technical Findings section.

# Tester Notes and Recommendations

The results of Example Corpo's Active Directory assessment are indicative of a domain environment in early stages of hardening. While system patching was well-maintained, core weaknesses in **authentication**, **ticket management**, and **password policies** introduced significant attack surfaces.

The following recurring weaknesses were noted:

- **Weak or poorly enforced password policies** allowed for successful offline cracking (Kerberoasting, AS-REP Roasting).
- **Service accounts** were configured with SPNs and weak credentials, creating privilege escalation opportunities.
- **Critical ticket-related misconfigurations** (Silver Ticket and Golden Ticket vulnerabilities) exposed the domain to stealthy persistence and lateral movement.

**Recommendations:**

- Implement strong password policies: minimum 16 characters for user accounts and 30+ characters for administrative/service accounts.
- Enforce Kerberos pre-authentication on all domain user accounts.
- Regularly rotate service account passwords and eliminate unnecessary SPN registrations.
- Monitor Active Directory ticket-granting events for anomalies (e.g., multiple TGTs issued to the same user).
- Reset the krbtgt account password twice in succession to invalidate potential Golden Tickets.
- Conduct regular security audits of Active Directory permissions and delegation settings.
- Harden service accounts by minimizing privileges and enforcing non-interactive logins where possible.

On a positive note, Example Corpo's domain controllers and critical infrastructure systems were fully patched against known software vulnerabilities, and initial alerting systems were partially effective at detecting suspicious activity during testing.

Overall, Example Corpo's Active Directory performed as expected for an organization undergoing its first full-scope domain penetration test.
We recommend addressing the issues outlined in this report and conducting annual assessments to track improvements and validate remediation efforts.

---

**Key Strengths and Weaknesses**

**Key Strengths:**

1. Patching and system updates were up to date across the network.
2. Some security alerting mechanisms triggered on suspicious authentication activity.

---

**Key Weaknesses:**

1. Weak password policies allowed successful offline cracking of user and service accounts.
2. Kerberos pre-authentication was not enforced on all domain user accounts (enabling AS-REP Roasting).
3. Service Principal Names (SPNs) were registered without strong password protection, enabling Kerberoasting attacks.
4. Service account hashes were compromised, allowing for Silver Ticket forgery.
5. The krbtgt account hash was not regularly rotated, enabling Golden Ticket creation and full domain compromise.
6. Lack of centralized monitoring of Kerberos TGT/TGS events and anomalies.
7. Incomplete segmentation between user workstations and domain controllers.
8. Minimal auditing of Active Directory permissions and ACLs.

---

By addressing these weaknesses and reinforcing the identified strengths, Example

Corpo can significantly improve its Active Directory security posture and reduce the risk of internal compromise.

# Vulnerability Summary & Report Card

The following tables illustrate the vulnerabilities found by impact and recommended remediations:

**Internal Penetration Test Findings**

| 4 | 1 | 0 | 0 | 0 |
|---|---|---|---|---|
| Critical | High | Moderate | Low | Informational |

| Finding | Severity | Recommendation |
|---|---|---|
| Internal Penetration Test | | |
| INT-001: AS-REP Roasting | Critical | Disable pre-authentication for all users unless required. Enforce strong password policies and implement auditing to detect abnormal Kerberos authentication attempts. |
| INT-002: Kerberoasting | Critical | Use complex, high-entropy passwords for service acco privileges. Monitor Kerberos ticket requests and imple possible. |
| INT-003: Pass-the-Hash Attack | Critical | Enforce credential guard and LSA protection. Limit lat admin access across systems and enabling network-l |
| INT-004: Golden Ticket Attack | Critical | Reset the KRBTGT account password twice to invalid Admin access and monitor ticket generation and usag |

# Findings

## Internal Penetration Test Findings

### Finding INT-001: Pass-the-Hash Attack

| | |
|---|---|
| Description: | Captured NTLM hashes were used to authenticate to other domain systems without needing to crack or know the users' plaintext passwords. This technique allowed unauthorized access to SMB shares and lateral movement within the domain. |
| Risk: | Critical Severity. An attacker can move laterally, access sensitive files, and impersonate users across the domain without detection if network protections (such as SMB signing) are not enforced. |
| System: | Domain-Joined Windows Servers and Workstations |
| Tools Used: | Mimikatz, NetExec (formerly CrackMapExec) |
| References: | https://attack.mitre.org/techniques/T1550/002/ |

Evidence:

- NTLM hashes were extracted from memory using Mimikatz (sekurlsa::logonpasswords).
- NetExec authenticated to systems using the extracted hashes via SMB without needing passwords.

```
meterpreter > kiwi_cmd sekurlsa::logonpasswords


Authentication Id : 0 ; 239716 (00000000:0003a864)
Session           : Interactive from 1
User Name         : Administrator
Domain            : CYBERCORP
Logon Server      : DC01
Logon Time        : 5/5/2025 7:36:32 AM
SID               : S-1-5-21-2705207573-3021489778-1621889878-500
        msv :
         [00000003] Primary
         * Username : Administrator
         * Domain   : CYBERCORP
         * NTLM     : 2b576acbe6bcfda7294d6bd18041b8fe
         * SHA1     : e30d1c18c56c027667d35734660751dc80203354
         * DPAPI    : 46d3e982af1e520569e64d9c14a876c4
        tspkg :
        wdigest :
```

```
┌──(kali㉿kali)-[~]
└─$ netexec smb 192.168.1.165 -u 'Administrator' -H '2b576acbe6bcfda7294d6bd18041b8fe'
 --shares
SMB         192.168.1.165   445    DC01             [*] Windows Server 2019 Standard 17
763 x64 (name:DC01) (domain:cybercorp.com) (signing:True) (SMBv1:True)
SMB         192.168.1.165   445    DC01             [+] cybercorp.com\Administrator:2b5
76acbe6bcfda7294d6bd18041b8fe (Pwn3d!)
SMB         192.168.1.165   445    DC01             [*] Enumerated shares
SMB         192.168.1.165   445    DC01             Share           Permissions     Rem
ark
SMB         192.168.1.165   445    DC01             -----           -----------     ---
SMB         192.168.1.165   445    DC01             ADMIN$          READ,WRITE      Rem
ote Admin
SMB         192.168.1.165   445    DC01             C$              READ,WRITE      Def
ault share
SMB         192.168.1.165   445    DC01             IPC$                            Rem
ote IPC
SMB         192.168.1.165   445    DC01             NETLOGON        READ,WRITE      Log
on server share
SMB         192.168.1.165   445    DC01             SYSVOL          READ,WRITE      Log
on server share
```

Remediation: Enforce strong passwords and enable multi-factor authentication (MFA) across all accounts. Disable NTLM where possible and require SMB signing to prevent token misuse. Regularly rotate privileged credentials and audit authentication logs.

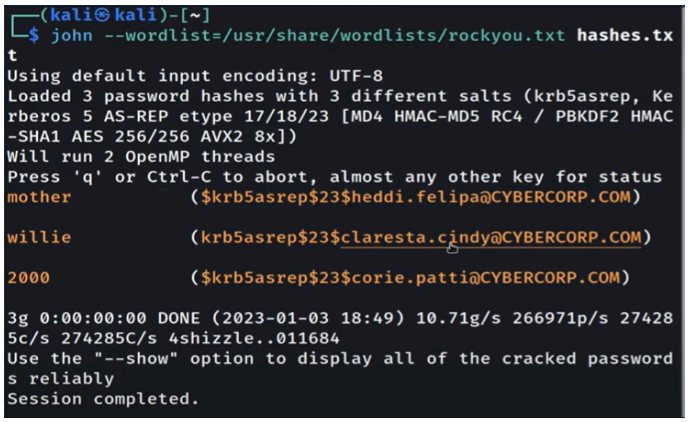
### Finding INT-002: AS-REP Roasting Attack

| | |
|---|---|
| Description : | Exploited domain user accounts that had Kerberos pre-authentication disabled. This allowed the tester to request encrypted authentication responses (AS-REP messages) offline and crack them to retrieve plaintext passwords. |

| | |
|---|---|
| Risk: | High Severity.<br>Offline password cracking poses a major threat without generating noise inside the domain. |
| System: | Active Directory Domain Controller |
| Tools Used: | Impacket GetNPUsers.py, John the Ripper |
| References: | https://attack.mitre.org/techniques/T1558/004/ |

**Evidence:**

- User accounts without Kerberos pre-authentication were enumerated.
- AS-REP encrypted hashes were captured and cracked using John the Ripper.
- AS-REP hashes cracked using John the Ripper with the rockyou.txt wordlist, revealing plaintext credentials for user accounts without pre-authentication




Remediation: Remove the “Do not require Kerberos preauthentication” setting from user accounts. Use long, complex passwords for service accounts and rotate them regularly. Monitor Kerberos pre-authentication failures to detect attacks early.

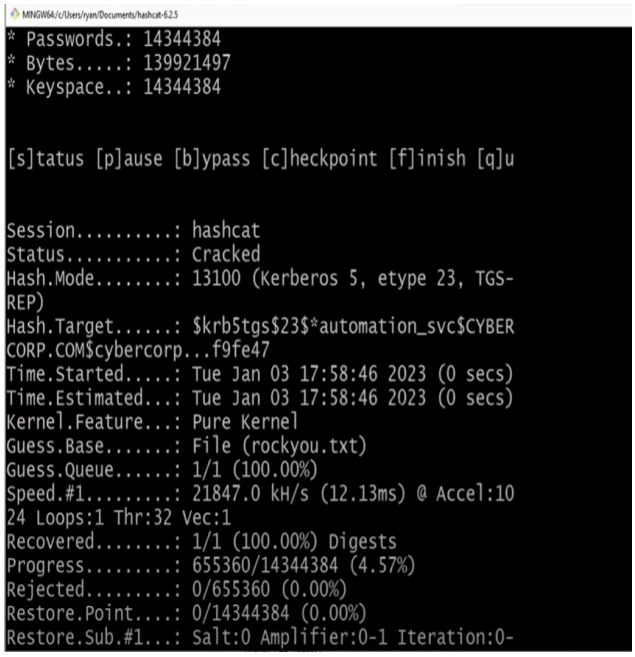
### Finding INT-003: Kerberoasting Attack

| | |
|---|---|
| Description: | |

| | |
|---|---|
| | The penetration tester requested service tickets (TGS) for service accounts and cracked the encrypted Kerberos ticket offline using a wordlist. This allowed the tester to recover the plaintext password for the service account. |
| Risk: | High Severity. Kerberoasting allows attackers to escalate privileges if service accounts use weak passwords. |
| System: | Active Directory Domain Controller |
| Tools Used: | Hashcat, impacket |
| References: | https://attack.mitre.org/techniques/T1558/003/ |

Evidence:

- A TGS ticket hash for the automation_svc account was dumped and cracked using Hashcat.
- Screenshot showing the cracked TGS hash and recovered password using rockyou.txt.



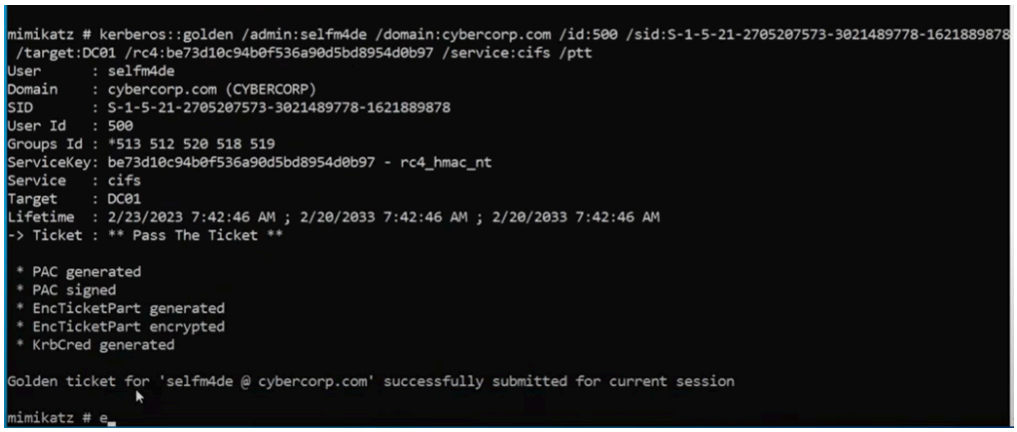

Remediation: Use strong, complex passwords for service accounts and rotate them regularly. Remove unnecessary SPNs and monitor Kerberos ticket activity for signs of abuse.

### Finding INT-004: Golden Ticket Attack

| | |
|---|---|
| Description: | By compromising the krbtgt account's NTLM hash, the penetration tester forged legitimate Ticket Granting Tickets (TGTs), allowing full domain-wide access and persistence. |
| Risk: | Critical Severity. Golden Tickets provide full, nearly undetectable control over the domain environment. |
| System: | Domain Controllers and Domain-Joined Systems |
| Tools Used: | Mimikatz |
| References: | https://attack.mitre.org/techniques/T1558/001/ |

Evidence:

- The krbtgt hash was extracted using Mimikatz.
- Forged TGTs were injected, allowing impersonation of privileged domain users without any login challenge.




Remediation: Reset the KRBTGT password twice to invalidate forged tickets if compromise is detected. Limit Domain Admin use and closely monitor Domain Controller security logs. Enable advanced detection of abnormal ticket activity.