jamk

2024

1 Johdanto

Testaa ryhmäsi kanssa MISP-järjestelmää osoitteessa misp.ttc60z.vle.fi
Tunnukset ovat admin@admin.test / AdminAdmin123-

Voit käyttää apuna ohjetta osoitteessa https://www.circl.lu/doc/misp/using-the-system

2 Tehtävät

Tutki ja selvitä seuraavat tehtävät. Tuota vastauksesta asiakirjamallin (thesis) mukainen dokumentti ja palauta se PDF-versiona Moodlen palautuslaatikkoon.

1. Mitä erilaisia jakeluasteita tapahtuman luomisessa voi käyttää? Mitä väliä jakeluasteella on?

2. Missä muodossa cybercrime-tracker.net toimittaa feedinsä?

3. Mikä käyttäjän "esko.morko" nids sid -numero on?

4. Kuinka monta attribuuttia löydät kyseisestä MISPistä aikaväliltä 1.9.2023-1.4.2024?

5. Minkä pankkiryhmän asiakas tapahtuman 1401 pahantekijä todennäköisesti on?

6. Kuinka monta virhettä varoitus- ja virhelokissa on?

7. Minkä niminen tagi on merkitty ID-numerolla 600?

8. Minkä nimiset aktiiviset tagit ovat taksonomiakirjastossa honeypot-basic?

9. Mikä organisaatio on kaikista isoimmalla ID-numerolla järjestelmässä?

10. Mikä MISP-serveriasetus on kriittisesti vioittunut kyseisessä serverissä?

Jyväskylän ammattikorkeakoulu	Postiosoite/Address	Puhelin/Tel.	Faksi/Fax	Internet	Y-tunnus
JAMK University of Applied Sciences	PL 207 FI-40101 Jyväskylä FINLAND	0207438100 +358 20 743 8100	(014) 4499694 +358 14 4499694	www.jamk.fi	1006550-2