Oblig 4 - Skadevare

IN2120 - høst 2023

Logg deg inn på sandbox-maskinen du har blitt tildelt, med RDP (som i oblig 1).

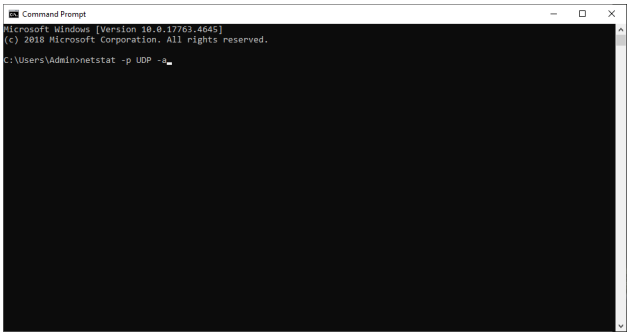
På Skrivebordet, i mappen for "Oblig 4" vil du finne programmet **Snaweetbook** fra **Gopplezonsoft**. Du kan tenke deg at dette er et program som "alle" bruker, "fordi det funker", men at du er litt skeptisk. I resten av laben skal du undersøke om dette programmet gjør noe suspekt.
Regn for sikkerhets skyld med at så lenge programmet kjører, er det ikke privat hva du gjør på maskinen.

Begynn med å dobbeltklikke på programmet. Det skal sprette opp et vindu. Snaweetbook er en personlig assistent", og siden dette bare er en labøvelse gjør den ikke mer enn å sprette opp en påminner om å være produktiv annethvert minutt. I det virkelige liv kunne Snaweetbook for eksempel vært et program som synkroniserte seg med kalenderen på mobiltelefonen din, som minte deg på Facebook-events eller som fulgte opp møteforespørsler du fikk på mail.

Du mistenker at Snaweetbook sender litt for mye informasjon om deg til Gopplezonsoft.

Åpne derfor en Windows-kommandolinje (**cmd.exe**, som du finner som "**Windows System -> Command Prompt**"i startmenyen) og kjør kommandoen:

```
netstat -p UDP -a
```



Programmet **netstat** vil vise deg hvilke Internet-forbindelser maskinen din opprettholder og lytter etter. Nærmere bestemt vil du se en liste med IP-adresser (Internet-adresser) og portnummer (som brukes for å skille mellom ulike forbindelser på samme maskin) i formatet <ip>:<port>, hvilken protokoll som brukes og hvilken tilstand porten er i (for eksempel om maskinen din har en etablert forbindelse, eller lytter etter innkommende forbindelser). Bryteren "-p UDP" velger at du skal se UDP-forbindelser istedenfor TCP, mens bryteren "-a" vil vise deg alle forbindelser (ikke bare de som er aktive, men de som lytter også). Prøv deg veldig gjerne frem med bare `netstat` eller `netstat -a`, men vi kan si så mye som at det Snaweetbook driver med her kommer til syne med `netstat -p UDP -a`. Vanligvis må man grave litt i hva som brukes til hva for å skjønne hvilke porter og forbindelser som er suspekte. Men her ser du kanskje med en gang at en av linjene ser ut som noe mer enn bare tilfeldige tall?

Oppgave 1

Hvilken ip og hvilket portnummer er det som dukker opp i lista og som skiller seg mest ut? Skriv svaret på formen <ip>:<port> (for eksempel 1.2.3.4:567). Er du usikker kan du prøve netstat-kommandoen med og uten Snaweetbook kjørende i bakgrunnen og sammenlikne.

Netstat-sjekken din gjør deg ikke akkurat mindre mistenksom, så du bestemmer deg for å bruke maskinen litt, som en vanlig bruker, for å se hva Snaweetbook finner på da.

En **KEYLOGGER** er kode som logger hvilke tastetrykk man skriver inn på en maskin. Dette er en stor sikkerhetsrisiko, ettersom keyloggere kan fange opp både passord, private meldinger, hva man ser etter på Internet osv. og dele denne informasjonen med folk man helst vil holde det hemmelig for. En keylogger kan altså gjøre at både kryptering av filer, forsøk på å være anonym på Internet, innlogging med brukernavn og passord, og andre slike sikkerhetsmekanismer mister sin beskyttende effekt.

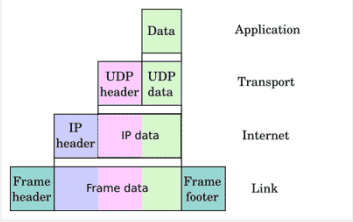
For å se om Snaweetbook inneholder en keylogger, eller sender noe annet muffins over Internet, starter du opp **Wireshark**. Wireshark er en såkalt *packet sniffer*, som kan fange opp hva som sendes til og fra din maskin. Vi har laget en snill oblig, så du behøver ikke å se etter forbindelser til andre maskiner, men velg "Adapter for loopback traffic capture"(forbindelser til egen maskin) i Wireshark. Vi ser etter UDP-pakker, så skriv inn og velg "UDP"i filter-linjen du finner øverst i vinduet og trykk på pila til høyre (hele input-linja skal bli grønn).

Prøv deretter å gå inn på noen nettsider, skrive litt i Notepad og i det hele tatt bruke tastaturet, frem til Snaweetbook har rukket å sprette opp minst 1 påminner om å være produktiv etter at du startet Wireshark. Så sjekker du i Wireshark hvilke Internet-pakker som er fanget opp, og klikker litt på dem for å se innholdet.

For noen vil dette med *pakker* være et helt nytt konsept:

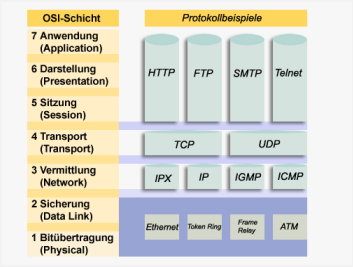
På litt samme måte som brev i konvolutter, sendes informasjon over Internet i pakker (packets). Hver pakke må da ha en slags oppsummering av hvor den skal, hvor den kommer fra, hva slags innhold den har, en indikasjon på om den er hel, osv., på samme måte som en konvolutt, slik at den skal bli sendt og behandlet riktig.

Denne informasjonen puttes som regel først, i en såkalt *header*. Selve innholdet man vil overføre, tilsvarende selve brevet, kalles da *data* eller *payload*. I noen sammenhenger bruker man også en *footer*, som gir noe avsluttende informasjon om dataene. Slike "data om dataene" som en header eller en footer altså er eksempler på, kalles *metadata* — av gresk "meta" ("μετά"), som betyr noe sånt som over/utenfor/forbi (dette er ikke funnet opp av Facebook). Metadata er vanlig i filer også, og headere og footere er et generelt konsept som for eksempel brukes i bildefiler, programfiler og videofiler. Annen "informasjon om informasjonen" kalles også metadata, så metadata om mobiltelefonbruken din er for eksempel hvem du har snakket med, når og hvor (ikke innholdet i samtalene).



En skisse av hvordan headerne følger etter hverandre i en UDP-pakke.
(Kilde: Serverfault)

På Internet er pakker som regel pakket inn i flere lag med metadata, som et brev i flere konvolutter, beregnet på hvert sitt nivå av sortering og behandling. De har derfor som regel flere headere etter hverandre. Det er vanlig at det kommer først en IP-header (Internet-adresse), deretter en TCP eller UDP header (for å holde styr på ulike forbindelser til samme maskin), deretter selve dataene. Det kan også være en header og footer utenpå dette igjen, for eksempel en såkalt Ethernet-frame. Og utenpå dette igjen kan det hende fysiske dingser bruker sine egne kontrollsignaler for rent fysisk overføring fra A til B, som pelles av igjen før du får noe inn på din maskin. En veldig vanlig teoretisk idé for hvordan dette deles inn i ulike lag (layers) er OSI-modellen. Det hender ofte at OSI-lagene glir litt inn i hverandre når noe er laget for den virkelige verden, men konseptet er greit å være klar over.



En tysk oppsummering av de 7 OSI-lagene, som også gir eksempler på hva som hører inn under hvert lag.
(Kilde: Public domain)

Det viktige her er bare at du får en slags "hands-on" forståelse for hva Internet-pakker er. Hvis du trykker på en linje med noe som er snappet opp i Wireshark, vil Wireshark vise deg en masse tolkning i tillegg til bare en hex dump av hele pakken. Hvis du trykker deg videre inn i denne tolkningen (for eksempel ved å trykke deg inn på "User Datagram Protocol" (UDP) og "Destination port") vil Wireshark markere med blått i hex dumpen hvor denne informasjonen finnes i pakken. Prøv deg gjerne litt frem, til du er komfortabel med konseptene pakke, header, payload og metadata!

Oppgave 2

Det aller første data-innholdet i hver Internet-pakke som sendes ut av Snaweetbook er en såkalt "tag", slik som <dette>. Hva er ordet mellom hakeparantesene i start-taggen fra Snaweetbook?

Gopplezonsoft beklager "feilen" som gjorde at disse Internet-pakkene ble sendt ut... De skylder på debug/feilsøkingskode under utviklingen av Snaweetbook, som de ved en feil hadde glemt å deaktivere i det ferdige produktet. Nå har de laget en ny versjon av Snaweetbook der denne "feilen" er reparert!

Mens Snaweetbook kjører (enten i bakgrunnen eller forgrunnen), tast inn ordet `upgrade` på tastaturet. (Husk å slippe hver tast før du trykker neste: Noen skriver så fort at de holder inne flere taster samtidig, og da fungerer det ikke.) Snaweetbook skal sprette opp en liten dialogboks som forteller at du nå har oppgradert programmet.

Skriv på nytt inn kommandoen `netstat -p UDP -a` i en Windows-kommandolinje. Nå ser vel alt greit ut?

En **ROOTKIT** er kode som skal gjøre det lettere å beholde tilgangen man har skaffet seg på en maskin. Typiske ting en rootkit vil gjøre er for eksempel å slette sikkerhetslogger, skjule filer/programmer/Internet-forbindelser, deaktivere virus-scanning eller åpne muligheten for enkel fjerninnlogging. Rootkits kan være veldig avanserte og bytte ut komponenter i selve operativsystemet slik at informasjonen man "ser" rett og slett ikke stemmer.

Oppgave 3

Fyr opp Wireshark igjen, hvis du ikke fortsatt har den oppe. Er det fortsatt noe som skjer når Reminder (den oppgraderte Snaweetbook) spretter opp påminnere om å være produktiv? Hvilket portnummer er det i så fall Reminder forsøker å sende data til?

Dette betyr faktisk ikke nødvendigvis at netstat lyver! Det netstat viste oss i starten av laben var at Snaweetbook satt og lyttet etter inkommende Internet-pakker. UDP krever ikke at man oppretter en forbindelse først, så det er fullt mulig for et program å sende avgårde UDP-pakker uten å sitte og lytte etter noe som helst. Et sleipt program kan til og med opprette og lukke TCP-forbindelser (*sånne som etableres ved å sende melding frem og tilbake, og som brukes til for eksempel nettsider eller e-mail*) så fort at du ikke rekker å se dem.

Men du husker at det faktisk sto noe og lyttet forrige gang, så nå vil du forsøke å koble deg til det du så sist, for å sjekke om netstat lyver...

For å sende data direkte til en internet-forbindelse bruker man ofte **netcat**.

Dette er egentlig et Linux-program, så hvis du vil kan du trykke på Cygwin-ikonet på skrivebordet og **skrive inn Linux-kommandoen** `nc -u <ip> <port>`**, der <ip> og <port> er de du så at sto og lyttet tidligere (i Oppgave 1).**

Alternativt kan du bruke en Windows-versjon av netcat som følger med programmet nmap, ved å **skrive inn** `ncat -u <ip> <port>` **i en Windows-kommandolinje.**

I begge tilfeller betyr "-u" at du vil kommunisere via UDP. Siden UDP kan sende "i blinde" uten noen fast forbindelse frem og tilbake, må du regne med at netcat bare står der når du har skrevet inn kommandoen, uansett, klar til å vise deg hva den mottar av Internet-pakker eller til å sende avgårde det du skriver inn.

Oppgave 4

Prøv nå å skrive inn ordet "CLEAN"(etterfulgt av linjeskift), slik at dette blir sendt via netcat. Får du noe svar? Hva er i så fall svaret?

Hint: Du kan komme deg ut av netcat igjen ved å trykke `[ctrl+c]` *på tastaturet.*

Nå ser det ut som Snaweetbook/Reminder sitter og lytter til forbindelser selv om netstat sier den ikke gjør det... Er det fortsatt den ekte, umodifiserte versjonen av netstat som kjører?

Oppgave 5

I hvilken mappe ligger den versjonen av netstat som kjøres nå?

Hint: Siste oppgave er med vilje litt mer tricky enn de andre. For å skjønne hva som foregår: Finn ut hva en PATH-variabel er for noe, sjekk hva PATH-variabelen er på labmaskinen din nå, og undersøk hvor netstat.exe ligger eller skal ligge.