**Delivery Date:** **{date | convertDate: ‘full’}**

**{name}** **Penetration Test Report**

**Submitted To:**

{company.name}

{client.firstname} {client.lastname}

Client Address

City, ST ZIP

Phone Number: {client.phone}

Email: {client.email}

**Submitted By:**

Dark Wolf Solutions

13454 Sunrise Valley, Suite 550

Herndon, VA 20171

Phone Number: (571) 287-7255

info@darkwolfsolutions.com

**Dark Wolf Solutions, LLC**

Dark Wolf Solutions operates at the nexus of mission and technology to meet our Nation's most challenging missions. We combine the most innovative emerging technologies with deep federal domain expertise through cutting-edge intelligence services, DevSecOps agile software development, information operations, penetration testing and incident response, applied research and rapid prototyping, machine learning, and engineering services.

We support a diverse portfolio of solutions and services for Defense, Intelligence, and Fortune 500 customers. Our team comprises analysts, support officers, and experienced engineers and integrators with hands-on expertise across many of the most relevant COTS, GOTS, and open-source technologies. We also regularly compete in premier competitions with an increasing number of conference wins and placements including IoT, Wireless and OSINT CTFs at DEF CON, Wireless CTFs at BSides, Splunk Boss of the SOC and the Navy’s HACKtheMACHINE.

For more information please visit us at: <https://www.darkwolfsolutions.com>

**Table of Contents**

[Engagement Points of Contact 2](#_Toc102037242)

[1.0 Introduction and Objectives 4](#_Toc102037243)

[2.0 Commendable Practices 4](#_Toc102037244)

[*Commendable Practices* 4](#_Toc102037245)

[3.0 Executive Summary – {name} Penetration Test 5](#_Toc102037246)

[3.1 Overview 5](#_Toc102037247)

[3.2 Findings Outline 6](#_Toc102037248)

[3.3 Engagement Scope and Timeline 6](#_Toc102037249)

[3.4 Risk Evaluation and Assessment 6](#_Toc102037250)

[3.5 Conclusion 7](#_Toc102037251)

[4.0 DWS Risk Rating (DWRR) 7](#_Toc102037252)

[5.0 Findings 9](#_Toc102037253)

[5.1 {title} 10](#_Toc102037254)

[6.0 Post Test Phase Recommendations (Clean up) 12](#_Toc102037255)

[6.1 Purpose 12](#_Toc102037256)

[6.2 Recommended Steps 12](#_Toc102037257)

[7.0 Appendix 13](#_Toc102037258)

[Appendix A: Reference Materials 13](#_Toc102037259)

[Appendix B: Risk Rating Methodology 14](#_Toc102037260)

[Appendix C: Penetration Testing Methodology 15](#_Toc102037261)

[DWS Playbook Reference 15](#_Toc102037262)

[DWS Playbook Excerpts 16](#_Toc102037263)

# Engagement Points of Contact

**Dark Wolf Solutions Team:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Project Role** | **Email** | **Phone** |
| {creator.firstname} {creator.lastname} | {role} | {creator.email} | {creator.phone} |
| {#collaborators}{firstname} {lastname} | {role} | {email} | {phone}  {/collaborators} |

**Client Team:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Contact Role** | **Email** | **Phone** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Introduction and Objectives

Dark Wolf Solutions, LLC (DWS) performed an {testtype} for {company.name} in {date}. The environment below is in accordance to the Dark Wolf Solutions Test Plan / Rules of Engagement document that was mutually agreed upon during the project planning phase of this test:

|  |
| --- |
| **Target Scope** |
| **{-w:p scope}{name}{/scope}** |

This test was conducted to identify gaps and vulnerabilities that could result in unnecessary risks to the target infrastructure. Upon completing these tests, DWS prioritized the identified vulnerabilities as to their impact to the overall security and included industry standard recommendations.

# Commendable Practices

DWS identified the following areas where {company.name} meets or exceeds industry best practices:

|  |  |
| --- | --- |
| **Finding** | **Description** |
| {#findings}{#vulnType == ‘Commendable’}**{title}** | {short\_desc}  {/vulnType == ‘Commendable’}  {/findings} |

# Executive Summary – {name} Penetration Test

This penetration test was conducted to identify gaps and vulnerabilities that could result in unnecessary risks to the infrastructure. Upon completing these tests, DWS prioritized the identified vulnerabilities as to their impact to the overall security and included industry standard recommendations to address the discovered issues.

|  |  |
| --- | --- |
| **Risk** | **Number of Vulnerabilities** |
| **Critical** | **{findings | count: ‘Critical’}** |
| **High** | **{findings | count: ‘High’}** |
| **Medium** | **{findings | count: ‘Medium’}** |
| **Low** | **{findings | count: ‘Low’}** |

*Vulnerability Summary*

## Overview

DWS identified vulnerabilities throughout the environment. These vulnerabilities were largely caused as the result of poor minimum baseline configurations, patching, password implementation, open shares with stored credentials in cleartext documents, and default configurations being enabled. DWS recommends that Critical and High-level vulnerabilities be addressed as soon as possible, and Medium and Low-level vulnerabilities be addressed within a minimum of 30-90 days.

## Findings Outline

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Vulnerability and Risk Rating** |  | **IP** | **Port/Protocol** | **Summary Description** |
| **{#findings}{#cvss.baseSeverity == ‘Critical’}{title}** | **{cvss.baseSeverity}** | {#hosts}  {@text | convertHTML}  {/hosts} | {#ports}  {@text | convertHTML}  {/ports} | {short\_desc}  {/cvss.baseSeverity == ‘Critical’}  {/findings} |
| **{#findings}{#cvss.baseSeverity == ‘High’}{title}** | **{cvss.baseSeverity}** | {#hosts}  {@text | convertHTML}  {/hosts} | {#ports}  {@text | convertHTML}  {/ports} | {short\_desc}  {/cvss.baseSeverity == ‘High’}  {/findings} |
| **{#findings}{#cvss.baseSeverity == ‘Medium’}{title}** | **{cvss.baseSeverity}** | {#hosts}  {@text | convertHTML}  {/hosts} | {#ports}  {@text | convertHTML}  {/ports} | {short\_desc}  {/cvss.baseSeverity == ‘Medium’}  {/findings} |
| **{#findings}{#cvss.baseSeverity == ‘Low’}{title}** | **{cvss.baseSeverity}** | {#hosts}  {@text | convertHTML}  {/hosts} | {#ports}  {@text | convertHTML}  {/ports} | {short\_desc}  {/cvss.baseSeverity == ‘Low’}  {/findings} |
| **{#findings}{#cvss.baseSeverity == ‘None’}{title}** | **{cvss.baseSeverity}** | {#hosts}  {@text | convertHTML}  {/hosts} | {#ports}  {@text | convertHTML}  {/ports} | {short\_desc}  {/cvss.baseSeverity == ‘None’}  {/findings} |

*Vulnerabilities Identified During Testing*

## Engagement Scope and Timeline

The testing period for this engagement occurred from {date\_start} to {date\_end}. The scope of testing is depicted below and requires the Client to whitelist all DWS consultants in order to gain access for testing. The testing itself was conducted via the approved AWS Kali AMI that was installed by the Client’s developer team.

|  |  |
| --- | --- |
| **Penetration Test Scope – {name}** | |
| **Testing Firm:** | Dark Wolf Solutions, LLC |
| **Method:** | {test\_scope.method} |
| **IP Range:** | {-w:p test\_scope.iprange}  {@text | convertHTML}  {/test\_scope.iprange} |
| **Type:** | {testtype} |
| **Intrusion Point:** | {test\_scope.intrusion} |
| **Testing Start Date:** | {date\_start} |
| **Testing End Date:** | {date\_end} |

*Penetration Test Scope*

## Risk Evaluation and Assessment

Organizational risk resulting from each finding is assessed based on two main criteria: the likelihood of exploitation and the impact resulting from that exploitation (see the [Dark Wolf Risk Assessment Matrix](https://docs.google.com/document/d/18FlF__ZXjupMT7MLCPXYY-elPoOy5EGJNy94OiuTb04/edit#heading=h.g6064hkqr042) for an example). The following chart is a consolidated risk assessment of all findings found applied against the CIA (Confidentiality, Integrity, Availability) triad. The CIA triad is a common model used to group and identify areas of risk to an organization within the realm of information security.

|  |  |  |
| --- | --- | --- |
| **Risk to Confidentiality – {risk\_eval.riskc}** | | |
| Likelihood of Unauthorized Access | **{risk\_eval.likelihoodua}** | {#risk\_eval.likelihood\_ua\_desc}  {@text | convertHTML}  {/risk\_eval.likelihood\_ua\_desc} |
| Impact of Unauthorized Access | **{risk\_eval.impactua}** | {#risk\_eval.impact\_ua\_desc}  {@text | convertHTML}  {/risk\_eval.impact\_ua\_desc} |
| Likelihood of Data Exfiltration | **{risk\_eval.likelihoodde}** | {#risk\_eval.like\_de\_desc}  {@text | convertHTML}  {/risk\_eval.like\_de\_desc} |
| Impact of Data Exfiltration | **{risk\_eval.impactde}** | {#risk\_eval.impact\_de\_desc}  {@text | convertHTML}  {/risk\_eval.impact\_de\_desc} |
| **Risk to Integrity – {risk\_eval.riski}** | | |
| Likelihood of unauthorized data manipulation | **{risk\_eval.likelihood\_udm}** | {#risk\_eval.likelihood\_udm\_desc}  {@text | convertHTML}  {/risk\_eval.likelihood\_udm\_desc} |
| Impact of unauthorized data manipulation | **{risk\_eval.impact\_udm}** | {#risk\_eval.impact\_udm\_desc}  {@text | convertHTML}  {/risk\_eval.impact\_udm\_desc} |
| **Risk to Availability – {risk\_eval.riska}** | | |
| Likelihood of application or service experiences DoS conditions | **{risk\_eval.likelihood\_dos}** | {#risk\_eval.likelihood\_dos\_desc}  {@text | convertHTML}  {/risk\_eval.likelihood\_dos\_desc} |
| Impact of application or service experiences DoS conditions | **{risk\_eval.impact\_dos}** | {#risk\_eval.impact\_dos\_desc}  {@text | convertHTML}  {/risk\_eval.impact\_dos\_desc} |

*CIA Triad Summary*

## Conclusion

{-w:p risk\_eval.conclusion}

{@text | convertHTML}

{/risk\_eval.conclusion}

# DWS Risk Rating (DWRR)

The DWRR is an internal mechanism in order to evaluate the risk of each vulnerability. The ratings range from least to most serious as: Note/Info, Low, Medium, High, Critical. This calculation is based upon the following four categories:

* Technical Impact
* Organizational Impact
* Vulnerability Factors
* Threat Agent Factors

Please see [Appendix B](#_4zsmq8s4qop7) for a more detailed description of how risk ratings are determined, based on industry best practices and impact.

# Findings

The following section outlines the vulnerability details that were discovered during testing. A description of the vulnerability/impact, recommendations, and screenshots (where applicable) are outlined in accordance with each vulnerability.

- This section was intentionally left blank -{#findings}

{#vulnType != ‘Commendable’}

## {title}

**Vulnerability Level: {cvss.baseSeverity}**

**Impacted NIST 800-53 Controls:**

**Affected Systems:**

|  |  |  |
| --- | --- | --- |
| **Host** | **Port/Protocol** | **Service** |
| **{#hosts}**  **{@text | convertHTML}**  **{/hosts}** | {#ports}  {@text | convertHTML}  {/ports} | {#service}  {@text | convertHTML}  {/service} |

**Description:**

{#description}

{@text | convertHTML}

{#images}

{%image}

*{caption}*

{/images}

{/description}

**Recommendations:**

{#remediation}

{@text | convertHTML}

{#images}

{%image}

Image 1 – {caption}

{/images}

{/remediation}

**References:**

{#references}

{.}

{/references}  
 {/vulnType != ‘Commendable’}

{/findings}

## 

# Post Test Phase Recommendations (Clean up)

## Purpose

The following section tracks the steps that should be taken after the conclusion of DWS penetration testing. Some of the steps where possible/practical were already carried out by DWS and marked as such under the “Completed By” column. Otherwise, {company.name} tasks are labeled accordingly and should be carried out within a timely manner.

## Recommended Steps

|  |  |  |  |
| --- | --- | --- | --- |
| **Host** | **Service** | **Task** | **Completed By** |
|  |  |  | <Client> |
|  |  |  | DWS |

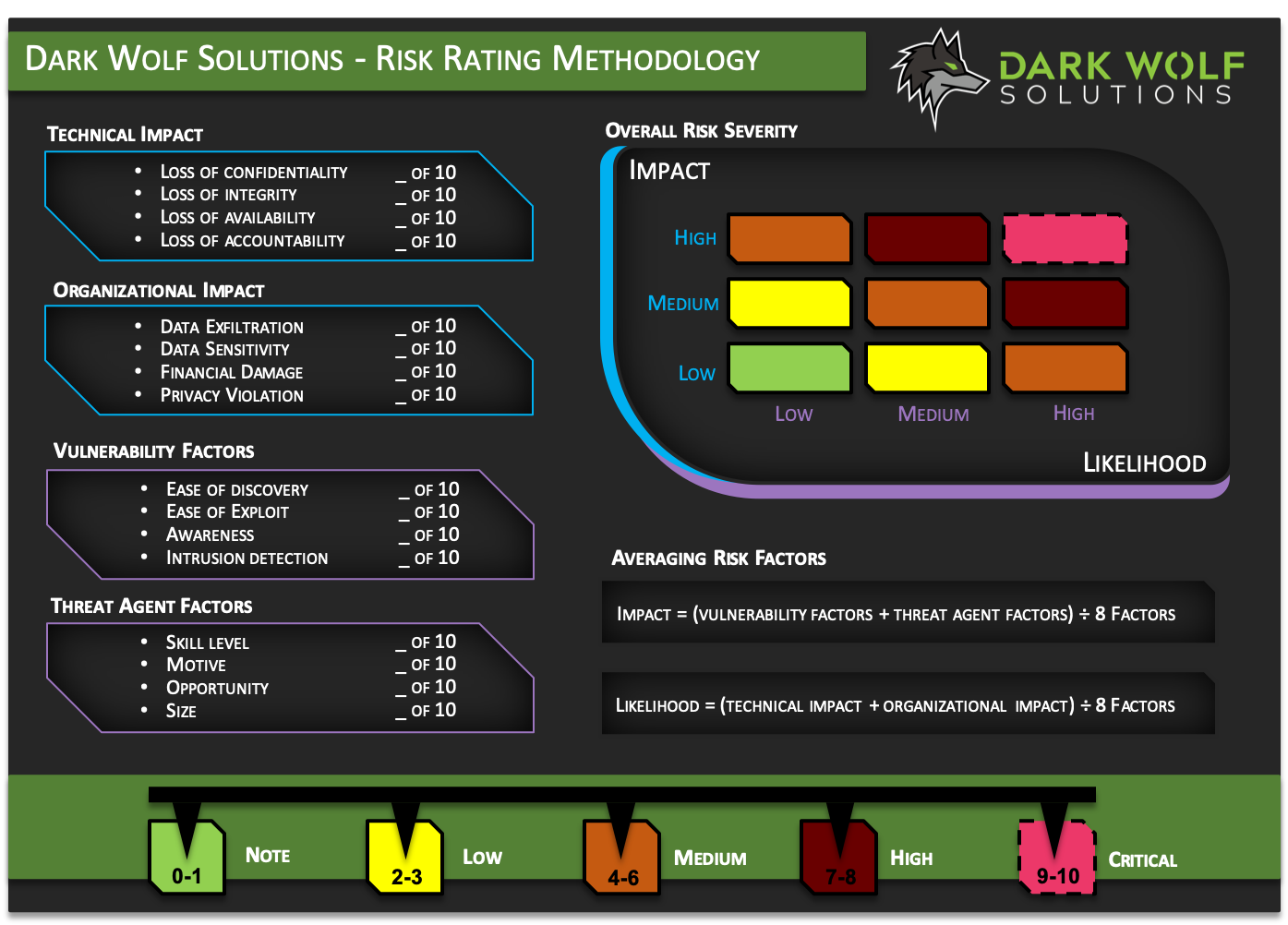
# Appendix

## Appendix A: Reference Materials

|  |  |
| --- | --- |
| **Reference Materials** | |
| **Penetration Testing Playbook** | The Dark Wolf Solutions Penetration Testing Playbook |
| **Dark Wolf Risk Rating (DWRR) Matrix** | Dark Wolf’s Matrix for Evaluating Vulnerabilities |
| [**CVSS 3.0/3.1**](https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator) | <https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator> |
| [**NIST 800-53\_r5**](https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final) | <https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final> |
| **OWASP Top 10** | <https://owasp.org/www-project-top-ten> |
| **OWASP Top 10 Checklist** | <https://owasp.org/www-project-web-security-testing-guide/assets/archive/OWASP_Web_Application_Penetration_Checklist_v1_1.pdf> |

*Supporting Documents and References*

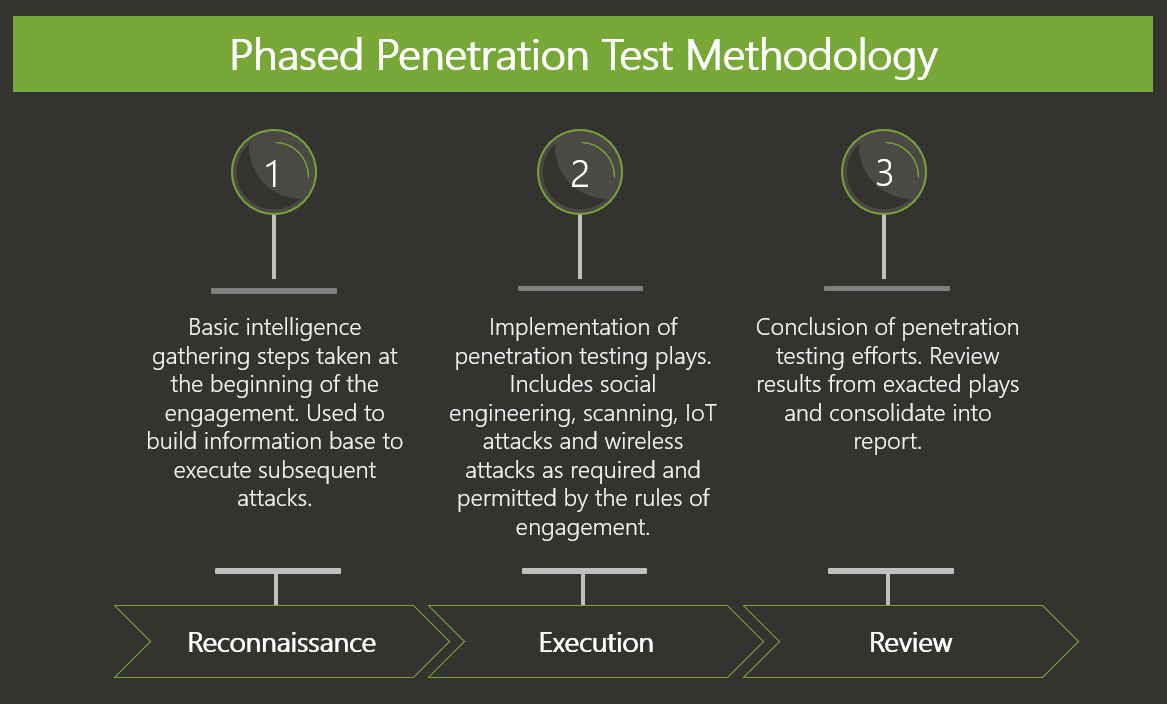
## Appendix B: Risk Rating Methodology

****

*Dark Wolf’s Risk Rating Methodology*

## Appendix C: Penetration Testing Methodology

DWS testers follow a three-phased approach to penetration testing – reconnaissance, execution, and review. The team generally begins an engagement by conducting reconnaissance using a combination of manual analysis of client-provided documentation and industry standard tools such as Kali Linux Security Distribution, Tenable’s Nessus, Network Mapper (Nmap), and Burp Suite where applicable.



*Dark Wolf’s Penetration Testing Methodology*

### DWS Playbook Reference

DWS security consultants have developed a comprehensive playbook for penetration testing that encompasses a full detailed methodology for internal and Client reference. A brief outline of the playbook is shown below to give a small insight into the full collection of documentation that is available upon request and approval by DWS management.

### DWS Playbook Excerpts

The plays provided here were documented in and selected from Dark Wolf’s “Penetration Testing Playbook”, an internal resource used to guide the team’s penetration testing efforts. Note that this selection of plays is not meant to be all-inclusive or completely encompassing of all testing activities, but rather is intended to provide a baseline sample of activities performed during the course of testing.

|  |  |
| --- | --- |
| **Play** | **Description** |
| Port Scanning | Port Scanning involves scanning one or multiple machines (servers, host machines, end user devices etc.) on an organization's network for open TCP and UDP ports. Port scanning is a quick and easy way to identify services running on a host machine or server. |
| Nessus Vulnerability Scanning | Nessus can be used as a nearly all-inclusive solution for detecting many high- and low-level vulnerabilities which can be leveraged in the testing efforts of other plays. Once the initial set up and reconnaissance has been conducted, Nessus is one of the primary tools that helps guide the tester where to focus their efforts next. |
| Open Source Vulnerability Scanning | Open-source vulnerability scanners like OpenVAS function much like the proprietary Nessus software. They are meant to be a nearly all-inclusive solution for detecting high and low-level vulnerabilities that can be leveraged for future exploitation and testing. Used correctly, they are just as powerful an automation tool as Nessus that guides the penetration tester on where to focus their efforts next. |
| Web Application Scanning | This play is designed to identify and fingerprint different web-based applications running on a network/host. Usually this is done on the organization’s public facing network but can be conducted on the internal network if a host is running any web services. The goal of this activity is to identify misconfigured web applications with potential security vulnerabilities for future exploitation. |
| Kubernetes Vulnerability Scanning / Manual Testing | Automated and manual testing of Kubernetes implementations was conducted to ensure there are no misformed K8 clusters or vulnerable nodes/pods exposed during testing. |
| Shared Directory Exploration | A low hanging fruit for an attacker with internal network access, the shared drives of networks without strict security policy enforcement will sometimes contain files with stored credentials and references to internal services used to develop the target’s software. A penetration tester can attempt to locate these using basic directory reconnaissance techniques. |
| Password Attacks | This play involves testing specified accounts and authentication endpoints by employing a mass quantity of common and customized password and username lists to successfully guess a victim’s credentials. The tester may also generate custom wordlists and username lists via applications such as Cewl, John, and Crunch. Through this testing, the penetration tester will look for weak authentication protection and default accounts. |
| Packet Capture / Analysis | Utilizing traffic capturing tools such as tcpdump, examples of traffic generated within the target network can then be analyzed for information gathering. |

*Plays Employed During Testing*