Lab Sheet 1 – 5% Tim Browning – C14519547

**Skills**

Security skills are very advanced and difficult to learn and understand. To achieve the level of knowledge and expertise needed for security, it normally requires at least 5-10 years of experience. Such skills include[1]:

* IPS penetration and vulnerability testing
* Firewall and intrusion detection/prevention protocols
* Application security and encryption technologies
* Subnetting, DNS, encryption technologies and standards, VPNs, VLANs, VoIP and other network routing methods
* Network and web related protocols (e.g., TCP/IP, UDP, IPSEC, HTTP, HTTPS, routing protocols, etc.)

**Certifications and Training**

A bachelor’s degree isn’t a good enough qualification to get a job with the government or a private company. There are many certifications which can give you a better understanding of security:

**GIAC Security Essentials (GSEC):** Is the leading provider of Cyber Security Certifications, globally recognized by government, military and industry leaders. This is ideal for computer scientists who want to have a career relating to security tasks. [2] The exam cost around $1000.

**Certified Information Systems Security Prof**:[2] Are globally acknowledged as the Gold Standard in for educating and certifying information security professionals. People who wish to do this exam must have 5 years of paid full-time work experience in 2 of the 8 domains of the CISSP which covers topics such as cloud computing, mobile security and development security. The exam is around $600.

**Systems Security Certified Practitioner:** [3]It is designed for candidates interested in the field of information security. The security of business environments is covered in this certificate. The exam costs around $250

### Discuss why there is a shortage of security personnel worldwide?

The certificates required to be in Security aren’t easy to get. They are expensive, difficult to pass and require previous to do them. Also what you learn for the certificate might change because the industry is moving so fast. A job in security requires you to continuously learn to keep up to date with the latest security prevention methods.

The methods that online criminals use are becoming more sophisticated and harder to prevent. The IT security team have a huge responsibility to prevent attacks.

The challenge in finding skilled professionals is due to a lack of adequate training.

What measures/actions should be taken to address this shortage?

**Create support programs:** Mentorships and other opportunities help new cybersecurity hires gain experience and learn.

**Build a cybersecurity ecosystem:** Get in contact with government organisations and educational institutions. Security experts can get involved and they can share their knowledge.

**Workforce Strategy:** Adjust your hiring strategy. Make sure the candidate has the appropriate experience.

**Hacking competitions:** Hacking competitions are proving to be useful in developing security skills.

## Do you think you have enough skills to be a security expert? If no what are you missing and if yes, what are your strengths?

No. The theory I have learnt is a good foundation but to be an expert in security I will need more practical experience. For example, working in a company for 5 to 10 years.

[1] “How to Become a Security Engineer | Requirements for Security Engineer Jobs,” *Cyber Degrees*. [Online]. Available: https://www.cyberdegrees.org/jobs/security-engineer/. [Accessed: 12-Feb-2018].

[2] “10 Security Certifications To Boost Your Career,” *Dark Reading*. [Online]. Available: https://www.darkreading.com/risk/10-security-certifications-to-boost-your-career/d/d-id/1322449. [Accessed: 12-Feb-2018].

[3] “10 Security Certifications To Boost Your Career.” [Online]. Available: https://www.darkreading.com/risk/10-security-certifications-to-boost-your-career/d/d-id/1322449?image\_number=3. [Accessed: 12-Feb-2018].