HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Analiza p0f alata

CCERT-PUBDOC-2003-09-41

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

P0f je alat za pasivno identificiranje (engl. *fingerprinting*) operacijskih sustava na udaljenim računalima. Za razliku od aktivne identifikacije operacijskih sustava, prilikom koje alati za identifikaciju udaljenim računalima šalju specifične pakete i na temelju njihovog odgovora prepoznaju operacijski sustav, tehnika pasivne identifikacije temelji se na analizi paketa koje udaljeno računalo i računalo na kojemu se nalazi alat razmjenjuju prilikom uobičajene komunikacije. Činjenica da ovakav način identifikacije ne generira nikakav dodatan promet čini taj proces nemogućim za detektiranje od strane IDS sustava.

Zahvaljujući određenim razlikama unutar TCP/IP stoga, koje su prisutne između različitih operacijskih sustava, ovakva metoda analize pokazala se kao prilično precizna. Dodatni podaci o udaljenosti računala koje se identificira mogu pomoći pri prikupljanju podataka o konfiguraciji udaljene mreže, tj. identifikaciji vatrozida ili maskiranja IP adresa.

P0f je jedan od prvih alata koji primjenjuje tehniku pasivnog identificiranja operacijskih sustava. U odnosu na prvu inačicu, napisanu 2000. godine, trenutna inačica (2.0) napisana je potpuno iznova i donosi niz poboljšanja.

Kao najvažnija poboljšanja u novijoj inačici mogu se navesti brži i stabilniji programski kod, napredna identifikacija IP maskiranja, identifikacija medija kojim je udaljeno računalo povezano s Internetom te reorganizirana baza "potpisa" na temelju kojih se vrši identifikacija.

2. Instalacija i konfiguracija

Za uspješnu instalaciju p0f-a, na Linux i Unix sustavima potrebno je imati sljedeće pakete:

- Libpcap 0.4 ili noviji
- GNU cc 2.7.x ili noviji
- GNU make 3.7x ili noviji (moguće je koristiti i BSD inačicu make-a)
- GNU bash, awk, grep, sed i textutils pakete

Na Unix operacijskim sustavima program se iz izvornog koda prevodi jednostavnim pokretanjem Build skripte koja se nalazu u korijenskom direktoriju p0f paketa. Build skripta će pokušati identificirati tip operacijskog sustava, i na temelju toga pokrenuti prevođenje aplikacije pomoću jedne od odgovarajućih Makefile datoteka iz mk/ direktorija.

Nakon prevođenja, p0f se pokreće iz naredbenog retka. Sve opcije koje je moguće koristiti prilikom pokretanja ovog programa detaljno su opisane unutar README datoteke, koja se nalazi u istom direktoriju.

Kod Windows operacijskog sustava potrebno je imati instaliran paket WinPCAP 3.0 ili noviji (http://winpcap.polito.it/). Nakon instalacije WinPCAP-a, p0f se jednostavno kompilira prema uputama danima u datoteci INSTALL.Win32, koja dolazi u paketu s izvornim kodom programa i također se pokreće u naredbenom retku konzole sustava.

Potrebno je naglasiti da Windows inačica, iako posjeduje sve funkcionalnosti kao i Unix inačica, ne podržava poslužiteljski način rada i ne odgovara na upite, što čini nemogućim njenu integraciju sa ostalim aplikacijama.

Ispravan rad p0f-a uspješno je ispitan na sljedećim operacijskim sustavima:

- NetBSD
- FreeBSD
- OpenBSD
- MacOS X
- Linux (jezgra 2.0 ili više)
- Solaris (2.6 ili više)
- Microsoft Windows
- AIX

3. Rad s p0f-om

Uobičajeno ponašanje pokrenutog alata je praćenje svih dolaznih konekcija i identifikacija sustava koji pokušavaju uspostaviti vezu s računalom. Pri tome se izlaz ispisuje na ekranu, a može se pohraniti i u datoteku, ukoliko je to potrebno za kasniju analizu.
Primjer:

```
# ./p0f
p0f - passive os fingerprinting utility, version 2.0.1
(C) M. Zalewski <lcamtuf@coredump.cx>, W. Stearns
<wstearns@pobox.com>
p0f: listening on 'eth0', 160 fingerprints, rule: 'any'.
161.53.64.3:34171 - Linux 2.4/2.6 (up: 1316 hrs)
  -> 161.53.64.145:80 (distance 0, link: ethernet/modem)
161.53.64.246:4293 - Windows 2000 SP4, XP SP1 (2) (firewall!)
  -> 161.53.64.145:80 (distance 0, link: ethernet/modem)
161.53.64.246:4294 - Windows 2000 SP4, XP SP1 (2) (firewall!)
  -> 161.53.64.145:80 (distance 0, link: ethernet/modem)
161.53.64.246:4297 - Windows 2000 SP4, XP SP1 (2) (firewall!)
  -> 161.53.64.145:110 (distance 0, link: ethernet/modem)
161.53.64.145:37302 - Linux 2.4/2.6 (up: 142 hrs)
  -> 161.53.64.246:113 (distance 0, link: ethernet/modem)
161.53.64.121:1265 - Windows XP Pro SP1, 2000 SP3
  -> 161.53.64.145:139 (distance 0, link: ethernet/modem)
161.53.64.246:4340 - Windows 2000 SP4, XP SP1 (2) (firewall!)
  -> 161.53.64.145:110 (distance 0, link: ethernet/modem)
161.53.64.145:37303 - Linux 2.4/2.6 (up: 142 hrs)
  -> 161.53.64.246:113 (distance 0, link: ethernet/modem)
161.53.64.246:4389 - Windows 2000 SP4, XP SP1 (2) (firewall!)
  -> 161.53.64.145:22 (distance 0, link: ethernet/modem)
```

3.1. SYN+ACK identifikacija

Pomoću –A opcije, p0f se pokreće u SYN+ACK načinu rada, u kojem alat pokušava identificirati operacijske sustave na koje se računalo na kojem je pokrenut pokušava spojiti. U ovakvom načinu rada, p0f koristi posebnu bazu "potpisa" koja se nalazi u datoteci `p0fa.fp`.
Primjer:

```
[root@cecilija p0f]# ./p0f -A
p0f - passive os fingerprinting utility, version 2.0.1
(C) M. Zalewski <lcamtuf@coredump.cx>, W. Stearns
<wstearns@pobox.com>
p0f: listening on 'eth0', 3 fingerprints, rule: 'any'.
161.53.64.249:80 - Linux 2.4 (firewall!) (up: 96 hrs)
  -> 161.53.64.145:37305 (distance 0, link: ethernet/modem)
161.53.64.3:80 - Linux 2.4 (up: 1317 hrs)
  -> 161.53.64.145:37306 (distance 0, link: ethernet/modem)
161.53.64.31:80 - UNKNOWN
[S12:128:1:64:M1460,N,W0,N,N,T0,N,N,S:A:?:?]
  -> 161.53.64.145:37307 (link: ethernet/modem)
```

Potrebno je napomenuti kako je preciznost ovakvog načina identifikacije, zbog vrlo šture baze potpisa, mnogo manja nego kod normalnog načina rada.

3.2. RST+ACK identifikacija

Treći način rada kojeg p0f podržava je RST+ACK/RST način rada, koji se omogućuje korištenjem opcije –R. U ovom načinu rada program će pokušati identificirati operacijske sustave udaljenih računala iz tri različita tipa prometa. Identificirana će biti računala na koje se računalo na kojem je pokrenut p0f

nije uspjelo spojiti ("*Connection Refused*"), konekcije koje su rezultirale *timeout*-om i sva računala koja odbacuju ili ne prepoznaju ACK pakete pri uobičajenoj komunikaciji.
Ovakav način rada, iako vrlo sličan prethodno opisanom (SYN+ACK), još uvijek nije u potpunosti implementiran, pa njegovo korištenje trenutno nije moguće.

3.3. Analiza snimljenog prometa

P0f omogućuje i naknadnu analizu prometa snimljenog pomoću tcpdump programa. Pomoću opcije `-s`, programu se specificira put do datoteke u kojoj je spremljena snimka prometa. Ovakav način rada koristan je kod forenzičke analize kompromitiranih računala.

4. Dodatne mogućnosti

4.1. Generiranje izvještaja

Za lakšu analizu izlaznih rezultata p0f-a, moguće je koristiti generator izvještaja koji dolazi u paketu sa programom. Generator se pokreće naredbom `p0frep` i omogućuje izvršavanje jednostavnih operacija poput sortiranja nad bilo kojom datotekom u koju je spremljen izlazni rezultat p0f aplikacije.
Sintaksa ove naredbe je sljedeća:

```
# ./p0frep logfile.txt sortby [ 'ipmask' 'sysmask' ]
```

pri čemu je značenje parametara redom:

- `logfile.txt` – datoteka u koju su pohranjeni izlazni rezultati identifikacije sustava;
- `sortby` – način na koji će se podaci razvrstati. Moguće opcije su `system` i `addr`, koje listu razvrstavaju po identificiranom tipu sustava, odnosno IP adresi udaljenog računala;
- `ipmask` – filtar (maska) za prikaz IP adresa. Npr. vrijednost 192.168.0 omogućiti će prikazivanje isključivo onih rezultata koji u sebi sadrže IP adresu podmreže 192.168.0;
- `sysmask` – filtar za prikaz operacijskih sustava. Primjena filtra identična je kao kod `ipmask` opcije.

4.2. Detekcija IP maskiranja

Ova inačica p0f alata u sebi ima ugrađenu mogućnost detekcije IP maskiranja. Koristeći opciju `-M`, programu se nalaže da analizom dolaznih upita pokuša uočiti da li se određene mreže, pomoću IP maskiranja, kriju iza jedne IP adrese. Na osnovu analize više faktora, p0f generira vrijednost koja označava vjerojatnost da se iza IP adrese krije više računala.
Sljedeći faktori utječu na generiranu vrijednost:

- razlike u "potpisima" operacijskog sustava detektiranim na istoj IP adresi:
  -3 boda za identičan operacijski sustav
  +4 boda za različit potpis istog tipa operacijskog sustava
  +6 bodova za detektirane različite operacijske sustave s iste adrese
- Detektirane NAT i zastavice vatrozida:
  +4 boda za različite NAT zastavice pronađene kod istih "potpisa"
  +4 boda za različite zastavice vatrozida pronađene kod istih "potpisa"
  +1 bod za svaku NAT i zastavicu vatrozida kod različitih "potpisa"
- Razlika u detektiranom tipu veze na Internet:
  +4 boda za svaki različiti medij uočen na istoj IP adresi
- Razlika u udaljenosti izvornog računala:
  +1 bod za svaku različitu udaljenost koja se detektira
- Vrijeme proteklo od prethodnog pojavljivanja

Konačni rezultat računa se po formuli zbroj bodova * 200 / 23 i iskazuje se kao postotak ukupne vjerojatnosti da se iza IP adrese krije maskirana mreža.
Što je dobivena vrijednost veća, veća je i pouzdanost ispravne identifikacije. Budući da se dobiveni rezultat množi sa 200 i nakon toga dijeli sa 23 (što predstavlja maksimalan broj bodova), mogući su i

nerealni ishodi od preko 100%, ali takve vrijednosti su vrlo rijetke. Preporučuje se provjeriti sve ishode veće od 0%, dok se rezultati preko 20% mogu smatrati sigurnom procjenom.
Opcijom –T (*treshold*) podešava se prag vjerojatnosti nakon kojega će p0f prijaviti detektirano maskiranje IP adresa. Na taj način vrlo je lako filtrirati lažno detektirane slučajeve. Razumna vrijednost –T parametra bila bi 10%.

4.3. Integracija s ostalim aplikacijama

Pof je moguće integrirati i sa ostalim aplikacijama na sustavu te na taj način dinamički upravljati ovlastima pristupa računalu, ovisno o udaljenom operacijskom sustavu koji pokušava pristupiti.
U tu svrhu koristi se –Q opcija prilikom pokretanja aplikacije. Princip integracije je taj da lokalna aplikacija na određeni *socket* šalje podatke koje p0f obrađuje te vraća adekvatan odgovor. Ispitivani paket šalje se na sučelje u obliku posebne `p0f_query` strukture koja se sastoji od sljedećih polja:

- `magic` – vrijednost ovog polja mora biti postavljena na `QUERY_MAGIC`;
- `id` – identifikacijska oznaka upita (umeće se u zaglavlje odgovora);
- `src_ad` – izvorna adresa aplikacije koja šalje upit;
- `dst_ad` – ciljna adresa za odgovor;
- `src_port` – izvorni mrežni port;
- `dst_port` – ciljni mrežni port.

Nakon upita, p0f vraća rezultat identifikacije u odgovoru koji sadrži polja sljedećeg oblika:

- `magic` - vrijednost ovog polja mora biti postavljena na `QUERY_MAGIC`;
- `id` - identifikacijska oznaka odgovora, kopirana iz `id` polja unutar upita;
- `type` – vrsta odgovora – moguće vrijednosti su `RESP_OK`, `RESP_BADQUERY` (označava grešku), `RESP_NOMATCH` (računalo nije identificirano);
- `genre[20]` – tip operacijskog sustava;
- `detail[40]` – inačica operacijskog sustava;
- `dist` – udaljenost identificiranog računala (sadrži vrijednost '-1' u slučaju nepoznate udaljenosti);
- `link[30]` – tip veze s kojom je udaljeno računalo spojeno u mrežu;
- `tos[30]` – informacija o ToS-u;
- `fw`, `nat` – uočen vatrozid ili NAT;
- `real` – polje koje označava da li je paket generiran od strane operacijskog sustava ili nekog posebnog alata za skeniranje mreže
- `score` – rezultat detekcije IP maskiranja
- `mflags` – zastavice koje označavanju način detekcije IP maskiranja

Korisnici OpenBSD sustava u ovom slučaju u mogućnosti su koristiti pf *fingerprinting* alat, koji se temelji na p0f alatu. Pomoću pf-a je moguće, u ovisnosti o identificiranom operacijskom sustavu, preusmjeravati ili blokirati upite sa udaljenih računala.

4.4. Proširivanje baze potpisa

Informacije o formatu u kojem su pohranjeni "potpisi" na temelju kojih se identificiraju operacijski sustavi, kao i sami potpisi, nalaze se u datoteci `p0f.fp`. Opširne upute za kreiranje novih potpisa sadržane u ovoj datoteci potrebno je detaljno proučiti prije nego se izvrši bilo kakvo dodavanje novih zapisa.
Nakon uređivanja datoteke i dodavanja novih otisaka, p0f se pokreće sa opcijom `–C`, kako bi se detektirali eventualni neispravno uneseni potpisi.
Isto pravilo odnosi se i na dodavanje zapisa u `p0fa.fp` i `p0fr.fp` baze, nakon čijeg uređivanja p0f pokrećemo sa opcijama `–A –C` odnosno `–R –C`.
Neidentificirane sustave moguće je prijaviti i programerima koji se brinu za održavanje baze potpisa. Prilikom posjete stranici http://lcamtuf.coredump.cx/p0f-help/, automatski će se uzeti potpis operacijskog sustava koji se koristi za pristupanje i ukoliko se sustav proglasi kao neidentificiran, korisnik će biti zamoljen da unutar Web forme unese detaljne podatke o svojem operacijskom sustavu. Svi prikupljeni potpisi uključivati će se u bazu koja dolazi s p0f-om, poboljšavajući na taj način njegovu preciznost pri identifikaciji sustava.

Tipičan primjer potpisa za Windows 2000 operacijski sustav, u bazi izgleda ovako:

```
# Windows XP and 2000. Most of the signatures that were
# either dubious or non-specific (no service pack data)
# were deleted and replaced with generics at the end.

65535:128:1:48:M*,N,N,S:.:Windows:2000 SP4, XP SP1 (1)
%8192:128:1:48:M*,N,N,S:.:Windows:2000 SP4, XP SP1 (2)
S45:128:1:48:M*,N,N,S:.:Windows:2000 SP4 (2)

S6:128:1:48:M*,N,N,S:.:Windows:XP SP1, 2000 SP4 (1)
S44:128:1:48:M*,N,N,S:.:Windows:XP Pro SP1, 2000 SP3
64512:128:1:48:M*,N,N,S:.:Windows:XP SP1 (2)
32767:128:1:48:M1452,N,N,S:.:Windows:XP SP1 (3)
```

Zapis za svaki otisak je formata :

```
wwww:ttt:D:ss:OOO...:QQ:OS:Details
```

Pri čemu pojedina polja imaju sljedeće značenje:

- `wwww` – veličina TCP prozora,
- `ttt` – inicijalna vrijednost TTL parametra,
- `D` – bit za onemogućavanje fragmentacije paketa (0-isključen, 1-uključen),
- `ss` – ukupna veličina SYN paketa,
- `OOO` – lista dodatnih polja koja se pojavljuju u paketu (detalji se nalaze u `p0f.fp` datoteci),
- `QQ` – lista nepravilnosti i neobičnih vrijednosti određenih polja u paketu, nastalih kao posljedica grešaka u kodu operacijskog sustava. Ovo polje se uglavnom ostavlja prazno.
- `OS` – tip operacijskog sustava,
- `Details` – detalji koji pobliže opisuju inačicu operacijskog sustava.

5. Ograničenja p0f-a

Prilikom upotrebe ovog alata potrebno je biti svjestan i njegovih ograničenja. Poznavanje ovih ograničenja ujedno predstavlja i efikasan način obrane protiv pasivnog identificiranja operacijskih sustava.

Proxy vatrozidi i slični uređaji ponašaju se netransparentno za bilo kakav oblik identifikacije operacijskog sustava putem TCP protokola, budući da se u takvim slučajevima identificira operacijski sustav samog *proxy* vatrozida, a ne računalo koje je izvor paketa. Također, ovaj alat nije moguće primijeniti niti kod klasičnih vatrozida koji imaju omogućenu normalizaciju paketa, jer "potpis" normaliziranog paketa ne odgovara operacijskom sustavu izvornog računala, kao niti operacijskom sustavu vatrozida.

Za uspješnu identifikaciju operacijskog sustava računalo na kojem se nalazi p0f alat mora primiti bar jedan SYN paket koji označava inicijalizaciju TCP veze od strane ispitivanog računala. U slučaju SYN+ACK pregledavanja, računalo sa kojega se testira mora biti u mogućnosti uspješno se spojiti na barem jedan mrežni port na ciljanom računalu kako bi primilo SYN+ACK paket.

Čak i ako je nemoguće uspostaviti vezu s udaljenim računalom jer ono odbija spajanje (odgovara RST+ACK paketima), moguće je identificirati sustav korištenjem `-R` opcije koja predstavlja RST+ACK način pregledavanja. Budući da većina operacijskih sustava ne postavlja posebne parametre unutar RST paketa, svi paketi ovakvog tipa izgledaju vrlo slično, što automatski čini ovu metodu manje preciznom od ostalih.

Kao najmanje precizna vrsta skeniranja smatra se SYN+ACK pregledavanje, zbog njene ovisnosti o sustavu sa kojega se vrši identifikacija.

6. Zaključak

P0f je vrlo brz i efikasan multiplatformski pasivni skener. Korištenje ovog programa oduzima vrlo malo procesorskih resursa, a njegov izvorni kod vrlo je jednostavan i optimiziran. Baza "potpisa" operacijskih sustava koju ovaj program koristi pokazala se kao detaljna i precizna, što naravno znači i

vrlo preciznu identifikaciju operacijskih sustava. Osim toga, bazu je moguće vrlo lako dopuniti vlastitim definicijama otisaka.
Mogućnost integracije p0f-a s ostalim servisima čini ga pogodnim za dinamičko primjenjivanje restrikcija pristupa (ovisno o operacijskom sustavu), što je uz provjeru ranjivosti udaljenih sustava svakako jedna od zanimljivijih primjena p0f-a.