

Yleinen runko diplomityölle:

1. Introduction

- Alustetaan kurssin ja työn tarkoitus, sekä tavoitteet ja yleiset vaatimukset (esimerkiksi keskittyminen open-source teknologioiden käyttöön, ei haluttu vendor lockata jne.)

2. Cloud and Network Security

- Alustetaan Pilvi- ja verkkoturvallisuus, sen historia, riskit, termistöt, yleisimmät ratkaisut

2.1 Kyberturvallisuus yleisesti

- Historiaa
- Yleistä termistöä

2.2 Pilviteknologiat yleisesti

- Historiaa
- Pilviarkkitehtuuri
 - Core stack
 - Hallinnointi puoli
- Pilvipalveluiden eri muodot (IaaS, PaaS & SaaS)

2.3 Verkkoturvallisuus (Network security)

- Historiaa
- Riskit ja uhat
- Yleisimmät ratkaisut organisaatioissa

2.4 Pilviturvallisuus

- Yleisesti
- Historiaa
- Riskit ja uhat
 - Esimerkki tapaus (tai tapauksia), kun joku ulkoinen taho on onnistunut pääsemään käsiksi järjestelmään tai aiheuttanut muutoin haittaa
- Yleisimmät ratkaisut riskien lieventämiseen, huomaamiseen ja estämiseen

3. Related Work (nimi voi muuttua)

- Jotenkin tällä kappaleella olisi tarkoitus esittää yleisesti kaikki kurssin laboratorioihin liittyvät aihe-alueet

3.1 State of the Art

- Miten vastaavanlaisia kursseja on järjestetty ja mihin niiden järjestelmät perustuvat
 - Verkkoturvallisuus kurssi esimerkki (esim. Cisco network security course)
 - Pilviturvallisuus kurssi esimerkki (esim. MOOC)
- Liittyviä kurssijärjestelmiä; Labtainers, Kubernetes-Goat, EKS Cluster Games ...

3.2 Networking protocols pohjustus

3.3 Fuzzaus

3.4 Digital Forensics

4. Technologies (nimi voi muuttua)

- Pääfokuksena esitellään teknologiat joita kurssilla käytetään ja niille vaihtoehtoisia korvikkeita, esitetään miksi tietyt teknologiat valittiin vaihtoehtojen yli

4.1 Yleinen ideologia (nimi todellakin muuttuu)

- Käydään vielä läpi minkälaisia vaatimuksia lähtökohtaisesti valituille teknologioille oli (sivuuttaa introductionin vaatimuksia)

4.2 Yleiset työkalut

- Esitellään yleiset työkalut joita kurssilla käytetään
- Rust
- Wireshark
- jne...

4.3 Virtuaalikoneet ja virtualisaatio

- Esitellään erilaiset virtuaalikoneet ja niiden hallinnointi järjestelmät yleisesti, QEMU/KVM (kurssilla käytetty), Virtualbox

4.4 Palomuurit ja NGFWs

- Yleisesti
- pfSense vs opnSense (kurssille oleellisin)
- Muut vaihtoehdot (esim. ufw)

4.5 SIEM järjestelmät

- Yleisesti
- Wazuh (kurssille oleellisin)
- Muut vaihtoehdot

4.6 Pilvi ympäristöjen pystytys teknologiat

- Terraform
- Ansible
- Muut vaihtoehdot

4.7 Kontti orkestraatio

- Yleisesti
- Docker
- Kubernetes
- Muut vaihtoehdot

5. Implementation (nimi voi muuttua)

5.1 Esitellään miten laboratorio ympäristöt ja tehtävät luotiin

5.2 Lab1/Lab2: Network Security

- Järjestelmä
- Tehtävät (pohjustus, ei liian tarkkaan)
- Kritiikki (suorituskyky joillain käyttöjärjestelmillä)

5.3 Lab3: Network Protocols

- Tehtävät (pohjustus, ei liian tarkkaan)

- Kritiikki (todella vaativa tehtävä TLS:n liittyen)

5.4 Lab4: Container Security (viikko jota en ollut tekemässä)

- Järjestelmä (lyhyesti, koska en ollut tekemässä tätä)
- Tehtävät (pohjustus, ei liian tarkkaan)
- Kritiikki (monesti pilviratkaisu alhaalla)

5.5 Lab5: Cloud Security

- Järjestelmä
- Tehtävät (pohjustus, ei liian tarkkaan)
- Kritiikki (yksi taski oli suoraan muualta, vastaukset löytyivät liian helposti)

5.6 Lab6: Digital Forensics

- Järjestelmä
- Tehtävät (pohjustus, ei liian tarkkaan)
- Kritiikki

5.7 Lab7: Security of Internet: The Big Picture

- Tehtävät
- Kritiikki

6. Results/Experiments

- Mitä huonoa huomattiin (esim. Luento vs laboratorio materiaali, AI:n käyttö...)

7. Future Work

Yleisesti mitä voisi parantaa seuraavaan iteraatioon, liittyen järjestelmiin ja tehtäviin

8. Summary

Käydään kokonaisuus vielä kertaalleen läpi