HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Analiza sniffing alata i zaštite

CCERT-PUBDOC-2001-11-06

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. Sažetak

U ovom dokumentu biti će kratko opisani osnovni postupci vezani za proučavanje i analizu Ethernet LAN mrežnog prometa (engl. ethernet sniffing), ili kako se to popularno zove 'snifanje mreže'.

2. Uvod

2.1. Uloga sniffers alata

Mrežni snifferi su programski alati koji omogućuju promatranje Ethernet mrežnog prometa, te bilježenje važnijih podataka, u svrhu njihove kasnije analize.
Spomenuti analizatori Ethernet mrežnog prometa tako predstavljaju vrlo moćan alat za administratore mrežnih sustava, budući da mogu bitno olakšati otkrivanje grešaka kod mrežnih protokola, te njihovo otklanjanje.
Analizom zaglavlja, te sadržaja podatkovnog dijela pojedinih Ethernet paketa, mogu se tako uočiti brojni problemi na različitim mrežnim slojevima, odnosno kod različitih mrežnih protokola, što uvelike može pomoći u otklanjanju grešaka.
No također s druge strane, ovi isti alati se vrlo često koriste u maliciozne svrhe od strane neovlaštenih korisnika, u svrhu dolaska do povjerljivih informacija korisnika, poput korisničkih imena, zaporki, i sl.
Na taj način neovlaštenom korisniku se otvara mogućnost neautoriziranog pristupa resursima sustava, gdje je osnovni cilj dolazak do ovlasti administratora sustava.

2.2. Problemi sniffers alata

Ovakvi alati u pogrešnim rukama, mogu biti puno opasniji nego što se to čini na prvi pogled, pogotovo u okolinama gdje povjerljivost i važnost podataka igraju veliku ulogu.
Naime, ukoliko se ne poduzmu odgovarajuće sigurnosne mjere neovlašteni korisnici na ovaj način mogu doći do korisničkih zaporki administratora sustava, čime im se automatski omogućuje preuzimanje potpune kontrole nad istim.
Također je moguće da se na ovaj način ugrozi rad raznih mrežnih uređaja, poput mrežnih usmjerivača i preklopnika, budući da se analizom mrežnog prometa također može doći do povjerljivih korisničkih imena i zaporki, kojima se omogućuju njihova administracija.
Jednako tako su ugroženi i svi mrežni protokoli na višim mrežnim slojevima, budući da je na ovaj način moguće doći i do povjerljivih informacija kojima se može narušiti integritet njihovog rada, te ugroziti korisnička privatnost.
Sve ove mogućnosti posljedica su činjenice što većina više ili manje iskusnih korisnika ne vodi previše računa o ovim mogućnostima, te ih je jednostavno ignoriraju.
Naime, koristeći razne 'nesigurne' aplikacije i protokole otkrivaju se razne povjerljive korisničke informacije, budući da se one računalnom mrežu šalju u istom obliku kako ih je korisnik unio, znači bez ikakvih dodatnih zaštita.
Servisi poput Telnet-a, FTP-a, HTTP-a, SMB-a, te brojni drugih, svoje podatke računalnom mrežom šalju u čisto tekstualnom obliku, što ih čini lako uočljivima, korištenjem alata opisanih unutar ovoga dokumenta.
Također treba napomenuti da su ovi alati iskoristivi u situacijama kada se dva računala između koji se želi promatrati mrežni promet nalaze na istom segmentu računalne mreže.

3. Sigurnosni rizik i preventivne mjere

3.1. Programski alati

Iako se zaštita od ovakvog tipa napada može na prvi pogled zamisliti kao vrlo problematično pitanje, te kao prilično težak problem, danas postoje kvalitetni mehanizmi zaštite od neželjenog promatranja mrežnog prometa.

Na primjer, jedno od mogućih rješenja je korištenje jednokratnih korisničkih zaporki, koje se koriste za samo jedno prijavljivanje u sustav, nakon čega postaju nevažeće. Njihovo slanje u čistom tekstualnom obliku, u tom slučaju neće predstavljati toliki problem, budući da one nakon prve prijave u sustav više nemaju nikakav poseban značaj.
No, u tom slučaju je posebnu pažnju posvetiti mehanizmu generiranja takvih jednokratnih zaporki, budući da prediktivnost tog postupka, napadaču može omogućiti nasumce pogađanje korisničke zaporke.
Rješenje ovog problema je da se ovakav pristup kombinira sa enkripcijom podataka, što bi u potpunosti napadaču onemogućilo dolazak do povjerljivih informacija.
U tu svrhu se svim korisnicima preporučuje korištenje SSH (Secure Shell) protokola, koji je sigurnija inačica Berkeleyeve skupine r* protokola (rlogin, rsh i drugi).

3.2. Jezgra operativnog sustava

Mnogi manje iskusni korisnici smatraju da će povećati sigurnost svog sustava, ukoliko unutar same jezgre operativnog sustava isključe programski modul koji omogućuje analizu i promatranje mrežnog prometa ('promiscuous' mod rada).
Iako bi takav pristup, možda u nekim pogledima imao smisla, on se nikako ne preporučuje, budući da mogućnost promatranja prometa predstavlja dragocjeni resurs, kada je u pitanju sigurnost sustava.
Na ovaj način se mogu uočiti različiti sigurnosti propusti unutar vlastitog sustava, te uočiti eventualni pokušaji napada na isti.
Sniffit, Ethereal, tcpdump, snoop sve su popularni alati za promatranje mrežnog prometa na Unix operativnim sustavima, koji mogu poslužiti u ranije navedene svrhe.
Čak bi se moglo preporučiti njihovo povremeno pokretanje preko noći na vlastitom sustavu, kako bi se na taj način uočili eventualni sigurnosni propusti, te provela kontrola prometa prema van i prema unutra.
Na taj način se pravovremeno može uočiti eventualno slanje nedovoljno zaštićenih podataka, te eventualna opasnost od njihovog otkrivanja.

3.3. Sklopovska rješenja

Preklapani Ethernet (engl. switched ethernet) može poslužiti kao neka vrsta rješenja ovog problema. Naime, Erthernet preklopnici se koriste u svrhu poboljšanja performansi Ethernet mreža, budući da se na taj način pojedini segmenti mreže odvajaju u zasebne kolizijske domene.
U takvom pristupu korištenje Ethernet sniffer alata može biti gotovo posve neupotrebljivo, budući da se lokalni mrežni promet ne prosljeđuje na sve segmente mreže, nego samo na onaj vlastiti, što će neovlaštenom korisniku onemogućiti pristup 'povjerljivim' segmentima Ethernet mreže.

4. Detekcija napada promatranjem mrežnog prometa

4.1. Općenito

Uočavanje aktivnosti vezanih za promatranje mrežnog prometa na određenom segmentu računalne mreže, može predstavljati vrlo ozbiljan problem. Uočavanje ovakvih neželjenih aktivnosti također može biti pokazatelj puno ozbiljnijih sigurnosnih problema, budući da pokretanje takvih alata zahtjeva ovlasti administratora sustava, što može biti pokazatelja da je napadač došao do administratorovih ovlasti na vašem sustavu.

4.2. Korištenje ifconfig komande

Najbolji način da se testira postojanje aktivnosti vezanih za promatranje mrežnog prometa, je da se upita sam operativni sustav. Naime, izvršavanjem komande

```
#  ifconfig -a
```

može se vrlo lako zaključiti da li se promatra mrežni promet na vašem segmentu mreže.

Ukoliko ova komanda u bilo kojem dijelu ispiše riječ 'promiscuous' , to je indikator postojanja aktivnosti vezanih za promatranje mrežnog prometa. No, također treba imati na umu da uvijek postoji mogućnost korumpiranja ove ili bilo koje druge komande, ukoliko se radi o ozbiljnijem napadu, te stoga i ovakav pristup treba uzeti sa određenom predostrožnošću.
Naime, ne treba zaboraviti da ono što se vidi na zaslonu vašeg stroja, ne mora uvijek biti realno stanje.

4.3. Programska rješenja

4.3.1. AntiSniff programski alat

AntiSniff je trenutno najnoviji i svojstvima najbogatiji programski alat za detekciju neovlaštenog promatranja mrežnog prometa unutar računalne mreže. AntiSniff osim što radi sa Ethernet mrežama, također radi i sa DSL mrežama, što ga čini još kvalitetnijim alatom.
Na sljedećih nekoliko redaka dan je ispis AntiSniff programskog paketa:

```
[root@bleeding anti_sniff]# ./anti_sniffer -t -n 100 -f TCPSYN -1 -t
10.0.0.11
[*]--Results of test--[*]
     status       : SUCCESS
     checktype    : DNSCHECK
     icmpTestType : ---
     promisc cnt  : 0
     errStr       :
     avg1         : 0
     avg2         : 0
     sent1        : 0
     recv1        : 0
     sent2        : 0
     recv2        : 0
     overflow     : NO
    machines list:
```

4.3.2. Ifstatus programski alat

Sljedeći vrlo koristan alat vezan za ovo područje, je mali, portabilni C programski paket pod imenom ifstatus.
Ifstatus programski paket testira mrežna sučelja na lokalnom sustavu, te pregledava da li koji od njih radi u 'promisciuous' modu, što predstavlja indikaciju promatranja mrežnog prometa. Ukoliko je to slučaj, prijavljuje se administratoru postojanje takvih aktivnosti.
Ovaj alat predstavlja vrlo praktično rješenje kada se koristi u kombinaciji sa cron demon programom. Naime, u tom slučaju crond program se konfigurira na način da u određenim vremenskim razdobljima pokreće ifstatus programski alat, koji će u slučaju primijećenih neregularnosti administratoru prijaviti upozorenje.
Upozorenje će se primiti u obliku e-mail poruke oblika:

```
Date: Tue, 22 Sep 1998 01:02:01 -0400
From: root (Cron Daemon)
To: root
Subject: Cron  run-parts /etc/cron.daily
X-Cron-Env:
X-Cron-Env:
X-Cron-Env:
X-Cron-Env:
X-Cron-Env:

WARNING: EXAMPLE.MEGAGLOBAL.NET INTERFACE eth0 IS IN PROMISCUOUS
MODE
```

4.3.3. CPM programski alat (Check Promiscuous Mode)

Princip rada CPM programskog paketa, identičan je načinu rada ifstatus programskog paketa.
Treba napomenuti da ukoliko se ovaj alat želi koristiti pod Linux operativnim sustavom, potrebno je prije samog prevođenja odkomentirati nekoliko SunOS 4.X include datoteka, budući da to može biti uzrok problema kod prevođenja ovog programa.
Naime, potrebno je unijeti promijene slične ovdje iznesenima:

```
diff -urN cpm.1.2/cpm.c cpm.1.2-linux/cpm.c
--- cpm.1.2/cpm.c       Fri Dec 22 11:42:42 1995
+++ cpm.1.2-linux/cpm.c Mon Sep 28 15:46:00 1998
@@ -14,8 +14,8 @@
 #include

  #include
-#include
-#include
+/*#include */
+/*#include */
 #include
 #include
 #include
```

Ispis CPM programa izgleda ovako u slučaju primijećenih neregularnosti:

```
./cpm
    8 network interfaces found:
      eth0:7: Normal
      eth0:6: Normal
      eth0:5: Normal
      eth0:3: Normal
      eth0:2: Normal
      eth0:1: Normal
      eth0: *** IN PROMISCUOUS MODE ***
      lo: Normal
    1 of them is in promiscuous mode.
```

4.3.4. LSOF programski paket

Vrlo je vjerojatno da je sustav kod kojeg su uočeni neovlašteni postupci promatranja mrežnog prometa, također doživio i napad na korisnički račun administratora sustava, budući da su ta dva elementa međusobno usko povezana.
Čak, štoviše velika je vjerojatnost da je to upravo posljedica neovlaštenog promatranja mrežnog prometa unutar istog sustava.
U takvim situacijama je vrlo velika vjerojatnost da su napadnute i izvršne komande na samom sustavu, te da se u tom slučaju ne može potpuno vjerovati porukama od strane operativnog sustava, budući da postoji mogućnost korumpiranosti istoga.
U takvim situacijama treba pribjeći korištenju drugačijih alata koji će omogućiti detekciju neovlaštenih aktivnosti napadača.
LSOF je programski paket koji se u takvim situacijama može pokazati kao vrlo praktično rješenje. Naime, LSOF je programski paket koji će iz sustava izvući sve one informacije koje mogu biti indikator spomenutih aktivnosti (npr. sve otvorene datoteke, cjevovode, mrežne utičnice i sl.).
Naime, mrežni promatrači će vrlo često na sustavu ostaviti otiske u vidu log datoteka ili nešto slično kao posljedica neovlaštene analize i promatranja mrežnog prometa, što se u ovom slučaju pokušava iskoristiti kao pomoćno sredstvo za otkrivanje neovlaštenih aktivnosti.
Slijedi primjer ispisa LSOF programa:

```
# lsof | more
COMMAND     PID  USER   FD   TYPE     DEVICE   SIZE/OFF   NODE NAME
init          1  root  cwd    DIR        3,1       1024      2 /
init          1  root  rtd    DIR        3,1       1024      2 e
kerneld      20  root    1u   CHR        4,0        0t0  10174
/dev/console
kerneld      20  root    2u   CHR        4,0        0t0  10174
/dev/console
```

4.3.5. Neped.c programski alat

Neped.c je programski alat, koji također može poslužiti kao odličan alat za detekciju neovlaštenih postupaka promatranja mrežnog prometa. Naime Neped.c traži sve strojeve na mreži čija sučelja rade u opasnom 'promiscuous' modu, te ih prijavljuje prikladnom porukom administratoru sustava.
Primjer ispisa ovog programa dan je u nastavku:

```
12:24am[mike@example] ~/ % ./neped eth0
-----------------------------------------------------------
> My HW Addr: 00:60:97:1B:27:C5
> My IP Addr: 10.10.10.18
> My NETMASK: 255.255.255.0
> My BROADCAST: 10.10.10.255
-----------------------------------------------------------
> Scanning ....
*> Host 10.10.10.13, 00:60:97:DD:E6:D6 **** Promiscuous mode
detected !!!
> End.
```

5. Zaključak

Na kraju se može zaključiti da vrijeme utrošeno na sprječavanje i detekciju neovlaštenih aktivnosti ovog tipa, nikako nije uzalud utrošeno vrijeme. Pravovremena detekcija problema ovog tipa, može uštedjeti velike muke administratorima sustava.
Također se u svrhu zaštite svim korisnicima preporučuje korištenje sigurnijih alata poput SSH protokola, kao supstitut nesigurnijim inačicama istih servisa poput telneta i sličnih drugih, budući da oni napadaču omogućuju lakši dolazak do povjerljivih informacija sustava.
Također se treba općenito paziti na administraciju mrežnih servise koji su pokrenuti na vašem sustavu, te posvetiti pažnju enkripciji povjerljivih podataka koji se šalju računalnom mrežom.
Također treba napomenuti da se strogo treba izbjegavati korištenje identičnih zaporki za servise koji su u određenoj mjeri zaštićeni od neovlaštenog promatranja, i za one koji svoje podatke računalnom mrežom šalju u čistom tekstualnom obliku, budući da to u velikoj mjeri narušava smisao ovih sigurnijih protokola i alata.