Elektrotehnički fakultet u Beogradu
Katedra za računarsku tehniku i informatiku

Zaštita računarskih sistema i mreža

- Rešenje prve laboratorijske vežbe -

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.
   verzija protokola: `v2c`
   community parametar: `si2019`
b. U fajlu *Telnet.pcapng* pronaći *username* i *password* koji se koriste.
   username: `korisnik`
   password: `veomasigurnalozinka`
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?
   username: `Username`
   password: `Qwi89R12m`
   sadržaj strane: `nalazi se u paketu 168 (lista linkova)`
   port: `443`
d. U fajlu *TLS.pcapng* pronaći koji se algoritmi kriptovanja koriste u svim TLS sesijama.
   algoritmi kriptovanja: `TLS_AES_128_GCM_SHA256, TLS_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256`
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?
   uređaj: `Server: 172.16.0.95 (Ubuntu-4ubuntu2.4)`
   algoritmi kriptovanja: `ECDSA-SHA2 i chacha20-poly1305`
   trajanje sesije: `~6.57 sekundi`
f. U fajlu *POP3.pcapng* pronaći *IP* adrese klijenta i mejl servera kojima se klijent obraća, a potom pronaći algoritme kriptovanja koji se koriste za zaštitu podataka u ovim sesijama.
   klijent: `91.187.154.108`
   server: `147.91.1.120, 147.91.8.8`
   algoritmi kriptovanja: `TLS_RSA_WITH_AES_128_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256`
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?

protokol: TCP
učestalost poruka: poruka se šalje na svakih ~60 sekundi
sadržaj poruka: nije vidljiv
adresa bota: 147.91.72.158

ii. Odrediti trenutak kada počinje napad i opisati napad. Odrediti intenzitet napada. Koja je *IP* adresa žrtve? Po kom portu se napad izvršava?
početak napada: 4813.046
opis napada: zatrpavanje žrtve UDP paketima
intenzitet napada: oko ~18850 paketa u sekundi pri čemu je svaki veličine 554B (9.96MB/s)
IP adresa žrtve: 103.95.221.167
port: 80

iii. Odrediti poruku kojom *command and control* centar zadaje komandu za napad. Koji je to paket po redu i šta je sadržaj komande?
paket: 981
sadržaj: Data: 00120000001e0901675fdda7200107023830
pretvoreno u decimalan oblik bajt po bajt:
0 0 18 0 0 30 9 1 **103 95 221 167** 32 1 7 2 56 48 (sadrži IP adresu žrtve)