УНИВЕРЗИТЕТ У БЕОГРАДУ - ЕЛЕКТРОТЕХНИЧКИ ФАКУЛТЕТ
Булевар краља Александра 73, 11000 Београд, Србија
Тел. 011/324-8464, Факс: 011/324-8681

КОМИСИЈИ ЗА СТУДИЈЕ II СТЕПЕНА ЕЛЕКТРОТЕХНИЧКОГ ФАКУЛТЕТА У БЕОГРАДУ

Комисија за студије II степена Електротехничког факултета у Београду, на својој седници одржаној 11.06.2019. године, именовало нас је у Комисију за преглед и оцену мастер рада кандидата Душана Дринића, дипл. инж. Електротехнике и рачунарства, под насловом „Анализа метода детекције и симулација ботнет мреже". Након прегледа материјала комисија подноси следећи

И З В Е Ш Т А Ј

1. Биографски подаци кандидата

Душан Дринић је рођен 23.10.1993. године у Београду. Завршио је основну школу "Радојка Лакић" у Београду као одличан ђак. Уписао је Гиманзију „Свети Сава" у Београду коју је завршио са одличним успехом. Електротехнички факултет уписао је 2012. године. Дипломирао је на одсеку за Телекомуникације и информационе технологије – смер Системско инжењерство 2017. године са просечном оценом 8,26. Дипломски рад одбранио је у августу 2017. године са оценом 10. Мастер студије на Електротехничком факултету у Београду, на Модулу Системско инжењерство и радио комуникације уписао је у октобру 2017. године.

2. Опис мастер рада

Мастер рад обухвата 40 страна, са укупно 30 слика, 6 табела и 16 референци. Рад садржи увод, 4 поглавља, закључак (укупно 6 поглавља), списак коришћене литературе, и списак скраћеница.

Предмет рада представља преглед и анализу постојећих метода за детекцију ботнет мрежа, као и симулацију једног метода детекције. У раду је дат опис и дефиниција ботнет мреже, а потом су изложени и анализирани постојећи методи детекције ботнет мрежа. У раду су коришћени алати Wireshark, Python, Scapy за потребе симулације којом се демонстрира један од метода детекције кроз практичан пример.

У уводном поглављу описан је проблем ботнет мрежа са становишта безбедности, описан је циљ рада и коришћене методе, а потом је изложена структура остатка рада по поглављима.

У другом поглављу дата је дефиниција ботнет мреже, потом је изложена класификација ботнет мрежа уз детаљан опис сваке класе. На крају је дат историјски преглед најпознатијих ботнет мрежа.

У трећем поглављу је изложена симулациона поставка ботнет мреже. Коришћено је виртуелно окружење за креирање ботмастер сервера и заражених машина. Потом је дат детаљан опис симулације од инсталације потребног софтвера до покретања потребних Python скрипти. На крају је дат пример контроле зараженог рачунара где се јасно види опасност ботнет мреже.

Четврто поглавље се бави методама детекције ботнет мрежа и представља централно поглавље тезе. Наведене су и детаљно описане основне методе детекције, а потом су наведени примери комбиновања основних метода којима се подиже успешност детекције.

У петом поглављу је симулиран пример детекције ботнет мреже. У питању је детекција HTTP ботнет мреже при чему се користи *anomaly-based* метода. Прво је дат кратак опис коришћених алата у симулацији. Сама симулациона поставка је већ описана у поглављу

3. Дат је детаљан опис како метода ради и како се врши детекција, при чему се хватају три критеријума за постојање ботнет мреже. Аларм се генерише само ако су сва три критеријума испуњена, а ако су испуњена само два критеријума генерише се упозорење. На крају су изложени резултати симулације који показују успешност рада методе.

У шестом поглављу су резимирани резултати тезе и наглашен је значај тематике ботнет мрежа и у будућности. Потом је дат списак коришћене литературе и списак скраћеница.

3. Анализа рада са кључним резултатима

Мастер рад Душана Дринића, дипл. инж. Електротехнике и рачунарства, је дао детаљан приказ постојећих метода за детекцију ботнет мрежа, као и класификацију постојећих типова ботнет мрежа. Основни доприноси рада су следећи:

1) детаљна класификација постојећих ботнет мрежа;
2) детаљна класификација постојећих метода детекције ботнет мрежа;
3) дата је симулација једног метода детекције којом се демонстрира и рад самих ботнет мрежа, али и метода детекције.

4. Закључак и предлог

Кандидат Душан Дринић, дипл. инж. Електротехнике и рачунарства, је у свом мастер раду успешно обрадио тему ботнет мрежа и њихове детекције. Душан је показао одлично сналажење у актуелној теми из области мрежне безбедности, као и добро познавање многих алата који је користио у практичном делу тезе. Резултати тезе се могу применити у лабораторијским вежбама које се баве мрежном безбедношћу, као и у пракси за побољшање заштите од ботнет напада. На основу изложеног, Комисија предлаже Комисији за студије II степена Електротехничког факултета у Београду да рад кандидата Душана Дринића, дипл. инж. Електротехнике и рачунарства, прихвати као мастер рад и кандидату одобри јавну усмену одбрану.

Београд, 30.08.2019. године

Чланови комисије:

др Зоран Чича, ванр. професор

др Дејан Драјић, ванр. професор