



security
engineering
pentesting
labs

Penetration Test Report

Company Name, Inc.

MM/DD/YYYY - MM/DD/YYYY

CONFIDENTIAL



1.1 DEBRIEFING 3

1.1.1 DISCLAIMER 3

1.1.2 RULES OF ENGAGEMENT 3

1.1.3 STATEMENT OF WORK 3

2.1 SUMMARY OF RESULTS 4

3.1 ATTACK NARRATIVE 5

3.1.2 INFORMATION GATHERING 5

3.1.3 INITIAL Foothold 6

3.1.4 PRIVILEGE ESCALATION 7

3.1.5 ACTIONS ON OBJECTIVES 8

4.1 AFFECTED ASSETS. 9

5.1 RISK RATINGS 10

6.1 REMEDIATIONS 11

7.1 CONCLUSION 12

APPENDIX 13

Penetration Test Report

Company Name, Inc. MM/DD/YYYY - MM/DD/YYYY



security
engineering
pentesting
labs

DEBRIEFING

This penetration test security assessment was officially approved on Month DD, YYYY at 24:00 CDT, and commenced no sooner than 24 hours after that mark.

This was a simulated attack on the system. This document serves as an overview of initial discoveries and any techniques employed.

The assessment adhered strictly to the Rules of Engagement put forth by management [see: Offsec] during the initial briefing and documentation delivered on Weekday, Month DD, YYYY.

Efforts were placed on the identification and exploitation of security weaknesses that could allow a remote attacker to gain unauthorized access to organizational data.

The attacks were conducted with the level of access that a general Internet user would have.

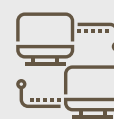
The assessment was conducted in accordance with the recommendations outlined in NIST SP 800-115 with all tests and actions being conducted under controlled conditions.



Summary of Results



Attack Narrative



Affected Assets



Risk Ratings



Remediations

DISCLAIMER

Be it known that this is a point-in-time assessment valid for a maximum of 45 days after initial disclosure of findings. The auditors are not responsible for remediation procedures, but instead can help provide direction for any on-site teams. This document does not serve as a clean bill of health. There is no such thing as a “fully comprehensive” penetration test. We will cover as much as we can in our best ability, and we will provide a detailed, honest report— every time.

RULES OF ENGAGEMENT & STATEMENT OF WORK

Rules and limitations as defined by management

Scope as defined by management

CONFIDENTIAL

Penetration Test Report

Company Name, Inc. MM/DD/YYYY - MM/DD/YYYY



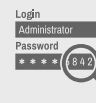
security
engineering
pentesting
labs

SUMMARY OF RESULTS

High-level summary of the discoveries, techniques, and events leading to system compromise



OSINT



Password Cracking



Privilege Escalation



Objectives

CONFIDENTIAL

Penetration Test Report

Company Name, Inc. MM/DD/YYYY - MM/DD/YYYY



security
engineering
pentesting
labs

ATTACK NARRATIVE

Information Gathering

Chronological depiction of events



Information Gathering

Screenshot

Screenshot

Screenshot

Screenshot

ALTERNATE USE:

Hide the images
and use this space
for links to artifacts

Event Screenshot 1
Event Screenshot 2
Event Screenshot 3
Event Screenshot 4

Event Evidence 1
Event Evidence 2
Event Evidence 3
Event Evidence 4

CONFIDENTIAL

Penetration Test Report

Company Name, Inc. MM/DD/YYYY - MM/DD/YYYY



security
engineering
pentesting
labs

ATTACK NARRATIVE

Establishing a Foothold

Chronological depiction of events

Login

Administrator

Password

* * * * 842

Establishing a Foothold

Screenshot

Screenshot

Screenshot

Screenshot

ALTERNATE USE:

Hide the images
and use this space
for links to artifacts

Event Screenshot 1
Event Screenshot 2
Event Screenshot 3
Event Screenshot 4

Event Evidence 1
Event Evidence 2
Event Evidence 3
Event Evidence 4

CONFIDENTIAL

Penetration Test Report

Company Name, Inc. MM/DD/YYYY - MM/DD/YYYY



security
engineering
pentesting
labs

ATTACK NARRATIVE

Privilege Escalation

Chronological depiction of events



Privilege Escalation

Screenshot

Screenshot

Screenshot

Screenshot

ALTERNATE USE:

Hide the images
and use this space
for links to artifacts

Event Screenshot 1
Event Screenshot 2
Event Screenshot 3
Event Screenshot 4

Event Evidence 1
Event Evidence 2
Event Evidence 3
Event Evidence 4

CONFIDENTIAL

Penetration Test Report

Company Name, Inc. MM/DD/YYYY - MM/DD/YYYY



security
engineering
pentesting
labs

ATTACK NARRATIVE

Actions on Objectives

Chronological depiction of events



Actions on Objectives

Screenshot

Screenshot

Screenshot

Screenshot

ALTERNATE USE:

Hide the images
and use this space
for links to artifacts

Event Screenshot 1
Event Screenshot 2
Event Screenshot 3
Event Screenshot 4

Event Evidence 1
Event Evidence 2
Event Evidence 3
Event Evidence 4

CONFIDENTIAL

Penetration Test Report

Company Name, Inc. MM/DD/YYYY - MM/DD/YYYY



security
engineering
pentesting
labs

AFFECTED ASSETS

Affected Assets

SUBNET: 10.11.12.0/23

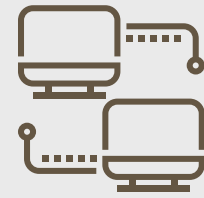
10.11.10.254, 10.11.10.253, 10.11.10.252, 10.11.10.250,
10.11.10.249, 10.11.10.246

SUBNET: 10.11.13.0/23

10.11.10.254, 10.11.10.253, 10.11.10.252, 10.11.10.250,
10.11.10.249, 10.11.10.246, 10.11.10.246, 10.11.10.246
10.11.10.246, 10.11.10.246, 10.11.10.246, 10.11.10.246
10.11.10.246, 10.11.10.246, 10.11.10.246, 10.11.10.246
10.11.10.246, 10.11.10.246, 10.11.10.246, 10.11.10.246

SUBNET: 10.11.13.13/20

10.11.10.254, 10.11.10.253, 10.11.10.252, 10.11.10.250,
10.11.10.246, 10.11.10.246, 10.11.10.246, 10.11.10.246



Affected Assets

CONFIDENTIAL

Penetration Test Report

Company Name, Inc. MM/DD/YYYY - MM/DD/YYYY



security
engineering
pentesting
labs

RISK RATINGS

Risk categorized by rating and criticality



Risk Ratings

CONFIDENTIAL

Penetration Test Report

Company Name, Inc. MM/DD/YYYY - MM/DD/YYYY



security
engineering
pentesting
labs

REMEDIATIONS

Recommended remediation techniques



Remediations

CONFIDENTIAL

Penetration Test Report

Company Name, Inc. MM/DD/YYYY - MM/DD/YYYY



security
engineering
pentesting
labs

CONCLUSION

Conclusion of results



Conclusion of Results

CONFIDENTIAL

Penetration Test Report

Company Name, Inc. MM/DD/YYYY - MM/DD/YYYY



security
engineering
pentesting
labs

APPENDIX

APPENDIX & DEFINITIONS

CONFIDENTIAL