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

{name}

Penetration Test Report

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:**

Jonathan Perez, Principal

Dark Wolf Solutions

13454 Sunrise Valley, Suite 550

Herndon, VA 20171

(770) 490-6655

Jonathan.Perez@darkwolfsolutions.com

1. 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 black badges such as wins at B-Sides DC (2016 and 2018) and DEFCON (2017).

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

Table of Contents

1.0 Dark Wolf Solutions, LLC 1

2.0 Engagement Points of Contact 3

2.1 Dark Wolf Solutions Team: 3

2.2 Client Team: 3

3.0 Executive Summary 4

3.1 Overview 4

3.2 Commendable Practices 4

3.3 Summary of Findings 4

4.0 <Vendor> <Drone> Penetration Test 6

4.1 Objectives 6

4.2 Engagement Scope 6

4.3 Penetration Testing Methodology 7

4.4 Risk Rating Methodology 7

5.0 UAS Package Overview 8

5.1 <Vendor> <Drone> UAS 8

5.2 <Component Name> Controller 8

5.3 <Vendor> <Drone> <Software Name> Flight Software 9

5.4 <Brand Name> Cameras 9

6.0 Assessment Findings 10

6.1 <Component Name> Flight Controller Findings 10

6.1.1 Findings Template 10

6.2 <Vendor> <Drone> UAS Findings 11

6.2.1 Findings Template 11

6.3 <Component Name> Findings 12

6.3.1 Findings Template 12

1. Engagement Points of Contact
   1. Dark Wolf Solutions Team:

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

* 1. Client Team:

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Contact Role | Email | Phone |
| Client Team | Project Role | Email | (XXX) XXX-XXXX |
| Client Team | Project Role | Email | (XXX) XXX-XXXX |
| Client Team | Project Role | Email | (XXX) XXX-XXXX |
| Client Team | Project Role | Email | (XXX) XXX-XXXX |

1. Executive Summary
   1. Overview

{#ex.overview}

{@text | convertHTML}

{/ex.overview}

The vulnerability count results are summarized below:

|  |  |  |  |
| --- | --- | --- | --- |
| Device Under Test | Low | Medium | High |
| {package.dronename} |  |  |  |
| {package.gcsname} |  |  |  |
| {package.fsname} |  |  |  |
| {package.payload1name} |  |  |  |
| { package.payload2name} |  |  |  |
| {package.payload3name} |  |  |  |
| {package.payload4name} |  |  |  |
| {package.payload5name} |  |  |  |
| {package.payload6name} |  |  |  |
| {package.radioname} |  |  |  |

* 1. Commendable Practices

DWS identified the following areas where {vendor} meets or exceeds industry best practices:

|  |  |
| --- | --- |
| Finding | Description |
|  |  |

* 1. Summary of Findings

DWS identified the following vulnerabilities during the {name} penetration test. 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.

|  |  |  |
| --- | --- | --- |
| Section and Title | Risk Level | Issue Description |
| {#findings}{title} | {@cvss.cellColor}  {cvss.baseSeverity} | {short\_desc}  {/findings} |

1. {name} Penetration Test
   1. Objectives

The purpose of this penetration test was to evaluate the {package.dronename}. {vendor} provided a control unit for drone operation, the {package.gcsname} running the {package.gcsos} operating system.

* Objective I - Identify and characterize the cybersecurity footprint of the {package.drone.name} to support the adjudication of an authority to operate before the system can be made available via the GSA schedule.
* Objective II - Test and assess the interfaces, components and payloads to build a body of evidence that supports an overall cyber risk assessment of each platform.
  1. Engagement Scope

Dark Wolf Solutions testers conducted their penetration test out of the {location} from {date\_start} to {date\_end}. While assessing these items, DWS focused on identifying vulnerabilities that would allow unauthorized access, installation of malicious software, third party data retrieval, or unauthorized control of the air vehicle.

DWS identified primary attack surfaces: The unmanned aircraft itself, the ground control station, and the wireless communications link between them.

UAS Cyber Attack Surface

A screenshot of a computer

Description automatically generated with low confidence

Each evaluation began with a physical assessment of the vehicle and ground control for access points and easily accessible memory devices. Based on findings in this phase, some access methods were presented. Accessible memory was extracted and dumped to another device and tested for encryption and data of interest. Access ports were connected to evaluator PC’s and tested for exposed data or ports. An analogous evaluation is performed against wireless access options (Wi-Fi, cell networks, radio links, etc.)

* 1. Penetration Testing Methodology

The Dark Wolf drone testing methodology is based on the following steps:

|  |  |
| --- | --- |
| Process | Process Description |
| Recon | The recon phase consists of searching for open-source information on the target of the security audit. All information potentially useful for an attacker is collected, for example: Types and versions of technologies used, technical documentation, component information, etc... |
| Mapping | The mapping phase consists of testers listing all functionalities and/or critical components of the audit target. This step enables pentesters to have a better visibility on the most crucial and exposed elements. By performing this breakdown, testers are better positioned to take findings from individual subsystems and consider how those findings are impacted by the nature of neighboring subsystems. |
| Discovery | The discovery phase is the attack phase: pentesters look for vulnerabilities through manual searches complemented by automated tools. The objective is to discover as many vulnerabilities as possible on the target. |
| Exploitation | The exploitation phase consists in testing possible exploitations of the flaws identified in the previous phase. This step allows using certain flaws as “pivots”, in order to discover new vulnerabilities. The exploitation of security vulnerabilities allows evaluating their real impact and thus their criticality level. |

* 1. Risk Rating Methodology

Dark Wolf assigns an overall risk rating primarily based on the level of effort required to exploit a given vulnerability and the severity of impact if said vulnerability is exploited. This determination includes consideration of NIST 800-53 controls impacted, CVE rating for publicly cataloged vulnerabilities, and compounding effects due to the presence of other related findings. This is summarized below in the Dark Wolf Risk Assessment Matrix.

Dark Wolf Risk Assessment Matrix

Graphical user interface

Description automatically generated

1. UAS Package Overview

{#package.overview}

{@text | convertHTML}

{/package.overview}

* 1. {package.dronename}

{#package.droneoverview}

{@text | convertHTML}

{#images}

{%image}

{caption}

{/images}

{/package.droneoverview}

* 1. {package.gcsname}

{#package.gcsoverview}

{@text | convertHTML}

{#images}

{%image}

*{caption}*

{/images}

{/package.gcsoverview}

* 1. {package.fsname}

{#package.fsoverview}

{@text | convertHTML}

{#images}

{%image}

*{caption}*

{/images}

{/package.fsoverview}

* 1. {package.payload1name}

{#package.payload1overview}

{@text | convertHTML}

{#images}

{%image}

*{caption}*

{/images}

{/package.payload1overview}

* 1. {package.payload2name}

{#package.payload2overview}

{@text | convertHTML}

{#images}

{%image}

*{caption}*

{/images}

{/package.payload2overview}

* 1. {package.payload3name}

{#package.payload3overview}

{@text | convertHTML}

{#images}

{%image}

*{caption}*

{/images}

{/package.payload3overview}

* 1. {package.payload4name}

{#package.payload4overview}

{@text | convertHTML}

{#images}

{%image}

*{caption}*

{/images}

{/package.payload4overview}

* 1. {package.payload5name}

{#package.payload5overview}

{@text | convertHTML}

{#images}

{%image}

*{caption}*

{/images}

{/package.payload5overview}

* 1. {package.payload6name}

{#package.payload6overview}

{@text | convertHTML}

{#images}

{%image}

*{caption}*

{/images}

{/package.payload6overview}

1. Assessment 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.

* 1. {package.dronename} UAS Findings

{#findings}

{#vulnType == ‘UAV Findings’}

* + 1. {title}

Description:

{#description}

{@text | convertHTML}

{#images}

{%image}

*{caption}*

{/images}

{/description}

|  |  |  |
| --- | --- | --- |
| Impact Level | Level of Effort | Overall Risk Level |
| {cvssObj.A} | {cvssObj.AC} | [{@cvss.cellColor}](mailto:%7b@cvss.cellColor%7d)  {cvss.baseSeverity} |
| Impacted NIST 800-53 Controls | | |
| {nist} | | |

Findings:

{#observation}

{@text | convertHTML}

{#images}

{%image}

*{caption}*

{/images}

{/observation}

Remediation Recommendations:

{#remediation}

{@text | convertHTML}

{#images}

{%image}

*{caption}*

{/images}

{/remediation}

{/vulnType == ‘UAV Findings’}

{/findings}

* 1. {package.flightstack} Flight Stack Findings

{#findings}

{#vulnType == ‘Flight Stack Findings’}

* + 1. {title}

Description:

{#description}

{@text | convertHTML}

{#images}

{%image}

*{caption}*

{/images}

{/description}

|  |  |  |
| --- | --- | --- |
| Impact Level | Level of Effort | Overall Risk Level |
| {cvssObj.A} | {cvssObj.AC} | [{@cvss.cellColor}](mailto:%7b@cvss.cellColor%7d)  {cvss.baseSeverity} |
| Impacted NIST 800-53 Controls | | |
| {nist} | | |

Findings:

{#observation}

{@text | convertHTML}

{#images}

{%image}

*{caption}*

{/images}

{/observation}

Remediation Recommendations:

{#remediation}

{@text | convertHTML}

{#images}

{%image}

*{caption}*

{/images}

{/remediation}

{/vulnType == ‘Flight Stack Findings’}

{/findings}

* 1. {package.gcsname} Ground Control Station Findings

{#findings}

{#vulnType == ‘GCS Findings’}

* + 1. {title}

Description:

{#description}

{@text | convertHTML}

{#images}

{%image}

*{caption}*

{/images}

{/description}

|  |  |  |
| --- | --- | --- |
| Impact Level | Level of Effort | Overall Risk Level |
| {cvssObj.A} | {cvssObj.AC} | [{@cvss.cellColor}](mailto:%7b@cvss.cellColor%7d)  {cvss.baseSeverity} |
| Impacted NIST 800-53 Controls | | |
| {nist} | | |

Findings:

{#observation}

{@text | convertHTML}

{#images}

{%image}

*{caption}*

{/images}

{/observation}

Remediation Recommendations:

{#remediation}

{@text | convertHTML}

{#images}

{%image}

*{caption}*

{/images}

{/remediation}

{/vulnType == ‘GCS Findings’}

{/findings}

* 1. {package.radioname} Radio Findings

{#findings}

{#vulnType == ‘Radio Findings’}

* + 1. {title}

Description:

{#description}

{@text | convertHTML}

{#images}

{%image}

*{caption}*

{/images}

{/description}

|  |  |  |
| --- | --- | --- |
| Impact Level | Level of Effort | Overall Risk Level |
| {cvssObj.A} | {cvssObj.AC} | [{@cvss.cellColor}](mailto:%7b@cvss.cellColor%7d)  {cvss.baseSeverity} |
| Impacted NIST 800-53 Controls | | |
| {nist} | | |

Findings:

{#observation}

{@text | convertHTML}

{#images}

{%image}

*{caption}*

{/images}

{/observation}

Remediation Recommendations:

{#remediation}

{@text | convertHTML}

{#images}

{%image}

*{caption}*

{/images}

{/remediation}

{/vulnType == ‘Radio Findings’}

{/findings}

* 1. Payloads Findings

{#findings}

{#vulnType == ‘Payload Findings’}

* + 1. {title}

Description:

{#description}

{@text | convertHTML}

{#images}

{%image}

*{caption}*

{/images}

{/description}

|  |  |  |
| --- | --- | --- |
| Impact Level | Level of Effort | Overall Risk Level |
| {cvssObj.A} | {cvssObj.AC} | [{@cvss.cellColor}](mailto:%7b@cvss.cellColor%7d)  {cvss.baseSeverity} |
| Impacted NIST 800-53 Controls | | |
| {nist} | | |

Findings:

{#observation}

{@text | convertHTML}

{#images}

{%image}

*{caption}*

{/images}

{/observation}

Remediation Recommendations:

{#remediation}

{@text | convertHTML}

{#images}

{%image}

*{caption}*

{/images}

{/remediation}

{/vulnType == ‘Payload Findings’}

{/findings}