HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Analiza NSAT programskog paketa

CCERT-PUBDOC-2003-04-13

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

NSAT (http://nsat.sourceforge.net) je jedan od mnoštva alata za sigurnosno pregledavanje računalnih mreža. Njegov zadatak je provjera mrežnih servisa na udaljenim računalima te otkrivanje propusta u njihovoj konfiguraciji i drugih sigurnosnih ranjivosti. Ovaj alat je sposoban detektirati inačice servisa i operacijskih sustava na kojima su pokrenuti te upozoriti na njihove nedostatke, a sadrži i nekolicinu dodatnih sigurnosnih provjera kao npr. detekciju ranjivih CGI skripti na Web poslužiteljima, uočavanje *backdoor*-ova, itd. U dokumentaciji programa nalaze se kratke upute koje korisnika informiraju o rizicima pokretanja pojedinih servisa, njihovim ranjivostima i metodama za uklanjanje ili ublažavanje istih.
Najnovija inačica kao novost donosi distribuirano pregledavanje pomoću kojeg je postupak moguće rasporediti na više računala i na taj ga način ubrzati.

2. Instalacija i održavanje

U korijenskom direktoriju paketa potrebno je pokrenuti `configure` skriptu koja će provjeriti konfiguraciju sustava i generirati `Makefile` datoteku. Program se prevodi naredbom `make` i instalira u ispravne direktorije naredbom `make install`. Datoteke se uobičajeno instaliraju u `/usr/local/share/nstat` i `/usr/local/bin`, s time da se staza `/usr/local/bin` obavezno mora nalaziti u PATH varijabli okoline. Izmjenom `Makefile` datoteke u korijenskom direktoriju programa moguće je promijeniti direktorije u koje se program instalira. Pri tome treba imati u vidu da je prilikom promjene uobičajenih instalacijskih direktorija potrebno prije prevođenja u datoteci `src/lang.h` upisati ispravne putove do `nsat.conf` i `nsat.cgi` datoteka (inicijalno se nalaze u `/usr/local/share/nsat`).
Program je bez poteškoća instaliran na Mandrake 9.0 distribuciji Linux-a i trebao bi biti kompatibilan sa svim Linux distribucijama i ostalim SysV i BSD sustavima. Moguće je očekivati određene probleme sa bibliotekama i *header* datotekama na nekim distribucijama Solarisa i nestandardnim derivatima UNIX-a na kojima ovaj program još nije u potpunosti testiran. U slučaju prevelikog broja upozorenja prilikom prevođenja preporučuje se ukloniti –ansi zastavicu.
Poželjno je na redovnoj bazi obnavljati liste sigurnosnih problema i konfiguracijske datoteke koje program koristi (`nsat.cgi`, `src/mod/snmp.h`). Najnovija inačica NSAT-a, kao i liste sigurnosnih problema mogu se pronaći na adresi http://nsat.sourceforge.net.
Program se deinstalira naredbom `make uninstall`.

3. Pokretanje

Pregledavanje se pokreće iz naredbenog retka naredbom `nsat` iza koje slijede argumenti pregledavanja i računala koja se pregledavaju. Npr.:

```
nsat [opcije] –h ime_računala
```

ili

```
nsat [opcije] –f datoteka
```

gdje datoteka sadrži popis IP adresa koje se pregledavaju. Moguće je pregledavati i cijeli niz uzastopnih IP adresa pomoću parametara `–s` i `–e`:

```
nsat [opcije] –s početna adresa –e završna adresa
```

Prilikom pokretanja program će potražiti `nsat.conf` datoteku i iz nje preuzeti ostale parametre pregledavanja.
U direktoriju u kojem je pokrenuto pregledavanje kreirati će se datoteke koje sadrže informacije o rezultatima. Opcijom `LogDir` u konfiguracijskoj datoteci omogućuje se spremanje rezultata

pregledavanja svakog računala u zaseban direktorij čije ime odgovara IP adresi računala. Sadržaj log datoteka je sljedeći:

- `.nspid` – sadrži identifikacijski broj pokrenutog NSAT procesa (PID), na ovaj način NSAT prilikom pokretanja detektira da li je pokrenut i ne dozvoljava dvostruko pokretanje,
- `.nsrc` – je *recovery* datoteka koja sadrži podatke o tijeku procesa pregledavanja; u slučaju prekinutog pregledavanja program na temelju podataka u ovoj datoteci nastavlja postupak
- `ports.log` – sadrži popis svih TCP servisa pronađenih na pregledanim računalima, npr.:
  ```
  192.168.0.1  - mysql  (dangerous)
  192.168.0.1  - X windows
  ```
- `os.log` – izvještaj o operacijskim sustavima koji se koriste na pregledanim računalima, operacijski sustavi identificiranju se *fingerprinting* metodom
- `ftp.log` – ova datoteka sadrži podatke o pronađenim FTP poslužiteljima i o eventualnim direktorijima u koje korisnici mogu pisati, npr.:
  ```
  192.168.0.1  -  220  ProFTPD  1.2.5  Server  (ProFTPD  Default
  Installation) [localhost]
  ```
- `ssh.log` – sadrži podatke o pronađenim SSH poslužiteljima
- `telnet.log` - sadrži podatke o pronađenim Telnet poslužiteljima
- `sendmail.log` - sadrži podatke o pronađenim SMTP poslužiteljima, npr.:
  ```
  192.168.0.1 220 localhost ESMTP Postfix (1.1.11) (Mandrake
  Linux)
  192.168.0.1 - allows expn
  192.168.0.1 - allows fakemail
  192.168.0.1 - allows spam
  ```
- `dns.log` – podaci o inačici DNS poslužitelja i eventualni odgovori na zastarjele IQUERY upite
- `httpd.log` – podaci o inačici HTTP poslužitelja i dodatnim modulima ukoliko su pronađeni
  ```
  192.168.0.1 - Apache-AdvancedExtranetServer/1.3.26 (Mandrake
  Linux/6.1mdk) mod_ssl/2.8.10 OpenSSL/0.9.6g sxnet/1.2.4 PHP/
  ```
- `pop2.log` i `pop3-log` – podaci o pronađenim POP poslužiteljima, npr.:
  ```
  192.168.0.1 - +OK POP3 localhost v2001.78mdk server ready
  ```
- `imap.log` - podaci o pronađenim IMAP poslužiteljima
- `finger.log` – rezultati pokušaja iskorištavanja sigurnosnih propusta u finger poslužiteljima
- `snmp.log` – prikupljeni podaci o SNMP servisima koji dozvoljavaju anonimni pristup s javnim *community* nizovima, npr.:
  ```
  192.168.0.1 - SARA
  192.168.0.1 - community:  public
  192.168.0.1 - community:  public - NOAUTH WRITE ACCESS
  ```
- `nntp.log` – podaci o pronađenim NNTP poslužiteljima
- `exports.log` – pronađeni NFS dijeljeni direktoriji kojima je dozvoljen pristup sa svih mreža
- `netstat.log` – snimke netstat stanja
- `backdoor.log` – podaci o pokušajima iskorištavanja poznatih *backdoor* portova, ukoliko su isti pronađeni, npr. pronađeni Back Orifice port:
  ```
  192.168.0.1  - 31337: << 220 ]x[
   >>
  ```
- `ircd.log` – podaci o pronađenim IRC poslužiteljima
- `xwindows.log` – pronađeni X poslužitelji koji odgovaraju na zahtjeve pristigle TCP protokolom
- `netbios.log` – netbios imena računala sa MS Windows operacijskim sustavima ili Samba poslužitelja
- `icmp.log` – podaci o odgovorima na ping pakete sa zabilježenim vremenskim oznakama (engl. *timestamp*), npr.:
  ```
  192.168.0.1 - latency 0 secs
  192.168.0.1 - timestamp: orig:69489923/recv:69489923/trans:0
  ```

- `rpc.log` – Pronađeni RPC servisi koji sadrže određene ranjivosti, npr.:

```
192.168.0.1  - 100000 111    tcp    2      134607641
192.168.0.1  - 100000 111    udp    2      134607641
192.168.0.1  - 100004 802    udp    2      134610144    VULNERABLE
192.168.0.1  - 100004 802    udp    1      134610144    VULNERABLE
192.168.0.1  - 100004 805    tcp    2      134610144    VULNERABLE
192.168.0.1  - 100004 805    tcp    1      134610144    VULNERABLE
192.168.0.1  - 100009 805    udp    1      134610134    VULNERABLE
192.168.0.1  - 600100069     807    udp    1      134609171
192.168.0.1  - 600100069     809    tcp    1      134609171
192.168.0.1  - 100007 816    udp    2      134610127
192.168.0.1  - 100007 816    udp    1      134610127
192.168.0.1  - 100007 819    tcp    2      134610127
192.168.0.1  - 100007 819    tcp    1      134610127
192.168.0.1  - 100024 987    udp    1      134610021    VULNERABLE
192.168.0.1  - 100024 991    tcp    1      134610021    VULNERABLE
192.168.0.1  - 1000032049    udp    2      134609854    VULNERABLE
192.168.0.1  - 1000032049    tcp    2      134609854    VULNERABLE
192.168.0.1  - 100005 992    udp    1      134609843    VULNERABLE
192.168.0.1  - 100005 992    udp    2      134609843    VULNERABLE
192.168.0.1  - 100005 995    tcp    1      134609843    VULNERABLE
192.168.0.1  - 100005 995    tcp    2      134609843    VULNERABLE
```

- `cgi.log` –popis pronađenih CGI skripti koje predstavljaju potencijalne ranjivosti
- `bo.log` – popis računala sa pronađenim Back Orifice *backdoor* programom
- `nlps.log` – informacije o pokušaju iskorištavanja nlps sigurnosnog problema
- `debug.log` – sadrži podatke o greškama u izvođenju programa (pojavljuje se samo ukoliko je program prevođen s `-debug` opcijom).

3.1. Konfiguracijska datoteka

Prilikom svog pokretanja NSAT čita konfiguracijsku datoteku `nsat.conf` i iz nje preuzima parametre pregledavanja. Zbog toga je prije pregledavanja obavezno potrebno urediti konfiguracijsku datoteku. Primjer ove datoteke nalazi se u paketu s izvornim kôdom, a inicijalna konfiguracijska datoteka prilikom instalacije se smješta u direktorij `/usr/local/share/nsat`. Originalnu datoteku se ne preporučuje mijenjati, već ju je poželjno koristiti kao primjer, tj. za svako pregledavanje napraviti novu datoteku po uzoru na inicijalnu. Opcijom `-C` *`datoteka`* programu se specificira koju će konfiguraciju koristiti.

Sama datoteka sastoji se od dva dijela. Prvi dio konfiguracijske datoteke odnosi se na konfiguraciju parametara pregledavanja kao npr. broj paralelno pokrenutih procesa, dok drugi dio određuje koji servisi će se pregledati i na koji način. Svaki parametar u konfiguracijskoj datoteci, vrlo je dobro komentiran pa ju nije potrebno detaljnije opisivati.

3.2. Recovery

Ukoliko NSAT pregledava više računala, kreirati će se *recovery* datoteka `.nsrc` u koju se spremaju opcije iz konfiguracijske datoteke, argumenti zadani prilikom pokretanja i podaci o obavljenom pregledavanju. Kako pregledavanje napreduje, ova datoteka se osvježava, tako da je u slučaju bilo kakvog incidenta ili prekida rada programa moguće nastaviti sa pregledavanjem tamo gdje je prekinuto.

U slučaju prekida rada, pri ponovnom pokretanju program će potražiti *recovery* datoteku te nastaviti sa pregledavanjem mreže. Potrebno je napomenuti da se u tom slučaju program pokreće bez ikakvih argumenata u naredbenom retku. Ukoliko prilikom svog pokretanja program detektira da je već pokrenut (mora se pokretati iz istog direktorija), proces pokretanja će se prekinuti. Na taj način vrlo je lako osigurati konstantan rad NSAT-a njegovim uzastopnim pokretanjem pomoću `cron` poslužitelja.

3.3. Pritajeni način rada

NSAT je moguće pokretati u pritajenom načinu rada (opcija `-c1`). Prilikom pokretanja program će se "pritajiti" i čekati sa pregledavanjem dok se ne završe sve korisničke aktivnosti. Na prvi znak korisničke aktivnosti program će se ponovo prestati s radom. Ovakav način rada pogodan je kod dugotrajnih intenzivnih skeniranja koja zahtijevaju mnogo resursa.

3.4. Distribuirano pregledavanje

Kao što je već spomenuto, ovaj alat podržava distribuirano pregledavanje. Distribuirano pregledavanje je prilično nova opcija u NSAT alatu. Iako prilikom testiranja nije bilo nikakvih problema, treba imati u vidu da je ova opcija još uvijek u beta fazi razvoja tj. da posjeduje ograničenu pouzdanost i nizak nivo sigurnosti. Ideja distribuiranog pregledavanja je raspodjela opterećenja na više računala ili pregledavanje više mreža odjednom.

NSAT se na udaljenim računalima pokreće kao agent (poslužiteljski način rada) koji osluškuje zahtjeve za pregledavanjem na portu 10235. Na jednom računalu se pokreće master NSAT proces (klijentski način rada) sa svim potrebnim opcijama, koji iz određene datoteke čita IP adrese agenata i raspodjeljuje zadatke agentima. Opterećenje se ravnomjerno raspoređuje na sve agente.

Opcije za distribuirano pregledavanje su sljedeće:

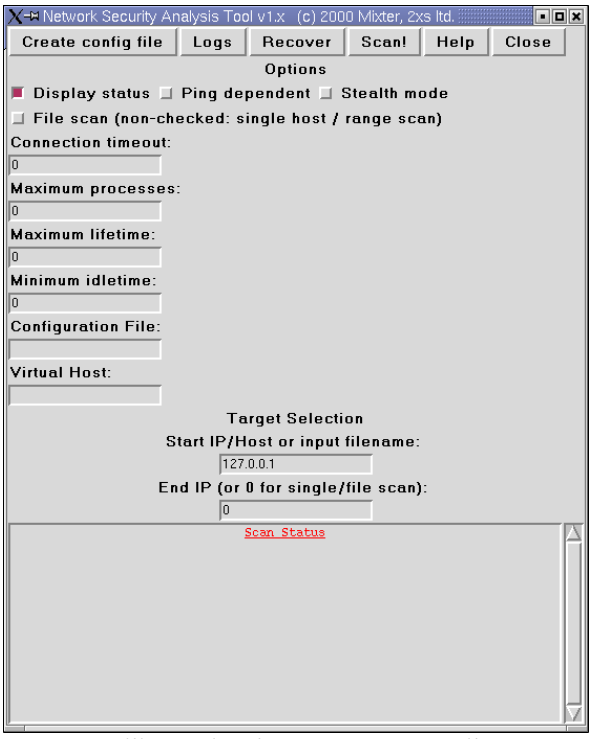
`-A` – pokreće NSAT kao agent-a. Program će se pokrenuti kao pozadinski proces koji osluškuje zahtjeve za pregledavanjem na portu 10235;

`-M` *`datoteka`* – Pokreće NSAT u master načinu rada. Program čita popis agenata iz *`datoteke`* i prosljeđuje im zahtjeve za pregledavanjem.

Zbog trenutne ograničene sigurnosti i pouzdanosti korištenje ove metode pregledavanja se ne preporučuje.

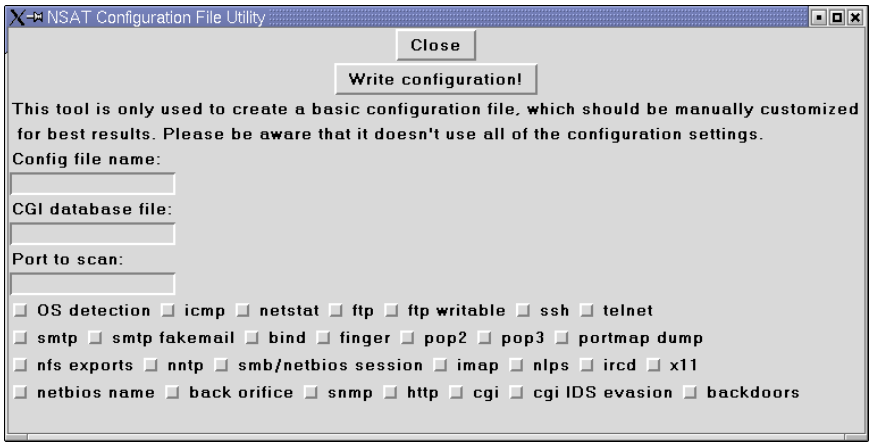
3.5. Grafičko sučelje

Nsat posjeduje i grafičko sučelje za X Window sustav koje se pokreće naredbom `xnsat`. Korištenjem ovog sučelja omogućeno je lakše kreiranje konfiguracijskih datoteka i pregledavanje rezultata te jednostavno podešavanje parametara pregledavanja. *Slika 1* prikazuje glavni prozor Xnsat sučelja.



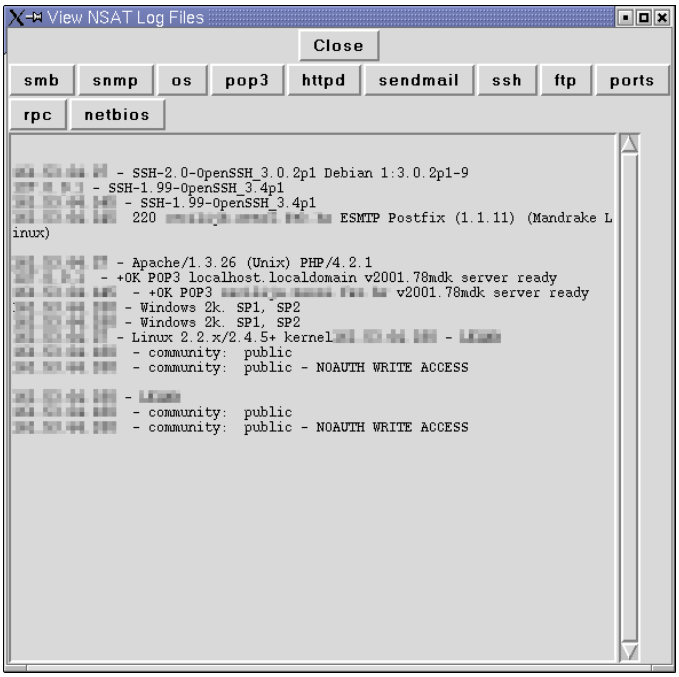
Slika 1: Glavni prozor XNSAT sučelja

Pritiskom na gumb `[Create config file]` otvara se prozor (*Slika 2*) u kojemu se jednostavnim označavanjem parametara kreira nova konfiguracijska datoteka. Potrebno je napomenuti da ovim sučeljem nije moguće podesiti sve parametre pregledavanja pa se za naprednija pregledavanja preporučuje ručno uređivanje datoteke.



Slika 2: Prozor za podešavanje parametra konfiguracijske datoteke

Na Slici 3 prikazan je prozor za pregledavanje rezultata. Kao i kod klasičnog pokretanja NSAT-a, datoteke u kojima su upisani rezultati pregledavanja nalaziti će se u onom direktoriju u kojemu je program pokrenut.



Slika 3: Prozor za pregledavanje rezultata skeniranja

4. Hardverski zahtjevi i sigurnost

Prilikom opsežnog skeniranja NSAT može poprilično opteretiti računalo na kojem je pokrenut. Ugrubo, svaki pokrenuti podproces zahtijeva 10 kbps propusnosti mreže, 50 kilobajta radne memorije i 0,3% procesorske snage (na Pentium klasi procesora). Ukoliko je program prevođen sa `-DEBUG` opcijom mogući su manji gubici u performansama.

Prilikom pisanja ovog alata poduzeti su svi koraci za eliminaciju potencijalnih nesigurnosti pomoću kojih bi bilo moguće kompromitirati računalo na kojemu je NSAT pokrenut. Upis u sve spremnike čija se veličina ne alocira dinamički strogo je kontroliran kako bi se izbjegla mogućnost napada

prepisivanjem spremnika. Pokretanje alata od strane korisnika koji nisu administratori kao i njihova intervencija za vrijeme izvođenja programa također su onemogućeni, što čini NSAT teoretski dovoljno sigurnim da bude pokrenut sa administratorskim ovlastima (*suid root*). Za iznimne slučajeve ostavljena je i opcija PARANOID_CHECK koja nije inicijalno uključena te ju je potrebno omogućiti prilikom prevođenja programa. Program preveden s ovom opcijom provesti će još nekoliko dodatnih provjera prije pokretanja kako bi eliminirao sve sigurnosne rizike. Ako se program namjerava pokretati kao *suid root*, preporučuje se prevođenje s ovom opcijom.

5. Zaključak

NSAT se pokazao kao prilično koristan alat, kojim je moguće relativno brzo pregledati mreže i prikupiti podatke o pokrenutim servisima i potencijalnim sigurnosnim problemima. Njegove mogućnosti daleko su od onih koje nude aplikacije poput Nessus-a ili komercijalnog Shadow Security Scanner-a, a velika primjedba može se uputiti na nepostojanje baze sigurnosnih problema na temelju kojih bi se podrobnije identificirali sigurnosni propusti kod pojedinih servisa. Testiranje je pokazalo da je detekcija operacijskih sustava prilično točna, što je vrlo pohvalno.