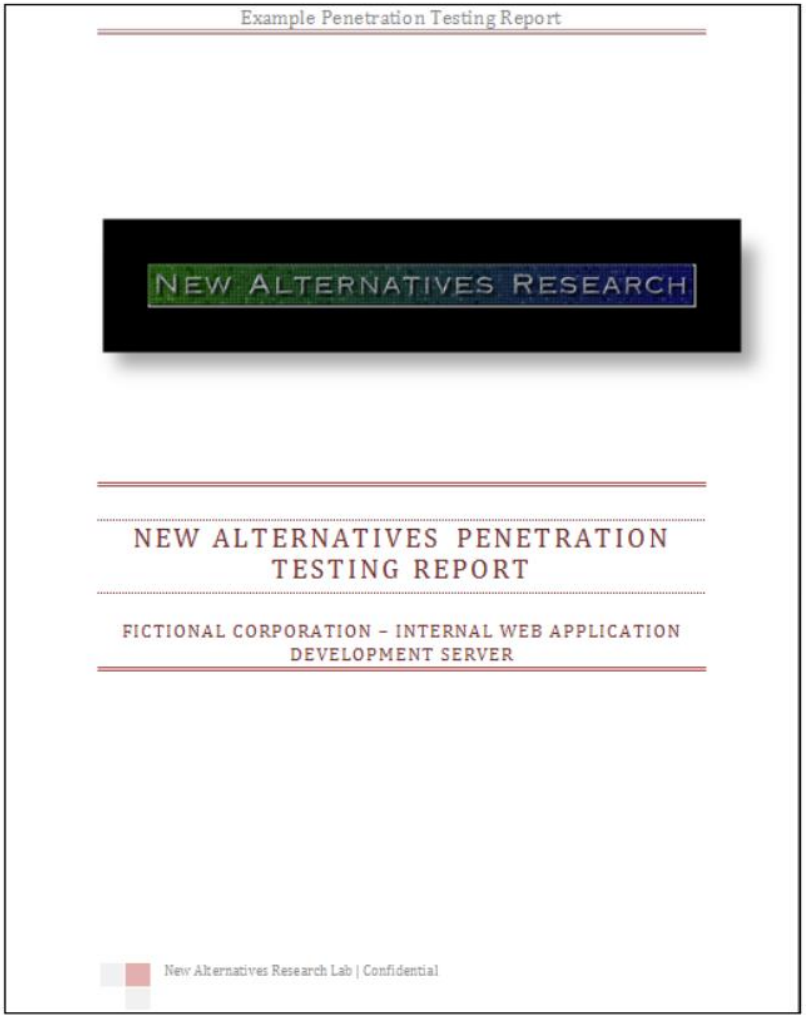
Trường ĐH CNTT TP. HCM

Bảo mật web và ứng dụng

Định dạng báo cáo

- **Cover page**
  - Provide a report name, version, date, author, service provider name, and intended party
  - Additional items:
    - The document security classification
    - Highlight results from other sections

Cover page



Example Penetration Testing Report

NEW ALTERNATIVES RESEARCH

NEW ALTERNATIVES PENETRATION TESTING REPORT

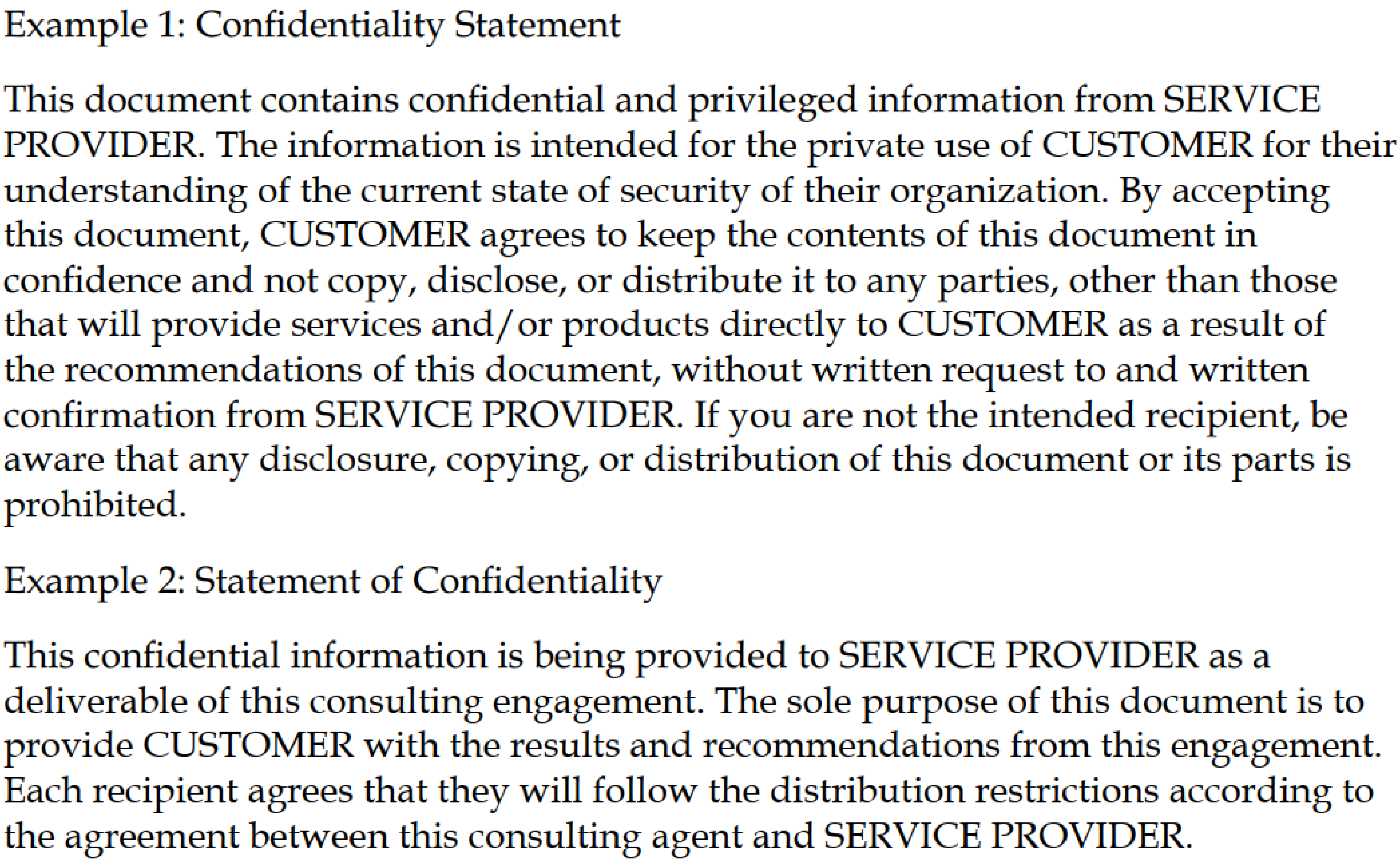
FICTIONAL CORPORATION – INTERNAL WEB APPLICATION DEVELOPMENT SERVER

New Alternatives Research Lab | Confidential

Report format

- **Confidentiality statement**
  - Protect information captured during the engagement
  - Should explain:
    - what level of security is involved with the document
    - who is authorized to view it
    - what is and what is not permitted to be copied, distribution rights
    - other legal language

Report format



Example 1: Confidentiality Statement

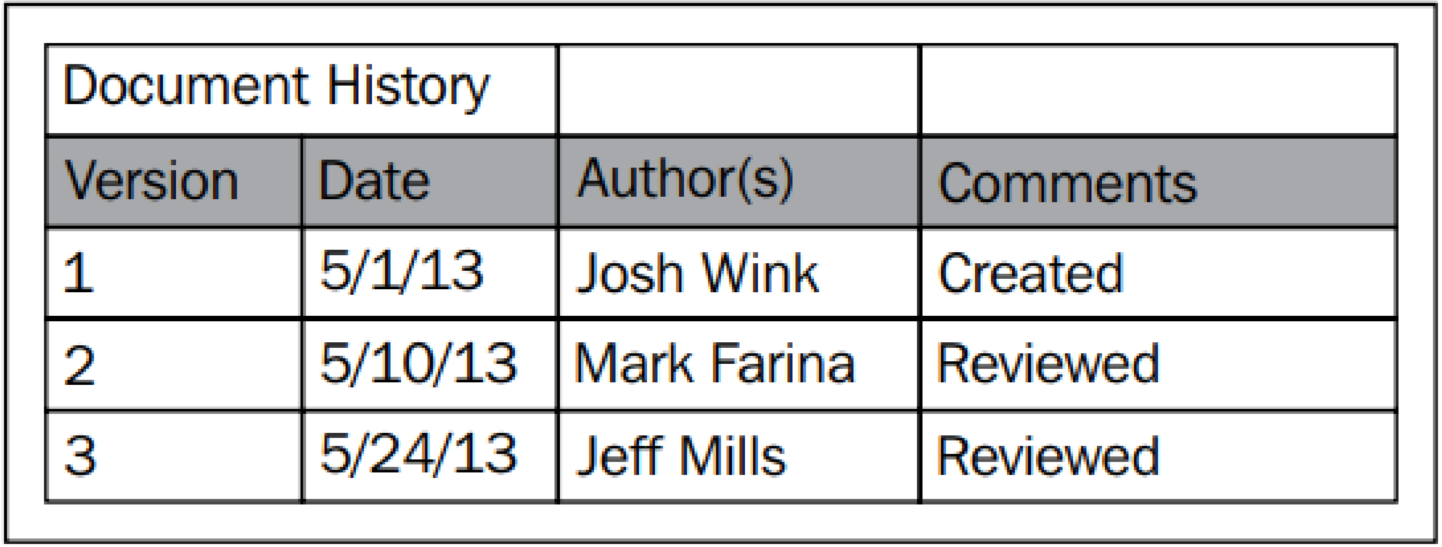
This document contains confidential and privileged information from SERVICE PROVIDER. The information is intended for the private use of CUSTOMER for their understanding of the current state of security of their organization. By accepting this document, CUSTOMER agrees to keep the contents of this document in confidence and not copy, disclose, or distribute it to any parties, other than those that will provide services and/or products directly to CUSTOMER as a result of the recommendations of this document, without written request to and written confirmation from SERVICE PROVIDER. If you are not the intended recipient, be aware that any disclosure, copying, or distribution of this document or its parts is prohibited.

Example 2: Statement of Confidentiality

This confidential information is being provided to SERVICE PROVIDER as a deliverable of this consulting engagement. The sole purpose of this document is to provide CUSTOMER with the results and recommendations from this engagement. Each recipient agrees that they will follow the distribution restrictions according to the agreement between this consulting agent and SERVICE PROVIDER.

Report format

- **Document control**
  - List what version and edits are made to a delivery proposal
  - Help readers leverage the latest version



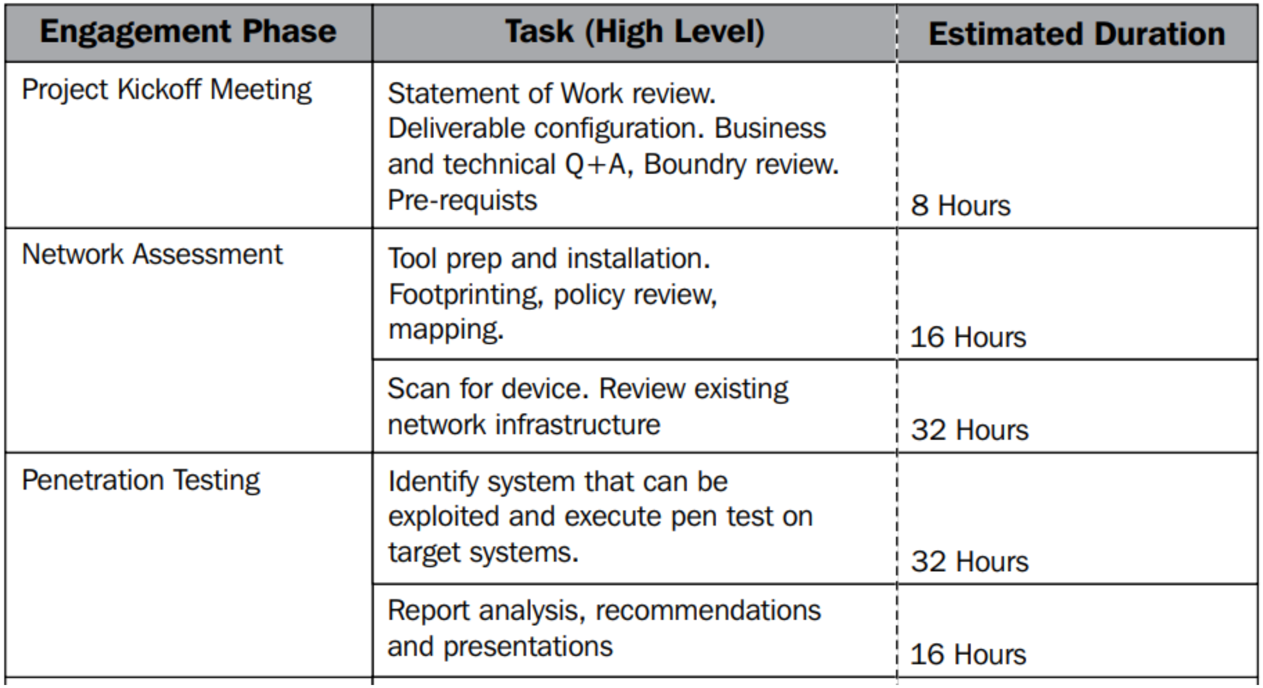
Document History			
Version	Date	Author(s)	Comments
1	5/1/13	Josh Wink	Created
2	5/10/13	Mark Farina	Reviewed
3	5/24/13	Jeff Mills	Reviewed

Report format

- **Timeline**

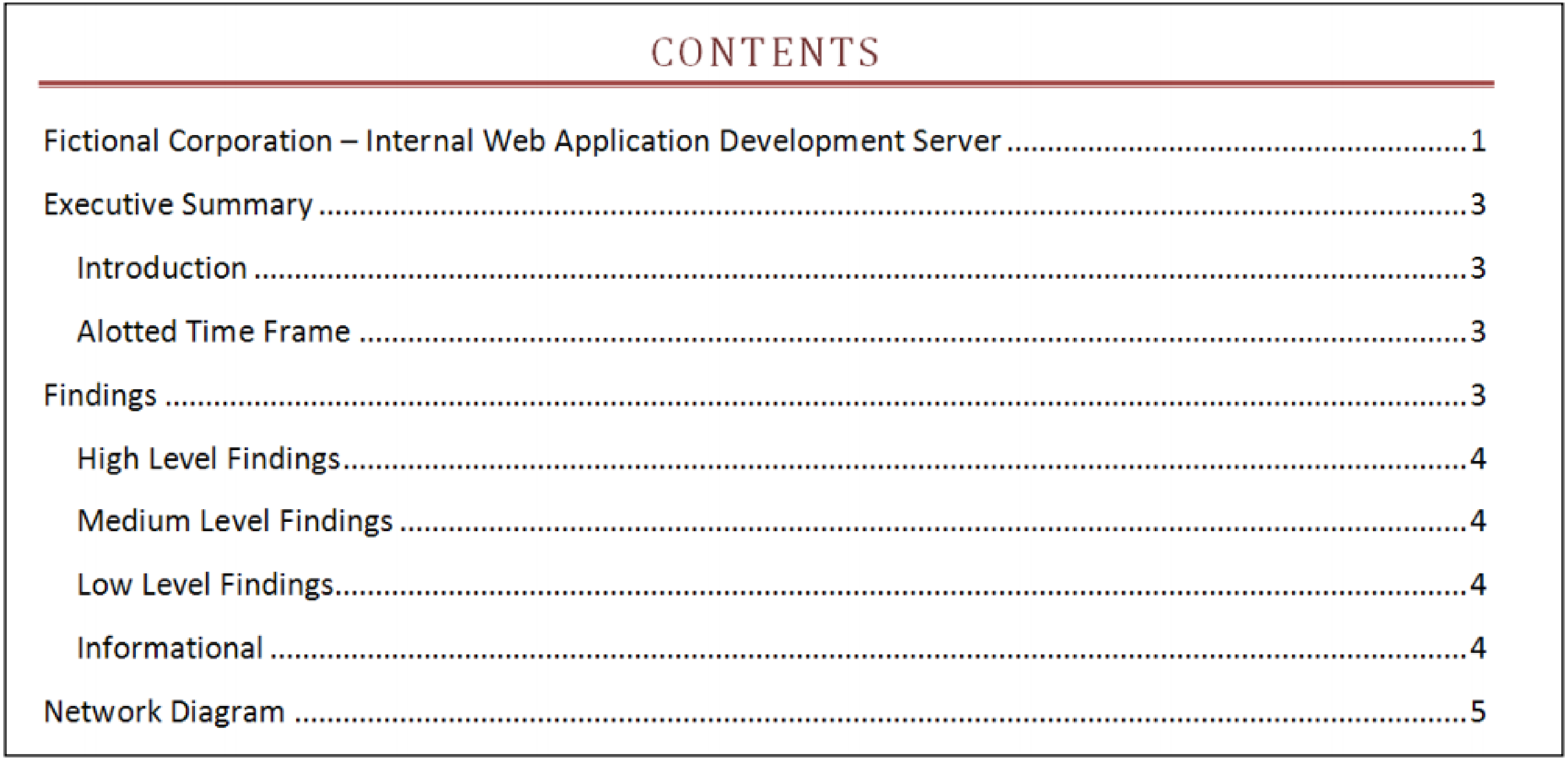
  Provide an estimate of hours for each phase of a project:

  - phase name
  - tasks to be completed
  - expected duration



Engagement Phase	Task (High Level)	Estimated Duration
Project Kickoff Meeting	Statement of Work review. Deliverable configuration. Business and technical Q+A, Boundry review. Pre-requists	8 Hours
Network Assessment	Tool prep and installation. Footprinting, policy review, mapping.	16 Hours
	Scan for device. Review existing network infrastructure	32 Hours
Penetration Testing	Identify system that can be exploited and execute pen test on target systems.	32 Hours
	Report analysis, recommendations and presentations	16 Hours

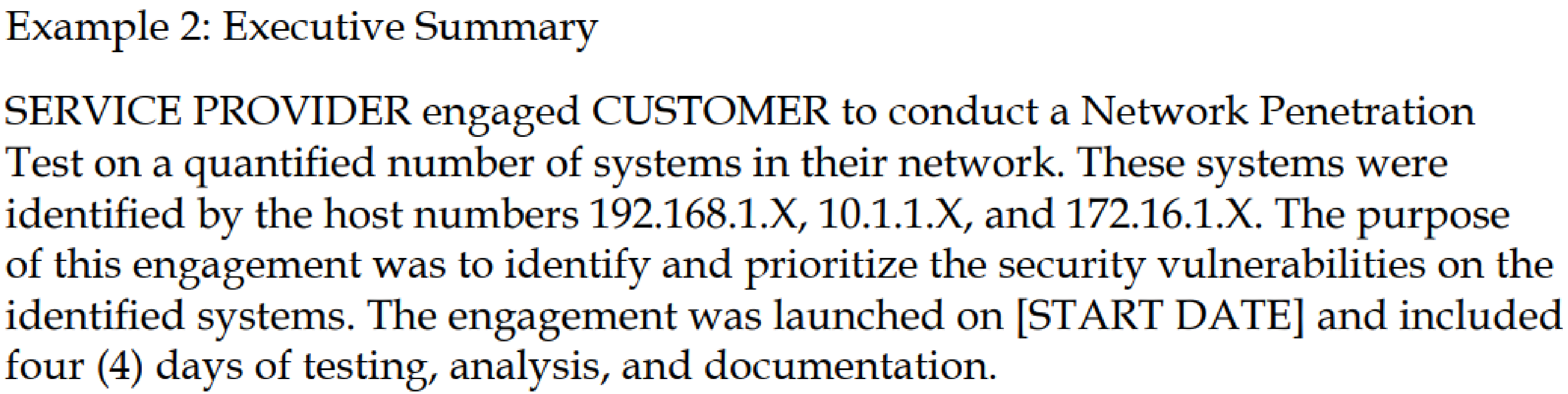
Index Table



CONTENTS

Report format

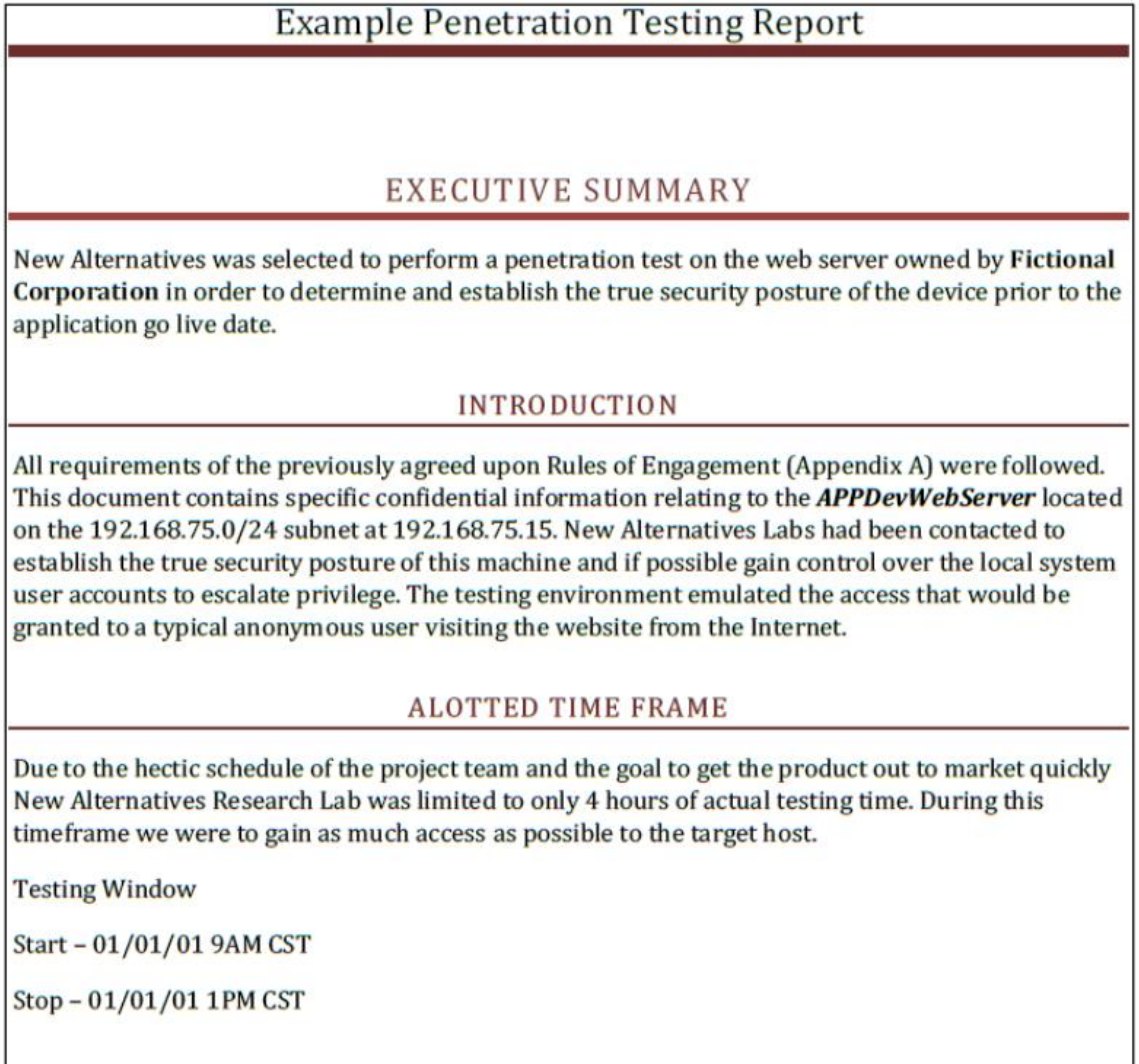
- **Executive summary**
  - Providing a high-level overview of why services were performed
  - Cover what led up to the issue being addressed, the problematic situation, and proposed solution with expected results



Example 2: Executive Summary

SERVICE PROVIDER engaged CUSTOMER to conduct a Network Penetration Test on a quantified number of systems in their network. These systems were identified by the host numbers 192.168.1.X, 10.1.1.X, and 172.16.1.X. The purpose of this engagement was to identify and prioritize the security vulnerabilities on the identified systems. The engagement was launched on [START DATE] and included four (4) days of testing, analysis, and documentation.

Executive Sumary



Example Penetration Testing Report

EXECUTIVE SUMMARY

New Alternatives was selected to perform a penetration test on the web server owned by **Fictional Corporation** in order to determine and establish the true security posture of the device prior to the application go live date.

INTRODUCTION

All requirements of the previously agreed upon Rules of Engagement (Appendix A) were followed. This document contains specific confidential information relating to the ***APPDevWebServer*** located on the 192.168.75.0/24 subnet at 192.168.75.15. New Alternatives Labs had been contacted to establish the true security posture of this machine and if possible gain control over the local system user accounts to escalate privilege. The testing environment emulated the access that would be granted to a typical anonymous user visiting the website from the Internet.

ALOTTED TIME FRAME

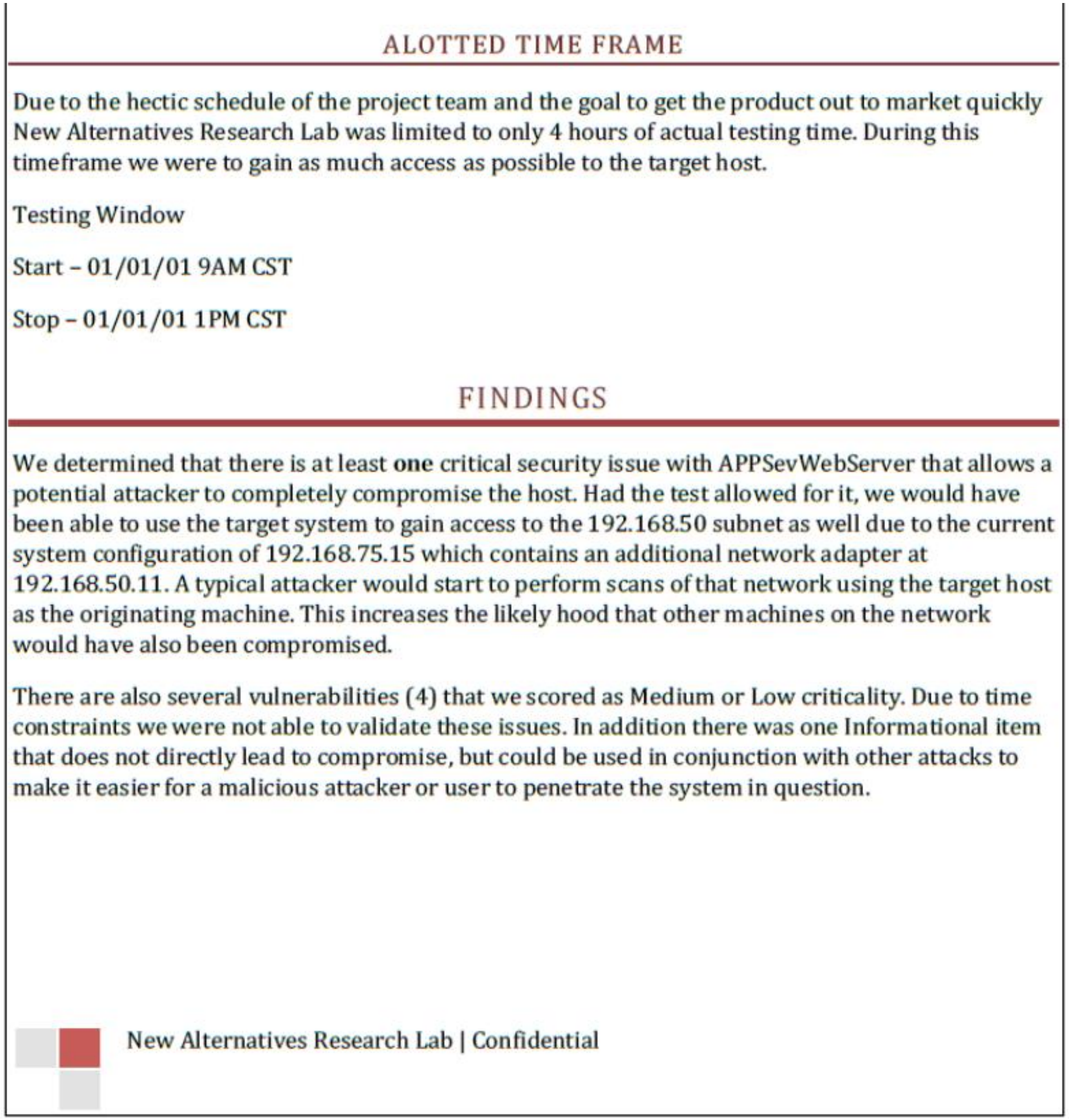
Due to the hectic schedule of the project team and the goal to get the product out to market quickly New Alternatives Research Lab was limited to only 4 hours of actual testing time. During this timeframe we were to gain as much access as possible to the target host.

Testing Window

Start – 01/01/01 9AM CST

Stop – 01/01/01 1PM CST

Findings



ALOTTED TIME FRAME

Due to the hectic schedule of the project team and the goal to get the product out to market quickly New Alternatives Research Lab was limited to only 4 hours of actual testing time. During this timeframe we were to gain as much access as possible to the target host.

Testing Window

Start – 01/01/01 9AM CST

Stop – 01/01/01 1PM CST

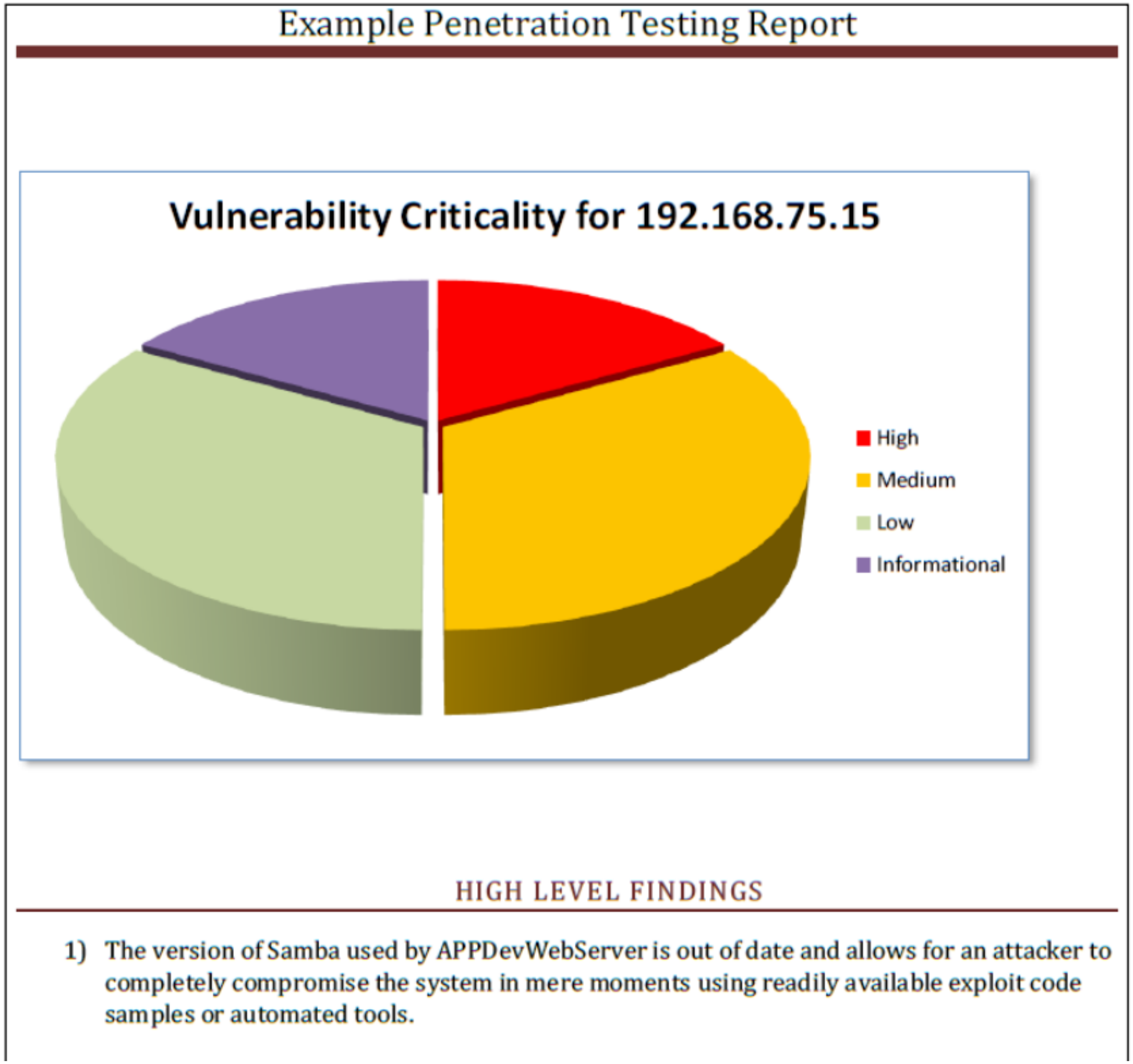
FINDINGS

We determined that there is at least **one** critical security issue with APPSevWebServer that allows a potential attacker to completely compromise the host. Had the test allowed for it, we would have been able to use the target system to gain access to the 192.168.50 subnet as well due to the current system configuration of 192.168.75.15 which contains an additional network adapter at 192.168.50.11. A typical attacker would start to perform scans of that network using the target host as the originating machine. This increases the likely hood that other machines on the network would have also been compromised.

There are also several vulnerabilities (4) that we scored as Medium or Low criticality. Due to time constraints we were not able to validate these issues. In addition there was one Informational item that does not directly lead to compromise, but could be used in conjunction with other attacks to make it easier for a malicious attacker or user to penetrate the system in question.

New Alternatives Research Lab | Confidential

Findings

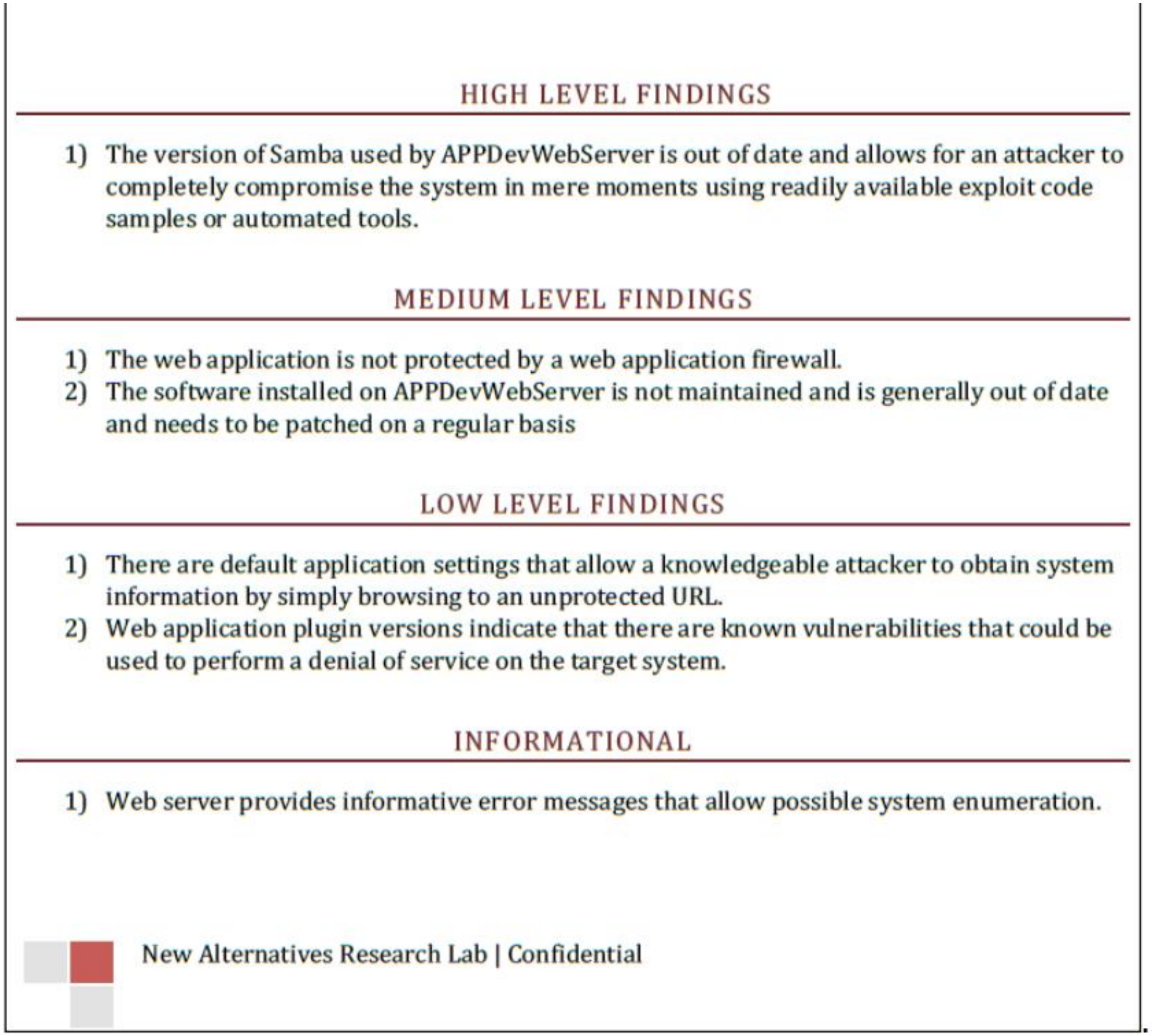


Example Penetration Testing Report

HIGH LEVEL FINDINGS

1) The version of Samba used by APPDevWebServer is out of date and allows for an attacker to completely compromise the system in mere moments using readily available exploit code samples or automated tools.

Findings



HIGH LEVEL FINDINGS

1) The version of Samba used by APPDevWebServer is out of date and allows for an attacker to completely compromise the system in mere moments using readily available exploit code samples or automated tools.

MEDIUM LEVEL FINDINGS

1) The web application is not protected by a web application firewall.
2) The software installed on APPDevWebServer is not maintained and is generally out of date and needs to be patched on a regular basis

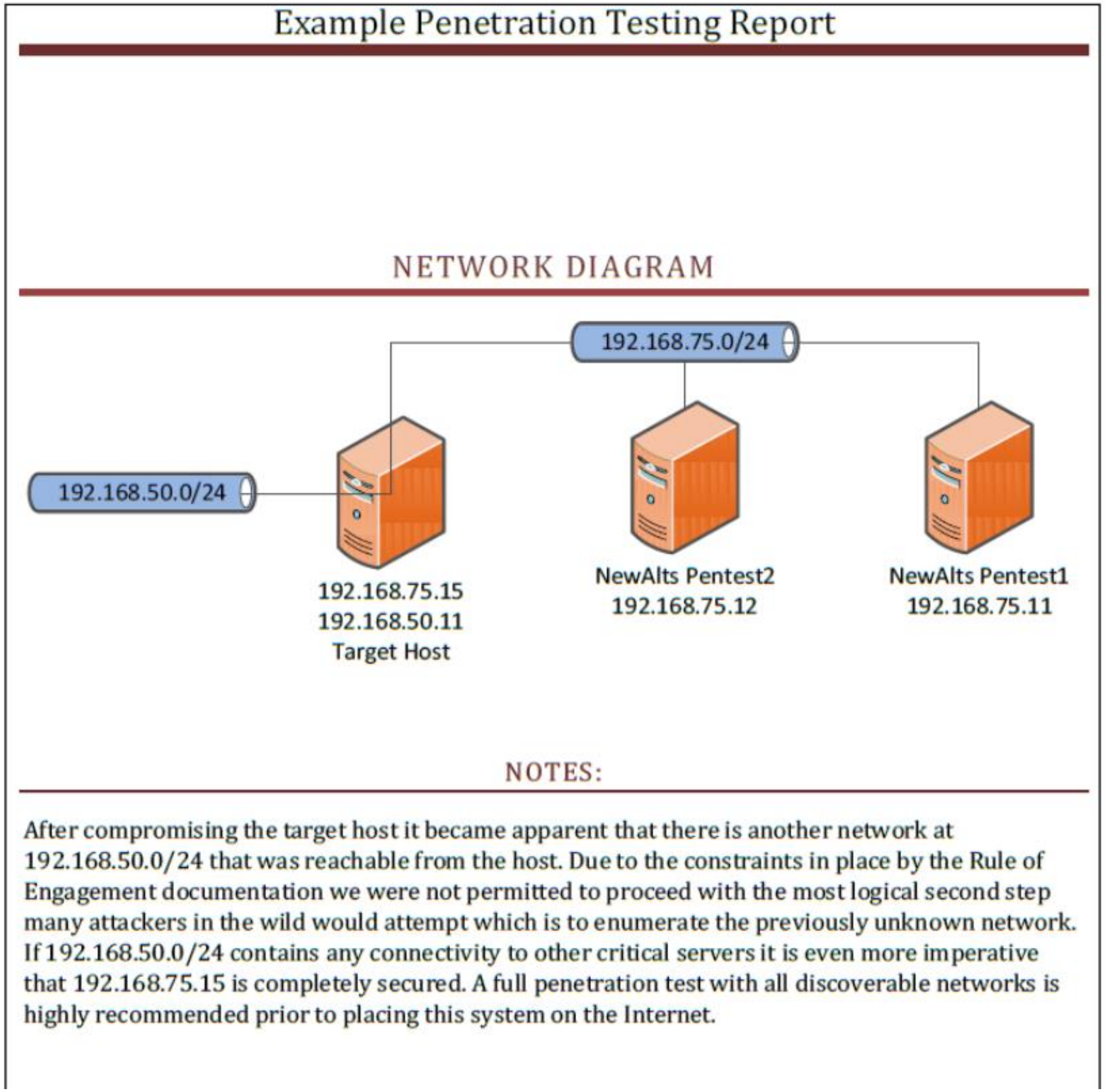
LOW LEVEL FINDINGS

1) There are default application settings that allow a knowledgeable attacker to obtain system information by simply browsing to an unprotected URL.
2) Web application plugin versions indicate that there are known vulnerabilities that could be used to perform a denial of service on the target system.

INFORMATIONAL

1) Web server provides informative error messages that allow possible system enumeration.

Network Diagram



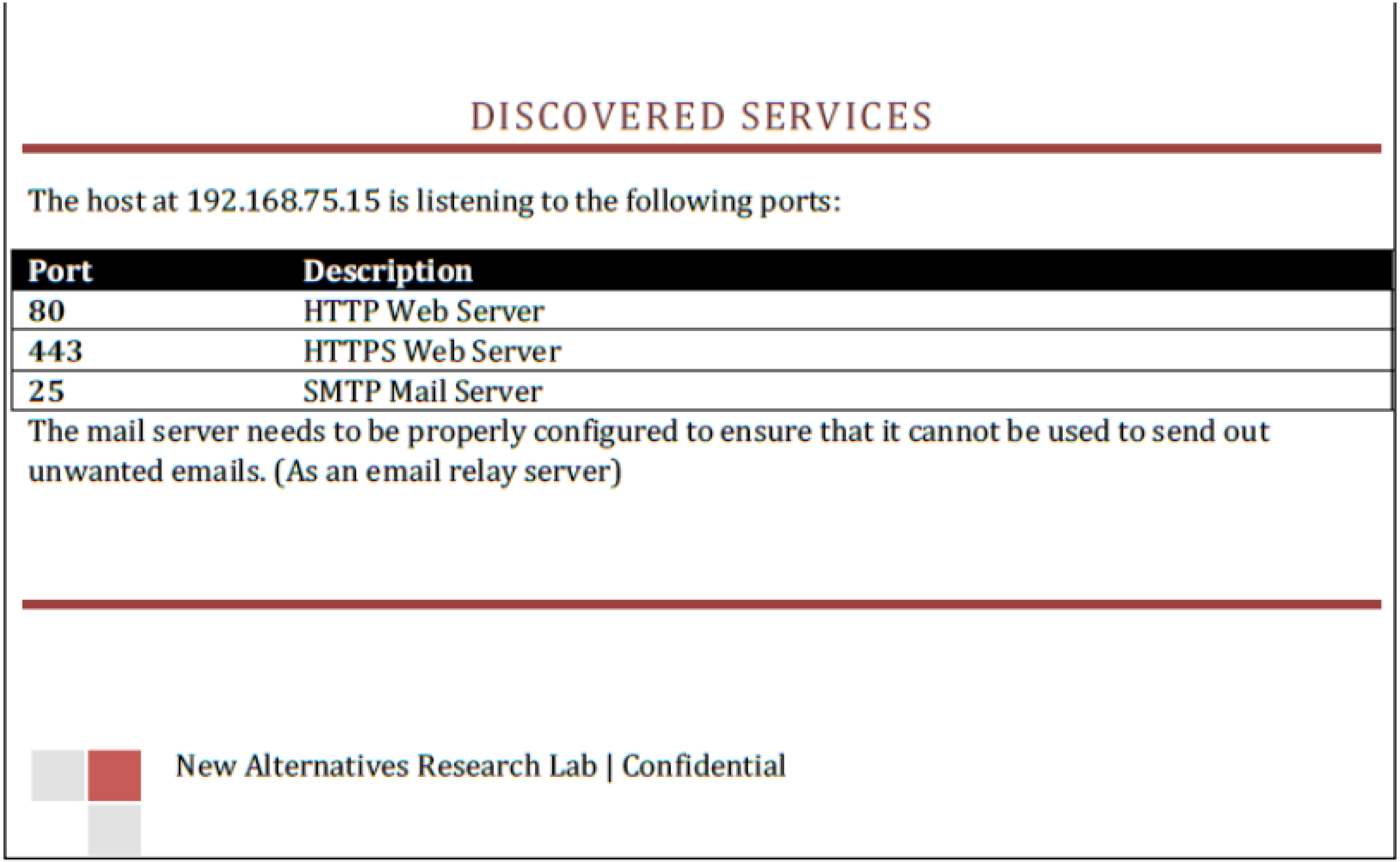
Example Penetration Testing Report

NETWORK DIAGRAM

NOTES:

After compromising the target host it became apparent that there is another network at 192.168.50.0/24 that was reachable from the host. Due to the constraints in place by the Rule of Engagement documentation we were not permitted to proceed with the most logical second step many attackers in the wild would attempt which is to enumerate the previously unknown network. If 192.168.50.0/24 contains any connectivity to other critical servers it is even more imperative that 192.168.75.15 is completely secured. A full penetration test with all discoverable networks is highly recommended prior to placing this system on the Internet.

Network Diagram



DISCOVERED SERVICES

The host at 192.168.75.15 is listening to the following ports:

Port	Description
80	HTTP Web Server
443	HTTPS Web Server
25	SMTP Mail Server

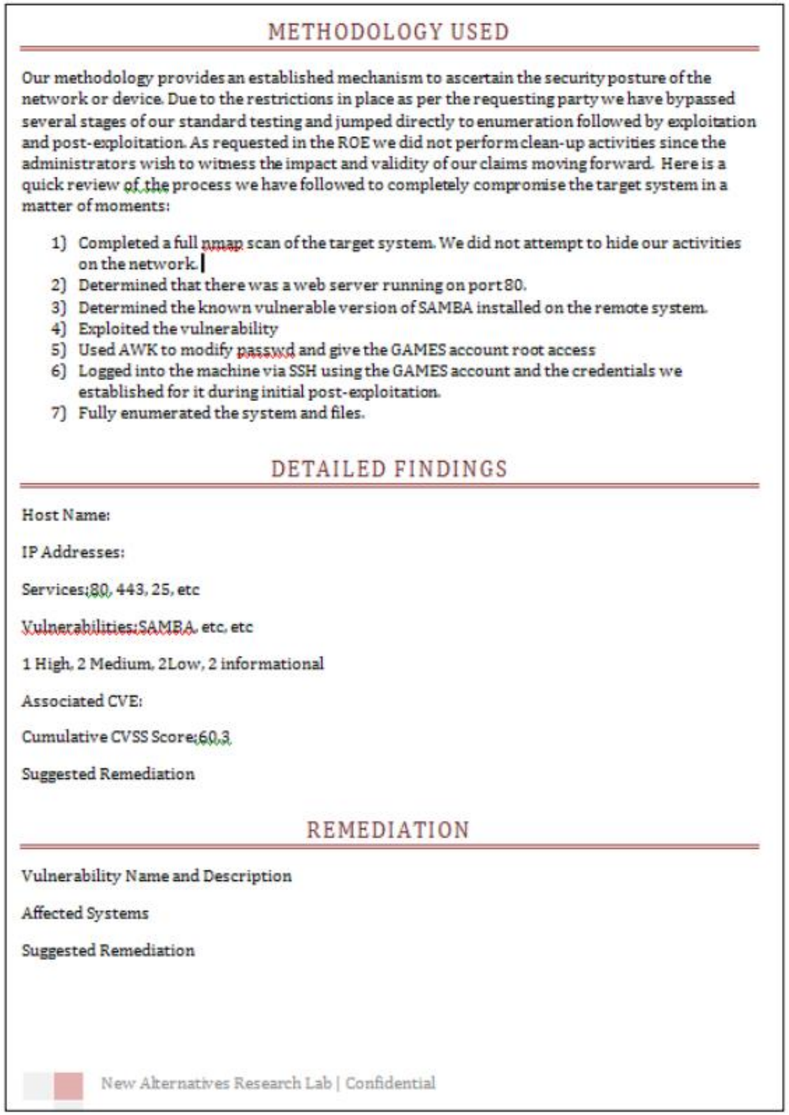
The mail server needs to be properly configured to ensure that it cannot be used to send out unwanted emails. (As an email relay server)

New Alternatives Research Lab | Confidential

Report format

- **Methodology**
  - Provide an overview of how you deliver services:
    - process for each phase
    - tools used
    - how you handle identifed threats
  - Develop diagrams showcasing process flow and resource reporting structures

Methodology



METHODOLOGY USED

Our methodology provides an established mechanism to ascertain the security posture of the network or device. Due to the restrictions in place as per the requesting party we have bypassed several stages of our standard testing and jumped directly to enumeration followed by exploitation and post-exploitation. As requested in the ROE we did not perform clean-up activities since the administrators wish to witness the impact and validity of our claims moving forward. Here is a quick review of the process we have followed to completely compromise the target system in a matter of moments:

1) Completed a full nmap scan of the target system. We did not attempt to hide our activities on the network.
2) Determined that there was a web server running on port 80.
3) Determined the known vulnerable version of SAMBA installed on the remote system.
4) Exploited the vulnerability
5) Used AWK to modify passwd and give the GAMES account root access
6) Logged into the machine via SSH using the GAMES account and the credentials we established for it during initial post-exploitation.
7) Fully enumerated the system and files.

DETAILED FINDINGS

Host Name:

IP Addresses:

Services:80, 443, 25, etc

Vulnerabilities:SAMBA, etc, etc

1 High, 2 Medium, 2Low, 2 informational

Associated CVE:

Cumulative CVSS Score:60.3

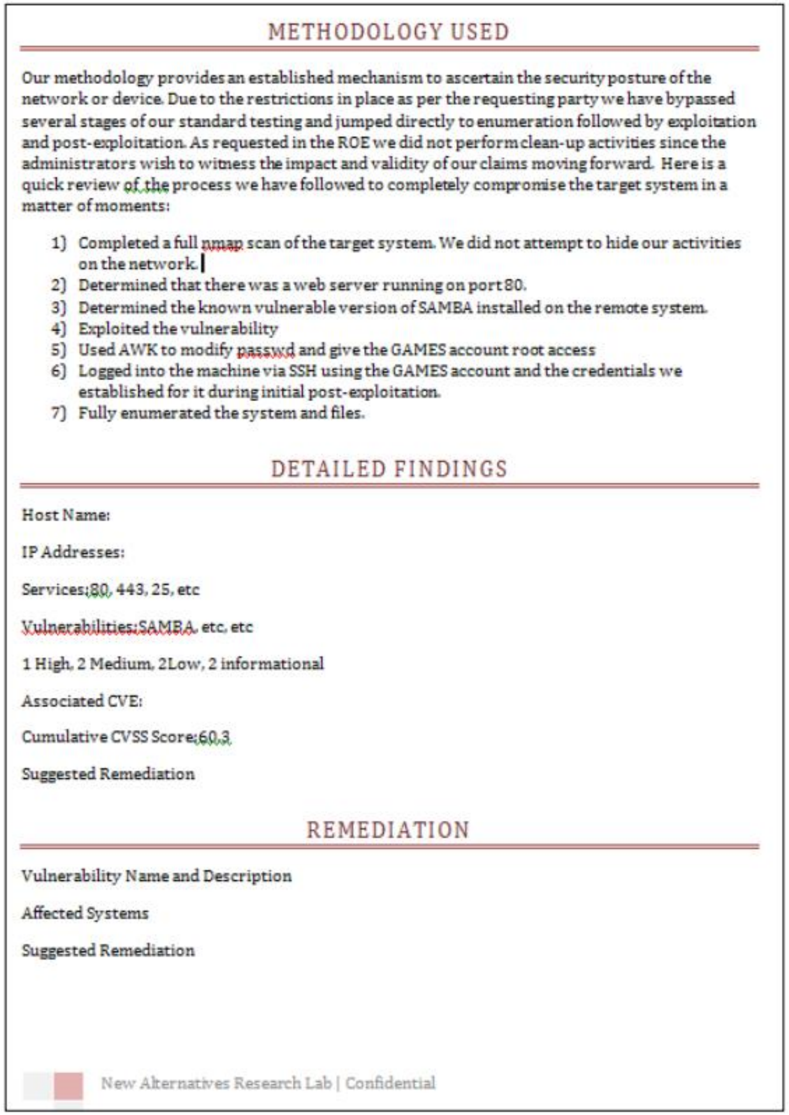
Suggested Remediation

REMEDIATION

Vulnerability Name and Description

Affected Systems

Suggested Remediation



METHODOLOGY USED

Our methodology provides an established mechanism to ascertain the security posture of the network or device. Due to the restrictions in place as per the requesting party we have bypassed several stages of our standard testing and jumped directly to enumeration followed by exploitation and post-exploitation. As requested in the ROE we did not perform clean-up activities since the administrators wish to witness the impact and validity of our claims moving forward. Here is a quick review of the process we have followed to completely compromise the target system in a matter of moments:

1) Completed a full nmap scan of the target system. We did not attempt to hide our activities on the network.
2) Determined that there was a web server running on port 80.
3) Determined the known vulnerable version of SAMBA installed on the remote system.
4) Exploited the vulnerability
5) Used AWK to modify passwd and give the GAMES account root access
6) Logged into the machine via SSH using the GAMES account and the credentials we established for it during initial post-exploitation.
7) Fully enumerated the system and files.

DETAILED FINDINGS

Host Name:

IP Addresses:

Services:80, 443, 25, etc

Vulnerabilities:SAMBA, etc, etc

1 High, 2 Medium, 2Low, 2 informational

Associated CVE:

Cumulative CVSS Score:60.3

Suggested Remediation

REMEDIATION

Vulnerability Name and Description

Affected Systems

Suggested Remediation

New Alternatives Research Lab | Confidential

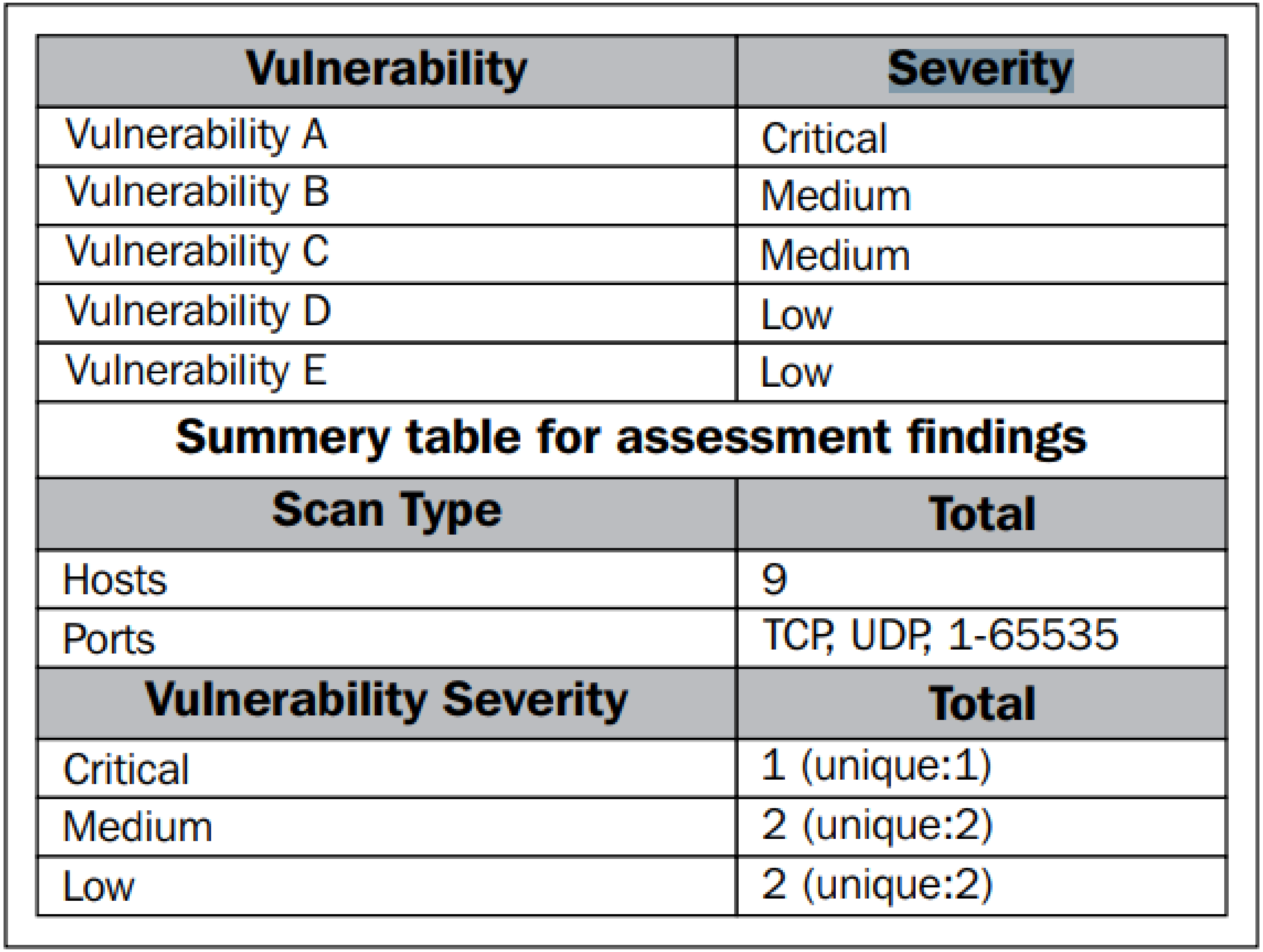
Report format

- **Detailed testing procedures**
  - The **target audience** is typically the **technical staff**, and the goal is to **provide as much information as possible**
  - **Customers may want to challenge** a highlighted item and repeat the steps used to validate the vulnerability, meaning they **want to know how** things are discovered, accessed, and exploited
  - **Subjects** to include are targets discovery, mapping, vulnerability assessment, architecture analysis, exploiting, and reporting

Report format

- **Summary of findings**
    - Where the findings from the services are explained, including how items identified may impact business
    - Best practice is including a **risk ranking to help customers understand** how to react to items identified

Report format



Vulnerability	Severity
Vulnerability A	Critical
Vulnerability B	Medium
Vulnerability C	Medium
Vulnerability D	Low
Vulnerability E	Low

Summery table for assessment findings

Scan Type	Total
Hosts	9
Ports	TCP, UDP, 1-65535

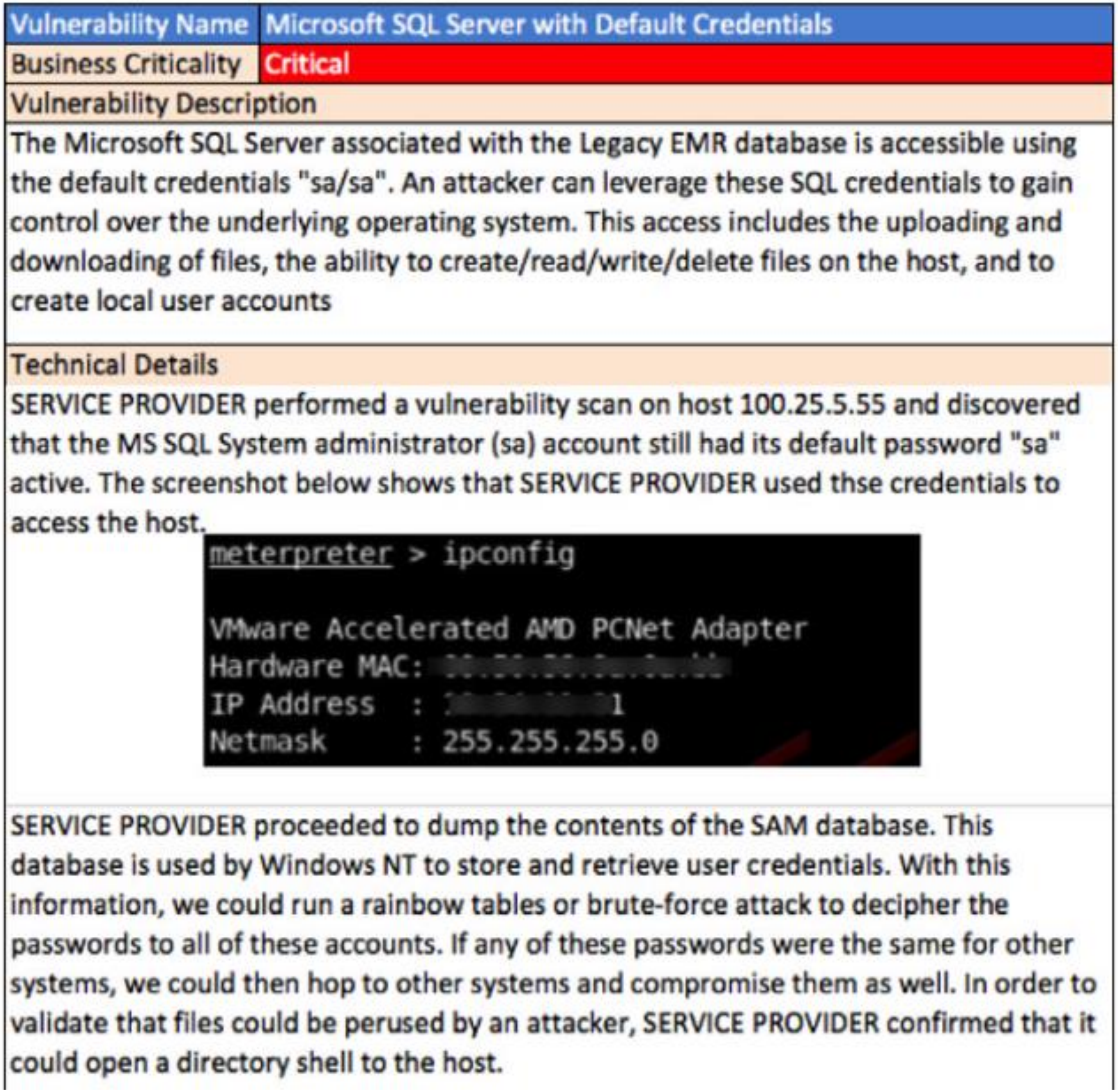
Vulnerability Severity	Total
Critical	1 (unique:1)
Medium	2 (unique:2)
Low	2 (unique:2)

Report format

- **Summary of findings:**
  - **Critical:** Immediate threat to key business processes
  - **High:** Indirect threat to key business processes / threat to secondary business processes
  - **Medium:** Indirect / partial threat to business processes
  - **Low:** No direct threat exists; vulnerability may be leverage with other vulnerabilities

Report format

- **Vulnerabilities**
  - Should include a **clear description** about the source of the weakness, **impact** to business operations and likelihood of being exploited
  - Some details that could be included:
    - Vulnerability name
    - Business criticality
    - Vulnerability description
    - Technical details
    - Affected systems
    - Affected ports
    - Recommended action



Vulnerability Name	Microsoft SQL Server with Default Credentials
Business Criticality	Critical

Vulnerability Description

The Microsoft SQL Server associated with the Legacy EMR database is accessible using the default credentials "sa/sa". An attacker can leverage these SQL credentials to gain control over the underlying operating system. This access includes the uploading and downloading of files, the ability to create/read/write/delete files on the host, and to create local user accounts

Technical Details

SERVICE PROVIDER performed a vulnerability scan on host 100.25.5.55 and discovered that the MS SQL System administrator (sa) account still had its default password "sa" active. The screenshot below shows that SERVICE PROVIDER used thse credentials to access the host.

```
meterpreter > ipconfig

VMware Accelerated AMD PCNet Adapter
Hardware MAC: [redacted]
IP Address  : [redacted]1
Netmask     : 255.255.255.0
```

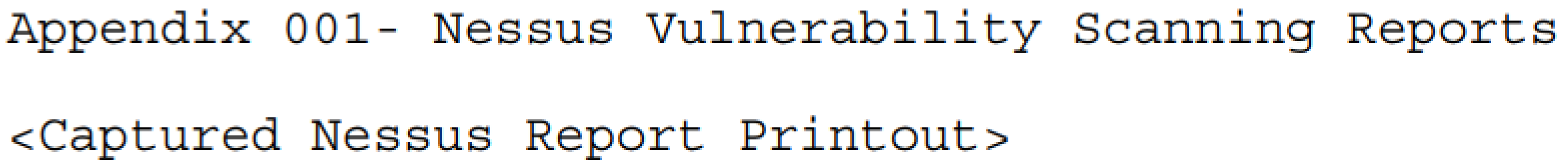
SERVICE PROVIDER proceeded to dump the contents of the SAM database. This database is used by Windows NT to store and retrieve user credentials. With this information, we could run a rainbow tables or brute-force attack to decipher the passwords to all of these accounts. If any of these passwords were the same for other systems, we could then hop to other systems and compromise them as well. In order to validate that files could be perused by an attacker, SERVICE PROVIDER confirmed that it could open a directory shell to the host.

Report format

- **Network considerations and recommendations**
    - **Explains recommendations** to remediate items found from services provided
    - **Include warnings of possible negative impact** with any suggested remediation along with confirming that steps provided do not guarantee to fix the problem or bring a system into compliance with a specific regulation

Report format

- **Appendices**
  - Lists additional information related to the deliverable report
  - Ex:



Appendix 001- Nessus Vulnerability Scanning Reports

<Captured Nessus Report Printout>

Report format

- **Glossary**

  Defne the meaning of terms used in the proposal

Tài liệu tham khảo

- OWASP
  - https://www.owasp.org/index.php/OWASP_Mobile_Security_Testing_Guide
  - https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents
- **Web Penetration Testing with Kali Linux**, Joseph Muniz, Aamir Lakhani

Bảo mật web và ứng dụng

Trường ĐH CNTT TP. HCM