iiNURTURE
Education Solutions
TOMORROW'S HERE

Chapter 4.1

Report Writing

Aim

To elaborate on the significance of good documentation and its benefits in ethical hacking, in terms of presenting the results of penetration testing in an organisation

Instructional Objectives

After completing this chapter, you should be able to:

- Discuss how documentation is carried out for the various stages of ethical hacking and penetration testing processes
- Discuss the various types of reports with examples
- Explain how documentation from various stages are combined to perform a comprehensive report
- Explain the importance of analysing various reports obtained from various tools at each stage and how to interpret false positives and manage false negatives
- Explain how vulnerabilities are rated in the report and the significance of rating them

Learning Outcomes

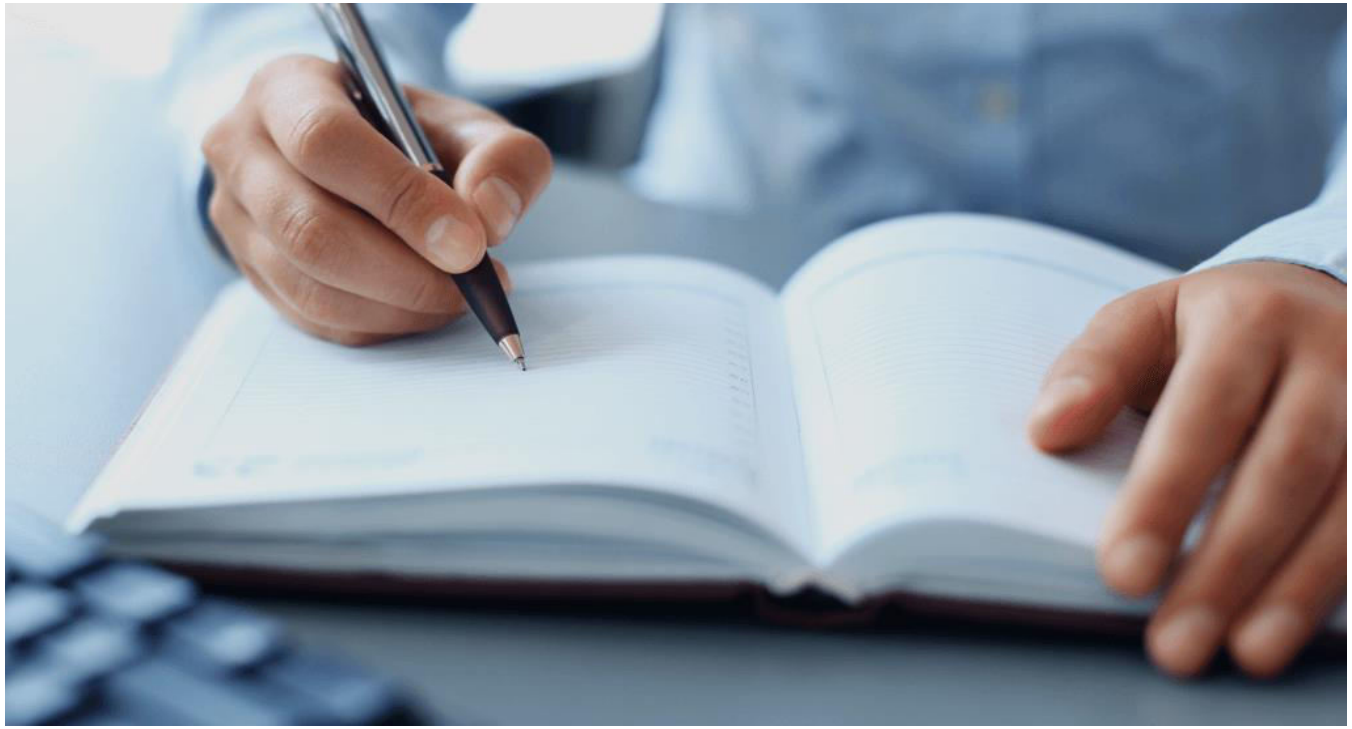
At the end of this chapter, you are expected to:

- Explain how various documents are prepared in ethical hacking and penetrating testing processes
- Differentiate various types of reports obtained in ethical hacking and penetration testing process
- Explain the process of combining documentation and preparing a comprehensive report based on the lab exercises performed
- Explain how to interpret the output from various tools used at each stage
- Discuss the significance of rating the vulnerabilities in a report
- Outline the methods used to rate vulnerabilities

Report writing

Introduction to Documentation and Report Writing

Investigation or an analysis in information security is to identify issues that pose a threat or an attack on information



Documentation is an art that needs to be mastered with effort and patience s

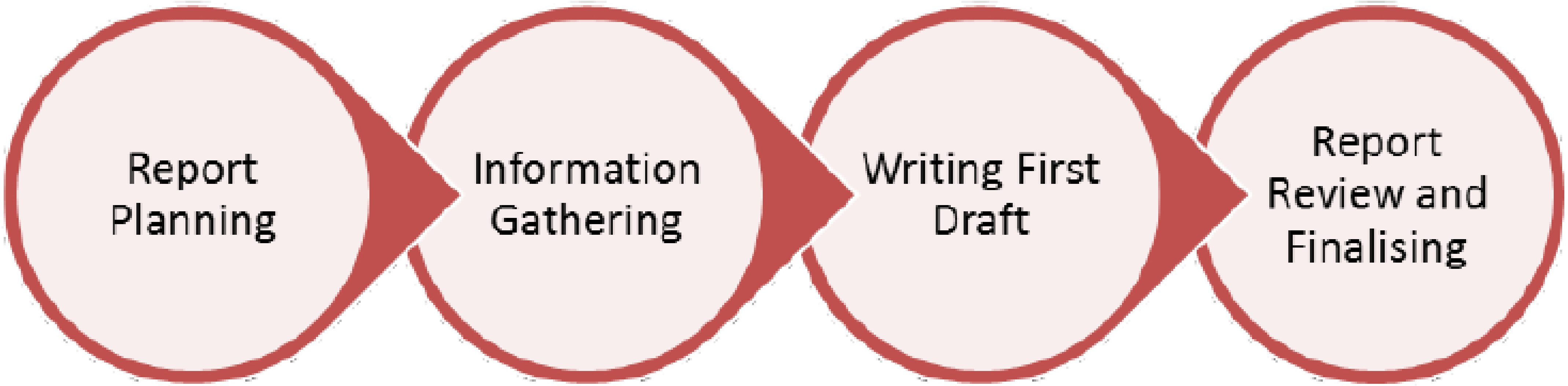
A penetrating testing report plays a significant role as it does the job of identifying the loopholes in the system and also outlines recommendations to address these issues

Significance of a Penetration Testing Report

- A penetration testing report can be considered as a valuable product of your hard work and serves as a great source for clients to complete the task that has been started, strengthening the security posture of their systems.
- The report has a lot of information that the client uses as input in making decisions about their information security setup.
- Facts indicated in the penetration report forms the basis for corrective measures to be taken up by organisations towards securing their systems.
- Hence, it is important for a report to reflect the actual scenario in simple words.

Phases in Report Writing

A penetration testing report will be referred to by various departments of a company, at different levels such as executives, middle management, information security professionals and higher management, as each of these employees have a role to play towards the safety of information and infrastructure of an organisation.



Report Planning

Information Gathering

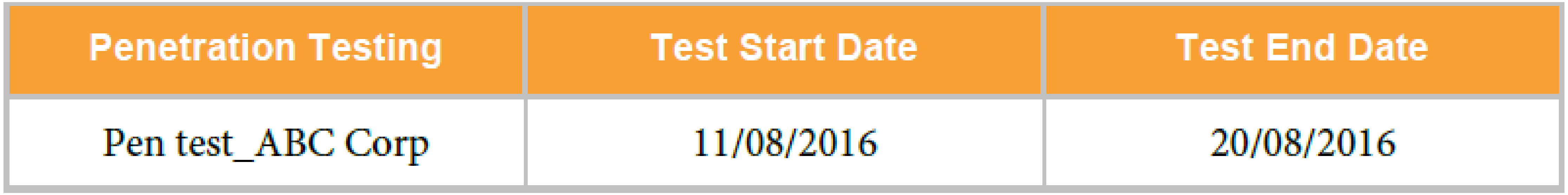
Writing First Draft

Report Review and Finalising

Setting a time frame

- The time frame for conducting a penetration test report is of utmost importance
- This transparency between the penetration tester and the organisation is crucial to plan the presence of key personnel during certain stages of the testing.

Indicating Time Factor in a Penetration Test Report



Penetration Testing	Test Start Date	Test End Date
Pen test_ABC Corp	11/08/2016	20/08/2016

Analyzing the target audience

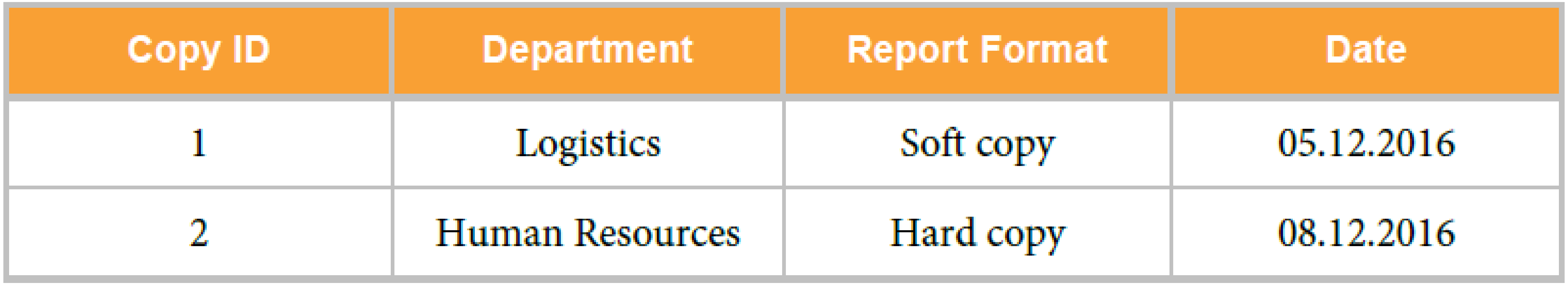
- The target user of a penetration testing report might belong to different hierarchy levels within an organisation, such as an Information Security Manager, Information Technology Head, Chief Information Security Officer or Technical Support.
- Hence, their expectations as well as their needs from this report will be different.
- Therefore, the requirements given below must be kept in mind while deciding on the form and style of the report.
    - Why does the company need this report?
    - What is their position in the organisation?
    - Does the report’s objective make sense to the company’s scope of work?
    - What is the individual’s role in implementing an action recommended in the report?

Classification of report

- Every organisation has its own guidelines for classifying information into categories such as private, public, confidential and critical.
- It is advisable to classify a penetration testing report as ‘confidential’ or even ‘highly confidential’ because it contains sensitive information such as IP addresses, account information, personal information, information about servers and corporate secrets.
- This is to make sure that the report doesn’t fall into the wrong hands or is misused.

Report distribution

To preserve confidentiality and integrity, a penetration testing report can be chosen to be distributed only to a single person or a selected number of people, either in the form of a hard or soft copy. A record of this has to be made in a simple tabular form as shown below:



Copy ID	Department	Report Format	Date
1	Logistics	Soft copy	05.12.2016
2	Human Resources	Hard copy	08.12.2016

Collecting Information

- Information is collected at every stage of penetration testing such as footprinting, scanning and assessing vulnerabilities.
- A significant amount of information also comes from tools run on computers and networks during tests.

First Draft

- The penetration testing report that you develop is not only a proof for your skills as an ethical hacker, but also reflects on your writing and comprehensive skills.
- Your ability to articulate and write in a manner that is easily understood by others, complements your professionalism.

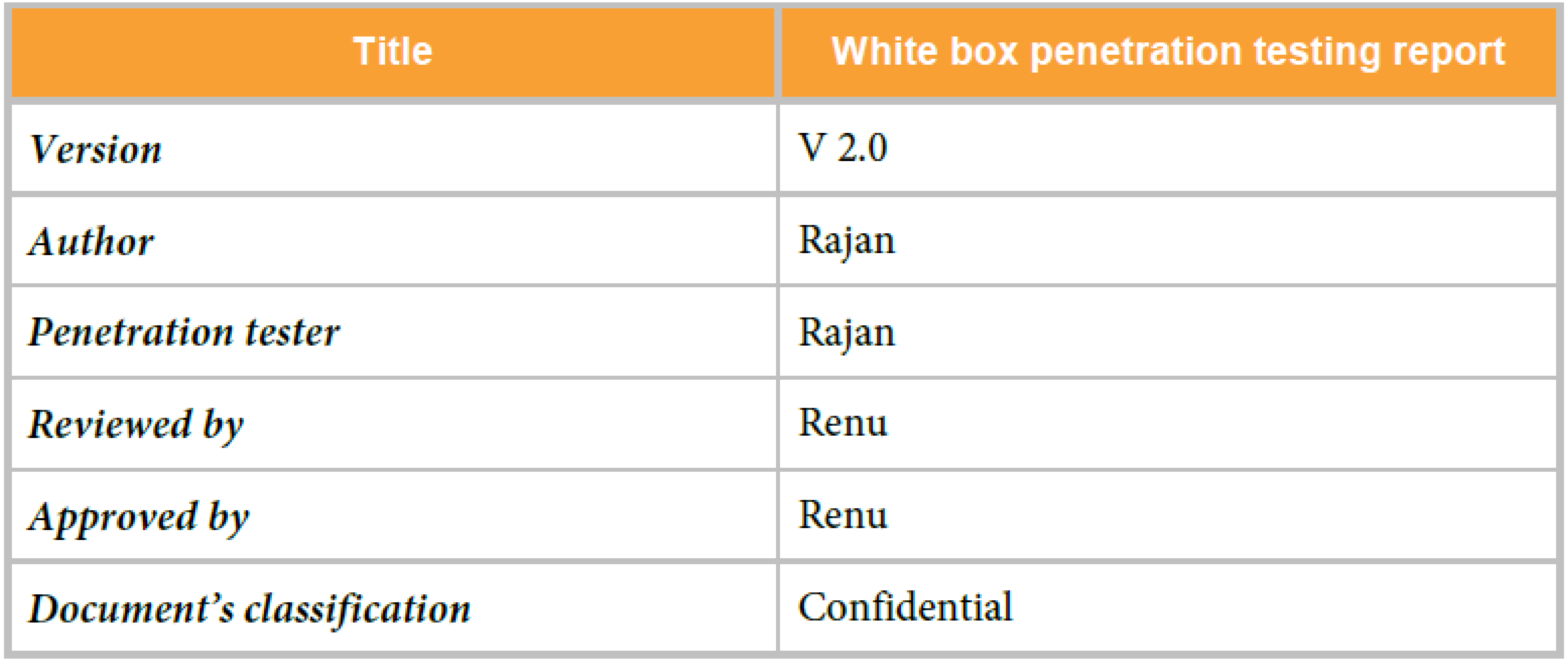
Review and Final Report

- Once the draft is ready, it can be shared with your peers for review and other team members involved in testing.
- Suggestions and improvements will follow and when the final report is ready, it is to be sent to the Quality Analysis team of the organisation.
- As the report will be an official announcement from the organisation, it must adhere to certain norms framed by the company, just like any other report.

Report Format

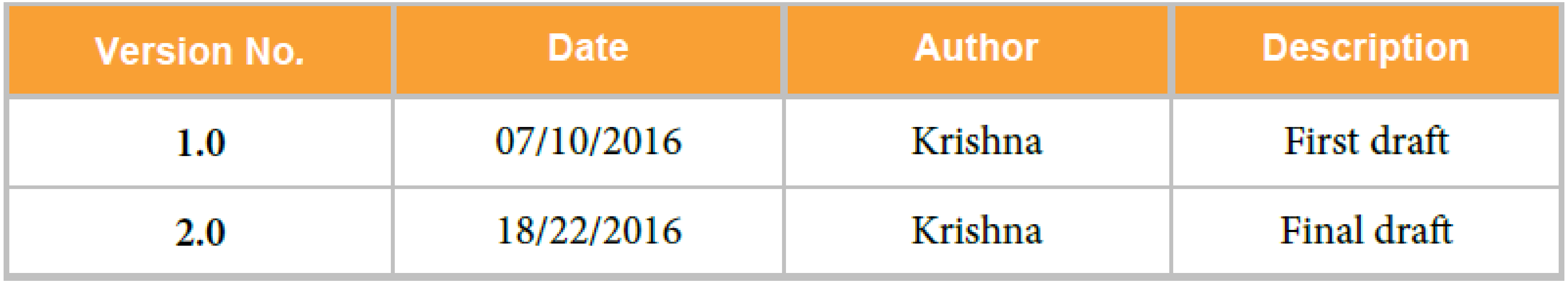
1. Organisations follow standard layouts and styles for all their official reporting
2. A table of contents or TOC
3. Executive Summary:
    a. Scope of work
    b. Objective
    c. Any assumptions made
    d. Timeframe of the assessment
    e. Summary of analysis
    f. Recommendations
4. Document properties

Indicating Document Properties in a Penetration Test Report



Title	White box penetration testing report
Version	V 2.0
Author	Rajan
Penetration tester	Rajan
Reviewed by	Renu
Approved by	Renu
Document’s classification	Confidential

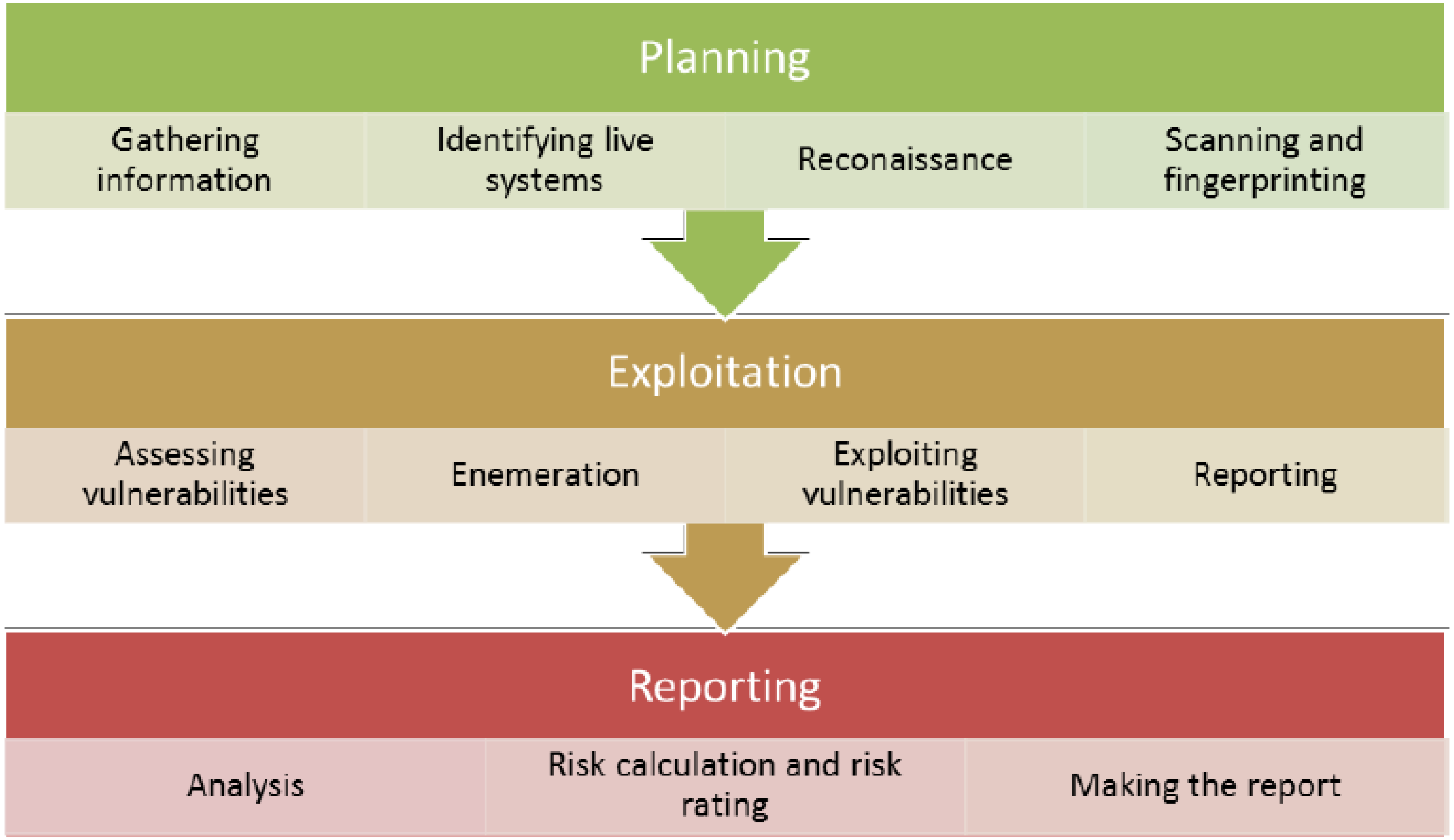
5. Version control is a very critical process that must be mandatorily carried out by all individuals who are responsible for documentation processing



Version No.	Date	Author	Description
1.0	07/10/2016	Krishna	First draft
2.0	18/22/2016	Krishna	Final draft

6. Methodology

Steps Involved in the Methodology Phase of a Penetration Test Report



Planning
- Gathering information
- Identifying live systems
- Reconaissance
- Scanning and fingerprinting

Exploitation
- Assessing vulnerabilities
- Enemeration
- Exploiting vulnerabilities
- Reporting

Reporting
- Analysis
- Risk calculation and risk rating
- Making the report

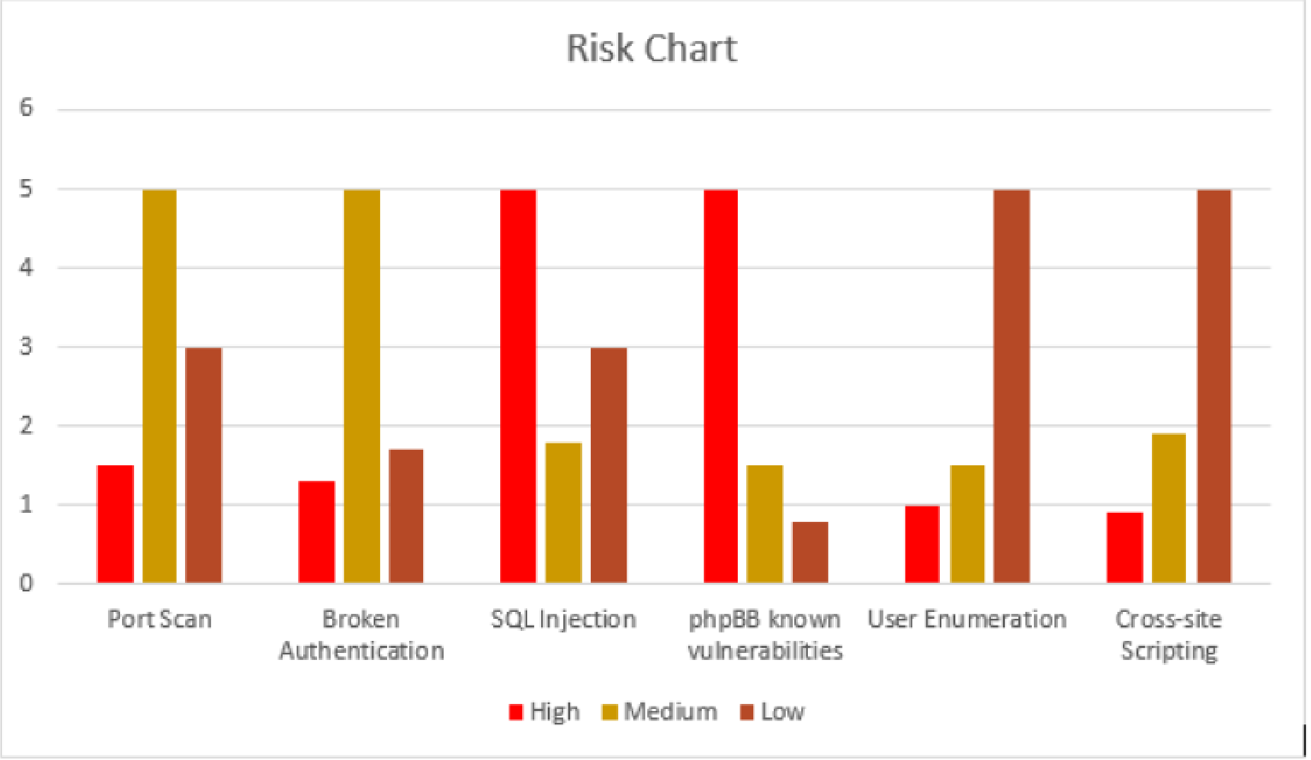
7. Findings

   a. Vulnerabilities Identified
   b. Impact
   c. Probability of an Attack
   d. Risk Evaluation
   e. Recommendation

8. References

9. Appendices

10. Glossary



Risk Chart in a Penetration Test Report

Example of a Penetration test report

- We have discussed some general rules and framework for preparing a Penetration test report that is normally followed by every tester.
- In practical scenarios, however, a slight deviation from these foundation principles is allowed as long as they convey correct information to the client.
- The deviations occur due to the testing environments and conditions that tester faces in a site.

Quiz / Assessment

1) One of the terms given below is not used to convey the classification of a report.			
a) Confidential	b) Vulnerable	c) Private	d) Public
2) The statement found at the beginning of a penetration report that clearly defines the purpose of the test is called:			
a) Scope of the report	b) Report objective	c) Document properties	d) Recommendations

Types of Reports

- Executive Report
- Technical Report
- Vulnerability Assessment Report
- Network Penetration Testing Report
- False Positive and False negatives

Executive Report

- An executive report is also known as an ‘executive summary’ and mainly covers the objectives of a penetration test and the top-level findings.
- The report is usually sent to the top management of the organisation to get a basic understanding of the whole exercise and arrive at decisions about taking immediate action against addressing the vulnerabilities that are marked as critical in the report.
- Some of the headings of an executive report have been listed below:

  a) Background
  b) Effectiveness of test
  c) Risk profile
  d) General findings
  e) Recommendation summary

Background

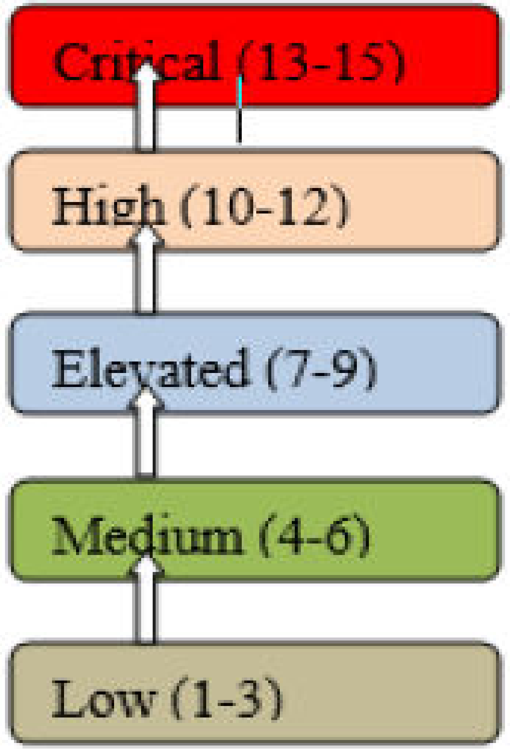
This section must outline the specific objectives of a penetration test and convey to the reader, under what conditions the test in being carried out.

Effectiveness of Test

This is a measure of the success of the penetration tester in achieving the objectives that he has set for himself or the client in the whole process.

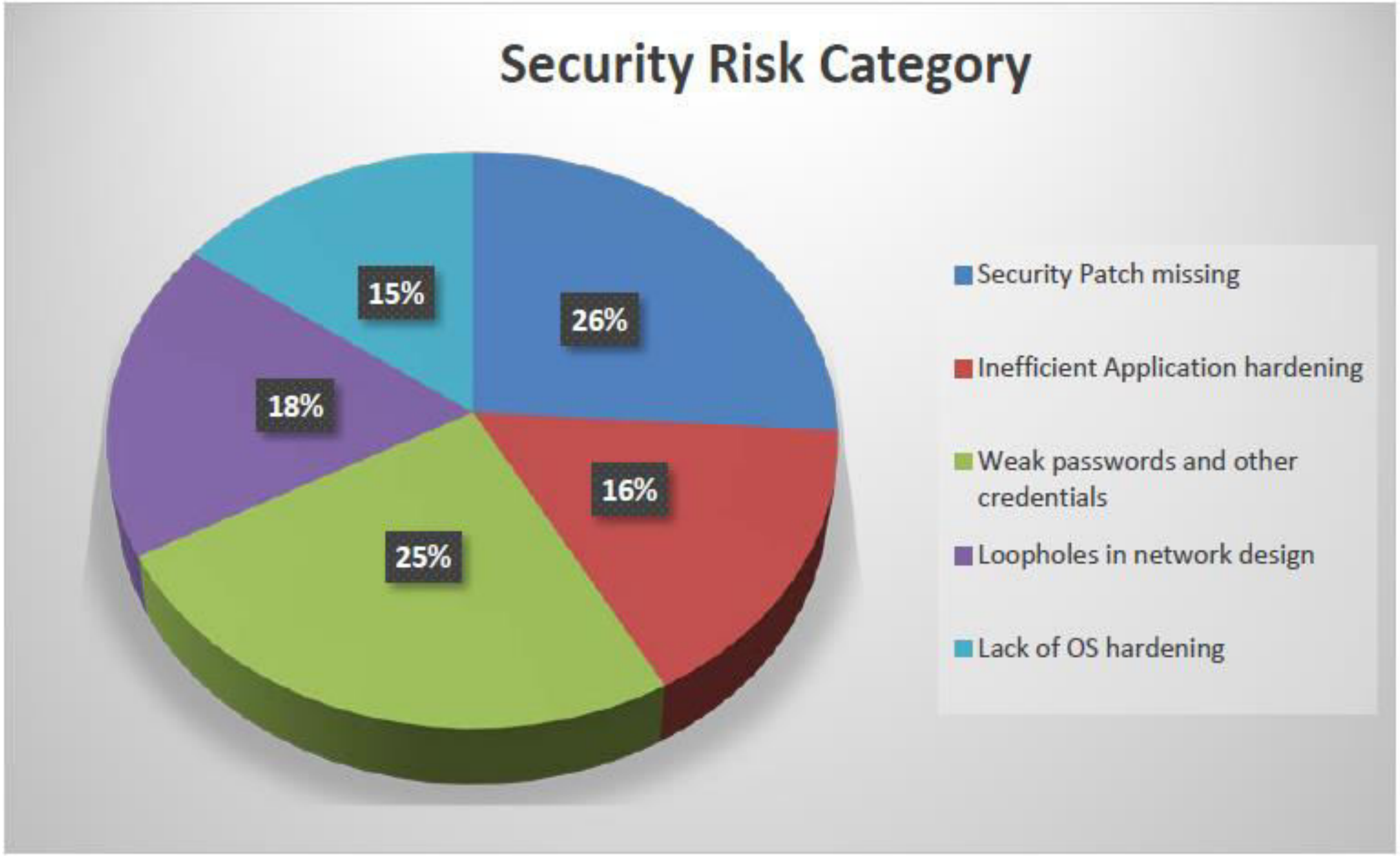
Risk Profile

This section rates the risks with numbers identified in a test, within a range of 1 to 15. There are different methods or frameworks such as DREAD that are available, on which the tester can base his opinion.



Understanding Risk Rates

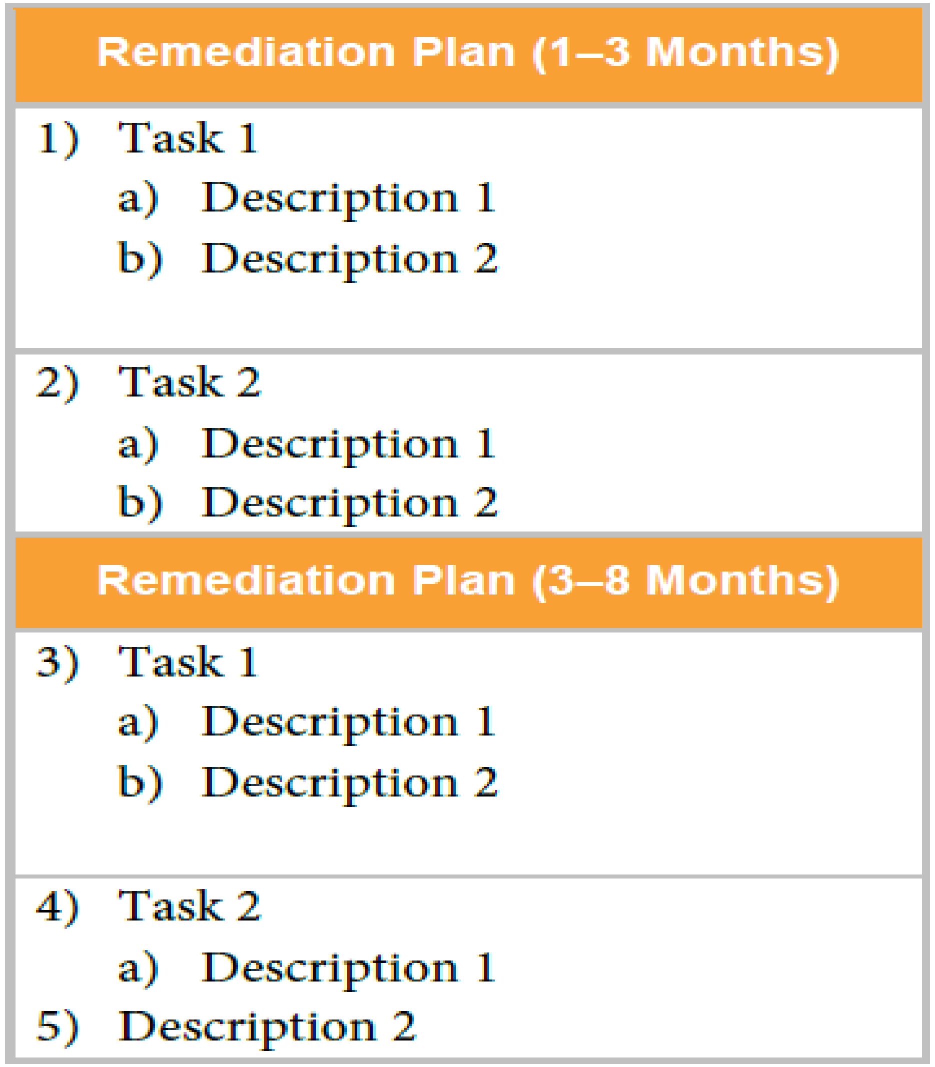
General Findings



Recommendation Summary

- This section of the report will provide the client with top-level understanding of the remediation process that needs to be implemented to address the issues indicated in the penetration test report.

Table Describing the Remediation Plan for First 3 months and 3–8 months



Remediation Plan (1–3 Months)
1) Task 1 a) Description 1 b) Description 2
2) Task 2 a) Description 1 b) Description 2
Remediation Plan (3–8 Months)
3) Task 1 a) Description 1 b) Description 2
4) Task 2 a) Description 1 5) Description 2

Technical Report

- All the technical aspects of the test including the testing methods, testing environment and security parameters are described in a technical record. The various sections of a technical report are explained below.

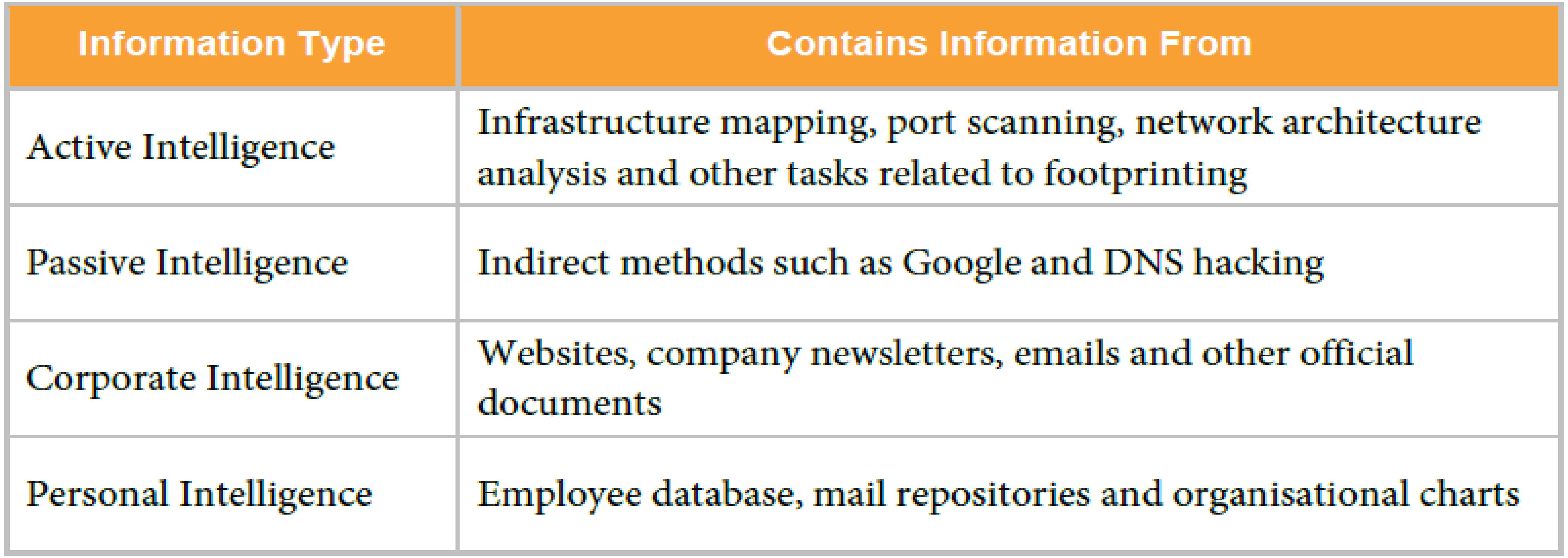
Introduction

- It is a general practice to have an ‘introduction’ paragraph for every document. It consists of the following:
  - Identity of the penetration tester and a representative of the client in charge of testing, including their contact information.
  - Objective and scope of the test.
  - Approach and strength of methods applied.
  - Threat rating.

Information Gathering:

Information is gathered from different sources. This helps the tester to prepare his assessment.

The sources can be classified as shown in table



Information Type	Contains Information From
Active Intelligence	Infrastructure mapping, port scanning, network architecture analysis and other tasks related to footprinting
Passive Intelligence	Indirect methods such as Google and DNS hacking
Corporate Intelligence	Websites, company newsletters, emails and other official documents
Personal Intelligence	Employee database, mail repositories and organisational charts

Vulnerability Assessment:

This is a process that defines, identifies and classifies the vulnerabilities in a computer, network, or communications infrastructure.

Confirming the Vulnerability

Once the vulnerabilities have been identified, the penetration tester would have exploited them just like the hacker, in order to find out what damage it causes to the system and how to avoid these damages. These details are documented in this section of the report.

Attack Phase

Once the penetration tester has exploited the vulnerabilities, he will attack the target system, again, with the mind-set and intentions of a hacker, to evaluate and record the events that occur in the 'attack phase'.

Risk/Exposure

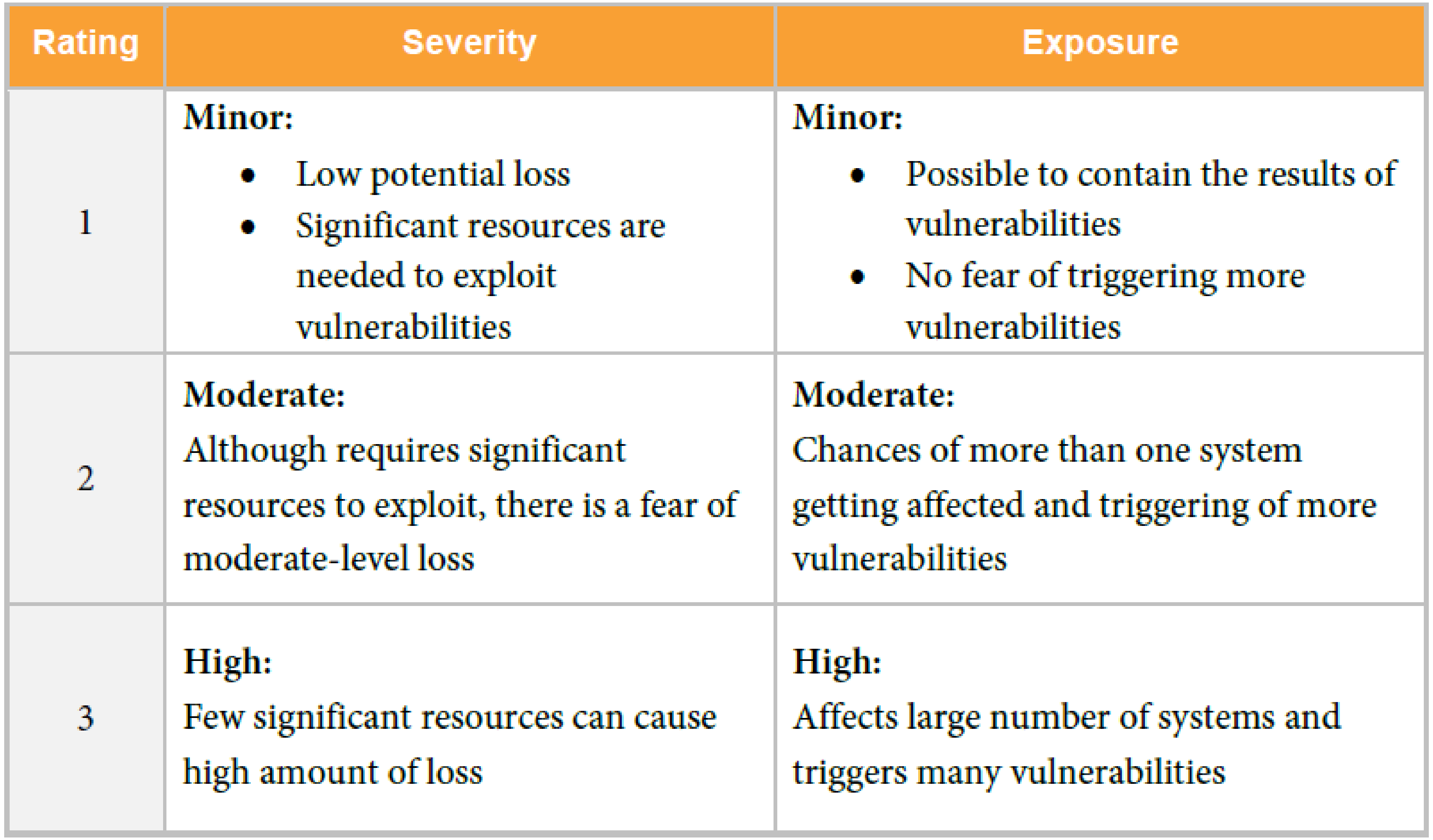
The final stage in the technical report is to write details about the probable frequency of the attack, estimations about the loss to the client at each instance of the attack (in case there are multiple attacks) and the impact of business owing to the exposure.

This provides the client with a broader view of the whole scenario and directs them towards having stringent security policies to avoid such occurrences in the future.

Vulnerability Assessment Report

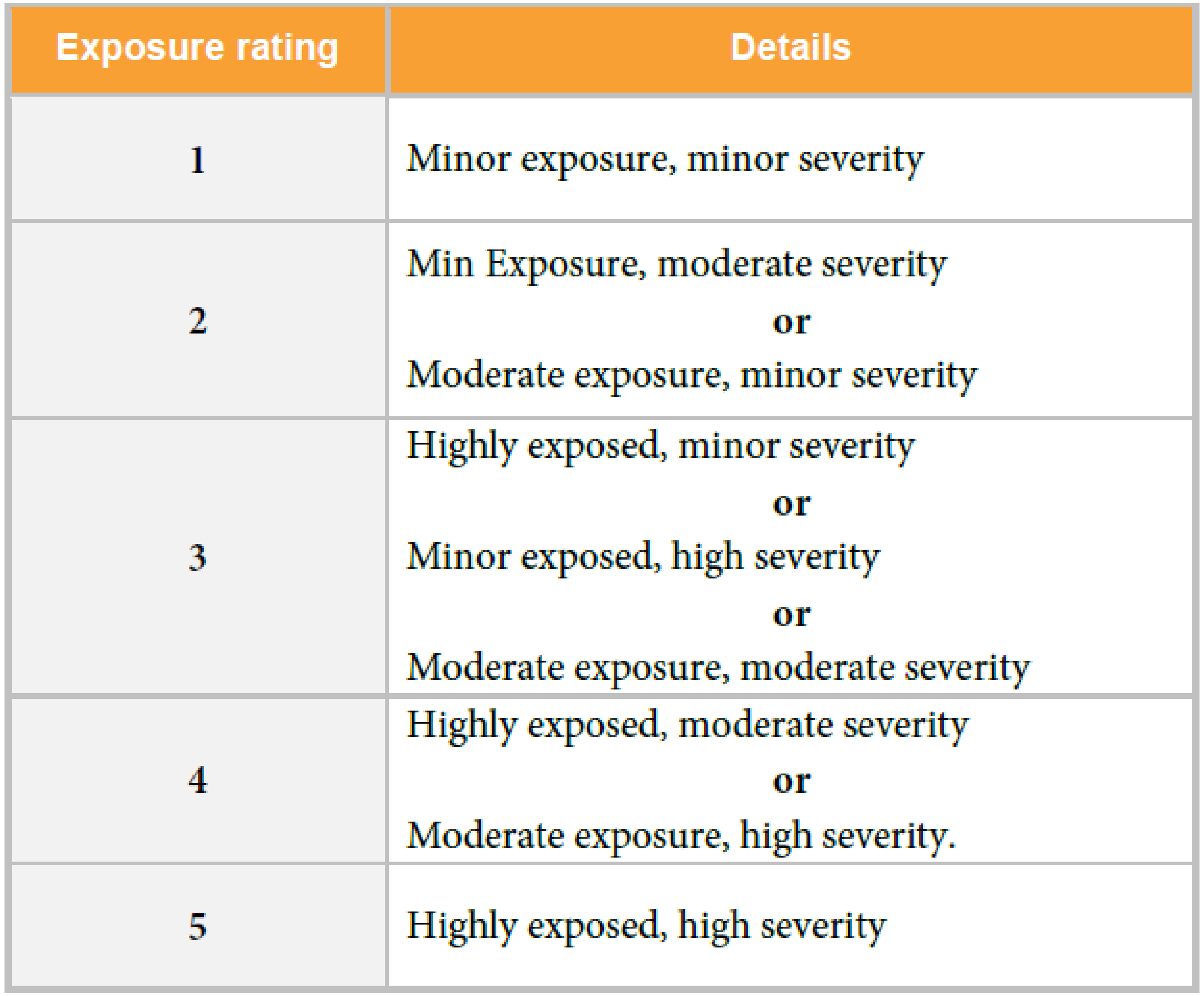
- The term ‘vulnerability assessment’ is given to the process of identifying potential vulnerabilities present in the target system and classifying threats into low, medium, high or critical, depending on the severity of the damage incurred to an organisation.
- Some of the tools used in this stage of testing are, Nessus, SAINT and Whisker to name a few.
- These vulnerabilities result in risks, which must be analysed, to evaluate their seriousness.

Vulnerability Ratings based on Severity and Exposure



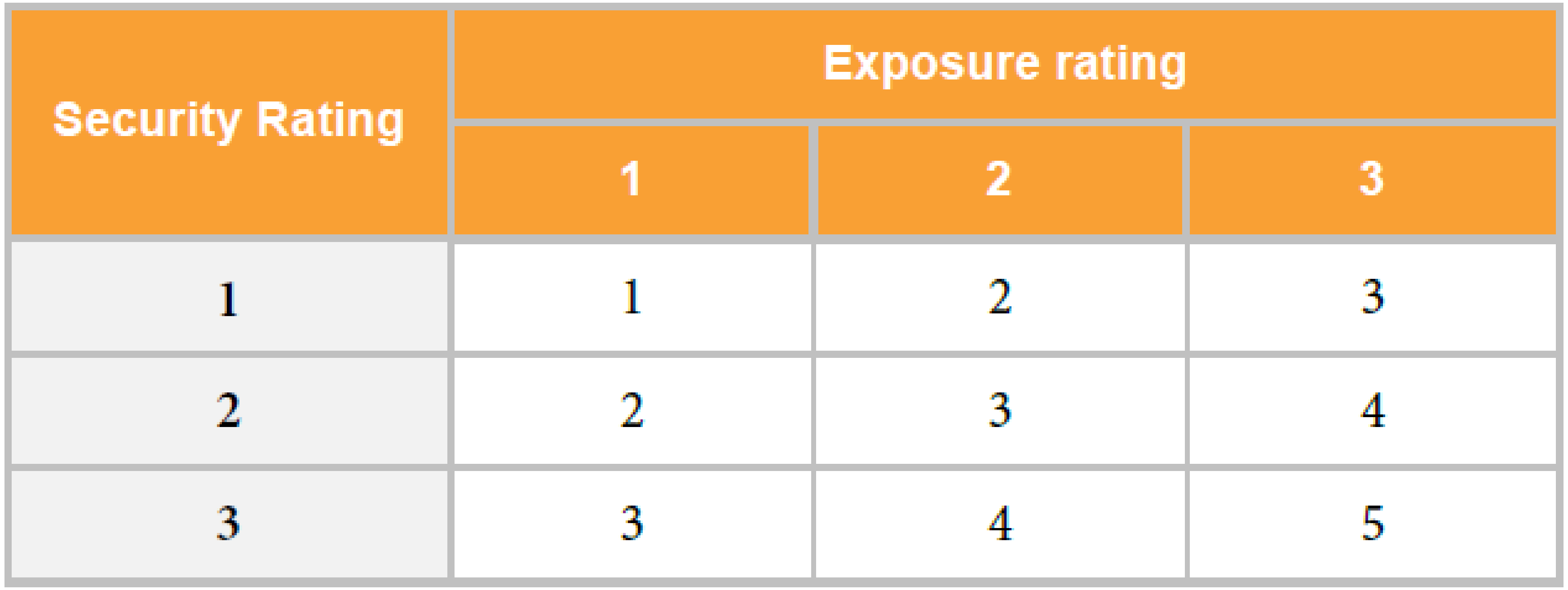
Rating	Severity	Exposure
1	**Minor:** • Low potential loss • Significant resources are needed to exploit vulnerabilities	**Minor:** • Possible to contain the results of vulnerabilities • No fear of triggering more vulnerabilities
2	**Moderate:** Although requires significant resources to exploit, there is a fear of moderate-level loss	**Moderate:** Chances of more than one system getting affected and triggering of more vulnerabilities
3	**High:** Few significant resources can cause high amount of loss	**High:** Affects large number of systems and triggers many vulnerabilities

Exposure Ratings



Exposure rating	Details
1	Minor exposure, minor severity
2	Min Exposure, moderate severity **or** Moderate exposure, minor severity
3	Highly exposed, minor severity **or** Minor exposed, high severity **or** Moderate exposure, moderate severity
4	Highly exposed, moderate severity **or** Moderate exposure, high severity.
5	Highly exposed, high severity

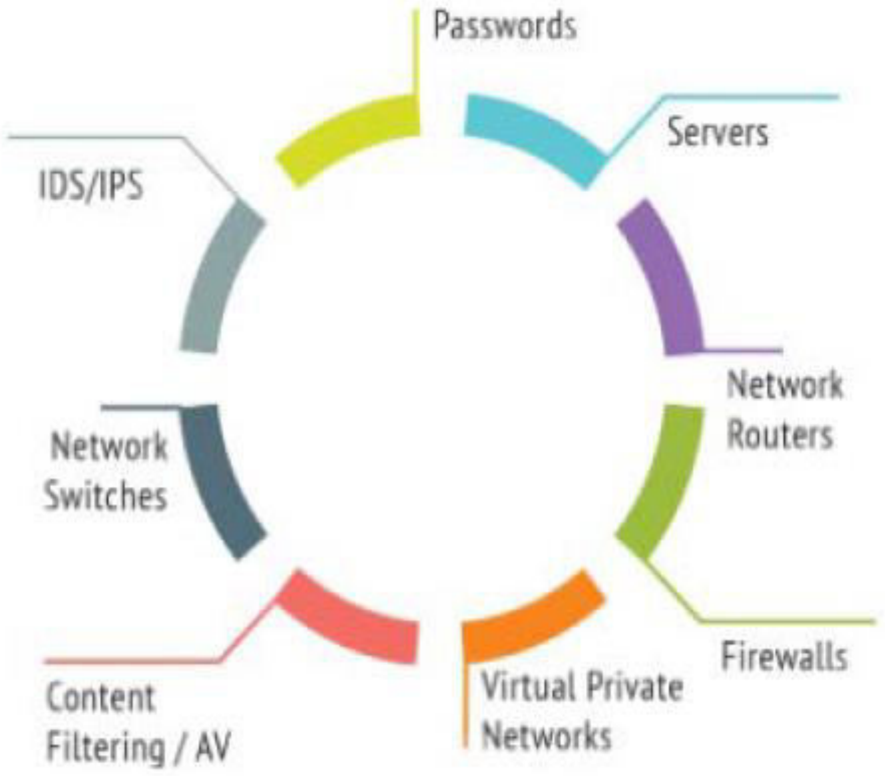
Determining Security Rating



Security Rating	Exposure rating		
	1	2	3
1	1	2	3
2	2	3	4
3	3	4	5

Network Penetration Testing Report

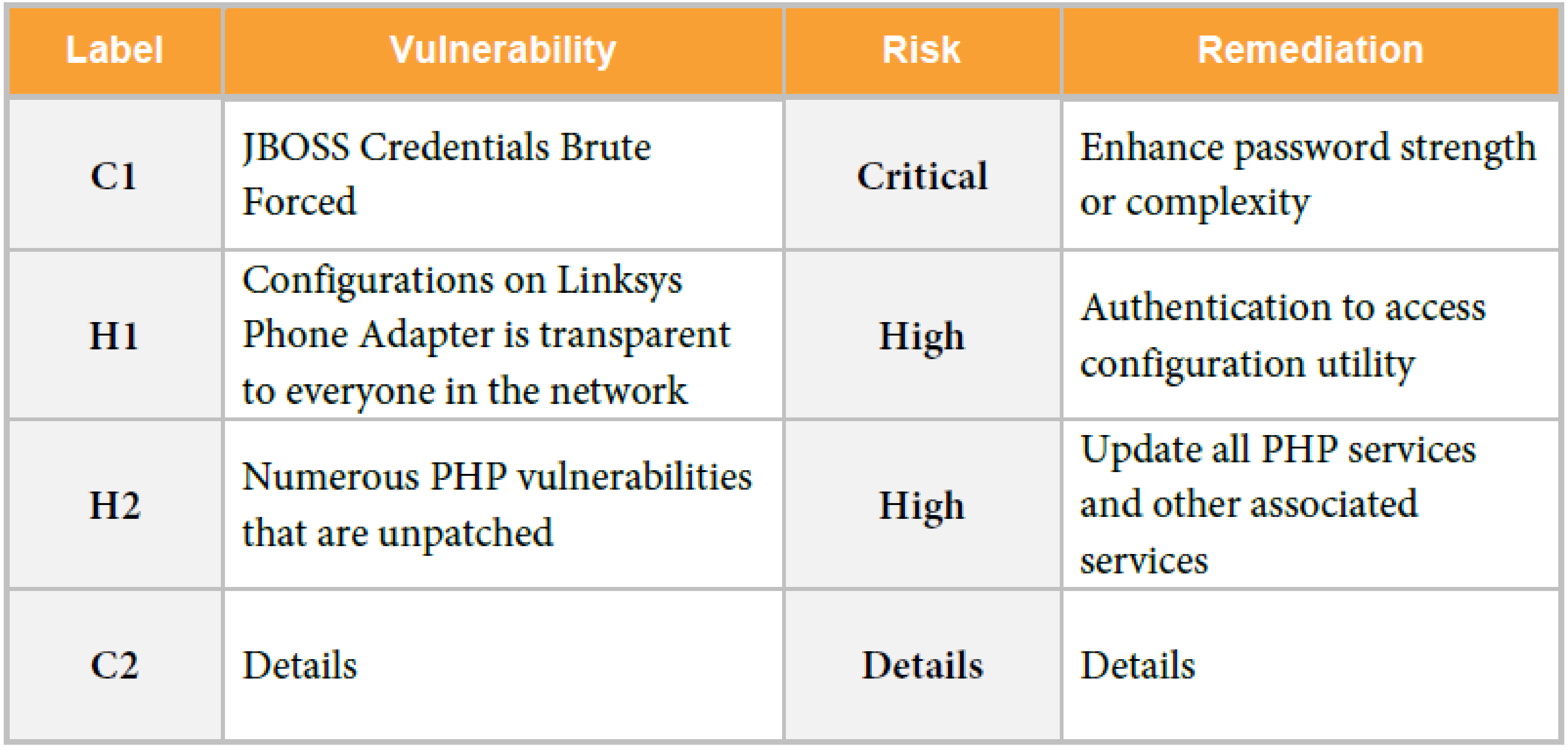
- Network penetration testing is conducted to identify the exploitable vulnerabilities in network systems, hosts and network devices such as routers and switches.
- In most cases, this term is used alternatively for a penetration test.
- The basic framework for conducting a network penetration test is called the Penetration Testing Execution Standard (PTES).



Executive Summary

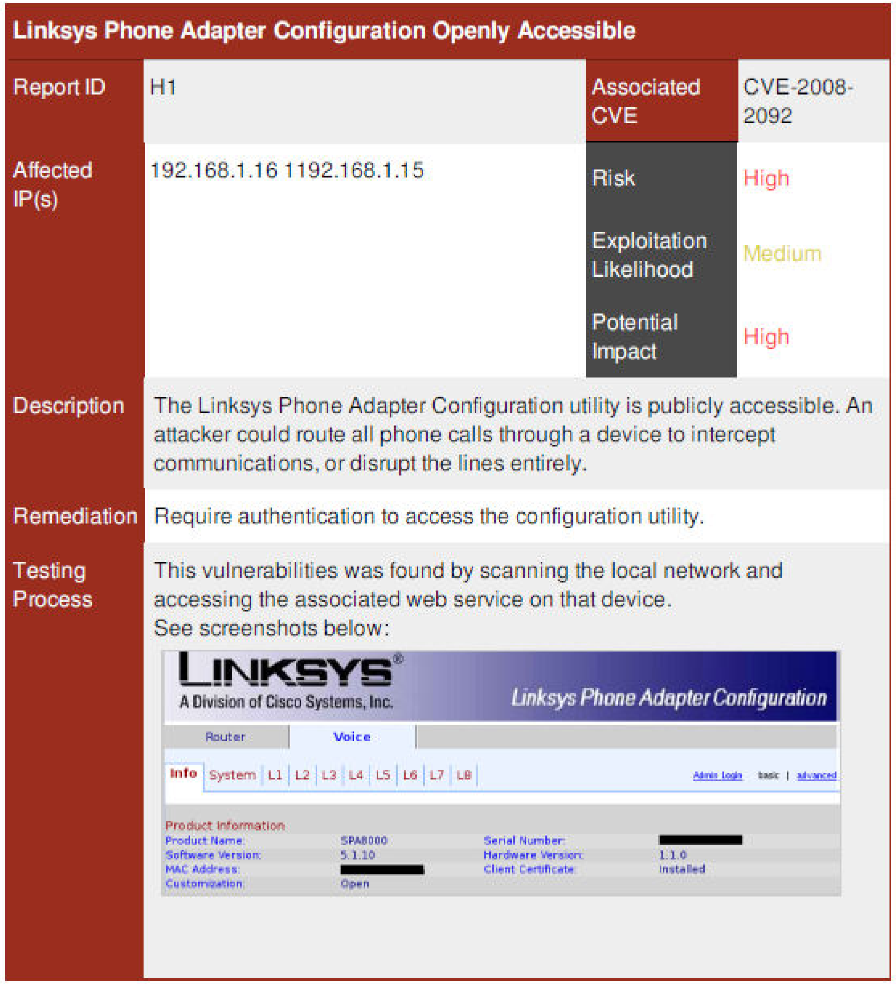
1. Strides Security conducted a network penetration test for First Clap Media Inc., with the objective of assessing the information security posture of the company and to recommend effective methods to strengthen its security.
2. This test was conducted on 08/12/2016. The initial mapping and reconnaissance of the client was done using a few commercial and proprietary tools which will be detailed in the report.
3. Based on the results obtained from the test, the system is declared to be under a CRITICAL risk, as there are numerous vulnerabilities contributing to asset loss and there is a higher likelihood of threat and high severity owing to the vulnerabilities in the system.

Vulnerability Overview



Label	Vulnerability	Risk	Remediation
C1	JBOSS Credentials Brute Forced	Critical	Enhance password strength or complexity
H1	Configurations on Linksys Phone Adapter is transparent to everyone in the network	High	Authentication to access configuration utility
H2	Numerous PHP vulnerabilities that are unpatched	High	Update all PHP services and other associated services
C2	Details	Details	Details

Diagnosis and Report of Linksys Phone Adapter Configuration



Linksys Phone Adapter Configuration Openly Accessible

Report ID	H1	Associated CVE	CVE-2008-2092
Affected IP(s)	192.168.1.16 1192.168.1.15	Risk	High
		Exploitation Likelihood	Medium
		Potential Impact	High
Description	The Linksys Phone Adapter Configuration utility is publicly accessible. An attacker could route all phone calls through a device to intercept communications, or disrupt the lines entirely.		
Remediation	Require authentication to access the configuration utility.		
Testing Process	This vulnerabilities was found by scanning the local network and accessing the associated web service on that device. See screenshots below:		

Product Information

Product Name:	SPA8000	Serial Number:	[redacted]
Software Version:	5.1.10	Hardware Version:	1.1.0
MAC Address:	[redacted]	Client Certificate:	Installed
Customization:	Open		

The characteristics one has to look for in a tool are;

Visibility

- The results of the test performed by the tool must be clearly visible to the tester and anyone who is a part of the test.

Extensibility

- Customisation is an important feature that you have to look in a tool because each system, testing environment and conditions is different

Configurability

- Some of the tools can be used for multiple test types, by making configuration changes to them.

Documentation

- Any tool that comes with documentation explaining the features and precise methods to use the tool, are preferred by penetration testers

Licensing Options

- Tools made for commercial purposes, sometimes come with strict license options that don't allow them to be used beyond a condition.

False Positive and False negatives

- Penetration testing is a very effective method of identifying the vulnerabilities present in systems. In most cases, this term is used alternatively for a penetration test.
- False positives and negatives are two of these loopholes.
- Very commonly encountered in Intrusion Detection Systems or IDS, you will also hear about them in web application vulnerability assessments.
- False positive is a term given to a situation where a penetration test picks up a vulnerability in a system that does not exist.
- On the contrary, a false negative refers to a real vulnerability that prevails in your system, but did not get identified in the penetration test.

False Negatives

False negatives are generated when an attack that must have raised an alarm fails to do so. Some of the reasons for this could be:

- In signature-based IDS systems, there may be a time delay to add the signature for a new type of attack.
- At certain times, one vulnerability can lead to two attacks and in a signature-based system; the scope of a rule will be limited to identify only a particular set of an attack vectors. In simple words, a signature rule that identifies ‘X’ as an attack, may fail to do so with ‘Y’, although both attacks stem from a single vulnerability, because of the rules defined in signature files

Quiz / Assessment

3) In DREAD, which is a method where each vulnerability is graded in certain categories, to arrive at a risk rating for the system, what does R stand for?			
a) Reliability	b) Resources	c) Reproducibility	d) Risk
4) The method used to gather information about a company's position and strategy in the business by studying data from a company's newsletters, journals and websites is called:			
a) Active intelligence	b) Passive intelligence	c) Personal intelligence	d) Corporate intelligence

e-References & External Resources

This articles gives a good insight into false positives and false negatives that make their way in Penetration test , https://isc.sans.edu/forums/diary/CSAM+Month+of+False+Positives+Ghosts+in+the+Pentest+Report/18861/

- *The article in* http://www.iwar.org.uk/comsec/resources/risks/itsg-04e.pdf *is a valuable guide in carrying out threat and Risk Assessment for an existing or new IT system*
- *The article* http://www.pentest-standard.org/index.php/Reporting#Technical_Report *gives a basic idea about Penetration test reporting*
- *Penetration testing Guidelines,* https://www.pcisecuritystandards.org/documents/Penetration_Testing_Guidance_March_2015.pdf

Image Credits

- Figure 4.1.6: https://www.redteamsecure.com/network-penetration-testing

External Resources

1. Kimberly Graves. *Official Certified Ethical Hacker Review Guide*
2. Patrick Engebretson. *The Basics of Hacking and Penetration Testing,* (Second edition)
3. Gregg, *Certified Ethical Hacker* (with CD), Pearson Education India

Activity

Online Activity
(30min)

Description :

Visit: www.vulnerabilityassessment.co.uk. Prepare a report on penetration test.

Thank You