

**Penetration Testing Report Template**

ATTENTION: This report contains confidential information and should only be viewed by authorized persons. Additionally techniques and tools discussed and demonstrated in this report should not be shared with entities other than the party for which this report was prepared.

**Document Details**

**Created by:** Infosec Institute

**For:** AMCE Corporation

**Delivered to:** Daffy Duck

**Classification:** Confidential

**Document History:** Version 1.1

**Contents**

**EXECUTIVE SUMMARY…………………………………………..….……4**

**APPROACH……………………………………………………..……...….….5**

**SCOPE…………………………………………………………………..………..6**

**KEY FINDINGS………………………………………………………..……….7**

**Insufficient Authentication…………………………….……….7**

**Improper Input Validation…………………………….………..8**

**Cleartext Authentication….……………………..….….….…10**

**Poor Passwords………………………………………………….…12**

**RECOMMENDATIONS……………………………………………….….13**

**Tactical Recommendations…………………………………..14**

**Strategic Recommendations…………………………………17**

**Overall Risk Chart/Summary………………………………..31**

**TECHNICAL REPORT……………………………………………………..32**

**Perimeter Security……………………………………..………..33**

**Port Scan Status…………………………………..…….….…….35**

**Service Banner Disclosure………………………….….……..36**

**CONCLUSION………………………………………………….……………55**

**APPENDIX……………………………………………………….…………..57**

**What each section should include.**

**EXECUTIVE SUMMARY**

Should include at least a single paragraph describing the overall posture of the security of the infrastructure or organization tested. It is catered to executives, so don’t be overly technical in this part.

**APPROACH**

The approach should have a basic description of how you approached the task.

**SCOPE**

What you conclude to be the scope of what’s to be tested. In this case it will be two virtual machines. You should also mention what is to be tested.

**KEY FINDINGS**

This should be a quick and short rundown of all the vulnerabilities you were able to exploit. There’s no need to go into any technical detail.

**RECOMMENDATIONS**

General recommendations on things to implement to improve or mitigate the weaknesses you were able to exploit.

**TECHNICAL REPORT**

Should include detailed technical explanations of what you exploited and how. This should include screenshots, command lists, etc.

**CONCLUSION**

This should be your overall conclusion as to the state of the security of these devices and a restating of your recommendations in general terms.

**APPENDIX**

This will include any references used for descriptions of vulnerabilities, exploits, etc. You will also want to include any technical words you’ve included that may not be common knowledge. For example, if you used the word SQL Injection in your executive part of the report, it would be good to have a definition of sql injection in this section so that an executivecould flip to these pages and understand the reference.