Welcome to

13. Running a Modern Network

Communication and Network Security 2019

Henrik Lund Kramshøj hlk@zencurity.com @kramse

Slides are available as PDF, kramse@Github

13-Running-a-Modern-Network.tex in the repo security-courses

Plan for today

Subjects

- BCP38 RFC2827: Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing
- Mutually Agreed Norms for Routing Security (MANRS)
- Testing security, evaluating and reporting
- Hardened network device configurations
- Jump hosts and management networks
- DDoS protection
- Check you network from outside RIPEstat, BGPmon

Exercises

- Look at your own networks, from the outside

Reading Summary

Browse
`https://www.manrs.org/`
and read this

`https://www.manrs.org/wp-content/uploads/2018/09/MANRS_PDF_Sep2016.pdf`

Browse / skim this:
`https://tools.ietf.org/pdf/bcp38.pdf` RFC2827: Network Ingress Filtering: Defeating Denial of Service Attacks

Infrastrukturer i praksis

Vi vil nu gennemgå netværksdesign med udgangspunkt i vores setup

Vores setup indeholder:

- Routere
- Firewall
- Wireless
- DMZ
- DHCPD, BIND, BGPD, OSPFD, ...

Den kunne udvides med flere andre teknologier vi har til rådighed:

- VLAN inkl VLAN trunking/distribution
- WPA Enterprise

Hvad taler for og imod - de næste slides gennemgår nogle standardsetups

En slags Patterns for networking

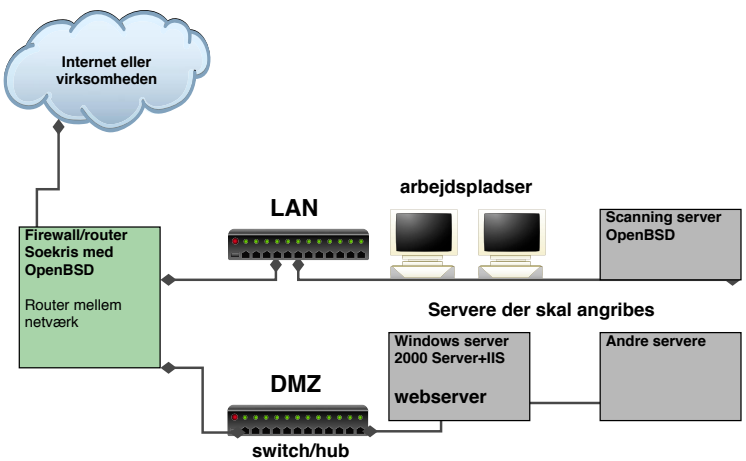
Netværksdesign og sikkerhed

Hvad kan man gøre for at få bedre netværkssikkerhed?

- Bruge switche - der skal ARP spoofes og bedre performance
- Opdele med firewall til flere DMZ zoner for at holde udsatte servere adskilt fra hinanden, det interne netværk og Internet
- Overvåge, læse logs og reagere på hændelser

Husk du skal også kunne opdatere dine servere

Basic Network



Du bør opdele dit netværk i segmenter efter traffik

Du bør altid holde interne og eksterne systemer adskilt!

Du bør isolere farlige services i jails og chroots

Intrusion Detection Systems - IDS

Angrebsværktøjerne efterlader spor

Det anbefales at have IDS og flow opsamling som minimum

Hostbased IDS - kører lokalt på et system og forsøger at detektere om der er en angriber inde

Network based IDS - NIDS - bruger netværket

Automatiserer netværksovervågning:

- bestemte pakker kan opfattes som en signatur
- analyse af netværkstrafik - FØR angreb
- analyse af netværk under angreb - sender en alarm

Planlægning af IDS miljøer

Før installationen scope

- Hvad er formålet - reaktion eller "statistik"
- Hvor skal der måles - hele netværket eller specifikke dele
- Hvad skal måles og hvilke operativsystemer og servere/services

Implementationen

- Er infrastrukturen iorden som den er
- Er der gode målepunkter - monitorporte
- Et målepunkt eller flere, Hvor meget trafik skal måles

Selve idriftsættelsen

- Ændringer af infrastrukturen
- Installation af udstyret og test af udstyret udenfor drift
- Installation i driftsmiljøet
- Test af udstyret i driftsmiljøet

Opsætning og konfiguration af IDS miljøer

Vælg en simpel installation til at starte med!

Undgå for alt i verden for meget information

- Start med en enkelt sensor
- Byg en server med database og "brugerværktøjer"
- Start med at overvåge dele af nettet
- Brug et specifikt regelsæt i starten - eksempelvis kun Windows eller kun UNIX
- Lav nogle simple rapporter til at starte med

Gør netværket mere sikkert før du lytter på hele netværket

Brug tcpdump/Ethereal til at se på trafik, lær IP pakker at kende

Brug Suricata og Zeek til at evaluere

- husk at man kan starte med vilkårligt værktøj og senere skifte til andre produkter
- Praktisk erfaring med eget netværk er nødvendigt og værdifuldt

Honeypots

Man kan udover IDS installere en honeypot

En honeypot består typisk af:

- Et eller flere sårbare systemer
- Et eller flere systemer der logger traffik til og fra honeypot systemerne

Meningen med en honeypot er at den bliver angrebet og brudt ind i

Undgå standard indstillinger

Giv jer selv mere tid til at patche og opdatere

Tiden der går fra en sårbarhed annonceres på internet til den bliver udnyttet er meget kort idag!

Ved at undgå standard indstillinger kan der måske opnås en lidt længere frist

NB: ingen garanti

Pattern: erstat Telnet med SSH

Telnet er død!

Brug altid Secure Shell fremfor Telnet

Opgrader firmware til en der kan SSH, eller køb bedre udstyr næste gang

Selv mine små billige Linksys switche forstår SSH!

Pattern: erstat FTP med HTTP

Jump Host

Hvis der kun skal distribueres filer kan man ofte benytte HTTP istedet for FTP

Hvis der skal overføres med password er SCP/SFTP fra Secure Shell at foretrække

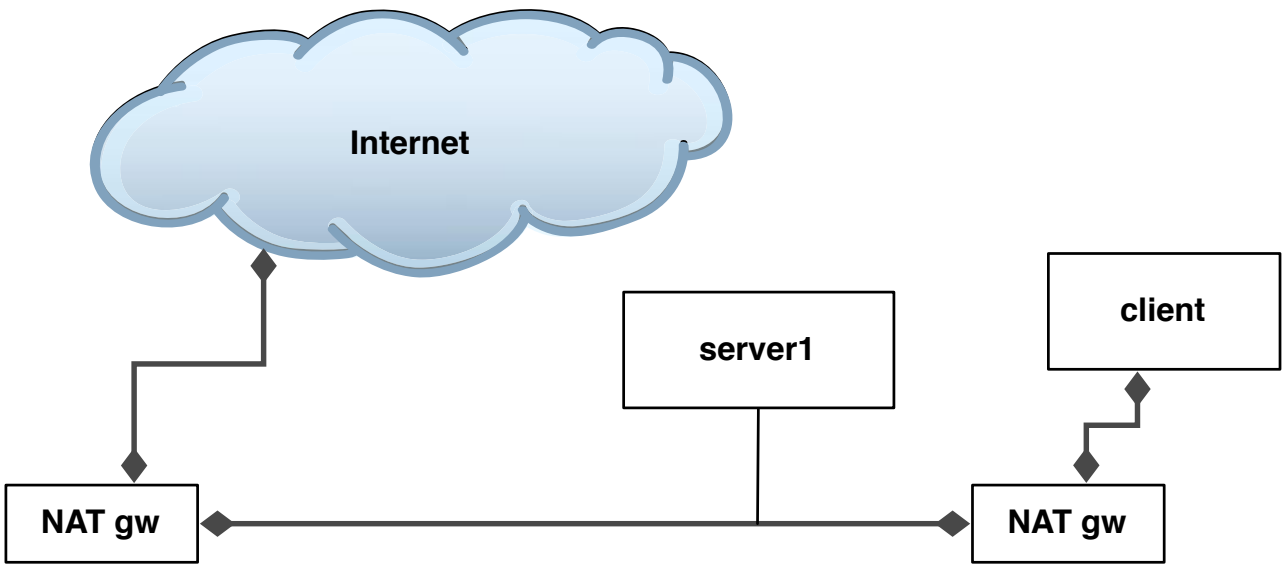
Anti-patterns

Nu præsenteres et antal setups, som ikke anbefales

Faktisk vil jeg advare mod at bruge dem

Husk følgende slides er min mening

Anti-pattern dobbelt NAT i eget netværk



Det er nødvendigt med NAT for at oversætte traffik der sendes videre ud på internet.

Der er ingen som helst grund til at benytte NAT indenfor eget netværk!

Anti-pattern blokering af ALT ICMP

```
# Simple stateful network firewall rules for allowing ICMP in IPv6 ICMPv6
# Allow ICMPv6 destination unreach
        $fwcmd6 add pass ipv6-icmp from any to any icmptypes 1
# Allow NS/NA/toobig (don't filter it out)
        $fwcmd6 add pass ipv6-icmp from any to any icmptypes 2
# Allow timex Time exceeded
        $fwcmd6 add pass ipv6-icmp from any to any icmptypes 3
# Allow parameter problem
        $fwcmd6 add pass ipv6-icmp from any to any icmptypes 4
# IPv6 ICMP - echo request (128) and echo reply (129)
        $fwcmd6 add pass ipv6-icmp from any to any icmptypes 128,129
# IPv6 ICMP - router solicitation (133) and router advertisement (134)
        $fwcmd6 add pass ipv6-icmp from any to any icmptypes 133,134
# IPv6 ICMP - neighbour discovery solicitation (135) and advertisement (136)
        $fwcmd6 add pass ipv6-icmp from any to any icmptypes 135,136
```

Lad være med at blokere for alt ICMP, så ødelægger du funktionaliteten i dit netMANRS

ICMPv4 beskedtyper

Type

- 0 = net unreachable;
- 1 = host unreachable;
- 2 = protocol unreachable;
- 3 = port unreachable;
- 4 = fragmentation needed and DF set;
- 5 = source route failed.

Tillad disse ICMP types:

- 3 Destination Unreachable
- 4 Source Quench Message
- 11 Time Exceeded
- 12 Parameter Problem Message

Lad være med at blokere for alt ICMP, så ødelægger du funktionaliteten i dit net

Anti-pattern blokering af DNS opslag på TCP

Det bliver (er) nødvendigt med DNS opslag over TCP

Store svar kræver TCP

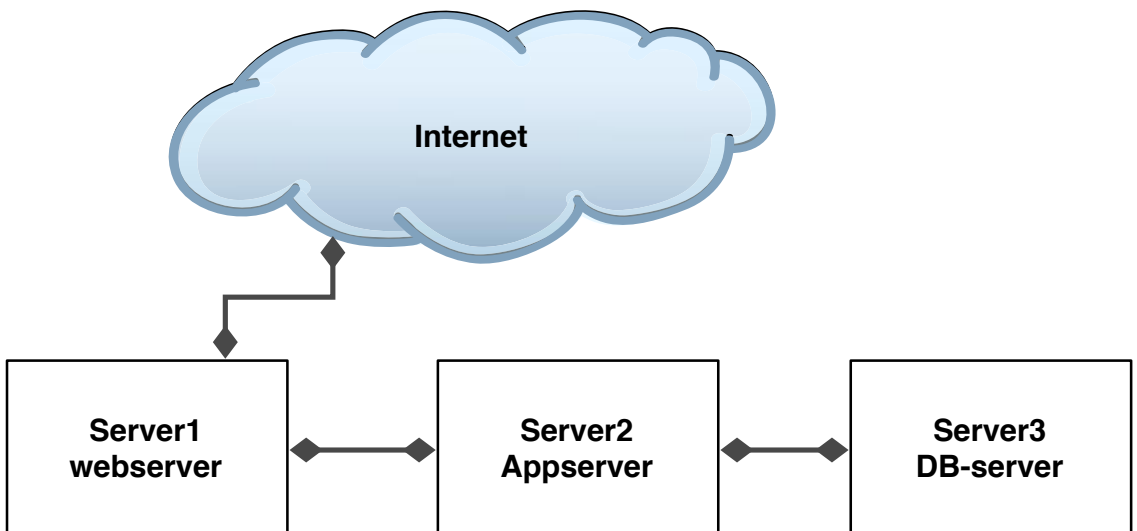
Det betyder at firewalls skal tillade DNS opslag via TCP

De nye forslag DNS over TLS (DoT) og DNS over HTTPS (DoH)

DNS kryptering bliver med TCP

Anbefaling i enterprise netværk:
Brug en caching nameserver, således at det kun er den som kan lave DNS opslag ud i verden

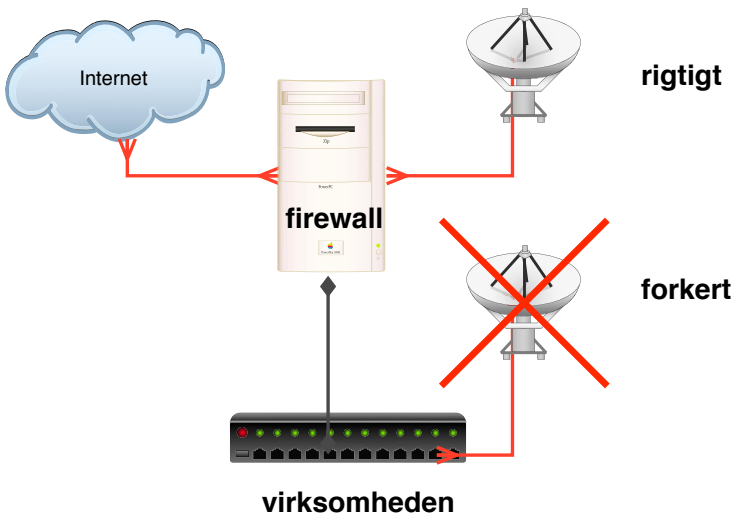
Anti-pattern daisy-chain



Daisy-chain af servere, erstat med firewall, switch og VLAN

Det giver et væld af problemer med overvågning, administration, backup og opdatering

Anti-pattern WLAN forbundet direkte til LAN



WLAN AP'er forbundet direkte til LAN giver risiko for at sikkerheden brydes, fordi AP falder tilbage på den usikre standardkonfiguration

Ved at sætte WLAN direkte på LAN risikerer man at eksterne får direkte adgang

At være på internet

RFC-2142 Mailbox Names for Common Services, Roles and Functions

Du BØR konfigurere dit domæne til at modtage post for følgende adresser:

- postmaster@domæne.dk
- abuse@domæne.dk
- webmaster@domæne.dk, evt. www@domæne.dk

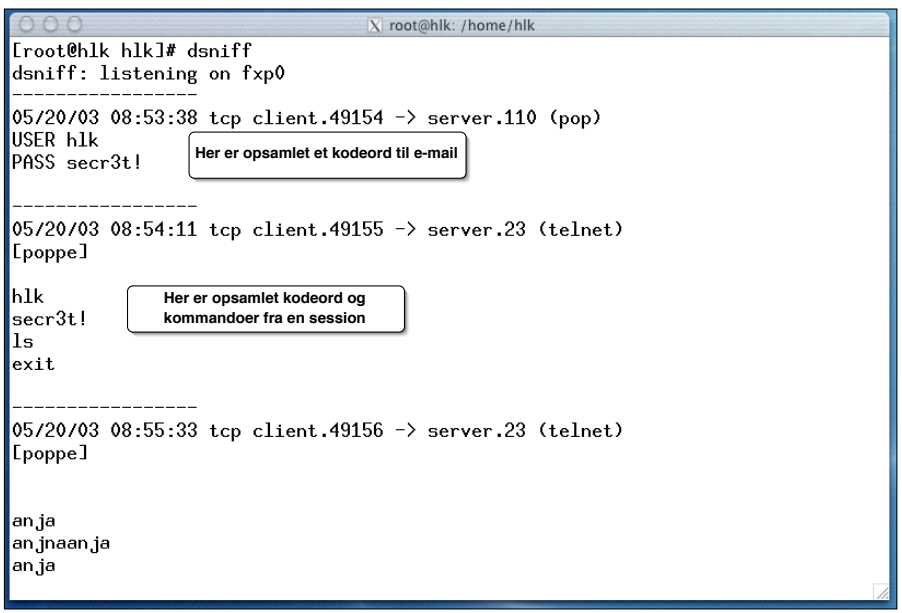
Du gør det nemmere at rapportere problemer med dit netværk og services

E-mail best current practice

MAILBOX	AREA	USAGE
ABUSE	Customer Relations	Inappropriate public behaviour
NOC	Network Operations	Network infrastructure
SECURITY	Network Security	Security bulletins or queries
...		
MAILBOX	SERVICE	SPECIFICATIONS
POSTMASTER	SMTP	[RFC821], [RFC822]
HOSTMASTER	DNS	[RFC1033-RFC1035]
USENET	NNTP	[RFC977]
NEWS	NNTP	Synonym for USENET
WEBMASTER	HTTP	[RFC 2068]
WWW	HTTP	Synonym for WEBMASTER
UUCP	UUCP	[RFC976]
FTP	FTP	[RFC959]

Kilde: RFC-2142 Mailbox Names for Common Services, Roles and Functions. D. Crocker. May 1997

Brug krypterede forbindelser



Især på utroværdige netværk kan det give problemer at benytte sårbare protokoller

Mission 1: Kommunikere sikkert

Du må ikke bruge ukrypterede forbindelser til at administrere UNIX

Du må ikke sende kodeord i ukrypterede e-mail beskeder

Telnet daemonen - telnetd må og skal dø!
FTP daemonen - ftpd må og skal dø!
POP3 daemonen port 110 må og skal dø!
IMAPD daemonen port 143 må og skal dø!

væk med alle de ukrypterede forbindelser!

Change management

Er der tilstrækkeligt med fokus på software i produktion

Kan en vilkårlig server nemt reetableres

Foretages rettelser direkte på produktionssystemer

Er der fall-back plan

Burde være god systemadministrator praksis

Fundamentet skal være iorden

Sørg for at den infrastruktur som I bygger på er sikker:

- redundans
- opdateret
- dokumenteret
- nem at vedligeholde

Husk tilgængelighed er også en sikkerhedsparameter

individuel autentificering!

ssh root@server1

Mange UNIX systemer administreres fejlagtigt ved brug af root-login

Undgå direkte root-login

Insister på `sudo` eller `su`

Hvorfor?

- Sporbarheden mistes hvis brugere logger direkte ind som root
- Hvis et kodeord til root gættes er der direkte adgang til alt!

Centralized management SSH, Jump hosts

A jump server, jump host or jumpbox is a computer on a network used to access and manage devices in a separate security zone. The most common example is managing a host in a DMZ from trusted networks or computers.

`https://en.wikipedia.org/wiki/Jump_server`

BCP38 RFC2827: Network Ingress Filtering

BCP38 RFC2827: Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing

`https://tools.ietf.org/pdf/bcp38.pdf` RFC2827: Network Ingress Filtering: Defeating Denial of Service Attacks

MANRS

Mutually Agreed Norms for Routing Security (MANRS) is a global initiative, supported by the Internet Society, that provides crucial fixes to reduce the most common routing threats.

`https://www.manrs.org/isps/`

`https://www.manrs.org/wp-content/uploads/2018/09/MANRS_PDF_Sep2016.pdf`

Testing security, evaluating and reporting

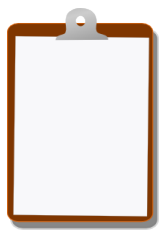
Hardened network device configurations

Jump hosts and management networks

DDoS protection

Check you network from outside RIPEstat, BGPmon

For Next Time



Think about the subjects from this time, write down questions

Next time is exam preparation

All books should be read by now

Visit web sites and download papers if needed

Retry the exercises to get more confident using the tools