THE COZY CROISSANT

Security Assessment Findings Report

Business Confidential

Date: January 14, 2023

Project: TCC23

Version 1.0

Table of Contents

Confidentiality Statement

This document is the property of The Cozy Croissant and XXXXXX-XX. This document contains sensitive information including proprietary and confidential information. This document shall not be distributed outside of The Cozy Croissant or the XXXXXX-XX without the express consent of both parties involved.

Disclaimer

This document contains information regarding the overall network and system security of the Cozy Croissant. While XXXXXX-XX maintains the highest standards of quality in their work, this document should not be construed as an exhaustive list of all possible vulnerabilities. We have intentionally focused on the areas with the highest risk and greatest vulnerability to attack to maximize the value of our services.

Due to the changing nature of the computer systems and networks, security vulnerabilities and risks will change over time; XXXXXX-XX recommends annual testing to maintain a good security posture in response to evolving threats.

Executive Summary

The Cozy Croissant enlisted the help of XXXXXX-XX's penetration testing services to test both their Corporate and Guest networks. This test was a reassessment of previous vulnerabilities as well as a test for new vulnerabilities present in The Cozy Croissant's networks. These tests took place over two days.

The purpose behind this penetration test is to help The Cozy Croissant better secure their critical infrastructure. This is important to both our firm and TCC as protecting their systems has a direct effect on a customer's experience at the Hotel. Our firm kept this in mind during the entire test to inform how we conducted our tests as well as label the criticality of vulnerabilities. It is of the utmost importance that customer data is secured to maintain The Cozy Croissant's commitment to their customers.

Out of all the findings our team discovered over the course of the assessment, a few stood out as especially important to highlight as they add considerable risk to The Cozy Croissant. The first of these are the guest kiosks located at the hotel. These kiosks are intended for customers to use to surf the web but have very limited permissions as it pertains to The Cozy Croissant's network. Unfortunately our firm was able to engineer multiple ways to break out of the limited capabilities provided by these kiosks. Ultimately these breakouts resulted in complete domain compromise. This has a huge impact on the availability, integrity, and confidentiality of the entire TCC network. Our firm wanted to highlight this vulnerability specifically as it is the single most important point of failure we were able to find.

Another of the large issues found within the network applies to PCI DSS. During our testing we discovered multiple violations of PCI DSS, which our firm felt was important to bring special attention too. As The Cozy Croissant is an organization that deals with large amounts of customer data, especially credit card information, these violations can cause serious issues. We have specifically listed all the violations we discovered in our testing and there is a table which shows which vulnerabilities apply to each PCI objective.

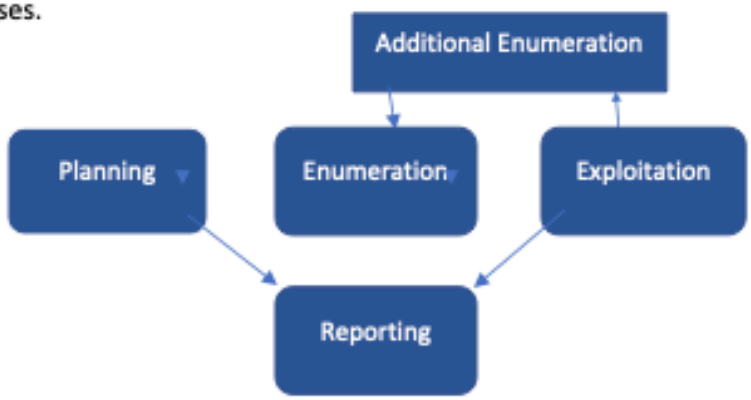
Finally, our firm did extensive retesting on the network segmentation that The Cozy Croissant implemented since the last testing of the network. While we were very impressed with the ACLs and other methods implemented, our firm was still able to circumvent these new additions and access the Corporate network through the Guest network. Just as before, the improper network segmentation is critical for The Cozy Croissant to harden as this attack poses a large risk to The Cozy Croissant's business operations. With the proper protections in place, many of the attacks performed in the testing of the network would be impossible and thus lower the risk to customer data, service uptimes, and overall safety of the network.

These attacks required much more maneuvering and complicated methods to execute compared to our previous test and so we do want to congratulate The Cozy Croissant on the steps they have taken to improve their network security. Overall The Cozy Croissant's security posture has increased heavily and we are very happy to report that a large majority of previous findings have been removed or remediated. Our firm truly believes that The Cozy Croissant is moving in a positive direction in their network security. Finally, our firm wanted to highlight the improvements made by TCC other than their network segmentation. Our team reported that changes made to both the password policy and password lockout policy mitigated multiple attacks that were previously possible. Again our firm is incredibly impressed with the measures taken by The Cozy Croissant and want to congratulate TCC.

Assessment Overview

On November 19th, 2022, XXXXXX-XX conducted a penetration test to evaluate the overall security posture of The Cozy Croissant. This test was conducted in accordance with industry standard best practices. The phases of the penetration test are as follows:

- Planning – Customer expectations and rules of engagement are obtained.
- Enumeration – Open-source intelligence and scanning are done to identify common vulnerabilities and weak areas.
- Exploitation – Confirm vulnerabilities by successfully completing an exploit and then perform more discovery based on new information.
- Reporting – Record all vulnerabilities, findings, successful exploits, and organizational strengths and weaknesses.



Assessment Components

Internal Penetration Test

The internal penetration test will simulate how an attacker would operate inside of the internal network. One member of the team will enumerate the network for vulnerabilities as well as carry out internal network attacks, such as: kerberoasting, token impersonation, pass-the-hash, golden ticket, web exploitations and more. The team member will gain access to hosts through these exploits. They will move through the network using lateral movement eventually attempting to gain access to the domain controller and domain admin accounts.

Compliance Summary

Payment Card Industry (PCI) Data Security Standards (DSS)

Due to the processing of customer payment information, The Cozy Croissant must comply with PCI DSS. The PCI DSS are a set of global standards that are used to help protect cardholder data and ensure that companies who accept, process, store, or transmit credit card information are doing so in a secure environment. Failure to comply with PCI DSS can result in large fines, damage to reputation, and loss of customer data for the organization. By following this set of standards, The Cozy Croissant can both avoid these damages to the organization as well as increase security across the board.

Reference:

https://listings.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf

PCI Objectives	PCI Requirements	Compliance Violation Findings
Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data.	- TCC013 - TCC031

	2. Do not use vendor-supplied defaults for system passwords and other security parameters.	
Protect Cardholder Data	3. Protect stored data.	- TCC003 - TCC004 - TCC009 - TCC014 - TCC025 - TCC027
	4. Encrypt transmission of cardholder data across open, public networks.	
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs.	- TCC019 - TCC032
	6. Develop and maintain secure systems and applications.	- TCC006 - TCC009 - TCC014 - TCC015 - TCC016 - TCC017 - TCC018 - TCC020 - TCC021

		- TCC022 - TCC023 - TCC024 - TCC027 - TCC028 - TCC029 - TCC030 - TCC033 - TCC034 - TCC035 - TCC036 - TCC037 - TCC038
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know.	- TCC009 - TCC014 - TCC025
	8. Identify and authenticate access to system components.	- TCC002 - TCC004 - TCC007 - TCC008 - TCC009 - TCC017 - TCC018 - TCC021 - TCC022
	9. Restrict physical access to cardholder data.	

Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data.	
	11. Regularly test security systems and processes.	
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel.	

NIST SP 1800-27B

The ability to properly comply with governing standards like PCI DSS requires strong frameworks set by established organizations. NIST, or the National Institute of Standards and Technology, is a non-regulatory federal agency that provides cybersecurity guidance. The NIST SP 1800 27B is a NIST special publication that outlines a cybersecurity framework specific to the hospitality industry. The use of this guide will provide The Cozy Croissant with a foundation for securing its infrastructure and complying with important standards such as PCI DSS.

Reference:

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-27.pdf

Finding Severity Ratings

This section is used to define the severity ratings for any vulnerabilities and measure risk impact. The severity ratings will follow the corresponding CVSS score range.

Severity	CVSS V3 Score Range	Definition
Critical	9.0 – 10.0	Straightforward exploitation typically results in high-level system access. Vulnerabilities of this category should be resolved immediately
High	7.0 – 8.9	Exploitation may involve more steps but could result in gaining elevated privileges and potentially significant downtime or data loss. Vulnerabilities in this category should be resolved as soon as possible.
Medium	4.0 – 6.9	Vulnerabilities are present but are not exploitable, involve many extra steps, and/or require social engineering. Vulnerabilities in this category should be resolved after high-priority issues are resolved.
Low	0.1 – 3.9	Vulnerabilities may be present but are not exploitable. Resolving these vulnerabilities would help to reduce the organization's attack surface. Vulnerabilities in this category should be resolved during the next period of planned maintenance.
Informational	N/A	No vulnerability exists. This category is reserved for findings that do not directly relate to exploitation but may provide an attacker with information that would assist them in an attack.

Risk Factors

Risk is measured by two factors: Likelihood and Impact.

Likelihood

Likelihood measures the probability of a vulnerability being exploited. Severity ratings are used for scoring based on how difficult the attack was, the tools available, the skill level of the attacker, and the environment of the client.

Impact

Impact measures the probability of the vulnerability having an effect on operations in the corporation. This includes the confidentiality, integrity, and availability of client-side systems and data, harm to software and/or hardware, and financial loss.

Scope

Assessment	Details
Corporate Network	10.0.0.0/24
Guest Network	10.0.200.0/24

Scope Exclusions

The team will not conduct any testing on any externally facing systems or IP addresses. No disruptive or destructive testing will be allowed on any systems.

Testing will be limited to the assigned subnets; the VPN and Pentest box(es) are out of scope.

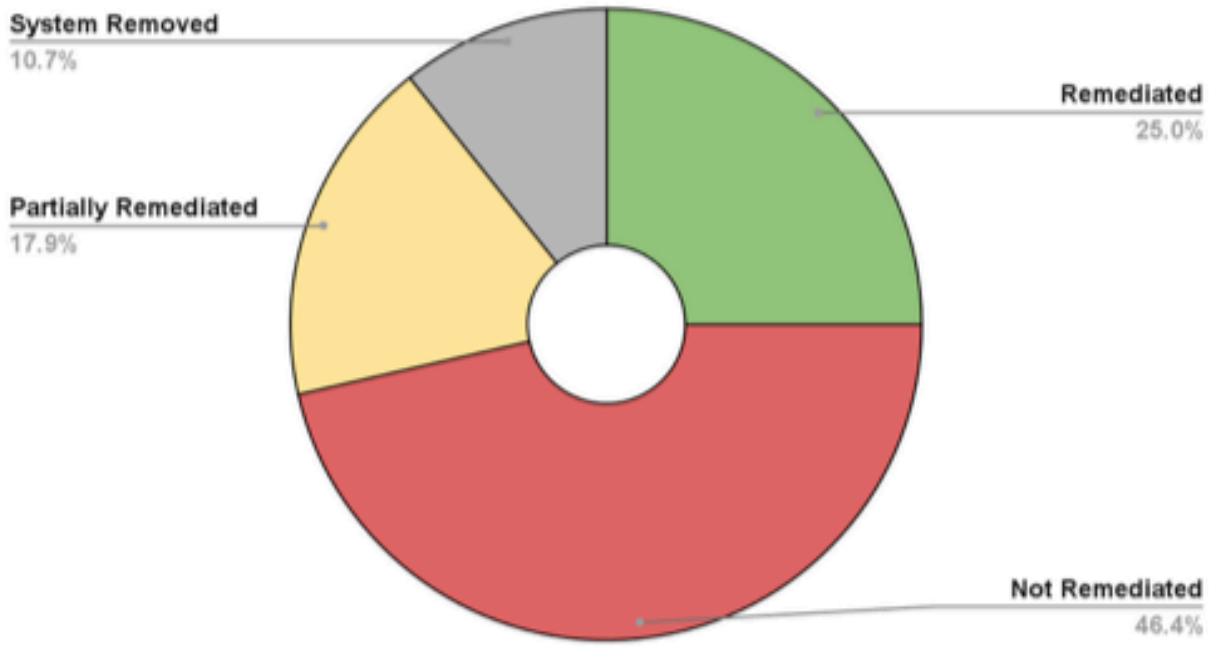
Client Allowances

The client will provide a Windows and Kali system for each tester; these will be used as an entry point to other systems.

Reassessment Summary

During the team's previous assessment, several vulnerabilities were found. These vulnerabilities have been reassessed to test any remediation attempted. This table shows a summary of the status of each previously discovered vulnerability.

Caegory Breakdown



Vulnerability Name	Severity	Remediation Status
Weak Password Policy	Critical	Partially Remediated
Debug Remote Code Execution	Critical	Remediated
Missing Access Control	Critical	Remediated
Database Dump on phpLDAPadmin	Critical	System Removed
Administrator Access without	Critical	Not Remediated

Authentication		
Plaintext Password Disclosure	Critical	Remediated
Improper Network Segmentation	High	Partially Remediated
Kiosk Breakout	High	Partially Remediated
NTLMv1 Enabled	High	Not Remediated
Privilege Escalation with Domain and Local Administrators	High	Not Remediated
Publicly Accessible PII and Credentials	High	Partially Remediated
SMB Signing Disabled	High	Not Remediated
Execution with Unnecessary Privileges	Medium	Not Remediated
Information Disclosure of Python Source Code	Medium	Not Remediated
Source Code Disclosure	Medium	Remediated
Insecure HTTP Usage	Medium	Partially Remediated
Guest Account on Domain Controller	Medium	Remediated
Clickjacking	Medium	System Removed
Plaintext Credential and Source Code Disclosure	Medium	Not Remediated
Cross Site Request Forgery	Medium	Remediated

Improper Error Handling	Low	Not Remediated
Backend Software Stack Version Disclosure	Low	Not Remediated
Server Version Disclosure	Low	Not Remediated
Web Application Version Disclosure	Low	System Removed
PHP Version Disclosure	Low	Not Remediated
Disabled Firewall	Low	Not Remediated
Weak Audit Policies	Info	Remediated
Disabled Windows SmartScreen	Info	Not Remediated

Vulnerability Report Card

Critical	High	Medium	Low	Informational
2	13	14	2	7

Vulnerability Summary

Severity	Vulnerability	Recommendation
Critical	**TCC001:** Administrator Remote Access without Authentication	Enforce the principle of least privilege
Critical	**TCC002:** Cleartext Credential Disclosure in Kiosk System	Encrypt passwords stored in the registry
High	**TCC003:** Insufficient LLMNR Configuration	Disable multicast name resolution via GPO
High	**TCC004:** Weak Password Policy	Increase overall password complexity
High	**TCC005:** Insufficient Hardening - Token Impersonation	Restrict token delegation
High	**TCC006:** Kiosk Breakout to Full Administrator Computer Access	Utilize well-developed kiosk lock software to prevent abuse of misconfigurations
High	**TCC007:** Security Misconfiguration - Local Admin Password Reuse	Require unique local admin passwords for each system in the network
High	**TCC008:** Cleartext Passwords in AD User Descriptions	Remove descriptions from Active Directory
High	**TCC009:** Improper Permissions on Customer Data	Associate individual customer data with each customer account
High	**TCC010:** Insecure Guest Permissions	Restrict permissions on guest accounts
High	**TCC011:** Privilege Escalation with Domain and Local Administrato	
High	**TCC012:** Privilege Escalation via Named Pipe Impersonation	Utilize a SIEM to detect and block attacks
High	**TCC013:** Improper Network Segmentation	Separate into two VLANs

High	**TCC014:** Plaintext PII and Credential Disclosure via Rewards Portal	Prevent disclosure of sensitive customer information
High	**TCC015:** SMB Signing Disabled	Require SMB signing on all Windows hosts
Medium	**TCC016:** Insecure Execution Policy	Change default user or install commercial off-the-shelf software for managing the kiosk controls
Medium	**TCC017:** Source Code and Plaintext Credential Disclosure	Remove passwords from the file and move the file to a non-hosted directory
Medium	**TCC018:** Publicly Accessible Query Logs	Move the logging location to a non-hosted directory
Medium	**TCC019:** User-Editable Windows Defender State from Kiosk	Utilize well-developed kiosk lock software to prevent abuse of misconfigurations
Medium	**TCC020:** Kiosk Breakout to New Window	Install commercial off-the-shelf software for managing the kiosk controls
Medium	**TCC021:** Automatic Sign in for Admin Jellyfin User	Create a new user to be the default login user
Medium	**TCC022:** Guest Account Present	Disable guest account
Medium	**TCC023:** User-Editable Internet Explorer Security Settings	Install commercial off-the-shelf software for managing the kiosk controls
Medium	**TCC024:** Insecure Code Logic	Fix software to properly generate passwords
Medium	**TCC025:** Unencrypted Customer PII in LDAP Database	Implement an encryption standard to ensure data is accessed only by intended means
Medium	**TCC026**: Username Discovery	Modify error messages to provide a generic response when an error occurs
Medium	**TCC027:** Plaintext Credential and Source Code Disclosure	Remove the password from the file and move the file to a secure location
Medium	**TCC028:** Vulnerable Service Version - SMBv1	Upgrade to SMBv3 and apply latest patches
Medium	**TCC029:** Plaintext Credential Disclosure	Ensure data is accessed only by intended means
Low	**TCC030:** Improper Error Handling	Prevent errors in web pages from revealing the error codes to a user

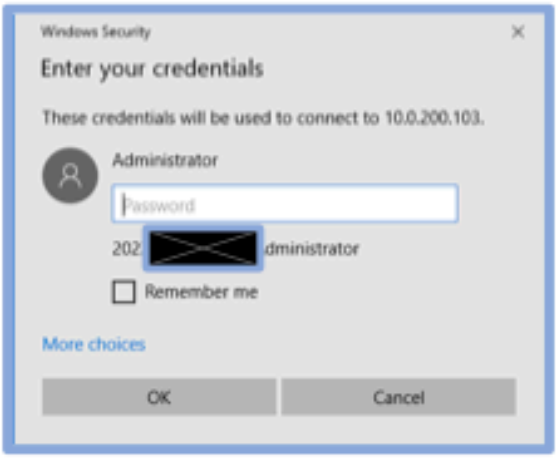
Low	**TCC031:** Improperly Configured System Firewalls	Configure firewall rules to only what is necessary
Info	**TCC032:** Improperly Configured Anti-Virus Software	Enable real-time protection
Info	**TCC033:** Eternal Blue Scan	Update Windows operating systems
Info	**TCC034:** Execution with Unnecessary Privileges	Change php to run as an unprivileged user
Info	**TCC035:** Disabled Windows SmartScreen	Enable SmartScreen
Info	**TCC036:** Software Version Disclosure	Remove version information disclosure content from services
Info	**TCC037:** [CVE-2021-43008] Improper Access Control in Adminer	Update Adminer
Info	**TCC038:** Outdated Software Versions	Update software

Technical Findings

Finding TCC001: Administrator Remote Access without Authentication	
Affected Hosts	10.0.200.101-104
CVSS: 9.3 | Critical	**Likelihood: Medium** No credentials are required by an attacker to exploit. The attacker needs to just provide the username "Administrator" with the password field left empty. **Technical Impact: High** If exploited, the attacker would gain local administrator access to the system. The attacker would initially be limited to the kiosk environment, however it has been demonstrated that the kiosk environment can be escaped.
Vulnerability Description	This vulnerability gives an authenticated user access to the local Administrator account, PowerShell, and other administrative tools. This can be used to pivot to other systems within the network.
Business Impact	This vulnerability demonstrates a PCI-DSS violation. The Cozy Croissant can be fined heavily by payment processors and credit card companies for any PCI-DSS violations.
Requirements to exploit	Physical access to the kiosk or access to the guest network is required to exploit.
Remediation	Enforce the principle of least privilege: do not run the kiosks as Administrator unless it is absolutely necessary. Additionally, ensure that all accounts are password protected.

Proof of Concept:

RDP can be used to connect to the affected systems as the Administrator account without any password as shown by the screenshots below.

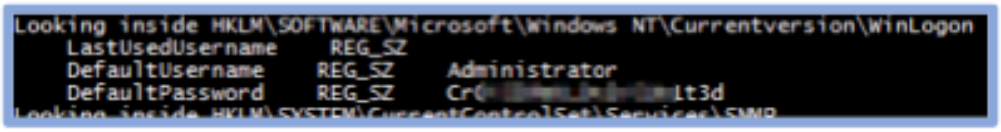



```
PS C:\Users\Administrator> whoami
kiosk03\administrator

PS C:\Users\Administrator> |
```

Finding TCC002: Cleartext Credential Disclosure in Kiosk System	
Affected Hosts	10.0.200.101 - 104
CVSS: 9.0 | Critical	**Likelihood: Medium** Accessing the cleartext credentials requires having access to the registry on the machine. This is achievable due to multiple previously discovered exploits on the same machine or other methods to obtain access. **Technical Impact: High** This credential pair was discovered to be valid for every system on both networks, allowing full administrator access on all machines.
Vulnerability Description	The WinLogin functionality of Windows stores some credentials in the registry for ease of access in the future. If the registry is accessible to a user or attacker, they can access the credentials and use them to login to corporate systems.
Business Impact	This vulnerability, when combined with others found, allows any user of the kiosks to locate a username and password that allows them to login to any of the systems on either network and take any action they desire. This includes accessing, editing, and deleting customer, employee, and company data. Cryptojacking malware could also be installed, which generates cryptocurrency for an attacker at the expense of The Cozy Croissant's computing and electricity.
Requirements to exploit	Access to system registry, used winPEAS to discover but not necessary
Remediation	The sysinternal tool, autologon, provides a way to encrypt passwords while they are stored in the registry, preventing a user who is viewing the registry from accessing usable secrets.
References	https://github.com/carlospolop/PEASS-ng/tree/master/winPEAS https://docs.microsoft.com/en-us/sysinternals/downloads/autologon

Proof of Concept:

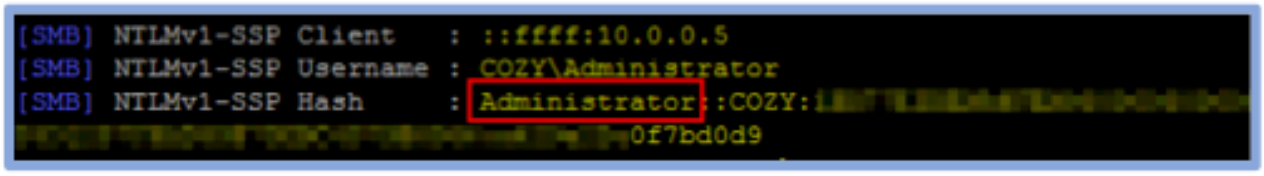
The following cleartext username and password pair was available at the HKLM\SOFTWARE\Microsoft\Windows NT\Currentversion\WinLogon:



Finding TCC003: Insufficient LLMNR Configuration	
Affected Hosts	10.0.200.101-104, 10.0.0.5,6,11,51,52
CVSS: 8.8 | High	**Likelihood: High** This attack is easy to run and requires very little work on the part of the attacker to perform. It is not uncommon for this attack to be triggered easily by normal day to day operations in an organization's network. **Technical Impact: High** This attack is highly dependent on the users who trigger the exploit. If a domain admin's hash is captured and cracked this can lead to a complete compromise of all machines in the network. In addition, if this attack results in normal user credentials it opens the doors to many more attacks in an Active Directory environment.
Vulnerability Description	An attacker running the responder tool poisons LLMNR traffic and redirects traffic to the attacker machine. Responder then dumps out the hashes of those users that had their traffic redirected. These hashes can then be cracked using tools such as Hashcat. Any of the hashes that can be cracked are potential user accounts that the attacker then has access to. In addition, NTLMv1 hashes captured can be used in Pass-the-Hash attacks.
Business Impact	This attack has adverse effects on TCC. Any attacker that utilizes this attack to gain credentials with access to important systems will have the ability to steal the personal information of customers, take down critical systems, and expand their foothold into The Cozy Croissant's network.
Requirements to exploit	Responder, Hashcat
Remediation	Disable multicast name resolution via GPO. See the below article for more information regarding this vulnerability and detailed remediation steps.
References	https://attack.mitre.org/techniques/T1557/001/

Proof of Concept:

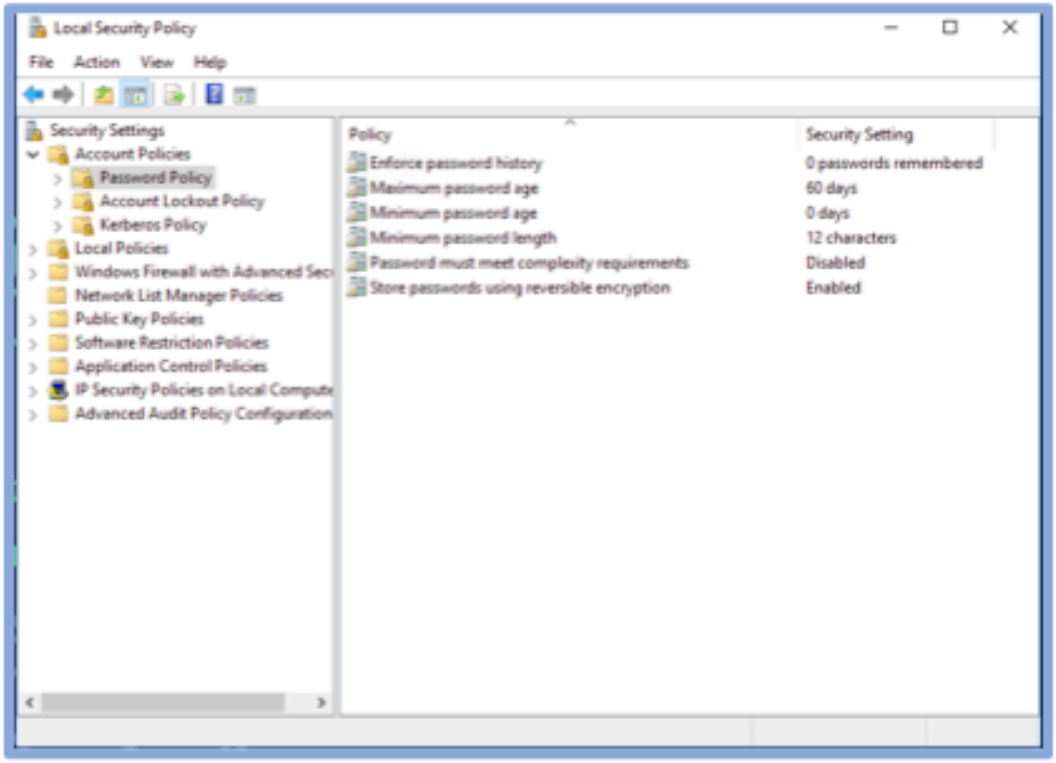
Administrator hash dumped from actions carried out on the Domain Controller:



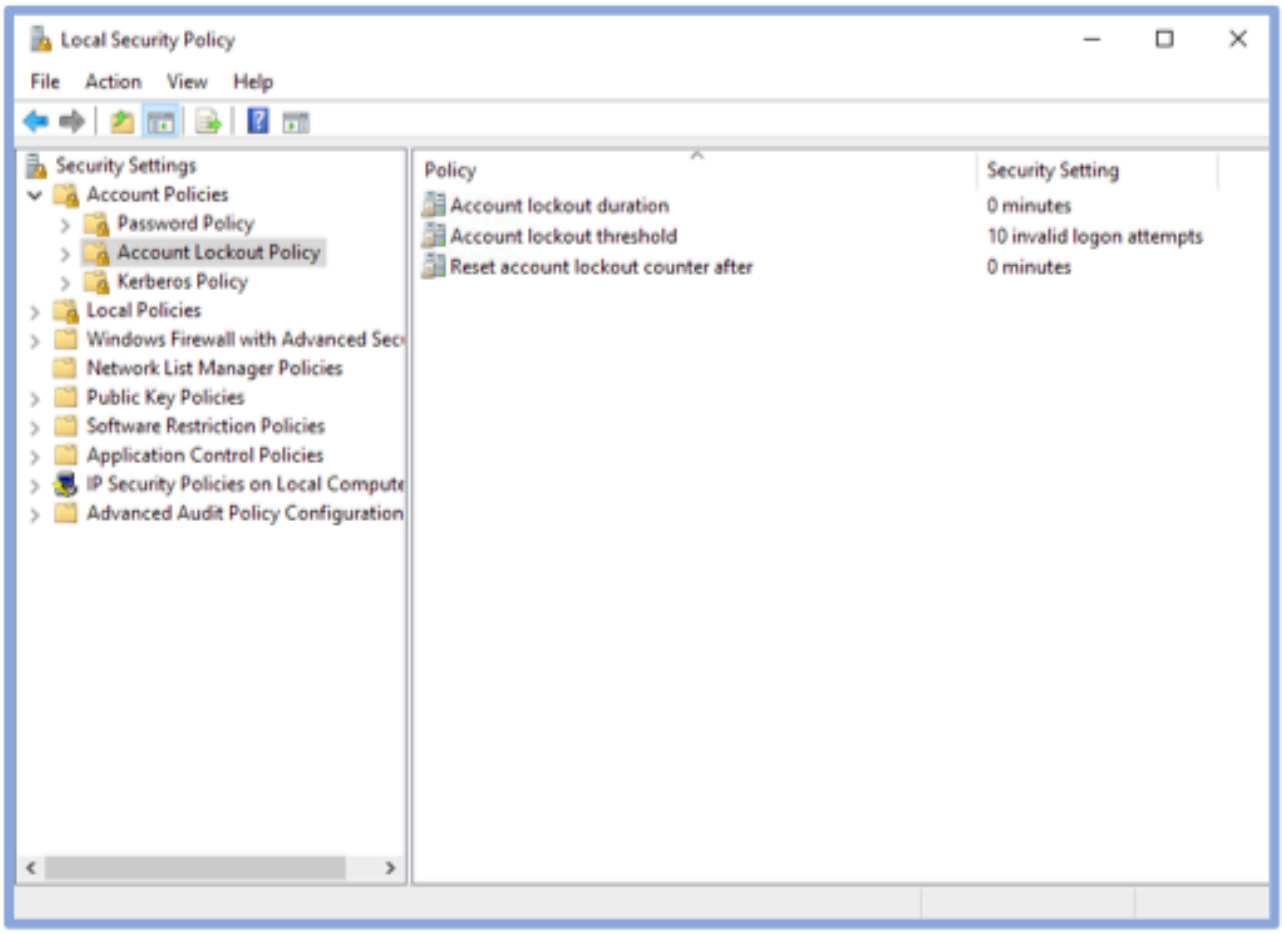
Finding TCC004: Weak Password Policy	
Affected Hosts	10.0.0.5-6, 10.0.0.11, 10.0.0.51-52, 10.0.0.200, 10.0.200.101-104
CVSS: 8.8 | High	**Likelihood: High** The password policy for both the users and customers are weak enough that there were many passwords that were either stored insecurely, or would be cracked easily. This means that it would be very likely that an attacker could exploit the weak password policies currently in place. **Technical Impact: High** A wide range of access could be gained due to the weak password policies in place. Access to customer information could easily be gained and damage to the customers data could take place. Additionally access could be gained to corporate systems by an attacker.
Vulnerability Description	The password policies in place can be potentially exploited to gain access to both customer and user accounts and information.
Business Impact	The customer password policy is especially weak which could lead to unauthorized access to many customer accounts. This would result in a great loss of trust in The Cozy Croissant. Additionally user passwords that are compromised could lead to much more dangerous exploitation on other systems. This could cause significant down time to mission critical systems and loss of data. Additionally, this vulnerability demonstrates a violation of PCI-DSS. The Cozy Croissant can be fined heavily by payment processors and credit card companies for any PCI-DSS violations.
Requirements to exploit	N/A
Remediation	User password policies should continue to be increased. This can be done by implementing a password history, enabling complexity requirements, disabling "Store passwords using reversible encryption", lockout counter and lockout duration should both be increased. These controls should be thoroughly implemented while still keeping in mind the risks of potential employee "password fatigue".
References	https://learn.microsoft.com/en-us/microsoft-365/admin/misc/password-policy-recommendations?view=o365-worldwide

Proof of Concept:

The following screenshot outlines The Cozy Croissant's domain password policy. The policy has improved since the initial test by including a length of 12 characters and a maximum password age of 60 days which are great improvements. There are however still further improvements that can be made. The most crucial are implementing a password history along with complexity requirements enabled. In addition disabling the option to store passwords using reversible encryption will help protect passwords while at rest in systems. Another recommendation in the realm of password requirements is the concept of password fatigue which regards not encumbering employees with unreasonable password requirements.



Additionally, the account lockout policy saw improvement but still needs further improvement to best secure The Cozy Croissant's network. The lockout duration and lockout counter both are set to 0 minutes meaning that although an account "locks" after 10 invalid attempts it is immediately unlocked counteracting the previous security control. Creating even a minimal lockout will limit potential brute force attacks to your networks.



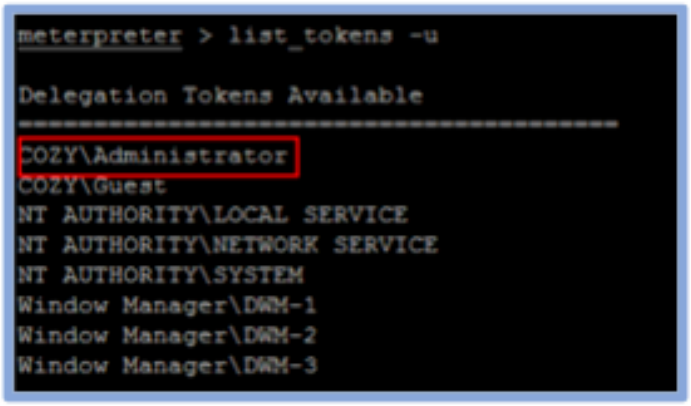
Customer passwords were also found to have a weak password policy. When customer passwords were dumped, many of them were as short as three characters and would easily appear in a password wordlist. It is advised that Customers are required to make strong passwords as well in order to protect their personal data.

Finding TCC005: Insufficient Hardening - Token Impersonation	
Affected Hosts	10.0.200.101-104, 10.0.0.5,6,11,51,52
CVSS: 8.5 | High	**Likelihood: High** An attacker can easily impersonate a token with the use of open-source tools. It is not uncommon for domain admins to log into computers and as such their tokens will be available. **Technical Impact: High** Once an attacker impersonates a token they are likely able to access new machines in the network as well as escalate privileges to that of a higher up user.
Vulnerability Description	An attacker can impersonate the token of another user by utilizing the Incognito module in Metasploit. This essentially makes them have the permissions of that impersonated user.
Business Impact	If an attacker is able to compromise a domain admin, they will be able to access more systems around the network. This can lead to loss of availability, integrity, and confidentiality across The Cozy Croissant's network.
Requirements to exploit	Any domain user, Metasploit, access to internal network, psexec
Remediation	Restrict token delegation. For full remediation see the references.
References	https://attack.mitre.org/techniques/T1134/003/

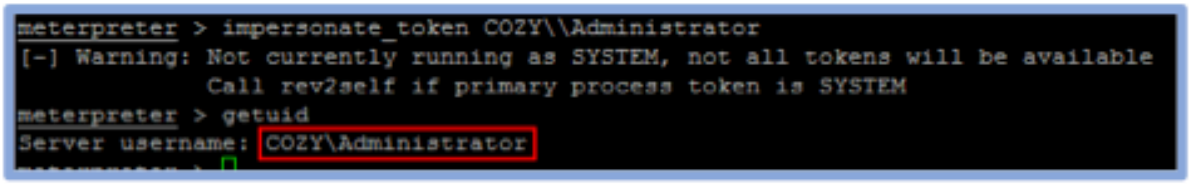
Proof of Concept:

Connection to any machine using psexec through Metasploit.

List the available tokens to the user signed in.



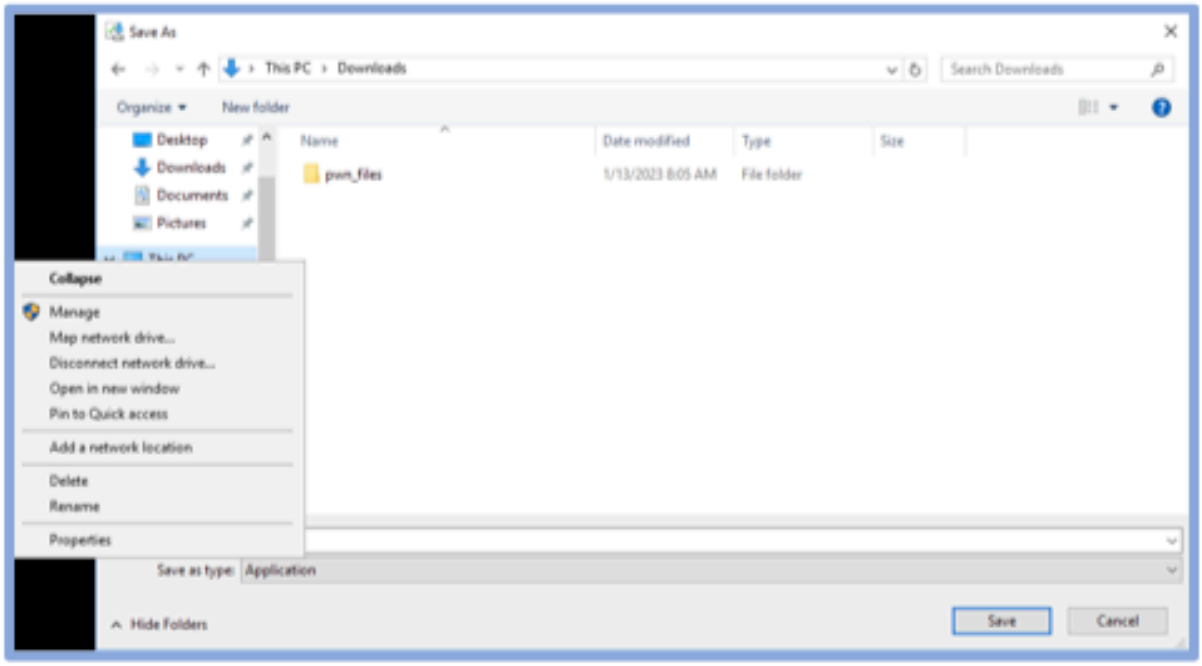
Token of Domain Administrator successfully impersonated.



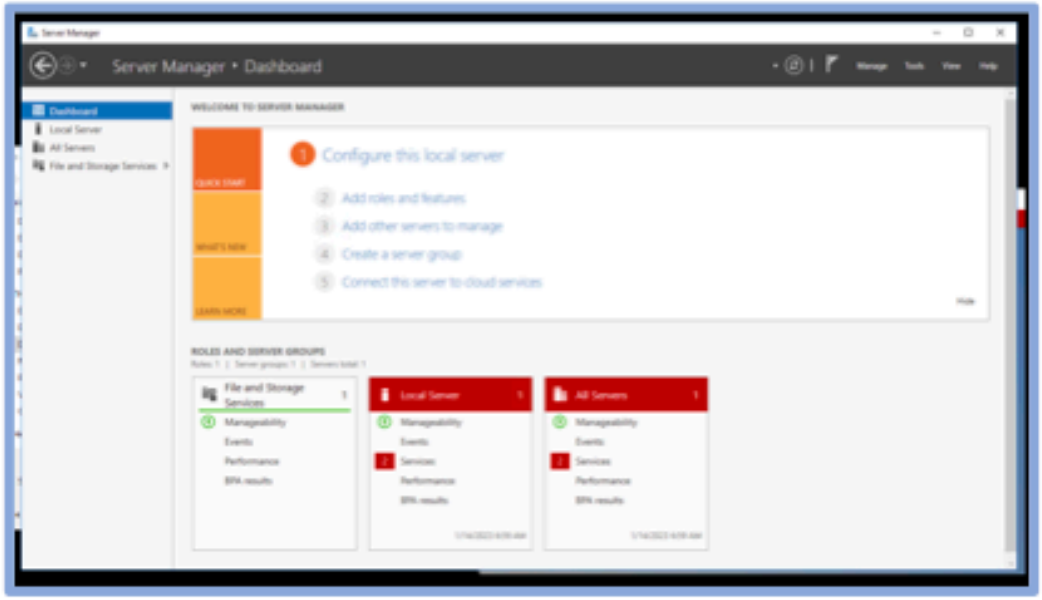
Finding TCC006: Kiosk Breakout to Full Administrator Computer Access	
Affected Hosts	10.0.200.101 - 104
CVSS: 8.3 | High	**Likelihood: Medium** To exploit this vulnerability, an attacker must make several highly-specific actions on the system that requires a sufficiently-advanced understanding of the Windows operating system. **Technical Impact: High** Full administrator system control and access is provided through this exploit to the attacker, allowing the installation of malware such as cryptojacking, spyware, and more.
Vulnerability Description	This vulnerability allows an attacker to escape the kiosk environment and access server management functionality and an administrator PowerShell prompt.
Business Impact	This vulnerability provides an attacker with full control of any of the kiosk systems, allowing them to install malware or take other malicious actions, which can lead to theft of guest data and disruption of business services. If this takes place, it can lead guests to either lose personal information and/or lose trust in the security of The Cozy Croissant. Cryptojacker malware can also be installed, which abuse the system resources for the financial gain of the attacker while creating costs for The Cozy Croissant.
Requirements to exploit	Access to the kiosk
Remediation	Utilization of well-developed kiosk lock software will prevent attackers from abusing the misconfigurations of the current in-house system (provided it is properly configured) and would provide tighter controls over the actions a user can take on the kiosk. Changing the default kiosk user to an unprivileged account would also prevent the later phases of this vulnerability from being exploited.

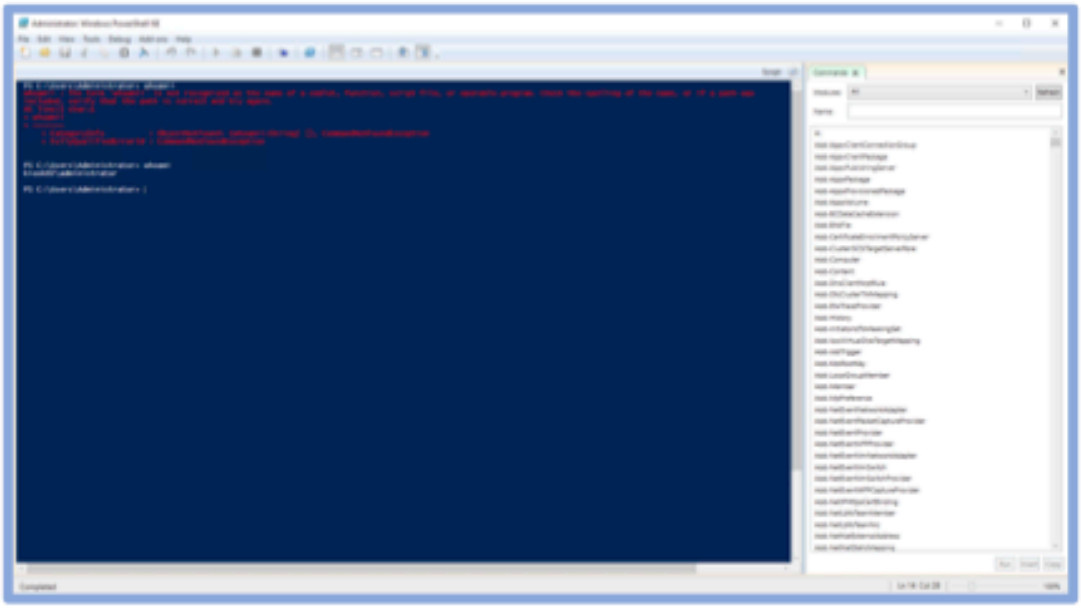
Proof of Concept:

1. Right click the image on the default web page and select "Save Image As"
2. In the file explorer window, right click "This PC" and select "Manage"



3. This brings up the Server Manager. Select Tools > Powershell ISE

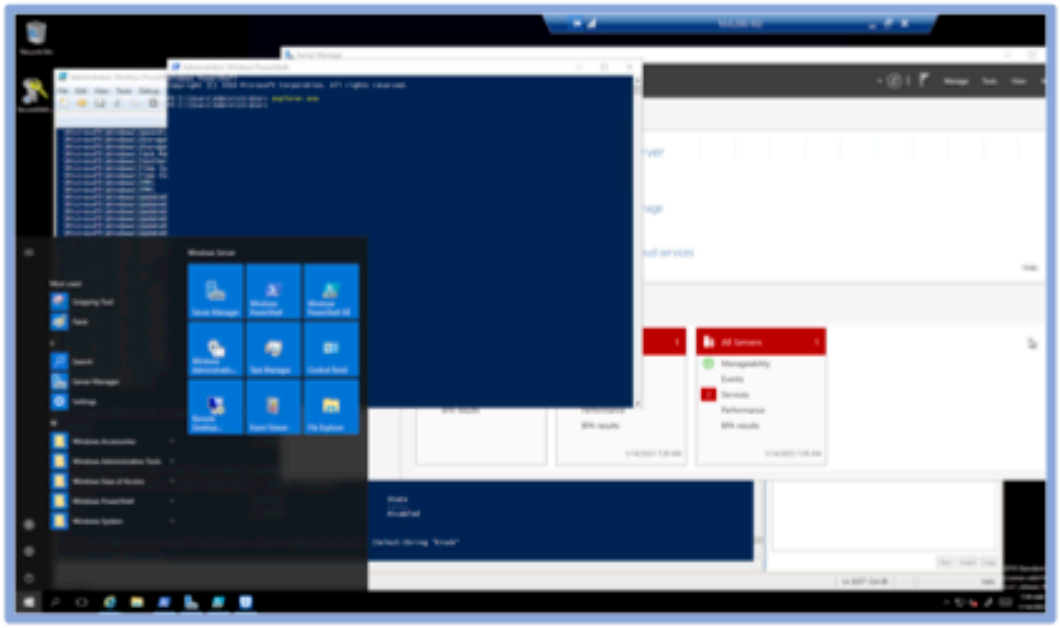




4. The following commands can be used to stop and disable the script running the kiosk security controls:

```
PS C:\Users\Administrator> Disable-ScheduledTask -TaskName kioskmode

TaskPath                                 TaskName                 State
--------                                 --------                 -----
\                                        kioskmode                Running


PS C:\Users\Administrator> Stop-ScheduledTask -TaskName kioskmode

PS C:\Users\Administrator> Disable-ScheduledTask -TaskName kioskmode

TaskPath                                 TaskName                 State
--------                                 --------                 -----
\                                        kioskmode                Disabled


PS C:\Users\Administrator>
```

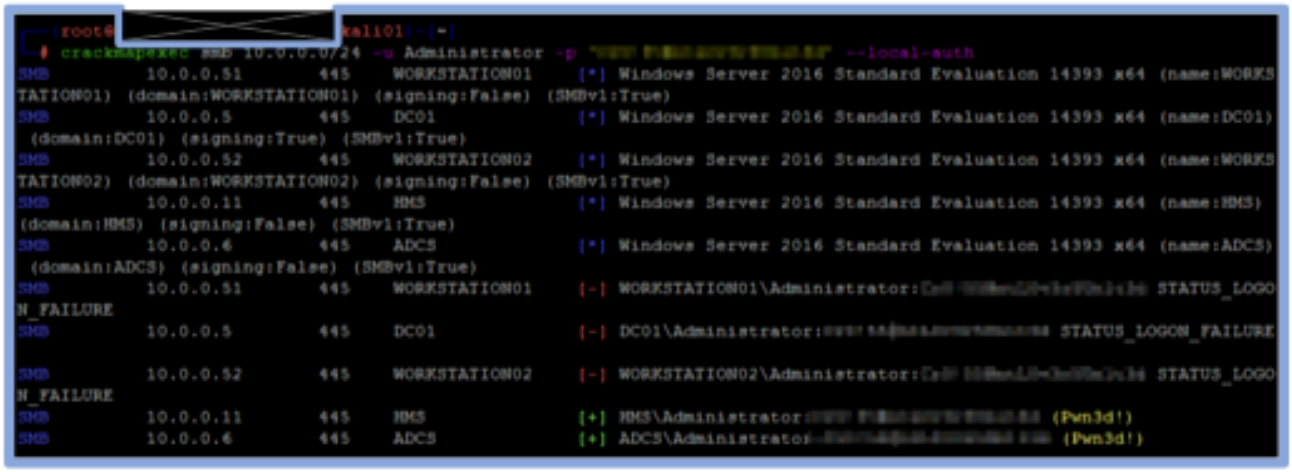
5. From here, the kiosk can be fully used as an administrator. By starting explorer.exe, the standard Windows GUI is returned.



Finding TCC007: Security Misconfiguration - Local Admin Password Reuse	
Affected Hosts	10.0.0.6, 10.0.0.11
CVSS: 8.0 | High	**Likelihood: Medium** It is likely that an attacker with valid credentials would attempt to use those on other machines. This attack does require valid credentials to be exploited. **Technical Impact: High** Password reuse, especially as an admin, allows an attacker to easily pivot between machines laterally and vertically in the network. This gives an attacker complete access to multiple systems which increases overall risk to the network.
Vulnerability Description	Utilizing either the password or NTLMv1 password hash of a local administrator user, an attacker can attempt to login to other machines using the same credentials.
Business Impact	If an attacker executed this attack, it would give them access to multiple systems, not just one. This increases the risk to The Cozy Croissant as the availability of multiple systems are at risk. In testing the systems affected were critical to the day to day function of the hotel.
Requirements to exploit	Valid Admin credentials on one machine, crackmapexec
Remediation	Require unique local admin passwords for each machine in the network. Consider implementing a PAM solution.
References	https://www.pentestpartners.com/security-blog/admin-password-re-use-dont-do-it/

Proof of Concept:

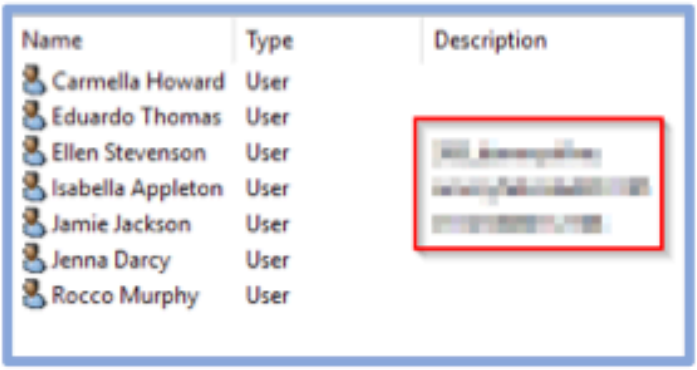
Once an attacker has valid credentials they can utilize crackmapexec to test any and all machines in a specified range as shown below. All machines that come back with successful login and (Pwn3d!) have the reuse issue.

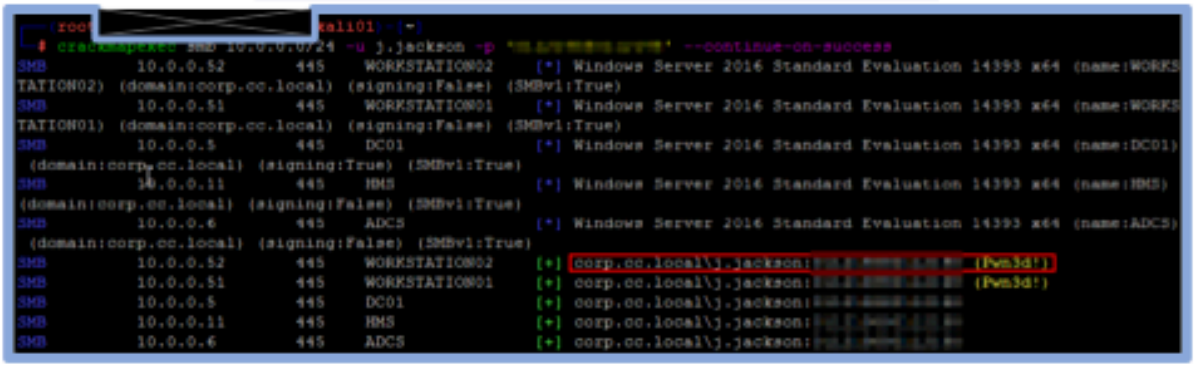


Finding TCC008: Cleartext Passwords in AD User Descriptions	
Affected Hosts	All
CVSS: 8.0 | High	**Likelihood: High** It is common for users to add sensitive information to their descriptions as there is an assumption it is secure and cannot be viewed by others. An attacker can easily view the descriptions of all users in a domain as long as they have one set of valid credentials. **Technical Impact: High** An attacker can utilize any cleartext passwords from the descriptions to gain access to new machines. If a Domain Admin is compromised this attack can lead to the compromise of the entire network.
Vulnerability Description	An attacker with valid credentials can use normal system enumeration to view the descriptions of any user in the domain regardless of permissions. In total, 8 users had their passwords listed in their descriptions with some of them being Domain Admins. These passwords can then be passed around the network to verify which computers they give access too.
Business Impact	An attacker who successfully carried out this attack would have the credentials for employees at The Cozy Croissant. If the attacker is able to compromise the domain as a result, there is a large risk of financial loss to TCC.
Requirements to exploit	Valid AD User credentials, command line access on a domain joined machine, internal network access, crackmapexec
Remediation	Remove the ability for employees to leave descriptions with their uses in Active Directory.

Proof of Concept:

Below is a screenshot showing the descriptions of users in the Domain with passwords stored. In total eight valid credentials were discovered in the descriptions of users. These user's credentials were verified by using crackmapexec to prove the login was valid.

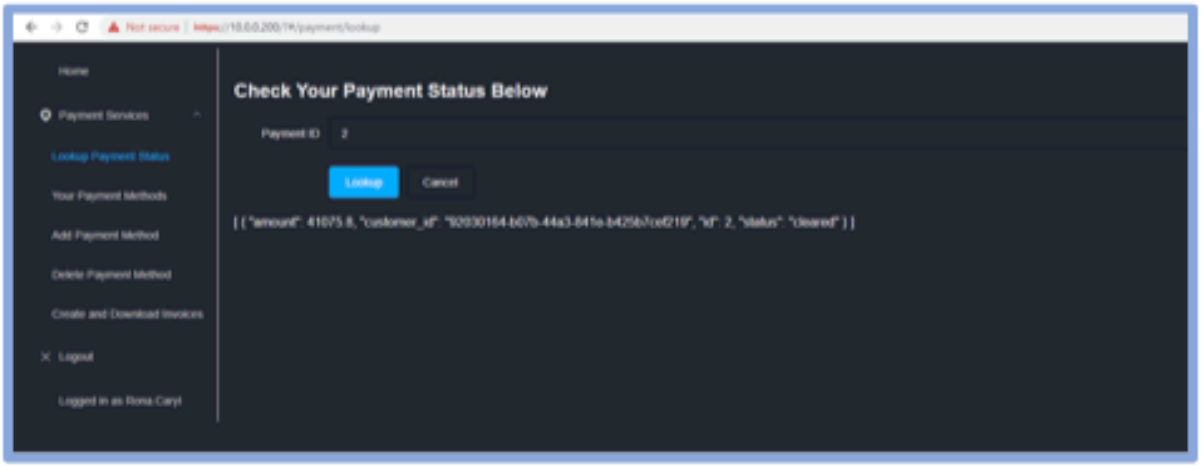




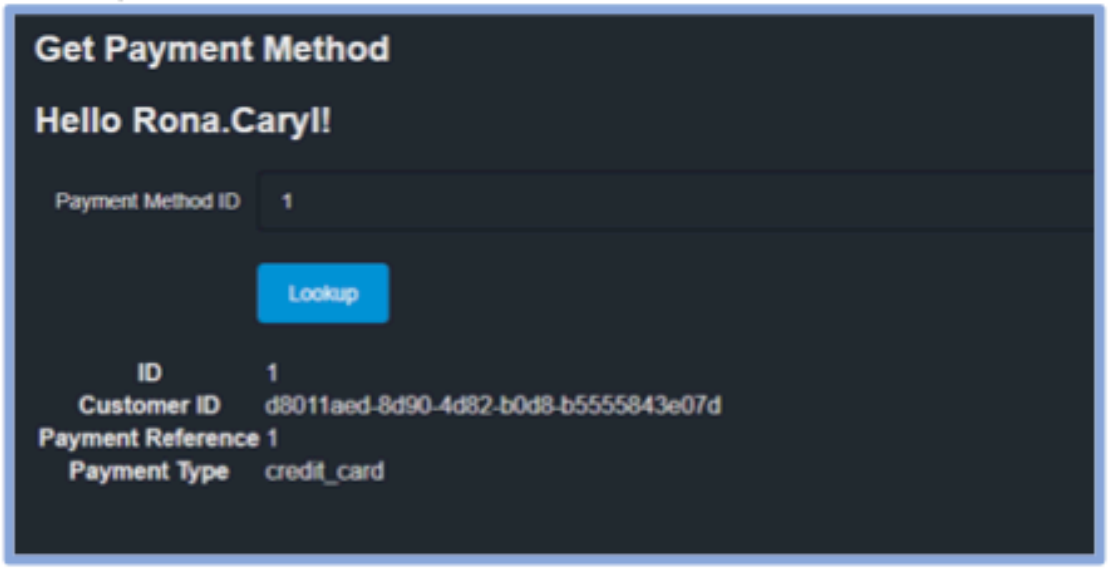
Finding TCC009: Improper Permissions on Customer Data	
Affected Hosts	10.0.0.200
CVSS: 7.9 | High	**Likelihood: Medium** This vulnerability requires a customer's credentials to be exploited. Once logged into the payment portal on this system, the attacker can view any customer's payment status, payment method, and customer invoices. Additionally, an attacker could delete customer payment methods. **Technical Impact: High** All customer payment methods could be easily deleted by an attacker. This attack results in a large loss in confidentiality, integrity, and availability.
Vulnerability Description	Attackers are able to view other customer payment methods, payment statuses, and invoices by inputting the corresponding ID. Additionally, attackers are able to arbitrarily delete payment methods by providing a payment method ID.
Business Impact	This vulnerability results in large amounts of sensitive customer data being exposed. Attackers could steal information from the customers as well as delete their payment methods. This would result in a large loss of trust in The Cozy Croissant as well as a large financial loss. Additionally, this vulnerability demonstrates a violation of PCI-DSS. The Cozy Croissant can be fined heavily by payment processors and credit card companies for any PCI-DSS violations.
Requirements to exploit	Credentials of a customer account and the ability to access the corporate network.
Remediation	Customer payment information should be associated with a specific customer account. When a customer queries for payment information, they should only be able to view records associated with their account.

Proof of Concept:

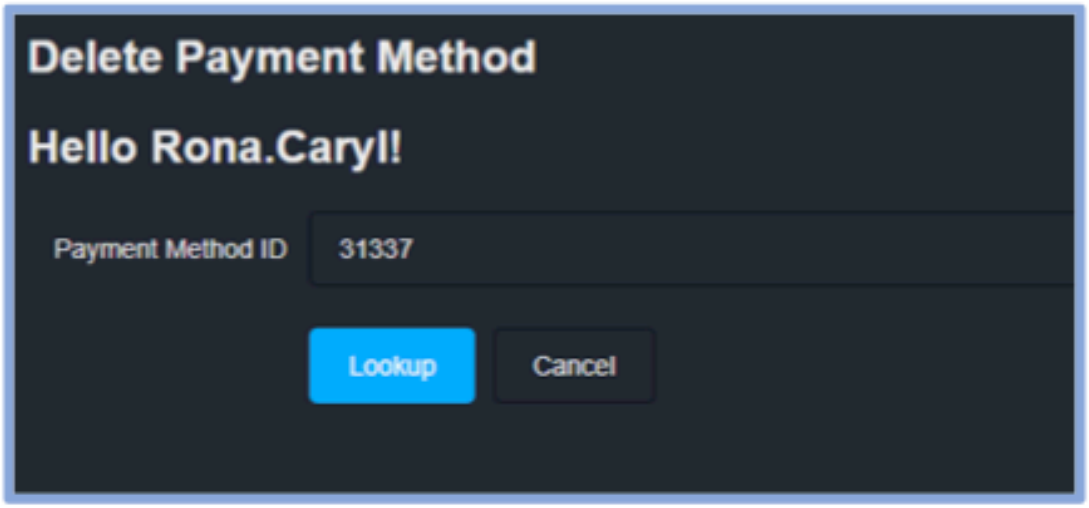
Accessing a customer's payment status:



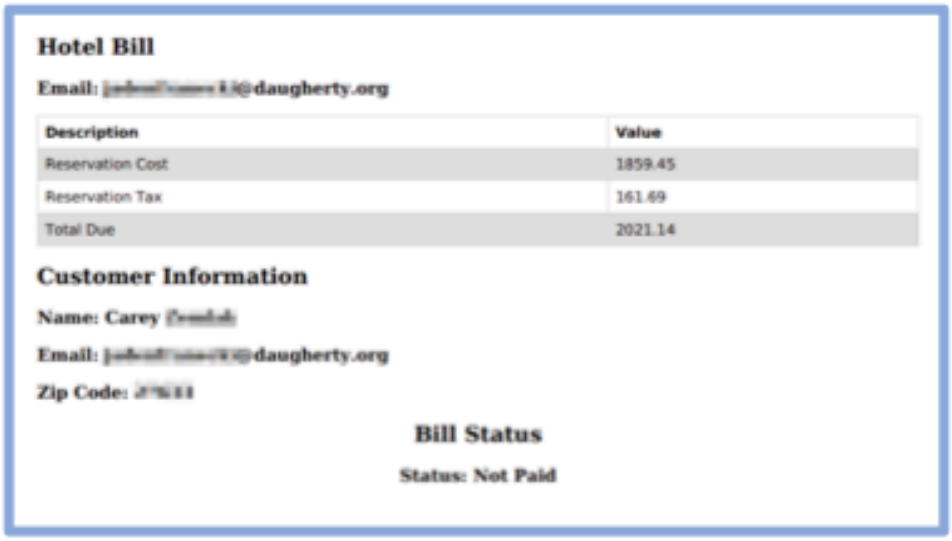
Accessing a customer's payment method (note that the logged in user is the same, but the customer IDs are different):



Access to delete a customer's payment method via the payment method ID:



Downloaded customer invoice:



Hotel Bill

Email: [redacted]@daugherty.org

Description	Value
Reservation Cost	1859.45
Reservation Tax	161.69
Total Due	2021.14

Customer Information

Name: Carey [redacted]

Email: [redacted]@daugherty.org

Zip Code: [redacted]

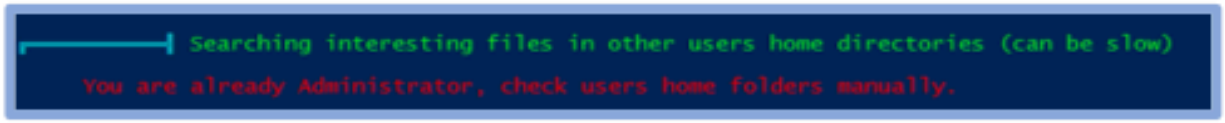
Bill Status

Status: Not Paid

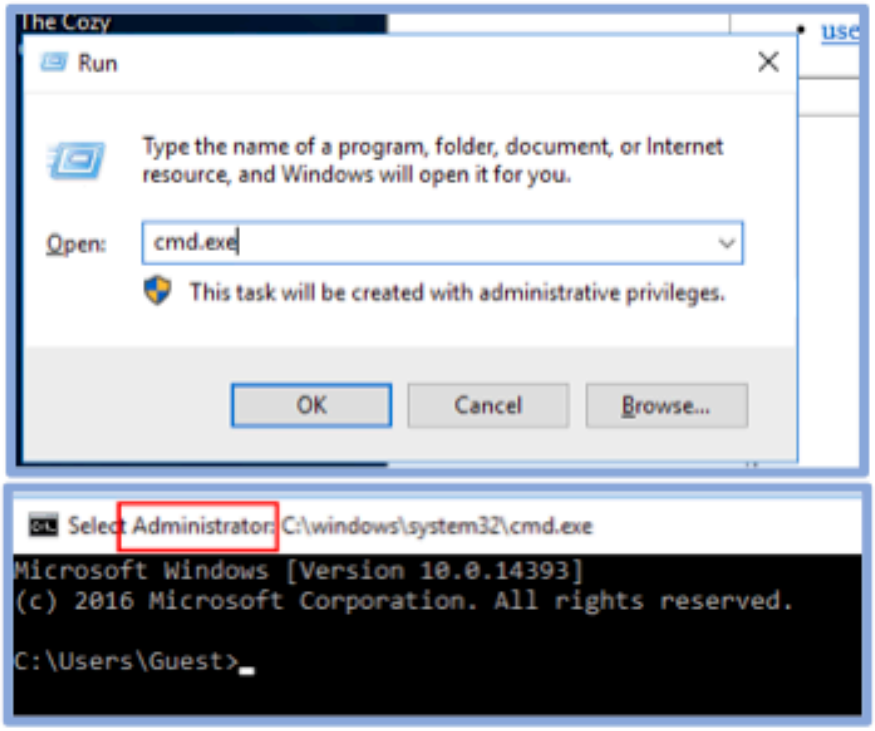
Finding TCC010: Insecure Guest Permissions	
Affected Hosts	10.0.0.51, 10.0.0.52
CVSS: 7.6 | High	**Likelihood: Medium** An attacker would require adjacent network access to exploit this vulnerability however it would be a likely vector given that access to the internal corporate network. **Technical Impact: Medium** From a technical perspective, this vulnerability allows for an attacker to gain control of either hotel workstation which compromises the confidentiality, integrity, and availability of the system and the data on the given system.
Vulnerability Description	This vulnerability regards the incorrect assignment of permissions to the guest account. This account has administrator permissions which allows an attacker to completely own the given local system.
Business Impact	If an attacker gained access to the employee workstations the data on those workstations can be compromised which could potentially include customer and employee data. In addition, if the availability of the workstations was compromised the business of The Cozy Croissant would be limited until they were restored.
Requirements to exploit	The requirement to exploit this vulnerability is adjacent network access along with guest account access which in The Cozy Croissant's case is a passwordless account.
Remediation	The guest account should have the least amount of permissions needed to fulfill the intended purpose for the account on the workstation. If there is no specific purpose for this user it is advised to disable the guest account outright.
References	https://learn.microsoft.com/en-us/microsoft-365/solutions/create-secure-guest-sharing-environment?view=o365-worldwide

Proof of Concept:

While running an enumeration script this line displayed that the guest account had local administrator permissions. This can cause a large issue if an outside attacker has unrestricted access to either hotel workstation locally.



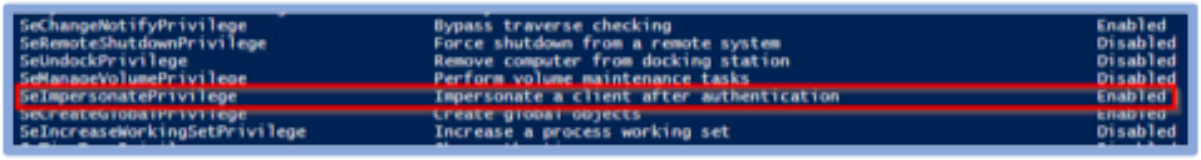
The guest user can start a console with administrator privileges.



Finding TCC011: Privilege Escalation with Domain and Local Administrators	
Affected Hosts	10.0.200.101 - 104, 10.0.0.51 - 52
CVSS: 7.5 | High	**Likelihood: Medium** Exploiting this vulnerability requires console access to the system as either a domain or local user. **Technical Impact: High** An attacker is able to become NT Authority\System if privileges are escalated with this vulnerability, allowing them to perform any action on the target including installing malware.
Vulnerability Description	If SeImpersonatePrivilege is enabled for a user, an attacker can use the PrintSpoofer.exe exploit to grant a system level shell.
Business Impact	If an attacker can gain system level access to these machines, they are able to have full control over it to take it down, edit or delete information, and install malware for various purposes, which would be severely detrimental to the technological, guest relations, and financial aspects of The Cozy Croissant.
Requirements to exploit	Access to the corporate network (for corporate hosts), domain or local access, PrintSpoofer.exe exploit
Remediation	Disable SeImpersonatePrivileges for all accounts
References	https://github.com/dievus/printspoofer

Proof of Concept:

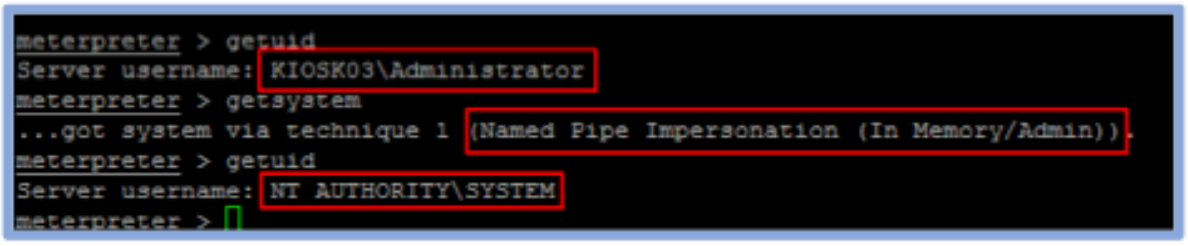
The following privilege is enabled on the users for the specified hosts that allow for PrintSpooler.exe to run and spawn a system level shell:



Finding TCC012: Privilege Escalation via Named Pipe Impersonation	
Affected Hosts	10.0.200.101 - 104
CVSS: 7.1 | High	**Likelihood: Medium** Exploitation of this vulnerability requires either a shell and an exploit on the system or a meterpreter session. Multiple exploits have been found to provide these on this machine. **Technical Impact: High** By exploiting this vulnerability, an attacker gains full access to the system, including the ability to view, edit, and remove any file on it. The host is not joined to a domain, so the access is confined to the machine.
Vulnerability Description	In this technique, Meterpreter creates a named pipe. Then a cmd.exe is created under the local system that connects to the Meterpreter named pipe. Meterpreter can then impersonate the local security privileges, in this case SYSTEM. This makes you the SYSTEM administrator. (Rapid 7 - See References)
Business Impact	If an attacker gains full access to the kiosk systems, as is possible with this vulnerability, they would be able to take down the kiosks, install malware for spying or cryptocurrency mining, or add it to a botnet. All these outcomes would cost The Cozy Croissant money in the form of used electricity and reduce or remove the effectiveness of the systems for their intended use cases.
Requirements to exploit	A shell or meterpreter session on the system
Remediation	Use a SIEM solution to detect this specific attack. Rules can be set to block an attacker from executing this type of attack.
References	https://learn.microsoft.com/en-us/windows/win32/ipc/impersonating-a-named-pipe-client?redirectedfrom=MSDN https://docs.rapid7.com/metasploit/meterpreter-getsystem/

Proof of Concept:

Below it is shown that the attacker is running as an Administrator on the system and is able to utilize the Named Pipe Impersonation to become the highest user, NT Authority\System.

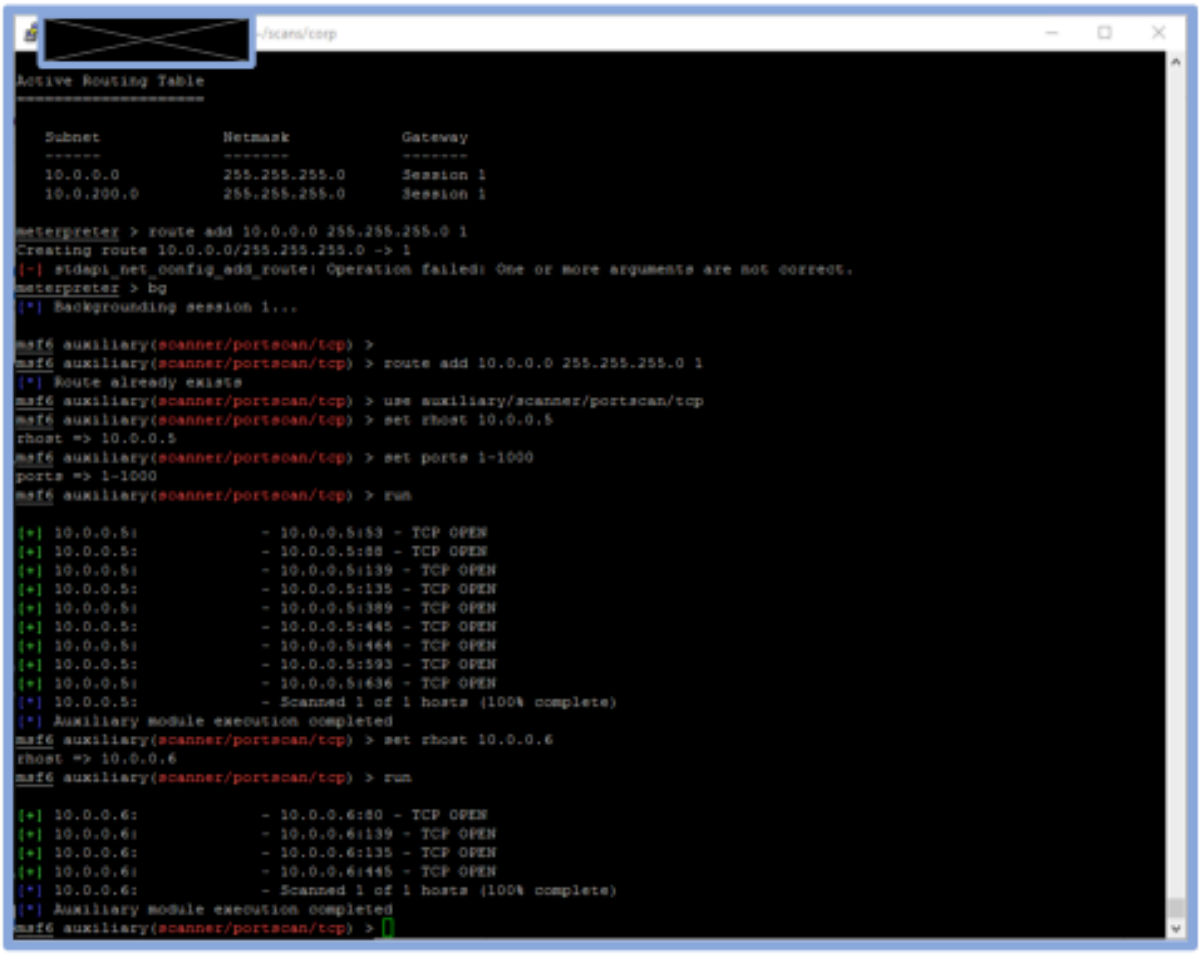


Finding TCC013: Improper Network Segmentation	
Affected Hosts	10.0.0.0/24
CVSS: 7.1 | High	**Likelihood:** With network ACLs implemented, the need to pivot past these controls becomes a necessity and makes this attack vector highly likely. **Technical Impact:** This attack vector circumvents the network ACLs which aim to block external access to the corporate network. From a technical perspective this renders the network ACLs less useful that intended.
Vulnerability Description	The corporate network is reachable from the guest network. Furthemore, the guest network can be accessed and compromised externally which renders the guest network into a pivoting point to counteract the segmentation put in place.
Business Impact	This attack vector impacts The Cozy Croissant as a whole by allowing a full network compromise to occur from an external source. A full network compromise can cripple regular business operations and result in large losses.
Requirements to exploit	This exploit requires access to the adjacent network which in this case is the guest network. This access can be procured through a variety of methods.
Remediation	In addition to the network ACLs preventing external access to the corporate network, virtual local area networks (VLANs) should be implemented to separate the guest and corporate network. Additionally, on the network infrastructure BPDU guard on all ports as well as MAC address filtering. Ensuring only designated trunk ports are able to trunk VLANs will aid in the overall segmentation of the corporate and guest network.
References	https://www.comparitech.com/net-admin/how-to-set-up-a-vlan/ https://www.geeksforgeeks.org/what-is-bpdu-guard-and-how-to-configure-bpdu-guard/

Proof of Concept:

The following screenshots show creating a pivoting route in metasploit along with utilizing the modular nature of metasploit to scan the internal corporate network with a tcp portscan. An initial Nmap scan

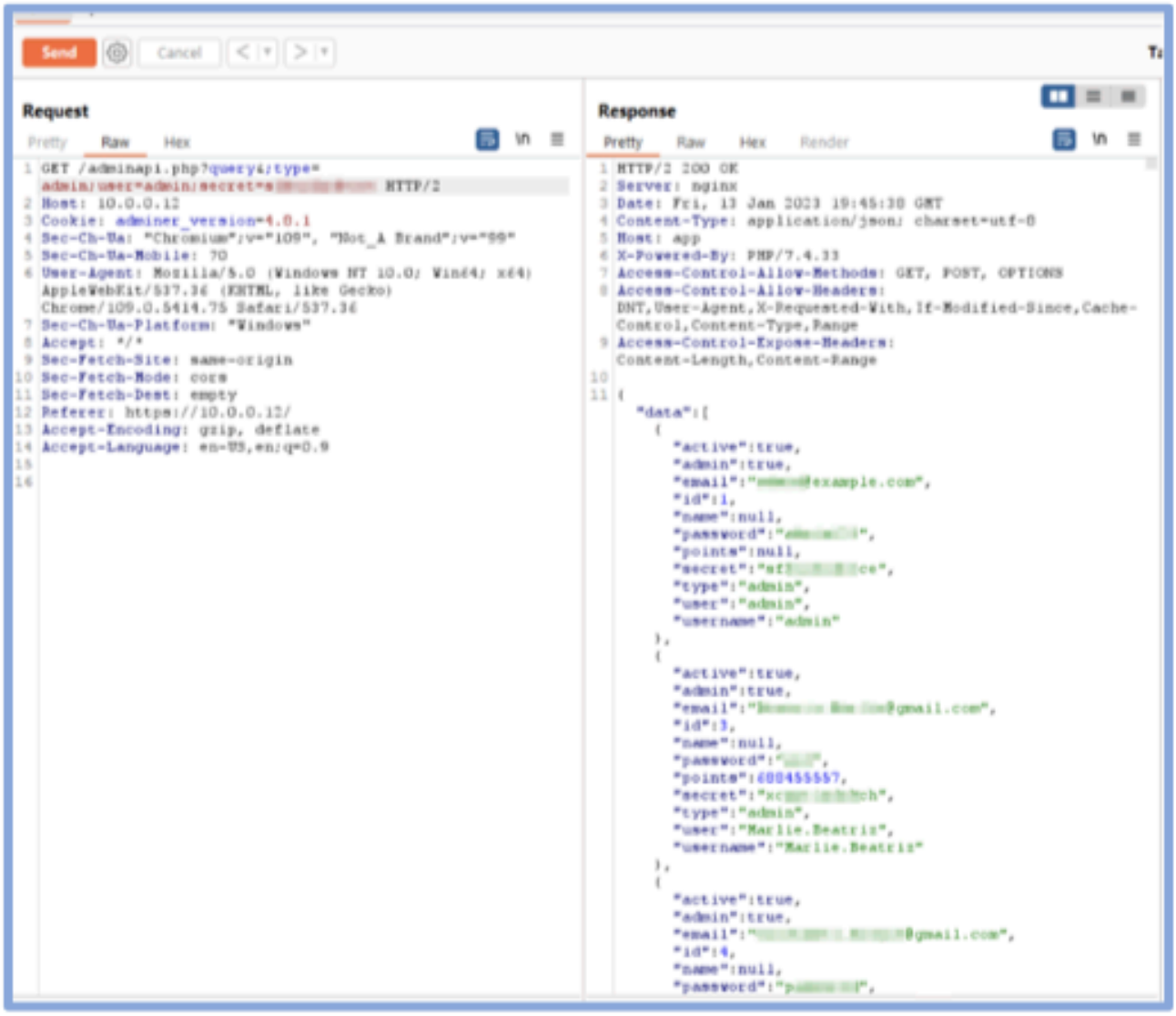
blocked all probes to the internal network however it can be seen that probes sent through the pivot point reveal what ports are open on the corporate hosts.



Finding TCC014: Plaintext PII and Credential Disclosure via Rewards Portal	
Affected Hosts	10.0.0.12
CVSS: 7.1 | High	**Likelihood: Low** Exploitation of this vulnerability requires an attacker to have access to the corporate network, have an admin credential to the rewards portal, and make a specific request to an API endpoint. All three combined make this unlikely to be exploited, but still very possible. **Technical Impact: High** The data found from this exploit provides an attacker with email addresses, usernames, passwords, secrets, and more. These credentials were also used to gain access to the payment portal, resulting in a large loss of confidentiality.
Vulnerability Description	The functionality of the rewards portal allows users to be queried for information. However, these queries' responses include plain-text passwords and other sensitive information related directly to customers. If an administrator secret is acquired, the entire database of customer information can be dumped with a single API call.
Business Impact	The information obtainable by leveraging this vulnerability reveals sensitive information about The Cozy Croissant's customers. This violates both privacy agreements with the customers and PCI-DSS. If a leak of this data were to occur, customer's confidence in the security of their information would be significantly degraded.
Requirements to exploit	Access to corporate network, administrator login to rewards portal.
Remediation	Edit the code for this API to prevent it from providing the sensitive customer information. Administrators should not need access to the passwords and secrets of other users.

Proof of Concept:

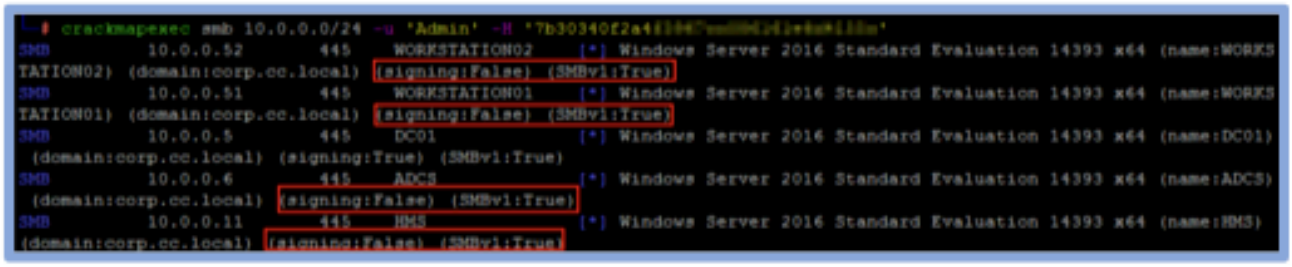
The request to make the dump of this data is as follows:



Finding TCC015: SMB Signing Disabled	
Affected Hosts	10.0.0.6,11,51,52
CVSS: 7.0 | High	**Likelihood: High** It is easy for an attacker to check if SMB signing is not enforced. It does not require any credentials for this attack to be carried out. **Technical Impact: High** Relay attacks that are made possible as a result of SMB signing not being enforced give an attacker credentials from users and allow them to potentially gain console access immediately.
Vulnerability Description	This vulnerability allows for an attacker to exploit a slew of SMB attacks. Most prominently SMB relay attacks that exploit a man in the middle type attack allow for the capturing of user hashes and information which can lead to system access through hashes or cracked passwords.
Business Impact	After an attacker grabs credentials using this attack, they would have access to more systems in The Cozy Croissant's network. This would lead to loss of availability, integrity, and confidentiality.
Requirements to exploit	MITM6, NLTMrelayx, Responder, Internal Network Access
Remediation	Require SMB signing on all Windows computers in the network. This policy should not only be enabled but should be enforced on every machine. An example of this is on 10.0.0.5 where it is enforced and prevents attacks of this type.
References	https://www.rapid7.com/db/vulnerabilities/cifs-smb-signing-disabled/ https://techcommunity.microsoft.com/t5/storage-at-microsoft/configure-smb-signing-with-confidence/ba-p/2418102

Proof of Concept:

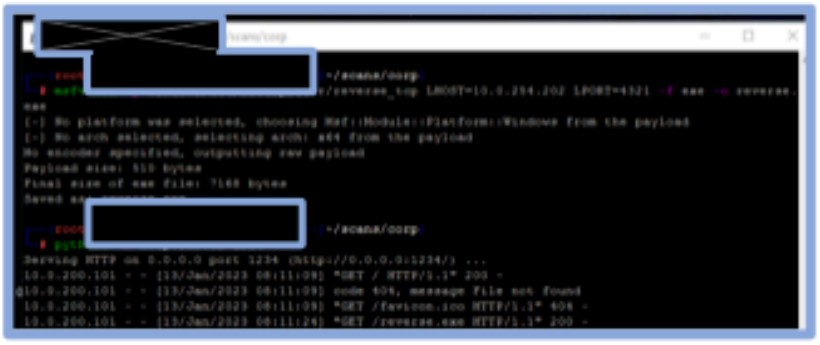
Below is a screenshot showing all four machines with SMB signing not enforced.



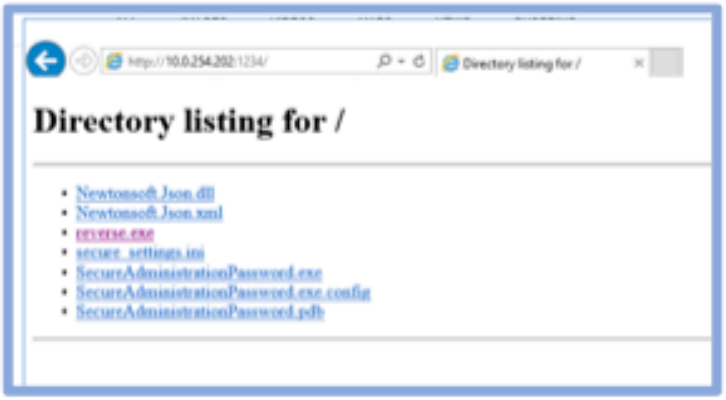
Finding TCC016: Insecure Execution Policy	
Affected Hosts	10.0.200.101-4
CVSS: 6.6 | Medium	**Likelihood:** An adversarial threat would likely compromise this lack of security controls as it is the publicly accessible kiosks that are affected. **Technical Impact:** The result of exploiting this vulnerability is unrestricted Administrator command line access. In addition, this attack results in a pivot point for attackers to utilize to reach the corporate network circumventing the network ACLs.
Vulnerability Description	This vulnerability is the lack of a security control preventing the use of executable files potentially containing malware or other malicious intentions. In our case, it resulted in the execution of a meterpreter reverse shell for the Administrator user.
Business Impact	From a business perspective, this vulnerability in itself can lead to a loss in confidentiality, integrity, and accessibility for the kiosk systems. Additionally, this vulnerability can lead to a change in scope for the attacker which can lead to further attacks on more critical infrastructure.
Requirements to exploit	The threshold for this attack vector is slightly complex however, the only requirement to launch an attack such as this is the breaking out of the restricted kiosk environment.
Remediation	A remediation for this vulnerability is to change the user running the underlying kiosk mode away from Administrator and give that user the least possible permissions. Another potential remediation is the investment into custom or commercial kiosk-specific software.

Proof of Concept:

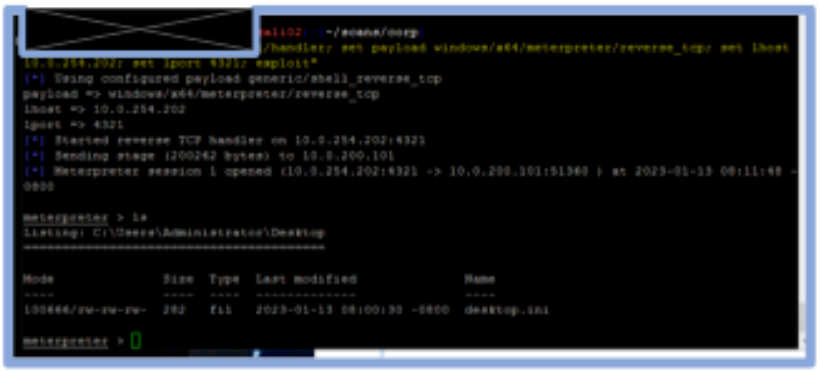
1. Repeat steps in Finding (TCC006) to break out of Kiosk systems
2. Host a reverse shell on the attacking host.



3. Navigate to and download the hosted reverse shell on the victim machine.



4. Setup a listener on the attacking host and execute the reverse shell to gain meterpreter shell access.

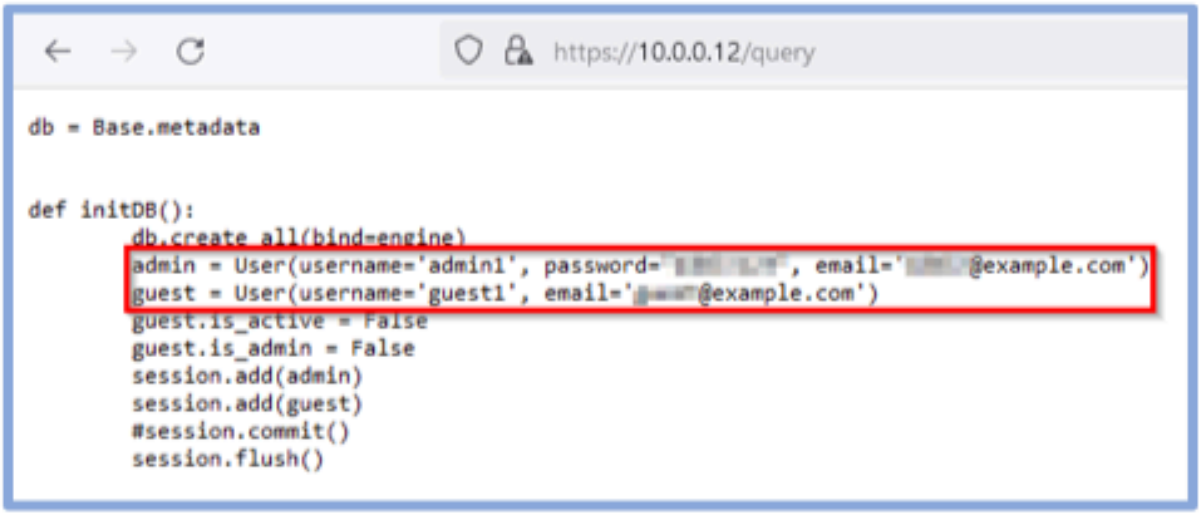


Finding TCC017: Source Code and Plaintext Credential Disclosure	
Affected Hosts	10.0.0.12
CVSS: 6.5 | Medium	**Likelihood: Medium** The endpoint (/query) is not hyperlinked anywhere on the webpage, so finding it is not obvious. Additionally, the attacker must have access to the corporate network. **Technical Impact: Medium** The /query endpoint contains information about the backend code that initialized the database as well as some of the data in it, including some valid credentials that provide admin access to the rewards application.
Vulnerability Description	This vulnerability hosts a Python file that initializes a database. While it is not executable, it provides an attacker with critical information about the structure of the database and valid user credentials for the web application the database supports.
Business Impact	The disclosure of this information does not directly cause impact to the functioning of the business. However, it assists attackers with future attacks against the system, which may have catastrophic consequences.
Requirements to exploit	Access to the corporate network
Remediation	Remove this file from a hosted directory and remove the passwords from the code to prevent an accidental leak of cleartext credentials.

Proof of Concept:

The following webpage is accessible to anyone with access to the corporate network and contains sensitive information:

(See next page)

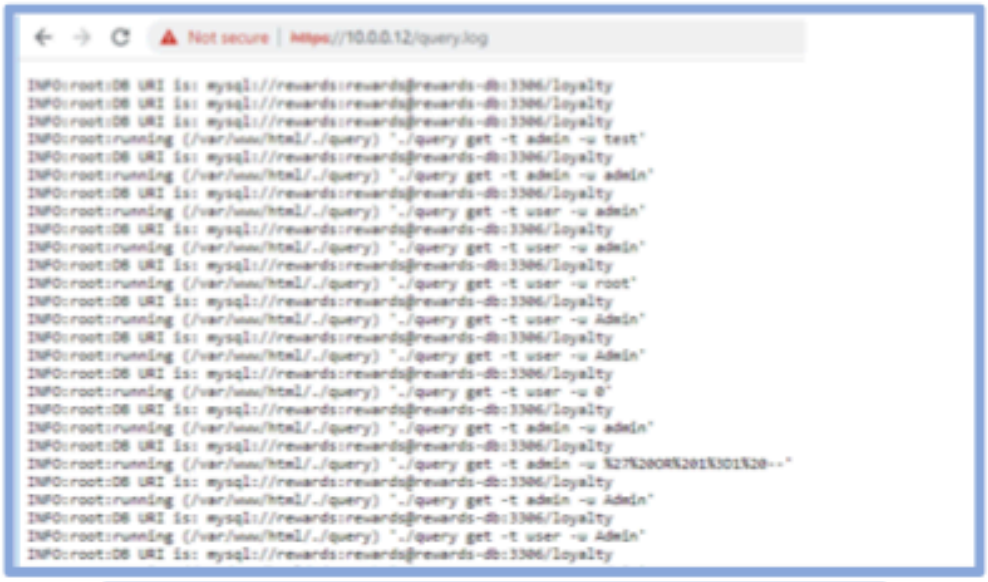


Finding TCC018: Publicly Accessible Query Logs	
Affected Hosts	10.0.0.12
CVSS: 6.5 | Medium	**Likelihood: Medium** The file containing the logs (query.log) is not hyperlinked anywhere on the webpage, so finding it is not obvious. Additionally, the attacker must have access to the corporate network. **Technical Impact: Medium** query.log contains information about the functionality of the API, usernames, and secrets. These secrets can be used with the API to gain access to confidential data.
Vulnerability Description	This vulnerability is a result of the API logging queries to a web-hosted directory (likely /var/www/html/). Thus, it is accessible to anyone with accessibility to the website.
Business Impact	The disclosure of this information does not directly cause impact to the functioning of the business. However, it assists attackers with future attacks against the system, which may have catastrophic consequences.
Requirements to exploit	Access to the corporate network
Remediation	Remove this file and move the system's logging location to a non-hosted directory and remove secrets from the logs.

Proof of Concept:

The following webpage is accessible to anyone with access to the corporate network and contains sensitive information:

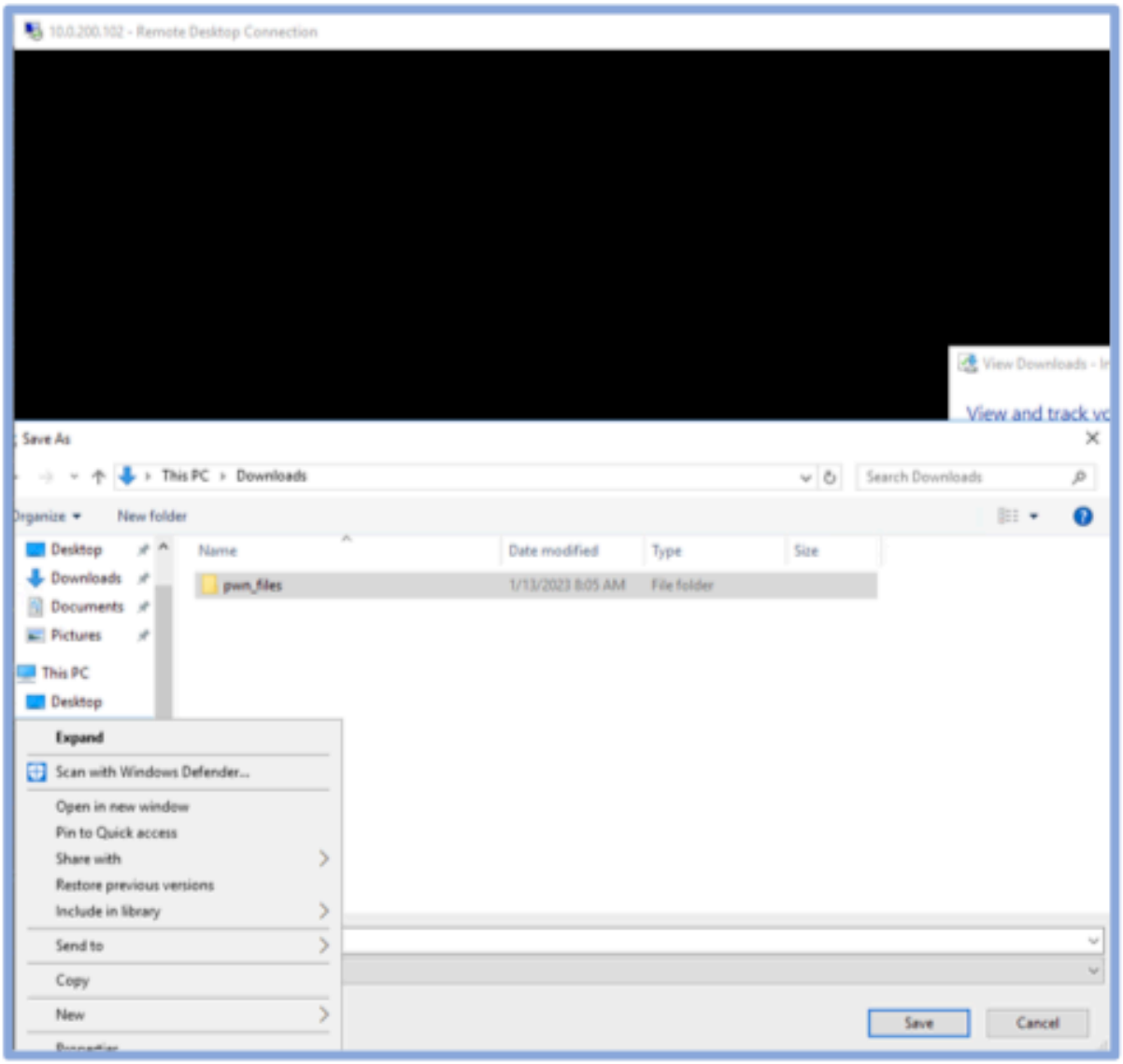
(See next page)



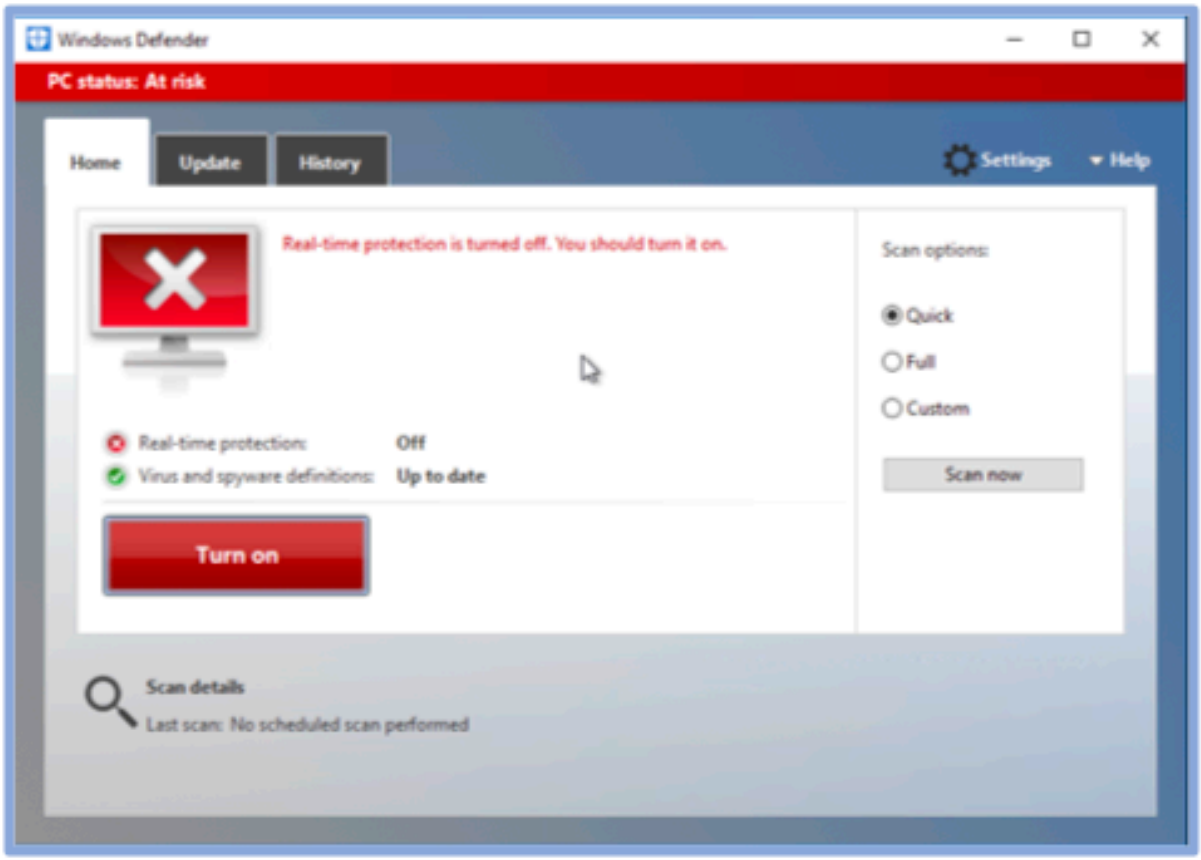
Finding TCC019: User-Editable Windows Defender State from Kiosk	
Affected Hosts	10.0.200.100 - 104
CVSS: 6.5 | Medium	**Likelihood: Medium** This vulnerability can be exploited with few steps, most of which are relatively straightforward. However, getting from the file manager to Windows Defender takes some out-of-the-box thinking. **Technical Impact: Medium** While Windows Defender was not enabled when the systems were provided for testing, this vulnerability still allows an attacker to turn it off if future security controls are implemented using Windows Defender.
Vulnerability Description	By taking some unintended actions in the kiosk mode of the computer, the Windows Defender console is accessible to any user.
Business Impact	Windows Defender is an important part of a defense-in-depth strategy to prevent cyber attacks against The Cozy Croissant. While this vulnerability does not directly cause any negative effects against the business operations, it can lead to other vulnerabilities being exploited, which can have catastrophic consequences.
Requirements to exploit	Access to the kiosk
Remediation	Utilization of well-developed kiosk lock software will prevent attackers from abusing the misconfigurations of the current in-house system (provided it is properly configured) and would provide tighter controls over the actions a user can take on the kiosk. Changing the default kiosk user to an unprivileged account would also prevent the later phases of this vulnerability from being exploited.

Proof of Concept:

1. Right click the image on the default web page and select "Save Image As"
2. Right click any folder in the file manager pop up and select "Scan with Windows Defender"



3. Change settings as desired



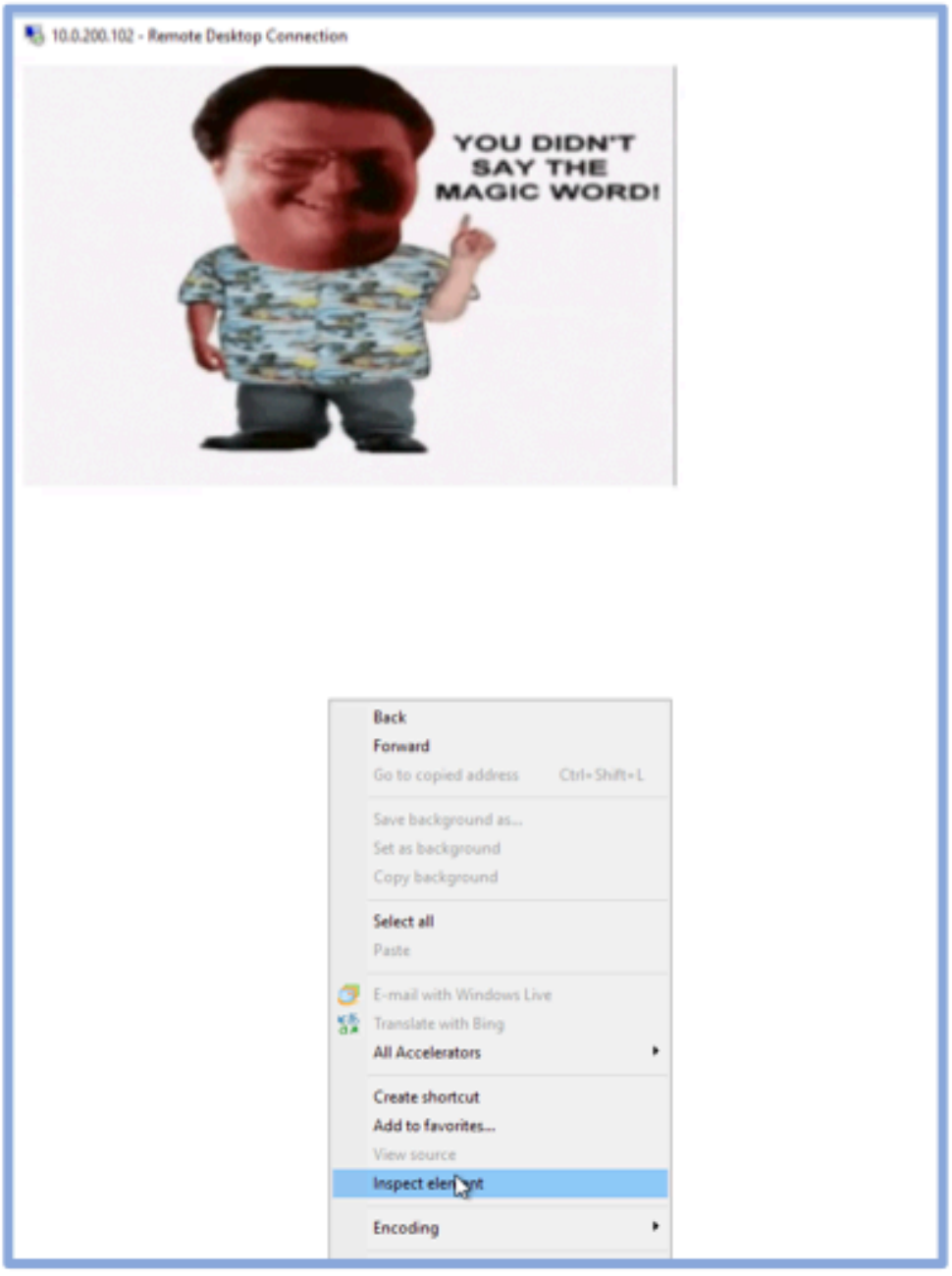
Finding TCC020: Kiosk Breakout to New Window	
Affected Hosts	10.0.0.101 - 104
CVSS: 6.5 | Medium	**Likelihood: High** This attack is easy to perform and available to be exploited as soon as the computer is accessed by an attacker. **Technical Impact: Medium** Kiosk breakout vulnerabilities provide attackers with more access to the functionality of the computer than intended. This can lead to future exploits or other malicious actions to be taken on the machine. As the guest network also has access to the corporate network, user-controlled browsing can disclose internal information.
Vulnerability Description	Any user of the kiosk can open a new browser window that allows for unrestricted internet browsing.
Business Impact	This vulnerability allows both visitors to The Cozy Croissant and attackers to take more actions on the kiosk computers than intended such as browsing to undesired sites, including sites that violate the family-friendly culture of The Cozy Croissant and sites that contain malicious content. In addition, having the kiosks not working properly degrades a customer's trust in the security of The Cozy Croissants systems.
Requirements to exploit	Access to the kiosk
Remediation	Utilization of well-developed kiosk lock software will prevent kiosk breakouts from occurring through exploitation of flaws in the environment (provided it is properly configured).

Proof of Concept:

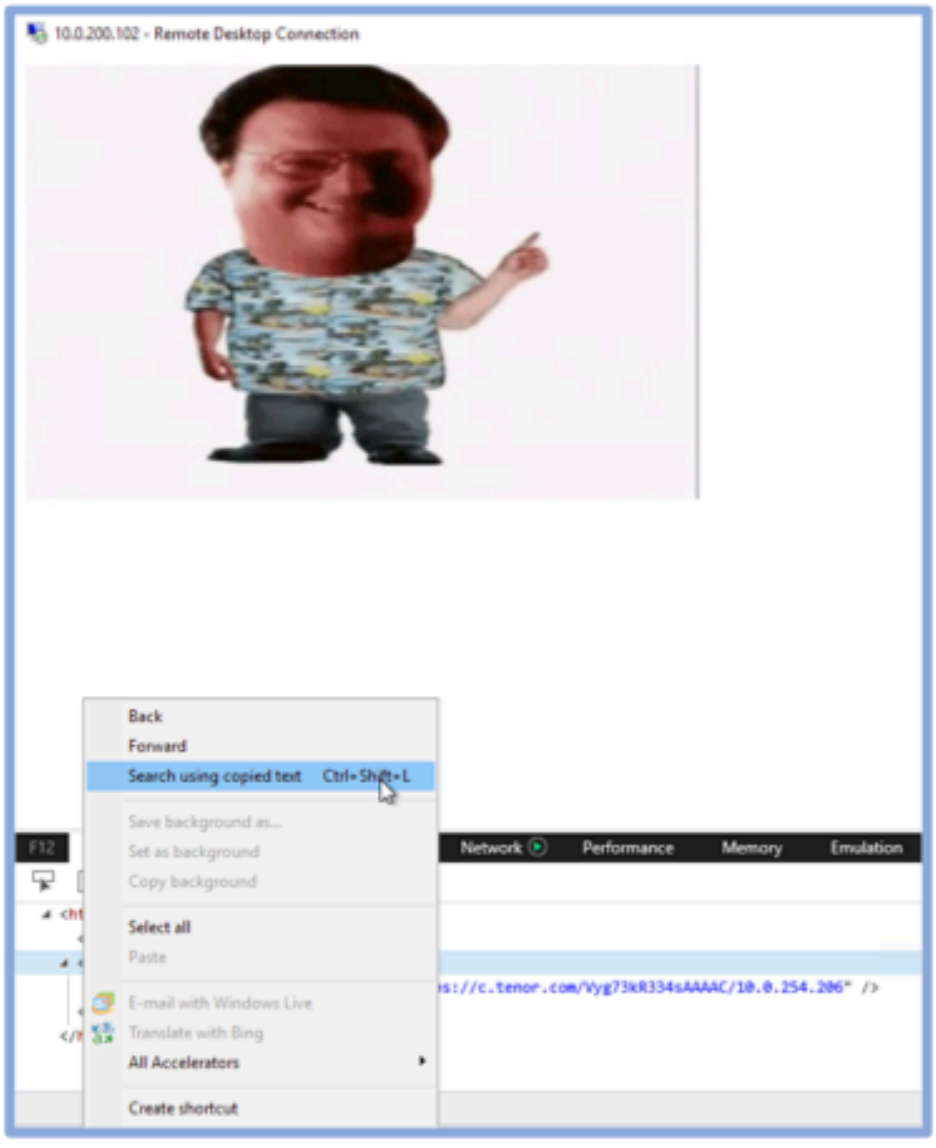
Method 1:

1. Access the kiosk through standard means
2. Right click > inspect element > copy any text

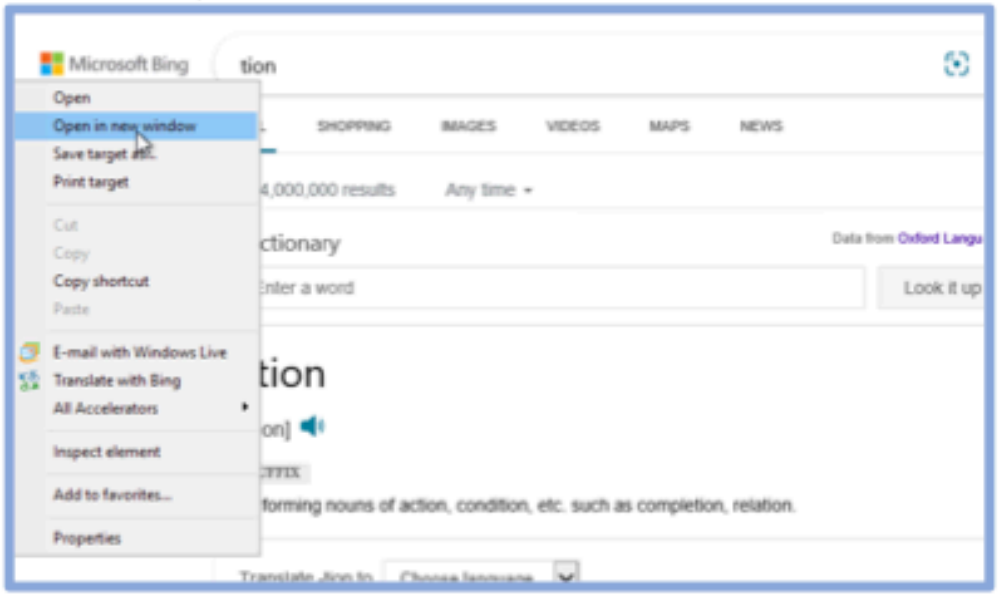
(Continued on next page)



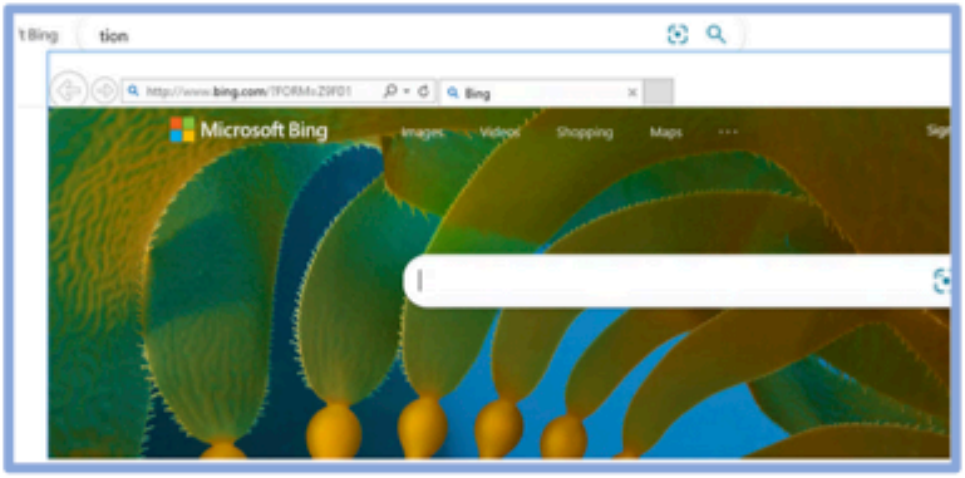
3. Right click > Search using copied text



4. Right click a link > open in new window



5. A new browser window (with the address bar available) will open up.

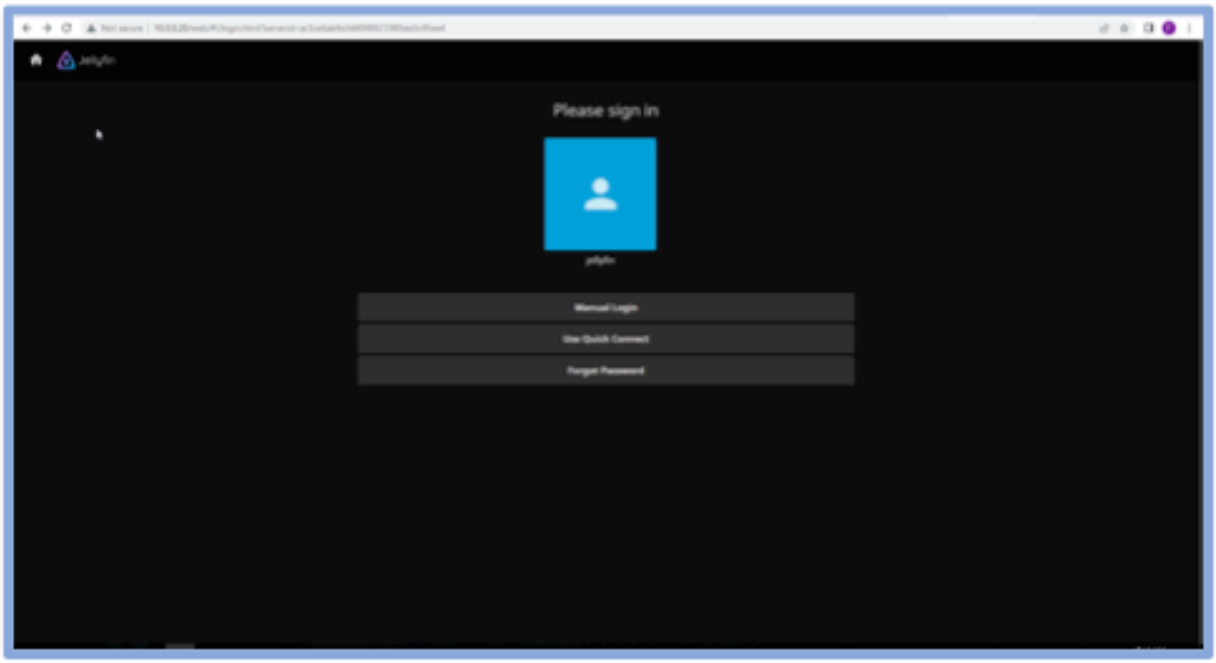


Finding TCC021: Automatic Sign in for Admin Jellyfin User	
Affected Hosts	10.0.0.20
CVSS: 6.3 | Medium	**Likelihood: High** As soon as the web UI for Jellyfin is loaded, the user is presented with the option of signing in as an admin user without requiring credentials. Anyone with access to the internal network can exploit this. **Technical Impact: Medium** The administrator account (jellyfin) on Jellyfin has access to removing media files from the server, preventing employees and guests from accessing them.
Vulnerability Description	Jellyfin allows for the configuration of users to be logged in with a single click, without authorization. The account that was configured as the default login (jellyfin) was an administrator, allowing anyone with access to the site to access the administrator dashboard.
Business Impact	The content desired to be served through the Jellyfin system can be permanently deleted through this vulnerability, removing guests' ability to access the media.
Requirements to exploit	Access to host
Remediation	Create a new user to be the default login user (if such functionality is desired) and require authentication to access the "jellyfin" user.

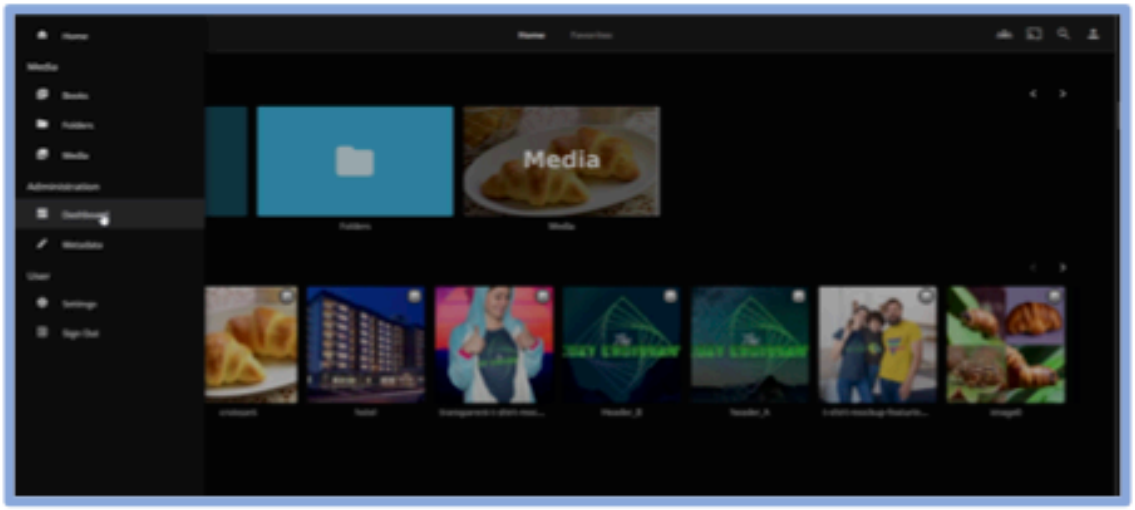
Proof of Concept:

(See next page)

Default login page:



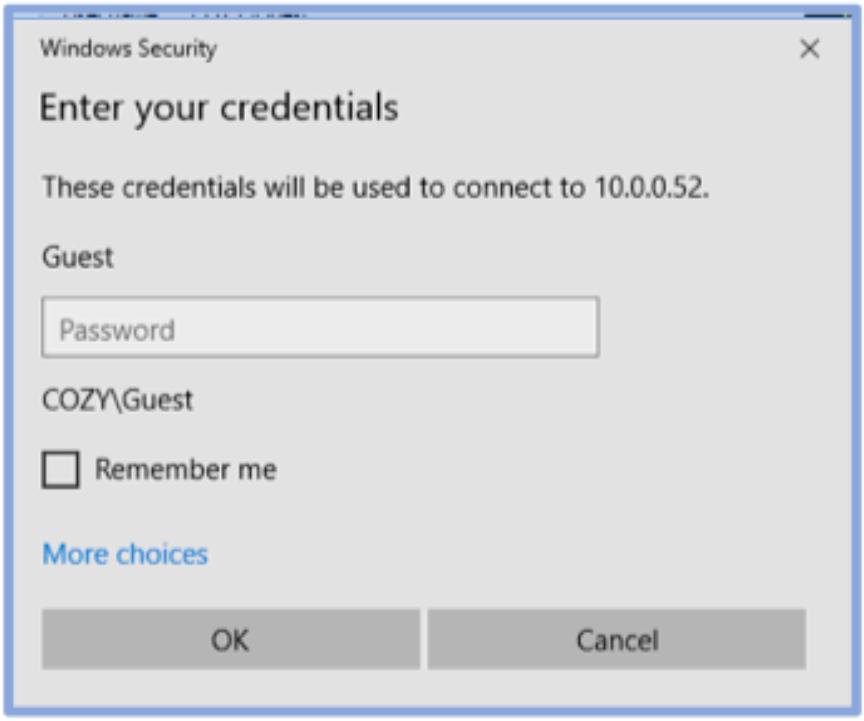
This user can access the administration dashboard



Finding TCC022: Guest Account Present	
Affected Hosts	10.0.0.51-52
CVSS: 6.3 | Medium	**Likelihood: Medium** There are no credentials required for this vulnerability. An attacker with access to the corporate network could easily connect via RDP to the workstation systems with the guest account. **Technical Impact: Medium** If this attack is exploited, an attacker could gain a foothold onto the workstation systems. This could lead to further enumeration and exploitation.
Vulnerability Description	An attacker with access to the corporate network can use RDP to login with the guest account and no password to the two workstations. This allows the attacker to gain initial access to the systems.
Business Impact	If an attacker can gain access to the workstations, there is a high risk that they could gain access to sensitive data stored on the system. Additionally, this vulnerability demonstrates a violation of PCI-DSS. The Cozy Croissant can be fined heavily by payment processors and credit card companies for any PCI-DSS violations.
Requirements to exploit	An attacker is required to have access into the corporate network and the ability to use RDP.
Remediation	The guest account should be removed from the affected hosts.

Proof of Concept:

Logging in via RDP with the guest account and no password:



Guest user's account settings showing no password required:

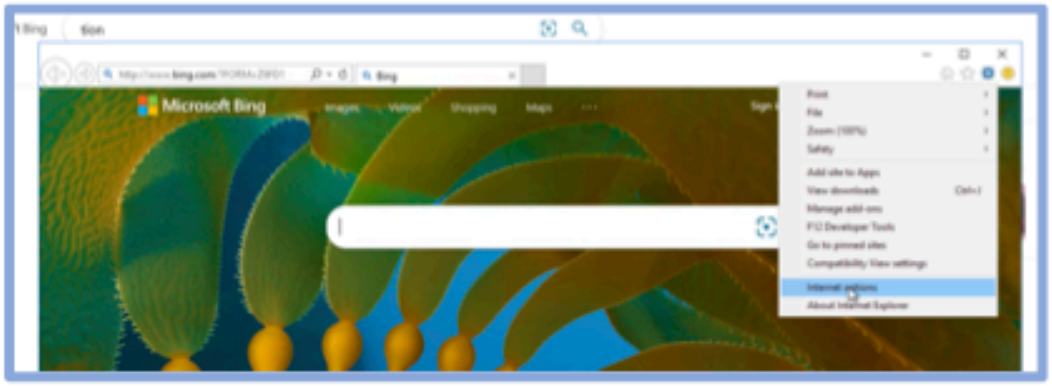
```
C:\Users\Guest>net user guest
User name                    Guest
Full Name
Comment                      Built-in account for guest access to the computer/domain
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            1/10/2023 6:14:55 AM
Password expires             Never
Password changeable          1/10/2023 6:14:55 AM
Password required            No
User may change password     No
```

Finding TCC023: User-Editable Internet Explorer Security Settings	
Affected Hosts	10.0.200.101 - 104
CVSS: 5.3 | Medium	**Likelihood: Medium** This exploit requires the kiosk system to be broken out of, with access to a full browser window. Due to another exploit discovered that allows this to happen with ease, this would not be a difficult follow-up vulnerability to exploit. **Technical Impact: Medium** Editing the security settings for Internet Explorer allows malicious webpages and files to be accessed, further compromising the system.
Vulnerability Description	This vulnerability allows a user who has broken out of the kiosk to edit the security settings of the Internet Explorer browser without authentication or authorization, compromising the security posture of the system.
Business Impact	This vulnerability lessens the security controls setup on the system. While not a destructive action in itself, it leads to exploitation of further vulnerabilities, which can have significant impact on the system.
Requirements to exploit	Access to the kiosk, method to access a full browser window
Remediation	Utilization of well-developed kiosk lock software will prevent access to the security settings menu of the browser (provided it is properly configured).

Proof of Concept:

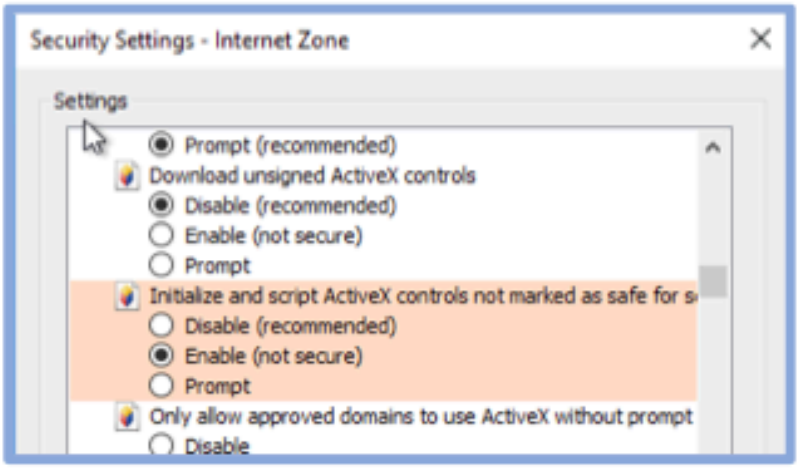
1. Access the kiosk and open a new browser window

2. Select the settings icon > internet options



3. Select security tab > custom level

4. Select changes to the security settings

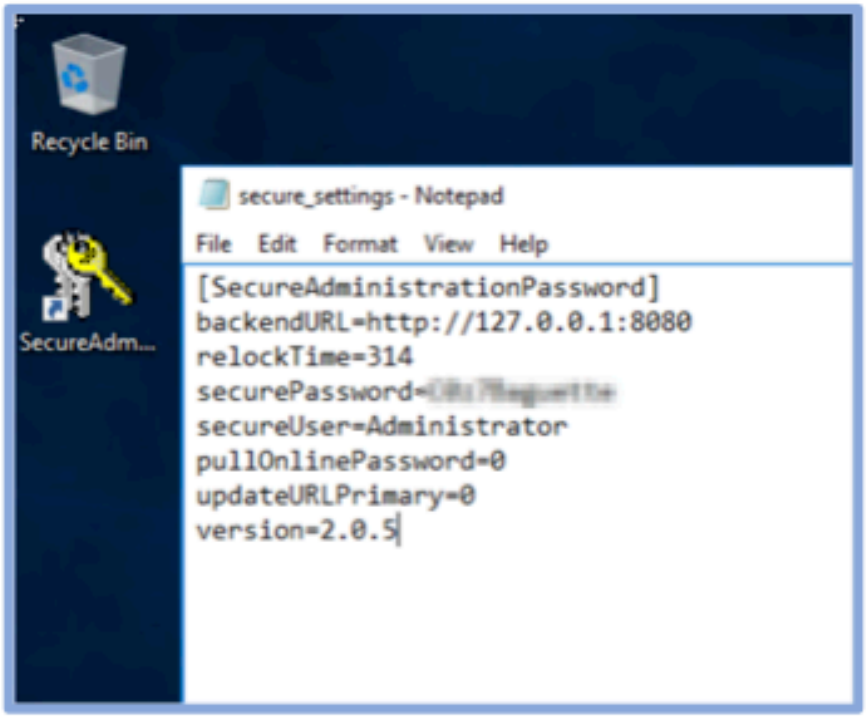


5. Click okay then apply and close the settings window

Finding TCC024: Insecure Code Logic	
Affected Hosts	10.0.200.0/24, 10.0.0.5,6,11,51,52
CVSS: 5.3 | Medium	**Likelihood: Medium** Due to this application being easily accessible and installed on every windows machine it is highly likely that an attacker with access will exploit this error in code logic. **Technical Impact: Medium** The hard-coded reuse of passwords for the SecureAdministrationPassword application will inherently cause company-wide password reuse. The impact of password reuse is the risk of a single point of failure leading to a total network compromise.
Vulnerability Description	After investigating the functionality of the executable it was seen that although it seemed the initial intent was to be a password generator that pulled secure passwords from a site called "dinopass"
Business Impact	An attacker with possession of this password tool would be able to likely compromise multiple accounts that used this application to set their passwords. This can lead to vital corporate information being exposed along with likely issues regarding service availability.
Requirements to exploit	In order to access this application either an attacker would simply have to have access to any windows machine on either the corporate or guest network. Vectors of attack could include breaking out of one of the kiosk environments or logging into one of the workstations using the guest account without a password.
Remediation	In order to properly fix the functionality of this application, the hard-coded values must be removed and the initial intent for dynamically pulling a password from the specified external source would need to be properly implemented. At that point, this application would be a valuable asset for The Cozy Croissant.

Proof of Concept:

The hard-coded settings for this application are seen in the same directory as the application itself. These settings set the value for the user and password and additionally set the option to pull a password online to off or 0.

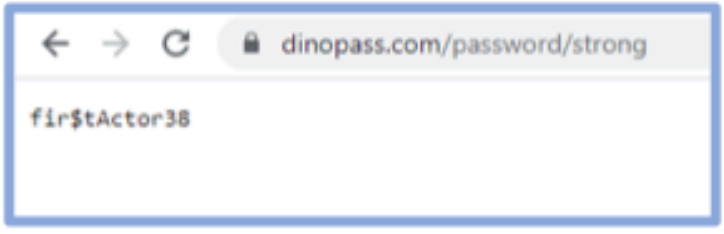


The code logic that sets the initial settings for this application is seen in the following screenshot. The repeated password and username are seen to be hard-coded.

```
// Token: 0x0600001E RID: 30 RVA: 0x00003120 File Offset: 0x00001520
public static void Initialize(string iniFile)
{
    IniFile SAPINI = new IniFile(iniFile);
    bool flag = !SAPINI.KeyExists("version", null);
    if (flag)
    {
        SAPINI.Write("backendURL", "http://localhost:9981", null);
        SAPINI.Write("relockTime", "120", null);
        SAPINI.Write("securePassword", "[redacted]", null);
        SAPINI.Write("secureUser", "Administrator", null);
        SAPINI.Write("pullOnlinePassword", "0", null);
        SAPINI.Write("updateURLPrimary", "0", null);
        string verstr = "2.0.5";
        SAPINI.Write("version", verstr, null);
        Program.SetState("version", verstr, false, true);
        Console.WriteLine("No INI File Detected, creating one now.");
    }
    else
    {
        Program.SetState("version", SAPINI.Read("version", null), false, true);
    }
    bool flag2 = SAPINI.KeyExists("backendURL", null);
    if (flag2)
    {
        Program.SetState("backendURL", SAPINI.Read("backendURL", null), false, true);
```

The code logic that should pull down a unique password every time it is triggered is seen below. If this logic is implemented instead of the former this application will increase overall security immensely. Additionally, a sample password from the queried password is seen below which demonstrates the potential benefit a secure version of this application can provide.

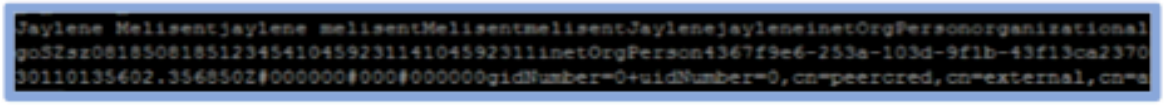
```
// Token: 0x06000020 RID: 32 RVA: 0x00003864 File Offset: 0x00001A64
public static void GetPasswordOnline()
{
    WebRequest request = WebRequest.Create("https://www.dinopass.com/password/strong");
    request.Credentials = CredentialCache.DefaultCredentials;
    HttpWebResponse response = (HttpWebResponse)request.GetResponse();
    Console.WriteLine(response.StatusDescription);
    Stream dataStream = response.GetResponseStream();
    StreamReader reader = new StreamReader(dataStream);
    string responseFromServer = reader.ReadToEnd();
    Console.WriteLine("Password from Online DinoPass API: '" + responseFromServer + "'");
    Program.SetState("securePassword", responseFromServer.TrimStart(new char[0]).TrimEnd(new char[0]).Trim(), false, true);
    reader.Close();
    dataStream.Close();
    response.Close();
}
```

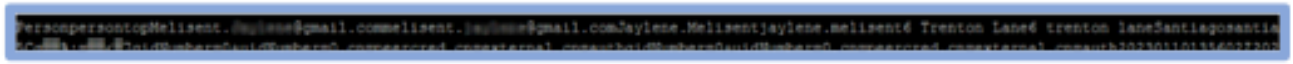


Finding TCC025: Unencrypted Customer PII in LDAP Database	
Affected Hosts	10.0.0.100
CVSS: 4.9 | Medium	**Likelihood: Low** Root credentials are needed to access this database. **Technical Impact: Low** Technically, this vulnerability does not present much impact. The primary technical usage of it would be to predict usernames and for social engineering purposes. However, within the context of securing customer data, it is incredibly impactful.
Vulnerability Description	The /var/lib/ldap/data.mdb file in the app-ldap-1 Docker container on the host contains unencrypted personally identifiable information (PII) about customers. This is accessible to the root user on the host.
Business Impact	Customers trust The Cozy Croissant to protect their personal data from exposure in accordance with the agreed-upon privacy policy. This vulnerability violates the privacy policy and PCI-DSS, eroding customer confidence in The Cozy Croissant and renders the company PCI-DSS non-compliant.
Requirements to exploit	Root access to the system
Remediation	Implementing an encryption standard compatible with the software running on the system will ensure that the data is only accessible through the intended means.

Proof of Concept:

The following two screenshots are example snippets of the file:

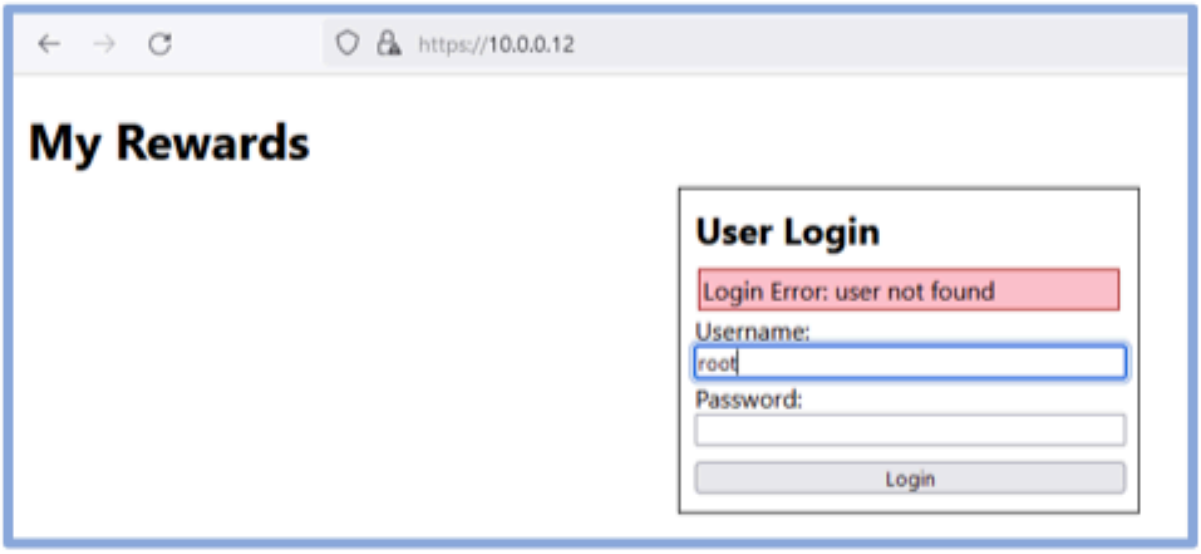


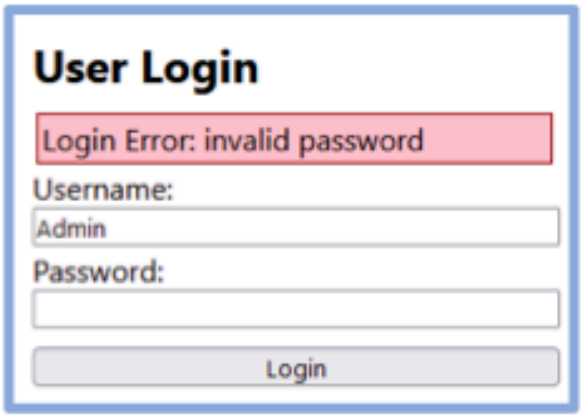


Finding TCC026: Username Discovery	
Affected Hosts	10.0.0.12
CVSS: 4.5 | Medium	**Likelihood: High** Unauthenticated users can easily access the web form without any special tools, experience, or known credentials. **Technical Impact: Medium** Unauthenticated users can determine whether a given username is invalid, and by extension, whether it is valid.
Vulnerability Description	If an outside user navigates to the hosted website and attempts to log in with a username that does not exist, the website returns the message "Login message: user not found". If the username does exist but the incorrect password is given, the website returns the message "Login error: invalid password". This allows the unauthenticated user to discover valid usernames by trial and error.
Business Impact	This exploit allows unauthorized users to discover system usernames, which decreases the security of TCC's systems and data.
Requirements to exploit	Access to the internal corporate network is the only requirement to exploit this vulnerability.
Remediation	Modify website error messages so that a generic response is given for incorrect credentials.

Proof of Concept:

1. The unauthenticated user navigates to the hosted website on 10.0.0.12.
2. The unauthenticated user attempts to log in with a username that does not exist (root).
3. The unauthenticated user attempts to log in with a username that does exist (with no password).
4. Unauthenticated users can determine if attempted usernames are valid based on error messages.

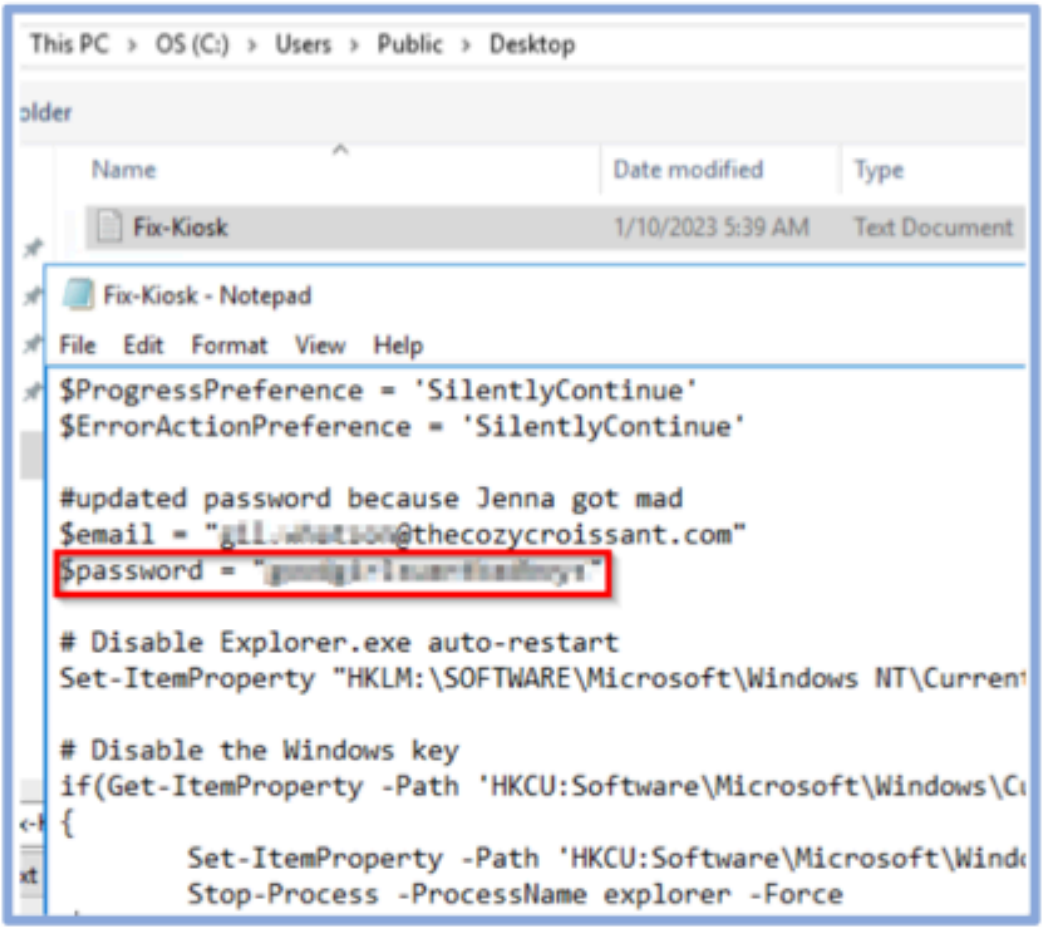




Finding TCC027: Plaintext Credential and Source Code Disclosure	
Affected Hosts	10.0.200.103
CVSS: 4.3 | Medium	**Likelihood: Medium** No credentials are needed as this file is accessible on KIOSK3, which is publicly accessible. This file is accessible on the desktop of the kiosk and only requires the user to break out of the kiosk program to access. **Technical Impact: Medium** This vulnerability discloses Gil Whatson's email address and password. This could allow attackers to impersonate Gil Whatson and send phishing emails or login as Gil.
Vulnerability Description	If an attacker can break out of the kiosk restrictions, they would be able to navigate to the C:\Users\Public\Desktop\ directory and access the Fix-Kiosk.txt file which contains Gil Whatson's email address and password in plaintext.
Business Impact	The information in this file can allow an attacker to create a convincing phishing attack or sign into a system as Gil. This gives an attacker the ability to damage any system Gil has access to modify.
Requirements to exploit	Ability to break out of kiosk
Remediation	This file should not be accessible on the public user's desktop or contain plaintext credentials. This file should be moved to a more secure location and remove the password from the file.

Proof of Concept:

Once the kiosk software is broken out of, the file can be accessed either on the desktop, or through the File Explorer and navigating to the C:\Users\Public\Desktop\ directory.



Finding TCC028: Vulnerable Service Version - SMBv1	
Affected Hosts	10.0.0.5,6,11,51,52
CVSS: 4.3 | Medium	**Likelihood: Medium** SMB version is easy to find and enumerate. User credentials would be required to execute any malicious actions. **Technical Impact: Medium** An attacker can cause a denial of service on affected machines as well as potential remote code execution in certain scenarios.
Vulnerability Description	SMBv1 is an old version of the SMB protocol that is vulnerable to multiple denial of service attacks as well as some remote code execution.
Business Impact	Denial of service is very dangerous for The Cozy Croissant as there are multiple critical computers running important portions of the business. If these attacks were carried out it would certainly affect the availability of TCC.
Requirements to exploit	Internal network access, valid user credentials.
Remediation	Upgrade to SMBv3 and apply the latest patches to the service.
References	https://techcommunity.microsoft.com/t5/storage-at-microsoft/stop-using-smb1/ba-p/425858

Proof of Concept:

Scan for machines with the older version

```
nmap -p445 10.0.0.0/24 --script smb-protocols
```

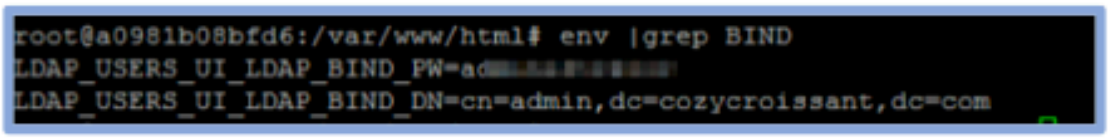
```
Host script results:
| smb-protocols:
|   dialects:
|     NT LM 0.12 (SMBv1) [dangerous, but default]
|     2.0.2
|     2.1
|     3.0
|     3.0.2
|_    3.1.1
```

Finding TCC029: Plaintext Credential Disclosure	
Affected Hosts	10.0.0.102
CVSS: 4.3 | Medium	**Likelihood: Medium** To exploit this vulnerability, an attacker must have access to the internal network and root credentials to the host. However, the password is in plaintext, making it trivial to access once the host is logged into. **Technical Impact: Medium** This password was determined to only be valid for the webapp served by the host. This account is an administrator account, however, so the impact is greater than a regular user. Thus, all functionality of the webapp should be considered accessible to an attacker who exploits this vulnerability.
Vulnerability Description	This vulnerability allows attackers to gain plaintext credentials for the webapp served by this host. The credentials are accessible because the application uses environment variables to store them for use in scripts and applications. While this is easy to implement, it is not secure.
Business Impact	Any user with this credential can edit details about LDAP accounts on the network. This can potentially disrupt the availability of users on the corporate network from utilizing network resources.
Requirements to exploit	Access to corporate network, root credentials for host
Remediation	The use of either hashed passwords for storage, or a centralized secrets repository should be used to make sure that no references to passwords are the plaintext credentials themselves.

Proof of Concept:

The following credential pair is accessible through these steps:

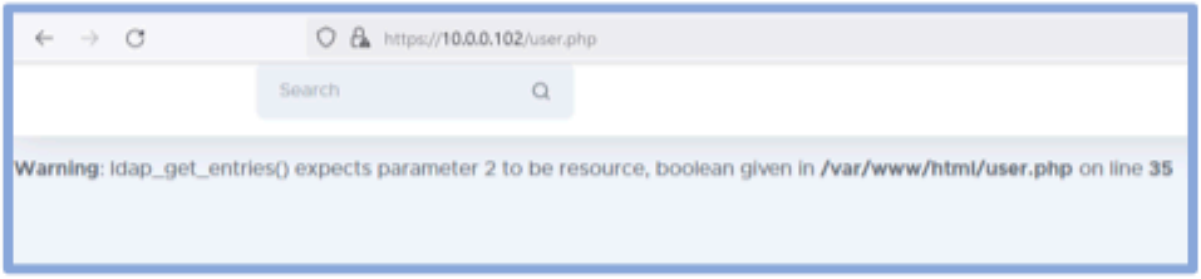
1. Login to host as root
2. Connect to the app-ldap-users-ui-1 Docker container with a shell
3. Run the "env | grep BIND" command to receive the following output.



Finding TCC030: Improper Error Handling	
Affected Hosts	10.0.0.102
CVSS: 3.5 | Low	**Likelihood: Medium** Anyone with access to the guest or corporate network can access this web page and view the errors if they provide incorrect input. **Technical Impact: Low** This error discloses the existence and path of a PHP file hosted on the web server and a protocol utilized by it (LDAP).
Vulnerability Description	This vulnerability occurs when the login page does not receive valid input. The script errors out and prints error information to the browser, giving an attacker more information about the environment.
Business Impact	This gives information to an attacker that could lead to further exploitation of The Cozy Croissant's infrastructure.
Requirements to exploit	Access to internal network.
Remediation	Implement a proper error page to be served to the user if any errors occur on the server.

Proof of Concept:

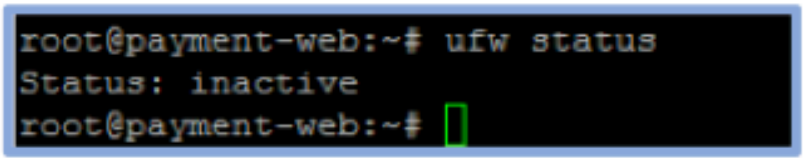
This is the error displayed when the page errors out:



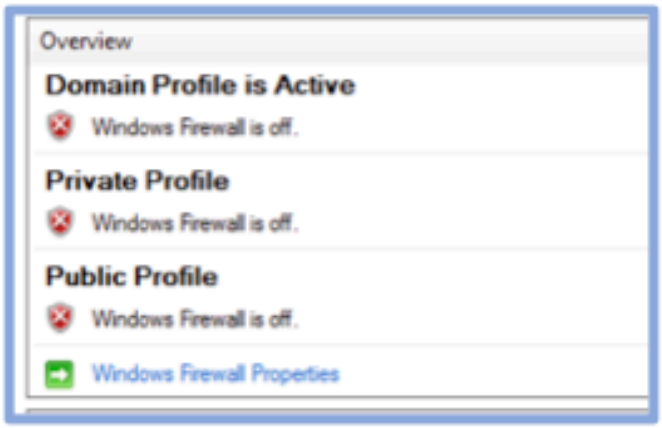
Finding TCC031: Improperly Configured System Firewalls	
Affected Hosts	10.0.0.5-7, 10.0.0.11-12, 10.0.0.20, 10.0.0.51-52, 10.0.0.100, 10.0.0.102, 10.0.0.200, 10.0.0.210
CVSS: 1.0 | Low	**Likelihood: Medium** It is likely that an attacker could send malicious traffic to the affected hosts with little to no restrictions. **Technical Impact: Low** Attackers can access ports that are not necessary for system functionality and the system may be able to send data over undesired
Vulnerability Description	The Windows and Linux firewalls have not been configured to limit inbound and outbound traffic.
Business Impact	This vulnerability, while not necessarily directly exploitable, has a large potential business impact due to PCI-DSS violations. The Cozy Croissant can be fined heavily by payment processors and credit card companies for any PCI-DSS violations.
Requirements to exploit	There are no requirements for exploitation.
Remediation	Configure firewall rules on the systems to only allow inbound and outbound traffic that is necessary for the services running on the systems.
References	

Proof of Concept:

Linux systems have their firewall (UFW) set to inactive.



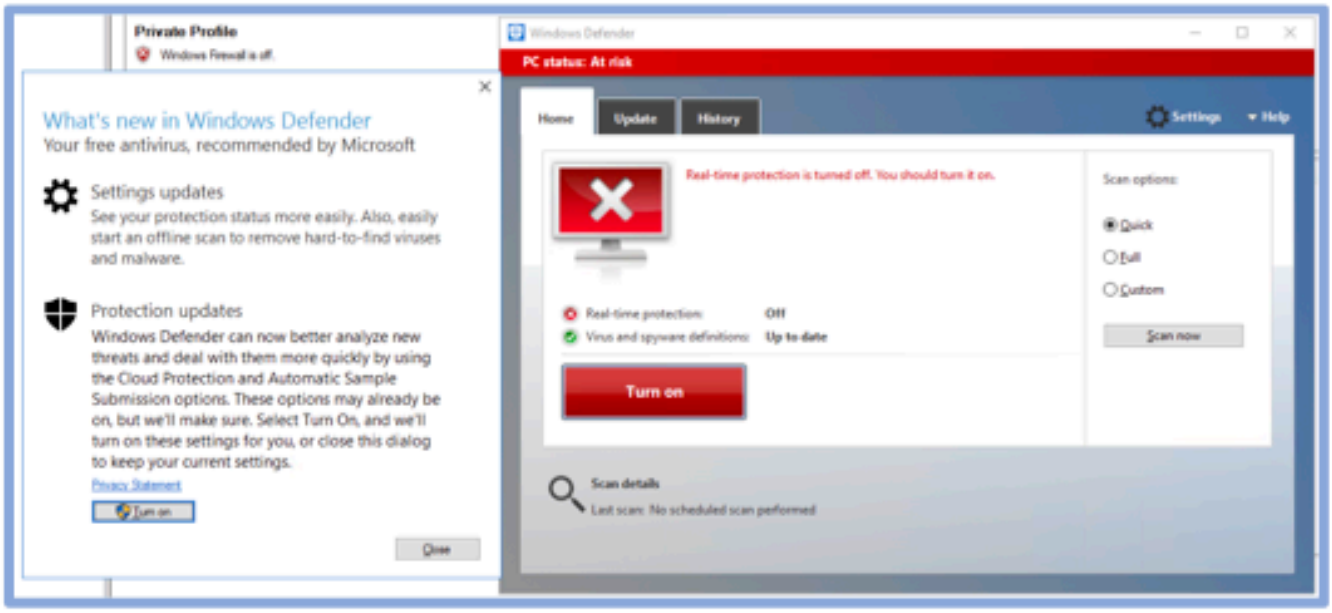
Windows systems have their firewall (Windows Firewall) set to inactive.



Finding TCC032: Improperly Configured Anti-Virus Software	
Affected Hosts	10.0.200.101-104, 10.0.0.5, 10.0.0.11, 10.0.0.20, 10.0.0.51-52
CVSS: N/A | Informational	
All of the Windows were found to have anti-virus software set up but not properly configured to be monitoring systems effectively.	

Proof of Concept:

Windows Defender has “Real-time protection” set to Off. This feature helps to prevent malware from being installed and run on the system. This should be turned on for all systems.



Finding TCC033: [CVE-2022-37958] Eternal Blue Scan	
Affected Hosts	10.0.0.6,11,51,52
CVSS: N/A | Informational	
Eternal Blue is an exploit involving writable SMB shares on old Windows machines. Our firm scanned all the Windows machines in The Cozy Croissant's website for this vulnerability. Eternal Blue has a high chance to disrupt / shutdown a computer when the exploit is run against it and as such our firm did not run the exploit except at the explicit directions of TCC's staff. In the testing we were unable to actually exploit this vulnerability but as such it does not mean it is not possible. This vulnerability is easily fixed by patching systems fully which will be included in another finding. We are including this information finding since this vulnerability was tested in person with representatives from TCC. We were unsuccessful in completing the exploit on the targets but did experience some small amount of downtime of the system test. Thus while we were unable to actually compromise any computers using this exploit it does still have merit to mention it.	

Proof of Concept:

Below is a scan from Metasploit indicating that with a normal user's credentials it is possible to exploit using Eternal Blue.

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > run

[+] 10.0.0.6:445          - Host is likely VULNERABLE to MS17-010!
4 (64-bit)
[*] 10.0.0.6:445          - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Finding TCC034: Execution with Unnecessary Privileges	
Affected Hosts	10.0.0.12
CVSS: N/A | Informational	
PHP is running as root on this system instead of the default user which is www-data. An attacker who knew this information could target PHP to leverage those privileges in an attack. This is not immediately exploitable, but could potentially be used in conjunction with other vulnerabilities.	

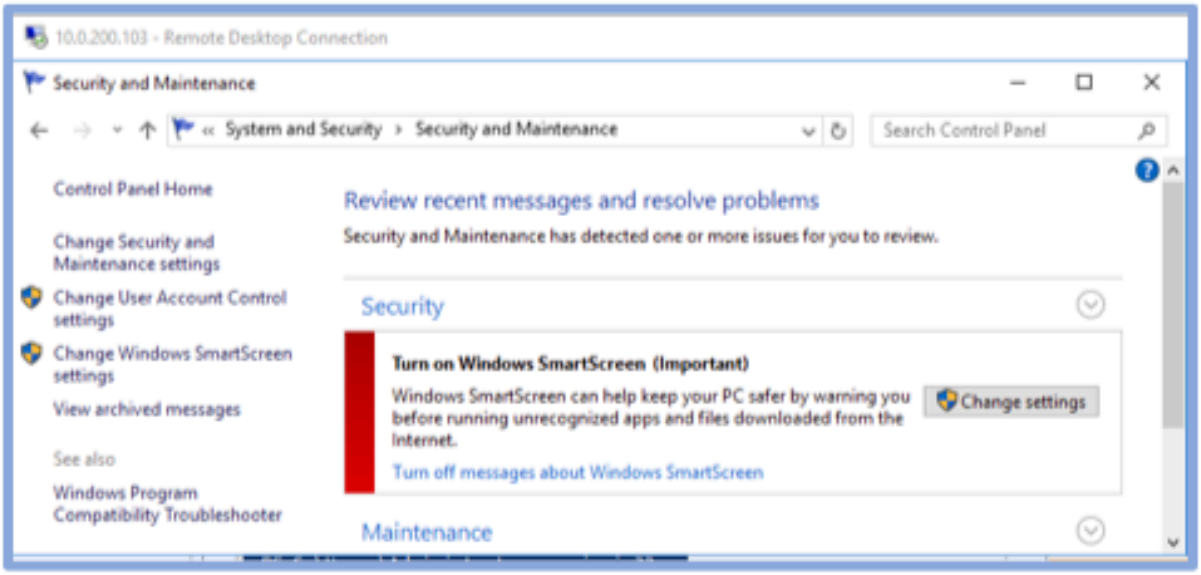
Proof of Concept:

ps aux | grep php shows process info for PHP, which is shown to be running as root.

Finding TCC035: Disabled Windows SmartScreen	
Affected Hosts	10.0.200.101-104
CVSS: N/A | Informational	
Windows SmartScreen is not enabled. Users will not be warned before running suspicious apps and executables. SmartScreen should be enabled to help users identify malicious files.	

Proof of Concept:

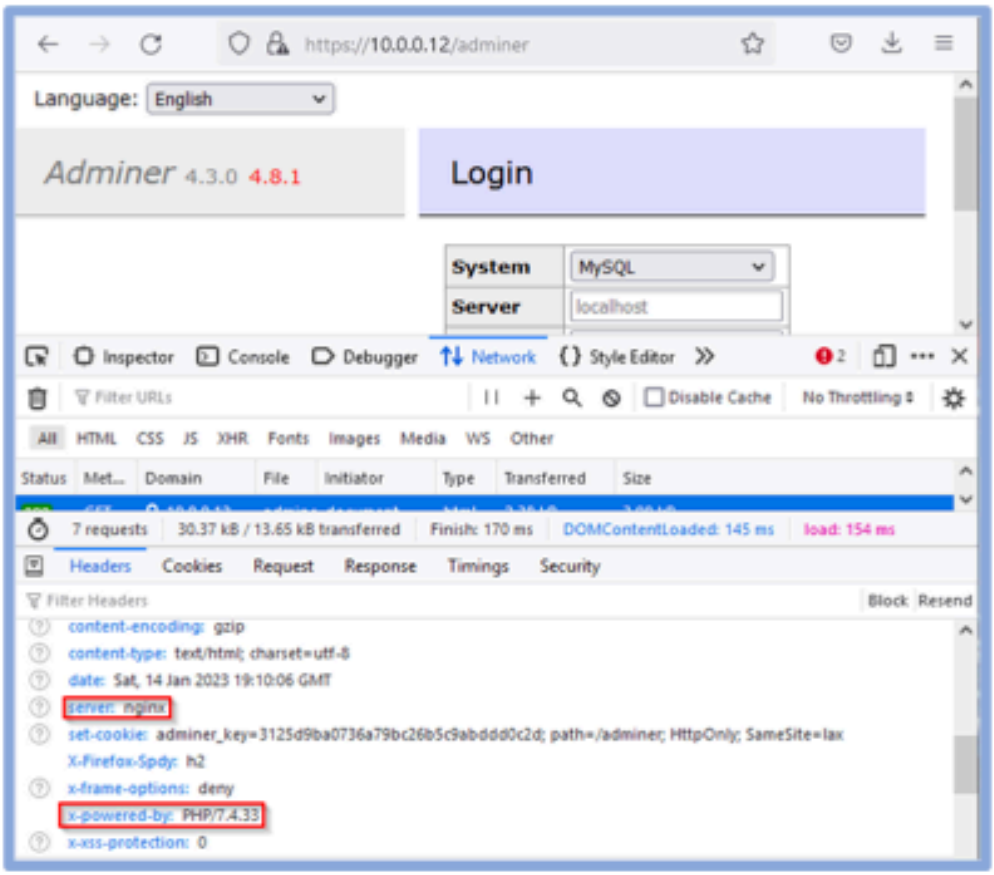
Windows SmartScreen is disabled, which means that users will not be warned about running malicious apps and executables.



Finding TCC036: Software Version Disclosure	
Affected Hosts	10.0.0.12, 20, 100, 102, 200, 210
CVSS: N/A | Informational	
Software versions are accessible by inspecting hosted websites on the affected systems. While not a vulnerability in itself, this information could disclose vulnerable versions to attackers. Each listed system disclosed versions of PHP, Apache, nginx, and/or OpenSSH.	

Proof of Concept:

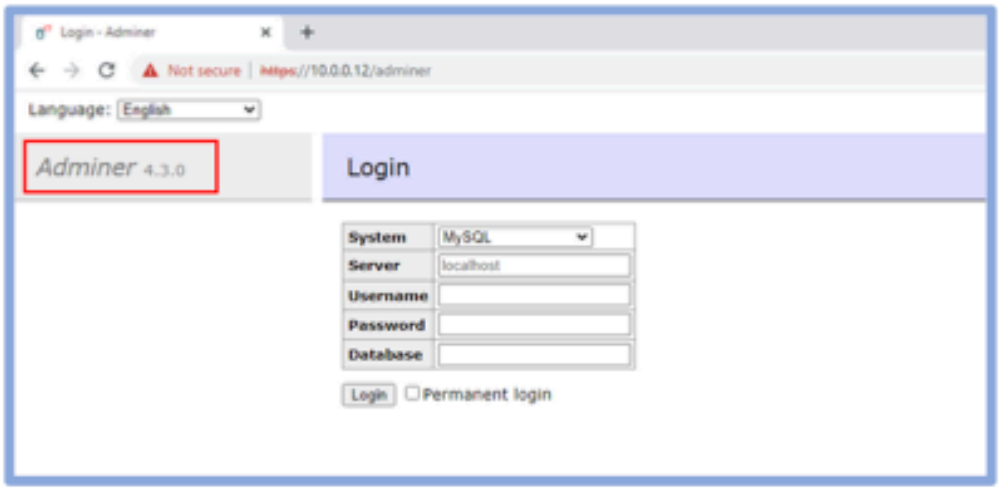
By using the F12 developer tools, users can inspect the source code of the hosted websites and discover the software versions used.



Finding TCC037: [CVE-2021-43008] Improper Access Control in Adminer	
Affected Hosts	10.0.0.12
CVSS: N/A | Informational	
Adminer contains an improper access control vulnerability, CVE-2021-43008 in Adminer versions 1.12.0 to 4.6.2, which has a CVSS score of 7.5. This vulnerability, if exploited, allows an attacker to arbitrarily read files on the system hosting Adminer. The attacker can exploit this vulnerability by hosting a MySQL database on their system and connecting the Adminer system to the maliciously hosted MySQL database. Once connected, the attacker can retrieve files that are on the Adminer system. While this vulnerability was not able to be exploited during the assessment, it was found that the Adminer version was very out of date and is theoretically vulnerable to this exploit and the version should be patched right away.	

Proof of Concept:

Adminer version can be seen to be 4.3.0 which falls within the vulnerable version range for CVE-2021-43008.



Finding TCC038: Outdated Software Versions	
Affected Hosts	10.0.0.7, 11, 12, 20, 100, 102, 200, 210
CVSS: N/A | Informational	
The listed systems had one or more softwares with outdated versions, including OpenSSH, PHP, OpenSLL, MySQL, nginx, PostgreSQL. Not all of these necessarily have vulnerabilities, but they should be updated to ensure long-term security.	

Appendix A: Physical Safe Security

Safe Compromises

Our team was given a small safe to check its physical security before The Cozy Croissant deployed them at large. In total, our team found three definite break-in paths and one theoretical break-in path.

First Safe Compromise

Our team noticed that certain buttons on the keypads were significantly more worn down than others; the buttons '2', '8', and 'E'. After some OSINT, we found that this safe model uses a 3-8 digit passcode. Assuming the passcode is a combination of 2 and 8, we conducted a small brute force of the possible combinations and discovered the passcode '8-2-2-E' to unlock the safe.

First Remediation

The first compromise can be easily remedied by changing the passwords on a regular interval. Even if the buttons get damaged over time, an attacker cannot guess a password easily based on the button's exterior wear.

Second Safe Compromise

Inside this safe model, there is a red button that is used to reset the keypad's passcode and enter a new one. A new passcode can be any 3-8 digit passcode followed by the 'E' button to save it. An attacker can press this red button from outside the safe by inserting a tool into the pre-drilled mounting holes on the bottom or back of the safe. Our team accessed this button via the bottom mounting holes. This allows an attacker to set the password and then use that password to unlock the safe.

Second Remediation

The second compromise can be remedied by blocking the mounting holes to prevent access to the inside of the safe from the outside. This could be achieved in a few ways. Using the mounting holes to bolt down the safe would prevent an attacker from both stealing a safe and getting inside the safe from the outside. If The Cozy Croissant wishes to keep safes unmounted, then a bolt or other cap like object can be fitted in the mounting holes and then secured in place so that an attacker cannot access the inside of the safe from outside.

Third Safe Compromise

This safe model uses a 7-pin tubular lock mechanism for the master key unlock. Using a lock pick set provided to us, our team was able to pick the lock and open the safe. While this did take our team a significant amount of time, an experienced attacker could pick this lock in under 10 minutes using the same tools. Additionally, an attacker may have access to a custom tool designed for this lock, and could pick the lock in under a minute.

Third Remediation

The only way to remedy this compromise is to completely restrict access to the key lock. While this is heavy-handed, as long as an attacker can access the 7-pin tubular lock, they can unlock and have access to the safe. Be aware that if the safe passcode is forgotten, or the internal batteries die, then access to the safe contents will be lost and the safe may need to be damaged to reobtain the items within. At the least, the battery issue can be avoided by replacing the 4 x AA batteries on a regular interval or as needed.

Theorized Safe Compromise

Our team has proposed an additional compromise to the safe's overall security. The proposed method could not be performed, but there is sufficient evidence to believe an attacker could use this method to break into the safe.

First Theorized Compromise

Utilizing the mounting holes on the safe, an attacker could break into the safe by removing the battery cover and dislodging a battery temporarily to reset the safe to its default password '1-5-9-E'. A specially made tool, such as a 3d printed tool, could easily remove the battery cover and dislodge a battery enough to reset the safe. While our team did not have such a tool, we were able to show using other utilities that the battery cover can be removed with ease, and only a singular battery must lose contact with the battery circuit for the safe to be reset upon placing the battery in contact with the circuit again.

This method is similar to the second safe compromise method shown above and will also be remedied with the same remediation plan.

Appendix B: Social Engineering Overview

Engagement Overview

In accordance with The Cozy Croissant's mission for their customers, the ability for employees to become defenders of their customers' privacy is of the utmost importance. Therefore, The Cozy Croissant requested further social engineering testing in addition to the initial testing. The target of this engagement was soliciting sensitive customer information over the phone, also known as Vishing. The front desk of The Cozy Croissant was the target of the Vishing test and the information requested was any personally identifiable information along with sensitive information. The attack vector for our Vishing test impersonated a TCC employee discovered in our initial OSINT investigation. The employee worked in the IT department and was driving to a police station to provide authorities with information about a possible criminal that had stayed at The Cozy Croissant and therefore needed the front desk employee to provide this information. This approach utilized common social engineering tactics such familiarity, authority, and urgency. All of these factors along with a friendly demeanor helps put the victim at ease by providing familiarity and encourages swift action by utilizing a sense of urgency and authority. In this scenario, the sense of urgency was introduced by the need for information to be given to law enforcement once the attacker "arrived on site" along with the need to "capture the criminal before they leave the state". Furthermore, authority was established by posing as not just a member of the IT team but that of an IT lead. This also provided a sense of familiarity since we posed as a real TCC employee. This exercise resulted in the compromise of 5 customers' first names along with one customer's personal information being divulged (Full Name, Address, Account Balance) along with sensitive information regarding the victim's credit card numbers, including the security code for said card.

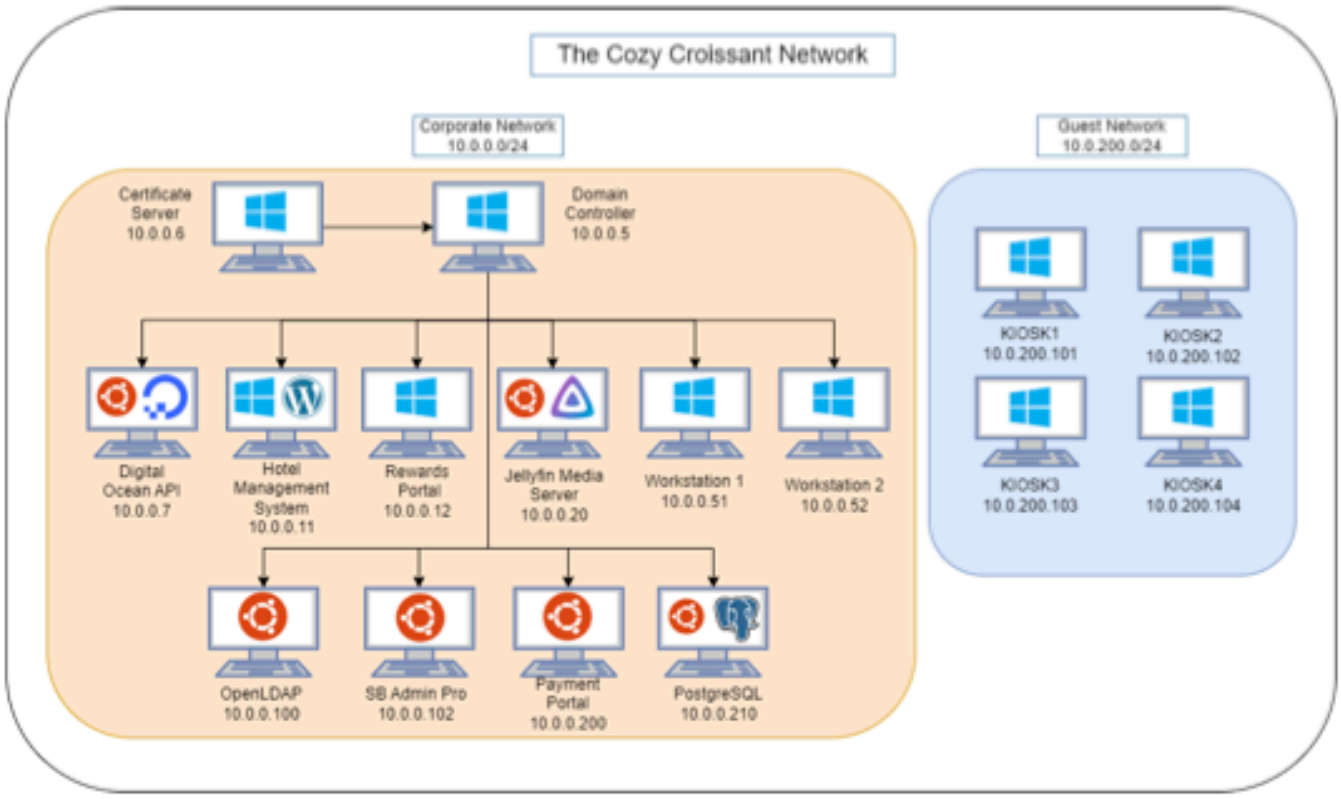
Remediation Suggestion

Remediation for social engineering exercise requires more thought than a simple path fix since this deals with humans rather than machines. The average social engineering leverages many characteristics of humans that are not necessarily bad, such as empathy. Employee training informing them of these attack vectors will help the overall security posture of The Cozy Croissant's staff. A focus during this training is to demonstrate a healthy skepticism when encountering potential attacks, a key to avoiding compromise. If the employee targeted had asked our consultant acting as an attacker to validate that they were who they said they were, then the attack would be severely limited and potentially exposed. Allowing employees authority to elevate potentially suspicious requests to involve multiple employees along with requesting aforementioned verification through whatever means

necessary will hinder an attacker's success at gathering credentials. The Cozy Croissant holds the values of being a kind, family-friendly hotel in a very high regard, and sacrificing kindness and empathy for the purpose of security is not advised. Therefore, the implementation of healthy skepticism and regularly requesting identification verification can help limit the risk of social engineering attacks while still providing courteous and customer focused service.

Appendix C: Network Diagram

The following diagram outlines the overall network architecture for The Cozy Croissant. The IP addresses along with the operating systems and critical applications hosted on the machines are noted in the diagram as well. In order to secure a network well, one must be organized carefully. Therefore, keeping meticulous note of all of the hosts on a network and their individual uses is paramount.



Appendix D: Methodologies

Penetration Testing Phases

These six phases are the model by which we conduct our penetration tests. They provide accountability and robustness in testing procedures. This ensures that the highest cost to value ratio is achieved while providing an excellent product to the client.

OWASP Top 10 on Next Page

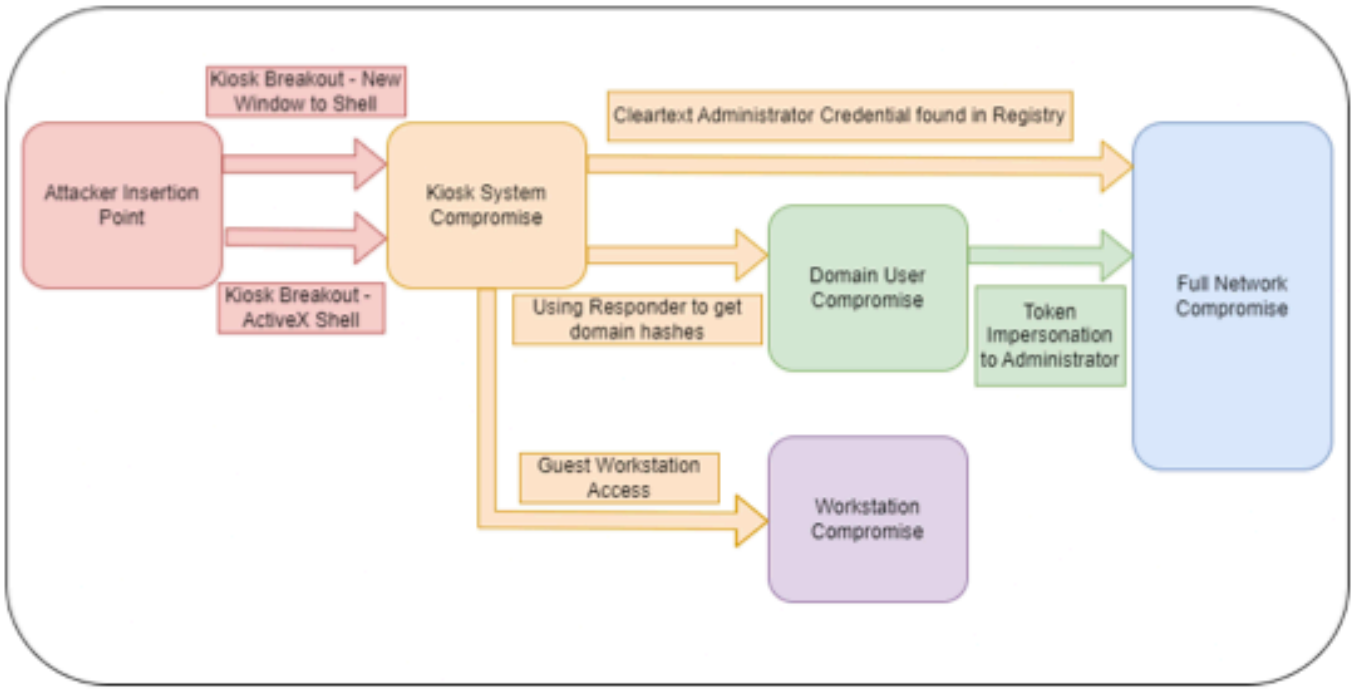
OWASP Top 10

The OWASP Top 10 are the 10 most commonly found vulnerabilities found in web applications. All web applications are tested against these vulnerabilities at minimum to ensure that the most vulnerabilities are discovered on each system and increase their security posture.

OWASP Top 10 - 2022	
1. Broken Access Control	2. Cryptographic Failures
3. Injection	4. Insecure Design
5. Security Misconfiguration	6. Vulnerable and Outdated Components
7. Identification and Authentication Failures	8. Software and Data Integrity Failures
9. Security Logging and Monitoring Failures	10. Server-Side Request Forgery (SSRF)

Appendix E: Attack Paths

The following chart shows the most likely attack paths for an adversary based on our findings report. There are two paths discovered to completely compromise the network and another separate vector to compromise the corporate workstations.



Appendix F: Technical Findings Legend

Finding TCC###: [CVE -] Vulnerability Name

Affected Hosts	*Targets/affected systems*
CVSS: *score | rating*	**Likelihood:** *Notes about the likelihood of exploitation, including the difficulty, credentials needed, etc.* **Technical Impact:** *Notes about the effect on TCC's systems and infrastructure if this vulnerability is exploited, including access gained, or damage to systems done*
Vulnerability Description	*A description of how the vulnerability works and what it allows an attacker to do*
Business Impact	*A description of the negative effects to TCC from a business standpoint*
Requirements to Exploit	*A list of requirements that may include tools, credentials needed, internal access, etc.*
Remediation	*General steps to correct any deficiencies specific to this instance of the exploit*
References	*Optional materials for additional reading*

Last Page