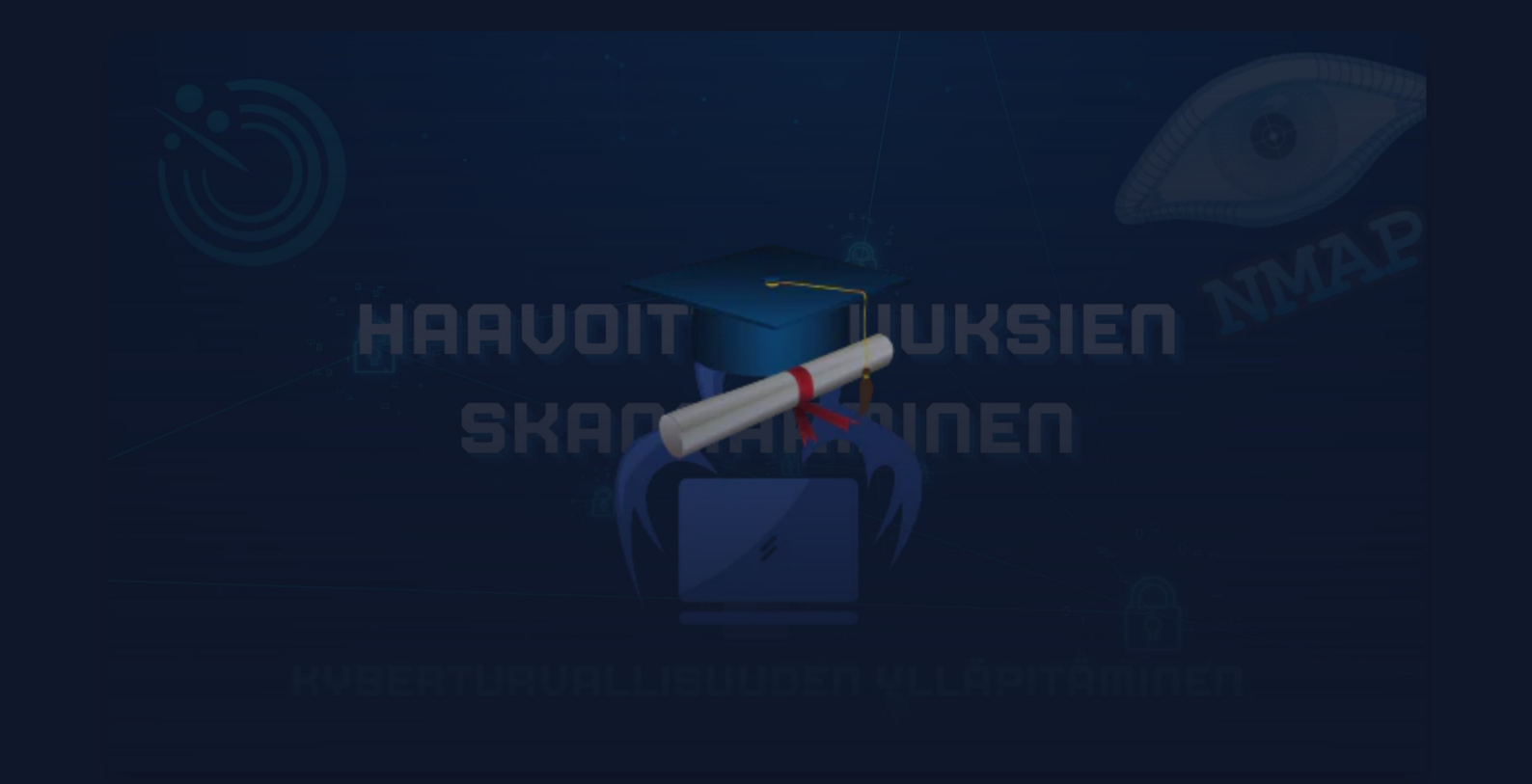


# Todistus

## Kyberturvallisuuden Ylläpitäminen - Haavoittuvuuksien Skannaaminen

Käyttäjä **s2200855@edu.bc.fi** on suorittanut **100%** osiosta **Kyberturvallisuuden Ylläpitäminen - Haavoittuvuuksien Skannaaminen**.


## Kuvaus:

Tämä polku vastaa kyberturvallisuuden ylläpitäminen (30 op) tavoitteeseen "Osaa skannata haavoittuvuuksia tarkastelun kohteena olevasta sovitusta verkosta". Polulla käymme läpi tietoverkkoja ja haavoittuvuuksia yleisesti, sekä harjoittelemme suosituimpien verkko- ja haavoittuvuus-skannerien kuten Nmap ja Nessus käyttöä.

## Suoritetut moduulit:

- Mitä ovat haavoittuvuusskannaukset ja miksi niitä tehdään?
- Haavoittuvuudet

- Tietoverkot ja TCP/IP -malli
- Tietoverkkojen fyysiset mediat
- Hubit ja kytkimet
- MAC-osoitteet
- ARP (Address Resolution Protocol)
- IP-osoitteet
- Aliverkot, verkkomaskit ja CIDR-notaatio
- Yhdyskäytävät ja reititys
- IP-protokolla
- ICMP (Internet Control Message Protocol)
- TCP (Transmission Control Protocol)
- UDP (User Datagram Protocol)
- DNS (Domain Name System)
- DHCP (Dynamic Host Control Protocol)
- Internetin osoitteet
- Asiakas-palvelin-malli
- Mikä on Nmap?
- Kohteen määrittäminen
- Isäntien havaitseminen
- Isännän löytämistekniikat
- Johdatus porttiskannaukseen
- Tulosteen tallennus ja tulosteen tarkkuuden määrittäminen
- Porttien määrittäminen
- Ajoitukseen liittyvät valinnat
- IPv6 skannaus
- TCP SYN -skannaus

- TCP connect -skannaus
- UDP-skannaus
- TCP FIN-, NULL- ja Xmas-skannaus
- TCP ACK -skannaus
- IP Protocol -skannaus
- Palveluiden tunnistaminen (-sV)
- Johdanto Nmap-skripteihin
- Mikä on Nessus?
- SSH kirjautumisen konfigurointi
- Skannauksen ajastaminen
- Skannaustulosten käsittely