

RMC

RED MOUNTAIN CONSULTING

Clear findings. Prioritized mitigations.

PENETRATION TEST REPORT

Prepared for *Example Organization*

DRAFT – *September 30th, 2025*

TABLE OF CONTENTS

EXECUTIVE SUMMARY 3
SCOPE 6
METHODOLOGY 6
FINDINGS 7
APPENDIX A: SEVERITY RATING CRITERIA 15
APPENDIX B: EXTERNAL PORT MAPPING 16
APPENDIX C: PASSWORD ANALYSIS 17
APPENDIX D: ABBREVIATIONS AND ACRONYMS 18

TABLES

Table 1: Summary of Findings, Severity, and Mitigation Status 7
Table 2: Recommendations Based on CIS Controls 14
Table 3: Severity Rating Descriptions 15
Table 4: Open Ports and Services on External Systems 16

FIGURES

Figure 1: Number of Findings Mapped to NIST Controls 4
Figure 2: NIST Cybersecurity Framework Categories 5
Figure 3: Domain Admin Login Sessions 9
Figure 4: ESC15 on ITUTIL08.EXAMPLE.COM 12
Figure 5: Unconstrained Delegation on User Accounts 13

EXECUTIVE SUMMARY

Overview

Red Mountain Consulting, LLC (RMC) conducted a Penetration Test (Pen Test) at the request of EXAMPLE COMPANY NAME (EXAMPLE). Jason Hill (info@rmcyber.io) led the assessment remotely from September 10–26, 2025, and internally from September 99–99, 2222. This report only covers the targets described within and makes no claims about the security of any system that was deemed out of scope or was not tested during this engagement.

Findings Summary

The assessment of the EXAMPLE COMPANY NAME (EXAMPLE) identified a total of twelve security findings, including two rated as high severity, nine as medium severity, and one as low severity. While no critical issues were observed, the high-severity items highlight potential paths for attackers to gain elevated access and compromise sensitive systems. The most significant risks are tied to the use of privileged accounts that are not strictly necessary and to weaknesses in Active Directory's certificate services, both of which increase the likelihood of an attacker escalating access and moving deeper into the network. Medium-severity issues were concentrated in areas such as identity management, password security, and service configurations, which together expand the organization's exposure to modern cyber threats. Although no single issue currently places EXAMPLE at imminent risk, the combination of findings represents a meaningful concern that, if left unaddressed, could lead to disruption of operations, unauthorized access to sensitive information, or reputational harm.

Recommendations

RMC recommends that EXAMPLE give priority to reducing its dependency on non-essential privileged accounts and correcting the weaknesses in Active Directory's certificate templates. Addressing these areas will substantially reduce the likelihood of a successful privilege-escalation attack and strengthen overall identity management. Beyond these top priorities, EXAMPLE should continue to refine password policies, harden legacy or unnecessary services, and ensure security settings in Active Directory align with current best practices. Implementing stronger monitoring of account activity and enforcing the principle of least privilege will further improve resilience. By focusing on these steps, EXAMPLE can materially lower its risk, close avenues for lateral movement, and position the organization to withstand the techniques most often leveraged in real-world cyberattacks.

Observed Strengths

While the assessment uncovered some areas for improvement, EXAMPLE has already demonstrated a strong commitment to cybersecurity. The organization benefits from effective network segmentation, robust host-based security controls, and solid password practices that exceed common standards in many peer organizations. These strengths provide a strong foundation for defense and significantly limit the exposure of sensitive systems. EXAMPLE's willingness to engage in a proactive assessment further underscores a culture of security awareness and a commitment to protecting its mission-critical operations.

Overall Summary

The EXAMPLE COMPANY NAME is operating with a lower-than-average level of security risk. While no critical issues were discovered, the presence of high-severity vulnerabilities tied to elevated account use and certificate service configurations highlights the importance of timely remediation. Addressing these concerns, along with the medium-severity findings, will further reduce the likelihood of account compromise, privilege escalation, and lateral movement within the environment. At the same time, EXAMPLE's existing strengths in network design, system hardening, and password management provide a solid platform on which to build. With focused improvements in identity and access management, EXAMPLE can move confidently toward a stronger, more resilient security posture that safeguards both its operations and its reputation.

NIST-Based Summary

The RMC team mapped all findings to applicable National Institute of Standards and Technology (NIST) controls as described in NIST Special Publication (SP) 800-53. Figure 1 illustrates the relevant control families cited based on findings. Please refer to NIST SP 800-53 for a full list of control families. The Findings section of this report provides specific mappings of controls to findings and the detailed technical description for each finding. Note that some findings may be mapped to multiple applicable NIST controls.

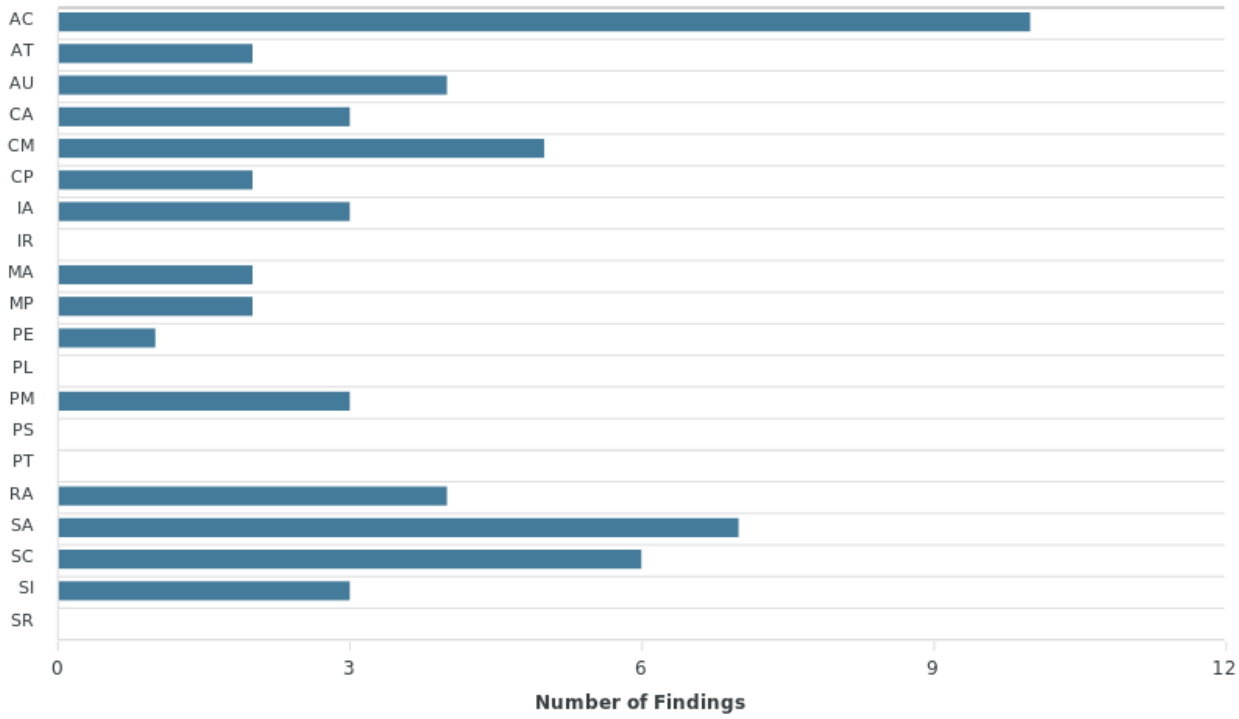


Figure 1: Number of Findings Mapped to NIST Controls

Control Family Abbreviations and Definitions

AC	Access Control	**PE**	Physical and Environmental Protection
AT	Awareness and Training	**PL**	Planning
AU	Audit and Accountability	**PM**	Program Management
CA	Assessment, Authorization, and Monitoring	**PS**	Personnel Security
CM	Configuration Management	**PT**	Personally Identifiable Information Processing and Transparency
CP	Contingency Planning	**RA**	Risk Assessment
IA	Identification and Authentication	**SA**	System and Services Acquisition
IR	Incident Response	**SC**	System and Communications Protection
MA	Maintenance	**SI**	System and Information Integrity
MP	Media Protection	**SR**	Supply Chain Risk Management

NIST Cybersecurity Framework

Pen Test findings are mapped to the NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, April 16, 2018, called the Cybersecurity Framework. Figure 2 illustrates the relevant functions and categories cited based on findings. Please refer to the NIST Cybersecurity Framework for a full list of functions and categories. The Findings section of this report provides specific mappings of categories to findings and the detailed technical description for each finding. Note that some findings may be mapped to multiple applicable NIST categories.

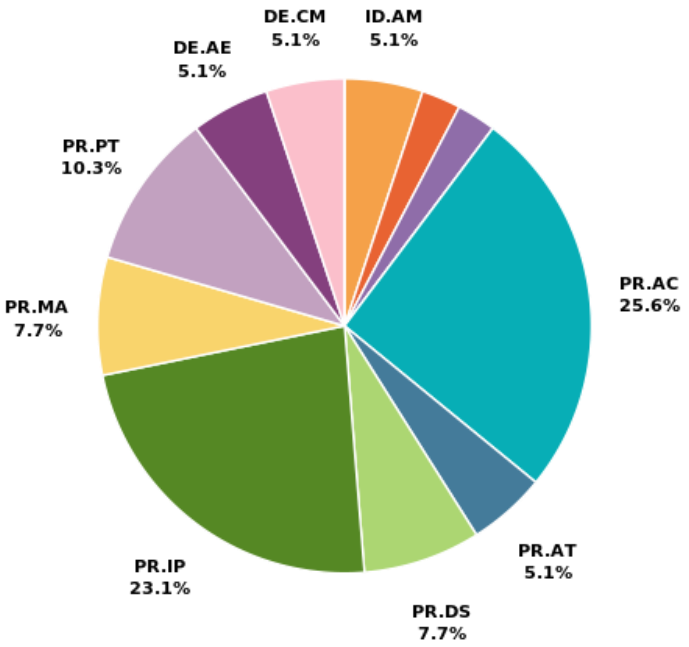


Figure 2: NIST Cybersecurity Framework Categories

Function and Category Abbreviations and Definitions

DE	Detect	PR	Protect
ID	Identify	RS	Respond

AC	Identity Management and Access Control	GV	Governance
AE	Anomalies and Events	IP	Information Protection Processes and Procedures
AM	Asset Management	MA	Maintenance
AT	Awareness and Training	MI	Mitigation
CM	Security Continuous Monitoring	PT	Protective Technology
DP	Detection Processes	RA	Risk Assessment
DS	Data Security	SC	Supply Chain Risk Management

SCOPE

External

14 of 64 scanned hosts were discovered to be live during testing of the following in scope targets:

123.456.789.123/32

Internal

220 of 7,162 scanned hosts were discovered to be live during testing of the following in scope targets:

10.75.231.0/24, 10.75.232.0/24, 10.90.27.0/24, 10.90.64.0/21, 10.90.72.0/24, 10.92.0.0/24, 10.190.30.0/24, 172.31.18.0/24, 10.50.5.0/24, 10.8.0.0/24, 10.8.10.0/24, 10.8.20.0/24, 10.8.21.0/24, 10.8.22.0/24, 10.8.30.0/24, 10.9.0.0/24, 10.9.10.0/24, 10.9.20.0/24, 10.9.21.0/24, 10.9.22.0/24, 10.9.30.0/24

METHODOLOGY

The Penetration Test consists of several phases detailed in the subsequent sections. At a high level, the Pen Test methodology involves:

- Gathering relevant information about the target organization and its assets
- Conducting vulnerability scanning of in-scope assets
- Manually analyzing in-scope assets and collected data
- Validating findings, including chaining together multiple vulnerabilities and misconfigurations where possible, to elevate privileges and access, or otherwise demonstrate significant impact
- Providing actionable deliverables to the stakeholder, including an out brief, final report, and raw assessment data

The RMC team utilizes this methodology from different contexts, dependent on the stakeholder's interests and accommodations, as well as the RMC team's ability to obtain various levels of access. The scenarios by which the RMC team conducts testing may include:

- External to the stakeholder's network, with no assumed access to assets or accounts other than what is accessible to the public
- Leveraging the access of a phished user in a standard phishing campaign
- Leveraging the credentials of a phished user in a credential harvesting campaign
- Internal to the stakeholder's network, with no initial access to the domain
- Access to the domain via a low privilege account
- Access to the domain via a privileged account

FINDINGS

The RMC team identified the following findings as potentially exploitable conditions that could lead to compromise of the confidentiality, integrity, and/or availability of the tested environment. Each finding includes a description, supporting details, and recommended steps for mitigation. The EXAMPLE COMPANY NAME team should review the findings and recommendations for technical weaknesses, shortcomings in processes and procedures, and systemic weaknesses in overall security posture.

Severity can be used to prioritize mitigation of findings. However, EXAMPLE COMPANY NAME is best equipped to develop a mitigation strategy based on business impact and priorities. Mitigation Status indicates whether a finding was mitigated during the assessment timeframe and is only adjusted when the RMC team can confidently validate that the finding was mitigated.

Findings Summary

	Finding Name	Severity	Mitigation Status
1	Non-Essential Use of Elevated Accounts	• High	• Not Mitigated
2	Vulnerable Certificate Templates	• High	• Not Mitigated
3	Dangerous Object Configuration	• Medium	• Not Mitigated
4	Insecure Active Directory Configuration	• Medium	• Not Mitigated
5	Insecure Group Policy Object Password Storage	• Medium	• Not Mitigated
6	Insecure SMB Usage	• Medium	• Not Mitigated
7	Insecure Storage of Credentials	• Medium	• Not Mitigated
8	LDAP Signing Not Required	• Medium	• Not Mitigated
9	Unnecessary Network Services	• Medium	• Not Mitigated
10	Unpatched System or Service	• Medium	• Not Mitigated
11	WebClient Service Enabled	• Medium	• Not Mitigated
12	Accounts Not Aligned with Password Policy	• Low	• Not Mitigated

Table 1: Summary of Findings, Severity, and Mitigation Status

See Appendix A for the criteria used to determine severity (Critical/High/Medium/Low/Informational).

Detailed Findings

ID	Finding	Severity	Type	Mitigation Status
1	Non-Essential Use of Elevated Accounts	• High	Internal	• Not Mitigated

Affected Systems

JACK@EXAMPLE.COM, MSEXBACKUP@EXAMPLE.COM, BOBD@EXAMPLE.COM, TENABLEADMIN@EXAMPLE.COM

Description

RMC observed that one or more Domain Administrator accounts are used to log into non-domain-controller systems. While Domain Admins inherently require high-level privileges, using these accounts on regular endpoints increases the risk of credential theft. If malware or an attacker compromises a non-domain-controller system where a Domain Admin is logged in, the attacker could capture credentials or Kerberos tickets, potentially enabling full domain compromise. Logging in with privileged accounts on non-essential systems unnecessarily broadens the attack surface and undermines security best practices designed to protect high-value credentials.

Recommended Mitigation

Organizations should enforce the principle of least privilege by restricting the use of Domain Administrator accounts to domain controllers and systems specifically designated for administrative tasks. Standard endpoints should be accessed with non-privileged accounts, and administrative sessions should be isolated to dedicated workstations. Monitoring and auditing privileged account logins can help detect deviations from this policy, ensuring that high-value credentials are not exposed unnecessarily and reducing the likelihood of domain-wide compromise.

Relevant Screenshots

This screenshot shows login sessions from domain administrator accounts to machines that are not domain controllers.

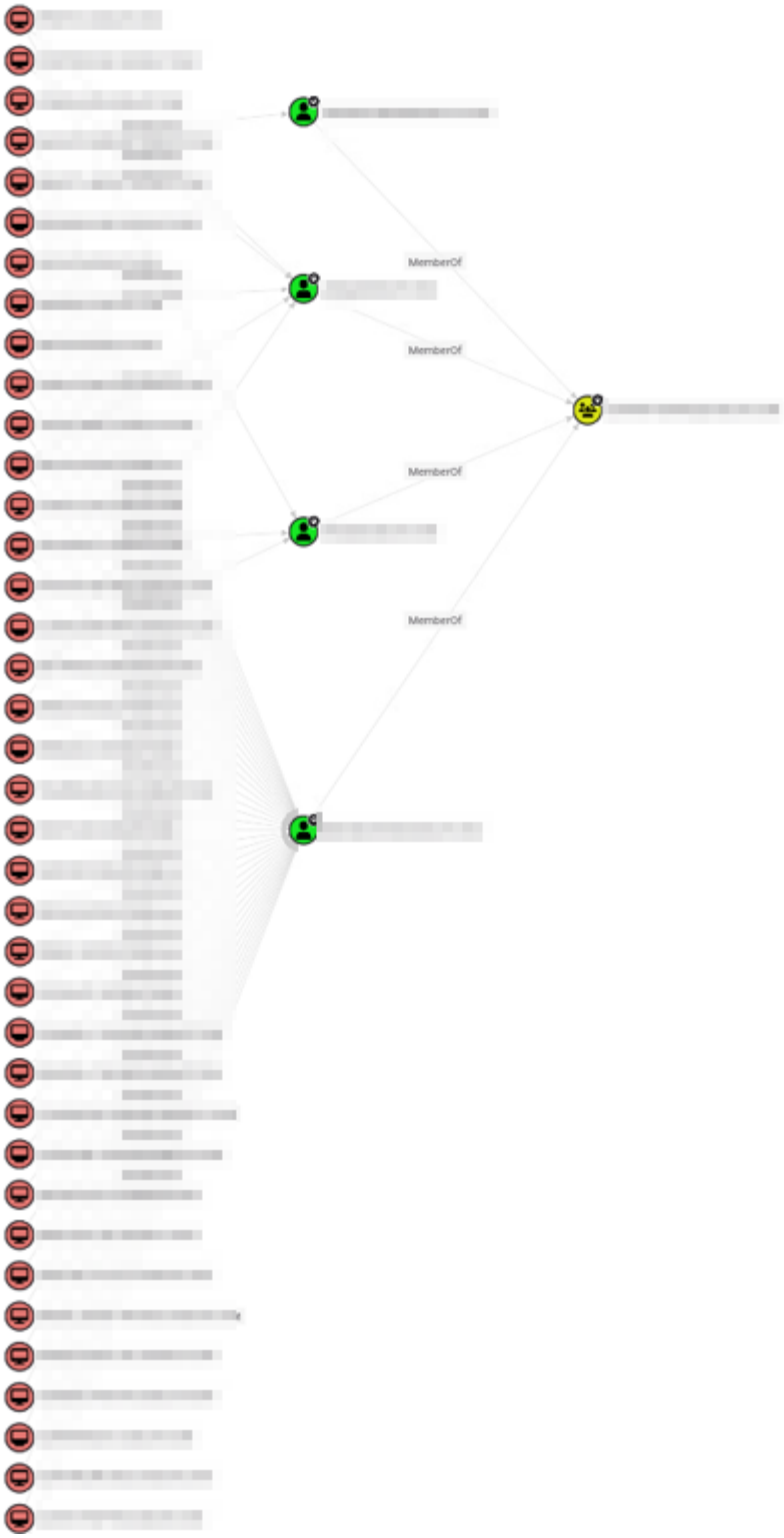


Figure 3: Domain Admin Login Sessions

Security References

NIST 800-53: AC-1, AC-2, AC-3, AC-5, AC-6, AC-8, AC-9, AC-24, AT-1, AT-3, AU-1, AU-2, AU-3, AU-6, AU-8, AU-11, AU-12, AU-14, IA-1, IA-2, PM-1, PM-10, PM-14, PM-15
NIST CSF: ID.AM-6, ID.GV-1, ID.GV-2, PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-6, PR.AT-1, PR.AT-2, PR.AT-4, PR.AT-5, PR.IP-11, PR.MA-2, PR.PT-1, DE.AE-3, DE.AE-5, DE.CM-3, DE.CM-7, DE.DP-1

ID	Finding	Severity	Type	Mitigation Status
2	Vulnerable Certificate Templates	• High	Internal	• Not Mitigated

Affected Systems

UTIL.EXAMPLE.COM, WebServer

Description

Active Directory Certificate Services (AD CS) provides templates for issuing and managing certificates. Such templates can include information about enrollment policies, predefined certificate settings, and other properties. Misconfiguring various elements of AD CS templates can result in domain escalation by unauthorized users (e.g., granting low-privileged users certificate enrollment rights, allowing requesters to specify a subjectAltName in the certificate signing request (CSR), not requiring authorized signatures for CSRs, granting FullControl or WriteDacl permissions to users).

The EXAMPLE environment contains Active Directory Certificate Services (AD CS) with templates that may be vulnerable to ESC15, a misconfiguration that allows a low-privileged user to request a certificate and inject arbitrary Application Policy OIDs. This could enable unauthorized authentication or enrollment actions, including impersonation of high-privilege accounts (e.g., Domain Admins), effectively resulting in domain compromise.

The specific vulnerability associated with ESC15 is tracked as CVE-2024-49019. Microsoft has released security updates in November 2024 that mitigate this issue by enforcing stricter validation of Application Policies on certificate requests, preventing attacker-supplied OIDs from being incorporated into issued certificates. RMC was not able to verify whether or not patches have been applied due to PKINIT not being supported by the environment.

Recommended Mitigation

It is recommended that the organization verify that the Windows Server hosting the Certificate Authority (CA) has applied the November 2024 security updates addressing CVE-2024-49019. All certificate templates should be audited to ensure that “Enrollee supplies subject” is not enabled unnecessarily, that EKUs and Application Policies are restricted to what is required, and that enrollment permissions are limited to authorized groups only. AD CS templates should be hardened according to Microsoft’s security best practices to prevent ESC15-like abuse, and monitoring should be implemented to detect suspicious certificate requests or anomalous Application Policy OIDs. These measures will reduce the risk of certificate-based privilege escalation and help ensure that the CA is not vulnerable to exploitation.

Relevant Screenshots

This screenshot shows the affected CA and certificate template configuration.

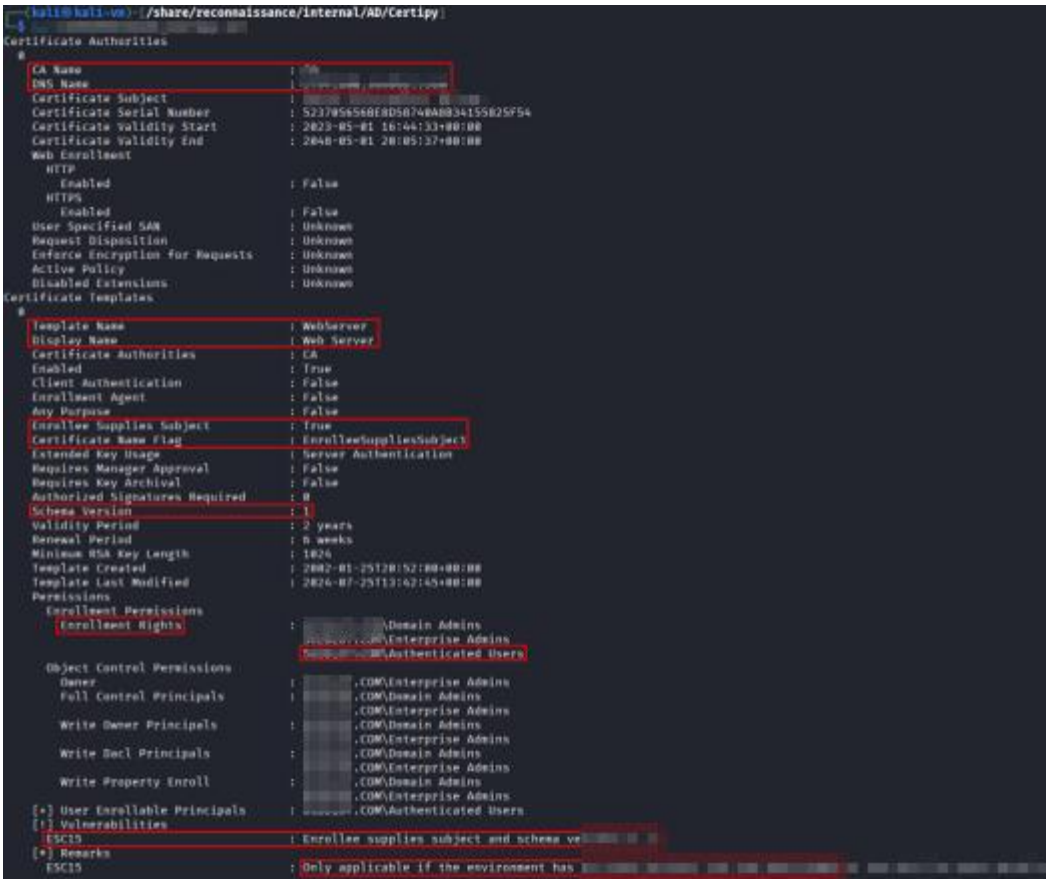


Figure 4: ESC15 on ITUTIL08.EXAMPLE.COM

Security References

NIST 800-53: CM-3, CM-4, SA-10, AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24
NIST CSF: PR.IP-3, PR.AC-4

ID	Finding	Severity	Type	Mitigation Status
3	Dangerous Object Configuration	• Medium	Internal	• Not Mitigated

Affected Systems

BOBBY@EXAMPLE.COM, ASPNET@EXAMPLE.COM, TENT@EXAMPLE.COM, SQLSERVICE@EXAMPLE.COM, TOM@EXAMPLE.COM

Description

One or more user accounts in the Active Directory environment have unconstrained delegation enabled. This configuration allows the account to impersonate any user who authenticates to it, across all services in the domain. When unconstrained delegation is set, the Kerberos Ticket Granting Ticket (TGT) of any user authenticating to the account can be used to access other network services with the privileges of the impersonated user. Both service accounts and standard user accounts with this setting significantly increase the risk of lateral movement and privilege escalation if the account is compromised.

Recommended Mitigation

It is recommended to disable unconstrained delegation for all user accounts unless absolutely necessary. Where delegation is required, implement constrained delegation or resource-based constrained delegation (RBCD) to restrict which services the account can delegate to. Audit all user accounts to identify and remediate unnecessary delegation privileges. Additionally, implement monitoring for ticket-granting events, anomalous Kerberos activity, and unauthorized access attempts to detect potential abuse of accounts with delegation enabled.

Relevant Screenshots

This screenshot shows delegation properties discovered on accounts in EXAMPLE.COM.

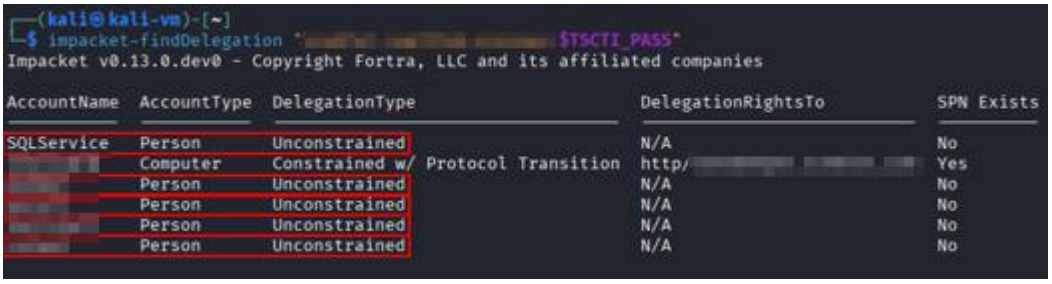


Figure 5: Unconstrained Delegation on User Accounts

Security References

NIST 800-53: AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24
NIST CSF: PR.AC-4

General Recommendations

To support the RMC team's goal of helping stakeholders improve their security posture, the assessment team identified general recommendations based on the Center for Internet Security's (CIS) Critical Security Controls for mitigating the risks discovered. Table 2 represents a high-level summary of prioritized recommended remediations and the associated findings. As always, EXAMPLE COMPANY NAME has a much deeper understanding of its business and technical environment standards that should determine the balance of implementation.

ID	Controls	Finding ID
1	Inventory and Control of Enterprise Assets	1, 4, 5, 6, 7, 8, 9, 10, 11, 12
2	Inventory and Control of Software Assets	4, 7, 8, 9, 10, 11
3	Data Protection	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12
4	Secure Configuration of Enterprise Assets and Software	1, 4, 7, 9, 11, 12
5	Account Management	1, 2, 3, 4, 6, 12
6	Access Control Management	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12
7	Continuous Vulnerability Management	5, 7, 9, 10
8	Audit Log Management	1, 7
9	Email and Web Browser Protections	4, 7, 9, 10, 11
10	Malware Defenses	
11	Data Recovery	
12	Network Infrastructure Management	8, 9, 10, 11
13	Network Monitoring and Defense	6, 9, 10, 11, 12
14	Security Awareness and Skills Training	1, 7
15	Service Provider Management	12
16	Application Software Security	4, 5, 6, 8, 9, 10, 11
17	Incident Response Management	
18	Penetration Testing	

Table 2: Recommendations Based on CIS Controls

The RMC team is available to assist with any follow-up that EXAMPLE COMPANY NAME may need. For additional information on RMC's assessment and service offerings, contact info@rmcyber.io.

APPENDIX A: SEVERITY RATING CRITERIA

The severity selected for each finding during the Pen Test is determined using the criteria outlined below.

Severity	Description
• Critical	Critical findings pose an immediate and severe threat to the environment due to ease of exploitation and significant impact. In most cases, critical findings are reported immediately and rapid mitigation should be considered.
• High	High findings may be leveraged by an adversary to obtain full control over a targeted asset. This includes but is not limited to: easily exploitable vulnerabilities that lead to complete compromise of an application, system, or network; significant router/firewall/server misconfigurations; weak password configurations that lead to administrator account compromise; or any vulnerability that can be exploited using readily available tools leading to significant compromise of an asset.
• Medium	Medium findings may be leveraged by an adversary to obtain some control over a targeted asset. This includes but is not limited to: unauthorized disclosure of sensitive customer or user account information; unauthorized read access to sensitive business information; weak anti-virus implementation/configurations; and lack of segmentation between untrusted and trusted networks.
• Low	Low findings typically encompass items of interest that are not readily exploitable and/or do not result in compromise to confidentiality, integrity, or availability of assets. The raw data and scan reports provided by the RMC team should be reviewed for additional findings that may have been deemed low severity but were not included in this report based on the minor risk they present. Due to time constraints, the RMC team prioritizes higher risk findings and may not be able to validate lower severity findings.
• Informational	Informational findings are potential weaknesses within the environment that cannot be readily exploited. These findings represent areas that should be investigated further, but do not require immediate action or mitigation.

Table 3: Severity Rating Descriptions

APPENDIX B: EXTERNAL PORT MAPPING

During external testing, the RMC team identified the following open ports/services on EXAMPLE COMPANY NAME's public-facing systems. It is recommended to review the data below, determine if any unnecessary ports/services are publicly accessible, and minimize the external attack surface where possible.

IP	Hostname	Ports	Services
123.11.7.68		443/tcp	https
123.11.7.68		80/tcp 443/tcp	http https
123.11.7.68		80/tcp 443/tcp	http https
123.11.7.68		80/tcp 443/tcp	http https
123.11.7.68		80/tcp	http
123.11.7.68		21/tcp 22/tcp 80/tcp 443/tcp	ftp ssh http https
123.11.7.68		80/tcp 443/tcp	http https
123.11.7.68		443/tcp	https
123.11.7.68		179/tcp 1491/tcp	bgp anynetgateway
123.11.7.68		443/tcp	https
123.11.7.68		443/tcp	https
123.11.7.68		179/tcp	bgp
123.11.7.68		1491/tcp 6068/tcp	anynetgateway gsmp
123.11.7.68		179/tcp	bgp

Table 4: Open Ports and Services on External Systems

APPENDIX C: PASSWORD ANALYSIS

RMC obtained the hashed passwords for all the EXAMPLE COMPANY NAME users during the assessment and attempted to obtain the clear text passwords represented by the hashed values. The following output shows statistical analysis of the clear text passwords recovered by the RMC team:

```
[+] Analyzing 100% (14/14) of passwords
    NOTE: Statistics below is relative to the number of analyzed passwords, not total number
of passwords

[*] Length:
[+]                          8: 14% (2)
[+]                          9: 14% (2)
[+]                         10: 14% (2)
[+]                         12: 14% (2)
[+]                         16: 14% (2)
[+]                         17: 14% (2)
[+]                         14: 07% (1)
[+]                         15: 07% (1)

[*] Character-set:
[+]             mixedalphanum: 28% (4)
[+]                       all: 28% (4)
[+]         mixedalphaspecial: 28% (4)
[+]      loweralphaspecialnum: 07% (1)
[+]      upperalphaspecialnum: 07% (1)

[*] Password complexity:
[+]                     digit: min(0) max(8)
[+]                     lower: min(0) max(12)
[+]                     upper: min(0) max(6)
[+]                   special: min(0) max(3)

[*] Simple Masks:
[+]                 othermask: 35% (5)
[+]             stringspecial: 28% (4)
[+]               stringdigit: 21% (3)
[+]        digitstringspecial: 07% (1)
[+]        stringdigitspecial: 07% (1)

[*] Advanced Masks:
[+] ?u?l?l?l?l?d?d?d?u?l?l?l?l?d?d?d: 07% (1)
[+]          ?u?l?l?l?l?l?d?d: 07% (1)
[+]        ?u?l?l?l?l?l?l?l?s: 07% (1)
[+] ?u?s?l?l?l?d?l?l?u?s?l?l?l?d?l?l: 07% (1)
[+] ?l?l?l?l?d?d?d?d?l?l?l?l?d?d?d?d?s: 07% (1)
[+]      ?u?l?l?l?l?u?l?l?l?s: 07% (1)
[+] ?u?s?l?l?l?d?l?l?u?s?l?l?l?d?l?l?s: 07% (1)
[+] ?u?l?l?l?l?l?l?l?u?l?l?l?l?l?l?s: 07% (1)
[+]  ?u?l?l?l?l?l?l?d?d?d?d?d: 07% (1)
[+] ?u?l?l?l?l?u?l?l?l?l?l?l?l?s: 07% (1)
[+]      ?u?l?l?l?l?l?l?d?d?d: 07% (1)
[+]  ?u?u?u?s?s?s?l?l?l?d?d?d: 07% (1)
[+]        ?u?l?l?l?l?l?l?d?s: 07% (1)
[+]          ?d?u?u?u?u?u?u?s: 07% (1)
```

APPENDIX D: ABBREVIATIONS AND ACRONYMS

ADCS	Active Directory Certificate Services
AES	Advanced Encryption Standard
ARP	Address Resolution Protocol
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
AV	Anti-Virus
C2	Command-and-Control
CA	Certificate Authority
CIFS	Common Internet File System
CIS	Center for Internet Security
CLI	Command Line Interface
CMS	Content Management System
CPL	Control Panel (File Format)
CSF	Cybersecurity Framework
DA	Domain Administrator
DACL	Discretionary Access Control List
DC	Domain Controller
DCC2	Domain Cached Credentials Version 2
DHCP	Dynamic Host Configuration Protocol
DHS	Department of Homeland Security
DLL	Dynamic-Link Library (File Format)
DLP	Data Loss Prevention
DNS	Domain Name System
DoS	Denial of Service
EDR	Endpoint Detection and Response
EOL	End-of-Life
EWS	Exchange Web Services

EXE	Executable (File Format)
FAST	Federal Attack Surface Testing
FCRM	Financial Crime Risk Management
FTP	File Transfer Protocol
FTPS	File Transfer Protocol Secure
GPO	Group Policy Object
HTA	Hypertext Markup Language Application (File Format)
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
IIS	Internet Information Services
IP	Internet Protocol
IPMI	Intelligent Platform Management Interface
ISCSI	Internet Small Computer Systems Interface
JS	JScript (Microsoft File Format)
LDAP	Lightweight Directory Access Protocol
LDAPS	Secure Lightweight Directory Access Protocol
LFI	Local File Inclusion
LLMNR	Link-Local Multicast Name Resolution
LSA	Local Security Authority
LSASS	Local Security Authority Subsystem Service
MAQ	Machine Account Quota
MFA	Multi-Factor Authentication
MS-EFSRPC	Microsoft Encrypting File System Remote Protocol
MitM	Machine-in-the-Middle
NBT-NS	NetBIOS Name Service
NIST	National Institute of Standards and Technology

NTLM	New Technology Local Area Network Manager
OS	Operating System
OTP	One Time Password
OWA	Outlook Web Access
PACE	Post-Assessment Closure Evaluation
PDF	Portable Document Format
PHI	Protected Health Information
PHP	Hypertext Preprocessor
PIF	Program Information File
PII	Personally Identifiable Information
POC	Point of Contact
PSK	Pre-Shared Key
PTH	Pass-the-Hash
RADIUS	Remote Authentication Dial-In User Service
RC4	Rivest Cipher 4
RDP	Remote Desktop Protocol
RPT	Remote Penetration Test
Pen Test	Penetration Test
SAM	Security Account Manager
SAN	Subject Alternate Name
EXAMPLE	EXAMPLE COMPANY NAME
SDK	Software Development Kit
SDLC	System Development Lifecycle
SFTP	Secure Shell File Transfer Protocol
SMB	Server Message Block
SNMP	Simple Network Management Protocol
SOCKS	Socket Secure

SP	Special Publication
SPN	Service Principal Name
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Sockets Layer
SSN	Social Security Number
TCP	Transmission Control Protocol
TGS	Ticket Granting Service
TGT	Ticket Granting Ticket
TLS	Transport Layer Security
UDP	User Datagram Protocol
UPS	Uninterruptible Power Supply
UPnP	Universal Plug and Play
VBA	Visual Basic for Applications
VPN	Virtual Private Network
WMI	Windows Management Instrumentation
WPA	Wireless Fidelity Protected Access
Wi-Fi	Wireless Fidelity
XDR	Extended Detection and Response
XLL	Excel Add-In (File Format)
XML	Extensible Markup Language
XSS	Cross-Site Scripting
iDRAC	Integrated Dell Remote Access Controller
mDNS	Multicast Domain Name System