HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Analiza DISCO programskog alata

CCERT-PUBDOC-2003-08-38

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

DISCO programski alat namijenjen je pasivnom otkrivanju aktivnih IP adresa na segmentima računalnih mreža. Kao dodatak otkrivanju IP adresa, DISCO program posjeduje i funkcionalnost za pasivnu identifikaciju (engl. *passive fingerprinting)* TCP SYN i TCP SYN/ACK paketa koja omogućuje utvrđivanje operacijskih sustava pokrenutih na računalima u mreži.

Spomenuta metoda utvrđivanja operacijskih sustava bazira se na poznatoj činjenici da različiti sustavi drukčije reagiraju na različito formirane mrežne pakete. Ovakvo specifično ponašanje posljedica je razlike u implementacijama TCP/IP stogova kod različitih operacijskih sustava, i već duže vrijeme koristi se kao podloga za identifikaciju operacijskih sustava pokrenutih na udaljenim računalima. Konkretno u ovom slučaju, DISCO program za identifikaciju sustava koristi specifičnosti implementacija TCP/IP stogova u pogledu načina generiranja TCP SYN i SYN/ACK mrežnih paketa.

Kako bi se na ovaj način omogućila pouzdana identifikacija operacijskih sustava potrebno je prethodno kreirati bazu podataka s odzivima različitih sustava na različite mrežne pakete. Nakon toga ciljanom se računalu šalju specijalno formirani paketi, prikupljaju se pripadajući odzivi, uspoređuju se s podacima u bazi podataka te se na temelju toga pokušava utvrditi o kojem se operacijskom sustavu radi.

Opisana metoda utvrđivanja operacijskog sustava naziva se još i aktivna identifikacija operacijskog sustava (engl. *active OS fingerprinting*). Razlog tome je činjenica da je za identifikaciju sustava na udaljenom računalu potrebno poslati određeni broj specijalno formiranih mrežnih paketa na to računalo, iz čega proizlazi da u postupku identifikacije aktivno sudjeluju dva računala. Osnovni nedostatak ovog pristupa je mogućnost detekcije malicioznih paketa na ciljnom računalu, na temelju čega administrator sustava može primijetiti da je računalo pregledavano. Za primjenu ove metode može se koristiti programski alat nmap.

Metoda pasivne identifikacije (engl. *passive OS fingerprinting*) slijedi isti koncept, ali je realizacija nešto drukčija. U ovom slučaju, umjesto da se šalju specijalno formirani mrežni paketi na ciljno računalo, i na temelju njegovog odgovora određuje vrsta operacijskog sustava, računalo s kojeg se provodi pasivna identifikacija samo hvata mrežne pakete koje generira ciljno računalo te na temelju njih pokušava odrediti koji je operacijski sustav na njemu pokrenut. Ovu metodu omogućava činjenica da svaki operacijski sustav ima svojih posebnosti kod kreiranja TCP/IP paketa, tako da je na temelju toga moguće s određenom točnošću utvrditi koji operacijski sustav je kreirao mrežne pakete koji su uhvaćeni.

Za određivanje vrste operacijskog sustava koji je generirao određene TCP pakete, najčešće se koriste sljedeća četiri parametra:

- TTL – *Time To Live* (vrijeme života paketa) vrijednost koju postavlja operativni sustav,
- *Window Size* – veličina prozora koju postavlja operativni sustav,
- DF – da li je *Don't Fragment* bit postavljen,
- TOS – i da li operativni sustav postavlja *Type of Service* (vrstu usluge) i na koju vrijednost.

Osim navedenih, u postupku identifikacije mogu se koristiti i drugi parametri TCP/IP paketa, uz uvjet da kod različitih implementacija TCP/IP stoga na različitim operacijskim sustavima postoje razlike koje se mogu iskoristiti u postupku identifikacije.

Analizom navedenih parametara TCP/IP paketa moguće je odrediti vrstu operacijskog sustava koji je generirao paket. Ova metoda nije posve pouzdana i za neke sustave radi bolje, a za druge lošije. Analizom samo jednog od navedenih podataka nije moguće precizno utvrditi o kojem se operacijskom sustavu radi, ali kombiniranjem više podataka iz TCP paketa zajedno, pouzdanost se povećava.

Prilikom korištenja pasivne metode identifikacije treba imati na umu da se paketi generirani od strane programskih alata kao što je npr. nmap, bitno razlikuju od paketa generiranih od strane operacijskog sustava na kojem je taj programski alat pokrenut. Ovu činjenica treba uzeti u obzir, budući da će interpretacija takovih paketa vrlo vjerojatno rezultirati pogrešnom identifikacijom operacijskog sustava ciljnog računala.

Drugi nedostatak ove metode je taj, što se vrijednosti parametara TCP/IP stoga na temelju kojih se provodi identifikacija sustava, mogu izmijeniti unutar samog operacijskog sustava. Operacijski sustav na kojem su vrijednosti TCP parametara promijenjene nije moguće otkriti ovom metodom.

Prednost ove metode je njena pasivnost, tj. na ciljano računalo se ne šalju nikakvi mrežni paketi na temelju kojih bi bilo moguće otkriti da je računalo pregledano.

2. Instalacija

DISCO programski alat može se dohvatiti s Interneta na Web adresi http://www.altmode.com/disco, u obliku .tar.gz paketa u kojem se nalazi izvorni kod programa.
Prije instalacije paket je potrebno otpakirati naredbom:

```
tar – xzvf disco-1.1.tar.gz
```

Nakon toga potrebno je instalaciju prilagoditi za operativni sustav na kojem će program biti pokrenut. To se postiže naredbom:

```
./configure
```

Program se iz izvornog koda u izvršne datoteke prevodi naredbom:

```
make
```

Izvršne datoteke se instaliraju na računalo naredbom:

```
make install
```

Prije pokretanja ove naredbe potrebno je prijaviti se na računalo kao root korisnik (`su` naredba).

3. Korištenje programa

DISCO program pokreće se iz komandne linije sa sintaksom:

```
disco [opcije]
```

Opcije koje je moguće koristiti prilikom pokretanja programa su:

- `-i` sučelje – prilikom pokretanja programa potrebno je odrediti sučelje (eth, ppp, ...) na kojem će DISCO hvatati mrežne pakete;
- `-N` – ako je ova opcija uključena, podaci o detektiranim IP adresama i otkrivenim operacijskim sustavima na mreži se neće ispisivati na STDOUT izlaz (u većini primjena to znači da se ti podaci neće ispisivati na ekranu terminala). Ova opcija je korisna ako se ti podaci zapisuju u datoteku;
- `-f` – ova opcija uključuje otkrivanje IP adresa koje će se bazirati na podacima iz SYN i SYN/ACK TCP paketa, koje DISCO uhvati na mreži;
- `-D` – uz ovu opciju uključenu, DISCO će detektirati sve IP adrese na mreži (bez ove opcije DISCO detektira samo IP adrese računala koja komuniciraju s računalom na kojem je DISCO pokrenut);
- `-S` – otkrivanje operacijskih sustava na mreži će se bazirati samo na podacima iz SYN TCP paketa;
- `-A` – jednako kao i `-S` opcija, samo što se identifikacija operativnih sustava bazira na podacima iz uhvaćenih SYN/ACK TCP paketa;
- `-s ime_datoteke` – uz uključenu ovu opciju, sadržaj TCP paketa na mreži se uzima iz datoteke generirane uz pomoć programa `tcpdump`;
- `-o ime_datoteke` – uz uključenu ovu opciju, svi rezultati se pohranjuju u datoteku s imenom `ime_datoteke`;
- `-r filter` – ova opcija se koristi u kombinaciji s opcijom `-s`. Kad je uključena, na uhvaćene pakete se prije korištenja primjenjuju pravila za filtriranje paketa (ova pravila su jednaka pravilima za filtriranje koja se koriste prilikom upotrebe `tcpdump` programa);
- `-u` – ako ova opcija nije uključena, DISCO će za otkrivanje IP adresa i operacijskih sustava na mreži koristiti sve IP pakete koje uhvati. To znači da postoji mogućnost da neka IP adresa i operacijski sustav budu detektirani više puta. Uključenjem ove opcije, DISCO će za detekciju koristiti SYN i SYN/ACK pakete koji su jedinstveni od trenutka kad je program pokrenut. Time se izbjegava višestruka detekcija istih IP adresa i operacijskih sustava;
- `-t` – ova opcija se koristi u kombinaciji s `-o` opcijom. Ako je uključena, DISCO u izlaznu datoteku dodaje i vrijeme (engl. *timestamp*) kad je koja IP adresa detektirana.

U slučaju da program nije u stanju detektirati o kojem se operacijskom sustavu radi, umjesto imena sustava ispisuju se podaci o sadržaju TCP paketa koje je taj sustav generirao. Ako je poznato o kojem se operacijskom sustavu radi (npr. sustav je na lokalnoj mreži) ti se podaci mogu dodati u datoteku `disco.fp` čime je omogućena detekcija tog operacijskog sustava u budućnosti.
Ispisa podataka o TCP paketu izgleda kao:

```
IP_adresa: wwww:ttt:mmmm:D:W:S:N:I:PT
```

gdje su:

- `wwww` – veličina prozora;
- `ttt` – vrijeme života paketa (engl. *time to live*);
- `mmmm` – maksimalna veličina segmenta;
- `D` – *do not fragment* zastavica;
- `W` – skaliranje prozora;
- `D` – *sackOK* zastavica;
- `N` – *nop* zastavica;
- `I` – veličina paketa;
- `PT` – vrsta paketa.

Primjer:

```
10.1.1.1: 16384:255:1460:1:0:0:1:44:S
```

U nastavku je primjer rezultata dobivenih korištenjem DISCO programskog alata.

```
Fri Aug 22 11:30:10 2003,161. 53. 64.145
Fri Aug 22 11:30:10 2003,161. 53. 64.180
Fri Aug 22 11:30:10 2003,194. 24.130. 12
Fri Aug 22 11:30:18 2003,161. 53. 64. 36
Fri Aug 22 11:30:18 2003,161. 53. 64. 36,Windows ME / 2000 / XP,S
Fri Aug 22 11:30:20 2003,161. 53. 64. 39
Fri Aug 22 11:30:21 2003,161. 53. 64.150
Fri Aug 22 11:30:23 2003,161. 53. 64.145,Linux 2.4.0 - Linux
2.4.18,S
Fri Aug 22 11:30:23 2003, 66. 35.250.165
Fri Aug 22 11:30:23 2003, 66. 35.250.165,Linux ,A
Fri Aug 22 11:30:24 2003,213.211.192.142
Fri Aug 22 11:30:24 2003,213.211.192.142,Linux 2.4.0 - Linux
2.4.18,A
Fri Aug 22 11:30:29 2003,161. 53. 64.226
Fri Aug 22 11:30:29 2003,161. 53. 64.  3
Fri Aug 22 11:30:29 2003,161. 53. 64.  6
Fri Aug 22 11:30:29 2003,161. 53. 64. 17
Fri Aug 22 11:30:29 2003,161. 53. 64.  4
Fri Aug 22 11:30:29 2003,161. 53. 64. 33
Fri Aug 22 11:30:31 2003,161. 53. 64.  1
Fri Aug 22 11:30:37 2003,161. 53. 64. 58
Fri Aug 22 11:30:41 2003,161. 53. 64.206
Fri Aug 22 11:30:45 2003,161. 53. 64. 24
Fri Aug 22 11:30:45 2003,161. 53. 64.246
Fri Aug 22 11:30:45 2003,161. 53. 64.117
Fri Aug 22 11:30:54 2003,161. 53. 64.228
Fri Aug 22 11:30:54 2003,161. 53. 64. 14
Fri Aug 22 11:31:05 2003,161. 53. 64.  7
Fri Aug 22 11:31:07 2003,161. 53. 64. 52
Fri Aug 22 11:31:09 2003,161. 53. 64.  7,33304:64:1460:1:0:1:1:64,A
Fri Aug 22 11:31:10 2003,161. 53. 64.101
Fri Aug 22 11:31:18 2003,161. 53. 64. 44
Fri Aug 22 11:31:19 2003,161. 53. 64.247
```

4. Zaključak

DISCO programski alat namijenjen je pasivnom otkrivanju aktivnih IP adresa na segmentima računalne mreže. Kao dodatak otkrivanju IP adresa, DISCO posjeduje i funkcionalnost za pasivnu identifikaciju operacijskih sustava na temelju TCP SYN i TCP SYN/ACK paketa.

Program se može koristiti u svrhu detekcije aktivnih IP adresa na segmentima računalnih mreža i otkrivanja operacijskih sustava koji su na njima pokrenuti. Program koristi metodu pasivnog *fingerprinting*-a tako da njegov rad nije moguće detektirati s drugih računala u mreži.