DEO I

UPOZNAVANJE ŽRTVE

SLUČAJ IZ PRAKSE: KAKO VAS UGROŽAVA GOOGLE

Prema svim kriterijumima, Google je jedna od retkih kompanija čija je tehnologija unela revoluciju u svet Interneta. Od samog nastanka, kada je bez prikazivanja reklama spartanski pretraživao Internet, do inicijalne emisije akcija (engl. *initial public offering*, IPO) koja je srušila sve uobičajene standarde, Google je postao nezaobilazan. Tehnologija Googlea omogućava funkcionisanje mnogih lokacija na Internetu, a njegov jednostavan portal za pretraživanje svake sekunde upotrebljavaju milioni ljudi. Dok ga većina koristi za pronalaženje svega mogućeg, od retko pominjanih podataka o podešavanju Linuxovog jezgra do lekova za išijas, nekolicina je otkrila Googleovu malu tajnu: on čuva veliku količinu informacija koje napadači svakodnevno koriste za pronalaženje, procenu i napadanje sistema na Internetu.

Često se kaže da najveća specijalnost može biti i najveća slabost. Drugim rečima, Google previše dobro radi to što radi, tj. izuzetno efikasno pronalazi podatke na Webu. Na svojim Web lokacijama, organizacije i korisnici veoma često ostavljaju poverljive podatke – čak i toliko poverljive informacije da je u to teško poverovati – a Google ih pronalazi, arhivira i prikazuje svakome ko ume da zada odgovarajući upit.

Tajnu Googleovog fatalno efikasnog i preciznog pročešljavanja milijardi Web stranica, čine njegovi roboti (Google Bots), koji velikom brzinom stalno pretražuju Internet. Ukoliko im se drugačije ne naredi, oni samostalno traže i pronalaze sve što sadrži svaka zadata hiperveza – što za vas može biti katastrofalno!

UHVATI I UČITAJ POMOĆU GOOGLEA

Kao što dobro znaju mnogi administratori i profesionalci u oblasti bezbednosti računara, svakoga dana se otkriva na desetine novih softverskih propusta. Teško je pronaći sve ranjive sisteme, a kamoli postići da svi oni stalno budu zakrpljeni. Napadači upravo na to računaju. Veštinu snimanja sistema (engl. *footprinting*) upotrebiće za pronalaženje ranjivih sistema i sočnih informacija pomoću kojih se vaša lokacija može napasti. Naročito je popularno upotrebiti Google kao mehanizam za pronalaženje. Evo kako se to radi.

Haker Jova ima mnooogo vremena. Dok vi procenjujete da li ćete još jedan vikend morati da provedete krpeći ranjive sisteme, on se trudi samo da pronađe sisteme zrele za napad i više nego spremne da mu otkriju sve svoje tajne. Jova je poboljšao svoj način hakerisanja pomoću Googlea – dakle, upotrebu Googlea za pronalaženje ranjivih sistema i poverljivih podataka. On sebe smatra izuzetnim hakerom Windowsa, a zapravo je majstor samo u otkrivanju lakih meta. Zavirimo u njegov svet, pogledajmo kako radi i kakva pretraživanja pokreće sa lokacije www.google.com.

Njegovo prvo pretraživanje izgleda sasvim bezazleno:

intitle:"Welcome to IIS 4.0"

Results **1 – 10** of about **63 for intitle:"Welcome to IIS 4.0"**. **(0.10** seconds**)**

Šta bi to on mogao da traži? Spisak Windows IIS 4.0 servera, koji imaju mnoštvo bezbednosnih propusta i za većinu napadača najčešće predstavljaju lak plen.

Jova sprema ove podatke i traži nove žrtve. Sledeći na njegovom spisku su korisnici koji s Weba pokreću VNC Server.

"VNC Desktop" inurl:5800

Results **1 – 10** of about **112** for **"VNC Desktop" inurl:5800**. **(0.27** seconds**)**

VNC Server dozvoljava korisnicima da se daljinski povežu sa računarom određenog korisnika i da upravljaju njime. Ta usluga se može podesiti tako da radi bez lozinke i da dozvoli direktan pristup određenom računaru. Jao!

Na poslednje mesto (ali ne po bogatstvu plena) dolazi uvek popularno i s vremenom provereno traganje za proširenjima Microsoftovog FrontPagea koja nisu propisno obezbeđena:

filetype:pwd service

Results **1 – 10** of about **173** for **filetype:pwd service**. **(0.28** seconds**)**

Pritisak na jednu od pronađenih hiperveza otkriva nekoliko korisničkih imena i UNIX lozinki:

```
# -FrontPage-
ekendall:bYld1Sr73NLKo
louisa:5zm94d7cdDFiQ
```

Haker Jova učitava primerak alatke John the Ripper za razbijanje lozinki i odmah provaljuje Louisinu lozinku, „trumpet“. Jovi je sada lepo – ima korisničko ime i lozinku za FrontPage.

Oštećivanje Web lokacija preko propusta FrontPage, bilo je u velikoj modi pre nekoliko godina i Jova odlučuje da, zarad starih vremena, napravi nekoliko „poboljšanja“ na Web stranicama pojedinih korisnika.

Posle pronalaženja više dobrih meta, haker Jova se okreće traganju za poverljivim informacijama na Webu, kao što su lozinke i finansijski podaci. Brzo zadaje kriterijum:

filetype:bak inurl:"htaccess | passwd | shadow | htusers"

Results **1 – 10** of about **59** for **filetype: bak inurl:"htaccess | passwd | shadow | htusers" (0.18** seconds**)**

i otkriva svakovrsne podatke o datotekama punim korisničkih imena i šifrovanih lozinki koje se lako mogu razbiti. U stvari, haker Jova je dobio premiju kada je s jednog od najboljih američkih univerziteta izvukao datoteku sa stotinama neskrivenih UNIX lozinki. Nije loše za nekoliko sekundi rada.

Jovo, šta kažeš da malo pređemo na hakerisanje baza podataka? Nema problema.

filetype:properties inurl:db intext:passwd

Results **1 – 10** of about **854** for **filetype:properties inurl:db intext:password (0.21** seconds**)**

Pritisak na jednu od pronađenih hiperveza otkriva lozinke za bazu podataka napisane nešifrovanim tekstom!

```
drivers=sun.jdbc.odbc.JdbcOdbcDriver jdbc.idbDriver
logfile=D:\\user\\src\\java\\DBConnectionManager\\log.txt
```

```
idb.url=jdbc:idb:c:\\local\\javawebserver1.1\\db\\db.prp

idb.maxconn=2

access.url=jdbc:odbc:demo
access.user=demo
access.password=demopw
```

Nažalost, Jovi nije mnogo stalo do vaše bezbednosti. S druge strane, možda nije ni vama, pošto na Webu ostavljate poverljive podatke. U potrazi za poverljivim podacima sada će pretražiti univerzitetske (.edu) lokacije.

"not for distribution" confidential site:edu

Results **1 – 10** of about **138** for **"not for distribution" confidential site:edu (0.20** seconds**)**

I ponovo je Jova nagrađen za umešnost u traganju. Jednim pritiskom tastera otkrio je preko 100 poverljivih dokumenata. Baš šteta što je u tom PDF dokumentu univerzitet ostavio brojeve socijalnog osiguranja svojih studenata.

Kako mu očekivanja da stvarno razbije te sisteme rastu, Jova odlučuje da krene konkretno:

This file was generated by Nessus

Results **1 – 10** of about **75,300** for **This file was generated by Nessus (0.20** seconds**)**

Nessus je veoma popularan skener softverskih propusta, koji upotrebljavaju mnogi administratori. Na žalost žrtava koje nemaju pojma da je tako nešto moguće, haker Jova je pronašao hiljade Nessusovih izveštaja što su nebrigom administratora ostavljeni na računarima korisnika. To je neverovatno obilje računara dostupnih sa Interneta, koji nude gotove spiskove sopstvenih softverskih propusta! Ima li za Jovu išta lakše? Ne mora čak ni da pokrene Nessus – upotrebiće samo ono što su mu administratori ostavili na poslužavniku.

Kao što ćete videti u narednim poglavljima, snimanje, skeniranje i popisivanje vredni su i neophodni koraci koje će napadač upotrebiti da otkrije vaše slabe tačke. Hakerisanje pomoću Googlea samo je jedna od metoda koju koriste vaši protivnici, pa bi trebalo da se pridržavate našeg saveta: opipajte sopstvene sisteme pre nego što to učine zlonamernici. Ne očajavajte ako vam se čini da ste ugroženi sa svih strana – i za hakerisanje postoje protivmere. Razmatraćemo ih u celoj knjizi.

POGLAVLJE 1

SNIMANJE SISTEMA

Pre nego što stvarno počne da se zabavlja, haker mora da sprovede tri neophodna postupka. U ovom poglavlju razmotrićemo prvi postupak – *snimanje sistema* (engl. *footprinting*), tj. veštinu prikupljanja podataka o cilju. Kada lopovi odluče da opljačkaju banku, oni ne uleću bezglavo u nju vičući: „Daj pare!" (barem ne oni pametniji), nego strpljivo prikupljaju podatke o njoj – kojim putem prolazi blindirano vozilo, tačno vreme transporta novca, raspored video-kamera, broj šalterskih službenika, gde su izlazi za bežanje, i sve ostalo što može da utiče na uspešan ishod poduhvata.

Isto važi i za uspešnog napadača na računare. Da bi mogao da izvede usredsređen i hirurški precizan napad (koji se teško otkriva), on mora da prikupi mnogo informacija. Zbog toga će napadač sakupiti sva moguća obaveštenja o svim aspektima sistema bezbednosti računara određene organizacije. Kao rezultat „opipavanja", hakeri stvaraju jedinstven *snimak* (profil) prisustva žrtve na Internetu, intranetu/ekstranetu ili u sistemu za daljinski pristup. Postupajući po strukturiranoj metodologiji, napadač može sistematski da izvlači podatke iz najrazličitijih izvora i da napravi snimak gotovo svake organizacije.

Sun Tzu je to uočio pre mnogo vekova i napisao u *Umeću ratovanja*: „Ako poznaješ i sebe i protivnika, ne boj se ishoda stotine bitaka. Ukoliko poznaješ sebe, ali ne i protivnika, za svaku ostvarenu pobedu doživećeš po jedan poraz. A ukoliko ne poznaješ ni sebe ni protivnika, bićeš poražen u svakoj bici."

Iznenadićete se kada saznate koliko je podataka o bezbednosnim merama vaše organizacije lako dostupno svima koji hoće da ih potraže. Neophodno je da o sebi saznate ono što protivnik o vama već zna!

ŠTA JE SNIMANJE SISTEMA?

Sistematsko i metodično opipavanje neke organizacije omogućava napadačima da sastave potpun profil njenog sistema obezbeđenja. Služeći se različitim alatkama i tehnikama, uz odgovarajuću dozu strpljenja, napadači mogu da razotkriju nepoznat entitet (organizaciju XYZ) i da ga svedu na sasvim određen opseg imena domena, mrežnih blokova i pojedinačnih IP adresa sistema koji su direktno povezani na Internet, kao i mnoge druge pojedinosti u vezi sa obezbeđenjem njenih računara. Iako postoje mnoge tehnike snimanja sistema, sve su uglavnom usmerene na otkrivanje informacija o sledećim okruženjima: Internetu, intranetu, daljinskom pristupu i ekstranetu. U tabeli 1-1 nabrojana su sva ova okruženja, zajedno sa izuzetno važnim podacima koje napadač želi da otkrije.

Zašto je snimanje sistema neophodno?

Snimanjem sistema sistematično se prikupljaju i identifikuju svi delići informacija o pomenutim tehnologijama. Bez dobre metodologije za sprovođenje opisanog istraživanja, sva je prilika da ćete propustiti ključne podatke koji se odnose na određenu tehnologiju ili organizaciju. Snimanje sistema je često najmučnija faza razotkrivanja sistema bezbednosti, ali je to istovremeno i najvažnija faza. Ono se mora sprovesti precizno i prema prethodno utvrđenom planu.

Tabela 1-1 Okruženja i važni podaci koje napadač može da otkrije

Tehnologija	Identifikuje
Internet	Ime domena
	Mrežne blokove
	Specifične IP adrese sistema dostupnih preko Interneta
	TCP i UDP usluge koje rade na svakom identifikovanom sistemu
	Arhitekturu sistema (na primer, Sparc ili *x*86)
	Mehanizme upravljanja pristupom i odgovarajuće liste za kontrolu pristupanja (ACL liste)
	Sisteme za otkrivanje upada (IDS sisteme)
	Sistemske podatke (korisnička imena i imena grupa, sistemska zaglavlja, tabele putanja, SNMP informacije)
	Imena DNS servera (servera imena domena)
intranet	Korišćene mrežne protokole (na primer, IP, IPX, DecNET i slično)
	Interna imena domena
	Mrežne blokove
	Specifične IP adrese sistema dostupnih preko intraneta
	TCP i UDP usluge koje rade na svakom identifikovanom sistemu
	Arhitekturu sistema (na primer, Sparc ili *x*86)
	Mehanizme upravljanja pristupom i odgovarajuće liste za kontrolu pristupanja (ACL liste)
	Sisteme za otkrivanje upada (IDS sisteme)
	Sistemske podatke (korisnička imena i imena grupa, sistemski natpisi, tabele putanja, SNMP informacije)
Daljinski pristup	Brojeve analognih/digitalnih telefona
	Vrstu sistema za daljinski pristup
	Mehanizam autorizacije
	VPN i srodne protokole (IPSEC, PPTP)
Ekstranet	Početak i odredište priključka
	Vrstu priključka
	Mehanizam upravljanja pristupom

SNIMANJE INTERNET SISTEMA

Iako su mnoge tehnike snimanja bezbednosnog sistema u različitim tehnologijama (Internet i intranet) slične, u ovom poglavlju ćemo se ograničiti na snimanje Internet veza neke organizacije. Pristup s daljine detaljnije ćemo analizirati u poglavlju 8.

Teško je dati detaljno uputstvo za snimanje bezbednosnog sistema, jer vas ta aktivnost može odvesti različitim putevima. Zato ćemo u ovom poglavlju skicirati osnovne korake koji bi trebalo da vam omoguće detaljno analiziranje snimka. Mnoge tehnike koje ćemo opisati mogu da se primene i na druge pomenute tehnologije.

Prvi korak: određivanje opsega snimanja

Najpre utvrdite opseg svojih aktivnosti tokom snimanja sistema. Želite li da opipate čitavu organizaciju ili ćete se ograničiti samo na određene ogranke, tj. lokacije? Šta je sa ekstranet mrežama, tj. mrežama koje koriste samo organizacija i njeni glavni poslovni partneri, ili s lokacijama za oporavljanje od katastrofa? Ima li drugih odnosa ili okolnosti koje treba uzeti u obzir? U nekim slučajevima već je teško identifikovati sve delove ciljne organizacije, da ne govorimo o tome kako je teško propisno ih obezbediti. Nažalost, hakeri nemaju simpatija za prezaposlene administratore. Oni koriste sve naše slabosti, u svim oblicima u kojima se one ispoljavaju. Ne dozvolite da o obezbeđenju vaših računara hakeri znaju više od vas!

Drugi korak: pribavite potrebno ovlašćenje

Jedna od stvari koje hakeri najčešće mogu da zanemare, a na koju vi morate obratiti naročitu pažnju, jeste ono što tehničko osoblje od milja zove „slojevi osam i devet sedmoslojnog OSI modela“; misli se na *odluke uprave* i *novac*. Ti slojevi se često probiju do našeg posla, a osobito su delikatni kada se radi o ovlašćenjima. Imate li ovlašćenje da uradite svoj posao? Kad je već reč o tome, koji je opseg vaših aktivnosti? Jeste li ovlašćenje dobili od prave osobe (ili osoba)? Da li ste ovlašćenje dobili napismeno? Jesu li u njemu navedene IP adrese koje treba proveriti? Pitajte ma kog profesionalnog ispitivača mreža šta je „besplatna izlaznica iz zatvora“, i sigurno će se nasmešiti.

Treći korak: javno dostupne informacije

I nakon tolikih godina provedenih na Webu, uvek me iznova zapanji nesagledivost Interneta – a pomislite samo koliko je još uvek mlad!

Pretraživanje javnih izvora

Popularnost:	*9*
Jednostavnost:	*9*
Uticaj:	*2*
Stepen rizika:	***7***

Upravo je zaprepašćujuća količina javno dostupnih informacija o vama, vašoj organizaciji, zaposlenima u njoj i svemu ostalom što vam može pasti na pamet.

Koje „igle“ tražimo „u plastu sena“?

- Web stranice preduzeća
- Srodne kompanije i delove preduzeća
- Pojedinosti o fizičkoj lokaciji preduzeća
- Telefonske brojeve, imena, elektronske adrese i lične podatke zaposlenih
- Vesti o tekućim događajima (integrisanju ili promeni vlasnika, otpuštanju radnika, brzom rastu itd.)
- Pravila za zaštitu privatnosti ili bezbednosna pravila iz kojih se može izvesti zaključak o primenjenom sistemu obezbeđenja
- Arhivirane podatke
- Nezadovoljne radnike preduzeća
- Mašine za pretraživanje, Usenet mreže, biografije zaposlenih
- Ostale bitne informacije

Web stranice preduzeća

Ako organizacija ima Web stranicu, pođite od nje. Često na Web stranici organizacije ima previše informacija koje mogu da pomognu napadaču. Na Web serverima organizacija viđali smo i pojedinosti o konfiguraciji obezbeđenja njihovih računara.

Osim toga, potražite komentare u izvornom HTML kodu Web stranica. U HTML oznakama za komentare (<, !, --) zakopane su mnoge stavke koje nisu za javno prikazivanje. Izvorni kôd ćete brže proveriti ako čitavu lokaciju preslikate na svoj disk i pregledate je kad niste na Mreži. Kada na računaru imate kopiju lokacije, traženje komentara i drugih upotrebljivih stavki obavite pomoću programa jer ćete tako efikasnije opipati Web lokaciju. Za preslikavanje čitave lokacije postoje odlični uslužni programi: Wget (http://www.gnu.org/software/wget/wget.html) za UNIX i Teleport Pro (http://www.tenmax.com) za Windows.

Obavezno ispitajte i druge lokacije, ne samo glavne „www“. Mnoge organizacije imaju lokacije za daljinsko pristupanje internim resursima preko čitača Weba. U toj ulozi često nastupa Microsoftov Outlook Web Access, koji deluje kao zastupnik internih Microsoft Exchange servera za sve što je sa Interneta. Tipične URL adrese ovog resursa su https://owa.*imekompanije*.com ili https://outlook.*imekompanije*.com. Slično tome, organizacije koje imaju velike centralne računare ili one iz serije AS/400, često pomoću usluge kao što je OpenConnect (http://www.openconnect.com) omogućavaju da im se daljinski pristupa preko čitača Weba. OpenConnect služi kao Java emulator terminala 3270 i u čitaču prikazuje „zeleni ekran“ za pristupanje internim velikim centralnim računarima i/ili onima iz serije AS/400.

Većina organizacija ima i virtuelne privatne mreže (engl. *virtual private network*, VPN), pa bi poseta lokacijama kao što su http://vpn.*imekompanije*.com ili http://www.*imekompanije*.com/vpn mogla otkriti lokaciju za pomoć krajnjim korisnicima pri povezivanju na VPN njihovog preduzeća. Na njoj se obično navodi ime proizvođača i broj verzije VPN-a, te detaljna uputstva o preuzimanju i konfigurisanju klijentskog VPN softvera. Katkada takve lokacije objavljuju čak i telefonski broj koji hakeri – izvinite, hteo sam da kažem radnici preduzeća – mogu pozvati ako imaju poteškoća pri povezivanju.

Srodne organizacije

Obratite pažnju na reference i hiperveze ka drugim organizacijama koje su na bilo koji način u vezi sa organizacijom koja je potencijalni cilj napada. Čak i kada organizacija dobro pazi koje podatke o sebi iznosi u javnost, njeni partneri možda ne razmišljaju toliko o bezbednosti. Na sopstvenim Web lokacijama oni mogu otkriti neke dopunske detalje koji, u kombinaciji s drugim informacijama, daju ubojitiju smesu podataka za napad nego što su to dale lokacije same organizacije koja se proverava. Vreme utrošeno na ispitivanje svih „tragova" često se na kraju višestruko isplati.

Detalji o fizičkoj lokaciji

Poštanska (ulična) adresa može mnogo pomoći odlučnom napadaču, zato što mu omogućava fizički nadzor zgrada, pretraživanje otpadnog papira organizacije, lažno predstavljanje njenim radnicima i druge netehničke napade. Ta adresa može dovesti i do neovlašćenog pristupa zgradama, ožičenim i bežičnim mrežama, računarima itd. Iz raznih izvora na Internetu, napadači mogu dobiti čak i detaljne satelitske snimke celog fabričkog kruga preduzeća. Meni omiljena lokacija za dobijanje takvih snimaka jeste Googleova http://www.keyhole.com (slika 1-1). Ona vam ceo svet (ili barem sve velike gradove sa okolinom) stavlja pred noge i omogućava uveličavanje satelitske slike odabrane poštanske adrese do neverovatnih pojedinosti i stepena jasnoće; za to stoji na raspolaganju dobro dizajnirana klijentska aplikacija. Drugi popularan izvor snimaka iz ptičje perspektive jeste http://terraserver.microsoft.com.

Slika 1-1 Pomoću usluga lokacije http://www.keyhole.com, svako može da dobije snimak vašeg privatnog ili poslovnog prostora, uveličan do neverovatnih pojedinosti i stepena jasnoće.

Telefonski brojevi, imena, adrese e-pošte i lični podaci zaposlenih

Pomoću telefonskih brojeva, napadači mogu saznati poštansku (uličnu) adresu organizacije – tome služe lokacije kao što su http://www.phonenumber.com, http://www.411.com i http://www.yellowpages.com. Pozivne brojeve mogu upotrebiti i za automatsko pozivanje opsega telefonskih brojeva (engl. *war-dialing*), da bi pronašli telefonske brojeve na kojima se javljaju modemi, i za lažno predstavljanje koje ih može dovesti do dodatnih informacija i/ili pristupa podacima.

Napadačima su naročito korisna imena i adrese e-pošte zaposlenih. Za korisničko ime zaposlenog u računarskoj mreži i prvi deo njegove adrese e-pošte, većina organizacija upotrebljava znakovni niz izveden od njegovog imena i prezimena (na primer, korisničko ime Petra Petrovića je ppetrovic, petarpetrovic ili petrovicpetar, a njegova adresa e-pošte ppetrovic@*imekompanije*.com ili nešto slično). Ko zna jedan od tih podataka, verovatno se može dosetiti kako glase ostali. Poznato korisničko ime napadaču će dobro doći kasnije, kada pokuša da pristupi sistemskim resursima. Sve te informacije mogu dobro poslužiti i prilikom lažnog predstavljanja.

Ostali lični podaci zaposlenih mogu se lako pronaći na Internetu; tome služe lokacije kao što su http://www.crimetime.com/online.htm, koja je povezana sa nekoliko izvora podataka, i http://www.peoplesearch.com, koja napadačima može dati lične podatke u opsegu od kućnog telefonskog broja i adrese do broja socijalnog osiguranja, kreditnog statusa i policijskog dosjea, između ostalog. Sve te podatke napadači mogu upotrebiti za postizanje svojih ciljeva – pošto se iznuda i ucena još uvek mnogo koriste.

Napadača zanima čak i kućni računar zaposlenog, zato što on verovatno ima neku vrstu daljinskog pristupa ciljnoj organizaciji. Program za snimanje tastature kućnog ili prenosivog računara zaposlenog, napadaču može lako doneti slobodan ulaz u unutrašnje odaje organizacije. Zašto da se haker muči sa zaštitnim barijerama, IDS-ovima, IPS-ovima itd. kada mu je mnogo lakše da se predstavi kao korisnik u koga organizacija ima poverenja.

Tekući događaji

Napadačima su tekući događaji često posebno zanimljivi. Integrisanje i kupovina preduzeća, skandali, otpuštanja radnika, naglo zapošljavanje, reorganizacija, prepuštanje poslova podizvođačima, češće angažovanje spoljnih saradnika i drugi događaji, mogu pružiti mogućnosti i otkriti tragove i situacije kojih ranije nije bilo. Na primer, spajanje računarskih mreža jedan je od prvih događaja nakon integrisanja ili kupovine preduzeća. Da bi se podaci razmenili brže, često se pri tom zanemaruje bezbednost. Zaposleni su skloni da kažu: „Znam da ovo nije najbezbedniji način da se obavi posao, ali moramo završiti što pre. Kasnije ćemo sve dovesti u red." U praksi, to „kasnije" često nikada ne nastupi, pa napadači dobijaju priliku da provalom u slabiji ogranak „iz pozadine" pristupe primarnom cilju.

Tokom navedenih događaja često postaje značajan i ljudski faktor. Tada je moral zaposlenih obično nizak (jer su masovna otpuštanja u tim situacijama redovna pojava), pa nije čudo da oni više vremena i pažnje posvećuju ažuriranju svojih radnih biografija nego pregledanju zapisnika mrežnih transakcija ili primeni najnovijih zakrpa. U najmanju ruku, osoblje je rastreseno. U takvim situacijama česte su

promene a s njima i pometnja, i većina ne želi da na druge ostavi utisak nekooperativnosti ili suprotstavljanja promenama. Time se povećava verovatnoća uspeha prilikom napada lažnim predstavljanjem.

Dešava se i suprotno. Kada se preduzeće naglo širi, procesi i postupci rada u njemu često zaostaju. Ko pazi na to da na orijentaciono predavanje za nove radnike ne dođe i neko nepozvan? Ko se ono šeta po kancelariji, novajlija ili neovlašćeno lice? Nije li ona nepoznata osoba, što sedi u sali za sastanke s prenosivim računarom u krilu, neželjeni gost? Je li po otpadni papir došao kamion preduzeća koje to inače radi? Da li je ono zaista spremačica?

Ako se akcije kompanije kotiraju na berzi, tekući događaji u njoj bivaju objavljivani na Internetu i tamo su lako dostupni. Kompanije čije su akcije prisutne na berzi, zakon primorava da izveštaje o poslovanju redovno šalju odgovarajućem državnom nadzornom telu (u SAD to je Komisija za promet novca i hartija od vrednosti – Securities and Exchange Commission, SEC). Ti izveštaji pružaju obilje informacija, a među njima su naročito zanimljivi 10-Q (tromesečni) i 10-K (godišnji), koje možete pogledati u bazi podataka EDGAR na adresi http://www.sec.gov (slika 1-2). Kada pronađete takav izveštaj, potražite u njemu ključne reči „merger“ (integrisanje preduzeća), „acquisition“ (kupovina), „acquire“ (kupiti) i „subsequent event“ (naredna aktivnost). Budite uporni, i moći ćete da napravite detaljnu organizacionu šemu celog preduzeća i njegovih podružnica. Slične podatke pružaju Web lokacije s poslovnim informacijama i one za trgovanje akcijama (deonicama). Slične lokacije postoje za sve velike berze širom sveta. Napadač može upotrebiti te podatke za pronalaženje slabih tačaka organizacije. Većina hakera bira put najmanjeg otpora, a zašto i ne bi?

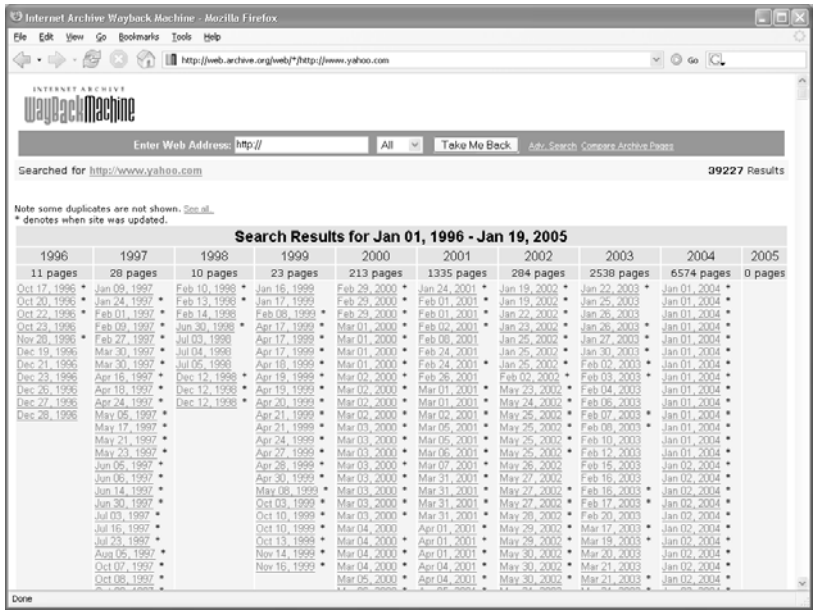
Slika 1-2 Američke kompanije čijim se deonicama trguje na berzi, moraju redovno da šalju izveštaje SEC-u. Oni sadrže zanimljive podatke o tekućim aktivnostima i organizacionoj strukturi preduzeća.

Pravila za zaštitu privatnosti, bezbednosna pravila i tehničke pojedinosti koje ukazuju na primenjen sistem bezbednosti

Napadaču očigledno koristi svaki podatak koji ga upoznaje s pravilima za zaštitu privatnosti, bezbednosnim pravilima i tehničkim pojedinostima o hardveru i softveru kojima se organizacija štiti. Kada se ti podaci pribave, najverovatnije će se pružiti i prilika da se iskoriste.

Arhivirani podaci

Ne zaboravite da sa nekih lokacija na Internetu možete preuzeti arhivirane kopije podataka koji više ne moraju biti dostupni u originalnom izvoru. Tako bi napadač mogao doći do informacija koje su sa Interneta namerno uklonjene iz bezbednosnih razloga. Primeri takvih lokacija su Wayback Machine na adresi http://www.archive.org (slika 1-3), http://www.thememoryhole.org i arhivirani rezultati koje Google daje u rubrici Cached results (slika 1-4).



Slika 1-3 Upit zadat lokaciji http://www.archive.org, otkriva stare stranice najvećeg američkog portala Yahoo!, arhivirane tokom više godina.

Nezadovoljni radnici

Još jedna realna pretnja bezbednosti organizacije mogu biti nezadovoljni radnici, bivši radnici i lokacije koje distribuiraju poverljive podatke o internim postupcima preduzeća. Da biste shvatili o čemu govorim, bacite pogled na lokacije kao što su http://www.f**kedcompany.com ili http://www.internalmemo.com. Zapitajte bilo koga da li je čuo priče o postupcima nezadovoljnih radnika, i naslušaćete se prilično iznenađujućih glasina. Nisu retki slučajevi da takvi ukradu, prodaju ili

drugima otkriju poverljive informacije preduzeća, oštete opremu, unište podatke, podese logičku bombu da se aktivira u unapred određeno vreme, ostave „mala vrata“ u računarskom sistemu da bi kasnije lako mogli da mu pristupe spolja i sl. Zbog toga se danas pri otpuštanju često zahteva da pripadnik službe obezbeđenja ili osoba iz kadrovske službe radniku lično saopšti odluku o otpuštanju i odmah ga isprati do kapije. Upit „link:www.*imekompanije*.com“, za jedno od Googlovih naprednijih pretraživanja, otkriva svaku Googleu poznatu Web lokaciju koja sadrži hipervezu ka ciljnoj organizaciji. To bi mogao biti dobar način za pronalaženje zlonamernih lokacija s podacima o ciljnoj organizaciji.

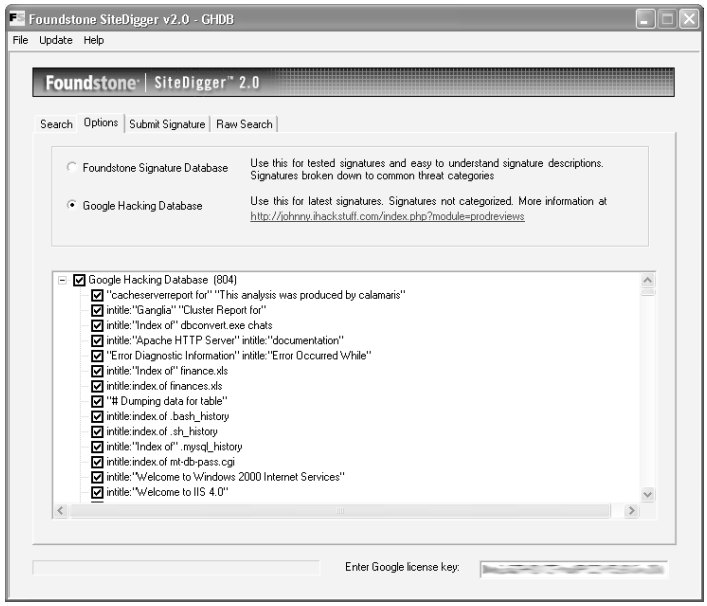
Slika 1-4 Sama priroda mašine za pretraživanje svima čini lako dostupnim arhiviran sadržaj stranica koje je mašina pretražila. Ovde vidimo arhiviranu verziju stranice http://www.yahoo.com iz Googleove arhive.

Mašine za pretraživanje, Usenet mreža i radne biografije

Današnje mašine za pretraživanje zaista su fantastične. Za nekoliko sekundi možete pronaći sve što bi vam ikada moglo zatrebati. Mnoge savremene popularne mašine omogućavaju naprednije pretraživanje, pomoću koga možete dopreti do onog delića podataka koji će iz osnova promeniti situaciju. Naše omiljene mašine za pretraživanje su http://www.google.com, http://search.yahoo.com, http://www.altavista.com i http://www.dogpile.com (to je metapretraživač, tj. on šalje upit mnogim drugim mašinama za pretraživanje, od njih prikuplja rezultate i prosleđuje ih vama). Vredi utrošiti vreme na upoznavanje njihovih mogućnosti za naprednije pretraživanje. Pomoću njih se može saznati toliko poverljivih podataka da su o tome napisane cele knjige, recimo *Google Hacking for Penetration Testers*, Johnnyja Longa (Syngress, 2004).

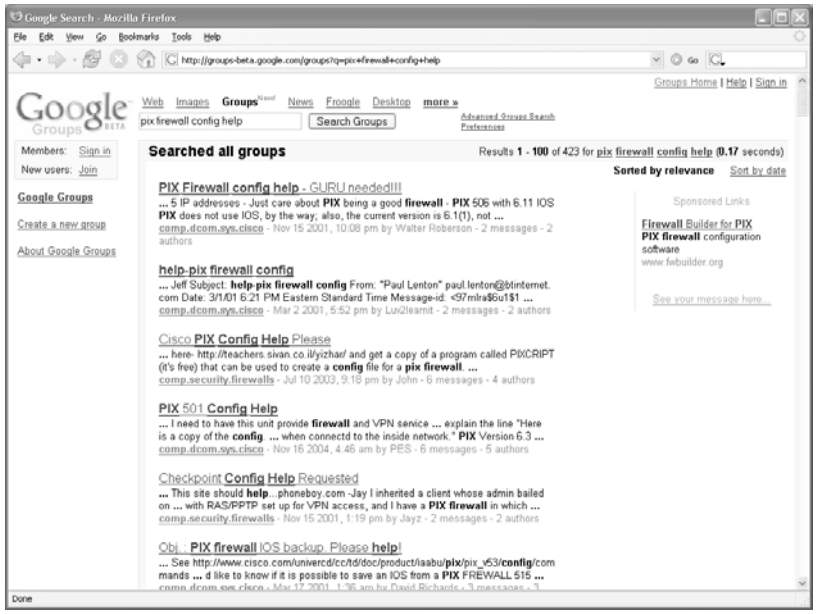
Daćemo jednostavan primer: ako Googleu zadate upit „allinurl:tsweb/default.htm“, on će vam otkriti Windows servere sa javnim Web priključkom za daljinski rad (Remote Desktop Web Connection). To bi moglo dovesti do konzolnog grafičkog pristupa serveru preko protokola za daljinsko pristupanje (Remote Desktop Protocol, RDP), za koji je potreban samo Internet Explorer i ActiveX RDP klijent, koji ciljni Windows server nudi napadaču kada je ova usluga uključena. Postoje doslovno stotine drugih upita koji otkrivaju sve, od javnih Web kamera, preko usluga daljinskog administriranja i lozinki, do baza podataka. Nećemo ovde ponovo otkrivati toplu vodu, nego vas upućujemo na jednu od odličnih lokacija za hakerisanje pomoću Googlea, http://johnny.ihackstuff.com. Johnny Long je napravio celu bazu podataka za hakerisanje pomoću Googlea (Google Hacking Database, GHDB), i stalno joj dodaje nove i zanimljive upite.

Naravno, nije dovoljno imati samo bazu podataka s gotovim upitima. Nedavno je objavljeno nekoliko alatki koje ovaj koncept dižu na još viši nivo: Athena na adresi snakeoillabs, koju je napisao Steve; SiteDigger, koji možete naći na adresi http://www.foundstone.com i Wikto na adresi http://www.sensepost.com/research/Wikto, koji su napisali Roelof i ekipa. Sve te alatke traže razne slabe tačke, greške, problematične konfiguracije, nestandardne podatke i zanimljive dragocene parčiće podataka o bezbednosti, koji se mogu naći na Web lokacijama širom sveta. SiteDigger (slika 1-5) omogućava ciljanje pojedinačnih domena, upotrebljava GHDB ili poboljšanu Foundstoneovu listu upita, omogućava slanje novih upita koji se dodaju bazi podataka, omogućava sirovo pretraživanje i, što je najbolje od svega, omogućava ažuriranje, tj. neposredno preuzima najnovije GHDB i/ili Foundstone upite da ne biste ništa propustili.



Slika 1-5 Foundstoneov SiteDigger pretražuje Googleovu arhivu; za pronalaženje ranjivih sistema upotrebljava spisak gotovih upita iz baze Google Hacking Database (GHDB).

I Usenet diskusione grupe i forumi predstavljaju bogat izvor poverljivih podataka. IT profesionalci najčešće koriste diskusione grupe za traženje pomoći u vezi s problemima koje sami ne znaju da reše. Google ima lep Web interfejs za Usenet diskusione grupe, upotpunjen njegovim već čuvenim mogućnostima naprednog pretraživanja. Na primer, jednostavan upit „pix firewall config help, otkriće stotine zahteva za pomoć – poslali su ih administratori koji ne znaju da konfigurišu Ciscovu zaštitnu barijeru PIX (slika 1-6). Deo tih poruka sadrži kopiju konfiguracije te barijere, što obuhvata IP adrese, liste za kontrolu pristupa, heširane lozinke, preslikavanje mrežnih adresa itd. Takvo pretraživanje možete poboljšati tako da otkrije samo poruke pristigle sa elektronskih adresa iz određenog domena (drugim rečima, @*imekompanije*.com) ili neke druge zanimljive znakovne nizove.



Slika 1-6 Još jedan primer kako Googleove mogućnosti za naprednije pretraživanje pomažu u brzom otkrivanju podataka važnih za napad.

I kada osoba koja traži pomoć zna da ne sme da objavi pojedinosti svoje konfiguracije na javnom forumu, desi se da ne prepozna lažno predstavljanje. Naime, napadač joj se javi s prijateljskom ponudom pomoći, ali da bi zaista mogao da pomogne, „potrebno mu je više pojedinosti". Ukoliko napadač, uprkos početnom oprezu umornog administratora, uspe da zadobije njegovo poverenje, dobiće od njega iste poverljive podatke.

Drugi zanimljiv izvor podataka jesu brojne radne biografije dostupne na mreži. Pošto je IT ogromna i veoma raznolika profesija, pronalaženje savršenog para radno mesto – radnik ume da bude veoma teško. Među najboljim načinima da se smanji veliki broj lažnih podudaranja jeste pružanje veoma detaljnih, često poverljivih, podataka u oglasima za radna mesta i u biografijama.

Zamislite organizaciju kojoj treba iskusan profesionalac u oblasti računarske bezbednosti za veoma konkretnu ulogu i funkciju. Osoba treba da je stručnjak za ovo, to i ono, da zna kako se programira ovo i ono ... shvatili ste. Preduzeće mora da objavi te pojedinosti (ime proizvođača i broj verzije uređaja s kojima se radi, konkretne odgovornosti, broj godina radnog iskustva itd.) da bi dobilo kvalifikovane ponude. Ukoliko organizacija traži profesionalca u oblasti računarske bezbednosti s, recimo, pet godina iskustva na poslovima zaštitnih barijera Check Point i IDS-a Snort, šta mislite koju barijeru i koji IDS ona ima? Ako traže stručnjaka za otkrivanje računarskih provala koji će sastaviti i voditi ekipu za odgovor na napade, šta to govori o njihovom trenutnom nivou sposobnosti otkrivanja provala i odgovora na njih? Zar nije verovatno da kod njih trenutno vlada nered u tom pogledu? Imaju li oni trenutno ikoga da to radi? Ukoliko oglas ne sadrži pojedinosti, možda se one mogu saznati telefonom. Isto važi i za zanimljivu biografiju – dovoljno je predstaviti se kao službenik agencije za zapošljavanje i postaviti pitanja. Takve pojedinosti mogu pomoći napadaču da sebi predoči detaljnu sliku iz koje se može izvesti zaključak o primenjenom sistemu obezbeđenja ciljne organizacije, a to je veoma važno znati kada se planira napad!

Ako Googleu pošaljete upit „*kompanija* resume firewall“, gde *kompanija* označava ime ciljnog preduzeća, verovatno ćete naći više radnih biografija (engl. *resume* ili *CV*) tekućih i/ili bivših radnika tog preduzeća. One sadrže veoma detaljne podatke o uređajima i programima koje organizacija koristi i novitetima koje uvode. Web lokacije za zapošljavanje, kao što su http://www. monster.com i http://www.careerbuilder.com, sadrže desetine miliona radnih biografija i oglasa za slobodna radna mesta. Njihovo pretraživanje (ako upitu dodate i ime ciljnog preduzeća) može doneti iznenađujuće tehničke pojedinosti. Da biste mogli pristupiti golemom broju biografija na takvim lokacijama, morate platiti pristupnu članarinu i to kao registrovana organizacija. Međutim, napadačima uopšte nije teško da registruju lažna preduzeća i plate pristupnu članarinu, jer tako dobijaju uvid u milione biografija.

Ostali zanimljivi podaci

Prethodno nismo pomenuli sve ideje i resurse, nego smo samo dali primer koji treba da vam posluži kao odskočna daska za samostalno prikupljanje podataka. Poverljivi podaci se kriju na svim stranama sveta, u raznim oblicima. Ukoliko odvojite vreme za maštovita i temeljna pretraživanja, to će se verovatno pretvoriti u veoma plodonosne vežbe – kako za napadače, tako i za branitelje.

Protivmere: bezbednost javnih baza podataka

Dobar deo prethodno razmatranih podataka mora biti javno dostupan i zato ih je teško ukloniti, naročito kada se radi o preduzećima čije se akcije kotiraju na berzi. Međutim, to ne znači da ih ne treba proceniti i razvrstati. Priručnik za bezbednost lokacija (engl. *Site Security Handbook*) RFC 2196, koji se može preuzeti sa adrese http://www.faqs.org/rfcs/rfc2196.html, odlično je štivo u kome su obrađeni mnogi problemi u vezi s pravilima bezbednosti. Redovno pregledajte prethodno pomenute izvore i potrudite se da uklonite poverljive podatke kad god možete. Preporučljivo je i korišćenje alijasa koji se ne preslikavaju na vas ili vašu organizaciju, naročito za diskusione grupe, liste slanja i druge javne forume.

Četvrti korak: popisivanje WHOIS i DNS

Popularnost:	*9*
Jednostavnost:	*9*
Uticaj:	*5*
Stepen rizika:	***8***

Privlačnost Interneta dobrim delom potiče od nepostojanja centralnog tela koje bi ga kontrolisalo, ali se u praksi s više njegovih funkcija mora centralno rukovoditi da bi se postigla interoperabilnost, sprečili sukobi oko IP adresa i obezbedila „univerzalna razrešivost" adresa preko svih geografskih i političkih granica. To znači da neko rukuje ogromnom količinom podataka. Ako makar i malo razumete kako se to zapravo radi, možete delotvorno da koristite to obilje informacija! Internet se mnogo promenio od svog nastanka. Još se menjaju i konkretni vidovi rukovanja tim podacima, kao i ustanove koje to obavljaju.

Dakle, pitate ko danas „upravlja" Internetom? Osnovnim funkcijama Interneta „upravlja" neprofitna organizacija Internet Corporation for Assigned Names and Numbers (ICANN; http://www.icann.org).

ICANN je tehničko telo za koordinaciju Interneta, nastalo 1998. objedinjavanjem velikog broja poslovnih, tehničkih, univerzitetskih i korisničkih Internet zajednica. ICANN preuzima odgovornost za skup tehničkih funkcija kojima je prethodno, na osnovu ugovora s vladom SAD, rukovodila ustanova Internet Assigned Numbers Authority (IANA; http://www.iana.org) i druge grupe. (IANA još uvek obavlja mnogo svakodnevnih operacija, ali sve će one jednog dana biti predate ICANN-u.) Konkretno, ICANN koordinira dodeljivanje sledećih identifikatora koji moraju biti globalno jedinstveni da bi Internet mogao da funkcioniše:

- imena Internet domena
- brojevi IP adresa
- parametri protokola i brojevi priključaka

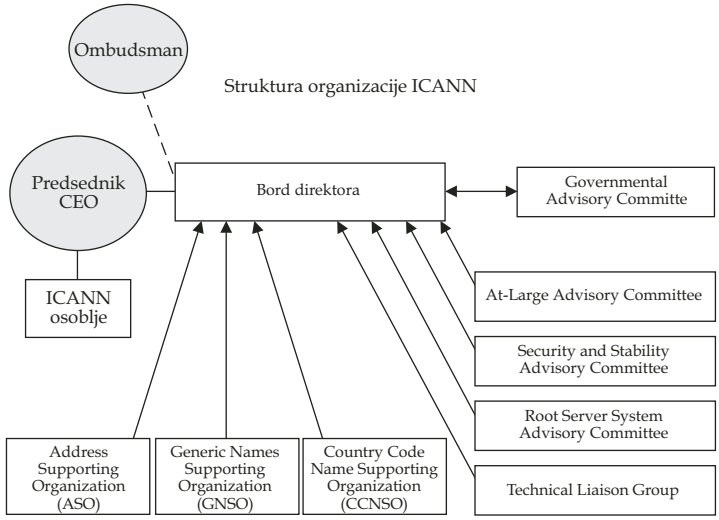
Pored toga, ICANN koordinira rad Internetovog korenskog sistema DNS servera da bi se stabilno odvijao.

Kao neprofitna korporacija u privatnom vlasništvu, ICANN je posvećen očuvanju stabilnog rada Interneta, podsticanju konkurencije, postizanju širokog prisustva globalnih Internet zajednica i razvoju strategije Interneta preko preduzeća u privatnom vlasništvu na osnovu opšte saglasnosti. ICANN podstiče na saradnju sve zainteresovane korisnike Interneta, preduzeća i organizacije.

Na slici 1-7 prikazana je organizaciona šema ICANN-a, dobijena posle njegove reorganizacije započete 2002. Prelazak na novu strukturu počeo je 15. decembra 2002, kada su na snagu stupili novi ICANN-ovi interni propisi.

ICANN ima više delova, od kojih nas sada zanimaju samo sledeća tri:

- Address Supporting Organization (ASO), http://www.aso.icann.org
- Generic Names Supporting Organization (GNSO), http://www.gnso.icann.org
- Country Code Domain Name Supporting Organization (CCNSO), http://www.ccnso.icann.org



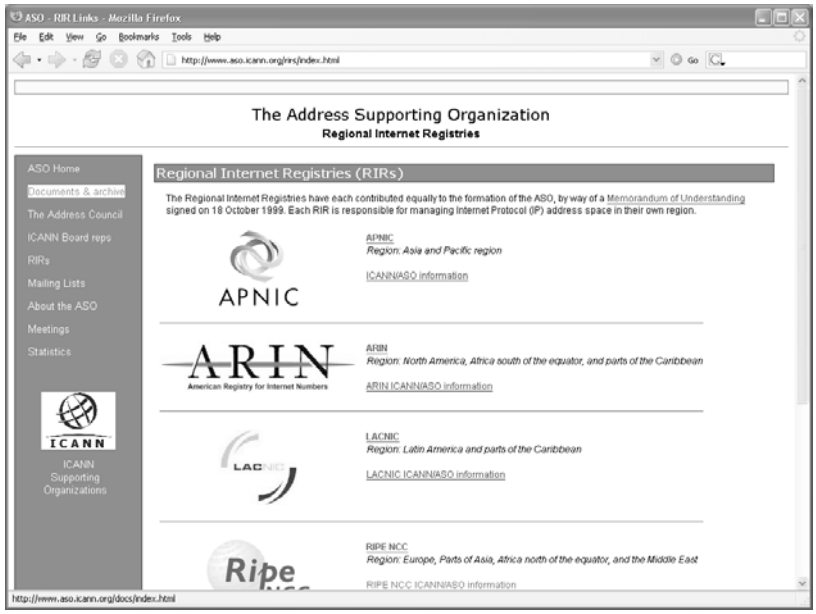
Slika 1-7 ICANN upravlja mnogim skrivenim osnovnim funkcijama Interneta.

ASO razmatra i razvija preporuke za strategiju IP adresa, i o tome izveštava Veće ICANN-a. ASO dodeljuje blokove IP adresa regionalnim registrima Interneta (RIR), koji u svojim regionima upravljaju javnim numeričkim resursima Interneta, dele ih zainteresovanima i registruju ih (slika 1-8). Zatim ti regionalni registri dodeljuju IP adrese organizacijama, davaocima usluga Interneta ili, u nekim slučajevima, nacionalnim registrima Interneta, (NIR) odnosno lokalnim registrima Interneta (LIR), ukoliko to zahtevaju pojedine vlade (većinom u komunističkim zemljama, u diktatorskim režimima itd.):

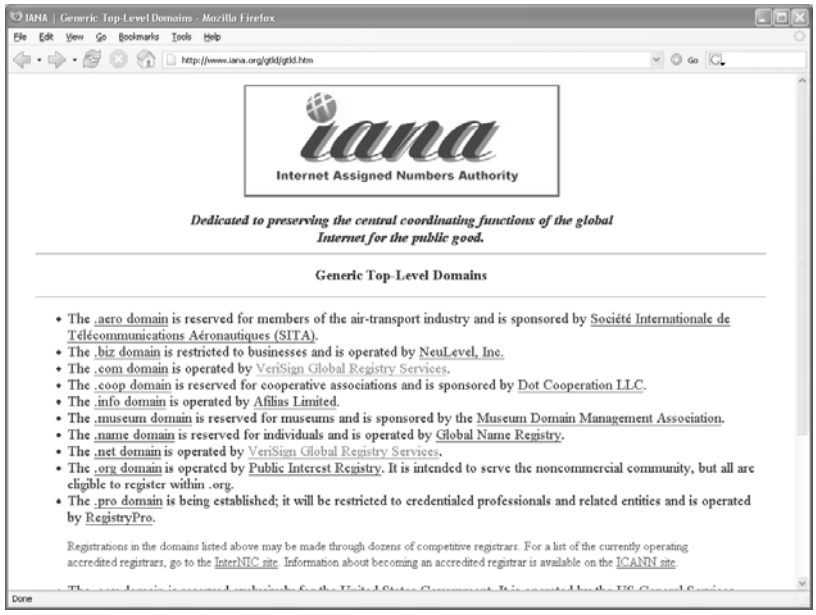
- APNIC (http://www.apnic.net) u pacifičkom regionu Azije
- ARIN (http://www.arin.net) u Severnoj i Južnoj Americi, te podsaharskim regionima Afrike
- LACNIC (http://www.lacnic.net) u Latinskoj Americi i delovima Kariba
- RIPE (http://www.ripe.net) u Evropi, delovima Azije, Africi severno od ekvatora i na Srednjem Istoku
- AfriNIC (http://www.afrinic.net, trenutno u statusu „posmatrača“) jednog dana će opsluživati oba dela Afrike, što sada rade ARIN i RIPE.

GNSO razmatra i razvija preporuke o imenima domena za sve generičke domene najvišeg nivoa i o tome izveštava Veće ICANN-a (slika 1-9). Imajte u vidu da GNSO *ne* registruje imena domena, nego je odgovoran za generičke domene najvišeg nivoa (na primer, domene .com, .net, .edu, .org i .info), čiji opis možete naći na adresi http://www.iana.org/gtld/gtld.htm.

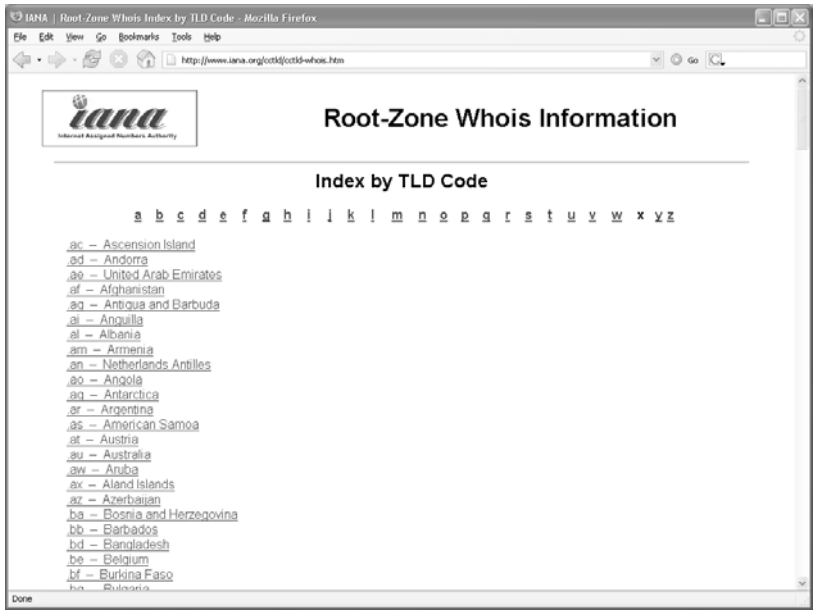
CCNSO razmatra i razvija preporuke o imenima domena za sve državne domene najvišeg nivoa i o tome izveštava Veće ICANN-a. Ponavljam, ICANN ne registruje imena domena. Konačna lista državnih domena najvišeg nivoa može se naći na adresi http://www.iana.org/cctld/cctld-whois.htm (i na slici 1-10).



Slika 1-8 Trenutno postoji pet regionalnih registara Interneta, četiri aktivna i jedan u statusu „posmatrača“.



Slika 1-9 GNSO upravlja generičkim domenima najvišeg nivoa.



Slika 1-10 CCNSO upravlja imenima domena za sve državne domene najvišeg nivoa.

Evo još nekih korisnih hiperveza:

- za dodeljivanje IP v4 adresa: http://www.iana.org/assignments/ipv4--address-space
- za usluge IP adresa: http://www.iana.org/ipaddress/ip-addresses.htm
- za IP adrese za specijalnu namenu: http://www.rfc-editor.org/rfc/rfc3330.txt
- za registrovane brojeve priključaka: http://www.iana.org/assignments/port-numbers
- za registrovane brojeve protokola: http://www.iana.org/assignments/protocol-numbers

S obzirom na sve to centralizovano upravljanje, pronalaženje podataka bi trebalo da bude jednostavno kao slanje upita toj centralnoj farmi superservera, zar ne? Ne baš. Upravljanje jeste prilično centralizovano, ali su podaci, iz tehničkih i političkih razloga, raspršeni po celom svetu na brojnim WHOIS serverima. Da stvari budu još zamršenije, sintaksa WHOIS upita, tip dozvoljenih upita, podaci koji su dostupni i formatiranje rezultata, razlikuju se znatno od jednog servera do drugog. Nadalje, mnoge ustanove za registraciju aktivno ograničavaju upite da bi se odbranile od pošiljaoca neželjenih poruka, hakera i preopterećenja resursa. I najzad, radi državne bezbednosti, podaci o domenima .mil i .gov uopšte nisu javno dostupni.

Zato s pravom možete pitati: „Pa *kako* da nađem podatke koji su mi potrebni?“ Pomoću određenih alatki, malo znanja koje se stiče samo iskustvom (jer ne piše u knjigama) i s nešto strpljenja, trebalo bi da možete uspešno pronaći pojedinosti o domenu i IP adresi gotovo svih registrovanih entiteta na planeti!

Pretraživanja o domenima

Imajte u vidu da se podaci o domenima (kao što je mikroknjiga.com) registruju nezavisno od svega što ima veze sa IP adresama (kao što su mrežni blokovi IP adresa, samostalni sistemi BGP brojeva itd.). To znači da ćemo u metodologiji imati dve zasebne putanje za pronalaženje tih pojedinosti. Počećemo od pojedinosti u vezi s domenima; kao primer poslužiće nam domen keyhole.com.

Prvo treba ustanoviti koji od brojnih WHOIS servera sadrži podatke koje tražimo. Opšti postupak je sledeći: ovlašćeni registar (engl. ***R**egistry*) za dati domen najvišeg nivoa, u ovom slučaju „.com“, sadrži podatke o ustanovi (engl. ***R**egistrar*) koja je registrovala domen ciljne organizacije (engl. ***R**egistrant*). Zatim se šalje upit toj ustanovi, a ona vraća podatke o organizaciji koja je registrovala konkretno ime domena. To se naziva „Tri R“ WHOIS upita (**R**egistry, **R**egistrar, **R**egistrant).

Na Internetu ima mnogo lokacija koje pružaju sve (sopstvene) WHOIS podatke, ali morate naučiti da sami pronađete podatke u slučajevima kada automatske alatke ne rade. Pošto su WHOIS podaci hijerarhijski, najbolje je početi od vrha tog stabla – od ICANN-a. Kao što smo već rekli, ICANN (IANA) je ovlašćeni registar za sve domene najvišeg nivoa i odlična početna tačka za zadavanje ručnih WHOIS upita.

NAPOMENA

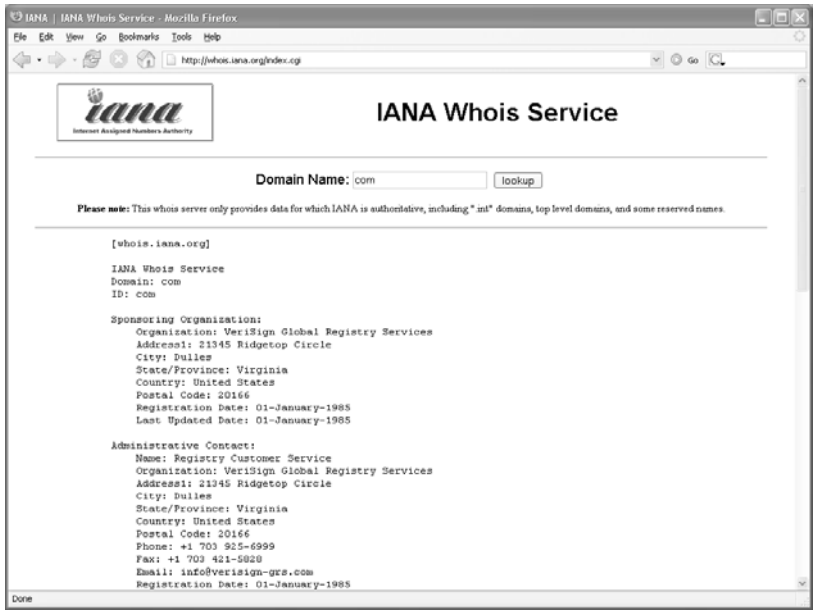
WHOIS pretraživanje možete obavljati s komandne linije bilo kog WHOIS klijenta (za šta je potreban izlazni pristup TCP-u na priključku 43) ili pomoću nezamenljivog čitača Weba. Naše iskustvo pokazuje da se metoda čitača Weba obično intuitivno lakše shvata i da je gotovo uvek dozvoljena u većini bezbednosnih arhitektura.

Na lokaciji http://whois.iana.org možemo pronaći ovlašćene registre svih .com domena. U ovom primeru (slika 1-11) vidimo da je za .com ovlašćen registar Verisign Global Registry Services, na adresi http://www.verisign-grs.com. Kada odemo do te lokacije (slika 1-12) i potražimo keyhole.com, videćemo da je taj domen registrovala ustanova http://www.markmonitor.com. Kada posetimo *tu* lokaciju (slika 1-13), šaljemo upit njenom WHOIS serveru (preko njenog Web interfejsa) i od njega dobijamo pojedinosti o registrovanom entitetu keyhole.com. Gotovo!

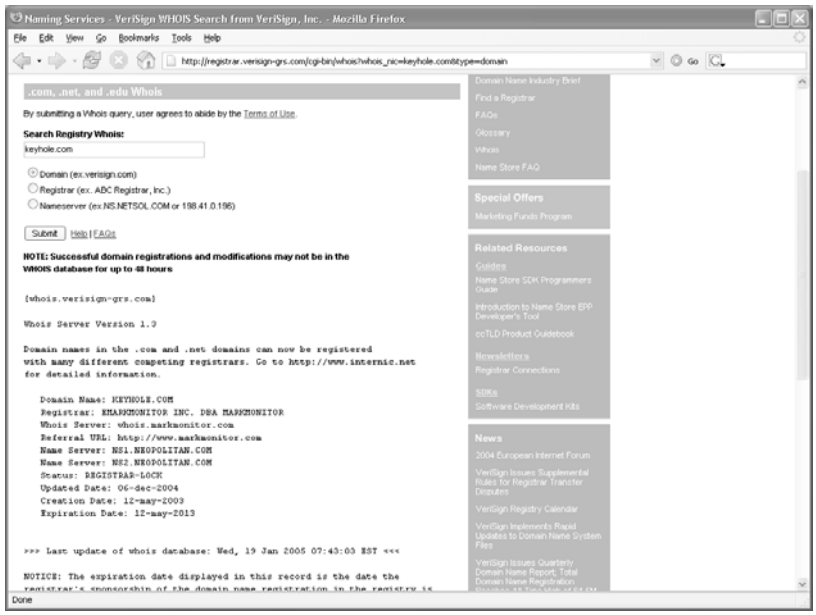
Pojedinosti o registrovanom entitetu obuhvataju poštansku (uličnu) adresu, telefonske brojeve, imena i elektronske adrese osoba za kontakt, imena DNS servera, IP adrese itd. Ako ste pažljivo pratili ovaj postupak, ne bi trebalo da imate previše poteškoća pri pronalaženju pojedinosti o registrovanim entitetima za sva (javna) imena domena na svetu. Ne zaboravite, ima domena (na primer, .mil i .gov) kojima se ne može pristupiti zadavanjem WHOIS upita.

Da ne bismo bili nepotpuni, navešćemo tri komande pomoću kojih se isto pretraživanje radi s komandne linije WHOIS klijenta:

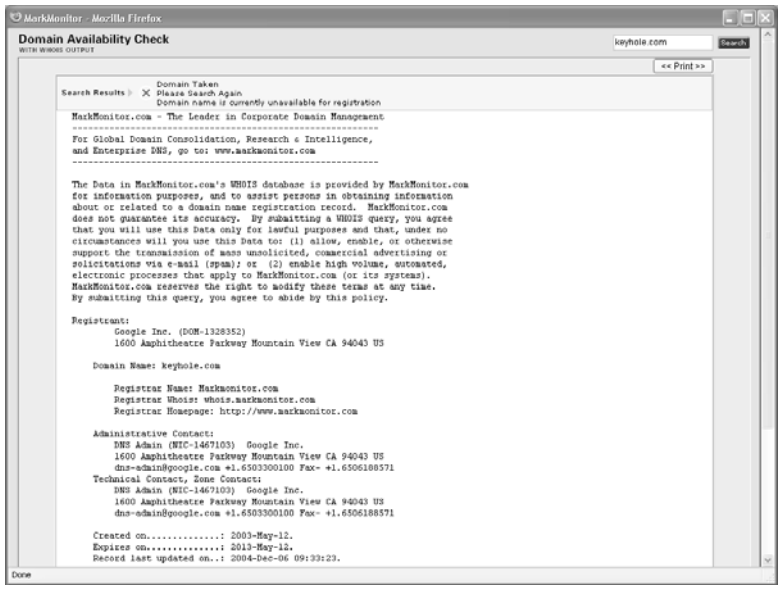
```
[bash]$ whois com -h whois.iana.org
[bash]$ whois keyhole.com -h whois.verisign-grs.com
[bash]$ whois keyhole.com -h whois.omnis.com
```



Slika 1-11 Pretraživanje domena počinjemo na lokaciji http://whois.iana.org.



Slika 1-12 Verisign Global Registry Services pokazuje ustanovu koja je registrovala domen keyhole.com.



Slika 1-13 Pojedinosti o domenu keyhole.com nalazimo na lokaciji odgovarajuće ustanove za registrovanje.

Evo i nekih lokacija koje, s različitim uspehom, pokušavaju da automatizuju ovaj postupak:

- http://www.allwhois.com
- http://www.uwhois.com
- http://www.internic.net/whois.html

I najzad, na raspolaganju vam je nekoliko grafičkih korisničkih interfejsa koji olakšavaju pretraživanje:

- SamSpade, http://www.samspade.org
- SuperScan, http://www.foundstone.com
- NetScan Tools Pro, http://www.nwpsw.com

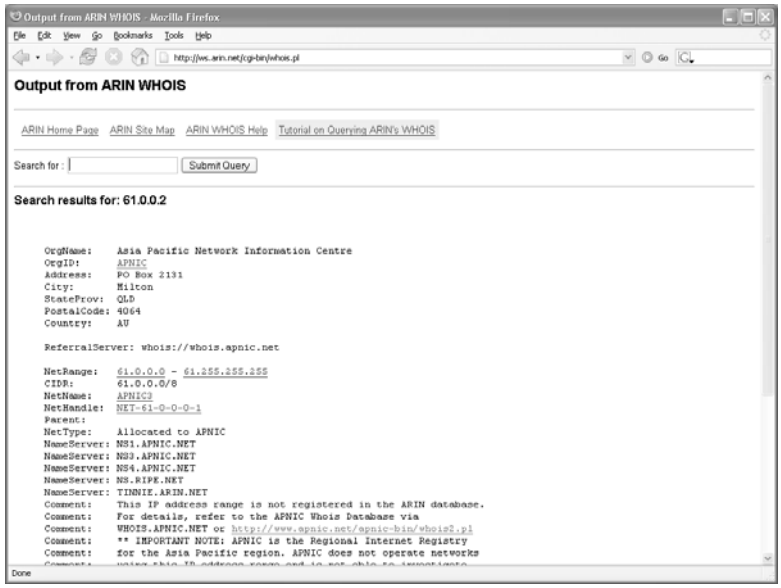
Nakon što pronađete odgovarajući WHOIS server za svoju ciljnu organizaciju, on će *možda* hteti da vam odgovori i na druge upite (ako ustanova za registrovanje to dozvoljava). Možda ćete tako pronaći sve domene koje određeni DNS server ugošćava ili sva imena domena koja sadrže određen znakovni niz. Većina WHOIS servera takve upite sve više odbija, ali se još uvek isplati baciti pogled da biste proverili šta sve ustanova za registrovanje dozvoljava. Možda je dozvoljeno baš ono što ste tražili.

Pretraživanja o IP adresama

U prethodnim odeljcima dobro su objašnjena pretraživanja o domenima, ali šta je sa registracijom IP adresa? Kao što je već rečeno, registraciju IP adresa obrađuju razne regionalne ustanove kojima je nadređen ICANN-ov ASO. Pogledajmo kako se pronalaze ovi podaci.

WHOIS server ustanove ICANN (IANA) trenutno još nije ovlašćen za registrovanje svih regionalnih ustanova za registraciju (kao što jeste za sve domene najvišeg nivoa), ali svaka regionalna ustanova zna kojim opsegom IP adresa upravlja. Zato ćemo na početku našeg pretraživanja odabrati bilo koju od njih. Ukoliko smo izabrali pogrešnu, ona će nas uputiti na pravu.

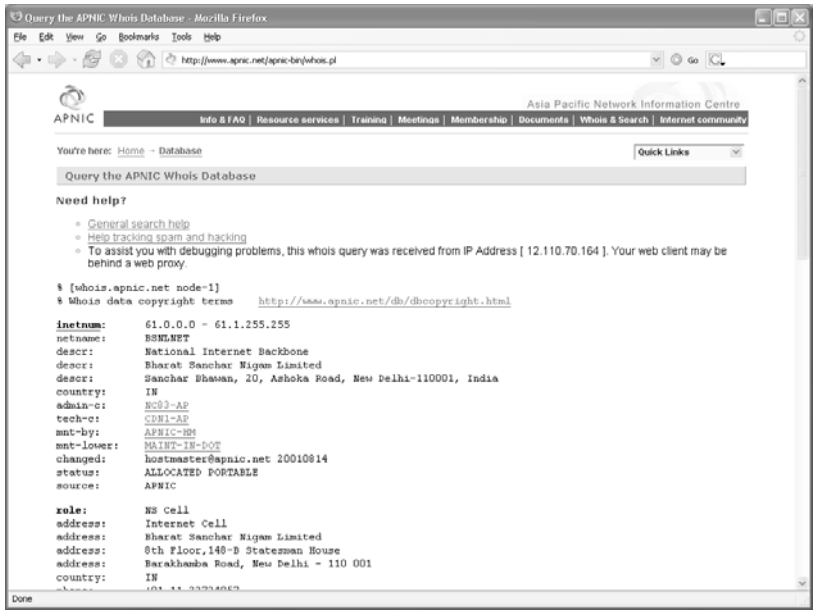
Pretpostavimo da ste tokom prelistavanja zapisnika o mrežnoj aktivnosti (što nikada ne propuštate da uradite, zar ne?) naleteli na zanimljivu stavku sa izvornom IP adresom 61.0.0.2. Najpre ćemo tu IP adresu upisati u WHOIS upit na lokaciji http://www.arin.net (slika 1-14), koja nam odgovara da tim opsegom IP adresa upravlja APNIC. Zatim idemo na APNIC-ovu lokaciju i tamo nastavljamo pretraživanje (slika 1-15). Ovde saznajemo da tom IP adresom upravlja indijska kompanija National Internet Backbone.



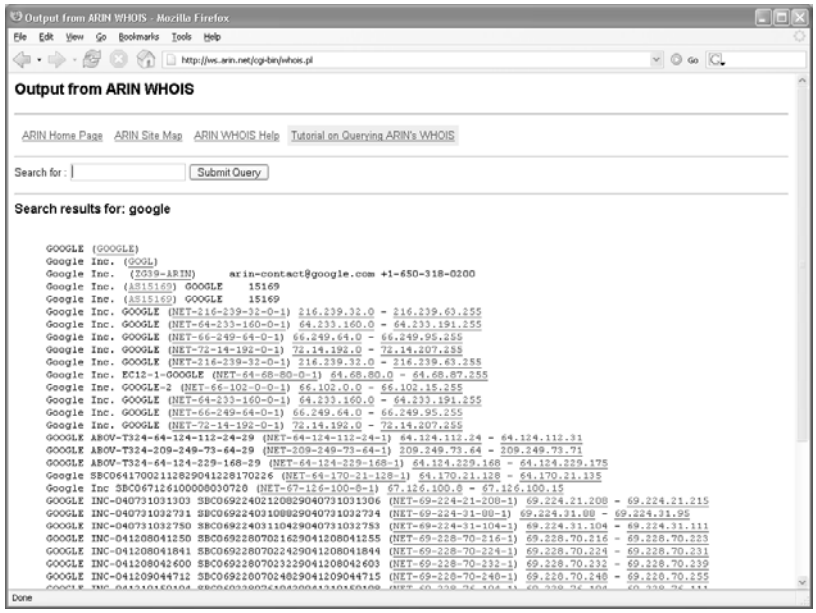
Slika 1-14 ARIN nam saopštava koju RRI treba da pretražimo.

Istim postupkom se svaka IP adresa na svetu može propratiti do svog vlasnika ili barem do osobe za kontakt, koja eventualno može biti voljna da vam saopšti preostale pojedinosti. Kao i za sve drugo, stepen kooperativnosti je različit i menja se prema kompaniji ili državi s kojom poslujete. Ne gubite iz vida da haker ima mnogo načina da sakrije svoju pravu IP adresu. IP adresa navedena u vašim zapisnicima aktivnosti lako može biti tzv. „oprana“ adresa.

Pretraživanjem WHOIS servera odgovarajuće regionalne ustanove za registrovanje, kome smo zadali doslovno ime ciljne organizacije, možemo otkriti i opsege IP adresa i samostalne sistemske (engl. *autonomous system*, AS) BGP brojeve koji „pripadaju“ toj organizaciji. Na primer, ako na lokaciji http://www.arin.net zadamo ime „Google“, dobićemo opsege IP adresa koje Google poseduje pod svojim imenom, kao i njegov AS broj, AS15169 (slika 1-16).



Slika 1-15 Ispostavlja se da je ta IP adresa vlasništvo indijske kompanije National Internet Backbone.



Slika 1-16 Ovde vidimo opsege IP adresa i BGP AS broj koje Google poseduje pod sopstvenim imenom.

U tabeli 1-2 navedene su razne alatke za WHOIS pretraživanje.

Tabela 1-2 Tehnike pretraživanja podataka o domenima i izvori informacija

Mehanizam	Izvor	Platforma
Web lokacija	http://whois.iana.org/	Bilo koja platforma s čitačem Weba
	http://www.arin.net	
	http://www.allwhois.com	
WHOIS klijent	WHOIS se isporučuje s većinom verzija UNIX-a	UNIX
	Fwhois je napravio Chris Cappuccio <ccapuc@santefe.edu>	
WS_Ping ProPack	http://www.ipswitch.com/	Windows 95/NT/2000/XP
Sam Spade	http://www.samspade.org/ssw	Windows 95/NT/2000/XP
Web verzija Sam Spade	http://www.samspade.org/	Bilo koja platforma s Web klijentom
Alatke Netscan	http://www.netscantools.com/nstpromain.html	Windows 95/NT/2000/XP
Xwhois	http://c64.org/<126>nr/xwhois/	UNIX sa X-om i GTK+ grafička biblioteka
Jwhois	http://www.gnu.org/software/jwhois/jwhois.html	UNIX

Važan podatak je i ime osobe za kontakt, zato što vas ono može dovesti do imena osobe odgovorne za Internet priključak ili zaštitnu barijeru. Kao odgovor na naš upit dobili smo i telefonski broj i broj faksa. Ti podaci su od ogromne pomoći kada se ispituje mogućnost neovlašćenog upada preko telefonske mreže. Samo pokrenite program za automatsko pozivanje opsega telefonskih brojeva (engl. *war-dialer*) „nahranjen“ dobijenim opsegom i na dobrom ste putu da otkrijete modemske brojeve organizacije. Pored toga, napadač se lakovernim osobama u organizaciji često lažno predstavlja kao administrator. Napadač će nesmotrenom korisniku čak poslati, u ime administratora, stručno „nacifranu“ poruku. Prosto je neverovatno koliko će se korisnika upecati i promeniti lozinku u bilo šta što im predložite, sve dok veruju da takav zahtev šalje službenik tehničke podrške.

Datumi pravljenja i modifikacije zapisa ukazuju na tačnost podataka u njemu. Ako je zapis napravljen pre pet godina i otada nije menjan, verovatno je zastareo barem deo tih podataka (recimo, ime administratora).

Poslednji podatak su ovlašćeni (engl. *authoritative*) DNS serveri. Prvi je primarni DNS server; slede sekundarni, tercijarni itd. Te podatke ćemo upotrebiti za ispitivanje baze podataka DNS, koje je objašnjeno u nastavku poglavlja. Pored toga, dobijeni opseg mrežnih adresa možemo upotrebiti kao početnu tačku u pretraživanju baze podataka ARIN.

Protivmere: obezbeđivanje javnih baza podataka

Dobar deo podataka iz raznih dosad razmotrenih baza, prilagođen je za javno objavljivanje. Kada organizacija registruje svoj domen na Internetu, mora da obznani i podatke o njegovom administratoru, registrovanim mrežnim blokovima i serverima ovlašćenim za imena. Međutim, to ne znači da pri tom ne treba uzeti u obzir bezbednost; naprotiv, podatke treba sročiti tako da otežaju posao napadačima.

Često se dešava da administrator napusti organizaciju, a da i dalje može da menja podatke o njenom domenu. Zato se najpre treba pobrinuti da podaci u bazi podataka ne budu zastareli – čim to postanu, ažurirajte podatke o osobama zaduženim za administriranje, tehnički deo posla i naplatu. Razmislite o telefonskim brojevima i adresama koje navodite u bazi. Oni mogu poslužiti kao polazište za napad pretraživanjem telefonskog opsega i za lažno predstavljanje. Mogli biste navesti određen besplatan telefonski broj (koji napadača može dovesti samo do Telekoma) ili broj koji nije u telefonskoj centrali vaše organizacije. Sem toga, znamo za nekoliko organizacija koje su, u nameri da sapletu potencijalnog napadača, navele ime fiktivnog administratora. Čim se nekom od zaposlenih telefonski ili e-poštom javi takav „administrator“, za službu računarske bezbednosti, to je znak da imaju posla s prevarantom.

Drugu opasnost pri registrovanju domena prouzrokuje način ažuriranja podataka koji dozvoljavaju neke od ustanova za registraciju. Primera radi, tekuća realizacija servera Network Solutions dozvoljava automatske izmene podataka o domenu koje stignu s Mreže. Identitet osobe koja se javlja u ime registrovanog domena, Network Solutions proverava metodom Guardian, što znači da upotrebljava bilo koju od tri različite metode provere identiteta: sadržaj polja FROM u poruci e-pošte, lozinku i šifru PGP (Pretty Good Privacy). Najslabija metoda provere identiteta je sadržaj polja FROM u poruci e-pošte. Zapanjujuće je što je polje FROM iz poruke e-pošte podrazumevana metoda identifikovanja. Posledice ovakvog izbora po bezbednost nesagledive su. Gotovo svako, i to „malim prstom leve ruke“, može da krivotvori adresu elektronske pošte i da promeni podatke koji se odnose na vaš domen, što je postupak poznatiji kao *otimanje domena* (engl. *domain hijacking*). Upravo to je, kako je 16. oktobra 1998. objavio *Washington Post*, doživeo veliki davalac Internet usluga, America Online. Neko se predstavio kao službenik AOL-a i promenio AOL-ove podatke o domenu, tako da je sav mrežni saobraćaj bio preusmeren na adresu autonete.net.

AOL se od ovog incidenta brzo oporavio, ali incident pokazuje ranjivost organizacije na Internetu. Treba se odlučiti za bezbednije rešenje, npr. lozinku ili PGP identifikaciju, da bi se omogućilo menjanje podataka o domenu. Naglasimo i to da je za identifikovanje pomoću obrasca Contact Form koji koristi server Network Solutions, neophodno da se prethodno uspostavi administratorska ili tehnička veza.

Peti korak: Ispitivanje DNS-a

Nakon što otkrijete sve domene dodeljene organizaciji, možete početi da ispitujete DNS. DNS je distribuirana baza podataka pomoću koje se IP adrese preslikavaju u imena umreženih računara, i obrnuto. Ako je DNS nebezbedno konfigurisan, moguće je otkriti podatke o organizaciji.

Prenosi zona

Popularnost:	*9*
Jednostavnost:	*9*
Uticaj:	*3*
Stepen rizika:	***7***

Jedan od najozbiljnijih propusta u konfiguraciji koje administrator sistema može da načini, jeste da omogući neovlašćenim korisnicima Interneta da prenesu zone DNS-a.

Prenos zone (engl. *zone transfer*) dozvoljava sekundarnom serveru da svoju bazu podataka sa zonama ažurira s primarnog servera. Tako se postiže da sistem nastavi da radi ako primarni DNS server otkaže. Prenos DNS zone u načelu treba da obavljaju samo sekundarni serveri. Mnogi serveri imena domena su, međutim, loše podešeni, pa omogućavaju prenose zona svakome ko to zatraži. To ne mora obavezno da bude loše ako se dostupne informacije odnose samo na sisteme povezane na Internet, iako olakšava napadačima da pronađu potencijalne ciljeve. Stvarni problem nastaje kada organizacija ne razdvaja spoljne od unutrašnjih, privatnih DNS servera. U tom slučaju, interna imena računara i njihove IP adrese izloženi su pogledima napadača. Kada informacije o internim IP adresama date u ruke korisniku Interneta koji za takve podatke nije ovlašćen, to je isto kao da ste mu dali plan ili mapu interne mreže organizacije.

Isprobajmo nekoliko metoda za prenos zona i analizirajmo podatke koje možemo na taj način da prikupimo. Iako se mnogim alatkama može izvesti prenos zone, razmatranje ćemo ograničiti na nekoliko najčešće korišćenih.

Zonu ćete jednostavno preneti ako upotrebite program nslookup, koji se isporučuje s većinom UNIX i Windows sistema. Komandu nslookup možemo da upotrebimo interaktivno:

```
[bash]$ nslookup
Default Server: ns1.example.net
Address: 10.10.20.2
> 216.182.1.1
Server: ns1.example.net
Address: 10.10.20.2
Name: gate.tellurian.net
Address: 216.182.1.1

> set type=any
> ls -d Tellurian.net. >\> /tmp/zone_out
```

Najpre pokrećemo nslookup u interaktivnom režimu. Kada se pokrene, program će ispisati podrazumevani server imena koji koristi, što je po pravilu DNS server organizacije ili DNS davaoca usluga Interneta. Međutim, naš server imena domena (10.10.20.2) nije ovlašćen za ciljni domen, tako da nema sve DNS zapise koje tražimo. Zbog toga programu nslookup moramo ručno da zadamo DNS server koji treba da pretražuje. U ovom primeru hoćemo da upotrebimo primarni server imena domena za Tellurian Networks (216.182.1.1). Setite se da smo taj podatak našli ranije na WHOIS serveru.

Posle toga, za vrstu zapisa biramo vrednost „any". To će omogućiti da preuzmemo svaki raspoloživi DNS zapis i dobijemo potpunu listu (`man nslookup`).

Na kraju, koristimo opciju `ls` da bismo izlistali sve povezane zapise u domenu. Parametar `-d` omogućava izlistavanje svih zapisa domena. Na kraj smo dodali tačku (.) da naznačimo potpuno ime domena, iako najčešće možete da je izostavite. Osim toga, rezultat smo preusmerili u datoteku /tmp/zone_out da bismo ga mogli koristiti i kasnije.

Pošto prenesemo zonu, pregledaćemo datoteku i u njoj potražiti informacije koje bi nam eventualno mogle pomoći da se usmerimo na određene sisteme. Pogledajmo simulirani rezultat, pošto Tellurian Networks ne dozvoljava prenos zone:

```
[bash]$ more zone_out
acct18          1D IN A    192.168.230.3
             1D IN HINFO  "Gateway2000" "WinWKGRPS"
             1D IN MX   0 tellurianadmin-smtp
             1D IN RP   bsmith.rci bsmith.who
             1D IN TXT   "Location:Telephone Room"
ce            1D IN CNAME  aesop
au            1D IN A    192.168.230.4
             1D IN HINFO  "Aspect" "MS-DOS"
             1D IN MX   0 andromeda
             1D IN RP   jcoy.erebus jcoy.who
             1D IN TXT   "Location: Library"
acct21          1D IN A    192.168.230.5
             1D IN HINFO  "Gateway2000" "WinWKGRPS"
             1D IN MX   0 tellurianadmin-smtp
             1D IN RP   bsmith.rci bsmith.who
             1D IN TXT   "Location:Accounting"
```

Nećemo detaljno analizirati svaki zapis, već ćemo izdvojiti glavne tipove. Vidimo da za svaku odrednicu imamo po jedan zapis tipa „A" koji označava IP adresu imena sistema na desnoj strani. Osim toga, svaki umreženi računar ima zapis HINFO koji identifikuje platformu ili tip aktivnog operativnog sistema (pogledajte RFC 952). Zapisi HINFO nisu nužni za korišćenje DNS-a, a napadačima pružaju obilje informacija. Pošto smo snimili rezultate prenosa zone u datoteku, možemo da ih obradimo pomoću UNIX-ovih programa grep, sed, awk ili perl.

Pretpostavimo da smo stručnjaci za sistem SunOS ili sistem Solaris. Mogli bismo pomoću programa da pronađemo IP adrese koje su u zapisu HINFO povezane sa Sparcom, Sunom ili Solarisom.

```
[bash]$ grep -i solaris zone_out |wc -1
     388
```

Vidimo da imamo 388 potencijalnih zapisa koji sadrže reč „Solaris“. Očigledno, imamo mnogo ciljeva.

Recimo da želimo da pronađemo probne sisteme, omiljenu metu napadača. Zašto? Prosto zato što takvi sistemi obično nisu bogzna kako obezbeđeni, njihove lozinke se lako provaljuju, a administratori ne brinu mnogo o tome ko im pristupa. To je savršen plen za svakog napasnika. Probne sisteme ćemo potražiti na sledeći način:

```
[bash]$ grep -i test /tmp/zone_out |wc -1
     96
```

Dobili smo 96 odrednica u datoteci zone koje sadrže reč „test“. To bi značilo da u zoni postoji priličan broj probnih sistema. Većina uljeza će razgledati i prevrtati ove podatke dok ne nađu konkretne tipove sistema s poznatom ranjivošću.

Imajte nekoliko stvari na umu. Opisanim postupkom možete da pretražujete samo po jedan server imena. To znači da postupak morate ponoviti za svaki server imena koji je ovlašćen za ciljni domen. Osim toga, pretraživali smo samo domen tellurian.net. Ako postoje poddomeni (na primer, greenhouse.tellurian.net), svaki bismo morali da pretražimo na isti način. Konačno, možda ćete dobiti poruku da ne možete da izlistate domen ili da se zahtev za prenos odbija. U tom slučaju, server je podešen tako da neovlašćenim korisnicima ne dozvoljava prenos zone. Zbog toga ne biste ni mogli da prenesete zonu s tog servera. Međutim, ako postoji više servera imena domena, možda ćete naći neki koji će vam dozvoliti da prenesete zonu.

Pošto smo vas uputili u ručnu varijantu postupka, znajte da postoji mnogo alatki koje postupak ubrzavaju, a među njima su host, Sam Spade, axfr i dig.

Alatka `host` postoji na većini UNIX sistema. Evo nekoliko jednostavnih načina njene primene:

```
host -1 tellurian.net
```

i

```
host -1 -v -t any tellurian.net
```

Ako IP adrese želite samo da sprovedete u skript komandnog okruženja, naredbom `cut` možete da izdvojite samo IP adrese iz rezultata naredbe `host`:

```
host -1 tellurian.net |cut -f 4 -d" " >\> /tmp/ip_out
```

Sisteme ne morate da snimate samo iz UNIX-a. Iste funkcije obezbeđuju mnogi Windowsovi programi, kao što je Sam Spade.

Najzad, možete da upotrebite jednu od najboljih alatki za prenošenje zone, Gaiusov program `axfr` (http://packetstormsecurity.nl/groups/ADM/axfr-0.5.2.tar.gz). Taj uslužni program će rekurzivno prenositi informacije o zoni i napraviti komprimovanu bazu podataka zone i datoteka koje se odnose na računare za svaki pretraživani domen. Možete da mu prosledite i domene najvišeg nivoa, kao što su com i edu, i da dobijete sve domene povezane s navedenim domenima. To se,

međutim, ne preporučuje, zato što svaki od tih domena najvišeg nivoa sadrži ogroman broj domena. Axfr pokrećete na sledeći način:

```
 [bash]$ axfr tellurian.net
axfr: Using default directory: /root/axfrdb
Found 2 name servers for domain 'tellurian.net':
Text deleted.
Received XXX answers (XXX records).
```

Da biste u bazi podataka koju je napravio program axfr pronašli tražene informacije, upišite:

```
[bash]$ axfrcat tellurian.net
```

Pronalaženje zapisa sistema za razmenu pošte (MX)

Prepoznavanje mesta na kome se rukuje poštom dobra je polazna tačka za pronalaženje zaštitne barijere mreže ciljne organizacije. Često se u komercijalnom okruženju poštom rukuje na istom sistemu na kome se nalazi i zaštitna barijera ili barem u istoj mreži. Tada možemo da upotrebimo komandu `host` i da prikupimo dodatne informacije:

```
[bash]$ host tellurian.net

tellurian.net has address 216.182.1.7
tellurian.net mail is handled (pri=10) by mail.tellurian.net
tellurian.net mail is handled (pri=20) by smtp-forward.tellu-
rian.net
```

Protivmera: obezbeđivanje baze podataka DNS

DNS podaci pružaju napadačima obilje informacija, zato treba smanjiti količinu informacija dostupnih preko Interneta. Kada je reč o konfiguraciji računara – domaćina, prenos zone se sme odobriti samo ovlašćenim serverima. Savremene verzije BIND-a mogu se podesiti komandom `allow-transfer` u datoteci named.conf. Ako želite da ograničite prenos zona Microsoftovog DNS servera, upotrebite opciju Notify. (Više o tome potražite na adresi http://www.microsoft. com/technet/prodtechnol/windows2000serv/maintain/optimize/c19w2kad. mspx.) U slučaju ostalih servera imena, pregledajte dokumentaciju i utvrdite kako se može ograničiti ili sprečiti prenos zone.

S druge strane, na mreži biste mogli da postavite zaštitnu barijeru ili usmerivač koji filtrira pakete, tako da uskraćuje pristup svim dolaznim zahtevima ka TCP priključku 53. Pošto zahtevi za traženje imena koriste protokol UDP, a zona se prenosi protokolom TCP, time se delotvorno osujećuje pokušaj prenosa zone. Međutim, predloženom protivmerom krši se RFC pravilo koje traži da se DNS upiti veći od 512 bajtova upućuju protokolom TCP. Po pravilu, zahtevi za DNS pretraživanje i nisu duži od 512 bajtova. Bolje rešenje bi bilo da se uvede šifrovano potpisivanje transakcija (Transaction Signatures, TSIG) i tako prenos zone dopusti samo računarima koji za to imaju dozvolu. Početnicu u kojoj je odlično objašnjeno realizovanje bezbednosnih TSIG mera u Bindu 9, naći ćete na adresi http://www.linux--mag.com/2001-11/bind9_01.html.

Ograničavanjem prenosa zone produžavate vreme za koje će napadači stići da ispitaju IP adrese i imena računara. Međutim, pošto je pretraživanje imena još uvek moguće, napadači mogu ručno da pretraže sve IP adrese određenog mrežnog bloka. Zato podesite spoljne servere imena tako da pružaju obaveštenja samo o sistemima koji su direktno povezani sa Internetom. Spoljni serveri imena ne smeju da odaju informacije o internoj mreži. To može da liči na preterivanje, ali verujte da smo videli loše podešene servere imena iz kojih smo mogli da izvučemo čak 16.000 internih IP adresa i odgovarajućih imena umreženih računara. I na kraju, ne preporučujemo da koristite zapise tipa HINFO. Kao što ćete videti u narednim poglavljima, operativni sistem ciljnog računarskog sistema možete da identifikujete s velikom preciznošću. Zapisi tipa HINFO omogućavaju napadačima da pomoću automatizovanih alatki lakše pronađu potencijalno ranjive sisteme.

Šesti korak: upoznavanje mreže

Pošto smo identifikovali mreže ciljne organizacije, pokušajmo da utvrdimo njihovu topologiju i potencijalne puteve pristupanja.

Otkrivanje putanje

Popularnost:	*9*
Jednostavnost:	*9*
Uticaj:	*2*
Stepen rizika:	***7***

Za ovaj posao možemo da upotrebimo program traceroute (ftp://ftp.ee.lbl.gov/traceroute.tar.gz) koji postoji u varijantama UNIX-a, a ima ga i Windows, gde se zove tracert.

Van Jacobson je napravio dijagnostičku alatku traceroute za praćenje puta IP paketa od jednog do drugog računara u mreži. Program traceroute koristi opciju vremena preživljavanja paketa (engl. *time-to-live*, TTL) da bi sa svakog mrežnog usmerivača (engl. *router*) izazvao slanje ICMP poruke TIME_EXCEEDED. Svaki usmerivač koji obrađuje paket istovremeno umanjuje vrednost TTL polja za jedinicu, pa TTL polje postaje svojevrstan brojač skokova. Program traceroute možemo da upotrebimo da bismo utvrdili tačnu putanju paketa. Kao što smo pomenuli, traceroute pomaže da otkrijete topologiju ciljne mreže i identifikujete mehanizme za kontrolu pristupa (kao što su programski izvedena zaštitna barijera ili usmerivač za filtriranje paketa) koji možda filtriraju saobraćaj.

Razmotrimo to na jednom primeru.

```
[bash]$ traceroute tellurian.net
traceroute to tellurian.net (216.182.1.7), 30 hops max, 38 byte
packets
 1 (205.243.210.33) 4.264 ms 4.245 ms 4.226 ms
 2 (66.192.251.0) 9.155 ms 9.181 ms 9.180 ms
```

```
3 (168.215.54.90) 9.224 ms 9.183 ms 9.145 ms
4 (144.232.192.33) 9.660 ms 9.771 ms 9.737 ms
5 (144.232.1.217) 12.654 ms 10.145 ms 9.945 ms
6 (144.232.1.173) 10.235 ms 9.968 ms 10.024 ms
7 (144.232.8.97) 133.128 ms 77.520 ms 218.464 ms
8 (144.232.18.78) 65.065 ms 65.189 ms 65.168 ms
9 (144.232.16.252) 64.998 ms 65.021 ms 65.301 ms
10 (144.232.15.130) 82.511 ms 66.022 ms 66.170 ms
11 www.tellurian.net(216.182.1.7) 82.355 ms 81.644 ms 84.238 ms
```

Vidimo putanju paketa koji do odredišta stiže u nekoliko skokova. Paketi putuju kroz razne sisteme bez blokiranja. Stoga pretpostavljamo da je na odredištu aktivan mrežni računar i da se prethodni skok (10) odnosi na usmerivač na obodu organizacije. Skok 10 može da bude programska zaštitna barijera ili jednostavan uređaj za filtriranje paketa – to još ne znamo. Kada na mreži naletite na aktivan sistem, ispred njega se obično nalazi uređaj za preusmeravanje (na primer, usmerivač ili zaštitna barijera).

Prethodni primer je veoma uprošćen. U složenom okruženju može da bude više putanja, odnosno uređaja za usmeravanje s više mrežnih veza (na primer, serijska skretnica Cisco 7500 ili uravnoteživači opterećenja). Štaviše, svaka veza može da ima drugačiju listu za kontrolu pristupa (engl. *access control list*, ACL). Mnoge veze će propustiti zahtev programa traceroute, ali će ga druge odbiti zato što imaju drugačiju ACL listu. Zbog toga je neophodno da programom traceroute ispitate celu mrežu. Pošto traceroute primenite na sve sisteme u mreži, počnite da sastavljate dijagram mreže koji treba da odslika arhitekturu mrežnog prolaza na Internet i lokaciju mehanizama pomoću kojih se kontroliše pristup. Taj dijagram se naziva *dijagram putanja za pristup* (engl. *access path diagram*).

Treba znati da većina varijanti programa traceroute u UNIX-u, pakete podrazumevano šalje protokolom UDP (User Datagram Protocol), uz opciju korišćenja protokola ICMP (Internet Control Messaging Protocol) koja se aktivira opcijom `-I`. U Windowsu, međutim, podrazumevano se šalje ICMP paket sa zahtevom za eho (engl. *echo request packet*). Prema tome, dužina vaše putanje može da varira, u zavisnosti od toga da li lokacija blokira protokol UDP ili protokol ICMP. Druga zanimljiva opcija programa traceroute aktivira se parametrom `-g`. Njome se korisniku omogućava da zada približno usmeravanje sa izvora. Dakle, ako mislite da će mrežni prolaz ciljnog računara prihvatiti pakete koji su usmereni već na izvoru (što je smrtni greh), pokušajte da aktivirate ovu opciju uz odgovarajuće pokazivače na skokove (više detalja o tome dobićete ako u UNIX-u zadate komandu `man traceroute`).

Treba da objasnimo još nekoliko opcija koje će vam možda pomoći da zaobiđete mehanizme za kontrolu pristupa dok pokušavate da snimite sistem. Opcija `-p` *n* programa traceroute omogućava da zadate početni broj UDP priključka (*n*) koji će se povećati za jedinicu nakon što pošaljete probni paket. Dakle, nećemo moći da koristimo fiksne brojeve priključaka ukoliko ne podesimo program traceroute. Srećom, Michael Schiffman je napravio zakrpu (http://www.packetfactory.net/

Projects/firewalk/traceroute.diff) za verziju 1.4a5 programa traceroute (ftp://ftp.cerias.purdue.edu/pub/tools/unix/netutils/traceroute/old) kojom se dodaje parametar `-S` da bi se sprečilo uvećavanje broja priključka. Kada je primenite, svaki paket koji pošaljete imaće fiksni broj priključka i možete da se nadate da će mehanizam za kontrolu pristupa takve pakete propuštati. Dobra polazna tačka je UDP priključak 53 (služi za DNS upite). Pošto mnoge lokacije dozvoljavaju ulazne pakete koji pretražuju DNS server, velike su šanse da će mehanizam za kontrolu pristupa propustiti naš sondažni paket.

```
[bash]$ traceroute 10.10.10.2
traceroute to (10.10.10.2), 30 hops max, 40 byte packets
 1 gate (192.168.10.1) 11.993 ms 10.217 ms 9.023 ms
 2 rtr1.bigisp.net (10.10.12.13) 37.442 ms 35.183 ms 38.202  ms
 3 rtr2.bigisp.net (10.10.12.14) 73.945 ms 36.336 ms 40.146 ms
 4 hssitrt.bigisp.net (10.11.31.14) 54.094 ms 66.162 ms 50.873 ms
 5 * * *
 6 * * *
```

U ovom primeru vidimo da je naše sondiranje programom traceroute (koji standardno šalje UDP pakete) blokirano zaštitnom barijerom.

Pošaljimo sada sondu s fiksiranim priključkom UDP 53, što izgleda kao DNS upit:

```
[bash]$ traceroute -S -p53 10.10.10.2
traceroute to (10.10.10.2), 30 hops max, 40 byte packets
1  gate (192.168.10.1) 10.029 ms 10.027 ms 8.494 ms
2  rtr1.bigisp.net (10.10.12.13) 36.673 ms 39.141 ms  7.872 ms
3  rtr2.bigisp.net (10.10.12.14) 36.739 ms 39.516 ms 37.226 ms
4  hssitrt.bigisp.net (10.11.31.14) 47.352 ms 47.363 ms 45.914 ms
5  10.10.10.2 (10.10.10.2) 50.449 ms 56.213 ms 65.627 ms
```

Pošto uređaj za kontrolu pristupa (4. skok) sada paketima ne može da nađe manu, on ih propušta. Prema tome, sistem iza uređaja za kontrolu pristupa možemo da ispitamo samo tako što ćemo poslati pakete s odredišnim priključkom UDP 53. Ukoliko sondirate sistem sa aktivnim UDP priključkom 53, nećete primiti uobičajenu povratnu ICMP poruku o nedostupnosti, pa nećete videti ni informaciju o računaru kada paket stigne na odredište.

Sve što smo dosad radili s programom traceroute uglavnom je bilo s komandne linije. Oni koji više vole grafičko okruženje, za otkrivanje putanja mogu da koriste VisualRoute (http://www.visualroute.com), NeoTrace (http://www.neotrace.com/) ili Trout (http://www.foundstone.com). Programi VisualRoute i NeoTrace grafički prikazuju svaki mrežni skok i spajaju ga s rezultatima WHOIS pretraživanja. Trout se izvršava višenitno, pa je jedan od najbržih uslužnih traceroute programa. VisualRoute deluje privlačno, ali ne radi dobro s velikim mrežama.

Imajte u vidu da se TTL vrednost upotrebljavana za ustanovljavanje putanja nalazi u IP zaglavlju, pa nismo ograničeni na UDP i ICMP pakete. Može se poslati doslovno bilo koji IP paket, čime dobijamo alternativne tehnike za otkrivanje putanja. Te tehnike omogućavaju prolazak naših paketa kroz zaštitne barijere koje blokiraju UDP i ICMP pakete. Dve alatke koje za otkrivanje putanja šalju TCP pa-

kete na određeni priključak prikladno su nazvane tcptraceroute (http://michael.toren.net/code/ tcptraceroute) i Cain & Abel (http://www.oxid.it). Postoje i dodatne tehnike pomoću kojih možete doći do važećih ACL lista određenih uređaja za kontrolu pristupa. Skeniranje protokola zaštitne barijere (engl. *firewall protocol scanning*) jedna je od takvih tehnika, kao i alatka firewalk; obe ćemo objasniti u poglavlju 11.

Protivmera: onemogućavanje pokušaja upoznavanja mreže

U ovom poglavlju dotakli smo se samo tehnika koje se koriste za upoznavanje mreže. U sledećim poglavljima obradićemo mnogo radikalnije tehnike. Međutim, postoji nekoliko mera koje možemo preduzeti da bismo prepoznali pokušaj ulaska opisanih sondi u sistem i sprečili ga. Mnogi komercijalni sistemi za otkrivanje upada (engl. *network intrusion detection system*, NIDS) i sistemi za sprečavanje upada (engl. *intrusion prevention system*, IPS), uspeće da uhvate ovu vrstu pokušaja upoznavanja mreže. Takvu aktivnost može da otkrije i jedan od najboljih besplatnih NIDS programa, Snort (http://www.snort.org) autora Martyja Roescha. Ako ste voljni da krenete u ofanzivu kada primetite da vas neko snima, pomoći će vam program RotoRouter koji je razvio Humble iz grupe Rhino9 (http://www.ussrback.com/UNIX/loggers/rr.c.gz). Taj uslužni program beleži pristigle zahteve programa traceroute i generiše lažne odgovore na njih. I najzad, u zavisnosti od načina rada vašeg sistema obezbeđenja, možda ćete mrežne usmerivače na obodu moći tako da podesite da saobraćaj ICMP i UDP paketa ograniče na određene sisteme, pa ćete smanjiti svoju izloženost spoljnom neprijatelju.

SAŽETAK

Kao što ste videli, napadači mogu da upoznaju i snime vašu mrežu na mnogo načina. Namerno smo ovu raspravu ograničili na uobičajene alatke i tehnike, ali imajte na umu da se svakoga dana razvijaju nove alatke. Pri objašnjavanju snimanja sistema koristili smo sasvim jednostavan primer. Često ćete se suočiti s herkulovskim zadatkom da identifikujete i snimite desetine i stotine domena. Zbog toga, kad god se to može, treba automatizovati aktivnosti, kombinujući skriptove komandnog okruženja i program expect, odnosno programe pisane na jeziku Perl. Mnogi napadači s bogatim iskustvom u prepoznavanju mreža i dobro opremljeni – nisu otkriveni. Prema tome, uvek nastojte da smanjite količinu i vrstu informacija koje cure zbog vašeg prisustva na Internetu i pomno nadgledajte saobraćaj usmeren ka vašem sistemu.