SAMPLE COMPANY LTD

Red Teaming Assessment 2021

Document Name:	red_teaming_assessemt_2021_v1.0.docx
Version:	v1.0
Project Number:	31337
Date of Delivery:	August 1st, 2021
Authors:	Security Analyst A, Compass Security Deutschland GmbH Security Analyst B, Compass Security Deutschland GmbH
Classification:	STRICTLY CONFIDENTIAL

Compass Security Deutschland GmbH, Tauentzienstraße 18, DE-107879 Berlin
T +49 30 21 00 253-0, team.csde@compass-security.com, www.compass-security.com

Table of Contents

1 Overview

1.1 To the Reader

This document is geared towards project teams, development personnel and other individuals concerned with the security issues of the SAMPLE COMPANY LTD information system and the result of the red team exercise. The purpose of this document is to summarize the results of the tests performed on the existing security systems using technical terminology. The points pertaining to security issues are listed in chapter 3.

1.2 Document Structure

Chapter	Content
1	Document overview
2	Executive summary explaining the outcome of the security tests
3	A list of the detected weaknesses as well as suggestions for improvement
4 - 5	Protocol of the performed security tests
6	Appendix

2 Management Summary

2.1 Overall Impression

From Mai until June 2021, Compass Security performed a red teaming exercise against SAMPLE COMPANY LTD (hereinafter referred to as "COMPANY"), during a XY person-day timespan. During this time, several realistic attacks were performed, starting from the public zone of the COMPANY headquarters. Compass Security managed to compromise several systems and high privileged account to eventually gain access to most of the critical systems. The attack remained undetected until the end of the tests and the activities were only partially logged or detected. Access to the highest security zone could not be achieved during this time frame.

Additionally, several technical and organizational vulnerabilities were identified during the test, which might have an impact on the confidentiality and integrity of the COMPANY information system. To achieve a high security standard, it is recommended to fix the discovered issues.

2.2 Introduction

Compass Security Deutschland GmbH (hereinafter referred to as "Compass"), as an independent branch of the Swiss Compass Security Network Computing AG, is a company specializing in security assessments and forensic investigations and is based in Berlin. We carry out penetration tests and security reviews for our clients, enabling them to assess the security of their IT systems against hacking attacks, as well as advising them on suitable measures to improve their defenses. Compass Security has considerable experience in national and international projects. Close collaboration with universities enables Compass to perform field research. Thus, our security specialists are always up to date.

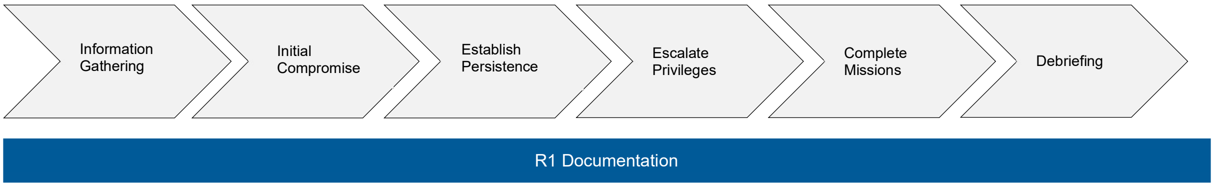
2.3 Objectives

The red teaming is intended to provide an attack simulation again the customer under real-life conditions. The following key questions and objectives will be pursued:

- Perform attacks again high-value targets defined with the customer (missions)
- Evaluate the effectiveness of the implemented security measure and detection capabilities.
- Train the Blue Team based on a realistic attack.
- Detailed suggestions on how to improve the security level.

2.4 Procedures

Compass Security divided the red teaming assessment in multiple phases as shown below. The results are summarized in this report.



Information Gathering

Initial Compromise

Establish Persistence

Escalate Privileges

Complete Missions

Debriefing

R1 Documentation

2.5 Missions

N/A

2.6 Results

N/A

2.7 Recommendations

N/A

3 Vulnerabilities and Remediation

3.1 Logging & Detection

The following table summarizes the monitoring and detection measures that can help detecting malicious activity similar as what was performed during the security test. A definition for each column is given here:

No.	Reference	Measure	Priority	Comment
Each issue is consecutively numbered.	Reference to the corresponding test case in the following chapters.	Explains the vulnerability identified during the analysis and means to detect related malicious activity.	Priority of the measure with regard to the threat posed by a successful exploitation. Three levels are possible: ▪ **High** ▪ **Medium** ▪ **Low**	Comment and additional information.

No.	Reference	Measure	Priority	Comment
1.	5.1	**Kerberoasting Monitoring** Any domain user can request a Kerberos ticket granting service (TGS) for accounts configured with a service principal name (SPN). Since the service account's NTLM hash is used to create the TGS, one can save the TGS and try to crack the password offline. This attack is known as Kerberoasting. To log the actions relevant to TGS, the setting `Audit Kerberos Service Ticket Operations` must be enabled. Event ID 4769 is the most relevant (A Kerberos service ticket was requested). This event will appear very often, especially on domain controllers. The detection should focus on unusual samples: ▪ Concentration of events over a short period. ▪ TGS requests with RC4 encryption (Type 0x17), because the more recent ciphers highly increase the complexity of the attack. These events can be forwarded by the Windows Event Forwarding (WEF) to a Windows Event Collector (WEC) to be stored centrally and available for correlation. More information: https://attack.mitre.org/techniques/T1208/ https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-kerberos-service-ticket-operations https://adsecurity.org/?p=3458 https://docs.microsoft.com/en-us/windows/security/threat-protection/use-windows-event-forwarding-to-assist-in-intrusion-detection	**High**	

3.2 Technical Vulnerabilities

The following table summarizes the security issues found during the security review. A definition for each column is given here:

No.	Reference	Weakness	Threat	Remediation	Rating	Comment
Each issue is consecutively numbered.	Reference to the corresponding test case in the following chapters.	Explains the vulnerability identified during the analysis.	Explains what could happen if the weakness is exploited.	Recommendation on how to correct the vulnerability.	Compass rating of the weakness and the corresponding threat: 💣 : Low 💣💣 : Medium 💣💣💣 : High **INFO** : Not security relevant issue *See section 6.1 for detailed description.*	

No.	Reference	Weakness	Threat	Remediation	Rating	Comment

2.	5.xx	**SMB and LDAP Signing not Required**
		
		In the analyzed network, SMB signing is not required on all the hosts.
		
		Packet signing allows the recipient of SMB packets to confirm the authenticity of the sender and helps preventing relaying and man-in-the-middle attacks.
			Unsigned communications make it possible to relay the credentials of a victim to other hosts.
			
			By relaying a SMB connection, the attacker can browse the shares of a server which doesn't require signing with the victim's rights. If the victim has administrative rights on the target, the attacker can gain the same permissions.
				Enforce SMB message signing in all hosts' configuration.
				
				On Windows, establish the recommended configuration via Group Policy using the following paths:
				
				SMB, for all hosts:
				`Microsoft network server: Digitally sign communications (always)`
				`Microsoft network client: Digitally sign communications (always)`
					💣💣💣	

3.3 Organizational Vulnerabilities

The following table summarizes the security issues found during the security review. A definition for each column is given here:

No.	Reference	Weakness	Threat	Remediation	Rating	Comment
Each issue is consecutively numbered.	Reference to the corresponding test case in the following chapters.	Explains the vulnerability identified during the analysis.	Explains what could happen if the weakness is exploited.	Recommendation on how to correct the vulnerability.	Compass rating of the weakness and the corresponding threat: 💣 : Low 💣💣 : Medium 💣💣💣 : High **INFO** : Not security relevant issue *See section 6.1 for detailed description.*	

No.	Reference	Weakness	Threat	Remediation	Rating	Comment
3.	5.xx	**Lack of Awareness Regarding Password Strength** Several clear text passwords of users and administrators were collected along the test. Although they all meet the requirements of the password policy, several are easy to brute-force due to the use of a pattern. An example would be the use of a dictionary word followed by a number as "Spring2019" for example.	Using brute-force attacks and mutation rules (for example put the first letter in uppercase, append current year, l33t sp34k, …), it is possible to recover clear text passwords from the hashes within a reasonable amount of time (several hours to several days).	The users should be taught how to choose a strong password. In particular, it should be clear that passwords should not be related to the user (name of the kids, current year or birthdate, …). Currently, it is thought to be safer to have a long password than a complex one. Therefore, users could be encouraged to use passphrases. Further, users should be made aware of the risks inherent to password reuse. For example, between a normal user and an administrative user or a user in one domain and the corresponding user in another domain.	💣💣	

3.4 Tidy Up

No.	Reference	Weakness	Threat	Remediation	Rating	Comment
4.		**Created User Account** At the end of the test, a new user was created and granted high privileges to test the detection of such a behavior: `DOMAIN\ADM_1337`	-	Remove the user account as soon as possible.	**INFO**	
5.		**Compromised User Credentials** During the test, credentials for several users were compromised, either as NTLM hash or in clear text: ▪ `Administrator` (local user on `H0001`) ▪ `DOMAIN\u1234`	-	If possible, change the passwords of the compromised accounts.	**INFO**	

4 Logbook

This table gives an overview of all actions that occurred during the red teaming engagement. It should give a good idea of what was performed at which time, what was successful or not. For more details on the techniques and tools that were used, a link to the test cases is provided, when relevant.

Date/Time	Event	Testcase details
04.05.2021	Created the Threema communication group and mutually exchanged the keys.	N/A (demo report)
18.05.2021	Started the OSINT phase.	N/A
06.06.2021 16:02	Sent first information gathering phishing e-mail to 6 people.	N/A
09.06.2021 09:08	Sent second information gathering phishing e-mail to 31 people.	N/A
16.06.2021 08:45	Sent fake job application e-mail to hr@domain.de	N/A
16.06.2021 11:04-11:12	Response to fake job application, website visit, download of malicious Word file, macro execution, information collection, response e-mail from HR.	N/A
27.06.2021 16:52	Sent phishing email with pretext X to email@domain.de E-mail contains word document with macro-enabled template. Template initiates staging of a cobalt strike beacon.	N/A
28.06.2021 07:47	Initial contact of remote beacon running on host `H0001` with user `u1234`.	N/A
30.06.2021		
13:30	Kerberoasting Attack against `domain.local.` Cracking the hashes was not successful.	5.1
14:11	Running SharpHound ingestor for the first time on `domain.local`	5.2

5 Red Teaming Activities

5.1 Kerberoasting domain.local

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	Was any vulnerability discovered during this test?	No.	As expected.	PASS
2.	Which techniques were used?	List of MITRE TTP ID(s).	T1208 - Kerberoasting	N/A
3.	Was any detection or alarm mechanism triggered?	Yes.	No.	FAIL

Details

Starting time	30.07.2019 – 13:30
Source host(s)	Host XYZ, IP 1.2.3.4

Running kerberoasting attack with one of the compromised users:

```
Rubeus.exe kerberoast /creduser:domain.local\U1234 /credpassword:[CUT BY COMPASS]
/dc:1.2.3.5 /outfile:kerberoast.out


   ______        _
  (_____ \      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \| ___ | | | |/___)
  | |  \ \| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/

  v1.4.2


[*] Action: Kerberoasting

[*] NOTICE: AES hashes will be returned for AES-enabled accounts.
[*]         Use /ticket:X or /tgtdeleg to force RC4_HMAC for these accounts.

[*] Using alternate creds  : domain.local\U1234
[*] Searching path 'LDAP://domain.local' for Kerberoastable users

[*] Found 12 user(s) to Kerberoast!

[CUT BY COMPASS]

[*] Roasted hashes written to : [CUT BY COMPASS]\kerberoast.out
```

5.2 Running SharpHound ingestor

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	Was any vulnerability discovered during this test?	No.	As expected.	PASS
2.	Which techniques were used?	List of MITRE TTP ID(s).	▪ T1482 - Domain Trust Discovery ▪ T1046 - Network Service Scanning	N/A
3.	Was any detection or alarm mechanism triggered?	Yes.	No.	FAIL

Details

Starting time	30.07.2019 – 14:11
Source host(s)	Host XYZ, IP 1.2.3.4

Running sharphound ingestor with the privileges of the current user account:

```
PS C:\> .\SharpHound.exe -c All,GPOLocalGroup -t 1 --StatusInterval 10000 -d domain.local
Initializing BloodHound at 2:11 PM on 8/6/2019
Resolved Collection Methods to Group, LocalAdmin, GPOLocalGroup, Session, LoggedOn, Trusts,
ACL, Container, RDP, ObjectProps, DCOM, SPNTargets
Starting Enumeration for domain.local
Status: 20 objects enumerated (+20 2/s --- Using 63 MB RAM )
Status: 20 objects enumerated (+0 1/s --- Using 62 MB RAM )
Status: 20 objects enumerated (+0 0.6666667/s --- Using 62 MB RAM )
[CUT BY COMPASS]
```

6 Appendix

6.1 Compass Weaknesses Rating

Please read this section to understand the Compass weaknesses rating.

6.1.1 What the rating IS NOT

It IS NOT a risk rating. The motivation and opportunity of threat agents as well as the financial impact is not taken into consideration as it cannot be determined by Compass Security.
All vulnerabilities are rated independent from other security controls that might be in place. Examples are:

- If Compass performs tests in the Intranet, border protection is not taken into consideration. We assume that the place we are testing from is hostile.
- If assessing systems in the Intranet, other systems in the Intranet that are not assessed are not taken into consideration for the rating.

6.1.2 What to do with the weaknesses table

- The customer should carefully review the weaknesses table and assess the risk based on the business impact. The final risk rating does not necessarily need to match the initial Compass rating.
- This internal rating should enable the customer to decide how the risk should be treated (e.g., mitigate, accept, avoid or transfer). The decision should be driven by the risk appetite of the company.
- A risk mitigation plan should be developed to schedule and prioritize the remediation of the individual weaknesses.

6.1.3 Examples

Rating	Severity	Examples
💣💣💣 High	▪ Exploitation is easy and leads to high privileges and/or affects many users. ▪ System can be controlled with little effort. ▪ High impact if vulnerability is disclosed. Fix should be implemented with highest priority. Keep in mind that an issue within a back-end system might not pose the same threat as one in an Internet-facing service.	▪ SQL Injection or Cross-Site Scripting (XSS) ▪ Privilege escalation vulnerabilities ▪ Remote shell vulnerabilities ▪ Authorization bypass vulnerabilities ▪ Default accounts with high privileges ▪ Security filter bypass ▪ Weak encryption ciphers or protocols ▪ Phone in surveillance mode ▪ XML External Entity (XXE)
💣💣 Medium	▪ Exploitation can lead to higher privileges if combined with other weaknesses. ▪ Exploitation requires significant effort. Fix should be implemented in a reasonable time.	▪ Exposed management interfaces ▪ Caching of sensitive data ▪ Denial-of-Service conditions ▪ Insecure cookie settings ▪ Disclosure of usernames, email-addresses ▪ Large attack surface due to open ports
💣 Low	▪ Abuse does not lead to higher privileges. ▪ Information disclosure vulnerabilities Can be solved in the long term.	▪ Disclosure of product and version (banners) ▪ Default pages and samples ▪ DNS zone transfer ▪ DNS reverse lookups
INFO	Just an informational point without security relevant implications.	▪ Usability and performance issues ▪ Developer and staging bugs ▪ Clean-up notes

6.1.4 Tests with result "INFO" and N/A

- All tests with the result "INFO" will be listed in the weaknesses table.
- All tests with the result "N/A" will NOT be listed in the weaknesses table.

6.2 Recheck Coloring

The following color code is used for pointing out, whether a previously identified vulnerability is solved, partly solved, not solved, no recheck conducted or if new vulnerabilities have been found.

Lavender	Red	Yellow	Green	Gray
🟪	🟥	🟨	🟩	⬛
A new vulnerability was found.	Vulnerability still exists.	Vulnerability was partially eliminated.	Vulnerability was eliminated.	No recheck conducted.

Wir begleiten Sie punktuell mit unserem Fachwissen bei der erfolgreichen Umsetzung Ihrer IT-Sicherheitsstrategie und freuen uns auf Ihre Kontaktaufnahme.

Compass Security Deutschland GmbH
Tauentzienstraße 18
10789 Berlin

Jan-Tilo Kirchhoff
Managing Director

Tel. 030 210 02 53-10

jan-tilo.kirchhoff@compass-security.com