HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Angel programski paket

CCERT-PUBDOC-2002-12-07

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

Angel je programski alat dizajniran s ciljem da korisnicima onemogući napade sa računala na kojem je instaliran. Angel je također u mogućnosti blokirati velik broj lokalnih DoS napada i kompromitiranje administratorskog korisničkog računa, ali pomoću njega nije moguće kontrolirati pakete koji pristižu na računalo. Alat je izveden kao kernel modul za 2.4 kernele i koristi netfilter podršku za filtriranje paketa. Modul je moguće kompilirati i na 2.2.xx kernel-u, ali u tom slučaju koristiti će se ipchains filtriranje paketa.

Na mrežnom nivou Angel pregledava sve izlazne pakete i ukoliko uoči bilo kakve nepravilnosti, blokira ih. Za pregledavanje paketa koriste se vatrozidne mogućnosti kernela koje omogućavaju hvatanje paketa na TCP/IP stogu. Angel prepoznaje i blokira sljedeće mrežne napade:

- Syn flood,
- Land,
- Smurf,
- Spoofing,
- Jolt,
- Ping of death,
- Ranjivosti u određenim protokolima (definirane u CVE-1999-0067, CVE-2000-0207, CAN-2000-0866, CVE-2000-0810, CVE-2000-0638, CVE-2000-0287, CAN-1999-0885, CAN-2000-0573, CVE-2000-0733, CVE-2000-0567, CVE-2000-0909, CAN-2000-0917),
- Outlook remote buffer overflow.

Na razini operacijskog sustava Angel pomoću odgovarajućih wrapper funkcija presreće i analizira sistemske pozive. Pozivi koji se smatraju ilegalnima, npr. pokretanje fork() naredbe u beskonačnoj petlji, blokiraju se, a legalni sistemski pozivi se propuštaju. Na razini operacijskog sustava Angel je u stanju prepoznati :

- Buffer overflow napade,
- Format string ranjivost,
- Malloc bombing,
- Fork bombing,
- Sniffing.

2. Princip rada

Linux Kernel 2.4 koristi sofisticirani vatrozidni sustav pod nazivom netfilter. Netfilter definira određene točke (engl. *hook points*) u TCP/IP stogu na kojima je moguće registrirati vlastite funkcije. Kada paket pristigne na *hook point* izvršiti će se sve funkcije registrirane za tu točku. Netfilter radi na IP mrežnom sloju što znači da svi paketi već imaju uredno formirana TCP i IP zaglavlja.

Angel za filtriranje paketa registrira funkciju `angel_hook()` koja po određenim pravilima pregledava izlazne pakete i na podatkovni mrežni sloj (engl. *data link layer*) propušta samo one koje smatra valjanima. U slučaju da funkcija naiđe na ilegalan paket odbacuje ga i u `/var/log/messages` upisuje upozorenje administratoru.

Osim provjere izlaznog TCP/IP stoga, prilikom pokretanja Angel modula, neki sistemski pozivi zamjenjuju se wrapper funkcijama, koje će pozvati originalnu kernel funkciju tek kada provjere da li je zahtjev legalan. Zamijenjen je `brk()` sistemski poziv, `fork()` porodica poziva (`vfork()` i `clone()`) i `execve()` poziv.

Zamjenom `fork()` poziva onemogućeni su fork bombing napadi kojima napadač uzastopnim pozivanjem `fork()` sistemskog poziva dovodi do uskraćivanja računalnih resursa. Na sličan način, zamjenom `brk()` poziva, onemogućeno je nekontrolirano zauzimanje memorije tj. malloc bombing napad.

Najzanimljivija je zamjena `execve()` poziva kojom je postignuto da se prije pokretanja svakog programa provjeri:

- da li je pokrenuti program SUID,
- da li varijable okružja sadrže skriveni shell kôd,
- da li varijable okružja sadrže "/" i "%" znakove,

– da li se skriveni shell kôd preko argumenata pokušava proslijediti programu.

3. Instalacija i konfiguracija

U daljnjem tekstu opisati će se postupak instalacije za trenutno najnoviju inačicu Angel-a (0.8.9.). Eventualne izmjene i nova izdanja modula mogu se potražiti na http://www.sikurezza.org:8000/angel/. Angel će raditi na bilo kojem Intel kompatibilnom procesoru i bilo kojoj distribuciji Linux-a koja koristi 2.4 kernel ili 2.2 kernel noviji od inačice 2.2.17.
U direktorij koji se kreira po želji potrebno je otpakirati tar.gz datoteku sa kôdom programa

```
# mkdir ime_direktorija
# tar -xzvf  angel.tar.gz -C ime_direktorija
```

U novonastalom direktoriju pod imenom `Angel-0.8.9/` ključni su direktoriji `doc/` u kojem se nalazi dokumentacija i `src/` koji sadrži programski kôd modula i pomoćnih programa. Modul i pomoćni alati kompiliraju se jednostavnim pokretanjem `make all` naredbe u direktoriju `src/`. Prije kompiliranja poželjno je otvoriti datoteku `Makefile` u direktoriju `src/module/` i provjeriti koje opcije su uključene. U nastavku je dan dio `Makefile` datoteke koji sadrži opcije za konfiguriranje modula.

```
# This is the Makefile for Angel - ( a.k.a. HOT-I 2 )
# (C) Aldo and The Sponge - 2000 - 2002
#
# Angel would prevent a script kiddie or a maliciuos user to
# starts attacks from its machine.
#
# 02 Feb 2001
# enjoy it.

MAJOR="0"
MINOR="8"
PATCH="9"
# EXTRA="@home-"
# EXTRA_LEVEL="2"

BUILD = $(shell date +%Y%m%d)

ANGEL_VERSION=$(MAJOR)"."$(MINOR)"."$(PATCH)""$(EXTRA)""$(EXTRA_LEVE
L)
CODENAME = "No CodE"

#DEBUG = y

# Ukoliko je parametar STATIC_REPORT uključen, modul će periodički
#generirati izvještaje o svome radu, bez mogućnosti mijenjanja
perioda od #strane korisnika
#STATIC_REPORT = y

# Uključuje upisivanje mnoštva dodatnih poruka u /var/log/messages
datoteku
VERBOSE = y

# omogućuje hvatanje SIGSEGV i SIGILL paketa.
# Za uključivanje ove opcije nije potrebno patchirati kernel kao što
to #piše u dokumentaciji programa
TRAP_SIGNALS = y

# Ukoliko je uključen, PARANOIC_SCAN vrši dvostruku provjeru
parametara sa #kojima se pokreću SUID programi, kako bi se smanjio
rizik buffer overflow #napada
```

```
# Omogućavanje PARANOIC_SCAN-a može rezultirati usporavanjem
execve() #sistemskog poziva
PARANOIC_SCAN = y

# Ovaj parametar uključuje MD5 kriptiranje zaporke s kojom je modul
#pokrenut. Na taj način napadaču s administratorskim ovlastima se
#onemogućuje pronalaženje zaporke u tekstualnom obliku jednostavnim
#pretraživanjem /dev/kmem datoteke.
MD5_SIGN      = y

# Definira da li će modul kod učitavanja očekivati MD5 hash ili
običnu #tekstualnu zaporku
# STARTUP_PASSWORD_IS_HASHED = y

# Ukoliko je sljedeća linija odkomentirana Angel neće kontrolirati
MTA #promet
LOCALHOST_LOOPBACK_SKIP_MAIL_CHECK = y

# DONT_LOG opcija isključuje prijavu napada u /var/log/messages
datoteku
# DONT_LOG = y

# Angel sadrži eksperimentalni pretraživač shell kôda. Budući da rad
modula #s ovom opcijom nije dovoljno stabilan, ne preporučuje se
njeno #uključivanje
# USE_EXPERIMENTAL_SCANNER=y

# Zabranom pisanja u /dev/kmem onemogućuje se namjerno isključivanje
modula #od strane iskusnih napadača
LOCK_KMEM=y

# Ovaj parametar omogućuje upis obavijesti o poduzetim akcijama u
#/var/log/angel datoteku
LOG_ANGEL=y

CC = gcc

# This is for Redhat 7.0 and Mandrake 7.x, 8.0 users who have a cvs
snapshot
# for gcc package and a kgcc is supplied in order to correctly
compile the
# kernel.
#CC = kgcc
```

Kao rezultat kompiliranja u direktoriju `src/module/` nalaziti će se kernel modul `angel.o` i shell skripte (`angel_load.sh` i `angel_unload.sh`) za njegovo učitavanje u kernel i zaustavljanje. Nakon kompiliranja potrebno je u direktoriju `src/module/` pokrenuti `make install` koji će modul kopirati u `/lib/modules/2.4.xx/kernel/net/ipv4/netfilter/` direktorij, a skripte za pokretanje i zaustavljanje u `/usr/local/bin` direktorij. Prije pokretanja skripte koja učitava modul potrebno je provjeriti da li je u nju upisana ispravna staza do direktorija u kojem se nalazi modul.

Dokumentacija koja se nalazi u `doc/` direktoriju pisana je u tex formatu i pokretanjem naredbe `make` prebacuje se u PostScript format. Naravno, tex datoteke je moguće prebaciti i u razne druge formate jednostavnim Linux/Unix naredbama (npr. `texi2html` i `texi2pdf`).

Zbog sigurnosnih razloga Angel modul se mora učitati s zaporkom. Na taj način, samo legitimni administrator računala može isključiti modul, tj. ako napadač i preuzme administratorske ovlasti neće moći isključiti modul. Modul se učitava pomoću shell skripte:

```
# angel_load.sh zaporka
```

Poruke o učitavanju upisuju se u `/var/log/angel` datoteku:

```
Nov 07 00:114:14 [angel] v0.8.9 build 20021102 ( No CodE ) is
starting up.
Nov 07 00:114:14 [angel] hook functions installed
Nov 07 00:114:14 [angel] sniffer handler installed
Nov 07 00:114:14 [angel] timer interrupt handler installed
Nov 07 00:114:14 [angel] module locked successfully
Nov 07 00:114:14 [angel]socket ioctl() hooked. Setting promiscous
mode disabled.
Nov 07 00:114:14 [angel]: 256 system calls pointer saved
Nov 07 00:114:14 [angel] Startup complete. Host is disarmed.
Nov 07 00:114:14 [angel] warning: outgoing mail control is disabled.
Nov 07 00:114:14 [angel] writing to /dev/kmem is denied
```

Naredbom `lsmod` može se provjeriti da je usage counter za modul Angel prilikom učitavanja postavljen na 1, što će spriječiti uklanjanje modula naredbom `rmmod`. Ukoliko je u `Makefile` datoteci uključena opcija `STARTUP_PASSWORD_IS_HASHED`, Angel će kao parametar za pokretanje očekivati MD5 hash inicijalne zaporke. Za kreiranje hash-a koristi se naredba `angel_md5` koja se nalazi u `/src/tools/` direktoriju.

Modul se uklanja skriptom `angel_unload.sh` kojoj je također kao parametar potrebno proslijediti zaporku. Ova skripta zapravo upisuje zaporku dva puta u `/dev/angel` i na taj način postavlja usage counter modula na nulu, što omogućuje uklanjanje modula `rmmod` naredbom.

4. Korištenje Modula

Jednom pokrenut, modul se kontrolira pomoću datoteka u `/proc/angel` direktoriju:

- ENV_CHECK_MODE: određuje koji će se testovi izvršiti nad varijablama okružja prije pokretanja SUID programa.
- LAST: informacija o posljednjem paketu koji je poslan.
- LOAD: informacija o opterećenju modula.
- MAX_BRK_DIMENSION: maksimalna veličina memorije koju proces može alocirati. Vrijednost je inicijalno postavljena na 20 MB.
- MAX_BRK_PER_JIFFIE: maksimalan broj brk poziva u 10 ms.
- MAX_FORK_PER_SEC: maksimalan broj fork poziva u sekundi.
- MAX_FORK_PER_USER: maksimalan broj fork poziva u sekundi po pojedinom korisniku.
- REPORT: izvještaj o radu modula.
- REPORT_MODE: određuje način ispisivanja izvještaja (automatski ili na zahtjev).
- REPORT_TIMEOUT: razmak između dva automatska izvještaja
- SEGFAULT_LAST: informacija o zadnjem procesu koji je izazvao segmentation fault grešku.
- SEGFAULT_LOG: uključuje logiranje svih segmentation fault grešaka.
- SHELLCODE: korištenje ove datoteke je još uvijek u testnoj fazi.
- STATS: statistika o broju spriječenih napada.
- UPTIME: vrijeme proteklo od uključivanja modula.
- VERSION: inačica modula.
- ACTION: ovaj parametar određuje akciju koja će se poduzeti kada Angel detektira napad. Trenutno je ovaj parametar podržan za LAND, SMURF, SPOOFING, SYNFLOOD napade. Moguće je zaustaviti, ignorirati ili zabilježiti napad.
- PROTO: određuje akciju koja se primjenjuje ovisno o korištenom protokolu (ICMP,TCP,UDP).

Kako korisnik ne bi morao ručno upisivati parametre u datoteke, u direktoriju `src/tools` nalazi se naredba `arc` pomoću koje se može upravljati modulom i očitavati razne parametre. `Arc –h` ispisati će na ekranu kratak opis svih parametara koje program prima. Vjerojatno je najvažniji parametar `–r` koji ispisuje statistiku spriječenih napada i općenite parametre vezane uz rad modula:

```
[root@localhost tools]# ./arc -r
Fri 08/11/2002, 03:36:02 PM
[AngeL] v0.8.9 build 20021102 ( No CodE ) activity report
up 31 min, load average: 0.00
```

```
Packet processed: 30 [ 0.016pps ]     Packet dropped: 5 [ 0.003pps ]
# of fork(): 270 [ 0.144calls/sec ]   #     of     brk():     294     [
0.157calls/sec ]

Network based attacks:

  Syn flood:              1
  Land:                   4
  Ping of death:          0
  Smurf:                  1
  Spoofing:               3
  Teardrop:               1
  IP insane packets:      0
  XShocK attack:          2
  Jolt:                   1
  HTTP:                   0
  FTP:                    0
  TELNET:                 0
  SENDMAIL:               0
  LPD:                    0

  Total:                  13

Host based attacks:

  Buffer overflow:        0
  Fork bombing:           1
  Malloc bombing:         2
  Locale X DoS:           0
  Env. shell warning:     0
  Sniffing attempt:       3
  Portscanning attempt:   1
  Format Bugs detected:   0
  Removed SuiD bit:       0
  Removed SgiD bit:       0
  Writing attempts to
  /dev/kmem:              2
  Total:                  9

Attacks blocked [ host + net ]: 22
```

Poruka o svakom pojedinom pokušaju napada nalazi se zapisana u `/var/log/messages` datoteci:

```
Nov 07 11:40:33 localhost kernel: [angel] JOLT (UDP) DoS attempt by
uid 0, to host 33554559 ( 1 )
Nov 07 11:41:03 localhost kernel: [angel]: Spoofing attempt no. ( 1
). Warning.
Nov 07 11:41:34 localhost kernel: [angel]: Land attempt no. ( 2 ).
Killed.
```

Ostale važnije opcije arc naredbe su:

- -H: procjenjuje broj fork() i malloc() poziva po sekundi i predlaže maksimalne vrijednosti parametara,
- -t: provjerava da li je modul učitan,
- -r: prikazuje izvještaj o radu modula,
- -L: prikazuje informaciju o posljednjem paketu koji je poslan na mrežu,
- -R mode[=delay]: određuje način generiranja izvještaja,
- -s [=log, =nolog]: uključuje/isključuje prijavljivanje segmantation fault grešaka,
- -F: prikazuje informacije o posljednjem procesu koji je uzrokovao segmantation fault grešku,

- -u: ispisuje vrijeme proteklo od aktiviranja modula,
- -v: ispisuje inačicu modula,
- -h: prikazuje pomoć (opis svih opcija).

5. Testiranje modula

Sposobnost modula da zaustavi napade testirana je s nekoliko exploit programa. Pokušani su syn flood, land, ping of death, smurf, spoofing, teradrop, Xshock i Jolt napadi.

```
     Syn flood:                1
 Land:                    4
 Ping of death:           0
 Smurf:                   1
 Spoofing:                3
 Teardrop:                1
 IP insane packets:       0
 XShocK attack:           2
 Jolt:                    1
 HTTP:                    0
 FTP:                     0
 TELNET:                  0
 SENDMAIL:                0
 LPD:                     0
```

Na lokalnoj razini program je testiran na Fork bombing i malloc bombing napade, kao i pokušaje praćenja mrežnog prometa (engl. *sniffing*) i pregledavanja portova (engl. *portscanning*).

```
Buffer overflow:          0
 Fork bombing:            1
 Malloc bombing:          2
 Locale X DoS:            0
 Env. shell warning:      0
 Sniffing attempt:        3
 Portscanning attempt:    1
 Format Bugs detected:    0
 Removed SuiD bit:        0
 Removed SgiD bit:        0
 Writing attempts to
 /dev/kmem:               2
 Total:                   9
```

Iz izvještaja o statistici spriječenih napada vidljivo je da je Angel uspješno zaustavio sve pokušaje napada, kao i pokušaje pisanja u `/dev/kmem` pomoću kojih iskusniji napadači mogu promijeniti lozinku i ukloniti modul iz kernela. Iako je modul zaustavio sve napade treba naglasiti da postoje mali problemi sa ispravnim prepoznavanjem tipa napada. Tako su npr. neki pokušaji pregledavanja portova identificirani kao pokušaj praćenja mrežnog prometa, a pokušaji land napada su prikazani kao spoofing napad.

6. Zaključak

Angel se pokazao kao vrlo stabilan i koristan modul za kernel. Budući da je program u razvojnoj fazi, tj. nije još dostigao inačicu 1.0, neke od opcija nisu u potpunosti podržane ili su nestabilne. Testiranja su pokazala da Angel, uz manje greške u identifikaciji tipa napada, uspješno prepoznaje i blokira sve napade za koje je predviđen.

Mana ovog softvera je vrlo neažurna dokumentacija koja je većinom pisana na talijanskom jeziku, kao i nemogućnost prepoznavanja novijih mrežnih napada.