JTE SECURITY

TCM

Security Assessment Findings Report

Business Confidential

Date: Sep. 8th, 2023
Project: 123-45
Version 1.0

Table of Contents

Confidentiality Statement

This document is the property of JTE Security. This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of JTE Security.

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. TCMS prioritized the assessment to identify the weakest security controls an attacker would exploit. TCMS recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

Contact Information

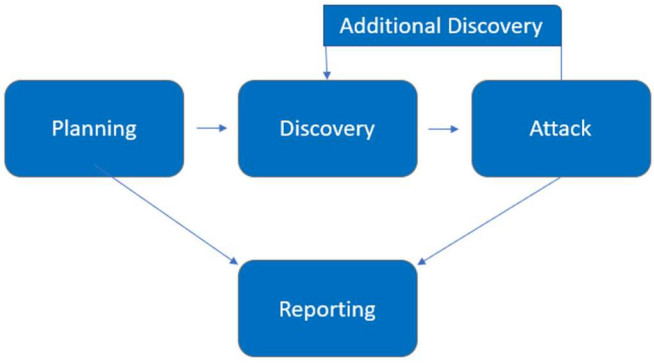
Name	Title	Contact Information
JTE Security		
Je'Shon Edwards	Lead Penetration Tester	Email: j3sh0n3dward5@gmail.com

Assessment Overview

From September 8th, 2023 to September 10th, 2023, JTE Security engaged TCM Security to evaluate the security posture of its infrastructure compared to current industry best practices that included an internal network penetration test. All testing performed is based on the NIST SP 800-115 Technical Guide to Information Security Testing and Assessment, OWASP Testing Guide (v4), and customized testing frameworks.

Phases of penetration testing activities include the following:

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



Assessment Components

Internal Penetration Test

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

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, TCMS did not perform any of the following attacks during testing:
- Denial of Service (DoS)
- Phishing/Social Engineering

All other attacks not specified above were permitted by Demo Corp.

Client Allowances

DC did not provide any allowances to assist the testing.

Executive Summary

JTES evaluated Demo Corp's internal security posture through penetration testing from September 8th, 2023, to September 10th, 2023. The following sections provide a high-level overview of vulnerabilities discovered, successful and unsuccessful attempts, and strengths and weaknesses.

Attack Summary

The steps below describe how the penetration tester obtained domain administrator access. Each step also provides remediation recommendations to help mitigate risk.

Step	Action	Recommendation
1	Poisoned LLMNR responses to obtain NetNTLMv2 hash of regular network user	Disable multicast name resolution via GPO.
2	Cracked NTLM hash offline of domain user wonderkid	Increase password complexity. Utilize multi-factor.
3	Performed a "kerberoast attack" with credentials gained from LLMNR attack which gave a domain admin and a hash for that admin account.	Use group-managed service accounts for privileged services
4	With the credentials given by the kerberoast attack performed a secretsdump attack which dumped the SAM which has hashes to all accounts and admins.	Increase password complexity for accounts.
5	Utilized discovered credentials to log into the domain controller.	

Remediation

Review action and remediation steps.

Security Strengths

SMB vulnerability scans

During the assessment, JTES had issues when scanning port 139 (SMB) tools such as smbclient / relay had blocked permission.

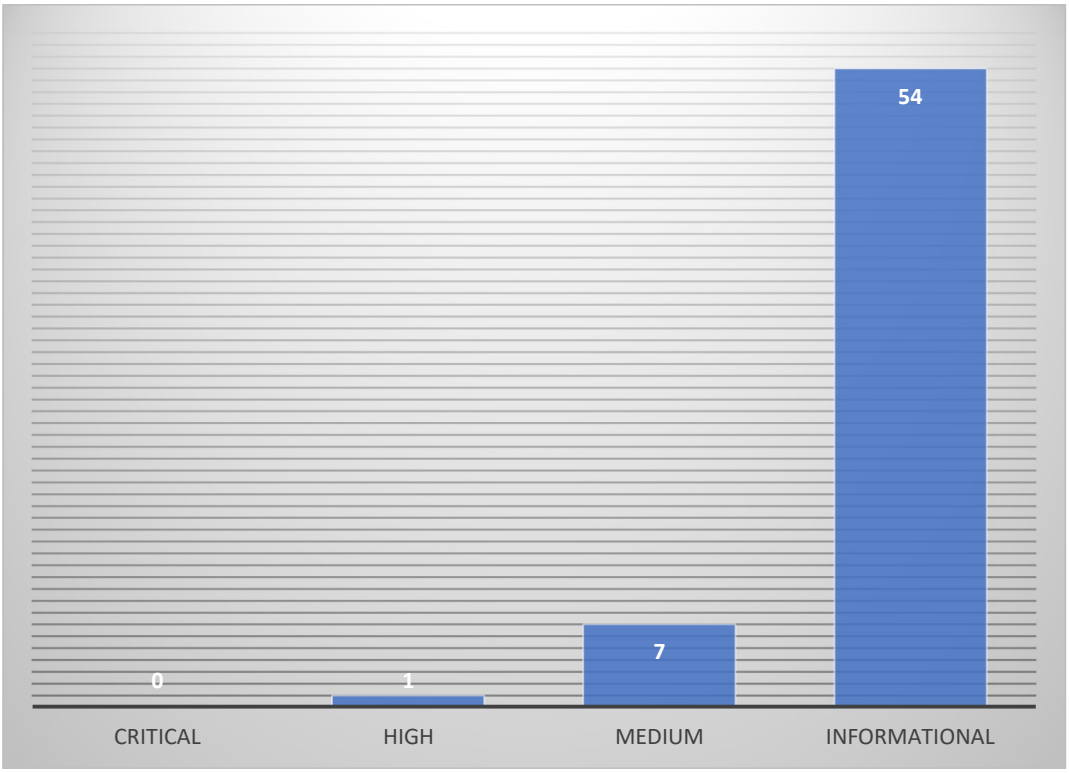
Security Weaknesses

Weak Password Policy

JTES successfully performed password guessing attacks against DC login forms, providing internal network access. A predictable password format of Password1 (basic and simple password) and Richmond! (domain name + special character) was attempted and successful.

Vulnerabilities by Impact

The following chart illustrates the vulnerabilities found by impact:



Internal Penetration Test Findings

Insufficient LLMNR Configuration (Critical)

Description:	Demo Corp allows multicast name resolution on their end-user networks. JTES captured 1 user account hashes by poisoning LLMNR traffic and cracked with commodity cracking software. The cracked accounts were used to leverage further access that led to the compromise of the Domain Controller.
Impact	Critical
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

Exploitation Proof of Concept

JTES gathered 1 user hash by running a LLMNR attack.

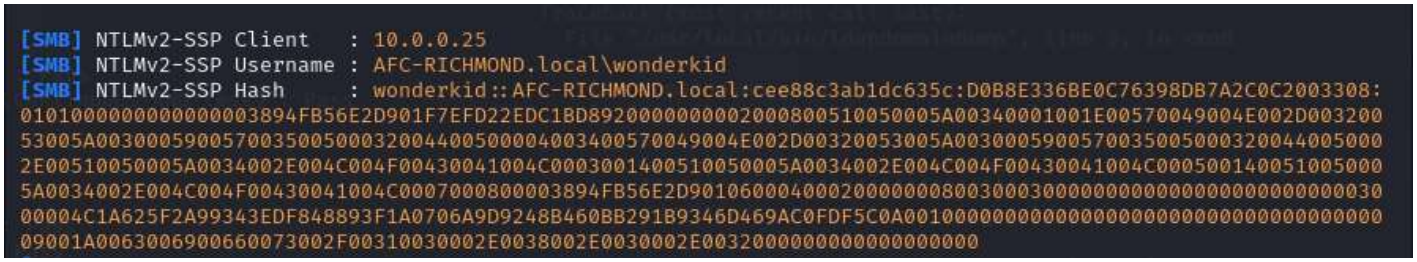


Figure 1: Captured hash of "wonderkid"

JTES used the hash given to crack that hash to use for the event of password spraying.

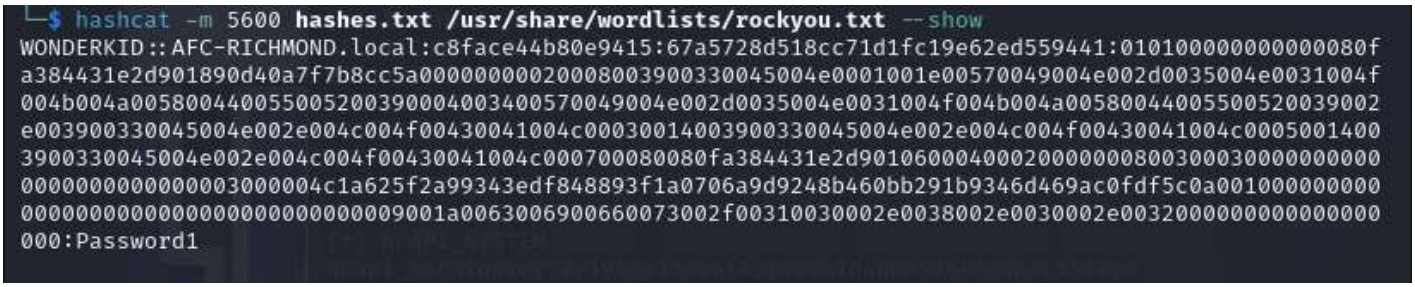


Figure 2: Cracked hash of "production"

JTES gathered furthermore information due to the password given. After running a “password attack” the ip address of the domain was given.

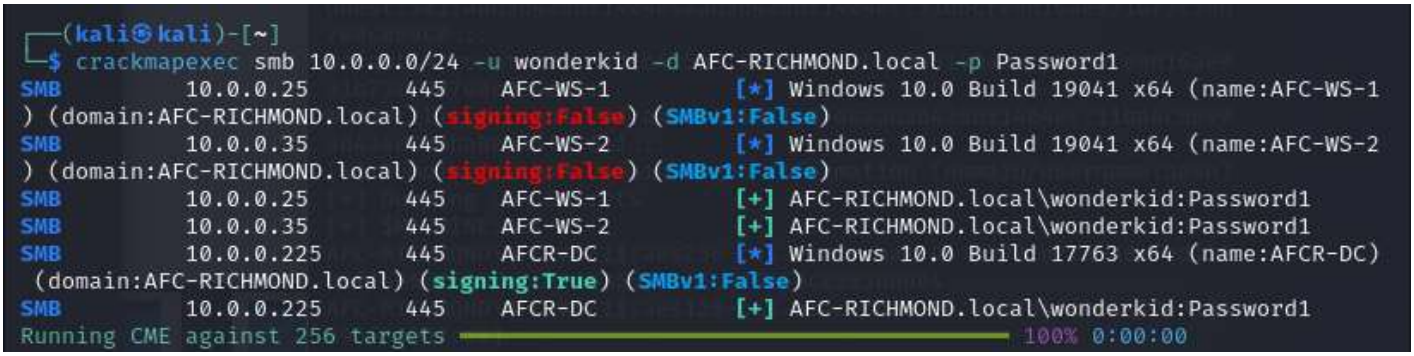


Figure 3: Domain ip given (10.0.0.25)

The ability to perform a keberoast attack in hopes of gaining a domain admin’s credentials, was successful and a domain admin has been compromised.

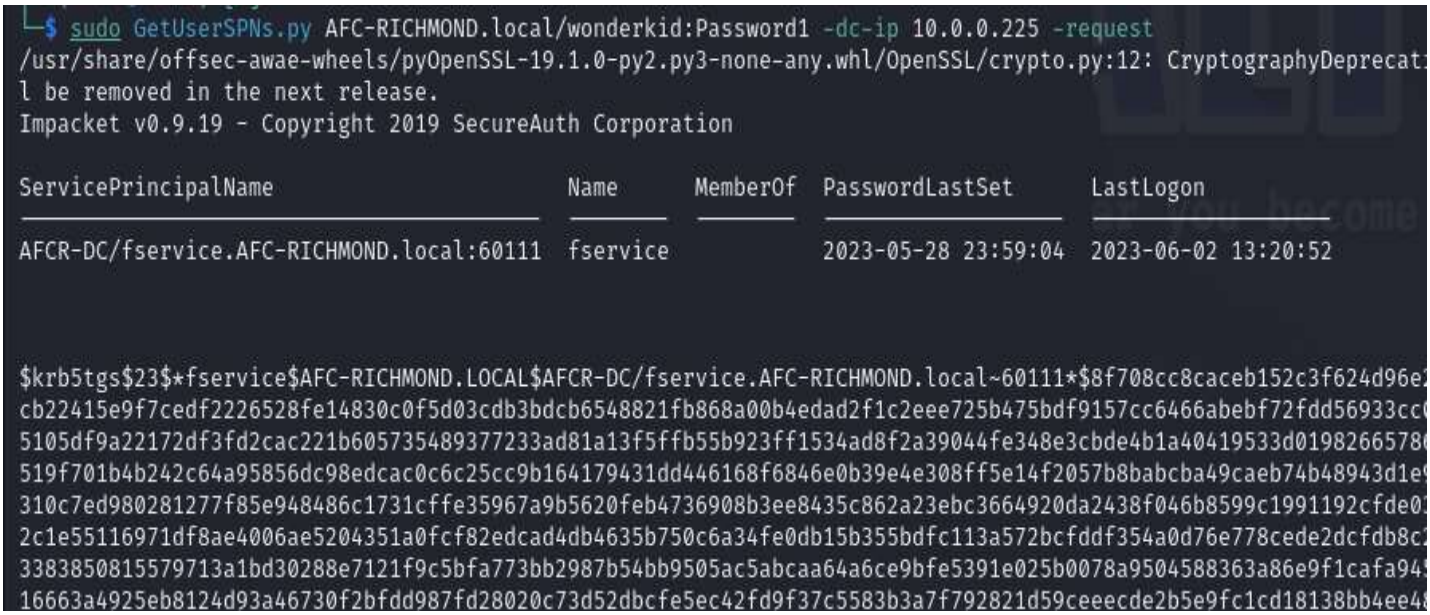


Figure 4: Domain User and hash given

With the Domain Admins credentials given JTES was able to perform an attack to dump hashes of the SAM.

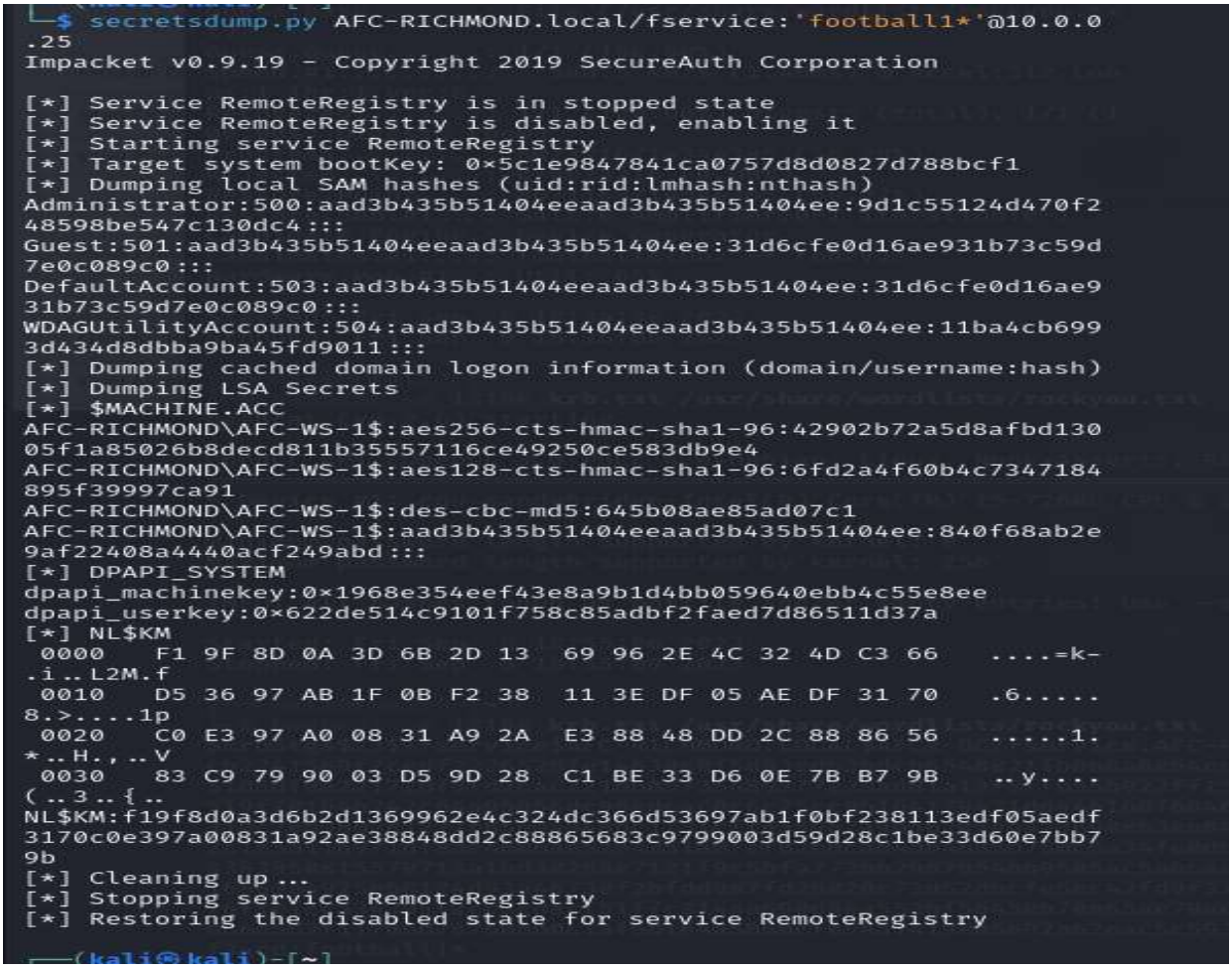


Figure 4: SAM dumped.

JTES was able to capture administrator passwords and hashes which leads to the dumping of the NTDS.dit and the Domain being compromised.

Insufficient LLMNR Configuration (Critical)

Description:	TCM allows multicast name resolution on their end-user networks. JTES captured a user account hashes by poisoning LLMNR traffic and cracked with commodity cracking software. The cracked accounts were used to leverage further access that led to the compromise of the Domain Controller.
Risk:	Likelihood: High – This attack is effective in environments allowing multicast name resolution. Impact: Very High – LLMNR poisoning permits attackers to capture password hashes to either crack offline or relay in real-time and pivot laterally in the environment.
System:	10.0.0.25
Tools Used:	Responder, Hashcat
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 hash of "wonderkid"

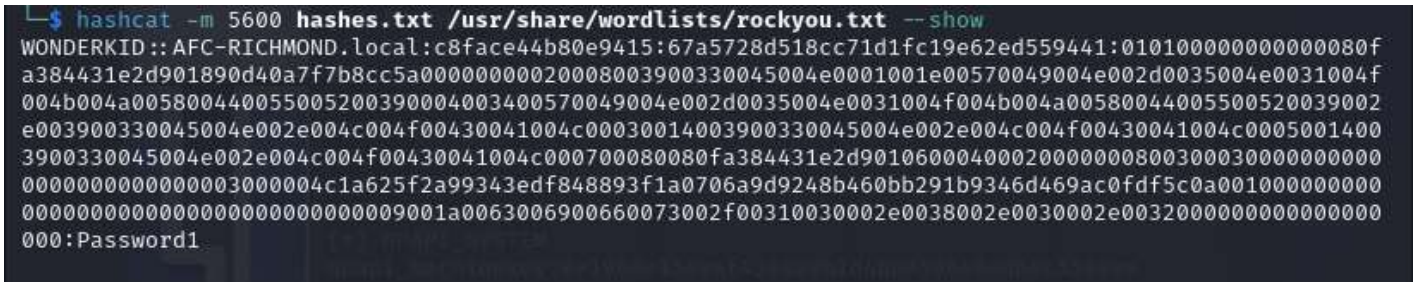


Figure 2: Cracked hash of "wonderkid"

Remediation

Disable multicast name resolution via GPO.

The cracked hashes demonstrate a deficient password complexity policy. If multicast name resolution is required, Network Access Control (NAC) combined with application whitelisting can limit these attacks.

Insufficient Password Complexity (Critical)

Description:	JTES dumped hashes from the domain controller and proceeded to attempt common password guessing attacks against all users. JTES cracked # passwords using basic password list guessing attacks and low effort brute forcing attacks. 2 cracked accounts had domain administrator rights.
Risk:	Likelihood: High - Simple passwords are susceptible to password cracking attacks. Encryption provides some protection, but dictionary attacks base on common word lists often crack weak passwords. Impact: Very High - Domain admin accounts with weak passwords could lead to an adversary critically impacting Demo Corp ability to operate.
System:	10.0.0.225
Tools Used:	Manual Review
References:	NIST SP800-53 IA-5(1) - Authenticator Management https://www.cisecurity.org/white-papers/cis-password-policy-guide/

Evidence

```
└─$ secretsdump.py AFC-RICHMOND.local/fservice:'football1*'@10.0.0
.25
Impacket v0.9.19 - Copyright 2019 SecureAuth Corporation

[*] Service RemoteRegistry is in stopped state
[*] Service RemoteRegistry is disabled, enabling it
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x5c1e9847841ca0757d8d0827d788bcf1
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:9d1c55124d470f2
48598be547c130dc4:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d
7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae9
31b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:11ba4cb699
3d434d8dbba9ba45fd9011:::
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
AFC-RICHMOND\AFC-WS-1$:aes256-cts-hmac-sha1-96:42902b72a5d8afbd130
05f1a85026b8decd811b35557116ce49250ce583db9e4
AFC-RICHMOND\AFC-WS-1$:aes128-cts-hmac-sha1-96:6fd2a4f60b4c7347184
895f39997ca91
AFC-RICHMOND\AFC-WS-1$:des-cbc-md5:645b08ae85ad07c1
AFC-RICHMOND\AFC-WS-1$:aad3b435b51404eeaad3b435b51404ee:840f68ab2e
9af22408a4440acf249abd:::
[*] DPAPI_SYSTEM
dpapi_machinekey:0x1968e354eef43e8a9b1d4bb059640ebb4c55e8ee
dpapi_userkey:0x622de514c9101f758c85adbf2faed7d86511d37a
[*] NL$KM
 0000   F1 9F 8D 0A 3D 6B 2D 13  69 96 2E 4C 32 4D C3 66   ....=k-
.i..L2M.f
 0010   D5 36 97 AB 1F 0B F2 38  11 3E DF 05 AE DF 31 70   .6.....
8.>....1p
 0020   C0 E3 97 A0 08 31 A9 2A  E3 88 48 DD 2C 88 86 56   .....1.
*..H.,..V
 0030   83 C9 79 90 03 D5 9D 28  C1 BE 33 D6 0E 7B B7 9B   ..y....
(..3..{..
NL$KM:f19f8d0a3d6b2d1369962e4c324dc366d53697ab1f0bf238113edf05aedf
3170c0e397a00831a92ae38848dd2c88865683c9799003d59d28c1be33d60e7bb7
9b
```

Figure 7: Excerpt of cracked domain hashes

Remediation

Implement CIS Benchmark password requirements / PAM solution. TCMS recommends that Demo Corp enforce industry best practices around password complexity and management. A password filter to prevent users from using common and easily guessable passwords is also recommended. Additionally, TCMS recommends that Demo Corp enforce stricter password requirements for Domain Administrator and other sensitive accounts.

Insufficient Privileged Account Management – Kerberoasting (High)

Description:	TCMS retrieved all user service principal names (SPNs) from the Demo Corp domain controller using a domain user-level account (IPT-001) in a Kerberoasting attack. Retrieving these user SPNs permitted TCMS to crack 4 account passwords. No service accounts were observed running as domain administrators. User accounts were observed running as a service, which is not best practice.
Risk:	Likelihood: High – Any account joined to the domain can request user SPNs. Impact: High – Using SPNs, it is possible to retrieve sensitive account password hashes and crack them offline.
Tools Used:	Impacket, Hashcat
References:	Kerberoasting details: https://adsecurity.org/?p=2293 Group Managed Service Accounts Overview

Evidence

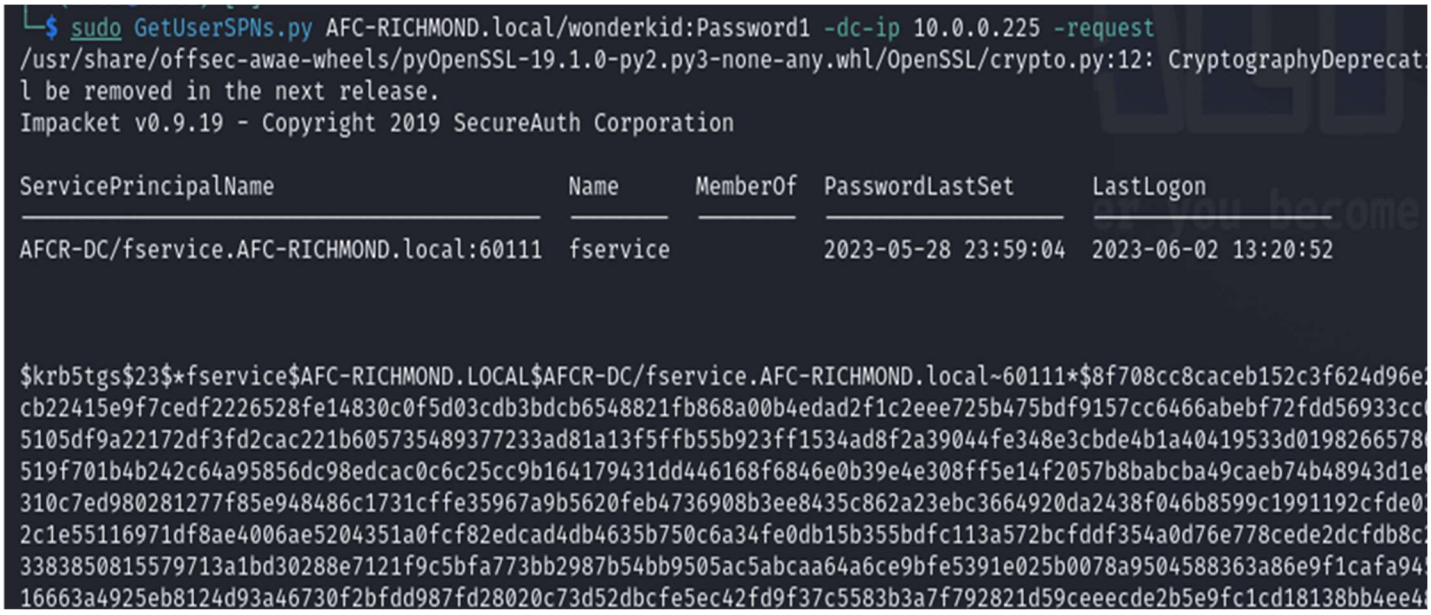


Figure 14: Cracked service accounts

Remediation

Use Group Managed Service Accounts (GMSA) for privileged services. GMSA accounts can be used to ensure passwords are long, complex, and change frequently. Where GMSA is not applicable, protect accounts by utilizing a password vaulting solution.

TCMS recommends configuring alert logging on domain controllers for Windows event ID 4769 whenever requesting a Kerberos service ticket. These alerts are prone to high false-positive rates but are a supplementary detective control. Tailor a security information and event management tool (SIEM) to alert on excessive user SPN requests.

JTE SECURITY

Last Page