

[Cover Page here]

NOTES

- Use numbered sub-headings, more professional, add some logs/output in main text (but most will be in appendix)
- Use appendix to link various logs/in-depth files to a Github Repo?

Contents

Executive Summary	1
Summary of Findings (Table format?)	1
Approach	1
Scope	1
Introduction	1
Background	1
Objectives	2
Methodology	2
Findings and Analysis	2
Phase 1: Intelligence Gathering	2
Nmap	2
Ldapsearch	4
ADRecon	7
Phase 2: Threat Modelling	10
Identified Assets	10
Threat Communities	10
Vulnerability Exploitation	11
Risk Rating of Threats	11
Phase 3: Vulnerability Analysis	12
Nessus	12
PingCastle	14
MSF	15
Phase 4: Exploitation	15
Phase 5: Post-Exploitation	16
Recommendations	16
Conclusion	16

Appendices	17
Appendix I: Full Reports	Error! Bookmark not defined.
Nmap	17
Nessus	17
PingCastle – GitHub link would be better	17
Appendix II: Tools & Methods Used	17

Executive Summary

This report presents the findings from a comprehensive penetration test and vulnerability assessment conducted on the "vulnAD.lab" domain. The purpose of this assessment was to identify and exploit vulnerabilities within the network and systems, with a focus on Active Directory security, focusing on well-known vulnerabilities and misconfigurations. Key findings include critical vulnerabilities and misconfigurations that allowed for unauthorised access to the domain and its assets, privilege escalation, potential data exfiltration and

--- various sub-headings here or under Scope: Hostnames & IP addresses; Summary of Findings (table), Summary of Recommendations,

Summary of Findings (Table format?)

Approach

This assessment was conducted under black-box conditions, simulating an attempt by an external attacker without initial access or previous knowledge. A wide range of tools, scripts and techniques were used during the various stages of the assessment to enumerate, assess and exploit the security of the network/domain.

--- Access was on the same subnet

Scope

The assessment targeted all systems within the "vulnAD.lab" domain, with particular emphasis on the Active Directory infrastructure and domain configurations to determine how vulnerable the domain is.

Introduction

Background

The vulnAD.lab domain represents a typical small corporate network with a mix of user and administrative accounts, critical servers and service accounts and shared

resources. This domain was assessed to identify security weaknesses that could be exploited in a real-world attack scenario.

Objectives

- To identify vulnerabilities and misconfigurations within the "vulnAD.lab" domain environment.
- To exploit identified vulnerabilities to assess the potential impact of identified vulnerabilities in a poorly configured AD Domain .
- To provide mitigation recommendations for identified vulnerabilities.

Methodology

The Penetration Testing Execution Standard (PTES) was followed, consisting of seven phases: Pre-engagement Interactions, Intelligence Gathering, Threat Modelling, Vulnerability Analysis, Exploitation, Post-Exploitation, and Reporting.

---- what each phase details

Findings and Analysis

Phase 1: Intelligence Gathering

During the Intelligence Gathering phase, various tools were used to map out the network and identify potential attack/entry points into the targeted domain. By identifying active hosts, services and configurations of the network, the info obtained in this stage regarding the configuration of the domain and its underlying structure will be quite beneficial in later stages of the assessment.

Nmap

Nmap, a reputable network scanning tool, was deployed on the attacking system (Kali) to conduct a comprehensive scan on the domain controller (DC) of the vulnAD.lab domain. An initial scan of the network identified in the scope showed the IP address "192.168.56.2" with several Windows Server related ports open, which prompted a comprehensive scan on the suspected host to determine if it was indeed the Domain Controller.

The following Nmap command was used to provide detailed information regarding the open ports/services on the DC:

```
nmap -A -p- -oA /home/kali/nmap_vulnAD.log 192.168.56.2
```

Figure 1 shows an Nmap scan that identifies several key open ports and services on the DC, providing a list of services to target in search for vulnerabilities and misconfigurations.

```
└─$ sudo nmap -A -p- -oA ~/nmap_vulnAD.log 192.168.56.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-26 14:37 GMT
Stats: 0:00:25 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 10.11% done; ETC: 14:40 (0:02:49 remaining)
Stats: 0:02:44 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 70.00% done; ETC: 14:40 (0:00:19 remaining)
Nmap scan report for 192.168.56.2
Host is up (0.00054s latency).
Not shown: 65515 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: 2024-03-26 14:39:13Z)
135/tcp   open  msrpc                  Microsoft Windows RPC
139/tcp   open  netbios-ssn           Microsoft Windows netbios-ssn
389/tcp   open  ldap                   Microsoft Windows Active Directory LDAP (Domain: vulnAD.lab0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?          Microsoft Windows SMB 1.0
464/tcp   open  kpasswd5?              Microsoft Windows RPC over HTTP 1.0
593/tcp   open  ncacn_http             Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap                   Microsoft Windows Active Directory LDAP (Domain: vulnAD.lab0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
5985/tcp  open  http                   Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
9389/tcp  open  mc-nmf                 .NET Message Framing
49666/tcp open  msrpc                  Microsoft Windows RPC
49667/tcp open  msrpc                  Microsoft Windows RPC
49669/tcp open  ncacn_http             Microsoft Windows RPC over HTTP 1.0
49670/tcp open  msrpc                  Microsoft Windows RPC
49672/tcp open  msrpc                  Microsoft Windows RPC
49685/tcp open  msrpc                  Microsoft Windows RPC
49758/tcp open  msrpc                  Microsoft Windows RPC
MAC Address: 08:00:27:2F:74:C5 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2019 (97%)
Aggressive OS guesses: Microsoft Windows Server 2019 (97%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: Host: DC1; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Figure 1: Win Server (DC) Nmap Scan Results

The Nmap scan shown above highlights several critical Windows Server/Active Directory related ports (all open), such as Kerberos (port 88/tcp), LDAP(port 389/tcp) and SMB (port 445/tcp). The open ports present a prime list of services to target for vulnerability analysis and exploitation. The aggressive scan listed Windows Server 2019 as the suspected operating system and provides the hostname of the server – “DC1”.

The info gathered from Nmap’s recon scan on the DC highlights several potential services (ports) to attempt unauthorised access/enumeration of the target domain. The lack of filtered ports also suggest services such as Kerberos, LDAP and SMB may not be secured with encryption and whilst the usual port for LDAPS (636/tcp) is listed,

further investigation is required to determine if this service has been configured correctly as the service for this port is listed as “tcpwrapped”.

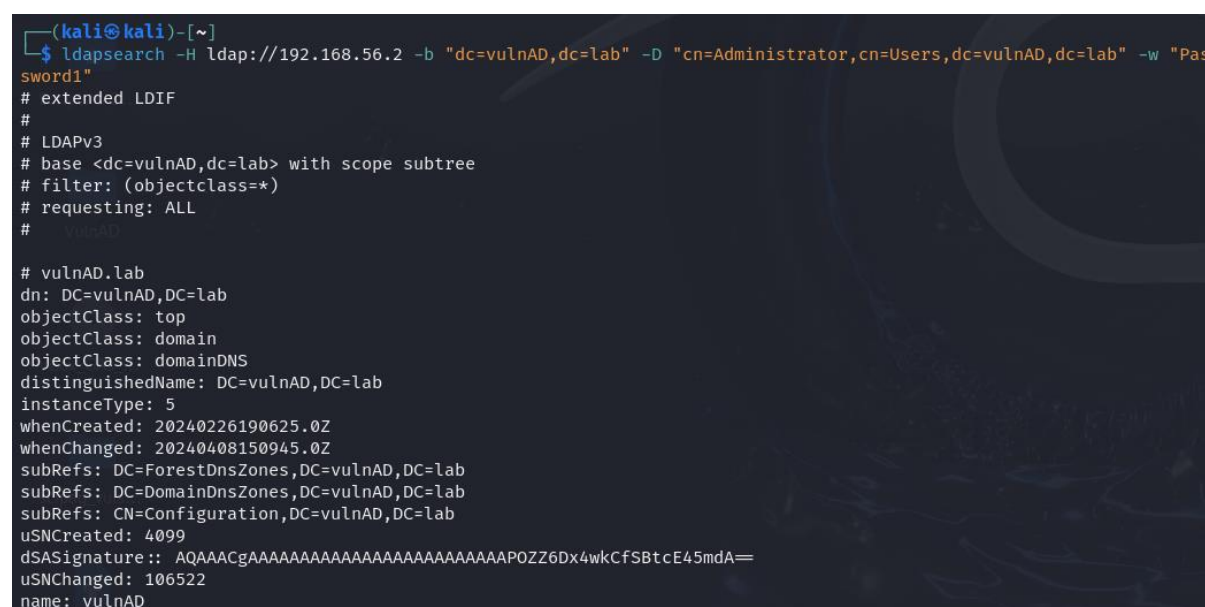
ldapsearch

This section details the process of enumerating the target’s AD Domain using the [ldapsearch](#) tool.

Anonymous LDAP querying was tested initially to determine if anonymous (non-authenticated) users could query info from the domain however, it seems the domain was configured to require authentication. Following this, a simple bind approach was tested using the credentials of the provided Domain Admin account (Administrator), which allowed for unrestricted querying and extraction of all AD objects and attributes.

Enumeration of Root Domain Forest

The following command was used for enumerating all objects in the root domain, including the “Users” OU and the “Computers” OU.



```
(kali㉿kali)-[~]
$ ldapsearch -H ldap://192.168.56.2 -b "dc=vulnAD,dc=lab" -D "cn=Administrator,cn=Users,dc=vulnAD,dc=lab" -w "Password1"
# extended LDIF
#
# LDAPv3
# base <dc=vulnAD,dc=lab> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
# vulnAD.lab
dn: DC=vulnAD,DC=lab
objectClass: top
objectClass: domain
objectClass: domainDNS
distinguishedName: DC=vulnAD,DC=lab
instanceType: 5
whenCreated: 20240226190625.0Z
whenChanged: 20240408150945.0Z
subRefs: DC=ForestDnsZones,DC=vulnAD,DC=lab
subRefs: DC=DomainDnsZones,DC=vulnAD,DC=lab
subRefs: CN=Configuration,DC=vulnAD,DC=lab
uSNCreated: 4099
dSASignature:: AQAACgAAAAAAAAAAAAAAAAAAAAPOZZ6Dx4wkCfSBtcE45mdA==
uSNChanged: 106522
name: vulnAD
```

Figure 2: Enumerating all objects in the domain

All AD objects were retrieved, including but not limited to user objects, groups (security and distribution groups) and the “System” container.

Enumerating all Users

One of the primary objectives of the Intel Gathering Phase, was to obtain a list of domain users. In this case, a list of all domain users was obtained. The ldapsearch command used to obtain the list of users was:

```
ldapsearch -x -H ldap://192.168.56.2 -D
"cn=Administrator,cn=Users,dc=vulnAD,dc=lab" -w "Password1" -b "dc=vulnAD,dc=lab"
"(objectClass=user)"
```

This command retrieved a list of all user objects in the “Users” OU container, revealing usernames, group memberships and various other attributes such as ‘primaryGroupID’ and the full name of all users.

```
# Guest, Users, vulnAD.lab
dn: CN=Guest,CN=Users,DC=vulnAD,DC=lab
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: Guest
description: Built-in account for guest access to the computer/domain
distinguishedName: CN=Guest,CN=Users,DC=vulnAD,DC=lab
instanceType: 4
whenCreated: 20240226190638.0Z
whenChanged: 20240226190638.0Z
uSNCreated: 8197
memberOf: CN=Guests,CN=Builtin,DC=vulnAD,DC=lab
uSNChanged: 8197
name: Guest
objectGUID:: mtD8RNY/jEGXA3AZJ6PjdW==
userAccountControl: 66082
badPwdCount: 0
codePage: 0
countryCode: 0
badPasswordTime: 0
lastLogoff: 0
lastLogon: 0
pwdLastSet: 0
primaryGroupID: 514
objectSid:: AQUAAAAAAAAUVAAGvejxdmWVG8s6BLK9QEAAA=
accountExpires: 9223372036854775807
logonCount: 0
sAMAccountName: Guest
sAMAccountType: 805306368
objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=vulnAD,DC=lab
isCriticalSystemObject: TRUE
```

Figure 3: Enumeration of all domain users

Enumeration of Domain Computers

The next step was to obtain the computers that had domain trust with the target.

```
ldapsearch -x -H ldap://192.168.56.2 -D
"cn=Administrator,cn=Users,dc=vulnAD,dc=lab" -w "Password1" -b "dc=vulnAD,dc=lab"
"(objectClass=computer)"
```

This ldap query returned details regarding every computer object in the domain, displaying attributes such as lastLogon, operating system and the dn.


```
(kali@kali) [~/Desktop/VulnAD/Pen-Testing/IntelGathering]
$ ldapsearch -x -H ldap://192.168.56.2 -D "cn=Administrator,cn=Users,dc=vulnAD,dc=lab" -w "Password1" -b "dc=vulnAD,dc=lab" "(objectClass=computer)"
# extended LDIF
#
# LDAPv3
# base <dc=vulnAD,dc=lab> with scope subtree
# filter: (objectClass=computer)
# requesting: ALL
#
# DC1, Domain Controllers, vulnAD.lab
dn: CN=DC1,OU=Domain Controllers,DC=vulnAD,DC=lab
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
objectClass: computer
cn: DC1
distinguishedName: CN=DC1,OU=Domain Controllers,DC=vulnAD,DC=lab
instanceType: 4
whenCreated: 20240226190718.0Z
whenChanged: 20240325151441.0Z
uSNCreated: 12293
uSNChanged: 36925
name: DC1
objectGUID:: wxGsBySu9EiYdNDgdJJBYg==
userAccountControl: 532480
badPwdCount: 0
codePage: 0
countryCode: 0
badPasswordTime: 0
lastLogoff: 0
lastLogon: 133560355747508807
localPolicyFlags: 0
pwdLastSet: 133534480610467933
primaryGroupID: 516
objectSid:: AQuAAAAAAAAUAAAAgvejxdmrvG8s6BLK6AMAAA=
accountExpires: 9223372036854775807
logonCount: 80
sAMAccountName: DC1$
sAMAccountType: 805306369
operatingSystem: Windows Server 2019 Datacenter Evaluation
```

Figure 4: Displaying all computers linked to the domain

Included in this search, was one of the key workstations used by several users – “WIN10-HOST”.

Users with Non-Expiring Passwords

A search was created to identify user objects with a specific flag set in the ‘userAccountControl’ attribute.

```
ldapsearch -x -H ldap://192.168.56.2 -D
"cn=Administrator,cn=Users,dc=vulnAD,dc=lab" -w "Password1" -b "dc=vulnAD,dc=lab"
"(&(objectClass=user)(userAccountControl:1.2.840.113556.1.4.803:=65536))"
```

This LDAP search identified multiple User accounts, including two service accounts, configured to have their passwords never expire. Two of these users had Admin privileges. This configuration for these accounts present a significant risk as they allow potentially compromised credentials to remain valid – this is a poor configuration.

Identified Accounts

1. Administrator Account – the built-in Administrator account, which is a member of two high-privilege security groups – Domain Admins and Enterprise Admins.
2. Guest Account – a built-in account for guest access – this is typically disabled however further investigation revealed this account is enabled.

3. Test User – appears to be a custom user account, part of the Domain Admins and Administrators groups, another high-privileged account.
4. Service Accounts – two service accounts 'svc_Exchange' and 'svc_SQLServer' are set to "Never expire" – this is poor practise and opens up these critical operational services to credential related attacks.

[add explanation/security impact here]

ADRecon

[ADRecon](#) is an automated tool that gathers info regarding an AD Environment. It can provide a view into the configuration of an AD Domain to determine how the domain has been configured. ADRecon obtains info relating to, but not limited to: Domain Forest structure, Password Policy, Domain Controllers, Users, ACLs and Privileged Accounts.

Findings

Reviewing the reports generated by ADRecon has identified several misconfigurations and security flaws within the target AD environment. These findings highlight areas of concern, where attackers could take advantage of misconfigurations and security oversights to compromise the domain.

----- fix the structure to include "Recommendations" or mitigation heading, maybe **table format??** Also link each .html file to appendix or github repo

1. **Mismanagement of Privileged Accounts:** The file 'GroupMembers.html' revealed the Administrator account is activated, as a group member of high-privilege groups such as Domain Admins and Enterprise Admins. It is considered good practise to rename or disable the built-in Administrator account due to the significant security risk it poses – attackers often target this account. The built-in admin account can not be locked out, which makes it a prime target for brute-force attacks in exploitation stages.
2. **Poor Password Policy:** The 'DefaultPasswordPolicies.html' report reveals several critical misconfigurations and a lack of best security practise implementation. The minimum password length is set to 4 characters, significantly below the industry best practices, which is generally a minimum of

8 characters. The acceptance of lower character passwords makes user and service passwords susceptible to brute-force attacks, credential stuffing and other password attacks.

3. Password Complexity Requirements Disabled – DefaultPasswords.html:

Not forcing password complexity provides users the option to assign a cryptographically weak password. Without forced complexity requirements, passwords can be guessable without any tools and makes users and service accounts particularly vulnerable to dictionary attacks.

4. Account Lockout Threshold - DefaultPasswordPolicies.html: This option is not enabled (set to 0 attempts). This policy is effectively disabled – accounts are not locked out after consecutive failed login attempts. This is a serious concern, the recommendation is to enable lockout of accounts with several consecutive failed login attempts, typically around 10 consecutive failed logon attempts should warrant an account lockout. The lockout duration option should also be adjusted accordingly.

5. Privileged Access Management (PAM) Disabled –

DomainControllers.html: PAM should be enabled as a mitigation for credential theft and general improved security. Real-time PAM solutions cover several areas of best security practise to ensure privileged accounts have an additional layer of security in the event of compromised access. Obtained from the 'Forest.html' report.

6. Poor DACLs - DACLs.html: Included in the 'DACLs.html' report, there are several entries that have "Pre-Windows 2000 Compatible Access" enabled, allowing read access to various objects in the domain. Standard domain users have access like "Mona Aliza" have read access to the root domain structure and "All" objects in the domain. Additionally, unauthenticated users (Anonymous Logon) have read access to several domain objects. There are excessive privileges applied to certain users and group memberships.

7. Critical Misconfiguration – Misconfiguration of DC Sync Rights: The “DS-Replication-Get-Changes-All” right is granted to the user ‘cheslie.alexia’. This is a high privilege right that enables an account to replicate the domain. The use of this replication right can be a lucrative target for an attacker, as it provides read and write access to all objects in AD, including the hashes of system and user accounts. Enabling AD Replication introduces a critical vulnerability known as DCSshadow which an attacker can exploit to escalate privileges and create or modify AD objects. With the lack of network monitoring and logging controls in place, it’s entirely possible an attacker exploiting this vulnerability could evade detection during the post-exploitation and data exfiltration phases.

8. Insecure LDAP Configuration – DomainControllers.html: Analysis indicates the current domain utilizes LDAP without SSL/TLS, transmitting data in clear text. This vulnerability allows attackers to potentially intercept and modify traffic between clients and domain controllers, leading to credential theft or session hijacking.

Recommendations: Upgrade to LDAP over SSL/TLS (LDAPS) to ensure all communications between LDAP clients and servers are encrypted. Implement proper certificate management practices to support LDAPS effectively.

9. Unrestricted Kerberos Ticket Lifetimes – GroupPolicies.html: The domain is configured to allow excessively long Kerberos ticket lifetimes, potentially increasing the window of opportunity for attackers to exploit valid tickets for lateral movement or privilege escalation.

Recommendations: Adjust Kerberos ticket policies to reduce ticket lifetimes and renewal times. This limits the usable lifespan of compromised tickets, reducing the risk of long-term persistence by attackers within the domain.

General Recommendations

Phase 2: Threat Modelling

This phase involves identifying the most valuable assets of the domain, and evaluating the threats that could potentially compromise domain assets. By analysing various attack vectors and the risks associated with existing misconfigurations and vulnerabilities, several critical threats were identified.

Identified Assets

1. The Domain Controller (DC) was identified as a critical asset due to its role in managing security policies and access control within the domain.
2. Service accounts with elevated privileges are crucial in the daily operations of the domain.
3. User credentials and high-privileged groups are high-value targets for attackers aiming to escalate privileges or gain access to confidential info.
4. Servers such as the “EXC-SERVER” and “SQL-SERVER1” are key infrastructure components of organisational environment ensuring core applications and services. “EXC-SERVER” appears to be a dedicated Exchange mail server, whilst “SQL-SERVER1” likely hosts database services for the organisation.
5. Data/File Stores storing sensitive info – customer data, financial records and confidential documents are almost exclusively stored on file/network stores.

Threat Communities

Considering both internal and external threat actors, the following threats were identified:

- 1. Internal Threats:** Internal threat actors can include employees, associate/contractors and other individuals with existing legitimate access to the AD Domain or its assets/infrastructure. Employees can often misuse their privileges or bypass security controls, which can lead to data breaches.
- 2. External Threats:** External attackers consist of cybercriminals and individuals/groups with malicious intentions who aim to employ a range of method: human vulnerabilities (phishing, social engineering); network vulnerabilities (domain misconfiguration and lack of controls) or OS

vulnerabilities. Competitors, hacktivists, nation-sponsored threat actors and Advanced Persistent Threat (APT) groups contribute to a significant number of attacks on organisations and present a serious threat to security and privacy of organisational assets.

Vulnerability Exploitation

- The poor password policy retrieved by ADRecon exposes users and key service accounts to brute-force and credential attacks. Attackers have unlimited opportunity to crack passwords without enabling lockout for accounts.
- Excessive privileges and a poor implementation of access controls may allow attackers to escalate privileges and employ lateral movement to gain access to other assets.
- The improper configuration of LDAPS (LDAP over SSL) and misconfigurations in the Kerberos authentication policies makes user and service accounts vulnerable to Kerberoasting, credential attacks and eavesdropping of LDAP traffic. Attackers could exploit vulnerabilities in the configuration of these policies to intercept and crack credentials, which can act as a gateway to gaining initial access to the domain.

Risk Rating of Threats

Threat	Likelihood	Impact	Overall Risk Rating	Recommendations
Brute-force attacks due to weak password policies	High	High	Critical	Enforce strong password policies and account lockout settings
Privilege escalation due to excessive user rights	Medium	High	High	Implement the principle of least privilege, PAM solutions and the use of “zero trust”

Kerberoasting exploiting Kerberos misconfiguration	High	Medium	High	Enable AES encryption for Kerberos and enable auditing/monitoring for abnormal authentication requests
Credential interception due to unencrypted LDAP	High	High	Critical	Implement LDAPS and disable LDAP unsecured
Internal threats from employees misusing access	Medium	High	High	Enhance monitoring of user activities and enforce strict access controls
External threats from cybercriminals and APTs	High	High	Critical	-----
Data breaches due to poor access controls	High	High	Critical	Restrict access to sensitive data using PAM and proper access controls

Phase 3: Vulnerability Analysis

A detailed view of the security posture of the target domain has been created, using multiple analysis tools. This section encompasses findings from Nessus, PingCastle and Metasploit Framework modules to identify, prioritise and analyse vulnerabilities threat actors may use to compromise the security of the domain.

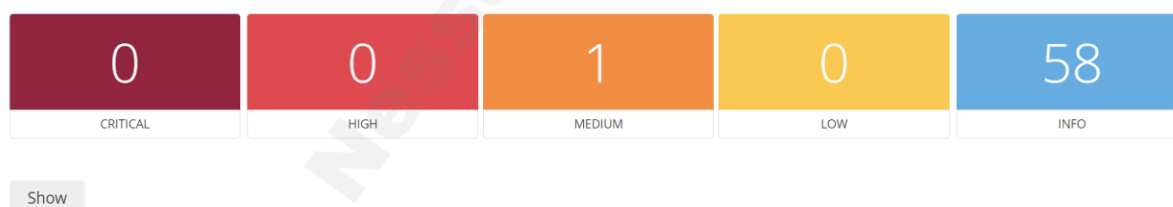
----- mention here or sub-chapters how the full reports can be found in the Appendix.

Nessus

The Nessus basic network scan covered two hosts – the domain controller “dc1.vulnAD.lab” (192.168.56.2) and the Windows 10 workstation “WIN10-HOST” connected to the domain. This comprehensive scan provides valuable insights into the security stance of the domain, specifically the network protocols and services running on the two hosts.

Figure 5 illustrates an alarming overview of the vulnerability analysis conducted by Nessus on the active hosts on the vulnAD.lab network. The scan identified a total of 101 vulnerabilities, divided into different severity categories. 45 vulnerabilities were classified as critical. 48 vulnerabilities were categorised as high severity and 7 medium severity vulnerabilities were identified.

192.168.56.10



dc1.vulnAD.lab



Figure 5: Nessus - Summary of Vulnerabilities found

A closer look at the vulnerabilities identified in the DC reveals a common occurrence – almost all the vulnerabilities are related to the lack of patches applied to the Windows Server. The majority of the flagged vulnerabilities can be linked to outdated software (Adobe Flash, NET Framework for instance) and missing security updates.

Security updates have been neglected, leaving the domain exposed to publicly known vulnerabilities that are several years old. Each unpatched vulnerability presents a potential entry point for attackers to infiltrate the network. A single security update can often include fixes to multiple vulnerabilities; therefore, the true number of exploitable vulnerabilities is unknown.

Severity	CVSS v3.0	VPR Score	Plugin	Name
CRITICAL	9.9	8.9	129717	KB4519338: Windows 10 Version 1809 and Windows Server 2019 October 2019 Security Update
CRITICAL	9.9	9.8	130901	KB4523205: Windows 10 Version 1809 and Windows Server 2019 November 2019 Security Update
CRITICAL	9.9	9.6	136501	KB4551853: Windows 10 Version 1809 and Windows Server 2019 May 2020 Security Update
CRITICAL	9.9	9.2	149382	KB5003171: Windows 10 version 1809 / Windows Server 2019 Security Update (May 2021)
CRITICAL	9.9	9.0	151588	KB5004244: Windows 10 version 1809 / Windows Server 2019 Security Update (July 2021)
CRITICAL	9.9	9.5	152435	KB5005030: Windows 10 Version 1809 and Windows Server 2019 Security Update (August 2021)

Figure 6: Security Updates from October 2019 onwards have not been installed

Installing all Windows updates (inc. security updates) would significantly improve the domain's security posture, in a simplified manner. The exception to the vulnerabilities identified on the Windows Server is the enabled NTLMv1 – an insecure, weak encryption protocol for storing user credentials. As an outdated protocol, NTLMv1 is vulnerable to pass-the-hash and brute-force attacks due to the lack of salting.

Severity	CVSS	Plugin	Name
MEDIUM	6.8*	63478	Microsoft Windows LM / NTLMv1 Authentication Enabled

For the Windows 10 workstation, the only vulnerability detected was “SMB Signing not required. Whilst this is not as severe as the vulnerabilities detected on the Domain Controller, not forcing SMB signing can allow an unauthenticated attacker to use man-in-the-middle attacks against the SMB server and modify the data without detection.

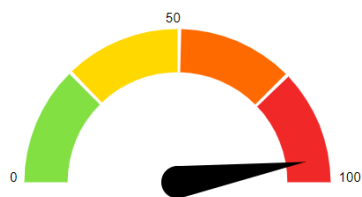
Nessus has provided valuable analysis of the network configuration of the hosts on the domain, and the configuration of both hosts. Remediation for these vulnerabilities is simple and can be achieved with proper configuration of group policies and patch management.

To confirm Nessus' reports on the missing updates was correct, a PowerShell script was used to check for the Windows patch updates on the DC. ---- Expand

PingCastle

An audit on the target domain was completed by PingCastle to identify and assess how vulnerable the domain is. PingCastle identified several critical areas of concern, highlighting the need for immediate security remediation. A Domain Risk Level score of 95/100 was given. The full PingCastle Report can be found in [Appendix II: PingCastle Report](#).

Indicators



Domain Risk Level: 95 / 100

It is the maximum score of the 4 indicators and one score cannot be higher than 100. The lower the better

[Compare with statistics](#)

[Privacy notice](#)

Figure 7: PingCastle - Domain Risk Level Score

Key Findings

---- 3-5 main topics here and a few bullet points/issues for each one

Inadequate Security Configurations **### DEL DO ABOVE ^^**

Policy	Severity	Impact	Recommended Solution
DES Encryption Enabled	High	A weaker encryption algorithm enabling successful cryptographic attacks	Disable DES encryption and enforce AES
NTLMv1 Enabled	High	Particularly susceptible to credential theft	Use NTLMv2 instead and disable NTLMv1
6 Accounts not using pre-authentication	Medium	Susceptible to AS-REP roasting attacks	Ensure Kerberos pre-authentication is enabled for all users and service accounts
Never Expiring Passwords	High	Old passwords are more likely to be reused.	Implement a password expiration policy and enforce regular password changes

MSF

Phase 4: Exploitation

- Tools Used: Kerbrute, Impacket, BloodHound, Hashcat.

- Successful exploited: password spraying success, AS-REP Roasting, Kerberoasting, and SMB relay attacks leading to unauthorized access.

Phase 5: Post-Exploitation

- Accessed sensitive files, escalated privileges, and demonstrated lateral movement. The Golden Ticket attack was used to maintain persistence within the network.

Recommendations

Provide recommendations to mitigate the vulnerabilities identified. E.g. patch management, least privilege policies, network segmentation.

Conclusion

The assessment uncovered several critical vulnerabilities within the "vulnAD.lab" environment, demonstrating the need for immediate remediation to protect against potential attacks. Regular security assessments are recommended to ensure ongoing protection against emerging threats.....

Appendix I: Full Reports

Nmap

Nessus

PingCastle – GitHub link would be better

Appendix II: Tools & Methods Used

- VirtualBox Setup
- **Glossary of Terms:** Definitions of technical terms used in the report.
- **Vulnerability Details:** Comprehensive details of each vulnerability discovered, including CVEs if applicable.
- **Tools and Scripts:** List and description of the tools/scripts used during the assessment. Version numbers, control environment etc.