1

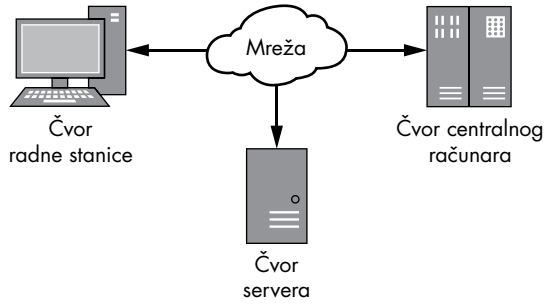
OSNOVE UMREŽAVANJA

Da biste napadali mrežne protokole, treba da razumete osnove umrežavanja računara. Što bolje shvatite kako se tipične mreže grade i funkcionišu, lakše ćete to znanje primeniti na hvatanje mrežnog saobraćaja, analizu i iskorišćavanje ranjivosti novih protokola.

Ovo poglavlje je uvod u osnovne koncepte mreža, sa kojima se svakodnevno srećete pri analizi mrežnih protokola. Ono će vam pomoći da utemeljite način razmišljanja o mrežnim protokolima i da tokom analize lakše pronađete bezbednosne propuste koji su vam ranije bili nepoznati.

Arhitektura i protokoli mreža

Hajde da se prvo pozabavimo osnovnim terminima umrežavanja i postavimo najvažnije pitanje: šta je mreža? *Mreža* (engl. *network*) je skup dvaju ili više računara koji se povezuju da bi delili informacije. Uobičajeno je da se svaki povezani uređaj na mreži naziva čvorom (engl. *node*), kako bi se koncepti mogli primenjivati na razne vrste uređaja. Na slici 1-1. prikazan je jednostavan primer.



Slika 1-1: Jednostavna mreža sa tri čvora

Na slici su prikazana tri čvora povezana u zajedničku mrežu. Svaki čvor može imati drugačiji operativni sistem ili hardver. Međutim, sve dok se na nekom čvoru poštuje skup pravila, ili *mrežni protokol* (engl. *network protocol*), taj čvor može da komunicira sa drugim čvorovima u mreži. Da bi se komunikacija odvijala na ispravan način, svi čvorovi u mreži moraju da poštuju isti mrežni protokol.

Mrežni protokol služi za obavljanje mnogih funkcija, uključujući jednu ili više od sledećih:

Održavanje stanja sesije Protokolima se obično implementiraju mehanizmi za pravljenje novih veza i ukidanje postojećih.

Identifikovanje čvorova preko adresiranja Podaci se moraju prenositi na ispravan čvor mreže. Nekim protokolima se implementira mehanizam za adresiranje kojim se identifikuju određeni čvorovi ili grupe čvorova.

Kontrolisanje toka Količina podataka koja se prenosi kroz mrežu ograničena je. Protokolima se mogu implementirati načini za upravljanje tôkom podataka, kako bi se povećala propusna moć i smanjilo kašnjenje.

Garantovanje redosleda prenesenih podataka Za mnoge mreže se ne može garantovati da će redosled u kome se podaci šalju odgovarati redosledu u kome se oni primaju. Protokol može promeniti redosled podataka i obezbediti njihov ispravan redosled pri isporuci.

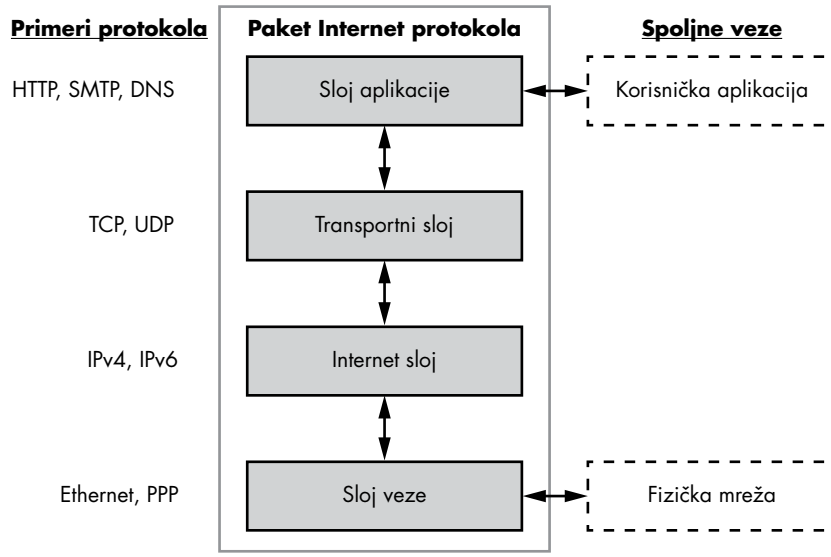
Otkrivanje i ispravljanje grešaka Mnoge mreže nisu potpuno pouzdane pa podaci mogu da se oštete. Važno je da se to oštećenje otkrije i, u idealnom slučaju, ispravi.

Formatiranje i kodiranje podataka Podaci nemaju uvek onaj format koji je pogodan za prenos preko mreže. Protokolom se mogu definisati načini kodiranja podataka, kao što je kodiranje engleskog teksta u obliku binarnih vrednosti.

Paket internet protokola (IPS)

TCP/IP je de facto protokol koji se koristi u savremenim mrežama. Iako TCP/IP možete posmatrati kao jedinstven protokol, on je zapravo kombinacija dvaju protokola: *protokola za kontrolu prenosa* (engl. *Transmission*

Control Protocol, TCP) i *internet protokola* (engl. *Internet Protocol, IP).* Ova dva protokola formiraju deo *paketa internet protokola* (engl. *Internet Protocol Suite, IPS),* konceptualnog modela po kome mrežni protokoli šalju mrežni saobraćaj preko interneta i u kome se mrežna komunikacija može raščlaniti u četiri sloja, kao što je prikazano na slici 1-2.



Slika 1-2: Slojevi paketa internet protokola

Ova četiri sloja formiraju *skup protokola* (engl. *protocol stack*). U nastavku se objašnjava svaki sloj IPS-a:

Sloj veze (sloj 1) Ovo je sloj najnižeg nivoa i njime se opisuju fizički mehanizmi koji se koriste za prenos informacija od jednog do drugog čvora u lokalnoj mreži. U najpoznatijije primere spadaju Ethernet protokol (ožičen i bežični), kao i protokol od tačke do tačke (engl. *Point-to-Point Protocol, PPP*).

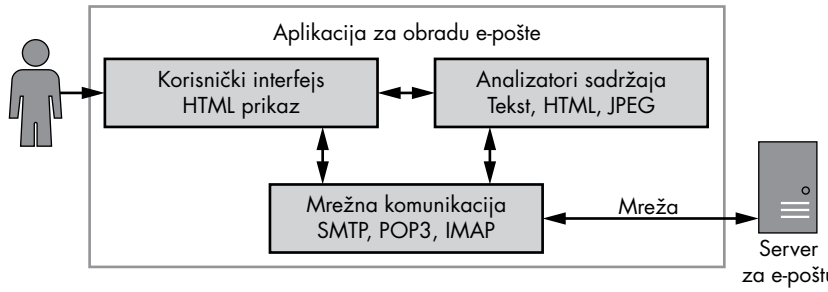
Internet sloj (sloj 2) Ovaj sloj sadrži mehanizme za adresiranje čvorova mreže. Za razliku od sloja 1, čvorovi ne moraju da se nalaze u lokalnoj mreži. Ovaj nivo sadrži IP; stvarni protokoli koji se koriste u savremenim mrežama mogu biti verzija 4 (IPv4) ili verzija 6 (IPv6).

Transportni sloj (sloj 3) Ovaj sloj je odgovoran za veze između klijenata i serverâ, čime se ponekad obezbeđuje ispravan redosled paketa, kao i multipleksiranje usluga. Multipleksiranje usluga omogućava da jedan čvor podrži više različitih usluga tako što se svakoj usluzi dodeljuje drugi broj, i taj broj se naziva *priključak* (engl. *port*). Na ovom sloju rade TCP protokol i *protokol za korisničke datagrame* (engl. *User Datagram Protocol, UDP*).

Sloj aplikacije (sloj 4) Ovaj sloj sadrži mrežne protokole, kao što su *protokol za prenos hiperteksta* (engl. *HyperText Transport Protocol, HTTP),* kojim se prenose sadržaji veb-stranica; *jednostavni protokol za prenos elektronske pošte* (engl. *Simple Mail Transport Protocol, SMTP),*

kojim se prenose elektronska pošta i *sistem imenovanja domena* (engl. *Domain Name System, DNS)*, kojim se ime konvertuje u čvor na mreži. U ovoj knjizi bavićemo se prvenstveno ovim slojem.

Svaki sloj je u interakciji samo sa slojem iznad ili ispod, ali moraju da postoje spoljne interakcije sa skupom. Na slici 1-2. prikazane su dve spoljne veze. Sloj veze je u interakciji sa vezom fizičke mreže, prenoseći na fizički medijum podatke kao što su električni ili svetlosni impulsi. Sloj aplikacije je u interakciji sa aplikacijom korisnika: *aplikacija* (engl. *application*) je skup srodnih funkcionalnosti pomoću kojih se korisniku pružaju usluge. Na slici 1-3. prikazan je primer aplikacije za obradu elektronske pošte. Usluga koja se pruža ovakvom aplikacijom jeste slanje i primanje poruka preko mreže.



Slika 1-3: Primer aplikacije za obradu elektronske pošte

Aplikacija se obično sastoji od sledećih komponenata:

Mrežna komunikacija Pomoću ove komponente odvija se komunikacija preko mreže i obrađuju dolazni i odlazni podaci. Za aplikacije za obradu e-pošte najčešće se koriste standardni protokoli kao što su SMTP ili POP3.

Analizatori sadržaja Sadržaj podataka koji se prenose preko mreže najčešće mora da se izdvoji i obradi. Takav sadržaji može da obuhvati tekstualne podatke, kao što je telo e-poruke, ili slike odnosno video zapise.

Korisnički interfejs (engl. *user interface, UI*) UI omogućava da korisnik pregleda primljenu e-poštu i sastavlja nove e-poruke za prenos. U aplikaciji za obradu e-pošte, UI omogućava prikaz e-poruka u veb-čitaču pomoću HTML-a.

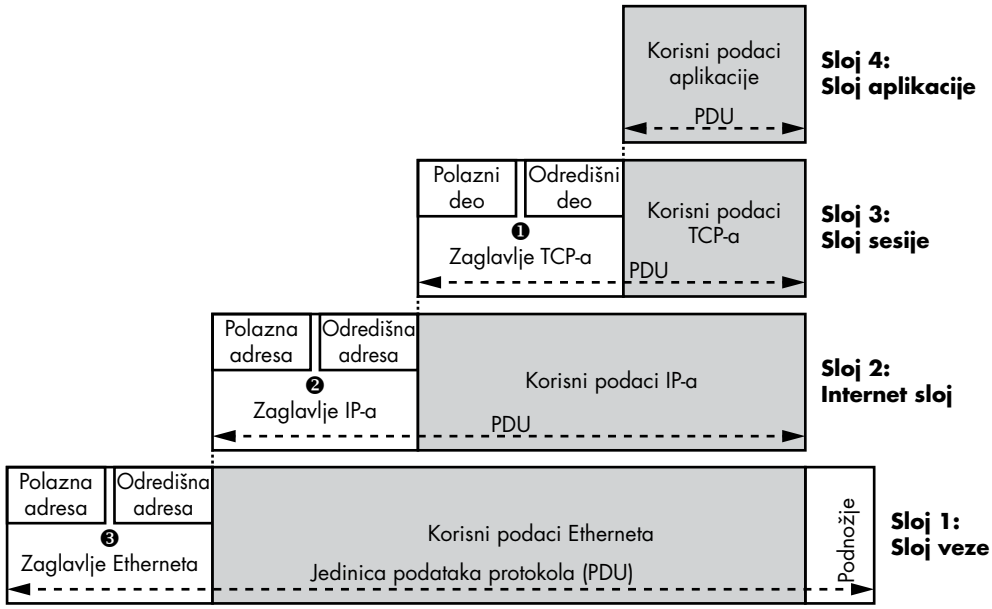
Imajte na umu da korisnik koji komunicira sa korisničkim interfejsom ne mora biti čovek. To može biti i neka druga aplikacija, kojom se automatizuje slanje i primanje e-pošte preko alatke sa komandnom linijom.

Kapsuliranje podataka

Svaki sloj u paketu internet protokola gradi se na sloju ispod i može da kapsulira podatke iz sloja iznad tako da oni mogu da se premeštaju iz jednog sloja u drugi. Podaci koje prenosi svaki sloj nazivaju se *jedinica podataka protokola* (engl. *protocol data unit, PDU).*

Zaglavlja, podnožja i adrese

PDU u svakom sloju sadrži korisne podatke koji se prenose. Uobičajeno je da se na početak korisnih podataka stavi *zaglavlje* (engl. *header*), koje sadrži informacije potrebne za prenos takvih podataka, kao što je *adresa* (eng. *address*) polaznih i odredišnih čvorova na mreži. Ponekad jedinica podataka protokola sadrži i *podnožje* (engl. *footer*), koje se dodaje na kraj korisnih podataka i sadrži vrednosti pomoću kojih se obezbeđuje ispravan prenos, kao što su informacije o otkrivanju grešaka. Na slici 1-4. prikazano je kako su jedinice podataka protokola raspoređene u paketu internet protokola.



Slika 1-4: Kapsuliranje podataka u IPS-u

Zaglavlje TCP-a sadrži broj polaznog i odredišnog priključka ❶. Ti brojevi priključaka omogućavaju da jedan čvor ima više jedinstvenih mrežnih veza. Brojevi priključaka za TCP (i UDP) kreću se u rasponu od 0 do 65535. Većina brojeva priključaka se po potrebi dodeljuje novim vezama, ali neki brojevi imaju posebna zaduženja, kao što je priključak 80 za HTTP. (Aktuelnu listu dodeljenih brojeva priključaka možete pronaći u datoteci */etc/services* na većini operativnih sistema srodnih Unixu.) Korisni podaci TCP-a i zaglavlje zajedno se nazivaju *segment*, dok se korisni podaci UDP-a i zaglavlje nazivaju *datagram*.

IP koristi polaznu i odredišnu adresu ❷. *Odredišna adresa* (engl. *destination address*) omogućava da se podaci šalju na poseban čvor u mreži. *Polazna adresa* (engl. *source address*) omogućava da prijemnik podataka zna koji je čvor poslao podatak i da prijemnik odgovori pošiljaocu.

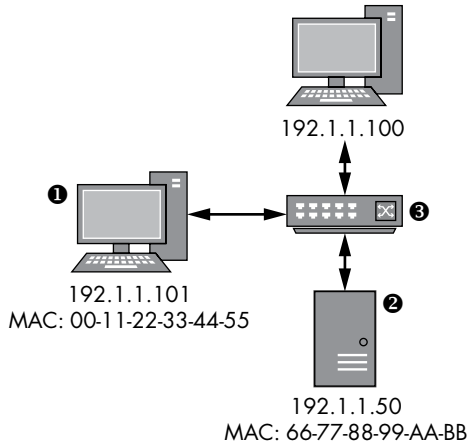
IPv4 koristi 32-bitne adrese, što ćete najčešće viđati u obliku zapisa od četiri broja razdvojena tačkama, kao što je 192.168.10.1. IPv6 koristi 128-bitne adrese, jer 32-bitne adrese nisu dovoljne za broj čvorova

na savremenim mrežama. IPv6 adrese se obično pišu u heksadecimlnim brojevima razdvojenih dvotačkama, kao što je fe80:0000:0000:0000:897b:581e:44b0:2057. Dugi znakovni nizovi sa brojevima 0000 sažimaju se u dve dvotačke. Na primer, prethodna IPv6 adresa se može napisati i kao fe80::897b:581e:44b0:2057. Korisni podaci IP-a i zaglavlje zajednički se nazivaju *paket* (engl. *packet*).

I Ethernet sadrži polazne i odredišne adrese ❸. Ethernet koristi 64-bitnu vrednost koja se naziva MAC adresa, ili *adresa za upravljanje pristupom medijumima* (engl. *Media Access Control*), a koja se obično zadaje tokom proizvodnje Ethernet adaptera. MAC adrese se najčešće pišu kao nizovi heksadecimalnih brojeva razdvojenih crtama ili dvotačkama, kao što je 0A-00-27-00-00-0E. Korisni podaci Ethernet-a, uključujući zaglavlje i podnožje, zajednički se nazivaju *okvir* (engl. *frame*).

Prenos podataka

Opišimo ukratko kako se podaci prenose sa jednog čvora na drugi pomoću modela za kapsuliranje podataka IPS-a. Na slici 1-5. prikazuje se jednostavna Ethernet mreža sa tri čvora.



Slika 1-5: Jednostavna Ethernet mreža

U ovom primeru, čvor ❶ sa IP adresom 192.1.1.101 želi da pošalje podatke pomoću IP-a na čvor ❷ sa IP adresom 192.1.1.50. (*Komutator* (engl. *switch*) ❸ prosleđuje Ethernet okvire među svim čvorovima u mreži. Komutatoru nije potrebna IP adresa, jer radi samo u sloju veze.) Evo šta je potrebno da bi se podaci poslali sa jednog čvora na drugi:

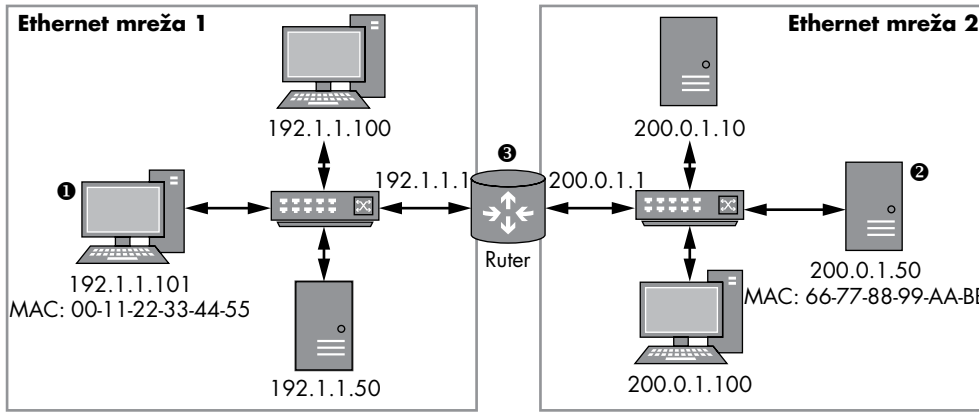
1. Čvor ❶ mrežnog skupa operativnog sistema kapsulira podatke aplikacije i transportnog sloja, i pravi IP paket sa polaznom adresom 192.1.1.101 i odredišnom adresom 192.1.1.50.
2. U ovoj tački operativni sistem može da kapsulira IP podatke kao Ethernet okvir, ali ne mora da zna MAC adresu odredišnog čvora. On može da zatraži MAC adresu za određenu IP adresu pomoću

protokola za razrešavanje adresa (engl. *Address Resolution Protocol, ARP*), koji šalje zahtev svim čvorovima mreže da nađu MAC adresu za odredišnu IP adresu.

3. Kada čvor ❶ primi ARP odgovor, on može da napravi okvir, zadajući lokalnu MAC adresu 00-11-22-33-44-55 kao polaznu, a 66-77-88-99-AA-BB kao odredišnu adresu. Novi okvir se prenosi preko mreže i prima ga komutator ❸.
4. Komutator prosleđuje okvir odredišnom čvoru, koji će raspakovati IP paket i potvrditi da je odredišna IP adresa odgovarajuća. Nakon toga se korisni podaci IP-a izdvajaju i prosleđuju u skup, kako bi ih primila aplikacija koja ih očekuje.

Rutiranje u mreži

Za Ethernet je potrebno da svi čvorovi budu direktno povezani u istu lokalnu mrežu. Taj zahtev predstavlja glavno ograničenje za stvarnu globalnu mrežu, jer nije praktično da se svaki čvor fizički povezuje sa svim ostalim čvorovima. Umesto da se traži da svi čvorovi budu direktno povezani, polazne i odredišne adrese omogućavaju da se podaci *rutiraju* (engl *routing*) kroz različite mreže, sve dok ne stignu na traženi odredišni čvor, kao što je prikazano na slici 1-6.



Slika 1-6: Primer rutirane mreže u kojoj su povezane dve Ethernet mreže

Na slici 1-6. prikazane su dve Ethernet mreže, svaka sa zasebnim opsegom IP mrežnih adresa. U nastavku se opisuje kako IP koristi ovaj model da pošalje podatke iz čvora ❶ mreže 1 u čvor ❷ mreže 2.

1. Čvor ❶ mrežnog skupa operativnog sistema kapsulira podatke aplikaciju i transportnog sloja, i pravi IP paket sa polaznom adresom 192.1.1.101 i odredišnom adresom 200.0.1.50.
2. Mrežni skup treba da pošalje Ethernet okvir, ali zbog toga što odredišna IP adresa ne postoji ni na jednoj Ethernet mreži sa kojom je čvor povezan, mrežni skup proverava *tabelu za rutiranje* (engl. *routing*

table) svog operativnog sistema. U ovom primeru, tabela za rutiranje sadrži element za IP adresu 200.0.1.50. Element pokazuje da ruter ❸ na IP adresi 192.1.1.1 zna kako da stigne na tu odredišnu adresu.

3. Operativni sistem koristi ARP da potraži MAC adresu rutera na adresi 192.1.1.1 i prvobitni IP paket se kapsulira u Ethernet okvir sa tom MAC adresom.
4. Ruter će primiti Ethernet okvir i raspakovati IP paket. Kada ruter proveri odredišnu IP adresu, utvrdiće da IP paket nije upućen ruteru, nego drugom čvoru u drugoj povezanoj mreži. Ruter će potražiti MAC adresu na adresi 200.0.1.50, kapsulirati prvobitni IP paket u novi Ethernet okvir i poslati ga u mrežu 2.
5. Odredišni čvor će primiti Ethernet okvir, raspakovati IP paket i obraditi njegov sadržaj.

Ovaj proces rutiranja može se ponoviti više puta. Na primer, da ruter nije bio direktno povezan s mrežom koja sadrži čvor 200.0.1.50, on bi pogledao u svoju tabelu za rutiranje i odredio sledeći ruter koji može da pošalje IP paket.

Jasno je da bi bilo nepraktično kada bi svaki čvor u mreži znao kako da stigne do svakog drugog čvora na internetu. Ako nema eksplicitno definisanog odredišnog elementa za rutiranje, operativni sistem šalje podrazumevani element tabele za rutiranje, koji se naziva *podrazumevani mrežni prolaz* (engl. *default gateway*) i sadrži IP adresu rutera koji može da prosledi IP pakete na odredište.

Moj model za analizu mrežnih protokola

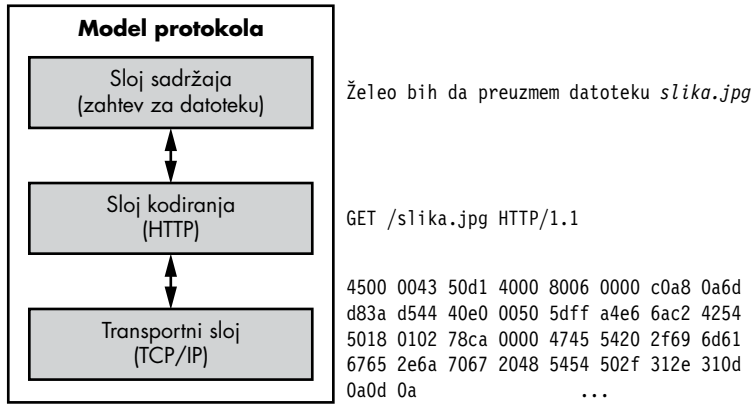
Paketom internet protokola opisuje se kako radi mrežna komunikacija; međutim, za potrebe analize, većina IPS modela nije relevantna. Ponašanje mrežnog protokola aplikacije lakše ćete razumeti ako upotrebite moj model. On sadrži tri sloja (slika 1-7), kojima se ilustruje način na koji bih ja analizirao neki HTTP zahtev.

U nastavku su tri sloja mog modela:

Sloj sadržaja Sadrži značenje predmeta komunikacije. Na slici 1-7. to podrazumeva formiranje HTTP zahteva za datoteku *slika.jpg*.

Sloj kodiranja Sadrži pravila za upravljanje načinom predstavljanja sadržaja. U ovom primeru, HTTP zahtev se kodira kao HTTP GET zahtev, u kome se zadaje datoteka koja se preuzima.

Transportni sloj Sadrži pravila za upravljanje načinom prenosa podataka sa jednog čvora na drugi. U ovom primeru, HTTP GET zahtev se šalje preko TCP/IP veze na priključak 80 udaljenog čvora.

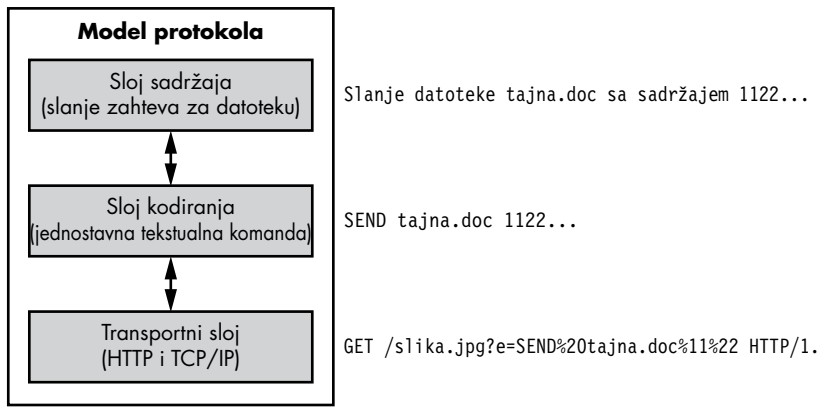


Slika 1-7: Moj konceptualni model protokola

Kada se model ovako raščlani, smanjuje se složenost protokola karakterističnih za aplikacije i omogućava da se iz mrežnog protokola izdvoje detalji koji nisu relevantni. Na primer, pošto nas ovde ne zanima kako se TCP/IP šalje na udaljeni čvor (podrazumevamo da će tamo već nekako stići), posmatramo TCP/IP podatke kao binarni prenos koji funkcioniše.

Da biste shvatili zašto je koristan ovaj model protokola, pogledajte sledeći primer: zamislite da proveravate da li je mrežni saobraćaj na udaru zlonamernog softvera. Otkrili ste da zlonamerni softver koristi HTTP da dobije komande od operatera preko servera. Na primer, operater može zatražiti da zlonamerni softver nabroji sve datoteke na zaraženom disku. Spisak datoteka se može poslati nazad na server i u toj fazi operater može zatražiti da se otpremi određena datoteka.

Ako bismo protokol analizirali iz perspektive načina na koji bi operator komunicirao sa zlonamernim softverom, kao što je zahtev za otpremanje datoteke, novi protokol bi se raščlanio u slojeve kao na slici 1-8.



Slika 1-8: Konceptualni model za protokol zlonamernog softvera korišćenjem HTTP-a

U nastavku se objašnjava svaki sloj novog modela protokola:

Sloj sadržaja Zlonamerna aplikacija šalje serveru ukradenu datoteku pod nazivom *tajna.doc*.

Sloj kodiranja Kodiranje komande za slanje ukradene datoteke jednostavan je tekstualni niz sa komandom `SEND`, iza koje slede ime datoteke i njeni podaci.

Transportni sloj Protokol koristi parametar HTTP zahteva za prenos komande. On se služi standardnim mehanizmom kodiranja znakovima za procenat, čime mu daje karakteristiku legalnog HTTP zahteva.

Obratite pažnju na to da u ovom primeru nismo uzimali u obzir slanje HTTP zahteva preko TCP/IP protokola; kombinovali smo kodiranje i transportni sloj sa slike 1-7. u transportni sloj na slici 1-8. Iako zlonamerni softver i dalje koristi protokole nižeg nivoa, kao što je TCP/IP, ovi protokoli nisu važni za analizu komande zlonamernog softvera za slanje datoteke. Razlog je taj što HTTP preko TCP/IP-a možemo da posmatramo kao jedan transportni sloj koji funkcioniše i usredsredimo se samo na jedinstvene komande zlonamernog softvera.

Ako posmatranje svedemo samo na one slojeve protokola koje treba da analiziramo, izbeći ćemo suvišan posao i usmeriti se na jedinstvene aspekte protokola. S druge strane, da smo ovaj protokol analizirali korišćenjem slojeva sa slike 1-7, mogli bismo pretpostaviti da zlonamerni softver zahteva samo datoteku *slika.jpg*, jer bi izgledalo da je to sve što se HTTP zahtevom obavlja.

Zaključak

U ovom poglavlju izložen je kratak pregled osnova umrežavanja. Bilo je reči o paketu internet protokola (IPS), uključujući protokole na koje ćete nailaziti u stvarnim mrežama, i opisano je kako se podaci prenose s jednog čvora na drugi u lokalnoj mreži i udaljenim mrežama preko rutiranja. Opisan je i način na koji možete da posmatrate mrežne protokole aplikacija, kako biste se lakše usmerili na jedinstvene funkcije protokola i ubrzali analizu.

U poglavlju 2, osnove umrežavanja ćemo koristiti da bismo savladali hvatanje mrežnog saobraćaja radi analize. Cilj hvatanja mrežnog saobraćaja jeste pristup podacima koji su vam potrebni da biste započeli analizu, utvrdili koji se protokoli koriste, i na kraju otkrili bezbednosne propuste koje možete iskorišćavati da biste pomoću tih protokola provaljivali u aplikacije.