



Welcome to

Network Security Threats

Communication and Network Security 2019

Henrik Lund Kramshøj hk@zencurity.com

Slides are available as PDF, kramse@Github
2-Network-Security-Threats.tex in the repo [security-courses](#)

Unencrypted data protocols



TFTP Trivial File Transfer Protocol



Trivial File Transfer Protocol - uautentificerede filoverførsler

De bruges især til:

- TFTP bruges til boot af netværksklienter uden egen harddisk
- TFTP benytter UDP og er derfor ikke garanteret at data overføres korrekt

TFTP sender alt i klartekst, hverken password

USER brugernavn og

PASS hemmeligt-kodeord

Still used for configuration files and firmwares

FTP File Transfer Protocol



File Transfer Protocol - filoverførsler

Bruges især til:

- FTP - drivere, dokumenter, rettelser - Windows Update? er enten HTTP eller FTP

FTP sender i klartekst

USER brugernavn og

PASS hemmeligt-kodeord

Der findes varianter som tillader kryptering, men brug istedet SCP/SFTP over Secure Shell protokol

FTP Daemon konfiguration



Meget forskelligt!

WU-FTPD er meget udbredt

BSD FTPD ligeså meget anvendt

anonym ftp er når man tillader alle at logge ind
men husk så ikke at tillade upload af filer!

På BSD oprettes blot en bruger med navnet `ftp` så er der åbent!

Network Layer Attacks



Yersinia

ARP flooding ARP spoofing

IP LAND, m.fl.

ICMP redirect



Routerne understøtter ofte ICMP Redirect

Med ICMP Redirect kan man til en afsender fortælle en anden vej til destination

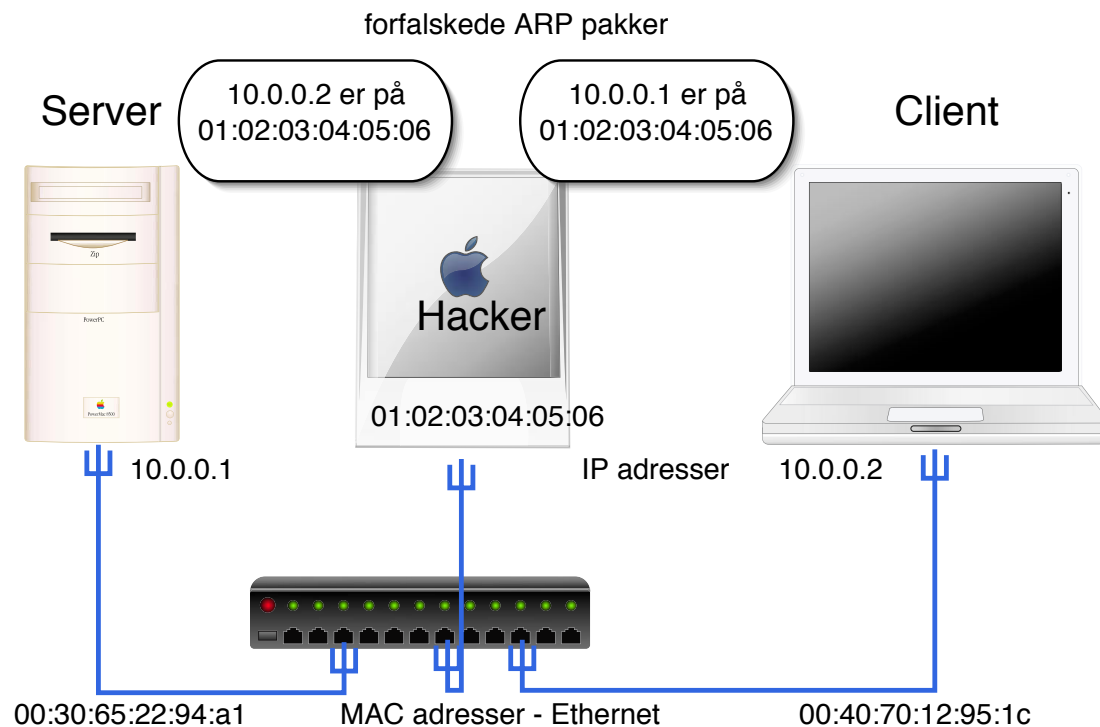
Den angivne vej kan være smartere eller mere effektiv

Det er desværre uheldigt, idet der ingen sikkerhed er

Idag bør man ikke lytte til ICMP redirects, ej heller generere dem

Det svarer til ARP spoofing, idet trafik omdirigeres

Hvordan virker ARP spoofing?



Hackeren sender forfalskede ARP pakker til de to parter

De sender derefter pakkerne ud på Ethernet med hackerens MAC adresse som modtager - han får alle pakkerne



Forsvar mod ARP spoofing



Hvad kan man gøre?

låse MAC adresser til porte på switche

låse MAC adresser til bestemte IP adresser

Efterfølgende administration!

arpwatch er et godt bud - overvåger ARP

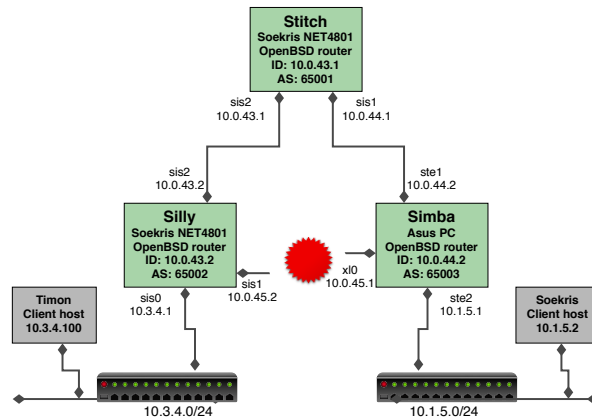
bruge protokoller som ikke er sårbare overfor opsamling

Transport Layer Attacks

TCP SYN flood TCP sequence numbers



Dynamisk routing



Når netværkene vokser bliver det administrativt svært at vedligeholde

Det skalerer dårligt med statiske routes til netværk

Samtidig vil man gerne have redundante forbindelser

Til dette brug har man STP på switch niveau og dynamisk routing på IP niveau

BGP Border Gateway Protocol



Er en dynamisk routing protocol som benyttes eksternt

Netværk defineret med AS numre annoncerer hvilke netværk de er forbundet til

Autonomous System (AS) er en samling netværk

BGP version 4 er beskrevet i RFC-4271

BGP routere forbinder sig til andre BGP routere og snakker sammen, *peering*

http://en.wikipedia.org/wiki/Border_Gateway_Protocol

Vores setup svarer til dette:

http://www.kramse.dk/projects/network/openbgpd-basic_en.html

RIP Routing Information Protocol



Gammel routingprotokol som ikke benyttes mere

RIP er en distance vector routing protokol, tæller antal hops

http://en.wikipedia.org/wiki/Routing_Information_Protocol

OSPF Open Shortest Path First



Er en dynamisk routing protocol som benyttes til intern routing

OSPF version 3 er beskrevet i RFC-2740

OSPF bruger hverken TCP eller UDP, men sin egen protocol med ID 89

OSPF bruger en metric/cost pr link for at udregne smart routing

http://en.wikipedia.org/wiki/Open_Shortest_Path_First

Vores setup svarer til OpenBGPD setup, blot med OpenOSPF

Båndbredestyring og policy based routing



Mange routere og firewalls idag kan lave båndbredde allokering til protokoller, porte og derved bestemte services

Specielt relevant for DDoS beskyttelse

Mest kendte er i Open Source:

- OpenBSD - integreret i PF
- FreeBSD har dummynet
- Linux Traffic Control

Det kaldes også traffic shaping

Routingproblemer, angreb



falske routing updates til protokollerne

sende redirect til maskiner

source routing - mulighed for at specificere en ønsket vej for pakken

Der findes (igen) specialiserede programmer til at teste og forfalske routing updates, svarende til icmpush programmet

Det anbefales at sikre routere bedst muligt - eksempelvis Secure IOS template der findes på adressen:

<http://www.cymru.com/Documents/secure-ios-template.html>

Med UNIX systemer generelt anbefales opdaterede systemer og netværkstuning

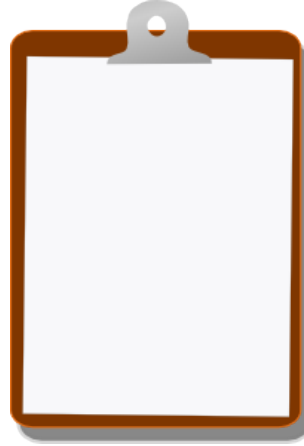
Source routing



Hvis en angriber kan fortælle hvilken vej en pakke skal følge kan det give anledning til sikkerhedsproblemer

maskiner idag bør ikke lytte til source routing, evt. skal de droppe pakkerne

For Next Time



- Think about the subjects from this time, write down questions
- Check the plan for chapters to read in the books
Most days have about 100 pages or less, but one day has 4 chapters to read!
- Visit web sites and download papers if needed
- Retry the exercises to get more confident using the tools