June 13, 2025

Prepared for Very Good Security

Full-Scope Penetration Test

Project	Version
Ethical Hacking Report Deliverable	1.0

Table of Contents

1.0 Executive Summary

On June 13, 2025, NetWorks Group (NWG) completed a comprehensive Penetration Test for Very Good Security (VGS). The objective of the test was to evaluate VGS's security stance by simulating how a potential attacker could gain unauthorized access to critical assets, data, logs, and sensitive information. This report summarizes the test results and provides recommendations to align with security best practices and regulatory requirements.

NWG's testing approach replicates the tactics used by various real-world threat actors, such as cybercriminals, nation-states, insiders, and opportunistic attackers. These actors often exploit vulnerabilities through stolen credentials, social engineering, phishing attacks, application flaws, and misconfigurations. To account for different access points, NWG tests from both an unauthenticated and assumed-compromised perspective. The report's **Section 5.0** highlights the individual vulnerability findings for VGS.

In addition to identifying vulnerabilities, NWG assesses an organization's detection and response capabilities. A lack of detection capability can also be considered a weakness. The report's **Section 3.0** covers these observations.

POSITIVE EFFORTS

- External systems are minimal and well-secured.
- Internal segmentation is effective, with no vault hosts or services identified from “genpop”.
- Internal detections and monitoring are timely and accurate.
- Excellent cyber hygiene practices are evident.

1.1 Threat Models

Unauthenticated Attacker

According to a recent Verizon study, 81% of cyber-attacks are initiated remotely[1]. Attackers aim to obtain sensitive information and compromise public systems to gain control over an organization's assets. To simulate real-world scenarios, NWG starts its penetration tests by identifying the organization's public presence, checking for any existing breaches, and examining public systems for potential vulnerabilities. NWG then carries out simulated attacks without prior knowledge or access to the organization. Measuring risk from this perspective clearly explains an organization's public security posture and highlights the areas that need improvement.

Public Compromise Risk for VGS	**LOW RISK**

Authenticated Attacker

NWG's "Assumed Compromise" tests simulate an attacker who has already gained access to an organization's assets. This is a crucial scenario to consider, as the IBM "Cost of a Data Breach" report revealed that in 2024, 16% of breaches analyzed began with compromised credentials[2], and another 7% were initiated by a malicious insider who had already been granted access. With the rapidly evolving threat landscape and the constant presence of zero-day vulnerabilities, organizations must clearly understand their post-compromise security posture. By measuring risk from this perspective, organizations can better defend against potential threats and protect their critical assets.

Assumed Compromise Risk for VGS	**LOW RISK**

[1] Verizon 2025 Data Breach Investigations Report retrieved from https://www.verizon.com/business/resources/T8f3/reports/2025-dbir-data-breach-investigations-report.pdf.
[2] IBM 2024 Cost of a Data Breach Retrieved from https://www.ibm.com/reports/data-breach.

1.2 Risk by Domain

The following scores represent NWG's best estimate of VGS's risk within individual domains. Risk is calculated based on the severity of individual findings in each domain, documented in **Section 5.0 - Matters Requiring Attention**.

External Network	**LOW RISK**

NWG only identified one low-risk finding on the external systems in scope.

Internal Network	**LOW RISK**

Only one internal vulnerability was identified. The CDE is well segmented and monitored for security events.

Detection & Response	**LOW RISK**

Attacks on the internal network were quickly identified and responded to. VGS demonstrated the ability to see NWG's terminal from the jumpbox when attacks occurred and additionally identified NWG's host OS that was tunneling traffic through the jumpbox. Attacks were detected on the network level, the host level, and even by a honeypot. NWG was impressed by the speed and capabilities of VGS's detections during this engagement.

1.3 Compromise Impact

The Full-Scope Penetration Test offers a comprehensive examination of the methods a potential attacker may employ to gain unauthorized access to VGS's assets and the areas they are likely to target. The test results are then used to identify potential areas of vulnerability and to assess the impact of a potential compromise on VGS.

By analyzing real-world threat actors' tactics, techniques, and procedures, NWG can accurately simulate various attack scenarios and determine the potential consequences of a breach. This includes the risk of sensitive company data being accessed, altered, or exfiltrated and possibly compromising the organization's security posture and critical systems.

This report's test results and recommendations are intended to help VGS make informed decisions about its security and implement best practices and compliance measures to better defend against potential threats. By taking a proactive approach to security, organizations like VGS can reduce the risk of a breach and protect their valuable assets.

2.0 Attack Methodology

NWG follows a standardized and structured approach while conducting penetration tests that align with the best practices defined by the National Institute of Standards and Technology (NIST). This methodology considers typical steps a malicious attacker would undertake to compromise a system or network. Following this standard methodology, NWG can thoroughly assess an organization's security posture, evaluate potential risks and vulnerabilities, and make relevant recommendations. The methodology is divided into several phases, each crucial in evaluating the organization's security. These phases include a comprehensive network infrastructure assessment, identifying security gaps, and assessing the organization's ability to detect and respond to an attack. The methodology also includes executing simulated attacks to test the organization's defense mechanisms and identify key assets and sensitive information that an attacker could target.

RECON	NWG collected publicly available information, including employee names and email addresses.
SCAN	NWG scanned the external scope for available services and applications, identifying possible entry points. External scope was limited to a few web services, proxies, and SSH services.
BREACH	NWG was unable to breach the external perimeter, and was provisioned two test systems internally by VGS to continue the testing.
PRIVILEGE ESCALATION	NWG was unable to escalate privileges during this engagement.
LATERAL MOVEMENT	No lateral movement was achieved during this engagement. NWG confirmed that the “genpop” environment is unable to access any hosts or services in the CDE ranges.
EXFILTRATION	Exfiltration of sensitive data was not conducted.

3.0 Detection

The following table categorizes various attack activities conducted by NWG with observed ratings for detection by VGS. The activities listed below represent detectable activities during the penetration test. NWG does not grade based on the difficulty of detection. For more information on detection ratings, see **Appendix B - Definitions**.

DOMAIN	ACTIVITY	DETECTION
EXTERNAL	Port Scanning	None
	Fingerprinting and Enumeration	None
	SSH User Enumeration	None
INTERNAL	Default Credential Enumeration	Fast
	Network Scanning	Fast
	Local Privilege Escalation Attempts	Fast
	Segmentation Testing Activities	Fast

Table 1: Attack Detection

4.0 Attack Narrative

4.1 External

NWG began the engagement by enumerating the external attack surface and associated public-facing infrastructure. This included scanning for exposed ports and services, misconfigurations, and known vulnerabilities. NWG also searched the dark web for exposed credentials and other leaked information from historical data breaches. NWG collected this information and compiled a list of possible usernames, passwords, and phone numbers.

The external scope for this assessment was limited to a few hosts, with minimal services available. Most were web services or web proxies that were configured with authentication or had no available content to test.

SSH services were identified externally on txt.live.verygoodproxy.com. While NWG was unable to gain access, weak encryption ciphers are supported. NWG recommends removing support for these ciphers to ensure better protection for data in transit.

```
[*] [2025.06.04-12:42:16] 15.197.254.86 - Server Information and Encryption
================================

  Type                    Value                                  Note
  ----                    -----                                  ----
  encryption.compression  none
  encryption.compression  zlib
  encryption.compression  zlib@openssh.com
  encryption.encryption   chacha20-poly1305@openssh.com
  encryption.encryption   aes128-ctr
  encryption.encryption   aes192-ctr
  encryption.encryption   aes256-ctr
  encryption.encryption   aes128-gcm@openssh.com
  encryption.encryption   aes256-gcm@openssh.com
  encryption.encryption   aes128-cbc                             Deprecated
  encryption.encryption   aes192-cbc                             Deprecated
  encryption.encryption   aes256-cbc                             Deprecated
  encryption.hmac         hmac-sha2-256-etm@openssh.com
  encryption.hmac         hmac-sha2-512-etm@openssh.com
  encryption.hmac         hmac-sha1-etm@openssh.com
  encryption.hmac         hmac-sha2-256
  encryption.hmac         hmac-sha2-512
  encryption.hmac         hmac-sha1
  encryption.host_key     rsa-sha2-512
  encryption.host_key     rsa-sha2-256
  encryption.host_key     ssh-rsa
  encryption.key_exchange curve25519-sha256
  encryption.key_exchange curve25519-sha256@libssh.org
  encryption.key_exchange curve448-sha512
  encryption.key_exchange ecdh-sha2-nistp521
  encryption.key_exchange ecdh-sha2-nistp384
  encryption.key_exchange ecdh-sha2-nistp256
  encryption.key_exchange diffie-hellman-group-exchange-sha256
  encryption.key_exchange diffie-hellman-group18-sha512
  encryption.key_exchange diffie-hellman-group17-sha512
  encryption.key_exchange diffie-hellman-group16-sha512
  encryption.key_exchange diffie-hellman-group15-sha512
  encryption.key_exchange diffie-hellman-group14-sha256
  encryption.key_exchange ext-info-s
  encryption.key_exchange kex-strict-s-v00@openssh.com
```

Figure 1: Weak SSH Encryption Ciphers

4.2 Internal

NWG began internal testing using jumpboxes within both [redacted] environments. These systems were provisioned by VGS in order for internal testing to occur. These systems required explicit source IP address permissions, in addition to SSH-key and password authentication to be able to access.

From the [redacted] jumpbox, NWG proceeded to enumerate available services and identified multiple SSH and various web-related services. Many of the services didn't appear to respond to attempts at enumeration and would often simply close connections after a few seconds.

Of the web applications that did respond, NWG identified login pages for a Palo Alto system and Keycloak. Attempts to authenticate to these services were detected by VGS. If the Palo Alto administration interface is not required to be available to systems similar to the jumpbox used by NWG, VGS should consider further isolating it. This would further reduce available attack surface to sensitive systems, even within the CDE.

An outdated version of tinyproxy was in use within the CDE. This version of tinyproxy is reported to be vulnerable to a remote code execution vulnerability (CVE-2023-49606), but NWG was unable to exploit it during the time of this engagement. There is a new version available which patches this vulnerability. NWG recommends that VGS review these services for opportunities to upgrade them.

```
host            port  info
----            ----  ----
                8888  tinyproxy/1.11.1 ( Via-1.1 tinyproxy (tinyproxy/1.11.1) )
                8888  tinyproxy/1.11.1 ( Via-1.1 tinyproxy (tinyproxy/1.11.1) )
                8888  tinyproxy/1.11.1 ( Via-1.1 tinyproxy (tinyproxy/1.11.1) )
```

Figure 2: Outdated Tinyproxy Services

Throughout the engagement, VGS was alerted to several activities taken by NWG. Had this been a real incident, VGS would have quickly isolated and disabled the system before reviewing additional event history to understand the threat and root cause.

4.3 Segmentation Testing

NWG reviewed the CDE ranges in scope from both jumpboxes. From the [redacted] jumpbox, no systems or services were available. ICMP, TCP, and UDP scans were performed in an attempt to identify systems. This highlights the effective segmentation in place for VGS's CDE.

5.0 Matters Requiring Attention

This section details specific problems that may increase the likelihood of a successful compromise. These items are often security best practices that the tester has directly observed, facilitated some compromise, or combined. These are consultative measures and are prioritized remediation guidelines to direct overall security strategy when reviewing this report. A detailed explanation of NWG scoring can be found in Appendix B. NWG has identified the following MRA's.

5.1 Outdated Tinyproxy Installation

Domain	**Internal**
Severity	**Medium**
Finding	Three instances of tinyproxy version 1.11.1 were identified within the CDE. This version has a known vulnerability which could result in a denial-of-service or even remote code execution. This issue was patched in version 1.11.2. 
Recommendations	Update to the latest version of Tinyproxy.

5.2 Weak SSH Encryption Ciphers Supported

Domain	**External**
Severity	**Low**
Finding	Externally exposed SSH services were supporting CBC encryption methods, which are considered less secure by today's standards. An adversary in a privileged position could attempt to downgrade connections for later decryption. txt.live.verygoodproxy.com:8022
Recommendations	NWG recommends disabling CBC-based encryption methods on SSH servers.

6.0 Roadmap

The Remediation Roadmap provides VGS with NWG's best estimate of an appropriate timeline for remediating the findings detailed in this report. The suggested timeline is based on NWG's years of observations, the urgency of the issue, and the time it will realistically take to implement. Also included are suggestions for other security testing activities based on industry standards for frequency.

IMMEDIATE	Determine if the jumpbox within the [redacted] should have the ability to see the Palo Alto device login page, and restrict access if needed. Update tinyproxy services to a supported version.
SHORT TERM	Disable CBC-based encryption for external SSH services.
LONG TERM	Continue performing security assessments on a regular basis or as environments evolve over time.

Appendix A Scope

Testing Began	6/2/2025
Testing Completed	6/13/2025
Additional Credentials Provided	Yes
External Network Tested	api.live.verygoodvault.com txt.live.verygoodvault.com txt.live.verygoodproxy.com
Internal Network Tested	[redacted]
Wireless Networks Tested	No
Attacks on Personnel	No
Physical Security Tested	No

Appendix B Definitions

Risk ratings, detection and response metrics, and severity scores presented throughout this document are determined based on NWG's years of experience in conducting security assessments. The following definitions categorize how NWG determines the scores issued:

Risk Scores

Risk ratings presented in **Section 1.1 Threat Models** are the cumulative representation of the severity of findings from each perspective. The "Public Compromise" risk score is based on vulnerabilities discovered without the organization providing NWG access or credentials. The "Assumed Compromise" risk score is based on the vulnerabilities discovered only after NWG provided some access or credentials.

Risk ratings presented in **Section 1.2 Risk By Domain** are derived from the severity scores issued to individual MRAs for each domain. A domain with at least one identified "High" severity MRA will be given a risk rating of "High."

A Risk Score will be "Low" if no findings or only Informational severity findings were discovered.

Severity Scores

Severity scores of "critical", "high", "medium", "low", and "informational" are issued in **Section 5.0 Matters Requiring Attention**. These scores are based on NWG's years of experience in conducting security assessments.

Critical	A "critical" severity MRA represents a significant, imminent threat to the organization or would have egregious consequences if leveraged by an attacker. Critical vulnerabilities should be addressed immediately.
High	A "high" severity MRA rating represents a likely threat to the organization. These vulnerabilities should be addressed as soon as possible.
Medium	A "medium" severity MRA rating poses some threat to the organization or its data or may be utilized in conjunction with other vulnerabilities in order to compromise the organization further.
Low	A "low" severity MRA rating may give an attacker useful information about the organization or aid in additional attacks.
Informational	An "informational" MRA rating, while not posing a specific threat, denotes relevant observations made during the engagement that were not categorized as vulnerabilities.

Detection Ratings

The Detection Matrix in **Section 3.0 Detection** provides various ratings based on the tester's observations. The following language is used to represent these observations:

None	No detection was reported to the tester.
Insufficient	Some detection was reported, but the tester identified that detection needed improvements was unactionable, or incomplete.
Slow	Detection procedures were executed, but the tester identified a significant time lapse between the attack and the detection.
Partial	Attacks were only detected during some incidents. Identical attacks were not detected at least once.
Fast/Effective	Detection procedures were executed within a reasonable timeframe. Attacks were fully identified.