datalinknetworks

Security Assessment

Outbound Security Report

Prepared for: Jonathan Doe
Prepared by: Austin Archer

3/23/2018

Scan Date: 4/1/2014

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	2
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	0
# Unrestricted sites	12

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

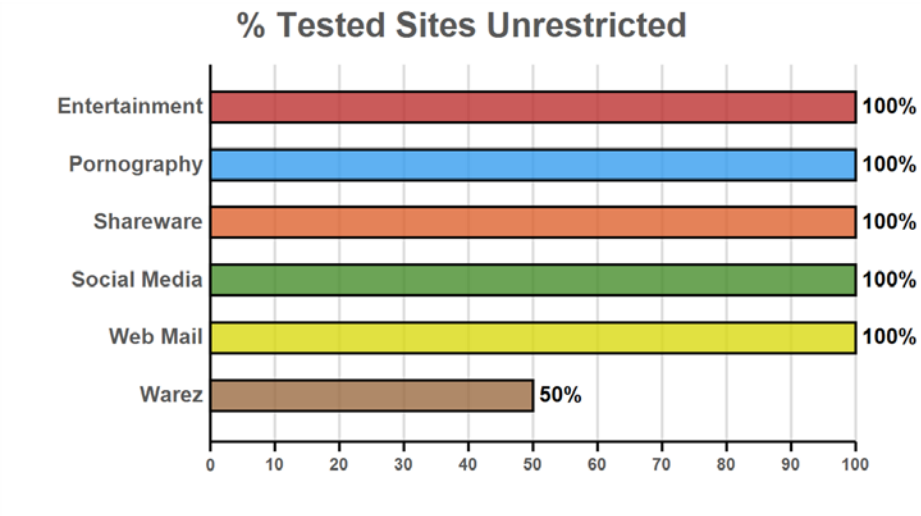
Some protocols should be highly restricted to systems which rely on them for their operation. Granting access to more than one system (unless specifically designated to require the protocol) is not recommended. The following table shows Internet-based protocols and highlights if these "allow, but limit"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



URL	Category	Unrestricted End Point(s)	Analysis
ESPN	Entertainment	DC01 tandem	Unrestricted
Playboy	Pornography	DC01 tandem	Unrestricted
YouPorn	Pornography	DC01 tandem	Unrestricted
Cnet.com	Shareware	DC01 tandem	Unrestricted
Tucows.com	Shareware	DC01 tandem	Unrestricted
Facebook	Social Media	DC01 tandem	Unrestricted
Google+	Social Media	DC01 tandem	Unrestricted
MySpace	Social Media	DC01 tandem	Unrestricted
YouTube	Social Media	DC01 tandem	Unrestricted
Isohunt.com	Warez	DC01 tandem	Unrestricted
Gmail	Web Mail	DC01 tandem	Unrestricted
Yahoo Mail	Web Mail	DC01 tandem	Unrestricted