Research Assignment 1: Services & Ports

Overview

The purpose of this assignment is for you to learn about well-known internet services and their associated ports and prepare a professional report.

This assignment may be done in groups of 1-3.

Objective

1. Identify internet services/ports to do research on
2. For each service do detail research about the service and its associated ports
3. Prepare a professionally written report

Well-known Internet Services and their Associated Ports

Prepare a report about 12 of the services and ports described in the table below. Try to find a pcap of a transaction of each protocol you are studying, and explain what you see.

Well Known ports: must be included	
netbios	137-139
microsoft-ds	445
Well Known ports: Choose 6	
ftp	21
ssh	22
smtp	25
dns	53
bootp	67/68
pop3	110
sunrpc	111
ntp	123
imap2	143
snmp	161
irc	194
ldap	389
microsoft-ds	445
ipp	631
rsync	873
Registered ports: Choose 4	
ms-sql	1433/1434
radius	1812
nfs	2049
mysql	3306
svn	3690
postgresql	5432
gnutella	6346/6347

Report Format and Contents

Your professional report should have the following structure:

Title Page:

- Course Code
- Assignment #
- Team Members

Table of Contents

Service and Ports – this is the body of your text

References and Bibliography

In the *Service and Ports* section every service should start on page and include

1. A detailed description of how the service works. Including:
   - The purpose of the service
   - A basic description of the protocol
   - Other ports commonly used for the service
   - The information the service might expose
   - How a business might make use of the service
   - How they may also be delivered via encrypted services, such as SSL, on other ports
   - References to appropriate RFCs. (Here is one of my favourite RFCs. Here is another.)
2. Known vulnerabilities of that service
3. Risks exposed by the service
4. How data is collected about that service, and what that data looks like (format and location of log files)
5. Mitigation of the risks exposed
6. A screen shot of each Wireshark analysis, with explanation.

Note:

Your report must be *original work*.

- Any material gathered from outside sources **must** be attributed with quotes and footnotes. **Papers submitted without references will be given a mark of ZERO**.
- Material generated from software must also be attributed.

Marks will rewarded for interpretation of data gathered, organization and presentation. Marks will not be awarded for cut and paste of data generated during the performance of lab exercises. However, this material should be used to support your analysis.

Plagiarism will not be tolerated, and will result in an Academic Dishonesty Report, and aggressive pursuit of appropriate consequences. See the Cheating and Plagiarism section of Seneca's Academic Policy for details. You are expected to be aware of these policies, and protestations of ignorance of them will fall upon deaf ears. You have been warned.

Deliverables:

A professional quality report – one hard copy AND one electronic copy.

The due date will be posted on the course website (Moodle)
Teams need only submit one electronic copy and one hard copy
Each team should ensure the team knows who will be submitting the soft & hard copies and the submitter should informt the team members when the submission has taken place – saying you did not know that the report had not been submitted is not an acceptable reason for a late assignment.

- Electronic Copy
  - Submit your report in '.docx' through the course's Moodle site before the due date and time
  - The submission should have the following name: LearnName_RA1.docx – the *LearnName* is that of the submitter.
  - *Email submissions will not be accepted* unless you have a problem with submitting your document to Moodle or you are late in submitting your copy.

- Hard Copy
  - The hard copy is due the first class after the due date.
  - Only one team member needs to submit a hard copy.