



# Security Assessment

## Outbound Security Report



CONFIDENTIALITY NOTE: The information contained in this report document is for the exclusive use of the client specified above and may contain confidential, privileged and non-disclosable information. If the recipient of this report is not the client or addressee, such recipient is strictly prohibited from reading, photocopying, distributing or otherwise using this report or its contents in any way.

Prepared for:  
Your Customer / Prospect  
Prepared by:  
Your Company Name



## Table of Contents

---

- 1 - Summary
- 2 - System Leakage
- 3 - System Controls
- 4 - User Controls
- 5 - Wireless Access

## 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.

<b>Assessment Summary</b>	
# End-points in Data Collection	3
<b>System Leakage</b>	
# End-points with protocol leaks	3
# Protocols leaked by all tested end-points	15
<b>System Controls</b>	
# Partially restricted protocols	0
# Unrestricted protocols	0
<b>User Controls</b>	
# Partially restricted sites	0
# Unrestricted sites	13

## 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)
135 / TCP	MS RPC	DC01 UTIL01
135 / UDP	MS RPC	DC01 UTIL01
137 / TCP	NetBIOS/IP	DC01 UTIL01
137 / UDP	NetBIOS/IP	DC01 UTIL01
138 / TCP	NetBIOS/IP	DC01 UTIL01
139 / TCP	NetBIOS/IP	DC01 UTIL01
139 / UDP	NetBIOS/IP	DC01 UTIL01

### 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)
<i>No issues detected</i>		

### 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)
6661 / TCP	Internet Relay Chat (IRC)	DC01 SE-Dresden UTIL01
6662 / TCP	Internet Relay Chat (IRC)	DC01 SE-Dresden UTIL01
6663 / TCP	Internet Relay Chat (IRC)	DC01 SE-Dresden UTIL01
6664 / TCP	Internet Relay Chat (IRC)	DC01 SE-Dresden UTIL01
6665 / TCP	Internet Relay Chat (IRC)	DC01 SE-Dresden UTIL01
6666 / TCP	Internet Relay Chat (IRC)	DC01 SE-Dresden



Protocol	Common Name	End Point(s)
		UTIL01
6667 / TCP	Internet Relay Chat (IRC)	DC01 SE-Dresden UTIL01
6668 / TCP	Internet Relay Chat (IRC)	DC01 SE-Dresden UTIL01



### 3 - System Controls

---

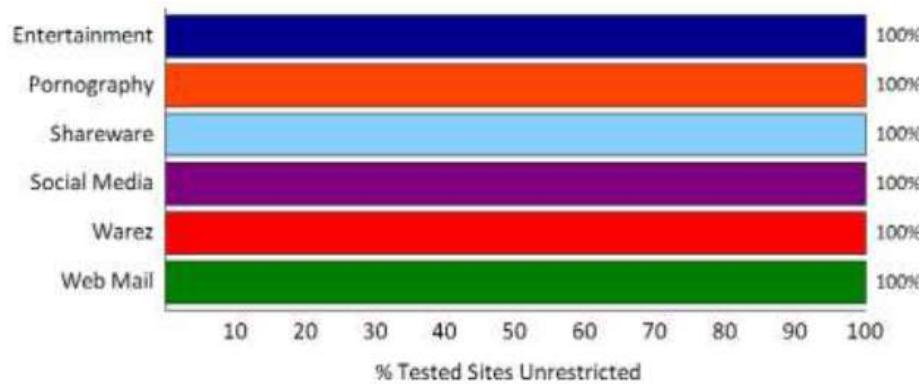
Some protocols should be highly restricted to systems which rely on them for their operation. Granting access to more than one system (unless specifically designated to require the protocol) is not recommended. The following table shows Internet-based protocols and highlights if these "allow, but limit"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

Protocol	Common Name	End Point(s)	Analysis
<i>No issues detected</i>			

## 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
<b>ESPN</b>	Entertainment	DC01 SE-Dresden UTIL01	<b>Unrestricted</b>
<b>Playboy</b>	Pornography	DC01 SE-Dresden UTIL01	<b>Unrestricted</b>
<b>YouPorn</b>	Pornography	DC01 SE-Dresden UTIL01	<b>Unrestricted</b>
<b>Download.com</b>	Shareware	DC01 SE-Dresden UTIL01	<b>Unrestricted</b>
<b>Tucows.com</b>	Shareware	DC01 SE-Dresden UTIL01	<b>Unrestricted</b>
<b>Facebook</b>	Social Media	DC01 SE-Dresden UTIL01	<b>Unrestricted</b>
<b>Google+</b>	Social Media	DC01 SE-Dresden UTIL01	<b>Unrestricted</b>
<b>MySpace</b>	Social Media	DC01 SE-Dresden UTIL01	<b>Unrestricted</b>
<b>YouTube</b>	Social Media	DC01 SE-Dresden UTIL01	<b>Unrestricted</b>
<b>Isohunt.com</b>	Warez	DC01 SE-Dresden UTIL01	<b>Unrestricted</b>
<b>Pirate Bay</b>	Warez	DC01 SE-Dresden UTIL01	<b>Unrestricted</b>
<b>Gmail</b>	Web Mail	DC01 SE-Dresden UTIL01	<b>Unrestricted</b>



URL	Category	Unrestricted End Point(s)	Analysis
<b>Yahoo Mail</b>	Web Mail	DC01 SE-Dresden UTIL01	<b>Unrestricted</b>



## 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	Low
202Xnet	Yes	WPA_PSK	Low
<b>Belkin_G_Wireless_B976AF</b>	<b>Yes</b>	<b>IEEE80211_Open</b>	<b>High</b>
<b>clear</b>	<b>No</b>	<b>IEEE80211_Open</b>	<b>High</b>
<b>clear-guest</b>	<b>No</b>	<b>IEEE80211_Open</b>	<b>High</b>
CLIENT	Yes	RSNA_PSK	Low
<b>HP8A74CE</b>	<b>No</b>	<b>IEEE80211_Open</b>	<b>High</b>
Kristie	Yes	RSNA_PSK	Low
SPLS-CORP	Yes	RSNA	Low