Cybersecurity Notes

**Week 1: Introduction to Cyber security**

**Monday-Friday**

**Tasks**

* Completed a penetration simulation on the red team hacking into a bank then transferring over fake funds into the bank account.
* Completed a defensive simulation on the blue team, detecting a suspicious IP address then forwarding the IP to an analyst team leader to block the IP in the firewall.
* Learning various definitions

**What did I learn?**

**Brute-forcing:** Is a method used to gain access to a system by systematically trying a large number of possibilities until the correct one is found.

- “-u” flag specifies the URL you are targeting and the “-w” flag is for brute forcing directories.

**Security analyst:** Security analysts are integral to constructing security measures across organisations to protect the company from attacks.

**Tasks:** *working with various stakeholders, producing reports about the safety of networks, and developing security plans.*

**Security engineer:** Security engineers develop and implement security solutions using threats and vulnerability data.

**Tasks:***Testing and screening security measures across software, monitor networks and reports, and identify and implement systems.*

**Incident responder:** Incident responders respond productively and efficiently to security breaches.

**Tasks:** *Developing an incident response plan, maintaining strong security responses, and preparation for future attack and post-incident reporting.*

**Digital forensics examiner:** Analysing incidents or working for law-enforcement.

**Tasks:** *Collecting, analysing, and documenting digital evidence.*

**Malware analyst:** A malware analyst's work involves analysing suspicious programs, discovering what they do and writing reports about their findings.

**Tasks:** *Documenting all reports/findings, conduct dynamic analysis of malware, reverse-engineer languages, carry out static analysis of malicious programs.*

**Penetration tester:** A penetration tester's job role is to test the security of the systems and software within a company.

**Tasks:** *Conduct tests on systems and networks, perform security assessments, evaluate and report on insights.*

**Red teamer:** Whilst red teamers are enacted to test the company's detection and response capabilities. This job role requires imitating cyber criminals' actions, emulating malicious attacks, retaining access, and avoiding detection.

**Tasks:** *Emulate the role of a threat, evaluate and report on insights.*