Linuxadministration I 1DV417 - Laboration 5
Brandvägg och DNS

Marcus Wilhelmsson
marcus.wilhelmsson@lnu.se

19 februari 2013

Innehåll

1 Inledning och mål

Två viktiga tjänster i nätverket är brandvägg och DNS. Brandväggar behövs dels för att skydda det interna nätverket mot intrång utifrån, men även för att förhindra att otillåten trafik tar sig ut från nätverket. Under denna laboration ska du därför undersöka hur en brandvägg kan konfigureras för att skydda ett nätverk ur olika synvinklar. Den vanligaste brandväggen i Linux är *netfilter/iptables*, du kommer därför bekanta dig med denna brandvägg.

För att förenkla kommunikationen över Internet och intranät används DNS-servrar. I denna laboration ska du undersöka hur zoner i DNS-servern BIND konfigureras och administreras. Du kommer att använda dig av två DNS-servrar, en master och en slave. Efter genomgången laboration kommer du ha praktisk kännedom om hur du:

- installerar och konfigureras en brandvägg baserad på IPtables.
- installerar och konfigurerar DNS-servern BIND.

2 Material och genomförande

Laborationen kommer genomföras i VMware Workstation som tillhandahåller möjligheten att köra flera virtuella datorer i en fysisk. Utför laborationens uppgifter och moment samt dokumentera vad du kommer fram till på de olika delarna. Vid redovisning av laborationen ska du med hjälp av laborationsrapporten på ett komplett sätt redovisa *vad* du har gjort, *hur* du har gjort det samt *vad* du kom fram till och *varför* du kom fram till det du gjorde.

3 Förberedelseuppgifter

Laborationen har två förberedelseuppgift. Se till att du genomfört förberedelseuppgifterna innan du påbörjar laborationen då du med hjälp av förberedelseuppgifterna ska genomföra laborationen.

1. Undersök vilka ICMP-paket som skickas och tas emot som svar från en exekvering av *ping*.
2. Ta reda på hur du aktiverar IP-forwarding permanent i Ubuntu.
3. Läs följande kapitel i boken:
    - Kapitel 17
    - Kapitel 22, sid. 935 – 937

4 Installation och konfiguration av Ubuntu

Denna laboration kräver fyra Ubuntu-maskiner

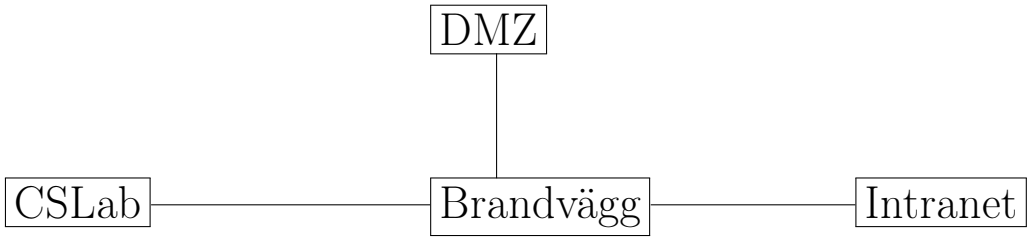
4.1 Installera nya maskiner

1. Installera en ny Ubuntu-server som ska agera brandvägg.
2. Förutom brandväggen ska du ha en Ubuntu-server som agerar webbserver i DMZ, två DNS-servrar samt en klient. Konfigurera maskinerna med lämpliga IP-adresser samt installera lämpliga paket för att uppnå den funktionalitet du önskar. Se även till att du vet hur du kopplar dig till CSLab-nätverket innan du påbörjar laborationen.

5 Brandvägg med iptables

Det är nu dags att konfigurera en brandvägg baserad på iptables. Nedan syns en bild på det scenario du ska sätta upp.

5.1 Bekanta dig med scenariot



5.2 Konfigurera iptables

Konfigurera nätverket så att följande krav uppnås. Vidare ska iptables konfigureras så att brandväggspolicyn uppfylls.

1. Sätt lämpliga IP-adresser enligt IP-adresseringsschemat på Hawk Wikin. Tänk på att du endast har ETT 24-bitarsnät att tillgå för adresstilldelning. Subnetta ner detta på ett lämpligt sätt för att kunna adressera både Intranet och DMZ. DMZ ska alltid ligga på det LÄGSTA av dina två subnät. Eftersom du befinner dig i Ny230 ska du använda de IP-serier som är associerade med den salen enligt Hawk Wikin.

2. För att ha en dator i DMZ-nätverket ska du se till att den tidigare installerade webbservern finns inkopplad här.

För att underlätta arbetandet med brandväggen ska du skapa en scriptfil där du skriver in de kommandon du använder för att ställa in brandväggen. Nedan finns ett exempel på hur en sådan fil kan se ut, det är sedan upp till dig att fylla på den med lämpliga regler.

Listing 1: iptables-regler.sh

```
#!/bin/bash

# Rensa alla regler
iptables -F
iptables -t nat -F
iptables -t mangle -F
# Applicera ACCEPT som policy
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -t nat -P PREROUTING ACCEPT
iptables -t nat -P POSTROUTING ACCEPT
```

I exemplet ovan är filen döpt till iptables-regler.sh och körs då genom *./iptables-regler.sh*.

5.2.1 Säkerhetspolicy

- Intranät ska kunna pinga alla datorer på CSLab-nätverket. Datorerna på CSLab-nätverket ska ha tillåtelse att svara tillbaka på dessa ICMP-paket.
- Datorer på Intranet ska kunna pinga brandväggen samt få svar.
- Anslutningar från CSLab till webbservern i DMZ på port 80 ska tillåtas. Webbservern i DMZ ska få svara tillbaka.
- Intranet ska få komma åt webbservern i DMZ på port 80 och webbservern i DMZ ska få svara tillbaka på dessa anslutningar.
- Datorer på Intranet ska få göra anslutningar till datorer i CSLab. Datorer i CSLab ska få svara tillbaka på dessa anslutningar. Datorer på Intranet ska även Source NATas bakom brandväggen när anslutningar görs från dem till CSLab.
- Alla andra anslutningar och paket ska nekas.

5.3 Installera routingprogramvara

Installera och konfigurera OSPF med hjälp av programvaran bird på brandväggen. Använd följande inställningar:

- Router ID: 10.230.x.255 där x motsvarar ditt IP i CSLab-nätet.
- Ta med nätverkskortet som är anslutet mot CSLab i OSPF-arean 0.0.0.0.
- Ta med resterande nätverkskort i OSPF-arean 0.0.0.x.
- Stäng av SNAT-regeln för Intranätet i brandväggen.
- Starta om bird samt kör programmet *birdc* och kör kommandot *configure* för att ladda om konfigurationen.

5.4 Kontrollera funktionalitet

På CSLab-nätverket finns en gemensam Wiki på adressen http://hawk.cslab.net, kontrollera att du kan komma åt denna från din interna klient. CSLab-nätverket har två st root-DNSer på 192.168.231.4 samt 192.168.229.4, sätt dessa IP-adresser som DNS-servrar i klienten temporärt tills du fått upp din egen DNS-struktur i nästa uppgift.

Det är rekommenderat att läsa på om CSLab-nätverket på Wikin om det är något kring nätverket som är oklart.

6 DNS-server med BIND

I denna uppgiften ska du undersöka hur du i Linux sätter upp en DNS-zon med tillhörande servrar. Du kommer i uppgiften att sätta upp två DNS-zoner, en forward lookup zone och en reverse lookup zone. DNS-zonerna kommer administreras av två DNS-servrar, en primär och en sekundär.

6.1 Förberedelser

Eftersom du kommer arbeta med två DNS-servrar behövs två virtuella maskiner enligt nedanstående uppgifter:

- Namn: ns1.aa222bb.ny230.se
- IP: 10.230.x.10
- RootDNS: Se Hawk Wiki
- Namn: ns2.aa222bb.ny230.se
- IP: 10.230.x.11
- RootDNS: Se Hawk Wiki

I byt ut aa222bb mot ditt användarnamn samt x mot ditt studentnummer i IP-adresslistan på Hawk Wiki. DNS-servrarna ska befinna sig på ditt DMZ. Installera även BIND om du inte redan gjort detta.

6.2 Konfiguration av den primära DNS-servern

Konfigurera ns1 så att konfigurationen överrensstämmer med tidigare uppgifter. Se även till att den har sig själv som DNS-server för att hantera DNS-uppslag.

6.2.1 Konfigurera zonen *aa222bb.ny230.se*

De virtuella maskinerna du arbetat med har BIND version 9 installerat. Du ska nu sätta upp en *forward lookup zone* för ditt nätverk. Sätt upp zonen med följande uppgifter

- Två DNS-servrar, en primär och en sekundär.
- E-postadressen till DNS-administratören är aa222bb@aa222bb.ny230.se.
- Använd följande tidsintervall:
  - sekundära DNS-servrar ska uppdatera zonen var tredje timme.
  - om en sekundär DNS-server inte får kontakt med den primära ska den försöka igen var tredje timme.
  - om en sekundär server inte får kontakt med den primära DNS-servern inom en vecka ska zonen förkastas.
  - resterande tidsintervall sätter du till lämpliga värden som du motiverar i rapporten.
- Det ska finnas en post som pekar på en e-postserver med tillhörande MX-post på ditt nätverk.
- Det ska finnastre klientmaskiner på ditt nätverk med tillhörande poster.

6.2.2 Konfigurera zonen för *reverse-uppslag*

Du ska du konfigurera en zon för reverse-uppslag.

- Konfigurera upp en *reverse zone* för 10.230.x.0/24 på den primära DNS-servern. Zonen ska innefatta du uppgifter som ingår i forward-zonen.

6.3 Testa DNS-zonerna

Kontrollera att du kan göra både forward- och reverse lookup till din zon. Använd verktyget *dig*.

6.4 Begränsa DNS-zonen

Du ska i detta moment begränsa vilka nätverk som får använda sig av den primära DNS-servern för att utföra namnuppslag.

- Begränsa den primära DNS-servern så att endast klienter från ditt nätverk får göra queries till servern. Använd allow-query.
- Be någon annan student kontrollera så att de inte kan göra queries direkt mot din server. Kommer du inte åt din grannes DNS-server? Har du öppnat brandväggsregler?
- Vad får denna begränsning för konsekvenser? Ska du behålla den eller ha kvar den?

6.5 Konfigurera den sekundära DNS-servern

Sätt upp ns2.aa222bbny230.se som sekundär DNS, även kallas slave. Gör detta för båda dina zoner.

7 Laborationsfrågor

1. Förklara följande DNS-postern: SOA, PTR, A, MX, CNAME.
2. Vad är *glue records*? Hitta dessa för din forward lookup zone.
3. Förklara skillnaden mellan en stateful firewall och en icke-stateful firewall.