HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Otkrivanje operacijskih sustava udaljenih računala

CCERT–PUBDOC–2007–11–210

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 4

2. METODE OTKRIVANJA UDALJENIH OPERACIJSKIH SUSTAVA 5

2.1. „KLASIČNO“ OTKRIVANJE UDALJENIH OPERACIJSKIH SUSTAVA 5
2.2. AKTIVNO OTKRIVANJE UDALJENIH OPERACIJSKIH SUSTAVA 5
2.3. PASIVNO OTKRIVANJE UDALJENIH OPERACIJSKIH SUSTAVA 6
2.4. OTKRIVANJE OPERACIJSKIH SUSTAVA NA TEMELJU SIGURNOSNIH PROPUSTA 7
2.5. OTKRIVANJE OPERACIJSKIH SUSTAVA ANALIZOM HTTP PROMETA 8

3. PREGLED ALATA ZA OTKRIVANJE OPERACIJSKIH SUSTAVA 9

3.1. *NMAP* 9
3.2. *RINGV2* 10
3.3. *P0F* 10
3.4. *HTTPRINT* 11
3.5. *XPROBE2* 11

4. IZBJEGAVANJE UDALJENOG OTKRIVANJA OPERACIJSKOG SUSTAVA 12

4.1. IZMJENA POZDRAVNIH PORUKA 12
4.2. UKLANJANJE ZNAKOVNIH NIZOVA 12
4.3. GAŠENJE NEPOTREBNIH USLUGA 13
4.4. ONEMOGUĆAVANJE ISPITNIH PORUKA 13

5. ZAKLJUČAK 14

6. REFERENCE 14

1. Uvod

Otkrivanje operacijskih sustava udaljenih računala provodi se usporedbom mrežnih podatkovnih paketa danog računala s odgovorima poznatih operacijskih sustava. Izvorni engleski nazivi takvih metoda, *OS fingerprinting* (eng. *Operating System*) ili *TCP/IP stack fingerprinting* (eng. *Transmission Control Protocol/Internet Protocol*), dobro ih opisuju usporedbom s uzimanjem otiska prsta (eng. *fingerprinting*). Kao što je identitet osobe moguće otkriti usporedbom njena otiska prsta s otiscima u policijskoj arhivi, tako je moguće utvrditi operacijski sustav udaljenog računala usporedbom njegova mrežnog prometa s karakterističnim „mrežnim otiscima" operacijskih sustava iz prethodno stvorene baze podataka.

Operacijski sustav koji se izvodi na udaljenom računalu moguće je otkriti prisluškivanjem mrežnih podatkovnih paketa koji u normalnom radu putuju među računalima. Takve metode otkivanja operacijskog sustava nazivaju se pasivnima. Aktivne metode uključuju slanje posebno oblikovanih podatkovnih paketa računalu čiji je operacijski sustav potrebno otkriti te analizu odgovora spomenutog računala. Ove metode u radu koriste sigurnosni stručnjaci, ali i zlonamjerni korisnici, za stvaranje mapa udaljenih računalnih mreža te za utvrđivanje potencijalnih sigurnosnih nedostataka u njima.

U dokumentu je dan pregled metoda otkrivanja operacijskih sustava udaljenih računala podijeljenih u pet skupina: klasične, aktivne i pasivne metode, metode temeljene na sigurnosnim propustima te one koje provode analizu HTTP prometa. Nakon toga slijedi kratak opis *Nmap*, *RINGv2*, *p0f*, *HTTPrint* i *xprobe2* popularnih alata za udaljeno otkrivanje operacijskih sustava. Na kraju dokumenta navedene su tehnike izbjegavanja otkrivanja operacijskih sustav.

2. Metode otkrivanja udaljenih operacijskih sustava

2.1. „Klasično“ otkrivanje udaljenih operacijskih sustava

Pojedina udaljena računala izvješćuju svakog korisnika koji se na njih spoji o svom operacijskom sustavu pa nije niti potrebno koristiti posebne tehnike. Na primjer, često se prilikom povezivanja na udaljeno računalo prema Telnet (eng. *TELecommunication NETwork*) protokolu korisnika putem pozdravne poruke obavješćuje o inačici operacijskog sustava na kojem se usluga izvodi.
FTP (eng, *File Transfer Protocol*) protokol također često pruža takve informacije, bilo u sklopu pozdravne poruke (eng. *banner*) ili ako ga se prozove SYST naredbom. I HTTP (eng. *HyperText Transfer Protocol*) protokol može biti iskorišten za otkrivanje udaljenog operacijskog sustava slanjem

```
GET / HTTP/1.0\n
```

zahtjeva.
Ako je na udaljenom računalu prisutan SNMP (eng, *Simple Network Management Protocol*) protokol na UDP (eng. *User Datagram Protocol*) portu 161 i ako je ostavljeno izvorno „*public*“ ime skupine (eng, *community name*) moguće je detaljno udaljeno ispitivanje ove usluge, a preko nje i računala na kojem se izvodi.
Protokoli koji omogućuju jednostavno otkivanje operacijskog sustava udaljenog računala uključuju:

- POP2 i POP3 (eng. *Post Office Protocol*),
- SMTP (eng. *Simple Mail Transfer Protocol*),
- SSH (eng. *Secure Shell*),
- NNTP (eng. *Network News Transfer Protocol*) i
- FINGER protokole.

Ako je na udaljenom računalu omogućeno stvaranje anonimnog FTP računa, moguće je preuzimanjem javne binarne datoteke, potrebne za rad FTP protokola (npr. datoteke */bin/ls*), utvrditi za koji operacijski sustav je ona oblikovana.
Jednostavniji način utvrđivanja operacijskog sustava udaljenog računala svakako je skeniranje njegovih priključaka (eng. *port scan*) nekim od raspoloživih alata, kao što su *Nessus* i *SAINT* (eng. *Security Administrator's Integrated Network Tool*) alati. Analizom liste dostupnih priključaka ponekad je moguće, njenom usporedbom s obrascima poznatih operacijskih sustava, utvrditi o kojem operacijskom sustavu se radi.
Operacijski sustav moguće je utvrditi i potpuno netehničkim metodama socijalnog inženjeringa, na primjer upoznavanjem sa sustavom kroz telefonske razgovore s korisnicima ciljanog računala ili IM (eng. *Instant Messaging*) komunikacijom sa sistemskim administratorom.

2.2. Aktivno otkrivanje udaljenih operacijskih sustava

Aktivne metode otkrivanja operacijskih sustava udaljenih računala najčešće su korištene, a sastoje se od slanja zahtjeva udaljenom računalu te pažljive analize tako iznuđenog odgovora. Ova skupina metoda uključuje

- **FIN sondiranje** – na poznati otvoreni priključak šalje se jedna poruka s postavljenom FIN (eng. *FINished*) zastavicom. Spomenutom zastavicom označuje se prestanak komunikacije pa ju operacijski sustavi ne očekuju ukoliko veza nije ostvarena. Uobičajeno ponašanje prilikom primitka neočekivane poruke s FIN zastavicom je njezino ignoriranje, no pojedini operacijski sustavi na takvu poruku odgovaraju RST (eng. *ReSet*) porukom. To može biti jedan od tragova za utvrđivanje operacijskog sustava.
- **TCP ISN uzorkovanje** – TCP protokol u radu koristi brojčane oznake za praćenje broja uspješno prenesenih okteta. Kod otvaranja nove veze operacijski sustav odabire početni ISN (eng. *Initial Sequence Number*) broj kojim započinje novi niz. Ovaj broj može bit konstanta, nasumični inkrement prošle vrijednosti, pseudonasumični ili pravi nasumični broj, ovisno o operacijskom sustavu.

- **ICMP citiranje** – Poruke o pogreškama ICMP (eng. *Internet Control Message Protocol*) protokola trebaju, zbog identifikacije, sadržavati manji dio zahtjeva koji je uzrokovao pogrešku (eng. *error quoting*), ali kod nekih operacijskih sustava ove poruke proširene su dodatnim sadržajima. Ovo je naročito korisno za identificiranje operacijskih sustava koji nemaju otvorenih portova na kojima očekuju poruke (eng. *listening port*).
- **ICMP TOS** – gotovo svi operacijski sustava u TOS (eng. *Type of Service*) polju poruke o nedostupnosti ICMP porta šalju nulu. Iznimka su Linux operacijski sustavi koje je na ovaj način moguće identificirati.
- **TCP Options** – dodatne mogućnosti TCP protokola predstavljaju njegovu nadogradnju koja omogućuje rad u nepouzdanim mrežama s velikim kašnjenjima. Broj podržanih dodatnih mogućnosti, kao i njihov redoslijed, mogu odati koji operacijski sustav se izvodi na udaljenom računalu.
- **Analiza usluga** – usluge, čija je prisutnost na udaljenom računalu utvrđena snimanjem portova, moguće je dodatno analizirati s ciljem identificiranja operacijskog sustava. Primjer pozadinskih aplikacija (eng. *daemon*) koje različito odgovaraju na određene zahtjeve, ovisno o operacijskom sustavu na kojem se izvode, su LDP (eng. *Label Distribution Protocol*), FTP, SMTP te pozadinske aplikacije za ispis na pisaču.
- **TCP ponovno slanje** – TCP protokol građen je tako da zahtijeva uspostavljanje i potvrđivanje veze te potvrdu primitka svakog paketa. U slučaju izostanka potvrde nedostavljeni paket se ponovno šalje. Izvorna inačica standarda (RFC 793) ne definira algoritam odabira vremena ponovnog slanja, dok su kod nove inačice (RFC 2988) ova vremena točno definirana. Činjenicu da pojedini operacijski sustavi implementiraju stariju inačicu standarda, ili različito interpretiraju noviju, moguće je iskoristiti za njihovo identificiranje. Postupak se sastoji od slanja SYN (eng. *SYNchronize*) paketa i neodgovaranja na pristigle SYN–ACK (eng. *ACKnowledge*) pakete. Pri tome se mjere vremena između uzastopnih pokušaja potvrđivanja veze i ona se uspoređuju s obrascima karakterističnima za određene operacijske sustave.

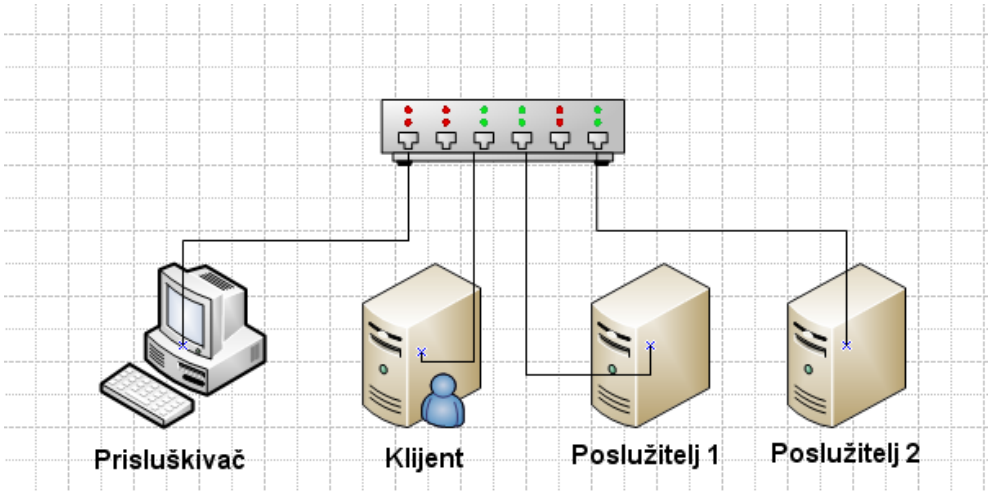
Gotovo svi alati za aktivno otkrivanje operacijskog sustava udaljenih računala koriste neke ili sve od navedenih metoda kako bi prikupili podatke i potom ih usporedili s vlastitom bazom podataka o poznatim operacijskim sustavima. Popularnost i zrelost takvih alata često je moguće procijeniti iz veličine njihovih baza podataka.

2.3. Pasivno otkrivanje udaljenih operacijskih sustava

Pasivno otkrivanje operacijskih sustava udaljenih računala provodi se prikupljanjem i analizom mrežnog prometa (eng. *sniffing*). Ovakve tehnike imaju očitih nedostataka kod spojnih (eng. *switched*) mreža jer prisluškivač mora biti na istom čvorištu (eng. *hub*) na kojem se nalaze poslužitelji i klijentska računala čije operacijske sustave je potrebno otkriti (*Slika 1*).

Alati za pasivno utvrđivanje udaljenih operacijskog sustava primjenjuju podskup tehnika koje u radu koriste aktivni alati. Pasivni alati, naime, nadziru samo legitiman promet, bez uvođenja posebno oblikovanih podatkovnih paketa na mrežu.

Za razliku od tehnika aktivnog otkrivanja udaljenih operacijskih sustava, koje u kratkom vremenu omogućuju obradu većih mreža, pasivno otkrivanje je znatno sporiji proces koji najbolje rezultate daje ako se primijeni na podacima prikupljenima kroz dulje razdoblje. Osnovnu prednost pasivnih metoda tako predstavlja mogućnost pretraživanja dnevničkih zapisa vatrozida i IDS (eng, *Intrusion Detection Systems*) sustava.



Slika 1: Prisluškivač mora biti na istom čvorištu na kojem se nalaze poslužitelji i klijentska računala čije operacijske sustave je potrebno otkriti

Kod prikupljenih mrežnih paketa ove metode najčešće pretražuju:

- TTL (eng. *Time To Live*) polje zaglavlja IP protokola u kojem je pohranjen maksimalan broj usmjerivača kroz koje paket može proći prije njegova odbacivanja. Pošiljatelj zapisuje ovaj broj u zaglavlje te se on prolaskom kroz svaki usmjerivač umanjuje za jedan. Kad se TTL broj izjednači s nulom pošiljatelja se o gubitku paketa obavješćuje ICMP porukom. Spomenuti boj razlikuje se kod pojedinih operacijskih sustava, na primjer kod Windows operacijskih sustava ima vrijednost 32, a kod Linux operacijskih sustava 64.
- Win (eng. *Window Size*) polje zaglavlja TCP protokola. Operacijsku sustav tijekom otvaranja veze u ovo polje pohranjuje veličinu spremnika za primitak poruka tako da drugo računalo može prilagoditi brzinu slanja paketa.
- DF (eng. *Don't Fragment*) zastavica zaglavlja IP protokola kojom se onemogućuje rastavljanje paketa na manje dijelove. Ako je ova zastavica postavljena i ako je paket prevelik s obzirom na mogućnosti mreže, bit će odbačen uz slanje ICMP poruke o pogrešci pošiljatelju.
- TOS (eng. *Type Of Service*) polje zaglavlja IP protokola koje sadrži četiri zastavice:
  - minimiziraj kašnjenje,
  - maksimiziraj propusnost,
  - maksimiziraj pouzdanost i
  - minimiziraj financijski trošak.

  Različite usluge koriste različite postavke ovih zastavica. Na primjer ovo polje omogućuje razlikovanje Telnet i SNMP paketa.

Pored pobrojanih pokazatelja pasivne metode prilikom otkrivanje udaljenih operacijskih sustava koriste i ISN broj, IP identifikacijski broj, postavke TCP i/ili IP protokola, sadržaj ICMP paketa idr.

2.4. Otkrivanje operacijskih sustava na temelju sigurnosnih propusta

Ako se sve navedene metode otkrivanja udaljenog operacijskog sustava pokažu neuspješnima moguće je pribjeći agresivnijoj metodi temeljenoj na sigurnosnim propustima svojstvenim za pojedine operacijske sustave. Osnovna pretpostavka je da se sigurnosne zakrpe primjenjuju dinamikom kojom se otkrivaju ranjivosti. Ako napadač krene s pokušajima iskorištavanja sigurnosnih propusta od starijih ka novijima, vjerojatno je da će jedan od pokušaja biti uspješan ukazujući pri tom o kojoj inačici operacijskog sustava se radi.

Na primjer, *Windows 95, 98* i *NT4* operacijske sustave teško je razlikovati zbog toga što se kod njih implementacije TCP protokola razlikuju tek neznatno. Pokušaj izvođenja osnovnog *WinNuke* napada i kronološkim napredovanjem prema novijim napadima s vremenom će otkriti ranjivost ciljnog operacijskog sustava te istovremeno i njegovu inačicu i/ili razinu nadograđenosti.

2.5. Otkrivanje operacijskih sustava analizom HTTP prometa

Prvi korak u postupku otkrivanja operacijskog sustava može biti otkrivanje inačice HTTP poslužitelja koja se izvodi na udaljenom računalu. Ovaj postupak provodi se analizom HTTP mrežnog prometa. Odgovore web poslužitelja moguće je jednostavno prilagoditi izmjenama konfiguracijske datoteke ili instalacijom dodataka (eng. *plug–ins*), pa je otkrivanje značajki operacijskog sustava analizom HTTP prometa (eng. *HTTP fingerprinting*) nešto složenije od analize TCP/IP protokola. Naime, za izmjenu implementacije TCP/IP stoga potreban je pristup programskom kodu na razini jezgre operacijskog sustava.

Najjednostavniji način identificiranja web poslužitelja je analiza *Server* polja unutar zaglavlja HTTP odgovora. Korištenjem TCP klijenta, npr. *netcat*, moguće je poslužitelju poslati zahtjev za slanjem odgovora koji sadrži spomenuto zaglavlje. Kako bi onemogućili brojne automatizirane napade na HTTP poslužitelje, administratori često izmjenjuju zaglavlja HTTP poruka. Ovo je kod poslužitelja otvorenog programskog koda vrlo jednostavno učiniti izmjenama koda i ponovnim prevođenjem. Izmjene nisu tako jednostavne kod komercijalnih paketa, ali su ipak moguće, na primjer izmjenama binarne datoteke, pomoću tzv. *hex* editora, ili programiranjem vlastitog dodatka poslužitelju. Dostupni su i komercijalni alati, kao *ServerMask*, koji izmjenama zaglavlja maskiraju HTTP poslužitelja.

Gotovi svi web poslužitelji razlikuju se po implementaciji HTTP protokola. Na ispravno oblikovane dobronamjerne zahtjeve većina poslužitelja odgovara jednako, u skladu sa standardom, no odgovori se mogu razlikovati u slučaju posebno oblikovanih zahtjeva. Ove razlike čine karakterističan otisak pojedinog poslužitelja. U tablici *Tablica 1* dani su primjeri zahtjeva na koje se odgovori pojedinih HTTP poslužitelja mogu razlikovati.

ZAHJEV	OČEKIVANI ODGOVOR
HEAD / HTTP/1.0	Normalan odgovor s HTTP zaglavljem.
DELETE / HTTP/1.0	Odgovor za slučaj u kojem DELETE operacija nije dozvoljena.
GET / HTTP/3.0	Odgovor na zahtjev s neispravnom oznakom inačice protokola.
GET / JUNK/1.0	Odgovor na zahtjev s neispravnom oznakom protokola.

Tablica 1: HTTP zahtjevi za otkrivanje poslužitelja i očekivani odgovori.

Primjeri odgovora Apache 1.3.23, Microsoft–IIS 5.0 i Netscape–Enterprize 4.1 poslužitelja na pobrojane zahtjeve dani su u tablici *Tablica 2*. U prvom stupcu navedeni su ispitivani poslužitelji, u drugom raspored polja u odgovorima na normalan zahtjev, u trećem vrijednost oznake odgovora na zahtjev s nedozvoljenom DELETE operacijom. Četvrti stupac sadrži vrijednost oznake odgovora na zahtjev s neispravnom oznakom inačice protokola dok su u posljednjem stupcu navedene vrijednosti oznake odgovora na zahtjev s neispravnom oznakom protokola.

POSLUŽITELJ	POLJA	DELETE	INAČICA	PROTOKOL
Apache 1.3.23	Date, Server	405	400	200
Microsoft–IIS 5.0	Server, Date	403	200	400
Netscape–Enterprize 4.1	Server, Date	401	505	nema zaglavlja

Tablica 2: Razlike u odgovorima pojedinih HTTP poslužitelja

Jasno, alati za otkrivanje web poslužitelja analizom HTTP prometa provode daleko veći broj testova. Nakon stvaranja otiska nepoznatog poslužitelja potrebno je odrediti kojem je od otisaka poznatih poslužitelje najsličniji. Postupke usporedbe moguće je podijeliti u dvije skupine:

- Testovi temeljeni na stablu odluka (eng. *decision tree*) postupno eliminiraju pojedine inačice poslužitelja. Takvi su testovi složeni zbog toga što svaki razmatrani poslužitelj daje svoj doprinos stablu odluka. Dodavanje novog HTTP poslužitelja zahtijeva izgradnju potpuno novog stabla odluka.
- Statistička analiza temelji se na određenom broju testova koji kao rezultate daju vrijednosti, tzv. težine (eng. *weight*), pridružene svakom od razmatranih poslužitelja. Konačna odluka o kojem poslužitelju se u danom slučaju radi donosi se usporedbom različitih težina pridijeljenih svakom poslužitelju. Preciznost ovakvih testova određena je algoritmima za dodjeljivanje i usporedbu težina.

3. Pregled alata za otkrivanje operacijskih sustava

3.1. *Nmap*

Nmap je alat otvorenog programskog koda namijenjen istraživanju računalne mreže brojnim tehnikama uz korištenje TCP, ICMP, UDP i IP protokola. Ovaj programski paket omogućuje:

- otkrivanje računala prisutnih na mreži,
- pobrojavanje otvorenih portova na pojedinim računalima,
- utvrđivanje raspoloživih usluga na pojedinim računalima te njihovih inačica i
- identificiranje operacijskih sustava.

Prvi korak u otkrivanju operacijskog sustava udaljenog računala je pretraživanje portova udaljenog računala. *Nmap* najbolje rezultate postiže ukoliko na ciljanom računalu otkrije jedan otvoren TCP port te po jedan zatvoren TCP i UDP port. Nakon toga alat provodi niz testova:

- T1 (test 1) – slanje TCP paketa s postavljenim SYN i ECN–Echo (eng. *Explicit Congestion Notification*) zastavicama na otvoreni TCP port,
- T2 – slanje TCP paketa bez postavljenih zastavica, tzv. NULL paketa, na otvoreni TCP port,
- T3 – slanje TCP paketa s postavljenim URG (eng. *URGent*), PSH (eng *PuSH*), SYN i FIN zastavicama na otvoreni TCP port,
- T4 – slanje TCP paketa s postavljenom ACK zastavicom na otvoreni TCP port,
- T5 – slanje TCP paketa s postavljenom SYN zastavicom na zatvoreni TCP port,
- T6 – slanje TCP paketa s postavljenom ACK zastavicom na zatvoreni TCP port,
- T7 – slanje TCP paketa s postavljenim URG, PSH i FIN zastavicama na zatvoreni TCP port
- PU (eng. *Port Unreachable*) – slanje UDP paketa na zatvoreni UDP port s ciljem dobivanja odgovora u obliku ICMP paketa s porukom o nedostupnosti porta,
- TSeq (eng. *TCP sequencability test*) – posljednji test koji Nmap provodi predstavlja, već opisano, TCP ISN uzorkovanje.

Nakon prikupljanja rezultata provedenih testova, *Nmap* stvara otisak nepoznatog operacijskog sustava i uspoređuje ga s otiscima u bazi podataka. U slučaju poklapanja javlja se poruka o uspješnom otkrivanju operacijskog sustava. Ako otisak nije pronađen u bazi podataka korisniku se nudi da, ukoliko zna o kojem operacijskom sustavu se radi, uvede novi otisak u bazu podataka putem web sučelja.

Prednosti *Nmap* programskog paketa pred drugim alatima za aktivno otkrivanje operacijskih sustava udaljenih računala su:

- Podržava tzv. *half–open* pretraživanje portova kod kojeg klijent prekida komunikaciju prije završetka TCP rukovanja (eng. *TCP three–way handshake*) pa većina osnovnih alata za uočavanje neovlaštenog pristupa računalu neće uočiti niti zabilježiti takvo pretraživanje.
- Provodi različite testove koristeći više protokola čime povećava vjerojatnost uspješnog otkrivanja operacijskog sustava i u slučaju prisutnosti filtriranja određenih vrsta prometa. Na primjer, kod pojedinih mreža može biti onemogućen ICMP promet pa pojedine *Nmap* testove nije moguće provesti.
- Velika baza podataka s preko 800 otisaka operacijskih sustava.
- Dobra podržanost različitih mrežnih uređaja kao što su usmjerivači, vatrozidi, prespojnici i pisači.
- Prema izvornim postavkama uspoređivanje prikupljenih otisaka s onima u bazi podataka provodi se prema strogim pravilima, ali uspoređivanje je moguće provesti i korištenjem neizrazite logike (eng. *fuzzy matching*).
- Ugrađene mogućnosti učenja.

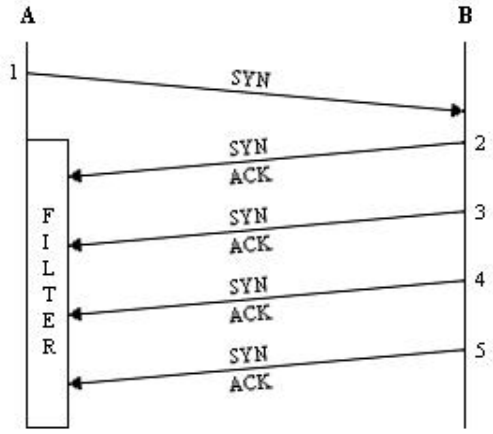
Moguće je primijeniti različite metode zaštite od otkrivanja operacijskog sustava pomoću *Nmap* alata, među ostalima:

- Uobičajene mrežne sustave preporučeno je zaštititi vatrozidom. Kod računala s vanjskim pristupom promet prema nekorištenim portovima treba tada onemogućiti. Ovime se *Nmap* alatu smanjuje broj izvodivih testova, a time i preciznost.
- Implementacije TCP/IP protokola moguće je izmijeniti, na primjer primjenama zakrpama jezgre operacijskog sustava, te tako promijeniti njegov otisak.

- IDS sustave za uočavanje neovlaštenog pristupa moguće je postaviti tako da uočavaju pokušaje otkrivanja operacijskog sustava pomoću *Nmap* alata zbog korištenja posebno oblikovanih mrežnih paketa.

3.2. *RINGv2*

RINGv2 je alat za otkrivanje operacijskog sustava udaljenog računala uz minimiziranje smetnji. Dostupan je kao dodatak *Nmap* programskom paketu, koji se tada naziva *Nmap–ringv2*. Ovaj alat koristi SYN_RCVD metodu otkrivanja operacijskog sustava koja se temelji na mjerenju RTO (eng. *Retransmission TimeOut*) vremena ponovnog slanja SYN–ACK paketa. Prvi korak ove metode je onemogućavanje primitka TCP paketa s postavljenim SYN i ACK zastavicama od računala kojeg korisnik odredi. Zatim se tom računalu na otvoreni TCP port šalje TCP paket s postavljenom SYN zastavicom. Udaljeno računalo pokušava potvrditi uspostavljanje veze slanjem SYN–ACK paketa, koji bivaju filtrirani uz mjerenje vremena između uzastopnih pokušaja. Opisani postupak prikazan je slikom *Slika 2*. Snimljena vremena predstavljaju otisak operacijskog sustava udaljenog računala koji se potom uspoređuje s otiscima poznatih operacijskih sustava u bazi podataka.



Slika 2: Ilustracija SYN_RCVD metode

Prednosti ovog alata, odnosno tehnike, su:

- Za uspješno otkrivanje operacijskog sustava *RINGv2* alatu dovoljan je jedan otvoreni TCP port. Kod računala koja su zaštićeni nekim od uređaja za filtriranje prometa najčešće je dostupan samo jedan TCP port, dok se paketi prema ostalim portovima filtriraju.
- Ova tehnika koristi standardni TCP paket tijekom pokušaja uspostavljanja uobičajene TCP veze, koja se nikad ne uspostavlja. Zbog toga ne dolazi do poremećaja udaljenog računala.
- Alat ima ugrađenu mogućnost učenja otisaka novih operacijskih sustava.

Vjerojatnost otkrivanja operacijskog sustava pomoću *RINGv2* alata moguće je smanjiti:

- postavljanjem računala iza vatrozida ili nekog drugog uređaja za filtriranje prometa. Preporuča se zatvoriti sve nepotrebne portove, a zatvaranjem svih TCP portova potpuno se onemogućuje otkrivanje operacijskog sustava pomoću ovog alata.
- Korištenjem alata kao što je *netfilter/iptables* moguće je izmijeniti RTO vremena svih odlaznih paketa te tako udaljenog korisnika koji pokušava otkriti operacijski sustav navesti na krivi trag.
- Postavljanjem računala iza *proxy* poslužitelja ili iza vatrozida koji podržava *SYN Relay* ili *SYN Gateway* tehnike moguće ga je efektivno skriti od *RINGv2* alata.

3.3. *p0f*

P0f (eng. *Passive OS Fingerprinting*) je alat za pasivno otkrivanje udaljenih operacijskih sustava udaljenih računala namijenjen Linux i Windows operacijskim sustavima. Omogućuje pretraživanje dnevničkih zapisa vatrozida, IDS sustava, usmjerivača i drugih mrežnih komponenti tako da je

operacijski sustav udaljenog računala moguće otkriti i bez uspostavljanja izravne veze s njim. Ovaj alat dakle omogućuje utvrđivanje operacijskih sustava računala:

- koja se povezuju na računalo s instaliranim *p0f* programskim paketom (SYN način rada),
- na koja se moguće povezati (SYN+ACK način rada),
- na koja se nije moguće povezati (RST+ način rada) te
- računala čiju komunikaciju je moguće prisluškivati.

P0f također omogućuje uočavanje prisutnosti vatrozida, korištenje NAT (eng. *Network Address Translation*) prevođenja adresa, prisustvo sustava za upravljanje opterećenjem mreže, udaljenost do udaljenog računala te utvrđivanje vremena njegove prisutnosti na mreži (eng. *uptime*).

3.4. *HTTPrint*

Httprint je alat za utvrđivanje inačice udaljenog web poslužitelja provođenjem analize HTTP prometa. Namijenjen je Windows, Linux, Mac OS X i FreeBSD operacijskim sustavima. Ovaj programski paket omogućuje i otkrivanje uređaja kao što su pristupne točke bežične mreže (eng. *wireless access point*), usmjerivači, preklopnici, kabelski modemi idr. Iako nije riječ o alatu otvorenog programskog koda, bez naknade je dostupan za osobne, obrazovne i druge nekomercijalne primjene. Na raspolaganju su inačica alata namijenjena korištenju u naredbenom retku i ona s grafičkim korisničkim sučeljem.
HTTPrint za analizu prikupljenih otisaka web poslužitelja koristi statističku analizu u kombinaciji s tehnikama temeljenim na neizrazitoj logici. Postupak otkrivanja web poslužitelja pojednostavljeno se može prikazati u sljedećim koracima:

1. Učitavanje skupa otisaka poznatih HTTP poslužitelja:
$$S=\{s_1, s_2 \ldots s_n\}.$$
2. Izvođenje testova na nepoznatom poslužitelju i stvaranje njegova otiska s_R.
3. Usporedba svih otisaka poznatih poslužitelja s otiskom nepoznatog poslužitelja korištenjem funkcije f_W koja rezultira skupom vrijednosti:
$$w_i=f_w(s_R, s_i), \text{ za } i=1,2\ldots n.$$
4. Funkcijom temeljenom na neizrazitoj logici f_C proračunava se vjerojatnost c_i da otisak s_i, kome odgovara težina w_i, najbolje odgovara otisku nepoznatog poslužitelja od svih poznatih otisaka iz skupa S, čiji je vektor težina označen s W:
$$c_i=f_C(w_i, W), \text{ za } i=1,2\ldots n.$$
5. Određivanje najveće vjerojatnosti iz vektora vjerojatnosti za sve poznate otiske C:
$$c_{max}=max(C)$$
6. Rezultat algoritma su svi otisci čija je vjerojatnost c_i jednaka c_{max}.

Otisci poznatih poslužitelja kod *HTTPrint* alata predstavljaju heksadecimalne vrijednosti pohranjene je u obliku ASCII (eng. *American Standard Code for Information Interchage*) znakovnih nizova unutar tekstualne datoteke. Bazu otisaka jednostavno je moguće proširiti prikupljanjem otisaka poznatih poslužitelja, a koji nisu u bazi, pomoću *HTTPrint* alata i njihovim kopiranjem (eng. *copy–paste*) u spomenutu tekstualnu datoteku.
Otkrivanje inačice HTTP poslužitelja pomoću *HTTPrint* programskog paketa moguće je spriječiti:

- izmjenama pozdravnog znakovnog niza HTTP poslužitelja (eng. *server banner string*),
- uklanjanjem pojedinih polja HTTP zaglavlja ili njihovim prerazmještanjem,
- izmjenama HTTP oznaka za pogreške, kakva je na primjer oznaka 404 kojom se korisnika obavješćuje o nepostojanja zatražene datoteke,
- instalacijom posebnih dodataka poslužitelju.

3.5. *Xprobe2*

Xprobe2 je alat za aktivno otkrivanje operacijskih sustava udaljenih računala, namijenjen Linux operacijskim sustavima. Za razliku od sličnih alata, *xprobe2* programski paket ne provodi pretraživanje portova udaljenog računala čiji operacijski sustav je potrebno otkriti. Za utvrđivanje operacijskog sustava ovom alatu potreban je barem jedan zatvoren UDP port, a identifikacija se provodi analizom ICMP protokola korištenjem neizrazite logike.

Riječ je o modularnom paketu što olakšava njegovu nadogradnju dodavanjem novih modula ili testova. Na raspolaganju je i API (eng. *Application Programming Interface*) sučelje koje korisnicima omogućuje pisanje vlastitih modula.
Xprobe2 se sastoji od dvije vrste modula:

- Moduli za utvrđivanje dostupnosti (eng. *reachability modules*) – prva dva modula koja se izvode tijekom pokušaja otkrivanja operacijskog sustava udaljenog računala pripadaju ovoj skupini
- Moduli za otkrivanje operacijskog sustava (eng. *fingerprinting modules*) – ovoj skupini pripadaju svi ostali moduli.

Prvi modul za utvrđivanje dostupnosti je *ICMP echo* modul, tijekom čijeg se izvođenja udaljenom računalu šalje takozvani *echo* ICMP zahtjev.
Drugi modul iz ove skupine je test TTL (eng. *Time To Live*) udaljenosti, koji na TCP port udaljenog računala šalje TCP paket s postavljenom SYN zastavicom. Cilj ovog testa je kao odgovor dobiti TCP paket s postavljenim SYN i ACK zastavicama, čime se označuje otvorenost danog porta, ili TCP paket s postavljenom RST zastavicom, koja označuje zatvoren port. U slučaju ne dobivanja odgovora jednak paket šalje se na sljedeći TCP port, s istim ciljem.
Osnovni moduli za otkrivanje operacijskog sustava su:

- Modul A – slanje ICMP paketa s *ICMP echo* zahtjevom.
- Modul B – slanje ICMP paketa s *ICMP timestamp* zahtjevom.
- Modul C – slanje ICMP paketa s *ICMP address mask* zahtjevom.
- Modul D – slanje ICMP paketa s *ICMP information* zahtjevom.
- Modul E – slanje UDP paketa oblikovanog kao DNS (eng. *Domain Name Service*) odgovor s ciljem dobivanja *ICMP port unreachable* poruke o nedostupnosti porta.

Nakon prikupljanja rezultata svih provedenih testova *xprobe2* provodi njihovu analizu i usporedbu s otiscima u vlastitoj bazi podataka. Rezultat je operacijski sustav s najvećom sličnošću ispitivanom operacijskom sustavu.
Prednosti ovog programskog paketa pred drugim alatima za otkrivanje operacijskih sustava udaljenih računala su:

- vrlo je brz jer se udaljenom računalu šalje malen broj paketa,
- malen utjecaj na udaljeno računalo,
- omogućuje identifikaciju mrežnih uređaja kao što su usmjerivači i preklopnici,
- mogućnost stvaranja vlastitih modula.

4. Izbjegavanje udaljenog otkrivanja operacijskog sustava

Kao što postoje brojne tehnike i alati za otkrivanje operacijskih sustava udaljenih računala, tako postoje i mnogi načini skrivanja takvih informacija od zlonamjernih korisnika. Pri tome treba imati na umu da primjena tehnika za onemogućavanje otkrivanja operacijskog sustava ne jamči sigurnost računala od udaljenih napada. One mogu biti samo dodatna razina zaštite, uz redovne nadogradnje i korištenje ostalih sigurnosnih alata.

4.1. Izmjena pozdravnih poruka

Pojedine usluge tijekom povezivanja korisniku šalju pozdravnu poruku čiji sadržaj može ovisiti o inačici aplikacije koja implementira uslugu. Izmjenu svih javnih pozdravnih poruka korištenih usluga kod nekih je programskih paketa moguće postići jednostavnom izmjenom pojedinih tekstualnih datoteka, dok je kod drugih potrebna promjena izvornog programskog koda i ponovno prevođenje. Opisanu metodu naročito je teško primijeniti na komercijalne alate čiji programski kod nije dostupan.

4.2. Uklanjanje znakovnih nizova

Datoteke s različitim sadržajem mogu sadržavati inkriminirajuće znakovne nizove, na primjer, web stranice mogu sadržavati automatski generirane komentare koji identificiraju alat pomoću kojeg je dana web stranica izrađena. Ako je takav alat vezan uz određeni operacijski sustav, na primjer *Microsoft Frontpage*, udaljeni zlonamjerni korisnik ima dobru polazišnu točku za analizu operacijskog sustava.

4.3. Gašenje nepotrebnih usluga

Otkrivanje operacijskog sustava na temelju usluga koje izvodi moguće je spriječiti gašenjem nepotrebnih usluga. Na raspolaganju su i alati koji omogućuju stvaranje privida pokrenutih usluga. Njihovom pravilnom upotrebom moguće je maskirati operacijski sustav.

4.4. Onemogućavanje ispitnih poruka

Promjenu reakcija IP stoga na ispitne upite (eng. *probe query*) daleko je lakše postići kod operacijskih sustava koji omogućuju izravnu manipulaciju dolaznih paketa putem točaka za izmjenu programskog koda unutar jezgre sustava (eng. *kernel mode OS hook*). Drugi način je izmjena pogonske aplikacije mrežne kartice. Na raspolaganju su alati koji omogućuju intervencije u IP stogu, a namijenjeni su Linux/Unix platformama. Primjer takvog programskog paketa je *netfilter/iptables* alat unutar 2.4.x jezgre Linux operacijskog sustava. Druga rješenja na razini jezgre operacijskog sustava uočavaju sumnjive pakete i jednostavno ih ignoriraju. Ovakav pristup djelotvoran je protiv alata koji koriste točno određen skup pravila za otkrivanje operacijskog sustava, kao što je *Nmap*, ali je manje učinkovit protiv tehnika temeljenih na neizrazitoj logici, kakve npr. koristi *Xprobe2* alat.

Računalo je od ispitnih paketa moguće zaštititi vatrozidom ili posebnim alatom, kakav je na primjer *Scrubber* programski paket.

Treći način za zaštitu računala od ispitnih poruka je korištenje NAT tehnologije. Kod mreža s implementiranim NAT sustavom, podatkovni promet svih računala provodi se preko jednog pristupnika (eng. *gateway*) pa računalima izvan takve mreže ona izgleda kao samo jedno računalo. Na ovaj način je uvelike otežana analiza skrivene mreže, pa prema tome i otkrivanje operacijskog sustava pojedinih računala.

5. Zaključak

Napretkom alata i tehnika za otkrivanje operacijskih sustava udaljenih računala razvijaju se i obrambene metode. Automatizirani sustavi nadogradnje operacijskih sustava , koji prije svega podižu njihovu razinu sigurnosti, također otežavaju identifikaciju. S druge strane, pooštravanje kaznenog progona računalnog kriminala čini masovne napade usmjerene na velik broj računala (eng. *script kiddy*) sve manje privlačnima. Za očekivati je, stoga, razvoj specijaliziranih napada usmjerenih na pojedine operacijske sustave ili usluge koje se na njima izvode. Izvođenje ovakvih napada neizbježno uključuje identifikaciju operacijskog sustava koji se izvodi na napadnutom računalu.

Ipak, lakoća kojom je danas moguće izvesti masovan napad donekle umanjuje vrijednost tehnika za sprječavanje otkrivanja operacijskog sustava. Tajnost operacijskog sustava dakle pridonosi njegovoj sigurnosti, ali ju ne jamči (eng. *Obscurity is not Security*).

6. Reference

[1] *TCP/IP stack fingerprinting*, http://en.wikipedia.org/wiki/TCP/IP_stack_fingerprinting, studeni 2007.

[2] Chris Trowbridge: An *Overview of Remote Operating System Fingerprinting*, SANS GIAC Practical, 2003.

[3] Ryan Spangler: Analysis *of Remote Active Operating System Fingerprinting Tools*, www.packetwatch.net/documents/papers/osdetection.pdf, studeni 2007.

[4] Bente Peterson: *Intrusion Detection FAQ: What is p0f and what does it do?*, http://www.sans.org/resources/idfaq/p0f.php, studeni 2007.

[5] Michael Zalewski: *the new p0f: 2.0.8 (2006–09–06)*, http://lcamtuf.coredump.cx/p0f.shtml, studeni 2007.

[6] Saumil Shah: *An Intoduction To HTTP fingerprinting*, http://www.net–square.com/httprint/httprint_paper.html, studeni 2007.