PRIMERI NAPADA NA RAČUNARSKE MREŽE

Računari u računarskim mrežama u većini slučajeva međusobno dele komunikacione kanale. To znači da bilo koji računar u mreži može da primi informaciju koja je namenjena za drugi računar. Proces preuzimanja i snimanja informacija odnosno mrežnih paketa koji se trasportuju mrežom u žargonu se naziva sniffing.

Najpopularniji način povezivanja računara je uz pomoć ethernet protokola koji radi tako da šalje mrežne pakete svim hostovima na istoj liniji. Zaglavlje paketa (engl. packet header) sadrži podatke o adresi ciljnog računara pri čemu samo taj računar treba da primi paket. Za računar koji MTVU lekcijeprihvata sve pakete kaže se da je u zajedničkom modu (engl. promiscuous mode).

Zbog toga što se u standardnom mrežnom okruženju informacije o imenu korisnika i njegovoj lozinki prenose kao otvoren tekst odnosno nešifrovane, jasno je da potencijalnom napadaču nije teško da dođe do ovih podataka analizom mrežnih paketa.

Postoji veliki broj programa za preuzimanje i analizu mrežnih paketa (engl. sniffers) koji su na raspolaganju za različite operativne sisteme do kojih se može veoma lako doći putem Interneta. Zlonamerno korišćenje ovakvih programa zabeleženo je i na našim prostorima, posebno na računarima akademske mreže.

Za Unix operativne sisteme kao sto su SGI, SunOs, Solaris, Linux i sl. na raspolaganju su obično izvorni kodovi ovih programa. Packetman, Interman, Etherman, Loadman, Snoop i Etherfind su samo neki od njih. Za DOS operativni sistem na raspolaganju su Gobbler, Ethdump i Ethload. Sa druge strane, postoje i komercijalni programi za analizu mrežnih paketa kao što su Network General i Microsoft's Net Monitor.

Da bi se otkrio sniffer koji samo prikuplja mrežne pakete bez izmena u mrežnom saobraćaju, potrebno je izvršiti fizičku kontrolu svih ethernet priključaka. Nemoguće je sa udaljenog računara izvršiti proveru računara za koji se sumnja da je u zajedničkom modu. Moguće je takođe pokrenuti sniffer tako da skuplja samo mrežne pakete koji su upućeni računaru na kojem on radi.

Za mrežni operativni sistem Novell 3.11 postoji program koji koristi analizu mrežnih paketa da bi svim korisnicima dodelio superuser korisnički nivo (nivo sa najviše ovlašćenja) ukoliko je superuser trenutno ulogovan na mreži. Da bi se ovakav napad sprečio, neophodno je uključiti potpisivanje mrežnih paketa (engl. packet signature). Ova opcija je u novijim verzijama Novell operativnog sistema po pravilu uključena.

Da bi se sprečila analiza mrežnih paketa, najčešće se koristi kriptografija zajedno sa digitalnim potpisivanjem paketa. Kod operativnih sistema Unix pored mnogih komercijalnih rešenja na raspolaganju je i Kerberos autentifikacioni server koji vrši autentifikaciju korisnika prema serveru i servera prema korisnicima, pri čemu se lozinke ne trasportuju kroz mrežu čak ni u šifrovanom stanju.
Trojanski konji i računarski virusi takođe predstavljaju potencijalnu opasnost po sigurnost mreže. Poznat je slučaj Inernet crva (engl. Internet MTVU lekcijeworm) iz ne tako davne 1988. godine koji je za veoma kratko vreme uspeo da se proširi na veliki broj umreženih računara.

Poseban problem može da bude činjenica da svaki korisnik ima mogućnost da namerno pošalje veliku količinu mrežnih paketa i na taj način ugrozi funkcionalnost mrežnog saobraćaja pa čak i mrežnih čvorova.

Ovakvi napadi poznati su pod nazivom bombardovanja elektronskom poštom (engl. e-mail bombing), a sastoje se u tome da napadač namerno šalje jednu poruku velikom broju korisnika ili jednom korisniku šalje veliku količinu poruka.

Poznat je i SYN-flood napad koji je korišćen za iscrpljivanje resursa računara priključenog na TCP/IP mrežu. Napadač šalje ciljnom računaru zahtev za uspostavljanje TCP veze (SYN) pri čemu je izvorna IP adresa u mrežnom paketu zamenjena nepostojećom ili pripada nekom drugom računaru. Napadač šalje veliki broj ovakvih zahteva kako bi naterao ciljni računar da neprestalno alocira svoje resurse za svaki od zahteva. Po prijemu zahteva ciljni računar alocira resurse potrebne za uspostavljanje i praćenje nove veze i odgovara sa SYN-ACK signalom na nepostojeću adresu. Kako na ovaj signal neće biti odgovora, u zavisnosti od svoje konfiguracije napadnuti računar će više puta bezuspešno pokušavati da šalje SYN-ACK signal. Sve ovo može rezultovati potpunim ili delimičnim onemogućavanjem mrežnih servisa na napadnutom računaru.