

DIPLOMSKI RAD br. 1684

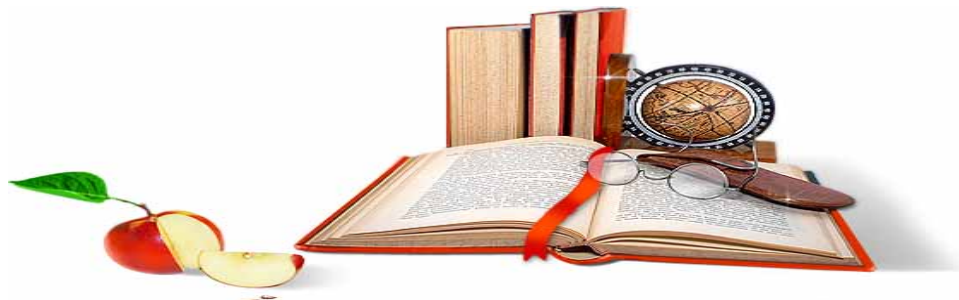
Forenzička analiza računalnog sustava

Sadržaj

1. Uvod	5
2. Forenzičke metode i procedure	6
2.1. Analiza sustava u radnom stanju	6
2.1.1. Prikupljanje i očuvanje dokaza	7
2.2. Analiza sustava <i>post-mortem</i>	11
2.2.1. Izrada forenzičke kopije	11
2.3. Prikupljanje mrežnih dokaza	11
2.4. Analiza prikupljenih podataka	12
2.4.1. Analiza forenzičke kopije	13
2.4.2. Analiza napadačkih programa	16
2.4.3. Analiza mrežnih dokaza	18
2.5. Dokumentiranje rezultata	20
3. Forenzički alati	22
3.1. Forenzički alat <i>PyFlag</i>	22
3.1.1. Korištenje	22
3.1.2. Instalacija	26
3.2. Forenzički alat <i>The Sleuth kit</i>	27
3.2.1. Korištenje	27
3.2.2. Grafičko sučelje <i>Autopsy</i>	37
3.2.3. Instalacija	38
4. Pripreme za analizu slučaja	39
4.1. Podešavanje radne okoline za forenzičku analizu	39
5. Forenzička analiza odabranih slučajeva	46
5.1. Forenzička analiza kompromitiranog GNU/Linux operacijskog sustava	46
5.1.1. Prikupljanje podataka	46
5.1.2. Analiza prikupljenih podataka	49
5.1.3. Zaključak analize slučaja	64
5.2. Analiza dnevnika sigurnosne stijene	64
5.2.1. Analiza korištenjem forenzičkog alata <i>PyFlag</i>	65
5.2.2. Analiza korištenjem baze podataka <i>MySql</i>	67
5.2.3. Zaključak analize slučaja	71
6. Zaključak	72
7. Literatura	73
8. Prilog A: Rezultat pretraživanja datoteke <i>process.lsof</i> za proces <i>3137/smbd</i>	76
9. Prilog B: Rezultat pretraživanja datoteke <i>process.lsof</i> za proces <i>15119/initd</i>	77
10. Prilog C: Rezultat pretraživanja datoteke <i>process.lsof</i> za proces <i>25241,25239/xopen</i>	78
11. Prilog D: Rezultat pretraživanja datoteke <i>process.lsof</i> za proces <i>25247/lsn</i>	79

[GOTOVI SEMINARSKI, DIPLOMSKI I MATURSKI TEKST](#)

**RADOVI IZ SVIH OBLASTI, POWERPOINT PREZENTACIJE I DRUGI EDUKATIVNI
MATERIJALI.**



WWW.SEMINARSKIRAD.ORG

WWW.MAGISTARSKI.COM

WWW.MATURSKIRADOVI.NET

WWW.MATURSKI.NET

NA NAŠIM SAJTOVIMA MOŽETE PRONAĆI SVE, BILO DA JE TO [SEMINARSKI](#), [DIPLOMSKI](#) ILI [MATURSKI](#) RAD, POWERPOINT PREZENTACIJA I DRUGI EDUKATIVNI MATERIJAL. ZA RAZLIKU OD OSTALIH MI VAM PRUŽAMO DA POGLEDATE SVAKI RAD, NJEGOV SADRŽAJ I PRVE TRI STRANE TAKO DA MOŽETE TAČNO DA ODABERETE ONO ŠTO VAM U POTPUNOSTI ODGOVARA. U BAZI SE NALAZE [GOTOVI SEMINARSKI, DIPLOMSKI I MATURSKI RADOVI](#) KOJE MOŽETE SKINUTI I UZ NJIHOVU POMOĆ NAPRAVITI JEDINSTVEN I UNIKATAN RAD. AKO U [BAZI](#) NE NAĐETE RAD KOJI VAM JE POTREBAN, U SVAKOM MOMENTU MOŽETE NARUČITI DA VAM SE IZRADI NOVI, UNIKATAN SEMINARSKI ILI NEKI DRUGI RAD RAD NA LINKU [IZRADA RADOVA](#). PITANJA I ODGOVORE MOŽETE DOBITI NA NAŠEM [FORUMU](#) ILI NA MATURSKIRADOVI.NET@GMAIL.COM