PENETRATION TEST REPORT

for

Sitting Duck BV

V 0.1
Amsterdam
January 1st, 2015

Document Properties

Client	Sitting Duck BV
Title	Penetration Test Report
Target	Target
Version	0.1
Pentester	FirstName LastName
Author	YourName
Reviewed by	FirstName LastName
Approved by	Melanie Rieback

Version control

Version	Date	Author	Description
0.1	January 1st, 2015	YourName	Initial draft

Contact

For more information about this Document and its contents please contact Radically Open Security B.V.

Name	Melanie Rieback
Address	Overdiemerweg 28 1111 PP Diemen The Netherlands
Phone	+31 6 10 21 32 40
Email	info@radicallyopensecurity.com

Table of Contents

1 Executive Summary

1.1 Introduction

...

This report contains our findings as well as detailed explanations of exactly how ROS performed the penetration test.

1.2 Scope of work

The scope of the penetration test was limited to the following target:

- Target

1.3 Project objectives

...

1.4 Timeline

The Security Audit took place between X and Y, 2015.

1.5 Results In A Nutshell

1.6 Summary of Findings

ID	Type	Description	Threat level

1.7 Summary of Recommendations

ID	Type	Recommendation

2 Methodology

2.1 Planning

Our general approach during this penetration test was as follows:

1. **Reconnaissance**
   We attempted to gather as much information as possible about the target. Reconnaissance can take two forms: active and passive. A passive attack is always the best starting point as this would normally defeat intrusion detection systems and other forms of protection, etc., afforded to the network. This would usually involve trying to discover publicly available information by utilizing a web browser and visiting newsgroups etc. An active form would be more intrusive and may show up in audit logs and may take the form of a social engineering type of attack.
2. **Enumeration**
   We used varied operating system fingerprinting tools to determine what hosts are alive on the network and more importantly what services and operating systems they are running. Research into these services would be carried out to tailor the test to the discovered services.
3. **Scanning**
   Through the use of vulnerability scanners, all discovered hosts would be tested for vulnerabilities. The result would be analyzed to determine if there any vulnerabilities that could be exploited to gain access to a target host on a network.
4. **Obtaining Access**
   Through the use of published exploits or weaknesses found in applications, operating system and services access would then be attempted. This may be done surreptitiously or by more brute force methods.

2.2 Risk Classification

Throughout the document, each vulnerability or risk identified has been labeled and categorized as:

- **Extreme**
  Extreme risk of security controls being compromised with the possibility of catastrophic financial/ reputational losses occurring as a result.
- **High**
  High risk of security controls being compromised with the potential for significant financial/ reputational losses occurring as a result.
- **Elevated**
  Elevated risk of security controls being compromised with the potential for material financial/ reputational losses occurring as a result.
- **Moderate**

Moderate risk of security controls being compromised with the potential for limited financial/ reputational losses occurring as a result.

- **Low**
  Low risk of security controls being compromised with measurable negative impacts as a result.

Please note that this risk rating system was taken from the Penetration Testing Execution Standard (PTES). For more information, see: http://www.pentest-standard.org/index.php/Reporting.

3 Reconnaissance and Fingerprinting

Through automated scans we were able to gain the following information about the software and infrastructure. Detailed scan output can be found in the sections below.

3.1 Automated Scans

As part of our active reconnaissance we used the following automated scans:

- nmap – http://nmap.org

4 Pentest Technical Summary

4.1 Findings

We have identified the following issues:

4.2 Non-Findings

In this section we list some of the things that were tried but turned out to be dead ends.

5 Future Work

6 Conclusion

Appendix 1 Testing team

Melanie Rieback	Melanie Rieback is a former Asst. Prof. of Computer Science from the VU, who is also the co-founder/CEO of Radically Open Security.
FirstName LastName	Info