SYSDRIVE

HomeNet
Security Assessment Report
Example

Date: December 1, 2020

Business Confidential

Table of Contents

Confidentiality Statement

This document is the exclusive property of SysDrive, LLC & <individual>. This document contains proprietary and confidential information. SysDrive may share this document in a redacted form by removing all personally identifiable information such as IP addresses and names as an example security assessment report. This report contains information relating to <individual>'s selected devices, thus <individual> owns the results of this report and may share as necessary.

Disclaimer

A vulnerability scan is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

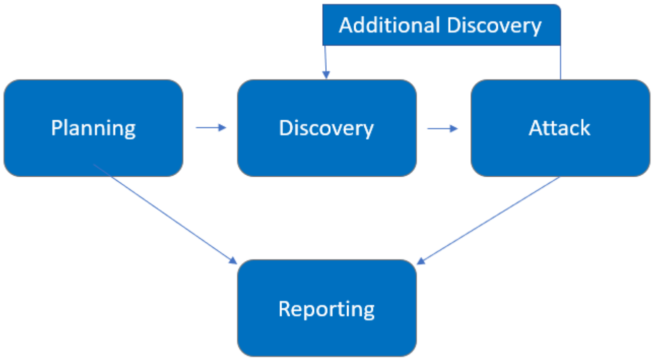
Time-limited engagements do not allow for a full evaluation of all security controls. SysDrive prioritized the assessment to identify the weakest security controls an attacker could exploit. SysDrive recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure successful remediation efforts and continued success of implemented security controls.

Assessment Overview

On December 1, 2020, SysDrive evaluated the security posture of the designated home-based infrastructure compared to current industry best practices that included an external penetration test. All testing performed is based on the NIST *SP 800-115 Technical Guide to Information Security Testing and Assessment, OWASP Testing Guide (v4), and customized testing frameworks*.

Phases of penetration testing activities include the following:

- Planning – Customer goals are gathered and rules of engagement obtained.
- Discovery – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
- Attack – Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.
- Reporting – Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.



Assessment Components

External Vulnerability Scan

An external vulnerability scan is the first step in emulating the role of an attacker attempting to gain access to an internal network without internal resources or inside knowledge. A SysDrive engineer performs scanning and enumeration to identify potential vulnerabilities in hopes of exploitation. For more in-depth reconnaissance, the engineer may attempt to gather sensitive information through open-source intelligence (OSINT), publicly available information, historical breached passwords, and more that can be leveraged against external systems to gain internal network access.

It is important to remember that an external network penetration test focuses on the ability for an attacker to find and exploit any potential vulnerability that would allow the attacker to gain access to the internal network from the Internet. External penetration tests do not perform any vulnerability scanning of devices inside the network. Though an external network assessment may not reveal any immediate vulnerabilities, all devices inside the network should always be routinely maintained for updates to ensure protection from additional attack vectors such as infected USB drives, email phishing campaigns, unsafe web browsing habits, or should an attacker find their way inside the network.

Severity Ratings for Findings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact. CVSS (Common Vulnerability Scoring System) is an open source, industry-standard rating scale which uses characteristics of an identified vulnerability such as level of possible damage, how likely is the vulnerability to be exploited, how easy is the vulnerability to use, etc. to produce a numerical score, which can then be classified into severity for easier identification and focus of remediation efforts.

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Medium	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization’s attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

Scope

Assessment	Details
External Vulnerability Scan	<tested IP address> Detected metadata: DNS: <fully-qualified domain name> ISP: <detected ISP> Location: <detected location>

Scope Exclusions

None

Executive Summary

SysDrive evaluated the designated network through an external network vulnerability scan on December 1, 2020. By leveraging a series of attacks, SysDrive found no immediate vulnerabilities to the perimeter security of the tested home network.

Summary of Open Services

The following table shows all network ports detected on the exterior of the device (available from the Internet), status, and any additional information:

Port #	State	Service	Version	Notes
80/tcp	open	http		The port is detected as "open" during simple scans but does not respond to additional detailed probing. This usually indicates the port is only being used for outbound traffic from inside the tested network to the Internet and is not configured to allow any inbound traffic. This port and service type are primarily used for web browsing.
81/tcp	open	http	Microsoft IIS httpd 8.5	This port and service type are primarily used for providing responses from a Microsoft IIS-based web server listening for client devices to connect on port 80.
443/tcp	open	ssl/ssl	Apache httpd (SSL-only mode)	In conjunction with additional information returned during the scan, this port and service appear to be hosting a website that returned a page title of "Testing Home Website"

541/tcp	open	reverse-ssl	SSL/TLS ClientHello	In conjunction with additional information returned during the scan, this port and service appear to be connected to a network device by “DeviceManufacurer”
8080/tcp	open	ssl/http	"FirewallDevice” security device httpd	In conjunction with additional information returned during the scan, this port and service appear to be connected to a network device by “DeviceManufacurer”
8081/tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)	This port and service type are primarily used for providing responses from a Microsoft IIS-based web server listening for client devices to connect on port 80.

Security Strengths

HTTP Redirected to HTTP

During the assessment, SysDrive engineers determined that configuration items were in place to automatically redirect web traffic from non-secure port 80 (HTTP) to secure port 443 (HTTPS).

Security Weaknesses

Untrusted SSL Certificate

Most commonly due to being a self-generated certificate or an improper import of an existing certificate, most current web browsers will notify a warning. Clients using strict SSL security checks and certificate-signing verification may not allow browsing a site with an untrusted SSL certificate.

Man-in-the-middle attacks could invalidate an SSL certificate signing chain. If a client receives and ignores untrusted SSL certificates on a regular basis due to “allowed exceptions” such as self-signed certificates, they likely will not recognize when a broken certificate chain is warning them of a legitimate SSL security breach.

Legacy Encryption In Use

As noted by listed vulnerabilities, 2 legacy SSL versions and 1 legacy encryption cypher are being accepted by the HTTPS web services. TLS1.0, TLS1.1, and SWEET32 SSL cypher have been depreciated as of March 2020 due to utilizing older encryption schemes that have been successfully breached. Since these encryption schemes able to be breached and thus do not provide optimal security, it is recommended they be retired if possible.

Vulnerabilities by Impact

0	0	4	0	29
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS	Name	Recommendation
Medium	6.4	SSL Certificate Cannot Be Trusted	Purchase or generate a proper SSL certificate for this service.
Medium	6.1	TLS Version 1.0 Protocol Detection	Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.
Medium	5.0	SSL Medium Strength Cipher Suites Supported (SWEET32)	Reconfigure the affected application if possible to avoid use of medium strength ciphers.
Medium	5.0	TLS Version 1.1 Protocol Detection	Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.1.
Info	N/A	Common Platform Enumeration (CPE)	
Info	N/A	Device Type	
Info	N/A	HSTS Missing From HTTPS Server	
Info	N/A	HTTP Methods Allowed (per directory)	
Info	N/A	HTTP Server Type and Version	
Info	N/A	Host Fully Qualified Domain Name (FQDN) Resolution	
Info	N/A	HyperText Transfer Protocol (HTTP) Information	
Info	N/A	L2TP Network Server Detection	
Info	N/A	OS Identification	
Info	N/A	OpenSSL Detection	
Info	N/A	Ping the remote host	

Info	N/A	Reverse NAT/Intercepting Proxy Detection	
Info	N/A	SSL / TLS Versions Supported	
Info	N/A	SSL Certificate 'commonName' Mismatch	
Info	N/A	SSL Certificate Information	
Info	N/A	SSL Cipher Block Chaining Cipher Suites Supported	
Info	N/A	SSL Cipher Suites Supported	
Info	N/A	SSL Perfect Forward Secrecy Cipher Suites Supported	
Info	N/A	SSL Root Certification Authority Certificate Information	
Info	N/A	Service Detection	
Info	N/A	Strict Transport Security (STS) Detection	
Info	N/A	TCP/IP Timestamps Supported	
Info	N/A	TLS Version 1.2 Protocol Detection	
Info	N/A	TLS Version 1.3 Protocol Detection	
Info	N/A	Traceroute Information	
Info	N/A	Unknown Service Detection: Banner Retrieval	
Info	N/A	Web Server robots.txt Information Disclosure	
Info	N/A	Web Site Client Access Policy File Detection	
Info	N/A	Web Site Cross-Domain Policy File Detection	

Additional Reports and Scans

Determined by the type of assessment, SysDrive may provide additional report information gathered during testing. This may include items such as vulnerability scan detailed findings. For more information, please see the following documents:

<none provided for this engagement>