# Case 2. Tunkeutumisen analysoiminen

Tässä tehtävässä on käytetty luvallisesti hyväksi tiedostoja, jotka on saatu Malware Traffic Analysis -palvelusta (brad@malware\_traffic). Tiedostoja on muutettu tehtävään sopivaan muotoon.

Tehtävä on laadittu niin, että sen pystyy tekemään vaihtoehtoisilla tavoilla riippuen käytössä olevista ohjelmistoista/mahdollisuuksista/innosta/pohjatiedoista:

* Jos pystyt käyttämään [SecurityOnion](https://securityonion.net/)- tai muuta IDS-järjestelmää, niin niitä saa ja kannattaa käyttää hyväksi (huomioi ajankohdaksi tammikuu 2019).
* Jos käytössäsi on vain Wireshark-ohjelma, niin tee tehtävä katsomalla SecurityOnioniin liittyvät kuvat ja tekemällä loput analyysistä Wiresharkilla itse.
* Tai tee jollakin omavalintaisella tavallasi mutta muista kertoa siitä palautuksen yhteydessä.

# Tehtävä

**Tehtävänä on analysoida erään tietomurron alkuna ollut verkkoon tunkeutuminen.**

1. *Noin 70% tietomurroista saa alkunsa käyttäjän toimista - Jan Mickos CGI*

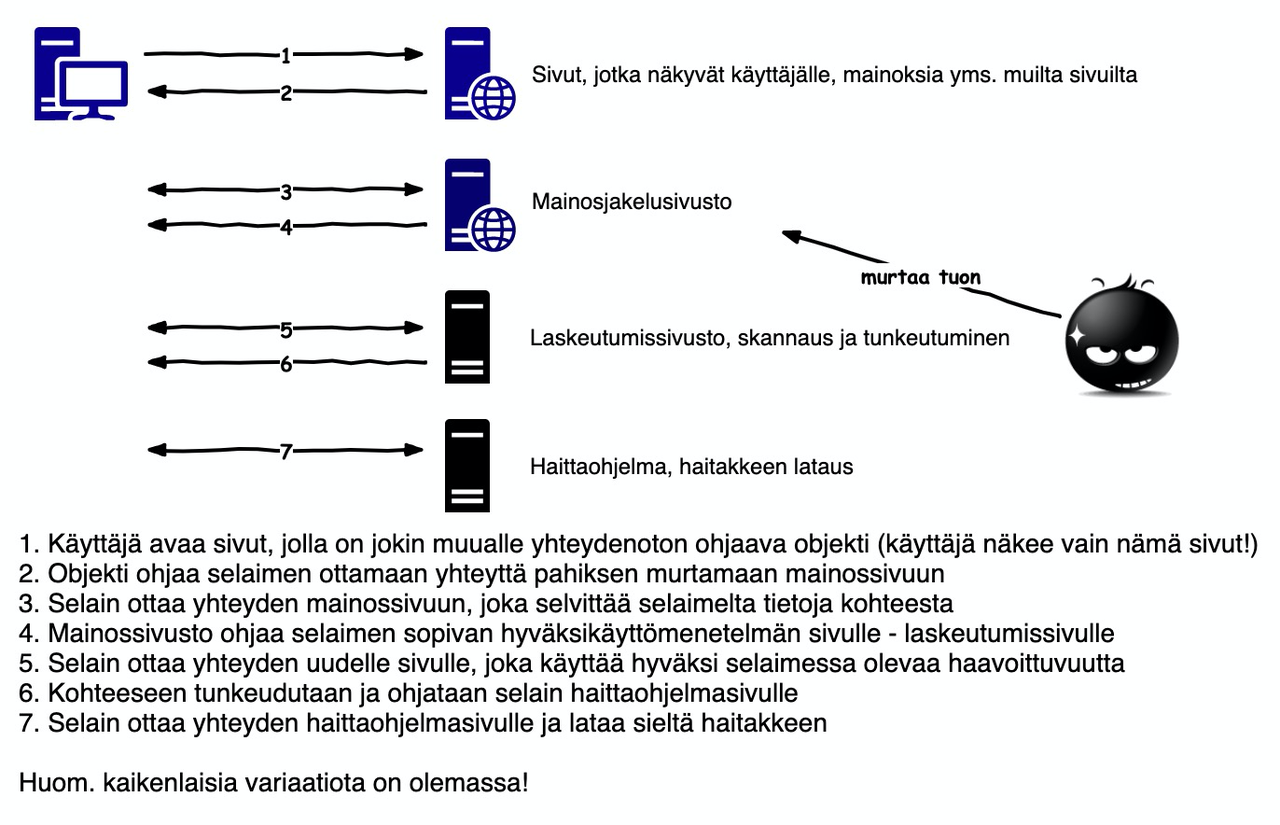
Käy läpi alla oleva skenaario ja materiaalit. **Vastaa tehtävässä oleviin kysymyksiin** ja palauta vastauksesi tallentamalla se palautuskansioon ja merkitse tehtävä Case2 suoritetuksi. Vastauksia tulee tukemalla ottamalla kuvakaappauksia esim. wiresharkin sopivista löydetyistä tiedoista. Tehtävän saa tehdä pienryhmissä mutta jokaisen on tehtävä palautus ja merkintä itse.

## Pohjatietoja (googleta)

1. Selvitä lyhyesti, mitä tarkoittaa/mikä on Exploit Kit?
2. Mihin ohjelmallisiin heikkouksiin (mihin ohjelmiin) Exploit Kitit yleensä iskevät kyntensä kiinni? Löydätkö muutamia?
3. Mitkä ovat olleet viime vuosien tunnetuimpia Exploit Kitejä? Etsi pari esimerkkiä ja niihin linkit vastaukseksi.
4. Mikä voisi olla hyvä suomennos Exploit Kit:lle?

## Analysointi

Alla on kuva, jossa on kaavio erään Exploit Kitin toiminnasta. Tutustu kuvaan ja analysoi sitten skenaarioon annettua dataa. Vastaa loppuihin kysymyksiin.



Tarvittavan pcap-tiedoston saat ladattua alta. **Tiedosto sisältää haittaohjelmia** (siis siellä pcap-tiedoston sisällä). Niitä ei ole vaarallista ladata koneelle pcap-tiedostomuodossa mutta jos tallennat ne sieltä tiedostoiksi (Export Objects), niin **älä missään nimessä aja niitä koneella**!

Voi myös olla, että joku virustorjuntaohjelma estää tiedoston lataamisen - onnittelut, käytössäsi on todella tarkka virustorjutaohjelmisto!

<https://www.dropbox.com/s/rd5yzyt59pwqxa6/case2.pcap?dl=0>

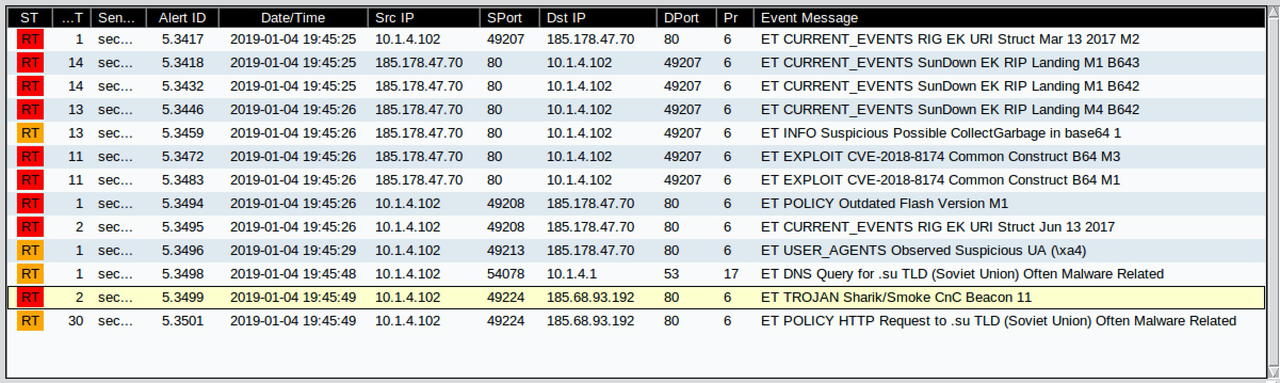
SecurityOnionilla saa asennuksen ja käyttöönoton jälkeen pcap-tiedoston ajettua komennolla so-import-pcap. Oheisessa linkissä lisätietoja:

https://securityonion.readthedocs.io/en/latest/so-import-pcap.html

Wiresharkilla saat ladatun pcap-tiedoston aukaistua normaalisti. Jotta tehtävään liittyvät maakoodit saa selville, tulee Wiresharkiin asentaa lokaatiotiedot, esim- MaxMind Geolite2 (ilmainen mutta vaatii rekisteröitymisen). Asennus tapahtuu seuraavan ohjeen mukaan: <https://wiki.wireshark.org/HowToUseGeoIP>

## Skenaario

Eräänä päivänä HaiTek Ltd:n tunkeutumisenhavaitsemisjärjestelmä näyttää tältä (huom. kuva Squirt-hälytysohjelmasta):



## Kysymyksiä

Etsi vastaukset kysymyksiin tekemällä analyysi käyttämällä Wiresharkia (tai muuta valitsemaasi tapaa):

1. Pitäisikö HaiTekissa olla huolissaan? Miksi/miksi ei?
2. Milloin hyökkäys tapahtui ja kauanko se kaiken kaikkiaan kesti?
3. Mikä Exploit Kit on skenaariossa kyseessä (vinkki: ei ole auringonlasku vaikka siltä ehkä näyttää)?
4. Selvitä skenaarioon liittyvät yksityiskohdat huomioiden aikaisempi kuva Exploit Kitin toiminnasta:
   1. Mikä on kohteen ip-osoite?
   2. Mikä on sen sivun IP-osoite, joka näkyy käyttäjän selaimessa? Entä URL-osoite?
   3. Mikä on mainosjakelusivuston ip-osoite ja domain-nimi?
   4. Mikä on laskeutumissivun ip-osoite?
   5. Mikä on haittaohjelmasivun ip-osoite?
5. Missä maassa (todennäköisesti) on skenaarion lailliset ja laittomat palvelimet? (tarvitse lokaatiedot tätä varten)
6. Mitä tarkoittaa IDS-järjestelmän (kuva yllä) havaitsema CnC (= C2)?
7. Minkä laitteiden välinen liikenne on ollut salattua? Voisiko siihen olla joku syy?
8. Liittyykö skenaarioon muita IP-osoiteita? Mitä ja mitä laitteita ne ovat?
9. Millainen oli se objekti, joka ohjasi selaimen murretulle mainossivustolle?
10. Mikä komponentti oli kohdelaitteessa (selaimessa) haavoittuvainen?
11. Mikä haittaohjelma kohteeseen ladattiin? Mitä se mahdollisesti tekee (googleta)?

Selvitä seuraavaksi, onko kohteeseen ladatut tiedostot tunnistettuja haittaohjelmia. Kohteeseen ladattiin kolme suurempaa tiedostoa (ne voi halutessaan erottaa Wiresharkilla pcap-tiedostosta). **Älä aja kyseisiä tiedostoja koneellasi**! Niitä ei kuitenkaan ole välttämätöntä erottaa tiedostoiksia vaan vastaavat tiedot on annettu alla.

Virustotal on palvelu, jossa voi tarkistaa tiedoston haitallisuuden (tunnistetaanko haitalliseksi). Se voidaan tehdä lataamalla tiedosto palveluun tai vielä kätevämmin - luomalla tiedostosta sha256-tiiviste ja hakemalla tietoja sen perusteella.

https://www.virustotal.com/gui/home/search

Voit testata prosessin millä tahansa omalla tiedostollasi. Luo tiedostosta ensin SHA256-tiiviste ja kokeile sitten hakea siitä tietoja Virustotal-palvelusta.

https://emn178.github.io/online-tools/sha256\_checksum.html

Tiedostoista filu2 ja filu3 toinen on haitallinen. Mikäli et halua ladata tiedostoja koneellesi (irrottaa niitä pcap-tiedostosta), niin alla on valmiiksi niiden SHA256-tiivisteet.

Filu2 tiiviste

d7bb1f853e55fa7f80f04bf1cd4b20129843a6821881dff0bf860dbcfbf33bac

Filu3 tiiviste

134c94abf9760683c74d4ebd54a06ae0db85320d77f97490986e4fdfea8c04ca

1. Käytä yllä annettuja tiivistearvoja sha256-tiivistearvoja ja testaa virustotal-palvelussa onko tiedostot tunnetusti haitallisia vai ei? Tunnistaako sen haitalliseksi suuri suomalainen virustorjuntaohjelmisto?
2. Mihin haavoittuvuuteen (CVE-tunniste) haittaohjelma liittyi? Mikä on CVE-tunniste?
3. Kuvaa omin sanoin mitä tapahtui, niin että sen ymmärtäisi oma isäsi/äitisi/mummosi/pappasi/puolisosi/pomosi jne. (= joku jolle tietoturva-asiat ei ole kovinkaan tuttuja ja jota ei todellakaan kiinnosta atk-terminologia)
4. Mikä seuraavista olisi todennäköisimmin estänyt tunkeutumisen (voit perustella, jos haluat:
   1. käyttäjän parempi valveutuneisuus
   2. virustorjuntaohjelma (vinkki: se toinenkin filu oli haittaohjelma)
   3. palomuuri
   4. ajantasaiset päivitykset

LOPPU