Hálózatok építése és üzemeltetése

Vizsga konzultáció

Vizsga

- Google kvíz
  - Teszt feladatok, ZH-hoz hasonlóan
  - Egyedi gyakorlati feladatok, amihez a HaEpUz VM saját példányát kell futtatni (BME Cloud, Smallville), kiugrókhoz hasonlóan
- Felkészülés
  - Előadások anyagai
    - slide-ok, videók
  - Gyakorlatok anyagai
    - slide-ok, videók
    - gyakorló feladatok és kiugrók
    - HaEpUz VM + csináljátok végig a feladatokat!

Vizsga

- Témakörök:
  - Linux alapok
  - szoftver szerszámok (ping, traceroute, netstat, tcpdump, wireshark, ifconfig, route, arp, ip, iptables, nslookup, dig, dhclient)
  - bash, python
  - hálózati funkciók (nat, firewall, dhcp, dns)
  - routing protokollok
  - SDN, OpenFlow
  - hálózatbiztonság
  - WiFi, WiFi biztonság
  - Internet
  - Mininet használata!

Egy ~~két~~ problémás ZH feladat

Hálózati funkciók

- Egy hoszt eth0 interfészén a default gateway-t szeretnénk beállítani. Melyik parancs(ok) végzi(k) el helyesen a konfigurációt?

A. `sudo route add default gw 192.168.0.1`
B. `sudo ip route add default via 192.168.0.1`
C. `sudo route add default gw 192.168.0.1 netmask 255.255.255.0`
D. `sudo route add -net 0.0.0.0 netmask 0.0.0.0 gw 192.168.0.1 eth0`

Bónusz feladat IMSc pontokért

- Egyszerű hálózatunkban a client gép a 10.0.0.0/24-es hálózton keresztül kapcsolódik a gateway géphez és azon keresztül a külvilághoz. Feltételezhetjük, hogy a client gép jól van konfigurálva. A client gépen a ping parancs futtatása után megvizsgáltuk a gateway gépet és az alábbi parancsokra a megadott válaszokat kaptuk. Milyen konfigurációs parancsok kiadása szükséges a gateway gépen, hogy a korábbi ping parancs működjön a client gépen?

Bónusz feladat IMSc pontokért


```
CLIENT:
=======
haepuz@haepuz-client:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.0.0.1        0.0.0.0         UG    0      0        0 enp0s9
10.0.0.0        0.0.0.0         255.255.255.0   U     0      0        0 enp0s9
192.168.56.0    0.0.0.0         255.255.255.0   U     0      0        0 enp0s8
haepuz@haepuz-client:~$
haepuz@haepuz-client:~$ ping -c1 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.

--- 8.8.8.8 ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms

haepuz@haepuz-client:~$
```

```
GATEWAY:
========
haepuz@haepuz-gw:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.1.1     0.0.0.0         UG    0      0        0 enp0s10
10.0.0.0        0.0.0.0         255.255.255.0   U     0      0        0 enp0s9
192.168.1.0     0.0.0.0         255.255.255.0   U     0      0        0 enp0s10
192.168.56.0    0.0.0.0         255.255.255.0   U     0      0        0 enp0s8
haepuz@haepuz-gw:~$
haepuz@haepuz-gw:~$
haepuz@haepuz-gw:~$ sudo iptables -t nat -nvL
Chain PREROUTING (policy ACCEPT 1 packets, 84 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 MASQUERADE  all  --  *      enp0s9  10.0.0.0/24          0.0.0.0/0
haepuz@haepuz-gw:~$
haepuz@haepuz-gw:~$
haepuz@haepuz-gw:~$ sudo iptables -nvL
Chain INPUT (policy ACCEPT 69 packets, 10902 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 49 packets, 5904 bytes)
 pkts bytes target     prot opt in     out     source               destination
haepuz@haepuz-gw:~$
```

ZH utáni témák

SDN

- Melyik NEM képzelhető el SDN alkalmazásként?

A. tűzfal
B. új TCP verzió saját torlódásvezérlési mechanizmussal
C. terhelés elosztó
D. legrövidebb útválasztás

SDN

- A lenti OpenFlow folyambejegyzés...
  - `cookie=0x0, duration=30s, table=0, n_packets=40, n_bytes=60000, idle_timeout=15, hard_timeout=35, idle_age=5, priority=65535, tcp, in_port=1, vlan_tci=0x0000, dl_src=00:00:00:00:00:01, dl_dst=00:00:00:00:00:02, nw_src=10.0.0.1, nw_dst=10.0.0.2, nw_tos=0, tp_src=1111, tp_dst=2222 actions=output:2`

A. 8s múlva még aktív lesz, ha csak egyetlen illeszkedő csomag érkezik pont 4s múlva
B. 15s múlva még aktív lesz, ha csak egyetlen illeszkedő csomag érkezik pont 8s múlva
C. átlagosan több mint 5 kbps forgalmat továbbított
D. által továbbított csomagok átlagos hossza kisebb mint 1000 byte.

SDN

- Egy reaktív logikájú kontrolleralkalmazás ...

A. nem működik megfelelően, ha a kapcsolók és a kontroller közti kapcsolat átmenetileg megszakad
B. a proaktív párjánál nagyobb csomagkésleltetést eredményez(het)
C. nem tudja a csomagok IP címét figyelembe venni
D. készíthető POX-ban.

Internet

- Az alábbi állítások közül mi igaz az Internetre?

A. Az Internet topológiáját az IANA nevű szervezet felügyeli.
B. Az Internet topológiája mérnöki tervezés és optimalizáció eredménye.
C. Az Internet spontán önszerveződéssel jött létre a különböző hálózatok lokális döntései nyomán.
D. Az Internet topológiáját a BGP protokoll segítségével lehet központilag megadni.

Internet

- Melyik állítás(ok) igaz(ak) az Internet alapegységeire, az Autonóm rendszerekre (AS, Autonomous systems)?

A. Az AS egy adminisztratív egységbe tartozó mérnökileg tervezett hálózat.
B. A BME saját hálózata egy AS.
C. A TMIT saját hálózata egy AS.
D. Az AS-eknek sorszámuk van, melyet a IANA nevű szervezet regisztrál.

Internet

- Melyek a hasonlóságok az Internet, a Facebook és a Debian csomagfüggőségek hálózatában?

A. Mindegyik spontán önszerveződéssel jött létre.
B. Mindegyik skálafüggetlen fokszámeloszlású.
C. Mindegyiknek az alapegységei (csomópontjai) elektronikus áramkörök.
D. Mindegyik kifejezetten sűrű hálózat.

Hálózatbiztonság

- Miért lehet sikeres egy ARP támadás?

A. A felhasználók figyelmen kívül hagyják az ARP tanúsítványokra vonatkozó figyelmeztető ablakokat
B. Hitelesnek elfogadott ARP üzenetet bárki készíthet, benne hamis információkkal
C. Az ARP vírus Linux és Windows gépeket is meg tud fertőzni
D. Az ARP protokollt meg lehet kerülni, a korábbi nyíltan támadható BGP protokoll használatával

Hálózatbiztonság

- Melyik NEM igaz a TCP SYN COOKIE védelem esetén?

A. A kliens gépeken nem szükséges módosítani a TCP vermet, csak a szerver oldalon
B. Használata során a kapcsolatfelépítések ideje megnőhet
C. A szerver csökkentett időablakokkal dolgozik, hogy minél hamarabb lezárja a kapcsolatokat
D. Sok TCP opció nem használható

Hálózatbiztonság

- A WPA TKIP algoritmus esetén miért alkalmazzuk még mindig a WEP blokkot?

A. Olyan megoldást kellett készíteni, ahol a régi eszközök továbbra is használhatóak maradnak
B. A WEP esetén nem volt gond a titkosítással csak a csoportkulcsot kellett lecserélni egyedire
C. A 128 bites kulcs megoldja a WEP problémáját, így a nagyobb kulccsal az továbbra is használható
D. A WPA TKIP megjelenése időpontjában még nem volt ismert, hogy gond lenne a WEP protokollal

Python

- Melyik jellemző NEM igaz a Python nyelvre?

A. hordozható
B. objektum orientált
C. statikusan típusos
D. interpretált

Python

- Mit takar az az állítás, hogy a Python nyelv dinamikusan (és erősen) típusos?

A. változót típusával együtt definiáljuk, ami futás során nem változhat meg
B. változót típusával együtt definiáljuk, ami futás során megváltozhat
C. változót típus nélkül definiálunk, de értékadás után típusa nem változhat meg
D. változót típus nélkül definiálunk, ami futás közben változhat

Python

- Melyik nyelvi kulcsszóval definiálható üres utasításblokk?

A. `continue`
B. `with`
C. `pass`
D. `None`

Python

- Milyen értékkel tér vissza az alábbiak közül a következő Python utasítás?
  - `[1, "0", "1", 0][1]`

A. 0
B. “1”
C. “0”
D. 1

Python

- Mit ír ki a következő Python kódrészlet?
  - `print( 2 * "AB"[:1] + "BA"[1:] * 2 )`

A. **"BBAA"**
B. **"AAAA"**
C. **"AABB"**
D. **TypeError: cannot concatenate 'int' and 'str' objects**

Python

- Milyen értékkel tér vissza az alábbiak közül a következő Python utasítás?
  - `[1, "0", "1", 0][-3:-1]`

A. `["0", "1"]`
B. `["0", "1", 0]`
C. `[1, "0", "1"]`
D. `[1, "0", "1", 0]`

Python

- Az alábbiak közül melyik Python utasítás értékelődik ki logikai igaz, azaz True értékként?

A. `42 in ["42", 42]`
B. `42 is ("42", 42)`
C. `42`
D. `"42"`

Gyakorlati feladatok

- Megadott script futtatása a saját HaEpUz VM-ben → saját Mininet környezet létrehozása, indítása
- Konkrét feladatok, kérdések
  - végrehajtás, munka a VM-ben
  - válaszok megadása a Google kvízben
    - opciók vagy
    - szövegdoboz a szintaktikailag helyes, kipróbált parancsok bemásolásával

Gyakorlati feladatok

- Példák a kvízekből

Kvíz: gyak2-3

- GW, CLIENT, INTERNET setup...
  - Ubuntu környezetben pl. a "sudo ntpdate ntp.ubuntu.com" parancs segítségével oldható meg az óra szinkronizálása egy központi szerverhez az NTP protokoll használatával. Szinkronizáld a CLIENT VM óráját! Ehhez milyen parancs(ok) kiadására volt szükség a GW VM-en?

Kvíz: gyak2-3

- GW, CLIENT, INTERNET setup...
  - Ubuntu környezetben pl. a "sudo ntpdate ntp.ubuntu.com" parancs segítségével oldható meg az óra szinkronizálása egy központi szerverhez az NTP protokoll használatával. Szinkronizáld a CLIENT VM óráját! Ehhez milyen parancs(ok) kiadására volt szükség a GW VM-en?
  - sudo iptables -A FORWARD -p udp --sport 123 -j ACCEPT
  - sudo iptables -A FORWARD -p udp --dport 123 -j ACCEPT

Kvíz: gyak4-5

- Saját mininetes hálózat indítása, környezet előkészítése
  - `wget -nv -O- https://sb.tmit.bme.hu/haepuz/ts | sudo sh /dev/stdin $NEPTUN`
  - ha nem akarjuk mindig a jelszót másolgatni: hozzunk létre a .ssh könyvtárban egy kulcspárt és a publikus kulcsot adjuk hozzá az authorized_keys fájlhoz. Pl.:
    - `cd ~/.ssh`
    - `ssh-keygen [3x enter]`
    - `cat id_rsa.pub >> authorized_keys`

Kvíz: gyak4-5

- Mininet hálózat: hosztok, szerverek, routerek (és persze switch-ek, linkek)
  - Ha a "Host A" gépről pingeljük a "Server" gépet, a "Host A" melyik interfészén történik a kommunikáció? Add meg a kérdéses interfész nevét!
  - Add meg az előző kérdés megválaszolásához (a forgalom megfigyeléséhez) használt parancsot!
  - A "Host B" gépről nem tudjuk pingelni a "Server" gépet, pedig innen is hasonlóan kéne működnie, mint a "Host A" gépről. Milyen parancs volt az, amivel sikerült felderíteni a hibát? (A hiba felderítéséhez persze több parancs használata szükséges, hacsak nem elsőre találjuk el. Itt most arra vagyunk kíváncsiak, amivel meglett a hiba.)
  - Add meg az előző hiba javításához használt parancsot/parancsokat!

Kvíz: gyak6

- Saját mininetes hálózat és kontroller indítása, környezet előkészítése
  - `wget -nv -O- https://sb.tmit.bme.hu/haepuz/table_error | sh /dev/stdin $NEPTUN`
  - egy felugró ablakban elindul egy mininetes hálózatemuláció és egy másik ablakban pedig egy pox kontroller
  - Próbáld ki, hogy a h1 hosztról nem lehet pingelni a h10-es hosztot. Azért nem, mert az egyik switch egyik folyamtábla-bejegyzésében szándékosan el van írva az output port értéke. A feladat megkeresni, hogy az elrontott folyamtábla-bejegyzéshez milyen cookie érték tartozik. A megoldás mezőbe ezt a cookie értéket kell hexadecimális formában beírni (pl. 0xa4).

Kvíz: gyak6

- Saját mininetes hálózat és kontroller indítása, környezet előkészítése (mininet, pox terminálok)
  - `wget -nv -O- https://sb.tmit.bme.hu/haepuz/star | sh /dev/stdin $NEPTUN`
  - A pox kontroller és a mininetes hálózat elindítása után a h1 hosztról sikeresen lehet pingelni a h2 hosztot. Azonban a ping kérésekre nem a h2 hoszt válaszol, mert a kontroller eltéríti a ping forgalmat egy másik hoszthoz, valamint a forgalomról egy másolatot is kiküldet a kapcsolóval egy nem létező porton. Mi annak a hosztnak a neve, ami a h2 felé küldött ping kérésekre válaszol (pl: h73)?
  - Mi annak a nem létező portnak a száma (pl: 211), ahova a kontroller a másolatot küldeti a kapcsolóval?
  - Hány darab folyambejegyzés található a kapcsoló folyamtáblájában?

Gyakorlati feladatok

- További példák

Hálózati funkciók

- Saját környezet indítása után...
  - a Troubleshooting gyakorlat bármelyik feladata (vagy ahhoz hasonló feladat...)
  - például:
    - ki kell találni, hogy mi a hiba a saját hálózatban
    - javítani kell a hibát
    - a már működő hálózatban le kell futtatni egy parancsot és a kapott választ kell megadni a kvízben

Hálózati funkciók

- Saját környezet indítása után...
  - milyen topológiájú hálózat indult el a Mininetben? (pl. opciók: 3 elemű lánc, 2 szintű fa, csillag, ...)
  - h1 hosztról h5 hoszt milyen átlagos körülfordulási idővel érhető el? (pl. opciók: adott idő intervallumok)
  - gateway – client konfiguráció, pl.
    - h1: client
    - r1: gateway
    - h5: remote server a külvilágban
    - mit kell konfigurálni?
      - .

Hálózati funkciók

- Saját környezet indítása után...
  - milyen topológiájú hálózat indult el a Mininetben? (pl. opciók: 3 elemű lánc, 2 szintű fa, csillag, ...)
  - h1 hosztról h5 hoszt milyen átlagos körülfordulási idővel érhető el? (pl. opciók: adott idő intervallumok)
  - gateway – client konfiguráció, pl.
    - h1: client
    - r1: gateway
    - h5: remote server a külvilágban
    - mit kell konfigurálni?
      - (ip_forward), nat (snat, dnat), firewall (esetleg dhcp, egyszerűsített dns)

OpenFlow

- Saját környezet indítása után...
  - hány darab folyambejegyzés található a kapcsoló folyamtáblájában?
  - ha az első bejegyzésre folyamatosan érkezik illeszkedő forgalom, akkor az indítás után hány másodperccel törlődik a bejegyzés?
  - ha a második bejegyzésre sosem érkezik illeszkedő forgalom, akkor az indítás után hány másodperccel törlődik a bejegyzés?

OpenFlow

- Saját környezet indítása után...
  - OpenFlow hálózat, nem az elvárt működés, mi az oka?
  - hibakeresés
    - flow táblák, bejegyzések, számlálók vizsgálata
    - hibás bejegyzések azonosítása
    - hibás bejegyzések javítása
    - működés validálása