Mr Vladimir Stanojević*
Visoka tehnološka škola strukovnih studija Šabac,
Republika Srbija
Dr Mladen Veinović
Univerzitet Singidunum Beograd,
Republika Srbija

UDK 004.7
Stručni članak
Primljen: 14. IX 2014.

ADMINISTRIRANJE I ZAŠTITA LAN MREŽE OBRAZOVNE INSTITUCIJE MULTIFUNKCIONALNIM LINUX BOX-om

SAŽETAK: Bezbednost računarskih sistema i mreža je kompleksna oblast, koja obuhvata raznoraznu opremu i softverske alate. Najčešće ali ne i jedino korišćeni u te svrhe jesu ruteri, firewall-ovi i proxy serveri. Prikazana je objedinjena implementacija tih alata, na računaru koji radi na linux kernelu, a sve instalirano samo sa jednom namenom, a to je ispunjavanje zadatih bezbedonosnih standarda računarskih resursa i mreže.

KLJUČNE REČI: bezbednost računarskih mreža i sistema, Ruter, Firewall, Proxy, Linux.

Uvod

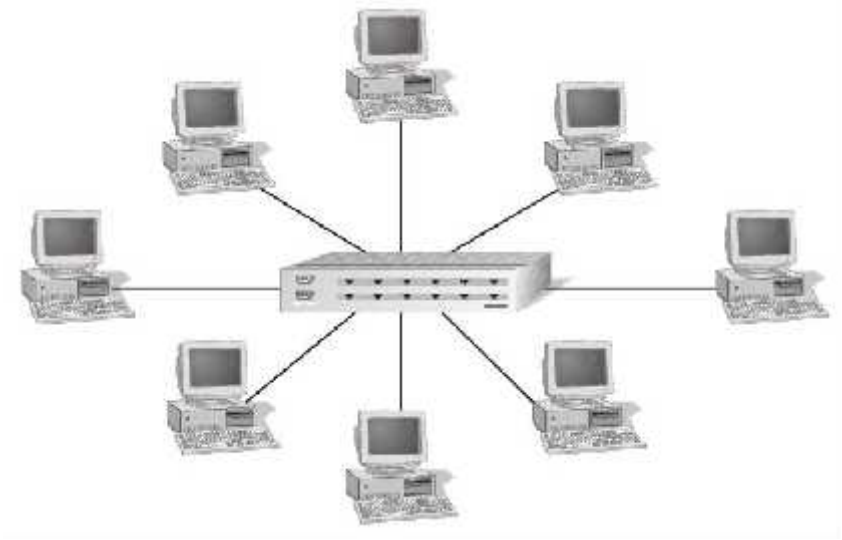
U ovom radu je obrađena problematika administriranja i zaštite LAN mreža na više nivoa, kao i korišćenjem skupa više alata. Sve to je implementirano objedinjeno na Linux kernelu. Polazna premisa je da je, u savremenim organizacijama i institucijama, elektronska obrada podataka, kao i njihovo distribuiranje kako u lokalnom nivou tako i preko interneta sve zastupljenije, pa samim tim i potreba za što efikasnijim administriranjem tih mreža, kao i zaštitom samih računarskih sistema i podataka sve veća. Prikazano je jedno rešenje koje objedinjuje više standardnih alata i tehnika u jednu kompleksnu funkcionalnu implementaciju bazirano na Linux kernel-u.

1. Lan mreža

1.1. Pojam i topologija Lan mreža

LAN mreža po definiciji podrazumeva neku grupu kompjutera koji se nalaze u blizini (u istoj zgradi, firmi i sl.) koji su međusobno umreženi. LAN se može povezati preko istih ili drugih mrežnih medijuma sa drugim LAN-ovima ili sa Internetom. Moderne LAN mreže uglavnom imaju topologiju „zvezde”, kao što je prikazano na slici 1.

*vlstanojevic@digipro.rs



Slika 1. Topologija „zvezde“ LAN mreže.

1.2. Problematika administriranja Lan mreža

Dakle, svi resursi koji su povezani u LAN su ravnopravno dostupni svim članovima LAN-a. Ovo je veoma pogodno za neke potrebe, ali je i uzrok potencijalnih problema kao što su:

- Ograničavanje ili potpuno sprečavanje prava pristupa određenim resursima pojedinim članovima LAN-a;
- Ograničavanje ili onemogućavanje prava pristupa internet sadržajima pojedinim ili svim članovima LAN-a;
- Ograničavanje ili onemogućavanje pristupa lokalnim resursima sa interneta.

Za postizanje ovih ciljeva koristi se raznovrsna hardverska oprema kao i softverski alati. Na tržištu već postoji veliki izbor uređaja koji izvršavaju pojedine od ovih funkcija, ali ne i uređaji koji omogućavaju dovoljno fleksibilno setovanje više objedinjenih funkcija. Npr. dosupni su raznovrsni router ili firewall uređaji, čak i proxy serveri, ali ne i u objedinjenom funkcionalnom obliku.

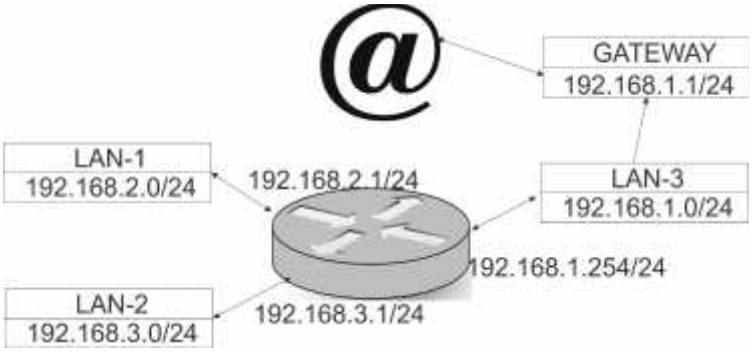
2. Objedinjena implementacija

Sve gore navedene funkcije se mogu objediniti korišćenjem običnog PC računara. Od dodatne opreme je jedino potrebno da isti poseduje više ethernet adaptera, konkretno n+1, gde je n=broj „podmreža“ u LAN-u. Na isti se instalira Linux kernel i odgovarajući softverski paketi, budući da su svi oni open-source i legalno dostupni, a u dugogodišnoj praksi dokazani kao pouzdani i stabilni. U konkretnoj implementaciji korišćena je Ubuntu[1] serverska distribucija konkretno verzija 14.04 koja je aktuelna u vreme pisanja ovog rada. Po instalaciji samog servera, pristupa se konfiguraciji mreže.

Za konkretni primer uzeto je da se LAN mreža sastoji od 2 podmreže internih korisnika, i da postoji internet konekcija koja je logički povezana na treću podmrežu. Internet ruter je od internet provajdera i njegova IP adresa je 192.168.1.1. Pošto je potrebno pratiti i ograničiti

[1] http://www.ubuntu.com

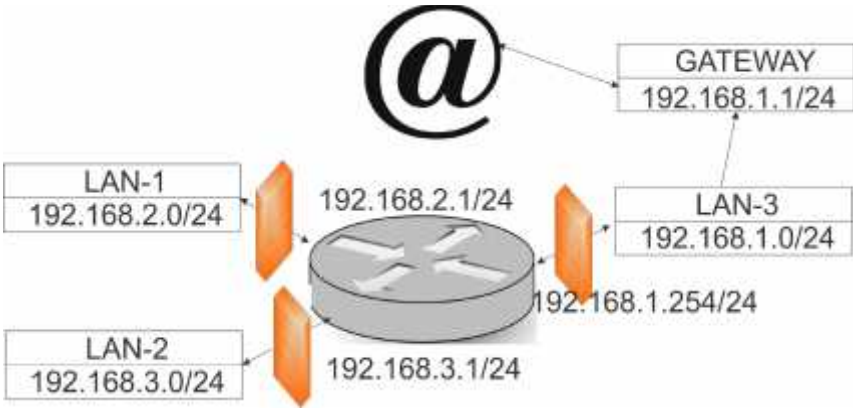
pristup neželjenim internet sadržajima, neophodno je da se taj ruter (u ovom slučaju gateway) prema internetu „izoluje“ od direktnog pristupa korisnika sa LAN-a. On dakle neće biti „član“ ni jedne od podmreža, već će pripadati trećoj podmreži, a međusobni saobraćaj između podmreža će se „rutirati“ na PC računaru koji će biti označen kao „box“ i tako nazivan u daljem tekstu. Dalje, zbog fleksibilnosti administriranja LAN mreže sa većim brojem računara koji rade kao radne stanice, obe „korisničke podmreže“ će biti konfigurisane korišćenjem DHCP servera koji će takođe biti implementiran na box-u.



Slika 2. Topologija LAN mreže sa implementiranim Box-om u funkciji rutera.

Konkretno setovanje mrežnih interfejsa i DHCP servera box-a je dato u prilogu 1. ovoga rada.

Osim funkcije rutera, box dakle vrši i funkciju DHCP servera i to za dve podmreže (192.168.2.0/24 i 192.168.3.0-24) kao što je prikazano na slici 2.



Slika 3. Box sa funkcijom firewall-a

Na slici 3 jasno je naznačeno da u okviru box-a funkcionišu 3 nezavisna (u smislu setovanja) firewall-a. Na taj način se postiže (ali ne samo to):

- Da računari iz podmreže LAN-1 ne mogu pristupati računarima/resursima iz podmreže LAN-2 i obrnuto;
- Da računari iz podmreža LAN-1 i LAN-2 mogu po nezavisno definisanim pravilima pristupati selektivno podmreži LAN-3 pa samim tim i/ili internetu;
- Da se računarski resursi obe podmreže LAN-1 i LAN-2 mogu zaštititi od neželjenog/neovlašćenog pristupa sa Interneta;

- Da se na samom box-u ili u okviru podmreža LAN-1 i/ili LAN-2 mogu hostovati određeni resursi/ servisi dostupni autorizovanim korisnicima sa interneta na strogo definisan način u željenom obimu.

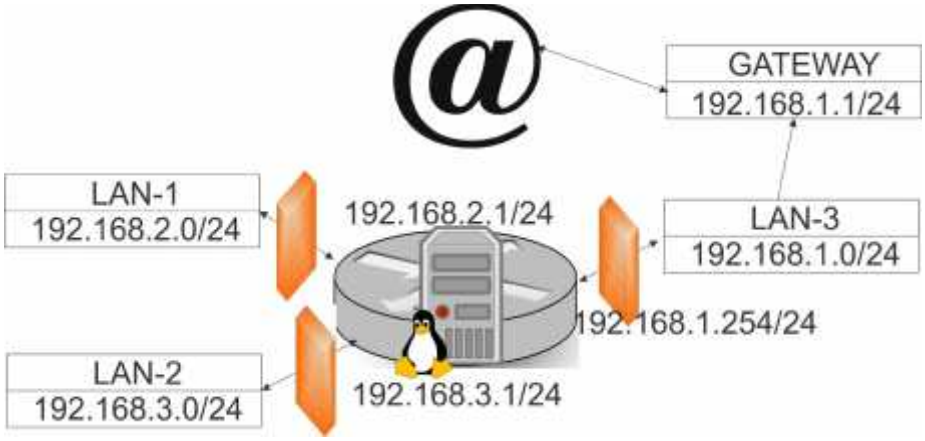
Konkretno setovanje firewall-a box-a je dato u prilogu 2. ovoga rada.

Osim ovih funkcija, na istom box-u moguće je implementirati i proxy server. Njegova funkcija je:

- Da „kešira“ internet sadržaje i da ih pruža kao odgovor na zahteve iz LAN-a, a da pritom ne prenosi podatke tj. sadržaje koje već ima u svom kešu sve dok su isti aktuelni, neograničen broj puta za neograničen broj korisnika. Uštede u performansama i rasterećenju internet linka su značajne.
- Da ograničava/onemogućava pristup određenim internet sadržajima, bazirano na pravilima tipa „po korsiniku“ i/ili „po sadržaju“.

U konkretnoj implementaciji prikazan je SQUID Proxy server verzija 3.1 aktuelna u vreme pisanja ovoga rada.

Na sledecćoj slici je prikazana konačna implementacija „all-in-one“ „box“-a koja objedinjuje sve funkcionalne module.



Slika 4. Blok shema multifunkcionale implementacije Linux box-a.

3. Spoljašnji rizici i pretnje

Osim razgraničenja pristupa pojedinim kategorijama korisnika/ računara unutar LAN mreže, sistem administratoru je potrebno da identifikuje potencijalne rizike i pretnje po bezbednost mreže, i da se preventivno zaštiti od njih. U zavisnosti od vrste servisa koji su aktivni unutar LAN mreže (deljeni folderi/dokumenti, printeri, proxy, ftp, email serveri itd), potrebno je zaštiti te resurse od neovlašćene upotrebe spolja.

Ako se posmatraju bezbednosni rizici vezani za email server, izuzevši očigledne rizike neovlašćenog čitanja elektronske pošte, od čega se svaki korisnik individualno štiti poverljivošću svoje lozinke, glavni rizici postoje od mogućnosti zloupotrebe lokalnog email servera od strane spamer-a, tj. subjekata koje spolja žele da zloupotrebe email server za masovno slanje email poruka na veliki broj email adresa. To osim što opterećuje lokalne resurse, povlači za sobom još niz potencijalnih problema kao npr. da se zloupotrebljeni server nađe na „crnim listama“, pa da i legitimna pošta upućena sa tog email servera bude odbijana od strane većine drugih email serve-

ra, ili potencijalni pravni problemi ako sadržina ili količina takvih email poruka naruše neki zakon ili nanesu štetu nekom trećem licu.

Takođe, potpuno realan scenario kompromitovanja bezbednosti mreže koja ima pristup internetu je i mogućnost da neko od korisnika lokalne mreže slučajno ili namerno instalira na jedan ili više računara u lokalnoj mreži neki softver koji će samostalno slati masovne spam email poruke i time kako uzurpirati resurse, tako i kompromitovati u pravnom smislu javnu IP adresu lokalne mreže sa istim potencijalnim posledicama kao u prethodnom slučaju.

Proxy server koji je izuzetno koristan za „uštedu internet resursa" mreže može takođe biti kompromitovan spolja, ako administrator mreže nesvestan opasnosti dozvoli neovlašćeno korišćenje istog. Najčešće u praksi se ne koristi autorizacija korisnika proxy servera (a naročito ne transparentnih proxy servera) individualnim korisničkim lozinkama, jer je to logistički veoma nezahvalno, i opet postoji realna mogućnost da neko spolja može zloupotrebiti jednu ili više korisničkih lozinki.

4. Mere zaštite od spoljašnjih rizika i pretnji

Na samom box-u potrebno je dakle:

- Onemogućiti slanje email poruka koristeći lokalni email server bez autorizacije, što je inače podrazumevano setovanje svih email servera. Najčešće korišćena metoda autorizacije je da se koristi korisničko ime i lozinka istovetne onima koje se koriste za čitanje primljene elektronske pošte. Na taj način autorizovani korisnici mogu čitati svoju elektronsku poštu i slati je, ali je zatvorena mogućnost da neki treći subjekt „spolja" (sa interneta) zloupotrebi email server i neovlašćeno šalje elektronsku poštu sa njega.

  Konkretno komanda za to pravilo na firewall-u je sledeća:

  iptables -A FORWARD -p tcp -m tcp --dport 25 -j DROP

- Onemogućiti bilo kakvo slanje elektronske pošte koja potiče iz domena LAN mreže, a ne šalje se kroz implementirani email server, nego „direktno" na odredišne email servere namenjenih primalaca. Ovo se postiže definisanjem pravila na ruteru box-a da se onemogući TCP komunikacija bilo kog računara kroz port 25 (SMTP port) direktno ka internetu, već taj port „kao izlazni" ostaje otvoren i na raspolaganju samo legitimnom email serveru na LAN mreži.

  Konkretno komanda za to pravilo na firewall-u je sledeća:

  iptables iptables -A OUTPUT -p tcp -m tcp -o eth1 –dport 25 -j DROP

- Onemogućiti „dolazne konekcije" na portu proxy servera (najčešće portovi 3128 ili 8080, zavisno od konkretne implementacije) koje potiču „od spolja" (sa intrerneta), i time efektivno sprečiti da neko neovlašćeno spolja koristi interni proxy server za neke nelegitimne i/ili nelegalne aktivnosti.

  Konkretno komanda za to pravilo na firewall-u je sledeća:

  iptables iptables -A INPUT -p tcp -m tcp -i eth1 --dport 3128 -j DROP

5. Rezultati

Ovakav „box“ je implementiran u Visokoj tehnološkoj školi strukovnih studija u Šapcu, i ovde su prikazani kvantitativni i statistički rezultati ovakve implementacije.

5.1. Kvantitativna analiza korišćenja Lan mreže

Tabela 1. kvantitativna analiza korišćenja LAN mreže i internet konekcije

U sledećoj tabeli su prikazani kvantitativni podaci o korišćenju LAN mreže sa akcentom na opterećenje/iskorišćenje internet konekcije za 24h.

Rb.	Vrsta saobraćaja	Broj IP paketa	Količina podataka	Relativni udeo
11.	Dolazni saobraćaj (protok podataka sa interneta)	6.21x10^6	588Mb	2.93%
22.	Unutrašnji saobraćaj koji uključuje sadržaje koji su potekli iz cache memorije proxy servera	35x10^6	14Gb	69.69%
33.	Odlaznio saobraćaj (protok podataka ka internetu	9.476x10^6	5.5Gb	27.38%
4.	UKUPNO:	50.686x10^6	20.088Gb	100%

Veoma indikativna je efikasnost proxy servera koji je opslužujući više stotina korisnika toga dana na otprilike 90 PC računara u lokalnoj mreži veliku količinu internet sadržaja „servira-o“ iz svoje keš memorije, rasterećujući u tolikoj meri internet konekciju ustanove, da je realni protok sadržaja sa interneta činio samo 2.93 % celokupnog mrežnog saobraćaja u lokalnoj mreži. Naravno ova brojka nije samo odnos keširanog/ internet sadržaja, već u „unutrašnji saobraćaj“ ulaze i svi interni transferi podataka u internim informacionim sistemima, te je realni udeo samih keširanih sadržaja nešto manji u realnom radu, a koliki tačno, prikazano je u tabeli br. 3.

U tabeli br.2 je prikazana struktura rutiranja paketa po specifičnim pravilima definisanim na ruterskoj servisnoj instanci box-a.

Tabela 2. Struktura paketa mrežnog saobraćaja koji potpadaju pod posebna pravila rutiranja.

Rb.	Vrsta saobraćaja prema pravilima rutiranja	Broj paketa	Relativni udeo
1.	Legitimni dolazni paketi sa interneta	2.42x10^6	52.27%
2.	Nelegitimni paketi - pokušaji zloupotrebe proxy server-a	0	0%
3.	Nelegitimni paketi - pokušaji prstupa face-book sajtu	32225	0.69%
4.	Nelegitimni paketi - pokušaji prstupa youtube sajtu	1898	0.04%
5.	Nelegitimni paketi - pokušaji http sesija mimo proxy server	4431	0.1%
6.	Nelegitimni paketi - pokušaji pristupa sadržajima na internetu na portovima 444-65535	183x10^3	3.95%
7.	UKUPNO	4,63x10^6	100%

Analizirajući dostupne podatke iz tabele 2 može se analizirati efikasnost firewall-a. U konkretnom uzorku je uočljivo da nije bilo pokušaja zloupotrebe proxy servera spolja, a da je veći broj neželjenih internet aktivnosti uspešno blokiran kako od strane korisnika (pristup facebook i youtube sajtovima), tako i ne zanemarljiv broj (4431) pokušaja konekcija na portovima od 444 do 65535 što su uglavnom maliciozni softveri koji su instalirani sa ili bez znanja korisnika na pojedinim računarima.

6. Zaključak

U ovom radu prikazano je jedno kompletno multifunkcionalno rešenje „all in one“ tipa za administriranje i zaštitu jedne LAN mreže koja se sastoji od više funkcionalnih „podmreža“.

Koristeći standardno dostupne alate, prikazana je višeslojna implementacija koja zadovoljava osnove kriterijume bezbednosti računarske mreže kako na spoljašnjem, tako i na unutrašnjem planu. Prikazane implementirane funkcionalne celine su višeslojne i kompatibilne, u smislu da se određene funkcionalnsti „nadograđuju“ na druge, i/ili međusobno interaguju sa ciljem postizanja zadatih ciljeva.

Osim strogo bezbednosnih funkcija, u prikazanoj implementaciji su korišćene i neke napredne administratorske funkcije kao ilustracija kako se može ograničiti pristup internet sadržajima svim ili određenim korisnicima iz razloga npr. radne discipline i slično, što se postavlja kao što češći zadatak pred administratore mreža.

Prezentovani su i statistički podaci koji su rezultat implementacije iz kojih se može objektivno ceniti efikasnost, obim i dometi implementacije, ali i uočiti eventualni propusti i isti se ispraviti, kroz kontinualni monitoring i ažuriranje implementacije, administrator mreže može uočiti neželjene aktivnosti i iste onemogućiti koristeći implementirane alate, dodavanjem novog seta pravila u ciljani funkcionalni modul.

LITERATURA

“Structure and Encapsulation in Distributed Systems: the Proxy Principle”. Marc Shapiro. International conference on Distributed Computer Systems (ICDCS), Cambridge, SAD, 1986.

“Network Forensics”, Sherri Davidoff i Jonathan Ham, Prentice Hall, 2012.

“Networking Bible”, Barry Sosinsky, Wiley Publishing Inc 2009.

“The official Ubuntu Book”, 2nd Edition, B. M. Hill, J. Bacon Canoncial Ltd, 2007.

“OpenFlow: Enabling Innovation in Campus Networks”, N. McKeown ACM Comp. Commun., april 2008.

“TCP/IP Network Administration”, Hunt Craig, 3rd Edition. O'Reilly, 2002.

“A security standard for LANs“, Kirkpatrick, M.E. Computer Security Applications Conference, 1989.

“Protecting your organisation's most valuable asset [LAN security]“,Gahan, C. Designing Secure Systems, IEE Colloquium, 1992.

“A Survey of Ethernet LAN Security”, Kiravuo, T. ; Sarela, M. ; Manner, J. Communications Surveys & Tutorials, IEEE Volume: 15 [1477 – 1491], 2013.

„A Verification framework for Analyzing Security Implementations in an Enterprise LAN”, Bera, P. ; Dasgupta, P. ; Ghosh, S.K. Advance Computing Conference, 2009.

"On Designing the Security System for LAN-Based Educational Management Information System", Fangming Guo ; Hua Song ,e-Business and Information System Security (EBISS), 2010

"A QoS-enabled secure LAN access control system", Feng Xiaoping ; Zhang Yunliang Consumer Electronics, Communications and Networks (CECNet), 2011.

"Maximizing Ethernet Security by Switch-Based Single Secure Domain", Wahid, Khan Ferdous Information Technology: New Generations (ITNG), 2010.

Vladimir Stanojevic, M.Sc.
Mladen Veinovic, Ph.D.

LAN NETWORK ADMINISTRATION AND PROTECTION OF EDUCATIONAL INSTITUTIONS USING THE MULTIFUNCTIONAL LINUX BOX-TV

Summary

Computer systems and Network security is a wide and complex area, involving various equipment and software tools. Mostly, but not only used for such purposes are routers, firewalls and proxy servers. In this paper, individual and combined implementations of theese tools are displayed, all implemented on Linux based computer, all installed with just one purpose, which is fulfilling a set of goals and standards of computer resources and network security.

Key words: Computer network and systems security, Router, Firewall, Proxy, Linux.