Tema 2

* **Publicare**:

- ~~***11 Ianuarie 2021 18:00***~~
- ~~din păcate, întâmpinăm probleme tehnice :D, amânăm marea lansare până mâine dimineață ora 09:00 :(~~
- ***2021-01-12 09:00***: Tema a fost lansată oficial! :D

* **Termen de predare**:

- ***27 Ianuarie 2021 23:55 - deadline HARD***

Tema constă în realizarea configurației unui set de exerciții pe o topologie simulată într-o mașină virtuală. Topologia este alcătuită din mașina guest și trei containere virtualizate cu ajutorul tehnologiei LXC (atenție: nu se folosește Docker, ca la laboratoare, însă modul de utilizare este similar). Mai multe detalii despre topologie găsiți la secțiunea Topologie.

Revizii:

Notare

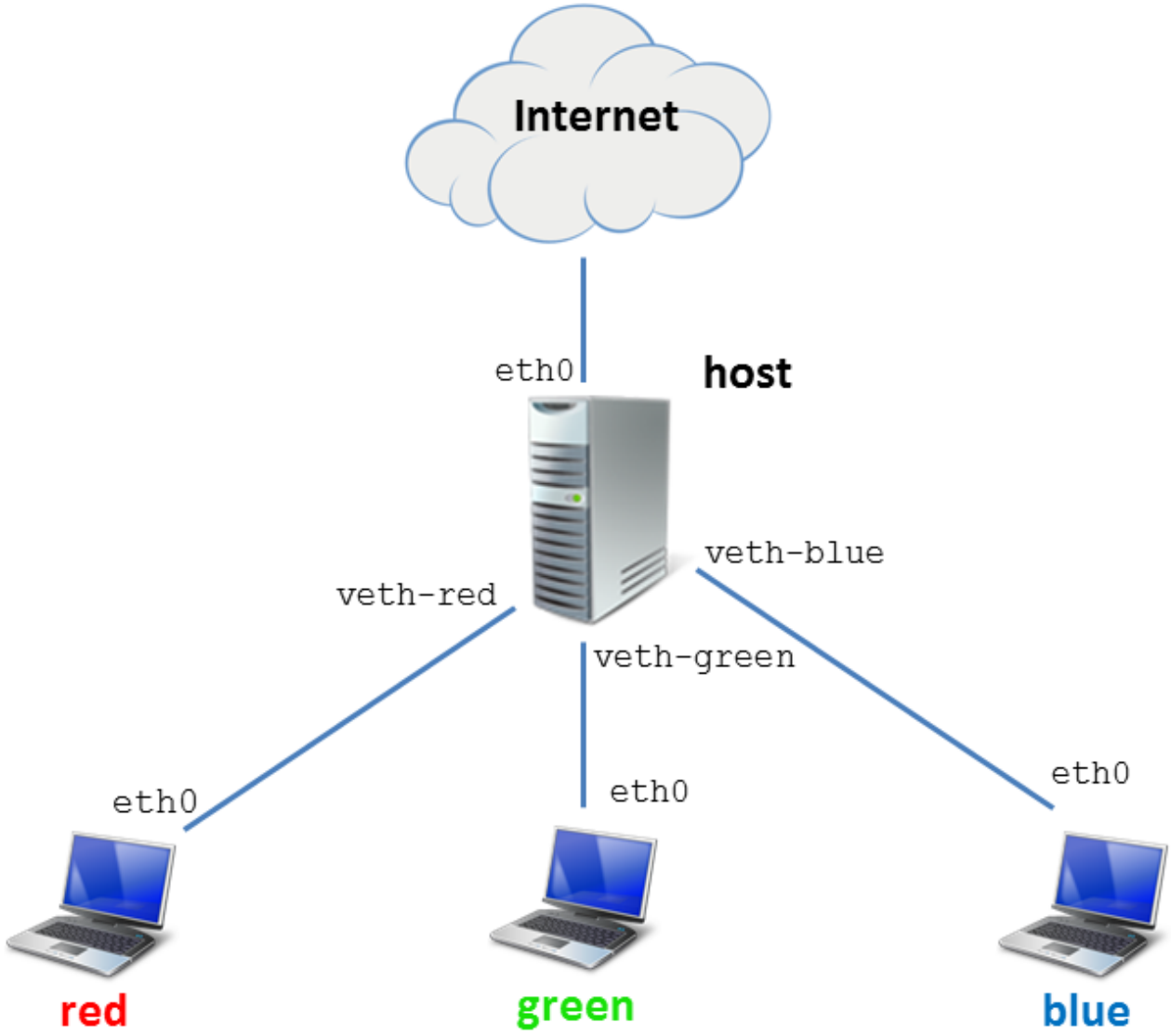
Fiecare exercițiu are un punctaj propriu. Nota pe întreaga temă este dată de suma punctajelor acumulate în urma rezolvării fiecărui exercițiu.

Punctajul maxim care se poate obține pe întreaga temă este 100 de puncte. Acest punctaj este echivalent cu 1.95 puncte din nota finală.

Există exerciții bonus cu ajutorul cărora puteți obține 125 de puncte. Din păcate, punctajul se trunchiază la 100 de puncte. Puteți rezolva exerciții bonus în schimbul exercițiilor obișnuite.

Nu este obligatorie rezolvarea tuturor exercițiilor. Exercițiile pot fi rezolvate în orice ordine, mai puțin în situația în care un exercițiu depinde de rezolvarea unui alt exercițiu.

Topologie



Mașina virtuală

Utilizare

- Momentan, imaginea VM a temei este disponibilă doar pe OpenStack.
- Pentru autentificare, utilizați credențialele **root/student** sau **student/student**.
- Notă: pe OpenStack, autentificarea cu username și parolă a fost dezactivată! Folosiți autentificarea cu chei, prezentată aici [https://cloud.curs.pub.ro/about/tutorial-for-students/].

Pași pentru accesare OpenStack

- Urmăriți pașii Tutorial Cloud [https://cloud.curs.pub.ro/about/tutorial-for-students/].
- Link dashboard: https://cloud-controller.grid.pub.ro/ [https://cloud-controller.grid.pub.ro/]
- Nume imagine: **RL 2020 Tema2**
- Tip instanță: **m1.small** (NU aveți nevoie de mai mult)
- **OBLIGATORIU:** autentificarea cu user și parolă a fost dezactivată, folosiți EXCLUSIV chei publice ssh (pe care ar trebui s-o aveți deja configurată în cadrul laboratoarelor).

Atenție! NU distrugeți instanța mașinii virtuale până nu ați încărcat arhiva finală pe RL Checker și ați obținut punctajul dorit (și să fiți siguri că nu veți mai avea nevoie să modificați nimic).

Pentru a rezolva tema este îndeajuns să prelucrați fișiere doar din directoarele /etc, /home și /root (atât pe host, cât și pe containere). NU instalați alte pachete în plus.

Verificarea temei

- Înainte de a rula checkerul, se recomandă descărcarea ultimului update prin rularea

```
root@host$ t2update
```

.

- Pentru verificarea temei este disponibil un checker local. Atenție: nu este substitut pentru depanare!
  - Altfel spus, contează soluția voastră, nu checker-ul.
  - Dacă, dintr-o greșeală, checker-ul dă rezulat pozitiv în cazul unui exercițiu rezolvat greșit nu înseamnă că se va puncta. O eventuală actualizare a checker-ul va puncta corect.
  - Obiectivul trebuie să fie rezolvarea corectă a enunțului. Checker-ul vine ca o confirmare (ne dorim cât mai sigură) a acelei rezolvări.
  - Punctajul afișat pe RL Checker va fi și cel acordat în catalog la final.
- Dacă sunt probleme, puteți să postați un mesaj pe thread-ul aferent de pe forum [https://curs.upb.ro/mod/forum/view.php?id=81538];
- Mașina virtuală conține checkerul (sursă închisă) și dispune de două scripturi pentru a face actualizarea și rularea sa mai simplă.
- Comenzile de mai jos pot fi rulate indiferent de directorul in care ne aflăm.
- Pentru a actualiza checker-ul:

```
t2update
```

- Pentru a rula checkerul:

```
t2check
```

- Exemple de folosire:

```
root@host:~# t2check 11
tests/test_11       .............  10.00/10.00

root@host:~# t2check
tests/test_01       .............  10.00/10.00
tests/test_02       .............  10.00/10.00
tests/test_03       .............  5.00/5.00
tests/test_04       .............  5.00/5.00
...

Total = [ 125.00/100.0 ]
```

Predarea temei

1. Pentru urcare soluție, rulați:

```
root@host$ t2check --save
```

2. Rezultatul este o arhivă semnată în directorul în care invocați comanda.
3. Folosind utilitarul scp, copiați acest fișier pe stația voastră locală (atenție să nu încurcați directoarele și să copiați o arhivă veche / salvată în altă parte!). Dacă sunteți conectat la OpenStack prin serverul intermediar fep.grid.pub.ro, va trebui să copiați mai întâi acolo, apoi s-o preluați pe stația voastră de lucru (alternativ, puteți folosi funcționalitatea de ProxyCommand a clientului ssh pentru o conexiune directă).
4. Încărcați arhiva pe RL Checker [https://curs.upb.ro/mod/lti/view.php?id=65090] (Moodle).

Recomandăm ca rezolvarea exercițiilor trebuie să se facă în mod persistent. La o repornire a mașinii virtuale, rezolvările trebuie să rămână active, altfel puteți întâmpina dificultăți la o revenire ulterioară asupra temei.

Folosiți comanda reboot înainte să testați de-a întregul.

Personalizarea temei

Rezolvările sunt particularizate pentru fiecare student (pe baza contului Moodle). Pentru a obține aceste date, accesați link-ul Moodle RL Checker [https://curs.upb.ro/mod/lti/view.php?id=65090].

Datele de particularizare afișate pe Moodle vor fi introduse şi în fişierul **/root/tema2.txt**, unde va trebui să păstrați formatul text VARIABILA=valoare (liniile noi în plus nu contează)! Atenție: nu puteți personaliza aceste valori, ele fiind verificate cu strictețe de către checker-ul online!

Informațiile generate anterior vor fi folosite în enunțul temei cu următoarele notații:

- $A = valoarea variabilei A
- $B = valoarea variabilei B
- $C = valoarea variabilei C
- $D = valoarea variabilei D
- $E = valoarea variabilei E
- $F = valoarea variabilei F
- $G = valoarea variabilei G
- $H = valoarea variabilei H
- $I = valoarea variabilei I
- $J = valoarea variabilei J
- $K = valoarea variabilei K

Discuții legate de temă

Toate discuțiile legate de probleme/întrebări/exerciții din tema de RL trebuie puse pe forumul temei [https://curs.upb.ro/mod/forum/view.php?id=81538]. Reguli de utilizare ale acestui forum:

- Nu se pun rezolvări pe forum.
- Fiecare întrebare legată de un task trebuie pusă pe thread-ul dedicat acelui task.
- În momentul în care puneți o întrebare, includeți în mesaj:
  - contextul în care a apărut problema pe care o semnalați
  - ce ați încercat să faceți pentru a repara problema
  - alte informații care pot descrie mai bine problema
  - dacă este vorba de rezolvarea unui task, cum ați verificat rezolvarea task-ului
- Verificați dacă cineva nu a mai întâmpinat aceeași problemă și i-a fost oferit un hint sau o soluție (lurk before you leap).
- Post-uri care nu sunt puse pe thread-ul corespunzător vor fi șterse.
- **Nu creați thread-uri noi de discuție! Vor fi șterse.**

Subiecte

Toate configurațiile să fie **persistente**. Trebuie să fie active și după repornirea mașinii virtuale.

Va trebui să realizați primele 5 exerciții în ordine. Întrucât aceste exerciții oferă, în final, conectivitate la Internet, restul se vor baza pe acestea!

Dacă folosiți mai multe scripturi (apelați dintr-un script alt script), folosiți căi absolute. Adică folosiți /root/scripts/make-juju.py în loc de ./make-juju.py pentru a nu se baza pe directorul actual de lucru (working directory).

Nu trebuie instalați nimic în plus pe mașina virtuală, nu ar trebui să fie nevoie.

Se recomandă citirea întregului set de exerciții înainte de rezolvarea temei. În mod asemănător, la rezolvarea unui exercițiu se recomandă citirea întregului subset de exerciții.

1. (**10 puncte**) Adresare IPv4
    a. Configurați cu adrese IP toate legăturile din topologie, astfel:
        - Rețeaua red: 10.11.$A.0/28
        - Rețeaua green: 10.11.$A.16/28
        - Rețeaua blue: 10.11.$B.32/30
        - Sistemul host va avea prima adresă asignabilă, iar containerul, pe cea de-a doua.
    b. Configurați rutarea IPv4 pentru a permite comunicarea între toate sistemele. Sistemele red, green și blue vor avea ruta default prin sistemul host.
2. (**10 puncte**) Adresare IPv6
    a. Configurați adrese IPv6 pentru întreaga rețea astfel:
        - Rețeaua red 2001:12:$C::/64
        - Rețeaua green 2001:12:$D::/64
        - Rețeaua blue 2001:12:$E::/64
        - Sistemul host va avea prima adresă asignabilă, iar containerul, pe cea de-a doua.
    b. Configurați rutarea IPv6 pentru a permite comunicarea între toate sistemele. Sistemele red, green și blue vor avea ruta default prin sistemul host.
3. (**5 puncte**) Realizați configurațiile necesare astfel încât echipamentele să poată fi accesate prin numele lor (folosiți numele host, red, green, respectiv blue). Adăugați intrări de hosts doar pentru adresele IPv4.
4. (**5 puncte**) Realizați configurațiile necesare pentru ca cele 3 containere sa aibă acces la Internet.
    - Configurați sistemul host astfel încât să facă translatarea doar pentru adresele IP configurate static pe interfețele containerelor, nu și pentru alte adrese din rețelele lor.
    - **Observație**: adresa IP de pe eth0 a sistemului host este asignată dinamic de către ISP, prin DHCP; configurarea trebuie realizată astfel încât conectivitatea la internet a containerelor să nu depindă de această adresă IP.
5. (**5 puncte**) Configurați cele 3 containere pentru a putea accesa resurse din Internet pe baza numelor de domeniu al acestora (DNS).
    - **Observație**: Fișierul /etc/resolv.conf este volatil. Ce scrieți in el nu va fi persistent! Găsiți altă soluție! (*hint*: distribuțiile moderne folosesc systemd-resolved)
6. (**10 puncte**) Configurați NAT pe sistemul host astfel încât:
    - Conexiunile pe porturile (22000 + $G), (22000 + $H), (22000 + $I), să conducă la conectarea SSH pe sistemele blue, green respectiv red.
    - Conexiunea pe portul (19123 + $J), să conducă la conectarea FTP pe sistemul red.
    - Conectarea pe portul (11337 + $K) să conducă la conectarea pe tracker-ul de pe sistemul green.
7. (**10 puncte**) Configurați filtrarea de pachete astfel încât:
    - conexiunile SMTP (port 25) inițiate de pe sistemul red să fie blocate *(inclusiv către host!)*;
    - conexiunile către tracker-ul ce rulează pe sistemul green să nu fie permise de pe sistemul red.
    - blocați TOATE conexiunile trimise către blue, mai puțin protocoalele icmp, ssh și ftp (atenție: NU blocați conexiunile inițiate de către blue / răspunsurile de la acestea! folosiți reguli **stateful**);
8. (**5 puncte**) Configurați serviciul de SSH pe toate sistemele astfel încât:
    - autentificarea cu utilizatorul student de pe oricare sistem să fie permisă pe toate celelate sisteme (tot în cadrul utilizatorului student) folosind chei publice;

- folosind alias-uri SSH [http://collectiveidea.com/blog/archives/2011/02/04/how-to-ssh-aliases/] să fie folosite comenzi simplificate pentru autenficarea pe sisteme:
  - ssh h să ducă către sistemul host cu utilizatorul student;
  - ssh r să ducă către sistemul red cu utilizatorul student;
  - ssh g să ducă către sistemul green cu utilizatorul student;
  - ssh b să ducă către sistemul blue cu utilizatorul student.
  - **Observație**: ssh-copy-id utilizează autentificare ssh pe bază de parolă pentru a copia cheia. Mașina virtuală pe OpenStack nu permite astfel de autentificare pe host, așadar veți fi nevoiți să autorizați cheia publică manual in fișierul corespunzător!

9. (**10 puncte**) Căutare recursivă printre pagini HTTP cu autentificare.
   - Creați pe sistemul red scriptul /home/student/scripts/retrieve-secret care să caute recursiv prin paginile de la http://host/forbidden/ [http://host/forbidden/] și să găsească sub-calea secret (e.g., http://host/forbidden/sub/cale/secret [http://host/forbidden/sub/cale/secret]).
   - Scriptul va trebui să afișeze DOAR conținutul acelei pagini găsite!
   - Va trebui să vă autentificați în formularul inițial pentru a putea accesa restul de pagini:
     - *username*: fs
     - *password*: cuba1337
   - Trebuie să păstrați cookie-ul furnizat în urma autentificării pentru restul de cereri recursive!
   - **Hint**: Atât wget cât și curl au opțiuni pentru a face mai facil acest lucru ;)
10. (**10 puncte**) Descărcare / încărcare fișiere prin ftp. Pe sistemul host:
    - Realizați un script /root/scripts/ftp-upload care uploadează DOAR fișierele de forma [0-9][0-9].txt (adică două cifre și extensia .txt) din directorul curent la URL-ul ftp://red/upload/ [ftp://red/upload/], autentificându-se cu utilizatorul fs și parola valuta$$.
    - Realizați un script /root/scripts/ftp-download care descarcă DOAR fișierele cu forma [A-Z]_[0-9].tar.gz (adică literă mare + underscore + o cifră și extensia .tar.gz) de la URL-ul ftp://red/download [ftp://red/download] în directorul curent. Descărcarea se face în mod anonim, fără autentificare.
    - **Notă:** Transferurile trebuiesc făcute în modul binar (și NU text)!
    - Pentru testare, puteți să vă creați structurile necesare (checkerul face acest lucru automat).
11. (**10 puncte**) Pe sistemul host este configurat un server de e-mail (SMTP):
    - Creați pe sistemul green scriptul /root/scripts/sendmail care să trimită un mesaj către contact@host ce va conține:
      - subiectul Promotie Corona
      - o linie cu text preluat din primul argument de apel al scriptului;
      - atașament cu fișierul attachment.bin preluat din directorul curent de unde este rulat scriptul.
12. (**5 puncte**) Pe sistemul host, creați un set de reguli de firewall pentru jurnalizarea acceselor realizate de la sistemul blue către serverul telnet de pe sistemul green.
    - Aceste reguli trebuie să genereze mesaje syslog care să fie salvate în fișierul /var/log/insecure.log.
    - Mesajele trebuie prefixat de șirul “insecure-telnet: ”.
    - **Hint:** fiecare mesaj de log trece, mai întâi, prin serviciul rsyslog, care decide în ce fișier va fi scris.
13. (**5 puncte**) Pe sistemul red, creați un script /root/scripts/get-host-port care va primi, ca prim argument, numărul unui port TCP (1-65535), și va scrie, la stdout, textul “adevarat” dacă acel port este deschis pe host (**inclusiv IPv6!**) si “sad” în caz contrar.
14. (**Bonus - 10 puncte**) Configurați un tunel GRE (Generic Routing Encapsulation) între red și green.
    - Denumiți interfețele de tunel dacic pe ambele capete.
    - Folosiți rețeaua IPv6 2021:20:$F::/64 pentru capetele tunelului.
15. (**Bonus - 15 puncte**) Configurați un server DHCP pe red pentru a furniza IPv4 în rețeaua tunelului GRE creat anterior.
    - Configurați serviciul de DHCP astfel încât să ofere adrese IP din spațiul 10.120.$A.0/24 prin tunelul GRE, iar containerul green să primească mereu a 100-a adresă IP asignabilă

(10.120.$A.100).

- *Hint:* Verificați ce pachet de server DHCP aveți instalat și faceți o alegere (aveți 2 posibilități).

rl/teme/tema2.txt · Last modified: 2021/01/12 08:37 by florin.stancu