

Subiecte examen practic RC 2007-2008

23 ianuarie 2008

1. a. Activati rutarea pe statie b. Setati o ruta statica catre gsp.ro folosind ca gateway ip-ul server-ului de DHCP.
2. Configurati un server DNS pentru <numelevostru>.ro. Trebuie sa aveti setate cel putin urmatoarele intrari: descrierea domeniului, rezolvarea directa, rezolvarea inversa, serverul de nume, serverul de mail, serverul ftp. Folositi IP-ul statiei voastre pentru toate intrarile. Convergenta pentru domeniul vostru trebuie sa aiba loc in maxim 2 ore.
3. Configurati un server de mail pentru domeniul <numelevostru>.ro. Instalati clientul de mail ALPINE si configurati-l in asa fel incat sa puteti citi mailul de la serverul proaspat configurat.
4. Respingeti pachetele care au ca destinatie adrese de IP private si multicast (cu exceptia adresei voastre).
5. Afisati toate conexiunile UDP la/de la masina locala dezactivand rezolvarea numelor de domeniu.
6. Folosind numai mecanisme de nivel 2, faceti ca pachetele spre default gateway sa nu ajunga la destinatie. Nu uitati sa scoateti setarea dupa ce ati fost notati pe acest subiect.
7. Limitati numarul de fisiere care poate fi creat de userul student la 100.
8. Configurati un server de web pentru domeniile www.pub.ro (cu alias pub.ro) si www.student.ro (cu alias student.ro). Activati CGI doar pentru www.pub.ro si creati un script CGI simplu (Hello World!).
9. a) Afisati tabela arp a statiei dezactivand translatarea adreselor IP si introduceti o intrare statica pentru default gateway in asa fel incat sa nu va pierdeti conectivitatea. b) Respingeti conexiunile din exterior la toate serverele configurate pana acum.
10. Configurati sistemul astfel incat utilizatorul student sa nu poata vedea ce alti utilizatori au cont in sistem.
11. a) Obtineti configuratia dinamica a interfetei de retea si notati-o. Introduceti aceasta configuratie in mod static si permanent. b) Adaugati o ruta cu caracter permanent catre hostul 192.168.1.2 cu metrica 30 si un gateway ales de voi. c) Afisati tabela de rutare.
12. Configurati statia voastra astfel incat sa fie autoritara pentru domeniul "examen.com". Configurati adrese alese de voi pentru serverele mail.examen.com si www.examen.com. Faceti o interogare catre serverul DNS local din care sa aflati numele serverului de mail pentru domeniul examen.com.
13. a) Verificati care este serverul DNS folosit in acest moment de sistemul de operare, notati aceasta adresa, si configurati serverul vostru de DNS sa foloseasca aceasta adresa ca adresa de forward. b) Schimbati serverul DNS folosit in mod curent cu serverul de pe statia locala. c) Afisati adresele serverelor de nume pentru domeniul yahoo.com folosind serverul DNS local.

14. a) Instalati serverul de mail postfix alegand domeniul cszone.com. Configurati o casuta postala virtuala pentru myuser@labrc.com, astfel incat mesajele pentru acest utilizator sa fie stocate in /var/mail/vhosts/labrc.com/myuser. b) Verificati trimitand un mesaj de la userul student@cszone.com catre myuser@labrc.com.
15. Instalati serverul Apache2 pe statia voastra si configurati modulul UserDir astfel incat webroot-ul pentru fiecare utilizator sa fie directorul www. Creati in "/home/student/www" directorul test. In directorul "test" creati fisierele "fis1.txt" si "fis2.txt" astfel incat aceste 2 fisiere sa poata fi accesate doar daca se cunosc caile exacte http://localhost/student/test/fis1.txt si http://localhost/student/test/fis2.txt, iar la accesarea URL-ului http://localhost/student/test sa apara un mesaj de tip Forbidden.
16. a) Modificati drepturile asupra directorului "test" de mai sus astfel incat la accesarea URL-ului http://localhost/student/test sa fie afisat continutul acestui director. b) Restrictionati accesul la "http://localhost/student/test" astfel incat sa fie cerute un user si o parola. c) Schimbati portul pe care asculta serverul web din 80 in 8080.
17. Instalati serviciul de ssh. a) Rejectati conexiunile ssh catre localhost. b) Blocati conexiunile de web si ftp initiate de pe statia locala.
18. a) Generati trafic folosind ping si capturati 5 pachete de tip echo-reply, afisand continutul acestora in hexa, folosind tcpdump. b) Instalati Wireshark si capturati pachetele arp request. c) Afisati tabela arp in mod text, impiedicand rezolutia adreselor IP in nume.
19. a) Folosind utilitarul netstat afisati toate conexiunile tcp in starea listening, afisand si numele programului si impiedicand rezolutia adreselor IP in nume. b) Folosind nmap scanati localhost-ul si detectati porturile deschise si sistemul de operare.
20. Creati un filtru care sa respinga (cu trimiterea unui mesaj ICMP inapoi catre sursa) conexiunile SSH initiate de catre localhost.
21. Sa se configureze temporar o subinterfata cu adresa IP 192.168.73.22/27 si adresa de broadcast corespunzatoare.
22. a. Adaugati permanent o ruta implicita catre 192.168.73.1. b. Protejati-va de atacurile de tip ARP Poisoning, stiind adresa MAC a gateway-ului, AA:BB:CC:DD:EE:FF.
23. Blocati toate pachetele ICMP de tipul echo request ce sunt destinate statiei voastre.
24. Aflați ce porturi din intervalul (1-1000) sunt deschise si versiunea serviciilor ce asculta pe porturile respective.
25. Configurati serverul Web astfel incit prin accesarea sitului www.test1.com si primii un mesaj scris de voi, iar prin accesarea sitului www.test2.com/test.txt si afisati fisierul test.txt. Pentru www.test1.com directorul radacina va fi /home/user1/www iar pentru www.test2.com este cel implicit.
26. Configurati Postfix astfel incat un mesaj trimis de la student@localhost catre alias@localhost sa fie trimis catre user1@rc.ro, user2@rc.ro ai test.practic@gmail.com. Dupa transmitere, mesajul se va afla in casutele postale ale utilizatorilor locali user1 si user2.
27. Configurati serverul de DNS pentru a raspunde la cereri pentru domeniul exemplu.ro. Serverul de nume asociat domeniului este ns.exemplu.ro. Serverele de mail asociate domeniului sunt mail1.exemplu.ro avand prioritatea de 1 si mail2.exemplu.ro avand prioritatea 3. Adresa administratorului este admin@exemplu.ro. Serverul de nume are adresa 172.16.10.20. Serverul mail1 are adresa 172.16.10.30. Serverul mail2 are adresa 172.16.10.40. mail1.exemplu.ro este alias pentru mail.exemplu.ro.

28. In reseaua interna aveti un server Web cu adresa 10.10.10.10. Permiteti doar statiilor din reseaua 193.1.1.0/24 accesul catre acest server. Interfata din exterior este eth1.
29. Afișati toate pachetele ICMP de tipul echo reply.
30. Modificati TTL-ul pachetelor plecate de pe statia locala la valoarea 3. Vizualizati campul modificat cu ajutorul unui utilitar de captura de pachete.
31. Activati rutarea si definiti o ruta default catre 10.38.96.96.
32. Instalati Postfix cu domeniul testrc.cs.pub.ro si trimiteti un email catre adresa test.practic@gmail.com
33. Sa se creeze un alias pentru adresa de e-mail test.practic@gmail.com si sa se trimita un mesaj catre acel alias.
34. a)Instalati serverul de web Apache2. Creati un nou user in sistem. Adaugati in directorul home al userului creat directorul www si in director fisierul index.html. b)Configurati UserDir pentru a redirectiona cererea http://localhost/ usernou catre acest director.
35. a. Instalati serverul de SSH, porniti-l pe portul 22222 si modificati mesajul din MOTD. b. Filtrati pachetele cu TTL egal cu 4 c. Rejctati conexiunile SSH catre serverul vostru de SSH dar permiteti conexiunile initiate local
36. Interceptati o conexiune telnet, redirectati traficul catre un fisier si afisati pachetele in ASCII
37. Instalati si configurati fail2ban pentru ca la a 4 greseala de parola ip-ul sa fie banat 3 minute si jumatate.
38. Sa se instaleze server-ul de DNS bind9, fiind master pentru domeniul "student.ro". Se va configura acesta pentru a raspunde la comenzile ping catre urmatoarele: a. "student.ro" b. "www.student.ro" c. "mail.student.ro"
39. Construiti o regula iptables prin care sa rejectati cererile ICMP care au ca adresa destinatie o adresa de broadcast.
40. Sa se afle ce calculatoare sunt pornite în reseaua locala.
41. Sa se instaleze un server DNS ca master pentru domeniul student.ro. Acesta va raspunde la cereri pentru urmatoarele: a. student.ro b. www.student.ro c. ftp.student.ro
42. Sa se stabileasca server-ul creat la punctul 3 ca fiind singurul server de nume pentru statia folosita. Apoi sa se afle toate serverele intermediare care se afla pe traseul de la statia curenta pâna la www.google.com.
43. Sa se instaleze server-ul de E-mail postfix, având ca domeniu cel configurat la punctul 4 si modul "Internet Site". Se va trimite un mesaj catre casuta de e-mail test.practic@gmail.com.
44. Sa se instaleze server-ul de IMAP courier-imap si apoi sa se trimita un mesaj de la user-ul "utilizator" catre el însusi folosind clientul de e-mail Thunderbird. Se va folosi protocolul IMAP, iar citirea mesajului se va face tot cu Thunderbird.
45. Sa se instaleze serverul de web "apache2". Se va deschide o fereastră de Firefox, iar la tastarea adresei www.student.ro va trebui sa apara o pagina cu urmatoarele informatii: a. Numele studentului b. Grupa studentului c. Data testului d. Numele asistentului e. Orice altceva
46. Sa se restrictioneze conexiunile catre www.yahoo.com initiate de pe statia locala.
47. Sa se afiseze valoarea TTL a pachetelor primite ca raspuns la un ping catre www.google.com.

48. Scrieti o regula de firewall care sa accepte pachetele echo-request din exterior dar sa limiteze numarul acestor pachete icmp la 1/s, astfel incat sa se permita testarea conectivitatii prin ping dar sa se evite o forma de atac de tip DoS.
49. a) Modificati valoarea TTL de la 64 la 32 pentru pachetele initiate de pe statia locala folosind utilitarul sysctl. Afisati variabila modificata tot cu sysctl. b) Dati ping catre www.yahoo.com si capturati pachetele icmp de tip echo request folosind tcpdump, astfel incat sa se observe modificarea facuta la pasul anterior (sa fie afisat si TTL-ul pachetelor).
50. a) Activati rutarea pe statia locala. Verificare afisand variabila modificata. b) Adaugati o ruta statica cu metrica 5 catre statia 10.20.30.40 folosind ca gateway adresa ip a default gateway-ului curent. Afisarea tabelii de rutare.
Exercitiile 3 si 4 presupun configurarea aceleiasi server DNS.
51. a) Tocmai ati cumparat domeniul test.com si trebuie sa configurati serverul DNS astfel incat sa cuprinda 2 servere de mail cu prioritatile 10 si respectiv 20. b) Interogati serverul DNS de pe statia locala pentru a afla adresele IP ale celor 2 servere de mail.
52. Serverul vostru va fi autoritar si pentru subdomeniul rc.test.com, subdomeniu care va cuprinde si serverul de web www.rc.test.com. Verificati configuratiile facute facand o cerere pentru a afla adresa IP a serverului web.
53. Instalati serverul de mail postfix (configurand ca domeniu pentru care mesajele sunt pastrate local labrc.com) si creati un utilizator virtual in domeniul @retele.com. Creati fisierul cu asocierea corespunzatoare, astfel incat pentru utilizatorul virtual - ionescu@retele.com - mesajele vor fi livrate catre casuta de email test.practic@gmail.com. Testarea se va face trimitand un mesaj de la userul curent (student)@labrc.com catre ionescu@retele.com.
54. Instalati un server de web care sa gazduiasca 2 site-uri: www.studentrc.ro si www.testrc.ro. Configurati serverul web in mod corespunzator si testati prin introducerea celor 2 adrese in browser, paginile afisate trebuind sa fie diferite.
55. Pentru un serverul de web de pe statia voastra: a) Adaugati un alias astfel incat la folosirea URL-ului www.studentrc.ro/home sa se afiseze resursele din /home/student. b) Realizati autentificarea pentru directorul /home/student astfel incat sa se ceara un user si o parola.
56. a) Filtrati pachetele care vin catre statia voastra avand TTL-ul egal cu 10. Verificare cu ping. b) Restrictionati traficul web care pleaca de pe statia locala. Verificare prin browser.
57. Scrieti o regula de firewall care sa accepte pachetele echo-request din exterior dar sa limiteze numarul acestor pachete icmp la 1/s, astfel incat sa se permita testarea conectivitatii prin ping dar sa se evite o forma de atac de tip DoS.
58. a) Folosind utilitarul netstat afisati toate conexiunile tcp in starea listening, afisand si numele programului (PID-ul) si impiedicand rezolutia adreselor IP in nume. b) Folosind nmap scanati localhostul si detectati porturile deschise si sistemul de operare.
59. a) Activati rutarea pe statie b) Adaugati o ruta cu metrica 100 catre 192.168.5.0/24 avand drept gateway unul dintre calculatoarele din laborator. c) Afisati tabela de rutare.
60. Schimbati adresa MAC a uneia dintre interfetele neconectate la retea in adresa 00:AA:AA:AA:AA:AA.
61. a) Care este serverul DNS pe care il interogheaza statia voastra? b) Pe langa serverul DNS pe care il interogheaza statia voastra, adaugati si un alt server, cu adresa ip, adresa voastra. c) Schimbati prioritatea de interogare astfel incat, atunci cand trebuie ca statia voastra sa afle ip-ul corespunzator unui nume, prima data sa fie interogat serverul dns si apoi sa se caute corespondenta in hosts.

62. a) Instalati serverul de email Postfix. Configurati serverul pentru domeniul mail.<numestudent>.ro
b) Trimiteti un mesaj catre casuta test.practic@gmail.com care sa aiba ca subiect "Test practic", expeditor "Popescu", adresa pe care se va raspunde student@cs.pub.ro
63. a) Instalati serverul web Apache2. Schimbati portul pe care acesta asculta in 8080. b) Schimbati directorul in care se vor cauta paginile web in /var/web. Plasati aici o pagina html care sa fie afisata default de browser cand este accesat serverul vostru de web. Pagina va contine un mesaj de intampinare de tipul: "Sunt serverul de web <NumeStudent>.
64. a) Configurati un server de web pentru domeniul <numestudent>.ro b) La accesarea adresei <numestudent>.ro/home/paginaparolata.html faceti astfel incat sa vi se ceara autentificare pentru vizualizarea paginii.
65. a) Instalati ssh si logati-va prin ssh la student pe localhost. b) Opriti conexiunile ssh de la localhost catre orice alta statie.
66. Capturati 10 pachete in hexa care nu sunt web intr-un fisier numit <numelevostru>.txt si care va au pe voi drept destinatie.
67. Pe masina locala avem un server web si un server de mail. Construiti o regula care sa accepte toate conexiunile catre serverul de web si mail dar nimic altceva.
68. Scanati localhost pentru a gasi porturile deschise (instalati un utilitar potrivit in cazul in care e nu este instalat).
69. Afisati in format hexazecimal continutul a 10 pachete din traficul de tip POP3 sau IMAP receptionat de statia locala.
70. Modificati mesajul de intampinare pentru Postfix in "Laugh in the face of danger" .Configurati serverul Postfix sa asculte conexiuni doar pe interfata de loopback.
71. Cresteti cu o unitate valoarea campului TTL din antetul IP pentru pachetele destinate calculatorului pe care lucrati.
72. Aflati care este serverul de nume pentru domeniul k.ro. Aflati adresa IP a unui server de e-mail pentru www.google.com
73. Creati utilizatorul alex. Trimiteti un email de la alex@labrc.cs.pub.ro catre utilizatorul virtual guest@testpractic.com. Mesajul sa ajunga la test.practic@gmail.com
74. Creati utilizatorul mihai. Configurati Apache2 astfel incat statia de lucru sa ofere gazduire site-ului practic.edu in directorul /home/mihai/www. La accesarea site-ului se va cere autentificare de tip htaccess.
75. Presupuneti ca sistemul actioneaza ca un gateway. Interfata de retea este cea de legatura cu Internetul. Presupuneti o interfata imaginara de legatura cu retea locala. Activati rutarea si configurati sistemul astfel incat accesarea portului 8080 din Internet sa duca la accesarea portului 80 al unei statiei 192.168.0.80 presupusa din retea locala.
76. Configurati in mod static nepermanent 2 subinterfete pentru eth0: o subinterfata cu adresa IP 192.168.1.194/24 si una cu adresa IP 192.168.1.66/16. Configurati ca server de nume 192.168.32.21. Activati rutarea intre cele doua retele.
77. Aflati numarul de statii active din retea locala. Identificati serviciile care ruleaza pe statia locala impreuna cu versiunea serviciilor lor.
78. Afisati tabela ARP fara translatarea adreselor IP in nume (afisare numerica). Adaugati o intrare statica in tabela ARP pentru gateway.
79. Afisati in format ASCII continutul a 10 pachete din traficul HTTP sau SSH.

80. Redirectati cererile pentru adresa yahoo.com catre google.ro:

```
# host google.ro
[.]
google.ro has address 72.14.221.104
[.]
# ping yahoo.com
PING yahoo.com (72.14.221.104) 56(84) bytes of data.
64 bytes from yahoo.com (72.14.221.104): icmpseq=1 ttl=241 time=46.2 ms [..]
```

81. Se presupune ca statia la care lucrati are rol de ruter pentru o retea locala conectata pe interfata de retea. Configurati sistemul astfel incat pachetele catre aceasta retea sa nu mai poata trece prin inca un ruter.
82. Configurati o legatura virtuala intre portul 8000 al statiei de lucru si portul 80 al statiei atlantis.cs.pub.ro. Astfel, prin conectarea la portul 8000 local, utilizatorul poate accesa serviciile web ale statiei atlantis.cs.pub.ro.
83. Creati utilizatorul alex. Creati directorul /home/alex/mysite. In acest director se vor afla 3 subdirectoare: a/, b/, c/. Accesarea adresei www.test.com trebuie afiseze structura directorului. Cand se va incerca accesarea subdirectorului c/ trebuie sa se afiseze mesajul de acces interzis.
84. Aflati care este serverul de mail pentru domeniul k.ro
85. Configurati in mod static permanent adresa 192.168.0.234/24 pe interfata de retea. Configurati 192.168.0.1 ca gateway al sistemului.
86. Configurati pe sistemul local bind9. Serverul DNS va fi autoritar pe domeniul pets.ro si va delega subdomeniul cats.pets.ro serverului 11.12.13.14 si dogs.pets.ro serverului 12.13.14.15.
87. Aflati adresele hardware ale statiilor active din retea locala.
88. Adaugati utilizatorul local alex. Configurati sistemul astfel incat mesajele trimise utilizatorului alex sa ajunga la test.practic@gmail.com
89. Pe ce interfata aveti legatura activa? Configurati doua subinterfete pentru aceasta interfata in mod permanent. Interfata fizica va fi configurata prin DHCP iar subinterfetele vor fi configurate static: 192.168.0.1/24, respectiv 10.1.1.2/16. Va fi adaugata o ruta catre retea 172.16.0.0/16 cu next-hop-ul 10.1.1.1.
90. Adaugati in sistem utilizatorul ioana. Configurati serverul Apache2 astfel incat folosirea URL-ului http://www.mysite.com/homeioana/ sa afiseze continutul directorului /home/ioana/www
91. Configurati serverul SSH sa asculte conexiuni doar pe interfata de Internet pe portul 2222. Dezactivati posibilitatea de conectare a utilizatorului root prin SSH.
92. Configurati Postfix astfel incat sa poata fi transmise mesajele catre atlantis.cs.pub.ro daca se face conectarea pe interfata de Internet. Hint: Nu trebuie sa apara mesajul "Relay access denied".
93. Configurati bind9 pentru a raspunde la cereri pentru zona debian.info astfel:
- (a) ns.debian.info are adresa 9.10.11.12
 - (b) debian.info este alias la ns.debian.info
 - (c) www.debian.info are adresa 11.22.33.44
 - (d) mail.debian.info este serverul de mail cu prioritatea 10⁰ este alias pentru www.debian.info

94. Filtrati traficul ICMP venit din reseaua locala spre statia locala mai putin cel de la statia x.y.z.33 (x.y.z.0 este adresa retelei)
95. Activati rutarea si configurati tabela nat astfel incat statiile din reseaua privata 192.168.0.0/24 sa se poata conecta la Internet prin intermediul interfetei de Internet. Precizare: Reteaua 192.168.0.0/24 este fictiva dar se presupune ca exista.
96. Folositi tcpdump pentru a captura 10 pachete de tip ICMP echo-reply destinate statiei locale. Afisati antetul de nivel 2. Afisati informatiile in format hexa si ASCII.
97. Configurati sistemul local astfel incat rularea comenzii ping test.com sa rezulte in testarea conectivitatii adresei IP a interfetei de Internet a sistemului local.
98. Folositi nmap pentru a obtine lista de statii active din reseaua locala. Obtineti rezultatul intr-un fisier in format care poate fi usor prelucrat folosind grep.
99. Configurati in mod permanent interfetele eth0 si eth1 cu adresele respectiv 192.168.0.1/24 si 10.1.1.2/16. Adaugati o ruta implicita catre 10.1.1.1 si o ruta catre reseaua 172.16.0.0/16 care sa aiba ca next-hop 192.168.0.2. Dupa configurarea fiecărei interfete se va afisa mesajul "Interfata eth0/1 a fost pornita"
100. Configurati Apache2 astfel incat folosirea URL-ului http://www.megasite.com/php-redirect/ sa faca redirectarea catre http://www.megasite.com/. In momentul accesarii URL-ului se va afisa o pagina informativa PHP. Pentru afisarea unei astfel de pagini fisierul PHP trebuie sa aiba continutul: <?php phpinfo (); ?>. Aveti nevoie de suport PHP.
101. Creati utilizatorul bianca. Rulati comanda xclock prin conectare SSH pe contul bianca. Comanda are ca efect afisarea unui ceas.
102. Creati utilizatorii dana si eugen. Configurati sistemul si serverul Postfix astfel incat mesajele catre andreea@test.com sa ajunga la utilizatorii locali dana si eugen.
103. Configurati bind9 sa asculte conexiuni doar pe interfata de Internet pe portul 5353.
104. Filtrati traficul DNS de tip UDP pe care sistemul il ruteaza catre statia x.y.z.33 din reseaua locala (x.y.z.0 este adresa retelei). Afisati tabela de filtrare cu precizarea indexului fiecărei reguli in tabela.
105. Se presupune ca sistemul local este un gateway avand in spate un LAN cu adresa 192.168.0.0/24. Activati rutarea si configurati tabela nat astfel incat sa se poata accesa serviciul SSH al statiei 192.168.0.1 prin intermediul portului 2222 al sistemului local (interfata de Internet).
106. Folositi nmap pentru a obtine lista de statii active din reseaua locala. Obtineti rezultatul intr-un fisier in format care poate fi usor prelucrat folosind grep.
107. Scrieti urmatoarele linii in fisierul myethers.txt:
 - (a) 141.85.37.1 ab:cd:de:00:01:02
 - (b) 141.85.37.2 ab:cd:de:00:01:03

Carei tabele ii pot fi asociate intrarile din fisier? Folositi acest fisier pentru a adauga intrari statice in tabela corespunzatoare.
108. Folositi tcpdump pentru a captura 3 pachete DNS de tip UDP catre statia ns.cs.pub.ro. Afisati informatii complete despre pachete (date, antet de nivel 2) in format hexa si ASCII.
109. Pe ce interfata aveti link? Configurati doua subinterfețe pentru interfata la care aveti link. Prima subinterfata va avea adresa 192.168.0.1/24, cea de-a doua 10.1.1.2/16. Configurati interfata fizica cu adresa 172.16.15.19/16 si adresa hardware 1a:2b:3c:4d:5e:6f. Adaugati o ruta implicita care sa aiba ca gateway 172.16.15.20.

110. Adaugati in sistem utilizatorul ioana. Configurati Apache2 astfel incat:
 - (a) folosirea URL-ului `http://www.vhost1.com` sa afiseze continutul directorului `/home/ioana/www`
 - (b) folosirea URL-ului `http://www.vhost2.com/ioana` sa afiseze continutul aceluiasi director (`/home/ioana/www`)
111. Creati un tunel HTTP peste SSH: portul 8888 local va realiza o conexiune prin tunel la portul 80 al `atlantis.cs.pub.ro`
112. Configurati Postfix astfel încât să asculte conexiuni pe portul 2525. De asemenea, serverul nu trebuie să furnizeze informații despre versiunea sa în momentul conectării (de exemplu atunci când se folosește telnet)
113. Configurați bind9 pentru a răspunde la cereri inverse pentru rețeaua 1.2.3.0/24 astfel:
 - (a) serverul de nume este `ns.debian.info` serverul de mail este `mail.debian.info` cu prioritatea
 - (b) 1.2.3.4 este adresa IP pentru `ns.debian.info`
 - (c) 1.2.3.5 este adresa IP pentru `ftp.debian.info`
 - (d) 1.2.3.6 este adresa IP pentru `www.debian.info`
114. Filtrați pachetele de inițiere de conexiune de la stația x.y.z.33 mai puțin cele de inițiere de conexiune pentru SSH. De asemenea, permiteți orice fel de formă de trafic HTTP (indiferent dacă este sau nu de inițiere de conexiune)
115. Folosiți tabela mangle pentru a incrementa valoarea TTL pentru pachetele care sunt rutate de sistemul local. Afișați tabela mangle cu precizarea indexului fiecărei reguli în tabelă.
116. Folosiți nmap pentru a afla versiunea sistemului de operare și a serviciilor care ascultă pe porturi mai mici de 1024 pentru `atlantis.cs.pub.ro`. Obțineți rezultatul într-un fișier format XML.
117. Configurati serverul SSH sa asculte conexiuni pe portul 12345. Configurati fail2ban pentru acest server pentru a filtra cererile de conexiuni aparute dupa 5 incercari nereusite timp de 5 minute.
118. Afișați conexiunile TCP și UDP ale sistemului local. Afișați numele de stații în format numeric (nu și porturile - să apară ssh și http în loc de 22, respectiv 80).
119. Sa se configureze 2 subinterfete ale interfeței active. Pe o subinterfața se va configura adresa 192.168.10.20/24. Pe cealaltă 192.168.20.10/24. Sa se configureze sistemul astfel incat sa permita rutarea de pachete intre cele 2 rețele.
120. Sa se adauge o ruta statica catre rețeaua 63.54.0.0/16 avand gateway 192.168.106.2 cu metrica 20.
121. Sa se monitorizeze traficul TCP care are ca port destinatie portul 2100. Deschideti un server TCP pe portul 2100. Sa se genereze trafic TCP pe portul 2100
122. Sa se configureze sistemul local astfel incat sa accepte conexiuni SSH pe portul 22106. Creati utilizatorii locali andreea si cristi. Sa se realizeze o conexiune SSH de pe utilizatorul andreea pe utilizatorul cristi de pe sistemul local fara sa se solicite parola.
123. Sa se configureze sistemul local astfel incat sa gazduiasca 2 site-uri web in acelasi timp: `www.rc.com` - continutul site-ului se gaseste in `/var/www/rc`; folosirea URL-ului `http://www.rc.com` va duce la afisarea mesajului "Hello, World" `www.pub.ro` - continutul site-ului se gaseste in `/var/www/pub`; folosirea URL-ului `http://www.pub.ro` va duce la afisarea mesajului "Goodbye, World"

124. Configurati bind9 pe sistemul local astfel incat, in urma unei interogari, adresa 10.38.4.4 sa corespunda numelui ftp.microsoft.com
125. Sa se trimita un mesaj catre utilizatorul local alina de la test@rc.com folosind directive SMTP. Sa se configureze Postfix astfel incat sa permita trimiterea de mesaje doar catre domeniul gmail.com indiferent de adresa IP calculatorului care a initiat mesajul.
126. Activati rutarea. Sa se modifice campul TTL al pachetelor rutate de catre masina locala cu valoarea 2.
127. Sa se determine ce sistem de operare foloseste sistemul atlantis.cs.pub.ro
128. Sa se filtreze pachetele de initiere de conexiune catre sistemul local cu exceptia traficului SSH. Precizare: Vor fi lasate sa treaca toate pachetele care reprezinta raspunsuri la conexiuni initiate de pe sistemul local
129. –
 - (a) Sa se asocieze unei subinterfete a interfetei active adresa 192.168.83.110/24 (1/3)
 - (b) Sa se adauge o ruta implicita avand ca gateway 192.168.83.4 (1/3)
 - (c) Sa se stabileasca ca server DNS 192.168.83.3 (1/3)
130. –
 - (a) Sa se instaleze un server SSH (1/5)
 - (b) Sa se adauge utilizatorul radu.
 - (c) Sa se creeze in directorul home al lui radu directorul rsubdir.
 - (d) Sa se creeze in home-ul utilizatorului student ierarhia: testdir/ file1.txt file2.txt file3.txt
* Folositi scp pentru a copia ierarhia testdir in directorul rsubdir din directorul home al lui radu.
131. Sa se monitorizeze primele 10 pachete destinate unei statii din retea 141.85.37.0/24. Sa se genereze trafic catre acea statie.
132. Sa se precizeze 2 adrese IP ale serverelor de nume autoritare pentru gmail.com
133. Sa se configureze Apache2 astfel incat URL-ul http://localhost:12345/ testrc/ sa acceseze fisierul /home/testrc/index.php. Directorul /home/testrc contine fisierele index.html si index.php.
134. Adaugati in sistem utilizatorii omar, stefan si elena. Configurati Postfix astfel incat sa obtinem o "lista de discutii" lista@localhost. Orice mesaj trimis catre lista@localhost ajunge in casutele postale ale utilizatorilor omar, stefan si elena.
135. Sa se configureze serverul Postfix astfel incat sa permita oricarei statii din retea 10.120.80.0/24 sa foloseasca serverul local pentru a trimite mesaje.
136. Sa se configureze si sa se testeze serverul bind9 pe sistemul local. Serverul este autoritar pentru cs.pub.ro. La cereri pentru adresa rc.cs.pub.ro serverul va raspunde cu adresa 192.168.20.1
137. Presupunand ca se face NAT (inside - 192.168.4.0/24) sa se aplice o regula prin care traficul destinat sistemului local pe portul 80 va fi redirectat catre 192.168.4.2 pe portul 8080.
138. Aflati serviciile care ruleaza pe porturile TCP 22, 25, 53, 80 si pe porturile UDP intre 100 si 200 ale sistemului local.

139. Configurati adresa IP 192.168.0.34/24 pe interfata eth0 si 10.10.0.45/24 pe interfata eth1. Configurati gateway-ul 192.168.0.1. Configuratiile trebuie sa fie permanente. Configurati adresa 172.16.0.56/24 pe subinterfata 1 a lui eth0 in mod nepermanent (temporar). Activati rutarea.
140. Adaugati o intrare permanenta in tabela ARP care sa asocieze adresa MAC 00:15:F2:85:1E:24 cu IP-ul 192.168.106.5. Dupa adaugare listati tabela ARP si apoi stergeti inregistrarea adaugata.
141. Configurati serverul de DNS pentru a raspunde la cererile pentru domeniul testrc.ro. Serverul de nume este ns.testrc.ro, serverele de email mail.testrc.ro, mailrc.testrc.ro cu prioritatile 5, respectiv 10. Adresa de email a administratorului este admin@testrc.ro si exista urmatoarele asocieri host <-> IP: testrc.ro <-> 192.168.0.1 ns.testrc.ro <-> 192.168.0.2 mail.testrc.ro <-> 192.168.0.3 mailrc.testrc.ro <-> 192.168.0.4 www.testrc.ro este un alias la mail.testrc.ro
142. Configurati serverul de email Postfix pentru a permite trimiterea de email-uri de la orice calculator din reseaua locala (192.168.106.0/24) catre orice domeniu. Testati configuratia facuta prin conectarea pe adresa setata la punctul 1 si trimitand un mesaj email la adresa: test.practic@gmail.com
143. Sa se schimbe portul pe care ruleaza serverul Apache2 in 8000. Adaugati utilizatorii liviu si stefan. Configurati Apache2 astfel incat o accesare a adresei http://localhost/liviu sa serveasca documentele din directorul /home/liviu/webdocs/. Pentru utilizatorul stefan dezactivati aceasta facilitate.
144. Sa se filtreze toate pachetele primite de statia voastra astfel incat sa nu se poata realiza conexiuni la serverul de web, iar la cel de SSH sa se poata realiza conexiuni doar de la IP-ul 192.168.106.1. Sa se modifice valoarea TTL a tuturor pachetelor care pleaca de la calculatorul vostru la valoarea 128.
145. Monitorizati toate pachetele care vin catre statie, pe portul 25, de la statia cu adresa MAC 00:E0:4C:F8:25:A5
146. Configurati serverul de SSH astfel incat sa se permita conectarea pe user-ul student folosind autentificare prin chei publice, fara a se cere parola user-ului ci passphrase-ul cu care a fost generata pereche cheie publica/cheie privata. Conectarea pe SSH se va realiza pe portul 220.
147. Sa se scaneze reseaua 192.168.0.0/24 pentru a determina calculatoarele active si serviciile rulate pe acestea.
148. Activati translatarea de adrese astfel incat statiile din reseaua 172.16.0.0/16 sa poata accesa Internet-ul prin intermediul interfetei eth2. Se presupune ca interfata eth2 are un IP preluat automat prin DHCP. Sa se faca un port forwarding astfel incat un serviciu de telnet care ruleaza intern pe statia cu IP-ul 172.16.35.178 sa fie disponibil din exteriorul retelei pe portul 5000.
149. Sa se configureze o interfata virtuala cu adresa 172.16.89.37/29 si adresa de broadcast corespunzatoare. Configurarea nu este permanenta.
150. Afisati doar pachetele prin care se initiaza si se termina o conexiune TCP.
151. Configurati serverul Web astfel incat prin accesarea sitului www.exemplu1.com sa primiti un mesaj de intampinare, iar prin accesarea sitului www.exemplu2.com/test.php sa afisati fisierul test.php. Pentru www.exemplu1.com directorul radacina va fi /home/user1/www iar pentru www.exemplu2.com este cel implicit. Serverul Web va asculta pe toate adresele IP active si pe portul implicit.

152. Configurati Postfix astfel incat un mesaj trimis catre alias@localhost sa fie trimis catre user1@prc.ro, user2@rc.ro si test.practic@gmail.com. Dupa transmitere, mesajul se va afla in casutele postale ale utilizatorilor locali user1 si user2.
153. a. Configurati serverul de DNS pentru a raspunde la cereri pentru domeniul test.ro. Serverul de nume asociat domeniului este ns.test.ro, serverele de mail asociate domeniului sunt mail1.test.ro avand prioritatea de 3 si mail2.test.ro avand prioritatea 4, iar adresa administratorului este admin@test.ro. Serverul de nume are adresa 192.168.1.2, serverul mail1 are adresa 192.168.1.3 iar serverul mail2 are adresa 192.168.1.4, mail1.test.ro este alias pentru testmail.test.ro. b. Deoarece baza de date a serverului DNS este modificata foarte des (o data la 2 zile), sa se evite lipsa unei convergente scazute pentru domeniile accesate.
154. Aflati informatii statistice despre traficul TCP si UDP.
155. Afisati in ASCII primele 40 de pachete dintr-o conexiune Web initiata catre statia voastra pe interfata eth0, numai de la adresa IP 192.168.1.1.
156. Determinati ce protocoale IP sunt filtrate pe statia voastra.
157. Limitati numarul de conexiuni SSH simultane catre statia voastra la 5.
158. Modificati valoare campului TTL pentru pachetele initiate de pe statia voastra.
159. a) Sa se configureze temporar pe interfara conectata la retea o subinterfata. Asignati subinterfetei o adresa IP din reseaua 172.16.0.0/16. b) Dati un ping catre www.yahoo.com, folosind subinterfata creata si setati numarul de pachete trimise la 4.
160. a) Listati programele de pe statia locala care accepta conexiuni din retea. b) Listati conexiunile initiate de/catre statia voastra.
161. Setati valoare implicita pentru TTL la numarul de hop-uri prin care trece un pachet ca sa ajunga la unul din serverele ce gazduieste www.google.ro
162. Rezolvati numele de domeniu www.iowa.gov folosind cereri nerecursive. Se va porni cu o interogare catre cs.pub.ro
163. Configurati bind9 astfel incat sa raspunda la cereri pentru domeniul test.net. Exista urmatoarele asocieri: ns.test.net va fi serverul master asociat domeniului ns2.test.net va fi serverul slave asociat domeniului mail.test.net va fi serverul de mail cu prioritatea 15 admin@test.net va fi adresa administratorului de sistem test.net are adresa 192.168.0.1 master.test.net are adresa 192.168.0.1 slave.test.net are adresa 192.168.0.2 ns.test.net este alias pentru master.test.net ns2.test.net este alias pentru slave.test.net
164. Configurati Postfix astfel incat toate mesajele catre admin@test.rc sa fie stocate local in /var/mail/inbox/admin. Se mai precizeaza ca pe statia locala nu exista utilizatorul admin.
165. Sa se adauge utilizatorul user1. Sa se creeze fisierul /home/user1/apachepages/first.txt (Prima linie a fisierului trebuie sa contina numele vostru si grupa) Instalati si configurati serverul de apache2 astfel incat la scrierea in browser a adresei: http://localhost/user1 sa fie afisat continutul fisierului first.txt.
166. Adaugati o regula astfel incat toate pachetele care sunt destinate statiei locale sa fie scrise in log.
167. Adaugati o regula care redirectioneaza toate pachetele destinate statiei locale, avand portul destinatie 80, catre portul 8080.
168. Sa se afiseze valoarea TTL a pachetelor primite ca raspuns la un ping catre "www.google.com".

169. a) Obtineti configuratia de retea in mod dinamic, b) dupa care introduceti datele respective in mod static si permanent.
170. a) Adaugati o ruta statica in tabela de rutare catre 87.248.113.14 prin default gateway, b) Stergeti ruta default. Testati functionalitatea rutei catre 87.248.113.14. c) In final, reveniti la configuratia initiala.
171. Instalati serverul DNS. Adaugati o zona inversa pentru care serverul este autoritar, in care IP-ul 1.2.3.4 sa aiba asociat numele "examen.ro". Sa se asigure timpi de convergenta scazuti. Testati functionarea.
172. Instalati Postfix (domeniul: "test.cs.pub.ro"). Configurati casuta de posta virtuala "examen@laborator.com". Pentru testare, trimiteti un mail de la "student" catre "examen@laborator.com", si verificati daca acesta a ajuns la destinatie.
173. Instalati Apache2. Configurati UserDir pentru a redirectiona "http://localhost/student" catre un director creat in directorul home al user-ului "student". Afisati continutul directorului in browser.
174. Creati in Apache2 un alias pentru directorul local "/usr/docs" cu numele "/documente". Creati 3 fisiere in "/usr/docs". Testati in browser.
175. a) Creati un utilizator cu numele vostru. b) Copiati prin SSH un fisier nou creat din home-ul user-ului "student" in home-ul utilizatorului nou creat.
176. Creati cu iptables un filtru care sa respinga (cu trimiterea unui mesaj ICMP inapoi catre sursa) conexiunile SSH initiate de catre localhost. Testati.
177. Adaugati o regula in iptables care sa faca drop pe toate pachetele destinate statiei pe portul 2222 cu exceptia pachetelor primite de la localhost. Testati.
178. a) Configurati statia locala sa ruteze traficul dintr-o retea locala. In retea locala aveti un server de web si unul de mail. Forwardati traficul de web si de mail catre aceste statii care au IP-urile 192.168.1.2 si respectiv 192.168.1.3. b) Realizati translatarea adreselor private din retea 192.168.1.0/24 la adresa publica a statiei voastre. c) Stergeti toate regulile din tabela filter.
179. a) Obtineti configuratia de retea in mod dinamic, b) dupa care introduceti datele respective in mod static si temporar.
180. a) Instalati un utilitar de captura de pachete. b) Stergeti tabela ARP. c) Afisati continutul mesajelor ARP Request si ARP Reply generate pentru aflarea MAC-ului gateway-ului. d) Afisati apoi rezultatul din tabela ARP.
181. Instalati serverul DNS. Faceti-l autoritar pentru zona "ro". Specificati doua servere de mail de prioritati diferite pentru respectiva zona: "mail1.ro" si "mail2.ro", care sa fie aliasuri pentru "calculator1.ro" si "calculator2.ro" (doua statii cu IP-uri oarecare). Interogati serverul DNS pentru a afla IP-urile finale ale serverelor de mail asociate zonei "ro".
182. Aflati IP-ul unui server de nume al domeniului "google.com", si creati o zona inversa care sa realizeze o corespondenta intre acel IP si numele "interzis.ro". Interogati serverul DNS local pentru testare.
183. Instalati Postfix (domeniul: "test.cs.pub.ro"). Creati un utilizator virtual "examen@lab.com" corespunzator contului de sistem "student". Testati prin transmiterea unui email catre examen@lab.com si verificati ajungerea acestuia la destinatie.
184. Instalati Apache2. Creati o gazda virtuala "www.examen.ro" pe portul 8080, avand in pagina principala mesajul: "Subiect 6". Testati in browser.

185. Schimbati numele index-ului implicit din "index.html" in "examen.html". Testati pe un site existent sau nou creat.
186. Instalati serverul SSH si modificati portul pe care acesta ruleaza in 3500. Creati un utilizator cu numele "examen" si conectati-va la el prin SSH de pe contul "student".
187. Creati un filtru care sa nu permita traficul Web catre "www.gsp.ro" de pe statia locala, iar in rest sa permita orice trafic.
188. Determinati ce statii din retea din care faceti parte sunt active. nmap va fi rulat in modul "Aggressive".
189. –
- Configurati Apache2 astfel incat sa serveasca cereri HTTPS pe portul 80 si HTTP pe 443.
 - Vor trebui sa aiba sens folosirea URL-urilor <https://www.secure.net:80>, respectiv <http://www.secure.net:443>
 - In momentul accesarii oricareia din URL-urile de mai sus se va afisa o pagina cu mesajul "Apache on-line".
190. –
- Configurati Apache2 astfel incat folosirea URL-ului <http://www.storage.org/> sa afiseze continutul directorului /var/www/archives continand trei fisiere: arc1.tar.gz, arc2.zip si arc3.rar.
 - Configurati Apache2 astfel incat icoana asociata arhivei rar sa fie aceeaasi ca si pentru arhivele tar.gz si zip.
191. –
- Configurati Apache2 astfel incat folosirea URL-ului <http://www.op-cwal.net> sa afiseze mesaj de tip forbidden.
 - Cu toate acestea, folosirea URL-ului <http://www.op-cwal.net/index.html> va conduce la afisarea unei pagini continand mesajul "Teleport successful"
192. –
- Configurati Apache2 astfel incat sa asculte conexiuni pe portul 8080 pe interfata de loopback si pe portul 8000 pe interfata de Internet (doar atat).
 - In plus, din considerente de securitate, dupa primirea unei cereri serverul trebuie sa trimita informatii minimale: nu se vor trimite informatii precum versiunea serverului, tipul de sistem de operare, modulele folosite, etc.
193. –
- Creati utilizatorul mircea.
 - Configurati sistemul astfel utilizatorul student sa se poata conecta prin SSH la utilizatorul mircea fara parola.
194. Folositi iptables pentru a configura sistemul local astfel incat:
- sistemul local poate folosi ping pentru a testa conectivitatea unei alte statii
 - o alta statie nu poate folosi ping pentru a testa conectivitatea sistemului local
195. Filtrati cererile de conectare HTTP de la statia x.y.z.33 din retea locala catre statia locala (x.y.z.0 este adresa retelei).

196. Afisati continutul a trei tabele importante din sistem cu dezactivarea rezolvarii adreselor in nume (afisare numerica).
197. Instalati si configurati serverul de nume BIND9 sa raspunda la cererile pentru zona tester.ro, zona aflata la adresa fizica a sistemului dumneavoastra si care zona sa aiba o zona de tip NS (ns.teste.ro), una MX (mail.teste.ro), aflata la adresa IP 192.168.0.101 si una FTP (ftp.teste.ro) aflata la adresa 192.168.0.102. NS-ul are aceeaasi adresa IP cu cea fizica a masinii la care lucrati. (Adresa fizica = adresa interfetei de retea active)
198. Instalati si configurati Postfix astfel incat domeniile locale sa fie mail.teste.ro si domeniile catre care accepta mesaje pentru a fi livrate catre orice destinatie sa fie 192.168.0.0/16.
199. Configurati Postfix astfel incat sa aiba ca domeniu virtual test.com, astfel ca adresele user1@test.com si user2@test.com sa fie destinatie finala, iar adresele fizice la care ajung mesajele sa fie user-ul student, respectiv adresa dumneavoastra de email.
200. Instalati si configurati Apache2 cu domeniile virtuale www.teste.ro si www.rclab.ro, care sa fie asignate adresei 127.0.0.1.
201. Scanati serverul dumneavoastra folosind utilitarul nmap, afisand informatii detaliate despre serviciile care ruleaza pe fiecare port gasit deschis si informatii detaliate despre sistem.
202. Configurati iptables-ul astfel incat statia dumneavoastra sa accepte conexiuni pe portul 80 doar din reseaua 192.168.0.0/16 si pe portul 53 doar de la adresa fizica a masinii.