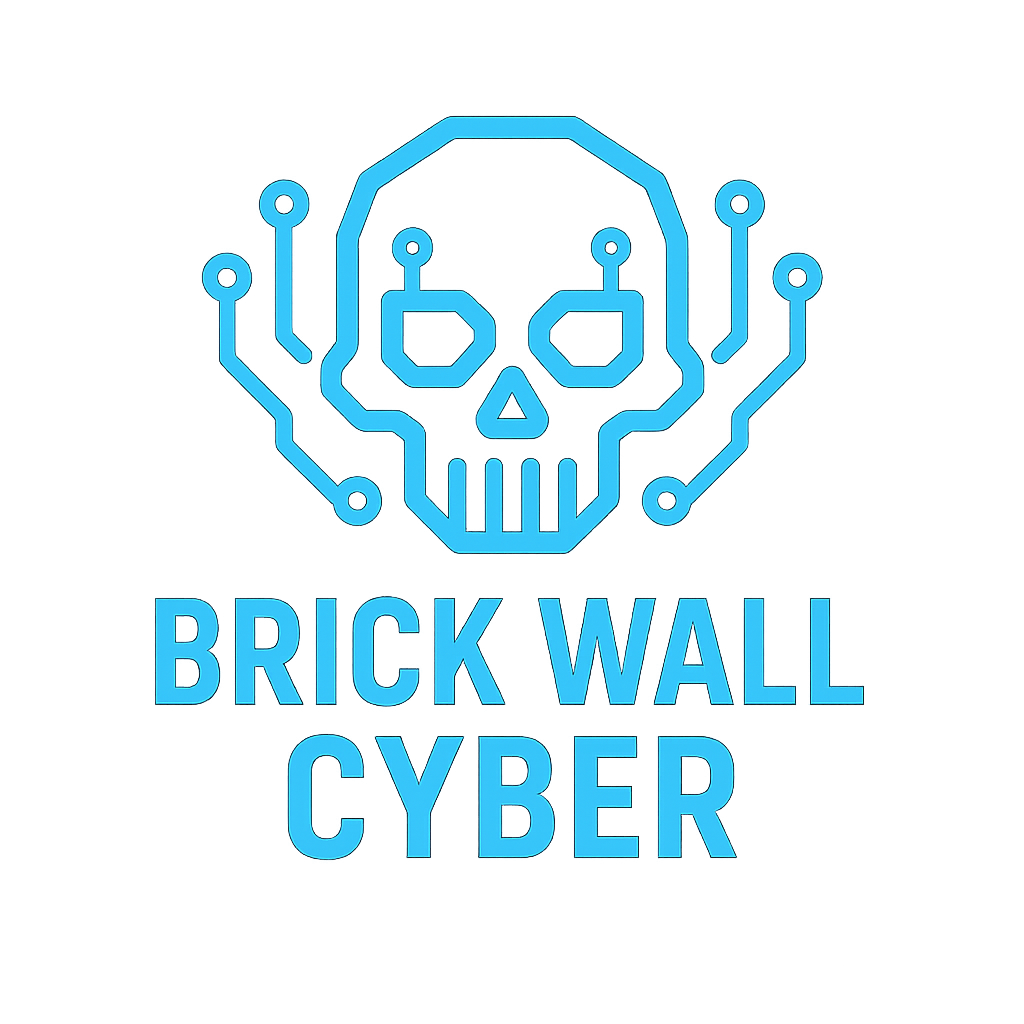
Vulnerability Assessment

**April 28th, 2025**



**Brick Wall Cyber**

**Security Assessment Team**

Nic Conine Principal Analyst

**Reggie Ashitey Security Analyst**

**Nic Conine Security Analyst**

**Brandon Pascucci Security Analyst**

**Sanjay Charitesh Makam Security Analyst**

Division of Responsibilities

**(Nic’s idea, you do not have to follow it) I think we can split this up fairly evenly. My idea is below**

Section 1: as it’s just a couple paragraphs of summaries basically i think only one person should do it as it’ll be simpler than splitting up paragraphs. So I can do Section 1 after we complete the report or someone else can.

Section 2: Someone should each do a different set. AKA one person do MICE, one do RASCL, one do Threat model.

Section 3: 3 out of the 4 members should each do 1 of the 3a and 3b. The final member should just do 3c. For example person a does 3.a1 and 3.b1 while person b does 3c

Section 4: each person does 4 ( put your name under it so we can keep track of who did what and who needs to do more)

In the boxes below in the contributions section everyone picks one thing from a section. I’ll put mine down as an example.

(I know for sections 2 there is only 3 so someone will get a “lucky break” so if you want you can split threat model into the 2 columns and then there is “4” mini parts)

(lastly put a date next to ur name that will represent when you expect to be done so we can hold each other accountable. Feel free to update the date as needed as well if you have to)

Nic wrote all of this so feel free to say anything in the discord or in this document if you think my idea of distribution can be improved.

| **Student** | **Expected Contributions** |
| --- | --- |
| Reggie Ashitey  (4/27) | * Filling out my four vulnerabilities with its information * 2.a.1 (“Threat Actor Motivations”) * 3.b.2, 3.b.3 * 4.h-k |
| Nicholas Conine  (4/24 end of day) | 2.RASCL  3.a1  3.b1  Section 3 is supposed to be done after section 4 but I put mine down after I finished my own section 4 elements as I noticed a definite theme. This is up to interpretation and I can change it if needed  4.a-d |
| Sanjay Makam | * I did section 2.a.2, 3.a, 4.e, 4.f, 4.g, 4.o, 4.p * I did index page |
| Brandon Pascucci  4.27 | 4.l-n  General formatting  Index page  Revising and editing grammatical errors |
|  |  |
| **Communication Plan** | |
| Discord Platform | |
| **Meeting Schedule** | |
| Meeting twice per week to discuss the progress on the project assignment | |

[**1. EXECUTIVE SUMMARY**](#_yspy8tt3f0xe) **6**

[**2. THREATS AND RISK**](#_1yssrot6jju1) **7**

[2.a Threat Assessment](#_omko7tmd8gqy) 7

[2.a.1 Threat Actor Motivations](#_a7dnmtyqkgno) 7

[2.a.2 Threat Model](#_dnnoakwbjrc1) 9

[2.b Risk Matrix](#_qtc51anu4pvv) 10

[2.c Prioritization Categories](#_ievzmkg8ce0u) 11

[**3. SUMMARY OF RESULTS**](#_68fj1tsn50jp) **12**

[3.a Key Findings](#_hjzukj352bu1) 12

[3.a.1](#_wfwwnqgz326d) Too Little User Authentication 12

[3.a.2](#_egcnjuxuadwn) Insufficient User Authentication Mechanisms 12

[3.a.3](#_ek2hkpq5ufcm) Flat Network Architecture 12

[3.b. Key Recommendations](#_qpegg82d2qw3) 12

[3.b.1](#_v5vhxjo08zjl) Multi-Factor Authentication 12

[3.b.2](#_27tabozgw2rw) Mandatory Authentication Layers 13

[3.b.3](#_6bc6rte41cuj) Deploy Internal Firewalls and Access Control Lists 13

[**4. VULNERABILITIES**](#_jw36m3731qa1) **14**

[4.a](#_sfc1wpum8fo3) Poor Password Requirements 14

[4.b](#_reub0yrj38je) Central User Authentication Vulnerabilities 14

[4.c](#_g7ll3ma111ce) Potential for Malpractice from Within 15

[4.d](#_majcqqfx0523) Outdated Systems 16

[4.e](#_gbwe8uyaxnmu) Lack of Network Segmentation 17

[4.f](#_8eyntjlm5mo4) Publicly Exposed Docker Services 17

[4.g](#_h7vavia7szi) Insecure Email Protocols + Weak Auth 18

[4.h](#_cpl0wmywvrvi) C2 Server Exposure 19

[4.i](#_5ogw5eotqt27) OpenVAS Scanner Exposure 19

[4.j](#_nn5dh98mlzwz) No Firewall Rules Between Subnets 20

[4.k](#_7tfwmi85r40l) DHCP and Root Access on Kali Linux Systems 21

[4.l](#_6510wk2bjfql) Administrative Permissions on Own Systems 21

[4.m](#_2439vmmb6ocv) OSSEC Update 22

[4.n](#_7hstzwlq6ukr) Use of SMBv1 23

[4.o](#_43dsu15qghm) Lack of Endpoint Detection and Response (EDR) Systems 23

[4.p](#_9kzerwkcu6nb) Misconfigured Cloud Storage Buckets 24

# 1. EXECUTIVE SUMMARY

The assessment made within this report is to enhance Brick Wall Cyber’s security mechanisms. The goal in our assessment is to point out clear holes in security that could lead to the loss of money or data within BWC’s infrastructure. We scoured across the available resources to analyze BWC’s network infrastructure, servers, hosts, and everything in between. Our assessment is successful in pointing out clear security hazards that must be fixed in order to keep the integrity of BWC intact.

We describe vulnerabilities in the system under 4 categories: Low Medium High Critical. In our assessment of BWC, we have found 8 Critical, 7 High, and 1 Medium vulnerabilities. You should address the vulnerabilities in accordance to their severity level. Critical first, then High, then finally medium. Failure to respond to Critical or High level vulnerabilities could result in serious damages to the operations of BWC.

Throughout our assessment of BWC, we encountered 3 main security concerns that repeated across the analysis. These 3 were as follows. First, there was too little User Authentication across BWC. Many servers that held resources that were easily exploited lacked any authentication to access. The lack of authentication in general leaves BWC open to attacks on valuable infrastructure. Second, when there was authentication it was very weak and was only one layer. As Well as very weak password policies where there were any. Finally, the network infrastructure is not segmented off. This leads to a flat design of the network, where it is very easy for attackers to cross different parts of the network. Therefore, allowing any attack to double or triple in its radius of servers affected.

After the assessment of BWC and identifying the 3 biggest threats. We listed 3 recommendations to those 3 threats that will help BWC mitigate and eliminate the threat of those 3 big security concerns. The first recommendation we made was to implement Multi-Factor Authentication (MFA). MFA will help create that second layer of protection against social engineering and phishing attacks. Making an MFA will need the user to verify their identity in 2 different ways that an attacker would struggle to get past. This is a simple thing to implement upon the already existing authentication there is. This will help strengthen the pre-existing authentication that is fairly weak. The next recommendation is Single Sign-On (SSO). SSO would help give authentication to places in BWC where authentication is vacant. This would allow the efficiency of workers as having no authentication but will not allow malicious actors to just wander into servers unchecked. SSO is just one login that grants access to multiple servers and would help strengthen the security of BWC while also strengthening the password policy as an employee would only need one strong password. SSO could be more taxing to implement, as you would have to implement the new SSO authentication system to almost all the servers. Finally, the last recommendation we make is to implement network firewalls and Access Control Lists (ACLs) to different segments of the network. ACLs and Firewalls would segment the network and not allow cross traffic to different networks without being checked first. This wouldn’t allow a breach on one server to spread to the rest of BWC like it could before. This would require a lot of effort to implement to each router and server on the network, as you would need to be very tedious and verify all servers work for employee activities while maintaining efficient workflow. It would require the most time and work but would easily be the most pivotal to protecting the BWC network.

# 2. THREATS AND RISK

## 2.a Threat Assessment

### 2.a.1 Threat Actor Motivations

| **Motivation** | **Relevance to Brick Wall Cyber** |
| --- | --- |
| Money | This motivation might have some relevance to BWC, as hackers might want to embezzle or take advantage of the monetary assets that BWC currently has. |
| Ideology | Since BWC is a cybersecurity firm that offers security services and pen testing, a potential threat actor might oppose the fact that this firm wants to protect clients in their infrastructure. So ideology has some relevance/severity to BWC. |
| Coercion | Unless there is a severe data leak and one of the employees inside BWC is trying to manipulate the company into making a tough decision, this motivation has little to no relevance to BWC. |
| Ego | This motivation has relevance to BWC as a threat actor might want to test how strong BWC’s defenses and security services are. Their strong sense of ego will try to put BWC to the test. |

| **Motivation** | **Relevance to Brick Wall Cyber** |
| --- | --- |
| Reciprocation | Reciprocation has little relevance or severity to BWC, as there are not many circumstances where BWC would make enemies or a situation where “payback” was necessary. The only reason Reciprocation would be relevant is if some hacker group was stopped by BWC and now wants “revenge” on BWC. |
| Authority | Authority could have some severity if BWC has government contracts and is defending some government or high priority infrastructure. If this is the case, then other governments or actors on behalf of other governments attacking BWC in an attempt to access this infrastructure would fall under the Authority category. |
| Scarcity | Scarcity would have little importance unless BWC was involved in defending a bank or some organization that protected resources. Then an attacker trying to breach BWC to get access to those resources could fall under scarcity. |
| Commitment / Consistency | Commitment is reasonable, as it could happen as a result of BWC defending a company that an entity or person thinks is morally or ideologically wrong. This can even go for BWC itself if they engage in activities that could go against people's morals. |
| Liking | Liking is unlikely unless a specific influencer, celebrity, or important person condemns BWC and then an attacker attacks BWC to gain likeness from that Person of Interest. |
| Social Proof | Social Proof can be more likely as if a separate Nation or group like anonymous condemns or inspires others to attack BWC for whatever reasoning those groups of interest provide. |

### 

### 2.a.2 Threat Model

| **Threat** | **High-level Mitigation** | **Importance for Brick Wall Cyber**  **(Low/Medium/High)** |
| --- | --- | --- |
| Spoofing | Implement strong authentication mechanisms such as Multi-Factor Authentication (MFA) and enforce strict identity verification on external-facing services. | High |
| Tampering | Use secure communication protocols (TLS 1.2+), integrity checks (hashing, digital signatures), and configuration management baselines. | High |
| Repudiation | Enable detailed logging and centralized log management. Implement non-repudiation techniques such as digitally signed transactions. | Medium |
| Information Disclosure | Encrypt data in transit and at rest. Harden servers against known vulnerabilities. Apply strict access controls and regular security audits. | High |
| Denial of Service | Deploy robust network firewalls, traffic filtering, rate limiting, and DDoS protection services for external-facing applications. | High |
| Elevation of Privilege | Apply the principle of least privilege across all systems. Conduct regular permission audits and patch privilege escalation vulnerabilities promptly. | Critical |

## 2.b Risk Matrix

| **RISK MATRIX** | | **THREAT IMPACT** | | | |
| --- | --- | --- | --- | --- | --- |
| **LIKELIHOOD** |  | **LOW** | **MEDIUM** | **HIGH** | **CRITICAL** |
| **RARE** | **Low** | **Low** | **Medium** | **Medium** |
| **UNLIKELY** | **Low** | **Medium** | **High** | **High** |
| **LIKELY** | **Low** | **Medium** | **High** | **Critical** |
| **VERY LIKELY** | **Low** | **Medium** | **Critical** | **Critical** |

## 

## 2.c Prioritization Categories

| **Mitigation Priority** | **Description** |
| --- | --- |
| **Immediate (Imme.)** | Finding has a critical business impact, likelihood, and risk. It damages the operation of the client.  Finding causes a direct violation of regulation, law, or compliance that applies to the client.  Finding leaks, Personally Identifiable Information, Sensitive Information, or information that can lead to further access to sensitive data.  Finding is related to previous indicators of compromise and suggests the occurrence of past cyberattacks. |
| **Short-term**  **(Short.)** | Finding has a high business impact, likelihood, and risk. It partially damages the operation of the client and has the potential for further exploitation.  Finding gives attackers direct access to a system or a service.  Finding allows the attackers to violate Confidentiality, Integrity, Availability of a system. |
| **Long-term**  **(Long.)** | Finding has a medium business impact, likelihood, and risk.  Finding is related to security misconfigurations which can lead to further potential attacks.  Finding allows attackers to partially violate Confidentiality, Integrity, Availability of a system. |
| **Eventual**  **(Evetl.)** | Finding has a low business impact, likelihood, and risk.  Finding is not following the best security practices.  Finding is a bug or an unintentional mistake that has little to no security implication. |

# 

# 3. SUMMARY OF RESULTS

## 3.a Key Findings

### 3.a.1 Too Little User Authentication

Throughout many programs, there seems to be not much user authentication. This could be a result of a desire to make logging in and managing work less complex, but as a tradeoff for easy accessibility it compromises security and leads to many holes for phishing, malware, and social engineering.

### 3.a.2 Insufficient User Authentication Mechanisms

Across multiple systems, there is a notable absence of multi-factor authentication (MFA) and a lack of enforced strong password policies. Centralized authentication servers and webmail services are particularly at risk, exposing the organization to phishing, credential stuffing, and privilege escalation attacks.

### 3.a.3 Flat Network Architecture

The current network setup lacks segmentation between critical assets and general employee workstations. This "flat" design makes lateral movement trivial once an initial compromise occurs. It severely undermines Brick Wall Cyber's ability to contain or isolate breaches, increasing the blast radius of any attack.

## 3.b. Key Recommendations

### 3.b.1 Multi-Factor Authentication

This can come in many forms, but just a simple two-factor authentication can easily stop many of these vulnerabilities. Also, just stricter requirements for authentication. Such as more complex passwords on emails and double or triple authentication on the centralized user authentication, as it takes only one successful breach on the central user authentication to get access to multiple or all services of BWC.

### 3.b.2 **Mandatory Authentication Layers**

Introduce Single Sign-On (SSO) with mandatory session timeouts and device verification mechanisms. This will reduce the complexity for users while significantly strengthening security against unauthorized access.

### 3.b.3 **Deploy Internal Firewalls and Access Control Lists (ACLs)**

Place firewalls and configure ACLs between network segments to restrict, monitor, and log inter-segment traffic. This will enhance the organization's ability to detect and respond to unauthorized access attempts quickly.

# 3.c. Response Plan

| **Mitigation Prioritization** | **Vulnerability** |
| --- | --- |
| **Immediate (Imme.)** | * Central User Authentication Vulnerabilities, Publicly Exposed Docker Services, Outdated Systems |
| **Short-term (Long.)** | * Poor Password Requirements, Lack of Network Segmentation, Insecure Email Protocols |
| **Long-term (Short.)** | * Potential for Malpractice from Within |
| **Eventual (Evetl.)** | * None Identified Yet |

# 

# 4. VULNERABILITIES

## 4.a Poor Password Requirements

| **Risk Analysis** | | **CVSS** | **Prioritization** |
| --- | --- | --- | --- |
| **Risk** | **High** | **8.8 High** | **Short.** |
| **Impact** | **High** |
| **Likelihood** | **Likely** |
| **Hosts Impacted** | Mail hosts in the DMZ subnet | | |

| **Description** |
| --- |
| The Mail host on the DMZ subnet passwords have a “minimum of 6 letters and must require upper/lower case.” This has no complex requirements for the password. This leaves the email accounts vulnerable to simply brute force attacks. If this exploit is performed on a higher ranking member in BWC and the email is compromised. Not only is any classified information that may be private and essential to clients now exposed. The now exploited email can be used to phish other members of BWC, and then leads to an infection of multiple computers across BWC. |

| **External References** |
| --- |
| <https://docs.google.com/spreadsheets/d/1vwUmK1Pnq63sa-mhXR17tNtHdy55WXxFwspHFEfVZqg/edit?gid=0#gid=0>  <https://www.first.org/cvss/calculator/3-0#CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H> |

## 4.b Central User Authentication Vulnerabilities

| **Risk Analysis** | | **CVSS** | **Prioritization** |
| --- | --- | --- | --- |
| **Risk** | **Critical** | **9.9 Critical** | **Imme.** |
| **Impact** | **Critical** |
| **Likelihood** | **Likely** |
| **Hosts Impacted** | Active Directory, File Server, NAT router, Employee workstations. | | |

| **Description** |
| --- |
| The central user authentication system is highly important to the functionality of BWC. If the central user authentication system is compromised, then several other systems and hosts are then compromised by proxy. There is no mention of Multi-Factor authentication, or password requirements. This is concerning as if you have a central user authentication system that allows access to multiple accounts it is a necessity to have both a strong password and good Multi-Factor authentication. It is clear that there is not enough security for a central user authentication system. |

| **External References** |
| --- |
| <https://docs.google.com/spreadsheets/d/1vwUmK1Pnq63sa-mhXR17tNtHdy55WXxFwspHFEfVZqg/edit?gid=896437154#gid=896437154>  <https://www.first.org/cvss/calculator/3-0#CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H> |

## 4.c Potential for Malpractice from Within

| **Vulnerability Name** | | **CVSS** | **Prioritization** |
| --- | --- | --- | --- |
| **Risk** | **High** | **5.5 Medium** | **Long.** |
| **Impact** | **High** |
| **Likelihood** | **Unlikely** |
| **Hosts Impacted** | File Server | | |

| **Description** |
| --- |
| The dangers of allowing every single user to read/write to every other group in BWC can be dangerous. While you do have to be a user in the system, we do not know how often the ACL is updated if at all. This means ex employees or even employees who were bought out can potentially introduce malware, phishing scam, social engineering, etc. While they cannot execute so the possibilities of an attack being extreme is low, there are still opportunities for an attack using read/write privileges. |

| **External References** |
| --- |
| <https://docs.google.com/spreadsheets/d/1vwUmK1Pnq63sa-mhXR17tNtHdy55WXxFwspHFEfVZqg/edit?gid=909989774#gid=909989774>  <https://www.first.org/cvss/calculator/3-0#CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:L/I:H/A:L> |

## 4.d Outdated Systems

| **Risk Analysis** | | **CVSS** | **Prioritization** |
| --- | --- | --- | --- |
| **Risk** | **Critical** | **9.0 Critical** | **Imme.** |
| **Impact** | **Critical** |
| **Likelihood** | **Likely** |
| **Hosts Impacted** | Active Directory, pfsense NAT router, DNS, Wordpress, SSH Jump, WWW, Mail. | | |

| **Description** |
| --- |
| All the hosts listed above are very old versions of the software they are running. The problem is that old versions do not have the current security defenses or capabilities. Making it very easy to breach and use malicious attacks on these systems. Failure to update and change these servers/systems to newer models will leave severe security holes open. Vital servers that allow BWC to run open to attack and can very easily be compromised |

| **External References** |
| --- |
| <https://docs.google.com/spreadsheets/d/1vwUmK1Pnq63sa-mhXR17tNtHdy55WXxFwspHFEfVZqg/edit?gid=896437154#gid=896437154>  <https://www.first.org/cvss/calculator/3-0#CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H>  [**https://docs.netgate.com/pfsense/en/latest/releases/versions.html**](https://docs.netgate.com/pfsense/en/latest/releases/versions.html)  [**https://releases.ubuntu.com**](https://releases.ubuntu.com)  [**https://www.ktchost.com/blog/centos-version-history/**](https://www.ktchost.com/blog/centos-version-history/) |

## 4.e Lack of Network Segmentation

| **Vulnerability Name** | | **CVSS** | **Prioritization** |
| --- | --- | --- | --- |
| **Risk** | **High** | **7.5 High** | **Short.** |
| **Impact** | **High** |
| **Likelihood** | **Likely** |
| **Hosts Impacted** | Internal network devices, Client-facing servers, Workstations across finance, HR, engineering | | |

| **Description** |
| --- |
| The network diagram shows minimal separation between critical servers, employee workstations, and client data systems. Flat networks dramatically increase risk: if an attacker breaches any internal device, they could easily pivot laterally to high-value targets like Active Directory or client databases. Lack of VLANs, internal firewalls, or segmented access controls magnifies exposure, making containment during incidents nearly impossible. |

| **External References** |
| --- |
| [NIST SP 800-125B: Secure Network Architecture](https://csrc.nist.gov/pubs/sp/800/125/b/final)  <https://www.cisa.gov/sites/default/files/publications/layering-network-security-segmentation_infographic_508_0.pdf>  <https://www.cyber.gc.ca/en/guidance/top-10-security-actions-no-5-segment-and-separate-information-itsm10092> |

## 4.f Publicly Exposed Docker Services

| **Risk Analysis** | | **CVSS** | **Prioritization** |
| --- | --- | --- | --- |
| **Risk** | **High** | **8.0 High** | **Imme.** |
| **Impact** | **High** |
| **Likelihood** | **Likely** |
| **Hosts Impacted** | Wordpress (10.0.0.9) | | |

| **Description** |
| --- |
| The Wordpress blog is containerized and publicly exposed with ports 80, 443, and 3306 open. Exposing the MySQL container externally is a significant risk. Default Docker networks are flat and can be exploited. Without hardened container isolation, an attacker gaining access to one container can break into the host or other containers. |

| **External References** |
| --- |
| <https://docs.docker.com/engine/security/>  <https://nvd.nist.gov/vuln/detail/CVE-2019-5736> |

## 4.g Insecure Email Protocols + Weak Auth

| **Risk Analysis** | | **CVSS** | **Prioritization** |
| --- | --- | --- | --- |
| **Risk** | **High** | **8.5 High** | **Short.** |
| **Impact** | **High** |
| **Likelihood** | **Likely** |
| **Hosts Impacted** | Mail (10.0.0.4) | | |

| **Description** |
| --- |
| The Mail server supports legacy protocols (SSL 2.0/3.0) and weak password policies. Combined, these make brute force and man-in-the-middle attacks feasible. The use of webmail (SquirrelMail) adds surface area for XSS or phishing exploits. This is critical for a security company that communicates sensitive data with clients. |

| **External References** |
| --- |
| <https://datatracker.ietf.org/doc/html/rfc8996>  <https://perception-point.io/guides/email-security/email-security-threats-solutions-8-critical-best-practices/> |

## 4.h C2 Server Exposure

| **Risk Analysis** | | **CVSS** | **Prioritization** |
| --- | --- | --- | --- |
| **Risk** | **Critical** | **9.8 Critical** | **Imme.** |
| **Impact** | **Critical** |
| **Likelihood** | **High** |
| **Hosts Impacted** | Kali Linux 2020.3 based system | | |

| **Description** |
| --- |
| The C2 server is used to maintain active reverse shells on compromised systems. Without network segmentation and access restrictions, if an attacker discovers the C2 server, they could hijack the command channels and potentially control not just compromised systems but launch new attacks internally or externally. For Brick Wall Cyber, an exposed C2 server is an existential risk during active pen-testing engagements. |

| **External References** |
| --- |
| <https://www.varonis.com/blog/what-is-c2>  <https://www.reflectiz.com/blog/c2-server/>  <https://www.extrahop.com/resources/attacks/c-c-beaconing> |

## 4.i OpenVAS Scanner Exposure

| **Risk Analysis** | | **CVSS** | **Prioritization** |
| --- | --- | --- | --- |
| **Risk** | **High** | **8.8 <High>** | **Short.** |
| **Impact** | **High** |
| **Likelihood** | **Medium-High** |
| **Hosts Impacted** | **OpenVAS Server (Ubuntu 20.04 system)** | | |

| **Description** |
| --- |
| OpenVAS is a vulnerability scanner capable of discovering network weaknesses. Without proper security controls (e.g., restricted access, updated software), an attacker could take over the OpenVAS server, gain detailed knowledge of Brick Wall Cyber’s systems, and exploit known vulnerabilities more easily. It represents a significant risk if compromised. |

| **External References** |
| --- |
| <https://hackertarget.com/openvas-scan/>  <https://www.cybrary.it/blog/vulnerability-assessment-using-openvas-first-scan> |

## 4.j No Firewall Rules Between Subnets

| **Risk Analysis** | | **CVSS** | **Prioritization** |
| --- | --- | --- | --- |
| **Risk** | **High** | **9.9 <Severe>** | **Imme.** |
| **Impact** | **Severe** |
| **Likelihood** | **High** |
| **Hosts Impacted** | Entire Sample Pen Test Client Network (pfSense NAT Router, OpenVAS, GoPhish, C2 Server, Kali Linux systems) | | |

| **Description** |
| --- |
| The pfSense NAT Router has no firewall rules in place to block access between different BWC subnets. This creates a flat network architecture, allowing an attacker who compromises one system to easily pivot and attack others. For Brick Wall Cyber, this drastically increases the potential impact of a breach, enabling a small compromise to become a full network-wide disaster. |

| **External References** |
| --- |
| <https://www.paloaltonetworks.com/cyberpedia/what-are-firewall-rules>  <https://www.portnox.com/cybersecurity-101/access-control-list-acl/>  <https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html> |

## 4.k DHCP and Root Access on Kali Linux Systems

| **Risk Analysis** | | **CVSS** | **Prioritization** |
| --- | --- | --- | --- |
| **Risk** | **Medium** | **8.5 <Severity>** | **Long.** |
| **Impact** | **Medium-High** |
| **Likelihood** | **Medium** |
| **Hosts Impacted** | All Kali Linux tester systems (dynamic IP assigned devices) | | |

| **Description** |
| --- |
| Kali Linux systems used by penetration testers are assigned IPs via DHCP and each tester has root access. Without static IP mapping or additional restrictions, a malicious actor could spoof a Kali system or intercept/modify network traffic easily. Brick Wall Cyber risks internal attacks or identity confusion among test systems, particularly during client engagements. |

| **External References** |
| --- |
| <https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/9/html/managing_networking_infrastructure_services/providing-dhcp-services_networking-infrastructure-services>  <https://www.techtarget.com/searchsecurity/feature/How-to-configure-and-customize-Kali-Linux>  <https://www.kali.org/docs/general-use/enabling-root/> |

## 4.l Administrative Permissions on Own Systems

| **Risk Analysis** | | **CVSS** | **Prioritization** |
| --- | --- | --- | --- |
| **Risk** | **High** | **9.8 <Severe>** | **Imme.** |
| **Impact** | **High** |
| **Likelihood** | **Unlikely** |
| **Hosts Impacted** | Any and/or all users based on last name and their systems | | |

| **Description** |
| --- |
| Users have administrative privileges on their own systems to install software and configure their own systems as needed. These administrative privileges can lead to malware installation, vulnerabilities created by misconfiguration of a system’s settings, and privilege escalation. These risks could lead to malware disruptions, data breaches, and ransomware attacks. All of this could be controlled by a central IT unit, but the privileges for each user would have to be reduced. Another possible solution is the least-privilege model. |

| **External References** |
| --- |
| [Administrator Permissions' Hidden Risks | Intellicomp](https://intellicomp.net/it-services-blog/hidden-perils-of-local-administrator-permissions/)  [Brickwall Cyber Infrastructure Description - Google Sheets](https://docs.google.com/spreadsheets/d/1vwUmK1Pnq63sa-mhXR17tNtHdy55WXxFwspHFEfVZqg/edit?gid=896437154#gid=896437154)  [The Risks of Excessive Admin Privileges – Frame Secure](https://framesecure.com.au/insights/essential-eight/the-risks-of-excessive-admin-privileges/)  [Poor Access Management: Top Security Risks and Mitigation Strategies](https://blog.netwrix.com/access-management-security-risks) |

## 4.m OSSEC Update

| **Risk Analysis** | | **CVSS** | **Prioritization** |
| --- | --- | --- | --- |
| **Risk** | **High** | **8.9 <High>** | **Imme.** |
| **Impact** | **High** |
| **Likelihood** | **Likely** |
| **Hosts Impacted** | BWC Client Systems | | |

| **Description** |
| --- |
| The current version of OSSEC on all of the BWC Client Systems is outdated. This needs to be updated to at least OSSEC version 3.8.0, but I recommend that they go to OSSEC Atomic 4.8.2 because of the added role based access control, malware protection, real time monitoring, and group agent management. The other issue is that all users are in control of their own downloads and system configuration, which could cause OSSEC to be misconfigured or tampered with, limiting its effectiveness. The role based access control would help combat this issue. |

| **External References** |
| --- |
| [Get OSSEC - OSSEC](https://www.ossec.net/ossec-downloads/)  [When the unexpected happens: FAQ — OSSEC](https://ossec-docs.readthedocs.io/en/latest/docs/faq/unexpected.html#:~:text=The%20IP%20address%20you%20configured%20the%20agent%20is,agent.%20Check%20if%20the%20IP%20address%20is%20correctly.)  [Brickwall Cyber Infrastructure Description - Google Sheets](https://docs.google.com/spreadsheets/d/1vwUmK1Pnq63sa-mhXR17tNtHdy55WXxFwspHFEfVZqg/edit?gid=1106036369#gid=1106036369) |

## 4.n Use of SMBv1

| **Risk Analysis** | | **CVSS** | **Prioritization** |
| --- | --- | --- | --- |
| **Risk** | **Critical** | **9.9 <Severe>** | **Imme.** |
| **Impact** | **Critical** |
| **Likelihood** | **High** |
| **Hosts Impacted** | File Server | | |

| **Description** |
| --- |
| The file server is compatible with SMBv1, which is a known security risk. SMBv1 does not have proper encryption, allows for remote execution of code, and facilitates the spread of malware. This was all showcased in the WannaCry ransomware attack. The compatibility of this may be important for other things the file server interacts with, but it is too risky to continue using and if something is not compatible anymore, it should also be updated. |

| **External References** |
| --- |
| [WannaCry explained: A perfect ransomware storm | CSO Online](https://www.csoonline.com/article/563017/wannacry-explained-a-perfect-ransomware-storm.html)  [Stop using SMB1 | Microsoft Community Hub](https://techcommunity.microsoft.com/blog/filecab/stop-using-smb1/425858)  [Brickwall Cyber Infrastructure Description - Google Sheets](https://docs.google.com/spreadsheets/d/1vwUmK1Pnq63sa-mhXR17tNtHdy55WXxFwspHFEfVZqg/edit?gid=909989774#gid=909989774) |

## 4.o Lack of Endpoint Detection and Response (EDR) Systems

| **Risk Analysis** | | **CVSS** | **Prioritization** |
| --- | --- | --- | --- |
| **Risk** | **Critical** | **9.3 Critical** | **Imme.** |
| **Impact** | **Critical** |
| **Likelihood** | **Likely** |
| **Hosts Impacted** | All employee workstations, internal servers, remote devices | | |

| **Description** |
| --- |
| Brick Wall Cyber currently lacks a deployed Endpoint Detection and Response (EDR) system across workstations and internal servers. Without EDR, advanced threats like fileless malware, insider threat activities, and persistent attack techniques can go undetected. Traditional antivirus solutions and firewalls are no longer sufficient in modern threat landscapes. The absence of EDR drastically reduces detection and rapid response capabilities, allowing attackers to dwell inside the network for extended periods without triggering alerts. |

| **External References** |
| --- |
| <https://attack.mitre.org/tactics/TA0005/> |

## 4.p Misconfigured Cloud Storage Buckets

| **Risk Analysis** | | **CVSS** | **Prioritization** |
| --- | --- | --- | --- |
| **Risk** | **Critical** | **9.6 Critical** | **Imme.** |
| **Impact** | **Critical** |
| **Likelihood** | **High** |
| **Hosts Impacted** | Cloud-hosted document repositories and backups | | |

| **Description** |
| --- |
| Several cloud storage buckets used for backup and document hosting are publicly accessible without authentication. These misconfigurations expose sensitive internal documentation, client reports, and configuration files to the public. Attackers could use this intelligence to craft highly targeted attacks, gain insight into internal systems, or directly exfiltrate valuable intellectual property. Particularly for Brick Wall Cyber, whose trust depends on safeguarding client data, this exposure represents a severe reputation and operational risk. |

| **External References** |
| --- |
| <https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-117a>  <https://cloud.google.com/storage/docs/access-control> |