Upotreba softverskih alata u cilju povećanja efikasnosti nastave iz predmeta vezanih za sigurnost računarskih komunikacija

Dalibor Dobrilović
Katedra za Informacione tehnologije
Univerzitet u Novom Sadu / Tehnički fakultet
"Mihajlo Pupin"
Zrenjanin, Srbija
ddobrilo@tfzr.rs

Borislav Odadžić
Katedra za Informacione tehnologije
Univerzitet u Novom Sadu / Tehnički fakultet
"Mihajlo Pupin"
Zrenjanin, Srbija
borislav.odadzic@gmail.com

Sadržaj— **U radu su prikazani rezultati istraživanja koja su imala za cilj stvaranje efikasnog okruženja koje bi se koristilo u nastavi iz predmeta vezanih za sigurnost računarskih komunikacija. U okviru pomenutih istraživanja vršena je evaluacija i razvoj softverskih alata za primenu u nastavi na visoškolskim ustanovama. Implementacija različitih scenarija za podršku laboratorisjkih vežbi je jedan od rezultata tog istraživanja. Uporedo sa eksperimantisanjem u korišćenju različitih softverskih alata za učenje koncepta računarskih mreža, započeta su istraživanja o primeni istih okruženja za praktičnu nastavu i laboratorijske vežbe iz predmeta vezanih za zaštitu podataka i računarskih mreža. U radu su prezentovani rezultati koji su proistekli iz tog istraživanja, koje još uvek u toku.**

Ključne riječi - GNS3; Virtual Box; sigurnost računarskih mreža; virtuelizacija; inženjerska edukacija

I. UVOD

Brz razvoj i ekspanzija informacionih tehnologija koja je prisutna u današnje vreme utiče na povećanje važnosti edukacije eksperata koji se bave tim tehnologijama. Edukacija eskperata ovih profila se vrši na tehničkim visokoškolskim ustanovama. Efikasnost nastave u najvećoj meri zavisi od laboratorijkih uslova u kojima se izvodi njen praktičan deo. Visoka cena opreme, njen brz razvoj i česte potrebe za nadogradnjom znatno otežavaju održavanje efikasnosti tih laboratorija. Zbog svih ovih uslova, raste i značaj softverskih rešenja u oblasti, kako računarskih mreža [1] tako i sigurnosti i zaštite podataka i računarskih mreža.

U ovom radu će biti prezentovani rezultati tekućeg istraživanja u oblasti primene softverskih alata za kreiranje efikasnog okuženja koji se može koristiti za vršenje laboratorijskih vežbi i praktičnih eksperimenata iz oblasti implementacije sigurnosnih mehanizama na sistemima u mrežnim okruženjima. Istraživanje predstavlja nastavak istraživanja koje je vršeno u pravcu modelovanja i implementacije efikasnog okruženja za laboratorijske vežbe i praktičnu nastavu iz predmeta Računarske mreže. U sklopu tog istraživanja kreirano je softversko okruženje bazirano na softveru za virtuelizaciju pod nazivom VNLab [1,2,3,4].

VNLab je hardversko-softverski model virtuelne mrežne laboratorije koji je strukturiran na sledeći način [2,3,4]. U hardverske komponente modela, spadaju server, radne stanice i mrežna infrastruktura koja omogućava upotrebu laboratorije i pristup VNLab serveru. VNLab je baziran na Microsoft Virtual Server 2005 R2 [5] softveru za virtuelizaciju. VNLab se hostuje na računaru sa host operativnim sistemom MS Windows 2003 i veb serverom Microsoft IIS 6.0 (Internet Information Server) [6].

Softverske komponente modela sastoje se od nekoliko elemenata koje omogućavaju funkcionisanje sistema. Microsoft Virtual Server 2005 R2 sa IIS 6.0 veb serverom čini osnovu za stvaranje virtuelne mreže i omogućava efikasnu infrastrukturu za pokretanje, rad i administraciju virtuelne laboratorije. Emulirana mreža se sastoji od velikog broja virtuelnih mašina. Broj od 40 virtuelnih mašina je dovoljan za kreiranje mrežnih scenarija i za izvođenje laboratorijskih vežbi. Virtuelne mašine emuliraju hardver i softver fizičkih računara zajedno sa njihovim mrežnim interfejsima (mrežnim karticama). Svaka virtuelna mašina može da emulira do 4 mrežne kartice (eng. Network Interface Card - NIC), jer je to maksimalan broj emuliranih virtuelnih mrežnih kartica koje podržava Virtual Server 2005. Na virtuelnim mašinama nalazi se instaliran CentOS i Trustix Linux koji se koriste u svakodnevnom radu laboratorije, a u eksperimentalnoj fazi upotrebe tu su još Scientific Linux, MicroCore, TinyCore itd.

Budući da se i ranije (2006) eksperimentisalo sa primenom tehnologije za virtuelizaciju u nastavi drugih predmeta [7], jedan od budućih pravaca istraživanja je bio usmeren u prilagođavanju VNLab okruženja za primenu u predmetima vezanim za sigurnost sistema i računarskih mreža. Ovaj razvoj je baziran po uzoru na sistem V-NetLab [8,9] u inicijalnoj fazi istraživanja, a od pomenutog sistema preuzeta je samo njegova namena za vežbanje sigurnosnih mehanizama i tehnika. Jedan pravac tog razvoja je baziran na proširenju primene VNLab okruženja [10], a drugi pravac u primeni sličnih softverskih okuženja sa kojima se ekperimentisalo u toku pomenutog istraživanja. Jedno takvo okruženje koje je pogodno za primenu u ove svrhe je GNS3 [11] framework za simulaciju

računarskih mreža u kombinaciji sa softverom za virtuelizaciju Oracle VirtualBox i CentOS operativnim sistemom.

U nastavku će biti opisana svaka od komponenti ovih sistema, način njegove upotrebe u nastavi, laboratorisjke vežbe koje su kreirane i iskustva sa njihovom upotrebom. Na kraju je dat pregled dosadašnjih rezultata istraživanja i precizirani pravci daljeg razvoja.

II. SOTVERSKO OKRUŽENJE ZA LABORATORIJSKE VEŽBE - SECLAB

SecLab je integrisano okruženje koje je bazirano na GNS3 softveru u kombinaciji sa pratećim softverskim paketima i softverom za virtualizaciju VirtualBox. Pored ovih paketa važan deo okruženja su i laboratorijske vežbe, kao i prateći softver koji ih podržava zajedno sa operativnim sistemom CentOS [12].

A. GNS3 (Graphical Network Simulator)

GNS3 je grafički simulator koji omogućava simulaciju kompleksnih mreža [1]. Da bi omogućio okruženje za simulaciju složenih komunikacionih sistema (Slika 1.), GNS3 je integrisan sa sledećim programskim paketima:

- Dynamips - Cisco IOS emulator,
- Dynagen – tekstualno bazirani interfejs za Dynamips,
- Qemu – generički i open source emulator i virtualizer,
- VirtualBox – besplatni softver za virtualizaciju,
- Wireshark - open-source program za analizu paketa.

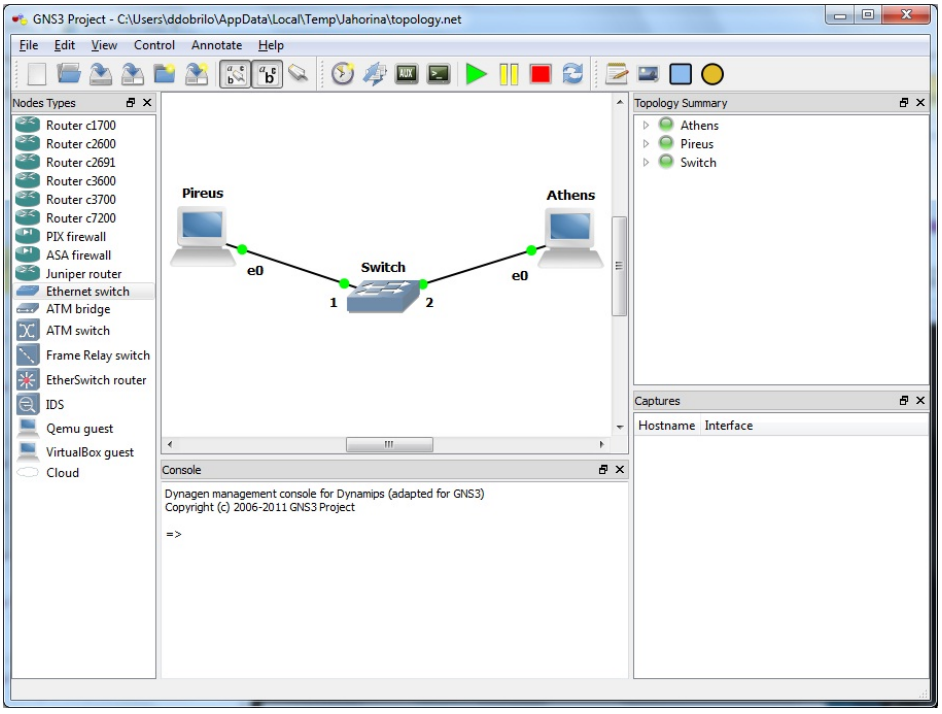
GNS3 je odličan alat za kreiranje laboratorijskih vežbi za inženjere, administratore i za pripremu ispita za sledeće sertifikate: Cisco (CCNA, CCNP, CCIP i CCIE), Juniper (JNCIAm, JNCIS i JNCIE) Redhat (RHCE, RHCT), Microsoft (MSCE, MSCA) i Novell (CLP). Može se koristiti za eksperimentisanje i rad sa Cisco IOS i Juniper JunOS operativnim sistemima [1].

B. Oracle Virtual Box

Oracle VM VirtualBox (ranije Sun VirtualBox i Sun xVM VirtualBox) [13] je softver za virtuelizaciju, koji je nastao kao proizvod Innotek GmbH kopanije. Oracle VM VirtualBox se instalira kao aplikacija na fizički računar i njen host operativni sistem i dozvoljava pokretanje virtuelnih mašina sa Guest operativnim sistemom. VirtualBox je kreiran za rad na Linux, Mac OS X, Windows XP, Windows Vista, Windows 7, Windows 8, Solaris, OpenSolaris i FreeBSD platformi. Postoji i podrška za sledeće Guest operativne siteme: Windows, Linux, BSD, OS/2, Solaris i dr. Aktuelna vezija 4.2.0, datira od septembra 2012. Sa verzijom 4, VirtualBox se distribuira kao besplatan softver pod GNU General Public License version 2 (GPLv2).

C. CentOS

CentOS je besplatna distribucija Linux operativnog sistema koja je zasnovana na komercijalnom izdanju Red Hat Enterprise Linux (RHEL) distribucije i sa kojom pokušava da očuva potpunu binarnu kompatibilnost. Ime CentOS je izvedeno od Community enterprise Operating System i predstavlja pokušaj da se korisnicima pruži besplatna platforma za poslovne sisteme. Jedno vreme CentOS je bio najzastuplenija platfroma za veb servere i pokrivao je oko 30% od ukupnog broja veb servera pod Linux operativnim sistemom.



Slika 1. GNS3 sa startovanim scenarijom za SSH protokol

D. *Instalirani softver za podršku*

Da bi se CentOS operativni sistem mogao koristiti za laboratorijske vežbe i eksperimentalan rad sa implementacijom sigurnosnih mehanizama na operativom sistemu virtuelnih mašina (CentOS) potrebno je da su instalirani sledeći paketi. Za realizaciju vežbi iz firewall sistema potrebno je da je instaliran *iptables* i *ip6tables*. Za rad sa SSH protokolom potrebno je da su instalirani *openssh-server*, *openssh-clients*, *openssh*. Za rad sa FTP serverom i SFTP, SSL i TLS protokolima, potrebno je instalirati *vsftpd* server. Za prikaz implementacije SSL/TLS protokola sa veb apache serverom potrebno je instalirati *apache* server i *mod-ssl*.

Paket *nmap* je potreban za izvođenje vežbi sa skeniranjem portova i provere sigurnosti servera. Alat *snort* je potreban za demonstraciju rada IDS (*Intrusion Detection System*) sistema. Za implementaciju IPSec protokola potrebno je instalirati *strongswan* paket.

E. *Dodatni softver*

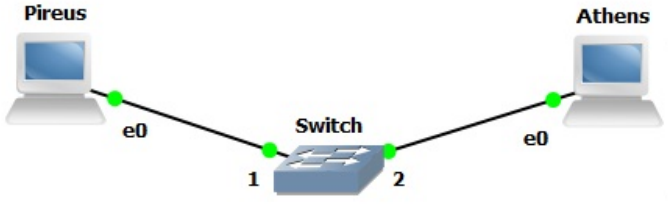
Ako je potrebno i da bi se podržao veći broj vežbi i tehnologija mogu se dodavati i druge softverske komponente, bez obzira da li se radi o operativnim sistemima ili instaliranom softveru. Primer za to mogu biti specijalizovane Linux distribucije namenjene za proveru i analizu sigurnosti sistema.

III. SCENARIJA ZA LABORATORIJSKE VEŽBE

SecLab je okruženje koje se sastoji od softverskih komponenata opisanih u prethodnoj sekciji. Važan deo ovog okruženja, sa stanovišta njegove upotrebe, predstavljaju i laboratorisjke vežbe koje su podržane u njemu. U ovoj sekciji će biti ukratko opisane te laboratorijske vežbe, njihova mrežna scenarija i koncepti koji se u njima mogu učiti i uvežbavati. Potrebno je napomenuti da je kreirano okruženje namenjeno sticanju praktičnih iskustava u implementaciji sigurnosnih mehanizama i za njihovo bolje razumevanje.

Za izvedbu svakog scenarija je potrebno minimalno dve vitualne mašine, kao što je to prikazano na slici 2. Jedna mašina predstavlja klijenta (Pireus), sa kojeg se obično vrši pristup na server (Athens). Implementacija sigurnosnih mehanizama se vrši na serveru, a njihova provera na klijentu.

Za neka scenarija, kao što je firewall-iptables moguće je dodati još jedan računar/firewall zbog proširenja mogućih scenarija.



Slika 2. GNS3 sa strartovanim scenarijom za SSH protokol

A. *SSH protokol i javni i tajni ključ*

Prvi opisani scenario obuhvata rad sa SSH protokolom [14,15] i pristup sa klijentskog računara bez autentifikacije uz upotrebu javnog i tajnog ključa. Za ovu vežbu je potrebno imati instaliran SSH serverski program na serveru i SSH klijentski program na klijentu. Studenti u toku vežbe trebaju da kreiraju javni i tajni ključ upotrebom naredbe *ssh-keygen* i uz upotrebu RSA algoritma. Zatim, potrebno je da prebace ključ sa klijenta na server uz upotrebu SCP (secure copy) naredbe. Na kraju potrebno je da provere da li logovanje na udaljeni server bez autentifikacije radi. Pre svih ovim akcija, studenti treba da kreiraju korisnički nalog na oba računara koji će se koristiti za vežbu.

Na kraju, studenti mogu da analiziraju rad SSH servera, njegovo startovanje i stopiranje, kao i osnovne elemente konfiguracionog fajla i izmenu pojedinih konfiguracionih parametara. Takođe se preoručuje upotreba klijentskog softvera za pristup SSH serveru sa opcijom –v, koja daje detaljne informacije o vezi koja se izvršava između dva računara.

B. *Sigurnost FTP servera i SFTP, SSL i TLS protokoli*

Drugi scenario zahteva instalaciju *vsftpd* FTP servera ili nekog sličnog, a demonstrira studentima pristup preko klasičnog FTP protokola i prenos podataka, a kasnije i prenos podataka sigurnijom vezom. U vežbi se vrši konfiguracija i startovanje FTP servera i prikaz pristupa sa FTP i SFTP protokolom. Nakon obavljene demonstracije, vrši se kreiranje sertifikata i rekonfiguracija FTP servera da bi se omogućio pristup i sa SSL/TLS [16] protokolima. U jednoj varijanti vežbe može se omogućiti paralelan (enkriptovani i neenkriptovani pristup), a na kraju samo enkriptovani pristup.

C. *Sigurnost Apache servera i SSL i TLS protokoli*

Treći scenario zahteva instalaciju *apache* [17] veb servera i *mod_ssl* modula. Za proveru vežbe mogu se instalirati i dodatni paketi kao što je tekstualni veb pretraživač *lynx*. U vežbi se vrši kreiranje samopotpisanog sertifikata (*self-signed certificate*) i osnovna konfiguracija veb servera. Provera pristupa se vrši sa klijentske mašine uz upotrebu tekstualnog browsera *lynx*. Budući da pristup preko tekstualnog browser-a ne pruža dovoljno ilustrativan prikaz za studente, može se izvštiti zamena klijentske mašine sa nekim drugim manjim Linux operativnim sistemom sa podrškom za grafičko okruženje kao što je DSL (*Damn Small Linux*). Instalirani CentOS u ovom scenariju je instaliran samo u tekstualnom modu, zbog potrebe za minimalnošću instalacije i njenom lakom prenosivošću na druge platfrome. U vežbi se studenti mogu naučiti i osnovim komandama paketa OpenSSL.

D. *Firewall sistemi*

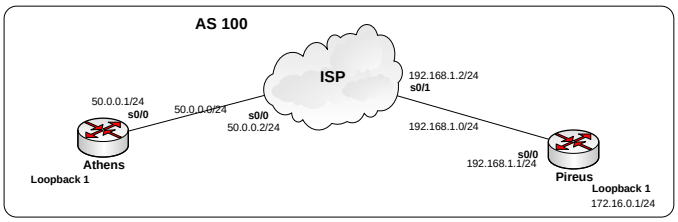
Za neka scenarija, kao što je firewall-iptables moguće je dodati još jedan računar/firewall zbog proširenja mogućih scenarija. U ovom slučaju se koriste samo dva računara. Na jednom (Athens) vrši se unos firewall pravila, a na drugom (Pireus) samo njihova provera. U ovoj vežbi se vrši praktičan rad i implementacija firewall sistema uz pomoć alata *iptables* [18], i njegova primena za filtriranje paketa, NAT i prosleđivanje portova u IPv4 okruženju. Takođe, uz upotrebu

ip6tables alata može se vršiti i implementacija filtriranja paketa u IPv6 okruženju. U vežbi se uče osnove firewall sistema i sintaksa naredbi za unošenje njihovih pravila.

Za razliku od prethodnih vežbi koje su prvo impementirane u opisanom SecLab okruženju. Ove dve vežbe su prvo formirane u VNLab okruženju gde su testirane nekoliko semestara, a zatim su portovane u SecLab okruženje sa manjim izmenama.

E. Proširenje podržanih scenarija

Proširenja scenarija za ovo okruženje su moguća. U toku je ekpserimentisanje sa scenarijom sa IPSec VPN Site-to-site uz implementaciju *strongswan* paketa. Zatim, implementacija SSH VPN u istom okruženju jedan je od mogućih pravaca. Na slici 3 je prikazan mogući scenario za IPSec VPN.



Slika 3. Mogući scenario za IPSec VPN

Druga dva scenarija su takođe u eksperimentalnoj fazi. Radi se o scenariju koji omogućuje proveru sigurnosti sistema uz upotrebu alata *nmap* [19]. U tu svrhu se može koristiti jedna virtuelna mašina za skeniranje i druga virtuelna mašina (ili više njih) kao server koji se skenira. U trenutnoj fazi istraživanja vežba je implementirana na nivou prototipa.

Druga vežba, koja je u sličnoj fazi razvoja je vežba koja se odnosi na IDS (*Intrusion Detection System*) [20], a koja je bazirana na alatu *snort*. Vežba je takođe implementirana na nivou prototipa. U ovom slučaju, kao i u svim prethodnim slučajevima, koristi se *open-source* softver na Linux platformi što pozitivno utiče na upotrebnu vrednost okruženja zbog njegove niske cene.

IV. ZAKLJUČAK

SecLab i prezentovano okruženje je uspešno korišćeno u nastavi iz predmeta Zaštita podataka i računarskih mreža na visokoškolsoj ustanovi (Univerzitet u Novom Sadu / Tehnički fakultet "Mihajlo Pupin" – Zrenjanin) u toku jednog semestra. Okruženje je pokrivalo deo laboratoriskih vežbi.

Prve tri opisane laboratorijske vežbe su korišćene u toku tog istog semestra. Druge dve laboratorijske vežbe (firewall) su korišćene u toku većeg broja semestara u okviru okruženja VNLab, koje je takođe kreirano na istom Fakultetu. U skorije vreme, i ove dve vežbe su prebačene u SecLab okruženje. Dve zadnje opisane vežbe (*nmap* i *snort*) su razvijene u prototip varijanti, a planira se uvođenje i IPsec i SSH VPN vežbi.

Okruženje se pokazalo kao dovoljno efikasno za upotrebu u nastavi. Okruženje je pouzdano, lako za instalaciju. Jedna od prednosti ovog okruženja je da je potpuno besplatno i studenti ga mogu lako instalirati za rad u kućnim vannastavnim uslovima. Okruženje se može koristiti u više varijanti. Iste vežbe koje su ovde prikazane mogu se implementirati samo na Oracle VirtualBox softveru za virtualizaciju, bez GNS3 okruženja. Tako se ne gubi ništa na funkcionalnosti, ali se gubi na grafičkoj prezentaciji scenarija koja je bitna za studente zbog boljeg razumevanja vežbe i lakšeg snalaženja u slučaju konfiguracije većeg broja mašina. Druga varijanta je mogućnost upotrebe Qemu softvera za virtuelizaciju, umesto VirtualBox-a. Jedan od pravaca daljeg rada na ovoj laboratoriji bi bio i upoređivnje performansi rada mogućih kombinacija softvera i odabira najbolje kombinacije.

Dalji rad na ovom projektu, pored opisanog proširenja seta vežbi sa IPSec i SSH VPN tunelima, bio bi i integrisanje Wireshark softvera za analizu mrežnog saobraćaja u ove vežbe. Wireshark je podržan od strane GNS3 i integrisan u ovo okruženje ali trenutno postoji problem sa njegovim korišćenjem u laboratorijskim vežbama. Prevazilaženjem ovog problema, bi se znatno podigao kvalitet vežbi a studentima omogućio detaljniji uvid u protokole i sigurnosne mehizme koji se koriste. Te vežbe bi bile realizovane po ugledu na [21].

LITERATURA

[1] Borislav Odadžić, Dalibor Dobrilović, "Softverski alati u nastavi računarskih komunikacija", XIII simpozijum o novim tehnologijama u poštanskom i telekomuikacionom saobraćaju, PosTel 2012, 04. i 05. decembar 2012. , Beograd, Srbija, pp 337-347.

[2] Dobrilovic D., Stojanov Z., Odadzic B., Design and Implementation of Online Virtual Network Laboratory, Advancement in Online Education: Exploring the Best Practices, Vol. 1, Chapter 10, Publication date: 2011 4th quarter, 2011.

[3] D. Dobrilovic, V. Jevtic, Z. Stojanov, B. Odadzic, "The Design Guidelines for Virtual Network Laboratories", Proceedings of IX IEEE International Symposium on Telecommunications, October 25-27, Sarajevo, Bosnia & Herzegovina, 2012.

[4] D. Dobrilovic, V. Jevtic, Z. Stojanov, B. Odadzic, "Usability of virtual network laboratory in engineering education and computer network course", Proceedings of joined 15th International Conference on Interactive Collaborative Learning and 41st IGIP International Conference on Engineering Pedagogy, September 26 – 28, Villach, 2012.

[5] Robert Larson, Janique Carbone, Microsoft Virtual Server 2005 R2 Resource Kit Chapter 7: Best Practices for Configuration and Performance, Microsoft Press, Redmond, USA, August, 2007.

[6] Mitch Tulloch, IIS 6 Administration, McGraw Hill, April, 2003.

[7] Dobrilović Dalibor, Stojanov Željko, Using virtualization software in operating systems course, Proceedings of the 4th IEEE International Conference on Information Technology: Research and Education - ITRE 2006, pp. 222-226, ISBN: 1-4244-0859-8, Tel Aviv, Israel, 16- 19 October 2006, DOI: 10.1109/ITRE.2006.381569

[8] K. Krishna, W. Sun, P. Rana, T. Li and R. Sekar, "V-NetLab: A Cost-Efective Platform to Support Course Projects in Computer Security", Proceedings of 9th Annual Colloquium for Information Systems Security Education (CISSE 05), Atlanta, USA, Jun, 2005.

[9] Sun W., Katta V., Krishna K., Sekar R., V-NetLab: An Approach for Realizing Logically Isolated Networks for Security Experiments, Proceedings of (CSET'08), San Jose, USA, July 28 – August 1, 2008.

[10] Dalibor Dobrilovic, Vesna Jevtic, Borislav Odadzic, Expanding the usability of virtual network laboratory in IT engineering education, International Journal of Online Engineering (iJOE) (Accepted for publication), 2013.

[11] http://www.gns3.net/gns3-introduction/, preuzeto septembra 2012.

[12] P. Membrey, T. Verhoeven, R. Angenendt, The Definitive Guide to CentOS, Apress, 2009.

[13] Oracle VM Virtual Box – User Manual (pdf version), http://download.virtualbox.org/virtualbox/UserManual.pdf, May 2012.

[14] T. Ylonen, C. Lonvick, RFC 4251, The Secure Shell (SSH) Protocol Architecture, January 2006.

[15] Daniel J. Barrett, Ph. D., Richard E. Silverman i Robert G. Byrnes, SSH: The Secure Shell, The Definitive Guide, http://www.snailbook.com/, 2009.

[16] T. Dierks, C. Allen, RFC 2246, The TLS Protocol, Version 1.0, January 1999.

[17] Ben Laurie, Peter Laurie, Apache: The Definitive Guide, 3rd Edition, O'Reilly Media, December 2002.

[18] Gregor N. Purdy, Linux iptables Pocket Reference, Firewalls, NAT & Accounting, O'Reilly Media, August 2004.

[19] Fyodor Lyon, Gordon, Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning. Insecure.com LLC., 2009.

[20] Toby Kohlenburg, Snort IDS and IPS Toolkit. Syngress Publishing Inc. 2007.

[21] J.F. Kurose, K.W. Ross, Computer Networking: A Topdown Approach, 4th edition, 2007.

ABSTRACT

Abstract—In this paper is presented the next phase of several years research with the goal of development of efficient environment created for usage in Computer Networks and related courses. Within this research the evaluation of created environement and its usage at university and courses within university curricula was performed. The implementation of various scenarios for laboratory exercises created to support this environment is one of the project results.

Parallely with the experimentation with usage of created environment and the similar software tools, the research is pointed towards the effort to expand the usability ot these enviornemnents not only to teaching networking concepts, but to teach the data and network security related issues. In this paper are presented the results of this ongoing research.

USAGE OF SOFTWARE TOOLS IN NETWORK SECURITY COURSES

Dalibor Dobrilović, Borislav Odadžić