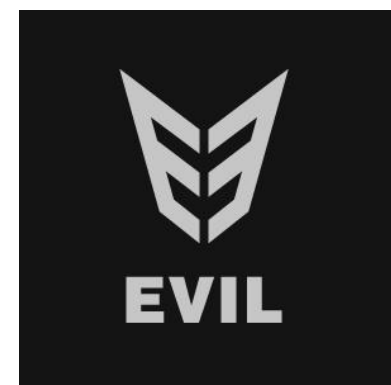


RIT

**Rochester
Institute of
Technology**

**2023 SECURITY
ASSESSMENT REPORT
PREPARED FOR**



Report Issued: December 11, 2023

TABLE OF CONTENTS

► EXECUTIVE SUMMARY	3
► DETAILED TECHNICAL FINDINGS AND RECOMMENDATIONS	4
► APPENDIX A: Evidence	16

► EXECUTIVE SUMMARY

Introduction




Group 5, LLC (“Group 5” or “we”) performed a security audit of Evil Corporation’s (EC) networks during the period of November 27, 2023 through December 10, 2023. The purpose of the assessment was to identify security vulnerabilities and gaps within the Evil Corporation environment which could allow for unauthorized access to EC systems or data and result in business disruption or loss of sensitive data. The assessment does not, nor was it intended to, guarantee the identification of all vulnerabilities due to the dynamic nature of EC’s information technology environment. Our findings represent a snapshot in time and any changes occurring after our assessment could affect the observations documented in this report.

Overall Network Security

Information Technology Security Assessment

Group 5 conducted this network audit using a combination of manual verification of different settings and configurations as well as some automated scanning or information gathering scripts. As a result of both the manual and automated testing, a number of vulnerabilities and other potential risks were identified.

Key among these observed issues are weak passwords throughout the environment as well as missing patches and updates across multiple systems. Both of these classes of issues are indicative of problems at the policy level. There is either a roadblock in adherence to the existing policy, or the existing policy does not properly address these concerns. Group 5 recommends that a thorough review of existing cybersecurity policies is conducted to ensure that they address all relevant areas of concern. Following that, a review of training and process adherence should further reveal where the disconnect between policies and implementation is occurring.

Good Practices		
<p>The use of AppArmour on the SUPPORT host is good practice, as are the file system permissions and access control. Similarly, the access control rules established through the Active Directory domain are effective and prevent users from having more access than is necessary. The chosen authentication method for the domain, Kerberos, is a secure and effective method and is configured in a way that balances usability with security.</p>		
Summary Observations		Recommendations
Password Policy		Revise password policy to require longer, more complex passwords that make it more difficult for attackers to gain control of an account using simple password attacks such as brute forcing or password spraying.
Patch Management		Revise or create a Patch Management policy to ensure that patches and updates are tested and applied to all devices within an appropriate time frame.
AD CS Domain Escalation		Remove vulnerable templates and perform periodic reviews to ensure that old, unused, or vulnerable templates are identified and addressed.

► DETAILED TECHNICAL FINDINGS AND RECOMMENDATIONS

Risk Definitions

During our assessment, we identified security weaknesses in applications and systems, and have provided recommendations to address those weaknesses. It is imperative that all remediation attempts are tested prior to deploying them into the production environment. Some recommendations may affect users of the system or could impact the roles and responsibilities of support personnel; thus, the impact of these recommendations from a risk, cost, performance, and operational perspective should be considered prior to implementation. Management should recognize its full responsibility for any decisions it makes regarding these recommendations and to consider all related matters before moving forward with remediation actions. Based on industry standard practices, the following relative ratings (Critical, High, Medium, Low, and Informational) have been assigned to each observation based upon the risk they pose to EC systems.

Relative Rating	Risk	Sophistication	Remediation Effort (Remediation)
Critical	Exposure presents a clear and immediate threat to business systems or data or could significantly impact business operations.		
High	Exposure could allow significant access to business systems or data or could significantly impact business operations.	Requires a high level of technical aptitude to execute the attack. The attack uses advanced manual techniques.	Recommendation requires the acquisition of hardware or software and/or requires significant research and implementation activities (> 40 hours).
Medium	Exposure could impact business systems or data, or business operations could experience a reduction in performance.	Requires a moderate level of technical aptitude to execute the attack. The attack uses manual techniques and can be discovered using an automated tool.	Recommendation may require the acquisition of hardware or software and/or moderate research and implementation activities (10 - 40 hours).
Low	Exposure should not impact business operations but should be addressed to meet expected business operation.	Requires a low level of technical aptitude to execute the attack. The attack is generally identified and exploited with only an automated tool.	Recommendation may require minor research and implementation activities (< 10 hours).
Informational	There is little to no risk associated with the observation and is provided only as context for other observations.		

Information Technology Security Assessment Observations and Recommendations

EXT-1: AD Password Policy		
Risk: High	Sophistication: Low	Remediation: Low
Observation		
Active Directory password requirements allow extremely vulnerable passwords that are well below accepted length and complexity standards.		
Affected Systems		
All domain joined devices and accounts.		
Impact		
Poor password complexity requirements allow domain users to create passwords which attackers are able to more easily crack through methods such as password spraying or brute-force guessing.		
Recommendation		
Required password length should be set to a minimum of eight characters, with complexity requirements enabled to decrease the ability of attackers to guess domain passwords through password spraying attacks.		
Passwords should have a lifetime that requires users to set a new password after some time to limit the ability of attackers to gain access using leaked or old passwords.		
Reference Documentation:		
<ul style="list-style-type: none">• https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/minimum-password-length• https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/password-must-meet-complexity-requirements		

EXT-2: Linux Password Policy		
Risk: High	Sophistication: Low	Remediation: Low
Observation		

EXT-2: Linux Password Policy

The root user account utilizes a weak password which should not be allowed by policy. The password policy for the SUPPORT machine is insufficient, using only the default PAM obscure module.

Affected System

- SUPPORT (192.168.56.30)

Impact

Using weak administrator credentials can have significant and far-reaching consequences for the security and integrity of a system or network.

The most immediate and obvious impact is the increased risk of unauthorized access. Weak credentials make it easier for attackers to guess or crack passwords, gaining unauthorized entry to sensitive systems and data.

Once an attacker gains access, they may have the ability to exfiltrate sensitive data. This could lead to a data breach, compromising sensitive information such as personal data, financial records, or intellectual property.

Attackers with administrator access can carry out a range of malicious activities, such as installing malware, altering configurations, deleting or modifying critical files, disrupting services, or launching attacks on other systems.

Weak credentials can be a stepping stone for privilege escalation attacks. Once inside a system, attackers may attempt to elevate their privileges to gain even more control over the infrastructure.

Recommendation

Require complex, unique passwords for all users.

Require multi-factor authentication.

Reference Documentation:

<https://orca.security/resources/blog/weak-host-password/#:~:text=Weak%20passwords%20of%20local%20user,and%20then%20gain%20unauthorized%20access.>

<https://www.crowdstrike.com/cybersecurity-101/lateral-movement/>

<https://attack.mitre.org/mitigations/M1027/#:~:text=Ensure%20that%20root%20accounts%20have,all%20systems%20on%20the%20network.&text=and%20%2Fetc%2Fshadow-,Ensure%20that%20root%20accounts%20have%20complex%2C%20unique%20passwords,all%20systems%20on%20the%20network.&text=Ensure%20only%20valid%20password%20filters%20are%20registered.>

EXT-3: AD CS Domain Escalation		
Risk: High	Sophistication: Medium	Remediation: Low
Observation		
<p>The Active Directory Certificate Services templates contain at least four known configurations which can be leveraged to escalate privileges within the domain.</p> <p>The following templates have been identified:</p> <ul style="list-style-type: none"> • ESC1 • ESC2 • ESC3 • ESC3-CRA • ESC4 <p>Due to how these templates are named, directly correlating the template name to the vulnerable configuration, it is possible that these vulnerable configurations were intentionally created.</p>		
Affected Server		
<ul style="list-style-type: none"> • BRAAVOS (192.168.56.23) 		
Impact		
<p>Depending on which vulnerable template is targeted, an attacker may be able to generate certificates enabling them to:</p> <ul style="list-style-type: none"> • Authenticate as any principal in the domain, • Sign new certificates, • Sign code, • Further escalate privileges throughout the domain 		
Recommendation		
<p>The vulnerable template configurations should be removed or reconfigured to remove the vulnerable settings.</p> <p>A template creation process should be created and followed to ensure that certificate templates are configured with secure and appropriate permissions.</p> <p>A periodic review of templates configured in the service should be conducted, checking for potentially vulnerable configurations as well as old or outdated templates.</p>		

EXT-3: AD CS Domain Escalation

Reference Documentation:

- https://specterops.io/wp-content/uploads/sites/3/2022/06/Certified_Pre-Owned.pdf

EXT-4: Linux Services Running with Elevated Permissions

Risk: **Medium**

Sophistication: **Medium**

Remediation: **Low**

Observation

Services running on the SUPPORT server are running with a higher than recommended level of permissions.
The apache2 service currently runs under the root user.

Affected Server

- SUPPORT (192.168.56.30)

Impact

An attacker who is able to successfully attack a service running under a high privilege account may be able to assume the permissions granted to that service account. This could lead to an escalation of the attacker's privileges on the system.

Recommendation

Services on all devices should be configured to run under accounts with the least possible privilege. For example, apache2 should be configured to run under a dedicated web service account such as www-data. This account should be granted permissions for only the files and directories that are directly required by the web service.

A periodic review of services and services account permissions should take place in order to identify any services running with inappropriate permissions.

Reference Documentation:

- <https://cwe.mitre.org/data/definitions/250.html>

EXT-5: Linux Patch Management		
Risk: Medium	Sophistication: Low	Remediation: Low
Observation		
Linux systems do not appear to be under patch management processes. Out of date and vulnerable versions of software are present on the system, some of which are multiple years old.		
Affected Server		
<ul style="list-style-type: none"> SUPPORT (192.168.56.30) 		
Impact		
<p>Unpatched systems are more vulnerable to exploitation, and are more often targeted by attackers.</p> <p>The specific impact will depend on the vulnerable software, the system, and other factors, however the presence of these vulnerabilities all serve to increase the attack surface which a malicious actor can make use of.</p>		
Recommendation		
<p>A review of existing patch management processes should be conducted to determine improvements which would ensure that all systems are appropriately receiving updates.</p> <p>Updates for software should be tested and applied within a reasonable time frame and according to the patch management policy. Software which is no longer being maintained or does not receive security updates should be evaluated for replacement where possible.</p>		
Reference Documentation:		
<ul style="list-style-type: none"> https://cwe.mitre.org/data/definitions/1104.html https://cwe.mitre.org/data/definitions/1395.html 		

EXT-6: Default Accounts Enabled		
Risk: Medium	Sophistication: Medium	Remediation: Low
Observation		

EXT-6: Default Accounts Enabled		
The Windows default Administrator user is enabled in Active Directory.		
Affected Systems		
Active Directory		
Impact		
Well-known account names can be targeted in brute-forcing, and the Administrator account is a member of several security groups with the ability to read and edit almost all information in the domain.		
Recommendation		
Disable or rename the Active Directory account "Administrator" so attackers are not able to use this account to gain admin access to the domain.		
Reference Documentation: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-default-user-accounts		

EXT-7: Multi-Factor Authentication for Admin Accounts		
Risk: Medium	Sophistication: Medium	Remediation: Low
Observation		
Weak passwords and no multi factor authentication to remediate the risk.		
Affected accounts		
<ul style="list-style-type: none"> Admin accounts 		
Impact		
Attackers who are able to guess the password of an admin account are immediately granted full access to the infrastructure, enabling them to create and delete accounts and read and edit any sensitive data in the domain.		
Recommendation		

EXT-7: Multi-Factor Authentication for Admin Accounts

Require multi-factor authentication for all users in the Administrators security group.
Monitor system administrator activity for failed login attempts or other evidence of attack.

Reference Documentation:

<https://actzero.ai/resources/blog/compromised-admin-account>
<https://attack.mitre.org/tactics/TA0003/>
<https://www.ekransystem.com/en/blog/system-server-administrators>

EXT-8: Windows Patch Management

Risk: **Medium**

Sophistication: **Medium**

Remediation: **Medium**

Observation

Windows systems do not appear to have any patch management processes. Out of date and vulnerable versions of software are present on multiple systems. Systems do not appear to have any consistent patching system and differ by multiple years.

[Sample of] Affected Systems

- MEEREEN (192.168.56.12)
- WINTERFELL (192.168.56.11)

Impact

Unpatched systems lack important security updates making them more vulnerable to exploitation, and are often weak points which are targeted by attackers. The specific impact will depend on the vulnerable software, system, and other factors. The widespread lack of up to date patches means there are likely multiple vulnerabilities that could be exploited.

Recommendation

A review of existing patch management processes (if any) should be conducted and updated to ensure that all systems are being reasonably kept up to date. Updates for software should be tested and applied within a reasonable time frame and according to the patch management policy. Software which is no longer being maintained or is otherwise not updateable should be evaluated for replacement where possible.

EXT-8: Windows Patch Management

Reference Documentation:

- [CWE - CWE-1104: Use of Unmaintained Third Party Components \(4.13\) \(mitre.org\)](#)
- [CWE - CWE-1329: Reliance on Component That is Not Updateable \(4.13\) \(mitre.org\)](#)
- [CWE-1395: Dependency on Vulnerable Third-Party Component](#)

EXT-9: Linux Host-Based Firewalls

Risk: **Low**

Sophistication: **Medium**

Remediation: **Medium**

Observation

Local firewalls are enabled but have not been configured to filter any traffic, which will allow malicious traffic to reach the host.

Affected Systems

SUPPORT (192.168.56.30)

Impact

Disabled or improperly configured firewalls may allow malicious traffic to reach the host as part of an attack.

Recommendation

Review firewall configurations to properly filter traffic that has a high chance of being malicious.

Allow only known-good traffic through the local firewall to help ensure the host can communicate with only trusted entities.

Reference Documentation: <https://www.redhat.com/sysadmin/firewalld-linux-firewall>

EXT-10: New AD User Policy

Risk: **Low**

Sophistication: **High**

Remediation: **Low**

Observation

There is no documented policy for adding new users to the AD environment.

EXT-10: New AD User Policy		
Affected services		
<ul style="list-style-type: none"> Active Directory 		
Impact		
The lack of a new AD user policy is not a security threat on its own. However, the lack of an established policy opens up the possibility for other vulnerabilities to go unnoticed.		
Recommendation		
Create and implement a process for adding new AD users to ensure that all new user activity is tracked and reviewed.		
Reference Documentation: <ul style="list-style-type: none"> CWE - CWE-286: Incorrect User Management (4.13) (mitre.org) 		

EXT-11: Appropriate Sudo Privileges		
Risk: Low	Sophistication: Medium	Remediation: Medium
Observation		
Users and groups that have been given permission to elevate privileges using sudo appear to include a student user, which may not be appropriate.		
Affected Systems		
<ul style="list-style-type: none"> SUPPORT (192.168.56.30) 		
Impact		
Inappropriate sudo privileges increases the attack surface for attackers. Users with inappropriate permissions may not have the same security as authorized sudo users and could be exploited more easily.		
Recommendation		
Review Sudo permission policy and all users that have been granted sudo privileges. Ensure that all users with sudo privileges are appropriate.		

EXT-11: Appropriate Sudo Privileges

Reference Documentation:

- [CWE - CWE-269: Improper Privilege Management \(4.13\) \(mitre.org\)](#)

EXT-12: LDAP Traffic Encryption

Risk: **Low**

Sophistication: **Medium**

Remediation: **Low**

Observation

Since signing is not required, as shown in the GPO, unencrypted traffic can be used.

Affected System

- Active Directory

Impact

Lack of signatures on LDAP communications can allow man-in-the-middle attacks that result in information disclosure and data tampering.

Recommendation

Require signing for LDAP traffic from both server and client.

Reference Documentation:

<https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-ldap-client-signing-requirements>

<https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/domain-controller-ldap-server-signing-requirements>

► APPENDIX A: Evidence

EXT-1: Active Directory Password Policy

Account Policies/Password Policy	
Policy	Setting
Enforce password history	24 passwords remembered
Maximum password age	37201 days
Minimum password age	1 days
Minimum password length	5 characters
Password must meet complexity requirements	Disabled
Store passwords using reversible encryption	Disabled

Group policy object defining password requirements for AD accounts.

EXT-2: Linux Password Policy

```
# here are the per-package modules (the "Primary" block)
password [success=1 default=ignore] pam_unix.so obscure sha512
```

Only the default “obscure” module is in use, which does not adequately check for password complexity.

EXT-3: AD CS Domain Escalation

```
PS C:\Windows\system32> certutil -CATemplates
ESC4: ESC4 -- Access is denied.
ESC3-CRA: ESC3-CRA -- Access is denied.
ESC3: ESC3 -- Access is denied.
ESC2: ESC2 -- Access is denied.
ESC1: ESC1 -- Access is denied.
DirectoryEmailReplication: Directory Email Rep
```

Certutil.exe output showing the names of the vulnerable certificate templates.


```

ESC1: ESC1 -- Access is denied.
msPKI-Enrollment-Flag = 0
msPKI-Certificate-Name-Flag = 1
CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT -- 1
msPKI-Private-Key-Flag = 1010000 (16842752)
CTPRIVATEKEY_FLAG_ATTEST_NONE -- 0
TEMPLATE_SERVER_VER_2003<<CTPRIVATEKEY_FLAG_SERVERVERSION_SHIFT -- 10000 (65536)
TEMPLATE_CLIENT_VER_XP<<CTPRIVATEKEY_FLAG_CLIENTVERSION_SHIFT -- 1000000 (16777216)
flags = 20220 (131616)
CT_FLAG_AUTO_ENROLLMENT -- 20 (32)
CT_FLAG_ADD_TEMPLATE_NAME -- 200 (512)
CT_FLAG_IS_MODIFIED -- 20000 (131072)
cn = ESC1
distinguishedName = ESC1
displayName = ESC1
templateDescription = User
pKIExtendedKeyUsage = 1.3.6.1.5.5.7.3.2 Client Authentication

```

Detailed output of the ESC1 template configuration. This shows the CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT flag is set, and the certificate has the Client Authentication OID applied. This combination is described in the ESC1 attack and can allow low-privileged users to generate certificates allowing authentication as any principal in the domain.

EXT-4: Linux Services Running with Elevated Permissions

```

root@student-server:/etc/init.d# systemctl show -pUser,UID apache2
UID=[not set]
User=
root@student-server:/etc/init.d#

```

systemctl output showing that the apache2 service has no UID or user specified, indicating that it is running under the root user account.

EXT-5: Linux Patch Management

```

sudo/bionic,now 1.8.21p2-3ubuntu1 amd64 [installed,upgradable to: 1.8.21p2-3ubuntu1.6]

```

apt output showing an outdated version of sudo on the SUPPORT server.

EXT-5: Linux Host-Based Firewall Not Configured

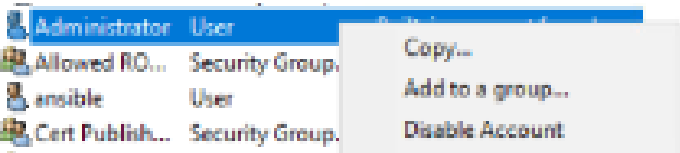
```
root@student-server:/etc/init.d# iptables -S
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
root@student-server:/etc/init.d# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
root@student-server:/etc/init.d#
```

Screenshot showing all firewall policies accept all traffic by default.

EXT-6: Default Accounts Enabled



Windows default account “Administrator” present in Active Directory and enabled.

EXT-8: Windows Patch Management

Source	Description	HotFixID	InstalledBy	InstalledOn
MEEREN	Update	KB3199986	NT AUTHORITY\SYSTEM	11/21/2016 12:00:00 AM
MEEREN	Update	KB4013418	NT AUTHORITY\SYSTEM	3/24/2017 12:00:00 AM
MEEREN	Update	KB4091664	NT AUTHORITY\SYSTEM	1/4/2019 12:00:00 AM
MEEREN	Update	KB4132216	NT AUTHORITY\SYSTEM	7/24/2018 12:00:00 AM
MEEREN	Security Update	KB4465659	NT AUTHORITY\SYSTEM	1/4/2019 12:00:00 AM
MEEREN	Security Update	KB4509091	NT AUTHORITY\SYSTEM	8/16/2019 12:00:00 AM
MEEREN	Update	KB4512495	NT AUTHORITY\SYSTEM	8/19/2019 12:00:00 AM

Patch history of MEEREEN (192.168.56.12). Patching has not been performed since 2019, 4 years out of date

Source	Description	HotFixID	InstalledBy	InstalledOn
-----	-----	-----	-----	-----
WINTERFELL	Update	KB5020627	NORTH\Administrator	12/12/2022 12:00:00 AM
WINTERFELL	Security Update	KB4470788	NT AUTHORITY\SYSTEM	3/5/2019 12:00:00 AM
WINTERFELL	Update	KB4488856	NORTH\Administrator	3/5/2019 12:00:00 AM
WINTERFELL	Security Update	KB4509095	NT AUTHORITY\SYSTEM	8/8/2019 12:00:00 AM
WINTERFELL	Security Update	KB4512037	NT AUTHORITY\SYSTEM	8/13/2019 12:00:00 AM
WINTERFELL	Security Update	KB4523204	NT AUTHORITY\SYSTEM	1/23/2020 12:00:00 AM
WINTERFELL	Security Update	KB4558997	NT AUTHORITY\SYSTEM	7/29/2020 12:00:00 AM
WINTERFELL	Update	KB4589288	NT AUTHORITY\SYSTEM	12/12/2022 12:00:00 AM
WINTERFELL	Security Update	KB5012170	NORTH\Administrator	12/12/2022 12:00:00 AM
WINTERFELL	Security Update	KB5019066	NT AUTHORITY\SYSTEM	12/12/2022 12:00:00 AM
WINTERFELL	Security Update	KB5020374	NT AUTHORITY\SYSTEM	12/12/2022 12:00:00 AM

Patch history of WINTERFELL (192.168.56.11). Patching has not been performed since 2022, nearly 1 year out of date.

EXT-12: LDAP Traffic Signing

Domain Controller	
Policy	Setting
Domain controller: LDAP server signing requirements	None

Group policy object showing no signing requirements for LDAP traffic.