DNS

DNS - Domain Name System
Angriffsmethoden

Hintergrund

- Domain Name System (DNS)
- Umsetzung von Domainnamen in IP-Adressen (forward lookup)
  - Bsp.: www.wikipedia.org -> 145.97.39.155
  - auch reverse lookup möglich
- hierarchische Datenbank
  - weltweit auf tausende von Servern verteilt
- Beschrieben in RFC 1034 und 1035
- Quelle: http://de.wikipedia.org/wiki

DNS-Security

- DNS ist zentraler Bestandteil einer vernetzten IT-Infrastruktur
  - Störung kann erhebliche Kosten nach sich ziehen
  - Verfälschung von DNS-Daten kann Ausgangspunkt von Angriffen sein
- verfügbare Sicherheits-Verfahren
  - TSIG (Transaction Signatures)
    - Einfaches, auf symmetrischen Schlüsseln beruhendes Verfahren, mit dem der Datenverkehr zwischen DNS-Servern gesichert werden kann
  - DNSSEC (DNS Security)
    - Asymmetrisches Kryptosystem, mit dem nahezu alle DNS-Sicherheitsanforderungen erfüllt werden können
    - Server-Server-Kommunikation und Client-Server-Kommunikation gesichert

DNS Angriffe

- Durch Manipulation DNS-Teilnehmer auf falsche Webseiten zu lenken
  - Ziel: Passworte, PINs, Kreditkartennummern usw. erhalten
  - DNS-Spoofing, Cache-Poisoning
- Internet-DNS durch Denial of Service Attacken komplett ausschalten
  - Ziel: Lahmlegen des Internet
  - DNS-Amplification-Angriff
- Gezielte Angriffe auf Einzelpersonen oder Unternehmen intensivieren

DNS Spoofing

- Man-In-The-Middle-Angriff
- Einem anfragenden Client wird eine Antwort mit einer falschen IP-Adresse untergeschoben
  - dieser wird auf eine falsche Web-Seite gelenkt
- Der Angreifer kann zwei Kommunikationspartnern die Identität des jeweils anderen vortäuschen
  - Er kann die Datenpakete beider Partner empfangen
  - Häufiges Ziel: Passworte, PINs, Kreditkartennummern usw. erhalten
- Weitere Infos bei http://www.bsi.de/gshb/deutsch/g/g05078.htm

Cache-Poisoning

- Einem anfragenden Client werden zusätzlich zur korrekten Antwort manipulierte Daten übermittelt
  - Client übernimmt diese in seinen Cache
  - verwendet diese später ungeprüft
- Details
  - In der Authority Section des Antwortpakets wird der umzuleitende Name (z.B. *de.wikipedia.org*) als angeblicher DNS-Server eingetragen
  - in der Additional Section steht die IP-Adresse (z.B. 1.2.3.4) eines vom Angreifer kontrollierten Servers
- Cache Poisoning Angriffe sind selten geworden
  - Aktuelle Nameserver akzeptieren keine ungefragt mitgelieferten Records mehr
  - Akzeptiert werden nur noch Records aus der tatsächlich angefragten Domain (sogenannte *in-bailiwick-Records*)

DNS-Amplification-Angriff

- Denial-of-Service-Angriff
  - nicht der DNS selbst das Angriffsziel
  - sondern ein unbeteiligter Dritter
  - Details
    - DNS-Server senden in manchen Fällen auf kurze Anfragen (60 Bytes) sehr lange Antworten (3000 Bytes)
      - Verstärkungsfaktor 50
    - Diese werden auf die IP-Adresse des Opfers gelenkt
      - Mittels IP-Spoofing
    - Internet-Zugang des Angriffziels wird gestört
  - Bsp
    - Der massivste DNS Amplification Angriff fand am 5. Februar 2006 statt
    - Ziel waren die Top Level Domain Server - also die wichtigsten Nameserver des Internets
    - Einige verzeichneten in einem Zeitraum von 20 Minuten Datenströme von ca. 60 Megabits pro Sekunde