|  |  |
| --- | --- |
| A picture of a winding road and trees  Information Security  [Document subtitle] | Abstract  [Draw your reader in with an engaging abstract. It is typically a short summary of the document. When you’re ready to add your content, just click here and start typing.]  Tommy Bedford  SE3IS11 |

**Contents**

[Introduction 2](#_Toc444877079)

[Method 2](#_Toc444877080)

[Reconnaissance 2](#_Toc444877081)

[Scanning 2](#_Toc444877082)

[Scanning System Vulnerabilities 2](#_Toc444877083)

[Conclusion 3](#_Toc444877084)

Information Security

# Introduction

# Method

## Reconnaissance

**Tools:**

* who.is
* w3dt.net

**OS Based Tools:**

* nslookup

## Scanning

**Accessibility:**

* Which IP addresses are accessible
* What they are running
* Any obviously open doors

**Basics:**

* Ping the address to see if it’ live.
* Scan the ports to see if are any are open
* Google ports numbers to get applications
* Google applications vulnerabilities.
  + 1-1023 are *system*: used by the OS
  + 1024-49151 are *registered* for a specific purpose
  + 49152-65535 are *custom*; used for whatever the user wants.
* Can just try and establish a TCP connection to the port:
  + Gives the system your IP address, details of the program used to connect, ect.
  + use sneaky manipulation of TCP protocol
* Send a TCP FIN Packet
  + Does not make a connection attempt; circumvents firewall.
  + If the port is in listen: no reply.
  + If the port is closed: responds with reset.

## Enumeration

* The process of validating the list of users you acquired when foot-printing.
* The evaluation of how safe it is to go ahead with the attack. A lengthy process that is usually automated. A case of measure twice and cut once.

**Spidering**

* Spidering is the automatic mapping of a website.
* A recursive program that follows all HTML links from the document.
* Can revel

## Penetration/Attack

* Gain and maintain connection for objective to be completed.

## Install back doors

## Covering Tracks

# Conclusion

**Notes**

LAMP architecture is made up of LINUX, APACHE, MySQL database management and PHP.

Version of PHP installed - phpBB2.0.23

Local WAMP server installed and configured. This is just a windows based version of the LAMP server

Any version of phpBB2.x security can be exploited by a CRSF (Cross-site request forgery) attack. Looked this up briefly <https://www.intelligentexploit.com/view-details.html?id=7671>