prometa koji zadovoljavaju zadani uvjet. Sintaksa tih uvjeta je intuitivna. Ne treba posebno objašnjavati što radi naredba "tcpdump host 192.168.1.1 and port 80 and not \(port https or port ftp\)". Bez obzira na ime, nije ograničen na TCP promet, već podržava i ostale IP protokole. Program je i odličan edukacijski alat. Već i letimični pregled ispisa tipičnog uspostavljanja veze dat će nam jasnu predodžbu što se ustvari događa u komunikaciji, koji su paketi poslani, a koji vraćeni kao odgovor.

Ethereal - detalji, detalji

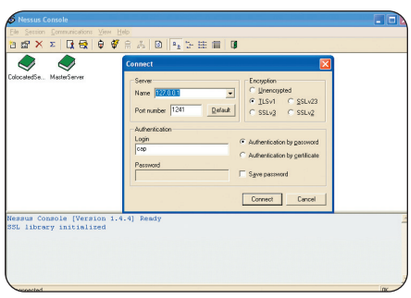
Korak iznad njega su alati koji prikazuju potpuni promet, zajedno sa sadržajem paketa. Osim dijagnostike, mogu se koristiti i u nelegalne svrhe, kao i za narušavanje privatnosti. Ipak, pretpostavlja se da osobe kojoj je dana moć *roota* ima neki stupanj moralne odgovornosti. Ethereal je grafički program koji ispisuje baš sve podatke o paketu do kojih može doći, čime postaje kompletan mrežni dijagnostički alat. Pakete može i logički povezati, a ne samo sekvencijalno izbacivati kako mu pristižu, što je bitno za opterećene mreže. Iz tih paketa se onda rekonstruira tijek podataka kao tekst ili sirovi bitovi.

Može i učitati prethodno snimljenu datoteku s prometom, što postaje osobito bitno kad se vidi koliko raznih mrežnih (pa i komercijalnih) programa slične namjene podržava. Vrlo su snažna i pravila za filtriranje, s većim brojem polja kao kriterija i bogatijom sintaksom, sve zapakirano u bogato grafičko sučelje. Postoji i tekstualni tethereal, iste namjene.

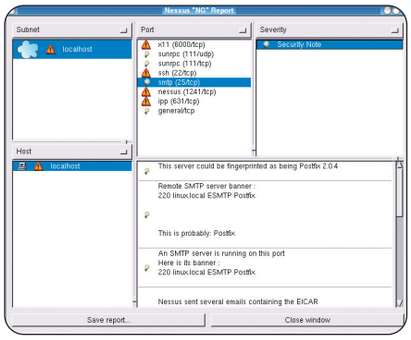
Dsniff - leteće šifre

Set programa objedinjen pod nazivom dsniff teže ćemo nazvati edukacijskim. Iako ne sumnjamo da su nastali iz časnih namjera, već prvo pokretanje glavnog programa bez ikakvih parametara počelo je ispisivati lozinke poslane POP3 protokolom (podržani su i ostali). Svrha ovog programa dakle nije testiranje mreže, već nelegalno skupljanje lozinki i sličnih podataka. Kao takvog ne bi ga ni spominjali, no u istom paketu postoje i drugi programi, također upitne legalnosti, no ipak korisniji.

Tcpkill "ubit" će trenutno aktivnu vezu prema nekom računalu (*tcpkill -9 host nekihost.com*). Sintaksa pravila identična je onoj tcpdump alata, a broj označava prioritet. To je vrlo korisno ako neko računalo pokrene velik prijenos podataka, onemogućivši tako rad drugima. Ako ne želimo biti toliko drastični,



▲ **Klijentsko sučelje Nessusa postoji i za Windows**



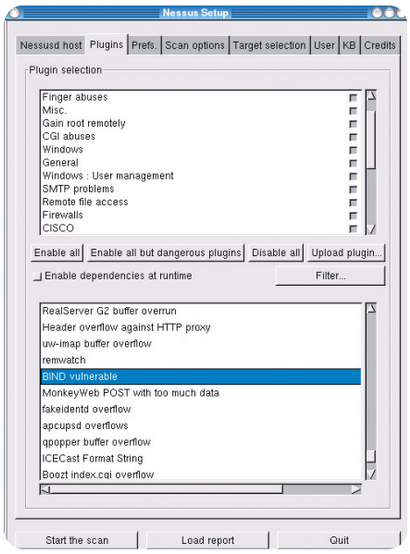
▲ **Ako Nessus pronađe otvoreni port, odmah će nas upozoriti što se iza njega krije i koje bi probleme mogli imati s tim**

možemo koristiti tcpnice koji će vezu samo usporiti. Primjer u kojem ćemo usporiti p2p programe je "tcpnice -n 20 port 6346 or port 6699".

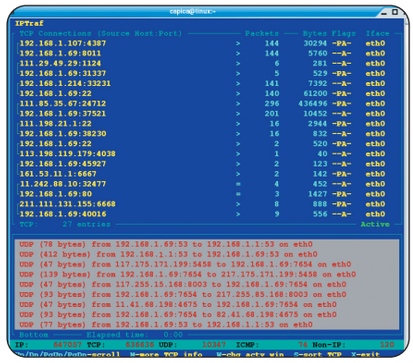
Ono po čemu je ovaj program zaista opasan jest mogućnost dekodiranja SSH kriptirane veze. Dio dsniff kolekcije (čije ime iz razumljivih razloga ne navodimo) presreset će sav promet namijenjen udaljenom računalu, sačuvati ga i poslati dalje, zadržavajući nekriptiranu lozinku. Može vidjeti i bilo koju utipkanu naredbu ili prikaz ekrana. Ne moramo naglašavati koliko je ovo ozbiljno. No, korisniku će se možda pojaviti obavijest "Warning: Host identification has changed", ali nažalost često se ignorira (to ne mora uvijek biti znak tog programa). Također podržava samo danas manje korišten SSH1 protokol (prema *man* stranici programa, to je zato što je autora grizla savjest zbog puštanja nečeg takvog na svjetlo dana).

Nessus - dobri duh

Osim nadzora prometa i čekanja da nas netko napadne, s vremena na vrijeme moramo i provjeriti je li neko računalo ranjivo, kako ne bi dozvolili da se napad zaista i dogodi. Programi koji to mogu saznati održavaju bazu



▲ **Nessus ima velik broj *pluginova* za većinu otkrivenih sigurnosnih rupa**



▲ **Nadzor mreže u stvarnom vremenu dobiva se programom iptraf**

poznatih problema provjeravajući svakog pojedinačno spajanjem na ispitivano računalo. Po nekima najbolji, Nessus je jedan od takvih alata. U osnovi se sastoji od servera i klijenta kao grafičkog sučelja, i to u Javi, GTK i Win32 izvedbi. Server se ne stavlja na ispitivano računalo, već na centralno koje će izvoditi same napade, a klijent je tek način njegova upravljanja. Tako se mogu održavati veći distribuirani sustavi, a svime se može upravljati jednim ili više klijenata. Velika mu je prednost što je vrlo ažuran; nove se informacije dodaju skoro na dnevnoj bazi.

Rad s njim vrlo je ugodan, bez nepreglednog broja opcija koje bi nas samo zbunjivale. Nakon završenog pregleda, osim što ćemo dobiti popis problema, saznat ćemo nešto više o njima, po čemu su problematični, te dobiti savjete kako ih i zakrpati.

Nije dovoljno jasno istaknuto u dokumentaciji, pa ćemo to mi učiniti: bitan korak instalacije serverske strane je i stvaranje korisnika - "nessus-adduser". Možda će biti potrebno stvoriti i licencu: nessus-mkcert. Daljnje korištenje vrlo je jednostavno.

Nmap - referenca

Što bi mi bez starog znanca, nmapa, kojeg čak i Microsoft preporuča za kontrolu Windows računala (spomenuli su da je *open source*). U prošlom smo broju na praktičnom primjeru vidjeli kako možemo doznati popis otvorenih portova na računalu. Taj se posao može proširiti na cijele podmreže, a ako smo nadobudni, i na čitav Internet. Njime vrlo brzo možemo otkriti koja su računala spojena na mrežu (*nmap -sP '192.168.0.*'*), provjeriti vrstu i verziju operacijskog sustava (-O opcija), a i vrstu servisa na određenom portu (-sV). U radu se koristi raznim trikovima kako bi neopažen prošao kroz *firewalle* i razne gore-spomenute sustave za detekciju. Može prikriti tragove (-d *decoy* opcija) kako bi se činilo da zahtjev dolazi s raznih računala.

Sve ga to čini trenutno najpopularnijim alatom te namjene na Linuxu (a očito - po Microsoftu - i šire). Iako neće pomagati savjetima kao Nessus, svoj će posao odraditi brzo i dobro.

Kako smo dosad u izgradnji sustava zaštite išli iznutra prema van, došli smo i do posljednjeg stupnja, potpune blokade, najsturenije dodirne točke prema vanjskom svijetu - Linux *firewalla*. No, o toj opsežnoj temi sljedeći put.