Elektrotehnički fakultet u Beogradu
Katedra za računarsku tehniku i informatiku

Zaštita računarskih sistema i mreža

- Prva laboratorijska vežba -

Analiza paketa i komunikacionih sesija pomoću *Wireshark* alata.

Zadatak. Pomoću *Wireshark* alata otvoriti odgovarajući *.pcapng* fajl i analizirati paket.

a. U fajlu *SNMP.pcapng* pronaći verziju protokola koja se koristi i vrednost *community* parametra.
b. U fajlu *Telnet.pcapng* pronaći *username* i *password* koji se koriste.
c. U fajlu *HTTP.pcapng* pronaći *username* i *password* koji se koriste za pristup sistemu i sadržaj prikazane strane. Po kom portu se odvija ova *HTTP* komunikacija?
d. U fajlu *TLS.pcapng* pronaći koji se algoritmi kriptovanja koriste u svim *TLS* sesijama.
e. U fajlu *SSH.pcapng* pronaći sa kojim uređajem je uspostavljena *SSH* sesija i koji se kriptografski algoritmi koriste za zaštitu te sesije. Koliko je trajala sesija?
f. U fajlu *POP3.pcapng* pronaći *IP* adrese klijenta i mejl servera kojima se klijent obraća putem *POP3* i *IMAP* protokola. Odrediti koji se kriptografski algoritmi koriste za zaštitu ovih protokola.
g. U fajlu *Malware.pcapng* je zabeležena komunikacija jednog bota sa svojim *command and control* centrom kao i početak *DoS* napada.
    i. Opisati način komunikacije bota sa *command and control* centrom koji je na *IP* adresi 45.80.37.176. Koj protokol se koristi za komunikaciju? Kakva je učestalost poruka? Koji je sadržaj poruka? Koja je adresa bota?
    ii. Odrediti trenutak kada počinje napad i opisati napad. Odrediti intenzitet napada. Koja je *IP* adresa žrtve? Po kom portu se napad izvršava?
    iii. Odrediti poruku kojom *command and control* centar zadaje komandu za napad. Koji je to paket po redu i šta je sadržaj komande?