

[Organization Logo, Name, and details]

Vulnerability Assessment Report

[Date]

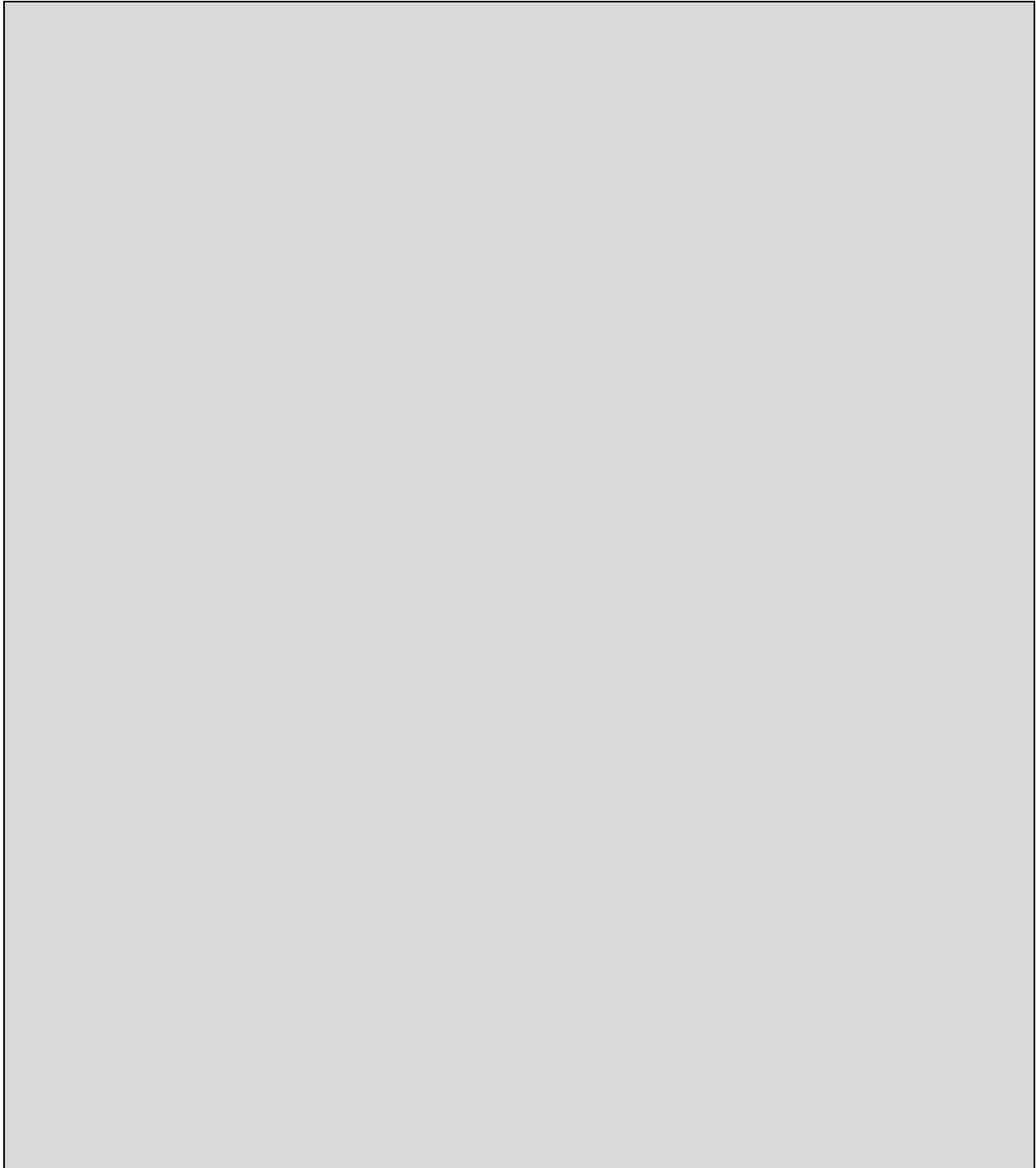
Document Details

Document Title	[Document Title]
Company	[Organization Name]
Recipient	[Document Author – Named Person]
Date	[Saved Filename]
Classification	[Confidential/Public/Private]
Document Type	[Report]
Version	[Document Version]
Author(s)	
Assessment Performed By	
Reviewed By	
Approved By	

Version History

Version Date	Version No.	Author	Comments

Executive Summary



1. Target Systems

The following table lists all devices that were targeted during this vulnerability assessment:

Target System Name	
Target System URL	
Test Type	
IP Addresses Discovered	
Network Details	
Web Server	
Network Ports	
System Configuration (Include Hardware and Software Configuration)	

2. Timeline

The timeline of the test is as below:

Category	Initiation Date/Time	Completion Date/Time

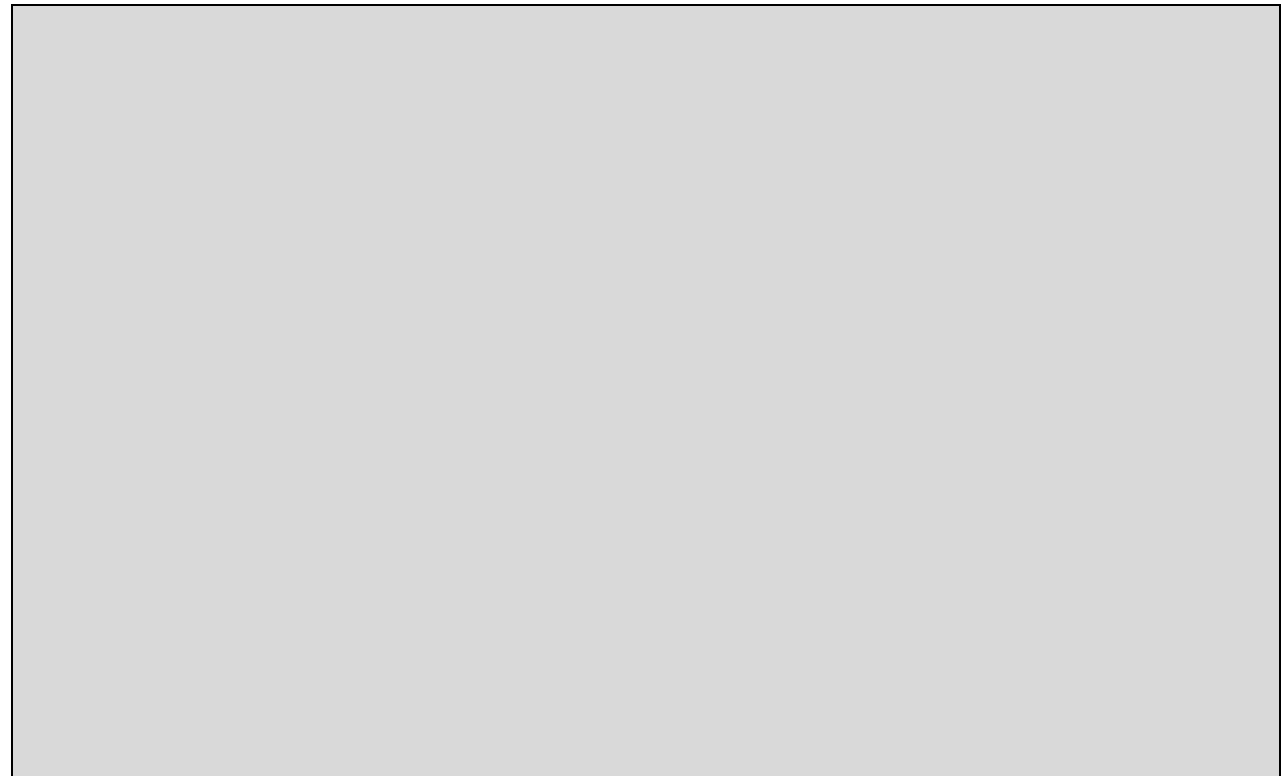
*Note: *Category column includes footprinting and reconnaissance, network scanning, host scanning, enumeration, etc.*

3. Summary of Evaluation

[Example:

- *Perform broad scans to identify potential areas of exposure and services that may act as entry points*
- *Perform targeted scans and manual investigation to validate vulnerabilities*
- *The test identified components to gain access to:*
 - *<10 IP addressed devices>*
- *Identify and validate vulnerabilities*
- *Rank vulnerabilities based on threat level, loss potential, and likelihood of exploitation*
- *Perform supplemental research and development activities to support analysis*
- *Identify issues of immediate consequence and recommend solutions*
- *Develop long-term recommendations to enhance security*
- *Transfer knowledge*

During the network-level security checks, we tried to probe the ports present on various servers and detect the services running on them with existing security holes, if any. At the web-application level, we checked the web servers' configuration issues, and (more importantly) the logical errors in the web application itself.]



4. Technical Rating Levels

[In the following sections, <Organization Name> uses a rating system using stars () to indicate the level of severity of our findings. All findings are vulnerabilities that have a business risk to the <Organization Name>.]*

5 Stars	*****	Critical	Intruders can easily gain control of hosts and network. This needs immediate attention.
4 Stars	****	High	Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. This should be addressed as soon as possible.
3 Stars	***	Elevated	This could result in potential misuse of the host by intruders. Address this at your convenience but do as soon as possible.
2 Stars	**	Moderate	Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions. Address this the next time you perform a minor reconfiguration of the host.
1 Stars	*	Low	Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities. Address this the next time you perform a major reconfiguration of the host.

5. Business Impact Rating

[Impact analysis involves estimating the adverse impact caused due to the exploitation of the vulnerability by the threat source.]

In the following sections, <Organization Name> uses the following business impact rating system

Magnitude of Impact	Impact Definition
High	Exploitation of the vulnerability may lead to: <ul style="list-style-type: none">▪ Highly costly loss of tangible assets▪ High damage to the mission or reputation of the organization▪ Even may lead to death of humans or severe injury

Medium	Exploitation of the vulnerability may lead to: <ul style="list-style-type: none">▪ Costly loss of tangible assets▪ May harm the organization's mission or reputation▪ May lead human injury
Low	Exploitation of the vulnerability may lead to: <ul style="list-style-type: none">▪ Loss of few tangible assets▪ May show slight effect on organization's mission or reputation

6. Risk Level

[The risk level is an assessment of the resulted impact on the networks.]

In the following sections, <Organization Name> uses the following risk rating system:

Risk Level	Description
Insignificant	Impacts non-critical systems, functions, and processes that can be replaced easily
Minor	Impacts non-critical systems, functions, and processes that are difficult to replace
Moderate	Affects systems, functions, and services containing small amounts of sensitive data
Major	Affect highly sensitive data and resources to impact business functionality
Severe	Affect mission critical data and resources, and result in severe business and financial losses

7. Technical Findings

The following table includes various identified network-level vulnerabilities along with their technical, business, and risk ratings:

Sr. No.	Network-Level Vulnerability	Vulnerability Details	Techniques/Tools Used	Technical Rating	Business Impact Rating	Potential Impact	Risk Rating	Recommendations

The following table includes various identified application-level vulnerabilities along with their technical, business, and risk ratings:

Sr. No.	Application-Level Vulnerability	Vulnerability Details	Techniques/Tools Used	Technical Rating	Business Impact Rating	Potential Impact	Risk Rating	Recommendations

The following table includes various identified operating system-level vulnerabilities along with their technical, business, and risk ratings:

Sr. No.	OS-Level Vulnerability	Vulnerability Details	Techniques/Tools Used	Technical Rating	Business Impact Rating	Potential Impact	Risk Rating	Recommendations

The following table includes various identified cloud vulnerabilities along with their technical, business, and risk ratings:

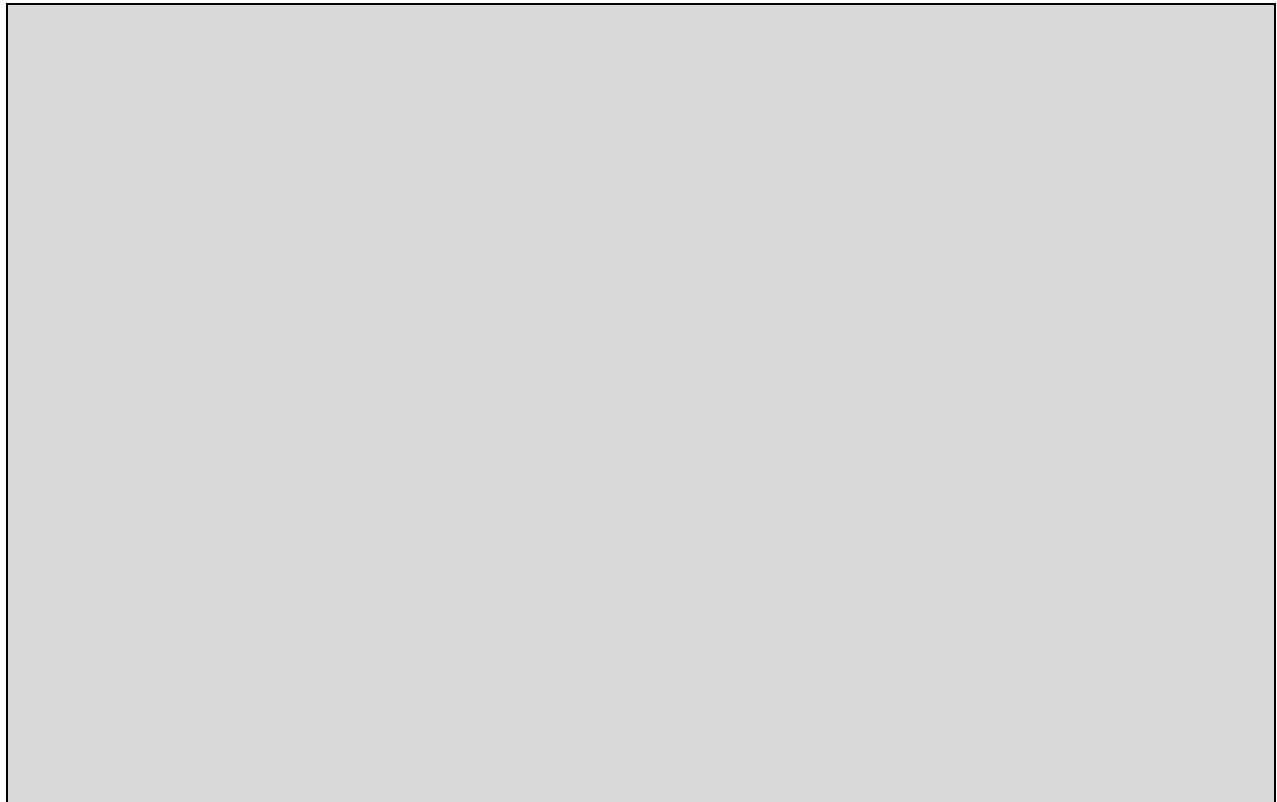
Sr. No.	Cloud Vulnerability	Vulnerability Details	Techniques/Tools Used	Technical Rating	Business Impact Rating	Potential Impact	Risk Rating	Recommendations

8. Summary of Findings

The Officer [or other named role] enables the [Name of the department – e.g., Incident Handling and Response Team] to identify when a series of events or weaknesses have escalated to become an incident. It is vital for the [Name of the department – e.g. Incident Handling and Response Team] to gain as much information as possible from the business users to identify if an incident is occurring or has occurred.]

Risk Level	Number of Risks
Insignificant	
Minor	
Moderate	
Major	
Severe	

[Insert a graph showing the summary of finding along with risk levels.]



9. Summary of Recommendations

[Give detailed recommendations based on the technical findings of the vulnerability assessment process.]

10. Conclusion

[Conclusion of the vulnerability assessment process.]