



HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Analiza AMAP programskog paketa

CCERT-PUBDOC-2003-08-32

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 obradu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Ovaj dokument predstavlja vlasništvo CARNet-a (CARNet CERT-a). Namijenjen je za javnu objavu, njime se može svatko koristiti, na njega se pozivati, ali samo u originalnom obliku, bez ikakvih izmjena, uz obavezno navođenje izvora podataka. Korištenje ovog dokumenta protivno gornjim navodima, povreda je autorskih prava CARNet-a, sukladno Zakonu o autorskim pravima. Počinitelj takve aktivnosti podliježe kaznenoj odgovornosti koja je regulirana Kaznenim zakonom RH.

Sadržaj

1. UVOD	4
2. INSTALACIJA	4
3. PRINCIP RADA	4
3.1. APPDEFS.TRIG DATOTEKA	5
3.2. APPDEFS.RESP DATOTEKA	5
4. NAČIN PRIMJENE	6
5. TESTIRANJE PROGRAMA	7
5.1. IDENTIFIKACIJA SERVISA NA UDALJENOM RAČUNALU	7
5.2. PRIKUPljanJE PORUKA SERVISA	9
5.3. PREGLEDAVANJE PORTOVA	10
6. ZAKLJUČAK	11

1. Uvod

AMAP programski paket (<http://www.thc.org>) prema svojim karakteristikama može se svrstati u skupinu alata za prikupljanje informacija o udaljenim računalima (engl. *information gathering tool*). Osnovna namjena programa je identifikacija nepoznatih servisa pokrenutih na nestandardnim TCP ili UDP portovima. Za razliku od klasičnih alata za pregledavanje portova (kao što je npr. nmap), koji omogućuju utvrđivanje stanja pojedinih TCP ili UDP portova, AMAP programski paket omogućuje identifikaciju servisa pokrenutih na njima.

Ova funkcionalnost pokazala se posebno korisnom za sigurnosne stručnjake koji se bave analizom i ispitivanjem sigurnosti računalnih sustava (engl. *vulnerability scanning, penetration testing, network identification*), no mogućnosti primjene programa puno su šire.

Osim mogućnosti identifikacije TCP i UDP servisa, program ima ugrađene i druge funkcionalnosti koje ga čine vrlo praktičnim i korisnim alatom prilikom obavljanja svakodnevnih zadataka vezanih uz administraciju i održavanje mrežnih računalnih sustava (pregledavanje portova – *port scanning*, prikupljanje poruka servisa – *banner grabbing*).

Testiranja provedena nad AMAP programskim paketom pokazala su da se radi o vrlo jednostavnom i modularnom programskom paketu, koji se zbog svojih karakteristika može preporučiti i mrežnim administratorima i stručnjacima koji se bave ispitivanjem sigurnosti računalnih sustava. Autori programa smatraju ga programom "nove generacije" za pregledavanje udaljenih računala.

S obzirom na namjenu i trenutne mogućnosti, u budućnosti se mogu očekivati nova poboljšanja i dodaci koji će podići kvalitetu programa te proširiti mogućnosti njegove primjene.

U ovom dokumentu opisani su osnovni postupci instalacije i način korištenja AMAP programa zajedno s popratnim primjerima.

2. Instalacija

Trenutna inačica AMAP programskog paketa nosi oznaku 4.2 i moguće ju je u obliku tar.gz arhive dohvatiti sa URL adrese <http://www.thc.org> (amap-4.2.tar.gz). Nakon što je programski paket dohvaćen s navedene adrese, potrebno ga je standardnim postupkom otpakirati u željeni direktorij.

```
# tar -xzf amap-4.2.tar.gz
```

Nakon toga slijedi postupak instalacije koji je vrlo jednostavan i tipičan za Linux programe koji dolaze u tar.gz arhivi. Radi se o sljedećem nizu naredbi:

```
# ./configure
# make
# make install
```

Ukoliko je sve prošlo bez greške, AMAP program je spreman za korištenje. AMAP program trenutno je dostupan samo za Unix/Linux operacijske sustave.

3. Princip rada

Identifikaciju servisa na zadanom TCP ili UDP portu AMAP program provodi na temelju slanja određenog broja tzv. "trigger" paketa na zadani port ciljnog računala te praćenja i analize pripadajućih odgovora. Primljeni odgovori uspoređuju se sa internom bazom u kojoj su pohranjeni podaci o upitima i odzivima različitih servisa, na temelju čega se s priličnom pouzdanošću može utvrditi o kojemu se servisu radi. Spomenuta baza realizirana je u obliku tekstualnih datoteka specifičnog formata prilagođenog načinu rada programa.

Inicijalne datoteke koje dolaze s AMAP programom zovu se `appdefs.resp` i `appdefs.trig`, te sadrže podatke o nekoliko različitih servisa koje je AMAP program u stanju identificirati (http, ftp, dns, smtp, SSL servisi itd.). Spomenute datoteke sadrže svu inteligenciju AMAP programa te će stoga njegova kvaliteta i pouzdanost uvelike ovisiti o količini informacija sadržanih u ovim datotekama. Što je veći broj informacija o različitim servisima pohranjen u ovim datotekama, to će program biti kvalitetniji i pouzdaniji.

Datoteka `appdefs.trig` sadrži informacije koje program koristi za formiranje zahtjeva prilikom identifikacije servisa na određenom mrežnom portu, dok datoteka `appdefs.resp` sadrži

pripadajuće odgovore na temelju kojih je moguće utvrditi o kojem se servisu radi. Kako je ranije spomenuto, ove datoteke imaju specifičan format i moguće ih je vrlo jednostavno nadopuniti novim potpisima. Ova mogućnost programu daje dodatnu kvalitetu, budući da korisnik sam može proširiti mogućnosti programa te ga na taj način prilagoditi svojim potrebama.

U nastavku je dan primjer `appdefs.resp` i `appdefs.trig` datoteka kako bi se pojasnio način rada AMAP programa.

3.1. Appdefs.trig datoteka

Kao što je već ranije spomenuto, `appdefs.trig` datoteka sadrži podatke koje program koristi za formiranje "*trigger*" paketa, pomoću kojih se provodi identifikacija servisa. Svaki redak datoteke odgovara točno jednom servisu i sadrži podatke potrebne za njegovu identifikaciju. Format zapisa ove datoteke je sljedeći (znak dvotočke ":" koristi se za međusobno odvajanje susjednih polja zapisa):

`labela: mrežni port: protokol: rizik: niz za identifikaciju servisa`
gdje su:

- `labela` – ime koje se koristi za referenciranje servisa;
- `mrežni port` – jedan ili više mrežnih portova odvojenih zarezom na kojima je tipično pokrenut ovaj servis. Parametar je opcionalan;
- `protokol` – identifikacija servisa provodi se samo ukoliko ciljani mrežni port odgovara ovdje definiranom protokolu. Moguće vrijednosti su: `tcp`, `udp` i `both`. Parametar je također opcionalan;
- `rizik` – binarna vrijednost kojom se označava da li formirani opit može štetno utjecati na ispitivani servis. Moguće vrijednosti ovog parametra su 0 i 1;
- `niz za identifikaciju` – znakovni niz koji se koristi za formiranje upita. Moguće ga je definirati ili u ASCII ili u heksadecimalnom obliku. Ovaj niz biti će smješten unutar tijela paketa nakon što je dovršen postupak uspostave veze u tri koraka (engl. *three way handshake*), ukoliko se radi o servisu baziranom na TCP protokolu.

Primjer:

```
smtp:25:tcp:0:"HELO AMAP\r\n"
ftp:21:tcp:0:"USER AMAP\r\n"
rpc:111,2049:udp:1:0x03 9b 65 42 00 00 00 00 00 00 00 00 02 00 0f 42 43
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
rpc:111,2049:tcp:1:0x80 00 00 28 18 72 db 5a 00 00 00 00 00 00 00 02
00 01 86 a0 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 00
dns:53:udp:1:0x00 00 10 00 00 00 00 00 00 00 00 00 00 00 00
```

3.2. Appdefs.resp datoteka

Za razliku od `appdefs.trig`, `appdefs.resp` datoteka sadrži podatke o mogućim odgovorima na poslano "*trigger*" pakete, na temelju čega je moguće utvrditi o kojem se servisu radi. Format zapisa je identičan s razlikom u značenju pojedinih polja:

`labela: niz za identifikaciju servisa: protokol: veličina: odgovor`
gdje su:

- `labela` – naziv koji AMAP ispisaće ukoliko primljeni paketi odgovaraju ovom servisu;
- `niz za identifikaciju servisa` – ukoliko je ovaj parametar naveden, servis će biti identificiran samo ukoliko je primljeni odgovor iniciran navedenim nizom za identifikaciju, odnosno *trigger paketom*. Samim time proizlazi da je parametar opcionalan;
- `protokol` – ovaj parametar zahtjeva da se primljeni odgovor odnosi na ovdje navedeni protokol. Kao i u prethodnom primjeru moguće su sljedeće vrijednosti ovog parametra: `tcp`, `udp`, `both`. Parametar je opcionalan;
- `veličina` – minimalna i maksimalna veličina primljenog odgovora. Vrijednosti se međusobno odvajaju zarezom;

- odgovor - niz s kojim se uspoređuje primljeni odgovor i na temelju kojeg se provodi identifikacija. Ukoliko primljeni odgovor odgovara ovom polju, na zaslon (ili u zadanu datoteku) ispisuje se labela koja označava identificirani servis;

Primjer:

```
dns::::\x80\x81\x00
dns-bind9:dns-bind:udp::^\...[\x00-\x7e].....\xc0
dns-bind8:dns-bind:udp::^\...[\x00-
\x7e].....[\^xc0]
ftp:ftp:tcp::^220.*\n331
ftp:ftp:tcp::^220.*\n530
ftp::tcp::^220.*FTP
ftp::tcp::^220 .* Microsoft .* FTP
http::tcp::^HTTP/0.
http::tcp::^HTTP/1.
http::tcp::<HEAD>.*<BODY>
http::tcp::<HTML>
http::tcp::^Invalid requested URL
http-apache-1::tcp::^HTTP/*\nServer: Apache/1
http-apache-2::tcp::^HTTP/*\nServer: Apache/2
ircd::tcp::/ircd.conf
ircd::tcp:::End of MOTD command.
ircd::tcp:::This server was created
ircd::tcp::Internet Relay Network
ircd::tcp::^:.* NOTICE AUTH
ircd::tcp::^ERROR Closing Link
.
.
.
```

Iz danog primjera može se primijetiti da jedan servis može imati više različitih odgovora na temelju kojih je moguće obaviti identifikaciju. Ukoliko drugo polje, koje predstavlja sadržaj "trigger" paketa nije navedeno, bilo koji odgovor koji odgovara nekom od zapisa rezultirati će potvrdnom identifikacijom određenog servisa.

4. Način primjene

U ovom poglavlju biti će opisane osnovne funkcije AMAP programa, zajedno s pripadajućim opcijama kojima je moguće utjecati na način njegova rada.

Tri su osnovna načina rada podržana kod AMAP programa. Način rada programa odabire se navođenjem odgovarajućeg parametra prilikom pokretanja programa.

- A (AMAP) - Identifikacija servisa na udaljenom računalu;
- B (Banner) - Prikupljanje poruka koje servisi javljaju izravnim spajanjem na pripadajući port (engl. *banner grabbing*);
- P (Portscan) - Pregledavanje portova udaljenog računala (engl. *port scanning*)

Ukoliko niti jedan od parametara nije naveden podrazumijeva se parametar A (AMAP), koji označava identifikaciju servisa.

Ovisno o zadanom parametru koji definira način rada programa ovisit će i ostali parametri, koje je moguće navesti u naredbenom retku. U nastavku (*Tablica 1*) je dan kratki pregled najosnovanijih parametara AMAP programskog paketa.

Parametar	Značenje
-i <file>	Računala i portove koji se žele identificirati program uzima iz ovdje navedene datoteke. Navedena datoteka mora biti generirana nmap programom za pregledavanje mrežnih portova (opcija - oM).
-u <tcp udp>	Navedeni mrežni portovi su ili tcp ili udp.

Parametar	Značenje
-l	" <i>Trigger</i> " paketi šalju se do prve uspješne identifikacije servisa, nakon čega se postupak identifikacije prekida. Ovom opcijom moguće je znatno ubrzati način rada programa.
-v	<i>Verbose</i> način rada. Ovom opcijom moguće je dobiti detaljnije informacije o radu programa.
-d	Ovom opcijom ispisuju se svi primljeni odgovori u heksadecimalnom obliku.
-b	Omogućuje se ispis poruke koju servis javlja prilikom izravnog spajanja na određeni port.
-o <file>	Izlazna datoteka u kojoj će biti pohranjeni rezultati pokretanja programa.
-D <file>	<i>Trigger</i> paketi i odgovori koje program koristi za identifikaciju servisa inicijalno se uzimaju iz datoteka <code>appdefs.trig</code> i <code>appdefs.resp</code> . Putem ovog parametra moguće je navesti proizvoljne datoteke koje će se koristiti za identifikaciju servisa na udaljenom računalu.
-p	Ovom opcijom moguće je poslati <i>trigger</i> pakete koji će odgovarati točno određenom servisu. Parametar kao argument prima labelu kojom je servis označen u datotekama <code>appdefs</code> .
-S	Ovom opcijom program neće provoditi testove na onim portovima na kojima je pokrenut servis s SSL (engl. <i>Secure Socket Layer</i>) podrškom. U suprotnome, program će probati utvrditi o kojem se servisu radi.
-R	Ovom opcijom program neće provoditi identifikaciju RPC (engl. <i>Remote Procedure Call</i>) provjere. U suprotnome, program će probati identificirati sve RPC servise i pripadajuće verzije što ponekada može biti prilično dugotrajan proces.
-c n	Broj istovremenih konekcija koje će program inicirati prilikom identifikacije. Inicijalna vrijednost ovog parametra je 32, a maksimalna moguća je 256.
-H	Ovom opcijom neće se slati <i>trigger</i> paketi, koji su označeni kao potencijalno opasni.

Tablica 1: Parametri AMAP programa

Iako je ovdje navedena većina parametara AMAP programa, svim korisnicima koji ga namjeravaju upotrebljavati preporučuje se detaljnija analiza svih parametara te njihovog značenja.

5. Testiranje programa

5.1. Identifikacija servisa na udaljenom računalu

U svrhu testiranja navedene funkcionalnosti AMAP programskog paketa nekoliko standardnih TCP servisa pokrenuto je na nestandardnim portovima, kako bi se na taj način utvrdile mogućnosti i kvaliteta programa. U sljedećoj tablici (Tablica 2) dana je lista servisa koji su testirani, zajedno s uobičajenim portom na kojem je servis inače pokrenut i onim lažnim koji je korišten u svrhu testiranja:

Ime servisa	Uobičajeni mrežni port	Port odabran u svrhu testiranja
FTP	21/TCP	2100/TCP
SSH	22/TCP	2200/TCP
SMTP	25/TCP	2500/TCP
HTTP	80/TCP	8000/TCP
HTTPS	443/TCP	4430/TCP

Tablica 2: Servisi odabrani za testiranje AMAP programa

Rezultati izvršavanja AMAP programa za svaki od navedenih portova dani su u nastavku:

FTP

```
[root@testing amap-4.2]# amap -v 192.168.1.100 2100
Using trigger file ./appdefs.trig ... loaded 22 triggers
Using response file ./appdefs.resp ... loaded 247 responses
Using trigger file ./appdefs.rpc ... loaded 450 triggers

amap v4.2 (www.thc.org) started at 2003-08-22 12:10:27 -
APPLICATION MAP mode

Total amount of tasks to perform in plain connect mode: 16
Waiting for timeout on 16 connections ...
Protocol on 192.168.1.100:2100/tcp (by trigger ssl) matches
ftp
Protocol on 192.168.1.100:2100/tcp (by trigger ssl) matches
smtp

Unidentified ports: none.

amap v4.2 finished at 2003-08-22 12:24:01
```

SSH

```
[root@testing amap-4.2]# amap -v 192.168.1.100 2200
Using trigger file ./appdefs.trig ... loaded 22 triggers
Using response file ./appdefs.resp ... loaded 247 responses
Using trigger file ./appdefs.rpc ... loaded 450 triggers
amap v4.2 (www.thc.org) started at 2003-08-22 12:23:58 -
APPLICATION MAP mode

Total amount of tasks to perform in plain connect mode: 16
Waiting for timeout on 16 connections ...
Protocol on 192.168.1.100:2200/tcp (by trigger netbios-
session) matches ssh
Protocol on 192.168.1.100:2200/tcp (by trigger netbios-
session) matches ssh-openssh

Unidentified ports: none.

amap v4.2 finished at 2003-08-22 12:24:01
```

SMTP

```
[root@testing amap-4.2]# amap -v 192.168.100.1 2500
Using trigger file ./appdefs.trig ... loaded 22 triggers
Using response file ./appdefs.resp ... loaded 247 responses
Using trigger file ./appdefs.rpc ... loaded 450 triggers

amap v4.2 (www.thc.org) started at 2003-08-22 15:02:10 -
APPLICATION MAP mode

Total amount of tasks to perform in plain connect mode: 16
Waiting for timeout on 16 connections ...
Protocol on 192.168.1.100:2500/tcp (by trigger netbios-
session) matches smtp

Unidentified ports: none.
```


amap v4.2 finished at 2003-08-22 15:02:13

HTTP

```
[root@testing root]# amap -v 192.168.1.100 8000
Using trigger file /usr/local/bin/appdefs.trig ... loaded 22
triggers
Using response file /usr/local/bin/appdefs.resp ... loaded
246 responses
Using trigger file /usr/local/bin/appdefs.rpc ... loaded 450
triggers
```

```
amap v4.2 (www.thc.org) started at 2003-08-22 12:34:05 -
APPLICATION MAP mode
```

```
Total amount of tasks to perform in plain connect mode: 16
Waiting for timeout on 16 connections ...
Protocol on 161.53.64.117:8000/tcp (by trigger http) matches
http
```

Unidentified ports: none.

amap v4.2 finished at 2003-08-22 12:34:11

HTTPS

```
[root@testing amap-4.2]# amap -v 192.168.1.100 4430
Using trigger file ./appdefs.trig ... loaded 22 triggers
Using response file ./appdefs.resp ... loaded 247 responses
Using trigger file ./appdefs.rpc ... loaded 450 triggers
```

```
amap v4.2 (www.thc.org) started at 2003-08-22 12:51:32 -
APPLICATION MAP mode
```

```
Total amount of tasks to perform in plain connect mode: 16
Protocol on 161.53.64.117:4430/tcp (by trigger ssl) matches
http
Waiting for timeout on 12 connections ...
```

Unidentified ports: none.

amap v4.2 finished at 2003-08-22 12:51:38

Na temelju priloženih rezultata može se primijetiti da je AMAP uspješno identificirao sve testirane servise. Sličnim testovima program je uspješno identificirao i MS Exchange servis, LDAP, POP3, RPC i dr.

Program u sebi ima ugrađenu i podršku za SSL protokol (engl. *Secure Socket Layer*), što omogućuje identifikaciju i onih servisa koji SSL protokol koriste za enkripciju i autentikaciju podataka koji se razmjenjuju između klijenta i poslužitelja.

Prosljeđivanjem `-d` opcije AMAP programu moguće je dobiti puno detaljniji ispis sadržaja paketa, ali ova opcija tijekom testiranja nije korištena.

5.2. Prikupljanje poruka servisa

Mogućnost prikupljanja poruka koje servisi javljaju prilikom izravnog spajanja na određeni TCP port (engl. *banner grabbing*) funkcionalnost je koja je do nedavno bila uključena u prilično malen broj

legitimnih sigurnosnih alata. S obzirom da ovaj postupak predstavlja jedan od prvih koraka prilikom provođenja gotovo svih sigurnosnih testova (kao i malicioznih aktivnosti), sve veći broj programa sadrži ovu mogućnost. Jedan od njih je i AMAP programski paket.

Spomenuta funkcionalnost, ugrađena u AMAP program, korisniku omogućuje prilično jednostavan i brz postupak utvrđivanja tipova i inačica servisa pokrenutih na udaljenom računalu. U sljedećem primjeru prikazan je način korištenja AMAP programa u ovom načinu rada:

```
[root@testing amap-4.2]# amap -Bq 192.168.1.100 1-65535
amap v4.2 (www.thc.org) started at 2003-08-22 15:59:38 - BANNER GRAB
mode

Banner on 192.168.1.100:22/tcp : SSH-1.99-OpenSSH_3.4p1\n
Banner on 192.168.1.100:25/tcp : 220 amap.test.com ESMTP Postfix
(1.1.11) (Mandrake Linux)\r\n
Banner on 192.168.1.100:110/tcp : +OK POP3 amap.test.com v2001.78mdk
server ready\r\n
Banner on 192.168.1.100:21/tcp : 220-Welcome to \r\n
Banner on 192.168.1.100:2100/tcp : 220 ProFTPD 1.2.5 Server (ProFTPD)
[cecilija.zesoi.fer.hr]\r\n
Banner on 192.168.1.100:3306/tcp : 0\n4.0.14-standardVRvz#<F,,
```

amap v4.2 finished at 2003-08-22 15:59:56

Opcijom *q* (Tablica 1) program se pokreće u tzv. *quiet* načinu rada, pri čemu se poruke o zatvorenim portovima ne ispisuju. Na ovaj način dobiva se kraći i pregledniji ispis.

5.3. Pregledavanje portova

Pregledavanje portova (engl. *port scanning*) posljednja je od mogućnosti ugrađenih u AMAP programski paket. Iako po svojim mogućnostima AMAP programski paket prilično zaostaje u odnosu na neke naprednije alate za pregledavanje portova (kao što je npr. *nmap*), za neke jednostavnije primjene program može dobro poslužiti. Za utvrđivanje stanja portova program koristi *full-connect* metodu pregledavanja portova u kojoj se u potpunosti dovršava postupak uspostave veze u tri koraka (engl. *three way handshake*). S obzirom na način rada *full-connect* metode pregledavanja portova, ista je vrlo lagana za detekciju te AMAP program iz toga razloga nije moguće koristiti za nevidljivo (engl. *stealth*) pregledavanje portova.

Primjer korištenja dan je u nastavku:

```
[root@testing amap-4.2]# amap -P 192.168.1.100 1-65535
amap v4.2 (www.thc.org) started at 2003-08-22 16:36:14 - PORTSCAN mode

Port on 192.168.1.100:21/tcp is OPEN
Port on 192.168.1.100:22/tcp is OPEN
Port on 192.168.1.100:25/tcp is OPEN
Port on 192.168.1.100:80/tcp is OPEN
Port on 192.168.1.100:110/tcp is OPEN
Port on 192.168.1.100:111/tcp is OPEN
Port on 192.168.1.100:139/tcp is OPEN
Port on 192.168.1.100:443/tcp is OPEN
Port on 192.168.1.100:2100/tcp is OPEN
Port on 192.168.1.100:3306/tcp is OPEN
Port on 192.168.1.100:5432/tcp is OPEN
Port on 192.168.1.100:6000/tcp is OPEN
Port on 192.168.1.100:8200/tcp is OPEN
Port on 192.168.1.100:32768/tcp is OPEN
```

amap v4.2 finished at 2003-08-22 16:36:19

6. Zaključak

U dokumentu je opisan AMAP programski paket za identifikaciju mrežnih servisa pokrenutih na udaljenom računalu. Postupak identifikacije provodi se slanjem specijalno formiranih "trigger" paketa te usporedbom primljenih odgovora s internom bazom, u kojoj su pohranjene informacije o različitim mrežnim servisima.

Provedena testiranja pokazala su da se radi o vrlo praktičnom i jednostavnom programu, a njegove karakteristike čine ga posebno atraktivnim za sigurnosne stručnjake koji se bave provjerama ranjivosti računalnih sustava, penetracijskim testovima i sl. Mogućnost prikupljanja poruka koje servisi otkrivaju prilikom izravnog spajanja na pripadajući port (engl. *banner grabbing*) te pregledavanje mrežnih portova (engl. *port scanning*), funkcionalnosti su koje ga čine primjenjivim i u druge svrhe.

S obzirom da kvaliteta programa uvelike ovisi o količini podataka pohranjenih u internoj bazi na temelju koje se provodi identifikacija, mišljenje je kako će kvaliteta programa i dalje rasti s vremenom kako se u bazu dodaju novi potpisi.