



OFFENSIVE SECURITY

Penetration Test Report for Internal Lab and Exam

oredreim@gmail.com

The Nothebook

Copyright © 2021 Offensive Security Ltd. All rights reserved. No part of this publication, in whole or in part, may be reproduced, copied, transferred or any other right reserved to its copyright owner, including photocopying and all other copying, any transfer or transmission using any network or other means of communication, any broadcast for distant learning, in any form or by any means such as any information storage, transmission or retrieval system, without prior written permission from Offensive Security. .

Contents

1	Executive Summary	2
1.1	Summary of Results	2
2	Attack Narrative	2
2.1	Remote System Discovery	2
2.2	Admin Webserver Interface Compromise	2
2.3	Interactive Shell to Admin Server	2
2.4	Administrative Privilege Escalation	2
2.5	Java Client Attacks	2
2.6	Escalation to Local Administrator	2
2.7	Deep Packet Inspection Bypass	2
2.8	Citrix Environment Compromise	2
2.9	Escalation to Domain Administrator	2
3	Conclusion	2
3.1	Recommendations	2
3.2	Risk Rating	2
4	Vulnerability Detail and Mitigation	2

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

```
1  #!/bin/bash
2  for port in $(seq 1 65535); do
3      timeout 1 bash -c "echo > "
4  done;wait
5
```

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