КОМИСИЈИ ЗА СТУДИЈЕ II СТЕПЕНА ЕЛЕКТРОТЕХНИЧКОГ ФАКУЛТЕТА У БЕОГРАДУ

Комисија за студије II степена, Електротехничког факултета у Београду, на својој седници одржаној 06.06.2023. године именовала нас је у Комисију за преглед и оцену мастер рада дипл. инж. Александра Ћирића под насловом „Практична имплементација решења за мрежну безбедност у симулатору мрежног окружења". Након прегледа материјала Комисија подноси следећи

И З В Е Ш Т А Ј

1. Биографски подаци кандидата

Александар Ћирић је рођен 08.09.1997. године у Београду. Завршио је основну школу „Јанко Веселиновић" у Београду као вуковац. Уписао је Трећу београдску гимназију у Београду у септембру 2012. године коју је завршио са одличним успехом. Електротехнички факултет уписао је 2016. године. Дипломирао је на одсеку за Телекомуникације и информационе технологије, модулу Системско инжењерство, 2021. Дипломски рад, на тему „Експериментална анализа и поређење RIP, OSPF i EIGRP протокола рутирања", одбранио је у мају 2021. године са оценом 10. Дипломске академске – мастер студије на Електротехничком факултету у Београду, на модулу Информационо комуникационе технологије уписао је у октобру 2021. године.

2. Извештај о студијском истраживачком раду

Кандидат Александар Ћирић је као припрему за израду мастер рада урадио истраживање релевантне литературе која се односи на област којој припада тема мастер рада. Конкретно, анализирани су постојећи проблеми и решења у области мрежне безбедности, основни протоколи и сервиси коришћени у ове сврхе, као и радно окружење и могућности *Cisco Packet Tracer* алата за мрежну симулацију. Истраживањем области утврђено је да постоји велики број опасности по сигурност и интегритет мрежног система, одакле можемо закључити да је обезбеђивање мреже неопходан корак у њеном очувању. Такође, утврђени су основни системи који се могу користити у ове сврхе, а то су: *Secure Shell* (SSH), *Access Control List* (ACL), *Zone-based Policy Firewall* (ZPF) и *IPsec VPN* тунел. Овим техникама се обезбеђује слојевита заштита и контрола приступа мрежи.

3. Опис мастер рада

Мастер рад обухвата 52 стране са укупно 19 слика, 14 табела и 15 референци. Рад садржи увод, 3 поглавља и закључак (укупно 5 поглавља), као и списак коришћене литературе, слика, табела и скраћеница.

Прво поглавље представља увод у коме је приказан проблем мрежне безбедности, затим су укратко споменути протоколи који су обрађивани и коришћени у раду, као и опис *Cisco Packet Tracer* алата.

У другом поглављу је описан развој и напредак мрежних технологија, као и претњи овим технологијама које се јављају у пракси. Приказани су различити типови нападача, неке од коришћених техника за напад на мрежну инфраструктуру, као и методологија приступа извршилаца напада.

У трећем поглављу су детаљно представљени *Secure Shell* (SSH), *Access Control List* (ACL), *Zone-based Policy Firewall* (ZPF) и *IPsec VPN* тунел технике заштите. Дата је

теоријска основа ових система, као и објашњење и приказ синтаксе коришћене за њихово конфигурисање и пуштање у рад.

Четврто поглавље приказује и описује мрежну топологију у симулационом окружењу *Cisco Packet Tracer* алата, која је коришћена за представљање рада система за заштиту. У овом поглављу је приказана синтакса за заштиту симулиране мреже и показани су постигнути резултати.

Шесто поглавље је закључак у оквиру кога је описан значај ефикасне имплементације мера мрежне безбедности, као и значај сваког појединачног протокола описаног у раду.

4. Анализа рада са кључним резултатима

Мастер рад дипл. инж. Александра Ћирића се бави приказом начина активирања заштитних система, њихове основне сврхе и практичном демонстрацијом рада целог система. Технике заштите којима је посвећено највише пажње у раду се пре свега односе на успостављање безбедног посредног приступа самим уређајима ради њихове конфигурације коришћењем *Secure Shell* (SSH) криптованог приступа. Након тога, приказан је начин формирања листе за контролу приступа (*Access Control List* - ACL), које представљају листе са информацијама о нивоу приступа различитим сегментима мреже. Затим је имплементиран *Zone-based Policy Firewall* (ZPF), који служи као филтер пакета који се размењују између различитих зона мреже. И на крају је коришћењем IPsec VPN тунела приказан и омогућен *remote* приступ уређају који је „физички" ван мреже, односно приступ мрежи успостављен посредством јавне мреже.

Анализа је спроведена пре свега имплементацијом целог система у симулатору мрежног окружења *Cisco Packet Tracer*, коришћењем мода рада у „реалном времену", након чега је у „симулационом моду" приказан изглед и проток пакета који се размењују

Основни доприноси рада су: 1) приказ рада и начина имплементације протокола и процедура заштите; 2) тестирање рада протокола и механизама заштите; 3) практична имплементација топологија за приказ рада протокола и механизама заштите, која може бити коришћена и у сврхе учења и за лабораторијске вежбе.

5. Закључак и предлог

Кандидат Александар Ћирић је у свом мастер раду успешно реализовао имплементацију протокола заштите у оквиру симулиране мрежне топологије и приказао њихов рад. Урађена анализа и имплементација потребних система за заштиту мреже показује разумевање значаја и начина рада безбедносних мрежних система.

Кандидат је исказао самосталност и систематичност у своме поступку као и способност за практичан рад спровођењем практичне имплементације протокола заштите.

На основу изложеног, Комисија предлаже Комисији за студије II степена Електротехничког факултета у Београду да рад дипл. инж. Александра Ћирића прихвати као мастер рад и кандидату одобри јавну усмену одбрану.

Београд, 08.12.2023. године

Чланови комисије:

Др Младен Копривица, доцент

Др Александра Смиљанић, редовни професор