HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Skeniranje računalnih mreža

CCERT-PUBDOC-2007-06-196

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument, koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

***LS&S*, www.lss.hr -** laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Razvojem mrežnih tehnologija porastao je broj korisnika računala i mreže. U korisnike Interneta i računalnih mreža u širem kontekstu svrstava se čitav niz više ili manje upućenih osoba - legitimnih korisnika, ali isto tako se ne može zanemariti i skupina zlonamjernih korisnika usmjerenih na postupke nanošenja štete. Takve zlonamjerne aktivnosti obuhvaćaju sve oblike napada od nedozvoljenog pristupa korisničkim informacijama do napada uskraćivanja resursa ili preuzimanja ovlasti nad ranjivim računalom. Napadači pri tome koriste poznate tehnike analize ranjivosti operacijskog sustava, servisa i Internetu orijentiranih aplikacija, mrežne infrastrukture te ostalih elemenata računalne mreže.

Analiza računalne mreže u kontekstu sigurnosti nužna je za ispravan i neometan rad svih priključenih računala. Sigurnosni pregled računalne mreže ne može se opisati jedinstvenim nizom aktivnosti koje je potrebno poduzeti u tu svrhu, nego se na ovom polju zahtijeva stručnost i razumijevanje problematike mreža u sigurnosnom kontekstu te poznavanje njihovog principa rada.

Većina korisnika računala smatra da su programi poput virusa, crva, tzv. *spyware* i ostalih zlonamjernih aplikacija glavna prijetnja računalima i mrežama. Stručnjaci na području računalne sigurnosti slažu se da prava opasnost prijeti od sigurnosnih nedostataka u postojećim legitimnim aplikacijama koje nisu nadograđene ili nad kojima nisu primijenjene odgovarajuće zakrpe nakon što opis ranjivosti postane javno dostupan. U tom slučaju, ovisno o svojstvima ranjivosti, zlonamjernim korisnicima je ponekad omogućen i neograničen pristup ranjivim sustavima žrtava. Zbog toga su razvijena mnoga programska rješenja koja omogućavaju sigurnosni pregled mreže i računala na njoj, slabih točaka i grešaka u konfiguraciji te pomažu u njihovom otklanjanju.

Dokument je koncipiran tako da od čitatelja ne zahtijeva značajnije poznavanje temeljnih pojmova i elemenata računalne sigurnosti. U početku je dan opći pregled sigurnosti računalnih mreža koji uključuje definiciju sigurnosnih nedostataka i standarde za njihovo imenovanje. Slijedi opis postupaka procjene ranjivosti sustava te obrazloženje potrebe za skeniranjem mreže. Potom dolazi opis često korištenih alata za skeniranje te opis tehnika skeniranja koji uključuje i odgovarajuće primjere.

2. Sigurnost računalnih mreža

2.1. Sigurnosni propusti

U početku razvoja računalne tehnologije ranjivostima su se smatrale pogreške u sklopovlju i programskoj podršci koje napadač može iskoristiti za ostvarenje nekog vlastitog, inače nedozvoljenog, cilja. Iz povijesnih razloga propusti su se nazivali engleskom riječju *bug* - buba, a isti se izraz ustalio i kod nas. S godinama i razvojem tehnologije, definicija se proširila dodavanjem na pogreške u konfiguraciji i postavkama računalnih sustava koje se također mogu iskoristiti za izvođenje zlonamjernih aktivnosti. Sve aktivnosti vezane uz stvaranje i primjenu zakrpa kojima se ispravljaju propusti, ispravke pogrešnih konfiguracija i aktivnosti općenito vezane uz sigurnost sustava danas se svrstavaju u jednu kategoriju - računalna sigurnost.

Ispravljanje sigurnosnih nedostataka sustava, aplikacija i servisa naizgled je jednostavan zadatak. Međutim, veličina administrirane računalne mreže čimbenik je koji izravno utječe na kompleksnost obavljanja tog zadatka. U prosječnoj računalnoj mreži, primjerice neke srednje velike tvrtke, postoji velik broj uredskih računala, korisnika s prijenosnim računalima i specifičnim aplikacijama te poslužitelja čiji je ispravan i neprekidan rad od velike važnosti za nesmetano funkcioniranje čitave organizacije. Dodatno, programska podrška podložna je sigurnosnim propustima, a jednako tako ni proizvođači sklopovske opreme ne izrađuju proizvode vodeći dovoljno brige o sigurnosti. Sve to pred administratore i stručnjake računalne sigurnosti stavlja vrlo zahtjevan zadatak koji u pravilu nikad nije u potpunosti riješen. Povrh svega, nadređeno osoblje kao i krajnji korisnici uvijek očekuju besprijekoran rad računalne potpore, a u slučaju možebitnih kvarova trenutne ispravke.

Praćenje pojavljivanja ranjivosti pojedinih programskih paketa nije jednostavan zadatak i zato su ponuđene usluge pretplatničke liste kod brojnih organizacija koje se bave upravo uočavanjem i kategorizacijom sigurnosnih ranjivosti. Neke od važnijih u svijetu i u Hrvatskoj su:

- SecurityFocus (http://www.securityfocus.com/),
- Secunia (http://secunia.com/),
- iDefense Labs (http://labs.idefense.com/intelligence/) i
- CARNet CERT (http://www.cert.hr/).

U idealnom slučaju proizvođači programske podrške trebali bi sami uočiti propuste unutar svojih paketa prije njihovog izlaska na tržište. Međutim, zbog dinamike koja se nameće u današnjem svijetu, često je potrebno poštivati stroga vremenska ograničenja. To je razlog pojave nedovršenih i nepotpuno verificiranih programskih paketa. Propuste u njima najčešće pronalaze nezavisni istraživači ili članovi istraživačkih timova organizacija koje se bave računalnom sigurnošću. Uobičajena je praksa zadržavanja informacija o uočenom nedostatku sve dok proizvođač ne objavi odgovarajuće ispravke. Unatoč tome, ne događa se rijetko da informacija o pronalasku dođe istovremeno do proizvođača i do javnosti. U tom se slučaju potencijalnim napadačima pruža velika prilika za nesmetano djelovanje.

2.2. CVE

Radi lakše kategorizacije i referenciranja na propuste, razvijen je standard označavanja propusta pod nazivom CVE (eng. *Common Vulnerabilities and Exposures*). Prije njegovog uvođenja proizvođači su imenovali propuste na različite načine, što je administratorima zadavalo velike probleme kod praćenja propusta i izvođenja nadogradnji. Novim standardom za svaki se propust uvodi jedinstveni identifikacijski broj u formatu CVE-<godina>-<broj>. Proizvođače se potiče na korištenje ovakve identifikacije sigurnosnih nedostataka kako bi se umanjili mogući nesporazumi vezani uz proizvoljno imenovanje propusta. Web stranica s opisom standarda i popisom svih zabilježenih propusta dostupna je na adresi http://cve.mitre.org.

2.3. Rizik od sigurnosnih propusta

Rizik zloupotrebe neke od ranjivosti ovisi o nekoliko čimbenika:

- procjeni posljedica možebitne uspješe zlouporabe,

- broju ranjivih sustava unutar organizacije,
- stupnju opasnosti koji prijeti od ranjivih sustava i
- izloženosti organizacije.

Jedan od logički ispravnih načina računanja stupnja rizika je umnožak slijedećih značajki:

- broja ranjivosti odnosno broja sigurnosnih propusta (V - *Vulnerability*),
- broja napada zabilježenog preko neke javne ili privatne usluge organizacije (A - *Attacks*),
- stupnja opasnosti koji je proporcionalan jednostavnosti iskorištavanja propusta (T - *Threat*) i
- izloženosti koja se definira kao mjera dostupnosti i mjera jednostavnosti zaštite (E - *Exposure*).

Iz toga proizlazi jednostavna formula:

```
Rizik = Vulnerability * Attacks * Threat * Exposure
```

Primjerice, za propust Sendmail poslužitelja izračun na nekoj ljestvici od 1 do 5 bi bio sljedeći:

- *V = 5*, jer ima velik utjecaj na cijeli sustav.
- *A = 2*, jer kod za iskorištavanje propusta nije dostupan, a zabilježen je i mali broj napada korištenjem ove ranjivosti.
- *T = 4*, jer se često iskorištavaju propusti zabilježeni kod aplikacija ove tvrtke.
- *E = 5*, jer je poslužitelj dostupan preko Interneta i nije ga lako zaštititi.

U ovom slučaju rizik iznosi 200.

3. Općenito o provjeri ranjivosti

Za uspješnu obranu od zlonamjernih korisnika, sigurnosni stručnjaci, administratori i svi oni koji žele zaštiti svoja računala i računalne mreže trebali bi proći identičan postupak koji prolaze i napadači kako bi ih uspješno onemogućili u njihovim namjerama. U nastavku poglavlja dan je opis postupaka koje se provode tijekom provjere ranjivosti neke računalne mreže.

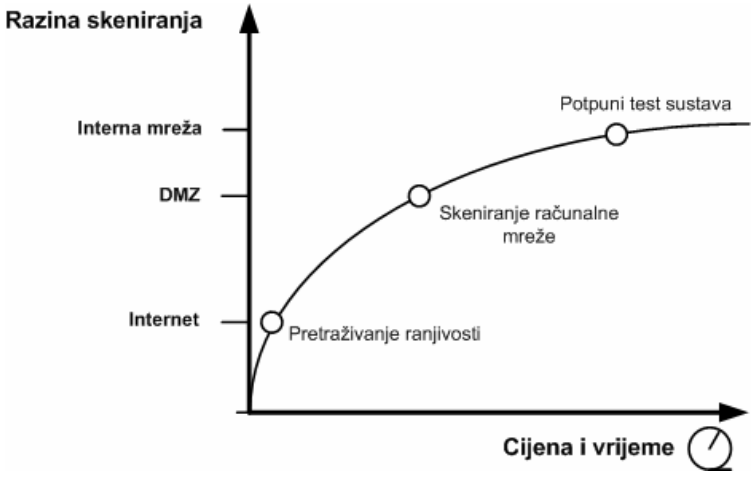
3.1. Definicija

Ranjivosti su prisutne u svim aplikacijama i nije ih moguće izbjeći. Računalna sigurnost kao dio IT tržišta zasigurno ne bi poprimila razmjere koje ima sada da ne postoje sigurnosni propusti. Budući da je čovjek autor svih aplikacija, pogreške su neizbježne, ali se njihov broj može umanjiti pravilnim načinom rada. Zbog toga prisutnost ranjivosti treba prihvatiti kao dio svakodnevnog života u računalnom svijetu i na odgovarajući način se prema tome odnositi.

Provjera ranjivosti izvodi se iz nekoliko razloga:

- radi procjene ranjivosti sustava i izvođenja potrebnih nadogradnji,
- zbog demonstracije razine sigurnosti sustava potencijalnim korisnicima,
- zbog ispunjavanja određenih zahtjeva.

Većina tvrtki koje se bave sigurnošću svojim korisnicima omogućuje različite usluge na području ispitivanja ranjivosti sustava. Slijedećim grafom prikazan je odnos razine procjene ranjivosti u odnosu na utrošeno vrijeme i cijenu.



Slika 1: Omjer dubine skeniranja i cijene

Provjera ranjivosti (eng. *Vulnerability scanning*) koristi automatizirane alate poput *eEye Retina*, *Nessus* i *QualysGuard* koji predstavljaju relativno jeftina rješenja za pronalaženje ranjivosti. Nedostatak im je ograničen broj ranjivosti koje ovako mogu prepoznati, te nemogućnost izvođenja koraka s ciljem poboljšanja sigurnosti.

Skeniranje računalne mreže (eng. *Network security assessment*) prema cijeni, vremenu trajanja i dubini analize nalazi se na sredini izvodivih testova. Obuhvaća automatizirane postupke analize, ali i testove koje izvode educirani sigurnosni stručnjaci. Konačna izvješća o sigurnosnom stanju kontroliranog objekta stvaraju isti stručnjaci te u njima daju profesionalne savjete o načinima poboljšanja sigurnosti.

Testiranje na proboj (eng. *Penetration testing*) obuhvaća potpunu analizu sustava korištenjem svih postojećih metoda provaljivanja, ali zato iziskuje veliku količinu vremena. U skupinu ovih testova pripadaju i socijalni inženjering, provjera sigurnosti bežičnih uređaja te druge metode, ali i svi postupci iz prethodno opisanih metoda.

3.2. Metode

S vremenom se skeniranje mreža podijelilo u četiri koraka koje su prihvatili kako napadači, tako i sigurnosni stručnjaci. Oni su:

- prikupljanje informacija o mreži (eng. *Network enumeration*),
- skeniranje podmreže i određivanje dostupnosti (eng. *Bulk network scanning and probing*),
- pronalaženje ranjivosti (eng. *Investigation of vulnerabilities*) i
- iskorištavanje ranjivosti (eng. *Exploitation of vulnerabilities*).

U nastavku slijedi detaljnije pojašnjenje svakog od njih.

3.2.1. Prikupljanje informacija o mreži

Pretraživanje javno dostupnih usluga je prvi korak kako sigurnosnog pregleda, tako i potencijalnog napada. Ono uključuje pretraživanje web stranica i novinskih grupa, WHOIS usluga dohvaćanja informacija od informacijskih središta (eng. *NIC - Network Information Center*) te dohvat informacija od imenskih poslužitelja (eng. *DNS - Domain Name System*). Kod potonjeg se podrazumijevaju podaci o strukturi mreže i korisnicima do kojih se dolazi bez izravnog pristupa objektu analize.

Ovaj dio postupka napada vrlo je važan jer određuje računala kojima zaštita nije na odgovarajućoj razini. Napadač upoznaje i periferne dijelove mreže kao što su podmreže i računala koja nemaju osobit značaj i često se preko njih usmjerava na ciljana računala ili uređaje. Tvrtke nerijetko zanemaruju takve sustave i koncentriraju se na one javno dostupne - web poslužitelje, poslužitelje elektroničke pošte i slično. Ključne informacije dohvaćene u ovom koraku obuhvaćaju detalje oko internih IP adresa prikupljenih od DNS poslužitelja, daju uvid u strukturu imenovanja računala napadane organizacije (imena domena, poddomena i računala) te odnos između IP adresa i fizičkih lokacija računala. Svi ovi podaci koriste se dalje u strukturiranom skeniranju ciljane mreže i potencijalnih

ranjivosti na njezinim računalima. Daljnje prikupljanje informacija nastavlja se s ciljem saznavanja detaljnih podataka o korisnicima, kao što su, primjerice, adrese elektroničke pošte, telefonski brojevi i fizičke adrese (lokacije) ureda.

3.2.2. Skeniranje podmreže i određivanje dostupnosti

Nakon određivanja javnog adresnog segmenta dodijeljenog ciljanoj mreži, slijedi ispitivanje aktivnih računala i servisa. Za to se koristi skeniranje na razini TCP, UDP i ICMP protokola. Servisi koje se uglavnom traži su HTTP, FTP, SMTP, POP3, ali i brojni drugi. Ključne informacije dohvaćene u ovom postupku su IP adrese aktivnih računala i popis na njima aktiviranih usluga. Moguće je doći i do informacija o postavkama vatrozida ili nekog drugog mehanizma filtriranja. Nakon prikupljanja svih potrebnih podataka u ovom koraku, napadač ili stručnjak za sigurnost mogu započeti tzv. *offline* analizu te pronaći najsvježije sigurnosne propuste u dostupnim servisima.

3.2.3. Pronalaženje ranjivosti

Novi sigurnosni nedostaci raznih programskih paketa uočavaju se svakodnevno. Kao dokaz postojanja nedostatka često se osnovnom opisu prilažu i programski kodovi ili aplikacije koje ranjivost iskorištavaju. Tako se svim zlonamjernim korisnicima daje pristup alatima za izvođenje napada. U uvodnom poglavlju spomenute su značajnije organizacije koje se bave sigurnošću i sigurnosnim preporukama na čijim stranicama se ove informacije i objavljuju. Prethodni korak istraživanja pokrenutih servisa ne daje dovoljne podatke o njihovim postavkama pa je u ovom koraku potrebno obaviti i dio ručnog testiranja. Ključne informacije dobivene ovim korakom obuhvaćaju podatke o prisutnim ranjivostima, ali i alate koji omogućuju njihovo iskorištavanje.

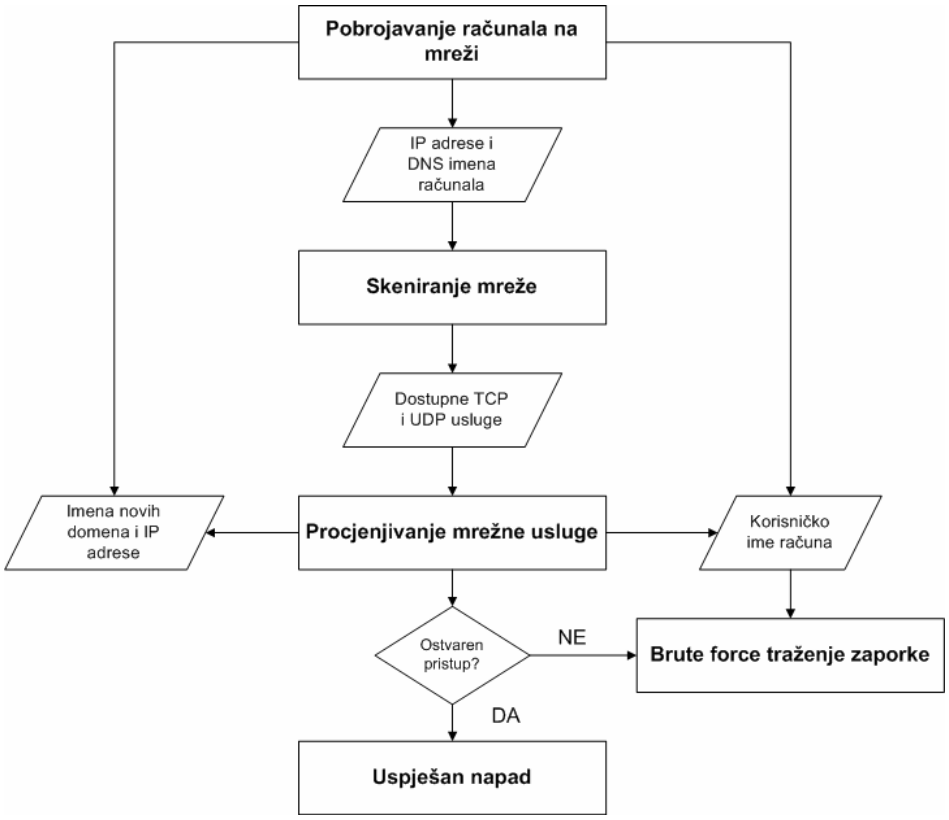
3.2.4. Iskorištavanje ranjivosti

U posljednjem koraku skeniranja mreže podrazumijeva se potpuna pripremljenost napadača odnosno sigurnosnog stručnjaka za izvođenje aktivnosti koje se temelje na iskorištavanju ranjivosti. Slijedi još provođenje samog postupka proboja ciljanog računala, što je u većini zemalja svijeta kazneno djelo. U ovoj poziciji napadač može učiniti nešto od slijedećeg:

- steći prava administratora sustava,
- preuzeti datoteke s korisničkim imenima i zaporkama,
- skriti tragove u dnevnicima (eng. *log*) i osigurati si "stražnji ulaz" kojim ponovo može pristupiti napadnutom računalu,
- preuzeti potencijalno osjetljive podatke i
- postaviti i koristiti alate za izvođenje napada na druga računala u okolici.

3.2.5. Kružna provjera

Procjene ranjivosti velikih računalnih sustava može postati kružni proces ukoliko se testiranja provode bez dovoljno potrebnih informacija. Za vrijeme testiranja mreže mogu se dobiti podaci koje je moguće koristiti u nekom drugom dijelu testiranja. Na slijedećoj slici je prikazan blok dijagram ovog pristupa.



Slika 2: Algoritam kružne provjere ranjivosti

Ovaj blok dijagram započinje procesom pretraživanja mrežnih uređaja nakon čega slijedi opsežno skeniranje mreže i postupak procjene ranjivosti uočenih servisa. Tijekom analize moguće je doći do novih podataka korisnim u nekom od prethodnih koraka.

3.3. Provođenje skeniranja

Sam postupak identificiranja ranjivosti pojedine organizacije je vrlo opsežan i težak zadatak. Za pronalaženje ranjivosti nije dovoljno samo instalirati i pokrenuti automatizirani postupak traženja na nekom mrežnom segmentu. Ovaj je problem mnogo složeniji i zahtijeva osjetno složenije postupke. U današnje vrijeme organizacije se sastoje od velikog broja poslužitelja, još većeg broja računala koji komuniciraju preko mnogobrojnih mrežnih kanala različitih brzina i kapaciteta. Budući da je 95% sigurnosnih provala izravna posljedica neodgovarajućih postavki programske podrške, mnogi ljudi smatraju da je provođenje ispitivanja sigurnosnih ranjivosti suvišan postupak. Međutim, takav stav nije ispravan. U računalnu sigurnost potrebno je neprekidno ulagati jer posljedice možebitnog napada mogu biti goleme.

Skeniranje mreže pod određenim okolnostima može opterećivati kako samu računalnu mrežu, odnosno mrežne resurse, tako i računala koja joj pripadaju. Skeniranje može uzrokovati i stanja u kojima servisi ne rade ispravno ili čak nekontrolirano prestaju s radom. Zato je prilikom sigurnosnog pregleda mreže vrlo važno pridržavati se određenih pravila i obavijestiti potrebno osoblje o provođenju testova.

Tu se podrazumijevaju slijedeće osobe:

- glavna i odgovorna osoba za IT sektor organizacije,
- administrator sustava koje se pregledava,
- administrator programske podrške i
- korisnici testiranih računala.

Kako bi korisnici mogli nesmetano obavljati svoj svakodnevni rad, poželjno je skeniranje mreže obavljati u noćnim satima ili tijekom vikenda.

Skeniranja za koja se pouzdano zna da dovode čitav sustav u DoS (eng. *Denial of Service*) stanje obavezno treba provoditi uz pristanak svih odgovornih osoba i nikako u radno vrijeme jer ova vrsta pregleda sigurno dovodi do zastoja u radu korisnika.

4. Alati

U dijelu koji slijedi opisane su temeljne smjernice vezane uz alate koji se koriste za skeniranje računalnih mreža.

4.1. Operacijski sustavi

Izbor operacijskog sustava koji će se koristiti tijekom procjenjivanja ranjivosti mreže ovisi o vrsti mreža koje će biti testirane, te o dubini analize koja se provodi. Često je potrebno pokrenuti skripte čije je izvođenje jedino moguće na Linux i Unix operacijskim sustavima. U nastavku su opisani često korišteni operacijski sustavi u kontekstu skeniranja računalnih mreža.

4.1.1. Windows

U ovu skupinu ubrajaju se sljedeći sustavi tvrtke Microsoft: NT 4.0, 2000, XP, 2003 Server te noviji sustavi temeljeni na istim tehnologijama. Neke inačice Windows sustava ne omogućuju izravan pristup mrežnom sloju. Međutim, kod pobrojanih inačica programerima je omogućen pristup jezgrinim funkcijama vezanim uz rad s mrežom pa su se pojavili brojni alati prethodno poznati jedino s Linux platformi. Tu su uključeni prvenstveno *nmap*, *dsniff* i *arpspoof*.

4.1.2. Linux

Operacijski sustav Linux najčešći je izbor za većinu sigurnosnih stručnjaka, ali i zlonamjernih korisnika. Linux platforma je sustav otvorenog koda, a jezgra operacijskog sustava osigurava potrebnu potporu za vodeće mrežne tehnologije i protokole. Svi napadi temeljeni na IP protokolu i alati za izvođenje napada mogu se izgraditi i izvoditi na Linux operacijskim sustavima bez većih poteškoća. Razlog tome je postojanje programskih biblioteka poput *libpcap* koje implementiraju sve važne funkcije za korištenje mreže.

4.1.3. MacOS X

Operacijski sustav MacOS X se temelji na BSD sustavima. Ovaj je sustav vrlo sličan Unix okruženju kako sučeljem, tako i načinom izvedbe operacijskog sustava, a sadrži uobičajene naredbene ljuske operacijskog sustava (*sh*, *csh* i *bash)* te korisne mrežne alate poput *telnet, ftp, rpcinfo, snmpwalk, host* i *dig* paketa.
MacOS X operacijski sustav je opskrbljen prevoditeljem izvornog koda za C/C++ jezik te mnoštvom zaglavlja i programskih biblioteka što omogućava izgradnju alata za procjenu ranjivosti. Ovdje su uključena tri vrlo korisna alata: *nmap*, *Nessus* i *Nikto*.

4.1.4. VMware

VMware je vrlo koristan program koji omogućuje izvođenje više instanci operacijskih sustava na jednom računalu. VMware Workstation je potpuno komercijalan paket koji se može koristiti pod Windows i Linux okruženjima.

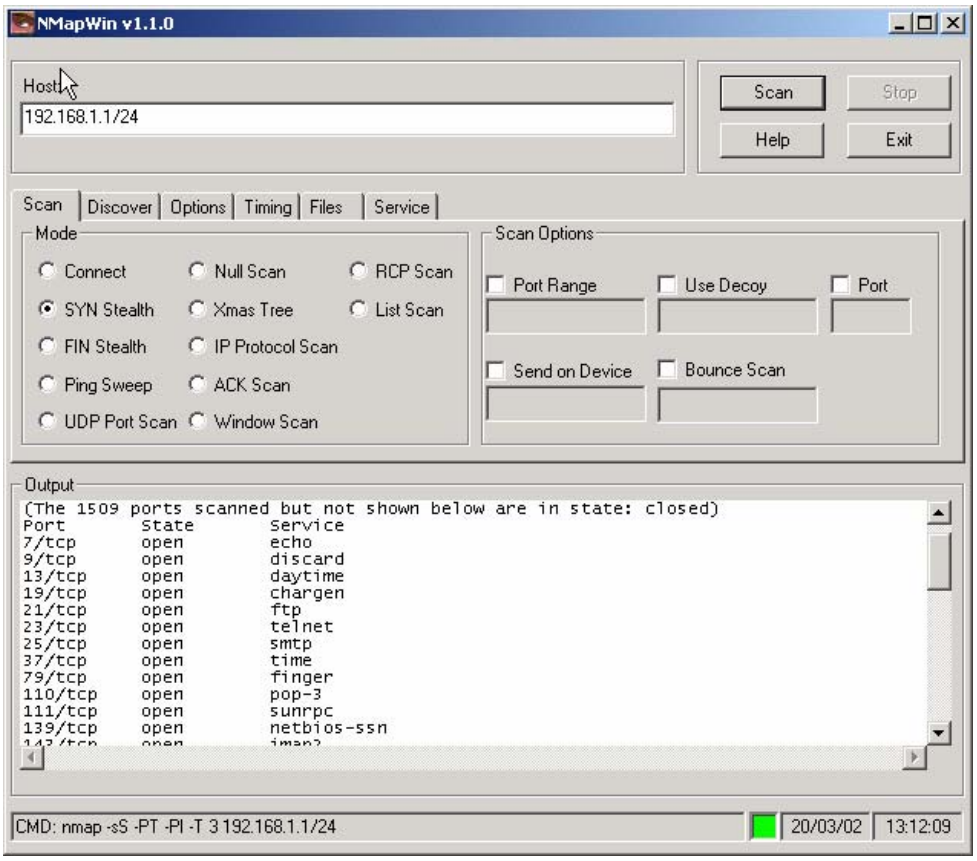
4.2. Alati otvorenog programskog koda

Broj dostupnih besplatnih alata otvorenog koda vrlo je velik. Ovdje su opisani samo najpoznatiji i najčešće korišteni alati.

4.2.1. *nmap*

Za pregled mrežnih priključaka (eng. *port*) razvijeno je mnoštvo alata. Jedan od najpoznatijih jest *nmap* (eng. *Network Mapper*). Radi se o besplatnom alatu otvorenog koda (eng. *Open Source*) kojim je

moguće odrediti koji su servisi pokrenuti na ciljanom računalu. Njegova namjena je procjena i poboljšanje sigurnosti sustava, ali se nerijetko koristi i u zlonamjernim aktivnostima.
Aplikacija sadrži mnoštvo optimizacija u pogledu skeniranja pa je prikladna za korištenje i na velikim računalnim mrežama, a ne samo za testiranje manjeg broja računala kao što je to slučaj s velikim brojem konkurentnih programa. *Nmap* koristi različite mehanizme provjere aktivnosti koje između ostalog uključuju i određivanje dostupnosti određenog računala, operacijskog sustava provjeravanog računala, otvorenih priključaka na tom računalu, vrste korištenog vatrozida i dr. Paket je raspoloživ za većinu danas korištenih operacijskih sustava, a postoji i nekoliko grafičkih sučelja budući da je izvorno paket namijenjen pokretanju u naredbenom retku.
Više informacija o Nmap paketu moguće je naći na njemu posvećenoj stranici: http://insecure.org/nmap/.



Slika 3: Nmap alat u NMapWin grafičkom sučelju

4.2.2. *finger*

Usluga zvana finger dostupna je na TCP priključku 79, a udaljenim korisnicima omogućava dohvat osobnih podataka lokalnih korisnika. Opis protokola dan je u dokumentu RFC 1288 (*The Finger User Information Protocol, December 1991*).
Poslužitelj je implementiran u obliku pozadinske aplikacije najčešće zvane *fingerd* (eng. *finger daemon*), a klijent aplikacija se naziva *finger*. Često je uključena u skup aplikacija koje dolaze sa samim operacijskim sustavom. Zadatak joj je da u korisniku čitljivom obliku prikaže informacije o sustavu ili korisniku nekog udaljenog sustava. Program daje informacije o tome da li je traženi korisnik trenutno prijavljen na sustav, adresu elektroničke pošte korisnika, puno ime i prezime. Pored ovih podataka, *finger* dohvaća i sadržaje `.project` i `.plan` datoteka iz korisnikovog `home` direktorija. Dakako, danas se postavlja pitanje sigurnosti i privatnosti korisnika koje u začetcima razvoja Interneta nije bilo toliko važno. Informacije dostupne ovom uslugom mogu se iskoristiti na različite načine u zlonamjerne svrhe. Pored toga, pozadinska aplikacija koja implementira poslužitelj

može sadržavati sigurnosne nedostatke kojima se napadač može okoristiti. Iz ovih razloga od 90-ih godina do danas ova se usluga sve manje koristi.

4.2.3. Skupina *ping* alata

Ovi alati izvorno su namijenjeni samo određivanju dostupnosti željenog računala čiju se IP ili simboličku adresu poznaje. U nastavku su opisana tri najčešće korištena alata iz ove skupine.

4.2.3.1 *ping*

Ping je alat koji se koristi za testiranje dostupnosti računala putem računalne mreže. Pregled započinje slanjem ICMP "*echo request*" pakete na odredišno računalo te čeka njegov odgovore. Odgovori su ICMP "*echo response*" paketi. Koristeći vremenski interval i brzinu odgovora ping procjenjuje vrijeme kružnog obilaska paketa, koje je najčešće reda veličine milisekunde te prijavljuje gubitak paketa u slučaju izostanka odgovora.
Korištenje je vrlo jednostavno, postoji nekoliko parametara koji se mogu kontrolirati, a na sljedećem ispisu dan je primjer provjere dostupnosti vlastitog računala preko povratnog sučelja i to slanjem ukupno tri paketa za provjeru:

```
C:\>ping 127.0.0.1 -n 3

Pinging 127.0.0.1 with 32 bytes of data:

Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

4.2.3.2 *hping*

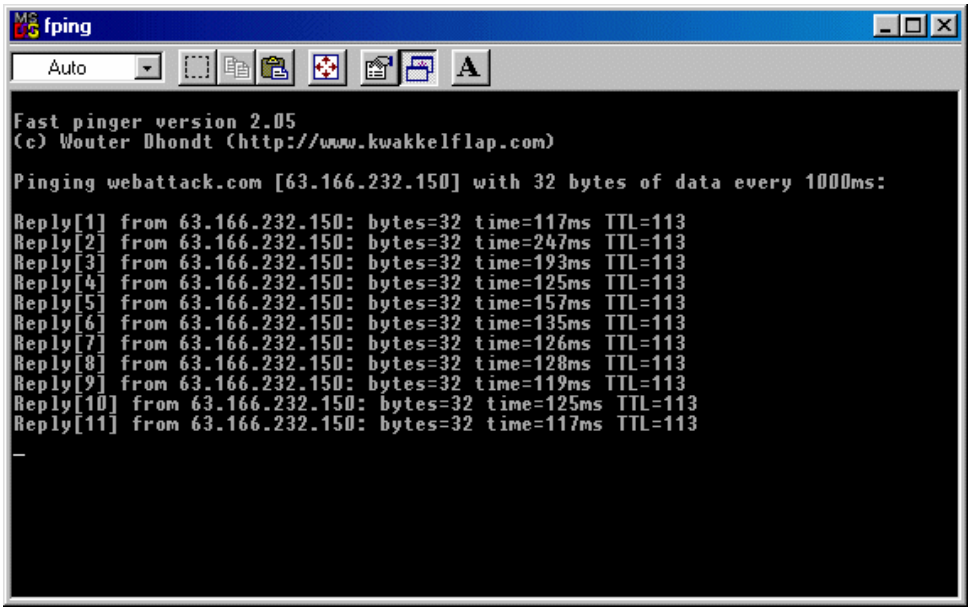
Hping je besplatan alat za generiranje i analizu paketa TCP/IP protokola. Ovaj je paket jedan od alata koji se koriste za ispitivanje sigurnosti i testiranje vatrozida, napredno skeniranje priključaka itd. Nova inačica *hping* alata, imenom *hping3*, podržava i automatizirano izvođenje zadataka definiranih skriptama. Ovo svojstvo korisniku omogućuje pisanje skripti vezanih uz manipulaciju TCP/IP paketima niske razine na jednostavan i pregledan način. *Hping*, poput mnogih alata koji se koriste u računalnoj sigurnosti, koristan je za sigurnosne stručnjake, ali i za zlonamjerne korisnike. Razvijen je za sljedeće operacijske sustave: Linux, FreeBSD, NetBSD, OpenBSD, Solaris, MacOs X i Windows.
U nastavku je dan primjer ispisa dobiven izvođenjem ovog alata.

```
# hping2 --scan known 1.2.3.4
Scanning 1.2.3.4 (1.2.3.4), port known
245 ports to scan, use -V to see all the replies
+----+----------+---------+---+-----+-----+-----+
|port| serv name |  flags  |ttl| id  | win | len |
+----+----------+---------+---+-----+-----+-----+
    9 discard    : .S..A...  64     0 32767    44
   13 daytime    : .S..A...  64     0 32767    44
   21 ftp        : .S..A...  64     0 32767    44
   22 ssh        : .S..A...  64     0 32767    44
   25 smtp       : .S..A...  64     0 32767    44
   37 time       : .S..A...  64     0 32767    44
   80 www        : .S..A...  64     0 32767    44
  111 sunrpc     : .S..A...  64     0 32767    44
  113 auth       : .S..A...  64     0 32767    44
  631 ipp        : .S..A...  64     0 32767    44
3306 mysql      : .S..A...  64     0 32767    44
6000 x11        : .S..A...  64     0 32767    44
6667 ircd       : .S..A...  64     0  3072    44
All replies received. Done.
```

4.2.3.3 *fping*

Fping je program sličan *ping* alatu koji koristi ICMP (eng. *Internet Control Message Protocol*) protokol, da bi odredio dostupnost računala. Od njega se razlikuje utoliko što mu se može zadati proizvoljan broj računala koja je potrebno provjeriti. Isto tako, može se oblikovati datoteka s popisom računala za ispitivanje. Umjesto čekanja na odgovor jednog računala, *fping* djeluje tako da šalje *ping* pakete svim računalima korištenjem algoritma kružnog dodjeljivanja. Ako neko od računala odgovori, ono će biti zabilježeno i uklonjeno s popisa računala koja treba provjeriti. Ukoliko računalo ne odgovori u zadanom roku na jedno ili više upita, smatrati će se nedostupnim.

Za razliku od *ping* aplikacije, *fping* je namijenjen za korištenje u skriptama. Također, izlaz ovog programa je vrlo pregledan i stoga ga je lako analizirati. Na slici ispod dan je jedan takav prikaz.



Slika 4: Demonstracija rada programa *fping*

4.2.4. *Strobe*

Radi se o alatu s područja mrežne sigurnosti zaduženom za pronalaženje otvorenih mrežnih priključaka na provjeravanom računalu ili skupini računala. Razvijen je s posebnim naglaskom na

smanjenje opterećenja mrežnih i računalnih resursa. Arhitektura aplikacije temelji se na paralelnim konačnim automatima. Na računalima s dovoljno pristupnih točaka (eng. *socket*), ovaj program može velikom brzinom skenirati velike mrežne segmente.

4.2.5. *QueSO*

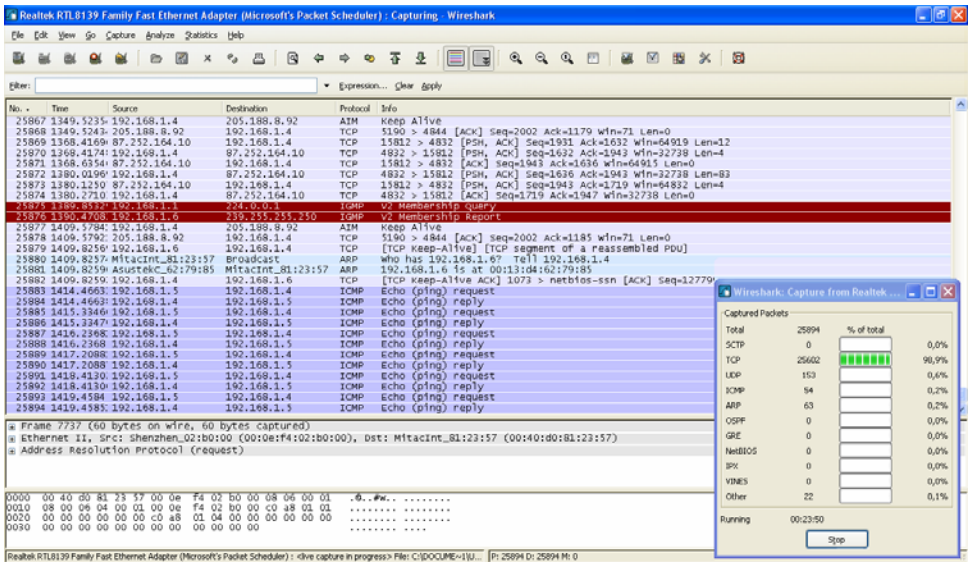
Namijenjen je prvenstveno određivanju pokrenutih operacijskih sustava na računalima čija su IP adresa ili simboličko ime poznati. Njegov rad temelji se na slanju neispravnih paketa prema ispitivanom računalu ili računalima te analizi primljenih odgovora. Pokazalo se da različiti sustavi različito odgovaraju na posebno oblikovane nepredviđene mrežne pakete i upravo tu činjenicu iskorištava ova aplikacija.
Više informacija o QueSO alatu dostupno je na adresi:
http://www.apostols.org/projectz/queso/

4.2.6. *p0f*

Riječ je o još jednoj aplikaciji za prepoznavanje operacijskog sustava ciljanog računala kojemu je poznata adresa. Za razliku od alata za aktivno određivanje operacijskog sustava poput *Nmap* ili *QueSO*, *p0f* djeluje pasivno. To znači da se njegovo prepoznavanje temelji na paketima koje generiraju druge aplikacije, poput web preglednika, raznih poslužitelja, klijenata elektroničke pošte i slično. Kod ovakvog principa prepoznavanja ne generiraju se posebni redundantni paketi pa ga programi namijenjeni sigurnosnoj zaštiti ne mogu uočiti. Zabilježeni paketi sadrže dovoljno informacija za određivanje operacijskog sustava zbog malih, ali postojanih razlika u izvedbi TCP/IP stoga, a katkada i propusta u implementaciji mehanizama namijenjenih mrežnoj komunikaciji.
Detaljnije informacije o alatu dostupne su na adresi:
http://www.stearns.org/p0f/

4.2.7. *Wireshark* (*Ethereal*)

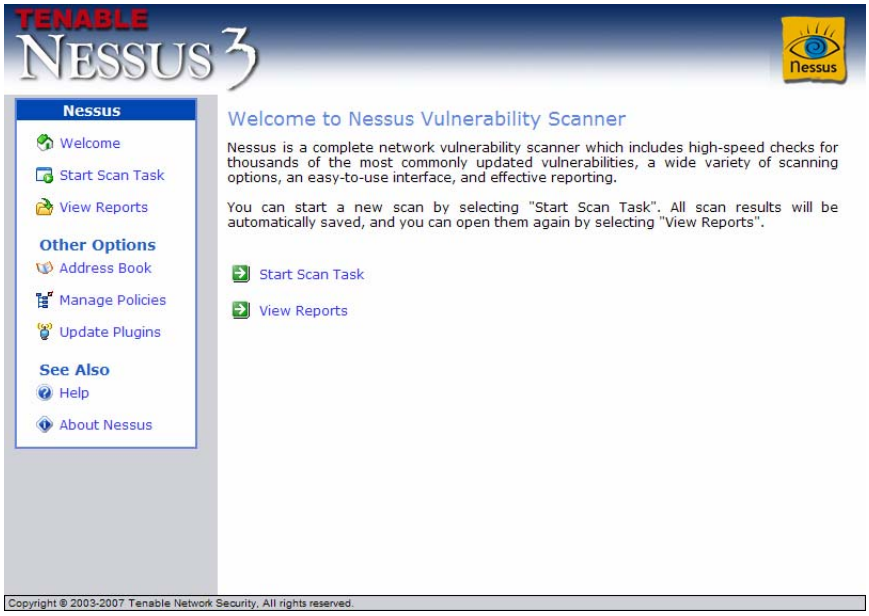
Ovo je jedna od najpoznatijih aplikacija za analizu mrežnog prometa, poznata i pod nazivom *Ethereal*. Aplikacija je namijenjena Linux, Unix, Windows i drugim korištenim operacijskim sustavima. Radi se o aplikaciji koja implementira mehanizam za analizu mrežnog prometa i koristi se vrlo često u analizi i razvoju protokola, edukaciji budućih mrežnih i sigurnosnih stručnjaka te otklanjanju propusta u mrežnoj komunikaciji.
Daljnje informacije o paketu dostupne su na adresi:
http://www.wireshark.org/.



Slika 5: Wireshark analizator

4.2.8. *Nessus*

Nessus je alat korišten za automatizirane postupke provjere ranjivosti koji se provode radi određivanja sigurnosnih nedostataka računala i računalnih mreža, a isporučuje se u besplatnoj i komercijalnoj inačici. Sastoji se od klijenta i poslužitelja pri čemu su raspoložive besplatne inačice za Windows, Mac OS X, Linux, Solaris i FreeBSD operacijske sustave. Velik broj korisnika sudjeluje u razvoju paketa, tako da je omogućeno i redovito osvježavanje popisa ranjivosti. Odlika ovog alata je velika baza ranjivosti i kvalitetan mehanizam generiranja izvješća nakon pregleda koji u potpunosti podržava CVE standard.



Slika 6: *Nessus* alat

4.3. Alati temeljeni na protokolima

Slijedi opis alata koji se temelje na iskorištavanju određenih protokola prema kojima su i grupirani.

4.3.1. Microsoft NetBIOS, SMB i CIFS

NetBIOS, Server Message Block (SMB) i Common Internet File System (CIFS) protokoli se koriste ponajprije kod mrežne komunikacije Microsoft Windows sustava za autentikaciju korisnika, dijeljenje datoteka i pristup servisima.
Ovdje se alati svrstavaju u dvije grupe:

- alate za prikupljanje informacija i
- alate za nasumično pogađanje zaporki metodom iscrpljivanja kombinacija.

4.3.1.1 Alati za prikupljanje informacija

Enum je alat koji šalje velike količine upita NetBIOS protokolom korištenjem TCP priključka 139. Alat može dohvatiti korisnička imena, pravila dodjele zaporki, podatke o dijeljenju resursa i detalje o drugim računalima u mreži.
Epdump je alat koji se koristi iz naredbenog retka, a temelji se na komunikaciji preko TCP priključka 135 za prikupljanje informacija o mrežnim sučeljima kao i detalja o RPC (eng. *Remote Procedure Call*) uslugama i imenovanim cjevovodima (eng. *Named Pipes*).
Nbtstat aplikacije je uključena u distribuciju svih Windows operacijskih sustava. Koristi se priključkom 137 i UDP protokolom za prikupljanje podataka poput imena računala, domene, detalja o prijavljenom korisniku, dijeljenim resursima i MAC (eng. *Media Access Control*) adresi mrežnog sučelja.

Usrstat aplikacija je dio Windows NT 4.0 Resource Kit paketa. Koristi se za prikupljanje detaljnih podataka o korisnicima udaljenog računala poput vremena zadnje prijave, punog imena i prezimena korisnika i korisničkog imena.

4.3.1.2 Alati za pogađanje zaporke

SMBCrack je iznimno brza aplikacija namijenjena pogađanju korisničkih zaporki na lokalnoj mreži. Koristi TCP priključak 139 i NetBIOS sjednicu.
WMICracker je alat namijenjen pogađanju zaporki korištenjem metode uzastopnih pokušaja, a koristi RPC servis preko TCP priključka 135.

4.3.2. DNS

DNS alati prikupljaju podatke iz neodgovarajuće postavljenih imenskih poslužitelja korištenjem TCP i UDP protokola na priključku 53. Alati iz ove skupine mogu preuzeti čitave tzv. "zone" datoteke koje sadrže određene informacije o domeni koju opisuju. Slijedi nekoliko alata korisnih za prikupljanje informacija na ovaj način.

- ***nslookup*** - naredba je uvrštena u distribucije gotovo svih operacijskih sustava među kojima su Windows NT, 2000 i XP, te distribucije svih Unix-temeljenih i MacOS operacijskih sustava. Alat može postavljati sve vrste upita DNS poslužiteljima, uključujući dohvat podataka o zoni i tzv. "*reverse lookup*" dohvat imena računala preko IP adrese.
- ***host*** i ***dig*** naredbe moguće je naći na svim Unix-temeljnim sustavima. Koriste se iz naredbenog retka za izvođenje svih oblika upita DNS poslužiteljima.
- ***ghba*** alat razvijen je s namjernom upotpunjavanja svojstava prethodna dva alata. Njegova namjena je dohvat imena iz IP adresa adresnog prostora klase C i B. Jednostavno se koristi pozivanjem poznate funkcije jezgre *gethostbyaddr()* za svaku IP adresu iz zadanog mrežnog segmenta.

4.3.3. HTTP i HTTPS

Razvojem HTTP poslužitelja i korištenjem relacijskih baza podataka kao mjesta na kome web aplikacije pohranjuju svoje podatke, HTTP i HTTPS protokoli postali su metom napada zlonamjernih korisnika. Sve veća složenost implementacije dinamičkih web stranica razlog je učestaloj pojavi čitavog niza specifičnih sigurnosnih nedostataka koji se mogu iskoristiti za niz zlonamjernih aktivnosti. Kao i na drugim segmentima ispitivanja mrežne sigurnosti i ovdje je prisutan velik broj alata od kojih se ističe nekoliko kvalitetnih. Oni su usmjereni na testiranje propusta poput mogućnosti umetanja proizvoljnog SQL koda i XSS (eng. *cross-site scripting*) ranjivosti.
Slijedi kratak opis nekoliko najpoznatijih alata:

- ***N-Stealth*** aplikacija namijenjena je Windows operacijskim sustavima i provodi standardne testove svih poznatih web servisa (*Microsoft IIS*, *Apache*, *Zeus* i drugi).
- ***Nikto*** je skener web poslužitelja koji može otkriti velik broj sigurnosnih nedostataka na značajnom broju danas dostupnih poslužitelja. Za svoj rad koristi programsku biblioteku *libwhisker*.
- ***CGIchk*** je modularan CGI skener namijenjen kako Windows tako i Unix operacijskim sustavima.

4.4. Komercijalni alati

Komercijalne alate za skeniranje računalnih mreža koriste najčešće administratori vrlo velikih organizacija. Radi se o vrlo skupim proizvodima čija se cijena mjeri u tisućama dolara. S druge strane, ovi proizvodi nude besprekidnu podršku, redovite nadogradnje kako i priliči skupim rješenjima.
Nekoliko komercijalnih paketa pobrojano je u slijedećem popisu:

- SAINT (http://www.saintcorporation.com/products/vulnerability_scan/saint/saint_scanner.html)
- ISS Internet Scanner (http://www.iss.net)
- Cisco Secure Scanner (http://www.cisco.com/warp/public/cc/pd/sqsw/nesn/)

5. Tehnike skeniranja

Poglavlje je usmjereno na tehničku izvedbu skeniranja IP mreža. Nakon obaveznih inicijalnih izvidnica za identificiranje IP adresnih prostora, mrežno skeniranje gradi jasnu sliku dostupnih računala i njihovih mrežnih servisa. Razlog izvođenja mrežnog skeniranja je uočavanje slijedećih svojstava mreže ili računala:

- dostupnosti odredišnog računala s mreže,
- dostupnosti TCP i UDP mrežnih servisa na odredišnom računalu,
- vrste operacijskog sustava odredišnog računala i njegovih postavki te
- postavki filtara mrežnog prometa i drugih sigurnosnih sustava, uključujući vatrozid, usmjerivače, skretnice te IDS (eng. *Intrusion Detection System*) sustave.

Za prikupljanje detaljnijih informacija slijede koraci procjenjivanja ranjivosti koji uključuju prikupljanje specifičnih informacija o TCP i UDP mrežnim uslugama koje se izvode na provjeravanim računalima,

5.1. Prikupljanje temeljnih informacija o mreži

Dohvat informacija o računalnoj mreži u potpunosti je legalna aktivnost i ne ovisi o organizaciji čiju se arhitekture mreže pokušava ustanoviti. Početak može biti usmjeren na prikupljanje temeljnih informacija o nazivima računala, imenima domena i korisnim podacima do kojih se može doći uporabom web pretraživača.

Slijedi dohvat informacija od informacijskih središta (NIC) korištenjem bilo koje dostupne aplikacije namijenjene upravo tome ili, najjednostavnije, korištenjem poznate *whois* naredbe. U slučaju ispitivane domene cert.hr do nekih informacija se moglo doći i korištenjem usluge HR-DNS službe. Rezultat je prikazan na slijedećoj slici.

Slika 7: Primjer prikupljanja podataka o mreži

Korištenjem *nslookup* alata moguće je doći do potrebnih informacija o imenima računala na kojima su pokrenuti poslužitelji za različite usluge.

```
$ nslookup
> set querytype=any
> cert.hr
Server:         161.53.64.3
Address:        161.53.64.3#53
Non-authoritative answer:
cert.hr mail exchanger = 20 mx2.CARNet.hr.
cert.hr mail exchanger = 10 mail.cert.hr.
cert.hr
        origin = dns.CARNet.hr
        mail addr = hostmaster.CARNet.hr
        serial = 2007041801
        refresh = 10800
        retry = 3600
        expire = 2419200
        minimum = 14400
cert.hr nameserver = dns2.CARNet.hr.
cert.hr nameserver = bjesomar.srce.hr.
cert.hr nameserver = dns.CARNet.hr.
Authoritative answers can be found from:
cert.hr nameserver = dns2.CARNet.hr.
cert.hr nameserver = bjesomar.srce.hr.
cert.hr nameserver = dns.CARNet.hr.
mail.cert.hr    internet address = 161.53.160.50
dns.CARNet.hr   internet address = 161.53.123.3
```

5.2. Skeniranje na IP razini

Različite metode skeniranja mreže na IP razini omogućuju određivanje ranjivosti mrežnih komponenata. U nastavku je dan popis tehnika mrežnog skeniranja zajedno s njihovim primjenama.

5.2.1. Tehnike skeniranja priključaka

Skeniranje priključaka vrlo je korisna tehnika za prikupljanje važnih informacija o računalima na mreži. Posebno je pogodna napadačima za izvođenje zlonamjernih aktivnosti budući da osigurava sve za to potrebne informacije.

Koncept mrežnog priključka ili *porta* može biti nejasan ukoliko se on pokuša vizualizirati kao jedna od sklopovskih utičnica na stražnjoj strani računala. Ovdje se radi isključivo o programskom konceptu gdje se svakom mrežnom paketu dodaje broj koji opisuje uslugu kojoj paket pripada. Svi paketi jedne usluge tako dobivaju jednak broj i moguće ih je prema njemu razlikovati. Primjerice, svi paketi koji pripadaju HTTP protokolu razmjenjuju se putem priključka 80, što znači da im je broj usluge također 80. Radi lakšeg snalaženja raspon dostupnih 65536 priključaka kategorizira se u tri razine:

- dodijeljeni priključci (eng. *Well Known Ports*) [0..1023],
- registrirani priključci (eng. *Registered Ports*) [1024..49151] i
- dinamički odnosno privatni priključci (eng. *Dynamic and/or Private Ports*) [49152..65535].

U prvu skupinu ubrajaju se priključci za usluge poput FTP, SMTP, Telnet, HTTP, DNS i druge. Drugi interval često korištenim aplikacijama omogućuje posjedovanje vlastitog priključka, a to su između ostalih antivirusne i aplikacije za razmjenu datoteka, računalne igre i sl. Dinamičke priključke može koristiti bilo koja aplikacija u proizvoljne svrhe.

Kako bi se osiguralo ispravno korištenje mrežnih priključaka stvorena je standardizacijska udruga IANA (eng. *Internet Assigned Numbers Authority*) koja propisuje vrlo stroge procedure za registraciju željene usluge na zadani priključak.

Važnost skeniranja priključaka ne smije se podcijeniti. Svi alati s ovog područja korisniku omogućuju ispitivanje ranjivosti ciljanog sustava bez saznanja administratora tog sustava. Na taj način napadač može planirati napade bez poticanja žrtve na sumnju. Prilikom razmjene informacija u komunikaciji između dvaju računala, spremaju se različiti podaci o uspostavljenoj vezi. Međutim, u ovom slučaju jedno računalo komunicira s mrežom drugog računala pri čemu se nikakvi podaci ne zapisuju u dnevnike sustava.

Postupak skeniranja priključaka dijeli se u nekoliko podvrsta:

- *vanilla* - pokušaj spajanja na svaki od 65536 priključaka s ciljem utvrđivanja otvorenih,
- *strobe* - pokušaj spajanja na određene priključke radi utvrđivanja njihove otvorenosti,
- *stealth scan* - nekoliko tehnika koje osiguravaju prikrivenost pokušaja uspostave veze ,
- *FTP bounce scan* - pokušaj usmjeravanja napada preko FTP poslužitelja kako bi napadač skrio svoju izvornu IP adresu,
- *Fragmented packets* - skeniranje slanjem nepotpuno oblikovanih mrežnih paketa koji prolaze kroz vatrozid,
- *UDP* - traži otvorene UDP priključke i
- *sweep* - pregledava isti priključak na nizu računala.

5.2.1.1 ICMP skeniranje

Pokretanjem ICMP *ping* skeniranja može se utvrditi je li neko računalo uključeno, a analizom primljenih odgovora moguće je odrediti i prisutan operacijski sustav .
U pravilu se šalju različite vrste paketa koje između ostalih obuhvaćaju već spomenuti "*echo request*", "*timestamp request*", "*information request*" i "*subnet address mask request*". Opisani *nmap* paket omogućuje jednostavno izvođenje ICMP pregleda mreže. Izvođenjem naredbe prikazane u ispisu može se vidjeti koliko je računala s javnim IP adresama dostupno unutar CERT domene.

```
# nmap sP PI 161.53.160.0/24

Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2007-06-26 03:29
CEST
Host infragwy.infra.CARNet.hr (161.53.160.1) appears to be up.
...   …   …
Host zg1.ntp.CARNet.hr (161.53.160.4) appears to be up.
Host 161.53.160.155 appears to be up.
Host lebrun.debian.org (161.53.160.165) appears to be up.
Host gw2.infra.CARNet.hr (161.53.160.254) appears to be up.
Nmap finished: 256 IP addresses (77 hosts up) scanned in 11.327 seconds
```

5.2.1.2 Legalne implikacije skeniranja priključaka

Skeniranje priključaka može se usporediti sa situacijom iz svakodnevnog života gdje potencijalni napadač zvoni na vrata svake kuće provjeravajući ima li nekoga unutra.
Ovdje se radi o temeljnoj tehnici koju koriste napadači za pristup žrtvama, a kojom mogu doći do saznanja o pokrenutim servisima, njihovim inačicama, kao i o operacijskom sustavu ciljanog računala. Sve informacije stečene na ovaj način napadaču omogućuju nedozvoljen pristup korištenjem odgovarajućih alata koji iskorištavaju postojeće propuste.
Upravo se zbog toga postavlja pitanje legalnosti i etike izvođenja skeniranja priključaka. S jedne strane se skeniranje priključaka smatra zlonamjernom aktivnošću, ali s druge strane tu tehniku koriste sigurnosni stručnjaci i administratori za utvrđivanje ranjivosti provjeravanog sustava odnosno njihove mreže. Legitimnost ove tehnike često se određuje okolnostima koje su prethodile izvođenju napada. Skeniranje samo po sebi nije napad jer u većini sustava ono ne šteti ni sustavu ni mreži. Zato postoji nejasnoća oko toga treba li skeniranje priključaka predstavljati zlonamjernu aktivnost samo po sebi ili tek nakon što se ustanovi da je ono prethodilo napadima. Ukoliko se može procijeniti svrha skeniranja, tada je lako odrediti i karakter skeniranja. Primjerice, ukoliko netko traži da li je otvoren priključak na komu se nalazi trojanski konj, očito se radi o zlonamjernom postupku.
Uspostavljanje dobro određenih pravila vezanih uz skeniranje priključaka može uvelike pomoći kod kategorizacije skeniranja.

5.2.2. Zaobilaženje filtara i izbjegavanje IDS sustava

Mehanizme za detekciju provale i ostale sigurnosne mehanizme može se zaobići korištenjem višestrukih krivotvorenih adresa izvorišta prilikom skeniranja priključaka.
Filtre poput vatrozida i usmjerivača u određenim slučajevima moguće je zaobići korištenjem specifičnih izvornih TCP ili UDP priključaka.

5.3. Korištenje IP paketa na niskoj razini

Alati poput *nmap*, *hping2* i *firewalk* omogućuju određivanje sadržaja IP paketa na niskoj razini. Ponekad ranjivosti sigurnosnih mehanizama omogućavaju paketima namijenjenim određenim TCP servisima prolazak kroz mrežni filtar, najčešće vatrozid, ali taj servis ne mora biti pokrenut na odredišnom računalu. Takve informacije korisno je poznavati jer se čak i mali propusti u integritetu sigurnosnih pravila mogu iskoristiti za uspješno izvođenje zlonamjernih aktivnosti.
Ovakvim metodama moguće je odrediti slijedeća svojstva:

- vrijeme rada ciljanog računala,
- TCP servise koje dozvoljava vatrozid te
- operacijski sustav ciljanog računala.

Alat *hping2* omogućuje oblikovanje IP paketa po želji korisnika sa ciljem analize odgovora odredišta. Slijedi primjer zadavanja naredbe alatu i rezultat izvršavanja.

```
# hping2 -c 3 -s 53 -p 139 -S 192.168.0.1
HPING 192.168.0.1 (eth0 192.168.0.1): S set, 40 headers + 0 data
ip=192.168.0.1 ttl=128 id=283 sport=139 flags=R seq=0 win=64240
ip=192.168.0.1 ttl=128 id=284 sport=139 flags=R seq=1 win=64240
ip=192.168.0.1 ttl=128 id=285 sport=139 flags=R seq=2 win=64240
```

6. Zaključak

U dokumentu je pokazan samo jedan manji dio čitavog područja sigurnosti računalnih sustava odnosno računalnih mreža. Opisani su koncepti sigurnosti računalnih mreža te rizik i način računanja rizika od napada zlonamjernih korisnika. Poglavlje posvećeno procjeni ranjivosti daje dobar uvod u problematiku skeniranja računalnih mreža i navodi metode procjene ranjivosti, svrhu skeniranja i opis provođenja skeniranja. Dan je i pregled često korištenih i poznatih alata za provođenje skeniranja podijeljenih u posebne skupine zbog veće preglednosti. Konačno, opisane su i neke tehnike skeniranja mreže uz primjere izvođenja opisanih alata.

Jasno je da će se područje računalne sigurnosti još uvelike širiti i zahtijevati nove stručnjake koji dobro poznaju sve potrebne segmente. Zato dokument pruža uvid u vrlo široko područje ispitivanja ranjivosti računalnih sustava, a za daljnje istraživanje preporuča se konzultiranje radova pobrojanih u popisu referenci.

7. Reference

[1.] Chris McNab: "Network Security Assessment", O'Reilly, ožujak 2004.

[2.] Steve Manzuik, Ken Pfeil, Andre Gold: "Network Security Assessment: From Vulnerability to Patch", Syngress, 2007.

[3.] HackerWacker, http://epsilon.hackerwhacker.com/freetools.php, lipanj 2007.

[4.] Safety Lab, http://www.safety-lab.com/en/, lipanj 2007.

[5.] Network Scanning Policy, http://www.comptechdoc.org/independent/security/policies/network-scanning-policy.html, lipanj 2007.

[6.] Port Scanning and its Legal Implications, http://www.asianlaws.org/cyberlaw/library/cc/ptscanning.htm, 2004.

[7.] Scanning Your Network, http://www.onlamp.com/pub/a/bsd/2001/04/18/FreeBSD_Basics.html, 2001.

[8.] Nmap scanner, http://insecure.org/nmap/, lipanj 2007.

[9.] Intrusion Detection Level Analysis of Nmap and Queso, http://www.securityfocus.com/infocus/1225, kolovoz 2000.

[10.] Hping alat, http://wiki.hping.org/, lipanj 2007.

[11.] Fping alat, http://fping.sourceforge.net/, veljača 2007.

[12.] Fping for Windows, http://www.kwakkelflap.com/fping.html, lipanj 2007.

[13.] Ping alat, http://en.wikipedia.org/wiki/Ping, lipanj 2007.