DEO I

Internet

Obuhvaćene teme:

- **Kako radi Internet**
- **Kako radi firewall (mrežna barijera)**
- **Ko hakeriše**
- **Motivacije hakera**
- **Osnove TCP/IP protokola**
- **TCP/IP protokoli višeg nivoa**
- **Kako hakeri eksploatišu slabosti TCP/IP protokola**
- **Kako funkcioniše šifrovanje**
- **Kako šifrovanje obezbeđuje bezbednost na Internetu**
- **Kako šifrovanje obezbeđuje mehanizam za dokazivanje identiteta korisnika**

1 Šta je firewall

NACIJE BEZ KONTROLISANIH GRANICA NE MOGU OSIGURATI BEZBEDNOST NJIHOVIH stanovnika, niti mogu sprečiti pljačkanje i krađu. Mreže bez kontrolisanog pristupa ne mogu omogućiti sigurnost ili privatnost pohranjenih podataka, niti mogu sačuvati mrežne resurse od hakerske eksploatacije.

Komunikaciona efikasnost koju Internet omogućava je prouzrokovala masovno priključenje privatnih mreža direktno na Internet. Direktne Internet konekcije olakšavaju hakerima da eksploatišu privatne mrežne konekcije. Pre postojanja Interneta, jedini način koji je omogućavao hakerima da se povežu od kuće na privatnu mrežu bio je direktno biranje telefonskog broja modemom preko javne telefonske mreže. Pitanju bezbednosti daljinskog pristupa nije posvećivano mnogo pažnje.

Kada povezujete Vašu privatnu mrežu na Internet, Vi je zapravo povezujete direktno sa svim drugim mrežama koje su trenutno priključene na Internet. Ne postoji centralna tačka kontrole bezbednosti - zapravo, bezbednost uopšte nije prisutna.

Firewalli se koriste za kreiranje kontrolnih tačaka bezbednosti (chekpoints), na granicama privatnih mreža. Na ovim kontrolnim tačkama firewalli ispituju sve pakete koji prolaze između privatne mreže i Interneta, u zavisnosti od toga da li odgovaraju pravilima politike programirane na firewallu. Ako je Vaš firewall propisno konfigurisan, u mogućnosti je da ispita svaki protokol kome je dozvoljen prolaz, a da ne sadrži ozbiljnije greške. Tako će Vaša mreža biti pošteđena nepotrebnih rizika.

Postoje na stotine raspoloživih firewall proizvoda kao i mnoštvo različitih teorija stručnjaka za bezbednost o tome kako treba koristiti firewalle u cilju osiguranja Vaše mreže. Ovo poglavlje će se baviti detaljnim istraživanjem operacija generičkog firewalla, ističući njegove glavne osobine. Takođe, biće reči i o tome kako ih razvijati u mrežama različitih veličina.

Elementi firewalla

Firewalli održavaju Vašu Internet konekciju što je moguće bezbednijom tako što ispituju i nakon toga odobravaju ili odbijaju svaki pokušaj povezivanja Vaše privatne mreže i spoljnih mreža, kao što je Internet. Snažni firewalli štite Vašu mrežu na svim softverskim slojevima - od sloja povezivanja podataka do aplikacionog sloja.

Firewalli se nalaze na granici Vaše mreže, povezani direktno na kola koja omogućuju pristup drugim mrežama. Iz tog razloga, firewalli su poznati kao pogranično obezbeđenje. Ovakav koncept pograničnog obezbeđenja veoma je bitan - bez njega svaki host (domaćin) na Vašoj mreži morao bi sam da obavlja funkciju firewalla, bespotrebno koristeći računarske resurse i povećavajući vreme potrebno za povezivanje, autentifikaciju i šifrovanje podataka u lokalnoj oblasti mreža velikih brzina. Firewalli omogućavaju centralizaciju svih bezbednosnih servisa na spoljnim mašinama koje su optimizovane i posvećene zadatku zaštite. Ispitivanje saobraćaja na graničnim mežnim prolazima je takođe korisno u sprečavanju hakerisanja propusnog opsega na Vašoj unutrašnjoj mreži.

Po prirodi, firewalli kreiraju "uska grla" (bottlenecks) između unutrašnjih i spoljnih mreža. Razlog za to je što sva saobraćajna tranzicija između ovih mreža mora proći kroz jednu tačku kontrole. Ovo je mala cena za bezbednost. S obzirom na to da su spoljne zakupljene linije relativno spore u poređenju sa brzinama modernih računara, zastoj prouzrokovan firewallima može biti kompletno transparentan. Većini korisnika su relativno jeftini firewall uređaji više nego dovoljni da se povežu sa Internet konekcijom T1 standarda. Za poslovne potrebe i potrebe ISP-a (Internet Service Provider - Dobavljač Internet usluga), čiji je Internet saobraćaj na mnogo višem nivou, razvijena je nova vrsta ekstremno brzih (i skupih) firewallova, koji su u mogućnosti da opsluže i najzahtevnije privatne mreže. Pojedine zemlje su čak cenzurisale firewalle na Internetu.

Firewalli primarno funkcionišu koristeći tri osnovna metoda:

- **Filtriranje paketa** Odbacuje TCP/IP pakete neautentifikovanih hostova kao i pokušaje povezivanja na neautentifikovane servise.
- **Network Address Translation (NAT)** Prevodi IP adrese unutrašnjih hostova i tako ih skriva od spoljnog praćenja. Ovaj metod se naziva i maskiranje IP adrese (IP address masquerading).
- **Proxy servisi** Uspostavljaju konekcije na visokim aplikacionim nivoima za unutrašnje domaćine u cilju da se kompletno prekine konekcija mrežnog sloja između unutrašnjih i spoljnih domaćina.

Moguće je korišćenje uređaja ili servera koji obavljaju samo jednu od navedenih funkcija; na primer, možete koristiti usmerivač koji obavlja filtriranje paketa, kao i proxy server na zasebnoj mašini. Na ovaj način, filter za pakete mora ili propustiti saobraćaj kroz proxy server ili se proxy server mora nalaziti van Vaše mreže, bez zaštite koju pruža filtriranje paketa. Oba načina su opasnija od korišćenja samo jednog firewall proizvoda koji obavlja sve bezbednosne funkcije u isto vreme. Većina firewalla takođe obavlja dva podjednako važna bezbednosna servisa:

- **Šifrovana autentifikacija** Omogućava korisnicima na javnim mrežama da dokažu svoj identitet firewallu, u cilju sprečavanja pristupa privatnim mrežama sa spoljnih lokacija.
- **Virtualno privatno umrežavanje(VPN)** Uspostavlja bezbednu konekciju između dve privatne mreže preko javnog medijuma kao što je Internet. Ovo omogućava korišćenje Interneta fizički odvojenim mrežama bez zakupljivanja direktnih linija. VPN-i se takođe nazivaju šifrovanim tunelima.

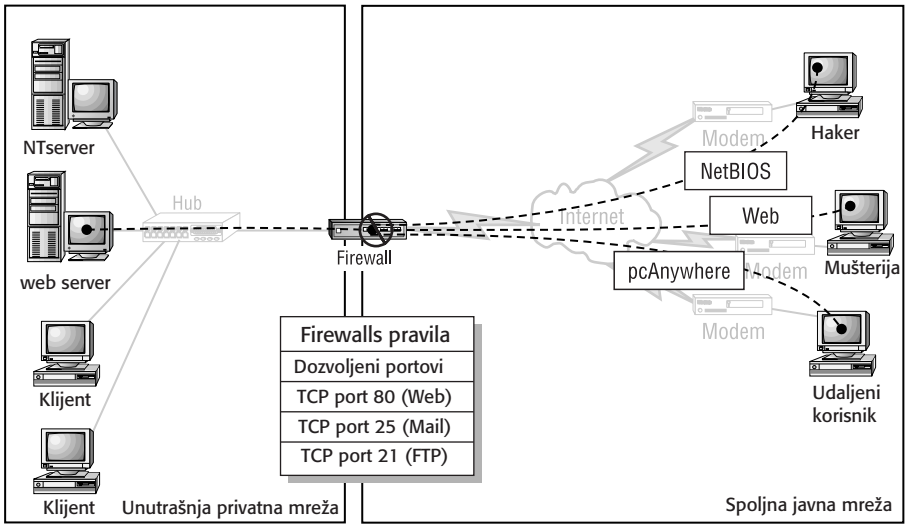
Takođe, neki firewalli obezbeđuju dodatne servise zasnovane na pretplati i nisu striktno povezani sa bezbednošću, ali će mnogi korisnici uvideti da su krajnje korisni:

- **Skeniranje virusa** Pretražuje dolazeće nizove podataka u potrazi za virusima. Ažuriranje servisa liste virusa zahteva pretplatu kod proizvođača firewalla.
- **Filtriranje prema sadržaju** Dozvoljava Vam da unutrašnjim korisnicima blokirate pristup određenim tipovima sadržaja po kategorijama, kao na primer pornografiji, sadržaju koji propagira govor mržnje ili informacije o hakerisanju. Trenutno aktuelne liste blokiranih sadržaja takođe zahtevaju pretplatu.

Da bi obezbedili servise bezbednosti, skoro svi firewalli koriste ove osnovne metode. Postoji mnoštvo firewall proizvoda i svi oni se takmiče za Vaš novac. Većina njih su veoma jaki proizvodi i razlikuju se samo u površnim detaljima. Ostatak ove sekcije pokriva pet primarnih funkcija koje većina firewalla pokriva.

Filtriranje paketa

Prvi Internet firewalli su bili jednostavni filteri paketa. Filtriranje paketa i danas ostaje jedna od ključnih funkcija današnjih firewalla. Filteri upoređuju mrežne protokole (kao što je IP) i pakete transportnih protokola (kao što je TCP) sa pravilima regulisanim u bazi podataka i prosleđju samo one koji potpadaju pod kriterijum specifikovanih pravila. Filteri mogu biti implementirani ili u ruterima ili u okviru TCP steka na serveru. (videti sliku 1.1)



Slika 1.1
Filtriranjem Internet konekcije se sprečava neželjeni saobraćaj

Filteri implementirani unutar usmerivača (ruter) sprečavaju da saobraćaj sumnjivog porekla stigne do odredišne mreže. S druge strane, moduli TCP filtera jednostavno sprečavaju tu specifičnu mašinu da odgovara na saobraćaj sumnjivog porekla. Svejedno, saobraćaj sumnjivog porekla još uvek može stići do mreže i napasti bilo koji računar. Usmerivači sa filterima štite sve računare na odredišnoj mreži od saobraćaja sumnjivog porekla. Zbog toga bi filtriranje na TCP steku servera (kao što je učinjeno na Windows NT) trebalo koristiti samo kao dodatak filtriranju na usmerivačima, ne kao i zamenu.

Tipično je da filteri slede ova pravila:

- Odbace dolazeće zahteve za konekciju, ali dozvole zahtevima za izlaznu konekciju da prođu.
- Eliminišu TCP pakete upućene na portove koji ne bi trebalo da budu raspoloživi za Internet (kao što je port za NetBIOS sesiju), ali dozvoljavaju prolaz paketima koji bi trebalo da su raspoloživi (kao što je SMTP). Većina filtera može tačno odrediti koji saobraćaj ide na određeni server - na primer, SMTP saobraćaj bi trebalo kroz port 25 da ide samo na IP adresu servera za poštu (mail server).
- Zabrane zahtev za pristup dolazeće konekcije određenim IP opsezima.

UPOZORENJE

Jednostavni filteri paketa ili ruteri sa fukcijom filtriranja paketa koji zahtevaju otvaranje portova iznad 1023 za povratne kanale, nisu efikasne bezbednosne mašine. Ovakvi filteri paketa ne sprečavaju unutrašnje korisnike ili Trojanske konje da postave servis na klijentskoj stanici kroz opseg portova iznad 1024 i da time jednostavno slušaju dolazeće pokušaje za konekcijom iz spoljnog okruženja. Firewalli (filteri za inspekciju komletnog stanja i bezbednosni proxyi) otvaraju kanale samo za servere koji su pozvani konekcionim pokušajem unutar bezbednog dela mreže; izaberite ih umesto jednostavnih filtera za pakete koji ne mogu upravljati stanjem konekcije.

Sofisticirani filteri proučavaju sve konekcije koje prolaze kroz njih, pri tom tražeći izdajničke znake hakerisanja, kao što je navođenje tačne putanje puta (source routing), preusmeravanje ICMP paketa i lažiranje IP adresa. Konekcije koje prikazuju ovakve karakteristike bivaju odbačene.

Unutrašnjim klijentima je uglavnom dozvoljeno da kreiraju konekcije ka spoljnim hostovima, a spoljni hostovi su uobičajeno sprečeni u iniciranju pokušaja konekcije. Kada unutrašnji host odluči da inicira TCP konekciju, on šalje TCP poruku na IP adresu i broj porta javnog servera (na primer, `www.microsoft.com:80` za konektovanje na web sajt Microsofta). U inicirajućoj konekcionoj poruci, TCP kaže udaljenom serveru koja mu je IP adresa i na kom portu sluša odgovor (na primer, `localhost:2050`).

Spoljni server tada šalje odgovor, transmitujući ga do datog porta gde ga unutrašnji host očekuje. Pošto firewall proverava sve podatke koji su razmenjeni između ta dva hosta, on zna da je konekciju inicirao unutrašnji host, koji je povezan na svoj unutrašnji mrežni interfejs, zna IP adresu tog hosta i zna na kom portu očekuje odgovor. Firewall zatim pamti da treba da dozvoli spoljnom hostu, čija se adresa nalazi u konekcionoj poruci, da vrati saobraćaj na IP adresu unutrašnjeg hosta samo na port koji je određen.

Kada učesnici u sesiji zatvore TCP konekciju, firewall briše unose u svojoj tablici stanja (memorija u kojoj se nalazi stanje konekcija) i time prekida mogućnost udaljenom hostu da dalje komunicira sa unutrašnjim. Ukoliko unutrašnji host prestane da odgovara pre zatvaranja TCP konekcije (na primer, zbog prekida veze) ili ako protokol koji je u pitanju ne podržava sesije (na primer, UDP), firewall će ukloniti unos u tablicu stanja konekcije nakon programiranog isteka vremena od nekoliko minuta.

Filtriranje u operativnom sistemu

Možda ne znate da većina verzija UNIX-a i Windowsa sadrži filtriranje paketa u interfejsu TCP/IP protokola. Da biste kontrolisali pristup individualnim serverima, možete koristiti ovakvo filtriranje kao dodatak snažnom firewallu; takođe, ovakav način filtriranja možete koristiti za omogućavanje dodatnih mera bezbednosti unutar Vaše mreže, bez dodatnih troškova za firewall. Kao što samo filtriranje nije dovoljno za zaštitu Vaše mreže u potpunosti, tako ni unutrašnje filtriranje operativnog sistema ne zadovoljava kreiranje kompletno bezbednog okruženja.

Ograničenja u bezbednosti filtriranja paketa

Filtriranje ne rešava u potpunosti problem bezbednosti na Internetu. Kao prvo, IP adrese računara u filteru su predstavljene u dolazećem saobraćaju, što pojednostavljuje određivanje tipa i broja Internet hostova u filteru, kao i praćenje napada na ove adrese. Filtriranje ne sakriva identitet domaćina u filteru.

Kao dodatak, filteri ne mogu proveriti sve fragmente jedne IP poruke, zasnovane na protokolima višeg nivoa, kao što su TCP zaglavlja, iz razloga što zaglavlje postoji samo u prvom fragmentu. Podeljeni fragmenti nemaju informacije o zaglavlju i mogu biti upoređeni samo sa IP pravilima, koja uobičajeno dozvoljavaju nešto saobraćaja kroz filter. Ovo omogućava greškama u odredišnim IP stekovima računara na mreži da se eksploatišu i mogu omogućiti komunikacije sa Trojanskim konjem instaliranim negde na mreži. Savremeniji firewallovi podržavaju povratak fragmentovanih podataka u pređašnje stanje i nakon toga primenu firewall pravila na njih.

Konačno, filteri nisu dovoljno složeni za proveru legitimnosti protokola u okviru paketa mrežnog sloja. Na primer, filteri ne ispituju HTTP pakete, sadržane u TCP paketima, radi utvrđivanja da li oni sadrže elemente kojima hakeri gađaju web pretraživač ili web server na kraju Vaše konekcije. Većina pokušaja modernog hakerisanja zasnovana je na iskorišćavanju ovih servisa viših slojeva TCP/IP steka, iz razloga što su firewalli gotovo eliminisali uspešno hakerisanje na mrežnom sloju, ako izuzmemo neugodne napade tipa "odbijanje izvršenja servisa" (DoS, denial-of-service).

Windows varijante

Postoje tri glavna tipa Windows sistema:

- 16-bitna verzija Windowsa, koja za osnovu ima MS-DOS, uključujući Windows 3.0, 3.1 i 3.11.
- 32-bitna verzija Windowsa, koja za osnovu ima MS-DOS, uključujuci Windows 95, 98 i ME.
- 32-bitna verzija Windowsa, koja se zasniva na NT kernelu, uključujući Windows NT 3.1, 3.5, 3.51, 4.0, 2000 i XP.

Kada kroz čitavu ovu knjigu budemo koristili termin "Windows", mislićemo na one verzije bazirane na NT kernel arhitekturi, ukoliko ne naznačimo drugačije.

Pri zaštiti Vaše mreže, nemojte se oslanjati isključivo samo na filtriranje ugrađeno u Vaš operativni sistem. Da biste podesili filtere da propuštaju samo one protokole koje ćete opsluživati, trebalo bi da u okviru Vaše mreže koristite funkcije filtriranja operativnog sistema. Ovo odvraća softver od rada na način koji ne očekujete i onemogućava funkcionisanje Trojanaca, čak i ako uspeju da se instaliraju.

Osnovno filtriranje operativnog sistema omogućava Vam definisanje prihvatljivih kriterijuma za svaki mrežni adapter u Vašem računaru za dolazeće konekcije bazirane na sledećem:

- Broj IP protokola
- Broj TCP porta
- Broj UDP porta

Filtriranje se uobičajeno ne koristi za izlazeće konekcije (one koje potiču sa Vašeg servera) i posebno je definisano za svaki adapter na Vašem sistemu.

NAPOMENA

Windows2000, za razliku od Windowsa NT4.0, podržava filtriranje izlazećih konekcija.

Jedan tipični server podešava servise za slušanje na sledećim portovima. Da bi ovi servisi pravilno funkcionisali, ovi portovi moraju biti otvoreni na filteru.

Jednostavni TCP/IP servisi uobičajeno slušaju na sledećim portovima:

Port	**TCP/IP servis**
7	Echo
9	Discard
13	Daytime
17	Quote of the day
19	Character generator

Internet serveri uobičajeno slušaju na sledećim portovima:

Port	**server**
21	File transfer protocol (FTP)
23	Telnet
70	Gopher
80	WorldWidWeb (HTTP)
119	NetNews (NNTP)
22	Secure shell
443	Secure HTTP (HTTPS)

Fajl serveri uobičajeno slušaju na sledećim portovima:

Port	Servis
53	Domain Name Service (DNS servis, ako je instaliran)
135	RPC Locator Service (samo Windows NT)
137	NetBIOS Name Service (samo WINS serveri)
139	NetBIOS Session Service (samo Windows mreža i SMB/CIFS serveri)
515	LPR se koristi od strane TCP/IP print servisa, ako je instaliran.
530	Remote Procedure Call (RPC konekcije koje koristi Windows NT WinLogon servis, kao i mnoge druge mrežne aplikacije visokog nivoa)
3389	Windows Terminal Services prihvata konekcije na ovom portu, koristeći RDP protokol

Serveri za poštu su uobičajeno konfigurisani da slušaju na sledećim portovima:

Port	Mail server
25	Simple Mail Transfer Protocol (razmena mail server - server)
110	Post Office Protocol verzija 3 (razmena pošte od servera ka klijentu)
143	Internet Mail Access Protocol (klijentov pristup mail serveru)

Ukoliko instalirate softver za druge servise, morate se uveriti da je filter na serveru podešen da sluša na portovima servisa - u suprotnom, servis neće raditi. Od proizvođača softvera saznajte koje portove koriste određeni servisi. Ovo se ne odnosi na pogranične firewalle, koje bi trebalo konfigurisati tako da propuštaju servis, ukoliko nameravate da javno omogućite taj servis.

Opšta pravila za filtriranje paketa

Postoje dva osnovna pristupa podešavanja bezbednosti.

Prvi, pesimistički, gde ćete isključiti sav pristup osim onog koji je neophodan i drugi, optimistički, gde ćete dozvoliti sav saobraćaj osim onog za koji znate da je štetan. U svrhu bezbednosti, trebalo bi da uvek imate pesimistički pristup, jer optimistički pristup pretpostavlja da unapred već znate svaku moguću pretnju, što je nemoguće. Uzmite u obzir uobičajene principe pri korišćenju filtriranja paketa:

- Zabranite sve protokole i adrese, a zatim dozvolite isključivo servise i hostove koje želite da podržite.
- Zabranite sve pokušaje konekcije ka hostovima unutar Vaše mreže. Dozvoljavajući bilo koju dolazeću konekciju, omogućavate hakerima da se povežu sa Trojanskim konjima ili da eksploatišu greške u softveru servisa.

- Filtriranjem odbacujte sve ICMP redirekcije i eho (ping) poruke. Odbacite sve pakete u kojima je navedena putanja paketa (source routing), jer je ovo retko legitiman metod povezivanja.
- Odbacite sva spoljna ažuriranja protokola rutiranja (RIP,OSPF) za unutrašnje rutere. Niko van Vaše mreže ne bi trebalo da emituje ažuriranja za RIP.
- Razmislite o tome da zabranite fragmentaciju veću od nule, zato što je ova funkcija uglavnom zastarela i podložna čestoj eksploataciji.
- Hostove na kojima se izvršava neki javni servis, kao što su web serveri ili SMTP serveri, postavite izvan oblasti filtriranja paketa, da ne biste, u protivnom, otvorili rupe u filterima.
- U zaštiti svoje mreže se ne oslanjajte samo na filtriranje paketa.

Prevođenje adresa iz mreže (Network Address Translation - NAT)

Prevođenje adrese iz mreže rešava problem skrivanja unutrašnjih hostova. NAT je zapravo proxy mrežnog sloja: jedan host čini zahteve u ime svih unutrašnjih hostova. Na taj način on skriva njihov identitet na javnoj mreži. Windows 2000, Linux i mnogi savremeni UNIX operativni sistemi obezbeđuju ovu funkciju kao deo samog operativnog sistema, dok Windows NT4.0 to ne čini.

NAT skriva adrese unutrašnjih hostova, konvertujući ih u adresu firewalla. Firewall zatim ponovo šalje podatke unutrašnjih hostova, koristeći sopstvenu IP adresu. Korišćenjem TCP broja porta, uspeva da prati koje se konekcije na javnom delu podudaraju sa hostovima na privatnom delu mreže. Gledano sa Interneta, sav saobraćaj sa Vaše mreže izgleda kao da dolazi sa jednog, ekstremno zaposlenog računara.

NAT efikasno skriva sve TCP/IP informacije unutrašnjih hostova od očiju Interneta. Prevođenje IP adresa omogućava da koristite bilo koji opseg IP adresa na unutrašnjoj mreži, čak i ako se te adrese već koriste negde na Internetu. Ovo znači da ne morate da tražite velike blokove adresa od ARIN-a. Takođe, ne morate da ponovo dodeljujete mrežne adrese onim računarima koje ste jednostavno priključili na mrežu pre povezivanja mreže na Internet.

UPOZORENJE

Sa NAT-om možete koristiti bilo koji blok IP adresa na Vašoj strani firewalla, ali čuvajte se problema koji mogu nastati pristupanjem Internet hostu sa istom javnom IP adresom, kao IP adresom nekog Vašeg unutrašnjeg računara. Da biste izbegli ovakve probleme, na delu firewalla koji je povezan sa Vašom privatnom mrežom, koristite rezervisane, u te svrhe, 192.168.0.0 ili 10.0.0.0 mreže.

Konačno, NAT dozvoljava multipleksiranje jedne javne IP adrese kroz celu mrežu. Mnoge male kompanije se nerado oslanjaju na usluge nekih dobavljača Internet servisa, koji su u nemogućnosti da im pruže velike blokove adresa zato što je i njihov sopstveni veoma mali. Možda ćete želeti da podelite jednu adresu dial-up ili kablovskog modema, a da tako nešto ne prijavite svom dobavljaču Internet usluga. Ova opcija je moguća korišćenjem NAT-a.

NAT je implementiran samo na TCP/IP nivou. Ovo znači da skrivena informacija unutar podataka, koji se prenose putem TCP/IP saobraćaja, može biti poslata ili servisima viših slojeva i time omogućiti iskorišćavanje slabosti u saobraćaju viših slojeva ili za komuniciranje sa Trojanskim konjem. Znači, ipak ćete morati koristiti servise viših slojeva, kao što je proksy, radi prevencije ugrožavanja bezbednosti servisa viših slojeva.

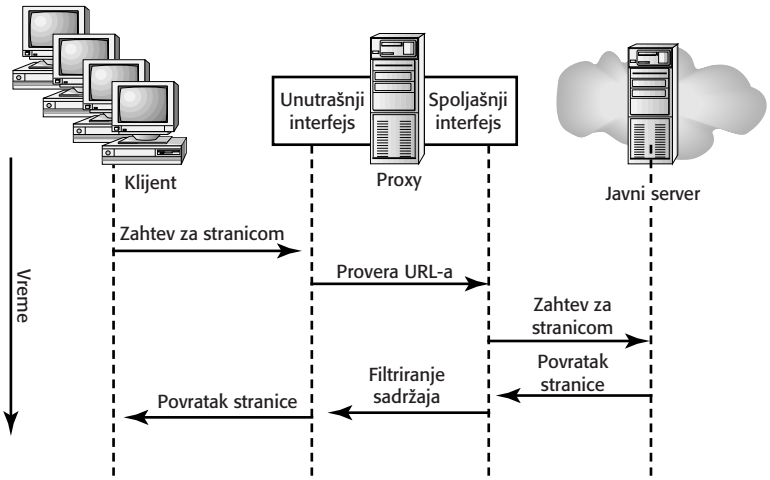
Mnogi protokoli, takođe, uključuju IP adresu hosta u podacima koji se prenose, tako da adresa postaje nevažeća kada se ponovo upiše prolaskom kroz NAT. Ovo se javlja u aktivnom modu FTP-a, H.323, IPSec i skoro svakom drugom bezbednosnom protokolu koji se zasniva na uspostavljanju sekundarnog komunikacionog niza između klijenta i servera.

NAT je, isto tako, problem za mrežne administratore koji će možda želeti da se, u administrativne svrhe, povežu sa klijentima iza NAT-a. Zbog toga što NAT poseduje samo jednu IP adresu, ne postoji mogućnost specifikovanja kojeg unutrašnjeg klijenta želite da dosegnete. Ovo sprečava podjednako i hakere i legitimne korisnike da se konektuju na nekog unutrašnjeg klijenta. Na sreću, mnoge savremene implementacije NAT-a dozvoljavaju kreiranje pravila za prosleđivanje saobraćaja kroz portove, što ipak omogućava da se povežete sa unutrašnjim klijentom.

Proxy

NAT rešava mnoge probleme Internet konekcija, ali ne sprovodi potpunu kontrolu podataka kroz firewall. U tom slučaju je moguće da neko uz pomoć mrežnog monitora pregleda saobraćaj koji dolazi iz Vašeg firewalla i na osnovu dobijenih informacija zaključi da firewall prevodi adrese drugih mašina. Hakeri na ovaj način mogu dobiti informacije potrebne za otimanje TCP konekcija ili za prolaz kroz firewall lažnom konekcijom.

Proxy aplikativnog sloja ovo sprečava. On Vam omogućava da potpuno zabranite protok podataka protokola mrežnog sloja i da dozvolite saobraćaj samo protokolima viših slojeva, kao što su HTTP, FTP i SMTP. Proxy aplikativnog sloja je specifično klijentsko-serverska kombinacija za protokol koji se koristi. Na primer, web proxy je kombinacija web servera i web klijenta. Serverski deo protokola proxya prihvata konekcije klijenata unutrašnje mreže, dok se klijentski deo protokola povezuje na javni server. Kada klijentski deo proxya primi podatke od javnog servera, serverska strana proxy aplikacije šalje podatke krajnjem unutrašnjem klijentu. Slika 1.2 prikazuje kako se ovaj proces odvija.



Slika 1.2
Proxy serveri primaju zahteve sa privatne mreže i ponovo ih generišu na javnoj mreži.

Proxy serveri pripadaju dvema mrežama koje nisu povezane ruterima. Kada klijent zaštićene mreže inicira zahtev prema serveru javne mreže, proxy server preuzima taj konekcioni zahtev i povezuje se na server javne mreže u ime klijenta zaštićene mreže. Proxy server, takođe, prosleđuje odgovor javnog servera klijentu na unutrašnjoj mreži. Proxy serveri prikazuju nezlonameran napad tipa "čovek-u-sredini" i daju primer kako bi neko mogao vršiti zlonamerne vrste obrade mrežnog saobraćaja.

Razlika između NAT i filtera sa jedne strane i aplikativnih proxya (kao što je Microsoft Proxy Server) sa druge strane je u tome što su klijentske aplikacije za Internet (uobičajeno) unapred podešene za komunikaciju sa proxyem. Na primer, uneta adresa Vašeg web proxya u Internet Explorer će prouzrokovati da Internet Explorer šalje sve zahteve tom proxy serveru, pre nego da sam razrešava adrese i uspostavlja direktne konekcije.

Aplikativni proxy ne mora biti pokrenut na firewallu; bilo koji server unutar ili izvan Vaše mreže može imati ulogu proxy servera. Ipak, ukoliko želite pravu bezbednost na mreži, trebalo bi da postavite i firewall i proxy. Mora postojati i neki tip filtriranja podataka zbog zaštite proxy servera od napada usmerenih preko mrežnog sloja tipa "denial of service" (kao što je "ping of death"). Svejedno, ukoliko se proxy ne pokreće na firewallu, neophodno je da otvorite kanal kroz taj firewall. Preporučljivo je da Vaš firewall obavlja i funkciju proxya. Ovo bi sprečilo prosleđivanje paketa javnog dela mreže kroz Vaš firewall.

Neki firewalli koji obavljaju i funkciju proxya su sofisticiraniji od ostalih. Neki imaju funkciju filtriranja IP protokola i maskiranje IP adresa, tako da mogu jednostavno blokirati unutrašnje konekcione pokušaje (na portu 80 u slučaju HTTP-a) ka udaljenim hostovima, pre nego da im je klijentski softver konfigurisan adresama proxy severa. U tom slučaju, firewalli koji obavljaju i funkcije proxya se povezuju na udaljeni server i zahtevaju podatke u ime blokiranog klijenta. Primljeni odgovori se vraćaju blokiranom klijentu pa uz pomoć NAT funkcije firewalla izgledaju kao da su poslati sa aktuelnog udaljenog servera. Za proxye koji rade na ovaj način se kaže da su transparentni.

Još bezbedniji proxyi su u mogućnosti da izvode filtriranje aplikativnog sloja za određeni saobraćaj. Na primer, neki firewall HTTP proxy traže Java ili ActiveX oznake u HTML stranicama koje ukazuju na ugnježđene aplete i zatim ih uklanjaju. Ovo sprečava da aplet bude izvršen na klijent kompjuteru i eliminiše rizik slučajnog učitavanja Trojanskog konja. Ova vrsta filtriranja je veoma važna zbog toga što obično filtriranje, maskiranje i proxy ne mogu sprečiti da se Vaša mreža ugrozi, ukoliko neko od Vaših klijenata ne učita skrivenog Trojanskog konja ugnježđenog unutar ActiveX apleta.

Možda ste primetili da, kako se penjemo uz stek mrežnih slojeva servisi bezbednosti postaju određeniji. Na primer, filtriranje je specifično za IP, TCP i zatim UDP. Aplikacije koje koriste IP sa ostalim protokolikma, kao što je "Banyan Vines", moraju koristiti specijalne, skupe ili neuobičajeno robusne firewalle.

Proxyi su naročito specifični zato što mogu raditi samo sa specifičnim naročitim aplikacijama. Na primer, morate posebno imati proxy softverske module za HTTP, FTP, Telnet. Pošto ovi protokoli evoluiraju (naročito HTTP), morate redovno ažurirati određene proxy softverske module.

Postoji mnogo pojedinačnih protokola, kao i protokola za koje ne postoji proxy. Proxy ne postoji za vlasničke aplikativne protokole kao što je Lotus Notes, tako da se ti protokoli moraju poslati kroz filtere mrežnog sloja ili da generički TCP proxy izvrši ulogu proxya, regenerišući pakete jednostavnim transferom u prenosu. SOCKS je specifična forma generičkog proxya, koji se ponekad naziva mrežni prolaz sloja kola (circuit-level gateway). Iako generički proksi ne može sprečiti napade i sadržaje protokola, ipak je bezbedniji od filtriranog usmeravanja, zato što se paketi mrežnog sloja potpuno regenerišu, uklanjajući zlonamerne formacije koje firewall ne detektuje.

U većini slučajeva, rad proxy servera se vrši korišćenjem kombinacije protokola servera i protokola klijenata na istoj mašini. Na primer, recimo da imate mrežu koja nije povezana na Internet, ali Vaš Windows server ima dve mrežne karte od kojih je jedna povezana sa Internetom, a druga sa privatnom mrežom. Ukoliko koristite funkcije terminal servisa Windowsa 2000 da biste se povezali sa serverom na njegovoj javnoj strani, onda možete pokrenuti klijenta terminalinih servisa i time se povezati sa mašinom koja se nalazi na unutrašnjem delu mreže. Ovo radi mnogo bolje nego što možete pretpostaviti, ali nije dobro koristiti u praksi radi bezbednosti mreže.

Koristite proxy servere za sve aplikativne protokole, kada god je to moguće. Razmislite o tome da onemogućite sve servise koje proxy ne podržava. Preporučljivo je i korišćenje proxya viših slojeva zbog njihove mogućnosti da uklanjaju sav izvršni sadržaj, kao što su ActiveX i Java apleti, sa web stranica.

Virtualne privatne mreže

Virtualne privatne mreže, poznate i kao šifrovani tuneli, dozvoljavaju bezbedno povezivanje dve fizički odvojene mreže preko Interneta. Podaci koji se razmenjuju na ovaj način su nevidljivi za neovlašćene entitete. VPN bi mogao biti predmet raznih neugodnih napada, kao što su pokušaji redirekcije, inicijalizovanje lažne konekcije ili bilo koji drugi vid napada dok se uspostavlja tunel. Ali, kada se VPN implementira kao integralni deo firewalla, autentifikacija i servisi za bezbednost firewalla se mogu iskoristiti da spreče eksploataciju tuneliranja.

Jednom kada su uspostavljeni, VPN tuneli su nepristupačni za eksploatisanje sve dok je šifrovanje bezbedno. Na granicama sa Internetom su smešteni firewallovi sa ciljem da služe kao odlične krajnje tačke za svaki kraj tunela. Zaključak je da Vaše privatne mreže mogu da propuštaju saobraćaj, podsećajući tako na dve podmreže istog domena.

VPN takođe dozvoljava korisnicima da adresiraju udaljene unutrašnje hostove direktno po njihovim skrivenim IP adresama; NAT i filteri paketa bi sprečili ovako nešto ukoliko pokušaj konekcije dolazi direktno sa Interneta.

SAVET

Point-to-Point Tunneling protokol (PPTP) za Windows NT obezbeđuje šifrovani tunel, korišćenjem servisa bezbednosti Remote Access servera. Windows 2000 obezbeđuje podršku za još savremeniji Layer2 Tunneling protokol (L2TP) i IPSecurity (IPSec) u transportnom modu. Većina distribucija Linuxa uključuje podršku za šifrovane tunele, kao što je Point-toPoint protokol (PPP) preko Secure Socket Layera (SSL).

Radije koristite zakupljene linije umesto VPN, ukoliko Vam troškovi ne predstavljaju problem. VPN koristite za sve komuniklacije organizacionih jedinica preko Interneta, ako nemate mogućnost da zakupite direktnu liniju ili ako su cene zakupa prevelike za Vaš budžet. Ako koristite VPN kao primarni konekcioni metod za povezivanje organizacionih jedinica, bolje performanse možete očekivati korišćenjem istog dobavljača Internet usluga na obe strane konekcije jer se, na taj način, zaobilaze usmeravanja kroz preopterećena područja komercijalne razmene na Internetu. Nikada ne razmenjujte privatne informacije između organizacionih jedinica preko Interneta bez upotrebe neke forme šifrovanja. Nešifrovana zaglavlja paketa sadrže važne delove informacije o strukturi Vaše privatne mreže.

NAPOMENA

Tehnički gledano, zakupljene linije su takođe ranjive, ali su pošteđene hakera sa Interneta. U slučaju da su Vaši podaci meta korporacijske špijunaže ili da želite da ih sačuvate od mogućnosti da ih država prisluškuje trebalo bi koristiti VPN na zakupljenim linijama.

Šifrovana autentifikacija

Šifrovana autentifikacija dozvoljava spoljnim korisnicima na Internetu da dokažu svoj identitet autorizovanih korisnika firewallu i da tako otvore konekciju kroz taj firewall ka unutrašnjoj mreži. Za šifrovanu autentifikaciju se može koristiti bilo koji bezbednosni autentifikacioni protokol. Kada je veza jednom uspostavljena, ona može, a i ne mora, biti šifrovana, što zavisi od firewall prozvoda koji se koristi i od toga da li je instaliran dodatni softver na klijentu u cilju da podržava tuneliranje.

Korišćenje šifrovane autentifikacije je pogodno zato što se pojavljuje na transportnom sloju između paketa softvera klijenta i firewalla. Kada je veza otvorena, bez smetnji će raditi sav aplikacioni softver i sistemski softver za prijavljivanje, što Vas oslobađa korišćenja specijalnih softverskih paketa za podršku Vašem firewallu. Nažalost, šifrovana autentifikacija smanjuje bezbednost Vašeg firewalla. Zbog prirode procesa nastaju sledeći problemi:

- Firewall mora odgovoriti ukoliko se pokuša povezivanje preko nekog porta. Ovo daje hakerima informaciju o postojanju firewalla
- Konekcija se uz pomoć ICMP-a može preusmeriti nakon što je veza uspostavljena, naročito ako je konekcija nešifrovana.
- Haker koji nadgleda uspostavljanje veze može kasnije lažirati svoju adresu i zameniti je adresom autorizovanog korisnika. Time će dobiti pristup mreži bez redirekcije neke od postojećih veza.
- Ukradeni lap-top sa odgovarajućim "ključevima" u sebi se može iskoristiti za dobijanje pristupa mreži.
- Radnici koji rade kod kuće mogu biti meta napada provalnika, jer se sa njihovih kompjutera može pristupiti mreži.
- Sama procedura procesa autentifikacije može biti poremećena ili manje sigurna, dozvoljavajući svakome na Internetu da otvori rupe na firewallu

Mala je mogućnost da se dogodi neki od ovih problema. Administratori okruženja sa srednjim ili malim rizikom ne bi trebalo da imaju probleme sve dok je konekcija šifrovana tokom trajanja.

Kreiranje efiektivne granične bezbednosti

Da biste održali minimalni nivo efektivne Internet bezbednosti, trebalo bi da kontrolišete bezbednost na Vašim mrežnim granicama, koristeći firewall koji obavlja sve tri osnovne njegove funkcije (filtriranje paketa, NAT i proxy servis viših slojeva). Vaši firewalli moraju biti posvećeni isključivo performansama funkcija firewalla; izbegavajte da pokrećete ostale servise, kao što su pošta, web ili drugi javni servisi, zajedno sa firewallom, osim ako softver za ove servise i za firewall ne dolaze od istog proizvođača. Čak i u tom slučaju, pripazite na rizike koje nose greške u softveru servisa viših slojeva, zbog toga što se mogu iskoristiti u svrhu premošćivanja Vašeg firewalla. Ovo nije samo teorija: UNIX-ov Sandmail i Internet Information Service (IIS) Windows web server su poznati po brojnim napadima tipa "propterećenje bafera". Ukoliko postavite ove servise na firewall, veoma lako Vas mogu kompromitovati.

Ponovimo dakle, jednostavno smanjite broj servisa na Vašem firewallu. Ovo redukuje kompleksnost softvera koji rade na mašini i time smanjuje mogućnost pada bezbednosti zbog grešaka operativnog sistema ili softvera za bezbednost. U slučaju Windowsa, potreban je rad samo nekoliko servisa unutar servisa "ControlPanel" da bi računar radio kao firewall. Isključite sve servise koje Vam server dozvoljava da isključite i podesite ih tako da se pokreću ručno. U slučaju Linuxa instalirajte samo one pakete koji su potrebni za rad firewalla ili selektujte opciju za instaliranje firewalla ukoliko postoji za datu distribuciju. Softver za instalaciju će isključiti sve servise koji su nepotrebni za rad firewalla. U svakom slučaju, ukoliko ovo ne radi, uvek možete potražiti softver za firewall na nekom drugom mestu.

Gomilanje servisa kao što su, HTTP, FTP, Telnet, Gopher i servis pošte na istu mašinu, koja se koristi kao Internet usmerivač i firewall, je oduvek predstavljalo iskušenje. To se dešava zbog toga što je jeftinije i što takva mašina, verovatno, ima dosta vremena za kompjutersku obradu i mnogo prostora na disku. Nažalost, malo je operativnih sistema dovoljno bezbednih i pošteđenih grešaka u kodu da bi mogli garantovati integritet servisa i to da pojedini sevisi neće oboriti firewall. Veoma je moguće i to da će se servisi viših slojeva pokrenuti na firewallu i obezbediti način da se nekako prevare bezbednosni servisi tog firewalla. I na kraju, kao što je pomenuto ranije u poglavlju, mnogi servisi sadrže okvire za prijavljivanje ili automatski generišu stranice sa greškama identifikujući tako firewall proizvod koji koristite. Ovo može biti opasno ako hakeri nađu slabosti u Vašem firewallu. Vi ipak želite da sakrijete koji operativni sistem koristi Vaš firewall.

Takođe, morate forsirati firewall politiku kontrole sa jedne tačke. Ukoliko imate veći broj firewalla u Vašoj kompaniji (svaki od njih povezuje filijalu sa Internetom), morate biti apsolutno sigurni da su identično konfigurisani. Veliku pomoć ovome daju osobine softvera za upravljanje firewallima na niviou celog preduzeća.

UPOZORENJE

Nedostatak bilo čega na firewallu može kompromitovati čitavu Vašu mrežu, pogotovo ako koristite bezbedno tuneliranje ili zakupljene linije za povezivanje filijala. Hakeri će se tada pojaviti tamo gde im je pružen najmanji otpor.

Razmatranje funkcionalnosti firewalla

Većina administratora smatra da firewall treba da bude baziran na istom operativnom sistemu kao i mrežni fajl serveri - UNIX firewalli za mreže bazirane na UNIX-u, a NT firewalli za mreže bazirane na Windowsu NT. Činjenica je da ne postoji razlog zbog kojeg bi operativni sistem firewalla bio isti kao i operativni sistem mreže. Osim u pojedinim slučajevima, na firewallu ionako nećete pokretati druge tipove softvera. Takođe, većina savremenih firewalla se proizvodi kao prekonfigurisani računar sa potpuno odgovarajućim operativnim sistemom.

Posao firewalla je da filtrira TCP/IP saobraćaj i, u većini slučajeva, neće biti potrebe da se posebno podešava. Možda će, u zavisnosti od organizacije, biti potrebno da im se podesi samo specifična politika bezbednosti. Neki firewalli su zasnovani na operativnim sistemima koji nisu ni u kakavoj vezi sa UNIX-om ili Windowsom; jednostavno oni odgovaraju bilo kojoj mreži.

Drugi, veoma važan faktor u odabiru firewalla je poznavanje njegovog operativnog sistema. Administrator bi trebalo da bude upoznat sa korisničkim interfejsom i kako da ispravno konfiguriše firewall. Većinu firewalla baziranih na Windowsu je jednostavnije podesiti nego one bazirane na UNIX-u. Međutim, veliki broj UNIX firewalla je zahvaćeno zbog korišćenja Jave ili web grafičkih interfejsa, koje možete pokrenuti sa udaljene lokacije.

Neki proizvođači firewalla tvrde da su njihovi proizvodi superiorni u odnosu na Windows ili standardne verzije UNIX-a, iz tog razloga što su proizvodi bazirani na snažnijoj implementaciji steka TCP/IP protokola ili na, teorijski, bezbednijem operativnom sistemu. Oni, takođe, tvrde da se greške u kodu Windowsa NT i UNIX-a mogu ekploatisati za prolaz kroz firewall. Ovo može biti istina, ali ti isti proizvođači ne mogu dokazati da slične greške ne postoje i na njihovim proizvodima. Ne postoji praktičan način na osnovu kojeg možete dokazati da greške u tako kompleksnom kodu ne postoje, što znači da proizvođači firewalla ne mogu imati veću sigurnost nego od velikih prizvođača kao što su Microsoft ili Sun.

Glavna prednost u korišćenju široko rasprostranjenog operativnog sistema kao osnove za firewall je ta što će kod koristiti, a na taj način i proveriti, milioni korisnika. Greške u kodu će u ovom slučaju biti lakše pronaći, a ispravke će se pojaviti mnogo brže. Mali proizvođači firewalla teško da će rešavati svoje greške ovako brzo, iz tog razloga što jednostavno nemaju tehničkih uslova za to. Ipak, uobičajeni operativni sistemi su predmet većeg broja napada hakera od ostalih operativnih sistema. Windows trpi teške udarce napada zbog toga što je najrasprostranjeniji operativni sistem i zato što hakeri mrze Microsoft.

Zbog ovoga je Windows najkompromitovaniji operativni sistem, iako UNIX (uključujući Linux) nema bolju bezbednost. Mnogi firewall proizvodi postavljeni na standardne operativne sisteme se ne oslanjaju na TCP/IP stekove ili servise viših slojeva tih operativnih sistema. Oni implementiraju sopstveni TCP/IP stek, tako da mogu imati kompletnu kontrolu nad operacijama steka. Sam operativni sistem služi kao platforma obezbeđujući funkcije kao što su podizanje sistema, izvršavanje više zadataka u isto vreme i korisnički interfejs.

Firewall proizvodi se ralikuju u sledećem:

- **Bezbednost** Neki firewall proizvodi su neverovatno slabi u obavljanju svog posla, zbog toga što se previše oslanjaju na osnovni operativni sistem, prepuni su grešaka koje se mogu eksploatisati ili postoji puno slabosti u protokolima za udaljenu autentifikaciju.
- **Interfejs** Neke firewalle je veoma teško konfigurisati zbog toga što ih morate administrirati preko Telneta ili prikačene konzole, što zahteva učenje nekih skripti komandne linije. Ostali koriste veoma intuitivne grafičke interfejse, koji konfigurisanje čine prilično lakim i očiglednim.
- **Funkcionalnost u okruženju preduzeća** Neki firewalli su sami po sebi tvrđave, dok se drugi oslanjaju na centralno uređene politike bezbednosti za sve firewalle u mreži.
- **Bezbednosne metode** Da bi omogućili bezbedno umrežavanje udaljenih filijala, mnogi firewalli nude veoma važne bezbednosne metode, kao što su VPN i šifrovana autentifikacija. VPN se posebno naplaćuje, tako da je često potrebno dokupiti dodatne licence.
- **Osobine servisa** Neki firewalli nude i servise kao što su FTP, HTTP, Telnet i drugi, tako da ne morate postavljati posebne mašine. Ove osobine mogu biti praktične, ali ukoliko se ne implementiraju ispravno, biće uzrok smanjivanja bezbednosti na samom firewallu. Takođe, mnogi servisi mogu otkriti verziju firewalla i time dozvoliti hakerima da iskoriste moguće slabosti u proizvodu.

Bezbednost je primarni kriterijum za sve firewalle. Sledeća važna osobina je lakoća korišćenja. Tek onda na red dolaze ostale osobine, performanse i servisi.

Problemi koje firewalli ne mogu rešiti

Nijedna mreža povezana sa Internetom ne može biti potpuno sigurna. Firewalli su naročito efektni i zadržaće hakere, ali postoji mnogo različitih načina za eksploataciju mrežnih konekcija, tako da nijedan metod nije potpuno siguran. Mnogi administratori greše, pretpostavljajući da će problem bezbednosti biti jednostavno rešen ispravnim postavljenjem firewalla. Ali to nije tako.

Na primer, recimo da kroz Vaš firewall jedino dozvoljavate prolaz pošte. Jedan od zaposlenih dobija poruku od filijale da im pošalje .CAD datoteku putem e-maila. Potvrđuje tačnost adrese u okviru "From" i zatim komandom "Reply to", neznajući, šalje pismo sa prikačenom .CAD datotekom hakeru koji je lažirao e-mail zahtev.

Zbog toga što adrese u okviru "From" i komandi "Reply to" ne moraju uvek biti iste, Vaš firewall ostaje bespomoćan u ovakvim slučajevima eksploatacije. Mnogi tipični korisnici nemaju iste adrese za "From" i "Reply to" (slično kao kada šalju pisma sa više adresa, a primaju sva na jednu).

Firewalli, takođe, ne mogu rešiti problem zaštite od protokola, kojima ste odlučili da dozvolite prolaz. Na primer, ukoliko imate na mreži postavljen Windowsov IIS, kao javni web server, Vaš firewall će do njega propuštati saobraćaj kroz port 80. Podražavajući tipičnu konekciju web pretraživača sa web serverom, hakeri će biti u mogućnosti da iskoriste brojne greške IIS-a, u cilju dobijanja administrativnog pristupa sa udaljene lokacije. Kada uspostave kontrolu nad web serverom, hakeri mogu, koristeći taj web server, da napadnu Vašu unutrašnju mrežu, ukoliko ih ne spreči dodatna firewall bezbednosna politika.

Postoji još jedna ozbiljna pretnja bezbednosti Vaše mreže: skriveni prolazi na granici sa Internetom. Modemi nude mogućnost da bilo koji korisnik na Vašoj mreži uspostavi vezu telefonskom linijom sa sopstvenim dobavljačem Internet usluga (ISP) i tako kompletno zaobiđe Vaš firewall. Modemi su veoma jeftini i prodaju se kao sastavni deo savremenih računara. Takođe, svi savremeni klijentski operativni sistemi imaju potreban softver za podešavanje modema u slučaju povezivanja sa svojim dobavljačem Internet usluga. Većina zaposlenih koji poznaju rad na računaru, sa svojih radnih mesta mogu pristupiti Internetu preko sopstevnih korisničkih naloga.

Veliki broj korisnika ne shvata da su sve IP konekcije potencijalni bezbednosni rizik. Modemske PPP konencije sa Internetom su dvostrukog smera, upravo kao i zakupljene linije. I postoji velika šansa da njihovi klijenti koriste deljenje datoteka, tako da njihovi računari mogu biti eksploatisani direktno sa Interneta.

UPOZORENJE

U radu sa firewallom, često se dozvoljava deljenje štampača i datoteka među radnim stanicama, iz tog razloga što je to jednostavan i efikasan način prenosa podataka. Ukoliko je jedan od korisnka prisutan na mreži, hakerima je omogućen put za jednostavan prenos podataka. Setite se da AOL (America on Line) nudi PPP servis, pa tako nije ništa sigurniji od bilo kog drugog dobavljača Internet usluga.

Zašto bi se korisnik odlučio za dial-up modemsku konekciju ukoliko poseduje već brzu i bezbednu Internet konekciju? Razlozi mogu biti sledeći:

- Vaš firewall ne propušta Internet Relay Chat (IRC), a oni žele da razgovaraju sa prijateljima.
- Mogu koristiti NetPhone da bi besplatno razgovali sa svojim majkama.
- Tako da mogu koristiti "PCAnywhere" od kuće.

- Zato što AOL koristi port koji Vaš firewall ne propušta, a oni žele da provere njihov lični e-mail.
- Zato što filtrirate FTP, a oni žele da preuzmu datoteku na svoj računar.
- Zato što je Vaša mreža konfigurisana da blokira stranice sa pornografskim sadržajem.

Korisnici se povezuju sa Internetom bez Vašeg znanja i time mogu narušiti podešenu bezbednosnu politiku. Da biste kontrolisali granicu Vaše mreže sa Internetom, morate kontrolisati sve prolaze. Ne sme biti moguće uspostaviti nov granični prolaz bez Vašeg znanja. Odstupanja od ovog pravila ugrožavaju bezbednost čitave Vaše mreže.

Poboljšanje bezbednosti granica

Evo nekoliko saveta u vezi sa preuzimanjem kontrole na Vašim graničnim prolazima:

- Smanjite broj konekcija sa Internetom na što je moguće manji broj: jedna po svakoj lokaciji. Mnoge velike organizacije dozvoljavaju samo jednu vezu sa Internetom i to iz glavnih predstavništava organizacije. Sve ostale filijale navode na tu vezu, koristeći iste FrameRelay linije kao i za konekciju unutrašnjih mreža. Čak iako koristite VPN za povezivanje Vaših filijala, razmislite o tome da ih usmerite preko Vašeg centralnog firewalla do veze sa Internetom - na ovaj način možete kontrolisati politiku firewalla na samo jednoj mašini.
- Nemojte dozvoliti dial-up konekcije na Internet. Uklonite modeme i sve ostale nekontrolisane uređaje za pristup mreži. Onemogućite slobodne COM portove u podešavanjima BIOS-a klijentskih računara i zaštite BIOS lozinkom da bi ste sprečili korisnike da menjaju bezbenosna podešavanja.
- Zabranite nedozvoljeno deljenje datoteka. Koristite deljenje podataka zasnovano na autentifikaciji korisnika ili u najmanju ruku sa lozinkama. Ukoliko nije neophodno, nemojte instalirati deljenje štampača i podataka na klijentske računare. Obučite korisnike da skladište sve podatke na mrežnim serverima za podatke i centralizujte izvorišta kao što su CD-ROM-ovi ili modemi.
- Konfigurišite unutrašnje klijentske računare IP adresama domena 192.168.0.0 ili 10.0.0.0, pošto se one ne usmeravaju preko Interneta. Na Vašem firewallu koristite NAT za prevođenje ovih unutrašnjih IP adresa u usmerive spoljne adrese. Ovo može sprečiti hakere da eksploatišu modemske konekcije Vaše mreže.

Bezbednosne opcije na granicama

Kada jednom pokrenete firewall na granici između Vaše mreže i Interneta, nastaće problem. Kako da obezbedite javne servise potrebne Vašim klijentima i da u isto vreme osigurate mrežu od napada? Postoji više od jednog odgovora na ovo pitanje, a koji je pravi, zavisi u potpunosti od stanja bezbednosti i nivoa potrebnih servisa.

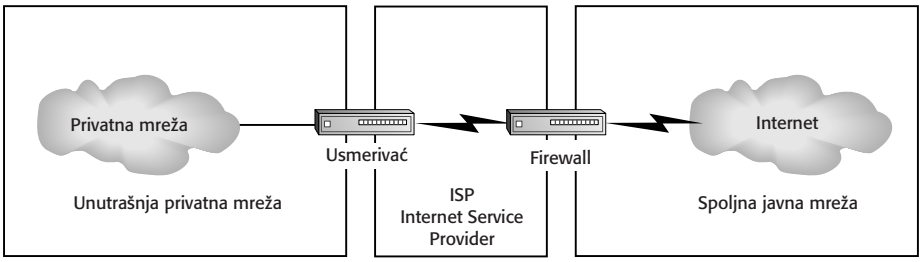
Kompanije su koristile različite metode za zaštitu svjih mreža, počevši od jednostavnih pa sve do veoma kompleksnih i rizičnih za samu bezbednost. Takvi metodi uključuju sledeće (u zavisnosti od rizika bezbednosti, od najnižeg ka najvišem):

1. Servisi filtriranja paketa
2. Jedan firewall sa unutrašnjim javnim serverima
3. Jedan firewall sa spoljnim javnim serverima
4. Dvostruki firewalli ili DMZ firewalli
5. Firewalli preduzeća
6. Isključenje sa mreže

Sledeća poglavlja opisuju svaki metod do detalja, kao i relativne rizike i probleme.

Servisi filtriranja paketa

Većina dobavljača Internet usluga omogućava filtriranje paketa kao dragoceni dodatak svojim servisima za mušterije sa zakupljenim linijama. Za nisku mesečnu cenu (oko 100 dolara) Vaš dobavljač Internet usluga će podesiti firewall na filtriranje saobraćaja koji ide ka i izvan Vaše mreže. Neki od dobavljača nude i proxy i NAT servere, ali možete i dalje rizikovati bezbednosne napade od ostalih mušterija koje opslužuje taj ISP. Setite se da i hakeri koriste ISP. Slika 1.3 ilustruje kako radi servis za filtriranje paketa.



Slika 1.3
Servis za filtriranje paketa

Postoji niz problema sa servisima za filtriranje na firewallu:

- Filteri paketa se mogu eksploatisati mnogo lakše nego kompletni firewalli
- Vaša bezbednost je u rukama nekog trećeg. Njegove motivacije ne moraju uvek da se podudaraju sa Vašim, pogotovo ukoliko dođe do legalnih nesuglasica između Vaše kompanije i njega
- Ne možete pouzdano kontrolisati odgovornost
- Nije u najboljem interesu ISP-a da Vas obavesti o kompromitovanju Vaše mreže

- Retko gde postoji mogućnost alarmiranja i upozoravanja
- Konfiguracija filtriranja je težak administrativni posao prepun mogućnosti za grešku. Re-konfiguracija Vas može činiti nervoznim ukoliko ISP ne poseduje kvalitetnu tehničku podršku klijentima
- Verovatno ste ranjivi i za ostale klijente ISP-a, smeštene u okvirima istog firewalla

Filteri paketa koje nudi ISP imaju sledeće prednosti:

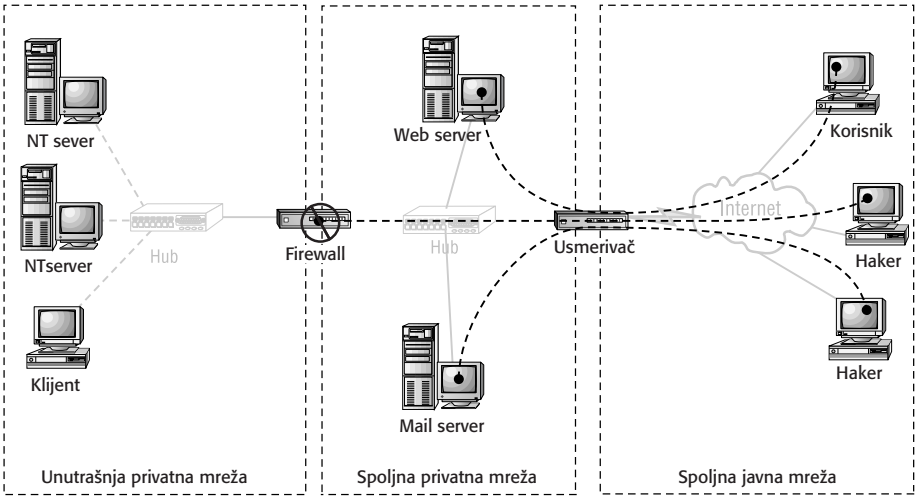
- Nema kapitalnog izdatka unapred.

Čak i ako bi ISP firewall servis bio kompletan, to i dalje ne bi bila dobra ideja jer prepuštate bezbednost Vaše mreže drugoj organizaciji. Ne znate ništa o zaposlenima u ISP-u i ne znate koje mere ISP može preduzeti ukoliko iz nekog razloga iskrsne sudski spor između Vaše i njihove kompanije. Tome dodajte ove jednostavne činjenice: većina ljudi hakuje, u najmanju ruku povremeno, i mnogi dobri hakeri rade za ljude koji ih mogu dovesti u akciju.

Lokalno kontrolišite i administrirajte sve bezbednosne servise za Vašu mrežu. Nemojte prepustiti odgovornost za bezbednost Vaše mreže nekoj spoljnoj organizaciji. Nemojte se olako oslanjati na filtere paketa kada želite zaštitu bezbednosti od Interneta.

Pristup sa jednim firewallom

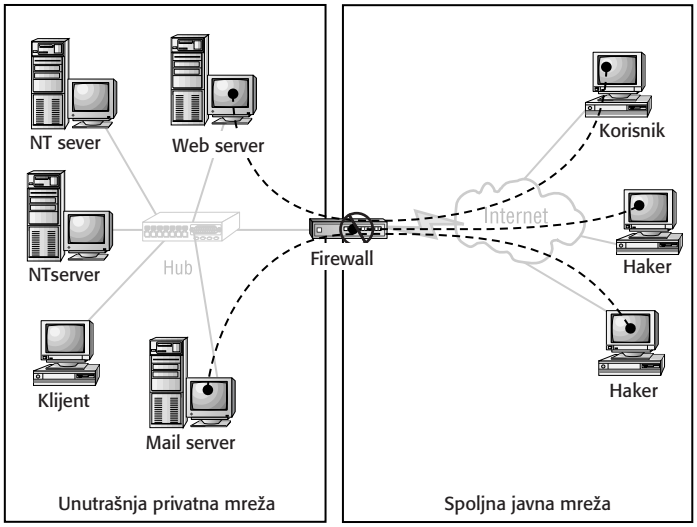
Najjednostavnije kompletno bezbednosno rešenje na granicama Vaše mreže je sa jednim firewallom. Sa njim i sa jednom konekcijom na Internet, centralizujete tačku kontrole. Slika 1.4 prikazuje rešenje bezbednosti sa jednim graničnim firewallom



Slika 1.4
Jedan firewall sa javnim serverima otvorenim ka Internetu

Imaćete problem ukoliko nastojite da obezbedite servise kao što su FTP sajt ili web sajt ili ukoliko želite da operišete sa serverom za poštu. Tada morate ili da otvorite konekciju kroz Vaš firewall do unutrašnjeg hosta ili da izložite Vaš javni server na Internetu bez zaštite firewalla. Oba metoda su rizična.

Problem sa postavljanjem javnih servera (kao što su serveri za poštu) izvan Vašeg firewalla je što su rizični za hakovanje. Možete podesiti ove računare da ne sadrže mnogo korisnih informacija, ali hakerski pokušaji mogu lako prouzrokovati "denial-of-sevice" ili u najmanju ruku prouzrokovati sramotu ukoliko hakeri modifikuju Vaše web stranice. Slika 1.5 prikazuje javne servere unutar firewalla



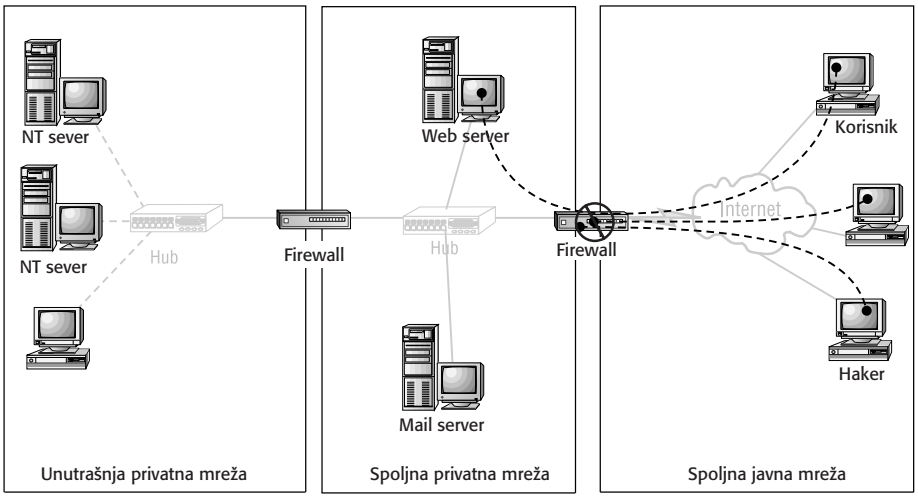
Slika1.5
Firewall sa zaštićenim javnim serverima i dozvoljenim saobraćajem

Problem sa otvaranjem putanje kroz Vaš firewall, radi pokušaja konekcije sa spoljne strane, je što postoji mogućnost da neodgovarajući paketi dospeju na Vašu unutrašnju mrežu ukoliko podsećaju na pakete kojima je dozvoljen prolaz. To, takođe, znači da haker koji pokušava da eksploatiše grešku servisa viših slojeva, može dobiti kontrolu nad računarom u okviru Vaše mreže - što je veoma opasna situacija. Iz ovog razloga veliki broj organizacija postavlja javne servere izvan svojih firewalla i jednostovno ne dozvoljava bilo kakve spoljne konekcije kroz firewall.

Dvostruki firewalli i demilitarizovane zone (DMZ)

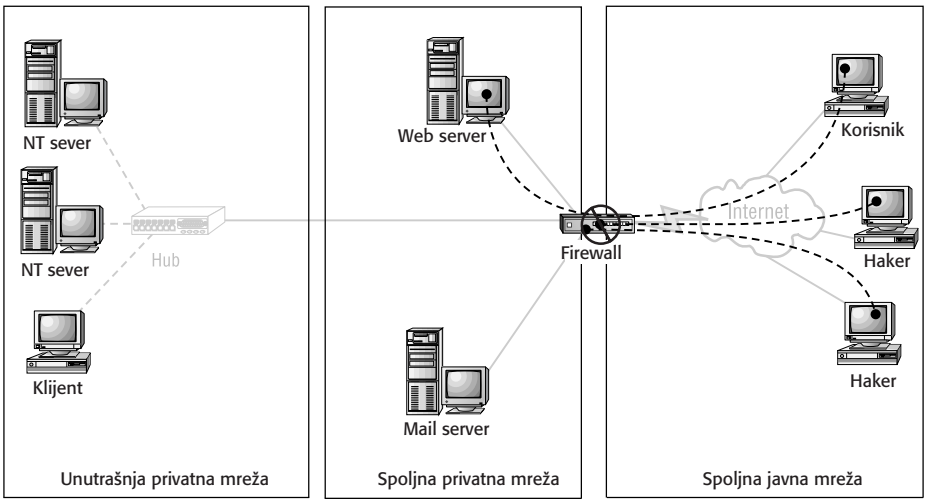
Sa dva nivoa firewall protekcije možete smanjiti izlaganje javnih servera riziku. U osnovi, postavite jedan firewall na Vašu Internet konekciju i osigurajte tako web server. To omogućava jaku bezbednost, a dozvoljava konekcione pokušaje sa Interneta servisima koje pružate.

Između takve mreže i Vaše unutrašnje mreže, smestite drugi firewall sa jačom bezbednosnom politikom koja jednostavno ne dozvoljana pokušaje sa spoljne strane i skriva identite unutrašnjih klijenata. Slika 1.6 prikazuje dva nivoa zaštite mreže sa dva firewalla



Slika 1.6
Dva firewalla postavljena tako da štite kompletnu mrežu

Najveći broj firewall proizvoda dozvoljava upotrebu demilitarizovanih zona, koje omogućavaju funkcionalnost posedovanja dva firewalla tako što sadrže različite bezbednosne politike za svaki postavljeni interfejs na firewallu. Sa tri postavljena interfejsa -spoljna mreža, unutrašnja mreža i mreža javnog servera - možete podesiti Vašu bezbednosnu politiku da blokira pokušaje konekcije na Vašu unutrašnju mrežu, ali možete i zaobići pojedine protokole do Vaših javnih servera. Ovo omogućava funkcionalnost dva firewalla korišćenjem samo jednog proizvoda. Ponekad se koristi i naziv *trostruko udomljni firewall*. Slika 1.7 prikazuje trostuko udomljeni firewall sa različitio podešenim bezbednostima za svaku mrežu.



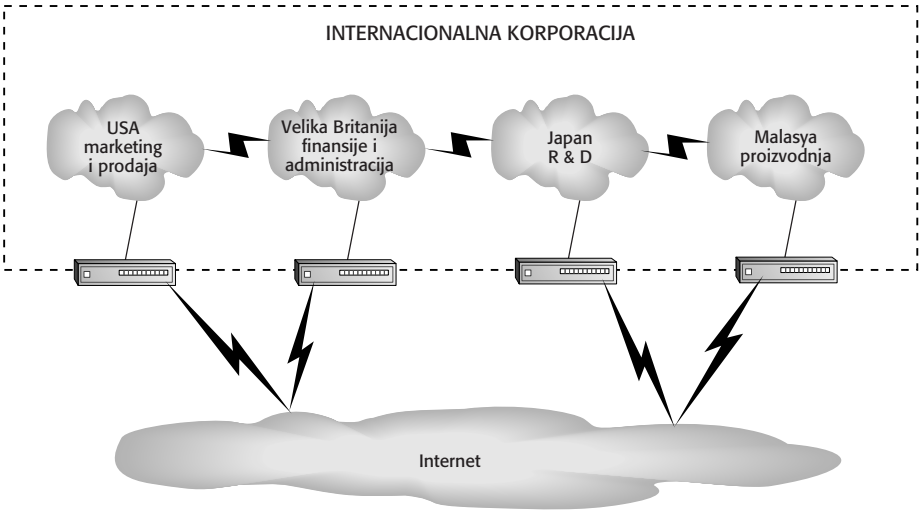
Slika 1.7
DMZ firewall omogućava različitu bezbednost za različite potrebe

NAPOMENA

Ukoliko želite da obezbedite javne servise i zaštitite unutrašnju mrežu, uvek koristite DMZ firewall ili dvostruke firewalle. Svaka bezbednosna politika zahteva svoj sopstveni firewall ili mrežni interfejs.

Enterprise firewall

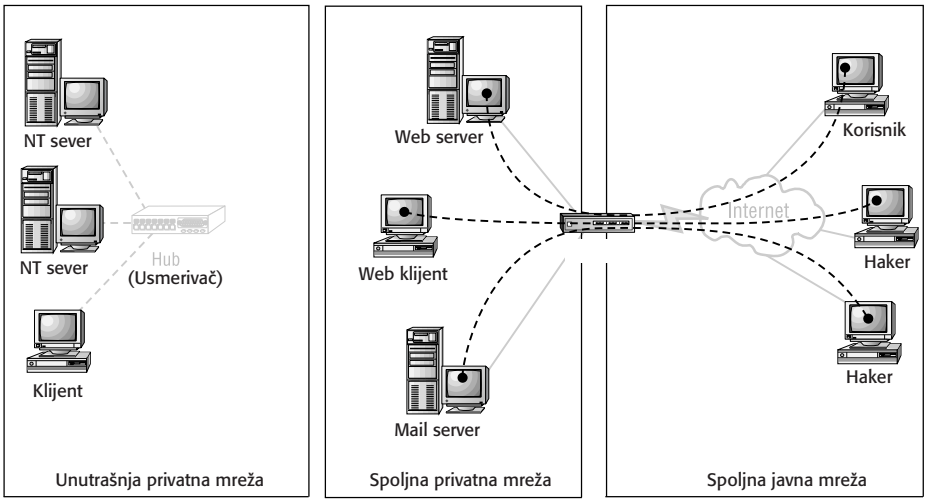
Enterprise firewalli su proizvodi koji dele jednu centralnu firewall politiku na više firewalla. Enterprise firewalli Vam dozvoljavaju da zadržite centralnu kontrolu bezbednosne politike, bez brige o tome da li je politika korektno implementirana na svakom firewallu u Vašoj organizaciji. Politika firewalla je obično zasnovana na bezbednosti radne stanice, a zatim replicirana na svaki firewall u okviru Vaše organizacije, koristeći neke od metoda bezbednosne autentifikacije. Slika 1.8 prikazuje preuzeće sa više firewalla, po jedan na svakoj Internet konekciji.



Slika 1.8
Više firewalla u preduzeću

Diskonekcija

Da biste korisnicima ponudili servis na Internetu i pristup unutrašnjoj mreži, nemojte povezivati Vašu privatnu mrežu na Internet. Najbolje je imati ih odvojene. Slika 1.9 prikazuje unutrašnju mrežu koja nije povezana sa Internetom.



Slika 1.9
Bezbednosni model diskonekcije nudi najveću zaštitu od upada sa Interneta.

Pošto ne postoji veza između Interneta i unutrašnje mreže, ovim metodom se dobija potpuna bezbednost. Javni serveri za web, FTP i poštu se nalaze zajedno sa nekoliko klijenata na malom mrežnom segmentu, povezanom na Internet. Klijentske radne stanice sadrže e-mail, news i web pretraživače, ali ne i osetljive podatke. Da bi proveravali elektronsku poštu, pretraživali web ili radili bilo šta drugo na Internetu, zaposleni moraju doći do spoljnih klijentskih radnih stanica.

Ovaj metod ima tri veoma važne prednosti:

- Privatna mreža je apsolutno bezbedna. Podaci se ne mogu slobodno prenositi između spoljne i unutrašnje mreže. Možete uzeti u obzir postavljanje prenosivog medijuma za skladištenje podataka velikog kapaciteta na jednom od klijenata ukoliko postoji potreba za prenosom velikih datoteka (ipak, ovo može biti bezbednosni problem).
- Potpuno je besplatno. Ne zahteva poseban softver i sofisticirani hardver. Čak možete postaviti zastarele računare na mesto klijentskih radnih stanica.
- Predstavlja prirodan način da sprečite zaposlene u gubljenju vremena na surfovanje po webu i skidanja sadržaja sa Interneta prouzrokujući time nestabilnost sistema.

I naravno, postoji jedna velika smetnja: zaposleni mrze ovaj način. Oni moraju preći određeni put do pristupnih radnih stanica, koje su karakteristično locirane na jednom centralnom području. Prenošenje podataka, takođe, predstavlja problem. Može stvoriti takozvana "uska grla" (bottlenecks) ukoliko ne postoji dovoljan broj pristupnih stanica. Mnogi korisnici jednostavno neće koristiti javne servise na ovaj način, što smanjuje efikasnost elektronske pošte i drugih važnih poslovnih alata.

I na kraju, metod diskonekcije je najbezbedniji i najneefikasniji način da svoje zaposlene povežete na Internet.

UPOZORENJE

Ukoliko koristite bezbednosni model diskonekcijom, može se desiti da Vaši zaposleni prekrše politiku bezbednosti i povežu se modemom na Internet. Budite sigurni da Vaša bezbednosna politika to sprečava i da zaposleni razumeju zašto ste izabrali baš ovaj model.

Ne povezujte svoju mrežu na javne mreže ukoliko postoji način da se to izbegne. Da biste povezali svoje korisnike sa Internetom, koristite mrežni model diskonekcijom. Da biste ponudili informacije o svojoj kompaniji, koristite FTP i web servise javnih agencija radije nego računare na unutrašnjoj mreži. Ovakav način Vas štedi rizika neovlašćenog pristupa Vašoj mreži.

PRIMER

Načini korišćenja firewalla

Nedavno su nas angažovali da izvedemo hakerski napad u cilju provere zaštite mreže jedne kompanije "slavnog imena", koja je angažovala drugu multinacionalnu kompaniju za zaštitu. Servis bezbednosti se sastojao od snažne mašine bazirane na UNIX operativnom sistemu postavljene na strani klijenta, a posao administracije, nadgledanje firewalla i hakerskih napada se obavljao sa udaljene lokacije.

Kada smo počeli napad, koristili smo tradicionalnu metodu skeniranja portova da bismo odredili šta se sve može videti na mreži klijenta. Skeniranje portova se lako detektuje i jedan je od napada za koji proizvođač zaštite pruža nadgledanje. Rezultat je otkrio moguću slabost (port 139 je bio otvoren ka jednom od unutrašnjih servera zbog "promene bezbednosne politike" - više o tome kasnije). Zatim smo koristili još jedan uobičajeni metod za eksploatisanje ovakve slabosti, automatsko pogađanje lozinke preko Interneta, uz pomoć uobičajenih listi lozinki. Ovu metodu je, takođe, lako detektovati i posebno je navedena na listi hakerskih tehnika za koje proizvođač servisa nudi nadgledanje i zaštitu. Listu lozinki koju smo koristili su specijalno kreirali hakeri analizom stotine hiljada eksploatisanih korisničkih naloga. Hakeri su kreirali listu prema statičkom rangiranju uobičajenosti lozinki i po tom redosledu napravili listu. Dok smo mi još uvek objašnjavali klijentu nemogućost pogađanja ovom metodom ukoliko se koriste složene lozinke, naš skener za automatsko pogađanje lozinke je već, uz pomoć generisane liste, pogodio lokalnu administratorsku lozinku. Kada smo pregledali sadržaj hard diska njihovog web servera, kompletirali smo izveštaj. Klijent je još uvek čekao obaveštenje servisa za nadgledanje bezbednosti. Obaveštenje nikada nije stiglo. Napokon, naš klijent je odustao od čekanja poziva posle dve nedelje i otpustio provajdera usluge.

U jednom drugom slučaju, još jedna naša mušterija se oslanjala na servis filtriranja paketa svog ISP-a. Firma klijenta je bila još uvek mala i nerazvijena, tako da se nalazio u slabijoj finansiskoj situaciji. Mi se nismo mnogo tome protivili .

Kao deo naših servisa za njega, pravili smo periodične hakerske napade na njegov server da bismo se time osigurali da ne postoji lak metod za eksploataciju kojim se može dobiti pristup. Nakon što smo potvrdili ispravnost usluge nekoliko puta, jedan sken je pokazao iznenadni pad servisa, otkrivajući portove NetBIOS sesije njihovog NT servera Internetu. Mapirali smo direktno jedan drajv na njihovom serveru preko Interneta!

Panični poziv njihovom ISP-u je potvrdio da je iz nekog razloga filter bio isključen. ISP nam nije mogao objasniti zašto se ovo desilo i koliko je dugo filter bio isključen. Jednostavno su ponovo uključili servis filrtiranja paketa i izvinili se.

Naš klijent je odlučio da je potrebno da sami administriraju bezbednost, pošto se ISP-u očigledno nije moglo verovati. Da bismo smanjili troškove na najmanji mogući nivo, preporučili smo firewall zasnovan na Linux operativnom sistemu ili samo računar sa Linux operativnim sistemom. Klijent se nije baš snalazio sa korisničkim interfejsom, pa je stoga odlučio da pređe na rešenje sa firewallom zasnovanom na Windows NT operativnom sistemu. Nabavili smo mašinu koju pokreće Windows NT Workstation i instalirali CheckpointFirewall-1. Iako je ovo rešenje skuplje, interfejs koji pruža je daleko lakši za upotrebu. Uspeli smo i da obučimo klijenta administraciji politike bezbednosti bez pomoći savetnika, što je dodatno smanjilo ukupne troškove. Oni sada imaju pouzdanu i bezbednu vezu sa Internetom.