

SADRŽAJ

1. UVOD	3
2. SAVREMENE RAČUNARSKÉ MREŽE.....	4
2.1 OSI (OPEN SYSTEMS INTERCONNECTION) MODEL.....	4
2.1.1 FIZIČKI SLOJ (PHYSICAL LAYER).....	5
2.1.2 SLOJ VEZE (LINK LAYER).....	5
2.1.3 MREŽNI SLOJ (NETWORK LAYER)	6
2.1.4 TRANSPORTNI SLOJ (TRANSPORT LAYER).....	6
2.1.5 SLOJ SESIJE (SESSION LAYER)	7
2.1.6 SLOJ PREZENTACIJE (PRESENTATION LAYER)	7
2.1.7 SLOJ APLIKACIJE (APPLICATION LAYER).....	7
3. NAPADI NA RAČUNARSKÉ MREŽE	7
4. VRSTE NAPADA.....	9
4.1 MAN IN THE MIDDLE	10
4.2 PHISHING.....	11
4.3 PHARMING.....	12
4.4 ADVANCED PERSISTENT THREATS	13
4.5 MALWARE.....	14
4.5.1 RAČUNARSKI VIRUSI	15
4.5.2 TROJANCI	15
4.5.3 CRVI.....	15
4.5.4 SPYWARE	16
4.5.5 ROOTKIT	16
4.6 TROVANJE KEŠA DNS SERVERA.....	17
4.7 DDOS (DISTRIBUTED DENIAL OF SERVICE) NAPADI.....	17
4.8 NAPADI NA WEB APLIKACIJE.....	18
4.8.1 NAPADI NA WEB APLIKACIJE UMETANJEM SQL NAREDBI.....	19

4.8.2 XSS (CROSS SITE SCRIPTING) - UNAKRSNO SKRIPTOVANJE.....	19
4.9 NAPADI NA BEŽIČNE MREŽE.....	20
4.9.1 SOFTVERI ZA SKENIRANJE MREŽA, RANJIVOSTI I HVATANJE PAKETA.	21
5. BEZBJEDNOST I TEHNIKE ODBRANE NA MREŽAMA.....	23
5.1 PRIMJENA KRIPTOGRAFSKIH ALGORITAMA U MREŽAMA I SISTEMIMA.....	23
5.1.1 SIMETRIČNI ALGORITMI.....	24
5.1.1.1 BLOKOVSKO ŠIFROVANJE.....	25
5.1.2 ASIMETRIČNI ALGORITMI.....	26
5.2 SIGURNOSNI SERVISI.....	27
5.3 HASH FUNKCIJE.....	28
5.4 DIGITALNI POTPIS I DIGITALNI SERTIFIKATI.....	28
5.5 ZAŠTITA NA APLIKATIVNOM NIVOU.....	30
5.5.1 END TO END ŠIFROVANJE.....	30
5.6 ZAŠTITA NA TRANSPORTNOM NIVOU.....	31
5.7 ZAŠTITA NA MREŽNOM NIVOU.....	32
5.7.1 VIRTUELNE PRIVATNE MREŽE (VPN).....	35
5.8 FIREWALL.....	36
5.8.1 FILTRIRANJE PAKETA.....	37
5.9 SISTEMI ZA OTKRIVANJE I SPRIJEČAVANJE NAPADA.....	37
5.10 METODE ZA POVEĆANJE ZAŠTITE I SIGURNOSTI NA MREŽAMA.....	38
5.11 OKVIR NULTOG POVJERENJA.....	39
5.12 SISTEM ZA UPRAVLJANJE INFORMATIČKOM BEZBJEDNOŠĆU.....	40
6. ZAKLJUČAK.....	42
7. LITERATURA.....	43
8. POPIS SLIKA.....	44