Resonance CyberSentinel

Uncovering Vulnerabilities, Fortifying Your Defense

BIGWIN-DEMO LLC
Security Assessment Finding Report

Business Confidential s

Date: July 31st, 2023
Project: Internal Penetration Testing
Version 1.0

Table of Contents

Confidentiality Statement

This document is the sole property of BIGWIN-DEMO LLC and Resonance CyberSentinel (RCS) and contains proprietary and confidential information. Any duplication, redistribution, or use of this document, whether in whole or in part and in any format, requires the approval of both BIGWIN-DEMO LLC and RCS. BIGWIN-DEMO LLC may share this document with auditors under non-disclosure agreements to demonstrate compliance with penetration testing requirements.

Disclaimer

A penetration test represents a specific point in time. All findings and recommendations are based on the information collected during the assessment period and do not account for any changes or modifications made after the completion of the assessment. Due to the limited timeframe of the engagement, not all security controls can be fully evaluated. Experts at RCS focused on identifying the most vulnerable security controls that an attacker might target and exploit. RCS advises conducting similar assessments annually, whether by internal teams or third-party assessors, to ensure the ongoing effectiveness of these controls.

Contact Information

Name	Tittle	Contact Information
Resonance CyberSentinel		
Annor Sylvester	Senior Security Assessor	Email: Asylvester@rc-sentinel.com
BIGWIN-DEMO LLC		
Martin Duke	CISO	Email: mduke@bigwin-demo.com

Assessment Overview

From July 15th, 2024, to July 26th, 2024, BIGWIN-DEMO LLC enlisted Resonance CyberSentinel (RCS) to assess the security posture of its infrastructure in relation to current industry best practices, including an internal network penetration test. All testing was conducted following the NIST SP 800-115 Technical Guide to Information Security Testing and Assessment, the OWASP Testing Guide (v4), and customized testing frameworks.
The phases of the penetration testing activities included:

- **Planning**: Gathering customer goals and establishing the rules of engagement.
- **Discovery**: Scanning and enumerating to identify potential vulnerabilities, weaknesses, and exploits.
- **Attack**: Confirming potential vulnerabilities through exploitation and conducting further discovery upon gaining a foothold in the customer's environment.
- **Reporting**: Documenting all identified vulnerabilities and exploits, failed attempts, and evaluating the company's strengths and weaknesses.

Assessment Components

Internal Penetration Test

An internal penetration test simulates the actions of an attacker operating within the network. RCS experts scan the network to identify potential vulnerabilities within hosts. Our experts conduct both standard and sophisticated internal network attacks, such as LLMNR/NBT-NS poisoning, other man-in-the-middle attacks, token impersonation, kerberoasting, pass-the-hash, golden ticket attacks, AD CS attacks, and many more.

Finding Severity Ratings

The table below outlines the severity levels and associated CVSS score ranges used throughout this document to evaluate vulnerability and risk impact.

Severity	CVSS V3 Score Range	Definition
Critical	9.0 -10.0	Exploitation is relatively simple and typically leads to a system-level breach. Immediate action planning and patching are strongly recommended.
High	7.0-8.9	Exploitation is more challenging but could result in elevated privileges and potentially lead to data loss or system downtime. It is recommended to develop an action plan and apply patches as soon as possible.
Moderate	4.0-6.9	Vulnerabilities are present but either cannot be exploited directly or require additional efforts, like social engineering, to be exploited. It is recommended to develop a plan of action and address these after higher-priority issues have been resolved.
Low	0.1-3.9	The vulnerabilities cannot be exploited but addressing them would minimize the organization's attack surface. It is recommended to create a plan of action and apply patches during the next maintenance window.
Informational	N/A	No vulnerabilities were found. The report includes observations made during testing, notes on strong controls, and additional documentation for reference.

Risk Factors

Risk is measured by (i) Likelihood, and (ii) Impact;

Likelihood

Likelihood assesses the probability of a vulnerability being exploited. Ratings are determined by considering factors such as the complexity of the attack, the tools at the attacker's disposal, the skill level of the attacker, and the environment of the client.

Impact

Impact evaluates how a vulnerability might affect operations, encompassing aspects such as the confidentiality, integrity, and availability of client systems and data, as well as potential reputational damage and financial losses.

Scope

Assessment	Details
Internal Penetration Test (IPT)	**10.x.x.x/16**

Scope Exclusions

Following the ROE, RCS did not perform the listed attacks below during the assessment:

- Denial of Service (DoS)
- Social Engineering
-

BIGWIN-DEMO LLC permitted RCS to perform all other attacks not specified in the ROE.

Client Allowances

The following allowances were provided by BIGWIN-DEMO LLC to RCS during the assessment:

- Access to BIGWIN-DEMO LLC network via (i) Dropbox, (ii) Port
- Access to the client's building

Executive Summary

RCS assessed BIGWIN-DEMO LLC's internal security posture by conducting penetration testing from July 15th, 2024, to July 26th, 2024. The sections below offer a summary of the vulnerabilities identified, detailing both successful and unsuccessful attempts, as well as the strengths and weaknesses observed during the assessment.

Scoping and Time Limitations

The scope of the engagement restricted the use of denial of service (DoS attacks) and social engineering tactics across all testing components. Additionally, there were time constraints on the testing process, with internal network penetration testing allowed for 10 business days that is July 15th, 2024, to July 26th, 2024.

Testing Summary

The network assessment looked at BIGWIN-DEMO LLC's internal network security posture. Internally, the RCS team scanned allowed BIGWIN-DEMO LLC's IPs per the ROE for vulnerabilities to assess network patching health. The team leveraged typical Active Directory exploits, including Link-Local Multicast Name Resolution (LLMNR) Poisoning, SMB relaying, IPv6 man-in-the-middle relaying, and Kerberoasting. Experts at RCS assessed the network's security posture by evaluating various risks, including open file sharing, default credentials, and sensitive information disclosure, in addition to vulnerability scanning and Active Directory attacks.

The RCS team determined that LLMNR was enabled in the network (Finding IPT-001), allowing for interception of user hashes through LLMNR poisoning. The hashes were cracked using dictionary attacks, indicating a weak password policy (Finding IPT-002). The RCS team used cracked passwords to gain access to many network workstations, indicating overly permissive user account settings.

RCS leveraged machine access and observed a local administrator account password stored cleartext in memory (Finding IPT-004) in the client's environment because WDigest was enabled, the RCS team used Mimikatz to extract cleartext credentials for the account.
The team was also able to extract local account hashes from each system probed by leveraging the compromised local administrator's credentials. The RCS team identified that local admin account hashes were

being reused between devices (Finding IPT-006), allowing for additional machine access via pass-the-hash attacks.

The RCS team used Mimikatz and other Impacket tools to dump hashes from compromised machines which allowed the RCS team to move laterally within the client's network, and later discover a machine that had been accessed by a Domain Administrator account (SQ_LService) which RCS team was able to crack its password hash indicating weak password policy (IPT-002). The testing team used this credential to gain access to the domain controller, compromising the entire domain. Refer to Finding IPT-011 for a detailed guide on how to reach Domain Admin.

The RCS team discovered that users could be impersonated through delegation attacks (Finding IPT-005), SMB relay attacks were possible due to disabled SMB signing (Finding IPT-005), and IPv6 traffic was not restricted, potentially leading to LDAPS relay and domain compromise.

The remaining findings were classified as high, moderate, low, or informational. Refer to the Technical Findings section for more details on the findings.

Tester Notes and Recommendations

The BIGWIN-DEMO LLC network's testing results indicate that the organization is conducting its first penetration test. The found vulnerabilities in Active Directory include LLMNR, IPv6, SMB disable on endpoint, and Kerberoasting, which are enabled by default.

Two things stood out during testing: a weak password policy and over permissive user account. Attackers often leverage weak password policies to gain access to a network, resulting in first-account compromises. Using standard dictionary attacks, our testing team discovered a weak password policy by cracking over 1,200 user accounts, including 24 Domain Administrator credentials.

BIGWIN-DEMO LLC is advised to review its password policy and consider requiring 15 or more characters for regular user accounts and 30 or more for Domain Administrator accounts. RCS team recommended that BIGWIN-DEMO LLC consider password blacklisting and provide a list of broken user passwords for the team to analyze. Finally, consider Privilege Access Management solutions (Privilege Account Tiering).
Overly permissive user accounts including local administrator compromised numerous devices on the network.

On the bright side, the RCS testing team raised many alerts during the engagement. The BIGWIN-DEMO LLC Security Operations team detected our vulnerability scans and warned us when we launched loud assaults on a compromised system. Although not all attacks were identified during testing, these notifications are a good start. The BIGWIN-DEMO LLC Security Operations team also detected when the RCS team created a domain administrator account and when the RCS team accessed machines with a specific domain administrator account (Honey Pot account). The technical results section includes additional recommendations on alerting and detection as needed.

Overall, the BIGWIN-DEMO LLC network behaved as anticipated for its initial penetration test. We recommend that the BIGWIN-DEMO LLC team evaluate the report's recommendations, mitigate discovered vulnerabilities, and re-test annually to strengthen their internal security posture.

Key Strengths and Weaknesses

The following identifies the key strengths demonstrated by the BIGWIN-DEMO LLC team during the assessment:

1. Observed some scanning of common enumeration tools (Nessus)
2. Mimikatz detected on some machines
3. BIGWIN-DEMO LLC uses up-to-date operating systems

Below are key weaknesses the RCS team observed during the assessment:

1. Service accounts were running as domain administrators
2. LLMNR is enabled within the network
3. IPv6 is improperly managed within the network
4. Service accounts utilized weak passwords
5. Password policy found to be insufficient
6. SMB signing is disabled on all non-server devices in the work
7. User accounts can be impersonated through token delegation
8. Domain administrators utilized weak passwords
9. WDigest was enabled on Up-to-date operating systems (Windows 10)
10. Local admin accounts had password re-use and were overly permissive
11. Vulnerable certificate Template

Vulnerability Summary & Report Card

The tables below highlight the identified vulnerabilities based on their impact and suggest corresponding remediation measures.

Critical	High	Moderate	Low	Informational
6	3	2	0	1

Findings	Severity	Recommendation
Internal Penetration Test		
IPT-001: Misconfigure LLMNR	Critical	Leverage GPO to disable multicast name resolution
IPT-002: Security Misconfiguration - IPv6	Critical	Restrict DHCPv6 traffic and incoming router advertisements in Windows Firewall via GPO
IPT-003: Insufficient Password Complexity	Critical	Implement CIS Benchmark password requirements / PAM solution.
IPT-004: Security Misconfiguration: WDigest enabled	Critical	Leverage GPO to disable WDigest
IPT-005: Insufficient Hardening – SMB Signing Disabled/ Enabled but Not Enforced	Critical	Enable and enforce SMB signing on all domain computers.
IPT-006: Security Misconfiguration – Local Admin Password Reuse	Critical	Utilize unique local admin passwords and limit local admin users via least privilege.
IPT-007: Insufficient Hardening – Token Impersonation	Critical	Restrict token delegation.
IPT-008: Insufficient Privileged Account Management – Kerberoasting	High	Leverage Group Managed Service Accounts (GMSA) for privileged services.
IPT-009: Insufficient Patch Management – SMBv1	Moderate	Upgrade to SMBv3 and apply latest patching.
IPT-010: Vulnerable certificate template (ESC4)	Moderate	Configure template not to grant users "Full Control"
IPT-011: Steps to Domain Admin	Informational	Review actions, and remediation steps

Technical Findings

Internal Penetration Testing Findings

Finding IPT-001: Misconfigured LLMNR (Critical)

Description:	BIGWIN-DEMO LLC enables multicast name resolution on their end-user networks. RCS experts intercepted LLMNR traffic and collected 34 user account hashes, successfully cracking four of them using standard cracking software. These cracked accounts were then used to gain further access, ultimately leading to the compromise of the Domain Controller.
Risk:	Likelihood: High – This attack is highly effective in environments that allows multicast name resolution. Impact: Very High – LLMNR poisoning enables attackers to capture password hashes, which can be cracked offline or used in real-time to relay and move laterally within the environment.
Systems:	All
Tool Leveraged:	Responder, Hashcat, John-The-Riper
Reference:	https://www.sternsecurity.com/blog/local-network-attacks-llmnr-and-nbt-ns-poisoning - Local Network Attacks: LLMNR and NBT-NS Poisoning https://nvd.nist.gov/800-53/Rev4/control/CM-6 - enhancement-1 – Configuration Settings

Artifacts:

Remediation
Use distinct local admin passwords. Restrict local admin accounts by applying the principle of least privilege. Consider adopting a PAM solution. For comprehensive mitigation and detection recommendations, refer to the MITRE guidelines Here.

The cracked hashes indicate a weak password complexity policy. If multicast name resolution is necessary, implementing Network Access Control (NAC) along with application whitelisting can help mitigate these attacks.

Finding IPT-002: Security Misconfiguration - IPv6 (Critical)

Description:	The TCMS team successfully relayed credentials to the Demo Corp domain controller using IPv6 DNS poisoning.
Risk:	Likelihood: High – IPv6 is typically enabled by default on Windows networks, and the tools and techniques needed for this attack are simple. Impact: Very High – If successful, an attacker could obtain domain administrator access.
Systems:	All
Tools Leveraged:	Impacket, MITM6
References:	MITM6

Artifacts:

Remediation

1. IPv6 poisoning exploits the fact that Windows still queries for an IPv6 address even in IPv4-only environments. If IPv6 is not used internally, the safest way to prevent mitm6 attacks is to block DHCPv6 traffic and incoming router advertisements in Windows Firewall through Group Policy. Disabling IPv6 completely may cause unwanted issues. To stop the attack, modify the following predefined rules to Block instead of Allow:
    a) (Inbound) Core Networking - Dynamic Host Configuration Protocol for IPv6 (DHCPV6-In)
    b) (Inbound) Core Networking - Router Advertisement (ICMPv6-In)
    c) (Outbound) Core Networking - Dynamic Host Configuration Protocol for IPv6 (DHCPV6-Out)
2. If WPAD is not used internally, disable it via Group Policy and stop the WinHttpAutoProxySvc service.
3. To mitigate relaying to LDAP and LDAPS, enable both LDAP signing and LDAP channel binding. Consider adding administrative users to the Protected Users group or marking their accounts as "Sensitive and cannot be delegated" to prevent impersonation through delegation.

IPT-003: Insufficient Password Complexity (Critical)

Description:	The RCS team extracted hashes from the domain controller and initiated common password guessing attacks on all users. They successfully cracked 1,200 passwords using simple password lists and minimal brute-force techniques. Among these, 24 accounts had domain administrator privileges.
Risk:	Likelihood: High – Weak passwords are vulnerable to cracking attempts. While encryption offers some defense, dictionary attacks using common word lists can often break weak passwords. Impact: Very High – Domain administrator accounts with weak passwords could allow an attacker to severely compromise Demo Corp's operations.
Systems:	All
Tools Leveraged:	Manual Review
References:	CIS Password policy guide NIST SP800-53 IA-5(1)_ Authenticator Management

Artifacts:

ACCOUNT	PASSWORD
ste[redacted]	Pa[redacted]
ma[redacted]	Jes[redacted]123
larr[redacted]	Sp[redacted]
lind[redacted]ner	Wi[redacted]
kwa[redacted]	Pa[redacted]
bry[redacted]s	Le[redacted]
SQl[redacted]	MY[redacted]23#

Remediation

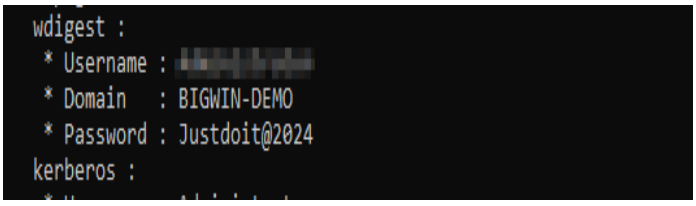
Implement CIS Benchmark password requirements or a Privileged access management (PAM) solution. RCS advises BIGWIN-DEMO LLC to adopt industry best practices for password complexity and management. It is also recommended to use a password filter to prevent users from choosing common or easily guessable

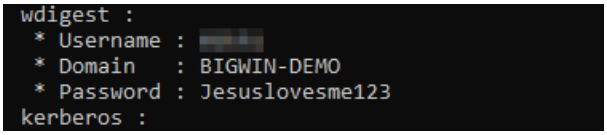
passwords. Furthermore, RCS suggests enforcing stricter password policies for Domain Administrators and other high-risk accounts.

Finding IPT-004: Security Misconfiguration- WDigest Enabled (Critical)

Description:	BIGWIN-DEMO LLC enable WDigest on some systems even though these systems are up-to-date system and WDigest is not enabled on them by default. WDigest stores the passwords of all logged-in users in clear text. The RCS team used the access obtained from IPT-001 and IPT-006 to move laterally through the network until they found a machine with Domain Admin credentials stored in WDigest.
Risk:	Likelihood: Moderate – This attack is effective in networks running outdated operating systems. Impact: Very High – WDigest stores credentials in clear text, allowing the theft of sensitive accounts, including Domain Administrator accounts.
Systems:	Four up-to-date operating systems (Windows 10)
Tools Leveraged:	Metasploit (load Kiwi), Mimikatz
References:	WDigest Security Risk Cleartext Password From Windows Memory

Artifacts:





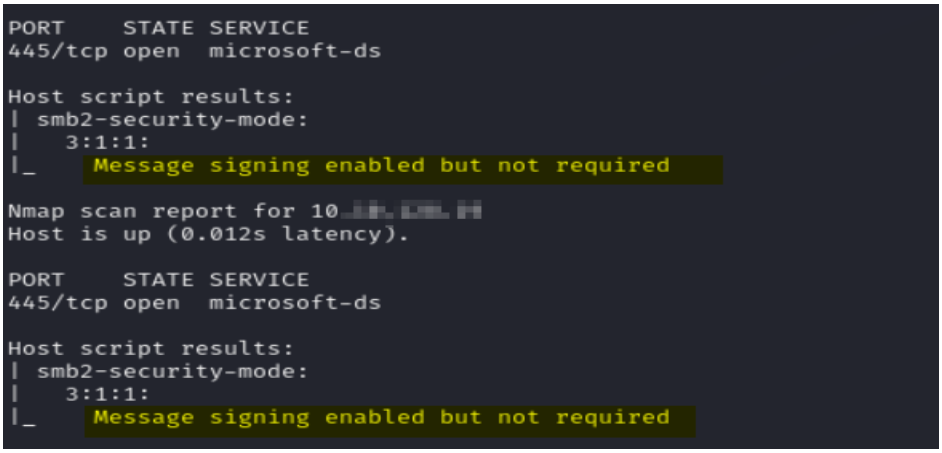
Remediation

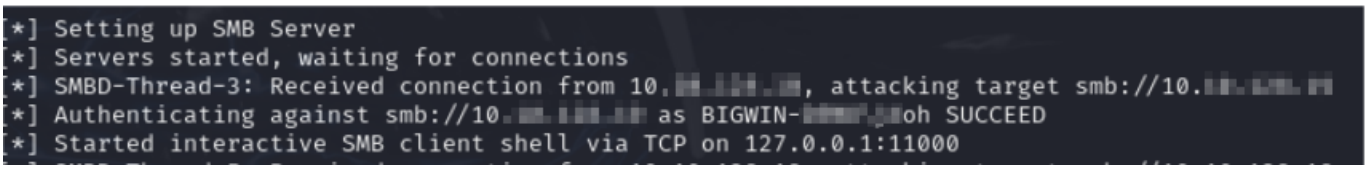
Leverage GPO to disable WDigest in the environment. Leverage Here for full detection and mitigation guidance.

Finding IPT-005: Insufficient Hardening - SMB Signing Disabled/Not Reinforced (Critical)

Description:	Demo Corp did not implement SMB signing on several devices. This omission could expose the network to SMB relay attacks, allowing attackers to gain system-level access without needing user passwords.
Risk:	Likelihood: High – Relaying password hashes is a straightforward technique that doesn't require offline cracking. Impact: High – If successfully exploited, an attacker can achieve code execution, enabling lateral movement throughout the network.
Systems:	RCS identified 619 hosts, attached is a list of identified hosts. (File Removed)
Tools Leveraged:	Nmap, Nessus, Responder, MultiRelay
References:	SMB Signing https://www.tenable.com/plugins/nessus/57608

Artifacts:





Remediation

Enable SMB signing on all domain computers at BIGWIN-DEMO LLC. If SMB signing causes performance issues, an alternative approach is to disable NTLM authentication, enforce account tiering, and limit the number of local admin users to help mitigate attacks. For comprehensive mitigation and detection strategies, refer to the MITRE guidance Here.

Finding IPT-006: Security Misconfiguration – Local Admin Password Reuse (Critical)

Description:	RCS team used local administrator hashes to access other machines in the network through a "pass-the-hash" attack. These hashes were obtained via access to machine IPT-001, which was compromised using a cracked account. Pass-the-hash attacks allow login without needing the account's password, so reusing the same local admin password (and hash) across multiple machines grants access to those systems. Using this method, RCS gained access to approximately 50 machines in the main office, leading to further account compromises and eventually the domain controller.
Risk:	Likelihood: High – This attack is highly effective in large networks where local admin passwords are reused. Impact: Very High – Pass-the-hash enables an attacker to move laterally and escalate privileges across the network.
System:	All
Tool Leveraged:	Crackmapexec, Impacket
References:	https://www.semperis.com/blog/how-to-defend-against-pass-the-hash-attack/ Relay Attack - TCM Security Pass The Hash

Artifacts:

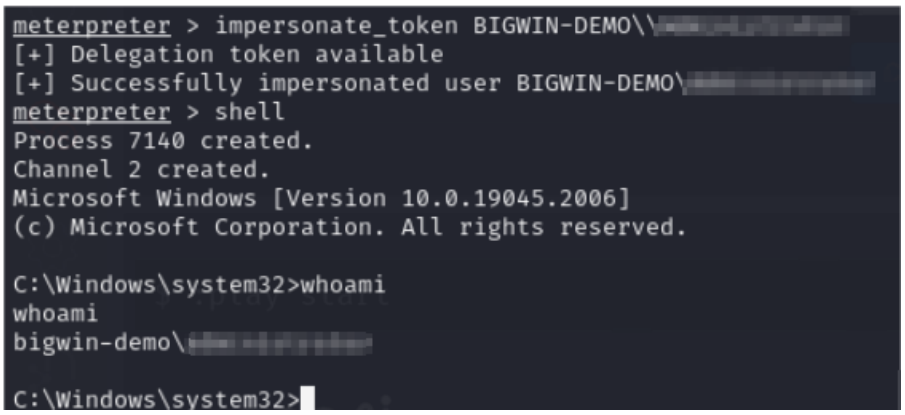
Remediation

Use unique passwords for local admin accounts and limit local admin users by following the principle of least privilege. Consider implementing a PAM solution. For detailed mitigation and detection strategies, refer to the MITRE guidance Here.

Finding IPT-007: Insufficient Hardening – Token Impersonation (Critical)

Description:	The RCS impersonated the token of "martinduke" to obtain Domain Administrator privileges
Risk:	Likelihood: High – The RCS team was able to view and impersonate tokens using open-source tools. Impact: Very High – If successfully exploited, an attacker could obtain domain administrator access.
System	All
Tool Leveraged:	Metasploit (Kiwi), Mimikatz (Incognito)
References:	NIST SP800-53 - Access Control Protection Accounts Configuration

Artifacts:



Remediation

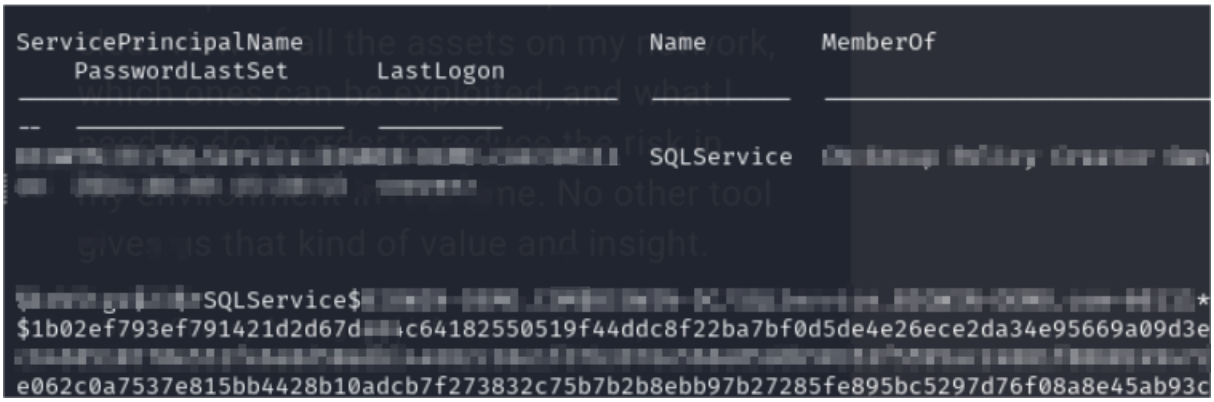
Restrict token delegation. For comprehensive mitigation and detection strategies, refer to the MITRE guidance

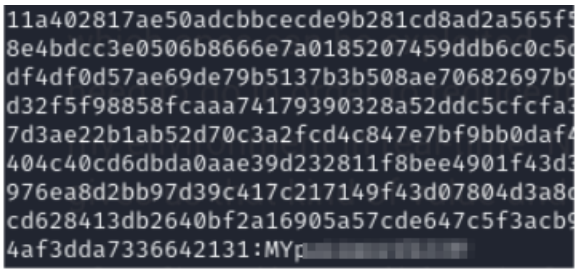
Here.

Finding IPT-008: Insufficient Privileged Account Management – Kerberoasting (High)

Description:	In the Kerberoasting attack, the RCS team used a domain user-level account (IPT-001) to retrieve user service principal names (SPNs) from the BIGWIN-DEMO LLC domain controller. This allowed TCMS to crack the passwords of four accounts. Service account was found running with domain administrator privileges	
Risk:	Likelihood: High – Any domain-joined account can request user SPNs. Impact: High – SPNs can be used to obtain sensitive account password hashes, which can then be cracked offline.	
Tool Leveraged:	Hashcat, John the Ripper, Impacket	
References:	Keberoasting	

Artifacts:





Remediation

Use Group Managed Service Accounts (GMSA) for privileged services, as they ensure passwords are long, complex, and frequently updated. If GMSA is inapplicable, use a password vaulting solution to protect accounts. The RCS team also recommends setting up alert logging on domain controllers for Windows event ID 4769, which will triggered when a Kerberos service ticket is requested. Although these alerts may generate many false positives, they serve as an additional detection measure. Additionally, a security information and event management (SIEM) tool should be configured to alert users of excessive SPN requests.

Finding IPT-009: Insufficient Patch Management – SMBv1 (Moderate)

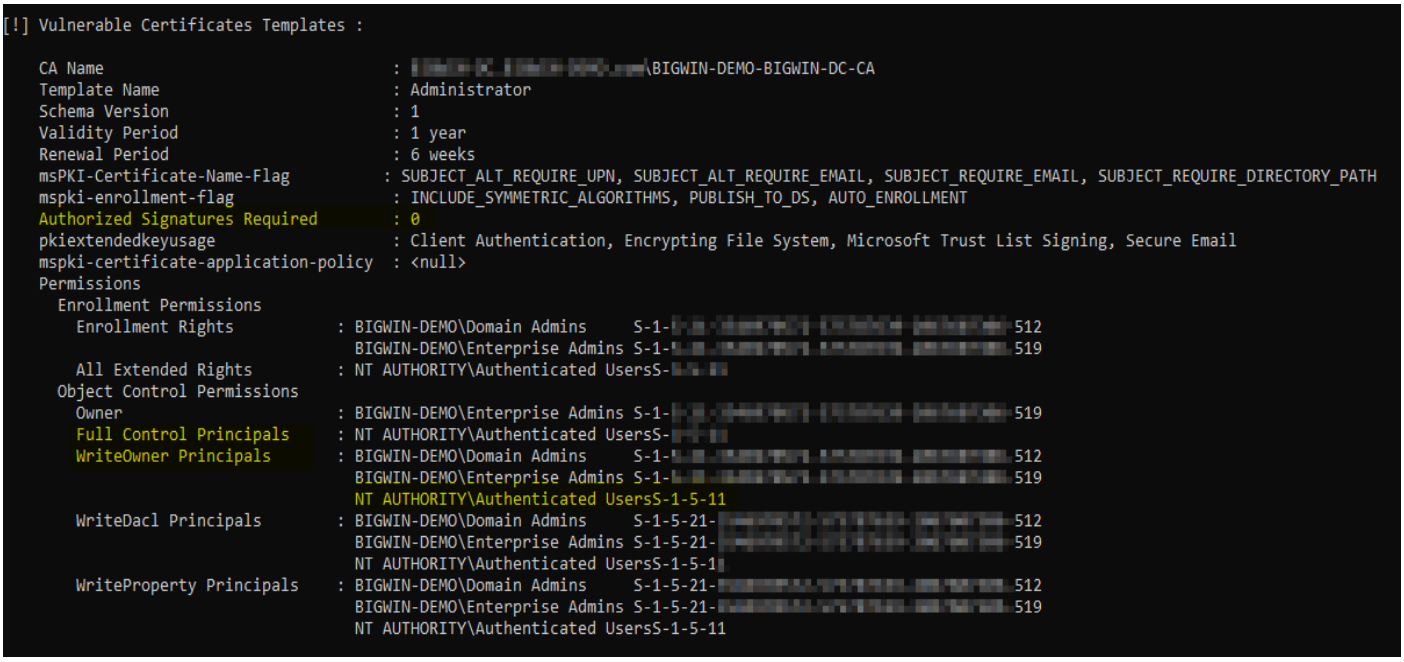
Description:	BIGWIN-DEMO LLC did not patch SMBv1, which is susceptible to various denial of service and remote code execution attacks. The RCS team confirmed the presence of the vulnerability but chose not to exploit it to avoid causing a denial of service.	
Risk:	Likelihood: Moderate – Basic scans can detect the SMB version, but an attacker would need to be on the internal network and identify a suitable exploit. Impact: Moderate – If exploited, an attacker could cause a denial of service and achieve code execution.	
System	10.x.x.x	
Tool Leveraged:	Nmap, Nessus	
References:	SMBv1 Remediation SMBv1 Hardening	

Remediation
Apply the latest patching, and upgrade to SMBv3 across the network.

Finding IPT-010: Vulnerable certificate template (ESC4) (Critical)

Description:	The RCS team identified a vulnerable Active Directory certificate template which allow authenticated uses to modify certificate template configuration n by enabling “write” permission. This template configuration grant authenticated users “Full Control” over the certificate template.
Risk:	
System:	Two Vulnerable certificate template identified
Tool Leveraged:	Certipy, Certify, Rubeus
References:	AD Certificates ADCS Misconfigurations

Artifacts:



Remediation

Configure to avoid all authenticate users to having Write or Full control over certificate template, enable **CA Manager Approval** on those Certificate Templates, and ensure that only the necessary users are allowed to enroll in this Certificate

Finding IPT-011: Steps to Domain Admin (Informational)

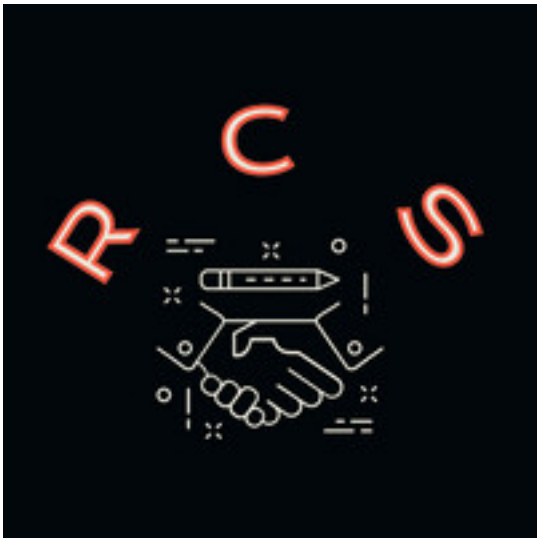
Steps	Actions	Remediation
1	NetNTLMv2 hash of a regular network user were obtained through poisoned LLMNR responses.	Leverage GPO to disable multicast name resolution.
2	Capture NTLM hashes for domain administrator {account name removed} was cracked “Password1!”.	Implement privilege account management (PAM) solution, and increase password complexity, implement MFA.
3	“Password1!” gave RCS team access to several hosts in the network.	Limit local administrators’ privileges, implement and enforce least privilege.
4	Through dumping hashed from compromise host, RCS obtained a cleartext password “Justdoit@2024” via WDigest	Leverage GPO to disable WDigest in the environment.
5	The RCS team through compromised overly permissive account with password “Justdoit@2024” got access to many hosts on the network.	Limit local administrators’ privileges, implement and enforce least privilege.
6	RCS team dump hashed from compromise host which disclosed other cleartext password of a domain account.	Leverage GPO to disable WDigest in the environment.
7	The RCS team leveraged discovered domain administrator credentials to log into the domain controller.	Apply recommend remediations.

Remediation

Review remediation steps in the listed findings.

Additional Scans and Report

The RCS team shares all test-related report data with clients, including Nessus files and comprehensive vulnerability scans in detailed formats. These reports provide raw scan results and highlight additional vulnerabilities the RCS team did not exploit. The RCS team also pinpoints security hygiene issues that, while less likely to result in a breach, present opportunities for improving defense in depth. For further details, refer to the "Detailed Scans and Reports" folder in your shared drive.



Resonance CyberSentinel

Uncovering Vulnerabilities, Fortifying Your Defense

Last Page