Computer Networks Attack Strategies Day-2

* Kommunikation gennem de forskellige lag og protokoller.
* TCP er forholdsvist tungt på grund af kvittering og den faste forbindelse.
* UDP er forholdsvist meget lettere da man bare sender pakker derudaf.
* Internetlaget tager sig af at route pakker gennem internettet.
* Netværkslaget har at gøre med tråde og Ethernet Networks som vi kobler til.
* Routeren bestemmer hvor hen i verdenen vi skal hen. Routeren kigger i internetlaget efter ip-adressen til den næste router som det næste trin på vejen eller selve slutdestinationen.
* Lagene snakker med hinanden hen over protokol, men snakker også ned gennem lagene fra applikation til transport til internet til Network. Det er dog stadig de samme lag der læser hinandens kommunikation/pakker, de skal bare ned gennem lagene for at nå på igen til det samme lag på den tilsvarene side. Vi skal ned igennem lagene og op igen på den anden side.
* Den eneste måde vi kan snakke sammen med vores pakker, er ved at gå gennem lagene.

En netværksprotokol er et regelsæt så begge parter kan snakke sammen.

Application layer pakker når fra A til B gennem de forskellige lag, startende med transport, til internet til Network.

Formålet med Transport Layer er at bryde data ned i mindre pakker o0g sende dem gennem end to end communication.

UDP er mindre tungt og bruges tit i forbindelse med afsendelse af meget data i real time, hvor det ikke er nødvendigt at vide om pakkerne når frem. For eksempel i streaming, ved et par mistede pakker bare virke som en clinch på skærmen i den anden ende.

En DNS-server kan modtage vores søgning efter et bestemt domæne, og returnere den tilhørende IP.

Når vi på et lokalt netværk bliver vi tildelt en IP-adresse af DHCP-serveren på vores router.

Man kan sætte sin DHCP server på sin router op til at udbyde den samme lokale Ip adresse til enkelte enheder op baggrund af enhedens MAC adresse (Media Access Controller, kommunikation mellem netværkskort).

Man kan lave angreb meget langt ned på protokollagene.

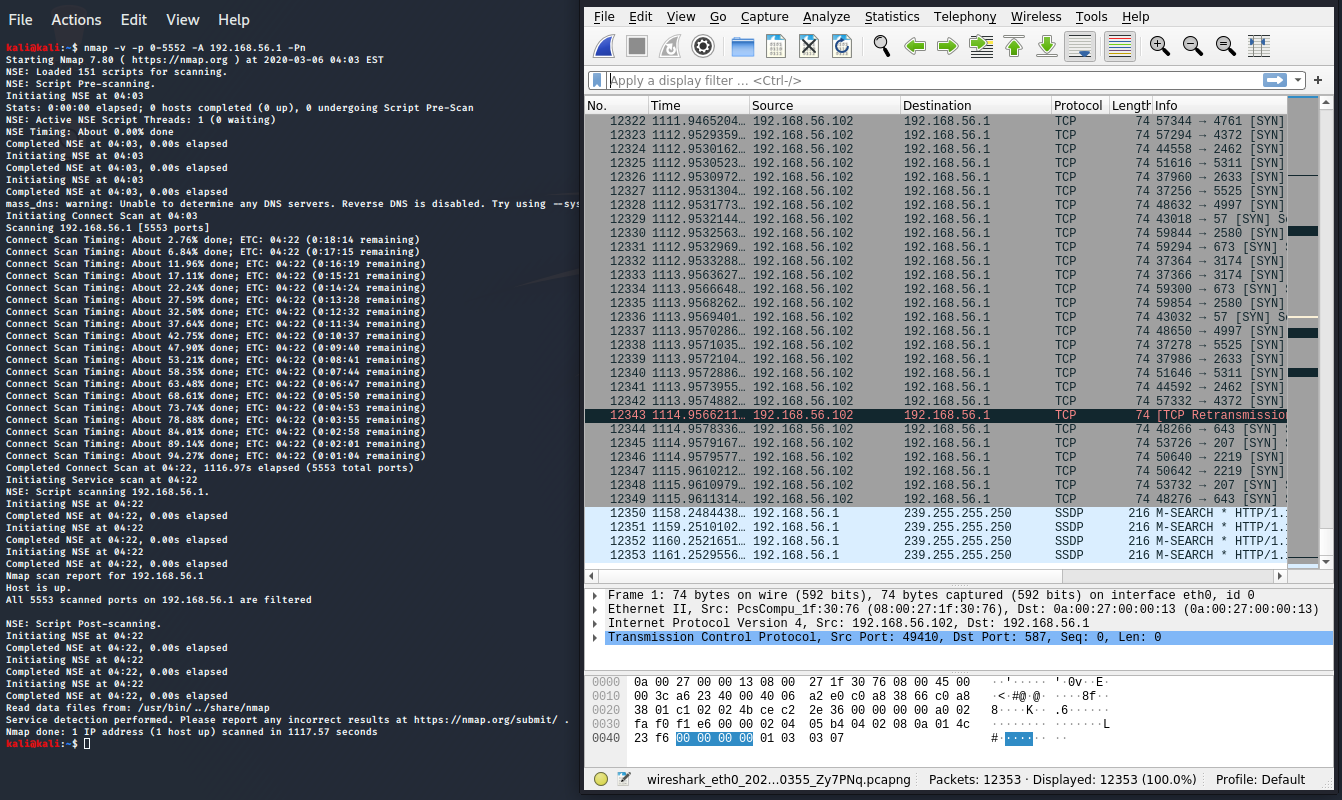
En hver TCP forbindelse starter med et SYN, derefter et SYN-ACK, og derefter en ACK.

Man har tidligere som hacker kunne blive ved med at spam sende flere SYN afsted og derved lave et Denial Of Service Attack (DoS angreb) da forbindelserne vil blive udmattet (Løbe ud af hukommelse).

DNS systems can be acctakced can for examble be Domain hijacking, where an attacker changes the direction f traffic away from the original server and over to new sceamy locations. Another….

Med ARP-spoofing kan man skjule sig som middle-man mellem din computer og den loakle router gateway. Herved kan man få folk til at sende request med information til den forklæte hackers computer som så kan misbruge det.

Spoofing – nogen der udgiver sig for noget de ikke er.

nmap -V(Versitile) -p(Port range) 0-5552 -A(Agressive) 192.168.56.1 (Gem sample)  


nmap er tæt på at være Denial of Service attack DoS da vi sender så mange pakker. Stort set alle professionelle sites vil kunne detektere det.

Hackere specialiserer sig typisk.

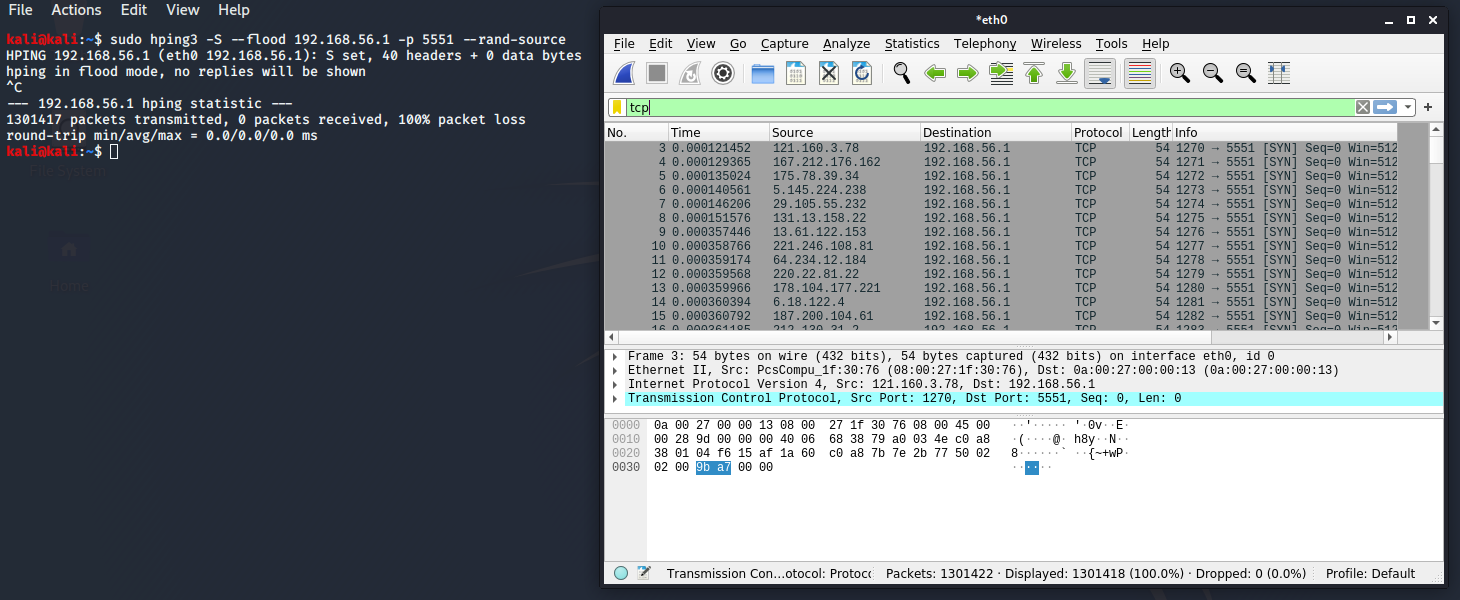
På Windows kan vi kunne se information på netværket mellem min maskine og den jeg snakker med.

sudo hping3 -S -V 192.168.56.1 -p 5551

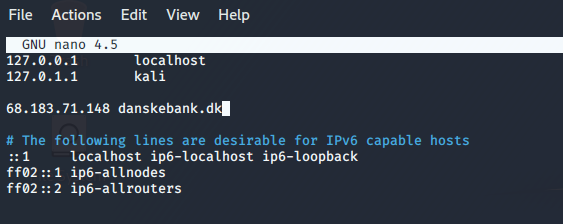
RST -restall – luk forbindelsen

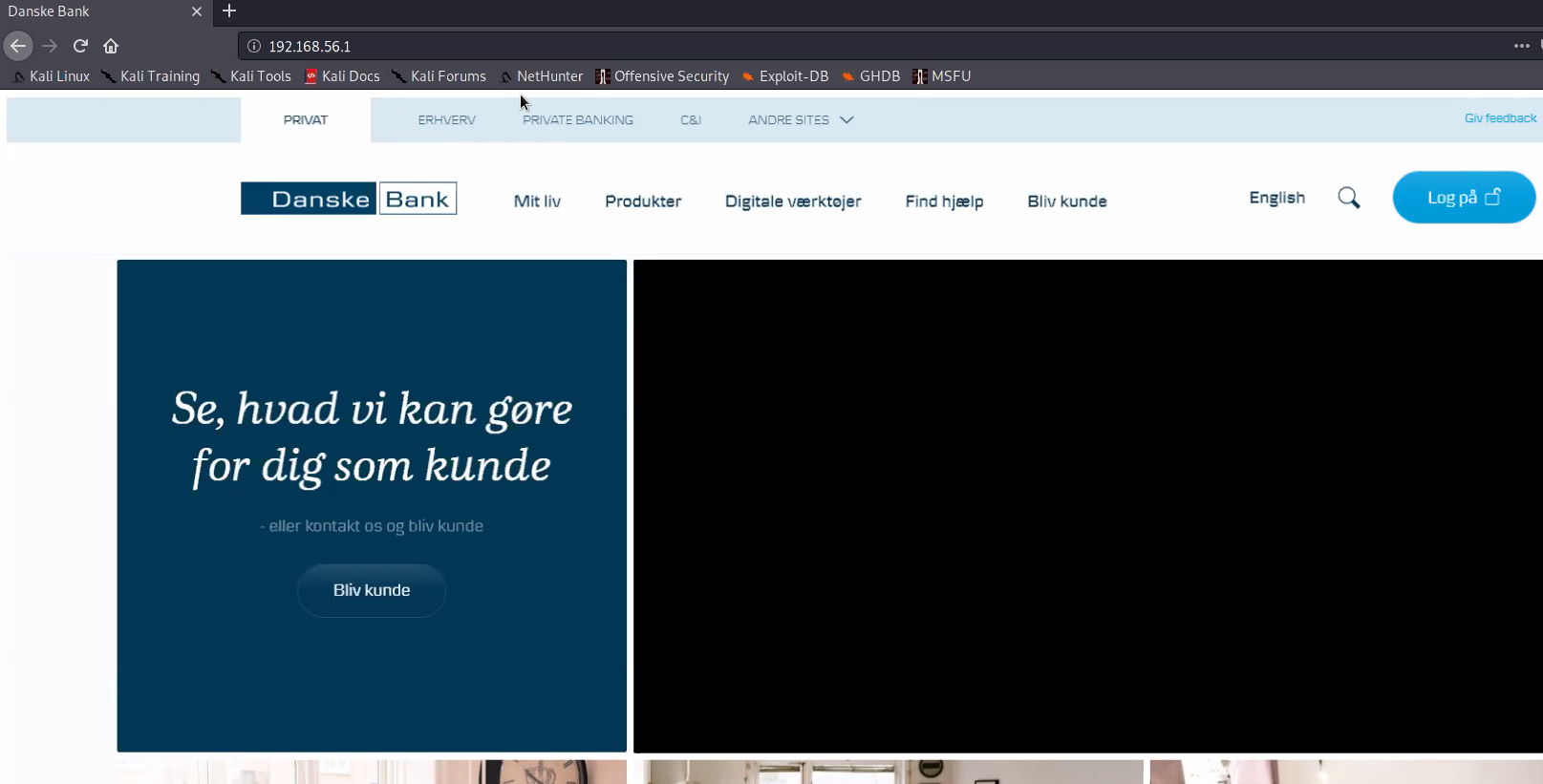
hping3 er et værktøj der kan samle of afsende pakker og analysere på disse pakker, packet generator og analysator.

Vi kan lavet et illustreret spook attack ved at skrive hping3 -S -V  192.168.56.1-p 5551 --rand-source ved at

Vi kan flodde og forsøge at lave et DoS ved at køre ved at skrive hping3 -S --flood  192.168.56.1-p 5551 --rand-source, hvorved der sendes enormt mange pakker i et fiorsøg på at lægge serveren(I vores tilfælde TCP-Ip stack) ned.  
  
  
Da vi køre den lokalt vil dette ikke have den store effekt, men hvis der nu var flere bots der gjorde dette kunne det lægge forindelsen ned.

Man kan gå ned og åbne den fil der indeholder vores lokale DNS cashe hvis man får adgang til selve maskinen, f.eks gennem en usb dongle. Dette virker kun hvis personen aldrig har brugt http//:danskebank.dk sp den ikke er blevet cashet før, og at den ikke er https.

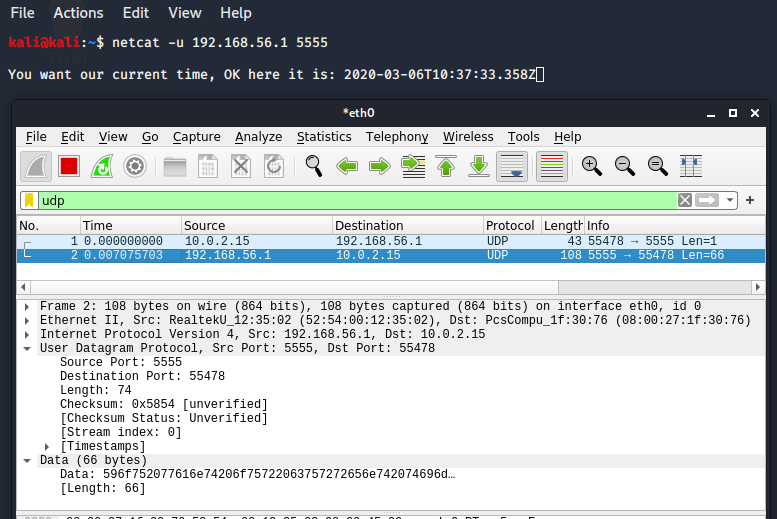
Her ændrer vi i vores DNS cashe i sudo nano /etc/hosts og indsætter 68.183.71.148 danskebank.dk, hvilket vil omdirigere brugeren når de i browseren prøver at tilgp danskebank.dk, til vores hackerside. Dette er i princippet et man in the middle attack.  


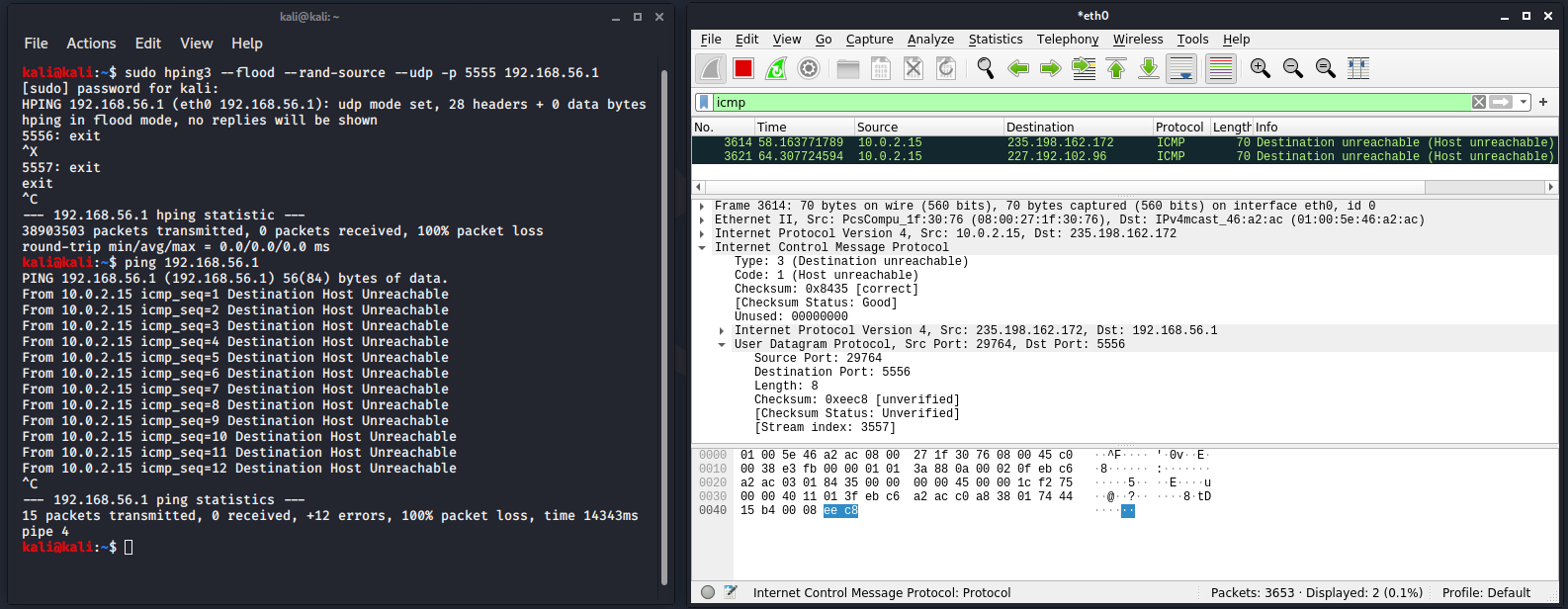
Hvis vi tilgår http//:danskebank.dk nu og vi har forgiftet DNS cashen og brugeren ikke ser at der kun står danske band uden ssl, har vi i princippet lavet et man in the middle attack. Dette kan kun bruges en gang, da hvis vi tilgår danske bank vil blive stoppet. Grundideen er at hvis man en gang har været på en site med https kan man ikke få lov at nedgradere til at tilgå med http fra den browser.  


Eksempel på DoS på en simpel UDP server ved flooding

UDP er typisk lidt mere kompliceret end TCP da vi selv skal lave vores pakke.

Netcat

Netcat -u 192.168.56.1 5555  


Las os prøve at lave et denial of service attack DOS ved at køre sudo hping3 –flood –rand-source –udp -p 5555 192.168.56.1  
Vi kan se at vores test server gik ned og ikke kan pinges eller retunere netcat mere.  


For at dette kan fungere skal man være på en bridged connection og have fået en tilsvarende ny IP fra den rigtige router. Min computer kan ikke længere komme på netværket og arpspoof ser ud til at fungere.