



2nd Assignment: Network Protocols and Architectures WS 09/10

Question 1: (10 + 10 + 10 = 30 points) *Domain and IP registries (Whois)*

In the lecture you learned about the Domain Name System (DNS). Another tool for finding out information about address spaces are the **whois** databases, e. g., RIPE, ARIN, and DENIC. Their content is managed by the organizations that manage the IP address space assignments, e. g., DENIC for Germany. These **whois** databases can be queried either via the **whois** command-line tool or via their Web-based frontends¹.

- Use a **whois** database to locate two non local DNS servers. Indicate which **whois** database and which query you used. Hint: Query for popular domain names such as **google.com**.
- Use the RIPE **whois** database to issue a query for both: **tu-berlin.de** and an IP address from the TU Berlin address space. Which output is more useful? What is the IP address range associated with TU Berlin? Who is managing this address space (mnt-by)?
- Describe how an attacker can use **whois** databases and the tools **nslookup** or **dig** to perform reconnaissance on an institution before launching an attack.

Question 2: (10 + 10 + 10 + 10 = 40 points) *Domain Name System*

- Use one of the tools **nslookup** or **dig** to send DNS queries to three DNS servers: Your local DNS server (default DNS server) and the two DNS servers you found in Question 1 (a). Issue a query for each of the different kinds of record types: A, NS, and MX. Summarize your findings.
- Use any of the tools to find a Web server that has multiple IP addresses. Does the **www.net.t-labs.tu-berlin.de** have multiple IP addresses?
- If a hostname has multiple IP addresses which of the IPs is used? How can this be leveraged?
- DNS is using UDP instead of TCP. If a DNS packet is lost, there is no automatic recovery. Does this cause a problem, and if so, how is it solved?

Question 3: (10 + 10 + 10 = 30 points) *Content Distribution Networks*

- A Content Distribution Network (CDN) replicates the same content in many locations throughout the world. A CDN typically directs clients to the appropriate replica by returning customized answers to DNS queries (e. g., by controlling the response to a request for the IP address of **www.heise.com**). Give two reasons why a CDN would return different IP addresses in response to the same DNS query, from different clients?
- When using DNS to direct clients to Web server replicas, a CDN typically sets the DNS Time-to-Live (TTL) to a small value. Why? Provide two negative implications of having a small TTL value.
- Does it make sense for an Internet Service Provider (ISP) to act as a CDN? If so, how would that work? If not, what is wrong with the idea?

Due Date: Thursday, November, 5th 2009 only until 13:55 h s. t.

- **As PDF files (no MS Office or Openoffice files):** uploaded via ISIS (<https://www.isis.tu-berlin.de/course/view.php?id=2172>)
- **On paper:** Postbox in the Telefunkenhochhaus (basement, behind the doorman right)
- Put your name, StudentID number (Matrikelnummer) **and** the name of your tutor on your solution.

¹See <http://www.ripe.net/whois>, <http://ws.arin.net/whois> or <http://www.denic.de/de/whois/index.jsp>.