ROBOCYBERWALL INC.

External Penetration Test Report

September 13, 2017

Presented To:

John Martinson Jr
RoboCyberWall Inc.
5555 Del Monte Dr,
Unit 2004
Houston, Texas 77056
admin@robocyberwall.com
713.589.2537

Submitted By:

Jules Carter
Senior Security Consultant
SecureWorks
One Concourse Parkway
Suite 500
Atlanta, GA 30328
877.905.6661
jcarter@secureworks.com
505.401.5252

Report Disclaimer Statement

Customer shall own all right, title, and interest in and to any written summaries, reports, analyses, and findings or other information or documentation prepared for Customer in connection with SecureWorks' provision of the Consulting Services to Customer (the "Customer Reports"). The provision by Customer of any Customer Report or any information therein to any unaffiliated third party shall not entitle such third party to rely on the Customer Report or the contents thereof in any manner or for any purpose whatsoever, and SecureWorks specifically disclaims all liability for any damages whatsoever (whether foreseen or unforeseen, direct, indirect, consequential, incidental, special, exemplary or punitive) arising from or related to reliance by any third party on any Customer Report or any contents thereof.

Copyrights and Trademarks

Table of Contents

1. Executive Overview

RoboCyberWall Inc. (RoboCyberWall) contracted with SecureWorks to perform the following security assessment task:

- External Penetration Test

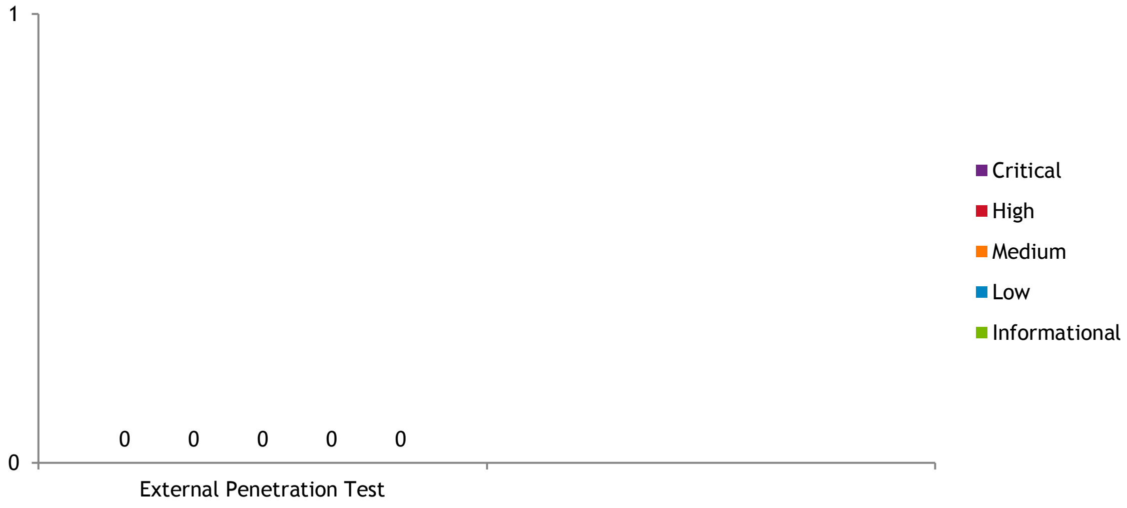
The security engagement occurred during the period from September 5, 2017, to September 8, 2017. The objective of this engagement was to identify vulnerabilities in RoboCyberWall's systems and network security that external adversaries could exploit.

During the course of the assessment, SecureWorks launched 6,593 probes and manual hack attempts on the RoboCyberWall protected server without accomplishing any breaches.

It is important to note that this report is not an objective measure, but is solely based upon observation and experience; it does not cover areas deemed out of scope or issues beyond the capabilities of this methodology.

1.1. Summary of Findings

A high-level overview of the results is presented below. Detailed results can be found in subsequent sections of this document.



- **External Penetration Test:** SecureWorks identified ZERO (0) critical-severity findings, ZERO (0) high-severity findings, ZERO (0) medium-severity finding, ZERO (0) low-severity findings, and ZERO (0) informational-severity findings.

2. External Penetration Test

During the period from September 5, 2017, to September 8, 2017, SecureWorks performed a technical network security assessment against a predetermined set of targets, including the following IPs and hosts:

Targets
165.227.116.82

2.1. Methodology

The assessment consisted of several phases, each detailed below along with the methodology, associated findings, and subsequent recommendations. SecureWorks utilizes the Penetration Testing Execution Standard (PTES) as the standard basis for penetration testing execution. The standard can be found here: http://www.pentest-standard.org.

Tools utilized are covered in the Penetration Testing Execution Standard Technical Guidelines (PTES-G), which can be found here:

http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines

2.1.1. Scope Validation

This step validates the target list provided. This is a safety measure and ensures the accuracy of subsequent findings. Activities included were:

- Ping sweeps and route tracing
- Footprinting of networks and systems
- Internet domain name registration searches
- Internet registry number searches
- Domain name service (DNS) lookups

2.1.2. Vulnerability Analysis

Vulnerability testing is the process of discovering flaws, in systems and applications, that can be leveraged by an attacker. These flaws can range anywhere from host and service misconfiguration to insecure application design. The process used to look for flaws varies and is highly dependent on the particular component being tested.

2.1.3. Manual Verification

Automated scanning tools occasionally fail to report some vulnerabilities. Therefore, manual verification does not rely on automated scanning. A testing methodology that solely relies on automated scan results can give a false sense of security.

Automated scanning tools often report false positives – reported vulnerabilities that are not actually present. For vulnerabilities discovered through automated scanning, manual verification ensures report findings are accurate and that the vulnerabilities reported are an accurate representation of your environment. Without this often-overlooked step, time may be wasted attempting to remediate vulnerabilities that don't exist.

2.1.4. Exploitation

The exploitation phase of the penetration test focuses solely on establishing access to a system or resource by bypassing security restrictions. The main focus is to identify the main entry point into the organization and to identify high-value target assets. Ultimately, the attack vector should take into consideration the success probability and highest impact on the organization.

2.1.5. Rules of Engagement

Systems were assessed and exploited to the extent described in the methodology.

2.2. Network Description

The IP address in scope for this engagement was a test host provided by RoboCyberWall. The device appeared to only be running two services: HTTPS and SSH on a non-standard port. The HTTPS server installed was the main target as that was the basis of this engagement.

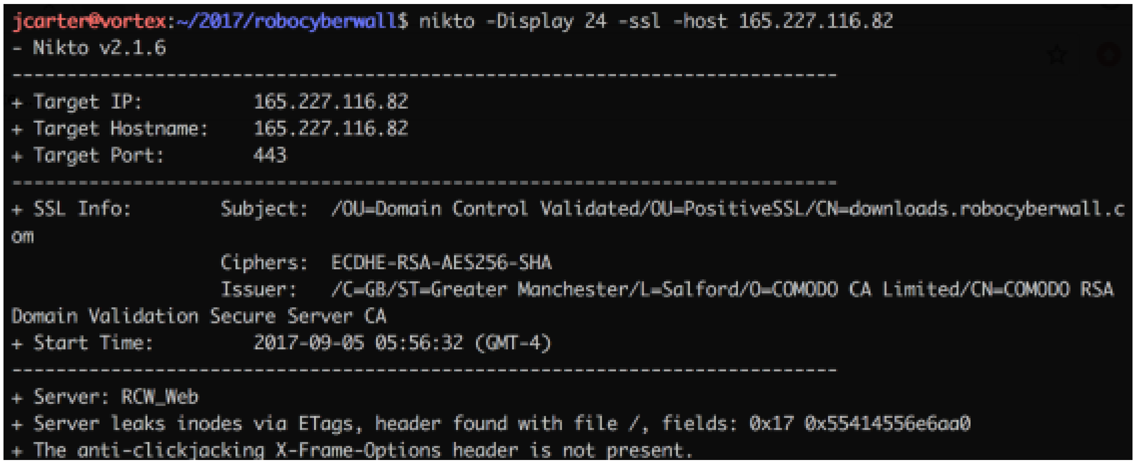
2.3. Narrative

SecureWorks began this engagement by utilizing open-source tools as well as proprietary scanners to find open ports or any potential vulnerabilities in the host provided by RoboCyberWall. One of these tools is the famous Network Mapper(nmap) tool:

```
nmap -v -sV -Pn -n -p- -oA results 165.227.116.82
```

SecureWorks only observed two open ports running at the time of testing: 443/tcp and 2020/tcp

SecureWorks began the manual testing phase of the engagement by attempting to find any applications installed on the host's HTTPs server. Several open-source tools were used during this phase including nikto and dirb:



```
jcarter@vortex:~/2017/robocyberwall$ nikto -Display 24 -ssl -host 165.227.116.82
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          165.227.116.82
+ Target Hostname:    165.227.116.82
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /OU=Domain Control Validated/OU=PositiveSSL/CN=downloads.robocyberwall.c
om
                   Ciphers:  ECDHE-RSA-AES256-SHA
                   Issuer:   /C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO RSA
Domain Validation Secure Server CA
+ Start Time:         2017-09-05 05:56:32 (GMT-4)
---------------------------------------------------------------------------
+ Server: RCW_Web
+ Server leaks inodes via ETags, header found with file /, fields: 0x17 0x55414556e6aa0
+ The anti-clickjacking X-Frame-Options header is not present.
```

SecureWorks was unable to find anything useful from these scans.

SecureWorks concluded testing without identifying any additional significant findings. Any additional details for findings are documented below.

2.4. Key Findings and Recommendations

The following set of tables lists key findings identified during the assessment, describes their severity, provides a remediation plan, and lists additional information where applicable.

2.4.1. Critical-Severity Findings

During the period of the assessment, no critical-severity vulnerabilities were identified

2.4.2. High-Severity Findings

During the period of the assessment, no high-severity vulnerabilities were identified

2.4.3. Medium-Severity Findings

During the period of the assessment, no medium-severity vulnerabilities were identified

2.4.4. Low-Severity Findings

During the period of the assessment, no low-severity findings were identified

2.4.5. Informational-Severity Findings

During the period of the assessment, no informational-severity findings were identified

2.5. Open Ports

At the time of the assessment, the following systems and services were identified:

IP	Hostname	Port	Service
165.227.116.82	downloads.robocyberwall.com	443/tcp 2020/tcp	RCW_Web OpenSSH

Appendix A: Key Terms

A.1 Severity Ratings

The following table defines SecureWorks Severity Ratings as used throughout this report.

Severity	Attributes
Critical	• Evidence of previous compromise (active incident). • Exploitation results in a disclosure of sensitive information or can pose a severe impact to Client's reputation. • Business Critical systems are heavily impacted, with the ability to alter information or change system settings. • The issue described resulted in a complete system compromise that gave the attacker the highest-level user privileges on the system. • The vulnerability resides directly on business critical systems. • Exploitation is trivial with publically available exploit code, or no exploit code is needed. • No authentication is required to exploit the vulnerable service or application. • Client has no countermeasures in place to defend against this successful attack, or the deployed countermeasures were ineffective.
High	• Exploitation may result in a disclosure of sensitive information, or may impact Client's reputation. • The issue described results in user-account or system compromise. • Exploitation is trivial with publically available exploit code, or no exploit code is needed. • No authentication is required or authentication is easily guessed/bypassed. • Client has no countermeasures in place to defend against this successful attack, or the deployed countermeasures were ineffective.
Medium	• Exploitation may result in the disclosure of a limited amount of moderately sensitive information. • Exploitation requires a skilled attacker. • Exploitation is non-trivial, and known exploit code either does not exist, or needs to be heavily modified to work effectively. • Client has countermeasures in place that might impede this attack. • Another attack vector is needed for successful exploitation, such as: • Client interaction • Social Engineering • Network or system misconfiguration
Low	• Critical client information/data is not directly at risk. • Requires several additional attack vectors, or one very complicated/rare vector, such as: • Control of the client system's internet connection • Man-in-the-Middle access • Previous compromise of a system • Insider access/knowledge • Exploitation is extremely difficult and/or time and resource intensive. • Client has countermeasures in place that prevent exploitation.
Informational	• Information that may be of interest to an attacker. • May provide data that can be used in conjunction with another attack. • Can aid in a higher-severity vulnerability.