

**DogPark | Team #1**

Dogpark (2023) Team #1 Overview

Produced By:

**Dogpark Team #:**

**Josiah Rodriguez**



# **1. Executive Summary**

The following document details the results of the network penetration test from 11/13/23 - 11/19/23 between 11:30 - 12:00. Three active networks were to be tested between this time, the DMZ, Screened Subnet, and the internal LAN. In between both networks, a total of 5 vulnerabilities were found. A number of the vulnerabilities outlined in this document have the potential to disrupt and actively stop the business operations of Nestler Team #1. Due to the severity of some of the vulnerabilities, we recommend Nestler Team #1 devotes significant resources remediating vulnerabilities with a Prioritization rating of CAT - 4, where out of the 5 vulnerabilities found, 1 had a Prioritization rating of CAT - 4, the highest possible rating. We also used the CVSS Metric to determine severity, and found that out of the 5 , two were considered to have a Critical rating, 1 had a High rating, and 1 had a moderate rating. We will also be using the MITRE ATT&CK Framework and the OWASP Framework.

# **2. Engagement Overview**

The purpose of this assessment was to evaluate the successful implementation and effectiveness of newly added security controls. Specifically, the organization was concerned with adherence to security best practices and maintaining the confidentiality, integrity, and availability of critical assets. Team #1 identified the following critical assets: PFSense Firewall. The particulars of the engagement are outlined further in the scope section of this report.

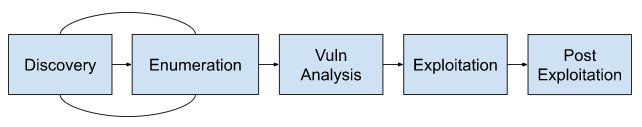
# **2.1 Scope**

Our firm worked closely with Team #1 management and the Technology Director, Vincent Nestler, to clearly define the scope of the engagement during the pre-testing phase. The engagement was stated to be an internal penetration test of two networks, conducted during active business operations between the hours of 12:00 and 11:30 from 11/13/23 - 11/19/23. The networks and corresponding IP ranges are outlined in the table below:

|  |  |  |
| --- | --- | --- |
| **Type** | **IP Range** | **Description/Systems** |
| DMZ | RANGE 1 | PFSense, Vyatta Router, Kali box |
| SubScreen | RANGE 2 | Database and Webserver |
| LAN | RANGE 3 | Vyatta Router, RHEL Client, Windows Client, AD-DNS |

# **2.3 Pentesting Methodology**

For our engagement we chose to abide by a modified version of the *Penetration Testing Execution Standard.* The modified standard chooses to disregard traditional methods like OSINT and focuses on network scanning. During the engagement, after a service or network device was first discovered it was helpful to further layer the initial information with more insightful scans. The more intensive scans targeted for specific services would provide important knowledge needed for vulnerability analysis and exploitation. Finally, after exploitation, post exploitation would be conducted to ensure every machine’s relevant information was captured successfully.



# **3. Metric Overview**

In an effort to properly communicate to the management of Team #1 the findings of the network security audit, a variety of metrics were used. Each metric detailed below, contributes to the categorizations and ranking of each vulnerability found.

# **3.1 CVSS Metric**

The Common Vulnerability Scoring System (CVSS) is a qualitative scoring system for vulnerability severity. The measure itself produces a score ranging from 0-10 depending upon a variety of different factors such as attack complexity and exploit maturity. The CVSS standard has been widely adopted across business, organizations, and governments as a way for ranking a particular vulnerability. By using the CVSS, we, as a penetration testing firm, are able to more accurately give advice in terms of what vulnerabilities to prioritize when it comes to remediation depending upon the threat posed to the organization and the resources the organization can allocate to handling aforementioned threats.

**CVSS SCORING v3.0**

|  |  |
| --- | --- |
| **SEVERITY** | **BASE SCORE RATING** |
| Critical | 9.0-10.0 |
| High | 7.0-8.9 |
| Medium | 4.0-6.9 |
| Low | 0.1-3.9 |

# **3.2z Remediation Prioritization Metric**

The Remediation Prioritization Metric is a tool designed to help organize TCC’s response to the results of the network security audit. The following metric can provide a playbook for recovery when combined with the remediation steps in the Findings section.

|  |  |
| --- | --- |
| **Remediation Priority** | **Description/Criteria** |
| Category - 4  (CAT - 4) | The finding has a critical CVSS score and high business impact.  Finding gives attackers arbitrary access to the underlying operating system or service. |
| Category - 3  (CAT - 3) | The finding has a high CVSS score and high impact on the business’s mission. The impact may result in system downtime, integrity of systems being corrupted, or confidentiality being broken. |
| Category - 2  (CAT - 2) | The finding has a medium impact on the immediate confidentiality, integrity, and/or availability of the business’s mission, but it isn’t detrimental. |
| Category - 1  (CAT -1) | The finding has a little to no impact on the immediate confidentiality, integrity, and/or availability of the business’s mission. |

# **3.4 MITRE ATT&CK Framework**

Throughout an ongoing incident, a malicious adversary takes a predefined path to achieve their goal. This malicious path can be mapped and documented through a matrix called the MITRE ATT&CK Framework. The MITRE ATT&CK Framework enables organizations to have insight into the depth and sophistication of an adversary. The matrix also allows for the use of a common language for expressing complex hacking techniques. Therefore, it was essential to leverage the MITRE ATT&CK Framework as a tool for our firm to categorize vulnerabilities.

# **3.5 OWASP**

The Open Web Application Security Project (OWASP) has been around since the end of 2001 and has been a staple of web security ever since. Like many other standards OWASP is dedicated to being a free and open source resource/non profit company dedicated to improving everybodies web security. OWASP has many materials regarding web security, but their best known project has been the OWASP Top 10. The OWASP Top 10 describes the most common and critical web vulnerabilities and is updated every couple of years. The current OWASP Top 10 (2021) is:

* Broken Access Control
* Cryptographic Failures
* Injection
* Insecure Design
* Security Misconfiguration
* Vulnerable and Outdated Components
* Identification and Authentication Failures
* Software and Data Integrity Failures
* Security Logging and Monitoring Failures
* Server-Side Request Forgery (SSRF)

Several of these vulnerability types were found during the engagement such as security misconfigurations and outdated components. The reason the OWASP Top 10 is so important is because it addresses a lot of the key design flaws in many web based systems. Had the various web apps been designed with the OWASP Top 10, the Web Security Testing Guide, or an equivalent standard in mind several of the vulnerabilities found by our form may have been eliminated.

# **4. Findings**

|  |  |  |
| --- | --- | --- |
| **Host: 172.16.0.1** | **Default Credentials for PostgreSQL** | **CVSS** |
| Risk | **Critical** | 9.2  Critical |
| Impact | **High** |
| Likelihood | **Very Likely** |

|  |  |
| --- | --- |
| MITRE ATT&CK | [T0812 - Default Credentials](https://attack.mitre.org/techniques/T0812/) |
| OWASP | [Security Misconfiguration](https://owasp.org/Top10/A05_2021-Security_Misconfiguration/) |
| Prioritization | CAT - 4 |

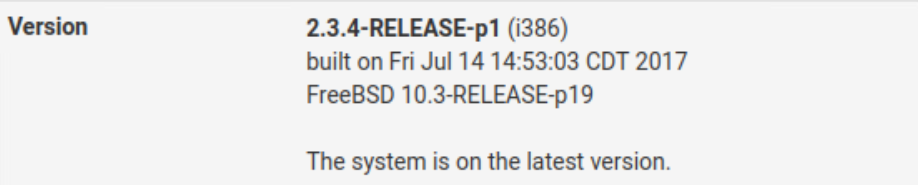
|  |
| --- |
| **Details** |
| Default credentials are the initial credentials present on a device, software, or service when very first created. These credentials are meant to act as placeholders while the system administrator updates these parameters. These default credentials are often public knowledge and widely available. |

|  |
| --- |
| **Replication** |
| During the active engagement our team managed to gain access to the PFSense firewall using default credentials  **Go to the 172.16.0.1 address found using netdiscover.**  Using the default credentials: USER: admin PASS: pfsense allowed us to login |

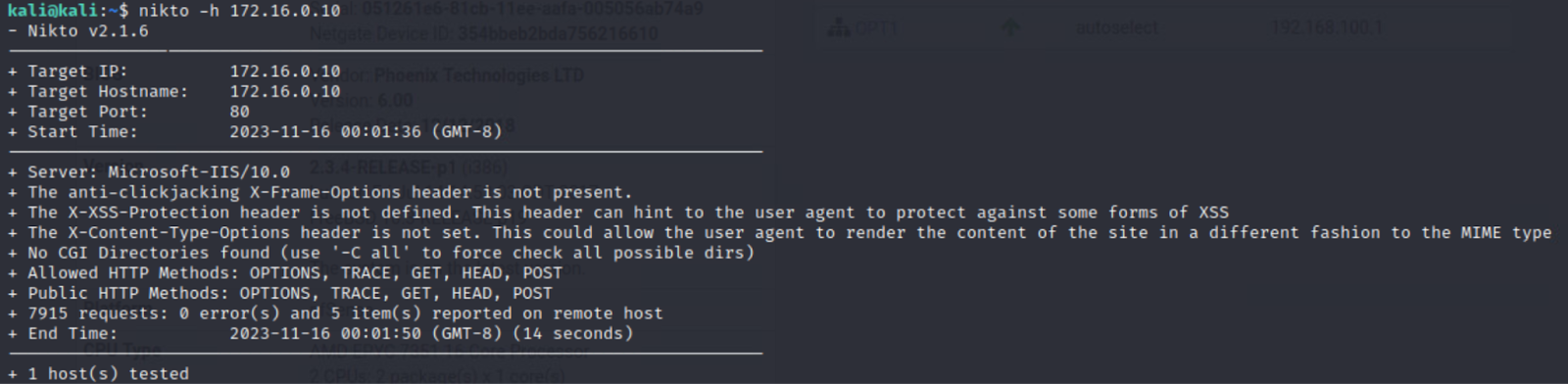
|  |
| --- |
| **Remediation** |
| System administrators must ensure that services are protected through proper password and access management. To accomplish this, administration shall log password changes. |

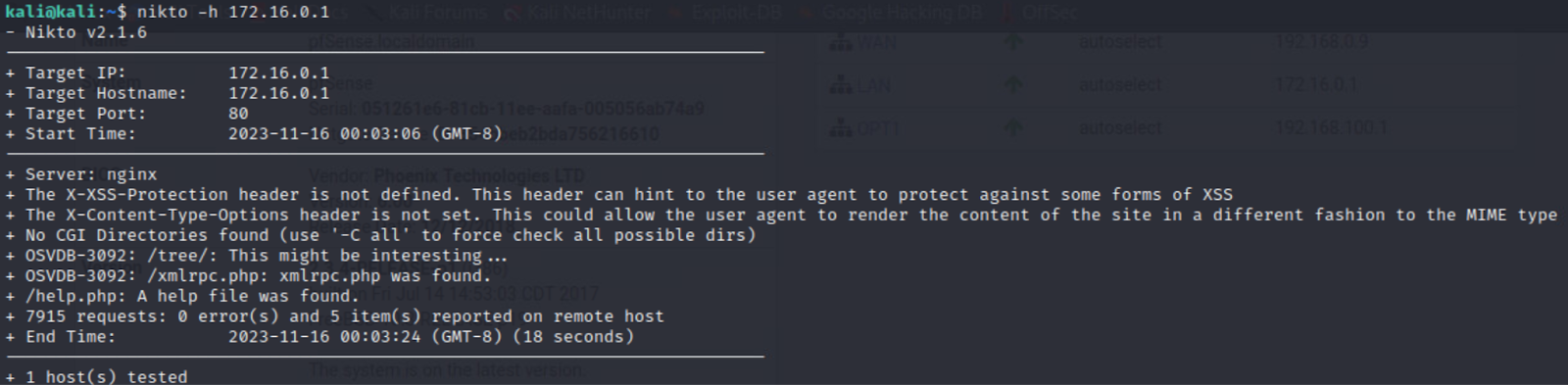
# **5. Potential Vulnerabilities**

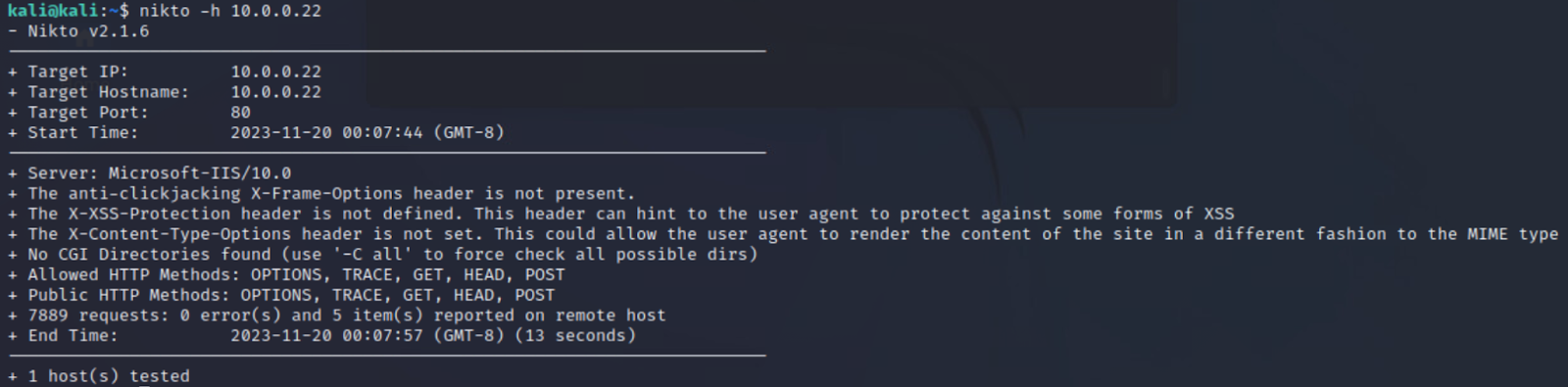
From this page we can gather that they are running PFSense 2.3.4



Running a nikto on 172.16.0.10 yielded this



Running a nikto on 172.16.0.1 yielded this

ran nikto on 10.0.0.22 to find 

# **5. Appendix of Tools**

|  |  |  |
| --- | --- | --- |
| **Tool Name** | **Purpose** | **Description** |
| [Nmap](https://github.com/nmap/nmap) | Enumeration | Port scanning, host enumeration |
| [Netdiscover](https://www.kali.org/tools/netdiscover/#:~:text=Netdiscover%20is%20an%20active%2Fpassive,used%20on%20hub%2Fswitched%20networks.) | Reconissance | an active/passive address reconnaissance tool, |
| [Nikto](https://cirt.net/Nikto2) | Vulnerability Scanner | web server scanner which performs comprehensive tests against web servers |