Vulnerability Assessment Report

November 13th, 2023

Defense Lab

Prepared by
Jason Taylor
jason@rufflabs.com

Prepared for
Defense Lab
Alice Smith
administrator@defense.local

Table of Contents

Confidentiality Statement

This report is the property of Defense Lab and Ruff Labs. The report contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both Defense Lab and Ruff Labs.

Defense Lab may share this report with external auditors under non-disclosure agreements to demonstrate penetration testing, and this report may be shared internally with Defense Lab staff as needed.

Disclaimer

This report is a sample report of a fictional virtual lab and does not reflect any actual organization. It serves as an example of what a penetration test report could look like.

This assessment is considered a snapshot in time. The findings and recommendations included reflect the information gathered during the assessment time frame and does not consider any changes made to the environment or systems outside of the testing period.

Time-limited engagements do not allow for a full evaluation of all security controls. This assessment was prioritized to identify the weakest security controls an attacker would exploit. It is recommended to have annual assessments performed, along with regular testing when major changes are made to the environment.

Contact Information

Below are contact details for all parties involved in this assessment.

Name	Title	Contact Details
Defense Lab		
Alice Smith	CEO	administrator@defense.local
Ruff Labs		
Jason Taylor	Penetration Tester	jtaylor@rufflabs.com

Assessment Overview

From March 1st, 2023 to March 3rd, 2023 Defense Lab engaged Ruff Labs to perform an internal vulnerability assessment. The assessment was performed using industry standard testing frameworks including those from NIST and OWASP, along with custom testing guidelines.

Internal Vulnerability Assessment

An internal vulnerability assessment is a comprehensive cybersecurity evaluation conducted within an organization's internal network and systems to identify potential weaknesses and security gaps. Unlike external assessments that focus on the perimeter, internal assessments delve into the organization's internal infrastructure, including servers, workstations, databases, and applications. The assessment involves various techniques such as vulnerability scanning, manual enumeration, and configuration review to uncover vulnerabilities that could be exploited by insiders or attackers who have already gained access to the internal network. By proactively identifying and remediating these vulnerabilities, organizations can strengthen their internal security defenses, protect sensitive data, and enhance their overall resilience against potential insider threats and targeted attacks.

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	CVSSv3 Score Range	Description
Critical	9.0 – 10.0	Severe impact, easily exploitable with widespread damage. Treat as an emergency and apply mitigations immediately.
High	7.0 – 8.9	Significant impact, exploit likely with widespread effects. Take immediate action and apply workarounds if needed.
Medium	4.0 – 6.9	Moderate impact may require user intervention for exploitation. Prioritize and address within a reasonable timeframe.
Low	0.1 – 3.9	Minor impact with limited exploitability. Address when possible and as resources permit.
None/Info	Not Applicable – 0.0	No impact on the system’s security. No immediate action required.

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

The assessment was performed on the following in-scope items:

In Scope Systems	Description
Network	172.25.30.0/24
Websites	web01.defense.local web02.defense.local

Scope Exclusions

The following are explicitly out-of-scope for the assessment:

Out of Scope Systems	Description
SQL Server	sql01.defense.local

- Denial of Service (DoS)

Client Allowances

Defense Lab provided the following allowances for this assessment:

- Kali Linux VM installed within client network.

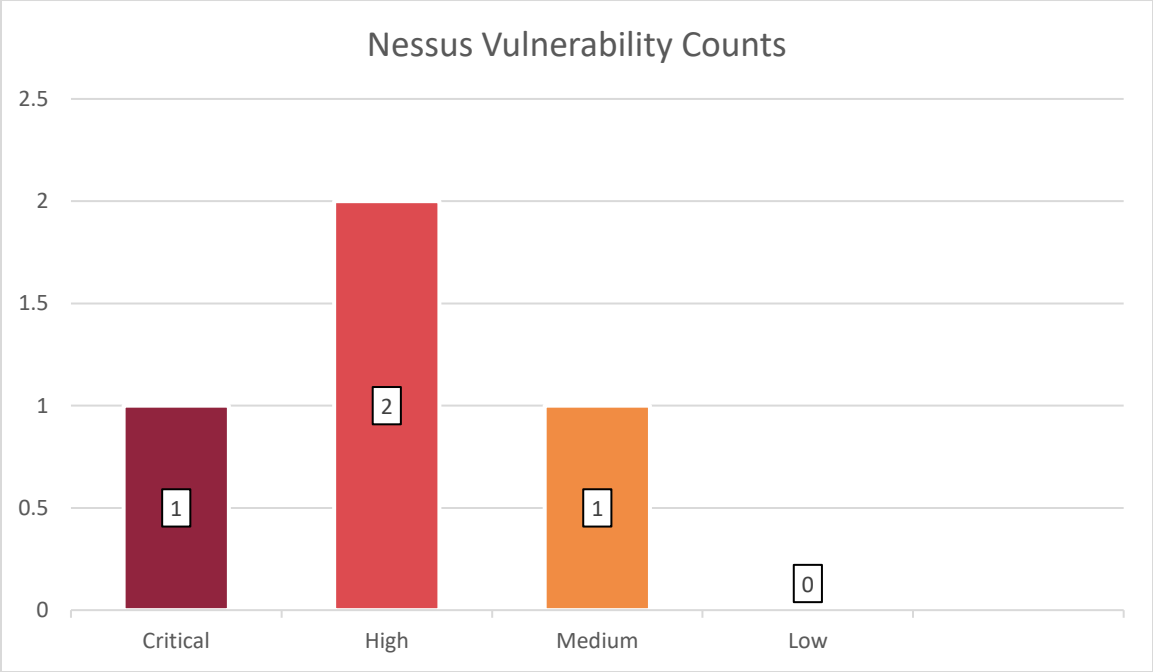
Executive Summary

Ruff Labs performed an internal network penetration test between March 1, 2023 and March 3, 2023 on Defense Lab's virtual lab network.

The internal network penetration test involved an assumed compromise Kali VM that was deployed on the client network and accessible to the tester.

Network recon, enumeration, and vulnerability scans and attacks were attempted from this Kali system in an effort to gain elevated privileges within the defense.local Active Directory domain network.

During the engagement a total of 4 findings were identified that require attention by Defense Lab.



Scoping and Time Limitations

The scope of this assessment involved direct VM access to the Vagrant lab network. Denial of Service and Social Engineering were not allowed during this assessment.

The assessment was allowed to take place over 48 hours.

Recommendations

Multiple software and operating system updates were found to be missing, including some that were over three months old since release. It is recommended that Defense Lab implement a patching program that includes processes and procedures for installing operating system and third-party software updates in a timely manner.

The patching process should include set guidelines on patch age. Best practice is to have critical and high patches installed within 30 days of release, mediums within 60 days.

Typical patching programs involve a staged approach, deploying patches to an initial pilot for a few days or a week before deploying to the rest of the environment in two or more stages. The goal would be to have all patches installed within a 30-day window.

In addition to the missing patches, there were multiple TLS related configuration issues that need to be addressed. Many of these involve adjusting ciphers and algorithms and disabling unsupported protocols.

Strengths and Weaknesses

During the assessment, the following key strengths were identified:

- Responder usage was identified, and alerts generated by Defense Lab analysts.

The following key weaknesses were identified:

- Poor password policy and enforcement resulted in multiple issues with passwords.
- Best practice domain security features like SMB Signing and NLA were not enabled.

Summary and Report Card

The following table summarizes all vulnerabilities that were identified by this assessment, along with recommendations to remediate the identified vulnerabilities.

Critical	High	Medium	Low	None/Info
1	2	1	0	0

Finding	Severity	Recommendation
001: Kerberoastable Accounts	Critical	Implement PAM solution to manage passwords.
002: Insufficient Password Policy	High	Implement improved password policies.
003: Local Admin Password Re-Use	High	Deploy LAPS or PAM to ensure unique passwords.
004: SMB Signing Not Required	Medium	Require SMB signing for all servers and workstations.

Findings

Finding 001: Kerberoastable account [Critical]

Description

The sqlservice account is susceptible to kerberoasting attacks. These attacks involve requesting a ticket from Active Directory which will include the password hash of the account. This hash can then be taken offline, and the attacker can attempt to crack this password.

Risk

Likelihood: Medium – To take advantage of a kerberoastable account the attacker needs to obtain the hashes and then take them offline to crack. This can be mitigated with very secure and long passwords.

Impact: High – Exploiting this vulnerability could lead to privileged access to the domain.

Systems

sqlservice@defense.local

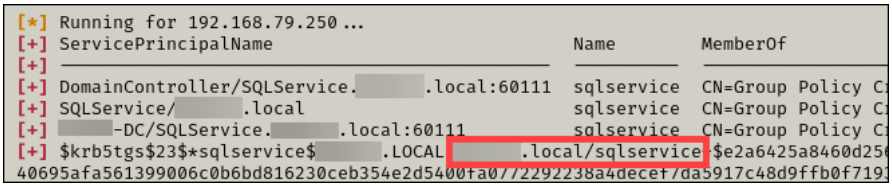
Tools Used

Metasploit

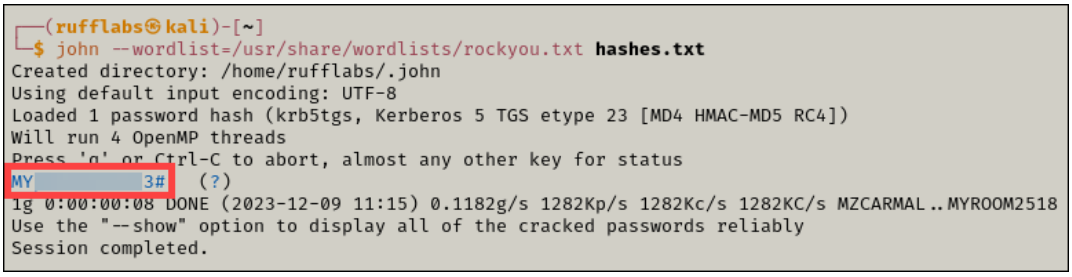
References

https://www.crowdstrike.com/cybersecurity-101/kerberoasting/

Evidence



Obtaining the password hash of the sqlservice account via kerberoast attack.



Password for sqlservice account was weak and able to be cracked.

Recommendation

Ensure service accounts have very long (25+ character), complex, generated passwords. This will minimize the risk of a password hash being successfully cracked.

Finding 002: Insufficient Password Policy [High]

Description

The Active Directory password policy does not implement industry best practices.

Risk

Likelihood: High - Weak passwords like “Winter2023!” are often used when sufficient password policies are not in place.

Impact: High – Weak password policy allows for weak and insecure passwords to be set, as well as re-using short easily guessed passwords.

Systems

defense.local

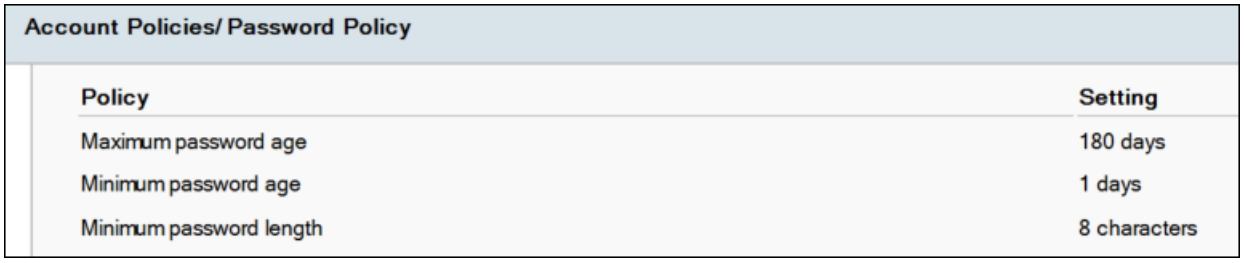
Tools Used

gpresults, NetExec

References

https://www.microsoft.com/en-us/research/wp-content/uploads/2016/06/Microsoft_Password_Guidance-1.pdf

Evidence



Account Policies/ Password Policy

Policy	Setting
Maximum password age	180 days
Minimum password age	1 days
Minimum password length	8 characters

Default Domain Policy’s Password Policy.

Recommendation

Update the domain password policy, recommended settings:
Require complexity: Yes
Maximum age: 90
Minimum length: 12

Finding 003: Local Admin password re-use [High]

Description

Local administrator accounts have the same password set. This can allow an attacker that gains access to one PC with administrator privileges to pivot to all other systems that share the same local password.

Risk

Likelihood: High – Anyone with local administrator on a workstation can obtain the password for the local administrator, which could lead to administrator access on other systems with the same password.

Impact: High – This could lead to compromise of multiple systems, where an attacker may have only initially had access to one system.

Systems

192.168.79.145, 192.168.79.220

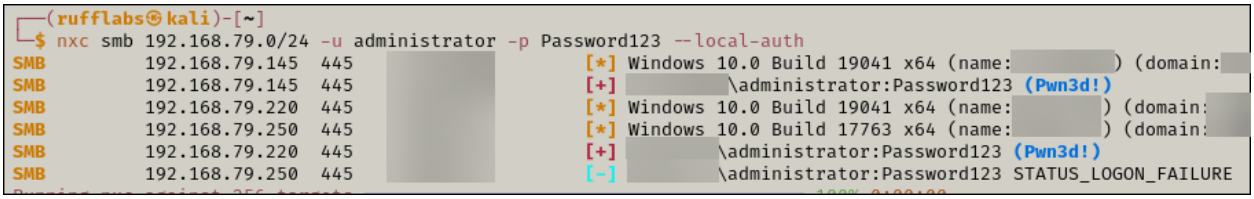
Tools Used

NetExec

References

https://learn.microsoft.com/en-us/windows-server/identity/laps/laps-management-policy-settings

Evidence



Testing local administrator password for re-use across the domain.

Recommendation

Use Microsoft Local Administrator Password Solution (LAPS) to manage and rotate all local administrator passwords via GPO. This ensures every PC has a unique password for the local administrator stored in Active Directory and accessible to Domain Administrators.

Finding 004: SMB Signing not required [Medium]

Description

SMB signing is not required, this allows attackers to employ machine-in-the-middle attacks to relay captured hashes to these hosts and authenticate as a user without knowing the associated password.

Risk

Likelihood: Medium – Attackers that gain access to machine-in-the-middle an authenticated user could pivot to other systems without SMB signing as the user.

Impact: Medium – Attacker could gain the same privileges as the user that they gain the password hash for.

Systems

192.168.79.145, 192.168.79.220, 192.168.79.250

Tools Used

nmap

References

https://www.beyondsecurity.com/resources/vulnerabilities/smb-signing-disabled

Evidence

```
┌──(rufflabs㉿kali)-[~]
└─$ nmap --script smb2-security-mode 192.168.79.0/24 -p445 -sCV
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-09 14:52 CST
Nmap scan report for 192.168.79.2
Host is up (0.0014s latency).

PORT    STATE  SERVICE      VERSION
445/tcp closed microsoft-ds

Nmap scan report for 192.168.79.145
Host is up (0.00057s latency).

PORT    STATE SERVICE       VERSION
445/tcp open  microsoft-ds?

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
```

SMB signing is not required.

Recommendation

Use Group Policy to require SMB signing.