YourIT!
Your Logo Goes Here

Security Assessment

Outbound Security Report

Scan Date: 2019/01/18

Prepared for: Your Customer / Prospect

Prepared by: Your Company Name

2021/02/03

Table of Contents

1 - Summary

This report is designed to point out issues that were detected while performing the security assessment. This includes issues found in the areas of system leakage, system control, and user control.

ASSESSMENT SUMMARY	
# End-points in Data Collection	8
SYSTEM LEAKAGE	
# End-points with protocol leaks	0
# Protocols leaked by all tested end-points	0
SYSTEM CONTROLS	
# Partially restricted protocols	0
# Unrestricted protocols	0
USER CONTROLS	
# Partially restricted sites	7
# Unrestricted sites	8

2 - System Leakage

Users inside your network are able to access and transmit to the following ports and protocols:

Windows Protocols

Internal Windows protocols in most cases should not be allowed to leave the local network.

PROTOCOL	COMMON NAME	END POINT(S)
No issues detected		

System Management Protocols

The following protocols can be leaked externally to an unknown source on the Internet. These protocols can convey security related information regarding network devices and be used to export configuration information.

PROTOCOL	COMMON NAME	END POINT(S)
No issues detected		

Exploitable Protocols

The following protocols have been known to leak information or can be used to create "phone home" scenarios that may permit access to your internal network.

PROTOCOL	COMMON NAME	END POINT(S)
No issues detected		

3 - System Controls

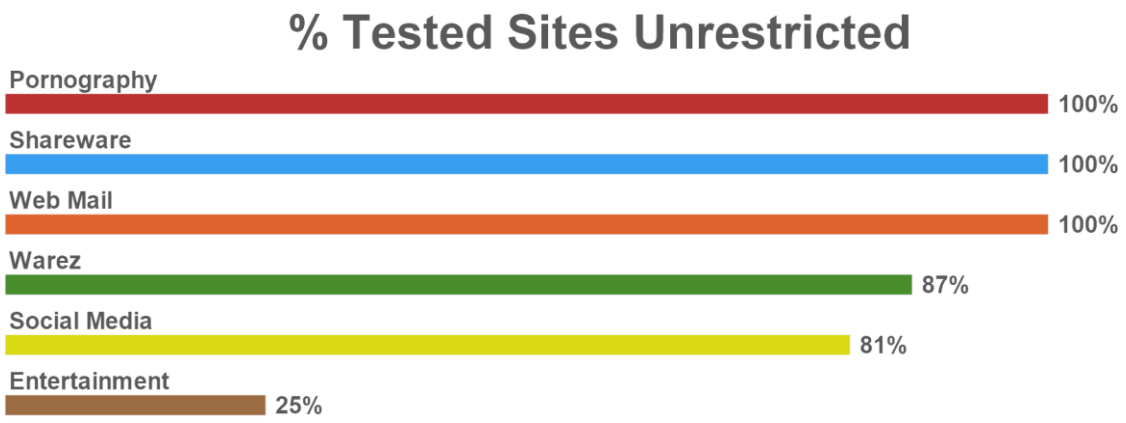
Some protocols should be highly restricted to systems which rely on them for their operation. Granting access to more than one system (unless specifically designated to require the protocol) is not recommended. The following table shows Internet-based protocols and highlights if these "allow, but limit" protocols are pervasive.

PROTOCOL	COMMON NAME	END POINT(S)	ANALYSIS
No issues detected			

4 - User Controls

An analysis of user controls indicates if content-filtering and access filtering has been implemented to prevent users from accessing potentially harmful websites and other Internet resources.

The following site categories were found to be accessible from various end-points:



Access attempts in red were able to access potentially harmful sites. Other entries attempted to but were unable to connect.

URL	CATEGORY	ACCESS ATTEMPTS	ANALYSIS
ESPN	Entertainment	GENAVE-PC INSP-TEST2 1001westerfield-deskpc dwhiteacer gilesmsi ibranaugh-hp400 milliehpz240 sketteringprodskhp	Partially Restricted
Playboy	Pornography	1001westerfield-deskpc dwhiteacer GENAVE-PC gilesmsi ibranaugh-hp400 INSP-TEST2 milliehpz240 sketteringprodskhp	Unrestricted
YouPorn	Pornography	1001westerfield-deskpc dwhiteacer GENAVE-PC gilesmsi ibranaugh-hp400 INSP-TEST2 milliehpz240 sketteringprodskhp	Unrestricted

URL	CATEGORY	ACCESS ATTEMPTS	ANALYSIS
Cnet.com	Shareware	GENAVE-PC INSP-TEST2	Unrestricted
Download.cnet.com	Shareware	1001westerfield-deskpc dwhiteacer gilesmsi ibranaugh-hp400 milliehpz240 sketteringprodskhp	Unrestricted
Tucows.com	Shareware	1001westerfield-deskpc dwhiteacer GENAVE-PC gilesmsi ibranaugh-hp400 INSP-TEST2 milliehpz240 sketteringprodskhp	Unrestricted
Facebook	Social Media	1001westerfield-deskpc dwhiteacer GENAVE-PC gilesmsi ibranaugh-hp400 INSP-TEST2 milliehpz240 sketteringprodskhp	Unrestricted
Google+	Social Media	1001westerfield-deskpc dwhiteacer GENAVE-PC gilesmsi ibranaugh-hp400 INSP-TEST2 milliehpz240 sketteringprodskhp	Unrestricted
MySpace	Social Media	GENAVE-PC INSP-TEST2 1001westerfield-deskpc dwhiteacer gilesmsi ibranaugh-hp400 milliehpz240 sketteringprodskhp	Partially Restricted
YouTube	Social Media	1001westerfield-deskpc dwhiteacer GENAVE-PC gilesmsi ibranaugh-hp400 INSP-TEST2 milliehpz240 sketteringprodskhp	Unrestricted

URL	CATEGORY	ACCESS ATTEMPTS	ANALYSIS
https://yts.am	Warez	1001westerfield-deskpc dwhiteacer gilesmsi ibranaugh-hp400 milliehpz240 sketteringprodskhp	Unrestricted
Isohunt.to	Warez	GENAVE-PC INSP-TEST2	Unrestricted
Pirate Bay	Warez	1001westerfield-deskpc dwhiteacer gilesmsi ibranaugh-hp400 milliehpz240 sketteringprodskhp	Unrestricted
Gmail	Web Mail	1001westerfield-deskpc dwhiteacer GENAVE-PC gilesmsi ibranaugh-hp400 INSP-TEST2 milliehpz240 sketteringprodskhp	Unrestricted
Yahoo Mail	Web Mail	1001westerfield-deskpc dwhiteacer GENAVE-PC gilesmsi ibranaugh-hp400 INSP-TEST2 milliehpz240 sketteringprodskhp	Unrestricted

5 - Wireless Access

Providing wireless access enables greater freedom within the workplace but can also pose potential security risks. The following table shows detected wireless networks and has any possible security issues highlighted. Some access points which are detected may not be a part of your network and their use should be discouraged as there is an inherent risk in connecting to foreign networks.

SSID	SECURED	SECURITY	RISK LEVEL
<blank>	Yes	RSNA_PSK	Low
DIRECT-34-HP M477 LaserJet	Yes	RSNA_PSK	Low
DIRECT-63-HP M252 LaserJet	Yes	RSNA_PSK	Low
DIRECT-be-HP M402 LaserJet	Yes	RSNA_PSK	Low
HP-Print-EB-Officejet Pro 6830	Yes	RSNA_PSK	Low
IRC Admin	**No**	**IEEE80211_Open**	**High**
MobileHousing1	Yes	RSNA_PSK	Low
MobileHousing2	Yes	RSNA_PSK	Low
PA_Conf_Rm	Yes	RSNA_PSK	Low
PA_Conf_Rm-guest	**No**	**IEEE80211_Open**	**High**
PAO2	Yes	RSNA_PSK	Low
PAO5	Yes	RSNA_PSK	Low