Internet Security 17.03.2010

TCP/IP 1/2

Network Protocol Stack

32 Bit Nr 2^{32} Adressen siehe vorige Vorlesung

Protocol Field: TCP / UDP usw

Fragmentation Field: see previous

Ethernet Aufbau (48 Bit Adressen)

Map MAC Adress to IP Adress to deliver packets

ARP: Map that ... - ist in

ARP messages in ethernet frame - broadcasted to all clients

Client fragt die Adresse mit ARP message ab

RARP (reverse ARP)

Siehe ARP cache! wichtig

Alle Caches füllen sich bei einer Anfrage!

IP Spoofing Admin - RAW Socket öffnen - alle Bits selber setzen!

ARP Poisoning

Fehler: Switch hat keinen ARP cache sondern nur Liste Mac → Anschluss

Eig egal ob switch od hub

ARP: Man in the Middle Attack

Man muss nicht Broadcasten, man kann auch an einzelne schicken!

Route to the Internet

Delivery of packets

IP Adresses bleiben gleich, aber MAC Adressen & IP Layer ändert sich;

In TCP ändert sich nur das TTL feld

Routing Tabelle kann man anschauen

UH → H: directly to host

3. Eintrag: Sendet alles andere zum Gateway

Man sendet Paket an den Gateway aber Dest. Adress ist zB von google.com

2 Routing Protocols EGP IGP

RIP: Tauschen d Routing Tabelle, wie viele HOPs es gibt

Multiple Network Attacks

Man in the Middle schwierig weil man irgendwo im Network Pfad sein muss – auf der kürzesten Route

ICMP unterstützt eig. IP (obwohl es darunter ist)

ist in IP eingepackt

ICMP Data Struktur hängt vom Typ der Nachricht ab

zB bei Ping ECHO Request

Sequence Number: welche ECHO #

identifier: Prozess ID von "Ping"

Pings kann man "blocken"

Spoof ICMP Request with spoofed IP adress mit broadcast
zB ECHO

– antworten DOS'en den anderen

Geht eigentlich nicht, weil Broadcast vom Gateway gedroppt werden soll!

Slide mit Adressen stimmt nicht ganz (geht nicht mit lokalen Adressen)

Es gibt ein Bit in IP das Fragmentation unterdrückt

Out out a host from a Network with ICMP unreachable

Traceroute – Zeigt wo Pakete durchgehen!
Geht indem TTL niedrig gesetzt wird – ICMP Time exceeded
Kann man auch "blocken" bzw unterdrücken

IPSec ist ein Krypto Tunnel zw. 2 Hosts
Im Standard IPV6 bereits enthalten