Centar Informacijske Sigurnosti

Firewalking

lipanj 2011.

CIS-DOC-2012-07-055

Upozorenje

Podaci, informacije, tvrdnje i stavovi navedeni u ovom dokumentu nastali su dobrom namjerom i dobrom voljom te profesionalnim radom CIS-ovih stručnjaka, a temelje se na njihovom znanju i petnaestak godina iskustva u radu u informacijskoj sigurnosti. Namjera je da budu točni, precizni, aktualni, potpuni i nepristrani.

Ipak, oni su dani samo kao izvor informacija i CIS ne snosi nikakvu izravnu ili posrednu odgovornost za bilo kakve posljedice nastale korištenjem podataka iz ovog dokumenta.

Ukoliko primijetite bilo kakve netočnosti, krive podatke ili pogreške u ovom dokumentu, ili imate potrebu komentirati sadržaj molimo Vas da to javite elektroničkom poštom na adresu info@CIS.hr.

O CIS-u

CIS izrađuje pregledne dokumente (eng. white paper) na teme iz područja informacijske sigurnosti koji će biti korisni zainteresiranoj javnosti, a u svrhu **podizanje njezine svijesti o informacijskoj sigurnosti** i **sposobnosti za čuvanje i zaštitu informacija i informacijskih sustava**. Pored toga, CIS razvija i održava mrežni portal www.CIS.hr kao referalnu točku za informacijsku sigurnost za cjelokupnu javnost; izrađuje obrazovne materijale namijenjene javnosti; organizira događaje za podizanje svijesti o informacijskoj sigurnosti u javnosti i pojedinim skupinama te djeluje u suradnji sa svim medijima.

CIS **okuplja mlade** zainteresirane za informacijsku sigurnost i radi na njihovom pravilnom odgoju i obrazovanju u području informacijske sigurnosti te pripremu za **profesionalno bavljenje informacijskom sigurnošću**.

Centar informacijske sigurnosti [CIS] nastao je 2010. godine na poticaj Laboratorija za sustave i signale[LSS] Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu, a kao posljedica 15togodišnjeg rada na istraživanju, razvoju i primjeni informacijske sigurnosti. LSS je među ostalim potaknuo osnivanje CARNetovog CERTa i sudjelovao u izradi Nacionalnog programa informacijske sigurnosti RH.

Smisao CISa je da bude **referentno mjesto za informacijsku sigurnost** za javnost, informatičare i posebno za mlade te da sustavno podiže njihovu svijest i sposobnosti u području informacijske sigurnosti.

Rad CISa podržava Ministarstvo znanosti, obrazovanja i sporta Republike Hrvatske, a omogućuju sponzori.

Prava korištenja

Sadržaj

1. Uvod

Vatrozid (eng. *firewall*) je često korištena sigurnosna komponenta u današnjim računalnim sustavima. Iako postoje različite vrste vatrozida, glavna uloga mu je filtriranje mrežnog prometa između lokalne i javne mreže. Jednako se koristi i za zaštitu osobnih računala, kao i za zaštitu većih informacijskih sustava.

Korištenjem vatrozida može se osigurati određena razina sigurnosti u sustavu, no razvojem Interneta javlja se i sve veći broj napada čiji je cilj narušiti njegovu sigurnost. Brojni su razlozi zbog kojih vatrozid može postati slaba točka sustava. Od neispravne konfiguracije, do programskih pogrešaka vezanih uz samu implementaciju vatrozida.

Jedna od brojnih tehnika narušavanja sigurnosti vatrozida je i *firewalking* . Ta tehnika pomaže potencijalnim napadačima prikupiti informacije o sustavu koji je meta napada. Tehnika se temelji na alatu *traceroute* koji je dostupan u većini operacijskih sustava. Važno je napomenuti da se korištenjem *firewalking* tehnike ne može dobiti izravan pristup sustavu, no može se prikupiti dovoljno informacija koje onda mogu biti polazna točka za izvođenje napada.

Vatrozid se često koristi kako bi se sakrili detalji o sustavu koji se želi zaštititi. Korištenjem tehnike *firewalking* potencijalni napadači mogu o zaštićenom sustavu saznati mnogo više informacija nego što je zaista izloženo javnosti. Upravo je to velika sigurnosna prijetnja, jer iako prividno zaštićen, sustav je i dalje podložan napadima.

Ovaj dokument detaljno će opisati princip rada *firewalking* tehnike i objasniti ključne pojmove vezane uz samu tehniku. Bit će navedene i kratko opisane mete podložne *firewalking* napadima. Također, bit će napravljen pregled poznatijih alata koji koriste tu tehniku i ukratko opisan njihov način rada i mogućnosti. Osvrnut će se i na neke od primjena *firewalkinga*, s naglaskom na primjene u etične svrhe te postupke koji se mogu poduzeti u cilju zaštite vlastitih sustava od napada temeljenih na toj tehnici.

2. Ciljevi napada

Glavne mete napada temeljenih na *firewalking* tehnici su sustavi koji se skrivaju iza vatrozida, te oni koji se nalaze u tzv. DMZ zoni (eng. *demilitarized zone*). Općenito, *firewalking* napadi namijenjeni su za narušavanje sigurnosti sustava koji filtriraju promet koji dolazi izvan lokalne mreže.

2.1. Vatrozid

Pojam vatrozid obuhvaća širok spektar značenja (programski, sklopovski, aplikacijski, mrežni, itd.), no u kontekstu *firewalkinga* gotovo uvijek se misli na vatrozid na mrežnom sloju. Takvi vatrozidi zapravo rade filtriranje mrežnih paketa (ulaznih i izlaznih). Pravila koja se primjenjuju prilikom filtriranja paketa mogu biti raznolika. Često se za filtriranje ulaznog prometa koriste liste pristupa (eng. *ACL , Access Control List*).

Moguće je primijeniti više uvjeta filtriranja kao što su filtriranje po IP adresi, priključnici (eng. *port*), protokolu i sl. U kontekstu *firewalkinga* najvažnije je filtriranje po raznim mrežnim protokolima te otvorene priključnice povezane s mrežnim servisima (npr. FTP usluga, DNS usluga i sl.). Nadalje, ukoliko vatrozid pamti stanja (eng. *stateful*) filtriranje se može raditi i na temelju konekcija (npr. različito filtriranje podataka za različite vrste uspostavljenih sjednica). Vatrozidi koji ne pamte stanja (eng. *stateless*) mnogo su jednostavniji od onih koji pamte stanja. Složenost vatrozida uvelike povećava vrijeme odziva sustava.

Treba naznačiti kako vatrozid nije namijenjen blokiranju cijelog prometa već poneke pakete treba i propustiti, i upravo to je činjenica na koju se oslanja *firewalking* tehnika. Uvijek postoje paketi koji mogu proći kroz vatrozid, a da bi zloćudni paketi prošli kroz njega potrebno je samo saznati koju vrstu paketa vatrozid propušta. Vatrozid je meta *firewalking* napada najčešće u slučajevima kada je krivo ili nepažljivo konfiguriran.

2.2. DMZ

Demilitarizirana zona (eng. DMZ, *demilitarized zone*) je podmreža unutar lokalne mreže organizacije koja sadrži servise javno izložene na Internetu. Koristi se kada je potrebno ostale dijelove lokalne mreže organizacije (one koji nisu javno izloženi na Internetu) zaštititi od potencijalnih vanjskih napadača. Korištenje DMZ predstavlja dodatnu razinu sigurnosti u sustavu. Sustav koji sadrži DMZ sigurniji je od sustava zaštićenog samo običnim vatrozidom.

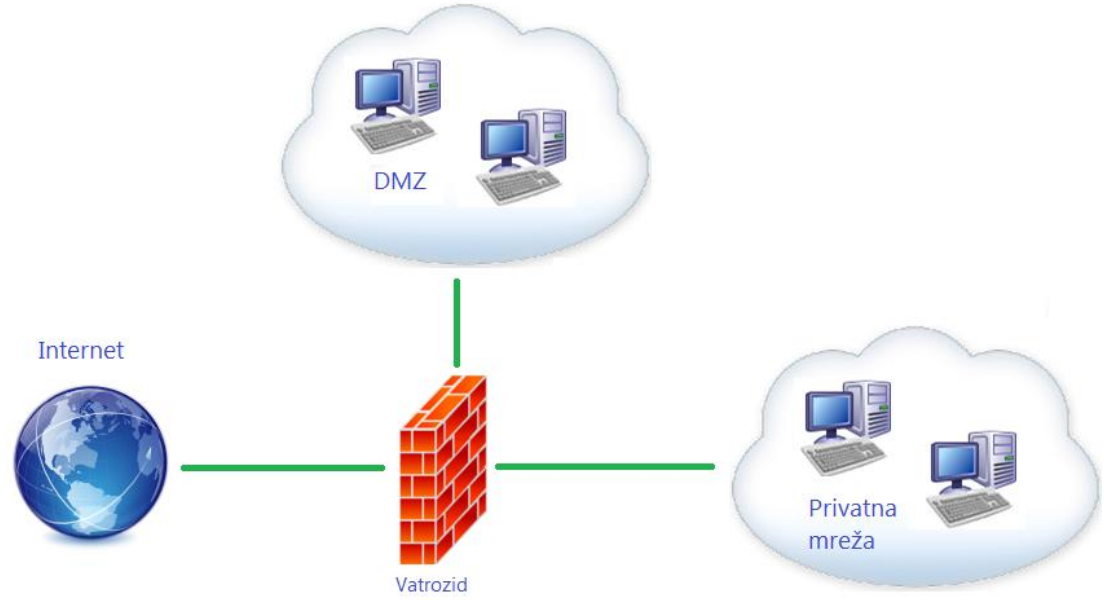
Poslužitelji koji se nalaze unutar demilitarizirane zone smiju komunicirati međusobno i s poslužiteljima izvan lokalne mreže, ali imaju ograničen pristup ostalim računalima unutar lokalne mreže. Važno je napomenuti da poslužitelji unutar zone smiju pružati usluge ostalim računalima unutar lokalne mreže (računala unutar lokalne mreže smiju pristupati DMZ, ali ne i obratno). Ograničenja pristupa postižu se korištenjem vatrozida.

Unutar zone se često stavljaju poslužitelji koji pružaju usluge vanjskim korisnicima. Takve usluge su primjerice DNS usluga, web poslužitelji, poslužitelji elektroničke pošte, FTP poslužitelji, VoIP poslužitelji i sl.

Problem je činjenica da poslužitelji i usluge unutar demilitarizirane zone često trebaju koristiti povjerljive podatke koji se nalaze na poslužiteljima u lokalnoj mreži izvan nje. Stoga se DMZ ne može sasvim odvojiti od ostatka lokalne mreže već se treba koristiti vatrozid.

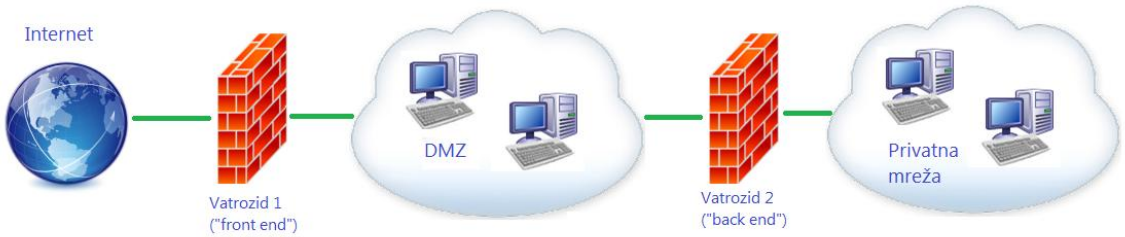
Najčešći načini implementacija DMZ su korištenjem jednog ili dva vatrozida.

Ukoliko se koristi jedan vatrozid on mora imati barem tri sučelja: sučelje za DMZ, sučelje prema vanjskom svijetu i sučelje prema privatnoj mreži (Slika 1.). U takvom slučaju vatrozid je jedinstvena točka ispada.



Slika 1. DMZ – jedan vatrozid
Izvor: CIS

Drugi način implementacije DMZ je uz pomoć dva vatrozida. To je sigurnija metoda jer ne postoji jedinstvena točka ispada. Prvi vatrozid propušta samo promet prema zoni (eng. *front end firewall*) dok se drugi vatrozid nalazi između zone i privatne mreže (eng. *back end firewall*) (Slika 2.). Ovaj način implementacije je sigurniji jer da bi se došlo do povjerljivih informacija koje se nalaze u privatnoj mreži treba proći kroz dva vatrozida koji ne moraju imati iste postavke niti iste ranjivosti.



Slika 2. DMZ – dva vatrozida
Izvor: CIS

Važno je napomenuti da se u DMZ arhitekturama često koriste vatrozidi na aplikacijskom, a ne mrežnom sloju. U tom slučaju teže je izvesti *firewalking* napade.

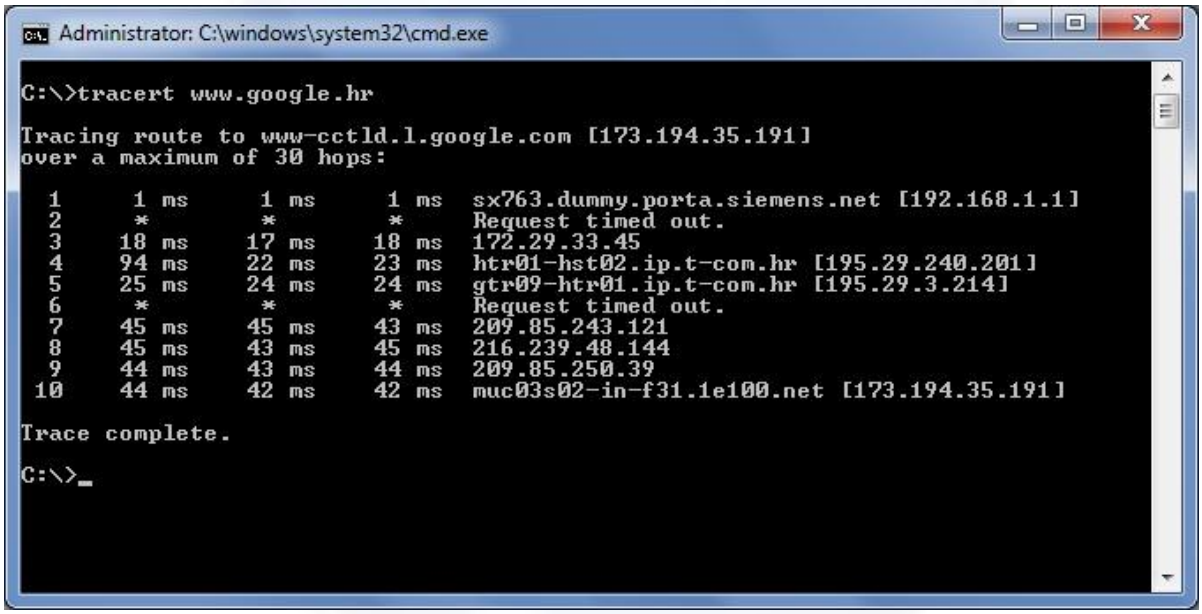
3. Traceroute

Sama tehnika *firewalking* temelji se na alatu *traceroute* koji je dostupan u većini poznatijih operacijskih sustava. Princip rada alata koji koriste *firewalking* tehniku vrlo je sličan principu rada alata *traceroute*, stoga će se prvo objasniti taj alat.

3.1. Princip rada

U operacijskim sustavima Windows koristi se alat tracert.exe, na Unix platformama, uključujući i Mac OS koristi se alat *traceroute*. Svi alati u načelu imaju jednak način rada.

Kada jedan poslužitelj u IP mreži šalje poruku drugom poslužitelju ta poruka neće s izvorišnog poslužitelja odmah doći do odredišnog već će obično putovati kroz nekoliko usmjernika. Alat *traceroute* služi za prikaz puta kojim putuje paket između dva poslužitelja u IP mreži. Ispis alata *traceroute* sastoji se od ispisa svih usmjernika koji se nalaze na putu od izvorišnog do odredišnog čvora, te vremena odziva određenog čvora. Slika 3. prikazuje ispis alata tracert na operacijskom sustavu Windows.



Slika 3. Ispis alata tracert.exe
Izvor: CIS

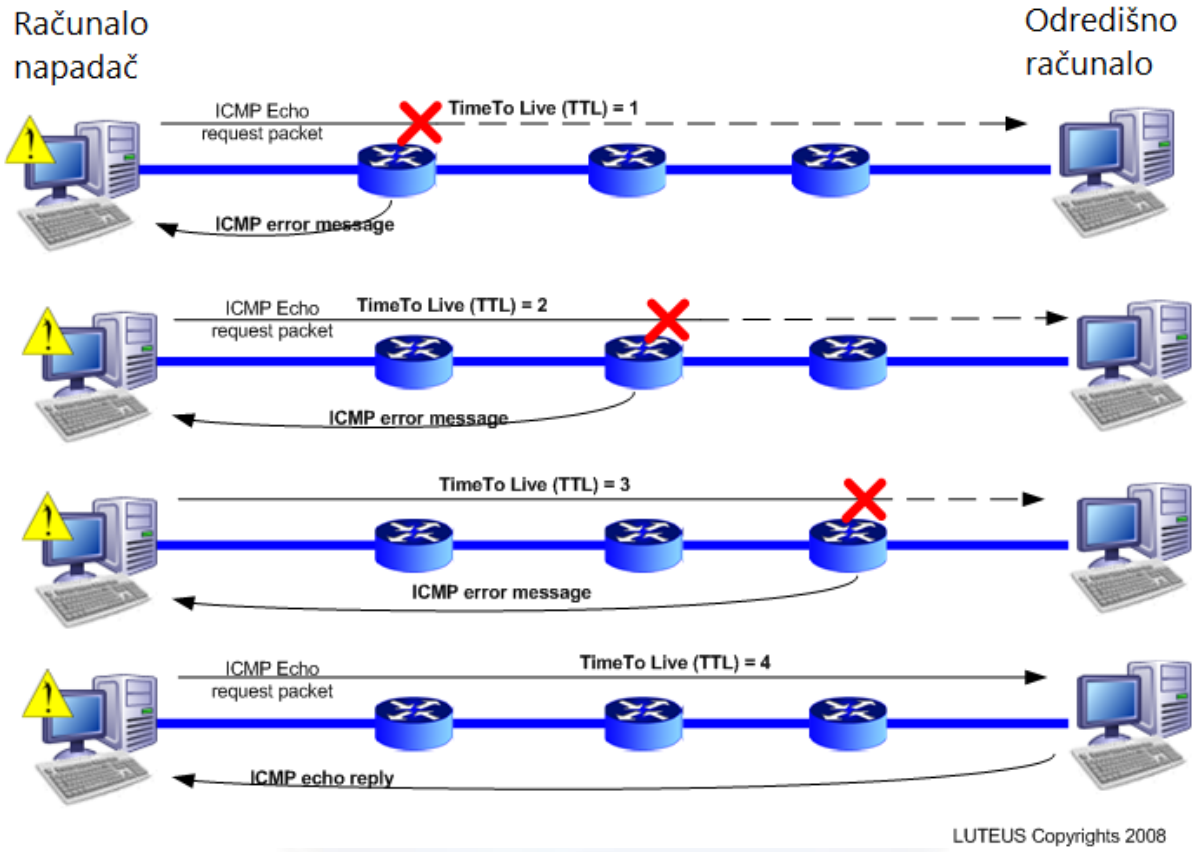
Informacije o usmjernicima kroz koje prolazi paket između dva poslužitelja ne mogu se pročitati iz samog paketa. Paket ne prolazi uvijek kroz iste usmjernike na svom putu. Kroz koje usmjernike će paket biti usmjeren ovisi o brojnim faktorima (npr. zagušenje mreže).

IP paket sastoji se od dva dijela: zaglavlja, u kojem se nalaze neke važne informacije o paketu i od dijela gdje se nalaze podaci koje paket prenosi. Unutar zaglavlja sadržana je informacija o polazišnom i odredišnom poslužitelju, ali ne i o svim usmjernicima kroz koje paket prolazi na svom putu. Te informacije mogu se saznati uz pomoć alata *traceroute*, a pritom se koristi TTL polje u zaglavlju IP paketa (eng. *time to live*).

Glavna funkcija TTL polja je sprječavanje beskonačnih petlji prilikom usmjeravanja paketa. Prilikom slanja IP paketa, polje TTL se postavi na neku pozitivnu vrijednost, te se svakim skokom na sljedeći usmjernik vrijednost polja smanjuje. Ukoliko vrijednost polja dosegne 0, usmjernik koji je primio paket odbacuje taj paket i šalje izvorištu poruku da je paket odbačen (*TTL Exceeded in Transit*). Takva poruka nikad ne dolazi do odredišta.

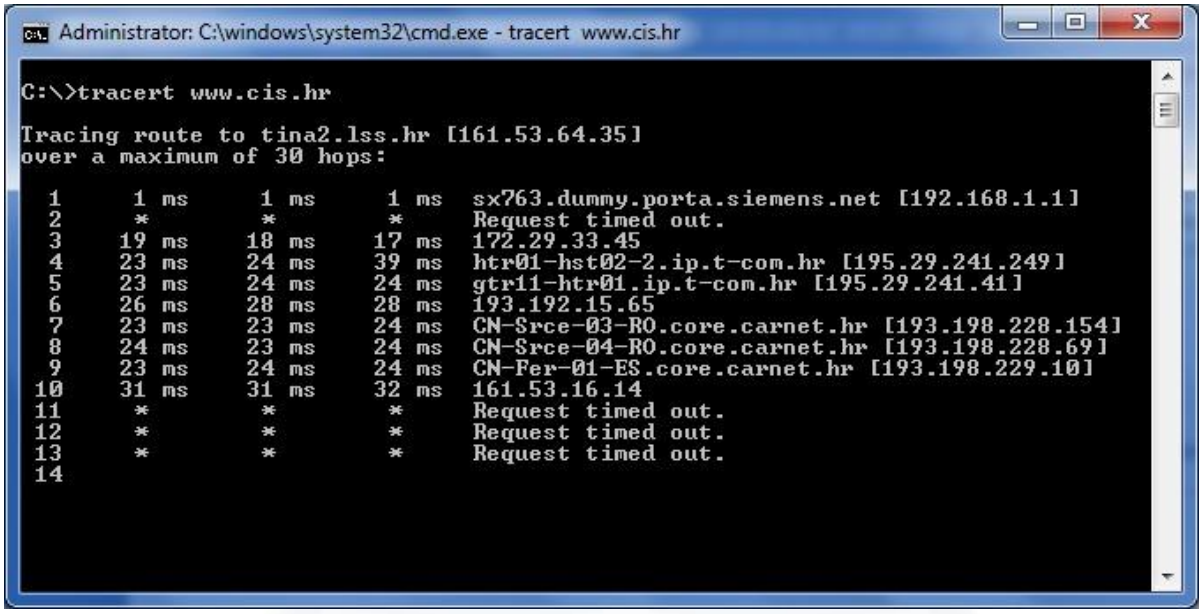
Alat *traceroute* postupno mijenja vrijednosti polja TTL od 1 na više kako bi iz odgovora da je paket odbačen saznao koji je točno čvor odbacio paket (Slika 4.) te na taj način doznaje IP adrese čvorova koji se nalaze između izvora i odredišta.

Windows inačica alata *traceroute* šalje ICMP *echo* pakete, dok Unix inačice koriste UDP datagrame. ICMP i UDP su transportni protokoli čiji paketi se mogu nalaziti unutar IP paketa. Najčešće se datagrami šalju na priključnicu 33434, te se broj priključnice povećava za svaki poslani paket. Tako visok broj priključnice uzima se jer je malo vjerojatno da će neka aplikacija koristiti upravo tu priključnicu. Također, važno je napomenuti da se obično šalju tri paketa odjednom (na slijedne priključnice), da bi se u slučaju gubitka jednog paketa ipak dobio odziv od poslužitelja. Na slici (Slika 3.) mogu se vidjeti tri različita vremena odziva za svaki usmjernik.



Slika 4. Grafički prikaz tracerouta
Izvor: LoriotPro, LUTEUS

Vatrozidi mnogih sustava konfigurirani su tako da blokiraju *ping* poruke kako bi se sakrili detalji o topologiji sustava. Ukoliko je vatrozid tako konfiguriran, prilikom pokušaja izvođenja *tracerouta*, neće se ispisati svi usmjernici do kraja, već će se u jednom trenutku početi ispisivati *Request timed out* poruke.Slika 5. prikazuje jedan takav primjer. U takvoj situaciji, korištenjem samo alata *traceroute*, teško je otkriti korisne informacije dalje od granica sustava.



Slika 5. Pokušaj tracerouta uz vatrozid
Izvor: CIS

3.2. Prikupljanje informacija uz pomoć tracerouta

Ponekad se korištenjem samo alata *traceroute* ipak mogu saznati neke informacije o topologiji sustava čak i kada je on zaštićen vatrozidom. Tehnike koje se prilikom toga koriste oslanjaju se na princip rada alata *traceroute* i nije ih moguće primijeniti u svim situacijama. Primjenjuju se najčešće kada je napadaču poznato kako je vatrozid konfiguriran.

3.2.1. Protocol subterfuge

Ovaj način prikupljanja informacija može se primijeniti kad vatrozid blokira sav ulazni promet osim ICMP poruka *ping* i *ping response*. Kao što je već spomenuto, na Unix platformama alat *traceroute* koristi UDP pakete, no korištenjem opcije „- I“ mogu se koristiti ICMP paketi kao što je to slučaj na Windows platformi.

```
zuul:~>traceroute 10.0.0.10
traceroute to 10.0.0.10 (10.0.0.10), 30 hops max, 40 byte
packets
 1  10.0.0.1 (10.0.0.1)  0.540 ms  0.394 ms  0.397 ms
 2  10.0.0.2 (10.0.0.2)  2.455 ms  2.479 ms  2.512 ms
 3  10.0.0.3 (10.0.0.3)  4.812 ms  4.780 ms  4.747 ms
 4  10.0.0.4 (10.0.0.4)  5.010 ms  4.903 ms  4.980 ms
 5  10.0.0.5 (10.0.0.5)  5.520 ms  5.809 ms  6.061 ms
 6  10.0.0.6 (10.0.0.6)  9.584 ms  21.754 ms  20.530 ms
 7  10.0.0.7 (10.0.0.7)  89.889 ms  79.719 ms  85.918 ms
 8  10.0.0.8 (10.0.0.8)  92.605 ms  80.361 ms  94.336 ms
 9  * * *
10  * * *
```

Slika 6. Traceroute uz korištenje UDP-a
Izvor: Cambridge Technology Partners

```
zuul:~>traceroute -I 10.0.0.10
traceroute to 10.0.0.10 (10.0.0.10), 30 hops max, 40 byte
packets
 1  10.0.0.1 (10.0.0.1)  0.540 ms  0.394 ms  0.397 ms
 2  10.0.0.2 (10.0.0.2)  2.455 ms  2.479 ms  2.512 ms
 3  10.0.0.3 (10.0.0.3)  4.812 ms  4.780 ms  4.747 ms
 4  10.0.0.4 (10.0.0.4)  5.010 ms  4.903 ms  4.980 ms
 5  10.0.0.5 (10.0.0.5)  5.520 ms  5.809 ms  6.061 ms
 6  10.0.0.6 (10.0.0.6)  9.584 ms  21.754 ms  20.530 ms
 7  10.0.0.7 (10.0.0.7)  89.889 ms  79.719 ms  85.918 ms
 8  10.0.0.8 (10.0.0.8)  92.605 ms  80.361 ms  94.336 ms
 9  10.0.0.9 (10.0.0.9)  94.127 ms  81.764 ms  96.476 ms
10 10.0.0.10 (10.0.0.10) 96.012 ms  98.224 ms  99.312 ms
```

Slika 7. Traceroute uz korištenje ICMP-a
Izvor: Cambridge Technology Partners

Slika 6. prikazuje korištenje alata *traceroute* uz vatrozid koji blokira UDP datagrame, dokSlika 7. prikazuje istu stvar, samo uz korištenje ICMP protokola. Alat *traceroute* na Unix platformi sadrži mnoge opcije koje se mogu koristiti za prikupljanje informacija o mreži ukoliko je poznato kako je vatrozid konfiguriran.

3.2.2. Nascent port seeding

Ova tehnika prikupljanja informacija koristi se nešto češće nego prethodna. U slučajevima kada vatrozid blokira sav ulazni promet osim određene priključnice. U primjeru na slikama (Slika 8, Slika 9, Slika 10 i Slika 11) korištena je UDP priključnica 53 koja se koristi za DNS uslugu.

U ovom načinu prikupljanja informacija, kao i u prethodnom, koriste se opcije alata *traceroute* i činjenice koje su poznate o konfiguraciji vatrozida.

Kroz vatrozid je moguće proći ukoliko znamo sljedeće činjenice:

- priključnica koja je otvorena (u primjeru koji slijedi priključnica 53)
- poznat je broj skokova potreban od izvora do vatrozida (u primjeru koji slijedi priključnica 8)
- moguće je upravljati početnom priključnicom tracerouta

```
zuul:~>traceroute 10.0.0.10
traceroute to 10.0.0.10 (10.0.0.10), 30 hops max, 40 byte
packets
 1  10.0.0.1 (10.0.0.1)  0.540 ms  0.394 ms  0.397 ms
 2  10.0.0.2 (10.0.0.2)  2.455 ms  2.479 ms  2.512 ms
 3  10.0.0.3 (10.0.0.3)  4.812 ms  4.780 ms  4.747 ms
 4  10.0.0.4 (10.0.0.4)  5.010 ms  4.903 ms  4.980 ms
 5  10.0.0.5 (10.0.0.5)  5.520 ms  5.809 ms  6.061 ms
 6  10.0.0.6 (10.0.0.6)  9.584 ms  21.754 ms  20.530 ms
 7  10.0.0.7 (10.0.0.7)  89.889 ms  79.719 ms  85.918 ms
 8  10.0.0.8 (10.0.0.8)  92.605 ms  80.361 ms  94.336 ms
 9  * * *
10  * * *
```

Slika 8. Traceroute
Izvor: Cambridge Technology Partners

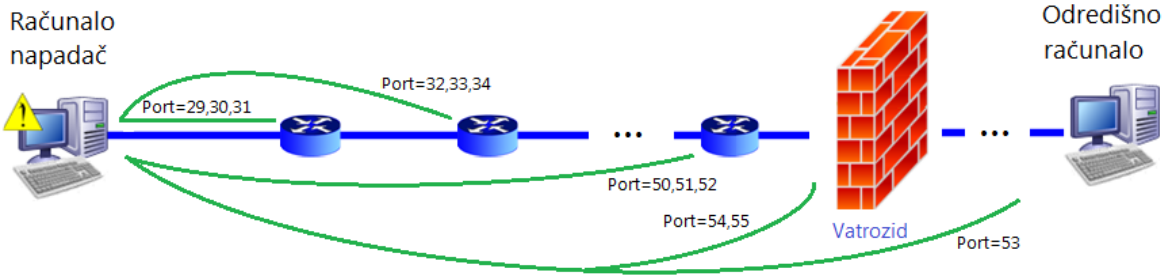
Kao što je ranije spomenuto, početna priključnica alata *traceroute* najčešće je 33434 te se on slijedno povećava za svaki poslani paket. Uz pomoć opcije -p početnu priključnicu moguće je postaviti na bilo koji pozitivan broj.

Također, moguće je upravljati brojem poruka koje se šalju na istu priključnicu (uobičajeno je to 3).

Početnu priključnicu na koju treba biti poslana poruka moguće je jednostavno izračunati iz sljedećih podataka:

- Željena priključnica – P = 53
- Broj skokova – B = 8
- Broj poruka koji se šalje na istu priključnicu – N = 3
- Početna priključnica – PORT

$$PORT = (P - (B * N)) - 1$$
$$PORT = (58 - (8 * 3)) - 1 = 28$$



Slika 9. Nascent port seeding
Izvor: CIS

Dakle ukoliko se kao početna priključnica postavi 28, jedna od tri poruke koje će se poslati na vatrozid bit će poslana upravo na priključnicu 53 koja je otvorena, te će poruka uspješno proći kroz vatrozid (Slika 9.).

Bitno je primijetiti da ova metoda nije uvijek primjenjiva. Naime, ukoliko se za početnu priključnicu dobije negativan broj ovu metodu neće biti moguće izvesti.

```
zuul:~>traceroute -p28 10.0.0.10
traceroute to 10.0.0.10 (10.0.0.10), 30 hops max, 40 byte packets
 1  10.0.0.1 (10.0.0.1)  0.501 ms  0.399 ms  0.395 ms
 2  10.0.0.2 (10.0.0.2)  2.433 ms  2.940 ms  2.481 ms
 3  10.0.0.3 (10.0.0.3)  4.790 ms  4.830 ms  4.885 ms
 4  10.0.0.4 (10.0.0.4)  5.196 ms  5.127 ms  4.733 ms
 5  10.0.0.5 (10.0.0.5)  5.650 ms  5.551 ms  6.165 ms
 6  10.0.0.6 (10.0.0.6)  7.820 ms  20.554 ms  19.525 ms
 7  10.0.0.7 (10.0.0.7)  88.552 ms  90.006 ms  93.447 ms
 8  10.0.0.8 (10.0.0.8)  92.009 ms  94.855 ms  88.122 ms
 9  10.0.0.9 (10.0.0.9)  101.163 ms * *
10  * * *
```

Slika 10. Nascent port seeding
Izvor: Cambridge Technology Partners

Sa slika (Slika 8 i Slika 10)se vidi kako se korištenjem ove metode može proći kroz vatrozid, no odmah prilikom sljedećeg skoka ponovno se poveća priključnica (na brojeve 54, 55 itd.) te vatrozid nastavlja odbacivati pakete. Ovo ograničenje nije moguće prevladati korištenjem ugrađenog *traceroute* alata, no vrlo jednostavnom preinakom izvornog programa moguće je u potpunosti zaobići vatrozid.

U primjeru na slici (Slika 11.)alatu je dodana opcija -S koja omogućuje fiksno zadavanje priključnice. Tako promijenjeni *traceroute* više ne povećava broj priključnice za svaku poslanu poruku, već sve poruke šalje na fiksnu priključnicu. Ovu dodatnu opciju alatu *traceroute* dodali su autori alata *Firewalk* prije nego što su se odlučili za razvoj tog alata.

```
zuul:~>traceroute -S -p53 10.0.0.15
traceroute to 10.0.0.15 (10.0.0.15), 30 hops max, 40 byte
packets
 1  10.0.0.1 (10.0.0.1)  0.516 ms  0.396 ms  0.390 ms
 2  10.0.0.2 (10.0.0.2)  2.516 ms  2.476 ms  2.431 ms
 3  10.0.0.3 (10.0.0.3)  5.060 ms  4.848 ms  4.721 ms
 4  10.0.0.4 (10.0.0.4)  5.019 ms  4.694 ms 4.973 ms
 5  10.0.0.5 (10.0.0.5)  6.097 ms  5.856 ms  6.002 ms
 6  10.0.0.6 (10.0.0.6)  19.257 ms  9.002 ms  21.797 ms
 7  10.0.0.7 (10.0.0.7)  84.753 ms * *
 8  10.0.0.8 (10.0.0.8)  96.864 ms  98.006 ms  95.491 ms
 9  10.0.0.9 (10.0.0.9)  94.300 ms *  96.549 ms
10  10.0.0.10 (10.0.0.10)  101.257 ms  107.164 ms  103.318 ms
11  10.0.0.11 (10.0.0.11)  102.847 ms  110.158 ms *
12  10.0.0.12 (10.0.0.12)  192.196 ms  185.265 ms *
13  10.0.0.13 (10.0.0.13)  168.151 ms  183.238 ms  183.458 ms
14  10.0.0.14 (10.0.0.14)  218.972 ms  209.388 ms  195.686 ms
15  10.0.0.15 (10.0.0.15)  236.102 ms  237.208 ms  230.185 ms
```

Slika 11. Nascent port seeding
Izvor: Cambridge Technology Partners

4. Firewalking tehnika

Kao što je ranije spomenuto, tehnika *firewalking* primjenjuje se za dobivanje informacija o sustavu ili mreži koju je potrebno napasti. Točnije rečeno, sam cilj *firewalking* tehnike je utvrditi može li određeni paket koji je poslao napadač proći kroz vatrozid ili neki drugi sustav za filtriranje prometa u mreži. *Firewalking* tehnika nije usmjerena prema odredišnom poslužitelju, već prema poslužitelju na kojem je vatrozid koji štiti odredišno računalo. Korištenjem tehnike *firewalking* može se utvrditi kakvi sve paketi mogu proći kroz sustav za filtriranje. Najvažnije od svega, moguće je otkriti koji se sve usmjernici nalaze iza vatrozida, a to je, kao što je ranije pokazano, teško izvedivo samo uz korištenje alata *traceroute*. *Firewalking* tehniku razvili su Mike D. Schiffman i David Goldsmith.

Ranije objašnjeno prikupljanje informacija uz pomoć tracerouta vrlo je slično *firewalking* tehnici. Alat *traceroute* radi na IP sloju, a poznato je da IP paket može enkapsulirati bilo koji transportni protokol (TCP, UDP ili ICMP). To znači da IP paket sadržava cijeli paket transportnog sloja te na njega dodaje svoje zaglavlje. Ta činjenica može se ponekad iskoristiti ukoliko je poznato kako je vatrozid konfiguriran.

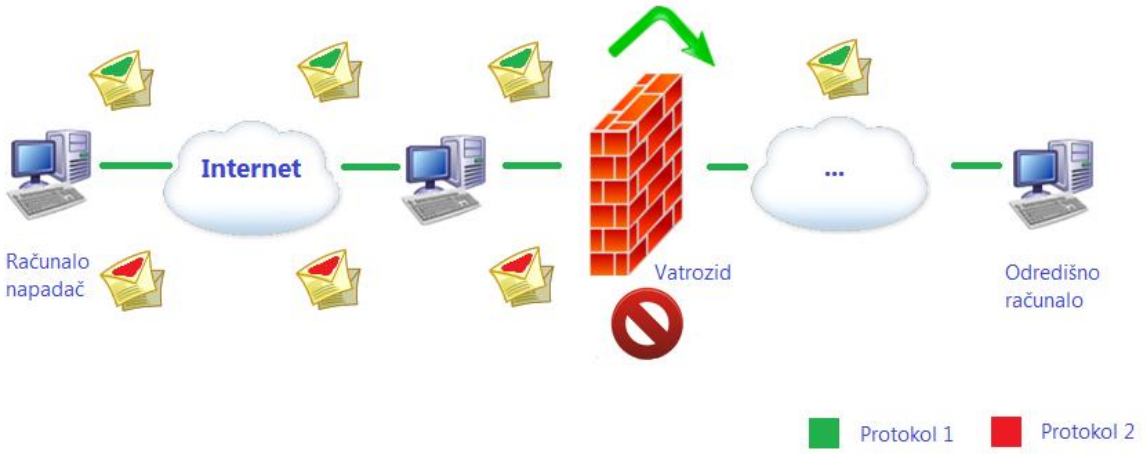
Ukoliko se pokuša alatom *traceroute* pristupiti sustavu koji je zaštićen vatrozidom paket koji će biti poslan vatrozidu bit će odbačen ukoliko ne zadovoljava pravila ACL-a. U tom slučaju jedina informacija koja se može prikupiti je na kojem čvoru se nalazi vatrozid. No, ne treba zanemariti važnost te informacije. Uz znanje na kojem je čvoru vatrozid može se pokušati proći kroz njega mijenjajući primjerice transportne protokole. Ukoliko vatrozid propusti određenu vrstu poruke može se saznati koji je usmjernik sljedeći nakon vatrozida, ali i koju vrstu prometa vatrozid filtrira. Ukoliko vatrozid blokira sav promet, može se utvrditi samo da vatrozid filtrira promet. Takav pristup postupnog otkrivanja informacija osnova je *firewalkinga*.

Da bi se uspješno izveo napad temeljen na *firewalking* tehnici potrebno je identificirati tri poslužitelja (Slika 12.)

Slika 12. Poslužitelji potrebni za firewalking napad
Izvor: CIS

- Računalo napadač
  - Računalo sa kojeg se izvodi *firewalking* napad.
- Zadnje računalo koje je odgovorilo
  - Zadnje računalo koje je poslalo odgovor korištenjem alata *traceroute* (zadnje računalo nakon kojeg slijedi vatrozid).
- Odredišno računalo
  - Računalo koje je odredište napada, zadnje računalo u nizu.
  - Računalo za koje se izvodi skeniranje.
  - Uvijek iza vatrozida.

Firewalking tehnika je na neki način proširenje ranije objašnjenih metoda prikupljanja informacija uz pomoć alata *traceroute* temeljena na mijenjanju protokola (eng. *protocol spoofing* - Slika 13.). Unutar IP paketa mijenja se transportni protokol. Poruka s protokolom 1 prolazi vatrozid, dok vatrozid odbacuje poruku s protokolom 2.



Slika 13. Firewalking – protocol spoofing
Izvor: CIS

Uz korištenje *firewalking* tehnike moguće je izvesti nekoliko različitih napada kojim se prikupljaju informacije. Prvim napadom moguće je skenirati protokole koje propušta vatrozid. To je tzv. *Firewall protocol scan* napad. Tom vrstom napada može se saznati koje sve protokole vatrozid propušta te koje su sve priključnice otvorene. Ta tehnika zapravo koristi napad grubom silom i stvara mnogo mrežnog prometa. Na sve željene priključnice šalju se IP paketi koji enkapsuliraju željene transportne protokole i bilježi se odziv sustava.

Sljedeća, malo naprednija vrsta napada je tzv. *Network mapping* napad. Nakon što se utvrde priključnice i protokoli koji se propuštaju moguće je saznati koji se poslužitelji nalaze iza vatrozida. Slanjem poruka svim poslužiteljima moguće je dobiti vrlo točnu sliku mreže iza vatrozida.

5. Alati

Najpoznatiji alat koji koristi *firewalking* tehniku zasigurno je alat Firewalk. Nekolicina drugih alata također koriste tu tehniku, no samo kao dodatnu funkcionalnost.

5.1. Firewalk

Firewalk je sigurnosni alat namijenjen operacijskim sustavima Linux. Nastao je 1998. godine kao posljedica razvijanja *firewalking* tehnike te želje da se napravi jedinstven alat kojim se na

jednostavan način primjenjuje ta tehnika. Autori alata su autori *firewalking* tehnike Mike D. Schiffman i David Goldsmith. Alat je izdan pod BSD licencom, posljednja izdana inačica alata je 5.0, a alat održava autor Mike D. Schiffman.

Alat Firewalk primjenjuje sve ranije navedene tehnike prikupljanja informacija. U početku je Firewalk bio konzolna aplikacija, dok je sa najnovijom inačicom firewalk/GTK dobio i grafičko sučelje.

5.1.1. Princip rada alata

Firewalk radi na način da šalje mnogo paketa na željeni vatrozid te sluša odzive sustava, bilježi ih i na temelju njih zaključuje kako izgledaju liste pristupa vatrozida (ACL). Alat radi u dvije faze - fazi otkrivanja mreže i fazi skeniranja.

Faza otkrivanja mreže radi vrlo slično kao *traceroute* alat. Na odredišni poslužitelj šalju se poruke sa poljem TTL koji se povećava od 1 na dalje te se prati odziv mreže. Sve to se radi da bi se saznala udaljenost (broj skokova) od izvorišnog poslužitelja do vatrozida. Na taj način se određuje zadnje računalo koje je odgovorilo prije vatrozida.

Nakon toga slijedi faza skeniranja. Alat *Firewalk* šalje TCP ili UDP pakete na razne priključnice (protokol ovisi o tome koja opcija je izabrana) i za svaki paket postavlja vremensko ograničenje (eng. *timeout*). Ukoliko vremensko ograničenje istekne prije nego što se vrati odgovor od vatrozida priključnica se smatra zatvorenom, u protivnom se smatra otvorenom.

```
zuul:#firewalk -n -P1-8 -pTCP 10.0.0.5 10.0.0.20
Firewalking through 10.0.0.5 (towards 10.0.0.20) with a maximum
of 25 hops.
Ramping up hopcounts to binding host...
probe:  1  TTL:  1  port 33434:  <response from> [10.0.0.1]
probe:  2  TTL:  2  port 33434:  <response from> [10.0.0.2]
probe:  3  TTL:  3  port 33434:  <response from> [10.0.0.3]
probe:  4  TTL:  4  port 33434:  <response from> [10.0.0.4]
probe:  5  TTL:  5  port 33434:  Bound scan: 5 hops <Gateway at
5 hops> [10.0.0.5]

port   1: open

port   2: open

port   3: open

port   4: open

port   5: open

port   6: open

port   7: *

port   8: open

13 packets sent, 12 replies received
```

Slika 14. Ispis alata Firewalk
Izvor: Cambridge Technology Partners

Problem predstavljaju paketi koji nisu odbačeni zbog vatrozida već iz drugih razloga (poslužitelj nije u funkciji, paket se izgubio, zagušenje mreže, IP adresa je iz nepovjerljivog izvora i sl.). Većinom se ti problemi mogu riješiti redundancijom poslanih poruka (kao i kod alata *traceroute*). Velik problem predstavlja situacija kada određeni paket neki poslužitelj odbaci prije nego on stigne do odredišnog poslužitelja na kojem je vatrozid. U toj situaciji se može činiti da je određena priključnica zatvorena iako je zapravo otvorena samo poruka do nje nije stigla.

Kako bi se riješila takva situacija odnosno spriječila pojava lažno zatvorenih priključnica izvodi se tzv. *slow walk*. *Slow walk* se također sastoji od dvije faze. Prva faza je jednaka prvoj fazi kod običnog skeniranja, dok se druga faza sastoji od skeniranja svakog

poslužitelja na putu do odredišnog. Na taj način je moguće izbjeći lažno negativne zatvorene priključnice, ali je skeniranje bitno usporeno.

5.1.2. Uporaba alata

Kao što je ranije naglašeno, alat se može koristiti kao konzolna aplikacija, a u novim inačicama i preko grafičkog sučelja.

Sintaksa naredbe u konzoli je sljedeća:

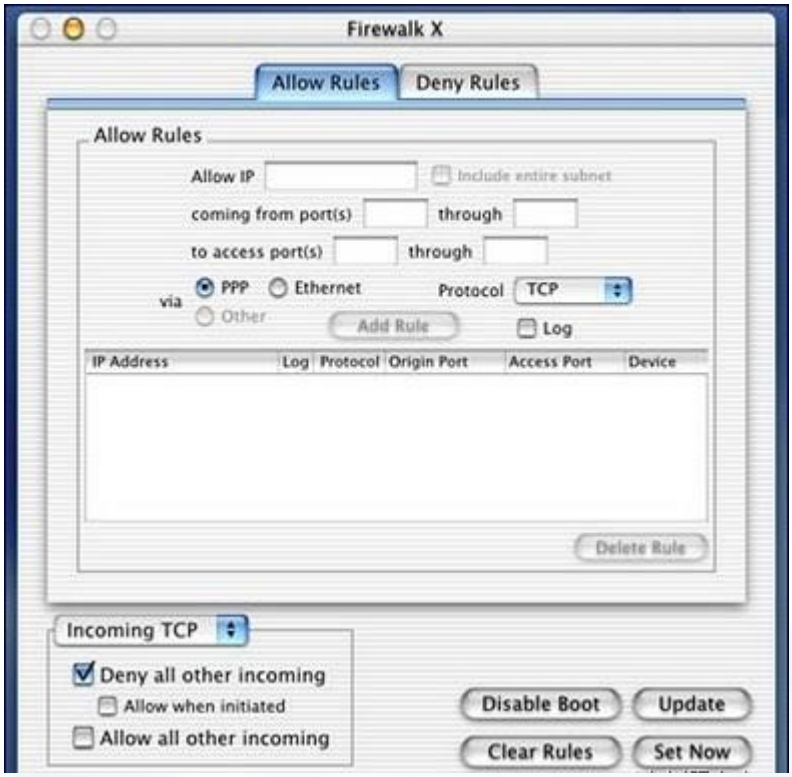
```
firewalk –p [protokol] –d [odredišna_priključnica] –s
[izvorišna_priključnica] [IP_vatrozida] [odredišni_IP]
```

Alat podržava i neke dodatne opcije. Tablica 1. prikazuje samo neke od važnijih opcija. Objašnjenja svih opcija mogu se pronaći na Internetu.

Opcija	Objašnjenje
-d	Odredišna priključnica koji se koristi u prvoj fazi rada alata (34434)
-h	Pomoć u programu
-P	Pauza između slanja poruka (sprječava da firewalk preplavi mrežu porukama)
-p	Protokol (TCP, UDP)
-S	Koje se sve priključnice skeniraju (navedeno u rasponima, npr. 1-130, 139, 1025)
-s	Izvorišna priključnica – u obe faze rada alata
-t	Mijenjanje početnog TTL (ovisi o udaljenosti vatrozida koji se želi skenirati)

Tablica 1. Opcije alata Firewalk
Izvor: CIS

Slika 14. prikazuje ispis alata Firewalk kao konzolna aplikacija, dok Slika 15. prikazuje grafičko sučelje alata Firewalk.



Slika 15. Firewalk – grafičko sučelje
Izvor: CIS

5.2. Ostali alati

Osim alata Firewalk čija je jedina namjena *firewalking*, postoji i nekolicina drugih alata koji mogu koristiti *firewalking* tehniku. Ti alati nude *firewalking* kao jednu od svojih ugrađenih mogućnosti ili se korištenjem tih alata uz malo truda može izvesti *firewalking* napad. Upravo iz razloga što *firewalking* nije njihova osnovna namjena, korištenje drugih alata za *firewalking* nešto je složenije od korištenja alata Firewalk.

5.2.1. Nmap

Nmap je programski alat namijenjen skeniranju otvorenih priključnica računala. Da bi to postigao služi se raznim tehnikama i nudi brojne druge mogućnosti. Osim svoje osnovne funkcionalnosti nudi izvođenje skripti koje imaju raznoliku namjenu (otkrivanje mreža, otkrivanje ranjivosti, iskorištavanje ranjivosti itd.). Skripte se izvode uz pomoć programske komponente koja se naziva Nmap Script Engine (NSE). Skripte mogu pisati korisnici za vlastitu namjenu, a s Interneta se također mogu preuzeti i već gotove skripte drugih korisnika. Na službenoj stranici alata Nmap također postoji repozitorij skripti složenih po kategorijama.

Skripta firewalk namijenjena alatu Nmap može se preuzeti sa službenih stranica alata. Napisana je po uzoru na alat Firewalk i koristi opisanu tehniku *firewalking*. Skripta je smještena u kategorije *safe* i *discovery*.

5.2.2. Hping

Hping je programski alat koji se koristi za skeniranje sustava i ispitivanje vatrozida. Alat pruža brojne mogućnosti, a neke od njih su slanje različitih paketa s različitim protokolima i

udaljeno skeniranje računala. Alatom se također mogu ispitivati odgovori poslužitelja. Zbog svojih mogućnosti alat Hping je povoljan za izvođenje *firewalking* napada, no izvođenje takvog napada malo je složenije nego korištenjem alata Firewalk. Razlog tome je što ne postoji automatizirana skripta niti dio programa koji bi sam izveo *firewalking* napad, već se paketi moraju ručno oblikovati i *firewalking* se mora izvoditi u koracima.

6. Primjena firewalkinga

Iako je *firewalking* relativno stara tehnika i danas se često koristi prilikom skeniranja mreža. *Firewalking* tehnika ima vrlo široku primjenu jer služi za prikupljanje informacija o sustavu. Prikupljene informacije se kasnije mogu koristiti u razne svrhe, no postupak prikupljanja je uvijek isti. Na *firewalking* se može gledati kao na napad ili dio napada jer se svaki pokušaj prikupljanja informacija u neetičke svrhe može smatrati napadom na sustav.

Primjena *firewalking* tehnike vrlo često nije sama po sebi dovoljna za prikupljanje svih potrebnih informacija o sustavu već se najčešće koristi zajedno s raznim drugim tehnikama i alatima. Primjena *firewalkinga* se često povezuje s korištenjem *port* skenera (npr. alat nmap). Važno je napomenuti kako *firewalking* nije alternativa skeniranju priključnica, već samo jedna od brojnih metoda kojom se skeniranje priključnica može izvesti. *Firewalking* tehnika može dati dodatne informacije o sustavu koji se skenira.

Nakon skeniranja sustava *firewalking* tehnikom potencijalni napadač može saznati na kojim priključnicama se promet ne filtrira uz pomoć vatrozida. Nakon toga nekom tehnikom može skenirati sustav i pronaći interne podmreže. Kada to zna može pokušati tunelirati pakete kroz dozvoljene priključnice i na taj način prodrijeti u sustav.

Ponekad je, ako se koristi alat Firewalk, potrebno nekoliko puta ponoviti skeniranje jer se ne može sa sigurnošću reći je li neka priključnica zaista zatvorena ili iz nekog drugog razloga ne šalje odgovore.

6.1. Primjena u penetracijskom testiranju

Penetracijsko testiranje ili etičko hakiranje je metoda provjere sigurnosti sustava koji se nalaze u neprijateljskom okruženju (najčešće Internet). Osoba koja izvodi testiranje simulira neprijateljskog napadača koji pokušava ugroziti sigurnost sustava. Prilikom penetracijskog testiranja osoba koja izvodi testiranje može koristiti širok spektar metoda, a cilj je pokušati ugroziti sustav na što više različitih načina.

Penetracijsko testiranje se najčešće izvodi u nekoliko faza. Faze su navedene u nastavku:

1. Prikupljanje informacija
2. Skeniranje
3. Pokušaj proboja (penetracije)
4. Zadržavanje pristupa i čišćenje tragova

Firewalking tehnika najčešće se primjenjuje u prve dvije faze penetracijskog testiranja.

Princip izvođenja *firewalking* napada je isti kao i kod korištenja *firewalkinga* u zloćudne svrhe iz razloga što osoba koja izvodi testiranje glumi napadača. Ne postoje propisani alati ili tehnike koji se moraju koristiti prilikom penetracijskog testiranja već svaka osoba ili organizacija koja izvodi testiranje sama izabire koje tehnike će koristiti. Ipak, *firewalking* je relativno često korištena tehnika prilikom penetracijskog testiranja. U svom radu koriste ju mnogi testeri bilo korištenjem alata Firewalk ili nekog drugog alata koji podržava mogućnost *firewalkinga*.

Glavna svrha korištenja *firewalking* tehnike prilikom penetracijskog testiranja je utvrditi koliko je siguran vatrozid promatranog sustava. Ukoliko osoba koja testira sustav uz pomoć *firewalking* tehnike otkrije neke informacije koje bi trebale biti zaštićene, potrebno je poduzeti mjere obrane od *firewalking* napada kako potencijalni napadači ne bi iskoristili te ranjivosti i neovlašteno pokušali ugroziti sigurnost sustava.

7. Obrana od firewalkinga

Firewalking tehnika može se pokazati kao štetna ukoliko se koristi u neetične svrhe. Stoga je vrlo važno biti svjestan mogućnosti takvog napada te poznavati mjere obrane.

Jedan od načina zaštite od *firewalking* napada je dobro podešavanje postavki vatrozida. Broj priključnica kroz koje vatrozid propušta promet trebao bi biti sveden na nužan minimum. Također je važno da administrator sustava u svakom trenutku zna koje priključnice su otvorene, a koji nisu.

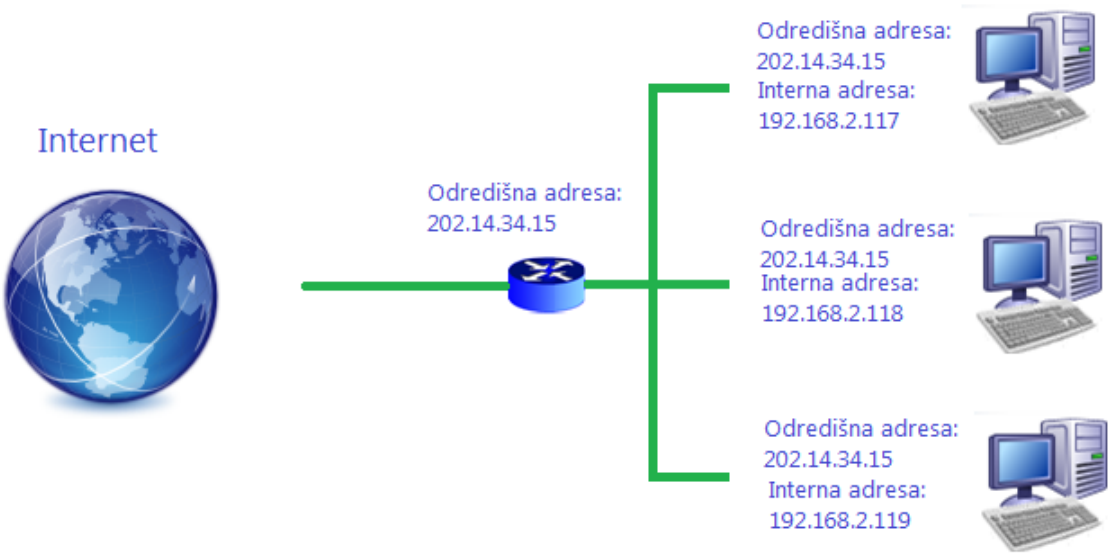
Drugi način je korištenje posredničkih (eng. *Proxy*) vatrozida jer se njihovim korištenjem ne mogu izvesti napadi temeljeni na TTL polju IP zaglavlja.

Za obranu od ove vrste napada moguće je također koristiti i vatrozide na višim razinama (primjerice vatrozide na aplikacijskom sloju).

Dodatna zaštita može se osigurati korištenjem IDS sustava (eng. *Intrusion Detection System*). *Firewalking* je metoda koja stvara mnogo mrežnog prometa. Moguće je da mrežni vatrozid ne stvara dnevničke zapise iz kojih bi se moglo otkriti napadača, no korištenjem IDS sustava moguće je otkriti neuobičajeno ponašanje u mreži. Važno je napomenuti da se čak i ako se koriste IDS sustavi, ne može jamčiti da će sustav biti siguran.

Jedno od možda najjednostavnijih rješenja ovog problema je onemogućiti izlazne *TTL Exceeded in Transit* poruke. No ukoliko se to primjeni, niti dobronamjerni korisnici neće moći koristiti alat *traceroute* (primjerice prilikom mrežne dijagnostike ili rješavanja nekog mrežnog problema).

Korištenje NAT protokola (eng. *Network Address Translation*) može biti jedna od mjera zaštite protiv *firewalking* napada. NAT protokol podrazumijeva mapiranje više internih računala na jednu IP adresu. Kada poruka stigne do poslužitelja, on može odrediti kojem je zapravo poslužitelju unutar lokalne mreže paket namijenjen te ga prosljeđuje na internu adresu tog poslužitelja. Internim adresama ne može se pristupiti izvan lokalne mreže te je stoga sustav siguran izvana.



Slika 16. NAT protokol
Izvor: CIS

Dobra praksa je također tzv. *Defense in depth* načelo. To načelo podrazumijeva korištenje više različitih metoda zaštite kako bi sustav bio sigurniji. Stoga je moguće istovremeno primijeniti i nekoliko gore navedenih metoda.

8. Zaključak

Uz sve veći broj korisnika Interneta raste i potreba za sve većom sigurnosti računalnih sustava. Prilikom izrade i održavanja računalnih sustava uvijek je dobro biti svjestan što većeg broja sigurnosnih prijetnji da bi se od njih bilo moguće obraniti. *Firewalking* tehnika ne spada u vrlo profinjene vrste napada, te ukoliko je administrator sustava svjestan mogućnosti napada može svoj sustav vrlo učinkovito zaštititi od takve vrste napada.

Važno je primijetiti kako *firewalking* kao vrlo jednostavna metoda, temeljena na alatu *traceroute* koji je prisutan u većini operacijskih sustava, može ozbiljno ugroziti sigurnost sustava. Upravo jednostavnost tehnike jedna je od njenih velikih prednosti. Većina vatrozida uopće ne bilježi promet na dozvoljenim priključnicama i zbog toga pažljivi napadač može prikupiti mnogo informacija o sustavu bez da ostavi tragove u dnevničkim zapisima vatrozida.

Firewalking je u suštini tehnika napada na sustav, i kao takva često je korištena u zloćudne svrhe. No, ne mora se uvijek primjenjivati na taj način. Poznavanje te tehnike može pomoći u obrani sustava od napadača (npr. penetracijsko testiranje).

Također, važno je istaknuti kako su mete *firewalking* napada vatrozidi, čija je osnovna namjena zaštita računalnih sustava. Korištenje vatrozida, ali i bilo kojih drugih sigurnosnih komponenti kod neiskusnih korisnika može izazvati lažni osjećaj sigurnosti. Zaključak ovoga dokumenta nikako ne bi smio biti da se vatrozidi zbog svoje nesigurnosti ne bi smjeli koristiti, već naprotiv da se zaštita sustava provodi slojevito, korištenjem više različitih sigurnosnih komponenti i tehnika zaštite.

9. Leksikon pojmova

Ping

Naredba pomoću kojeg je moguće provjeriti da li neko računalo na Internetu radi i koliko mu je vremena potrebno da odgovori na neki upit. Naredba se zadaje u obliku ping ime-računala
https://kb.iu.edu/data/aopu.html
http://www.manpagez.com/man/8/ping/

Priključnica

Krajnje točke u komunikaciji transportnih protokola - Brojčane vrijednosti temeljem kojih računalo po prihvatu podataka zna koju uslužnu programsku potporu (servise) mora aktivirati te na koji način razmjenjivati podatke na transportnom sloju.

http://searchnetworking.techtarget.com/definition/port-number
http://www.iana.org/assignments/port-numbers

TCP - Transmission Control Protocol

Jedan od dva protokola usmjeravanja koja se koriste u Internetu, uspostavlja logičku vezu između krajnjih računala i osigurava pouzdani prijenos. TCP se nalazi na transportnom sloju OSI modela. - Jedan od dva protokola usmjeravanja koja se koriste u Internetu. Uspostavlja logičku vezu između krajnjih računala i osigurava pouzdani prijenos.

http://www.webopedia.com/TERM/T/TCP.html
http://www.networksorcery.com/enp/protocol/tcp.htm
http://searchnetworking.techtarget.com/definition/TCP

Usmjernik

Uređaj koji usmjerava pakete između računalnih mreža - Usmjernici su uređaji koji imaju barem dva sučelja na različitim mrežama, a usmjeravaju pakete do njihovog odredišta. Na svom putu, paketi prolaze kroz nekoliko usmjernika, a svaki zasebno određuje put kojim će ga dalje slati.

http://www.webopedia.com/TERM/R/router.html
http://searchnetworking.techtarget.com/definition/router

IP protokol

Internet Protocol - IP je jedan od glavnih protokola u Internetu, a koristi se za usmjeravanja paketa kroz Internet. U tu namjenu, dodjeljuje IP adrese izvora paketa i njegovog odredišta na temelju kojih će se paketi usmjeravati kroz nekoliko računalnih mreža.

http://compnetworking.about.com/od/networkprotocolsip/g/ip_protocol.htm

VoIP - Voice over IP

VoIP je skup internetskih tehnologija, komunikacijskih protokola i tehnologija prijenosa kako bi se ostvario prijenos govora preko IP mreže. VoIP koristi protokole za podršku sjednice poput SIP-a i SAP-a za uspostavljanje i raskid sjednica, tj. poziva.

http://voip.about.com/od/voipbasics/a/whatisvoip.htm
http://www.edinformatics.com/internet/voice_over_IP.htm
http://transition.fcc.gov/voip/

Vatrozid

Vatrozid (eng. *Firewall*) je skup komunikacijskih nakupina koji služe kako bi odvojili privatnu mrežu od javne. Sastoje se od programa koji služe kako bi pratili i upravljali promet između računala i mreža. Vatrozidi mogu propuštati, blokirati, šifrirati promet na temelju pravila koja korisnik postavlja.

http://searchsecurity.techtarget.com/definition/firewall
http://kb.iu.edu/data/aoru.html

DNS - Domain Name System

Domain Name System (DNS) je hijerarhijski sustav imenovanja izgrađen na distribuiranim bazama podataka za računala, usluge ili bilo koji resurs spojen na Internet ili privatnu mrežu.

http://www.kb.iu.edu/data/adns.html
http://www.webopedia.com/TERM/D/DNS.html
http://searchnetworking.techtarget.com/definition/domain-name-system

Napad grubom silom

U kriptografiji napad grubom silom podrazumijeva strategiju pronalaska tajnog ključa ili lozinke koja se, u teoriji, može iskoristiti protiv svakog kriptografskog algoritma. Općenito podrazumijeva sistematično isprobavanje svih mogućih kombinacija dok se ne otkrije ispravna. U najgorem slučaju mora se proći kroz sve mogućnosti.

http://www.computerhope.com/jargon/b/brutforc.htm
http://www.imperva.com/resources/glossary/brute_force.html
https://www.owasp.org/index.php/Brute_force_attack

TTL - Time to live

U IP protokolu TTL označava koliko još usmjeritelja podatkovni paket smije proći prije nego dođe do odredišta. Neki drugi protokoli TTL-om označavaju koliko dugo neka informacija smije postojati prije nego se odbaci jer je zastarjela.

http://searchnetworking.techtarget.com/definition/time-to-live
http://kb.mediatemple.net/questions/908/Understanding+TTL+%28time-to-live%29

10. Reference

[1] David Goldsmith, Michael Schiffman: Firewalking, http://packetfactory.openwall.net/projects/firewalk/firewalk-final.pdf, srpanj 2012.

[2] David Irby: Firewalk: Can Attackers See Through Your Firewall, http://www.giac.org/paper/gsec/312/firewalk-attackers-firewall/100588, srpanj 2012.

[3] Firewalk, http://packetfactory.openwall.net/projects/firewalk/index.html, srpanj 2012.

[4] O'Reilly Media: Advanced IP Network Scanning Methods, http://www.codewalkers.com/c/a/Server-Administration/Advanced-IP-Network-Scanning-Methods/, srpanj 2012.

[5] A description on how to use the Firewalk network tool, http://www.hacktoolrepository.com/article/10/A%20description%20on%20how%20to%20use%20the%20Firewalk%20network%20tool, srpanj 2012.

[6] Chinmayee N.: A seminar on Firewalking, http://seminarsonly.files.wordpress.com/2009/03/firewalking.doc, srpanj 2012.

[7] Michael Schiffman: Firewalk, http://www.scribd.com/doc/81321212/FireWalk-Attack, srpanj 2012

[8] Firewall Testing From the Eye of a Hacker, http://www.vesaria.com/Firewall/Testing/eye_of_hacker.php, srpanj 2012.