Abertay University

Hackers Handbook

M. Hayden

BSc Ethical Hacking
Abertay University
Dundee, United Kingdom
StudentNumber@abertay.ac.uk

December 4, 1985

Abstract

A Bill To Make provision about the interception of communications, equipmentinterference and the acquisition and retention of communications data, bulk personal datasets and other information; to make provision about the treatment of material held as a result of such interception, equipment interference or acquisition or retention; to establish the Investigatory Powers Commissioner and other Judicial Commissioners and make provision about them and other oversight arrangements; to make further provision about investigatory powers and national security; to amend sections 3 and 5 of the Intelligence Services Act 1994; and for connected purposes.

Contents

1 Introduction

Some text used to fill space taken from the Investigatory Powers Bill (Parliament, 2016).

More information about LaTeX & Tex can be found on the Hack Soc wiki [1].

1.1 Layout

1.1.1 Colin White Paper CMP319 2016/17

As a suggestion, your report should include:

1. Introduction
   (a) Introduction to the report
   (b) Aim of your work
   (c) An overview of your methodology (i.e. each step that you have conducted to penetrate the network and the tools that you have used).
2. Procedure and Results
   (a) This section should succinctly describe your practical work and findings
   (b) Any results should be presented in an easy to read format.
   (c) Include any relevant screenshots. These should be clearly labelled and referenced within the text of your report.
3. References
   (a) References should be cited according the university's referencing criteria (http://www.abertay.ac.uk/media/Referencing.pdf)
   (b) You should cite appropriate references throughout your report.
4. Appendices
   (a) Any large volume of information should be included in Appendices.

[1] https://hacksoc.co.uk/latex

1.1.2 David White Paper One CMP314 2016/17

The following structure is suggested:

1. Introduction [15%]
   (a) Abstract
   (b) Introduction
   (c) Overview of chosen area
   (d) Your Objectives
2. Procedure and Results [20%]
   (a) An explanation of what you did and what you found
   (b) A discussion of the practical steps included in your investigation
   (c) The results should be easily followed and understood and should, where appropriate, include any relevant screenshots
3. Discussion [20%]
   (a) Critical evaluation of the results
   (b) Description of any further investigative work that could be performed in future research
   (c) Any countermeasures.
4. Conclusions [10%]
5. References & Bibliography [10%]

1.2 Background

1.3 Overview

1.3.1 LaTeX

"LaTeX, which is pronounced 'Lah-tech' or 'Lay-tech', is a document preparation system for high-quality typesetting. It is most often used for medium-to-large technical or scientific documents but it can be used for almost any form of publishing."[2]

1.3.2 Technology Two

[2]https://www.latex-project.org/about/

2 Aims & Objectives

2.1 Aims

- Enslave Humanity
- Defeat C

2.2 Objectives

- Build AI
  - Write AI framework
  - Train it on cat pics
  - Deploy TLS
- Setup Windows 10 Virtual Machine in VMWare
- Setup Linux on Windows

3 Procedure

4 Discussion & Comparison

4.1 Cats Are Awesome

5 Conclusion

References

Parliament (2016). *Investigatory Powers Bill*. Tech. rep. publications.parliament.uk. URL: http://www.publications.parliament.uk/pa/bills/lbill/2016-2017/0040/17040.pdf (visited on 11/30/2016).

Acronyms

2FA Two Factor Authentication.

AES Advanced Encryption Standard.

API Application Programming Interface.

AWS Amazon Web Services.

CA Certificate Authority.

CVE Common Vulnerabilities & Exposures.

DLP Data Loss Prevention.

Git Free and open source distributed version control system.

HSTS HTTP Strict Transport Security.

HTTP Hypertext Transport Protocol.

HTTPS Hypertext Transport Protocol Secure.

MS Microsoft.

OWASP Open Web Application Security Project.

PaaS Platform as a Service.

RCE Remote Code Execution.

S3 Amazon Simple Storage Service.

SQL Structured Query Language.

SQLi Structured Query Language Injection.

TLS Transport Layer Security.

UI User Interface.

URL Uniform Resource Locator.

VM Virtual Machine.

Appendices

A Definition of ”interception” etc.

Interception in relation to telecommunication systems

1. For the purposes of this Act, a person intercepts a communication in the course of its transmission by means of a telecommunication system if, and only if -

   (a) the person does a relevant act in relation to the system, and

   (b) the effect of the relevant act is to make any content of the communication available, at a relevant time, to a person who is not the sender or intended recipient of the communication.

   For the meaning of ”content” in relation to a communication, see section 233(6).

2. In this section ?relevant act?, in relation to a telecommunication system, means -

   (a) modifying, or interfering with, the system or its operation;

   (b) monitoring transmissions made by means of the system;

   (c) monitoring transmissions made by wireless telegraphy to or from apparatus that is part of the system.

3. For the purposes of this section references to modifying a telecommunication system include references to attaching any apparatus to, or otherwise modifying or interfering with -

   (a) any part of the system, or

   (b) any wireless telegraphy apparatus used for making transmissions to or from apparatus that is part of the system.

4. In this section ?relevant time?, in relation to a communication transmitted by means of a telecommunication system, means -

   (a) any time while the communication is being transmitted, and

   (b) any time when the communication is stored in or by the system (whether before or after its transmission).