



2. Blatt: Network Protocols and Architectures WS 09/10

Aufgabe 1: (10 + 10 + 10 = 30 Punkte) *Domain und IP Datenbanken (Whois)*

In der Vorlesung habt ihr das Domain Name System (DNS) kennengelernt. Ein weiteres Mittel, um Informationen über Adressbereiche herauszufinden, sind `whois`-Datenbanken, z. B. RIPE, ARIN und DENIC. Deren Inhalt wird von den Organisationen, die IP-Adressbereiche ausgeben, verwaltet, z. B. von der DENIC für Deutschland. Diese Datenbanken können entweder mit dem Kommandozeilentool `whois` oder mit einem web-basierten Frontend¹ abgefragt werden.

- Benutze verschiedene `whois`-Datenbanken, um die Namen zweier nicht lokaler DNS-Server herauszufinden. Gib an, welche Datenbanken und Anfragen du dabei benutzt hast. Hinweis: Frag einfach nach bekannten Domain-Namen wie `google.com`.
- Benutze die RIPE `whois`-Datenbank, um sowohl `tu-berlin.de` als auch eine IP-Adresse aus dem Adressbereich der TU Berlin abzufragen. Welche Ausgabe ist nützlicher? Welcher IP-Adressbereich ist zur TU Berlin zugehörig? Wer verwaltet diesen Adressbereich (mnt-by)?
- Beschreibe wie ein Angreifer die `whois` Datenbank und Tools wie `nslookup` oder `dig` dazu benutzen kann Daten auszuspähen bevor er eine Attacke beginnt.

Aufgabe 2: (10 + 10 + 10 + 10 = 40 Punkte) *Domain Name System*

- Benutze eines der Tools `nslookup` oder `dig`, um drei DNS-Server zu befragen: Deinen lokalen DNS-Server (voreingestellt) und die beiden DNS-Server aus Aufgabe 1 (a). Generiere Anfragen nach den Einträgen zu je drei verschiedenen Typen: A, NS und MX. Fasse deine Ergebnisse kurz zusammen.
- Benutze eines der Tools, um einen Webserver zu finden, der mehrere IP-Adressen hat. Hat `www.net.t-labs.tu-berlin.de` mehrere IP-Adressen?
- Welche IP Adresse wird benutzt, falls ein Hostname mehrere IP adressen hat? Wie kann man dieses Funktionalität ausnutzen?
- DNS benutzt UDP statt TCP. Falls ein DNS Paket verloren geht gibt es keine automatische Fehlerbehandlung. Stellt das ein Problem dar? Falls ja, wie wird dieses gelöst.

Aufgabe 3: (10 + 10 + 10 = 30 Punkte) *Content Distribution Networks*

- Ein Content Distribution Network (CDN) kopiert den selben Inhalt an viele Standorte in aller Welt. Typischerweise leitet ein CDN Benutzer zum passenden Standort weiter in dem individuelle Antworten auf DNS Anfragen gegeben werden (z. B., indem die Antwort auf eine Anfrage nach der IP-Adresse für `www.heise.de` gesteuert wird). Gib zwei Gründe an warum ein CDN verschieden IP-Adressen als Antwort auf die selbe DNS Anfrage von verschiedenen Endsystemen liefern würde.
- Wenn DNS benutzt wird um Endsysteme an verschiedene Standorte weiterzuleiten, wird vom CDN normalerweise der DNS Time-to-live (TTL) auf einen kleinen Wert gesetzt. Warum? Gib zwei Nachteile von kurzen TTL Werten an.
- Ist es sinnvoll, daß ein Internet Anbieter (ISP) als CDN agiert. Falls ja, wie würde das funktionieren? Falls nein, was ist an der Idee falsch?

¹Zum Beispiel: <http://www.ripe.net/whois>, <http://ws.arin.net/whois> oder <http://www.denic.de/de/whois/index.jsp>

Abgabe bis Donnerstag, den 5. November 2009 nur bis 13:55 h s. t.

- **Als PDF Dateien (keine MS Office oder OpenOffice Dateien):** mittels ISIS hochladen (<https://www.isis.tu-berlin.de/course/view.php?id=2172>)
- **In Papierform:** Postfach im Telefunkenhochhaus (Erdgeschoss, hinter dem Pförtner rechts)
- Gib auf deiner Lösung deinen Namen, deine Matrikelnummer **und** den Namen deines Tutors an.