SICHERHEIT IN INTERNETPROTOKOLLEN

CARSTEN STROTMANN

Created: 2024-09-26 Thu 06:40

AGENDA

- TCP/IP Protokollfamilie
- Spoofing
- DoS - Denial-of-Service
- DDoS - Distributed Denial of Service
- Angriff auf Inhalte
- Angriff auf Protokolle
- Angriff auf Anwendungen
- IPv6 Security

TCP/IP PROTOKOLLE

- Die Grund-Protokolle der IPv4 Protokollfamilie entstanden Ende der 1970er Jahre und wurden 1983 eingeführt
- Die IT-Landschaft unterschied sich von der heutigen:
  - Keine mobilen Rechner
  - Zentrale "Grossrechner" mit mehreren Benutzern
  - Anschluss an andere Netze über ein einziges "Gateway"
  - Die Anzahl der Benuzter war überschaubar (Universitäten, Forschungseinrichtungen)
- Resultat: keine eingebauten Sicherheitsfunktionen in der TCP/IP-Protokollfamilie

SPOOFING

- UDP Source Adressen spoofing
- DNS Antwort Spoofing
- ICMP Spoofing
- ARP Spoofing

"DENIAL OF SERVICE (DOS)" ANGRIFFE

- SYN-Flood
- ICMP 'Ping-of-Death' (heute kein Problem mehr)
- ICMP 'land' Angriff, ICMP 'smurf' Angriff (heute kein Problem mehr)
- TCP 'Reset'
- DHCP "exhaustion" Angriff

"DISTRIBUTED DENIAL OF SERVICE (DDOS)" ANGRIFFE

- UDP Reflection Attack (DNS, NTP, "chargen")
- ICMP Reflection Attacks
- Angriffe auf Krypto (NSEC3, TLS-Handshake)

ANGRIFFE AUF INHALTE

- DNS Cache-Poisioning
- Clock Attacks (NTP)
- Pervasive Monitoring (Überwachung) RFC 7258
  https://tools.ietf.org/html/rfc7258
- TLS/SSL Angriffe (BREACH, CRIME, HEARTBLEED, FREAK, ROBOT …)

ANGRIFFE AUF PROTOKOLLE

- TCP Sequence Number Angriffe
- Fragmentation Angriffe (DNS, Firewall)
- Unauthorisierte DHCP Server (IPv4 und IPv6)
- Unauthorisierte DNS Server
- TCP/TLS Connection Hijacking
- DNS Cache Poisioning

IPV6 SICHERHEITSPROBLEME (1/2)

IPv6 hat ähnliche Sicherheitsprobleme wie IPv4, nur mit längeren Adressen :)

- ICMPv6 neighbor solitication/advertisement spoofing
- Router spoofing
- IPv6 redirection spoofing
- DHCP spoofing

IPV6 SICHERHEITSPROBLEME (2/2)

- Spoofed DNS Resolver in Router Advertisements
- Dublicate Address Detection DoS
- Router/Neighborhood Advertisements Flooding (DoS)
- Multicast Spoofing (DoS oder MITM)
- Extension Header Angriffe
- Source Routing Angriffe
- The Hackers Choice IPv6 Toolkit https://www.thc.org/thc-ipv6/ oder https://github.com/vanhauser-thc/thc-ipv6.git