Hakerske tajne: zaštita mrežnih sistema

ranjiv 1. Podložan fizičkom ili emocionalnom povređivanju. 2. Podložan napadu: "Ranjavaju nas i voda i zemlja, bez flote ili armije." (Alexander Hamilton) 3. Koji se može napadati ili kritikovati. 4. Povodljiv, podložan ubeđivanju ili iskušenju.

Bilo da ste toga svesni li ne, kada se od kuće ili s posla povežete na Internet, veoma ste ranjivi. U stvari, kada se povežete na Internet, postajete (voljno ili prisilno) član zajednice korisnika jednog ogromnog sistema - sistema koji prevazilazi značaj pojedinca i u kome vreme i prostor gotovo ništa ne znače. Povezanost Interneta dovodi sve učesnike u blizak kontakt. Vaš prvi sused tako može biti zlonamerni haker iz neke daleke zemlje ili nadareni klinac iz komšiluka koji pretražuje vaš sistem iz čiste radoznalosti.

Kao i u svakoj drugoj zajednici, ni ovde nisu svi njeni članovi ugledni. Više ne možete da otvorite novine a da vas svakodnevno ne zasipaju skandalima ili aferama iz inače mirnog dela društva. Isto je i u kibernetskoj zajednici na Internetu. U širom sveta povezanoj mreži, gde je gas uvek "do daske", događaji iz "crne hronike" smenjuju se velikom brzinom. Najtužnije je to što se u mrežnoj zajednici nalaze i veoma bistre osobe koje svoj izuzetan talenat i slobodno vreme radije koriste za činjenje zla nego za dobrobit drugih.

Ne treba da istražujete istoriju Interneta da biste uočili neverovatan "napredak" u zloupotrebi računara. Verujem, u stvari, da brzina kojom se ranjive tačke otkrivaju i zloupotrebljavaju daleko prevazilazi brzinu rasta snage računara prema Murovom zakonu. Možda bi i korisnici Interneta koji brinu o bezbednosti sistema trebalo da formulišu sopstveni zakon: "Napadači na Internetu odmah će otkriti i zloupotrebiti svaku ranjivu tačku. Što je ciljni sistem primamljiviji, napad će se brže dogoditi." Nažalost, korisnici Interneta uglavnom ne misle da su upravo oni zanimljivi ciljevi, što nije tačno. U to može da se uveri svako ko na kućnom računaru instalira zaštitnu barijeru. Mnogo ću lakše izbrojati zemlje iz kojih ne pokušavaju da se povežu s mojim računarom nego one iz kojih to čine. Svakoga dana, barem desetak osoba pokušava da uspostavi komunikaciju s mojim računarom, služeći se nekom dobro poznatom trojanskom aplikacijom i sličnim softverom. Zašto ti ljudi, dan za danom, pokušavaju da upadnu u moj sistem? Odgovor je jednostavan - zato što često uspevaju da prona?u ranjiv računar koji će zatim zloupotrebiti.

Hakerisanjem i zloupotrebom tuđih sistema nekada se bavio relativno mali broj dobro potkovanih stručnjaka. Danas, me?utim, postoje alatke tipa "pokaži i pritisni", "učitaj i pokreni", "prevedi i izvrši", koje u rukama zlonamernika postaju ubojito oružje. Nije proteklo mnogo vremena od trenutka kada smo shvatili da su skeniranje signalom ping i SYN poplave osnovne metode za uskraćivanje usluga. Ubrzo je uskraćivanje usluga napredovalo toliko da je napad počeo da se izvodi distribuirano, posredstvom "nedužnih" UNIX računara. Ova tehnika je smesta preneta na drugu platformu, koja se mogla još lakše zloupotrebiti - na Windows, u kom rade hiljade korisnika povezanih kablovski ili preko digitalne pretplatničke linije (DSL). Dobar primer ubrzanog razvoja zloupotrebe jeste tehnologija programskog "crva", pomoću koje se trojanski programi rasprostiru mrežom bez posredovanja korisnika. Od kraja 2000. do sredine 2001, suočili smo se sa crvima Bymer, Linux Ramen, Lion, SADMIND, Leave i Code Red. Crv Code Red verovatno je dosad naneo najveću štetu - procenjuje se da direktna šteta, uvećana za troškove čišćenja sistemâ, prelazi nekoliko milijardi dolara. Ovakvo "hakerisanje pomoću automatskog pilota" višestruko uvećava moć napadača i istovremeno mu štedi vreme, pa su šanse za uspeh napada mnogo veće. Bez obzira na različite tehnike kojima se služe današnji virusi, svima je zajedničko sledeće: ako obezbedite ranjive tačke koje oni zloupotrebljavaju, neće moći da vam nanesu nikakvu štetu. U ovoj knjizi opisane su te ranjive tačke i predložene mere pomoću kojih možete da ih zaštitite.

Bezbednost kao tržišni pokazatelj

U industriji je konkurencija velika i bezbednost se više ne smatra samo garancijom za pravilno obavljanje usluga već postaje i tržišni pokazatelj. Vremenom će objavljeni slučajevi narušavanja bezbednosti početi značajno da utiču na kretanje berzanskih akcija i uskomešaće korporacijske službe za odnose s javnošću. Situacija je jasna: opasnost od napada s Interneta biće sve veća, ali će i pored toga kompanije sve više transakcija pokušavati da obave preko Interneta. Prkoseći riziku, kompanije će biti sve vidljivije na Internetu. Zašto je to tako? Zato što je Internet prepun pogodnosti koje su za njih životno značajne. Zbog svega toga, kompanije moraju biti na oprezu, uvek spremne da se suoče s pažnjom koju će im posvetiti zlonamerni pojedinci. Iako postoje brojni rizici kada poslujete preko Interneta, verovatno je najgore ako izgubite ugled. Narušavanje ugleda iz bezbednosnih razloga najbrži je način da izgubite poverenje potrošača i poslovnih partnera. Ako zbog narušavanja bezbednosti u javnost procure poverljive informacije, bilo vaše bilo vaših klijenata, vaš posao može katastrofalno da se završi. Nijedna poslovna aktivnost to ne može da izbegne.

Č;ak i na mrežama kompanija koje pomno vode računa o bezbednosti postoje ranjive tačke i zbog toga kompanije neprestano moraju da budu na oprezu kako bi smanjile rizik od napada. Prvi korak je sticanje znanja, a sa znanjem dolazi i prilika da se sazri i odraste. Knjiga u vašim rukama jedna je od najmoćnijih alatki koja će vam pomoći da uvećate svoje znanje iz oblasti bezbednosti. Čitajte je, prelistavajte, koristite. Veoma cenim autore ove knjige, jer od njih godinama tražim i dobijam odlične savete. Hakerske tajne je svojevrsna Biblija o ranjivim tačkama sistema i merama za njihovu zaštitu. Nadam se da će informacije koje u njoj nađete pomoći da bolje obezbedite svoju kompaniju. U budućnosti će najbolji ugled na tržištu imati kompanije koje investiraju u vredne i nadarene saradnike, elastične tehnologije koje se lako prilagođavaju novim bezbednosnim rizicima i u procese koji doprinose neprekidnom poboljšavanju sistema. Kompanije koje to ne prihvate verovatno će se naći na prvim stranama dnevnih listova - i to ne radi pohvale.

Pete Murphy

Uprava za zaštitu sistema

Bank of America

4.8.2001.

Peter F. Murphy je potpredsednik za bezbednost Uprave za zaštitu sistema banke Bank of America. Uprava ima tim za odgovaranje na upade u računarske sisteme, a u njene aktivnosti spadaju i otkrivanje upada, utvr?ivanje ranjivosti, obrada napada, krivična istraga i održavanje regionalnih centara za oporavljanje sistema. Poseban tim je zadužen za planiranje i testiranje nepredviđenih situacija u računarskoj mreži.

Pete već sedamnaest godina radi na razvoju sistema, preispitivanju tehnologija i obezbeđivanju podataka za potrebe banaka i finansijskih institucija. On je član udruženja za proveru bezbednosti i kontrolu informacija (engl. Information Systems Audit and Control Association). Ima diplomu nadzornika za informacione sisteme, saraðuje u radnoj grupi za otkrivanje ranjivosti sistema, delu Komisije za zaštitu važnih infrastruktura (engl. Commission on Critical Infrastructure Protection) predsednika SAD, i saraðuje u grupi za razmenu bezbednosnih informacija u mreži (engl. Network

Security Information Exchange, NSIE) kao delu predsednikovog Saveta za bezbednost nacionalnih komunikacija (engl. National Security Telecommunications Advisory Council, NSTAC).

Hakerske tajne: zaštita mrežnih sistema

O autorima

Stuart McClure

Stuart McClure, jedan od koautora nedavno objavljene knjige Hacking Exposed Windows 2000, u ovo, treće izdanje knjige Hakerske tajne: zaštita mrežnih sistema unosi deceniju svog iskustva u oblasti informacionih tehnologija i bezbednosti. Skoro tri godine Stuart je saraðivao u nedeljnoj rubrici Security Watch (http://www.infoworld.com/security) mrežnog časopisa InfoWorld, posvećenog prioritetnim problemima obezbeðenja, napadima na sisteme i njihovim ranjivim tačkama.

Pre nego što je sa saradnicima osnovao Foundstone, Stuart je u kompaniji Ernst & Young bio viši rukovodilac u grupi za ispitivanje sistema bezbednosti koja se bavila upravljanjem projektima, utvrð ivanjem anatomije napada i upada u sisteme i proverom tehnologije. Stuart je prethodno bio analitičar bezbednosti u Centru za testiranje časopisa InfoWorld, gde je proverio gotovo što mreža i bezbednosnih programa, a specijalizovao se za zaštitne barijere, programe za nadziranje bezbednosti i za otkrivanje upada u sisteme i infrastrukturu javnog ključa (PKI). Pre nego što je došao u InfoWorld, Stuart je kao stručnjak za mreže, sisteme i bezbednost radio za mnoge organizacije koje se bave informacionim tehnologijama i održavao različite platforme (Novell, NT, Solaris, AIX, AS/400).

Stuart je diplomirao na Univerzitetu države Kolorado u Bulderu, a stekao je i brojne druge diplome, uključujući CISSP organizacije ISC2, CNE od Novella i CCSE od Check Pointa.

Joel Scambray

Joel Scambray, koautor knjige Hacking Exposed Windows 2000, doprineo je da izdanja iz serije Hakerske tajne postanu bestseleri. Joel piše na osnovu dugogodišnjeg iskustva savetnika za bezbednost. Tokom godina, on je sakupio i u praksi proverio obilje bezbednosnih tehnologija, a projektovao je i analizirao bezbednosnu arhitekturu najrazličitijih aplikacija i proizvoda. Joel drži predavanja o bezbednosti Windowsa 2000 u mnogim organizacijama, pa i u Institutu za računarsku bezbednost (CSI), Institutu za obuku MIS-a, organizacijama SANS, ISSA, ISACA i u velikim korporacijama, a u Foundstoneu vodi kurs o vrhunskom hakerisanju Windowsa. On je direktor firme Foundstone, Inc. (http://www.foundstone.com), a prethodno je bio jedan od rukovodilaca kompanije Ernst & Young, glavni analitičar InfoWorldovog Centra za testiranje i direktor sektora za informacione tehnologije velike agencije za promet nekretnina. Joel je završio postdiplomske kurseve na Kalifornijskom univerzitetu (UCLA) u Dejvisu i Los An?elesu, a ima i diplomu stručnjaka za bezbednost informacionih sistema (CISSP).

George Kurtz

George Kurtz je izvršni direktor Foundstonea (http://www.foundstone.com), kompanije koja nudi najsavremenija rešenja za obezbeðivanje računarskih sistema. G. Kurtz je með unarodno priznat stručnjak za bezbednost i u svojoj uspešnoj karijeri proverio je na stotine zaštitnih barijera, mreža i lokacija za elektronsku trgovinu. On ima veliko

iskustvo u otkrivanju upada i radu s zaštitnim barijerama, postupcima odbrane od napada i rešenjima za daljinski pristup. Kao izvršni direktor i suosnivač Foundstonea, George objedinjuje izuzetnu poslovnu pronicljivost i poznavanje tehničkih aspekata bezbednosti. Te njegove osobine oblikuju strategiju Foundstonea, ali istovremeno pomažu klijentima da shvate kako (ne) obezbeđivanje sistema može da utiče na njihove poslove. Preduzetni Georgeov duh doveo je Foundstone u sam vrh organizacija koje nude "čista" rešenja za probleme bezbednosti. On je koautor nedavno objavljene knjige Hacking Linux Exposed, a redovno učestvuje na skupovima posvećenim bezbednosti i često je citiran (The Wall Street Journal, InfoWorld, USA Today, Associated Press). On je, tako?e, nezaobilazan sagovornik u razgovorima o incidentima iz oblasti bezbednosti, naročito na televiziji (CNN, CNBC, NBC, FOX i ABC).

Saradnici

Christopher Abad, inženjer za istraživanje i razvoj u Foundstoneu, studira matematiku na Kalifornijskom univerzitetu, a ima veliko iskustvo u kriptografiji, obezbeđivanju mreža i programiranju. Dao je značajne doprinose na polju bezbednosti, a posebno je zapaženo njegovo pionirsko istraživanje koncepta pasivnog mapiranja mreže, o čemu je održao niz prezentacija na mnogim skupovima posvećenim bezbednosti.

Stephan Barnes je pomoćnik direktora prodaje u Foundstoneu. Stephan je prethodno radio kao viši rukovodilac za bezbednost elektronske trgovine kompanije Ernst & Young, a pre toga je bio rukovodilac grupe za obezbeđivanje računarskih sistema Arthura Andersena. Pored iskustva koje je stekao na obezbeđivanju Interneta i elektronske trgovine, Stephan se tokom deset godina rada specijalizovao za daljinske napade pomoću programa za automatsko pozivanje i za sisteme modemskog prijavljivanja i govorne pošte - tehnika neophodnih pri proveravanju spoljnog bezbednosnog profila bilo kojeg savremenog preduzeća. Stephanove ekspertize obuhvataju proveru bezbednosti firmi iz oblasti finansija, telekomunikacija, osiguranja, proizvodnje, distribucije, javnih službi i visoke tehnologije. On je učesnik mnogih skupova posvećenih bezbednosti i predavač u brojnim srodnim organizacijama. Stephan je već 20 godina poznat pod pseudonimom M4phr1k. Njegova Web strana nalazi se na adresi http://www.m4phr1k.com.

Marshall Beddoe je inženjer za istraživanje i razvoj u firmi Foundstone. Istraživao je pasivno mapiranje mreža, otkrivanje daljinskih napada, operativni sistem FreeBSD i nove tehnike napada, u saradnji s više neprofitnih grupa za bezbednost. Marshall je za Vojsku SAD i za nekoliko velikih kompanija osmislio i održao kurseve o naprednim tehnikama upada u sisteme.

Erik Pace Birkholz (CISSP, MSCE) glavni je savetnik Foundstonea, specijalizovao se za testiranje napada i upada u sisteme, kao i za projektovanje bezbednosne arhitekture. Erik drži poznate Foundstoneove kurseve: "Ultimate Hacking: Hands On" i "Ultimate NT/2000 Security: Hands On". Pre Foundstonea je, kao rukovodilac tima za proveru, radio za West Coast Consulting Group u okviru firme Internet Security System (ISS). Prethodno je radio kod Ernsta & Younga, u njihovoj službi za usluge u elektronskoj trgovini. Bio je i član National Attack and Penetration team i instruktor na kursu "Extreme Hacking". Erik je dve godine radio i kao istraživač analitičar Nacionalnog udruženja za bezbednost računara (NSCA). On je predavao na konferenciji Black Hat i na Konferenciji za bezbednost Interneta (TISC). Objavljivao je članke u časopisima The Journal of the National Computer Security Association i Foundstoneovom Digital Battlefield. Erik je sarađivao u pisanju knjige Hacking Exposed Windows 2000 i drugog izdanja knjige Hakerske tajne: zaštita mrežnih sistema.

Yen-Ming Chen (CISSP, MCSE) glavni je izvršni savetnik Foundstonea i rukovodilac savetovališta za bezbednost. Yen-Ming ima četvorogodišnje iskustvo u administriranju UNIX i Internet servera. On veoma dobro poznaje i oblasti bežičnog umrežavanja, kriptografije, otkrivanja upada i oporavka sistema. Č;lanke je objavljivao u časopisima SysAdmin, UnixReview i sličnim tehničkim

publikacijama. Pre Foundstonea, Yen-Ming je radio u Centru za kibernetsku bezbednost (CMRI, CMU), na sistemu za otkrivanje upada zasnovanom na korišćenju programskog agenta. Aktivno je saraðivao i na razvoju sistema za otkrivanje upada u mreže, snort. Yen-Ming je diplomirao matematiku na Nacionalnom univerzitetu na Tajvanu, a magistrirao na Odseku za informacione umrežene sisteme na univerzitetu Carnegie Mellon.

Clinton Mugge (CISSP), tako?e jedan od glavnih savetnika Foundstonea koji radi u konsultantskoj službi za bezbednost klijenata, specijalizovao se za proveru bezbednosti mreža, testiranje proizvoda i arhitekture sistema bezbednosti. On ima sedmogodišnje iskustvo u obezbeðivanju (uključujući i fizičko obezbeðivanje računara) arhitekture mreža i ispitivanju slučajeva špijunaže. Saraðivao je s vladinim agencijama i korporacijama koje se bave informacionim tehnologijama, na pripremi odgovora na napade i proveravanju bezbednosti mreža. Pre nego što je došao u Foundstone, i on je radio za Ernsta & Younga, a još pre toga bio je kontraobaveštajni agent u vojsci SAD. G. Mugge učestvuje na stručnim skupovima, piše za rubrike u časopisima i tehnički je recenzent knjige Incident Response (Osborne/McGraw-Hill, 2001). On je magistar menadžmenta, a diplomirao je marketing. Njegova elektronska adresa je clinton.mugge@foundstone.com.

David Wong je stručnjak za bezbednost računara i jedan je od savetnika u Foundstoneu. On je testirao mnoge alatke za obezbeðivanje računara, kao i za simuliranje napada, odnosno otkrivanje upada u sisteme. David je prethodno bio softverski inženjer u velikoj telekomunikacionoj kompaniji, gde je usavršavao programe za ispitivanje i nadgledanje mreža.

Melanie Woodruff (MCSE) savetnik je za bezbednost u Foundstoneu i specijalizovala se za procenjivanje napada iz perspektive Interneta, intraneta i modemskog pristupanja. Gða Woodruff ima bogato iskustvo u pružanju konsultantskih usluga iz oblasti bezbednosti klijentima iz finansijskih, upravnih i trgovinskih organizacija. Pre nego što je došla u Foundstone, bila je savetnik za informatičku bezbednost konsultantske firme Big Five. Gða Woodruff je diplomirala na Odseku za informacione sisteme i upravljanje na Univerzitetu Sinsinati u Ohaju.

Tehnički saradnici

Tom Lee (MCSE) rukovodi sektorom za informacione tehnologije u Foundstoneu. On se trudi da Foundstoneov sistem održi u radnom stanju, da ga sačuva od uljeza i - što je mnogo izazovnije - od zaposlenih. Tom ima desetogodišnje iskustvo u administriranju sistema i mreža, i radio je na obezbeð ivanju najrazličitijih sistema, od Novella i Windowsa NT/2000 do Solarisa, Linuxa i BSD-a. Pre dolaska u Foundstone, bio je rukovodilac za informacione tehnologije na Kalifornijskom univerzitetu u Riversajdu.

Eric Schultze se bavio informacionim tehnologijama i bezbednošću poslednjih devet godina, uglavnom proveravajući i obezbeðujući Microsoftove tehnologije i platforme. On aktivno učestvuje na skupovima posvećenim bezbednosti (NetWorld+Interop, Usenix, BlackHat, SANS, MIS) i povremeno predaje u Institutu za računarsku bezbednost. G. Schultze je o stručnim temama govorio i na televiziji (NBC, CNBC) i pisao u mnogim publikacijama (TIME, ComputerWorld i The Standard). Ericovi prethodni poslodavci bili su Foundstone, SecurityFocus.com, Ernst & Young, Price Waterhouse, Bealls i Salomon Brothers. On je bio saradnik na prvom izdanju knjige Hakerske tajne, a sada je rukovodilac za bezbednost u korporaciji Microsoft.

Hakerske tajne: zaštita mrežnih sistema

Neznanje je neprijatelj

"Posmatraj neprijatelja jer će on prvi otkriti tvoje greške."

Antisten, atinski filozof, 440. p.n.e.

Odvajkada smo se oslanjali na znanja i iskustva naših starijih; njihovo usmeravanje i vođenje sačuvali su nas od nebrojenih nesreća koje su pretile da nas unište. Međutim, u današnjem vanzemaljskom svetu računarske bezbednosti koji se neprestano menja, malo je sedih mudraca u korporacijama. Digitalni ratnici današnjice nemaju čak ni približnu putnu mapu obezbeđenja, a kamoli utvr?enu strategiju kojom bi se suprotstavili tajnovitom neprijatelju.

Ako želite da poboljšate svoju bezbednost i da pobedite neprijatelja, morate ga poznavati, s njim se družiti i od njega učiti. Hakeri su isuviše vešti i uporni da bismo ih olako shvatali. Oni se, po samoj svojoj prirodi, neprekidno usavršavaju i pronalaze nove tehnike, i često kao duhovi neprimetno promaknu kibernetskim pejzažem. Slično virusu, oni se stalno preobražavaju i prilagođavaju, tako da ih je izuzetno teško pratiti.

Današnji svet liči na haotično digitalno bojno polje. Tehnologija i računari svakoga trena zaposedaju nova područja našeg svakodnevnog života, nudeći nam jednostavnije i efikasnije življenje, a pri tome skrivaju mračnu tajnu koja ugrožava njihovu egzistenciju. Æice kojima se kreću milijarde elektrona na Internetu čuvaju ogromnu tajnu, koju smo tek nazreli i počeli da izvlačimo na svetlost dana: svet zlonamernih hakera. Ako budete čitali knjige kao što je Hakerske tajne, posmatrali hakere i učili od njih, počećete da razumevate njihove napade, kako rade, šta rade i zbog čega to rade. Takva saznanja su i najjače oružje profesionalaca iz domena bezbednosti koji se spremaju da im se suprotstave.

Oslobodite se iluzija

Hakeri mogu da pronađu vaš računar na Internetu za pola sata. Svakoga trenutka, celog božjeg dana, zli hakeri lutaju digitalnim predelima u potrazi za slabim i lakim plenom. Potencijalnih žrtava je mnogo, jer malo ko razume probleme bezbednosti, a još manje je onih koji umeju da smanje rizik od napada. Jeste li znali da se svake godine obelodani preko 800 propusta u računarskim sistemima? Koliko takvih slabih mesta vi znate?

O tom mračnom podzemnom svetu malo se zna, a donedavno gotovo da i nije bilo potkovanih stručnjaka koji bi mogli da razmatraju taktike hakera na javnom forumu kao što je ovaj. Na tradicionalnom bojnom polju, neprijatelja možete da vidite i dodirnete, neprijatelja koji se vlada po pravilima rata i razuma - kvaliteti koji su nepoznati u današnjoj kibernetskoj anarhiji. Kao profesionalci za bezbednost, treba da ocenimo opseg napada, da pomognemo kompanijama da se oporave od njega i da sprovedemo konkretne mere za odbranu računarskih sistema. Ali, kako ćemo se odbraniti ako ne upoznamo neprijatelja?

Naredna poglavlja nisu prazne priče koje su izmislili studenti Fakulteta dramskih umetnosti. To su istinske tehnike i priče sa stvarnog digitalnog ratišta na kome se nalazimo. Neprijatelj je pred vratima, vidljiv samo malom broju stručnjaka za bezbednost. Unutar korica ove knjige sakupljeni su saveti tih stručnjaka. Morate saznati način razmišljanja i motivacije neprijatelja, naučiti njegove tehnike i, najvažnije od svega, shvatiti kako da ga pobedite.

Šta je novo u trećem izdanju ove knjige

Digitalni svet se menja brže nego i sama misao. Izgleda kao da svakoga sata isplivavaju na površinu nove hakerske alatke, tehnike i metode. Prikupiti ih, obavestiti svet o njima, prevesti ih na razumljiv jezik - pravi je izazov. Kao u prethodnim izdanjima, i u ovom smo dali sve od sebe da biste dobili najsvežije tehnološke i tehničke novosti.

Obilje novog sadržaja

Nabrojaćemo samo neke od novih tema koje su uvršćene u treće izdanje:

Novi napadi na bežične mreže 802.11.

1. Analiza crva Code Red.
2. Novi napadi na Windows, naročito na Windows 2000 i Windows XP/.NET Server.
3. Ažurirane hakerske metodologije za elektronsku trgovinu.
4. Razrada novih alatki i trikova za distribuiran napad radi odbijanja vršenja usluga (distributed denial of service, DDoS).
5. Nova ranjiva tačka na znakovnom nizu za formatiranje, otkrivena u Windowsu i UNIX-u, koja preti da će preuzeti neslavni primat od napada prelivanjem bafera.
6. Novootkriveni slučajevi upada na početku svakog dela knjige.
7. Ažuriran opis napada na bezbednost sistema Windows 9x, Millennium Edition (ME), Windows NT/2000/XP/.NET Server, UNIX, Linux, NetWare i desetinu drugih platformi, zajedno s odgovarajućim merama zaštite.
8. Revidirano i obnovljeno poglavlje o napadima iz daljine, s novim saznanjima o PBX hakerisanju i hakerisanju preko sistema govornih poruka, kao i ažuriran VPN odeljak.
9. Prateća Web lokacija http://www.hackingexposed.com s vezama ka svim alatkama i izvorima na Internetu koji se pominju u knjizi.
10. Kompakt disk s odabranim alatkama za sprovo?enje vrhunske bezbednosti koje čekaju da ih instalirate, vezama ka Web lokacijama na kojima možete da na?ðte najnovije verzije alatki za uspostavljanje bezbednosti koje se pominju u knjizi, i bazom podataka s podrazumevanim lozinkama koja sadrži uobičajeno korišćene lozinke.

Olakšano snalaženje u knjizi, poboljšane slike, procenjivanje rizika

Uz nesebičnu pomoć našeg izdavača, kompanije Osborne/McGraw-Hill, i treće izdanje Hakerskih tajni objavili smo u poznatom formatu:

Tehnika svakog napada istaknuta je odgovarajućom sličicom na margini:

Ova sličica označava napad

Kada je vidite, znajte da tu opisujemo alatku ili metodologiju za prodiranje u sistem.

- Svakom napadu može se parirati sprovođenjem praktičnih, primerenih i isprobanih mera koje su takođe označene posebnom sličicom:

Ova sličica označava mere zaštite

Ona stoji pored saveta kako da rešite problem.

- Odlučili smo da oznakama:

NAPOMENA

SAVET

UPOZORENJE

- obeležimo delove teksta koji skreću pažnju na detalje koje često previđamo.
- Temeljno smo prečistili i sav kôd koji se nalazi u listinzima, na snimcima ekrana i u dijagramima, i pri tome smo vodili računa da u listinzima polucrnim slovima istaknemo ono što unosi korisnik.
- Uz svaku vrstu napada naveden je i stepen rizika, zasnovan na procenjivanju tri komponente i združenom iskustvu autora knjige:

Popularnost:	Učestalost korišćenja u lovu na žive mete, pri čemu 1 označava najre?u a 10 najširu primenu.
Jednostavnost:	Veština potrebna za izvo?enje napada, pri čemu 1 označava iskusnog programera sistema bezbednosti, a 10 korisnika s malo ili nimalo iskustva.
Uticaj:	Potencijalna šteta prouzrokovana uspešnim izvo?enjem napada, pri čemu 1 označava otkrivanje nevažnih informacija o cilju, a 10 preuzimanje naloga administratora sistema ili ekvivalentnu štetu.
Stepen rizika:	Dobija se kao prosek vrednosti tri navedene komponente.

Poruka čitaocima

Potrudili smo se da vam prenesemo pravovremene, tačne i izuzetno korisne informacije o hakerskim tehnikama i alatkama, i da vas istovremeno naoružamo znanjem za odbranu od hakera. Nadamo se da ćete u ovoj knjizi naći i nešto vrednije od trikova i igračaka - na primer, da ćete razumeti potrebu da obezbeđujete svoje vredne informacije, jer svetom haraju mnogi zlonamernici. Srećan rad!

Hakerske tajne: zaštita mrežnih sistema

Slučaj iz prakse: odavanje tajni

Uzbueni ste jer je vaš blistavi server s najnovijim i najboljim hardverom upravo stigao iz prodavnice, tako nalickan da samo što ne progovori. Pre nego što ste ga i naručili, od prodavca ste kapriciozno zahtevali da na njega instalira Windows 2000. Osim toga, naglasili ste mu da server napuni svim mogućim aplikacijama za elektronsku trgovinu. "Baš je to zgodno", mislite, "mogu da naručim šta god hoću i da server postavim u našem računskom centru, a pri tome ne moram ništa da konfigurišem." Život je zaista lep.

Računski centar dobija nov server i sledi vaše uputstvo da zameni zastareli NT server novim. Vi ih zdušno uveravate kako je prodavac hardvera brižljivo konfigurisao sistem, zadajući čak i IP adresu. Zamena računara prolazi bez teškoća. Razmišljate kako ovo prilago?avanje sistema po narudžbini podiže tehnologiju "utakni i koristi" na viši nivo. Nažalost, takav postupak podiže i hakerisanje na viši nivo.

Vaš superserver je, u stvari, pravo sito kroz koje cure informacije - kao da čekaju da ih pokupi neki haker koji se tu slučajno zadesi. Ako su priključci 139 i 445 širom otvoreni, to će biti dovoljno i hakeru početniku. Kratka anonimna veza s vašim serverom otkriće mu obilje informacija iz kojih može da utvrdi koji korisnici imaju administratorska ovlašćenja, kada se poslednji korisnik prijavio na sistem, gde su skriveni deljeni podaci, kada je poslednji put menjana lozinka, kao i to da li je za prijavljivanje uopšte potrebna lozinka. Sve ove informacije može da prikupi - ili kako mi to kažemo, popiše - preko anonimne sesije i nekoliko otvorenih priključaka koje će otkriti opipavanjem vašeg okruženja. Skeniranje i popisivanje (engl. *enumerating*) dve su osnovne tehnike koje će većina hakera upotrebiti da bi ustanovili jesu li vaši sistemi ranjivi. Kada odate ove podatke, gotovi ste!

Prema našem iskustvu, ovakav scenario je više nego realan i odlučni hakeri mu posvećuju najviše vremena. Što više obaveštenja napadač prikupi, veće su mu šanse da prodre kroz obezbeđenje. Iako mediji obožavaju senzacionalističke izveštaje o osvajanju sistema "pritiskom na dugme", vešt i motivisan napadač će možda mesecima opipavati i popisivati ciljno okruženje pre nego što ga stvarno napadne. Mnogi korisnici ovakvu situaciju dodatno pogoršavaju jer naivno veruju da će prodavac računara dovoljno obezbediti sistem. Č;ast pojedinim prodavcima koji tu i tamo isključe poneku uslugu, ali većina novih sistema samo čeka da ih neko napadne. Ne uljuljkujte se iluzijom da je vaš sistem bezbedan samo zato što je fabrički konfigurisan. Takve konfiguracije su po pravilu usmerene na to da korisnik ne zatraži odmah tehničku pomoć od proizvođača, a ne da zaustave hakere.

Dobro obratite pažnju na tehnike koje opisujemo u prva tri poglavlja. Opipajte sopstveni sistem pre nego što to učine zlonamernici!

Haker mora da prođe kroz tri neophodne faze pre nego što stvarno počne da se zabavlja. U ovom poglavlju razmotrićemo prvu fazu - snimanje sistema (engl. footprinting), veštinu prikupljanja podataka o cilju. Kada lopovi odluče da opljačkaju banku, oni ne uleću bezglavo u nju zahtevajući novac (barem ne oni pametniji), nego mukotrpno 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. On mora da prikupi obilje informacija kako bi mogao

da izvede usredsređen i hirurški precizan napad (koji neće biti lako otkriven). Zbog toga će napadač sakupiti sva moguća obaveštenja o svim aspektima sistema bezbednosti računara određene organizacije. Kao rezultat "opipavanja", hakeri stvaraju jedinstven snimak (engl. footprint) ili profil prisustva žrtve na Internetu, intranetu/ekstranetu ili sistemu za daljinski pristup. Postupajući po strukturiranoj metodologiji, napadač može sistematski da izvlači podatke iz najrazličitijih izvora i da napravi snimak bilo koje organizacije.

Šta je snimanje sistema?

Metodično opipavanje neke organizacije omogućava napadačima da sastave potpun profil njenog sistema obezbeđenja. Služeći se različitim alatkama i tehnikama, napadači mogu da svedu nepoznatu veličinu (npr. priključak na Internet ciljne kompanije) na odre?enu oblast imena domena, mrežnih blokova i pojedinačnih IP adresa sistema koji su direktno povezani na Internet. 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 su nabrojana sva ova okruženja, zajedno s izuzetno važnim podacima koje napadač želi da otkrije.

Zašto je snimanje sistema neophodno?

Snimanjem sistema se sistematično 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.

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 9.

Tabela 1-1. Okruženja i kritični 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 X86)
	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)
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 X86)
	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 prstup	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

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: odre?ivanje opsega vaših aktivnosti

Najpre utvrdite opseg svojih aktivnosti tokom snimanja sistema. Želite li da opipate čitavu organizaciju ili da se ograničite na odre?ene lokacije (na čitavu korporaciju ili samo na njene ogranke, na primer)? U nekim slučajevima je vrlo teško identifikovati sve delove ciljne organizacije. Srećom, Internet obiluje mogućnostima za sužavanje opsega tih aktivnosti i istovremeno omogućava izvestan uvid u vrstu i količinu javno dostupnih informacija o izabranoj organizaciji i njenim radnicima.

Pretraživanje javnih izvora

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

Ako organizacija ima Web stranu, požite od nje. Često se na Web strani organizacije nalazi neverovatna količina informacija koje mogu da pomognu napadaču. Na Web serverima organizacija viđali smo i bezbednosne opcije za konfigurisanje njihove zaštitne barijere (engl. *firewall*). Od drugih zanimljivih stavki, tamo možete naći:

adrese

- srodne kompanije i delove preduzeća
- vesti o integrisanju ili promeni vlasnika
- telefonske brojeve
- imena i elektronske adrese za stupanje u vezu
- pravila za zaštitu privatnosti ili bezbednosna pravila iz kojih se može izvesti zaključak o

primenjenom sistemu obezbeđenja

veze ka drugim Web serverima koje koristi data organizacija.

Osim toga, u izvornom HTML kodu Web strane treba potražiti komentare. Mnoge stavke koje nisu za javno prikazivanje zakopane su u HTML oznakama za komentare, kao što su <, !, i --. 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, možete da pomoću programa tražite komentare i druge upotrebljive stavke, i time efikasnije opipate 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/teleport/home.htm) za Windows.

Pošto proučite Web strane, možete pretraživati javne izvore da biste prikupili podatke o ciljnoj organizaciji. Vesti, izjave za štampu i sličan sadržaj mogu vam dati dodatna obaveštenja o stanju organizacije i njenom bezbednosnom sistemu. Neke Web lokacije, kao što su finance.yahoo.com i http://www.companysleuth.com, sadrže obilje takvih informacija. Ako pravite profil organizacije koja se uglavnom oslanja na Internet, možda ćete, pretražujući vesti o njoj, otkriti da je imala brojne incidente s obezbeđenjem lokacije. Za ovu aktivnost biće dovoljno da upotrebite pretraživač Weba. Međutim, postoje i naprednije alatke za pretraživanje i složeniji kriterijumi pomoću kojih možete da dođete do dopunskih obaveštenja.

Mi preporučujemo paket alatki za pretraživanje FerretPRO firme FerretSoft (http://www.ferretsoft.com). WebFerretPRO omogućava istovremeno pretraživanje pomoću nekoliko pretraživača. Osim toga, druge alatke iz ovog paketa omogućavaju da pretražujete IRC, USENET, elektronsku poštu i baze podataka. Isto tako, ukoliko želite da besplatno kombinujete rezultate nekoliko pretraživača, posetite lokaciju http://www.dogpile.com.

Pretraživanje USENET poruka koje su slali korisnici ciljnog sistema često daje korisne informacije. Jednom smo videli poruku s radnog naloga administratora sistema koja se odnosila na novu lokalnu telefonsku centralu. Takvu skalameriju on do tada nije video i tražio je savet kako da isključi podrazumevane naloge i lozinke. Smučilo nam se od pomisli na "grebatore" koji su, kad su to pročitali, zadovoljno trljali ruke i pripremali se da besplatno telefoniraju preko te kompanije. Ne treba ni naglašavati da uvid u rad jedne organizacije i tehnički nivo njenog osoblja možete da steknete i ako samo čitate njihove poruke.

Na kraju, možete da se poslužite i naprednim mogućnostima pretraživača, kao što su AltaVista ili Hotbot. Preko tih sistema možete da pretražite sve lokacije koje sadrže hiperveze ka domenu ciljne organizacije. To vam možda na početku neće ni privući pažnju, ali razmotrite ovaj slučaj. Pretpostavimo da neko iz organizacije odluči da uspostavi piratsku Web prezentaciju kod kuće ili na lokaciji ciljne mreže. Organizacija ne obezbeđuje, niti je odobrila taj Web server. Dakle, da bismo pronašli potencijalne piratske Web lokacije, treba da odredimo koje se lokacije povezuju sa serverom izabrane organizacije (slika 1-1).

Slika 1-1. Kada želite da pronadete sve lokacije koje sadrže vezu ka ciljnom domenu, u pretraživaču AltaVista zadajte naredbu `link:www.adresa.com`.

U rezultatu pretraživanja vidite sve lokacije koje se povezuju s lokacijom http://www.10pht.com i istovremeno sadrže reč "hacking". Dakle, takvu mogućnost pretraživanja lako možete da iskoristite za pronalaženje lokacija povezanih sa ciljnim domenom.

Primer sa slike 1-2 prikazuje ograničavanje pretraživanja na odre?enu lokaciju. Pretraživali smo lokaciju http://10pht.com tražeći sve pojave reči "mudge". Upit iz primera se lako može prilagoditi za traženje stavki koje vas zanimaju.

Slika 1-2. Kada na odredenoj lokaciji želite da nadete zadati tekst (na primer, „mudge"), u AltaVisti upotrebite naredbu `host:lokacija.com`.

Ovi primeri, očigledno, ne mogu da vas pouče šta sve treba da tražite na svojim putovanjima - razmišljajte kreativno. Ponekad i najčudnovatiji upit pruži korisne rezultate.

Pretraživanje baze EDGAR

Kada osmatrate kompanije čijim deonicama se javno trguje, koristite bazu podataka EDGAR na adresi http://www.sec.gov (slika 1-3). Nju održava američka Komisija za promet novca i hartija od vrednosti (Securities and Exchange Commission, SEC).

Slika 1-3. U bazi podataka EDGAR možete da pretražujete javne dokumente i da steknete uvid o veličini kompanije identifikujući njene sastavne delove.

Jedan od najvećih problema svih kompanija jeste održavanje njihovih priključaka s Internetom, naročito ako aktivno preuzimaju druge firme ili se udružuju s njima. Prema tome, treba obratiti pažnju na firme koje su nedavno ušle u sastav kompanije. Dve najbolje publikacije koje izdaje pomenuta Komisija jesu 10-Q i 10-K. Prva od njih, 10-Q, objavljuje kratak pregled aktivnosti organizacije u poslednjem tromesečju. Ovaj dokument se neprekidno ažurira, a sadrži i podatke o kupovini, odnosno prodaji drugih firmi. Dokument 10-K je godišnji izveštaj o aktivnostima kompanije i nije svež kao 10-Q. Dobro je da u ovim dokumentima potražite ključne reči "subsidiary" (podre?ena organizacija, filijala) ili "subsequent events" (naredne aktivnosti). Tako možete da do?ete do obaveštenja o firmama koje je kompanija nedavno preuzela. Kompanije često previše žurno uključuju računarski sistem preuzetih firmi u mrežu korporacije, pa ne vode dovoljno računa o bezbednosti. Zbog toga ćete verovatno moći da na?ete slabu tačku u bezbednosnom sistemu preuzete firme koja će vam omogućiti da prodrete u glavnu kompaniju. Napadači su oportunisti i rado će iskoristiti zbrku koja se obično javlja prilikom spajanja mreža.

Kada pretražujete bazu podataka EDGAR, tragajte za imenima firmi koja se razlikuju od imena glavne kompanije, jer je to suštinski važno za naredne faze, u kojima ćete pretraživati organizaciju postavljajući upite bazama o vlasnicima domena. (O tome će biti reči u odeljku "Drugi korak: popisivanje mreže".)

Protivmera: obezbeđivanje javnih podataka

Većina podataka o kojima smo govorili mora da bude dostupna javnosti; to posebno važi za kompanije čijim se deonicama javno trguje. Međutim, treba vrednovati i klasifikovati vrstu podataka koja se izlaže javnosti na uvid. Priručnik za obezbeđivanje lokacije (Site Security Handbook, RFC 2196), nalazi se na adresi http://www.ietf.org/rfc/rfc2196.txt; to je odlično štivo u kome su obra?eni mnogi problemi u vezi s pravilima bezbednosti. Na kraju, preporuka: sa svojih Web strana izbacite sve nepotrebne podatke koji bi napadaču olakšali pristupanje vašoj mreži.

Drugi korak: popisivanje mreže

Popularnost:	9
Jednostavnost:	9
Uticaj:	5

Stepen rizika:	8

Prvi korak u popisivanju mreže jeste otkrivanje imena domena i mreža pridruženih odre?enoj organizaciji. Imena domena svedoče o prisustvu organizacije na Internetu i najčešće podsećaju na ime kompanije, npr. "AAAAFasade.com" ili "DobraKapljica.com".

Da biste popisali ove domene i pronašli mreže koje su s njima povezane, morate da pročešljate Internet. Postoji više baza podataka o domenima koje mogu da vam ponude obilje informacija o svakoj organizacionoj jedinici koju želite da ispitate. Do pred kraj 1999. godine, monopol na glavni registar imena domena (com, net, edu i org) imala je kompanija Network Solutions, koja je takve podatke čuvala na svojim "whois" serverima. Danas postoji nekoliko akreditovanih registara domena (http://www.internic.net/alpha.html). Postojanje ovih novih registara malo otežava istraživanje (pogledajte odeljak "Pretraživanje registara domena", kasnije u ovom poglavlju). Da bismo našli podatke, treba da pretražujemo pravi registar.

Baze s podacima o domenima mogu se pretraživati različitim postupcima (tabela 1-2). Bez obzira na različitost postupaka, trebalo bi da uvek dobijete iste podatke. Za domene mimo uobičajenih com, net, edu ili org, čitaoce upućujemo na servere navedene u tabeli 1-3. Još jedan koristan izvor, naročito za pronalaženje whois servera izvan SAD, jeste adresa http://www.allwhois.com. To je jedna od najpotpunijih kolekcija servera s informacijama o domenima na Internetu.

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

Mehanizam	Izvor	Platforma
Web lokacija	http://www.networksolutions.com/ http://www.arin.net	Bilo koja platforma s čitačem Weba
Whois klijent	Whois se isporučuje s većinom verzija UNIX-a Fwhois je napravio Chris Cappuccio <ccapuc@santefe.edu>	UNIX
WS_Ping ProPack	http://www.ipswitch.com/	Windows 95/NT/2000
Sam Spade	http://www.samspade.org/ssw	Windows 95/NT/2000
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
Xwhois	http://c64.org/~nr/xwhois/	UNIX sa X-om i GTK+ grafička biblioteka

Tabela 1-3. Zvanični, vojni i me?unarodni izvori o bazama s informacijama o domenima

Whois server	Adresa
Dodeljivanje IP adresa za Evropu	http://www.ripe.net
Dodeljivanje IP adresa za pacifički deo Azije	http://whois.apnic.net
Armija SAD	http://whois.nic.mil
Vlada SAD	http://whois.nic.gov

Svaki upit može da vam pruži drugačije podatke. Sledećim vrstama upita pronalazi se najveći deo podataka potrebnih hakerima da bi započeli napad:

Pretraživanje registara dobijaju se specifični podaci o registru i whois serverima

- Pretraživanje organizacija dobijaju se svi podaci koji se odnose na odre?enu organizaciju

- Pretraživanje domena dobijaju se svi podaci koji se odnose na određen domen
- Pretraživanje mreže dobijaju se svi podaci koji se tiču određene mreže ili jedinstvene IP adrese

Pretraživanje osoba za kontakt (Point of contact, POC) dobijaju se podaci o odre?enoj osobi, najčešće licu zaduženom za kontakte

Pretraživanje registara domena

Otkad su se pojavili deljeni registri (tj. sistem s više registara), obavezno se od servera whois.crsnic.net mora zatražiti lista domena koji eventualno odgovaraju izabranom cilju i podaci o registrima koji se odnose na te domene. Neophodno je da utvrdimo važeći registar kako bismo u sledećim koracima mogli da pošaljemo detaljne upite odgovarajućim bazama podataka. U primeru ćemo kao ciljnu organizaciju koristiti "Acme Networks", a upit poslati iz UNIX-ovog (Red Hat 6.2) komandnog okruženja. U verziji komande *whois* koju ćemo koristiti, opcija @ omogućava da zadamo alternativnu bazu podataka. U nekim *whois* klijentima zasnovanim na BSD tehnologiji (na primer, OpenBSD ili FreeBSD) može se upotrebiti opcija *-a* za zadavanje alternativne baze podataka. Upotrebite komandu *man whois* da biste saznali više o tome kako se šalju upiti iz vašeg *whois* klijenta.

Pri ovakvom pretraživanju preporučujemo da koristite džokere, jer ćete tako dobiti više rezultata pretrage. Tačka (.) iza reči "acme" daće listu svih domena koji počinju na "acme", a ne samo onih koji odgovaraju isključivo reči "acme". Isto tako, u dokumentu na adresi http://www.networksolutions.com/en_US/help/whoishelp.html potražite dodatna obaveštenja o zadavanju složenih upita. Saveti koje ćete naći u tom dokumentu pomoći će vam da sprovedete mnogo preciznije pretraživanje.

[bash]$ whois "acme."@whois.crsnic.net

[whois.crsnic.net]

Whois Server Version 1.1

Domain names in the .com, .net, and .org domains can now be registered with many different competing registrars. Go to http://www.internic.net for detailed information.

ACMETRAVEL.COM

ACMETECH.COM

ACMES.COM

ACMERACE.NET

ACMEINC.COM

ACMECOSMETICS.COM

ACME.ORG

ACME.NET

ACME.COM

ACME-INC.COM

Ako nas posebno zanima, na primer, organizacija acme.net, detaljnije pretraživanje možemo da ponovimo da bismo pronašli odgovarajući registar.

[[bash]$ whois "acme.net"@whois.crsnic.net

Whois Server Version 1.1

Domain names in the .com, .net, and .org domains can now be registered with many different competing registrars. Go to http://www.internic.net for detailed information.

Domain Name: ACME.NET

Registrar: NETWORK SOLUTIONS, INC.

Whois Server: whois.networksolutions.com

Referral URL: www.networksolutions.com

Name Server: DNS1.ACME.NET

Name Server: DNS2.ACME.NET

Vidimo da je Network Solutions registar za ovu organizaciju, što je bilo sasvim uobičajeno i za sve druge organizacije na Internetu pre usvajanja sistema deljenih registara. U narednim pretraživanjima ćemo upite morati da uputimo bazi podataka odgovarajućeg registra, jer se detaljni podaci koje tražimo tamo nalaze.

Pretraživanje organizacija

Pošto identifikujemo registar, možemo da potražimo i organizaciju. U ovom pretraživanju pretrešćemo određeni registar tražeći ime organizacije, što je šira pretraga nego kad tražimo samo ime domena. Moramo da upotrebimo rezervisanu reč "name" (ime) i da upit pošaljemo registru Network Solutions.

[bash]$ whois "name Acme Networks"@whois.networksolutions.com

Acme Networks (NAUTILUS-AZ-DOM) NAUTILUS-NJ.COM

Acme Networks (WINDOWS4-DOM) WINDOWS.NET

Acme Networks (BURNER-DOM) BURNIER.COM

Acme Networks (ACME2-DOM) ACME.NET

Acme Networks (RIGHTBABE-DOM) RIGHTBABE.COM

Acme Networks (ARTS2-DOM) ARTS.ORG

Acme Networks (HR-DEVELOPMENT-DOM) HR-DEVELOPMENT.COM

Acme Networks (NTSOURCE-DOM) NTSOURCE.COM

Acme Networks (LOCALNUMBER-DOM) LOCALNUMBER.NET

Acme networks (LOCALNUMBERS2-DOM) LOCALNUMBERS.NET

Acme Networks (Y2MAN-DOM) Y2MAN.COM

Acme Networks (Y2MAN2-DOM) Y2MAN.NET

Acme Networks for Christ Hospital (CHOSPITAL-DOM) CHOSPITAL.ORG

Iz rezultata pretrage vidimo da su sa organizacijom Acme Networks povezani mnogi domeni. Među utim, jesu li mreže zaista povezane s ovim domenima ili su samo registrovane za buduću upotrebu, odnosno radi očuvanja zaštitnog znaka? Moramo nastaviti da kopamo sve dok ne prona?emo "živu" mrežu.

Kada ovakvim postupkom pretraživanja ispitujete veliku organizaciju, možda ćete kao rezultat dobiti na stotine zapisa. Pre nego što su zloupotrebe postale izuzetno učestale, sa servera kompanije Network Solutions mogli ste da preuzmete čitav domen com. Danas su whois serveri sistema Network Solutions podešeni tako da daju samo prvih 50 rezultata.

Pretraživanje domena

Na osnovu rezultata pretraživanja organizacija, kandidat koji najviše obećava jeste domen Acme.net, budući da se organizacija zove Acme Networks. (Naravno, sva imena i reference su izmišljeni.)

[bash]$ whois acme.net@whois.networksolutions.com

[whois.networksolutions.com]

Registrant:

Acme Networks (ACME2-DOM)

11 Town Center Ave.

Einstein, AZ 21098

Domain Name: ACME.NET

Administrative Contact, Technical Contact, Zone Contact:

Boyd, Wooody [Network Engineer] (WB9201) woody@ACME.NET

201-555-9011 (201)555-3338 (FAX) 201-555-1212

Record last updated on 13-Sep-95

Record created on 30-May-95

Database last updated on 14-Apr-99 13:20:47 EDT.

Domain servers in listed order:

DNS.ACME.NET 10.10.10.1

DNS2.ACME.NET 10.10.10.2

Ova vrsta pretraživanja daje rezultate koji se odnose na:

registrovanu organizaciju

- ime domena
- službene kontakte
- vreme nastajanja i ažuriranja zapisa

primarni i sekundarni server imena domena (DNS servere).

Sada u vama treba da se probudi detektiv. Analizirajte rezultate i pronađite način koji će vam obezbediti više informacija. Višak ili curenje informacija često zovemo "mamac", jer napadača mame da bolje usredsredi napad. Pogledajmo detaljnije o čemu se tu radi.

Pregledom podataka o registrovanoj organizaciji (registrantu) možemo da utvrdimo da li taj domen pripada organizaciji koju želimo da snimimo. Znamo da je sedište kompanije Acme Networks u Arizoni, pa je opravdana pretpostavka da se dobijeni podaci mogu iskoristiti za našu analizu snimka. Imajte na umu da sedište registranta ne mora da se poklapa sa geografskim odredištem firme. Mnoge organizacije se prostiru na više geografskih područja i svaki takav deo ima sopstveni priključak na Internet, ali svi delovi mogu da budu registrovani na ime jedinstvene organizacije. Najbolje je da posetite tu Web lokaciju i da utvrdite da li se stvarno radi o željenoj organizaciji.

Podaci za stupanje u službenu vezu s organizacijom veoma su važni, jer iz njih možete da saznate ime osobe zadužene za povezivanje na Internet ili za održavanje zaštitne barijere. Tu su i broj telefona, odnosno faksa. Oni su od neprocenjive vrednosti kada isprobavate upad u sistem s daljine - samo pokrenite program za automatsko pozivanje, i na dobrom ste putu da otkrijete brojeve modema. Osim toga, uljezi se često predstavljaju kao službenici zaduženi za kontakte i zloupotrebljavaju poverenje običnih korisnika u organizaciji. 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.

Iz datuma nastanka i izmene zapisa može se suditi o tačnosti podataka. Ako je zapis nastao pre pet godina i od tada nije ažuriran, velike su šanse da su neki podaci (npr. podaci za stupanje u službenu

vezu) zastareli.

Poslednja grupa podataka otkriva zvanične servere imena domena. Prvi je primarni DNS server, a zatim slede sekundarni, tercijarni itd. Ti podaci biće nam potrebni za ispitivanje DNS-a, o čemu će biti reči kasnije u ovom poglavlju. Osim toga, možemo pokušati da iskoristimo navedenu mrežnu oblast kao polaznu tačku za pretraživanje mreža u bazi podataka ARIN.

SAVET

Kada uz HST zapis koji je dobijen whois upitom upotrebite naredbu *server* , moći ćete da otkrijete i druge domene pridružene istom DNS serveru. Sledeći postupak pokazuje kako to da uradite.

Pretražite domene na prethodno opisan način.

1. Prona?ite prvi DNS server.
2. Izvršite whois pretraživanje o tom DNS serveru:

```
whois "HOST 10.10.10.1"@whois.networksolutions.com
```

1. Locirajte HST zapis za DNS server.
2. Izvršite whois pretraživanje uz naredbu server, koristeći odgovarajući HST zapis:

```
whois "SERVER NS9999-HST"@whois.networksolutions.com
```

Pretraživanje mreža

Američki registar Internet brojeva (American Registry for Internet Numbers, ARIN) još je jedna baza podataka koju možemo da upotrebimo za pronalaženje mreža koje su povezane s ciljnim domenom. U ovoj bazi podataka čuvaju se informacije o mrežnim blokovima i njihovim vlasnicima. Vrlo je važno da se istraživanjem utvrdi da li ciljna organizacija stvarno poseduje sistem ili ga pak deli s drugom organizacijom, odnosno iznajmljuje od davaoca usluga Interneta (ISP).

U našem primeru, pokušaćemo da identifikujemo sve mreže koje poseduje kompanija "Acme Networks". Pretraživanje baze podataka ARIN obično je plodonosno, jer se ona ne ograničava na prikazivanje samo 50 rezultata kao Network Solutions. Obratite pažnju na upotrebu džokera ".".

[bash]$ whois "Acme Net."@whois.arin.net

[whois.arin.net]

Acme Networks (ASN-XXXX) XXXX 99999

Acme Networks (NETBLK) 10.10.10.0 - 10.20.129.255

Mreže možemo i detaljnije pretražiti ako iskoristimo odre?eni mrežni blok (10.10.10.0):

[bash]$ whois 10.10.10.0@whois.arin.net

[whois.arin.net]

Major ISP USA (NETBLK-MI-05BLK) 10.10.0.0 - 10.30.255.255

ACME.NETWORKS, INC. (NETBLK-MI-10-10-10) CW-10-10-10

10.10.10.0 - 10.20.129.255

ARIN obezbe?uje zgodan mehanizam pretraživanja na Webu (slika 1-4). Analizirajući rezultat, utvrð ujemo da je davalac usluga Interneta "Major ISP USA" povezan na okosnicu Mreže i da je organizaciji Acme Networks dodelio mrežu klase A (potpuno objašnjenje protokola TCP/IP naći ćete u knjizi Richarda Stevensa TCP/IP Illustrated Volume 1). Prema tome, zaključujemo da se radi o mreži koju poseduje Acme Networks.

Slika 1-4. Baza organizacije ARIN najlakše se pretražuje s njihove Web lokacije.

Pretraživanje informacija o osobama za kontakt

Pošto jedna osoba može da administrira domene za više organizacija, preporučljivo je da se pretraže informacije o osobama za kontakt (POC) prema korisničkom nalogu za pristup bazi podataka (engl. user's database handle). Tražimo nalog "WB9201", dobijen prethodnim pretraživanjem domena. Tako možete da otkrijete domen za koji i ne znate da postoji.

[bash]$ whois "HANDLE WB9201"@whois.networksolutions.com

Boyd, Woody [Network Engineer] (WB9201) woody@ACME.NET

BIG ENTERPRISES

11 TOWN CENTER AVE

EINSTEIN, AZ 20198

201-555-1212 (201)555-1212 (FAX) 201-555-1212

Mogli smo potražiti i @Acme.net i dobiti listing elektronskih adresa osoba za kontakt. Od rezultata prikazujemo samo početak listinga:

[bash]$ whois "@acme.net"@whois.networksolutions.net

Smith, Janet (JS9999) jsmith@ACME.NET (201) 555-9211

(FAX) (201) 555-3643

Benson, Bob (BB9999) bob@ACME.NET (201) 555-1988

Manual, Eric (EM9999) ericm@ACME.NET (201) 555-8484

(FAX) (201) 555-8485

Bxon, Rob (RB9999) rbixon@ACME.net (201) 555-8072

Protivmera: obezbe?ivanje javne baze podataka

Veliki deo informacija sadržanih u bazama podataka koje smo dosad pominjali, namenjen je javnosti. Kada organizacija želi da registruje domen na Internetu, neophodni su podaci za uspostavljanje službene veze, podaci o registrovanim mrežnim blokovima i o zvaničnom serveru imena domena. Me?utim, sve to treba na odgovarajući način obezbediti da bi se uljezima što više otežao posao.

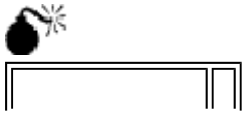
Č;esto se dešava da osoba zadužena za službene veze napusti organizaciju, ali da i dalje ima mogućnost da menja podatke o domenu organizacije. Zbog toga najpre treba obezbediti da podaci u bazi podataka budu ažurni. Ako treba, ažurirajte podatke koji se odnose na uspostavljanje administrativne, tehničke i finansijske službene veze. Proverite i navedene telefonske brojeve i adrese. Oni mogu da budu polazna tačka za daljinski upad ili za lažno predstavljanje (engl. social engineering). Razmislite o tome da li bi bezbednosti doprinelo ako biste se opredelili da koristite besplatne telefonske brojeve ili brojeve izvan telefonske centrale vaše organizacije. Uzgred, neke organizacije koriste lažne administratore, radi zavo?enja eventualnih napadača. Ako bilo koji službenik primi elektronsku poruku ili telefonski poziv od lažnog administratora, to može da bude alarm za službu obezbeđenja mreže.

Prilikom registrovanja domena postoji još jedna opasnost, koja potiče od načina na koji neki registri omogućavaju ažuriranje. Na primer, tekuća realizacija servera Network Solutions dozvoljava automatsko menjanje podataka koji se odnose na domen. Ovaj server potvr?uje identitet registranta pomoću tri metode: polja FROM iz poruka e-pošte, lozinke i PGP-ključa. Zapanjujuće je što je polje FROM iz poruke e-pošte podrazumevana metoda identifikovanja. Posledice ovakvog izbora po bezbednost su nesagledive. 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 se to, kako je 16. oktobra 1998. objavio Washington Post, dogodilo velikom davaocu 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 putem obrasca Contact Form koji koristi server Network Solutions neophodno da se prethodno uspostavi administrativna ili tehnička veza.

Treći korak: ispitivanje DNS-a

Pošto otkrijete sve pridružene domene, počnite da pretražujete server imena domena (DNS). DNS je distribuirana baza podataka koja se koristi za preslikavanje IP adresa u imena računara i obrnuto. Ako DNS server nije bezbedno konfigurisan, od njega se mogu dobiti informacije koje "otkrivaju" organizaciju.

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, me?utim, 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.

Jednostavan način da prenesete zonu jeste da upotrebite program *nslookup* , koji se isporučuje s većinom UNIX i NT sistema. Komandu *nslookup* možemo da upotrebimo interaktivno:

[bash]$ nslookup

Default Server: dns2.acme.net

Address: 10.10.20.2

>> server 10.10.10.2

Default Server: [10.10.10.2]

Address: 10.10.10.2

>> set type=any

>> ls -d Acme.net. >> /tmp/zone_out

Najpre pokrećemo *nslookup* u interaktivnom režimu. Kada se pokrene, program će ispisati podrazumevani server imena koji on koristi, što je po pravilu DNS server organizacije ili DNS davaoca usluga Interneta. Me?utim, naš server imena domena (10.10.20.2) nije ovlašćen za ciljni domen, tako da nema sve DNS zapise koje tražimo. Zbog toga moramo programu *nslookup* ručno da zadamo DNS server koji treba da pretražuje. U ovom primeru hoćemo da upotrebimo primarni server imena domena za Acme Networks (10.10.10.2). 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 završimo prenos zone, pregledaćemo datoteku i u njoj potražiti informacije koje bi nam eventualno mogle pomoći da se usmerimo na odre?ene sisteme. Pogledajmo rezultat:

[bash]$ more zone_out

acct18 1D IN A 192.168.230.3

1D IN HINFO "Gateway2000" "WinWKGRPS"

1D IN MX 0 acmeadmin-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 acmeadmin-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 kao što su *grep* , *sed* , *awk* ili *perl* .

Pretpostavimo da smo stručnjaci za sistem SunOS ili sistem Solaris. Mogli bismo pomoću programa da prona?emo IP adrese koje su u zapisu HINFO povezane sa SPARC-om, 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 da bi našli posebne vrste 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 Acme.net. Ako postoje poddomeni (na primer, greenhouse.Acme.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. Me?utim, 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 me?u njima su *host* , Sam Spade, *axfr* i *dig* .

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

```
host -1 Acme.net
```

ili

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

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

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

Sisteme ne morate da snimate samo iz UNIX-a. Mnogi Windowsovi programi obezbe?uju iste funkcije (slika 1-5).

Slika 1-5. Ako radije koristite Windows, pomoću višenamenskog programa Sam Spade možete da prenesete zonu, kao i da obavite druge poslove koji se odnose na snimanje sistema ciljne organizacije.

Najzad, možete da upotrebite jednu od najboljih alatki za prenošenje zone, Gaiusov program *axfr* (http://ftp.cdit.edu.cn/pub/linux/www.trinux.org/src/netmap/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 domenima *com* , odnosno *edu* . To se, međutim, ne preporučuje. *Axfr* pokrećete na sledeći način:

[bash]$ axfr Acme.net

axfr: Using default directory: /root axfrdb

Found 2 name servers for domain 'Acme.net':

Text deleted.

Received XXX answers (XXX records).

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

[bash]$ axfrcat Acme.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. Č;esto 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 Acme.net

Acme.net has address 10.10.10.1

Acme.net mail is handled (pri=22) by smtp-forward.Acme.net

Acme.net mail is handled (pri=10) by gate.Acme.net

Ako se komanda *host* upotrebi samo uz ime domena, bez ikakvih parametara, prvo će pokušati da razreši zapise tipa A, a onda zapise tipa MX. Navedeni rezultati se slažu s podacima koji su ranije dobijeni *whois* pretraživanjem i s podacima iz baze ARIN. Prema tome, možemo da smatramo da smo pronašli mrežu koju treba da ispitujemo.

Protivmera: bezbednost DNS servera

Server imena domena sadrži obilje informacija koje napadači mogu da iskoriste, pa zato treba smanjiti količinu informacija dostupnih preko Interneta. Kada je reč o serveru, prenos zone se sme odobriti samo ovlašćenim serverima. Savremene verzije BIND-a se mogu 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://support.microsoft.com/support/kb/articles/q193/8/37.asp.) U slučaju ostalih servera imena, pregledajte dokumentaciju i utvrdite kako se može ograničiti ili sprečiti prenos zone.

S druge strane, na mreži možete 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, predloženom protivmerom krši se RFC pravilo koje traži da se zahtevi 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. Primer u kome se realizovanje bezbednosnih TSIG mera objašnjava korak po korak naći ćete na adresi http://romana.ucd.ie/james/tsig.html.

Ograničavanjem prenosa zone produžavate vreme koje će napadačima biti potrebno 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 s 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.

Četvrti korak: upoznavanje mreže

Pošto smo identifikovali mreže naše žrtve, 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 u Windowsu NT. U Windowsu NT se on iz istorijskih razloga zove *tracert* .

Traceroute je dijagnostička alatka koju je Van Jacobson prvobitno napravio 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 obra?uje 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 identifikuje mehanizme za kontrolu pristupa (programski izvedenu zaštitnu barijeru ili usmerivač za filtriranje paketa) koji možda filtriraju saobraćaj.

Razmotrimo to na jednom primeru.

[bash]$ traceroute Acme.net

traceroute to Acme.net (10.10.10.1), 30 hops max, 40 byte packets

1 gate2 (192.168.10.1) 5.391 ms 5.107 ms 5.559 ms

2 rtr1.bigisp.net (10.10.12.13) 33.374 ms 33.443 ms 33.137 ms

3 rtr2.bigisp.net (10.10.12.14) 35.100 ms 34.427 ms 34.813 ms

4 hssitrt.bigisp.net (10.11.31.14) 43.030 ms 43.941 ms 43.244 ms

5 gate.Acme.net (10.10.10.1) 43.803 ms 44.041 ms 47.835 ms

Vidimo putanju paketa koji napušta usmerivač (mrežni prolaz) i do odredišta stiže u tri (2-4) skoka. Paketi putuju kroz razne sisteme bez blokiranja. Iz našeg prethodnog istraživanja znamo da MX zapis za Acme.net ukazuje na gate.acme.net. Stoga pretpostavljamo da je to aktivan mrežni računar i da se prethodni skok (4) odnosi na usmerivač na obodu organizacije. Skok 4 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 ure?aj 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). 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 NT, 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. 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) 37.945 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 * * *

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 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 37.872 ms

3 rtr2.bigisp.net (10.10.12.14) 36.739 ms 39.516 ms 37.226 ms

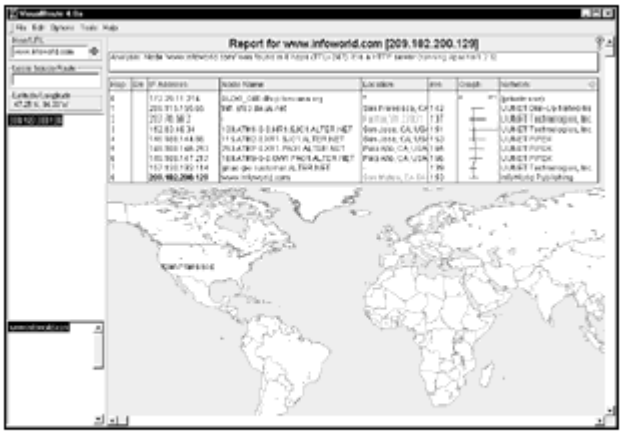
4 hssitrt.bigisp.net (10.11.31.14) 47.352 ms 47.363 ms 45.914 ms

5 10.10.10.2 (10.10.10.2) 50.449 ms 56.213 ms 65.627 ms

Pošto uređaj za kontrolu pristupa (korak 4) sada ne može da na?e manu paketima, 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 sa komandne linije. Oni koji više vole grafičko okruženje, za otkrivanje putanja mogu da koriste VisualRoute (http://www.visualroute.com) ili NeoTrace (http://www.neotrace.com/). Program VisualRoute grafički prikazuje svaki mrežni skok i spaja ga s rezultatima *whois* pretraživanja. Ovaj program, prikazan na slici 1-6, deluje zanimljivo, ali ne radi dobro s velikim mrežama.



Slika 1-6. VisualRoute, pravi biser među alatkama za otkrivanje putanja, pruža informacije o mrežnom skoku i geografsku lokaciju računara, rezultate whois pretraživanja i informacije iz zaglavlja Web servera.

Postoje dodatne tehnike čijom primenom možete da do?ete do važećih ACL lista određenih uređaja za kontrolu pristupa. Skeniranje protokola zaštitne barijere (engl. firewall protocol scanning) jedna je od takvih tehnika, a objasnićemo je u poglavlju 11.

Protivmera: onemogućavanje pokušaja upoznavanja mreže

U ovom poglavlju smo se samo dotakli tehnika koje se koriste za upoznavanje mreže. U sledećim poglavljima ćemo obraditi mnogo radikalnije tehnike. Postoji, me?utim, nekoliko mera koje možemo preduzeti da bismo identifikovali i sprečili ulazak opisanih sondi u sistem. Mnogi komercijalni sistemi za otkrivanje upada (engl. network intrusion detection system, NIDS) 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://packetstorm.securify.com/UNIX/loggers/rr-1.0.tgz). Taj uslužni program beleži pristigle zahteve programa *traceroute* i generiše lažne odgovore na njih. U zavisnosti od načina rada vašeg sistema obezbe?enja, možda ćete mrežne usmerivače na obodu moći tako da podesite da saobraćaj ICMP i UDP paketa ograniče na odre?ene sisteme, i tako smanjite 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. Imajte na umu, međutim, 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* . Postoje mnogi napadači koji nikada nisu bili otkriveni, s bogatim iskustvom u prepoznavanju mreža i dobro opremljeni. 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.

Hakerske tajne: zaštita mrežnih sistema

Skeniranje

Ako snimanje sistema uporedimo sa otkrivanjem mesta na kome se informacije nalaze, skeniranje možemo da shvatimo kao kuckanje po zidovima da bismo utvrdili gde se nalaze vrata i prozori. Snimanjem dobijamo spisak mrežnih i IP adresa pomoću upita tipa whois i prenosa zone. Tim tehnikama napadači dobijaju dragocene podatke: imena zaposlenih i brojeve telefona, opsege IP adresa, DNS i poštanske servere i sl. Sada treba da utvrdimo koji su sistemi živi i dostupni s Interneta, a za to ćemo koristiti različite alatke i tehnike kao što su automatsko skeniranje mreže signalom ping, skeniranje priključaka i alatke za automatsko otkrivanje.

Naglašavamo da IP adrese koje su otkrivene prilikom prenosa zone ne moraju da budu dostupne s Interneta. Moraćemo da proverimo svaki ciljni sistem da bismo utvrdili da li je živ i preko kojih priključaka osluškuje, ukoliko takvi priključci uopšte postoje. Videli smo mnoge ravo podešene servere imena domena koji dozvoljavaju izlistavanje IP adresa privatnih mreža (na primer, 10.10.10.0). Pošto se ovim adresama ne može pristupiti s Interneta, uzalud ćete se mučiti ako to pokušate. U dokumentu RFC 1918 potražite više obaveštenja o tome koji se opsezi IP adresa smatraju nedostupnim (http://www.ietf.org/rfc/rfc1918.txt).

Pre?imo sada na sledeću fazu prikupljanja informacija - skeniranje.

Otkrivanje živih sistema

Jedan od osnovnih koraka pri mapiranju mreže jeste izvo?enje automatskog skeniranja opsega IP adresa i mrežnih blokova signalom ping (engl. ping sweep) da bi se utvrdilo jesu li pojedini sistemi aktivni. Komanda *ping* obično se koristi za slanje ICMP paketa ECHO (tipa 8) ciljnom sistemu u nadi da će on uzvratiti ICMP paketom ECHO_REPLY (tipa 0), što bi značilo da je živ. Premda je ova komanda prihvatljiva za određivanje broja živih sistema u malim i srednjim mrežama, ona nije dovoljno efikasna u korporacijskim mrežama. Skeniranje mreže klase A može da potraje satima, ako ne i danima. Morate znati da otkrivate žive sisteme na više načina, i zato u narednom odeljku predočavamo izbor raspoloživih tehnika.

Skeniranje mreže signalom ping

Popularnost:	10
Jednostavnost:	9
Posledice:	3
Procena rizika:	7

Za automatsko skeniranje signalom ping možete da upotrebite mnoge alatke koje postoje i u UNIX-u i u Windowsu NT. Jedna od takvih tehnika, oprobana u UNIX-u, jeste korišćenje programa *fping* (http://packetstorm.securify.com/Exploit_Code_Archive/fping.tar.gz). Za razliku od uobičajenih uslužnih programa koji čekaju odgovor svakog sistema pre nego što pre?u na sledeći, fping će poslati opšti zahtev za odgovor, slično cirkularnom pismu. Tako će fping proveriti skup IP adresa znatno brže nego *ping* . On se može koristiti na dva načina: bilo tako što mu se IP adrese šalju sa standardnog ulaza, ili tako što ih očitava iz datoteke. Očitavanje adresa iz datoteke je jednostavno -

samo napravite datoteku sa IP adresama smeštenim u uzastopne redove:

192.168.51.1

192.168.51.2

192.168.51.3

...

192.168.51.253

192.168.51.254

Tada parametrom -f očitajte datoteku:

[tsunami]$ fping -f in.txt

192.168.51.254 is alive

192.168.51.227 is alive

192.168.51.224 is alive

...

192.168.51.3 is alive

192.168.51.2 is alive

192.168.51.1 is alive

192.168.51.190 is alive

Opcija -a komande fping prikazaće samo žive sisteme. Možemo je kombinovati s opcijom -d da bismo razrešili imena računara. Najčešće koristimo opciju -a sa skriptovima komandnog okruženja, a opciju -d kada nas zanimaju sistemi koji imaju jedinstvena imena. Druge opcije kojima se podaci čitaju iz datoteke, kao što je opcija -f, mogu da pomognu kada sastavljate skript za automatsko skeniranje. Komandom fping -h dobićete potpun spisak raspoloživih opcija. Drugi uslužni program koji se pominje u celoj knjizi jeste Fyodorov nmap (www.insecure.org/nmap), ali njega ćemo detaljnije razmotriti u nastavku poglavlja i zasad samo pominjemo da se pomoću njegove opcije -sP može izvesti i automatsko skeniranje signalom ping.

[tsunami] nmap -sP 192.168.1.0/24

Starting nmap V. 2.53 by fyodor@insecure.org (www.insecure.org/nmap/)

Host (192.168.1.0) seems to be a subnet broadcast

address (returned 3 extra pings).

Host (192.168.1.1) appears to be up.

Host (192.168.1.10) appears to be up.

Host (192.168.1.11) appears to be up.

Host (192.168.1.15) appears to be up.

Host (192.168.1.20) appears to be up.

Host (192.168.1.50) appears to be up.

Host (192.168.1.101) appears to be up.

Host (192.168.1.102) appears to be up.

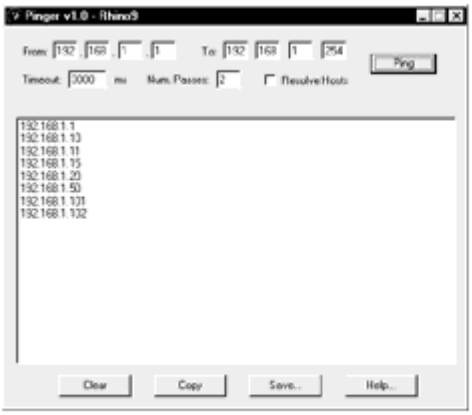
Host (192.168.1.255) seems to be a subnet broadcast

address (returned 3 extra pings).

Nmap run completed -- 256 IP addresses (10 hosts up) scanned

in 21 seconds

Za korisnike Windowsa, besplatan program Pinger (slika 2-1) grupe Rhino9 (http://www.nmrc.org/files/snt/ jedan je od najbržih raspoloživih programa za automatsko skeniranje. Slično programu fping, i on istovremeno šalje više ICMP paketa ECHO, a zatim čeka odgovore. Pinger takođe omogućava da razrešite imena računara i da rezultat snimite u datoteku. S Pingerom se po brzini može meriti komercijalni proizvod Ping Sweep firme SolarWinds (www.solarwinds.net). Ping Sweep može da bude brz kao munja, jer omogućava da uzastopno šaljete pakete sa zadatim vremenskim intervalom između dva slanja. Kada vrednost tog intervala postavite na 0 ili 1, moći ćete da skenirate mrežu klase C i da razrešite imena računara za manje od sedam sekundi. Pažljivo koristite ove alatke jer lako možete da zagušite vezu, kao što je ISDN linija od 128 K ili Frame Relay (da ne pominjemo satelitske ili IR veze).



Slika 2-1. Program Pinger grupe Rhino9 jedan je od najbržih uslužnih programa za automatsko skeniranje signalom ping, a uz to je besplatan.

Od ostalih uslužnih programa za automatsko skeniranje signalom ping iz Windowsa pomenimo

WS_Ping ProPack (www.ipswitch.com) i NetScanTools (www.nwpsw.com). Te alatke su dobre za skeniranje malih mreža, ali rade znatno sporije od programa Pinger ili Ping Sweep. Iako su zbog grafičkog radnog okruženja ugodniji za oko, WS_Ping ProPack i NetScanTools imaju ograničene mogućnosti skriptovanja i automatizovanja.

Šta se događa ako ciljna lokacija blokira protokol ICMP? Nije retkost da nai?ete na lokaciju o čijoj bezbednosti se vodi računa i zato je protokol ICMP blokiran na spoljnom mrežnom usmerivaču ili na zaštitnoj barijeri. Iako je protokol ICMP blokiran, postoje alatke i tehnike pomoću kojih ipak možete da utvrdite da li su sistemi iza barijere živi. One, međutim, nisu precizne ni efikasne kao uobičajeni postupak automatskog skeniranja signalom ping.

Kada je saobraćaj koji se odvija protokolom ICMP blokiran, prva tehnika koju ćete upotrebiti da biste utvrdili jesu li računari živi biće skeniranje priključaka (engl. port scanning). (Skeniranje priključaka ćemo detaljnije objasniti u nastavku poglavlja.) Skeniranjem svih uobičajenih priključaka na potencijalnim IP adresama možemo da prona?emo žive računare ukoliko na ciljnom sistemu možemo da otkrijemo otvorene priključke, odnosno one koji osluškuju. Opisana tehnika je spora i ne daje uvek nedvosmislen rezultat. Jedna od alatki koja se koristi za ovakvo skeniranje priključaka jeste program nmap. Ranije smo pomenuli da nmap podržava ICMP skeniranje. Með utim, on ima i napredniju opciju, TCP ping scan (TCP skeniranje). Ona se aktivira parametrom -PT i brojem priključka, a najčešće je to 80, jer se obično dopušta prolaz od spoljnih usmerivača ili kroz glavnu zaštitnu barijeru do tog priključka sistema u demilitarizovanoj zoni (DMZ). Ova opcija će omogućiti slanje paketa TCP ACK ka ciljnoj mreži i čekati paket RST koji označava da je računar živ. Pretpostavlja se da će ACK paketi lakše proći kroz zaštitnu barijeru koja ne čuva informacije o stanju sesije.

[tsunami] nmap -sP -PT80 192.168.1.0/24

TCP probe port is 80

Starting nmap V. 2.53

Host (192.168.1.0) appears to be up.

Host (192.168.1.1) appears to be up.

Host shadow (192.168.1.10) appears to be up.

Host (192.168.1.11) appears to be up.

Host (192.168.1.15) appears to be up.

Host (192.168.1.20) appears to be up.

Host (192.168.1.50) appears to be up.

Host (192.168.1.101) appears to be up.

Host (192.168.1.102) appears to be up.

Host (192.168.1.255) appears to be up.

Nmap run completed (10 hosts up) scanned in 5 seconds

Kao što vidite, ova metoda efikasno utvrđuje da li je sistem živ čak i kada su blokirani ICMP paketi. Dobro je pokušati skeniranje uobičajenih priključaka kao što su SMTP (25), POP (110), AUTH (113), IMAP (143), ali i drugih priključaka koji su jedinstveni za ciljnu lokaciju.

Hping (http://www.kyuzz.org/antirez/) još je jedan uslužni program za TCP skeniranje, a ima više TCP mogućnosti od programa *nmap* . Hping korisniku omogućava da upravlja specifičnim opcijama TCP paketa i da paket tako podesi da pro?e kroz odre?ene ure?aje za kontrolu pristupa. Kada odredišni priključak zadate uz opciju -p, moći ćete da zaobi?ete izvesne uređaje za kontrolu pristupa, što je slično tehnici koja se izvodi pomoću programa traceroute (opisan je u poglavlju 1). Hping se može upotrebiti za automatsko TCP skeniranje, a usitnjeni paketi koje šalje mogu da zaobiđu pojedine uređaje za kontrolu pristupa.

[tsunami] hping 192.168.1.2 -S -p 80 -f

HPING 192.168.1.2 (eth0 192.168.1.2): S set, 40 data bytes

60 bytes from 192.168.1.2: flags=SA seq=0 ttl=124 id=17501 win=0 time=46.5

60 bytes from 192.168.1.2: flags=SA seq=1 ttl=124 id=18013 win=0 time=169.1

U izvesnim slučajevima, jednostavni uređaji za kontrolu pristupa ne mogu pravilno da obrade usitnjene pakete, pa ih propuštaju i tako im omogućavaju da utvrde da li je ciljni sistem živ. Obratite pažnju na to da se, kad god je priključak otvoren, vraćaju indikatori TCP SYN (S) i TCP ACK (A). Hping se lako može integrisati u skriptove komandnog okruženja pomoću opcije za brojanje paketa -cN, gde N označava broj paketa koji se šalju pre nego što se nastavi. Iako ova metoda nije brza kao neke metode automatskog ICMP skeniranja koje smo ranije opisali, možda ćete morati da je primenite zbog specifičnosti konfiguracije ciljne mreže. O programu hping više reči biće u poglavlju 11.

Poslednja alatka koju ćemo analizirati jeste icmpenum firme Simple Nomad (http://www.nmrc.org/files/sunix/icmpenum-1.1.1.tgz). To je zgodan programčić za ICMP popisivanje koji omogućava da brzo identifikujete žive sisteme tako što šalje uobičajene ICMP pakete ECHO, ali i ICMP zahteve TIME STAMP, odnosno ICMP zahteve INFO. Ako obodni usmerivač ili zaštitna barijera spreče ulazak paketa ICMP ECHO, još uvek možemo da identifikujemo sistem pomoću drugih ICMP tipova:

[shadow] icmpenum -i2 -c 192.168.1.0

192.168.1.1 is up

192.168.1.10 is up

192.168.1.11 is up

192.168.1.15 is up

192.168.1.20 is up

192.168.1.103 is up

U ovom primeru smo izlistali celu mrežu 192.168.1.0 klase C koristeći ICMP zahtev TIME STAMP. Međutim, prava snaga programa icmpenum je u tome što on može da identifikuje sisteme šaljući im maskirane pakete koji izmiču otkrivanju. To je moguće zato što on podržava maskiranje paketa opcijom -s i pasivno osluškuje odgovore pomoću parametra -p.

Ukratko, ovaj korak nam omogućava da žive sisteme otkrijemo slanjem ICMP paketa ili selektivnim skeniranjem priključaka. Od 255 mogućih adresa unutar opsega klase C, utvrdili smo da je nekoliko računara živo i njih ćemo detaljno ispitati. Na taj način smo prilično smanjili ciljni skup, uštedeli vreme i suzili fokus naših aktivnosti.

Zaštita od automatskog skeniranja signalom ping

Iako automatsko skeniranje može da vam liči na bezopasno dosa?ivanje, veoma je važno da takvu aktivnost otkrijete ukoliko se dogodi. U zavisnosti od strategije vašeg sistema bezbednosti, možda ćete automatsko skeniranje hteti i da blokirate. U nastavku razmatramo obe opcije.

Otkrivanje Kao što smo naglasili, mapiranje mreže automatskim skeniranjem proverena je metoda upoznavanja mreže pre stvarnog napada. Zbog toga je otkrivanje te aktivnosti presudno za prepoznavanje potencijalnog napadača i vremena mogućeg napada. Osnovnu metodu za otkrivanje automatskog skeniranja nude programi za otkrivanje upada kao što je snort (http://www.snort.org).

Na računarima takve napade može da otkrije i zabeleži nekoliko UNIX-ovih uslužnih programa. Ako prepoznate ICMP pakete ECHO koji stižu iz odre?enog sistema ili mreže, to može da znači da neko pokušava da upozna mrežu vaše lokacije. Posvetite toj aktivnosti dužnu pažnju jer uskoro može da usledi pravi napad.

Windowsovi programi za otkrivanje skeniranja signalom ping prilično su retki. Me?utim, postoji šerverski/besplatan program Genius, vredan pažnje. Aktuelna verzija je 3.1 i može se naći na adresi http://www.indiesoft.com. Genius ne otkriva skeniranje sistema ICMP paketima ECHO, nego skeniranje određenog TCP priključka. Komercijalno rešenje za otkrivanje TCP skeniranja priključka jeste program BlackICE, firme Network ICE (www.networkice.com). Taj proizvod je mnogo više od pukog detektora TCP skeniranja priključka, ali se može upotrebiti i u tu svrhu. U tabeli 2-1 pobrojane su i druge alatke za otkrivanje skeniranja pomoću kojih možete uspešnije da nadgledate svoj sistem.

Tabela 2-1. Neke od UNIX-ovih alatki za otkrivanje skeniranja signalom ping

Program	Izvor
Scanlogd	http://www.openwall.com/scanlogd
Courtney 1.3	http://packetstorm.securify.com/UNIX/audit/courtney-1.3.tar.Z
Ippl 1.4.10	http://pltplp.net/ippl/
Protolog 1.0.8	http://packetstorm.securify.com/UNIX/loggers/protolog-1.0.8.tar.gz

Sprečavanje Premda je otkrivanje automatskog skeniranja signalom ping neophodan korak, njegovo sprečavanje - koliko god je moguće - još je bolje. Preporučujemo da pažljivo odmerite koju ćete vrstu ICMP saobraćaja dozvoliti u svojim mrežama ili na odre?enim sistemima. Postoji više tipova ICMP paketa - ECHO i ECHO_REPLY su samo dva od njih. Mnogim lokacijama nisu potrebne sve vrste ICMP saobraćaja ka svim sistemima koji su direktno povezani na Internet. Iako skoro svaka zaštitna barijera može da spreči prolazak ICMP paketa, iz organizacionih razloga može da bude neophodno da se omogući prolaz izvesnim paketima. Ako takva potreba postoji, pažljivo razmotrite kojim ćete vrstama ICMP paketa odobriti prolazak. Minimalistički pristup bi podrazumevao da u demilitarizovanu zonu mreže propustite samo ICMP pakete ECHO_REPLY, HOST_UNREACHABLE i TIME_EXCEEDED. Ukoliko ICMP saobraćaj može pomoću lista za kontrolu pristupa da se ograniči samo na specifične IP adrese vašeg dobavljača usluga Interneta, to rešenje je još bolje. Time ćete dobavljaču omogućiti da proverava povezivanje, a u izvesnoj meri

ćete obeshrabriti pokušaje ICMP skeniranja sistema direktno povezanih s Internetom.

ICMP je moćan protokol za dijagnostikovanje problema na mreži, ali se lako može i zloupotrebiti. Omogućavanje neometanog ICMP saobraćaja kroz vaše granične mrežne prolaze dozvoljava zlonamernicima da izvedu tzv. napad radi uskraćivanja usluga (na primer, Smurf). Još je gore što će napadači, ako stvarno ugroze jedan od vaših sistema, moći da se na mala vrata uvuku u operativni sistem i u njega ubace maskirane podatke unutar ICMP paketa ECHO, služeći se programom kao što je loki. Više detalja o programu loki potražite u časopisu Phrack Magazine, tom 7, broj 51 od 1. septembra 1997. članak 06 (http://www. phrack.org/show.php?p=51&a=6).

Druga zanimljiva ideja, koju je razvio Tom Ptacek a u Linuxu realizovao Mike Shiffman, jeste korisnička usluga pingd. Ona obrađuje sav saobraćaj ICMP paketa ECHO i ECHO_REPLY na nivou umreženog računara. Iz jezgra operativnog sistema uklanja se podrška za obradu ICMP paketa ECHO, a njima se bavi pingd pomoću sirove ICMP utičnice. U suštini, time se na sistemskom nivou obezbeđuje mehanizam kontrole ping paketa. Pingd postoji i za Linux, a možete ga preuzeti s adrese http://packetstorm.securify.com/UNIX/misc/pingd-0.5.1.tgz.

ICMP pretraživanje

Popularnost:	2
Jednostavnost:	9
Uticaj:	5
Stepen rizika:	5

Skeniranjem signala ping (ili pomoću ICMP paketa ECHO) možete otkriti samo vrh ledenog brega ukoliko vas zanimaju ICMP informacije o sistemu. Pomoću ICMP paketa, možete da saznate štošta o sistemu. Na primer, UNIX-ovom alatkom icmpquery (http://packetstorm.securify.com/UNIX/scanners/icmpquery.c) ili alatkom icmpush (http://packetstorm.securify.com/UNIX /scanners/icmpush22.tgz) možete da zahtevate sistemsko vreme (i na taj način utvrdite vremensku zonu u kojoj se sistem nalazi) tako što ćete mu poslati ICMP poruku tipa 13 (TIMESTAMP). Isto tako, možete da zahtevate mrežnu masku određenog ured aja ako mu pošaljete ICMP poruku tipa 17 (ADDRESS MASK). Maska mrežne kartice je izuzetno važna, jer preko nje možete da utvrdite koje se sve podmreže koriste. Kada to znate, napade možete da usmerite na pojedinačne podmreže preskačući, na primer, adrese predviđene za neusmereno slanje podataka. Icmpquery ima opcije i za otiskivanje sistemskog vremena i za zahtevanje maske adresa:

icmpquery <-query> [-B] [-f fromhost] [-d delay] [-T time] targets

where <query> is one of:

-t : icmp timestamp request (default)

-m : icmp address mask request

The delay is in microseconds to sleep between packets.

targets is a list of hostnames or addresses

-T specifies the number of seconds to wait for a host to

respond. The default is 5.

-B specifies 'broadcast' mode. icmpquery will wait

for timeout seconds and print all responses.

If you're on a modem, you may wish to use a larger -d and -T

Kada pomoću programa icmpquery želite da saznate sistemsko vreme usmerivača, izvršićete sledeću komandu:

[tsunami] icmpquery -t 192.168.1.1

192.168.1.1 : 11:36:19

Ako želite da saznate mrežnu masku usmerivača, izvršite komandu:

[tsunami] icmpquery -m 192.168.1.1

192.168.1.1 : 0xFFFFFFE0

NAPOMENA

Postoje usmerivači i sistemi koji ne dozvoljavaju odgovaranje na ICMP zahteve TIMESTAMP ili NETMASK, tako da će rezultati rada s programima *icmpquery* i *icmpush* varirati od sistema do sistema.

Mere zaštite od ICMP pretraživanja

Najbolja preventiva je da na graničnim mrežnim usmerivačima blokirate tipove ICMP paketa pomoću kojih se odaju informacije. Najmanje što treba da preduzmete jeste da onemogućite ulazak u mrežu paketa sa zahtevima TIMESTAMP (tip 13) i ADDRESS MASK (tip 17). Ako na obodu mreže koristite Cisco usmerivače, pomenuta ograničenja možete da sprovedete pomoću sledećih ACL lista:

access-list 101 deny icmp any any 13 ! timestamp zahtev

access-list 101 deny icmp any any 17 ! address mask zahtev

Ovakvu aktivnost može da uoči i sistem za otkrivanje upada, kao što je snort (www.snort.org). Naredni listing pokazuje kako snort signalizira da je otkrio upad:

[**] PING-ICMP Timestamp [**]

05/29-12:04:40.535502 192.168.1.10 -> 192.168.1.1

ICMP TTL:255 TOS:0x0 ID:4321

TIMESTAMP REQUEST

Otkrivanje usluga koje rade ili osluškuju

Dosad smo žive sisteme identifikovali automatskim ICMP ili TCP skeniranjem i prikupljali smo odre?ene ICMP informacije. Sada smo spremni za skeniranje priključaka svakog sistema.

Skeniranje priključaka

Popularnost:	10
Jednostavnost:	9
Posledice:	9
Procena rizika:	9

Skeniranje priključaka (engl. port scanning) postupak je povezivanja sa TCP i UDP priključcima ciljnog sistema da bi se utvrdilo koje su usluge aktivne ili u stanju osluškivanja (engl. listening). Pronalaženje priključaka koji osluškuju presudno je za određivanje vrste operativnog sistema i korišćenih aplikacija. Aktivne usluge mogu neovlašćenom korisniku da odobre pristup loše konfigurisanim sistemima, a mogu se otkriti i verzije programa sa bezbednosnim propustima. Alatke i tehnike za skeniranje priključaka poslednjih su godina znatno napredovale, ali mi ćemo se ograničiti na nekoliko najčešće korišćenih, koje mogu da nam obezbede obilje informacija. Sledeće tehnike za skeniranje priključaka razlikuju se od dosad opisanih, pomoću kojih smo samo utvrđivali da li je ciljni sistem živ. U nastavku ćemo poći od pretpostavke da su sistemi živi i pokušaćemo da otkrijemo sve aktivne priključke, jer su to potencijalne tačke pristupa našem cilju.

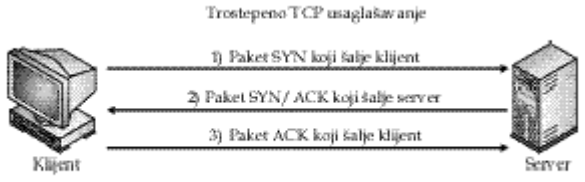
Kada skeniramo priključke ciljnog (ciljnih) sistema, treba da identifikujemo sledeće:

- TCP i UDP usluge koje su aktivne na ciljnom sistemu
- vrstu operativnog sistema
- specifične aplikacije ili verzije određenih usluga.

Vrste skeniranja

Pre nego što se prihvatimo neophodnih alatki, razmotrićemo različite tehnike skeniranja priključaka koje su nam na raspolaganju. Fyodor je jedan od pionira primene različitih tehnika skeniranja priključaka; mnoge od njih je ugradio u svoju alatku nmap. Veći deo tehnika skeniranja o kojima će biti reči razradio je upravo Fyodor.

- Skeniranje preko TCP spoja (engl. TCP connect scan) Ovim tipom skeniranja povezujemo se sa ciljnim priključkom i sprovodimo potpuno trostepeno usaglašavanje (SYN, SYN/ACK i ACK). Tu akciju ciljni sistem lako otkriva. Trostepeno TCP usaglašavanje prikazano je na slici 2-2.



Slika 2-2. (1) Slanje paketa SYN, (2) primanje paketa SYN/ACK i (3) slanje paketa ACK.

- Skeniranje tipa TCP SYN Ova tehnika se zove poluotvoreno skeniranje (engl. half-open

scanning), pošto se ne ostvaruje potpuna TCP veza, već se ciljnom priključku šalje paket SYN. Ako od priključka zatim primimo paket SYN/ACK, možemo da zaključimo da priključak osluškuje (da je u stanju LISTENING). Ako primimo paket RST/ACK, to obično znači da ciljni priključak nije aktivan. Zatim šaljemo paket RST/ACK tako da se potpuna veza nikada ne ostvaruje. Ova tehnika je diskretnija od ostvarivanja potpune TCP veze i ciljni sistem je možda neće zabeležiti.

- Skeniranje tipa TCP FIN Ovom tehnikom se ciljnom priključku šalje paket FIN. Prema dokumentu RFC 793 (http://www.ieft.org/rfc/rfc0793.txt), ciljni sistem treba da uzvrati paketom RST za sve priključke koji su zatvoreni. Tehnika obično radi samo sa UNIX-ovim TCP/IP stekovima.
- TCP skeniranje tipa "božićne jelke" (Xmas Tree) Ovom tehnikom se ciljnom priključku šalju paketi FIN, URG i PUSH. Prema dokumentu RFC 793, ciljni sistem treba da uzvrati paketom RST za sve zatvorene priključke.
- Nulto TCP skeniranje (Null) Ovom tehnikom se isključuju (resetuju) svi indikatori. Prema dokumentu 793, ciljni sistem treba da uzvrati paketom RST za svaki zatvoren priključak.
- Skeniranje tipa TCP ACK Ovom tehnikom se otkrivaju pravila zaštitne barijere. Njome se može utvrditi da li je zaštitna barijera samo filtar za pakete koji dozvoljava prolaz jedino za uspostavljene veze (veze sa uključenim bitom ACK) ili je reč o barijeri koja čuva informacije o sesiji, sa složenim mehanizmom propuštanja paketa.
- Skeniranje TCP prozora Ovom tehnikom se otkrivaju otvoreni kao i filtrirani/nefiltrirani priključci na nekim sistemima (na primer, na sistemima AIX i FreeBSD), a prema odstupanju koje se javlja u izveštaju o veličini TCP prozora.
- Skeniranje tipa TCP RPC Ova tehnika je specifična za sisteme UNIX i koristi se za otkrivanje i identifikovanje priključaka za daljinsko pozivanje procedura (Remote Procedure Call, RPC), programa koji su s njima povezani i verzija tih programa.
- Skeniranje tipa UDP Ovom tehnikom se ciljnom priključku šalje paket protokolom UDP. Ako ciljni priključak odgovori porukom "ICMP port unreachable", to znači da je priključak zatvoren. Ukoliko ne primimo takvu poruku, možemo da zaključimo da je priključak otvoren. Pošto je UDP poznat kao protokol kome ne treba povezivanje, preciznost ove tehnike umnogome zavisi od opterećenja mreže i sistemskih resursa. Pored toga, UDP skeniranje postaje veoma sporo ukoliko njime skenirate uređaj koji detaljno filtrira pakete. Ako UDP skeniranje želite da primenite putem Interneta, pripremite se na nepouzdane rezultate.

Izvesne realizacije protokola IP imaju neugodnu osobinu da uzvraćaju paketom RST za svaki skeniran priključak, bilo da se on osluškuje ili ne. Zbog toga rezultati koje dobijete takvim skeniranjem mogu da variraju; međutim, skeniranje tipa TCP SYN i skeniranje preko TCP spoja rade u svim slučajevima.

Identifikovanje aktivnih TCP i UDP usluga

Alatke za skeniranje priključaka su ključna komponenta snimanja sistema. Iako za UNIX i NT postoje brojne ovakve alatke, razmatranje ćemo ograničiti na one popularnije, koje su se s vremenom dokazale.

strobe

Strobe je osvedočeno dobar uslužni program za skeniranje TCP priključaka, a napravio ga je Julian Assange (ftp://ftp.FreeBSD.org/pub/FreeBSD/ports/distfiles/strobe-1.06.tgz). Taj program je jedan od najbržih i najpouzdanijih raspoloživih TCP skenera. U najvrednije osobine programa strobe spada njegova sposobnost da optimizuje sistemske i mrežne resurse i da ciljni sistem skenira efikasno. Pored toga, strobe u verziji 1.04 i novijima doslovno će oteti zaglavlje priključka s kojim se poveže (ukoliko postoji) i time omogućiti identifikovanje operativnog sistema računara i aktivnih usluga. Otimanje zaglavlja detaljnije objašnjavamo u poglavlju 3.

U rezultatima skeniranja strobe izlistava svaki aktivan TCP priključak:

[tsunami] strobe 192.168.1.10

strobe 1.03 © 1995 Julian Assange (proff@suburbia.net)

192.168.1.10 echo 7/tcp Echo [95, JBP]

192.168.1.10 discard 9/tcp Discard [94, JBP]

192.168.1.10 sunrpc 111/tcp rpcbind SUN RPC

192.168.1.10 daytime 13/tcp Daytime [93, JBP]

192.168.1.10 chargen 19/tcp ttytst source

192.168.1.10 ftp 21/tcp File Transfer [Control] [96, JBP]

192.168.1.10 exec 512/tcp remote process execution;

192.168.1.10 login 513/tcp remote login a la telnet;

192.168.1.10 cmd 514/tcp shell like exec, but automatic

192.168.1.10 ssh 22/tcp Secure Shell

192.168.1.10 telnet 23/tcp Telnet [112, JBP]

192.168.1.10 smtp 25/tcp Simple Mail Transfer [102, JBP]

192.168.1.10 nfs 2049/tcp networked file system

192.168.1.10 lockd 4045/tcp

192.168.1.10 unknown 32772/tcp unassigned

192.168.1.10 unknown 32773/tcp unassigned

192.168.1.10 unknown 32778/tcp unassigned

192.168.1.10 unknown 32779/tcp unassigned

192.168.1.10 unknown 32804/tcp unassigned

Iako je strobe veoma pouzdan program, treba znati i njegova ograničenja. To je samo TCP skener i ne može da skenira UDP priključke. Iako smo ga ranije koristili, pomoću njega smo videli samo polovičnu sliku. Osim toga, on skenira priključak samo preko TCP spoja. Premda to doprinosi pouzdanosti rezultata, ciljni sistem lako otkriva takvu aktivnost. Ako želimo nešto više od onoga što strobe može da ponudi, moramo da zavirimo dublje u kutiju s alatkama.

udp_scan

Pošto strobe skenira samo TCP priključke, možemo da upotrebimo udp_scan, program koji su 1995. napisali Dan Farmer i Wietse Venema. On potiče iz paketa SATAN (Security Administrator Tool for Analyzing Networks). Mada je paket SATAN pomalo demodiran, njegove alatke i danas rade sasvim dobro. Nove verzije paketa, sada pod imenom SAINT, mogu se naći na adresi http://wwdsilx.wwdsi.com. Mnogi drugi uslužni programi tako?e skeniraju UDP priključke, ali smo utvrdili da je udp_scan jedan od najpouzdanijih. Iako je udp_scan pouzdan, nezgodno je to što ga poznatiji IDS programi prepoznaju kao deo paketa SATAN. Prema tome, ova alatka ne spada baš u diskretne. Po pravilu, njome ćemo skenirati sve opštepoznate priključke ispod 1024 i određene visokorizične priključke iznad 1024.

[tsunami] udp_scan 192.168.1.1 1-1024

42:UNKNOWN:

53:UNKNOWN:

123:UNKNOWN:

135:UNKNOWN:

netcat

Još jedan odličan uslužni program je netcat ili nc, koji je napisao Hobbit (hobbit@avian.org). Budući da on može da obavi mnogo različitih poslova, kao i čuveni perorez "švajcarac", tako ćemo ga i nazivati u našoj kutiji s alatkama. U knjizi ćemo razmatrati mnoge od njegovih naprednih mogućnosti, a zasada samo navedimo osnovno skeniranje TCP i UDP priključaka. Opcijama -v i -vv dobijate detaljan ili veoma detaljan izveštaj. Opcijom -z obezbeđujete nulti U/I režim za skeniranje priključaka, a opcijom -w2 zadajete period neaktivnosti za svaku vezu. nc podrazumevano koristi protkol TCP. Prema tome, ako hoćemo da skeniramo UDP priključke, moramo da zadamo opciju -u, kao u drugom od sledećih primera.

[tsunami] nc -v -z -w2 192.168.1.1 1-140

[192.168.1.1] 139 (?) open

[192.168.1.1] 135 (?) open

[192.168.1.1] 110 (pop-3) open

[192.168.1.1] 106 (?) open

[192.168.1.1] 81 (?) open

[192.168.1.1] 80 (http) open

[192.168.1.1] 79 (finger) open

[192.168.1.1] 53 (domain) open

[192.168.1.1] 42 (?) open

[192.168.1.1] 25 (stmp) open

[192.168.1.1] 21 (ftp) open

[tsunami] nc -u -v -z -w2 192.168.1.1 1-140

[192.168.1.1] 135 (ntportmap) open

[192.168.1.1] 123 (ntp) open

[192.168.1.1] 53 (domain) open

[192.168.1.1] 42 (name) open

Network mapper (nmap)

Pošto smo opisali osnovne alatke za skeniranje priključaka, posebnu pažnju posvetićemo vrhunskoj alatki, programu nmap (Network Mapper). Fyodorov program *nmap* (http://www.insecure.org/nmap) obezbeđuje osnovno TCP i UDP skeniranje uz primenu opisanih tehnika. Retko se nalazi alatka koja u jednom paketu sadrži toliko mogućnosti. Ispitajmo neke od njenih najkorisnijih osobina.

[tsunami]# nmap -h

nmap V 2.53 Usage: nmap [Scan Type(s)] [Options] <host or net list>

Some Common Scan Types ('*' options require root privileges)

-sT TCP connect () port scan (default)

* -sS TCP SYN stealth port scan (best all-around TCP scan)

* -sU UDP port scan

-sP ping scan (Find any reachable machines)

* -sF, -sX, -sN Stealth FIN, Xmas, or Null scan (experts only)

-sR/-I RPC/Identd scan (use with other scan types)

Some Common Options (none are required, most can be combined):

* -O Use TCP/IP fingerprinting to guess remote operating system

-p <range> ports to scan. Example range: '1-1024, 1080, 6666, 31337'

-F Only scans ports listed in nmap-services

-v Verbose. Its use is recommended. Use twice for greater effect.

-P0 Dont' ping hosts (needed to scan www.microsoft.com and others)

* -Ddecoy_host1, decoy2[,...] Hide scan using many decoys

-T <Paranoid|Sneaky|Polite|Normal|Aggressive|Insane> General timing policy

-n/-R Never do DNS resolution/Always resolve [default: sometimes resolve]

-oN/-oM <logfile> Output normal/machine parsable scan logs to <logfile>

-iL <inputfile> Get targets from file; Use '-' for stdin

* -S <your_IP>/-e <devicename> Specify source address or network interface

-- interactive Go into interactive mode (then press h for help)

[tsunami] nmap -sS 192.168.1.1

Starting nmap V. 2.53 by fyodor@insecure.org

Interesting ports on (192.168.1.11):

(The 1504 ports scanned but not shown below are in state: closed)

Port State Protocol Service

21 open tcp ftp

25 open tcp smtp

42 open tcp nameserver

53 open tcp domain

79 open tcp finger

80 open tcp http

81 open tcp hosts2-ns

106 open tcp pop3pw

110 open tcp pop-3

135 open tcp loc-srv

139 open tcp netbios-ssn

443 open tcp https

nmap ima i druga svojstva koja treba da ispitamo. Videli smo sintaksu koja se koristi pri skeniranju jednog sistema. Međutim, uz nmap ćemo lako skenirati i celu mrežu. On omogućava da u sistem unesemo opseg adresa koristeći CIDR (Classless Inter-Domain Routing) konvenciju za obeležavanje blokova (pogledajte RFC 1519 - http://www.ietf.org/rfc/rfc1519.txt). To je pogodan format koji nam dozvoljava da oblast zadamo npr. ovako: 192.168.1.1-192.168.1.254. Obratite pažnju i na to da smo opcijom -o naložili programu da rezultat sačuva u zasebnoj datoteci. Opcijom -oN rezultati bi bili snimljeni u čitljivom formatu.

[tsunami]# nmap -sF 192.168.1.0/24 -oN outfile

Ako želite da rezultati u datoteci budu razdvojeni znakom tabulatora kako biste kasnije mogli da ih obra?ujete nekom alatkom, upotrebite opciju -oM. Pošto od ovakvog tipa skeniranja očekujemo mnogo informacija, uvek je pametno da ih snimimo u datoteku. Ponekad će biti korisno da kombinujete opcije -*oN* i - *oM* da biste rezultate snimili u oba formata.

Pretpostavimo da ste posle opipavanja odre?ene organizacije utvrdili da se u njoj kao primarna zaštitna barijera koristi jednostavan ure?aj za filtriranje paketa. Tada možemo da upotrebimo opciju -f programa nmap da bismo pakete usitnili. Ovom opcijom se zaglavlje TCP paketa razbija na više paketa, što uređaju za kontrolu pristupa ili IDS sistemu može da oteža otkrivanje skeniranja. Savremeni uređaji za filtriranje paketa i programske zaštitne barijere najčešće poređaju sve IP fragmente u niz pre nego što ih provere. Stariji ure?aji za kontrolu pristupa ili uređaji od kojih se zahteva maksimalan učinak možda neće ponovo objediniti pakete pre nego što ih propuste.

U zavisnosti od složenosti ciljne mreže i njenih računara, skeniranje koje smo do sada analizirali lako može biti otkriveno. Opcija -D programa nmap zatrpava ciljne lokacije nevažnim informacijama, čime otežava otkrivanje napadača. Osnovni preduslov za uspeh ove opcije jeste da se lažno skeniranje aktivira istovremeno kada i pravo. To se postiže imitiranjem izvornih adresa i mešanjem lažnog skeniranja s pravim skeniranjem priključka. Ciljni sistem će tada odgovarati i na lažne adrese i na pravo skeniranje. Pored toga, ciljna lokacija ima dodatni posao da prati sva skeniranja i da pokuša da razluči koje je lažno a koje pravo. Imajte na umu da lažna adresa mora postojati (biti aktivna) ili ćete skeniranjem ciljni sistem preplaviti SYN paketima i stvoriti uslove za uskraćivanje usluga.

[tsunami] nmap -sS 192.1681.1 -D 10.1.1.1

www.target_web.com,ME -p25, 139, 443

Starting nmap V. 2.53 by fyodor@insecure.org

Interesting ports on (192.168.1.1):

Port State Protocol Service

25 open tcp smtp

443 open tcp https

Nmap run completed -- 1 IP address (1 host up) scanned in 1 second

U navedenom primeru, nmap izvodi i lažno skeniranje kako bi otežao otkrivanje pravog.

Druga korisna osobina ovog programa jeste tzv. identifikaciono skeniranje (engl. ident scanning). Skeniranje ident (RFC 1413 - http://www.ietf.org/rfc/rfc1413.txt) služi za utvrđivanje identiteta korisnika određenog TCP priključka, a to se postiže razmenom informacija s priključkom 113. Mnoge verzije identa uzvratiće imenom vlasnika procesa koji se odvija kroz taj određeni priključak. Me?utim, ovakvo skeniranje je najuspešnije protiv sistema UNIX.

[tsunami] nmap -I 192.168.1.10

Starting nmap V. 2.53 by fyodor@insecure.org

Port State Protocol Service Owner

22 open tcp ssh root

25 open tcp smtp root

80 open tcp http root

110 open tcp pop-3 root

113 open tcp auth root

6000 open tcp X11 root

Obratite pažnju na to da iz rezultata skeniranja možemo da utvrdimo vlasnika svakoga procesa. Pronicljiv čitalac će uočiti da Web server radi s administrativnim ovlašćenjima, a ne kao korisnik bez posebnih ovlašćenja, npr. nobody. Takva bezbednosna praksa je vrlo loša. Izvođenjem identifikacionog skeniranja saznajemo da će napadači biti nagra?eni administratorskim privilegijama ukoliko provale u Web server i uspeju da izvršavaju komande.

Poslednja tehnika koju razmatramo jeste skeniranje preko FTP posrednika (engl. FTP bounce scanning). Na taj napad ukazao je Hobbit. U svojoj poruci iz 1995. na Bugtraqu (http://www.securityfocus.com/templates/archive.pike?list=1&msg= 199507120620.CAA18176@narq.avian.org), on je istakao neke unutrašnje propuste protokola FTP (RFC 959 - http://www.ietf.org/rfc/rfc0959.txt). Napad preko FTP posrednika je u suštini lukava metoda razotkrivanja veza preko FTP servera zloupotrebljavanjem podrške za zastupničke FTP veze. Kao što je Hobbit naglasio u pomenutoj poruci, napadi preko FTP posrednika "mogu da se upotrebe za: slanje poruka elektronske pošte i diskusionih grupa čiji se izvor praktično ne može utvrditi; vršenje pritiska na servere na različitim lokacijama; prepunjavanje diskova; pokušaje zaobilaženja zaštitne barijere - i istovremeno su neprijatni i teško se utvr?uju". Štaviše, preko FTP posrednika možete i da skenirate priključke i da tako prikrijete svoj identitet ili, što je još bolje, da zaobi?ete mehanizme kontrole pristupa.

Naravno, program nmap podržava ovu vrstu skeniranja svojom opcijom -b, ali za to mora biti ispunjeno nekoliko uslova. Najpre, FTP server mora da ima direktorijum u koji je dozvoljeno upisivanje i iz koga se može čitati, npr. direktorijum /incoming. Zatim, FTP server mora da dopusti programu nmap da mu komandom PORT pruži lažne informacije o priključku. Premda opisana tehnika može da bude veoma efikasna pri zaobilaženju mehanizma kontrole pristupa i za prikrivanje identiteta počinioca, ona može da bude i veoma spora. Osim toga, mnoge nove verzije FTP servera ne dozvoljavaju ovu vrstu zlonamerne aktivnosti.

Pošto smo prikazali na delu neophodne alatke za skeniranje priključaka, treba da objasnimo i kako se

analiziraju podaci dobijeni svakom od njih. Bez obzira na to koju alatku koristimo, uvek pokušavamo da otkrijemo otvorene priključke kroz koje cure informacije o operativnom sistemu. Na primer, kada su otvoreni priključci 139 i 135, ciljni operativni sistem je skoro sigurno Windows NT, jer on uobičajeno osluškuje na ta dva priključka. To je razlika izme?u njega i Windowsa 95/98 koji osluškuju samo na priključku 139.

Ako nastavimo da pregledamo rezultat koji nam je isporučio strobe, utvržujemo da su na ciljnom sistemu aktivne mnoge usluge. Ako bi trebalo da pogažamo najbolje što umemo, rekli bismo da sistem radi pod UNIX-om. Do tog zaključka dolazimo zato što vidimo server za mapiranje priključaka (111), priključak za usluge Berkeley R (512-514), NFS (2049) i priključke viših brojeva, počev od 3277X. Postojanje takvih priključaka obično znači da se na sistemu izvršava UNIX. Štaviše, ako bi trebalo da pogažamo i varijantu UNIX-a, rekli bismo da je u pitanju Solaris, pošto znamo da on RPC usluge obično izvršava u oblasti 3277X. Imajte, ipak, na umu da to samo pretpostavljamo i da na sistemu ne mora da bude Solaris.

Jednostavnim skeniranjem TCP i UDP priključaka moći ćemo lako da dožemo do pretpostavki o izloženosti sistema koji ciljamo. Primera radi, ako je priključak 139 otvoren na Windows NT serveru, on može da bude izložen velikom riziku. U poglavlju 5 razmatramo uroženu ranjivost Windowsa NT i objašnjavamo kako se priključak 139 može iskoristiti za ugrožavanje bezbednosti sistema. I UNIX sistem u našem primeru je izložen riziku, jer se sa aktivnim uslugama može svašta raditi, a poznato je i da imaju mnoge ranjive tačke. Na primer, usluga daljinskog pozivanja procedura (engl. Remote Procedure Call, RPC) i usluga mrežnog sistema datoteka (engl. Network File System, NFS) dva su glavna puta preko kojih potencijalni napadač može da ugrozi bezbednost UNIX servera (više o tome u poglavlju 8). S druge strane, uslugu daljinskog pozivanja nije moguće ugroziti ukoliko nije aktivna. Prema tome, zapamtite da veći broj aktivnih usluga u sistemu povećava verovatnoću njegovog ugrožavanja.

Skeneri priključaka koji rade pod Windowsom

Dosad je bilo reči o skenerima priključaka sa aspekta korisnika UNIX-a, ali znači li to da korisnici Windowsa neće moći da se zabavljaju? Naravno da ne znači - sledeće alatke za skeniranje priključaka nalaze se na samom vrhu naše kutije s alatkama zato što su brze, tačne i svestrane.

NetScanTools Pro 2000

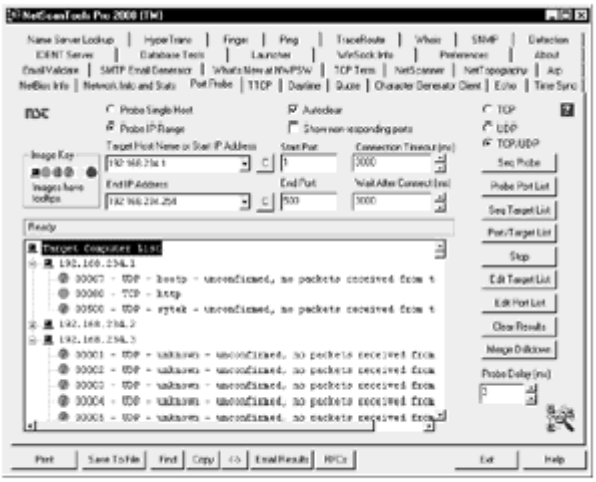
Jedna od najkorisnijih alatki za razotkrivanje mreža, NetScanTools Pro 2000 (NSTP2K), nudi skoro svaku zamislivu uslugu unutar jedinstvenog okruženja: DNS pretraživanje koje obuhvata nslookup i dig uz axfr, *whois* , automatsko skeniranje signalom ping, skeniranje tabela NetBios imena, SNMP šetnje i još mnogo toga. Program može da radi više poslova uporedo. Možete da skenirate priključke jedne mreže, dok istovremeno otkrivate aktivne računare na drugoj mreži (tako nešto ne preporučujemo za velike mreže, osim ako ste izuzetno strpljivi).

NetScanTools Pro 2000, na kartici Port Probe, ima i jedan od najboljih skenera priključaka koji radi pod Windowsom. Moć tog programa ogleda se u fleksibilnom zadavanju cilja i priključaka (i ciljne IP adrese i liste priključaka mogu da se uvezu iz tekstualnih datoteka), podršci za TCP i UDP skeniranje (mada ne selektivno u pogledu priključaka) i brzini izvršavanja višenitnih procesa. Loše je to što rezultat daje u pomalo nezgrapnom obliku koji se teško analizira pomoću skriptova ili alatki za rad s podacima. Naravno, zbog grafičke prirode, ovaj program se ne može uključiti u skript. Poželeli bismo i da se rezultat neke funkcije (npr. NetScanner) može direktno proslediti drugoj (kao što je Port Probe).

Sve u svemu, NSTP2K (http://www.nwpsw.com) jeste profesionalno napisan program koji se redovno ažurira servisnim paketima, ali je ipak skuplji od konkurenata. Osiromašena verzija, nazvana NetScanTools (aktuelna verzija 4), može se besplatno isprobavati 30 dana, ali po

mogućnostima nije ni blizu verzije Pro 2000. (Na primer, ona ne izvodi UDP skeniranje.)

Kada koristite program NSTP2K, setite se da na kartici IDENT Server deaktivirate server za identifikaciju, da iz TCP priključka 113 ne biste slušali odgovore kad god "ispalite" paket prema njemu. Slika 2-3 prikazuje NSTP2K prilikom skeniranja mreže osrednjeg opsega.

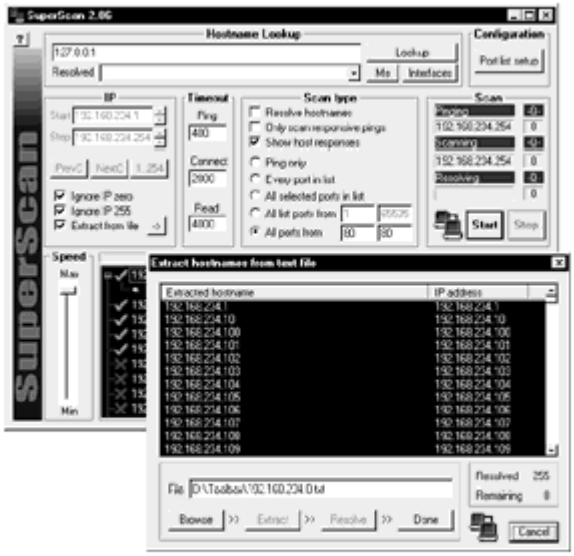


Slika 2-3. NetScan Tools Pro 2000 je jedna od najbržih, najfleksibilnijih Windowsovih alatki za razotkrivanje mreža i skeniranje priključaka.

SuperScan

Program SuperScan firme Foundstone može se preuzeti s adrese http://www.foundstone.com/rdlabs/termsofuse.php?filename=superscan.exe. To je još jedan brz i fleksibilan skener TCP priključaka s vrlo prihvatljivom cenom - besplatan je. Kao i NSTP2K, on omogućava fleksibilno zadavanje ciljnih IP adresa i lista priključaka. Posebno je zgodna opcija Extract From File (slika 2-4). Ona je najbolje opisana u sistemu pomoći, iz koga navodimo jedan pasus da biste se uverili kako ta alatka može da vam uštedi vreme:

"Pomoću opcije Extract From File, program čita bilo koju tekstualnu datoteku i iz nje izvlači ispravne IP adrese i imena računara. Program je veoma inteligentan kada pronalazi ispravna imena računara u tekstu, ali će možda biti potrebno da prethodno iz teksta uklonite zbunjujuće delove. Možete da pritisnete Browse and Extract koliko god puta želite, koristeći svaki put druge datoteke, i program će uvek dodati nova imena na listu. Duplikati se automatski uklanjaju. Kada prona?ete sva imena računara, pritiskom na dugme Resolve pretvorićete ih u brojčane IP adrese i tako ih pripremiti za skeniranje priključaka."



Slika 2-4. Funkcija Extract From File programa SuperScan zaista je svestrana – iz tekstualne datoteke uvozi imena računara i IP adrese. Ako ima više datoteka, napraviće zbirnu listu pripremljenu za skeniranje priključaka.

Ništa ne može biti lakše od toga, što se i vidi na slici 2-4. SuperScan sadrži i najiscrpnije liste priključaka koje smo dosad videli. Priključke možete, dodatno, ručno da birate i da ih uklanjate iz liste i tako što detaljno podesite program. SuperScan je i veoma brz.

WinScan

WinScan, program koji je napisao Sean Mathias iz firme Prosolve (http://www.prosolve.com), besplatan je skener TCP priključaka koji se isporučuje i u grafičkoj verziji (winscan.exe) i u verziji koja radi sa komandne linije (scan.exe). Verziju koja radi sa komandne linije primenjujemo rutinski u skriptovima zato što ona može da skenira mreže klase C i daje rezultat koji se lako programski analizira. Pomoću uslužnih programa strings, tee i tr firme Mortice Kern Systems Inc. (http://www.mks.com), sledećom komandom s konzole Windowsa NT mogu se skenirati opštepoznati priključci u opsegu 0-1023 na mreži i rezultati dobiti u tri kolone razdvojene dvotačkom (IP adresa:ime usluge:priključak):

scan.exe -n 192.168.7.0 -s 0 -e 1023 -f | strings | findstr |

/c:"/tcp" | tr \011\040 : | tr -s : : | tee -ia results.txt

Parametar -f programa scan.exe ne bi trebalo koristiti ako su veze spore, jer rezultati mogu da budu nepouzdani. Rezultati našeg skripta izgledaju približno ovako:

192.168.22.5:nbsession:139/tcp

192.168.22.16:nbsession:139/tcp

192.168.22.32:nbsession:139/tcp

Zahvaljujemo se Patricku Heimu i Jasonu Glassbergu na ovoj "kratkoj" komandi.

ipEye

Nemojte misliti da vam trebaju isključivo Linux i nmap da biste izveli neuobičajena skeniranja. Program ipEye Arnea Vidstroma (http://ntsecurity.nu) iz Windowsove komandne linije skenira

priključke i sprovodi skeniranje tipa SYN, FIN i tipa božićne jelke. Ograničenja ove zgodne alatke su što radi samo pod Windowsom 2000 i što računare skenira jedan po jedan. Evo primera rezultata ovoga programa posle SYN skeniranja TCP priključka 20 s namerom da se izbegnu pravila filtriranja na mrežnoj skretnici, slično onome što bismo postigli primenom opcije -g programa nmap:

C:\Toolbox>ipeye.exe 192.168.234.110 -syn -p 1 1023 -sp 20

ipEye 1.1 - (c) 2000, Arne Vidstrom (arne.vidstrom@ntsecurity.nu)

- http://ntsecurity.nu/toolbox/ipeye/

1-52 [closed or reject]

53 [open]

54-87 [closed or reject]

88 [open]

89-134 [closed or reject]

135 [open]

136-138 [closed or reject]

139 [open]

...

636 [open]

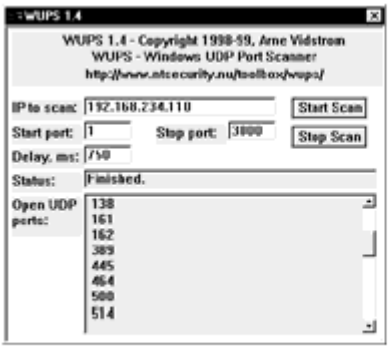
637-1023 [closed or reject]

1024-65535 [not scanned]

Pošto su mnoge liste za kontrolu pristupa usmerivača i zaštitnih barijera podešene tako da dozvoljavaju ulazni saobraćaj za usluge poput DNS (UDP 53) i FTP (TCP 20), SMTP (TCP 25) i HTTP (TCP 80), skener priključaka može da izbegne kontrolu maskirajući pakete u dolazni saobraćaj takve vrste. Međutim, morate znati adresni prostor iza zaštitne barijere ili usmerivače, što nije lako ukoliko se preslikavaju mrežne adrese (engl. Network Address Translation, NAT).

WUPS

Skener UDP priključaka za Windows (Windows UDP Port Scanner, WUPS), koji je tako?e napisao Arne Vidstrom, može se naći na adresi http://ntsecurity.nu. To je pouzdan, grafički orijentisan i relativno brz (zavisno od parametra zadrške) skener UDP priključaka, iako u jednom trenutku može da skenira samo sekvencu zadatih priključaka na jednom računaru. To je solidna alatka za brzo i "prljavo" UDP skeniranje ciljnog računara (slika 2-5).



Slika 2-5. Windowsov skener UDP priključaka (WUPS) ispituje sistem na kome se izvršava usluga SNMP (UDP 161).

Sažetak skeniranja priključaka

Tabela 2-2 prikazuje spisak popularnih programa za skeniranje priključaka i njihovih mogućnosti.

Tabela 2-2. Popularne alatke za skeniranje i njihove osobine

Skener	TCP	UDP	Nevidljivost	Izvor
UNIX				
Strobe	X			ftp://ftp.FreeBSD.org/pub/FreeBSD/ports/distfiles/strobe-1.06.tgz
Tcp_scan	X			http://wwdsilx.wwdsi.com/saint/
Udp_scan		X		http:// wwdsilx.wwdsi.com/saint/
Nmap	X	X	X	http://www.inscure.org/nmap
Netcat	X	X		http://packetstorm.securify.com/UNIX/utilities/nc110.tgz
Windows				
Netcat	X	X *		http://www.atstake.com/research/tools/nc11nt.zip
NetScanTools Pro 2000	X	X		http://www.nwpsw.com
SuperScan	X			http://members.home.com/rkeir/software.html
WinScan	X			http://www.prosolve.com
IpEye	X			http://ntsecurity.nu
WUPS		X		http://ntsecurity.nu
Fscan	X	X		http://www.foundstone.com/rdlabs/termsofuse.php?filename=fscan.exe

* Upozorenje: Netcatovo UDP skeniranje ne radi pod NT-om, pa se ne oslanjajte na njega.

Mere zaštite od skeniranja priključaka

Otkrivanje Napadači često skeniraju priključke da bi na udaljenom sistemu otkrili TCP i UDP priključke koji osluškuju. Otkrivanje te aktivnosti je od presudne važnosti za donošenje zaključka o tome kada će se napad dogoditi i ko će ga izvršiti. Osnovne metode za otkrivanje skeniranja priključaka jesu sistemi za otkrivanje upada, kao što su snort i RealSecure firme Internet Security System.

Snort (http://www.snort.org) jeste odličan program za otkrivanje upada, posebno stoga što se često objavljuju dopunski potpisi napada i što je besplatan. Možda ste dosad već shvatili da je to jedan od

naših omiljenih sistema za otkrivanje upada. (Zapamtite da verzije 1.x ne rade dobro sa usitnjenim paketima.) Evo dela listinga jednog pokušaja skeniranja priključaka:

[**] spp_portscan: PORTSCAN DETECTED from 192.168.1.10 [**]

05/22-18:48:53.681227

[**] spp_portscan: portscan status from 192.168.1.10:

4 connections across 1 hosts: TCP(0), UDP (4) [**]

05/22-18:49:14.180505

[**] spp_portscan: End of portscan from 192.168.1.10 [**]

05/22-18:49:34.180236

Što se tiče UNIX-a, nekoliko uslužnih programa kao što je scanlogd (http://www.openwall.com/scanlogd/), koji rade na pojedinačnim računarima, mogu da otkriju i da zabeleže opisane napade. Štaviše, Psionicov PortSentry iz projekta Abacus (http://www.psionic.com/abacus/) može tako da otkrije aktivan napad i odgovori na njega. Jedan način odgovaranja na pokušaj skeniranja priključaka jeste da se automatski uspostave pravila filtriranja na nivou jezgra operativnog sistema, uz dodato pravilo za zabranu pristupa iz smera napadačkog sistema. Takvo pravilo se utvrđuje u konfiguracionoj datoteci programa PortSentry; ono će se razlikovati od sistema do sistema. Za računar pod Linuxom 2.2.x čiju zaštitnu barijeru podržava jezgro operativnog sistema, pomenuto pravilo u datoteci portsentry.conf izgledaće ovako:

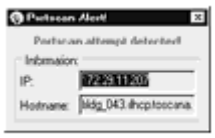
New ipchain support for Linux kernel version 2.102+

KILL_ROUTE="/sbin/ipchains -I input -s $TARGET$ -j DENY -l"

PortSentry radi s većinom UNIX-ovih varijanti, računajući i Solaris. Ako prepoznate šemu skeniranja priključaka s određenog sistema ili mreže, setite se da to možda znači da neko pokušava da upozna mrežu vaše lokacije. Obratite dužnu pažnju na takvu aktivnost, jer posle nje može da usledi napad iz svih oružja. Imajte na umu i to da nije dobro da aktivno uzvraćate ili blokirate pokušaje skeniranja priključaka, jer će napadač verovatno upotrebiti IP adresu nekog drugog sistema, tako da će vaš protivnapad biti preusmeren na nevine sisteme. Odličan članak o tome, koji je napisao Solar Designer, nalazi se na adresi http://www.openwall.com/scanlogd/P53-13.gz. U njemu su predočeni i dodatni saveti za napadanje i projektovanje sistema koji otkrivaju skeniranje priključaka.

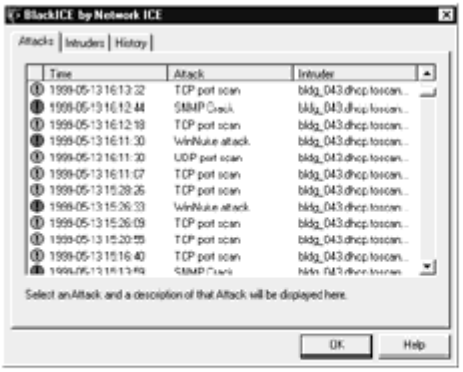
Zaštitne barijere bi trebalo da budu tako podešene da otkrivaju pokušaje skeniranja priključaka. Neke u tome uspevaju bolje od drugih. Na primer, mnoge zaštitne barijere imaju definisane opcije za otkrivanje SYN skeniranja, dok potpuno zanemaruju FIN skeniranje. Najteži deo otkrivanja takve aktivnosti jeste pretresanje gomile datoteka s izveštajima; za to preporučujemo Psionicov Logcheck (http://www.psionic.com/abacus/logcheck/). Preporučujemo i da svoje senzore tako podesite da vas preko elektronske pošte odmah obaveštavaju o incidentima. Kad god je moguće, primenite beleženje uz graničnu vrednost (engl. threshold logging) kako napadač ne bi pokušao da izvede napad uskraćivanja usluge, prepunjavajući vam poštansko sanduče. Beleženjem uz graničnu vrednost, pozivi na uzbunu se grupišu i šalje se informacija o svima zajedno, umesto da se sistem uzbunjuje pri svakom pojedinačnom znaku mogućeg sondiranja sistema. Minimum mera bezbednosti podrazumeva sistem izveštavanja zasnovan na izuzecima koji bi vas upozoravao da neko skenira priključke lokacije. Lance Spitzner (http://www.enteract.com/~lspitz/intrusion.html) napravio je alert.sh, uslužni program prilago?en zaštitnoj barijeri Firewall-1, koji otkriva i prati skeniranje priključaka kroz Firewall-1 i izvršava se kao korisnički alarm (User Defined Alert).

Što se tiče Windowsa NT, postoji nekoliko uslužnih programa koji mogu da otkriju jednostavno skeniranje priključaka. Prvi takav program je Genius 2.0 firme Independent Software (http://www.indiesoft.com/). Genius 3.0 je objavljen za Windows 95/98 i Windows NT 4.0. Osim što otkriva jednostavno skeniranje TCP priključaka, on može i štošta drugo, ali i njegova osnovna funkcija opravdava da ga dodate u sistemsku paletu. Genius će tokom zadatog perioda osluškivati sve zahteve za otvaranje priključaka, a kada otkrije skeniranje, otvoriće upozoravajući okvir za dijalog s napadačevom IP adresom i DNS imenom:



Genius otkriva i uobičajene TCP veze i skeniranje tipa SYN.

Drugi program koji otkriva skeniranje priključaka na Windowsu jeste BlackICE (slika 2-6) firme Network ICE (http://www.networkice.com). To je prvi proizvod koji koristi programske agente za otkrivanje upada i namenjen je verzijama Windowsa 9x i NT. On se mora kupiti, ali Network ICE namerava da ponudi i besplatnu verziju. Na kraju, pomenimo ZoneAlarm (http://www.zonelabs.com/), moćan Windows program koji objedinjuje funkcionalnost zaštitne barijere i IDS sistema. ZoneAlarm je besplatan kada se koristi za lične potrebe.



Slika 2-6. Osim što otkriva skeniranje TCP priključaka, BlackICE nudi i neke napredne potpise za otkrivanje upada, obuhvatajući UDP skeniranje, anonimne sesije, pcAnywhere ping, WinNuke, ECHO skeniranje, otkrivanje putanja, Smurf i mnoge druge napade.

Sprečavanje Premda je teško sprečiti nekoga da skeniranjem priključaka izvi?a vaš sistem, izloženost neprijatelju možete da umanjite ako deaktivirate sve nepotrebne usluge. To u UNIX-ovom okruženju možete da izvedete tako što ćete u datoteci /etc/inetd.confg nepotrebne usluge pretvoriti u komentare i deaktivirati ih u skriptovima za pokretanje sistema. Taj postupak ćemo detaljnije razmotriti u poglavlju 8.

I u Windowsu NT treba da deaktivirate sve usluge koje nisu neophodne. To je mnogo teže zbog načina na koji NT radi, budući da je u njemu priključak 139 veoma zaposlen. Me?utim, neke usluge možete da deaktivirate iz menija Control Panel | Services. O opasnostima po Windows NT i merama zaštite koje možete da preduzmete detaljno pišemo u poglavlju 5. Osim toga, Tiny Software (www.tinysoftware.com) nudi sjajan modul za jezgro operativnog sistema Windowsa NT koji filtrira pakete i omogućava da zaštitite mnoge osetljive priključke.

Ako imate drugačiji računar ili operativni sistem, morate pogledati odgovarajući priručnik da biste saznali kako da smanjite broj aktivnih priključaka na zaista neophodnu meru.

Prepoznavanje operativnog sistema

Kao što smo dosad pokazali, raspolažemo mnogim alatkama i raznim tehnikama skeniranja. Ako se sećate, prvi cilj skeniranja priključaka bio je da na napadnutom sistemu otkrijemo TCP i UDP aktivne priključke. Sada će naš cilj biti da prepoznamo operativni sistem koji skeniramo.

Prepoznavanje operativnog sistema

Popularnost:	10
Jednostavnost:	8
Uticaj:	4
Stepen rizika:	7

Tokom faze otkrivanja ranjivosti računara, što ćemo obrazložiti u narednim poglavljima, trebaće nam specifični podaci o njegovom operativnom sistemu. Uvek moramo misliti na to da u stvari pokušavamo što tačnije odrediti ranjivost ciljnog sistema. Prema tome, moramo biti prilično ube?eni u to da smo u stanju da identifikujemo ciljni operativni sistem. Možemo da primenimo jednostavne tehnike otimanja zaglavlja (opisujemo ih u poglavlju 3), koje će prikupiti informacije o uslugama, kao što su FTP, telnet, SMTP, HTTP, POP i dr. To je najjednostavniji način otkrivanja operativnog sistema i s njim povezanih verzija aktivnih usluga. Dabome, postoje i alatke koje će nam u tome pomoći. Dve od najpreciznijih alatki kojima raspolažemo jesu svemoćni nmap i program queso, a oba podjednako omogućavaju da uzmemo otisak steka.

Uzimanje otiska aktivnog steka

Pre nego što pokrenemo nmap ili queso, treba da objasnimo značenje termina "otisak steka". Uzimanje otiska steka (engl. stack fingerprinting) izuzetno je moćna tehnologija pomoću koje s visokim stepenom sigurnosti možete da sudite o operativnom sistemu umreženog računara. Postoje brojne sitne razlike u realizaciji IP steka raznih proizvo?ača. Proizvo?ači prilikom pisanja TCP/IP steka često različito tumače odre?ene RFC preporuke. Analizom tih razlika možemo prilično pouzdano da pogodimo o kom se operativnom sistemu radi. Da bi se dobio maksimalno verodostojan rezultat, za uzimanje otiska steka nužno je da postoji makar jedan priključak koji osluškuje. Nmap će pokušati, kako najbolje ume, da pogodi aktivan operativni sistem, čak i ako nije otvoren nijedan priključak. Me?utim, rezultati neće biti pouzdani. Č;lanak u kome je ova tema iscrpno analizirana napisao je Fyodor, a objavljen je u časopisu Phrack Magazine; sada se može naći na adresi http://www.insecure.org/nmap/nmap-fingerprinting-article.html.

Sledi opis oru?a pomoću kojih se može razlučiti o kom se operativnom sistemu radi:

- Sonda FIN Paket FIN se šalje otvorenom priključku. Kao što je ranije predočeno, ako se poštuje dokument RFC 793, priključak ne bi trebalo da odgovori. Me?utim, mnoge realizacije steka (npr. kod Windowsa NT) odgovoriće signalom FIN/ACK.
- Sonda s lažnim indikatorom U TCP zaglavlju paketa SYN zadaje se nedefinisani TCP indikator. Neki operativni sistemi, npr. Linux, kao odgovor će poslati paket sa istim indikatorom.
- Uzorkovanje broja inicijalnog niza (Initial Sequence Number, ISN) Osnovna pretpostavka je da će se otkriti šema u inicijalnom nizu koji je TCP realizacijom izabran za odgovaranje na zahtev za povezivanje.
- Traženje bita "ne usitnjavaj" Neki operativni sistemi, radi poboljšanja performansi, uključuju bit "ne usitnjavaj".

- Početna veličina TCP prozora Prati se početna veličina prozora na vraćenim paketima. U nekim realizacijama steka ta veličina je jedinstvena i može da pruži presudna obaveštenja tokom uzimanja otiska.
- Vrednost ACK IP stekovi za polje ACK koriste različit redni broj, tako da će vam neke realizacije vratiti vrednost koju ste poslali, a druge će je uvećati za 1.
- Prigušivanje poruka o ICMP greškama Operativni sistemi mogu da slede dokument RFC 1812 (www.ietf.org/rfc/rfc1812.txt) i da ograniče učestalost slanja poruka o greškama. Ako šaljete UDP pakete nekom priključku s proizvoljno izabranim visokim brojem, moći ćete da prebrojite poruke koje su se u zadatom intervalu vratile neisporučene.
- Tekst ICMP poruke Operativni sistemi daju različita obaveštenja kada do?e do ICMP greške. Analizom teksta poruke možete da pretpostavite o kom se operativnom sistemu radi.
- Integritet u odrazu poruke o ICMP grešci Neke realizacije steka mogu da izmene IP zaglavlja kada povratno šalju poruku o ICMP grešci. Ispitujući izmene u zaglavljima možete da pravite pretpostavke o ciljnom operativnom sistemu.
- Vrsta usluge (Type of service, TOS) Kada se dobije poruka "ICMP port unreachable", ispituje se TOS. U većini realizacija steka ova vrednost je 0, ali može da bude i drugačije.
- Rad sa usitnjenim paketima Kao što su Thomas Ptacek i Tim Newsham istakli u svom znamenitom članku "Uskakanje, izbegavanje i uskraćivanje usluga: izmicanje otkrivanju upada u mrežu" (http://www.clark.net/~roesch/idspaper.html), različiti stekovi različito rukuju s delovima paketa koji se preklapaju. Neki stekovi će pri ponovnom sastavljanju paketa nove podatke upisati preko starih i obrnuto. Analizom načina na koji je sondažni paket ponovo sastavljen, moći ćete da donosite sudove o ciljnom operativnom sistemu.
- TCP opcije Ove opcije su prvobitno definisane dokumentom RFC 793, a ažurirane su u dokumentu 1323 (www.ietf.org/rfc/rfc1323.txt). Naprednije opcije iz dokumenta RFC 1323 sve su brojnije u savremenim realizacijama steka. Kada pošaljete paket s više takvih opcija (npr. za "prazan hod" - NOP, maksimalnu veličinu segmenta, faktor uvećanja prozora ili za otiskivanje sistemskog vremena), moći ćete da pravite odre?ene pretpostavke o prirodi ciljnog operativnog sistema.

Opcija -O programa nmap obuhvata pomenute tehnike (osim rada sa usitnjenim paketima i prigušivanja poruka o ICMP greškama). Razmotrimo kako u tom pogledu stoji naša ciljna mreža:

[tsunami] #nmap -O 192.168.1.10

Starting nmap V. 2.53 by fyodor@insecure.org

Interesting ports on shadow (192.168.1.10):

Port State Protocol Service

7 open tcp echo

9 open tcp discard

13 open tcp daytime

19 open tcp chargen

21 open tcp ftp

22 open tcp ssh

23 open tcp telnet

25 open tcp smtp

37 open tcp time

111 open tcp sunrpc

512 open tcp exec

513 open tcp login

514 open tcp shell

2049 open tcp nfs

4045 open tcp lockd

TCP Sequence Prediction: Class=random positive increments

Difficulty=26590 (Worthy challenge)

Remote operating system guess: Solaris 2.5, 2.51

Koristeći opciju programa nmap za uzimanje otiska steka, lako ćemo i tačno utvrditi vrstu ciljnog operativnog sistema. Č;ak i ako na njemu nema otvorenih priključaka, nmap će pokušati da ga pogodi:

[tsunami]# nmap -p80 -O 10.10.10.10

Starting nmap V. 2.53 by fyodor@insecure.org

Warning: No ports found open on this machine, OS detection will be MUCH less reliable

No ports open for host (10.10.10.10)

Remote OS guesses: Linux 2.0.27 - 2.0.30, Linux 2.0.32-34,

Linux 2.0.35-36,

Linux 2.1.24 PowerPC, Linux 2.1.76, Linux 2.1.91 - 2.1.103,

Linux 2.1.122 - 2.1.132; 2.2.0-pre1 - 2.2.2, Linux 2.2.0-pre6

- 2.2.2-ac5

Nmap run completed -- 1 IP address (1 host up) scanned in 1 second

Kao što vidite, iako nijedan priključak nije bio otvoren, nmap je ipak pogodio da se radi o Linuxu.

Jedna od najboljih osobina programa nmap jeste ta što se njegov spisak potpisa čuva u datoteci nmap-os-fingerprints. Svaki put kada iza?e nova verzija programa, ta datoteka se ažurira novim potpisima. Danas je u njoj pobrojano na stotine potpisa. Ako želite da u nmap dodate nov potpis i tako povećate njegovu upotrebljivost, to možete da uradite na adresi http://www.insecure.org:80/cgi--bin/nmap-submit.cgi.

Iako izgleda da nmap precizno otkriva operativni sistem, on nije prvi program koji je primenio takvu tehniku. Queso, koji može da se preuzme s adrese http://packetstorm.securify.com/UNIX/scanners/queso-980922.tar.gz, jeste alatka za otkrivanje vrste operativnog sistema koja je ugledala svetlost dana pre nego što je Fyodor u nmap ugradio sličnu funkcionalnost. Treba naglasiti da queso nije skener priključaka i da operativni sistem otkriva preko jedinstvenog otvorenog priključka (standardno, preko priključka 80). Ako priključak 80 na ciljnom serveru nije otvoren, treba zadati priključak koji jeste, što ćemo i videti na primeru u kome je zadat priključak 25.

[tsunami] queso 10.10.10.20:25

10.10.10.20:25 * Windoze 95/98/NT

Mere zaštite od otkrivanja operativnog sistema

Otkrivanje Mnoge ranije pominjane alatke za otkrivanje skeniranja priključaka mogu da uoče i pokušaje otkrivanja operativnog sistema. Mada ne ukazuju direktno da se odvija akcija otkrivanja operativnog sistema pomoću programa nmap ili queso, one će prepoznati skeniranje uz TCP ocije, npr. uz uključen indikator SYN.

Sprečavanje Voleli bismo da postoji lak način za sprečavanje otkrivanja operativnog sistema, ali taj zadatak nije jednostavan. Možemo na brzinu da prekrojimo kôd operativnog sistema ili da izmenimo neki njegov parametar kako bismo promenili jednu od karakteristika otiska steka koja ga čini jedinstvenim. Takva akcija, međutim, može negativno da se odrazi na rad operativnog sistema. Na primer, FreeBSD 4.x podržava opciju jezgra TCP_DROP_SYNFIN namenjenu zanemarivanju paketa SYN+FIN koje koristi nmap kada uzima otisak steka. Kada se ova opcija uključi, to može da spreči otkrivanje operativnog sistema, ali istovremeno ukida podršku za RFC 1644 (TCP dodaci za transakcije).

Verujemo da samo robusni, obezbeđeni zastupnici ili zaštitne barijere treba da budu izloženi skeniranju preko Interneta. "Bezbednost putem prikrivanja" ne treba da bude moto vaše prve linije odbrane. Čak i ako napadači otkriju vaš operativni sistem, sistem mora da im onemogući da prodru do cilja.

Pasivno prepoznavanje operativnog sistema

Popularnost:	5
Jednostavnost:	6
Uticaj:	4
Stepen rizika:	5

Već smo prikazali kako se efikasno - pomoću alatki kao što su nmap i queso - može aktivno uzeti

otisak steka. Opisane tehnike otkrivanja steka aktivne su po samoj svojoj prirodi. Svakom sistemu smo slali pakete da bismo utvrdili odre?ene specifičnosti njegovog mrežnog steka, na osnovu čega smo mogli da zaključujemo o vrsti njegovog operativnog sistema. Pošto smo morali da šaljemo pakete operativnom sistemu, mrežnom obezbeđenju je bilo srazmerno lako da utvrdi da smo lansirali sondu za otkrivanje operativnog sistema. Posle takvih tehnika, napadač može očekivati da bude otkriven.

Pasivno uzimanje otiska steka

Aktivno i pasivno uzimanje otiska steka koncepcijski su slični, ali će u drugom slučaju napadač, umesto da šalje pakete operativnom sistemu, pasivno pratiti mrežni saobraćaj da bi utvrdio koji se operativni sistem koristi. Lance Spitzner je opsežno istraživao ovu oblast i potom napisao zvaničan dokument u kom je objasnio svoja zapažanja. Dokument se nalazi na adresi http://project.honeynet.org. Marshall Beddoe i Chris Abad su napisali program siphon, alatku za pasivno mapiranje priključaka, identifikovanje operativnog sistema i utvrđivanje topologije mreže; on se može naći na adresi http://www.gravitino.net/projects/siphon. Pogledajmo kako radi pasivno uzimanje otiska steka.

Pasivni potpisi

Da bi se identifikovao operativni sistem, mogu se koristiti različiti potpisi. Mi ćemo se ovde ograničiti na nekoliko atributa koji su povezani sa TCP/IP sesijom:

- TTL Šta kao vreme preživljavanja operativni sistem zadaje izlaznom paketu?
- Veličina prozora Koju vrednost operativni sistem zadaje parametru Window Size?
- DF Da li operativni sistem uključuje bit Don't Fragment ("ne usitnjavaj")?

Pasivnom analizom svakog atributa i upoređivanjem rezultata s informacijama iz baze podataka, možete da utvrdite vrstu udaljenog operativnog sistema. Iako ovaj postupak ne garantuje da ćete svaki put dobiti ispravan odgovor, atribute možete kombinovati i tako povećati pouzdanost zaključka. Upravo ovu tehniku sprovodi program siphon.

Pogledajmo na jednom primeru kako to radi. Ako pomoću telneta uspostavimo vezu između sistema shadow (192.168.1.10) i sistema quake (192.168.1.11), pomoću programa siphon ćemo moći pasivno da odredimo vrstu operativnog sistema.

[shadow]# telnet 192.168.1.11

Snort, naše omiljeno njuškalo, može delimično otkriti put paketa tokom naše telnet sesije.

06/04-11:23:48.297976 192.168.1.11:23 -> 192.168.1.10:2295

TCP TTL:255 TOS:0x0 ID:58934 DF

S*A* Seq: 0xD3B709A4 Ack: 0xBE09B2B7 Win: 0x2798

TCP Options => NOP NOP TS: 9688775 9682347 NOP WS: 0 MSS: 1460

Na osnovu naša tri TCP atributa, nalazimo da je:

- TTL = 255
- veličina prozora = 2798
- DF = Yes

Pogledajmo sada datoteku osprints.conf programa siphon u kojoj je baza s otiscima sistema:

[shadow]# grep -i solaris osprints.conf

Window:TTL:DF:Operating System DF = 1 fcr ON, 0 for OFF.

2328:255:1:Solaris 2.6 - 2.7

2238:255:1:Solaris 2.6 - 2.7

2400:255:1:Solaris 2.6 - 2.7

2798:255:1:Solaris 2.6 - 2.7

FE88:255:1:Solaris 2.6 - 2.7

87C0:255:1:Solaris 2.6 - 2.7

FAF0:255:0:Solaris 2.6 - 2.7

FFFF:255:1:Solaris 2.6 - 2.7

Vidimo da četvrta odrednica u potpunosti odgovara rezultatima: veličina prozora 2798, TTL 255 i uključen bit DF (vrednost 1). Tako, pomoću programa siphon, tačno određujemo vrstu operativnog sistema.

[crush]# siphon -v -i x10 -o fingerprint.out

Running on: 'crush' running FreeBSD 4.0-RELEASE on a(n) i386

Using Device: x10

Host Port TTL DF Operating System

192.168.1.11 23 255 ON Solaris 2.6 - 2.7

Kao što vidite, srazmerno lako smo uspeli da pogodimo vrstu ciljnog operativnog sistema - Solaris 2.6. Ponavljamo, to smo otkrili a da računaru 192.168.1.11 nismo poslali nijedan paket.

Da bi otkrio informacije o potencijalnoj žrtvi, napadač može da iskoristi pasivno uzimanje otiska tako što će se povezati s njenom Web lokacijom i analizirati tragove na mreži, ili pak tako što će upotrebiti alatku poput programa siphon. Iako je ova tehnika efikasna, ona ima izvesna ograničenja. Prvo, aplikacije koje formiraju sopstvene pakete (npr. nmap) ne koriste isti potpis kao i operativni sistem. Zbog toga vaši rezultati ne moraju da budu tačni. Drugo, udaljeni računar lako može da promeni atribute za povezivanje.

Solaris: ndd -set /dev/ip ip_def_ttl 'broj'

Linux: echo 'broj' > /proc/sys/net/ipv4/ip_default_ttl

NT: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\ Tcpip\Parameters

Zaštita od pasivnog otkrivanja operativnog sistema

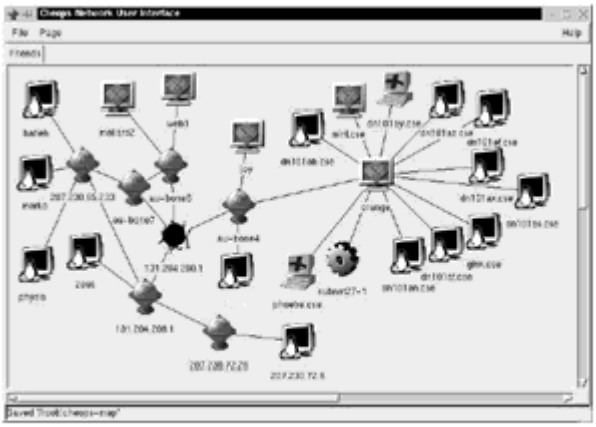
Pogledajte odeljak "Mere zaštite od otkrivanja operativnog sistema", ranije u ovom poglavlju.

Sve zajedno: automatske alatke za otkrivanje

Popularnost:	10
Jednostavnost:	9
Posledice:	9
Procena rizika:	9

Postoje mnoge alatke za prepoznavanje mreža, a svakoga dana se pojavljuju i nove. Premda ne možemo da navedemo svaku postojeću alatku, ipak ćemo se na kraju poglavlja osvrnuti na još dva uslužna programa koji zavre?uju pažnju.

Cheops (http://marko.net/cheops/) - čita se Kiops - prikazan je na slici 2-7. To je grafički uslužni program projektovan s namerom da bude svestrana alatka za mapiranje mreže. Cheops objedinjuje karakteristike programa ping i traceroute, može da skenira priključke i da otkriva vrstu operativnog sistema (pomoću programa queso) - sve u jedan mah. Cheops ima jednostavno grafičko okruženje koje vizuelno predstavlja sisteme i povezane mreže, i tako omogućava da se lakše shvati teren.



Slika 2-7. Cheops nudi mnoge usluge mapiranja mreže – sve na jednom mestu.

Tkined je deo paketa Scotty koji se nalazi na adresi http://wwwhome.cs.utwente.nl/~schoenw/scotty/. To je program za analizu mreže, pisan programskim jezikom Tcl, i objedinjuje različite alatke, pa omogućuje da otkrivate i IP mreže. To je prilično fleksibilan program pomoću koga možete da upoznajete mrežu, a rezultate prikazuje grafički. Mada nije namenjen otkrivanju vrste operativnog sistema, on će obaviti mnoge zadatke koji su pomenuti u poglavlju 1. Paket Scotty, osim programa *tkined* , sadrži i više vrednih skriptova koji olakšavaju otkrivanje.

Mere zaštite od automatskih alatki za otkrivanje

Alatke, kao što su *tkined* i cheops koriste kombinaciju do sada opisanih tehnika. Pojedinačne mere zaštite od tih tehnika važe i za zaštitu od ovih automatskih alatki.

Sažetak

Opisali smo alatke i tehnike koje su neophodne za automatsko otkrivanje aktivnih računara, skeniranje TCP i ICMP priključaka i za otkrivanje vrste operativnog sistema. Pomoću alatki za automatsko skeniranje signalom ping možete da utvrdite aktivne sisteme i da izaberete potencijalne ciljeve. Koristeći brojne alatke i tehnike za TCP i UDP skeniranje možete da identifikujete aktivne usluge i da na osnovu toga pravite pretpostavke o stepenu ranjivosti svakog ciljnog sistema. Na kraju smo pokazali kako napadači mogu da s velikom preciznošću utvrde ciljni operativni sistem. U narednim poglavljima ćemo pokazati da su podaci koje na ovaj način prikupimo od presudne važnosti za organizovanje usredsređenog napada.

Hakerske tajne: zaštita mrežnih sistema

Komentar o bezbednosti računarskih mreža

Cisco Systems

Marko je bio vrlo razočaran ocenom njegovog rada i rešio je da se šefovima žestoko osveti. Njegov poslodavac, firma igrice.com, mlada je kompanija u usponu, pa nije imala dovoljno vremena da se posveti bezbednosti. U stvari, kada su malobrojni i preopterećeni članovi odeljenja za informacione tehnologije projektovali mrežu, nisu detaljno razradili plan njenog obezbeđivanja. Za povezivanje mreže firme igrice.com s Internetom upotrebljen je jedan usmerivač, ali njegove prednosti u obezbeđ ivanju interne mreže nisu bile iskorišćene. Jednostavna, komutirana interna mreža firme igrice.com podešena je za udoban rad, a ne da bude bezbedna. Server za pristupanje mreži ne proverava identitet pomoću jednokratnih lozinki. Pohvalno je što su stručnjaci iz IT odeljenja obezbedili internu mrežu zaštitnom barijerom, ali je pitanje zašto tako nisu zaštitili Web lokaciju firme. Premda je mreža sigurno bila ranjiva spolja, od unutrašnjeg neprijatelja ona se uopšte nije mogla odbraniti. Marko se dao na posao.

Pošto je skenirao mrežu, Marko je imao prilično jasnu sliku o njenim slabim tačkama, koje su se gotovo same nudile. Usmerio je svoje istraživanje na NT domene za finansije i razvoj, kao i na podatke o zaposlenima, i tamo pronašao nekoliko lakih lozinki koje je sačuvao. Preko pristupačnijih naloga uspeo je da ugradi trojanske programe koji su mu obezbedili potpunu daljinsku kontrolu domena, a zatim je ugradio programska njuškala kako bi osluškivao elektronsku poštu i saznao šta se priča o njegovom napadu. Ugradio je i nekoliko tempiranih "bombi" nameštenih da automatski eksplodiraju, a zatim pročešljao domene ne bi li pronašao informacije koje se mogu unovčiti. To je bio tek početak Markovog subverzivnog poduhvata...

Tokom poslednje dve decenije, računarska industrija je doživela dramatičnu transformaciju od "zatvorenih" mreža oformljenih oko centralnih računara do "otvorenih" mreža koje koriste Internet. Kompanije se užurbano uključuju u elektronsku trgovinu da bi ostale konkurentne i ubrzano povezuju u mrežu poslovne partnere, obezbeđujući im pristupanje s daljine. Međutim, korišćenje prednosti Interneta donosi i opasnosti na koje kompanije moraju da budu pripravne. Kada otvorite svoju mrežu ka Internetu, time suštinski uvećavate rizik. Kao što je pokazao navedeni scenario, zanemarivanje bezbednosti će veštim hakerima ponuditi zgodne prilike za zloupotrebu.

Naravno, crv Code Red, virus Melissa i neki vrlo razglašeni napadi uskraćivanja usluga privukli su pažnju poslovnih ljudi i stručnjaka za informacione tehnologije. Jasno je da su i najmoćnije kompanije ranjive - u stvari, one i jesu najčešće mete napada. Opasnost od hakera sve više raste, postaje sve neuhvatljivija i potencijalno pogubnija. Bezbednost informacija više ne možete da potisnete u drugi plan kada želite da izgradite mrežu ili da distribuirate nove aplikacije.

Američka vlada ima u ovoj oblasti značajnu ulogu, jer od kompanija i organizacija zahteva da bezbednosne mere usaglase s novim propisima o zaštiti informacija. Nijedan direktor ne želi da mu policija zakuca na vrata kada pokušava da utvrdi kako je haker uspeo da mrežu njegove firme iskoristi za napad na druge. Zakonsko normiranje "posledične odgovornosti" moglo bi znatno da doprinese investiranju u elektronsko poslovanje.

Kako preduzeća mogu da umanje rizik u ovom neuhvatljivom i opasnom okruženju, a da ipak iskoriste velike pogodnosti Interneta? To je ključno pitanje. Žao mi je što moram da kažem da ne postoji jasan i jednostavan odgovor. Čarobni štapić je samo bajka. Svaka kompanija koja nudi

jedinstven proizvod ili uslugu "za rešavanje svih vaših bezbednosnih problema" lažno prikazuje svoje mogućnosti.

Gra?enje i održavanje bezbedne mreže je neophodno ukoliko kompanija želi da bez problema iskoristi ekonomske pogodnosti koje joj pruža Internet. Svaka organizacija je drugačija i ima sopstvene razloge zbog kojih se opredeljuje za elektronsko poslovanje. Me?utim, jasno je da njena bezbednosna strategija mora dosledno da prati postavljene ciljeve. Postoji pet ključnih elemenata svake bezbednosne strategije koji, nadovezujući se logičnim redosledom, sačinjavaju potpun plan obezbeđivanja mreže:

1. Pravila ponašanja Imate li jasna pravila ponašanja koja su u skladu sa ciljevima koje želite da postignete elektronskim poslovanjem? Da li su s tim pravilima upoznati svi zaposleni u svim ograncima radne organizacije? Bez napisanih pravila ponašanja nemate jasan cilj koji želite da dostignete, niti odgovarajući "aršin" da izmerite postojeće stanje. Kako mislite da stignete na odredište ako ga niste unapred utvrdili?
2. Planovi Kakva je vaša strategija za uvođenje pravila ponašanja? Imate li celovit bezbednosni plan svoje mreže za elektronsko poslovanje? Ta razmatranja ne treba da obuhvate samo aplikacije i tehnologije koje vaša mreža podržava danas nego i one koje mislite da koristite u budućnosti. Upitajte se da li je vaša bezbednosna infrastruktura projektovana tako da može da zaštiti i podrži mrežna rešenja sledeće generacije, kao što su IP telefonija, bežične lokalne mreže, distribucija sadržaja i njima slična?
3. Proizvodi Koje su ključne tehnologije i usluge potrebne za sprovođenje plana i postizanje zadatih ciljeva? Kako ih treba rasporediti da bi se ostvario neophodan nivo bezbednosti, učinka, prilagodljivosti i kvaliteta usluga? Koliko je za vaš izbor odgovarajućih proizvoda bitna podrška potrošača? Na ova pitanja nije lako odgovoriti i često je potrebna detaljna analiza ponuda proizvođača da bi se izabralo najbolje moguće rešenje.
4. Postupci Kako ćete u hodu održavati svoju bezbednosnu infrastrukturu? Kakvim ćete merilom ocenjivati svoj bezbednosni status? Ako dođe do narušavanja bezbednosti, na koji način ćete rešiti problem? Jasno definisani operativni postupci presudno utiču na uspeh plana obezbeđ enja. Primena bezbednosnih tehnologija neodvojiva je od stalnog nadgledanja, testiranja i prilagođavanja mreže.
5. Osoblje Koji su resursi neophodni za uspešno sprovođenje plana obezbeđivanja i primenu odgovarajućih proizvoda i postupaka? Da li ćete deo svoje bezbednosne infrastrukture poveriti nekoj specijalizovanoj firmi ili ćete sve obaviti u okviru kuće? Osoblje neophodno za uspešno obezbeđivanje elektronskog poslovanja presudan je ali često zanemaren element koji može znatno da uveća sporedne troškove. S obzirom na to da su iskusni administratori u oblasti bezbednosti prava retkost, ovom pitanju posvetite dužnu pažnju.

Šta ćete, dakle, prvo uraditi? Deo vašeg projekta obezbeđivanja mora biti i obaveza da upoznate neprijatelja. Bezbednost rada na mreži dosad nije bila u centru pažnje, ali je svaki napad koji mediji objave sve više njemu primiče. Važno je da organizacije skinu veo tajne s bezbednosnih izazova s kojima se suočavaju. Knjiga Hakerske tajne će vam pomoći da bolje razumete u čemu se sve ogleda ranjivost sistema bezbednosti i koji su mehanizmi moguće zloupotrebe njegovih slabih tačaka. To će vas istovremeno poučiti kako da uspešno sprovedete solidnu strategiju obezbeđivanja svog sistema.

David G. King, Jr.

direktor sektora za marketing i bezbednost
virtuelnih privatnih mreža

kompanije Cisco Systems

Hakerske tajne: zaštita mrežnih sistema

Priključci

Najveći deo posla u svakoj proceni bezbednosti jeste pronalaženje svih aktivnih sistema na mreži, pa precizan spisak priključaka i njihovih vlasnika može da bude suštinski značajan za prepoznavanje većine bezbednosnih propusta. Pretraživanje svih priključaka (ima ih 131.070, odnosno od 1 do 65.535 za TCP i za UDP) za svaki računar može da traje danima, u zavisnosti od primenjene tehnike, te bi za pronalaženje otvorenih vrata, tj. ranjivih usluga, trebalo koristiti uži spisak priključaka i usluga.

Sledeći spisak nikako nije potpun, a neke navedene aplikacije mogu da osluškuju na sasvim drugačijim priključcima. Međutim, pomoću ovog spiska možete da otpočnete uspešno traganje za piratskim aplikacijama. Priključci popisani u tabeli obično se koriste za dobijanje podataka od računara ili za pristupanje računarima. Detaljniji spisak priključaka potražite na adresi http://www.iana.org/assignments/port-numbers.

Usluga ili aplikacija	Priključak/Protokol
echo	7/tcp
systat	11/tcp
chargen	19/tcp
ftp-data	21/tcp
ssh	22/tcp
telnet	23/tcp
SMTP	25/tcp
nameserver	42/tcp
whois	43/tcp
tacacs	49/udp
xns-time	52/tcp
xns-time	52/udp
dns-lookup	53/udp
dns-zone	53/tcp
whois++	63/tcp/udp
bootps	67/tcp/udp
bootps	68/tcp/udp
oracle-sqlnet	66/tcp
tftp	69/udp
gopher	70/tcp/udp
finger	79/tcp
http	80/tcp
alternativni Web priključak (http)	81/tcp
kerberos ili alternativni Web priključak (http)	88/tcp
pop2	109/tcp
pop3	110/tcp

Usluga ili aplikacija	Priključak/Protokol
sunrpc	**111/tcp**
sqlserv	118/tcp
nntp	119/tcp
ntp	123/tcp/udp
ntrpc ili dce (epmap)	135/tcp/udp
netbios-ns	137/tcp/udp
netbios-dgm	138/tcp/udp
netbios	139/tcp
imap	143/tcp
snmp	161/udp
snmp-trap	162/udp
xdmcp	177/tcp/udp
bgp	179/tcp
snmp-checkpoint	256/tcp
ldap	389/tcp
netware-ip	396/tcp
timbuktu	407/tcp
https/ssl	443/tcp
ms-smb-alternate	445/tcp/udp
ipsec-internet-key-exchange(ike)	500/udp
exec	512/tcp
rlogin	513/tcp
rwho	513/udp
rshell	514/tcp
syslog	514/udp
printer	515/tcp
printer	515/udp
talk	517/tcp/udp
ntalk	518/tcp/udp
route	520/udp
netware-ncp	524/tcp
irc-serv	529/tcp/udp
uucp	540/tcp/udp
klogin	543/tcp/udp
mount	645/udp
remotelypossible	799/tcp
rsync	873/tcp
samba-swat	901/tcp

Usluga ili aplikacija	Priključak/Protokol
	1024-1030/tcp
rpc Windowsa 2000	
	1024-1030/udp
socks	1080/tcp
kpop	1109/tcp

bmc-patrol-db	1313/tcp
notes	1352/tcp
timbuktu-srv1	1417-1420/tcp/udp
ms-sql	1433/tcp
citrix	1494/tcp
sybase-sql-anywhere	1498/tcp
funkproxy	1505/tcp/udp
ingres-lock	1524/tcp
oracle-srv	1525/tcp
oracle-tli	1527/tcp
pptp	1723/tcp
winsock-proxy	1745/tcp
radius	1812/udp
remotely-anywhere	2000/tcp
cisco-mgmt	2001/tcp
nfs	2049/tcp
compaq-web	2301/tcp
sybase	2368
openview	2447/tcp
realsecure	2998/tcp
nessusd	3001/tcp
ccmail	3264/tcp/udp
ms-active-dir-global-catalog	3268/tcp/udp
bmc-patrol-agent	3300/tcp
mysql	3306/tcp
ssql	3351/tcp
ms-termserv	3389/tcp
cisco-mgmt	4001/tcp
nfs-lockd	4045/tcp
rwhois	4321/tcp/udp
postgress	5432/tcp
secured	5500/udp
pcanywhere	5631/tcp
vnc	5800/tcp
Usluga ili aplikacija	**Priključak/Protokol**
vnc-java	**5900/tcp**
xwindows	**6000/tcp**
cisco-mgmt	**6001/tcp**
arcserve	6050/tcp
apc	6549/tcp
irc	6667/tcp
font-service	7100/tcp/udp
web	8000/tcp
web	8001/tcp

web	8002/tcp
web	8080/tcp
blackice-icecap	8081/tcp
cisco-xremote	9001/tcp
jetdirect	9100/tcp
dragon-ids	9111/tcp
iss agent sistemskog skenera	9991/tcp
iss konzola sistemskog skenera	9992/tcp
stel	10005/tcp
netbus	12345/tcp
trinoo_bcast	27444/tcp
trinoo_master	27665/tcp
quake	27960/udp
backorifice	31337/udp
rpc-solaris	32771/tcp
snmp-solaris	32780/udp
reachout	43188/tcp
bo2k	54320/tcp
bo2k	54321/udp
netprowler-manager	61440/tcp
pcanywhere-def	65301/tcp