

Ludwig-Maximilians-Universität München
und Technische Universität München

Prof. Dr. D. Kranzlmüller
Prof. Dr. H.-G. Hegering

Praktikum IT-Sicherheit
Übungsblatt 06

13. Domain Name System (DNS)

- (a) Installieren Sie das Softwarepaket BIND9 und konfigurieren Sie den neu installierten Dienst so, dass er beim Systemstart automatisch gestartet wird und folgende Konfiguration realisiert:
- i. Der Rechner `dns4a11` ist Master für die Zone `secp-int.lab.nm.ifl.lmu.de`.
 - ii. Für alle unbekanntten Anfragen sowie Reverse Lookup ist der Rechner `dns4a11` als Forwarder einzutragen.
 - iii. Alle Rechner mit ungerader Ordnungsnummer sind als Master für eine neu zu erstellende DNS-Zone zu konfigurieren. Die in der folgenden Tabelle aufgelisteten Domänen sollen von den genannten Mastern verwaltet werden:

Domäne	Netz	Master
sub01.sec-int.lab.nm.ifl.lmu.de	192.168.216.0/29	pcsec01
sub02.sec-int.lab.nm.ifl.lmu.de	192.168.216.8/29	pcsec03
sub03.sec-int.lab.nm.ifl.lmu.de	192.168.216.16/29	pcsec05
sub04.sec-int.lab.nm.ifl.lmu.de	192.168.216.24/29	pcsec07
sub05.sec-int.lab.nm.ifl.lmu.de	192.168.216.32/29	pcsec09
sub06.sec-int.lab.nm.ifl.lmu.de	192.168.216.40/29	pcsec11
sub07.sec-int.lab.nm.ifl.lmu.de	192.168.216.48/29	pcsec13
sub08.sec-int.lab.nm.ifl.lmu.de	192.168.216.56/29	pcsec15
sub09.sec-int.lab.nm.ifl.lmu.de	192.168.216.64/29	pcsec17
sub10.sec-int.lab.nm.ifl.lmu.de	192.168.216.72/29	pcsec19
sub11.sec-int.lab.nm.ifl.lmu.de	192.168.216.80/29	pcsec21
sub12.sec-int.lab.nm.ifl.lmu.de	192.168.216.88/29	pcsec23
sub13.sec-int.lab.nm.ifl.lmu.de	192.168.216.96/29	pcsec25
sub14.sec-int.lab.nm.ifl.lmu.de	192.168.216.104/29	pcsec27
sub15.sec-int.lab.nm.ifl.lmu.de	192.168.216.112/29	pcsec29
sub16.sec-int.lab.nm.ifl.lmu.de	192.168.216.120/29	pcsec31
sub17.sec-int.lab.nm.ifl.lmu.de	192.168.216.128/29	pcsec33
sub18.sec-int.lab.nm.ifl.lmu.de	192.168.216.136/29	pcsec35
sub19.sec-int.lab.nm.ifl.lmu.de	192.168.216.144/29	pcsec37
sub20.sec-int.lab.nm.ifl.lmu.de	192.168.216.152/29	pcsec39

- iv. Alle anderen Rechner sind Slaves für den Master ihres Subnetzes.
 - v. Zonentransfers sind nur für den assoziierten Slave eines Masters erlaubt.
 - vi. DNS-Abfragen über den Slave sollen nur für das zugehörige Subnetz möglich sein.
 - vii. Der DNS-Daemon aller Rechner soll nur auf das Produktivinterface `eth1` gebunden sein.
- (b) Tragen Sie Ihren Nameserver in die `/etc/resolv.conf` ein. Welche Auswirkungen hat das?
- (c) Überprüfen Sie im Logfile, ob Ihr Nameserver korrekt starten konnte und dokumentieren Sie die Ergebnisse in Ihrer Ausarbeitung.
- (d) Überprüfen Sie die Funktionalität Ihrer Nameserver mit `host`, `dig` und `nslookup` und dokumentieren Sie Ihre Erkenntnisse in Ihrer Ausarbeitung. Weitere Informationen zu den Befehlen `host`, `dig` und `nslookup` finden Sie in den Man-Pages.

14. DNS Security Extentions (DNSSEC)

- (a) Generieren Sie jeweils ein KSK/ZSK-Schlüsselpaar und signieren Sie ihre Zone.
- (b) Tragen Sie ihren ZSK im DNS der übergeordneten Zone auf dem Rechner `dns4a11` ein.
- (c) Denken Sie daran, dass jede Änderung an der Konfiguration ein Resign der betroffenen Zone erforderlich macht!
- (d) Überprüfen Sie ihre Konfiguration.