P10

Wednesday, 22 May 2024 12:06

10 Application-Layer Protokolle I

1 Thema des Praktikums

Im folgenden Praktikum werden verschiedene Protokolle des Application Layers untersucht. Anhand der Beispiele soll die Funktion und Wirkungsweise dieser Protokolle praktisch getestet und vertieft werden.

Die Schwerpunkte des Praktikums sind:

- DNS (Domain Name System) und WHOIS (Internet Directory Service)
- DHCP (Dynamic Host Configuration Protocol) und TFTP (Trivial File Transfer Protocol)

2 Vorbereitung

dig (domain information groper) ist das zurzeit empfohlene Tool um Informationen von DNS-Servern abzufragen.

Beantworten Sie die untenstehenden Fragen, indem Sie die Anwendungsbeispiele unter dem folgenden Link studieren https://www.thegeekstuff.com/2012/02/dig-command-examples/

und die verwendeten Optionen mit den Angaben der «man page» vergleichen:

http://manpages.ubuntu.com/manpages/cosmic/man1/dig.1.html

Q01 *Welche Bereiche in der Ausgabe gibt es, die ein-/ und ausgeschaltet werden können?*

commentline, authority section, additional section, stats section, answer section

Q02 *Wie kann man eine kurze Anzeige erhalten?*

dig +short

Q03 *Was bedeuten die folgenden Record-Typen?*

A: Verknüpft eine Domain mit einer IPv4-Adresse

AAAA: " IPv6-Adresse

MX: Gibt den Mailserver für die Domain an und priorisiert diese.

CNAME: Zeigt auf eine andere Domain und dient dazu, Aliases für eine Domain zu erstellen.

3 Versuchsdurchführung DNS (Domain Name System)

- Die PCs bleiben zunächst am Schulnetz angeschlossen. Starten Sie diese unter Linux.
  Hinweis: Falls Sie im Folgenden eine Dokumentation der Ein- und Ausgaben wünschen, benutzen Sie putty (ssh → localhost) und schalten das Logging ein.

4 Überprüfung der DNS-Konfiguration

Der DNS-Server löst Netznamen auf, indem er die zugehörigen IP-Adressen ermittelt. Für die Abfrage verwendet die IP-Anwendung einen Resolver, der die Abfrage an einen der konfigurierten Name-Server sendet. Der unter Linux meistbenutzte Resolver ist der **systemd-resolved Service**. Er ermittelt via DHCP die DNS-Server und die Domäne und speichert diese Angaben unter:

```
/var/run/systemd/resolve/resolv.conf
```

Q04 *Wie lauten auf den Labor-PCs die Einträge für die DNS-Server und die Domäne?*

160.85.192.100

160.85.193.100

search zhaw.ch

Anmerkung: In der Theorie wurde vermittelt, dass das File /etc/resolv.conf die DNS-Konfiguration beinhalte. Dieser Widerspruch wird im optionalen Abschnitt 0 aufgelöst.

- Vergleichen Sie die Angaben im File mit der direkten Statusabfrage des Resolvers:
  ```
  resolvectl status
  ```

5 Einfache DNS Abfrage

systemd-resolve kann direkt für Abfragen verwendet werden:

```
resolvectl query nantes.zhaw.ch
```

Im Folgenden verwendeten Befehle dig und host sind allgemeiner.

- Ermitteln Sie mit dem Befehl host die Adresse eines beliebigen ZHAW-Hosts.
  ```
  host nantes.zhaw.ch
  ```
- Führen Sie den gleichen Befehl ohne die Domain Bezeichnung (zhaw.ch) aus.
  ```
  host nantes
  ```

Q05 *Warum muss die Domäne nicht angegeben werden?*

wir sind in der gleichen Domain

Q06 *Wie lautet der dig Befehl, der die ähnlichste Ausgabe wie der host Befehl macht?*

dig nantes.zhaw.ch +noall +answer

6 Arbeitsweise eines Resolvers

Im Folgenden soll der Name www.zhaw.ch schrittweise aufgelöst werden:

- Erste lokale Abfrage nach den Root-Servern:
  ```
  dig . ns
  ```

Q07 *Wie viele solche Root-Server gibt es?*

13

- Machen Sie dieselbe Abfrage nochmals aber an einen der Root-Server:
  `dig @a.root-servers.net. . ns`

Q08 *Welche Information ist gegenüber der 1. Abfrage hinzugekommen?*

Additional Section (A & AAAA)

- Wählen Sie einen beliebigen Root-Server aus und bestimmen Sie die Server der Top Level Domain ch. Beispiel für f.root-servers.net.:
  `dig @192.5.5.241 ch. ns`

Q09 *Warum gibt es in der ADDITIONAL SECTION: doppelt so viele Einträge wie in der AUTHORITY SECTION:?*

IPv4 + IPv6

- Wählen Sie aus der obigen Liste einen der Server für die Top Level Domain ch. und fragen Sie diesen nach den Name-Servern der Second Level Domain «zhaw.ch».

Q10 *Wie lautet der Befehl (unter Verwendung der IP-Adresse)?*

dig @130.59.31.41 zhaw.ch NS

```
3600    IN      NS      ns1.zhaw.ch.
3600    IN      NS      scsnms.switch.ch.
3600    IN      NS      ns2.zhaw.ch.

3600    IN      A       130.59.31.26
3600    IN      A       160.85.104.61
3600    IN      A       160.85.104.60
3600    IN      AAAA    2001:620:0:ff::a7
```

Q11 *Wie heissen die Server der Domain zhaw.ch und was fällt auf, wenn Sie deren Domänen betrachten?*

- Machen Sie mit Hilfe eines DNS-Servers der ZHAW eine Adressabfrage des Hosts www.zhaw.ch:
  `dig @160.85.104.60 www.zhaw.ch. A`

Q12 *Was bedeutet CNAME in der Answer-Section?*

canonical name record

- Vergleichen Sie diese Adressen der ZHAW Server mit denen in der DNS-Konfiguration.

Q13 *Wie erklären Sie den Unterschied?*
(Hinweis: Versuchen Sie mit `dig @160.85.104.60 nantes.zhaw.ch. A` *nochmals die Adressabfrage von nantes.zhaw.ch).*

macht SOA anstatt CNAME

- Bestimmen Sie die Namen und Adressen der Mail-Server der ZHAW.

Q14 *Wie lautet der Befehl?*

dig zhaw.ch MX

zhaw-ch.mail.protection.outlook.com

7 WHOIS (Domain Name and Network Number Directory Service)

Unter Linux gibt es den Befehl whois, mit dem Informationen zu Internet-Domänen und deren Eigentümern abgefragt werden können. Die Abfrage läuft im Klartext zu einem Whois-Server.

- Führen Sie Abfragen zu diversen Domains aus (beispielsweise zhaw.ch, google.com, kernel.org).
- Beobachten Sie mit Wireshark, wie die Abfrage und das Resultat übertragen werden.

Q15 *Welcher Dienst wird von whois verwendet (Transport / Host / Port)?*

TCP, Port 43

- **Zeigen Sie die Resultate dem Laborbetreuer.**

8 Bootstrap Protokolle

Im Folgenden sollen Sie analysieren, in welchen Schritten ein ZHAW-PC konfiguriert wird.

- Verbinden Sie gemäss Abbildung 1 die PCs mit einem Hub und dem ZHAW-LAN.

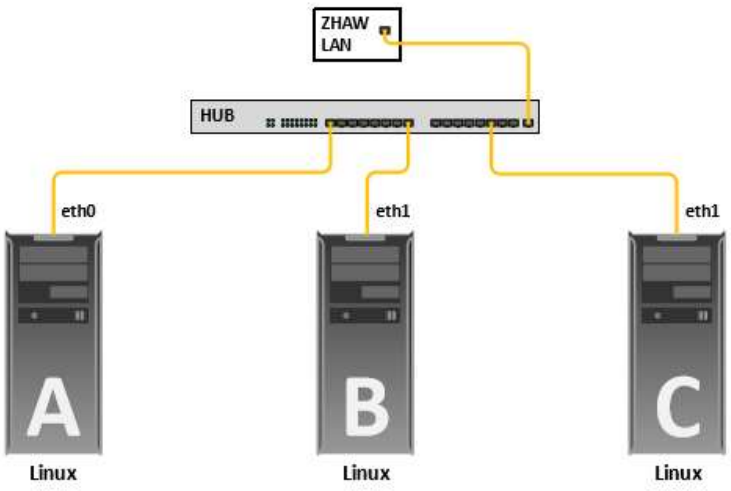

Abbildung 1

- Zeichnen Sie mit Wireshark auf PC B (und allenfalls auch PC C) den Bootvorgang von PC A auf.

9 DHCP

- Setzen Sie im Wireshark einen Filter, dass nur die DHCP-Meldungen angezeigt werden.

Q16 *Wie lautet der Filterausdruck im Wireshark für die DHCP-Meldungen? Warum?*

dhcp

Q17 *Offensichtlich gibt es mehrere DHCP Vorgänge. Woran erkennen Sie, welche DHCP-Meldungen zusammengehören?*

Transaction ID

- Bestimmen Sie die IP-Adresse vom PC A und suchen Sie in der Aufzeichnung, wo diese zugeteilt wird.
- Tragen Sie in Tabelle 1 die zugehörigen DHCP-Meldungen ein.

Source	Destination	Typ	Zweck (Ihre Interpretation)	
0.0.0.0	255.255.255.255	Discover	hallo? brauche IP-Adresse	C
160.85.20.1	160.85.20.121	Offer	moin, hier deine IP-Adresse	S
0.0.0.0	255.255.255.255	Request	passt	C
160.85.20.1	160.85.20.121	ACK	passt	S

Tabelle 1

Q18 *Wem gehört die Absenderadresse der Offer-Meldung?*

DHCP-Server

Q19 *Wo steht die Adresse des DHCP-Servers? Welches ist seine IP-Adresse?*

160.85.192.100

Q20 *Warum ist es sinnvoll, dass der gleiche Server für DHCP und DNS zuständig ist (vergleiche Abschnitt 4)?*

direkt weitergeben, konsistenz

Q21 *Wie gross ist die vereinbarte Lease Time?*

900s ≙ 15 min

Q22 *Welche Konfigurationselemente liefert der DHCP-Server nebst IP Adresse und Netzmaske?*

Q23 *Wie läuft die Erneuerung des Lease ab? An welche Adresse läuft die Anfrage?*

- Betrachten Sie nun die erste DHCP-Meldungssequenz.

Q24 *Was fällt Ihnen auf bezüglich DHCP-Server und IP-Adresse?*

- **Zeigen Sie die Resultate dem Laborbetreuer.**

10 Zusatzaufgaben für Interessierte: dig trace und whois Informationen

dig unterstützt eine Test-Funktionalität, bei welcher der konfigurierte Name Server umgangen wird und der Resolver selbst die komplette Namensauflösung übernimmt (Option: +trace)

- Bestimmen Sie nochmals den gesamten Suchweg für die Namensauflösung von www.zhaw.ch:
  `dig www.zhaw.ch +trace`

Q25 *Welche Unterschiede zu den Ergebnissen bei Q07 bis Q11 beobachten Sie?*

Die Verwendung des whois Befehls mit Namen als Anfrageziel liefert je nach Toop-Level Domain sehr unterschiedliche bzw. überhaupt keine Ergebnisse. Die IP Adressen werden durch andere Organisationen verwaltet.

- Machen Sie whois Anfragen auf die IP Adressen von Rechnern der Domains, die sie in Aufabge 7 verwendet hatten.
  `whois <IP-Adresse>`

Q26 *Welche Unterschiede stellen Sie fest?*

- **Zeigen Sie die Resultate dem Laborbetreuer.**