Vulnerability Assessment

December 9, 2024

Brick Wall Cyber

Security Assessment Team

Kylee Kublin, Principal Analyst

Cooper Broll, Security Analyst

Kisakye Kirabo, Security Analyst

Division of Responsibilities

Student	Expected Contributions
Kylee Kublin	Executive Summary, Vulnerabilities e-l, Summary of Results b
Kisakye Kirabo	Threats and Risks a-c, Vulnerabilities m-p
Cooper Broll	Vulnerabilities a-d, Summary of Results a, Formatting
Communication Plan	
Communication will be occurring through our group chat, being able to ask questions and advise different team members on their sections if necessary.	
Meeting Schedule	
Dividing Initial Parts by 11/25, Final Group Meeting before submission 12/5 for review	

1. EXECUTIVE SUMMARY

Within Brick Wall Cyber, vulnerabilities and other weaknesses that are currently found within all systems are seen as perfect opportunities for attackers to exploit Brick Wall Cyber and gather money, sensitive data, and more. Motivations for attacks include money, ideology, coercion, ego, reciprocation, authority, scarcity, commitment/consistency, liking, and social proof. Within Brick Wall Cyber, money drives financial gain-driven attacks, while ideological differences may prompt attacks from those opposed to the company's beliefs. Coercion can occur if attackers are from rival firms seeking to steal clients. Ego motivates attacks from those seeking recognition for their technical skills, and authority may be targeted for personal revenge. Reciprocation can involve potential employees exploiting sensitive information, while commitment/consistency involves building trust with employees to gain access to data. Liking involves using propaganda for notoriety, and social proof seeks to damage the company's reputation. To prevent these risks, securing vulnerabilities and protecting sensitive data is essential.

There are currently 5 immediate vulnerabilities, 8 high vulnerabilities, 2 medium vulnerabilities, and 1 low vulnerabilities. Immediate issues include Windows 7 End-of-Life systems, lack of firewall rules, and privilege escalation, which expose outdated systems, enable data breaches, and grant full access to client data. High vulnerabilities involve Windows 8 End-of-Life systems, weak password policies, unautomated scans, local admin privileges, active reverse shell, and DHCP subnet issues, allowing internal attackers to alter security and access accounts. Medium vulnerabilities include outdated OSSEC 3.0.5 and ELK system misconfigurations, which could enable DoS attacks. The low vulnerability is the use of a standard baseline configuration with unnecessary restrictions.

Within the Brick Wall Cyber systems, we have found major vulnerabilities within the firewall systems, many other outdated systems, and the usage of potential privilege escalation. With the current firewall system, there are no firewall rules in place, creating ways for attackers to access vulnerabilities within a network and allow for attackers to move laterally throughout all the systems.Outdated systems lead to increased security risks and threats, with attackers being able to find holes to execute attacks. As for privilege escalation, internally or externally, attackers could use their privileges to access client data and have access to confidential systems.

It is recommended that Brick Wall Cyber configures a strict firewall, update software, and review all user privileges in order to eliminate vulnerabilities and prevent future attacks. By configuring a strict firewall with regular audits and patches, it would allow for the elimination of any unwanted vulnerabilities, be simply updated with vendor security patches, and be created by third party security teams. An update of software is extremely important since it will enhance performance and improve overall system stability, since newer versions of systems are more compatible with current compliance standards and allow for automated vulnerability management. Lastly, reviewing all user privileges, will only give those authorized access to sensitive data and reduce any future attacks, done with the tiers of PAM or an internal security team.

2. THREATS AND RISK

2.a Threat Assessment

2.a.1 Threat Actor Motivations

Motivation	Relevance to Brick Wall Cyber
Money	An attacker may use software such as ransomware, malware, phishing, or stealers to take employee/consumer information in return for money.
Ideology	An attacker may attack Brick Wall Cyber because they do not agree with the beliefs of the organization of its employees. It could be due to political reasons as well.
Coercion	An attacker could be from another rival company trying to take down Brick Wall Cyber and put their own company in the lead for potential consumers. Coercion could also involve financial gains as well.
Ego	An attacker may attack Brick Wall Cyber just to feel accomplished for using their technical abilities to attack a company and maybe even get recognition.

Motivation	Relevance to Brick Wall Cyber
Reciprocation	The attacker might first try to gain the trust of Brick Wall Cyber and potentially become an employee. This gets them closer to the system and they can be more exposed to sensitive information.
Authority	The attacker may be looking to attack a high-level official inside of Brick Wall Cyber or a client of Brick Wall Cyber who is a political figure.
Scarcity	An attacker makes a false sense of urgency that the servers are not working, potentially trying to

	manipulate the company into listening to their orders.
Commitment / Consistency	An attacker makes an employee feel comfortable sharing information with them through schemes such as phishing emails, online surveys, and bait-and-switch tactics.
Liking	An attacker might attack Brick Wall Cyber to get public notoriety and further an agenda they believe in. They could potentially use the Brick Wall Cyber to spread propaganda maybe through the website or even directly through client/employee personal devices.
Social Proof	An attacker could send lots of false bot reviews about Brick Wall Cyber and make the company look untrustworthy. This could be done by a rival company. They could also spread malware to clients of Brick Wall Cyber to ruin the company's credibility and help boost the business of other companies.

2.a.2 Threat Model

Threat	High-level Mitigation	Importance for Brick Wall Cyber (Low/Medium/High)
Spoofing	Avoid suspicious links and attachments, wary of unknown callers, strong passwords and two-factor authentication, regular software and network updates	High

Tampering	Multi-factor Authentication, Digital Signatures, Firewalls, Https usage, HMAC usage, Educate users	High
Repudiation	Digital signatures, strict access controls, detailed logging, multi-factor authentication	Medium
Information Disclosure	Strict access controls, data encryption, data masking, logging and monitoring, regular vulnerability assessments, input validation	High
Denial of Service	Network Layer Protection, Monitoring and Detection such as network traffic analysis and alerting systems, application layer protection and DDoS mitigation services	Medium
Elevation of Privilege	Strict access	High

	control, Monitoring for suspicious activity, Privileged account management such as multi-factor authentication, strong password policies	

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 Firewall Rules

The lack of firewall rules is an extreme risk to the entire company. It leaves the company extremely vulnerable to all sorts of attacks. Having no firewall rules is nearly the same as not having a firewall at all because traffic is not being limited or inspected. Malware, ransomware, and unauthorized access requests are able to freely enter the network and expose extreme amounts of information with ease. There is also no segmentation between networks in this system without the firewall rules being in place, meaning there is very limited security. The firewall and its rules are very basic and easy security systems that must be in place for a network to have even a base level of security. Without one, there is no real security realistically. There is no end to the amount of issues this lack could cause and the amount of attacks it would allow.

3.a.2 Outdated Systems

Many systems analyzed have outdated software which leads to increased security risks. Windows 7 and Windows 8 are still being utilized in the corporate subnet, which leads to serious security threats. Both of these are no longer supported by Microsoft, thus no longer receive security updates and are vulnerable to well-documented attacks. Windows 10 is also utilized, and while not outdated yet, it will stop receiving support in under a year in October 2025. Another outdated system is OSSEC 3.0.5, which is not up to date with the current stable release 3.0.6, or the development version 3.0.7. Using this outdated software could cause a lot of risks.

3.a.3 Severity and Privilege Escalation

Because of the setup of this network, there are multiple ways an attacker could gain access to a smaller part of the system, and quickly gain access to extremely sensitive data or information. Alternatively, threat actors could escalate their user privileges and gain access to much more vital systems, and make an insignificant attack an extremely dangerous one. The lenient password requirements on the email system could lead to one of these attacks, where an attacker could easily break a weak password in a variety of ways, then proceed to either gain sensitive information found in the mailbox or launch a phishing scheme to extract information from unsuspecting victims willing to trust internal mail. Otherwise, the existence of extremely loose allowances of local administrative access in the corporate subnet would allow for low-level attacks into low-level user systems to quickly gain access to far greater information than warranted to be accessible in this system. In the Kali Linux systems used for penetration testing, users have root access which—if gained access to by an attacker—could lead to serious security breaches as an attacker has full unrestricted control over the terminal. Finally, the active reverse shell—which grants attackers long-term access to compromised systems—could be used to slowly, methodically search for both vulnerable information and slowly gain privileges and access to more vital systems. With all of these weaknesses considered, privilege escalation and severity escalation are extreme risks and are likely to happen. If they remain in place, the smallest attack could become a very serious one.

3.b. Key Recommendations

3.b.1 Configuring A Strict Firewall With Regular Audits and Patches.

All systems interacting with private client data lack firewall regulations that expose the environment to unrestricted communication between subnets and potential data breaches. It is recommended that a strict firewall is set up, meaning that there will be very limited access rules and only essential traffic is let in and out a network (denying all, allowing specific approach). Since Brick Wall Cyber consistently deals with vulnerabilities and risks entering their networks, establishing a firewall that eliminates any unwanted vulnerability would be key to protecting their reputation and client data. This can be done by using a managed security service provider, dedicated IT consultants, cloud service providers with firewall management features, or other specialized firewall configuration companies. Also by installing regular audits and patches to this system, it would ensure that vulnerabilities are proactively identified and addressed. This is easily done by downloading and installing security patches to the firewall chosen once they are released by the vendor.

3.b.2 Update Software and Create Automated Vulnerability Scans

With all systems running on outdated versions of software and non-automated vulnerability scans that only occur on a quarterly basis, it is vital that all software is updated and done so regularly, in addition to creating automated vulnerability scans. By updating software across all systems within Brick Wall Cyber, it can improve security, enhance performance through bug fixes, give access to new features, have better compatibility with other systems, and increase overall system stability. By removing Windows 7 and 8, it would be vital to replace it with Windows 11 or 10 to have the newest features and replace OSSEC 3.0.5 with OSSEC 3.6.0 to prevent any further vulnerabilities. As for automatic vulnerability scans, it will significantly reduce the time and effort

needed to identify security weaknesses, proactively do threat detection, have cost savings, and facilitate compliance with security standards. This can be done with Nessus, OpenVAS, Rapid7, Nmap, and other automated vulnerability management software.

3.b.3 Review User Privileges and Create A Privileged Access Manager

It is recommended that all user privileges are re-evaluated and that there is an immediate stop to potential privilege escalation when performing penetration tests, done by introducing a privileged access manager. It is vital that users do not have access to administrative privileges, and that it is limited since local administrative rights can disable antivirus, install malware, encrypt data, and move laterally within a network. By reviewing user privileges, it would ensure that only those authorized within a system have access to sensitive data and that any potential attack risk can be limited. Also by introducing a privileged access manager, it can reduce security risks by controlling privileged access to systems, detecting and preventing potential security breaches, along with minimizing insider threats. This can be done with software that includes tiers of PAM or through an internal security team.

3.c. Response Plan

Mitigation Prioritization	Vulnerability
Immediate (Imme.)	• Windows 7 End-of-Life Systems • Lack of Firewall Rules • Privilege Escalation • Outdated WordPress Version • Outdated Docker Version
Short-term (High)	• Windows 8 End-of-Life Systems • Weak Password Requirements • Unautomated Vulnerability Scans • Local Administrative Privileges • Active Reverse Shell • DHCP Subnet

	• DNS Amplification Attacks
Long-term (Medium)	• OSSEC 3.0.5 • Remotely configuring with ELK
Eventual (Low.)	• Standard Base-Line Configuration • Mail Server

4. VULNERABILITIES

4.a Windows 7 End-of-Life Systems

Risk Analysis		CVSS	Prioritization
Risk	**High**	**8.7** **<Severity>**	**Imme.**
Impact	**High**		
Likelihood	**High**		
Hosts Impacted	All systems running Windows 7 in the corporate subnet.		

Description
Windows 7 is a system no longer supported by Microsoft, as of January 14, 2020, and no longer receives any updates. This importantly includes security updates, meaning there is a myriad of highly dangerous exploits such as CVE-2020-0796 which allows remote code execution and privilege escalation. This outdated software is a critical vulnerability in the subnet.

External References
- Microsoft End of Support - NIST CVE-2019-0708 - NIST CVE-2020-0796

4.b Windows 8 End-of-Life Systems

Risk Analysis		CVSS	Prioritization
Risk	**Medium**	**7.0** **<Severity>**	**High**
Impact	**Medium**		
Likelihood	**Medium**		
Hosts Impacted	All systems running Windows 8 in the corporate subnet.		

Description
As of January 10, 2024, Windows 8 is no longer supported or receiving updates from Microsoft. Importantly, this extends to vital security updates, meaning there are no more patches that will happen, even if there are extreme security breaches. However, due to multiple years of updates, there are fewer security risks than Windows 7. There aren't any well-documented risks right now, but the simple fact that there are two entirely new versions of Windows (10 and 11) with new security shows that 8 is outdated.

External References
- Microsoft End of Support

4.c Lack of Firewall Rules

Vulnerability Name		CVSS	Prioritization
Risk	**High**	**8.5** **<Severity>**	**Imme.**
Impact	**High**		
Likelihood	**High**		
Hosts Impacted	All systems in the MSSP client network.		

Description

There is a lack of firewall rules in the MSSP client network which exposes the environment to unrestricted communication between subnets, which would allow a hacker who has gained access to laterally move through systems. Gaining access to one system in this subnet would likely allow access into all other systems with ease. This unrestricted access could create extreme data breaches, privilege escalation, and other network exploits.

External References
- Total Compliance Training Firewalls - Paloalto Networks Firewall Rules - Fortinet Lateral Movement

4.d Weak Password Requirements

Risk Analysis		CVSS	Prioritization
Risk	**High**	**8.2** **<Severity>**	**High**
Impact	**High**		
Likelihood	**High**		
Hosts Impacted	Mail server and all user accounts accessing email.		

Description
The current password policy is very weak with only six letters and lowercase and uppercase letters required. Passwords should be required to be at least twelve (if not even higher, sixteen is much better), and have a mix of letters, numbers, and symbols. Attackers could gain access to accounts with weak passwords, gain access to sensitive information, and launch phishing schemes. Without change, this weak security poses a significant threat.

External References
- Microsoft Create and Use Strong Passwords - CISA Password Requirements

4.e Unautomated Vulnerability Scans

Risk Analysis		CVSS	Prioritization
Risk	**High**	**7.5** **<Severity>**	**High**
Impact	**High**		
Likelihood	**Medium to High**		
Hosts Impacted	All Brick Wall Cyber Client Systems		

Description
Through the internal IT/Ops system and on the OpenVAS host, there are only quarterly vulnerability scans done on all Brick Wall Cyber systems. Vulnerability assessments involve scanning and analyzing systems for known vulnerabilities, misconfigurations, and weaknesses. Using assessments such as the VAPT (Vulnerability Assessment and Penetration Testing) assessment on an automated basis can help identify weaknesses.

External References
- Scytale- VAPT in Cybersecurity

4.f Local Administrative Privileges

Risk Analysis		CVSS	Prioritization
Risk	**High**	**8.1** **<Severity>**	**High**
Impact	**High**		
Likelihood	**High**		
Hosts Impacted	All user systems.		

Description

Found on the corporate subnet, by giving users administrative privileges on their own systems to install software and configure their own systems, it gives each user full control of company files, directories, services, and other resources on local devices. Although it allows the organization to spend less time and money establishing user roles, an attacker could take control of any or all local resources and data at any time, exposing the network to malware, etc.

External References
- Local Admin Privileges- Double Edged Sword - Microsoft- Local Admin

4.g Privilege Escalation

Risk Analysis		CVSS	Prioritization
Risk	**High**	**9.0** **<Severity>**	**Imme.**
Impact	**High**		
Likelihood	**Medium**		
Hosts Impacted	On Kali Linux but access to client systems.		

Description
By having root access on Kali Linux for even just penetration testing, it could lead to privilege escalation, where an attacker can discover and exfiltrate sensitive data from the Linux that is in direct contact with clients. With this ability to gain initial access to a limited or full shell of a basic client, they could gain access to the root user and then have ultimate control over all systems in the client basis.

External References
- Linux Privilege Escalation

4.h Active Reverse Shell

Risk Analysis		CVSS	Prioritization
Risk	**High**	**7.5** **<Severity>**	**High**
Impact	**High**		
Likelihood	**High**		
Hosts Impacted	All successfully hacked systems (including users).		

Description
An active reverse shell allows for an attacker to maintain access to a compromised system over an extended period of time. By keeping this open on successfully hacked systems, it could allow an attacker full unauthorized remote access to systems that contained sensitive information and for the attacker to potentially steal/modify data, inject malware, or escalate access within former client's networks (creating disloyalty and mistrust for the company).

External References
- Reverse Shell Attacks - Persistent Reverse Shell

4.i OSSEC 3.0.5

Risk Analysis		CVSS	Prioritization
Risk	**High**	**6.9** **<Severity>**	**Medium**
Impact	**High**		
Likelihood	**Medium**		
Hosts Impacted	All BWC Client Systems and Windows Systems		

Description
OSSEC provides a simplified centralized management server to manage policies across multiple operating systems. This specific version has potentials for vulnerabilities since it is an older version, leaving room for unpatched bugs and other critical vulnerabilities. With it also being an older version, there is a large potential for attackers to find weaknesses, specifically DoS attacks or log injections.

External References
- OSSEC. - Denial of Service Attack on OSSEC

4.j Standard Base-Line Configuration

Risk Analysis		CVSS	Prioritization
Risk	**Medium**	**N/A** **<Severity>**	**Low**
Impact	**Medium**		
Likelihood	**Low**		
Hosts Impacted	All new BWC systems		

Description
Utilizing a baseline configuration is beneficial for initially ensuring that user and device configuration settings are compliant with the baseline settings. However, this is not tailored to specific hardware, software, or operational needs within different systems within an organization. Therefore, there may be unnecessary restrictions or vulnerabilities that come to light with the user being hindered from productively solving them.

External References
- Microsoft- Security Baselines - Base-line Standards

4.k DHCP Subnet

Risk Analysis		CVSS	Prioritization
Risk	**High**	**7.6** **<Severity>**	**High**
Impact	**High**		
Likelihood	**Medium**		
Hosts Impacted	All user systems		

Description
All user systems within the employee workstation work off of the DHCP subnet, which has the potential to be attacked by rogue DHCP servers, machine-in-the-middle attacks, DHCP starvation, spoofing, relay attacks, and scripting vulnerabilities. This is due to unauthorized devices gaining access to this shared IP address and therefore being able to spread different forms of attacks until they find success.

External References
- DHCP Servers. - NIST- DHCP attack

4.l Remotely configuring with ELK

Risk Analysis		CVSS	Prioritization
Risk	**Medium**	**6.8** **<Severity>**	**Medium**
Impact	**High**		
Likelihood	**Medium**		
Hosts Impacted	All Client Systems		

Description

There are possibilities for attackers to gain unauthorized access, potentially viewing or modifying sensitive log data. This can lead to brute-force attacks on weak or default credentials, cross-site scripting, or privilege escalation if roles are not properly defined or restricted. Also with its ability to log data, there could be potentials for attackers to inject or manipulate logs before they are indexed by ELK.

External References
- Elastic- Potential Remote Code Execution - Stack- Elastic Vulnerabilities

4.m DNS Amplification Attacks

Risk Analysis		CVSS	Prioritization
Risk	**High**	**7.5** **<Severity>**	**High**
Impact	**High**		
Likelihood	**Likely**		
Hosts Impacted	pfSense NAT Router Port 53		

Description
If the DNS server is not configured to respond only to legitimate requests (i.e., using access control lists or IP whitelisting), it could be used in DNS amplification attacks. Malicious actors can exploit open DNS resolvers to amplify DDoS attacks. If the DNS server isn't configured with proper security settings (e.g., DNSSEC), attackers might be able to poison the DNS cache with malicious data.

External References
- NIST Cybersecurity Framework - DHCP Servers What Is DNS - How to prevent DDoS

4.n Mail Server

Risk Analysis		CVSS	Prioritization
Risk	**High**	**8.2** **<Severity>**	**High**
Impact	**Likely**		
Likelihood	**High**		
Hosts Impacted	pfSense NAT Router Port 25 and Mail		

Description
Exposing port 25 (used for sending mail) could allow attackers to exploit the server for spam or email spoofing unless proper SMTP authentication and anti-relay measures are in place. The mail server could have vulnerabilities that could lead to email interception or remote code execution. Attackers might also exploit weak or default credentials.

External References
- NIST Cybersecurity Framework - Enable or disable SMTP (Microsoft) - What is SMTP Authentication

4.o Outdated Docker Version

Risk Analysis		CVSS	Prioritization
Risk	**Critical**	**9.0** **<Severity>**	**Imme.**
Impact	**High**		
Likelihood	**Very Likely**		
Hosts Impacted	Wordpress		

Description
Docker 18.04 is quite old (released in April 2018) and may contain known vulnerabilities that have been patched in later releases. Docker regularly releases security updates to address bugs, performance issues, and vulnerabilities. Also, Docker containers are often run with default configurations that can pose risks, such as default network settings, insecure image pulling, or lack of resource limits (e.g., CPU and memory limits).

External References
- Docker Security Announcements - What are container? - Introduction to containers and docker - Docker Container Security

4.p Outdated WordPress Version

Risk Analysis		CVSS	Prioritization
Risk	**Critical**	**8.7** **<Severity>**	**Imme.**
Impact	**Critical**		
Likelihood	**Likely**		
Hosts Impacted	WordPress		

Description
WordPress 5.2.2 was released in May 2019. Since then, numerous security patches have been released. Using an outdated version increases the likelihood of known vulnerabilities being exploited. Common security issues in older WordPress versions are Cross-Site Scripting (XSS), SQL Injection, Remote Code Execution (RCE), and File Inclusion vulnerabilities.

External References
- WordPress - CAPEC-310 OWASP 2021-A6 - Vulnerable WordPress Version