OFFENSIVE SECURITY

Penetration Test Report for Internal Lab and Exam

oredreim@gmail.com

The Nothebook

02 of july 2021

Contents

1 Executive Summary

1.1 Summary of Results

The present document take the results obtain in the auditory section made with the machine **The Nothebook**

Figure 1: here goes the caption of the images

2 Attack Narrative

2.1 Remote System Discovery

```
#!/bin/bash
for port in $(seq 1 65535); do
    timeout 1 bash -c "echo > "
done;wait

```

Listing 1: Script de algo

2.2 Admin Webserver Interface Compromise

2.3 Interactive Shell to Admin Server

2.4 Administrative Privilege Escalation

2.5 Java Client Attacks

2.6 Escalation to Local Administrator

2.7 Deep Packet Inspection Bypass

2.8 Citrix Environment Compromise

2.9 Escalation to Domain Administrator

3 Conclusion

3.1 Recommendations

3.2 Risk Rating

4 Vulnerability Detail and Mitigation