Hálózatok építése és üzemeltetése

Vizsgafeladatok

Vizsga

- Google kvíz
  - Teszt feladatok, ZH-hoz hasonlóan
  - Egyedi gyakorlati feladatok, amihez a HaEpUz VM saját példányát kell futtatni (BME Cloud, Fured), kiugrókhoz hasonlóan
- Felkészülés
  - Előadások anyagai
    - slide-ok
  - Gyakorlatok anyagai
    - slide-ok
    - 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
  - Internet
  - Mininet használata!

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

gyak3 gyakorló feladatok

- traceroute
  - Vizsgáljuk meg, hogy a GW VM milyen útvonalon (routereken keresztül) éri el a www.stanford.edu gépet és analizáljuk azt is, hogy ennek hogy történik a felderítése a traceroute program segítségével! Ehhez a következő lépéseket hajtsuk végre:
    - Találjuk ki a www.stanford.edu névhez tartozó IPv4 címet!
    - A wireshark program segítségével vizsgáljuk a beazonosított IPv4 címre kimenő és onnan bejövő forgalmakat (a releváns interfészen)!
    - A traceroute program default beállításával indítsuk a vizsgálatot a www.stanford.edu gépre!

gyak3 gyakorló feladatok

- traceroute
  - Milyen típusú forgalommal történik a tesztelés és milyen lépésekben? Milyen protokoll, IP cím, port szám, TTL érték, stb. van beállítva, hány csomaggal történik a vizsgálat?
  - Honnan milyen válaszok érkeznek?
  - Ezek alapján hogyan azonosítható az útvonal?

gyak3 gyakorló feladatok

- traceroute
  - Milyen típusú forgalommal történik a tesztelés és milyen lépésekben? Milyen protokoll, IP cím, port szám, TTL érték, stb. van beállítva, hány csomaggal történik a vizsgálat?
    - default 3 UDP csomag/port a célcímre, destination port: 33434, 33435, 33436 TTL=1, …
  - Honnan milyen válaszok érkeznek?
    - Routerek válaszolnak, ICMP üzenet: TTL exceeded
  - Ezek alapján hogyan azonosítható az útvonal?
    - Akinél “elfogy” a TTL válaszol, aki tovább engedi nem küld választ (tipikusan nem használt portok)

gyak3 gyakorló feladatok

- traceroute
  - Hány hop-ból áll az útvonal? Milyen IPv4 című routerekből áll az útvonal?
  - Alakítsuk át úgy a vizsgálatot, hogy ICMP Echo Request csomagokkal történjen a tesztelés és ne kelljen kivárni a felesleges mérések ereményét! Vizsgáljuk a forgalmat wireshark segítségével.

gyak3 gyakorló feladatok

- traceroute
  - Hány hop-ból áll az útvonal? Milyen IPv4 című routerekből áll az útvonal?
    - Mérésfüggő útvonal és hop szám
  - Alakítsuk át úgy a vizsgálatot, hogy ICMP Echo Request csomagokkal történjen a tesztelés és ne kelljen kivárni a felesleges mérések ereményét! Vizsgáljuk a forgalmat wireshark segítségével.
    - sudo traceroute -m 8 -I www.stanford.edu

Példa 1

- Saját mininetes hálózat és kontroller indítása, környezet előkészítése
  - `wget -nv -O- http://ib213.tmit.bme.hu:8888/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).

Példa 2

- Saját mininetes hálózat és kontroller indítása, környezet előkészítése (mininet, pox terminálok)
  - `wget -nv -O- http://ib213.tmit.bme.hu:8888/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?

Példa 3

- Saját mininetes hálózat és kontroller indítása, környezet előkészítése (mininet, pox terminálok)
  - `wget -nv -O- http://ib213.tmit.bme.hu:8888/haepuz/startsv2 | sh /dev/stdin $NEPTUN`
  - A létrejött hálózatban a kontroller csak IP csomagokat továbbít. A h1 hosztról két hoszt kivételével sikeresen lehet pingelni a többi hosztot. Ezen a két hoszton szándékosan elrontottunk valamit. A két rossz hoszt közül mi a kisebb sorszámú hoszt neve?
  - A két rossz hoszt közül mi a nagyobb sorszámú hoszt neve?
  - Ha nem szeretnénk felesleges parancsokat kiadni, milyen parancs kiadásával kezdjük a hiba elhárítását a kisebb/nagyobb sorszámú hoszton?
    - arp; ip addr del; ip link set dev; ip route; ip addr add; route del default gw; dhclient -v; sysctl -w net.ipv4.ip_forward=1

Példa 4

- Saját mininetes hálózat és kontroller indítása, környezet előkészítése (mininet, pox terminálok)
  - `wget -nv -O- http://ib213.tmit.bme.hu:8888/haepuz/balancerv4 | sh /dev/stdin $NEPTUN`
  - Közvetlenül a hálózat elindítása után hány darab folyambejegyzés található összesen a kapcsolók folyamtáblájában (minden kapcsoló minden bejegyzését összeadva)?
  - A h0 hosztról a 10.0.0.10 címre indított ping hatására hány darab ARP request - response üzenetváltás történik?
  - A h0 hosztról a 10.0.0.10 címre indított ping-re (ICMP echo request) melyik hoszt fog válaszolni (pl: h25)?
  - A h0 hosztról a 10.0.0.10 címre indított UDP forgalmat melyik hoszt fogadja (pl: h25)?
  - Ha a h0 hosztról a 10.0.0.10-es gépre szeretnénk belépni ssh-val a 22-es porton (és be lenne konfigurálva megfelelően az ssh hozzáférés), akkor melyik hosztra jutnánk be (pl: h25)?
  - A h0 hosztról a 10.0.0.10-es címre indított http kéréseket melyik hoszton működő szerver szolgálná ki (pl: h25)? (Default porton működő webszervereket feltételezünk.)

Példa 5

- Saját mininetes hálózat indítása, környezet előkészítése
  - `wget -nv -O- http://ib213.tmit.bme.hu:8888/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`

Példa 5a

- 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!

Példa 5b

- Mininet hálózat:
  - A "Host A" és "Host C" eszközök között milyen interfészeken halad a forgalom? Add meg a parancsot, amivel ezt feltérképezted és add meg a parancs kimenetét!
  - A "Host C" egy /24-es alhálózatra csatlakozik. Rajta kívül még több más eszköz is csatlakozik ugyanerre az alhálózatra. A "Host A" gépről próbáld pingelni a "Host C"-nél eggyel nagyobb IP címmel rendelkező eszközt! Melyik IP címről érkezik válasz? Hány interfészen halad át a csomag?
  - Jelentkezz be arra az eszközre, amelyikhez az utolsó azonosított interfész tartozik! (A bejelentkezéshez használható IP cím a hálózat indításakor szintén listázásra került.) Mi okozza a hibát? Add meg a felderítéshez használt egyetlen parancsot, annak kimenetéről a hibát okozó sort, valamint egy egy mondatos magyarázatot arról, hogy ez mit jelent!
  - Adjál olyan megoldást a problémára, ami a kérdéses alhálózat minden elemére javítja a hibát! Másold be a használt parancsot/parancsokat!

Gyakorlati feladatok

- Még milyen jellegű feladatok várhatók?

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