

## Analiza i prikupljanje DNS paketa

Vrsta: Diplomski | Broj strana: 60 | Nivo: Fakultet elektrotehnike i računarstva

### Sažetak

Predmet promatranja ovog diplomskog rada je područje DNS protokola vezano uz brojne kritične sigurnosne prijetnje prema DNS poslužiteljima. U radu se razmatra izrada sustava distribuiranog pasivnog prisluškivanja DNS komunikacije uz istovremenu opću i sigurnosnu analizu navedenog prometa, identifikaciju sigurnosnih problema te predstavljanje rezultata korisniku. Uz razradu DNS problematike i pojedinosti sustava za analizu DNS prometa te formalno testiranje sukladnosti standardima, obavljena su i praktična mjerenja na centralnim DNS poslužiteljima Zavoda za elektroniku, mikroelektroniku, računalne i inteligentne sustave Fakulteta elektrotehnike i računarstva u Zagrebu te Fakulteta strojarstva i brodogradnje u Zagrebu.

### Ključne riječi

DNS protokol, DNS trovanje, analiza DNS prometa, sustavi za otkrivanje neovlaštenog upada.

### Abstract

### Keywords

DNS protocol, DNS poisoning, DNS traffic analysis, Intrusion Detection Systems.

### Sadržaj

1. Uvod.....	1	2. Imenički sustav domena.....	3
2.1. Tipovi DNS upita.....	3	2.2. DNS Resource Record.....	6
2.3. Tipovi DNS zapisa.....	7	2.4. DNS upiti i odgovori.....	9
2.5. Tipovi DNS poslužitelja.....	12	2.6. Sigurnosni problemi.....	14
2.7. Metode analize prometa u poslužiteljima.....	15	2.8. Pregled postojećih specijaliziranih alata.....	18
3. Sustav za nadzor i analizu DNS prometa.....	20	3.1. Razrada implementacije.....	21
3.2. Komponente i karakteristike sustava.....	26	3.3. Otkrivanje problematičnog prometa.....	30
3.4. Daljnji rad.....	32	4. Rezultati i razmatranje.....	33
4.1. Formalno testiranje sustava.....	33	4.2. Mjerenja u produkciji i diskusija rezultata.....	35
5. Zaključak.....	47	6. Literatura.....	49
7. Dodatak A: Sadržaj priloženog medija (CD/DVD).....	51	8. Dodatak B: Upute za instalaciju.....	52
9. Dodatak C: Upute za korištenje.....	53	Popis oznaka i kratica	
Popis tablica		Tablica 2.1: Odjeljci u DNS paketu.....	9
Tablica 2.2: Prikaz zaglavlja u DNS paketu.....	10	Tablica 2.3: Polja u odjeljku upita.....	12
Tablica 2.4: Pregled analize prometa u DNS poslužiteljima.....	16	Tablica 2.5: Pregled alata za DNS analizu.....	18
Tablica 4.1: Referentna konfiguracija Bind poslužitelja.....	33	Tablica 4.2: Utjecaj nadzora na DNS performanse.....	35
Tablica 7.1: Sadržaj priloženog medija.....	51	Popis slika	
Slika 2.1: Rezolucija u DN.....		<b>NAMERNO UKLONJEN DEO TEKSTA.....</b>	
Slika 3.2: Arhitekturni prikaz komunikacije u sustavu.....	25	Slika 3.3: Tijek akcija obrade DNS paketa.....	29
Slika 3.4: Međuodnos programskih klasa.....	30	Slika 4.1: Raspodjela ukupnog broja incidenata na FSBU.....	37
Slika 4.2: RFC1918 upiti (privatne adrese).....	38	Slika 4.3: Odgovori na nepostojeće upite.....	38
Slika 4.4: Odgovori različiti od upita.....	39	Slika 4.5: Višestruki odgovori na upit.....	39
Slika 4.6: A-za-A sigurnosni incidenti.....	40	Slika 4.7: Nedoželjeni znakovi u	

upitu.....	40	Slika 4.8: Nepoznati tip		
upita.....	41	Slika 4.9: Povratna pogreška od DNS		
poslužitelja.....	41	Slika 4.10: Nepoznate vršne		
domene.....	42	Slika 4.11: Skupni prikaz zabilježenih incidenata na FSB-		
u.....	43	Slika 4.12: Raspodjela ukupnog broja incidenata na ZEMRIS-u.....	45	Slika
4.13: Skupni prikaz zabilježenih incidenata na ZEMRIS-u.....	46			

**----- OSTATAK TEKSTA NIJE PRIKAZAN. CEO RAD MOŽETE  
PREUZETI NA SAJTU. -----**

[www.maturskiradovi.net](http://www.maturskiradovi.net)

**MOŽETE NAS KONTAKTIRATI NA E-MAIL: [maturskiradovi.net@gmail.com](mailto:maturskiradovi.net@gmail.com)**