AFC RICHMOND

Security Assessment Findings Report
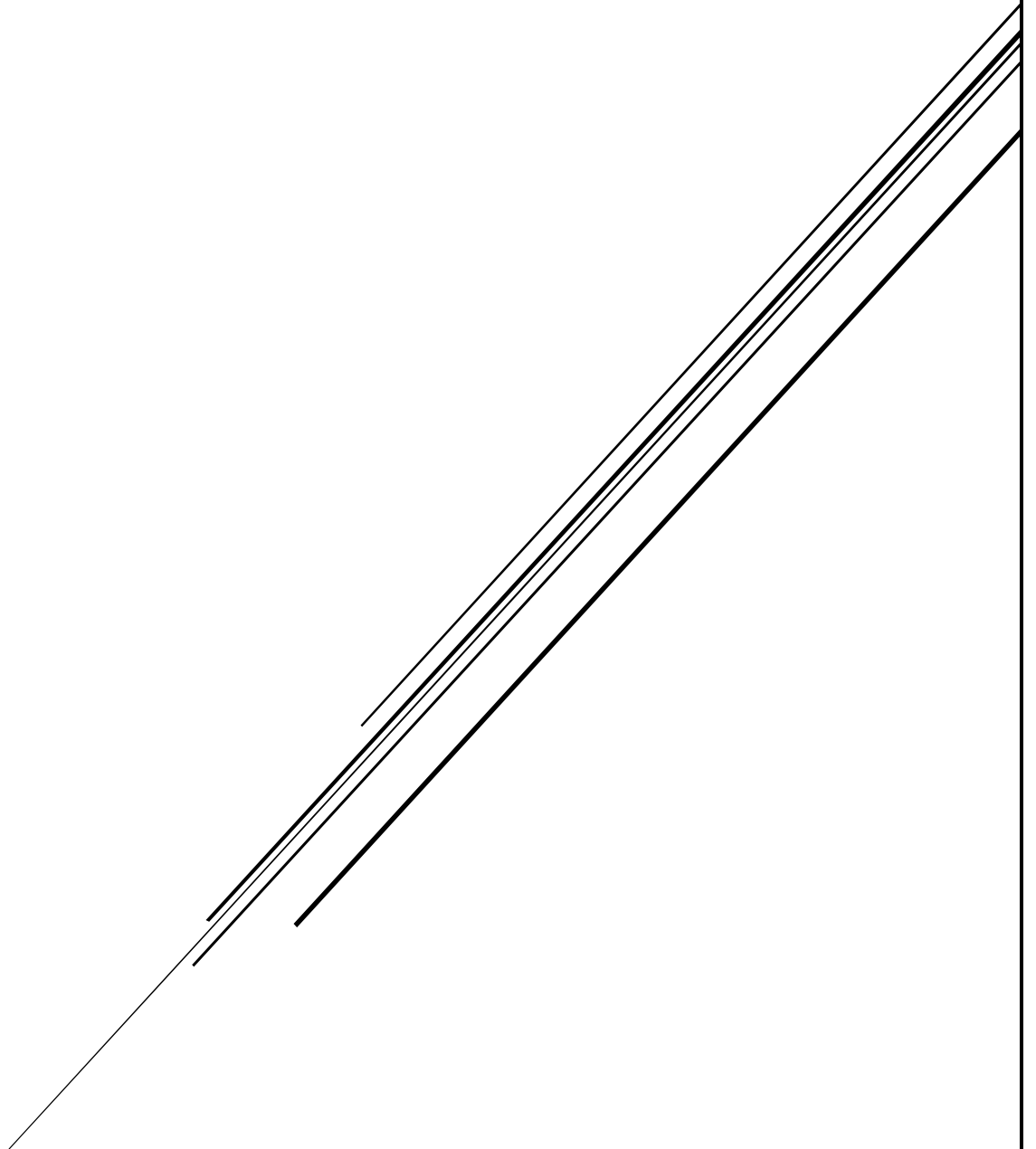
Table of Contents

Confidentiality Statement

This document is the exclusive property of AFC-Richmond (AFCR) and MA Security (MAS). This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both AFCR and MAS.

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

Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

Time-limited engagements do not allow for a full evaluation of all security controls. MAS prioritized the assessment to identify the weakest security controls an attacker would exploit. MAS recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

Contact Information

Name	Title	Contact Information
MA Security		
Manimaran Arivumani	Penetration Tester	Email: manimaranarivumani@gmail.com

Assessment Overview

From March 11th, 2024, to March 15th, 2024, AFC-Richmond engaged MAS to evaluate their internal security posture of its infrastructure compared to current industry best practices. All testing performed is based on the NIST SP 800-115 Technical Guide to Information Security Testing and Assessment, OWASP Testing Guide (v4), and customized testing frameworks.

Phases of penetration testing activities include the following:

- Planning – Customer goals are gathered, and rules of engagement obtained.
- Discovery – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
- Attack – Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.
- Reporting – Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.
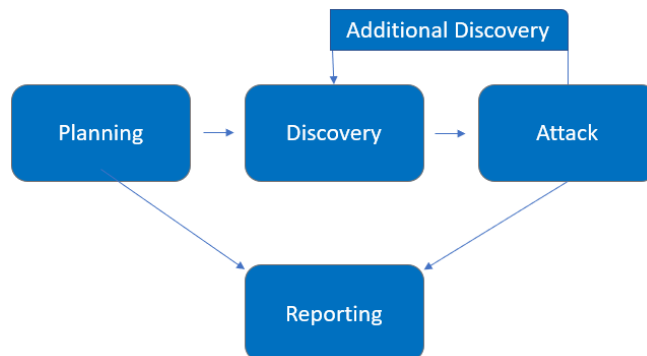
Assessment Components

Internal Penetration Test

An internal penetration test emulates the role of an attacker from the inside of a network. An engineer will scan the network to identify potential host vulnerabilities and perform common and advanced internal network attacks, such as: LLMNR/NBT-NS poisoning and other man-in-the-middle attacks, token impersonation, kerberoasting, pass-the-hash, golden ticket, and more. The engineer will seek to gain access to hosts through lateral movement, compromise domain user and admin accounts, and exfiltrate sensitive data.

Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Moderate	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

Scope

Assessment	Details
Internal Penetration Test	10.0.0.0/24

Scope Exclusions

Per client request, MAS did not perform any Denial-of-Service attacks and attacks of public facing infrastructure during testing.

Client Allowances

Demo Corp provided MAS the following allowances:

- Internal network access via a VPN connection.

Executive Summary

MAS evaluated the internal security posture of AFC-Richmond (AFCR) over the course of March 11th, 2024, to March 13th,2024. MAS was able to successfully compromise AFCR's domain controller within a day of internal testing. The following sections will first describe the techniques used by MAS to gain domain access to AFCR's internal network. It will then conclude by listing out the key strengths and weaknesses of AFCR's internal network with suggestions of possible remediations.

Testing Summary

MAS was able to gain initial footing into AFCR's internal network using Link-Local Multicast Name Resolution (LLMNR) poisoning. MAS discovered LLMNR was enabled (Finding IPT-001) and was able to capture the hash of user wonderkid. MAS took this hash offline and using a dictionary attack was able to crack wonderkid's hash with relative ease (Finding IPT-002). AFCR, to its credit, had used industry best practice of least privileges by not giving this user any administrative access on AFCR's network. This helped prevent MAS from using a pass the hash/password attack to gain further lateral or vertical movement within AFCR's internal network.

Furthermore, using the credentials of wonderkid MAS was next able to conduct a kerberoasting attack (Finding IPT-003). This attack allowed MAS to obtain the hash of service account fservice. The newly captured hash was once again taken offline and cracked using a dictionary attack, and thus further signifying AFCR's failure to enforce a strong password complexity requirement (Finding IPT-002). The credentials of fservice were able to be passed around AFCR's network and allowed MAS to gain local administrator access to computer AFC-WS-1.

The local administrative access to network computer AFC-WS-1 allowed MAS to dump additional hashes. One of the hashes MAS was able to recover from this hash dump was the hash of a local administrator account. This administrator account hash was once again successfully cracked (Finding IPT-002) and due to password reuse (Finding IPT -004) provided MAS with local admin level access to machine AFC-WS-2. The admin access to machine AFC-WS-2 allowed MAS to install mimikatz (a tool used to steal credentials), without any need for obfuscation (Finding IPT-OO5).

The execution of mimikatz on AFC-WS-2 provided MAS with the account credentials of a domain admin account stored in the credmanager as a cleartext password. The compromise of a domain admin account allowed MAS to access the domain controller. From which MAS was able to fully compromise the domain and dump the NTDS.DIT file.

MAS during the initial enumeration phase also discovered that SMB signing was disabled (Finding IPT-007). However, we were not able to leverage this vulnerability during the exploitation phase as we could not catch hashes of valuable accounts during our testing period.

MAS also discovered token impersonation was also possible in AFCR's network (Finding IPT-006). However, for similar reasons to SMB attacks we were not able to fully exploit this vulnerability due to our limited testing time frame.

Key Security Strengths and Weaknesses

The following was identified by MAS as some key internal network strengths of AFCR:

1) MAS identified that low level users were prevented from being administrators on local computers, indicating the presence of security best practice of least privileges.
2) IPV6 was disabled in the network and thus stopped MAS from using many IPV6 related exploits such as mitm6.
3) Using Nessus and Nmap, MAS was able to perform vulnerability scanning of AFCR's internal network. However, we were not able to find many patching related vulnerabilities.

The following was identified by MAS as some key internal network weaknesses of AFCR:

1) LLMNR was enabled in the network thus allowing the capture of user credentials.
2) Insufficient password complexity allowed MAS to crack captured hashes with ease.
3) Password reuse allowed for easy lateral movement within AFCR's network.
4) No alerts were triggered during engagement indicating either weak or worse no anti-virus/firewall protections.
5) Cleartext password stored in the credmanager.
6) Token impersonation was possible.
7) SMB signing was found to be disabled.

Tester Recommendations

AFCR has the bare bones of a secure network this includes some of the key strengths identified above. However, with the inclusion of the following key suggestions AFCR's network posture can be further fortified and improved upon:

1) Disable LLMNR in the network.
2) Use strong Network Access Control (NAC) and application whitelisting.
3) Enforce a stronger password complexity requirement.
4) Have unique local admin passwords.
5) Use strong anti-virus and firewall protections.
6) Make changes to GPO to prevent users from storing network passwords in the credmanager.
7) Restrict token delegation and limit user/group token creation permissions.
8) Enable SMB signing on all non-server machines on the network.
   .

Vulnerability Summary & Report Card

Finding	Severity	Recommendation
IPT-001: Insufficient LLMNR Configuration	Critical	Disable multicast name resolution via GPO.
IPT-002: Insufficient Password Complexity	Critical	Incorporate CIS Benchmark password requirements/PAM solutions.
IPT-003: Kerberoasting	Critical	Use Group Managed Service Accounts (GMSA)/Password vaulting solutions. `
IPT-004: Password Reuse	Critical	Utilize unique local admin passwords/PAM solutions.
IPT-005: Weak Anti-Virus/Firewall Protections	Critical	Incorporate a strong Anit-Virus/firewall in AFCR's network.
IPT-006: Token Impersonation	High	Restrict token delegation and limit user/group token creation permissions.
IPT-007: SMB Signing Disabled	High	Enable SMB signing on all non-server machines.
IPT-008: Steps to Domain	Informational	Review action and remediations steps.

Technical Findings

Finding IPT-001: Insufficient LLMNR Configuration (Critical)

Description:	Multicast name resolution was found to be enabled on AFC-WS-1. MAS was able to use LLMNR poisoning and using responder was able to capture the hash of user wonderkid. Wonderkid's hash was taken offline and cracked using hashcat.
Tools Used:	Responder, Hashcat
System:	10.0.0.25
References:	Stern Security - Local Network Attacks: LLMNR and NBT-NS Poisoning NIST SP800-53 r4 IA-3 - Device Identification and Authentication NIST SP800-53 r4 CM-6(1) - Configuration Settings

Evidence

Figure 1-Captured wonderkid's hash using responder.

Remediation

Disable LLMNR via GPO. Alternatively, if LLMNR is vital to the smooth functioning of the organization, then AFCR could use network access control (NAC) combined with application whitelisting as mitigation techniques.

For further guidance please refer to the MITRE guidance here.

Finding IPT-002: Insufficient Password Complexity (Critical)

Description:	MAS was able to easily crack most of the captured account hashes using dictionary attacks. The accounts whose passwords MAS was able to successfully compromise includes: wonderkid, fservice and local administrator.
Tools Used:	Hashcat, Manual Review
System:	10.0.0.25, 10.0.0.35
References:	NIST SP800-53 IA-5(1) - Authenticator Management https://www.cisecurity.org/white-papers/cis-password-policy-guide/

Evidence

Figure 2-The captured hash of service account fservice was easily cracked using a dictionary attack.

Figure 3-The hash of local admin was also easily cracked using a dictionary attack.

Remediation

MAS was only able to crack three account hashes due to time constraints. However, we strongly believe we could have cracked more hashes with a slightly altered wordlist relating to football and AFC-Richmond. Hence, we strongly recommend that AFCR incorporates CIS Benchmark password requirements/PAM solutions. Also, the organization must enforce industry best practices as it pertains to password complexity. The organization could also look at enabling password filter which will stop users from creating easily crackable passwords.

Finding IPT-003: Kerberoasting (Critical)

Description:	MAS was able to use a kerberoasting attack to obtain the hash of an AFCR service account, fservice. The hash of this account was taken offline and successfully cracked due to IPT-002.
	MAS observed that the compromised service account was not running as a domain administrator, However, the account was a local administrator on machine AFC-WS-1 which set MAS up for further attacks (IPT-004).
Tools Used:	GetUserSPNS.py, Hashcat
System:	10.0.0.25, 10.0.0.35
References:	Kerberoasting details: https://adsecurity.org/?p=2293 Group Managed Service Accounts Overview

Evidence

Figure 4-MAS was able to obtain hash of service account fservice using a kerberoasting attack.

Figure 5-The fservice account credentials gave MAS local admin access on machine AFC-WS-1.

Remediation

MAS recommends AFCR to use Group Managed Service Accounts (GMSA) for privileged service accounts. GMSA will offer additional protection to AFCR's network through ensuring that GMAS accounts' password complexity and that these accounts have their passwords changed frequently. Alternatively, AFCR could use a password vaulting solution.

MAS also recommends that AFCR use alert logging on domain controllers whenever a kerberos service ticket is requested. MAS also recommends that AFCR tailor their SIEM to alert on excessive user SPN requests.

Finding IPT-004: Local Admin Password Reuse (Critical)

Description:	MAS was able to gain easy lateral movement from machines AFC-WS-1 to AF-WS-2 due to local admin password reuse. The local administrator hash was discovered by dumping the secrets of machine AFC-WS-1 using the account credentials of fservice. The local administrator's hash was cracked due to IPT-002 from which MAS was able to RDP into AFC-WS-2(IPT-005).
Tools Used:	Secretsdump.py, Crackmapexec, Hashcat
System:	10.0.0.25, 10.0.0.35
References:	https://capec.mitre.org/data/definitions/644.html https://tcm-sec.com/pentest-tales-001-you-spent-how-much-on-security/

Evidence


```
└─# crackmapexec smb 10.0.0.0/24 -u administrator -H aad3b435b51404eeaad3b435b51404ee:9d1c55124d470f248598be547c130dc4 --local-auth
SMB     10.0.0.35    445    AFC-WS-2    [*] Windows 10.0 Build 19041 x64 (name:AFC-WS-2) (domain:AFC-WS-2) (signing:False) (SMBv1:False)
SMB     10.0.0.25    445    AFC-WS-1    [*] Windows 10.0 Build 19041 x64 (name:AFC-WS-1) (domain:AFC-WS-1) (signing:False) (SMBv1:False)
SMB     10.0.0.35    445    AFC-WS-2    [+] AFC-WS-2\administrator:9d1c55124d470f248598be547c130dc4 (Pwn3d!)
SMB     10.0.0.25    445    AFC-WS-1    [+] AFC-WS-1\administrator:9d1c55124d470f248598be547c130dc4 (Pwn3d!)
SMB     10.0.0.225   445    AFCR-DC     [*] Windows 10.0 Build 17763 x64 (name:AFCR-DC) (domain:AFCR-DC) (signing:True) (SMBv1:False)
SMB     10.0.0.225   445    AFCR-DC     [-] AFCR-DC\administrator:9d1c55124d470f248598be547c130dc4 STATUS_LOGON_FAILURE
Running CME against 256 targets ─────────────────────── 100% 0:00:00
```

Figure 4-MAS was able to able to discover that password reuse was present in the AFCR's network using crackmapexec.

Remediation

Utilize unique local admin passwords. This, consequently, will help to prevent easy lateral movements within AFCR's network such as the one achieved by MAS. AFCR should also think about incorporating PAM solutions.

Finding IPT-005: Weak Anti-Virus/Firewall Protections (Critical)

Description:	AFCR was not able to pick up any of MAS network traffic. This is indicative of a weak or worse no anti-virus and firewall protections being present in AFCR's internal network. Ultimately, a weak anti-virus/firewall presence is what lead to MAS being able to fully compromise AFCR's domain. It allowed for mimikatz to be installed on network computers from which cleartext credentials of a domain admin account stored in the credmanager were obtained.
Tools Used:	Nessus, Nmap, Mimikatz
System:	All
References:	https://attack.mitre.org/mitigations/M1049/

Evidence

Figure 5-Screenshot of mimikatz running on AFC-WS-2 and obtaining domain admin credential from the credmanager.

Figure 6-MAS was able to use the captured domain admin credentials to dump the NTDS.DIT file and compromise the domain controller completely.

Remediation

The presence of a weak anti-Virus and a weak firewall was clear from the onset of MAS's investigation period, whereby we were not notified of any scanning we were doing of AFCR's network. A good anti-virus and a strong firewall will not eliminate all security risks. However, a good anti-virus and a strong firewall at best can eliminate many of the straightforward attack vectors and at worst make it more difficult for attackers. For instance, any good anti-virus would have been easily able to pick up mimikatz running on their network. This, while would have not completely taken mimikatz out of the table, however it would have made it difficult for MAS to use without any obfuscation.

MAS also recommends that AFCR make changes to their GPOs to prevent users from storing their passwords in the credmanager. More specifically, enable the "do not allow storage of passwords and credential for network authentication" GPO.

Finding IPT-06: Token Impersonation (High)

Description:	MAS discovered that token impersonation was allowed on both AFC-WS-1 and AFC-WS-2. However, MAS was only able to impersonate tokens of accounts with local administrative privileges. This was due to MAS not being able to catch any domain admins logging into the two network computers during our short testing period.
Tools Used:	Metasploit, Incognito
System:	10.0.0.25, 10.0.0.35
References:	NIST SP800-53 r4 CM-7
	NIST SP800-53 r4 AC-6
	https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/how-to-configure- protected-accounts

Evidence

Figure 7-Successfully impersonated the token of a local admin account.

Figure 8-Shell access as a local administrator.

Remediation

AFCR should restrict token delegation and limit user/group token creation permission. For further information, please visit the following MITRE framework link here.

Finding IPT-007: SMB Signing Disabled (High)

Description:	MAS during our enumeration phase detected AFCR's non-server machines of having SMB signing disabled. However, due to time constraint MAS was not able to fully leverage this vulnerability as we could not catch any valuable account hashes during our testing period.
Tools Used:	Nessus, Nmap, Responder, NTLMRelayx
System:	10.0.0.25,10.0.0.35
References:	CIS Microsoft Windows Server 2012 R2 v2.2.0 (Page 180) https://github.com/lgandx/Responder/blob/master/tools/MultiRelay.py

Evidence

Figure 9-Using a Nmap scan MAS was able to confirm that machine AFC-WS-1 had SMB signing disabled.

Figure 10-Using a Nmap scan MAS was also able to confirm that machine AFC-WS-2 had SMB signing disabled.

Remediation

Enabling SMB signing on all non-server computers on AFCR's domain will completely stop this attack. However, if AFCR were worried about performance issues, alternatively the organization could look at disabling NTLM authentication. For further guidance please visit the following MITRE framework link here.

Finding IPT-008: Steps To Domain Admin (Informational)

The following table summarizes how MAS was able to compromise AFCR's domain:

Step	Action	Recommendation
1	Obtained user wonderkid's password hash using responder and LLMNR poisoning.	Disable LLMNR, alternatively using network access control combined with application whitelisting can help to prevent this attack.
2	Cracked user wonderkid's hash using a dictionary attack and hashcat.	Enforce a strong password complexity policy.
3	Used wonderkid's credentials to do a kerberoasting attack. From which MAS was able to gain the hash of the account fservice. MAS was able to crack this account's password using a dictionary attack.	Enforce a strong password policy.
4	Used fservice account credentials to gain the password hash of a local administrator account. MAS was able to crack this account's hash. Furthermore, due to password reuse, MAS was able to use this local administrator's credentials to move laterally and gain admin access to machine AFC-WS-2.	Use unique local administrator passwords/PAM solution.
5	With admin access to AFC-WS-2, MAS was able to install mimikatz on the machine and obtain the cleartext password of a domain admin account whose credentials were stored in the credmanager.	Implement strong anti-virus and firewall protections in AFCR's network. Also stop users from saving passwords in the credmanager. AFCR can achieve this by enabling the "do not allow storage of passwords and credential for network authentication" GPO.
6	Utilized the domain admin credentials to gain access to the domain controller and dump the NTDS.DIT file.	

Last Page