

SADRŽAJ

1	UVOD	1
1.1	Ciljevi istraživanja i hipoteze	1
1.2	Metode istraživanja.....	2
1.3	Pregled i sadržaj rada.....	3
2	PREGLED POSTOJEĆIH ISTRAŽIVANJA	5
3	TEORIJSKE OSNOVE.....	6
3.1	TCP trostruko rukovanje	6
3.2	HTTP protokol.....	7
3.3	DoS napadi	9
3.3.1	Slowloris/Slowheader.....	10
3.3.2	Slowbody/Slowpost/RUDY	12
3.3.3	Slowread.....	13
4	TEHNOLOGIJE I ALATI KORIŠTENI U REALIZACIJI PROJEKTA	16
4.1	Nginx	16
4.2	Apache	16
4.3	Docker	17
4.4	Slowhttpstest	19
4.5	Zabbix.....	19
5	OPIS KONTROLISANOG TESTNOG OKRUŽENJA	21
6	TEHNIKE NAPADA	23
6.1	Slowloris/Slowheader napad	24
6.2	Slowbody/Slowpost/RUDY napad	25
6.3	Slowread napad.....	25
7	TEHNIKE ODBRANE	27
7.1	Apache.....	27
7.1.1	Vremensko ograničenje trajanja HTTP zahtjeva	27
7.1.2	Vremensko ograničenje trajanja TCP konekcije.....	28
7.1.3	Limitiranje broja konekcija	28
7.2	Nginx	29
7.2.1	Vremensko ograničenje trajanja HTTP zahtjeva	29

7.2.2	Vremensko ograničenje trajanja TCP konekcije.....	30
7.2.3	Limitiranje broja zahtjeva i konekcija.....	31
7.3	Docker	33
8	REZULTATI ISTRAŽIVANJA	34
8.1	Slowheader/Slowloris napad	35
8.1.1	Podrazumijevana konfiguracija.....	35
8.1.2	Izmijenjena konfiguracija.....	37
8.2	Slowbody/Slowpost/RUDY napad.....	39
8.2.1	Podrazumijevana konfiguracija.....	39
8.2.2	Izmijenjena konfiguracija.....	41
8.3	Slowread napad.....	44
8.3.1	Podrazumijevana konfiguracija.....	44
8.3.2	Izmijenjena konfiguracija.....	46
9	ANALIZA I DISKUSIJA.....	49
10	ZAKLJUČAK	51
11	PRILOZI.....	52
11.1	Instalacija Slowhttpstest-a na Ubuntu 22.04	52
11.2	Instalacija Docker-a na Ubuntu 22.04	53
11.3	Instalacija Zabbix-a na Ubuntu 22.04.....	55
11.4	Kreiranje Docker kontejnera i Apache veb server konfiguracija.....	58
11.5	Kreiranje Docker kontejnera i Nginx veb server konfiguracija.....	64
11.6	Docker iptables konfiguracija	69
12	POPIS TABELA	70
13	POPIS SLIKA	71
14	LITERATURA.....	74