СИМУЛАЦИЈА НАПАДА НА РАЧУНАРСКУ МРЕЖУ И АНАЛИЗА ПАКЕТА КОРИШЋЕЊЕМ GNS3 И WIRESHARK

Марија Зајегановић[1] Милан Павловић[2] Марко Андрејић[3] Слободан Чабаркапа[4] Никола Курбалија[5]

Резиме: Рачунарске мреже су постале саставни део нашег свакодневног живота, рада, комуникације, учења и забаве. Оне се непрестано мењају и побољшавају. Као такве, често су мета многих напада и зато их је неопходно заштитити. Тимови стручњака се тиме баве и за потребе истаживања и обучавања у области безбедности рачунарских мрежа се користе многи мрежни емулатори и анализатори пакета. У овом раду ће бити представњено неколико студија случаја које описују најчешће нападе на рачунарску мрежу као и технике којима се ти напади спречавају. Ти одабрани случајеви ће бити описани и анализирани јавно доступним алатима. За мрежни емулатор ће бити коришћен *GNS3*, а за анализатор пакета и протокола *Wireshark*.

Кључне речи: мрежни емулатор, анализатор пакета, студије случаја, напад на мрежу, безбедност мреже, *ARP Spoofing*, *DHCP Spoofing*, *Network Sniffing*

SIMULATING COMPUTER NETWORK ATTACK AND ANALYZING PACKETS USING GNS3 AND WIRESHARK

Abstract: Computer networks have become a part of our everyday life, work, communication, learning, and fun. They always change and get better. This makes them targets, which need to be protected from potential malicious attacks. Teams of experts do this, and to meet the needs of research and training in cyber security, many different emulators and packet analyzers are being used. In this paper, a few case studies will be presented, that describe most common computer network attack types, and techniques that prevent such attacks. The cases are described and analyzed through publicly available tools. GNS3 is used as a network emulator, and Wireshark as a packet analyzer.

Key words: network emulator, packet analyzer, case study, network attack, network security, ARP Spoofing, DHCP Spoofing, Network Sniffing

1. УВОД

Тема безбедност рачунарских мрежа је толико актуелна да су стручњаци у тој области развили алате којима она може да се реализује. Основни принципи сигурности информација су познати под називом *CIA* (*CIA triad, Confidentality, Integrity, Availability*). Они обухватају поверљивост, интегритет и доступност, што чини срж безбедности рачунарских мрежа. Ова три појма заједно чине модел за развој безбедносних полиса и представљају основни концепт и циљеве за успостављање и очување рачунарске мреже безбедном [1], [2]. Стручњаци за сајбер сигурност користе низ различитих вештина и дисциплина када штите податке у сајбер простору, пазећи да увек остану на страни закона. У заштитне мере спадају технологија, људски фактори, политика и пракса. Коначно, корисници сајбер простора треба да постану боље

[1] мр, Академија техничко-уметничких струковних студија Београд одсек Висока школа за информационе и комуникационе технологије, Здравка Челара 16, Београд, e-mail: marija.zajeganovic@ict.edu.rs
[2] др, Академија техничко-уметничких струковних студија Београд одсек Висока школа за информационе и комуникационе технологије, Здравка Челара 16, Београд, e-mail: milan.pavlovic@ict.edu.rs
[3] студент, Академија техничко-уметничких струковних студија Београд одсек Висока школа за информационе и комуникационе технологије, Здравка Челара 16, Београд, e-mail: marko.andrejic.2011.18@ict.edu.rs
[4] дипл.инж., Академија техничко-уметничких струковних студија Београд одсек Висока школа за информационе и комуникационе технологије, Здравка Челара 16, Београд, e-mail: slobodan.cabarkapa@ict.edu.rs
[5] спец.струк.инж, Академија техничко-уметничких струковних студија Београд одсек Висока школа за информационе и комуникационе технологије, Здравка Челара 16, Београд, e-mail: nikola.kurbalija@ict.edu.rs

упознати са претњама и да успоставе културу учења и свести о потреби безбедности и поштовања политика, процедура и смерница које се односе на безбедност у сајбер простору како би заштитили себе и организацију од напада [3].

Веома важно за мрежног администратора је да зна да разликује и класификује претње и нападе на мрежу као и да одбрани мрежу од тих напада и претњи. Претње можемо поделити у две групе: унутрашње и спољашње претње. Спољашње претње су претње које долазе изван компаније, док унутрашње долазе из компаније, као на пример незадовољни радник, шпијун и слично. С друге стране, напади на мрежу се односе на већ извршене акције или оне које су у току, искоришћавањем слабости и пропуста у мрежи са циљем оштећења мреже и мрежних ресурса, крађе информација, брисања података, итд. Напади могу бити пасивни и активни. Пасивни се користе за добијање информација о мрежи и системима али не мењају ништа на њима, док активни напади покушавају да на одређене начине направе измене у мрежи као што су мењање или брисање конфигурације и/или података.

Алати који се данас користе за нападе на мрежу и рачунаре су углавном бесплатни и јавно доступни свима, што доводи до закључка да није потребно много труда и времена да се изврши било какав напад на мрежу. Ако нападач има одређене вештине и искуство, могуће је извршити напад на мрежу и не оставити никакав траг о томе. Зато је изузетно значајно да се јавно доступни алати искористе у сврху обучавања будућих стручњака у области безбедности рачунарских мрежа. У овом раду ће управо бити приказан мрежни емулатор *GNS3* и анализатор пакета *Wireshark*, који се користе за реализацију три примера напада на рачунарску мрежу са циљем да се помоћу тих студија случаја стекну вештине неопходне будућем стручњаку у области безбедности рачунарских мрежа.

2. АНАЛИЗАТОР ПАКЕТА *WIRESHARK*

Анализирање пакета (енгл. *packet sniffing*) је процес бележења и обрађивања података у реалном времену док ти подаци путују мрежом, како би се боље разумело шта се дешава у мрежи у неком периоду. „Снифер" пакета је алат или софтвер који се користи за анализирање пакета и служи за „хватање" необрађених података који путују мрежом. Да би се уопште и могли анализирати пакети на мрежи, прво је потребна мрежна картица која подржава промискуитетни режим. То је режим у којем мрежна картица може да види све пакете који се преносе мрежом. Анализирањем тих пакета се могу сазнати карактеристике и перформансе мреже, може се лоцирати проблем у мрежи, проверити ко се налази на мрежи и ко са ким комуницира, открити да ли се тренутно одиграва нека врста напада или загушења у мрежи и могу се тестирати протоколи и апликације које су рањиве и подложне нападима. Различити анализатори пакета имају и различите спецификације и могућности. Приликом избора анализатора веома је важно обратити пажњу на то које протоколе подржава, на ком оперативном систему ће се користити, колика је цена анализатора, да ли постоји подршка односно јасно написана документација. Имајући све ово у виду, међу анализаторима пакета првог избора свакако се налази *Wireshark*.

Wireshark је бесплатан анализатор пакета отвореног кода [4] који се првенствено користи за анализирање мреже, детектовање напада и пропуста у мрежи, откривање грешака и наравно за едукацију. Развио га је *Gerald Komb* 1998. под називом *Ethereal* и након што је *Gerald Komb* напустио пројекат, због правних проблема са именом и заштитним знаком, преименован је 2006. године у *Wireshark*. Он подржава преко хиљаду различитих протокола, почевши од оних основних као што су *IPv4* и *IPv6*,

DHCP, *ARP*, па све до оних напреднијих као што су то *DNP3* и *BitTorrent* протоколи. С обзиром да је то софтвер отвореног кода, његов код је јавно доступан те свако може учествовати у његовом развоју, било да је у питању развој нових функција или додавање неких нових протокола које још увек не подржава. Налази се под *GNU Public Licencom* (*GPL*), што значи да га свако може користити у било које сврхе, биле оне едукативне, личне или комерцијалне, а подржава готово све велике оперативне системе. Заједница која ради на његовом развоју је једна од најактивнијих заједница отвореног кода на свету, те тако има велику подршку, која наравно зависи и од самих корисника.

Графички интерфејс *Wireshark*-а је кориснички веома прилагодљив и углавном не захтева много ресурса рачунара и мреже. Након покретања *Wireshark*-а увек се прво бира мрежни интерфејс на коме ће се пратити и бележити пакети и на њему се може одмах поставити неки филтер како би се ближе дефинисали пакети који се „снифују".

Wireshark може бити веома користан како у мањим тако и у већим мрежама. Одличан је и за анализирање бежичног саобраћаја, а има могућност и подршку за *VoI*P саобраћај и пакете, где се може користити за откривање грешака приликом преноса говора и *SIP* пакета. Све ове описане могућности *Wireshark*-а су одличне докле год се ради о анализирању мрежа на једној локацији. У ситуацијама када је потребно анализирати мрежу на неком удаљеном серверу или рутеру, *Wireshark* постаје практично неупотребљив и тада је потребно користити друге анализаторе протокола.

У овом раду је *Wireshark* коришћен као анализатор протокола првог избора у едукативне сврхе за анализу пакета у мрежи у којој су симулирани добро познати и често коришћени напади на рачунарску мрежу, као и одбрана од њих.

3. МРЕЖНИ ЕМУЛАТОР *GNS3*

Симулатори и емулатори мреже су софтверски програми помоћу којих се могу дизајнирати и тестирати виртуелне мреже на рачунару. Ови програми су углавном бесплатни за разлику од хардверских уређаја који могу бити изузетно скупи, нарочито за обуку и за особе које тек улазе у свет рачунарских мрежа.

Graphical Network Simulator-3 (*GNS3*) је бесплатни софтвер отвореног кода [5] који представља софтверски мрежни емулатор који користе мрежни инжењери широм света за тестирање и конфигурисање виртуелних мрежа различитих топологија. Првобитно је *Jeremy Grossman* креирао тај софтвер да би могао да се обучи за стицање *CCNP* сертификата, а данас се више од 10 година, од 2008. године, користи за једноставно прављење и конфигурисање мрежа, снимање мрежа у виду одговарајућег пројекта, као и за тест окружења у којима се може тестирати безбедност мреже уз помоћ одређених алата. *GNS3* је софтвер отвореног кода на којем свако може да ради и да помогне при његовом даљем развијању, а доступан је на свим великим опеартивним системима. У почетку је подржавао само *Cisco* уређаје, а данас су у њему подржани многи уређаји других произвођача као и уређаји са софтвером отвореног кода. Значајна предност *GNS3* емулатора је та што може да се интегрише са хардверским уређајима који се могу повезати са *GNS3* пројектом и тако проширити виртуелна мрежа, као и могућност интеграције *Wireshark*-а у сам *GNS3* који се може користити за анализирање пакета и мреже унутар пројекта.

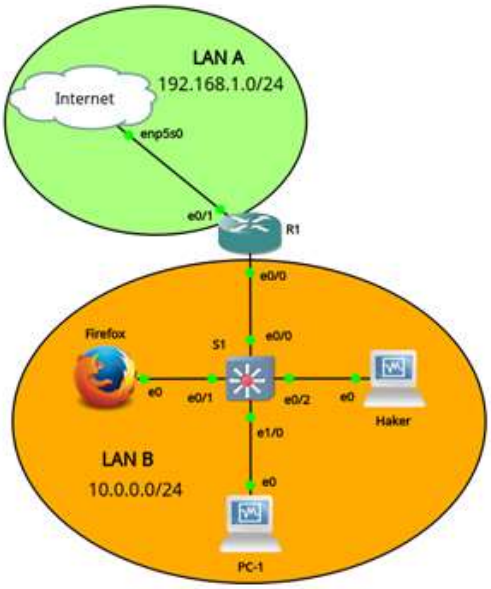
У овом раду је *GNS3* коришћен као емулатор мреже у едукативне сврхе за симулацију добро познатих напада на рачунарску мрежу и искоришћена је могућност интеграције *Wireshark*-а у сам *GNS3* пројекат.

4. ПРИМЕРИ СИМУЛАЦИЈЕ НАПАДА НА РАЧУНАРСКУ МРЕЖУ

Напади на рачунарску мрежу се могу извршити на различитим слојевима OSI модела. Безбедносна решења попут *VPN*-а, *firewall*-а, *IPS/IDS* уређаја и слично, мрежни администратори користе за заштиту од 3. до 7. слоја. Међутим, ако је 2. слој угрожен, то ће утицати на све слојеве изнад. Да би се спречили напади на 2. слоју, важно је познавати механизме који на том слоју постоје. Нападе на 2. слоју можемо поделити у следеће категорије: напади на *MAC* табелу, *VLAN* напади, *DHCP* напади, *ARP* напади, напади на *IP* и *MAC* адресе и *STP* напади. *MAC flooding* напад се често сматра „кључем“ за даље нападе на мрежу у циљу крађе података и поверљивих информација, или надгледање саобраћаја ради планирања већих напада. Након тог напада, следе остали попут ових који су симулирани за потребе овог рада: *ARP Spoofing*, *DHCP Spoofing* и *Network Sniffing*.

4.1. ARP Spoofing

На слици 1 је приказана мрежа која се користи за симулацију *ARP Spoofing*-а.

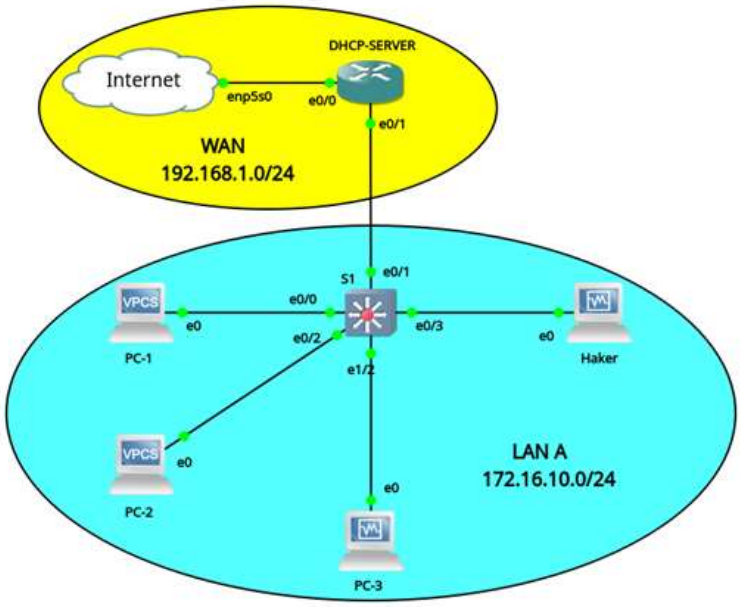


Слика 1 – ARP Spoofing

ARP протокол ради тако што хост шаље бродкаст захтев са питањем чија је одређена *IP* адреса и чека на *ARP* одговор од власника те *IP* адресе у виду његове *MAC* адресе. Уз помоћ одређених алата, хакер може злоупотребити то и одговорити на туђи *ARP* захтев да је тражена *IP* адреса његова и тако послати своју *MAC* адресу. Циљ овог напада је да се нападач представи рачунару као његов подразумевани излаз, док се правом подразумеваном излазу (рутеру) представља као тај рачунар, тако да кад год рачунар иницира неку комуникацију ка некоме ван мреже, пакет ће прво доћи до нападача, а затим ће се проследити ка дестинацији. За ову симулацију је коришћен алат *arpspoof* који омогућава нападачу да се лажно представља другим уређајима. Нападач податке о мрежи прикупља алатом *Nmap*. Док је напад у току, уз помоћ анализатора протокола *Wireshark* могу се забележити размењени пакети. У *ARP* кешу се може уочити да су две различите *IP* адресе упарене са истом *MAC* адресом. То указује да је *ARP Spoofing* напад у току. *ARP Spoofing* напад се може спречити конфигурисањем *Dynamic ARP Inspection* (*DAI*). Када се та опција подеси на свичу кроз који се одвија саобраћај, пакети који су намењени нападачу ће бити одбачени.

4.2. DHCP Spoofing

На слици 2 је приказана мрежа која се користи за симулацију *DHCP Spoofing*-а.

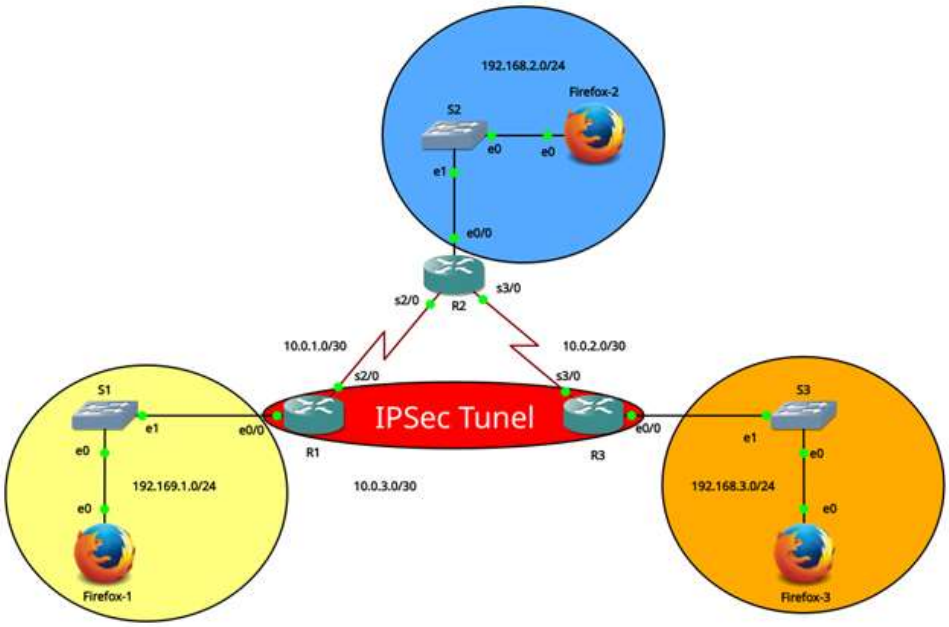


Слика 2 – DHCP Spoofing

DHCP Starvation и *DHCP Spoofing* су напади у којима хакер прво изврши напад на *DHCP* сервер у мрежи тако што шаље велики број *DHCP DISCOVER* порука са лажним *MAC* адресама како би „истрошио" све адресе *DHCP* сервера. Ако *DHCP* сервер одговара на ове поруке, све адресе које су слободне за резервацију, убрзо ће бити истрошене и овај тип напада представља *DHCP Starvation*. Једном када дође до тога, хакер може поставити свој (злонамерни) *DHCP* сервер који ће одговарати на друге *DHCP DISCOVER* поруке и додељивати хостовима параметре које је хакер подесио. Један од тих параметара може бити *IP* адреса подразумеваног излаза, коју нападач може подесити да буде његова *IP* адреса а затим прослеђивати саобраћај ка правом подразумеваном излазу. Овај тип напада се зове *DHCP Spoofing*. Да би се заштитили од оваквог типа напада, на рутеру или свичу се конфигурише *DHCP Snooping* опција која ради проверу *DHCP* порука на поверљивим портовима и на основу тога и *DHCP snooping binding* табеле одлучује да ли ће *DHCP* пакет бити прихваћен или одбачен. У овој симулацији нападач користи прво *Yersinia* алат и командом *yersinia -G* започиње *DHCP Starvation* напад. Како је за то време укључен анализатор протокола *Wireshark*, може се приметити веома велики број *DHCP DISCOVER* порука. Након исцрпљивања правог *DHCP* сервера, лажни *DHCP* сервер може започети са изнајмљивањем својих параметара. Детектовање *DHCP Spoofing* напада може бити компликована ствар, јер уређаји добијају *TCP/IP* параметре који су на неку начин у потпуности валидни. Зато је важно такав напад унапред спречити, што се постиже конфигурисањем *DHCP Snooping*-а. То је безбедносна могућност која се користи за спречавање *DHCP Spoofing* напада и ради на принципу филтрирања *DHCP* порука на неповерљивим портовима. *DHCP Snooping* се конфигурише на свичу и подразумевано су сви портови неповерљиви. Само портови на које су повезани *DHCP* сервери се постављају као поверљиви, што би значило да само на тим портовима могу пролазити *DHCP* пакети као што су *DHCP OFFER* и *DHCP ACK*, док то није могуће на неповерљивим портовима

4.3. Network Sniffing

На слици 3 је приказана мрежа која се користи за симулацију *Network Sniffing*-а.



Слика 3 – Network Sniffing

Network Sniffing се не сматра правим нападом, али у сваком случају представља претњу па га је због тога потребно спречити. *Network Sniffing* подразумева „ослушкивање" мреже или њено надгледање, ради прикупљања одређених информација (података). Ово може подразумевати и њихово прикупљање ради утврђивања проблема у мрежи и њеног тестирања, а може се и злоупотребити ради крађе података и поверљивих информација. У овој конкретној симулацији се показује како се *Wireshark* може искористити да се надгледају пакети који пролазе кроз незаштићену мрежу, мрежу без енкрипције, као и да се „ухвате" поверљиви подаци као што су корисничко име и лозинка за приступ неком веб серверу, а затим се показују могућности *IPSec* протокола и *IPSec VPN* тунела за спречавање прикупљања тих података тако што се сви подаци између конифигурисаних уређаја шаљу криптовано.

5. ЗАКЉУЧАК

Рачунарске мреже су саставни део свих активности данашњице, начина како комуницирамо, учимо, послујемо, забављамо се, једном речју саставни део начина како живимо. Зато оне представљају све видљивију, а тиме и све осетљивију мету сајбер напада. Сваки уређај, био он мрежни или крајњи мора бити заштићен.

Данас свако мора бити свестан значаја безбедности рачунарских мрежа, а посебно је важно да што већи број стручњака буде обучено у тој области. Захваљујући *open source* алатима, то је изводљиво у све већем обиму. Постојање заједница које раде на усавршавању тих алата чини их доступним за образовање.

У овом раду су коришћени мрежни емулатор *GNS3* и анализатор протокола *Wireshark* за симулацију напада на рачунарску мрежу и реализацију одбране од њих. Представљени су напади на 2. слоју у приступном делу мреже. Показано је да уз познавање природе напада може ефикасно од напада да се одбрани. Одабрани су они

напади који су најчешћи и чијим се спречавањем онемогућава реализација напада који се на њих могу надовезати.

6. ЛИТЕРАТУРА

[1] Zajeganović M., Zajić G., Kurbalija N., Pavlović M., Čabarkapa S. (2019) *Encription types overview*. 14th International conference on Risk and safety engineering. Kopaonik. Serbia. ISBN 978-86-6211-116-6

[2] Stallings, W. (2014): *Osnove bezbednosti mreža: aplikacije i standardi*, Beograd: CET

[3] Mitić M., Zajeganović M., Kurbalija N., Čabarkapa S., Pavlović M. (2020) *Web server security*. 15th International conference on Risk and safety engineering. Kopaonik. Serbia. ISBN 978-86-6211-124-1

[4] https://www.wireshark.org/download/docs/user-guide.pdf

[5] https://docs.gns3.com/docs/