

DNS Advanced

Underleverantör: IP-Solutions

Datum

- 23-25 May, 2011
Stockholm

Denna kurs går igenom mer komplexa DNS ämnen såsom DNS i kombination med brandväggar och "Split-DNS". Grundlig genomgång av DNSSEC är en central (och allt viktigare) del av kursen och likaså TSIG (DNS transaktionssignaturer), EDNS(0) och dynamiska uppdateringar.

Det finns en uppenbar koppling mellan DHCP och dynamiska uppdateringar och denna kurs behandlar därför utöver dynamiska uppdateringar även i detalj interaktion mellan DHCP och dynamiska uppdateringar.

Målgrupp

Denna kurs siktar parallellt på flera olika målgrupper. Dels givetvis nätverkstekniker, nätverks- och DNS-administratörer. Men även beslutsfattare, IT-strateger, konsulter, säkerhetsfolk och andra som vill ha en djupare förståelse för hur de moderna tilläggen till DNS fungerar och hänger ihop, och på vilka sätt det kommer att påverka framtida DNS-hantering.

Förkunskaper

Kunskaper motsvarande [DNS Introduktionskurs](#).

Övrigt

Denna kurs finns som schemalagd utbildning och presentationen ges på svenska eller engelska. Under kursen blandas teoretiska presentationer med praktiska övningar. Vi kan även hålla denna kurs företagsintern. Kontakta oss för att få reda på hur vi kan hjälpa er med anpassade kurser.

Längd

3 dagar

Svårighetsgrad



Agenda

Quick Repetition of Traditional DNS

Principles Behind the DNS Protocol:

- autonomy, coherence, redundancy

Packet Format:

- The different parts of the DNS message and their usage

Name Server Implementations

- BIND (both authoritative and recursive server)
- NSD (authoritative-only server)
- Unbound (recursive-only server)
- Other implementations
- Differences, pros and cons

Lab Exercise: Compilation and Installation of the DNS Software

DNS Vulnerabilities Overview

Role Separation for Name Servers:

- inevitable when deploying DNSSEC
- different implementation alternatives
- usage together with TSIG
- pitfalls

TSIG: Signing DNS Transactions

- Symmetric encryption
- Symmetric algorithms: HMAC-SHA1, HMAC-SHA256
- Securing zone transfers (server-server)
- Securing queries (client-server)
- BIND: TSIG Configuration in named.conf:
 - key, server and masters directives
- NSD: TSIG Configuration in nsd.conf:
 - key: attributes and the use of the NOKEY keyword
- Securing the transport vs securing the data

Lab Exercise: Using TSIG Between Master and Slave

- Configuration
- Need for synchronized clocks
- Debugging

BIND: rndc

- remote management via rndc: pros and cons
- Key management
- Configuration of rndc.conf

Firewall Issues

- Split-DNS
- Forwarding
- Internal delegations
- Queries “leaking” to the wrong side
- management of internal connections
- multiple versions of the name space and DNS coherency
- varying functionality in different implementations
- “forward” zones and stub zones
- Split-DNS in conjunction with DNSSEC

Lab Exercise: Firewalls, Forwarding, Split-DNS

EDNS(0):

- framework for DNS protocol extensions
- usage of the OPT pseudo-RR
- fields in the DNS packet that are expanded via EDNS(0) and their use

Introduction to DNSSEC

- Background, threat scenario, the Kaminsky attack, etc
- Walkthrough of the concepts

DNSSEC: Validation of Signed DNS Data

- “Trusted keys” and validation of data
- What does “security apex” mean?
- What should happen when data doesn’t validate?

Lab Exercise: Configuration of a Validating Resolver

DNSSEC: Publication of Signed DNS Data

- Asymmetric encryption with public keys
- Asymmetric algorithms: RSA, DSA
- KSK and ZSK: different operational uses for keys

DNSSEC: Protocol Extensions and New Record Types:

- RRSIG: digital signature of DNS records
- DNSKEY: publik key stored and distributed via DNS
- DS: identification of the “KSK” in use

DNSSEC Low-Level Tools:

- dnssec-keygen to create keys
- dnssec-signzone to sign zones

Lab Exercise: Publishing a DNSSEC signed zone

- Create the configuration
- Generate the keys and add them to the zone
- DNSSEC Zone Signing

DNSSEC Key Rollover: Replacing Old Keys with new Keys

- Policy management
- Delegation Signer and parent interaction
- Parent/child interaction with examples
- Tools to simplify DNSSEC management

Lab Exercise: The DS Record and Interacting with your Parent

- Closing the signature chain from the parent

- Verification of the signature chain
- Debugging

Resolver Issues

- Suitable API
- Securing the "last mile"
- The requirement for a "clear path"

Lab Exercise: Key Rollover of ZSK and KSK

- Logging

DNSSEC Protocol Extension: ADE (Authenticated Denial of Existence)

- Why is ADE so important?
- NSEC: Filling out the empty space to facilitate ADE
- NSEC3: When zone contents must not be listed

Lab Exercise: NSEC3

DNSSEC High-Level Tools

- OpenDNSSEC

Lab: OpenDNSSEC

- others

International Outlook:

- Signing different Top-Level domains
- Signing the root zone
- Development and adjustment of different systems for DNSSEC

Dynamic Update

- The four different roles: Client, Authoritative name server for forward zone, Authoritative name server for backward zone and the DHCP server
- Security policies
- Granularity in access rights: control over nodes or entire sub-trees, restrictions on available record types
- update-policy{}
- Alternatives for authentication: TSIG (symmetric key), SIG(0) (asymmetric key), GSS-TSIG
- Comparison SIG(0) vs TSIG

Lab exercise: Manual Dynamic Update

- Name server configuration
- How to trigger the dynamic update automatically
- Client configuration
- Name server configuration

- Design choices in environments with a mix of dynamic and static DNS data
- Dynamic update of DNSSEC secured data: key management, signatures

Lab Exercise: Automatic Dynamic Update (with DHCP)

- Name server configuration
- Relation DHCP server and name server

Summary