Penetration Test Report | Client Name

Client Name

Ghost Exploit | @gh0stxplt"

date

Contents

1 Executive Summary

1.1 Overview

Discuss at a high level what, why, how, who, and when. Target audience is Executives who may not care for all the details

1.2 Summary of Results

Give an overview of the most important findings from the penetration test

1.3 Overall Risk Rating

lorem ipsum

Note Example: Lorem ipsum dolor sit amet, consectetur adipiscing elit. Nam aliquet libero quis lectus elementum fermentum.
Fusce aliquet augue sapien, non efficitur mi ornare sed. Morbi at dictum felis. Pellentesque tortor lacus, semper et neque vitae, egestas commodo nisl.

1.4 Prioritized Remediation Efforts

What findings need to be remediated first and foremost

2 Scope of Work

2.1 Overall Scope

Explain the scope of the assessment

2.2 Risk Appetite

Discuss client's risk appetite; how much risk are they willing to accept? More information

2.3 Attack Persona

Define how you are attacking the system (e.g. black box, APT, internal) as defined by the client

2.4 Target Assets

Summarize assets in scope; this is expanded upon in the Findings section for each asset

Asset	Value (1 - 5)	IP Address (if known)
Web Server	2	192.168.x.x
AD Server	5	192.168.x.x
Workstation 1	1	192.168.x.x

3 Methodologies

Explain your methodology when apporaching the assessment

3.1 Information Gathering & Enumeration

Reiterate what the scope of the test was and provide enumeration steps taken (e.g. automated scan results or manual testing findings)

Enumeration information

3.2 Findings

The penetration testing portions of the assessment focus heavily on gaining access to a variety of systems. During this penetration test, I was able to successfully gain access to **X** out of the **X** systems.

3.2.1 System IP: 192.168.x.x

Copy this section down to the `\newpage` for each system within the test scope. If multiple vulnerabilities are found, copy the `Vulnerability Findings to Severity` as needed.

3.2.1.1 Service Enumeration

Nmap Scan Results:

Vulnerability Finding 1:

Vulnerability Fix:

Severity:

Vulnerability Finding 2:

Vulnerability Fix:

Severity:

3.2.1.2 Privilege Escalation Achieved? (Y/N)

If you achieved privilege escalation on the machine this section can be used. Otherwise the informational sections can be ommited.

Additional Priv Esc info

Vulnerability Exploited:

Vulnerability Explanation:

Vulnerability Fix:

Severity:

Exploit Code:

Proof Screenshot:

Figure 3.1: Image Placeholder

3.3 Maintaining Access

Discuss how access can be maintained within the compromised environment and show POC

3.4 House Cleaning

Explain what items were cleaned up after the test and show proof screenshots that the items no longer exist within the client environment

4 Additional Items

4.1 Appendix A - Descriptive Title:

Lorem

4.2 Appendix B - Code Used:

```
code here
```

4.3 Appendix C - Tools Utilized: