

Ludwig-Maximilians-Universität München
und Technische Universität München
Prof. Dr. H.-G. Hegering

Praktikum IT-Sicherheit
Übungsblatt 06

16. Domain Name System

- (a) Installieren Sie über YaST das Softwarepaket BIND. Konfigurieren Sie den Dienst so, dass er beim Booten automatisch gestartet wird.
- (b) Was sehen Sie mit `netstat -an` und wie ist das zu interpretieren (Informationen über Man-Page und/oder Internet)?
- (c) Ihr Nameserver soll folgende Eigenschaften erfüllen:
 - i. Der Daemon soll auf das Produktivinterface `eth1` hören. Nach einem Neustart des Dienstes durch das Startskript überprüfen Sie mit `netstat -an` und `telnet <IP-Adresse> 53` und anhand des Logfiles, ob Ihre Konfiguration erfolgreich war.
 - ii. Für die Domäne `secp.nm.informatik.uni-muenchen.de` ist der Rechner `pcsec04` als Master zuständig, für die Reverse-Zonen unseres Netzbereichs `192.168.216.0/24` ist der Rechner `pcsec10` als Master zu konfigurieren. Alle anderen sind Slave für diese Zonen. Überprüfen Sie Ihre Konfiguration anhand der Logfiles und mittels Zonentransfers: `host -l -a secp.nm.informatik.uni-muenchen.de <ip-adresse-nameserver>`.
Hinweis zur Namensgebung: z.B. `pcsec01 (192.168.216.193)`, `pcsec01-eth2 (192.168.216.1)`, usw.
 - iii. Für die Domäne `uni-muenchen.de` verweisen Sie auf den Rechner `test4a11`. Somit ist `test4a11` für diese Domäne als Forwarder einzutragen.

- gen. Überprüfen Sie Ihre Konfiguration wieder anhand der Logfiles und mit den bereits bekannten Tools `host`, `dig` und/oder `nslookup`.
- iv. Ein Zonentransfer soll nur von der IP-Adresse des `secserver (192.168.216.254)` und Ihres Partnerrechners erlaubt sein. Was hat das für Konsequenzen bzgl. der Masterzonen? Was ist hier zu beachten?
- v. DNS-Queries sollen nur von der eigenen Maschine und dem `secserver` erlaubt sein. Überprüfen Sie Ihre Einstellungen mittels `nslookup`-Abfragen. Welche Konsequenzen hat das für die Zonen, für die Ihre Rechner Master oder Slave sind? Was ist hier zu beachten und an der Konfiguration zu ändern?
- vi. Für alle anderen Anfragen ist der Rechner `secserver` als Forwarder einzutragen.

- (d) Tragen Sie Ihren Nameserver in die `/etc/resolv.conf` ein. Welche Auswirkungen hat das?
- (e) Überprüfen Sie im Logfile, ob Ihr Nameserver korrekt starten konnte und dokumentieren Sie die Ergebnisse in Ihrer Ausarbeitung.
- (f) Überprüfen Sie die Funktionalität Ihres Nameservers mit `host` 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.

17. Telnet & SSH

- (a) Stoppen Sie alle verfügbaren Dienste und testen Sie das Ergebnis mit `nmap`. Was sehen Sie? Aktivieren Sie zur Zeit nur Ihren Nameserver. Was sehen Sie mit `nmap`?
- (b) Starten Sie Telnet so, dass er vom `tcpwrapper` und `xinetd` kontrolliert wird und sich User nur von der IP-Adresse Ihres Partnerrechners und vom `secserver` einloggen können.
- (c) Installieren Sie den SSH Daemon und konfigurieren Sie ihn so, dass er nur auf Ihrem Interface `eth1` hört und nur von Ihrem Partnerrechner und dem `secserver` aus angesprochen werden kann. Wie können Sie die Richtigkeit Ihrer Konfiguration überprüfen? Was sehen Sie, wenn Sie mit `nmap` alle Ihre

Interfaces scannen? Was sehen Sie mit `netstat -an` und wie ist das zu interpretieren?

- (d) Verfolgen Sie mittels Programmen zum Mithören von Netzwerkverkehr sowohl eine Telnet, als auch eine SSH Verbindung. Wenn Sie eine SSH Sitzung mittels `tcpdump` mithören, was ist der Unterschied zu Telnet?

Informationen zu `nmap`, `tcpd`, `xinetd`, usw. finden Sie in den Man-Pages.