

# **Active Directory Security: Comprehensive Analysis of a Vulnerable & Misconfigured Domain**

Awais Riaz

c3585124

A dissertation submitted in partial fulfilment of the requirements of Leeds Beckett University for the degree of BSc (Hons) Cyber Security.

May 2024



LEEDS  
BECKETT  
UNIVERSITY

# Abstract

This dissertation investigates the evolving landscape of security challenges surrounding Active Directory (AD) environments. As a prominent centralised directory service, AD remains an increasingly attractive target for threat actors seeking unauthorised access to networks and privileged data. This study conducts a comprehensive vulnerability assessment of an intentionally misconfigured AD domain – vulnAD.lab. The assessment aims to replicate the common security weaknesses found in real-world networks.

The study (this dissertation and a Vulnerability Assessment Report) identify critical vulnerabilities within the vulnAD.lab domain, such as insecure authentication, the use of legacy (outdated) protocols, poor password policies, excessive user privileges and the misconfiguration of core network services allowing for unauthorised access to organisational assets. Identified misconfigurations and vulnerabilities were then exploited to demonstrate their potential impact. The exploitation phase was introduced into the Vulnerability Assessment in order to demonstrate how attackers could exploit these misconfigurations, vulnerabilities, and security flaws to gain unauthorised access, escalate privileges, move laterally within a network and exfiltrate sensitive data. The findings from the Vulnerability Assessment Report allowed for discussion regarding the implementation of robust security controls/practices in order to safeguard AD environments.

Key concepts covered in this study include: vulnerability assessment, AD exploitation techniques, AD security misconfigurations, mitigation strategies, threat modelling, risk analysis.

# Student's Declaration

Leeds Beckett University Dissertation Declaration

Mohammad Awais Riaz

*Awais Riaz*

# Acknowledgements

Behnam Bazli, Senior Lecturer – First Supervisor

Taimur Bakhshi, Senior Lecturer – Second Supervisor

# Table of Contents

List of Tables.....	i
List of Figures .....	ii
Chapter One: Introduction .....	1
1.1    Background .....	1
1.2    Rationale .....	3
1.3    Aims and Objectives .....	3
1.4    Report Structure .....	5
Chapter Two: Literature Review .....	7
2.1 Introduction.....	7
2.2 Literature Summary Table.....	8
2.3 AD Security: Analysing Vulnerabilities, Misconfigurations & Threats ..	10
2.4 Threat Landscape Analysis of AD .....	17
Chapter Three: Methodology .....	20
3.1 Introduction.....	20
3.2 Research Methodology .....	20
3.3 Design Methodology: Agile Scum .....	20
3.4 Technical Methodology: PTES .....	24
Chapter Four: Review of Technologies .....	27
4.1 Introduction.....	27

4.2 Design & Configuration of Vulnerable AD – vulnAD.lab .....	27
4.3 WazeHell's Vulnerable AD Script.....	29
4.4 Tools & Methods Used in the Vulnerability Assessment .....	30
4.5 Technological Insights Gained from the AD Assessment.....	36
Chapter Five: Vulnerable AD Assessment Findings & Analysis .....	37
5.1 Introduction.....	37
5.2 Design & Implementation .....	37
5.3 Vulnerability Assessment Findings .....	41
5.4 Discussion of Results .....	45
Chapter Six: Project Evaluation.....	46
Chapter 7: Conclusion .....	48
7.1 Summary.....	48
7.2 Conclusions.....	48
7.3 Future Works.....	48
References.....	49
Appendix A: Product Dev – Vulnerability Assessment of the Vulnerable AD Domain (vulnAD.lab).....	54
Appendix B: Product Dev – Design & Implementation Documentation .....	55
Misconfigurations Made to Vuln AD Domain.....	55
Challenges Encountered During VulnAD.lab Implementation .....	57

Appendix C: Original Project Specification (November 2023).....	59
Project Aim .....	59
Project Expectations.....	59
Appendix D: Generative AI Use.....	61
Appendix E: Ethics Approval .....	63

## List of Tables

Table 1: Literature Summary.....	9
Table 2 : Top 10 Most Common Network Misconfigurations in Large Organisations (NSA & CISA, 2023).....	10
Table 3: Risk Assessment of the existing threat landscape .....	19
Table 4: Tools used in the Intel Gathering Phase.....	31
Table 5: Tools used in the Vulnerability Analysis Phase .....	32
Table 6: Tools used in the Exploitation Phase.....	34
Table 7: Tools used in the Post-Exploitation Phase .....	35
Table 8: Risk Rating of identified vulnerabilities and misconfigurations .....	43



## List of Figures

Figure 1: GenericAll is the access control in place for a Domain Controller (Isakov, 2023, Figure 5.30) .....	13
Figure 2: Recommendations for addressing insufficient ACLs for network services, such as LDAP (NSA & CISA, 2023).....	14
Figure 3: Using Mimikatz to obtain a user's NTLM hash (Francis, 2021, Figure 16.15) .....	16
Figure 4: Insights into Cybersecurity breaches (Verizon, 2023, Figure 6. Select Key Enumerations) .....	18
Figure 5: Visual Representation of Agile vs Scum (Jain, 2023) .....	21
Figure 6: Initial Product Development Cycle.....	22
Figure 7: Revised Product Development Cycle .....	23
Figure 8: Revised Project Plan with Tasks .....	23
Figure 9: The 7 Stages of PTES (Layer 8 Security, 2023) .....	24
Figure 10: Vulnerable AD Setup Topology .....	28

# Chapter One: Introduction

## 1.1 Background

### 1.1.1 Introduction to Active Directory (AD)

Microsoft's Active Directory (AD) is widely recognised as the industry dominant directory service for the Windows operating system, serving as a centralised database directory service for networked domains. Approximately 90% of the Global Fortune 1000 companies utilise AD as the primary method for authentication and authorisation (Crandall, 2021). At its core, Active Directory Domain Services (AD DS) holds essential data relating to users, computers, and other resources, such as printers and file share servers, allowing seamless access to resources across a network. This form of centralised infrastructure facilitates fast and convenient access to networked resources, enhancing the operational efficiency for organisations (Morano, 2022).

Beyond its role in user and resource management, AD offers further essential services designed to meet the various network administration needs of organisations. These services include Lightweight Directory Services (LDS) and Active Directory Federation Services (AD FS). LDS provides simplified directory access to applications using the LDAP protocol (Microsoft, 2018), while AD FS enables Single Sign-on (SSO) functionality, simplifying the authentication process for users.

### 1.1.2 Importance of Securing Active Directory

The ubiquitous use of AD and its prominent attack surface make it a prime target for malicious actors aiming to exploit vulnerabilities and compromise organisational assets. As the industry-leading centralised system, AD's attack surface is increasingly attractive to attackers who aim to infiltrate domains with malicious intentions, presenting significant security challenges for organisations worldwide.

According to Simons (2015), Director of Program Management for AD at Microsoft, 90% of companies are running Active Directory, with 500 million active account users collectively authenticating 10 billion times a day. Alarming, 95 million (19%) of those accounts are under attack every day, highlighting the critical need for implementing robust security measures in domains to protect users and employees from AD attacks.

In AD environments, there are several security threats including vulnerabilities in both Windows and AD-reliant protocols such as Kerberos, NTLM, LDAP and DNS settings. If these protocols on the domain controller are misconfigured, AD can be exposed to exploits by malicious actors. For example, poorly configured user permissions or weak password policies could allow authorised users to access sensitive/critical resources. Similarly, a lack of user and device logging can make it easier for malicious and suspicious activity to go unnoticed.

Securing AD remains a challenge due to its nature of acting as a centralised hub for key operations within organisations. Network services and applications are often integrated directly into AD, which tempts organisations to prioritise accessibility over the implementation of strong security controls (Crandall, 2021).

Larger organisations typically have a complex design structure, with trees and child

domains used to partition data from other domains. The use of multiple domains can add complexity to enforcing security measures. However, organisations can utilise GPOs (Group Policy Objects) to enforce consistent and proper security measures across multiple domains and networks (Ebad, 2022).

## 1.2 Rationale

The ideology of this project is underpinned by the pressing need to demonstrate the detrimental impacts of poorly configured AD domains and to showcase the use of robust security controls in domain environments. The widespread implementation of AD makes it an attractive target for attackers who aim to exploit its extensive attack surface through various methods of infiltration and enumeration. The Verizon 2023 DBIR provides some alarming and eye-opening statistics from 16,312 security incidents, of which 5,199 were confirmed data breaches. The overview of the report outlines that 49% of breaches involved stolen credentials and 24% of the security incidents were ransomware related (Verizon, 2023).

A single point of entry in a centralised domain can act as a gateway for attackers to move laterally and escalate privileges to gain full control of the entire domain with enterprise admin credentials. It is therefore crucial for organisations to fortify AD against evolving threats, from various forms of threat actors. By investigating the AD security landscape, this project aims to provide strategies and solutions to organisations in order to safeguard their networks.

## 1.3 Aims and Objectives

### 1.3.1 Project Aim

The primary aim of this project is to identify and document the security vulnerabilities commonly associated with misconfigured AD environments; utilising these insights to design an intentionally vulnerable AD domain. A comprehensive vulnerability assessment will then be completed, investigating security vulnerabilities, misconfigurations and general inadequate security controls within the Vulnerable AD Domain.

The assessment will go beyond the scope of a typical vulnerability assessment by demonstrating the exploitation of key findings (vulnerabilities), to highlight the impact of insufficient and/or inadequate security measures and misconfigurations. This study aims to provide insights and recommendations obtained from the Vulnerability Assessment (hereby referred to as “VA”) and exploitation stages, highlighting the critical need for robust and contemporary security measures in AD environments.

**Research Question:** How can misconfigurations and poor security controls in AD contribute to introducing vulnerabilities, and what measures can be adopted to safeguard against these weaknesses?

### 1.3.2 Objectives

#### **Objective 1: Research Prevalent AD Misconfigurations & Vulnerabilities, Best Practices & Industry Standard Security Measures**

- Conduct thorough research into common misconfigurations of AD domains using research papers, threat analysis reports and comprehensive books discussing the configuration and exploitation of Active Directory.
- Investigate best practises for securing AD and its reliant protocols, focusing on mitigation strategies for common AD misconfigurations and vulnerabilities.

#### **Objective 2: Design a Vulnerable AD Domain**

- To create a virtual sandboxed environment for the Vulnerable AD Domain.
- Integrate various misconfigurations and security flaws into the AD Domain, utilising insights from prior research. Misconfigurations include, but are not limited to: misconfigured access controls, weak authentication encryption/mechanisms and overprivileged accounts. Inadequate security measures, failing to meet best practices, will also be implemented.
- Document the design process of the Vulnerable AD Domain, recording key vulnerabilities and security flaws introduced.

#### **Objective 3: Conduct a Comprehensive Vulnerability Assessment (VA) & Demonstrate Exploitation of Identified Vulnerabilities & Misconfigurations**

- Perform a comprehensive assessment of a poorly configured domain directory service (AD Domain) and its associated protocols and suite of software including LDAP, ACLs, Windows Server and Kerberos authentication.
- Investigate the (mis)configuration of access controls and permissions which could allow threat actors to bypass security controls and gain unauthorised access to organisational assets.
- Investigate the threat and impact of identified vulnerabilities and outdated legacy protocols.
- Utilise a range of pen-testing tools and methods to identify, test and demonstrate how threat actors could exploit vulnerabilities and misconfigurations in an AD Domain.

#### **Objective 4: Documentation & Reporting**

- Document the tools and methods used in the Vulnerability Assessment (VA) and/or the exploitation phase – e.g. screenshots, logs, output from tools. This will assist in providing supporting evidence for the Vulnerability Assessment Report.
- Create a detailed report of the VA, documenting and reporting on the findings, methodology and tools used in the assessment and exploitation stages.

### **1.4 Report Structure**

In the following chapters, this report will explore various aspects of the project:

**Chapter 2: Literature Review** – provides a comprehensive review of the research literature reviewed, which provide industry-standard practices in designing and securing AD environments, ranging from in-depth guides on AD design to reports and documentation. This chapter will also cover how the literature has been implemented into the design and exploitation phases of the vulnAD.lab domain.

**Chapter 3: Methodology** – this chapter will focus on the project design methodology and the product methodology implemented in the design and assessment of the Vulnerable AD Domain.

**Chapter 4: Review of Technologies** – this chapter will focus on the tools, methods and resources implemented in the design and assessment of the Vulnerable AD Domain. This includes an overview and justification of the key tools used during the Vulnerability Assessment.

**Chapter 5: Findings & Analysis** – presents the results of the Vulnerability, providing an overview of the vulnerabilities discovered, their exploitability and suitable remediation. This chapter provides insights into the poor security posture of the AD Domain.

**Chapter 6: Project Evaluation & Product Evaluation** – evaluates the project, the change in project scope and the effectiveness of the product (vulnAD.lab).

**Chapter 7: Summary & Conclusions** – this final chapter will provide a comprehensive summary of the findings, recommendations and conclusions drawn from the research and implementation phases of the project.

# Chapter Two: Literature Review

## 2.1 Introduction

This literature review aims to gauge the threat landscape of AD from the various forms of literature used during the research and implementation phases of this project. Utilising insights from research papers, journal articles (by industry experts) and specialised books on designing and implementing secure AD domains. By critically analysing these literature resources, this review aims to highlight the valuable insights obtained from resources where challenges and solutions of the AD ecosystem have been identified as a means of meeting the project objectives declared in the [Product Specification](#).

The main themes of literature reviewed in this chapter are: security challenges of AD domains, best practises for securing AD environments, pen-testing and vulnerability assessment (including the methodology) and threat landscape analysis. Key findings used to advance the project will be assessed in this chapter to determine the role of research conducted and its significance in the project's scope and direction. A table containing a summary of the primary literature sources used is included to provide an overview of the fundamental points discussed in literature resources.



## 2.2 Literature Summary Table

Resource Title	Proposed Work	Pros	Cons
<b>Book: Mastering Active Directory: Design, deploy, and protect AD DS for Windows Server 2022.</b>	An in-depth detailed, comprehensive guide on designing and securing AD.	Provides detailed best practises for securing AD environments, whilst providing understanding of core topics.	This resource is not directly AD Security related; the primary focus is on designing and deploying AD.
<b>Research Paper: On Attacking Kerberos Authentication Protocol in Windows AD Services.</b>	Conducts a practical survey on attacking the Kerberos Authentication protocol in Windows AD environments.	Offers thorough practical insights into various forms of Kerberos Authentication vulnerabilities.	Focuses specifically on Windows OS, lack of coverage of Linux systems using Kerberos.
<b>Book: Pentesting Active Directory and Windows-based Infrastructure: A comprehensive practical</b>	Provides detailed analysis and practical steps for penetration testing within AD environments. Various attacks are covered.	Diverse coverage of penetration testing techniques, tools and methods specific to AD and Windows infrastructures. Provided guidance on	This resource does not cover mitigation and remediation methods for preventing these attacks. The focus is on testing and exploitation.

guide to penetration testing Microsoft infrastructure.		conducting vulnerability assessments.	
---	--	--	--

*Table 1: Literature Summary*

## 2.3 AD Security: Analysing Vulnerabilities, Misconfigurations & Threats

The significant role AD plays in safeguarding organisational assets cannot be downplayed due to the evolving landscape and tactics used by malicious actors, who aim to exploit vulnerabilities and gain network access to domain services. Despite its prominent role in the industry, AD is susceptible to several security vulnerabilities if security controls are not configured correctly, which can subsequently threaten the integrity and confidentiality of organisational assets. A recent publication released by the National Security Agency (NSA), in collaboration with the Cybersecurity and Infrastructure Security Agency (CISA), emphasises the critical need of addressing security misconfigurations in AD environments. The report ‘Top Ten Cybersecurity Misconfigurations’ (NSA & CISA, 2023) identifies the top ten most common cybersecurity misconfigurations in large organisations (shown in Table 2), detailing the “tactics, techniques and procedures (TTPs)” threat actors use to exploit the subsequent misconfigurations (NSA & CISA, 2023).

<b>1. Default configurations of software and applications</b>
<b>2. Improper separation of user/administrator privilege</b>
<b>3. Insufficient internal network monitoring</b>
<b>4. Lack of network segmentation</b>
<b>5. Poor patch management</b>
<b>6. Bypass of system access controls</b>
<b>7. Weak or misconfigured multifactor authentication (MFA) methods</b>
<b>8. Insufficient access control lists (ACLs) on network shares and services</b>
<b>9. Poor credential hygiene</b>
<b>10. Unrestricted code execution</b>

*Table 2 : Top 10 Most Common Network Misconfigurations in Large Organisations (NSA & CISA, 2023)*

The misconfigurations in Table 2, provided by the NSA and CISA, provide some general requirements that will inform the design methodology for assessing the security posture of the Vulnerable AD. Many of these misconfigurations will be assessed within the Vulnerable AD Domain environment. Additionally, this advisory

report acts as a framework for implementing misconfigurations and security flaws in the Vulnerable Domain.

### 2.3.1 Kerberos Authentication

#### 2.3.1.1 Understanding Authentication in Active Directory

Authentication and authorisation are handled primarily by the Kerberos protocol – an open standard protocol (not proprietary to Microsoft) that ensures secure authentication between domain controllers (DCs) and clients. Kerberos authentication can be integrated with a variety of applications and services using the same standard (Kerberos V5), making it a flexible and robust authentication protocol for AD domain environments (Motero et al., 2021).

The Kerberos protocol operates using a trusted middleman known as the Key Distribution Centre (KDC) which plays a crucial role in enabling secure encrypted communication between clients and services, acting as a safeguard from man-in-the-middle (MITM) attacks and packet sniffing from attackers (Francis, 2021). The DC uses two services: Authentication Service (AS) and the Ticket-Granting Service (TGS) within the KDC process to authenticate user or service requests; this process ensures the requests are authentic and confidential (Motero et al., 2021).

In the chapter titled 'Best Security Practises' in the book 'Mastering AD', Francis (2021) describes a typical Kerberos authentication in these steps:

1. **Initial Authentication:** A logon request containing the user's credentials is sent to the KDC (domain controller).
2. **AS Request:** The user's system sends a request to the AS within the KDC.
3. **TGT Generated:** Once the user's creds have been verified, the AS issues a TGT (Ticket Granting Ticket) encrypted with a secret key (aka session key) which is only known to the KDC and the user.
4. **TGS Request:** When the user requires access to a service, the user's device will request a service ticket from the TGS using the TGT.
5. **Service Ticket Generated:** If the TGT is valid, the TGS issues a service ticket for the requested service. This ticket is encrypted with a key shared only between the TGS and the service.

- 6. Service Request:** The user's system sends the service ticket back to the requested service.
- 7. Access Granted:** The service provider verifies the service ticket with its own key and grants access if the ticket is valid.

The use of a secret cryptographic key ensures secure communication between the KDC and the client during the authentication process. Whilst the built-in security controls implemented within the Kerberos protocol provide additional security, attackers are able to circumvent these controls through various vulnerabilities and misconfigurations.

#### 2.3.1.2 Critical Analysis of Authentication Literature

The paper "On Attacking Kerberos Authentication Protocol in Windows Active Directory Services: A Practical Survey" by Motero et al. (2021) offers a practical analysis of various methods utilised by attackers to exploit Kerberos authentication in Windows AD DS environments. Unlike Francis (2021), this comprehensive paper provides detailed examples of real-world exploitation methods, demonstrating the practical consequences of authentication vulnerabilities in AD domains. Conversely, Francis (2021) provides a foundational understanding of Kerberos authentication in AD and does not discuss, in detail, potential vulnerabilities and exploitation techniques used by threat actors. Although Francis (2021) does mention how attackers can potentially intercept and spoof Kerberos Authentication tickets, he omits to mention methods to mitigate these vulnerabilities.

In contrast, Motero et al. (2021) offer a comprehensive analysis of the vulnerabilities associated with Kerberos authentication within AD DS. They use a systematic methodology that covers various aspects of the vulnerability/attack lifecycle: attack objectives, analysis of detection methods and proposed mitigation strategies.

The detailed analysis and exploitation of Kerberos vulnerabilities by Motero et al. (2021) acts as a beneficial resource in configuring the Vulnerable AD Domain. In the vulnerable domain, Kerberos was (mis)configured to replicate the vulnerabilities demonstrated in Motero et al's paper – Golden Ticket, Silver Ticket and Pass the Ticket (PtT) attacks. Adjustments were made to the Domain Group

Policy to force Kerberos authentication with weak encryption types and turning off Kerberos Authentication monitoring – these changes can be found in [Appendix B](#). These changes ensured the vulnerable AD Domain was vulnerable to common and impactful Kerberos authentication exploits.

### 2.3.2 LDAP Misconfigurations

Lightweight Directory Access Protocol (LDAP) is a critical component of Active Directory, typically bundled with the AD DS package. LDAP is used in Microsoft's AD domain environments to allow users to interact with AD's centralised systems. However, if misconfigured LDAP can be susceptible to enumeration attacks.

1. **Opting out of LDAPS (LDAP over SSL):** By default, LDAP traffic (tcp/389) is unencrypted, which will query and return traffic in cleartext. Francis (2021) discusses the importance of enabling LDAPS and disabling unsecured LDAP connections using simple bind on port 389 to prevent attackers from intercepting LDAP queries.

```
ObjectDN           : CN=KINGSLANDING,OU=Domain Controllers,DC=sevenkingdoms,DC=local
AceQualifier       : AccessAllowed
ActiveDirectoryRights : GenericAll
ObjectAceType      : None
AceFlags           : None
AceType            : AccessAllowed
InheritanceFlags    : None
SecurityIdentifier  : S-1-5-21-4243769114-3325725031-2403382846-1116
IdentityReferenceName : stannis.baratheon
IdentityReferenceDomain : sevenkingdoms.local
IdentityReferenceDN   : CN=stannis.baratheon,OU=Crownlands,DC=sevenkingdoms,DC=local
IdentityReferenceClass : user
```

*Figure 1: GenericAll is the access control in place for a Domain Controller (Isakov, 2023, Figure 5.30)*

2. **Use of weak ACLs:** LDAP directories without ACLs can allow attackers to gain unauthorised access to data in the enumeration stage of an attack. Isakov (2023) identifies which ACLs have been used to assign access to objects in the domain, specifically targeting permissions such as GenericAll and GenericWrite on computers in the domain. These two ACLs are attractive to attackers as they can be abused to enumerate unauthorised data. The GenericAll attribute grants full rights to an object, meaning attackers can add users to a group, reset passwords and escalate privileges.

The report ‘Top Ten Cybersecurity Misconfigurations’ (NSA and CISA, 2023) also provides guidance on the use of “Insufficient ACLs on network shares and services”. The report highlights how a lack of ACLs can allow malicious actors to exfiltrate data from shared drives and folders. The recommendations are provided in the Figure 3 below (NSA and CISA, 2023).

Misconfiguration	Recommendations for Network Defenders
Insufficient ACLs on network shares and services	<ul style="list-style-type: none"> <li>• <b>Implement secure configurations for all storage devices</b> and network shares that grant access to authorized users only.</li> <li>• <b>Apply the principal of least privilege</b> to important information resources to reduce risk of unauthorized data access and manipulation.</li> <li>• <b>Apply restrictive permissions to files and directories</b>, and prevent adversaries from modifying ACLs <a href="#">[M1022]</a>, <a href="#">[D3-LFP]</a>.</li> <li>• <b>Set restrictive permissions on files and folders containing sensitive private keys</b> to prevent unintended access <a href="#">[M1022]</a>, <a href="#">[D3-LFP]</a>.</li> <li>• <b>Enable the Windows Group Policy security setting, "Do Not Allow Anonymous Enumeration of Security Account Manager (SAM) Accounts and Shares,"</b> to limit users who can enumerate network shares.</li> </ul>

*Figure 2: Recommendations for addressing insufficient ACLs for network services, such as LDAP (NSA & CISA, 2023)*

- 3. Anonymous Binding Enabled:** Allowing anonymous LDAP binds can expose sensitive directory info to unauthenticated users on the network, including attackers. Disabling the Group Policy setting “Do Not Allow Anonymous Enumeration of Security Manager (SAM) Accounts and Shares” can allow attackers to enumerate AD objects using LDAP without authenticating - no username or password required (NSA & CISA, 2023). An attacker could:
- View user accounts and their attributes (OUs, group memberships and contact details)
  - Enumerate Admin accounts and users with high privileges
  - Query computers and servers joined to the domain, including servers for critical operations like exchange, SQL and web servers

NSA & CISA (2023) have combined Anonymous Binding and Insufficient ACLs as one misconfiguration and list them both as the eighth most common “network misconfiguration”. The report advises network and system

administrators to enable the Group Policy setting (mentioned above) to “limit users who can enumerate network shares” (NSA & CISA, 2023).

### 2.3.3 Outdated Protocols & Encryption

Protocols on operating systems are updated and revised constantly in order to improve the security of key services such as SMB, NTLM and SSL. Over time, vulnerabilities within hash functions are discovered, posing security risks to organisations using “broken” hashing algorithms and insecure encryption types. It is considered good security practise to disable legacy protocols and encryption methods and enforce newer versions to mitigate against vulnerabilities.

#### 2.3.3.1 SMBv1

Microsoft’s SMB (SMBv1) was introduced in 1992. Although SMB1 was superseded by SMBv2 in 2007, it wasn’t deprecated until 2014 (Deland-Han, 2023). Ten years later, SMBv1 is still likely used by thousands of organisations using older printers and network servers that rely on the legacy SMBv1. In 2017, a chain of critical exploits part of the zero-day exploit package known as “Eternal Blue” were exploited in the SMBv1 protocol (Constantin, 2017). Although Microsoft patched the vulnerabilities a month before the exploit was leaked, there were several ransomware and hacking groups that used the exploits to infect hundreds of thousands of computers running SMBv1 in the next few months.

SMBv1 has lacked basic security features such as encryption and signing, making the protocol particularly vulnerable to MITM attacks (Bergson, 2018). Microsoft (Constantin, 2017) and the NSA & CISA (2023) strongly urge organisations to switch to the more secure and reliable SMBv2 and SMBv3 protocols to mitigate against many of the security concerns of SMBv1.

A common misconfiguration with SMB is not enforcing SMB signing – this should be enabled for both the client and server in order to mitigate against MITM and pass-the-hash (PtH) attacks; a recommendation by NSA and CISA (2023).



### 2.3.3.2 NTLMv1

NTLM (Network Technology LAN Manager) was replaced by Kerberos as the default authentication protocol for AD from 2000. Despite being deprecated in favour of Kerberos and NTLMv2, NTLMv1 is still used in older systems.

Francis (2021) explores the vulnerabilities of the outdated NTLMv1 authentication protocol in a practical manner. By using the exploitation tool Mimikatz, Francis was able to extract a user's NTLM hash from the LSASS memory. One mitigation provided by Francis to prevent attackers from obtaining NTLM hashes is to use the Protected Users group to prevent credential caching, removing the need for NTLM.

```
Authentication Id : 0 ; 3059384 (00000000:002eae8)
Session          : Interactive from 3
User Name        : liam
Domain           : REBELADMIN
Logon Server      : REBEL-PDC-01
Logon Time       : 15/04/2017 08:35:20
SID              : S-1-5-21-4041220333-1835452706-552999228-1230
msv :
  [00010000] CredentialKeys
    * NTLM      : 947e1646ca81470d18fdb6d976ba8d6a
    * SHA1      : aabc44618a0645c/ddd29ca5/f95bacc318/1b6
  [00000003] Primary
    * Username  : liam
    * Domain    : REBELADMIN
    * NTLM      : 947e1646ca81470d18fdb6d976ba8d6a
    * SHA1      : aabc44618a0645c7ddd29ca57f95bacc3f1871b6
tspkg :
wdigest :
  * Username  : liam
  * Domain    : REBELADMIN
  * Password  : (null)
kerberos :
  * Username  : liam
  * Domain    : REBELADMIN.COM
  * Password  : (null)
ssp :
credman :
```

Figure 3: Using Mimikatz to obtain a user's NTLM hash (Francis, 2021, Figure 16.15)

Bergson (2018) observes that advances in hardware and algorithms have made NTLMv1 vulnerable to credential theft. He strongly encourages the retirement of NTLMv1, instructing organisations to only allow NTLMv2 responses to improve security. Another advisement is to enable the policy setting "Network security: Do not store LAN Manager hash value" to prevent attackers from obtaining access to LM hashes in the local SAM database.

The NSA and CISA (2023) also advise disabling the use of the NTLM protocol as it is “susceptible to PtH” attacks. They warn the use of easily crackable passwords and NTLMv1 can allow attackers to elevate privileges and move laterally within networks.

Isakov (2023) describes two primary methods to obtain NTLM hashes: MITM attacks and coerced authentication – both these methods exploit vulnerabilities within the NTLMv1 protocol. To mitigate these threats, Isakov recommends removing the implementation of NTLMv1. If this is not possible (or ideal), enforcing a strong password policy and implementing network security features.

## 2.4 Threat Landscape Analysis of AD

The ubiquitous use of AD by thousands of organisations around the world and the centralised nature of the service makes it an appealing target for threat actors. High-level Microsoft executive Alex Simons stated approximately 90% of Global Fortune 1000 companies are utilising AD (Simons, 2015). Therefore, it stands to reason that threat actors (primarily threat groups) are focusing their efforts on targeting the underlying tools, protocols and services provided by AD Domains. Simons revealed there are over 10 billion authentication processes every day, across 500 million active user accounts. An alarming 95 million (19%) of these accounts face attacks every day, underscoring the significant and persistent threats towards AD environments.

According to Simons (2015), attackers often maintain access to compromised networks for more than 200 days before they are detected, allowing them plenty of time to move laterally within the network, escalate privileges and achieve their objective – this could be data exfiltration, ransomware deployment or other malicious activities that would benefit them.

### 2.4.1 Prevalent Threats in AD

The prevalence of AD across global organisations makes it an attractive target for threat actors aiming to gain unauthorised access to sensitive organisational assets. There are three main methods attackers use to gain access to organisations (Verizon, 2023):

- Stolen Credentials
- Phishing
- Exploitation of Vulnerabilities

One ubiquitous threat that affects all domains is the theft and misuse of credentials. In the last five years, there has been a significant increase in the use of stolen credentials by attackers. Figure 4 shows nearly half (49%) of all breaches in 2021-2022 involved the use of compromised credentials (Verizon, 2023). This statistic demonstrates the importance of credentials to attackers, signifying the cruciality of implementing secure authentication controls within AD.

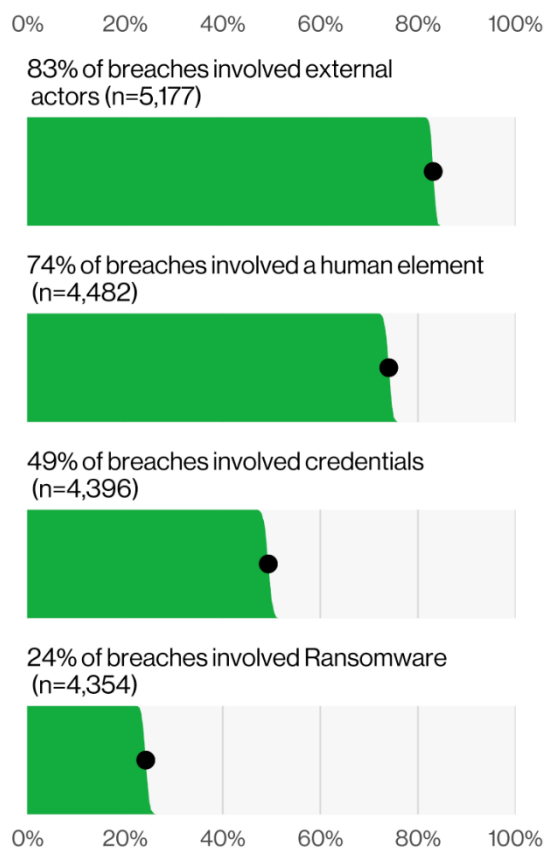


Figure 4: Insights into Cybersecurity breaches (Verizon, 2023, Figure 6. Select Key Enumerations)

AD Domains are constantly being scanned in search for exploitable vulnerabilities to assist in lateral movement. For instance, more than 32% of scans relating to the landmark Log4j vulnerability occurred within a month of it being released (Verizon, 2023). This illustrates how quick attackers can be to exploit the latest vulnerabilities.

## 2.4.2 Threat Assessment of AD

This table provides an overview of some of the most common threats to domain environments.

Threat	Explanation	Likelihood	Potential Impact
Stolen Credentials	Often the first method attackers will use to gain access to a domain.	Medium	Medium (High without MFA)
Phishing Attacks	A popular form of deception designed to fool users into sharing sensitive info. Malware can be injected into emails or websites that can be used to gain access (National Cyber Security Centre, 2018).	High	Medium
Exploits	Attackers can exploit vulnerabilities within AD or computers linked to the domain.	Medium	High
Ransomware	A form of malware that encrypts files and locks access to the operating system until demands are met	Medium	Critical
Misconfigurations of AD and networks	Poorly configured DCs or services can be exploited by threat actors	Medium	High

*Table 3: Risk Assessment of the existing threat landscape*

# Chapter Three: Methodology

## 3.1 Introduction

This chapter presents the methodologies used throughout the course of the project. The primary aim of this chapter is to outline the research conducted into methodologies and design ideologies, and to justify the chosen methodology and design approach.

A structured approach is required during the vulnerability assessment phase in order to correctly assess the security posture of the domain. A methodology provides structured framework for identifying vulnerabilities, assessing the attack surface and assisting with the documentation process. To ensure the aims and objectives of the project were achieved, this project adopted the Penetration Testing Execution Standard (PTES) as the methodology for designing and testing the Vulnerable AD Domain. The Agile Scrum framework was used to guide the project management and the product development process.

## 3.2 Research Methodology

This project involved the use of primary and secondary research methods. The first phase of the project involved an extensive review of existing research and literature, this was to inform the design and testing of the Vulnerable AD Domain. The secondary research was centred around the critical analysis of existing literature, whilst primary research focused on practical first-hand testing in a virtualised environment (Virtual Box).

## 3.3 Design Methodology: Agile Scrum

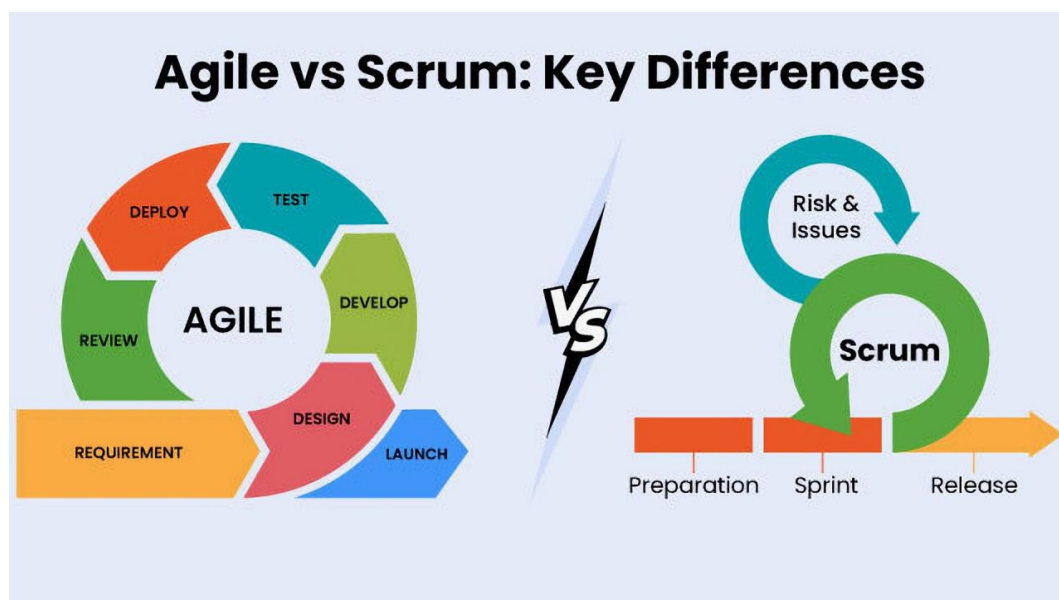
Agile Scrum is an Agile based framework used for project management (Rehkopf, 2023). The premise of Scrum is to provide a flexible and iterative product design philosophy. In the development and assessment phases of the VAD, Scrum was the prevailing methodology for the project, allowing for a flexible scope and adaptation of objectives, if required.

### 3.3.1 Alternative Methodologies

During the research and planning stage of the project, several methodologies were considered, including highly regarded options such as Waterfall and Spiral.

The Waterfall framework was a key contender due to its structured approach and clear project phases, however it was ultimately rejected in favour of Scrum due to its inflexibility with adjusting the objectives and tasks of the project (Nguyen, 2015).

The Spiral Model incorporates risk management during the product development and uses an iterative approach (just like Scrum), which was a significant benefit (Kanjilal, 2023). Unfortunately, like the Waterfall method, the Spiral Model relies on a set plan and does not allow for much adaptation. It is also considered to be complex and not suitable for smaller projects (Kanjilal, 2023).



*Figure 5: Visual Representation of Agile vs Scum (Jain, 2023)*

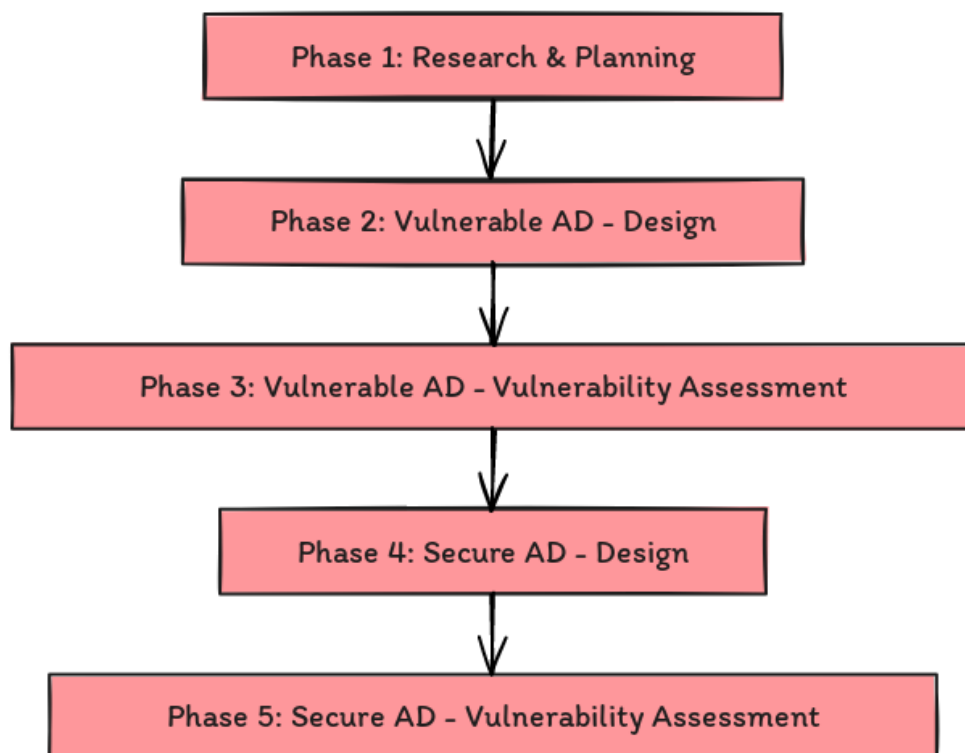
### 3.3.2 Justification of Agile Scrum ----adjust

Agile Scrum was the selected choice for the project due to its iterative and adaptive workflow, which allowed for objectives to be broken down into sprints with individual tasks. Prior to starting the product development, one of the main concerns of the project was the possibility of scaling down the project due to the overambitious objectives set in the original project specification. Scrum's ability to accommodate changes to the project scope and product development was the principal factor in selecting it.

The adaptability of Scrum makes it ideal for IT and Cyber Security projects, where complexities and unpredictable challenges often arise (Hewitt, 2024). Anticipating the possibility of potential challenges and setbacks, Scrum's iterative approach provides flexibility to address issues that may occur and ensures that the project remains on track even if adjustments to the project are required.

### 3.3.3 Implementation of Agile Scrum in Product Development

The [original project specification](#) details five objectives. These five objectives acted as the baseline for the product development cycle; five objectives, five phases. The original aim of the project was to design and assess two AD Domains; one vulnerable and one secure. This is illustrated in the flowchart below.



*Figure 6: Initial Product Development Cycle*

However shortly into the product development, a decision was made to adjust the scope of the project to focus solely on the Vulnerable AD Domain. This was due to the realisation that the aim of designing, implementing/misconfiguring security controls and conducting a Vulnerability Assessment of two AD Domains (each with their own detailed report and documentation) was not feasible to achieve in the limited time. Time constraints and the need for comprehensive documentation throughout the process meant it was necessary to limit the scope of the project. To complete an achievable and quality product, the decision was made to concentrate solely on the Vulnerable AD Domain (Phases 1-3).

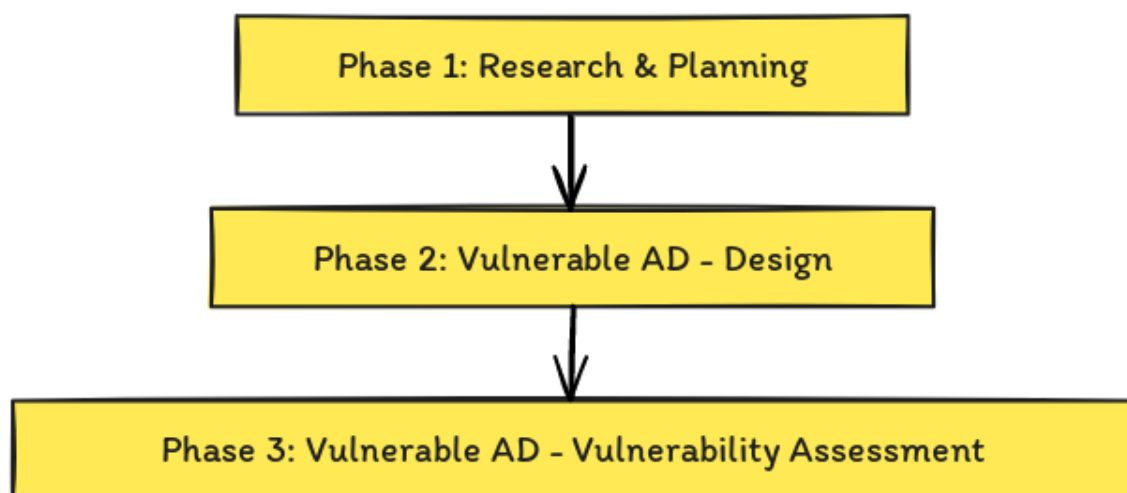


Figure 7: Revised Product Development Cycle

The ability to easily refine the project scope using Agile Scrum meant the sprints (each phase), and the tasks remained unchanged, highlighting the adaptability of Scrum projects. The project was restructured into three main phases: Research & Planning, Vulnerable AD: Design, and Vulnerable AD: Vulnerability Assessment. Each phase represents an Agile Scrum sprint. This is shown in the flowchart in Figure 7.

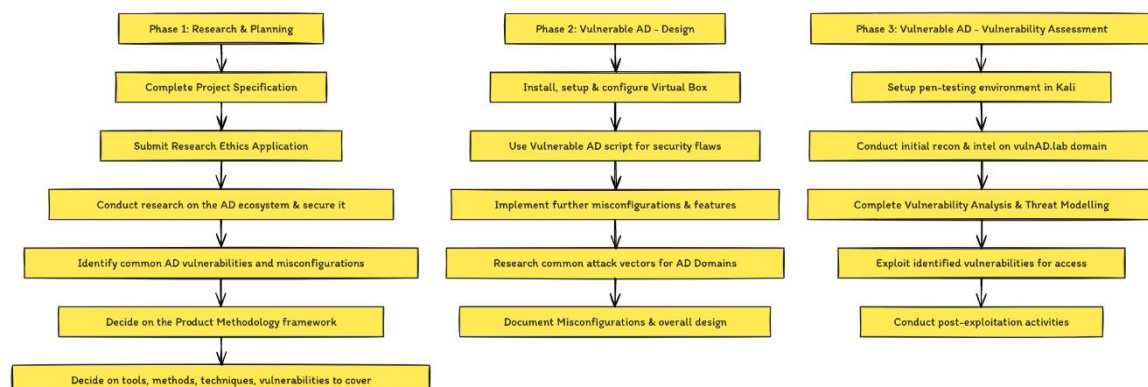


Figure 8: Revised Project Plan with Tasks



Illustrated above is a breakdown of each phase in the revised project plan.

### 3.4 Technical Methodology: PTES

#### 3.4.1 Overview of PTES

Penetration Testing Executive Standard (PTES) is a globally recognised methodology that provides a comprehensive and structured penetration testing framework. The PTES framework is made up of two components (Finn, 2024):

- Pen-Test Guidelines – outlines the seven key stages of the pen-test phase, providing a methodical approach for conducting security assessments.
- Technical Guidelines – provides a comprehensive list of tools, techniques and methods that may aid in the seven key stages of the pen-test.

The seven main areas the PTES methodology focuses on are displayed in the graphic below.

#### 3.4.2 Rationale for choosing PTES

The decision to adopt the Penetration Testing Execution Standard (PTES) as the primary form of methodology was due to the comprehensive guidance provided in the PTES Technical Guidelines, covering every critical phase of pen-testing/security assessments. The guidance provided aligns well with the project's objectives of assessing and improving AD security.

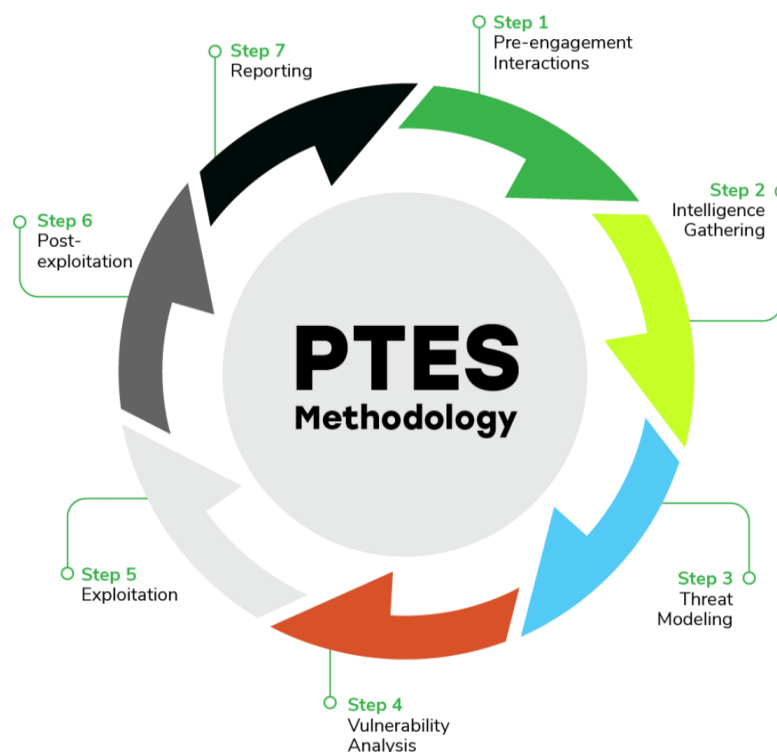


Figure 9: The 7 Stages of PTES (Layer 8 Security, 2023)

Included in the Technical Guidelines are an extensive list of tools, methods and techniques that cover various aspects of pen-testing/security assessments. For instance, in Section 2: Intelligence Gathering, dozens of tools and methods are included – ranging from OSINT (open-source intelligence) to internal and external foot printing techniques. A structured framework is provided for Vulnerability Analysis, suggesting the use of tools in passive testing, brute-forcing, vulnerability searching (common misconfigurations/default passwords) and automated scanning tools (PTES, 2014).

Moreover, the PTES technical guidelines cover attacks and protocols that are relevant to AD environments, such as LDAP and Kerberos attacks. These attacks provided an excellent example of exploiting weaknesses/misconfigurations in access controls and user authentication mechanisms.

### 3.4.3 Collaboration of PTES with Agile Scrum

In order to conduct a comprehensive security assessment of the Vulnerable AD Domain, the PTES methodology was followed as the guiding framework for assessing the security of the VAD. Each phase in the PTES methodology represents an Agile Sprint. This allows for a simplified but focused approach to each aspect of the Vulnerability Assessment. The sprints below relate to Phase 3: Vulnerable AD Vulnerability Assessment.

**Sprint 1: Intelligence Gathering** – this sprint was dedicated to gathering info regarding the Vuln AD, focusing on identifying potential attack vectors into the targeted domain.

**Sprint 2: Threat Modelling** – the info gathered in the previous phase was used to develop a threat model of the domain. Potential vulnerabilities and identified misconfigurations in Sprint/Phase 1 were used to assess threats based on the STRIDE framework.

**Sprint 3: Vulnerability Analysis** - using a combination of automated and manual tools, a detailed analysis of the target systems (DC and Win 10 PC) was completed.

**Sprint 4: Exploitation** – identified vulnerabilities and misconfigurations in previous stages were exploited.

**Sprint 5: Post-Exploitation** – privilege escalation, lateral movement and further exploitation of the domain.

**Sprint 6: Documentation & Reporting** - the final sprint involved creating the Vulnerability Assessment of the VAD and enhancing existing documentation to ensure the reporting of the VAD Assessment was to a comprehensive standard.

# Chapter Four: Review of Technologies

## 4.1 Introduction

This chapter will review the key technologies used in the development of this project. The use of practical tools will be assessed to gauge their purpose and effectiveness in identifying and evaluating the security of the misconfigured domain. A critical evaluation of the tools and methods used to identify and assess the security of the VAD will be conducted.

## 4.2 Design & Configuration of Vulnerable AD – vulnAD.lab

The design of the VAD Domain – vulnAD.lab – was one of the core components of the project. The vulnerable domain was designed and intentionally configured to deviate from industry best security practices; in order to simulate a real-world domain environment of a domain with poorly configured and/or improper security controls in place.

### 4.2.1 Virtualisation Environment - VirtualBox

The virtualisation environment acts as the foundation for the operating systems used in the design and assessment of the vulnAD.lab domain. Oracle VirtualBox was the chosen hypervisor for this project due to its ease of use and widely recognised compatibility with various operating systems. VirtualBox hosted two VMs (virtual machines) that comprised the vulnAD.lab domain. The use of a hypervisor allowed for a controlled and isolated testing environment.

The alternative hypervisor option, VMWare, is considered to be more suitable for large-scale projects and has certain features like snapshots locked behind a paywall or subscription service. VirtualBox on the other hand, is a free open-source with a simple UI and snapshot capabilities which is a key aspect of ensuring strong backup and recovery practices.

#### 4.2.1.2 Virtual Machines Configuration

The configuration of VirtualBox is illustrated in Figure 10.

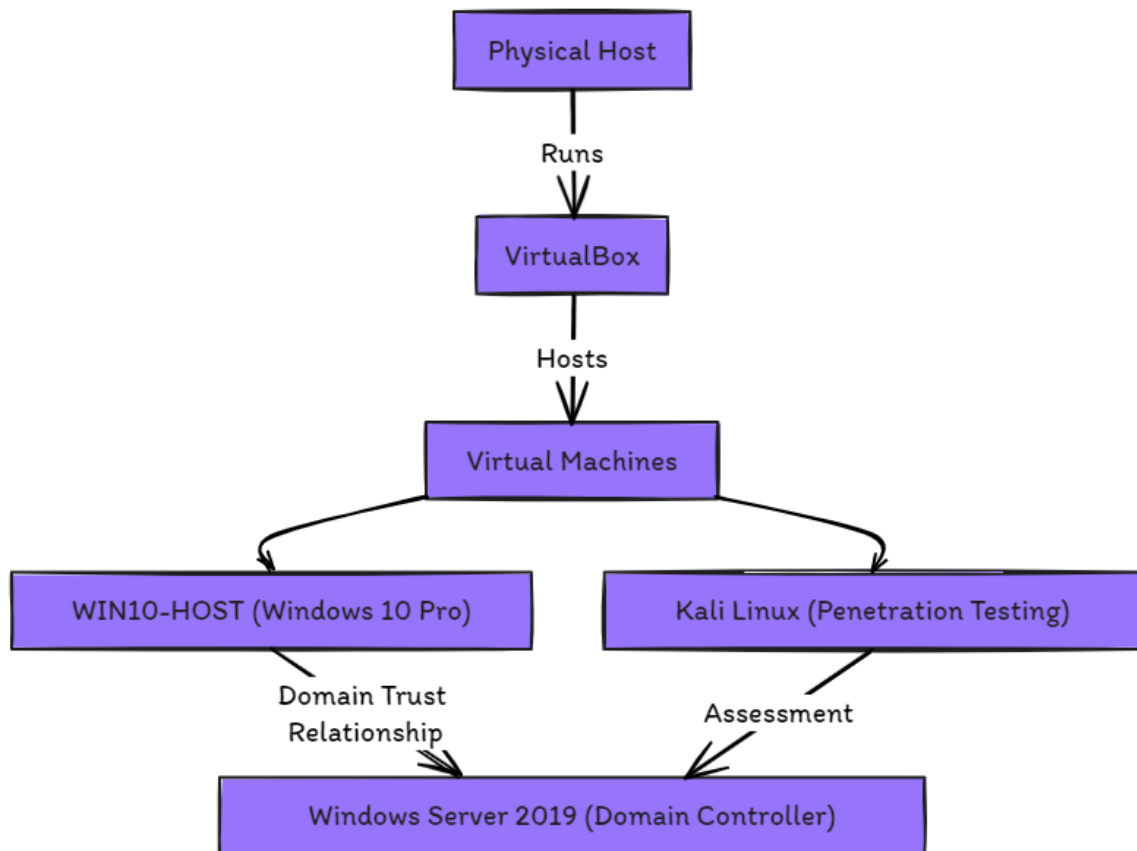


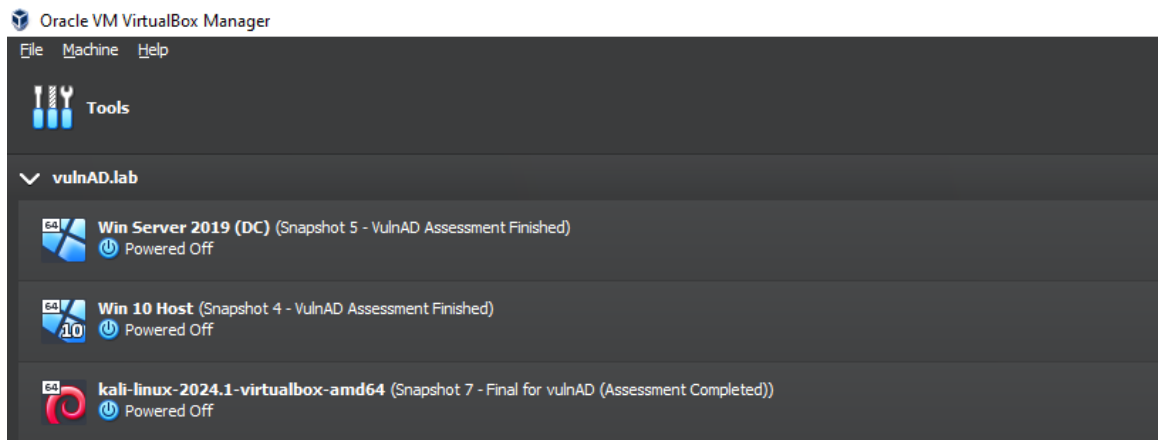
Figure 10: Vulnerable AD Setup Topology

- The physical host represents the first layer of hardware running Oracle VirtualBox Manager. It is responsible for allocating system resources such as CPU, memory and storage for the VMs.
- VirtualBox Manager is the hypervisor, allowing the management of all VMs on the physical host. This single process can emulate several systems, each running their own operating system.

#### The VMs running via VirtualBox:

- **Windows Server 2019:** hosting AD DS and acting as the Domain Controller of the VAD Domain. Windows Server 2019 - v1809 (2018), Build No: 10.0.17763.
- **WIN10-HOST (Windows 10 Pro):** the client machine with a domain trust link to the DC.

- **Kali Linux** was utilised in the assessment and exploitation of the VAD. Kali Linux has an extensive range of penetration testing tools pre-installed, making it the ideal OS to assess and attack the VAD.



*Figure 11: VMs used in Oracle VirtualBox*

## 4.3 WazeHell's Vulnerable AD Script

WazeHell's [Vulnerable-AD script](#) (safebuffer, 2020) is a simple yet highly effective PowerShell script which was utilised early into Phase 2 of the project, after setting up Windows Server and installing AD DS. This script integrated several vulnerabilities and automated the process of creating users, groups and most importantly, introducing several misconfigurations and vulnerabilities.

### 4.3.1 Justification of WazeHell's Script

WazeHell's PowerShell script was chosen as it provided the ability to misconfigure the VAD Domain at its core – it acted as the ideal starting point for a vulnerable domain by replicating common security vulnerabilities and configuring the domain in way which would attract attackers.

Whilst there are other scripts available to automate the process of creating a typical AD Domain environment quickly, WazeHell's script automated the process of generating groups, services and accounts relevant for a Vulnerable AD Domain. Most importantly, a range of misconfigurations, vulnerabilities and poor security practises which were introduced by the script and simulated insecure configurations often targeted by attackers in real-world AD breaches and attacks.

Further details regarding WazeHell's script and its specific functions can be found in.

## 4.4 Tools & Methods Used in the Vulnerability Assessment

A suite of specialised and industry-standard tools were used to conduct the VA of the vulnAD.lab domain. Across the four practical stages of the PTES methodology, a minimum of 10 tools were used to assess and/or exploit the security weaknesses of the VAD. Detailed findings and analysis obtained from tools and methods can be viewed in the [Vulnerable AD Domain Vulnerability Assessment Report](#).

Tables 4–7 detail the tools used across several phases of the VA, listing their usage, purpose and the reasons for selecting them over alternative options.

#### 4.4.1 Intelligence Gathering Tools

Tool	Purpose	Alternative Tool	Reason for selection
<b>Nmap</b>	An essential tool for enumerating the domain network, including the two targeted hosts – Windows Server 2019 (DC) and the WIN10-HOST client. Detailed scans revealed open ports, running services and the potential misconfigurations of services.	Zenmap	Nmap is more flexible, allowing the use of specific options/parameters.
<b>ldapsearch</b>	Used to query the domain via the LDAP protocol to enumerate the domain structure.	LDP.exe	LDP was available on the DC (Windows), however a suitable Linux based tool was required for use on the Kali system.
<b>ADRecon</b>	Specifically designed for enumerating AD domains, this tool aided in gaining useful info regarding the structure and configuration of the domain, whilst providing insights into the objects (users, groups and permission sets).	PowerView	ADRecon is far more comprehensive, producing reports regarding user accounts, permissions, domain structure and other areas of interest.

*Table 4: Tools used in the Intel Gathering Phase*



#### 4.4.2 Vulnerability Analysis Tools

Tool	Purpose & Usage	Alternative Tool	Reason for selection
<b>Nessus</b>	An industry-standard vulnerability scanner which was used to determine the vulnerability of the domain. A scan of the network revealed several vulnerabilities and misconfigurations within the AD environment.	OpenVAS	Nessus was chosen due its extensive library of plugins and constantly updated vulnerability database (Yen, 2024).
<b>PingCastle</b>	This tool provided a security audit report, rating the domain based on risk factors. PingCastle played a significant role in identifying and prioritising identified vulnerabilities.	BloodHound	Initially both tools were going to be used, however there were issues with configuring BloodHound. On its own, PingCastle was instrumental in identifying inadequate security controls.
<b>Metasploit (MSF)</b>	Briefly used to test the exploitability of identified vulnerabilities.	N/A	N/A

Table 5: Tools used in the Vulnerability Analysis Phase

#### 4.4.3 Exploitation Tools

Tool	Purpose & Usage	Alternative Tool	Reason for selection
<b>Kerbrute</b>	A powerful utility used for brute-forcing Kerberos authentication mechanisms such as lack of pre-authentication, cryptographically insecure encryption types and password spraying.	Hydra	Specifically targeted for Kerberos testing/exploitation making it more effective than Hydra at exploiting Kerberos misconfigurations.
<b>Mimikatz</b>	Used to extract various types of credentials and cached service tickets from the memory dump (LSASS).	CrackMapExec	Mimikatz is able to extract a range of credentials, tokens and various forms of credentials.
<b>Impacket</b>	This tool was heavily relied upon during the exploitation of SMB and other attacks. Several python scripts are included with this tool, which provided the ability to target a range of vulnerabilities and misconfigurations and maximise the attack surface.	MSF (Metasploit Framework)	MSF provides plenty of modules for exploitation and post-exploitation, however Impacket's scripts are tailored towards exploiting via the SMB protocol making it more suitable and applicable for exploiting the domain.
<b>Hashcat</b>	Hashed credentials (primarily passwords) were cracked using Hashcat during the exploitation	John the Ripper	Hashcat is more suited towards brute-forcing than John. Hashcat supports more hash

	and post-exploitation phases. Hashed credential formats include: NTLM, DCC2, Kerberos 5 tickets and MD5.		formats than John, which does not support DCC2 (hashcat, 2024).
--	--	--	---

Table 6: Tools used in the Exploitation Phase

#### 4.4.4 Post-Exploitation Tools

Tool	Purpose & Usage	Alternative Tool	Reason for selection
<b>Evil-WINRM</b>	A Windows Remote Management tool used for executing commands on targeted systems, allowing for further exploitation and lateral movement within the domain. PtH attack was conducted to gain access to the DC.	PowerShell Empire	A simpler option providing access to the Windows system. Additional features were not required to demonstrate post-exploitation activities.
<b>Mimikatz</b>	Utilised to extract additional credentials and session tokens during lateral movement and post-exploitation.	N/A	Acts as a post-exploitation tool through privilege escalation, additional harvesting of credentials and tokens to allow for persistent access.

<b>DCShadow using Mimikatz</b>	An exploitation technique that exploits the DCSync vulnerability. It is used to replicate the DC in order to push malicious changes to AD objects, essentially providing full control of the DC and by extension, the entire domain.	MSF Module	Mimikatz offers further post-exploitation and data harvesting features.
<b>xFreeRDP</b>	An RDP (Remote Desktop Protocol) client used in Kali to connect to the compromised systems with a graphical interface. This tool allowed for additional control over the targeted system and further exploitation.	rdesktop	xFreeRDP is better supported for newer systems.

*Table 7: Tools used in the Post-Exploitation Phase*

## 4.5 Technological Insights Gained from the AD Assessment

The vulnerability assessment conducted on the vulnAD.lab domain utilised a wide range of pen-testing tools to determine the security posture of the domain. This comprehensive assessment revealed significant findings that emphasise the complexity and multifaceted approach of implementing and maintaining security features in AD, as a means of providing some mitigation against threat actors.

### 4.5.1 Effectiveness of Vulnerability Analysis Tools

The effectiveness of vulnerability scanners/analysis tools such as Nessus and PingCastle presented the powerful danger of vulnerabilities and misconfigurations. The misconfiguration of a single policy or protocol in Windows can result in several gaps in security, making the domain a prime target for attackers.

Nessus highlighted several critical weaknesses, primarily related to outdated patches and the misconfiguration of key protocols such as SMBv1 and NTLM. PingCastle's ability to audit an entire network and reveal minor (and major) misconfigurations in policies can highlight threats attackers can use to gain access to the domain network.

### 4.5.2 Importance of Implementing Best Security Practices

The insights from the VA Report underscore the importance of adhering to best security practices through the implementation of properly configured security controls. Following best practices for designing and securing AD domains can significantly reduce the threat surface for attackers, which mitigates the risk of potential breaches/attacks. Utilising security measures such as MFA, zero-trust (also principle of least privileges), proper patch management and proper network monitoring, configuration and auditing provides a defence against threat actors.

The tools used in the analysis of vulnerabilities and exploitation phases were crucial in identifying and exploiting the weaknesses of the VAD domain. The findings and analysis gained from these tools not only allowed for the identification and/or exploitation of misconfigurations and vulnerabilities, but also showcase the potential entry points and attack vectors threat actors may target.

# Chapter Five: Vulnerable AD Assessment Findings & Analysis

## 5.1 Introduction

This chapter presents a detailed discussion of the findings from the Vulnerability Assessment of the vulnAD.lab domain (also referred to as the “VAD”). The full report can be viewed in [Appendix A](#); extensive documentation including scripts, logs, screenshots and command output can be accessed on [Github](#).

The vulnAD.lab domain was intentionally designed and misconfigured to simulate a real-world enterprise network that has been poorly configured, allowing for a controlled environment to investigate the prevalent security flaws that are often exploited by threat actors. The use of a virtualised environment, using VirtualBox, provided the necessary controlled environment in which to implement, examine and test (the exploitability of) common security weaknesses applicable to real-world AD environments.

## 5.2 Design & Implementation

This section will provide an overview of the implementation process and testing methodology applied during the VA of the misconfigured AD Domain – vulnAD.lab. The aim of designing and assessing a vulnerable domain was to gain first-hand experience and knowledge in the prevalent security flaws in AD Domain environments, and to be able to offer remediations, mitigations and recommendations for improving AD Security.

### 5.2.1 Implementation Process

The vulnAD.lab was configured in a manner that allowed for the implementation of common vulnerabilities and misconfigurations using literature relating to the design of AD, best security practises and official guidelines.

### 5.2.1.1 Specific Misconfigurations & Vulnerabilities Introduced

Listed below are some of the misconfigurations and vulnerabilities intentionally introduced in the vulnAD.lab domain. For the full list of vulnerabilities, misconfigurations and poor security practices implemented in the domain, refer to [1.4 Risk Ranking](#) in the Vulnerability Assessment Report (Riaz, 2024).

#### Group Policy Object (GPO) Misconfigurations

1. **Outdated Protocols:** The GPO was severely misconfigured to introduce vulnerabilities that weakened the security of the domain. For instance, NTLMv1 was enabled, a deprecated and outdated protocol known for its susceptibility to various types of cryptographic attacks, was enabled to introduce credential attacks such as PtH and brute-forcing.
2. **Inadequate Account Lockout Policies:** Account lockout policies were left undefined to allow the attacker unlimited attempts to brute-force credentials, without triggering an account lockout. The minimum password length was set to only four characters, significantly lowering the complexity of user passwords. As a result, passwords were substantially easier to crack.

#### Service and User Account Misconfigurations

1. **Excessive Permissions:** Service accounts handling tasks for critical services such as exchange\_svc and http\_svc were assigned excessive privileges and added to high-privileged groups like “Domain Admins”, failing to meet the principle of least privilege outlined in the CISA & NSA Report (CISA & NISA, 2023).
2. **Kerberoasting:** Exchange\_svc and mssql\_svc were configured to be vulnerable to Kerberoasting, allowing attackers to extract the hashes of service tickets.
3. **AS-REP Roasting:** Several accounts had the pre-authentication check disabled for Kerberos requests. This introduced the AS-REP Roasting attack, allowing attackers to request Kerberos tickets from the DC without credentials.

#### LDAP & Kerberos Misconfigurations

1. **Disabled LDAPS (LDAP over SSL):** By not securing LDAP traffic with SSL/TLS, LDAP queries are unencrypted. This introduces the data interception and manipulation threats such as the MiTM attack.
2. **Kerberos Weak Encryption:** The preferred encryption algorithm was set to DES and RC4, two of the weakest encryption algorithms for Kerberos authentication. This presented the opportunity to identify and test the exploitability of Kerberos attacks such as Pass-the-ticket, brute-forcing and other credential attacks.

### **Poor use of ACLs & Permission Controls**

1. **Misconfigured ACLs:** Access Control Lists were intentionally misconfigured for several AD objects, utilising excessive ACLs for non-privileged users such as “GenericAll” and “WriteOwner”. The implementation of this misconfiguration was to demonstrate how poorly configured ACLs could be exploited by threat actors aiming to gain access to sensitive organisational assets and making unauthorised changes to data. This feature was implemented using WazeHell’s script (safebuffer, 2020).
2. **Password Stored in Object Description:** A password was stored in a user’s description field, disclosing the user’s credentials.

For the full list of vulnerabilities, misconfigurations and poor security practices implemented in the domain, refer to [1.4 Risk Ranking](#) in the Vulnerability Assessment Report (Riaz, 2024).

#### **5.2.1.2 Vulnerability Testing & Exploitation**

In the testing phase, vulnerabilities and misconfigurations implemented during the design process were subjected to testing and exploitation to test their impact and severity. This was a critical phase as it involved practically demonstrating the implications of poor security practices and misconfigurations to provide insights and increase awareness of attacks utilised by malicious actors in real world scenarios.

### **Proposed 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 the real-world by malicious actors. This domain, and its linked systems, were intentionally configured with specific vulnerabilities and misconfigurations to simulate prevalent industry threats and to ensure a suitable practical demonstration of threats and exploits.

This assessment was conducted under grey-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.

### **Objectives of the Vulnerability Assessment & Exploitation Phase**

The primary objective of this Vulnerability Assessment was to identify and exploit vulnerabilities and misconfigurations within the vulnAD.lab domain environment. The specific goals are as follows:

- To identify vulnerabilities and misconfigurations within the "vulnAD.lab" domain environment, ensuring the assessment and exploitation process is documented with logs, output from tools and figures.
- To exploit identified vulnerabilities to assess the potential impact of identified vulnerabilities in a poorly configured AD Domain .
- To provide actionable recommendations for identified vulnerabilities and exploits.

## Exploitation Techniques, Tools & Methods Used

Please refer to [Chapter 3: Technical Reporting](#) of the Vulnerability Assessment Report (Riaz, 2024) for the detailed breakdown of findings from each tool, method and technique in assessing and exploiting the vulnerabilities of the VAD domain.

### 5.2.2 Challenges Encountered

During the design and implementation of the vulnerable domain (product development), several key challenges were encountered that impacted the implementation and testing phases of the project. These issues were resolved in time, however for certain issues several hours were spent on troubleshooting and addressing the issue.

- Corrected network configuration from NAT to Internal Network for a working networking configuration between VMs, primarily the Windows 10 client PC and the Windows Server 2019 (DC).
- Hardware limitations caused slowdowns and performance issues with VirtualBox. The host system's RAM was upgraded from 8GB to 24GB in order to improve performance and stability.
- A lack of storage space due to snapshots of all three VMs meant another hardware upgrade was required. An additional 1TB of storage space was added to the host system to allow for additional snapshots and to prevent system errors.

The full list of issues encountered can be found in [Appendix B](#).

## 5.3 Vulnerability Assessment Findings

### 5.3.1 Key Findings

The vulnerability assessment of the vulnAD.lab domain utilised a range of industry-relevant tools to identify and analyse various security vulnerabilities and misconfigurations, in order to understand the threat landscape of AD and provide recommendations for mitigating these issues.

The findings of the Vulnerability Assessment can be found in [Chapter 3: Technical Reporting](#) of the vulnAD.lab VA Report (Riaz, 2024). A brief ranking of the vulnerabilities and exploitation of the configuration of the VAD is shown below in Table 8.

Vulnerability ID	Description	CVSS Score	Impact	Remediation Urgency
VULN001	Improper Authentication	9.8	Critical	High
VULN002	Usage of Legacy/Deprecated Protocols	5.4	Medium	Medium
VULN003	Lack of Patch Management & Outdated System	7.0	High	High
VULN004	Data Exposure due to Misconfigured ACLs and insufficient access controls	8.5	High	High
VULN005	AS-REP Roasting	8.1	High	Urgent
VULN006	Kerberoasting	7.8	High	High
VULN007	Excessive Account Privileges	8.8	High	High
VULN008	Credential Harvesting via Mimikatz	9.4	Critical	Urgent
VULN009	Inadequate Password Policies	8.0	High	Urgent
VULN010	Insecure (Misconfigured) LDAP	7.5	High	Medium
VULN011	Insufficient Logging and Monitoring	6.5	Medium	Medium

VULN012	Use of Default Credentials (for users and service accounts)	8.5	High	Urgent
VULN013	DC Replication introducing DCSync Vulnerability	9.1	Critical	Urgent
VULN014	Pass-the-Hash Attacks	8.3	High	High
VULN015	Poor DACLS (Discretionary Access Control Lists)	8.2	High	Medium
VULN016	Account Lockout Threshold not Configured	6.7	Medium	High
VULN017	Severe Kerberos Misconfigurations	8.6	High	Urgent
VULN018	Never Expiring Passwords enabled for Domain Users	7.2	High	High
VULN019	Password Spray Attacks	8.0	High	Urgent
VULN020	Brute-forcing credentials	7.9	High	High
VULN021	Improperly configured RDP Access	7.6	Medium	High
VULN022	PAM (Privileged Access Management) Disabled	N/A	Medium	Medium

*Table 8: Risk Rating of identified vulnerabilities and misconfigurations*

### 5.3.2 Recommendations & Mitigation Strategies

Using the vulnerabilities identified in the previous section (and the Vulnerability Analysis), several recommendations and mitigation strategies were proposed. These recommendations, detailed fully in the [Chapter 4 of the VA report](#), are summarised here to provide actionable remediation steps to mitigate the security flaws uncovered during the assessment. These recommendations are in no way restricted to the VAD and are applicable to all AD domains. Most the recommendations are derived from best security practises and/or guidelines. Further advisories and security suggestions can be viewed in certain phases of the report – notably sections 3.1.4 and 3.4.1.4 of the VA report.

#### 5.3.2.1 Patch Management

- Implement a routine patch management plan
- Consider implementing automated patch deployment tools (such as Windows Server Update Services) to enforce targeted system updates for machines
- Perform regular vulnerability scans to detect new vulnerabilities and apply necessary patches

#### 5.3.2.2 Enforce Strong Password Requirements

- Enforce complex password requirements, ideally a minimum of 12 characters
- Implement an account lockout policy to prevent brute-force attacks
- Enforce regular password changes

#### 5.3.2.3 Add Network Security Protections & Monitoring

- Disable legacy protocols like SMBv1 and LDAP unsecured with more secure versions
- Implement intrusion detection prevention systems
- Utilise auditing and logging for all domain computers, in addition to increased monitoring and logging on DCs
- Develop an incident response plan to be prepared to be breaches and attacks

#### 5.3.2.4 Role Based Access Controls (RBAC)

- Utilise RBAC to ensure permissions are proper and required, adhering to the principle of least privilege

#### 5.3.2.5 Multi-Factor Authentication (MFA)

- Deploy MFA for all domain users
- Integrate MFA with SSO (Single Sign-On)

These recommendations not only address the vulnerabilities but also utilise industry best practices to fortify the security posture of the AD domain against future threats.

## 5.4 Discussion of Results

This section explores the findings from the VA conducted on the vulnAD.lab domain using insights from the VA Report, the literature reviewed and the significance of AD security.

### 5.4.1 The Relevance of vulnAD.lab with the real-world

The vulnerabilities identified in the VAD domain, such as Kerberoasting, credential extraction (Mimikatz) and the exploitation of misconfigured GPOs are genuine real-world threats to AD Domains. These vulnerabilities and attacks are relied upon by attackers who aim to gain network access. Frost & Sullivan (2020) stress how the implementation of weak or lax security controls, such as the use of common passwords, can make AD environments prime targets for attackers aiming to compromise the confidentiality, integrity and availability of organisational assets.

Misconfigurations relating to user privileges and account policies often allow attackers to escalate privileges and move laterally within the network, as stated by Verizon (2023) and CISA & NSA (2023).

### 5.4.2 Project Rationale & Objectives

The primary aim of this project was to demonstrate the detrimental impact of security weaknesses in AD domain environments. This project has developed a practical framework for testing and improving security in AD.

The rationale behind the project was to demonstrate the importance of configuring and implementing proper security controls in AD domains due to the threat landscape and w

## Chapter Six: Project Evaluation

The primary aim of the project was to assess and demonstrate robust security measures within Active Directory to enhance the security of a domain by conducting a comprehensive assessment of a Vulnerable AD Domain. The project originally planned to assess two AD domains; this scope however was adjusted to focus solely on the VAD Domain (vulnAD.lab) due to concerns regarding the overambitious aims and objectives. These concerns were confronted and a decision was made to adjust the objectives of the project in order to realistically complete the requirements.

The adjustment of the objectives ensured a successful project/product was achievable in the remaining timeframe. The Agile Sprint methodology thankfully allowed for a modification of the project scope. The modification of the project scope (to focus solely on the VAD) allowed for a more comprehensive and detailed implementation of misconfigurations in the vulnAD.lab domain, in addition to allowing for more detailed documentation. Learning of best security practices and implementations of strong AD security still remained relevant to the project even after the change in scope, due to the fact that recommendations and remediation methods were required for the VAD Domain Report.

The project successfully met its revised objectives and achieved the aim. This involved conducting a comprehensive vulnerability assessment of a misconfigured AD domain after designing and implementing an intentionally VAD domain plagued with misconfigurations, vulnerabilities, a lack of adherence to best security and general security practices and overall poor security controls. The use of the PTES methodology allowed for a structured yet systematic approach to conducting the VA.

In addition to identifying numerous critical vulnerabilities and conducting a thorough vulnerability analysis/assessment, a strong understanding of attack vectors and their consequences in overall security were learnt.

The project encountered several challenges. Technical issues relating to the virtualisation environment and the vast amount of research into relevant and

compatible testing tools were more time-consuming than originally thought. The original scope of the project was overambitious – designing two separate AD Domains with contrasting purposes and implementation philosophies, and then conducting vulnerability assessments of both domains (including a Vulnerability Assessment/Pen-Test Report) followed by an evaluation of the two domains was not achievable within the time frame.

It often takes a team full of experienced system and network administrators alongside security professionals several months to design and implement a secure AD Domain. Whilst it could have been possible within the timeframe, the quality of the Secure AD Domain would not have been up to par with industry standards.

The core product – vulnAD.lab – was designed to demonstrate the exploitability of misconfigurations in AD domain environments. A rigorous assessment was then conducted to determine the exploitability of each vulnerability and misconfiguration, offering remediation and mitigations to combat AD threats.



# Chapter 7: Conclusion

## 7.1 Summary

This dissertation has provided detail regarding the design, implementation and assessment of a Vulnerable AD Domain. Prevalent security flaws in AD Domains reported by Microsoft and other reputable well-renowned sources were researched, understood and implemented into the VAD to demonstrate the implications of poorly configured features in AD. The attack surface and attack vectors were identified, and mitigation methods were provided to remediate against these issues.

## 7.2 Conclusions

Key findings revealed that even minor configurations and security oversights can open the door to security breaches, threats and threat actors; thus highlighting the need for robust security controls and effective remediations. The VA outlined that the implementation of best practices, such as enforcing strong password policies, disabling outdated protocols and implementing MFA can play a crucial role in mitigating the risk of compromising organisation assets.

## 7.3 Future Works

There are several areas where further research and implementation of security features could allow for a more refined project:

- Impact of Emerging threats such as cloud infrastructure
- The design of a secure AD domain with strong security practices implemented in a separate domain would allow for an interesting and useful comparison of the two domains – vulnAD.lab and secureAD.lab.

## References

- Bergson, P. (2018) Retire Those Old Legacy Protocols. *Microsoft Tech Community*, 12 February [Online blog]. Available from: <<https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/retire-those-old-legacy-protocols/ba-p/259396>> [Accessed 25 March 2024].
- Constantin, L. (2017) *Decades-Old Network Protocol Puts Companies At Risk And Refuses To Die* [Online]. Forbes. Available from: <<https://www.forbes.com/sites/lconstantin/2017/07/21/decades-old-network-protocol-puts-companies-at-risk-and-refuses-to-die/>> [Accessed 15 April 2024].
- Crandall, C. (2021) Active Directory Sits in a Dangerous Security Blind Spot. 10 September [Online blog]. Available from: <<https://www.securitymagazine.com/articles/96063-active-directory-sits-in-a-dangerous-security-blind-spot>> [Accessed 14 January 2024].
- Deland-Han (2023) *SMBv1 Is Not Installed by Default in Windows 10 Version 1709, Windows Server Version 1709 and Later Versions* [Online]. Available from: <<https://learn.microsoft.com/en-us/windows-server/storage/file-server/troubleshoot/smbv1-not-installed-by-default-in-windows>> [Accessed 02 March 2024].
- Ebad, S. A. (2022) Lessons Learned from Offline Assessment of Security-Critical Systems: The Case of Microsoft's Active Directory. *International Journal of System Assurance Engineering and Management* [Online], 13 (1) February, pp. 535–545. Available from: <<https://link.springer.com/article/10.1007/s13198-021-01236-2>> [Accessed 18 February 2024].
- Finn, T. (2024) Penetration Testing Methodologies and Standards [Online]. IBM Blog. Available from: <<https://www.ibm.com/blog/pen-testing->

[methodology/www.ibm.com/blog/pen-testing-methodology](https://methodology/www.ibm.com/blog/pen-testing-methodology)>

[Accessed 19 March 2024].

Francis, D. (2021) Mastering Active Directory: Design, Deploy, and Protect Active Directory Domain Services for Windows Server 2022 [Online]. Available from:

<<https://ieeexplore.ieee.org/document/10162719>>

[Accessed 18 Jan 2024].

hashcat (2024) Hashcat/Hashcat [Online]. hashcat. Available from:

<<https://github.com/hashcat/hashcat>>

[Accessed 1 Mar 2024].

Hewitt, N. (2024) Implementing Scrum for Cybersecurity Teams • TrueFort.

*TrueFort*, 20 March [Online blog]. Available from: <<https://truefort.com/scrum-cybersecurity/>>

[Accessed 23 April 2024].

Isakov, D. (2023) *Pentesting Active Directory and Windows-based Infrastructure: A comprehensive practical guide to penetration testing Microsoft infrastructure* [Online]. Packt Publishing Ltd. Available from:

<[https://www.google.co.uk/books/edition/Pentesting\\_Active\\_Directory\\_and\\_Windows/z9ffEAAAQBAJ?hl=en&gbpv=0](https://www.google.co.uk/books/edition/Pentesting_Active_Directory_and_Windows/z9ffEAAAQBAJ?hl=en&gbpv=0)>

[Accessed 17 Jan 2024].

Jain, I. (2023) Agile Vs Scrum: Key Differences [Online image]. Available from:

<[https://media.licdn.com/dms/image/D4D12AQHHPsJ0fa44wA/article-cover\\_image-shrink\\_720\\_1280/0/1689758555897?e=2147483647&v=beta&t=c-x5xV0DnMsJjTMEG5r2gxJY1ij\\_ul2fWMOjDgNvp-Q](https://media.licdn.com/dms/image/D4D12AQHHPsJ0fa44wA/article-cover_image-shrink_720_1280/0/1689758555897?e=2147483647&v=beta&t=c-x5xV0DnMsJjTMEG5r2gxJY1ij_ul2fWMOjDgNvp-Q)>

[Accessed 23 April 2024].

Kanjilal, J. (2023) *Overview of Spiral Software Development* [Online].

Developer.com. Available from: <<https://www.developer.com/project-management/spiral-software-development/>>

[Accessed 23 April 2024].

Layer 8 Security (2023.) Information Security Penetration Testing & Threat Detection & [Online image]. Available from: <<https://layer8security.com/wp-content/uploads/2023/01/ptes-img.png>>

[Accessed 24 April 2024].

Microsoft (2018) *AD LDS Is a Mode of Active Directory That Provides Directory Services for Applications* [Online]. Available from:

<<https://learn.microsoft.com/en-us/previous-versions/windows/desktop/adam/what-is-active-directory-lightweight-directory-services>>

[Accessed 14 February 2024].

Morano, J. (2022) What Is Active Directory? 26 September [Online blog].

Available from: <<https://www.quest.com/solutions/active-directory/what-is-active-directory.aspx>>

[Accessed 13 February 2024].

Motero, C. D., Higuera, J. R. B., Higuera, J. B., Montalvo, J. A. S. and Gómez, N. G. (2021) On Attacking Kerberos Authentication Protocol in Windows Active Directory Services: A Practical Survey. *IEEE Access* [Online], 9, pp. 109289–109319. Available from:

<<https://ieeexplore.ieee.org/abstract/document/9501961>>

[Accessed 7 November 2023].

Nguyen, T. (2015) *Integrating Security into Agile Methodologies* [Online].

Available from:

<<https://www.umsl.edu/~sauterv/analysis/F2015/Integrating%20Security%20into%20Agile%20methodologies.html.htm>>

[Accessed 22 April 2024].

NSA & CISA (2023) *NSA and CISA Red and Blue Teams Share Top Ten Cybersecurity Misconfigurations* [Online]. Available from:

<[https://media.defense.gov/2023/Oct/05/2003314578/-1/-1/0/JOINT\\_CSA\\_TOP\\_TEN\\_MISCONFIGURATIONS\\_TLP-CLEAR.PDF](https://media.defense.gov/2023/Oct/05/2003314578/-1/-1/0/JOINT_CSA_TOP_TEN_MISCONFIGURATIONS_TLP-CLEAR.PDF)>.

Özeren, S. (2023) *DCShadow Attack Explained - MITRE ATT&CK T1207* [Online]. Available from: <<https://www.picussecurity.com/resource/blog/dcshadow-attack-explained-mitre-attack-t120>>

[Accessed 9 April 2024].

PTES (2014) PTES Technical Guidelines - The Penetration Testing Execution Standard [Online]. Available from: <[http://www.pentest-standard.org/index.php/PTES\\_Technical\\_Guidelines](http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines)>

[Accessed 19 March 2024].

PTES (2014) The Penetration Testing Execution Standard [Online]. Available from: <[http://www.pentest-standard.org/index.php/Main\\_Page](http://www.pentest-standard.org/index.php/Main_Page)>

[Accessed 19 March 2024].

Rehkopf, M. (2023) *What Is Scrum? [+ How to Start]* [Online]. Atlassian. Available from: <<https://www.atlassian.com/agile/scrum>>

[Accessed 21 March 2024].

Riaz, A. (2024) Vulnerability Assessment: vulnAD.lab [Online]. Vulnerability Assessment. p. 52. Available from: <<https://github.com/WasiG-619/Vulnerable-AD-Assessment-Exploitation/blob/main/vulnAD.lab%20-%20Vulnerability%20Assessment%20Report.pdf>>

safebuffer (2020) Vulnerable-AD [Online]. Available from: <<https://github.com/safebuffer/vulnerable-AD>>

[Accessed 01 Nov 2023].

Simons, A. (2015) *Active Directory Czar Rallies Industry for Better Security, Identity* [Online]. ZDNET. Available from: <<https://www.zdnet.com/article/active-directory-czar-rallies-industry-for-better-security-identity/>>

[Accessed 15 February 2024].

Verizon (2023) Figure 1. Select Key Enumerations [Online image]. Available from: <<https://raw.githubusercontent.com/vz-risk/dbir/gh->

[pages/2023/figures/148df1dd-cd6d-4de7-aef3-4db1f3f0b4eb-2-1.png>](#)

[Accessed 18 February 2024].

VirtualBox (2010) *VirtualBox User Manual* [Online]. Available from:

<<https://www.virtualbox.org/manual/ch01.html>>

[Accessed 27 March 2024].

Yen, L. (2024) OpenVAS vs. Nessus: Top Vulnerability Scanners Compared.

*Datamation*, 23 February [Online blog]. Available from:

<<https://www.datamation.com/security/openvas-vs-nessus/>>

[Accessed 14 April 2024].

## Appendix A: Product Dev – Vulnerability Assessment of the Vulnerable AD Domain (vulnAD.lab)

The Vulnerability Assessment Report is included in this section. Other Product Dev assets such as: VMs, Vuln AD configuration and documentation and the security assessment can be viewed in the following appendices or alternatively via [Github](#).

<https://github.com/WasiG-619/Vulnerable-AD-Assessment-Exploitation>



Vulnerable AD Domain Vulnerability Assessment Report.pdf

# Appendix B: Product Dev – Design & Implementation

## Documentation

### Misconfigurations Made to Vuln AD Domain

These are notes made during the design and implementation phase of vulnAD.lab.

#### Group Policy

- Misconfigured GPOs for Password Policies
- Poor Account Lockout/monitoring Policies
- Insufficient Minimum Password Length Requirement (only 4 chars, no complexity requirements)

#### Service/User Account Misconfigs

- Kerberoasting enabled on service accounts (exchange\_svc, mssql\_svc, http\_svc)
- Service accounts with more permissions than necessary, such as being added to "Domain Admins" or "Enterprise Admins" groups
- AS-REPRoasting vulnerabilities introduced on several accounts - clemence.lotty, enrica.brinn, bonnee.kevina & nicolina.marion
- Service accounts with weak or default passwords, e.g., "ch4ng3m3" and "SQL@Passw0rd"
- Service accounts are configured to have non-expiring passwords – "passwords do not expire" option ticked in ADUC.
- Default passwords set for users (Changeme123!) or the use of common passwords, allowing for password spraying attacks.

#### ACLs & Permissions

- Bad Access Control List (ACL) configurations created to allow unauthorised access - GenericAll, GenericWrite, WriteOwner, WriteDACL, Self, and WriteProperty access across various groups



- A password has been stored in the description of a user object
- DCSync rights provided to a standard domain user, introducing the DCShadow vulnerability.
- A share on the DC's network drive (containing sensitive info) has been misconfigured to allow anonymous access, with no access controls, effective permissions and restrictions in place.

## Kerberos Configuration Vulnerabilities

- Enabled weak encryption types for Kerberos (DES\_CBC\_CRC, DES\_CBC\_MD5, RC4\_HMAC\_MD5) while disabling stronger ones (AES128-CTS-HMAC-SHA1-96, AES256-CTS-HMAC-SHA1-96)
- Disabled Kerberos pre-authentication for specific users/service accounts, including admin users

## LDAP Misconfigurations

- Anonymous Binding enabled, allowing unauthenticated users to query the LDAP Directory
- Channel Binding disabled, Allowing for NTLM relaying attacks
- LDAPS Disabled, preventing encrypted LDAP traffic, viewable to attackers monitoring the network
- Poor ACLs implemented on critical objects, such as allowing r,w+x permissions to the anonymous logon group.

## Other Vulnerabilities & Poor Op Sec Practices Introduced

- Use of out-of-date software – have not installed any updates on the DC or the WIN10-HOST.
- Enabling SMBv1 and other insecure network protocols
- Lack of network monitoring or auditing.
- Disabling antivirus and Windows Defender on the client (WIN10-HOST) PC
- Configured the firewall to allow incoming connections to various ports and services – without authentication

- SMB Signing disabled, susceptible to MITM attacks
- Golden Ticket attacks are possible through improper TGT handling

## Challenges Encountered During VulnAD.lab Implementation

### 07-03-24 – Incorrect VBox Network Config (1hr)

- Set from Nat to Internal Network instead when realised could not ping devices (kali → WIN10-HOST)
- After leaving the domain (on the WIN10-HOST), could not rejoin, pings timing out. It seems the DNS Service on DC is not responding to queries.

### 08-03-24 – Technical Restrictions with RAM

- Struggling to have multiple VMs open – if more than 1 VM is running, the Win Server often crashes and comes up with a VirtualBox RAM error and pauses the VM.
- Will aim to upgrade the RAM of my laptop – HP ProBook 450 G7, currently only has 8GB of RAM. Win Server only has 2GB of RAM, with chrome and Word open, LT struggles

### 11-03-24 – RAM Upgraded from 8GB to 24GB

- Bought 16GB RAM from CEX for £18 – 2666MHZ DDR4. Installed RAM in LT today so total RAM is now 24GB of RAM.
- Increased RAM Allocations for all 3VMS

### 26-03-24 – Further Network Issues

- NAT Access on Kali VM works however the Fortinet firewall is blocking most activity, excluding common pages like Google. Unable to access Github to get the Bloodhound .py scripts.

### 27-03-24 – Vbox Guest Additions not working on Kali

- Couple hrs spent troubleshooting, reinstall of VBox Guest Additions package did not work
- Solution: Reverted to Snapshot 1 (Kali)

### 28-03-24 – Storage Issues on LT & OneDrive Sync

- The use of snapshots and backups has taken up all the space – 240GB of LT Storage
- Solution: Move earlier snapshots to OneDrive. Rely more on External HDD for backups and keep snapshots on the External HDD to free up space. Free up local space by keeping items on the cloud only
- Fix: Added External SSD to Laptop now total space is 1.2TB and Moved the VMs to the 2<sup>nd</sup> drive – so I now have 102GB free, previously had only 8GB of disk space free. Now I am not restricted with the number of snapshots I can use, allowing for better backup & recovery of VMs.

# Appendix C: Original Project Specification (November 2023)

## **Project Title: Securing Active Directory: Assessment & Implementation of Strong Domain Security**

### **Project Aim**

The primary aim of this project is to evaluate and demonstrate robust security measures within Active Directory (AD) to improve the overall security of a networked domain. This will be achieved by conducting a comprehensive assessment of a vulnerable AD domain system and using the insight and findings of the assessment to design a secure domain with robust and contemporary security measures.

The assessment into the vulnerable AD domain will aim to investigate security vulnerabilities within the AD domain system and, by extension, its linked systems such as Windows Server and protocols such as LDAP; misconfiguration of access controls and permissions; vulnerability assessment and exploitation; and outdated protocols.

A restructured AD system will be created incorporating the knowledge and insight provided by assessing the vulnerable domain. The aim with this system will be to incorporate greatly improved security measures to ensure the network and domain are secure from attacks. This will be achieved by introducing strong authentication, robust access controls lists (ACLs), implementation of a scheduled update/patch window and enforcing relevant privileges, in addition to incident prevention and response measures such as logging and IDS (Intrusion Detection System).

### **Project Expectations**

#### **Objective 1: Conduct a Vulnerability Assessment of a misconfigured Vulnerable AD domain**

- Perform a comprehensive assessment of a poorly configured domain directory service (AD domain) and its associated protocols and suite of software including LDAP, ACLs, Windows Server and Kerberos authentication.
- Investigate the (mis)configuration of access controls and permissions which could allow threat actors to bypass unauthorised access.
- Investigate the threat and impact of identified vulnerabilities and outdated legacy protocols.

#### **Objective 2: Research Best Security Practises for AD and Network Domain Security**

- Research contemporary best security practices for securing AD and other related protocols.
- Identify industry standards and guidelines to assist in the development of the secure AD domain system.
- Integrate the insight of contemporary practises (from research) to integrate security measures that are effective and appropriate for modern day systems.

### **Objective 3: Design a Secure AD Domain**

- Develop a structured secure AD domain based on the findings from the vulnerability assessment and research conducted.
- Integrate advanced security measures to mitigate the risk of exploits from current vulnerabilities and to improve the overall security of the network.
- Implement a strong authentication process, strong access controls, a schedule for implementing updates/patches, the principle of least privilege and an effective incident prevention and response measures.

### **Objective 4: Analyse the Secure AD Domain against Guidelines & Industry Benchmarks and the vulnerable domain**

- Analyse the newly implemented and improved security protocols of the second AD domain by comparing it to industry benchmarks.
- Assess the “secure” AD system’s ability to mitigate against vulnerabilities present in the vulnerable AD system – and its overall domain security.
- Simulate security incidents to determine the effectiveness of incident response protocols and real-time security mitigation and prevent security attacks.

### **Objective 5: Documentation & Reporting**

- Create comprehensive documentation detailing the project and its various stages, from initial research to report writing.
- Produce an end stage report summarising the outcome of the project and findings of Active Directory security configuration by comparing the findings and research of an insecure vs a secure domain.
- Produce a report that assesses how effective the outcome of the project aligns with the project objectives.

## Appendix D: Generative AI Use

I understand that to use the work and ideas of others, including generative AI output, without full acknowledgement, is academic unfair practice.

I confirm that this coursework submission is all my own, original work and that all sources, summaries, paraphrases and quotes are fully referenced as required by the LBU Academic Regulations.

### DECLARATION OF GENERATIVE AI USE:

I DID use Generative AI technology in the development, writing, or editing of this assignment.

Generative AI Tool (e.g. ChatGPT)	How generative AI Tool was used	Reference
ChatGPT 3.5	Summary of Research Papers (Research)	OpenAI. (2023). ChatGPT (Sept 12 version) [Large language model]. <a href="https://chat.openai.com/chat">https://chat.openai.com/chat</a>
ChatGPT 3.5	To create a PowerShell script for identifying installed Windows Updates (Product Dev)	OpenAI. (2023). ChatGPT (Sept 14 version) [Large language model]. <a href="https://chat.openai.com/chat">https://chat.openai.com/chat</a> Link to Script: <a href="https://github.com/WasiG-619/Vulnerable-AD-Assessment-Exploitation/blob/main/Vulnerability%20Analysis/Nessus/check_missing_KB_updates.ps1">https://github.com/WasiG-619/Vulnerable-AD-Assessment-Exploitation/blob/main/Vulnerability%20Analysis/Nessus/check_missing_KB_updates.ps1</a>
ChatGPT 3.5	Providing synonyms and advice on general report structure (Dissertation)	OpenAI. (2023). ChatGPT (Sept 14 version) [Large language model]. <a href="https://chat.openai.com/chat">https://chat.openai.com/chat</a>

ChatGPT 3.5	Troubleshooting issues with VirtualBox (Product Dev)	OpenAI. (2023). ChatGPT (Sept 14 version) [Large language model]. <a href="https://chat.openai.com/chat">https://chat.openai.com/chat</a>
ChatGPT 3.5	Troubleshooting issues and errors with AD setup and pen-testing (Product Dev)	OpenAI. (2023). ChatGPT (Sept 14 version) [Large language model]. <a href="https://chat.openai.com/chat">https://chat.openai.com/chat</a>


## Appendix E: Ethics Approval


The Ethics approval application (#121466) for the project was submitted on 20<sup>th</sup> Nov 2023 and approved by First Supervisor – Behnam Bazli on 13<sup>th</sup> February 2024.


[New Application](#) | [My Applications](#)c3585124 | [Logout](#)

### My Applications




**New Application**  
If you wish to submit a new application, click on 'New Applications' above.

**Existing applications**  
If you wish to edit an existing application prior to submission, click on the Application Title or select the 'Edit/Continue'  button.

If you have submitted an application and now need to make changes to it, click on the 'Make Revision/Copy'  button. Please add to the title the version number (for example, v2).

10  records per page

Search:

Title	Risk Category	Status	Date Created	Action
<a href="#">Securing Active Directory: Assessment &amp; Implementation of Strong Domain Security</a>	Risk Category 1	 Approved by supervisor	20-NOV-23	 

Showing 1 to 1 of 1 entries

[← Previous](#) | 1 | [Next →](#)

### **Riaz, Mohammad Awais (Student)**

**From:** researchethics@leedsbeckett.ac.uk  
**Sent:** 13 February 2024 20:48  
**To:** Riaz, Mohammad Awais (Student)  
**Subject:** Research Ethics

Application Ref: 121466  
Applicant Name: MOHAMMAD RIAZ  
Project Title: Securing Active Directory: Assessment & Implementation of Strong Domain Security

Dear MOHAMMAD RIAZ, Behnam Bazli has confirmed that the above project has been approved and can commence.

This project has received research ethical approval in line with the Research Ethics Policy and Procedures of Leeds Beckett University.

Please note that if you wish to make substantial changes to the project, new ethical approval would be required.

Sent on behalf of the Research Supervisor.