



Physical Penetration Test

Prepared for: Sample Inc

COMPLETE REPORT

April 20, 2026

Red Sentry

This engagement was performed in accordance with the Statement of Work, and the procedures were limited to those described in that agreement. The findings and recommendations in this report reflect the systems, scope, and timeframe defined in the Statement of Work.

While every effort was made to provide thorough coverage, no security assessment can identify every possible issue, and results should not be interpreted as a guarantee of complete security.

Contact Information

+1 (888) 337-0467

hello@redsentry.com



TABLE OF CONTENTS

Summary.....4

 Project Overview..... 4

 Goals..... 4

 Dates..... 4

 Findings..... 4

 Scope..... 5

Tests Performed.....6

Findings.....7

Appendices.....9



SUMMARY

Project Overview

Sample Company engaged Red Sentry to assess the security of their physical environments. The following report details the findings identified during the engagement.

Goals

Identify vulnerabilities in the company’s physical perimeter that could be leveraged by an attacker.

Dates

April 08, 2026	April 08, 2026 - April 17, 2026	April 20, 2026
KICKOFF	TESTING PERIOD	DELIVERY

Findings Overview

During the assessment, the testing team identified multiple security findings across the environment.

A finding represents a unique security issue with a distinct root cause.

Instances represent the number of instances where that issue appears within the assessed environment.

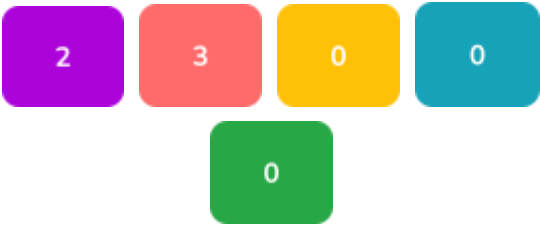
The following table summarizes the identified findings and the number of Instances observed during testing.

Severity	Finding ID	Instances
CRITICAL	T00U64Q-F0001	2
	T00U64Q-F0002	2
HIGH	T00U64Q-F0003	1
	T00U64Q-F0004	5
	T00U64Q-F0005	4

Overall Grade



GRADE



Scope

- Test Location 1
- Test Location 2

EXECUTIVE SUMMARY

The assessment team conducted a penetration test on Sample Company's physical environment. Overall, the perimeter needs serious attention as the assessment team found numerous critical and high-severity issues.

First, following the order of severity, X critical-severity issues were identified. These consist of Entry Barriers Bypass and Vulnerable Requests to Exit Sensors.

Second, during the assessment, X high-severity issues were found. These are principally related to instances of Cisco Smart Install Enabled, SMB Signing Not Required, and Default Credentials in Use on the assets.

In summary, the organization's security posture requires serious attention. The assessment team highly recommends implementing security measures and training employees on security policies, implementing secondary security mechanisms and adjusting the sensibility and position of the sensor, enforcing SMB signing, and implementing new credentials with strong passwords to reduce the potential attack surface.

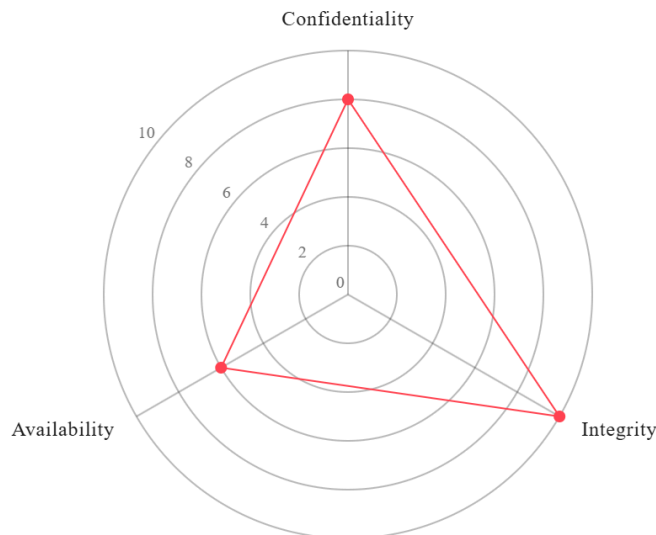


Figure 1: Security risk chart

Based on the findings, the assessment team identified the following risks:

- Confidentiality was affected to a high extent by SMB not being enforced and the use of default credentials.

- Entry Barriers Bypass, Cisco Smart Install Enabled, and Vulnerable Request to Exit Sensors have affected integrity to a high extent.
- Finally, availability was affected by the Vulnerable Request to Exit Sensors to a medium extent.

As the image above shows, there's an overall high risk as Confidentiality and Integrity risk scores are above 7.

As a general rule, an overall risk below 4 shows low business impact, between 4 and 7 medium impact and above 7 high impact.

Test Performed

During a physical pentest, the team combines techniques from social engineering and black box network testing with specialized techniques for gaining physical access:

API Discovery

Using a proxy connection, intercept HTTP connections to discover underlying APIs that could expose resources for an unauthenticated user.

Access Control System Testing

Test the effectiveness of biometric scanners, badge readers, or other access control devices through cloning, tampering, etc.

Alarm and Sensor Evasion

Attempt to bypass motion sensors, door alarms, and other detection systems without triggering them, or testing the response time or effectiveness of those systems once triggered.

Authentication Bypass

We used a set of attacks to access information requiring session tokens. This involves active user enumeration attacks and password spraying from standard common lists.

Credential Stuffing

Attempt to make use of relevant leaked credentials gathered from the Dark Web or any other public or paid source.

Dumpster Diving

Search recycle bins or trash receptacles for sensitive information such as passwords or confidential documents.

Evacuation and Emergency Procedure Testing

Evaluate the performance of security controls, maintenance of locked doors or areas, and actions of staff during an emergency to determine whether security measures are properly followed.

Known Vulnerabilities

Search for CVEs based on the technology stack being used.

Lockpicking and Bypassing

Utilize a variety of methods to gain access to electronic or manually locked doors, cabinets, or other secure areas.

Physical Barrier Testing

Evaluate the effectiveness of fences, walls, gates, or other barriers throughout a facility.

Reconnaissance:

Utilize publicly available tools to gather sensitive information, such as that provided with a Shodan search. This also includes physical surveillance and observation of security measures, etc.

Security Camera Avoidance

Attempt to identify and avoid detection by security cameras by making use of blindspots or disabling the technologies.



Sensitive Data Exposure

Analyze all of the information available to an unauthenticated user that could be leveraged against the company's confidentiality.

Social Engineering

Attempt to manipulate employees or security personnel to gain access or information by posing as maintenance, delivery, IT workers, or other trusted personnel.

Tailgating and Piggybacking

Attempt to follow an authorized person into a secure area with or without their knowledge or attempt to convince them to allow entry into the said area.

Unauthorized Device Placement

Attempting to plant rogue devices such as USB drives, cameras, wifi emitters, network sniffers, etc to capture information or disrupt operations and whether employees take note of and report the resultant suspicious activity.

Physical Penetration Test Findings

ENTRY BARRIERS BYPASS

CRITICAL

Identifier	T00U64Q-F0001
Severity	Critical
Instances	2

Description

Many secure locations implement a comprehensive physical security policy mandating barriers at all entry points, coupled with restricted access mechanisms such as keys, proximity cards, PIN pads, or the presence of a vigilant security guard or receptionist. These measures are crucial in maintaining a secure environment by controlling who can enter the premises.

Malicious actors can bypass security by exploiting vulnerabilities in physical security and human behavior. They might use subtle tactics to evade receptionists, scout for less fortified entrances, or employ social engineering techniques to gain entry.

Instances (2)

- Test Location 1 #123
- Test Location 1, Breakroom.

Evidence

During the assessment process, the security team found two instances of physical barriers that could be bypassed.

Main Entrance:

After analyzing the security measures implemented on the main entrance door, the security team was able to bypass the closing mechanism by pushing the lock bolt back into place.

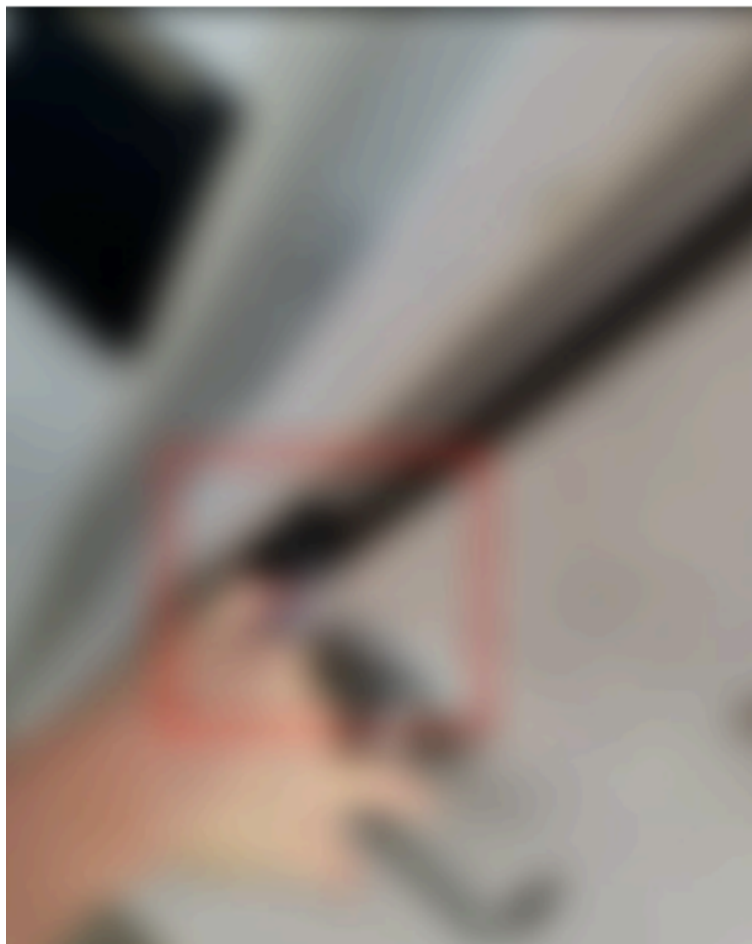


Figure 2: Main Entrance open.

As can be seen in the picture above, the security team was able to successfully open the door and gain access to the building.

Breakroom:

After accessing the building, the assessment team found an internal door that led to the Breakroom. The lock mechanism of this room could be opened by manipulating the latching bolt with a pry bar.



Figure 3: Breakroom opened with a pry bar.

As can be seen in the picture, the security team gained access to the breakroom, where an unlocked box that contained several keys was found on the wall.

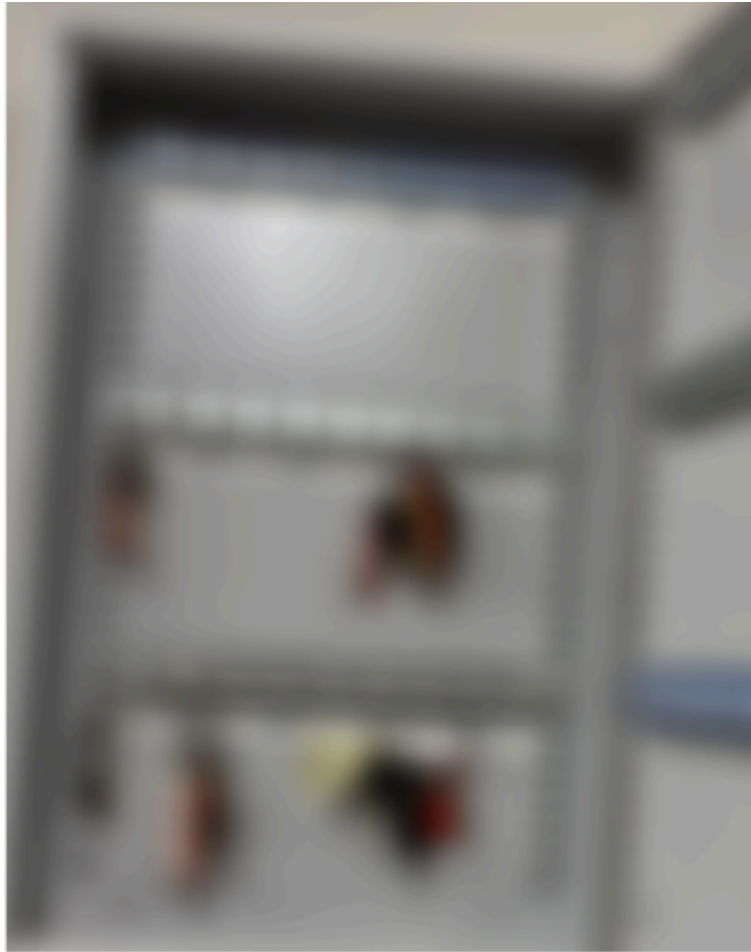


Figure 4: Wall box with keys.

This vulnerability allows unauthorized entities to bypass security measures and access restricted areas or sensitive information. This vulnerability can cause several significant impacts on the business, leading to financial losses, reputational damage, and reduced customer trust. Promptly addressing this vulnerability is essential to protect the company's integrity.

Steps for Recreation

1. Verify the above listed issues on XX's compound.

Recommendations

To mitigate the risk of this issue, the assessment team recommends the following steps:

- Enhance visitor management policies to diminish the chances of unauthorized entry further. Encourage employees to actively approach and question unescorted visitors or those without proper visitor badges.

- Regularly train employees on security protocols and raise awareness about the tactics used by malicious actors. Promote a 'see something, say something' policy, encouraging everyone to actively participate in maintaining security.
- Electronic access control systems should be incorporated to monitor and enforce physical security policies effectively. These systems are invaluable for identifying potential security breaches, such as doors left or held open longer than usual or forced entry without a proper access control token.

Resources

Physical Security

<https://www.cisa.gov/topics/physical-security>

Protect the Physical Security of Your Digital Devices

<https://www.cisa.gov/resources-tools/training/protect-physical-security-your-digital-devices>

Cybersecurity and Physical Security Convergence

https://www.cisa.gov/sites/default/files/publications/Cybersecurity%2520and%2520Physical%2520Security%2520Convergence_508_01.05.2021.pdf

Tailgating: A Common Courtesy and a Common Risk

<https://www.securitymagazine.com/articles/86026-tailgating-a-common-courtesy-and-a-common-risk>

10 Strategies to Prevent Tailgating

<https://www.buildings.com/industry-news/article/10189912/10-strategies-to-prevent-tailgating>

VULNERABLE REQUEST TO EXIT (REX) SENSORS

CRITICAL

Identifier	T00U64Q-F0002
Severity	Critical
Instances	2

Description

A Request to Exit (REX) sensor system allows personnel to exit a facility without manual door unlocking. A common variant of these sensors is the Passive Infrared (PIR) motion sensor, typically positioned near exit doorways. These sensors detect shifts in infrared radiation, rather than motion per se, within a designated time frame.

Any alteration in the ambient temperature within the sensor's detection range can activate the system; subsequently, malicious individuals can exploit temperature sensors by using compressed air or objects to trigger false activations and unlock doors.

Instances (2)

- Test Location 2, #345 (Front Door)
- Test Location 2, #345 (Back Door)

Evidence

During the assessment process of Test Location 2, the security team noted that two access doors had a gap between the two doors, and there was a visible exit sensor, as shown in the following picture.



Figure 5: Gap between the entrance doors.

After identifying these conditions, the assessment team used a can of compressed air that was turned upside down, pushed the straw through the gap between the doors, and propellant sprayed until the content reached the motion sensor's target area, as can be seen in the picture below.



Figure 6: Compressed air through security doors.

After performing the described actions, the security sensor was successfully triggered, releasing the magnetic lock and subsequently opening the door.

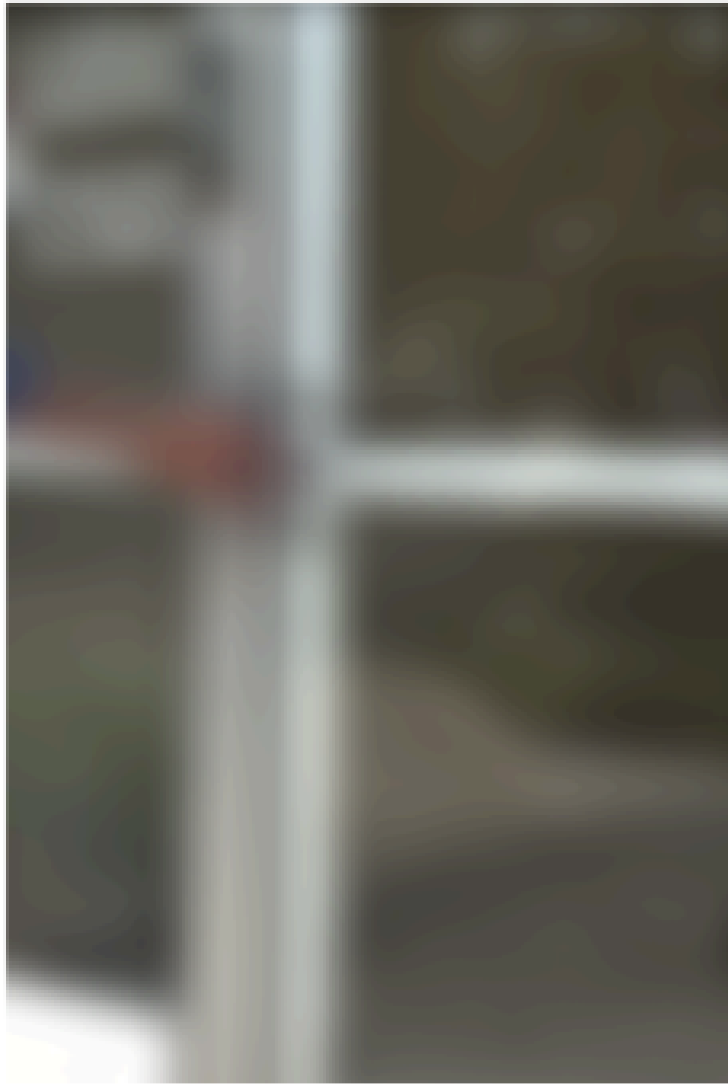


Figure 7: Opened Door.

This vulnerability can compromise the security of the organization. These security breaches can lead to unauthorized access by malicious actors. By bypassing the security protocols, one can gain access to the organization's facilities, causing data breaches by accessing sensitive data within the facility.

Steps for Recreation

1. Use a compressed air can and follow the details section listed above at the listed locations.

Recommendations

To mitigate the risk of this issue, the assessment team recommends the following steps:

Configure Sensor Positioning and Sensitivity Settings:

- Move the sensor back: Position the sensor further away from the door so that tools such as cans of compressed air cannot easily reach the detection zone. This makes it more difficult for an attacker to affect the sensor's field of view.
- Lighted exit signs or similar barriers: Install physical barriers like lighted exit signs in front of the sensor. These barriers should be placed strategically to obstruct direct access from the outside, making it difficult to manipulate the sensor without triggering the barrier first.
- Recalibrate the sensor: Regularly recalibrate the sensor to ensure it responds accurately to actual threats while ignoring false positives. This calibration should include simulated attacks with tools like canned air to adjust sensitivity settings accordingly.

Implement Secondary Mechanisms:

- Touch-sensitive door handles: Install handles that require a human touch to unlock. This secondary mechanism ensures that even if the PIR sensor is triggered, the door will not unlock without additional verification.
- Floor pressure plates: Use pressure-sensitive plates that require a certain weight threshold to be met before the door unlocks. This adds another layer of security, ensuring the door only opens when someone is physically present.
- Consult local fire codes: Ensure that any additional security measures comply with local fire safety regulations and facility requirements. This step is crucial to maintaining both security and safety standards.

Compensating Controls:

- Video monitoring: Install surveillance cameras at exit points to monitor for suspicious activity. Real-time monitoring and recording can help in quickly identifying and responding to any attempts to manipulate the sensors.
- Alarm systems: Integrate the sensors with alarm systems that alert security personnel when an unauthorized exit attempt is detected. This immediate response can prevent unauthorized access and potential breaches.

Resources

Request to Exit Sensor Bypass:

<https://warroom.rsmus.com/request-exit-sensor-bypass/>

Sensor Triggering:

<https://www.redteamtools.com/canisters-of-r134a-for-rex-sensor-triggering/>



CISCO SMART INSTALL ENABLED

HIGH

Identifier	T00U64Q-F0003
Severity	High
Instances	1

Description

Smart Install (SMI) is a Cisco network device protocol that enables zero-touch configuration and management of network devices. It allows new devices to be configured by a Smart Install director without authentication or authorization. The lack of authentication in the system allows malicious actors to exploit it for various purposes, including downloading sensitive information, making configuration changes, and causing security breaches or service disruptions.

Instances (1)

- 192.122.10.24 (Test Location 2)

Evidence

During the assessment of Sample Company's facilities, after accessing Test Location 2 building, the security team had access to an open office where a network jack was used to access the corporate network. After running several scans, the security team found an instance of Cisco Smart Install running in one of the hosts.



Figure 8: Cisco Smart Install instance running.

As seen in the previous figure, after accessing the host, the security team was able to download a Cisco Running configuration file, which included Type 5 and Type 7 password hashes.



Figure 9: Type 5 and 7 password hashes dumped.

After retrieving both password hashes, the assessment team reversed both hashes and successfully revealed the cleartext password, as can be seen in the following picture.



Figure 10: Type 5 hash reversed.

Exploitation of Cisco Smart Install can lead to unauthorized access, causing data breaches and service disruptions. This compromises operational integrity, leading to financial losses, reputational damage, and loss of customer trust. Immediate patching and enhanced security measures are essential to safeguard assets and ensure business continuity.

Steps for Recreation

1. Run a nmap scan using the open ethernet jack on Location 2 building. Verify that Cisco Smart Install is installed.
2. Use the python exploit from <https://github.com/AlrikRr/Cisco-Smart-Exploit> to dump the hashes.

Recommendations

To mitigate the risk of this issue, the assessment team recommends the following steps:

- Disable Smart Install if it is not being used. This can be done by using the no vstack command.
- If there is a need to use Smart Install or it cannot be disabled on a specific device, use access control lists to restrict TCP port 4786 access to the necessary Smart Install director and clients.
- To limit the impact of compromised Cisco device configuration access, it is recommended to:
 - Ensure that passwords are not stored in cleartext. Use centralized AAA authentication instead of local authentication where possible.
 - Use secret (MD5 hashed) password encoding instead of Type 7 or weaker.

Resources

Mitigating and Detecting Potential Abuse of Cisco Smart Install Feature

<https://blogs.cisco.com/security/cisco-psirt-mitigating-and-detecting-potential-abuse-of-cisco-smart-install-feature>

Smart Install Configuration Guide

https://www.cisco.com/c/en/us/td/docs/switches/lan/smart_install/configuration/guide/smart_install/concepts.html

Cisco Smart Install Protocol Misuse

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170214-smi>

SMB SIGNING NOT REQUIRED

HIGH

Identifier	T00U64Q-F0004
Severity	High
Instances	5

Description

SMB signing is a security feature in the SMB protocol that uses a session key and the AES algorithm to generate a signature for every SMB message. This signature is included in the SMB header and is used to verify the message's authenticity. Enabling SMB signing helps to prevent man-in-the-middle attacks on the network by ensuring that the message is not tampered with during transmission.

Instances (5)

- 192.168.55.7
- 192.168.50.23
- 192.168.50.2
- 192.168.50.88
- 192.168.50.122

Evidence

The assessment team identified numerous instances of hosts that had SMB signing enabled but not required. As can be seen in the following figure:

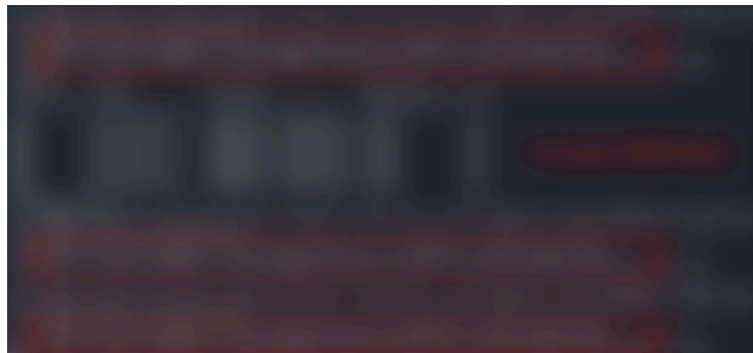


Figure 11: Hosts without SMB message signing required

Without the enforcement of SMB signing, attackers can intercept and modify SMB traffic, leading to unauthorized data access, data manipulation, and the spread of malware. Devices should have SMB signing enabled to harden them against attackers inside the internal network, as these attackers may perform Man in the Middle (MITM) and SMB relay attacks to attempt to steal credentials or impersonate other users.

Steps for Recreation

1. Use the nmap and nse script to check if the SMB signing was disabled or not required:

```
nmap --script smb-security-mode.nse -p445 IP
```

Recommendations

To mitigate the risk of this issue, the assessment team recommends the following steps:

- Enforce message signing in the host's configuration.
- On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always).'
- In Samba, the setting is called 'server signing.' See the 'see also' links for further details.
- This PowerShell Command can be used to turn SMB signing:
 - **`Set-SmbServerConfiguration -RequireSecuritySignature $True -EnableSecuritySignature $True -EncryptData $True -Confirm:$false`**

Resources

About SMB Signing

<https://docs.microsoft.com/en-US/troubleshoot/windows-server/networking/overview-server-message-block-signing>

About the Importance of SMB Signing

<https://www.securance.com/blog/smb-signing>

DEFAULT CREDENTIALS IN USE

HIGH

Identifier	T00U64Q-F0005
Severity	High
Instances	4

Description

Management Interfaces allow users to handle different systems and devices, such as applications, services, and devices. These interfaces can be accessed through web portals or console-based services. Some examples of systems commonly using Management Interfaces are VOIP phone systems, multi-function printers, networked security E1 Digital Directs, switches, firewalls, routers, and wireless access points (AP).

When these management interfaces are initially set up, they often come with a default username and password that can be used to perform administrative-level tasks in the system. The default credentials may be available in the vendor's documentation or instructional manuals. If those are still enabled, it would pose a significant security risk to the security of the underlying asset.

Instances (4)

- 192.144.59.51 (admin:123456789)
- 192.144.59.5 (:maintenance)
- 192.144.59.8 (user:456)
- 192.144.59.22 (admin:administrator)

Evidence

During the assessment process, the security team discovered an instance of Default Credentials in Use related to an Axis camera management portal, the access to this portal was configured with default credentials.



Figure 12: Default credentials used to access.

As shown in the figure above, the assessment team could log in to the Axis portal by introducing the manufacturer's credentials set by default, consequently having access to restricted information and functionalities. This vulnerability can lead to system breaches, data theft, and unauthorized control over critical functions. Hence, default passwords expose networks and devices to a high risk of cyber-attacks, underscoring the importance of changing them to strong, unique passwords during initial configurations.

Steps for Recreation

1. Navigate to the Locations listed below.
2. Login with the default passwords listed.

Recommendations

To mitigate the risk of this issue, the assessment team recommends the following steps:

- Changing the default password and setting a strong password.
- Password must contain characters from at least three of the following categories:
 - Uppercase characters (A through Z)

- Lowercase characters (a through z)
- Numerical characters (0 through 9)
- Special characters (!, @, #, \$, etc)

Resources

Risks involved with the usage of default passwords

<https://www.giac.org/paper/qsec/317/default-password-threat/100889>

About Default Credentials usage

https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/04-Authentication_Testing/02-Testing_for_Default_Credentials

APPENDIX (A) SEVERITY DESCRIPTION

The assessment team used the following criteria to rate the findings in this report. Red Sentry derived these risk ratings from the industry and organizations such as OWASP.

The severity of each finding in this report is independent. Finding severity ratings combine direct technical and business impact with the worst-case scenario in an attack chain. The more significant the impact, and the fewer vulnerabilities that must be exploited to achieve that impact, the higher the severity.

Critical

A purple rounded rectangular badge with the word "CRITICAL" in white, uppercase letters.

Vulnerability is an otherwise high-severity issue with additional security implications that could lead to exceptional business impact. Examples: trivial exploit difficulty, business-critical data compromised, bypass of security controls, direct violation of communicated security objectives, and large-scale vulnerability exposure.

High

A red rounded rectangular badge with the word "HIGH" in white, uppercase letters.

Vulnerability may result in direct exposure including, but not limited to: the loss of application control, execution of malicious code, or compromise of underlying host systems. The issue may also create a breach in the confidentiality or integrity of sensitive business data, customer information, and administrative and user accounts. In some instances, this exposure may extend farther in the infrastructure beyond the data and systems associated with the application.

Medium

MEDIUM

Vulnerability does not lead directly to the exposure of critical application functionality, sensitive business and customer data, or application credentials. However, it can be executed multiple times or leveraged in conjunction with another issue to cause direct exposure. Examples include brute-forcing and client-side input validation.

Low

LOW

Vulnerability may result in limited exposure of application control, sensitive business and customer data, or system information. This type of issue provides value only when combined with one or more issues of a higher risk classification. Examples include overly detailed error messages, the disclosure of system versioning information, and minor reliability issues.

Informational

INFO

Finding does not have a direct security impact but represents an opportunity for additional layers of security, is considered a best practice, or has the possibility of turning into an issue over time. Finding is a security-relevant observation that has no direct business impact or exploitability, but may lead to exploitable vulnerabilities. Examples include poor communication between organizations, documentation encouraging poor security practices, or lack of security training.