HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Analiza cb_PMM programskog alata

CCERT-PUBDOC-2003-05-20

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

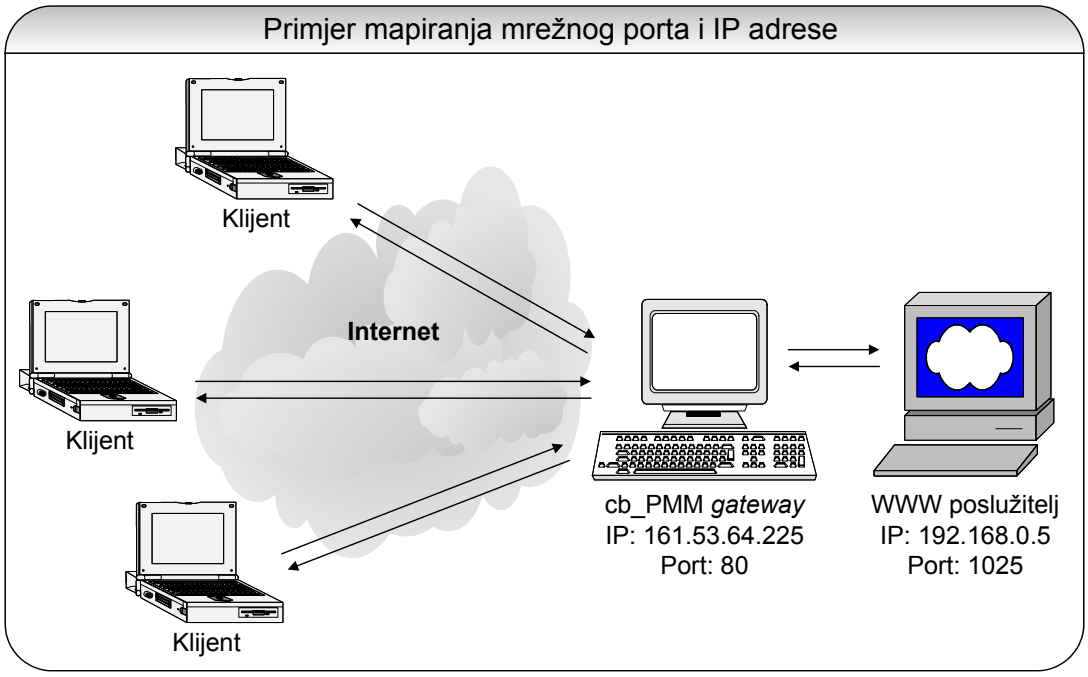
CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Cb_PMM je mrežni programski alat s dvije osnovne funkcije. Prva je mapiranje TCP portova i IP adresa, a druga praćenje TCP konekcija.
Mapiranje mrežnih portova omogućava prosljeđivanje konekcija, upućenih na određenu IP adresu i mrežni port na neki drugi port i IP adresu. Ova funkcija omogućava programu cb_PMM da radi kao *gateway* na razini TCP protokola. Gledano sa strane klijenta, mapiranje mrežnih portova i IP adresa je posve transparentno.
Primjer mapiranja mrežnih portova i IP adresa prikazan je na sljedećoj slici (Slika 1).



Slika 1: Primjer mapiranja mrežnog porta i IP adrese

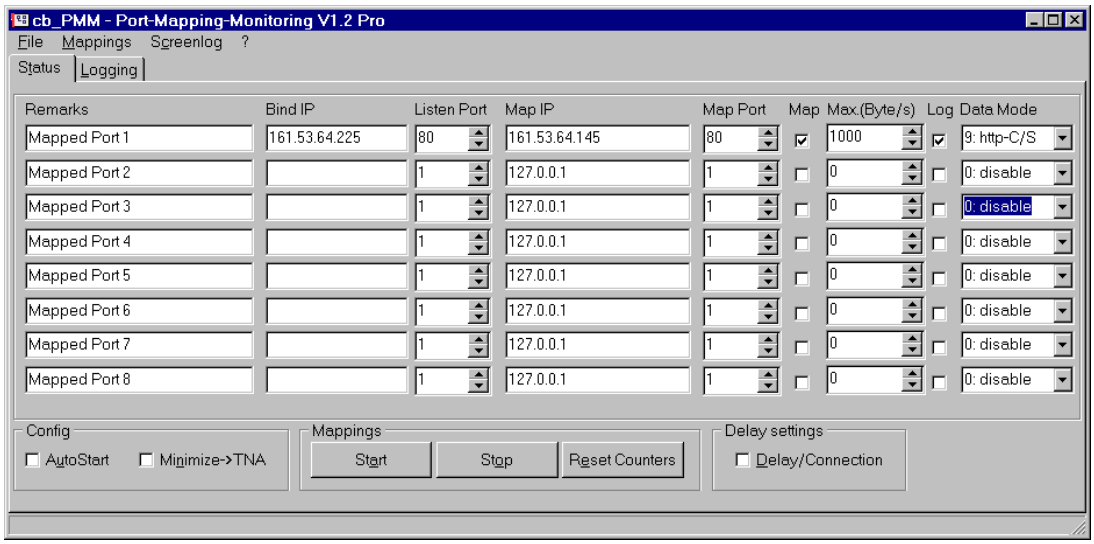
U primjeru sa slike, računalo na kojem je instaliran cb_PMM programski alat spojeno je na Internet i ima javnu IP adresu 161.53.64.225. Klijenti s Interneta svoje Web zahtjeve šalju na tu adresu i port 80. Program cb_PMM prima sve pakete s odredišnim portom 80 i prosljeđuje ih na privatnu IP adresu 192.168.0.5 na kojoj je pokrenut Web poslužitelj na portu 1025. U navedenom primjeru se program cb_PMM koristi kao *gateway* prema Internetu za WWW poslužitelj pokrenut na lokalnoj mreži.
Program cb_PMM omogućava simultano mapiranje do osam mrežnih portova i IP adresa. Isto tako, za svaku mapiranu konekciju moguće je odrediti najveću propusnost prijenosa podataka. Ova se funkcija može koristiti za simuliranje sporih TCP konekcija.
Druga funkcija programa cb_PMM je praćenje mrežnog prometa i zapisivanje TCP podataka koji su prošli kroz mapirane konekcije. Podaci se mogu pratiti u stvarnom vremenu ili se mogu snimati u log datoteke. Program omogućava praćenje svih podataka sadržanih u TCP paketu. Za prikazivanje podataka koji se prate moze se koristiti obican ASCII prikaz ili heksadecimalni prikaz.

2. Instalacija

Cb_PMM programski alat može se skinuti s Interneta na Web adresi http://www.creativebytes.net/cb_PMM/download.htm, u obliku zip arhive u kojoj se nalazi izvršna datoteka programa. Nakon otpakiranja zip arhive nije potrebno pokretati nikakvu dodatnu instalaciju programa.

3. Konfiguracija i pokretanje

Nakon pokretanja programa otvara se konfiguracijski prozor (Slika 2) u kojem je potrebno podesiti parametre koji se odnose na IP adrese i portove koje se želi mapirati.



Slika 2: Prozor za konfiguraciju

U ovom je prozoru potrebno upisati IP adrese i brojeve mrežnih portova koji se žele mapirati. Podaci koje je potrebno upisati su sljedeći:

- Remarks – ovo je proizvoljan parametar i nije ga potrebno mijenjati. Tu se može upisati ime mapirane konekcije radi kasnije lakše administracije.
- Bind IP - ovdje se upisuje IP adresa s koje se promet preusmjerava na mapiranu IP adresu.
- Listen Port – broj porta koji se preusmjerava.
- Map IP – IP adresa na koju se preusmjerava mrežni promet.
- Map Port – port na koji se preusmjerava mrežni promet.
- Map – uključuje ili isključuje preusmjeravanje mrežnog prometa za određeni par IP adresa (adresa na koju promet dolazi i adresa na koju se promet preusmjerava).
- Max.(Byte/s) – određuje maksimalni promet (propusnost) preko mapirane IP adrese. Ova opcija se može koristiti za simuliranje spore mreže. Ako je ova opcija postavljena na 0 tada mrežni promet nije ograničen.
- Log – ovom opcijom se uključuje ili isključuje praćenje (logiranje) mrežnog prometa pripadajućeg para IP adresa.
- Data Mode – ovom se opcijom određuje način logiranja sadržaja TCP paketa.
- AutoStart – ako je ova opcija uključena, mapiranje IP adresa će biti pokrenuto odmah prilikom pokretanja programa.
- Minimize -> TNA – ako je ova opcija uključena, prilikom pokretanja programa biti će pokrenuto i mapiranje IP adresa, a program će se pokrenuti minimiziran u *Tray* sustava.
- Delay/Connection – ukoliko je ova opcija uključena, ograničenja na propusnost definirana opcijom Max.(Byte/s) se primjenjuju na svaku pojedinu TCP konekciju zasebno. To znači da, ukoliko je ograničenje propusnosti za neki par IP adresa postavljeno na 500B/s, tada će maksimalna propusnost za svaku TCP konekciju koja ide preko tih IP adresa biti 500B/s. Ako je ova opcija isključena, tada će ukupna propusnost za sve konekcije zajedno biti 500B/s.

Cb_PMM podržava nekoliko načina logiranja (zapisivanja) sadržaja mrežnog prometa. Načini logiranja koji se mogu koristiti su:

- Disable – ne zapisuju se podaci iz TCP paketa. Prati se samo statistika mrežnog prometa za konekciju, tj. zapisuje se samo informacija o količini primljenog i poslanog prometa.
- Char – podaci se zapisuju u običnom ASCII formatu (nema nikakvog dodatnog filtriranja).
- ASCII – zapisuju se samo podaci sa znakovima koji se mogu prikazati na ekranu (posebni znakovi se izbacuju).
- ASCII+ - isto kao i ASCII način zapisivanja, samo što se posebni znakovi zamjenjuju točkom ('.').
- Hex – podaci se bilježe u heksadecimalnom prikazu.

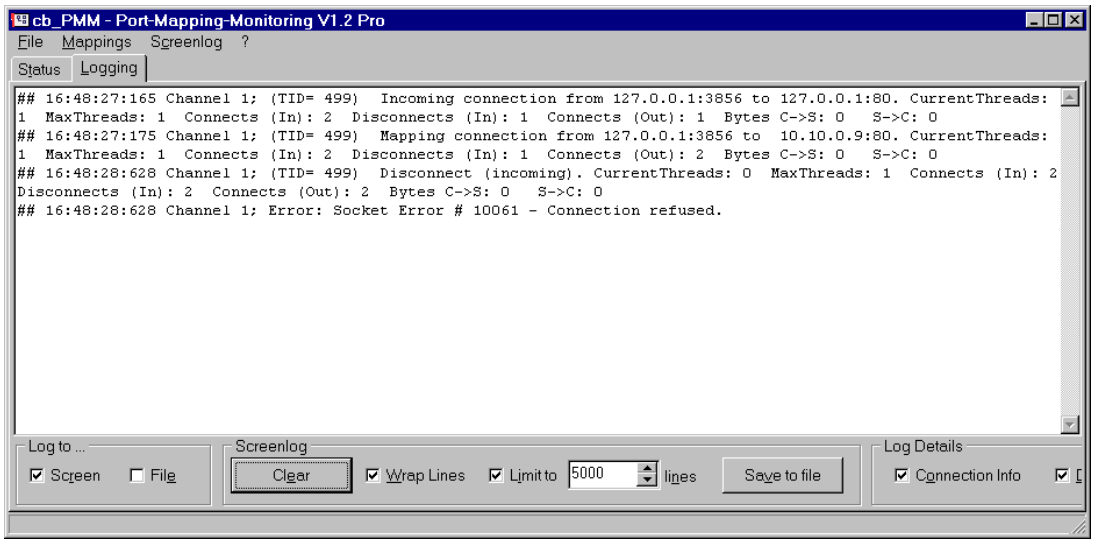
- Auto – ako se primljeni podaci nalaze u opsegu definiranom ASCII znakovima (znakovi koji se mogu prikazati na ekranu), tada se oni bilježe kao ASCII znakovi. U protivnom, podaci se bilježe u heksadecimalnom prikazu.
- http-H – bilježe se samo zaglavlja HTTP paketa.
- http-C – bilježe se samo zaglavlja i podaci HTTP paketa primljenih od klijenta.
- http-S – bilježe se samo zaglavlja i podaci HTTP paketa koje šalje poslužitelj.
- http-C/S – bilježi se cjelokupni HTTP promet.

Nakon sto su podešeni svi parametri, postavljena konfiguracija se može snimiti u datoteku (opcija `File->Save Config`).

Mapiranje IP adresa se pokreće odabirom opcije `Start`, a može se zaustaviti opcijom `Stop`. Opcija `Reset Counters` poništava brojače koji prate količinu poslanog i primljenog prometa za svaki par mapiranih IP adresa.

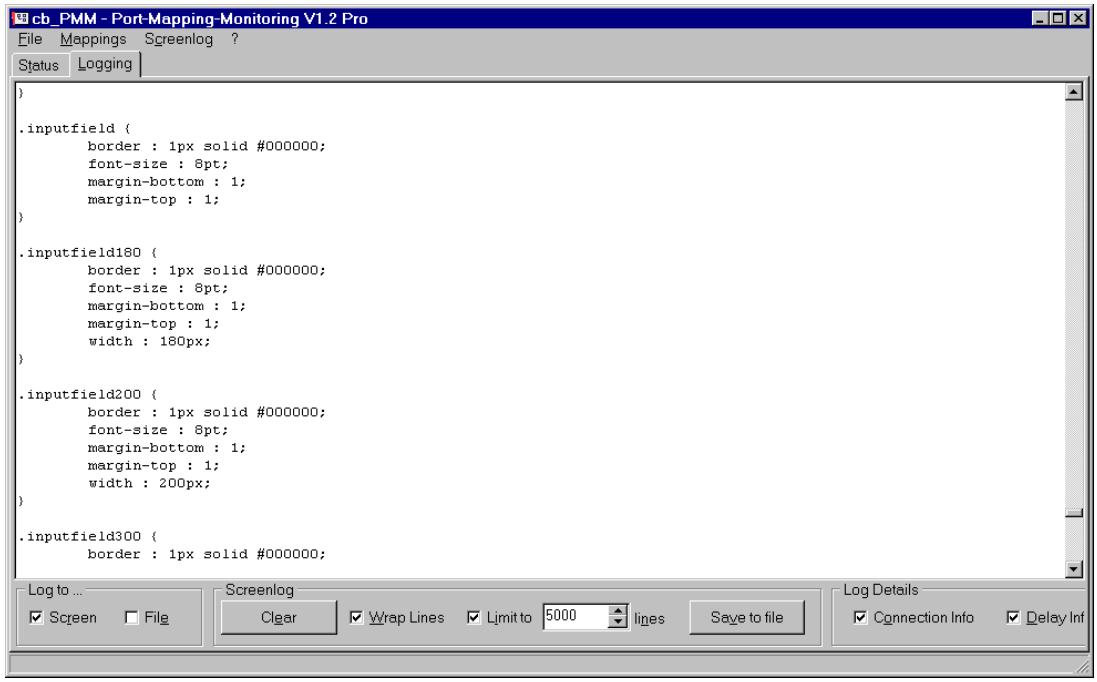
4. Mogućnosti programa

Program cb_PMM je u stanju mapirati i pratiti maksimalno osam IP adresa i mrežnih portova. Nakon što je pokrenut, ovisno o podešenoj konfiguraciji, program preusmjerava promet između mapiranih IP adresa i bilježi podatke o primljenim TCP paketima. Podaci o mrežnom prometu mogu se pohranjivati izravno u datoteku, ili se mogu prikazivati unutar cb_PMM programa (opcija `Screenlog`, Slika 3).

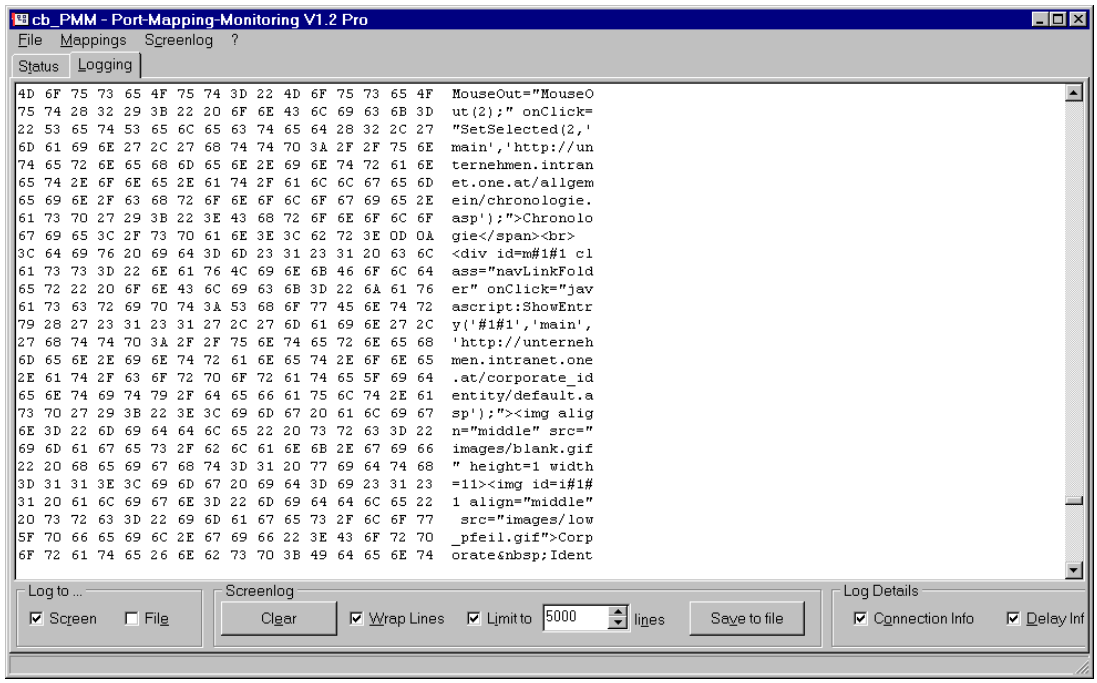


Slika 3: Prikaz prikupljenih podataka unutar programa cb_PMM

Ovisno o odabranom modu bilježenja prikupljenih podataka iz TCP paketa, podaci će biti zabilježeni u ACSII ili heksadecimalnom obliku (Slika 4 i Slika 5).



Slika 4: ASCII prikaz



Slika 5: Heksadecimalni prikaz

Podaci prikazani na ekranu se u bilo kojem trenutku mogu pohraniti u datoteku odabirom opcije `Save to file`. Osim bilježenja samih podataka iz TCP paketa, moguće je uključiti i bilježenje podataka o konekcijama (opcija `Connection info`) i podataka o kašnjenju TCP paketa (`Delay info`).

5. Zaključak

Program cb_PMM omogućava simultano mapiranje do osam mrežnih portova i IP adresa. Isto tako, za svaku mapiranu konekciju moguće je odrediti najveću propusnost prijenosa podataka. Ova se funkcija može koristiti za simuliranje sporih TCP konekcija.

Drugu funkciju cb_PMM programa predstavlja praćenje mrežnog prometa i zapisivanje TCP podataka koji su prošli kroz mapirane konekcije. Podaci se mogu pratiti u stvarnom vremenu ili se mogu snimati u log datoteke. Program omogućava praćenje svih podataka sadržanih u TCP paketu, a moguće je i odabrati praćenje i prikaz samo određenih dijelova TCP paketa, kao što su zaglavlje ili podatkovni dio.