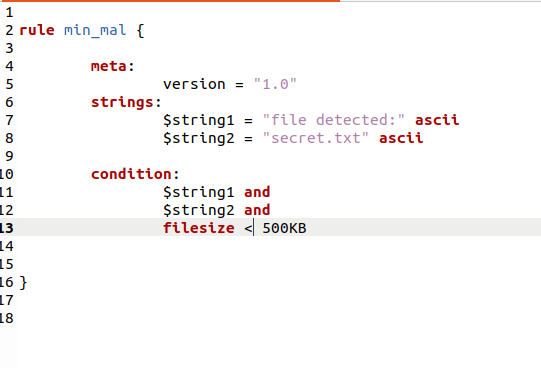
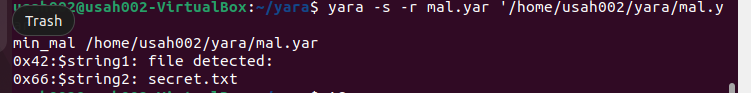
1. Skriver **sudo apt install yara** i ubuntu terminalen
2. Hvis du får opp feilmelding
3. Skriver : sudo dpkg –configure -a og prøver igjen ( det virker)
4. Lager en path : mkdir /home/usah002/yara/
5. https://drive.google.com/drive/folders/18Ob\_2NRMh5RFl31XmddMImNBRBWdcduJ laster ned filene manuelt og legger dem deretter inn i yara filen

oppgave 2 :

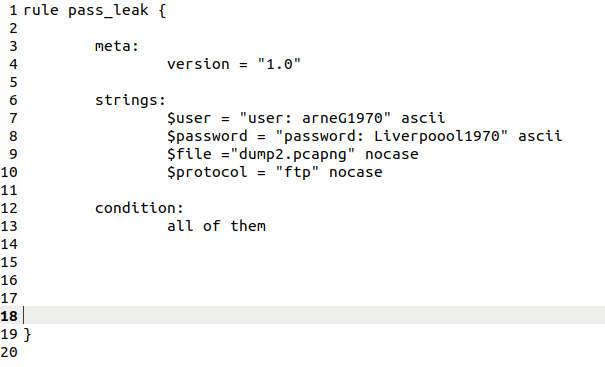
klikker på mal.yar I ubuntu og endrer slik at den detekterer bare secret.txt og legger inn filesize < 500kb for å få opp filnavnet og lagrer



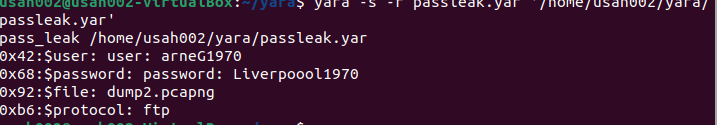
Deretter skriver yara -r -s mal.yar (og kopierer inn pathen til filen) i terminalen og får opp som forventet:/



Oppgave 3



Lager en ny regel: tester med terminalen og får opp leaked bruker og passord:



Oppgave 4 :

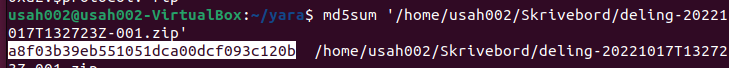
**Lag en deteksjon for fil.zip. Ta med filesize i condition for å øke treffsikkerheten. Ta med md5sum i**

**condition for å få treffsikkerheten enda bedre. (her må dere bruke hash modulen, google er din venn).**

**For å få til dette må du vite md5summen til filen. Ta den md5summen og gå til virustotal. Søk etter**

**md5summen der, hvilken fil er det vi har med å gjøre?**

**Skriver md5sum+ <<filnavn>> og får opp md5summen**

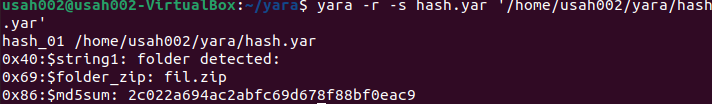
****

**Lager en yar fil med navnet hash\_01:**

**Et bilde som inneholder tekst

Automatisk generert beskrivelse**

Sjekker



Oppgave 5:

**her finner dere mange regler for deteksjon av APTer. Se på APT\_Sofacy\_Fysbis.yar. Hvilken APT er**

**dette? Klarer dere å finne gruppen igjen i Mitre Att&ck? Studer matrisen til gruppen**

I APT\_Sofacy\_Fysbis.yar. er dette en :

Detects Sofacy Fysbis Linux Backdoor\_Naikon\_APT\_Sample1 er APT som er brukt og dette er command and interpreter i execution matrisen som denne apt-en bruker. Denne apt-en er også klassifisert som en malware ifølge mitra att&ck.org

Denne ble brukt av den russiske hackergruppen APT28

Oppgave 6 :

Du jobber som analytiker i en SOC. Fra en god kilde får du beskjed om at en APT dere frykter baserer

<https://www.ipaddressguide.com/cidr> og skriver inn ip addressen :

infrastrukturen sin på 204.12.12.32/27

Hva er første IP i range?

Hva er siste IP i range?

Klarer du å finne ut hvilken APT det er?

2^(32-27) = 2^5=32 32+32= gir 64 addressen ender på 63

Første adresse er : 204.12.12.32

Siste er =204.12.12.63

Bruker whois på ip adressen og finner ut av at den tilhører money paper inc

Google : CIDR 204.12.12.32 apt finner : APT28 og APT29