HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Honeypot sustavi

CCERT-PUBDOC-2003-06-26

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 4

2. OSNOVNA NAČELA 4

3. VRIJEDNOST *HONEYPOT* SUSTAVA 4

4. PREDNOSTI I NEDOSTATCI 5

4.1. PREDNOSTI 5
4.2. NEDOSTACI 6

5. TIPOVI HONEYPOT SUSTAVA 6

6. PROGRAMSKI ALATI 7

6.1. KFSENSOR 7
6.2. HONEYD 9

7. HONEYNET SUSTAVI 10

8. ZAKLJUČAK 12

1. Uvod

U ovom dokumentu opisana je tehnologija *honeypot* sustava, područje računalne sigurnosti kojemu je osnova namjena detekcija neovlaštenih aktivnosti te prikupljanje novih spoznaja i informacija o tehnikama i alatima koje neovlašteni korisnici koriste prilikom provođenja malicioznih aktivnosti. Opisana su osnovna načela na kojima se bazira rad *honeypot* sustava, zajedno s njihovim značajem i područjem primjene. Također su analizirani i različiti tipovi sustava, s obzirom na način rada i namjenu, a dani su i primjeri konkretnih implementacija.

2. Osnovna načela

Honeypot sustavi relativno su nova tehnologija u području računalne sigurnosti i njihova popularnost iz dana u dan neprestano raste. Koncept primijenjen kod *honeypot* sustava smatra se iznimno velikim potencijalom u pogledu unaprjeđenja sigurnosti računalnih i komunikacijskih sustava. Nove ideje i metodologije, koje proizlaze kao rezultat njihove primjene, omogućuju razvoj novih sigurnosnih rješenja i produkata, što je jedna od najvećih vrijednosti *honeypot* sustava (Poglavlje 3).

Svakodnevnim razvojem novih računalnih tehnologija i servisa paralelno se povećava i broj računalnih incidenata na javnom Internetu. Neovlašteni korisnici vrlo brzo pronalaze sigurnosne propuste u novim tehnologijama, na temelju čega razvijaju specijalne alate i tehnike kojima se zaobilaze definirane sigurnosne mjere. Iako je vrijeme potrebno za reakciju i suzbijanje novootkrivenih sigurnosnih prijetnji na Internetu znatno smanjeno u odnosu na prije nekoliko godina, redovito se javljaju novi maliciozni programi (virusi, crvi, i sl.) koji pomiču dosegnute granice.

Potreba za kvalitetnim mehanizmima koji će omogućiti prikupljanje informacija o takovim aktivnostima neophodan je korak za kvalitetnu i učinkovitu zaštitu od malicioznih korisnika. Jedno od rješenja, koje je opisano u ovom dokumentu, upravo su *honeypot* sustavi.

Pod *honeypot* sustavima smatraju se svi oni računalni resursi (poslužitelji, računalne mreže, i sl.) koji su predviđeni da budu napadnuti ili kompromitirani od strane neovlaštenih korisnika. Osnovi cilj ovakvog pristupa je prikupljanje novih spoznaja o tehnikama i alatima koje neovlašteni korisnici upotrebljavaju za kompromitiranje računalnih resursa, kako bi se na taj način razvile nove ideje i alati za efikasnije sprječavanje neovlaštenih aktivnosti. Načini implementacije i mogućnosti primjene vrlo su raznolike, što ove sustave čini vrlo fleksibilnima i iskoristivima u različitim područjima računalne sigurnosti.

Jedna od definicija *honeypot* sustava, koja proizlazi iz spomenute općenitosti i fleksibilnosti, kaže da su to oni računalni resursi čija vrijednost leži u mogućnosti njihovog neovlaštenog i neautoriziranog korištenja.

Treba naglasiti da ideja *honeypot* sustava nije identifikacija i krivično procesiranje neovlaštenih korisnika uključenih u računalni kriminal, već isključivo saznavanje tehnika kojima se oni koriste. Štoviše, jedna od mjera kvalitete *honeypot* sustava je upravo ta da neovlašteni korisnik nikada ne sazna da su njegove aktivnosti zabilježene *honeypot* sustavom.

U posljednje vrijeme aktualna su i rješenja u kojima se *honeypot* sustavi koriste kao sustavi za detekciju neovlaštenih aktivnosti (engl. *Intrusion Detection System*). Ova ideja znatno se razlikuje u odnosu na klasične IDS sustave (*rule-based IDS*, *anomaly-based IDS* i sl.), i danas se sve češće mogu naći radovi koji međusobno uspoređuju ove tehnologije. Programski alati koji implementiraju *honeypot* IDS sustave sve su češći (KFSensor, Spectra, itd...), a neki od njih opisani su i u ovom dokumentu (Poglavlje 6).

3. Vrijednost *honeypot* sustava

Tri vrlo važna područja računalne sigurnosti o kojima je potrebno voditi računa prilikom implementacije računalno komunikacijskih sustava su:

- Prevencija (engl. *prevention*) – postupak uspostave sustava koji će računalne resurse zaštiti od neovlaštenih korisnika;
- Detekcija malicioznih aktivnosti (engl. *detection*) – postupak koji podrazumijeva identifikaciju sigurnosnih nedostatka u sustavu prevencije te obavješćivanje administrativnog osoblja o uočenim, potencijalno sumnjivim aktivnostima;

- Reakcija (engl. *response* ili *reaction*) – način na koji organizacija ili odgovorno osoblje reagira na detekciju neovlaštenih aktivnosti;

Iako svaka od navedenih komponenti ima svoje mjesto i značaj u području računalne sigurnosti, sustavi za prevenciju i detekciju imaju posebnu težinu. Uspostava kvalitetnih sustava za prevenciju i detekciju neovlaštenih aktivnosti u velikoj će mjeri smanjiti sigurnosni rizik od neovlaštenih aktivnosti koje prijete s Interneta.

Honeypot sustavi, kao sigurnosno rješenje, mogu se svrstati u sve tri skupine (ovisno o tipu *honeypot* sustava (Poglavlje 5)). Mogućnost detekcije neovlaštenih aktivnosti, te prikupljanje novih spoznaja o korištenim alatima i tehnikama neovlaštenih korisnika, koje se kasnije koriste za razvoj novih sigurnosnih rješenja, svojstva su koja to potvrđuju.

Kao što je već ranije spomenuto, jedna od primarnih uloga *honeypot* sustava je detekcija malicioznih aktivnosti na mreži te prikupljanje informacija potrebnih za njihovu analizu. Oni ne pružaju nikakve usluge ili servise za legitimne korisnike te su u tom pogledu potpuno neupotrebljivi. Jedan od osnovnih preduvjeta za uspostavu kvalitetnog *honeypot* sustava je upravo taj da se na njima ne nalaze servisi i usluge namijenjeni legitimnim korisnicima. Ovaj uvjet garantira da će *honeypot* sustavi bilježiti samo maliciozni promet neovlaštenih korisnika, a ne aktivnosti legitimnih korisnika.

Treba napomenuti da uspostava *honeypot* sustava u pravilu ne rezultira podizanjem sigurnosnog nivoa računalne mreže i okolnih sustava. Ova tvrdnja prvenstveno se odnosi na istraživačke *honeypot* sustave (iako se ista često može primijeniti i na komercijalna rješenja - Poglavlje 5), gdje se u sustav namjerno unose ranjivosti koje će privući pažnju neovlaštenih korisnika. Budući da vrijednost sustava raste s brojem zabilježenih malicioznih aktivnosti, unesene ranjivosti vrlo često su visokog sigurnosnog rizika, što uz nedostatne mjere zaštite može prouzročiti ozbiljne probleme za okolne sustave.

Pogrešno je mišljenje da će postavljanje *honeypot* sustava računalnu mrežu zaštiti od malicioznih aktivnosti neovlaštenih korisnika. Nasuprot, površno i nepažljivo postavljen *honeypot* sustav najčešće donosi nove sigurnosne probleme, koji se mogu negativno odraziti na mreže i sustave koji su na bilo koji način (ili logički ili fizički) povezani s istim. Iz ovog razmatranja proizlaze visoki zahtjevi za stručnošću i iskustvom osoba uključenih u postavljanje i održavanje sustava.

Međusobna veza između različitih tipova *honeypot* sustava i njihovog utjecaja na sigurnosna svojstva računalnog sustava opisana je u poglavlju 5.

4. Prednosti i nedostatci

U ovom poglavlju opisane su osnovne prednosti i nedostatci *honeypot* sustava.

4.1. Prednosti

Slijedi kratka lista nekih od prednosti *honeypot* sustava. Osim općenitih prednosti koje proizlaze iz temeljnih karakteristika same tehnologije, navedene su i neke prednosti ispred ostalih tehnologija slične namjene (IDS, alati za provjeru integriteta, i sl.). Prednosti su:

- mogućnost prikupljanja novih spoznaja o tehnikama i alatima neovlaštenih korisnika;
- malen broj lažnih upozorenja – budući da *honeypot* sustavi najčešće ne obavljaju niti jednu drugu zadaću osim prikupljanja informacija o neovlaštenim aktivnostima, većina mrežnog prometa koji se zabilježi vezan je uz namjenu sustava. Ukoliko se sustav koristi kao IDS rješenje, ovo predstavlja značajnu prednost, budući da IDS sustavi vrlo često generiraju vrlo velike količine lažnih upozorenja (ovisno o kvaliteti konfiguracije sustava);
- relativno mala količina prikupljenih podataka – *honeypot* sustavi karakteriziraju se relativno malom količinom podataka koji bilježe. Za razliku od sigurnosnih rješenja kao što su mrežni (engl. *network based*) i poslužiteljski (engl. *host-based*) sustavi za detekciju neovlaštenih aktivnosti, *honeypot* sustavi bilježe i pohranjuju znatno manje količine podataka. S obzirom na namjenu sustava zabilježeni podaci najčešće su korisni podaci o aktivnostima neovlaštenih korisnika s vrlo malim brojem lažnih upozorenja (engl. *false positive*);
- fleksibilnost – brojne mogućnosti i vrlo široko područje primjene jedna je od osnovnih karakteristika *honeypot* sustava;

- skromni zahtjevi na računalne resurse – svojstvo *honeypot* sustava da bilježe isključivo maliciozne aktivnosti neovlaštenih korisnika čini ih manje zahtjevnima na računalne resurse potrebne za implementaciju sustava. Računalo generacije Pentium I s 128 MB radne memorije i tvrdim diskom prosječne veličine (20, 40 GB) zadovoljiti će većinu potreba;
- mogućnost analize kriptiranih protokola – bez obzira o kojem se servisu ili protokolu radi, *honeypot* sustav zabilježit će maliciozne aktivnosti usmjerene prema njemu;
- jednostavnost – iako sama implementacija kvalitetnog i pouzdanog *honeypot* sustava nije nimalo trivijalan zadatak, sama ideja i koncept vrlo su jednostavni. Za implementaciju nisu potrebni složeni algoritmi, tablice stanja i sl., kao što je slučaj s drugim tehnologijama kojima se žele detektirati i identificirati aktivnosti neovlaštenih korisnika. Za neke jednostavnije primjene moguće je iskoristiti i gotove alate kao što su `netcat` i dr.

4.2. Nedostaci

- mogućnost detekcije samo onih neovlaštenih aktivnosti koje su usmjerene prema *honeypot* sustavu – osim nedostataka, ovo je jedno o najvećih ograničenja *honeypot* sustava. Svi napadi usmjereni prema ostalim računalima na mreži ostati će nezabilježeni;
- unošenje dodatnog sigurnosnog rizika u računalne sustave na kojima je postavljen honeypot – budući da je osnovna ideja *honeypot* sustava u tome da on bude kompromitiran, sigurnosni rizik koji se time unosi za ostale računalne resurse postaje viši. Ukoliko sustav nije pažljivo osmišljen i ukoliko nisu definirane odgovarajuće mjere zaštite, ovakvi sustavi vrlo često mogu prouzrokovati probleme za legitimna računala i servise.

5. Tipovi Honeypot sustava

Ovisno o tipu i namjeni, *honeypot* sustave moguće je podijeliti u dvije osnovne skupine. To su:

- Komercijalni *honeypot* sustavi (engl. *production honeypot systems*) – namijenjeni su prvenstveno unaprjeđenju sigurnosnih karakteristika računalnih sustava. Njihova primarna uloga je detekcija i prevencija neovlaštenih aktivnosti usmjerenih prema ciljnom sustavu, dok se u drugom planu nalazi potreba za prikupljanjem i analizom detektiranih događaja. Njihova vrijednost mjeri se u broju uspješno detektiranih neovlaštenih aktivnosti te o učinkovitosti mjera njihovog suzbijanja.
- Istraživački *honeypot* sustavi (engl. *research honeypot systems*) – za razliku od komercijalnih, istraživački *honeypot* sustavu imaju posve drukčiju namjenu. Njihov primarni zadatak je prikupljanje i analiza novih informacija o aktivnostima neovlaštenih korisnika, a vrijednost im se mjeri u količini prikupljenih informacija i u broju uspješno identificiranih i analiziranih aktivnosti.

Dodatnu podjelu moguće je obaviti na temelju nivoa interakcije između neovlaštenog korisnika i *honeypot* sustava. Viši nivo interakcije između neovlaštenih korisnika i *honeypot* sustava u pravilu podrazumijeva kompleksniji sustav, veći angažman oko administracije, veću cijenu te viši sigurnosni rizik za okolne sustave.

U ovom smislu moguće je definirati sljedeću podjelu:

- Nisko-interaktivni *honeypot* sustavi – karakteriziraju se relativno jednostavnim postupkom instalacije i održavanja, niskim sigurnosnim rizikom te ograničenim brojem događaja koje je ovim putem moguće prikupiti. Preporučljivo za manje iskusne korisnike koji se prvi puta susreću s *honeypot* rješenjima.
- Visoko-interaktivni *honeypot* sustavi – složeniji sustavi s većim angažmanom oko instalacije i održavanja. Omogućavaju detekciju složenijih neovlaštenih aktivnosti te alata i tehnika kojima se napadači koriste. S obzirom na dopušteni nivo interakcije s neovlaštenim korisnicima ovakvi sustavi predstavljaju znatno viši sigurnosni rizik. Preporučuju se na korištenje naprednijim korisnicima s iskustvom u ovom području.

Iako je na nekim mjestima moguće naći i detaljniju podjelu s obzirom na nivo interakcije između neovlaštenog korisnika i *honeypot* sustava, ovakva podjela trenutno je najprihvaćenija.

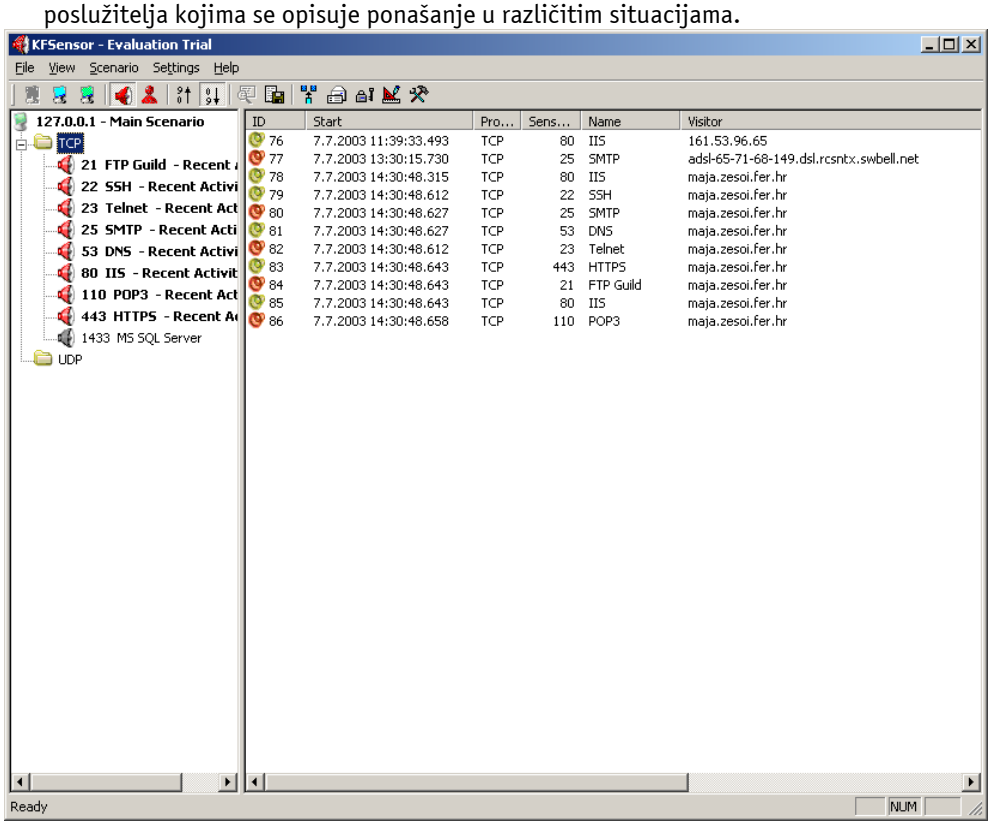
6. Programski alati

Trenutno postoji nekoliko programskih alata koji omogućuju postavljanje *honeypot* sustava. Neki od njih su komercijalni (Spectra, KFSensor), a neki od njih su besplatni (Honeyd). U ovom dokumentu biti će navedene osnovne karakteristike KFSensor i Honeyd programa, kako bi se ukratko dao uvid u njihova svojstva i mogućnosti primjene.

6.1. KfSensor

KFSensor (http://www.keyfocus.net/kfsensor/) programski paket predstavlja komercijalno *host-based honeypot* rješenje za Windows operacijske sustave. Program se može opisati kao nisko-interaktivni *honeypot* sustav s jednostavnim i intuitivnim grafičkim sučeljem (*Slika 1*) te jednostavnošću upotrebe, što ga čini prihvatljivim rješenjem i za manje iskusne korisnike. Nakon postupka instalacije programa, koji je tipičan za programske pakete namijenjene Windows operacijskim sustavima, potrebna su minimalna podešavanja koja će omogućiti osnovnu *honeypot* funkcionalnost.
Fleksibilnost i modularnost KFSensor programa korisniku omogućuje dodavanje novih funkcionalnosti i svojstava te prilagođavanje programa osobnim potrebama. Program podržava emulaciju različitih mrežnih poslužitelja i servisa s različitim nivoima interakcije između neovlaštenih korisnika i *honeypot* sustava.
Dva su osnovna tipa mrežnih poslužitelja koje je moguće definirati:

- *Sim Banner* poslužitelj – najjednostavnija emulacija mrežnih poslužitelja s vrlo niskim nivoom interakcije između neovlaštenih korisnika i *honeypot* sustava. Na konekcije klijenta (neovlašteni korisnik) poslužitelj odgovara s odgovarajućom, korisnički podesivom porukom (engl. *banner*), nakon čega se prekida veza. Bilo kakve naprednije razmjene podataka nisu moguće.
- *Sim Standard* poslužitelj – naprednija emulacija mrežnih servisa u kojoj je moguće preciznije definirati ponašanje pojedinog servisa. Administrator sustava definira osnovne parametre poslužitelja kojima se opisuje ponašanje u različitim situacijama.



Slika 1 - Grafičko sučelje KFSensor programskog paketa

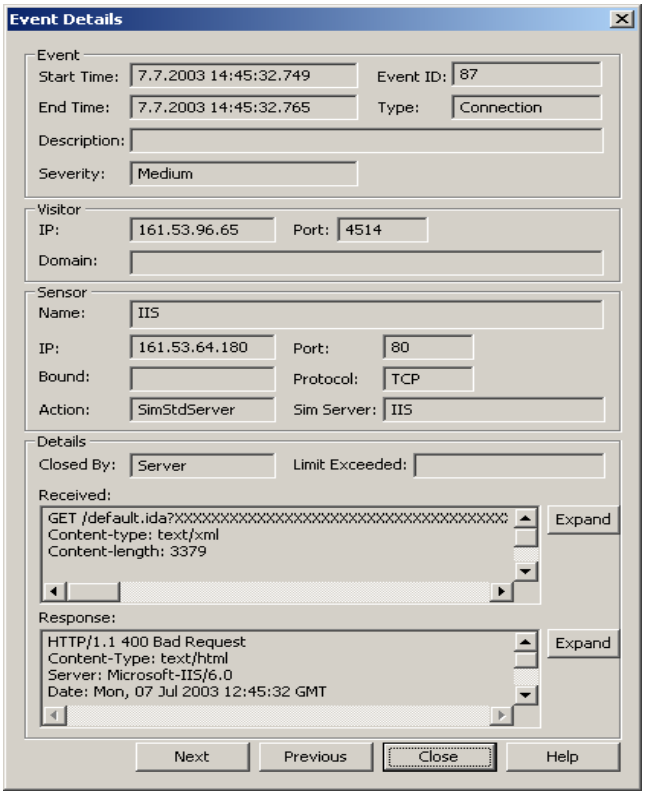
Jedna od vrlo praktičnih mogućnosti KFSensor programa je mogućnost definicije različitih scenarija. Scenariji se najbolje mogu opisati kao različiti profili, od kojih svaki opisuje točno jedan sustav s pripadajućim postavkama i servisima. Npr., moguće je definirati dva različita profila s imenima Linux i Windows od kojih jedan emulira Windows, a drugi Linux operacijski sustav. U **Windows** profilu u tom će se slučaju definirati mrežni servisi koji odgovaraju Windows operacijskim sustavima (Microsoft IIS, i sl.), dok će se u **Linux** profilu definirati servisi koji odgovaraju Linux platformama (Sendmail, Apache, Proftpd i sl.)

Nakon konfiguracije servisa i pokretanja sustava (**Start Server** opcija) isti će početi pratiti i bilježiti sve konekcije inicirane prema bilo kojem od emuliranih poslužitelja. Svaka nova konekcija biti će zabilježena u glavnom prozoru programa te će se, ovisno o odabranom načinu, obavijestiti administrator. Obavješćivanje administratora moguće je u obliku zvučnog signala, treperenja prozora programa ili putem poruka elektroničke pošte.

Svaki događaj biti će zabilježen odgovarajućom bojom (crvena, žuta, zelena) čime se označava sigurnosni rizik detektiranog događaja. Za svaki detektirani događaj biti će zabilježeni različiti podaci kao što su:

- datum i vrijeme kada je događaj detektiran (**Start Time**);
- datum i vrijeme kada je prekinuta zabilježena aktivnost (**EndTim**e);
- IP adresa i mrežni port servisa uz koji je detektiran događaj (**Sensor IP**, **Sensor Port**);
- IP adresa i mrežni port s kojeg je zabilježena konekcija (**Visitor IP**, **Visitor Port)**;
- protokol uz koji je događaj vezan (**Protocol**);
- upit klijenta (**Recieved**);
- odgovor poslužitelja (**Response**);
- podatak o tome tko je prekinuo konekciju (**Closed By**);
- broj primljenih i poslanih okteta (**Recieved Bytes**, **Response Bytes**);
- itd…

Koji će od zabilježenih podataka biti prikazani unutar sučelja programa, ovisiti će o konfiguraciji programa. Dvostrukim klikom miša na bilo koji od zabilježenih događaja moguće je dobiti detaljnije informacije (*Slika 2*).



Slika 2 - Podaci o detektiranom događaju

6.2. Honeyd

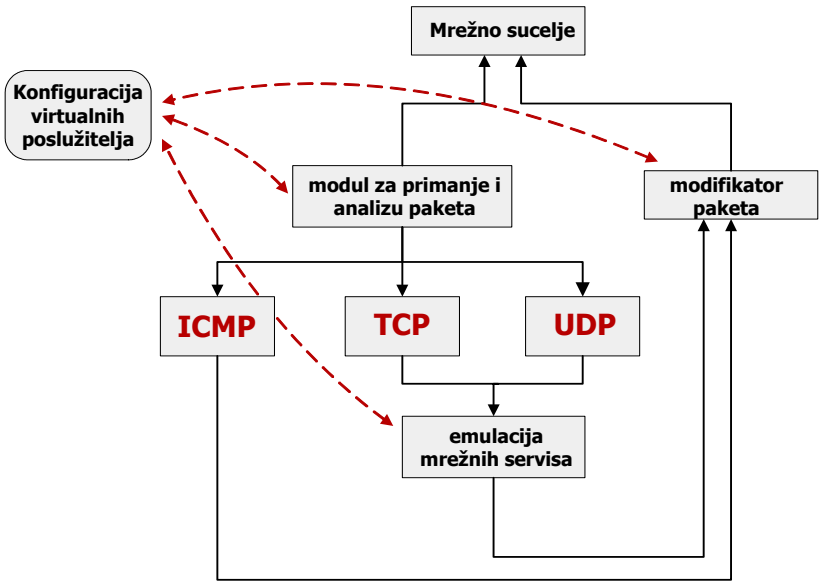
Honeyd program (http://www.citi.umich.edu/u/provos/honeyd/) je besplatna *Open-source* implementacija *honeypot* sustava namijenjena Linux operacijskim sustavima. Prema svojim karakteristikama *honeyd* program može se svrstati u skupinu istraživačkih *honeypot* sustava. Za razliku od ranije opisanog KFSensor programa, *honeyd* nešto je kompliciraniji u pogledu konfiguracije i održavanja, tako da se može preporučiti iskusnijim korisnicima s poznavanjem rada Linux operacijskih sustava.

Program omogućuje kreiranje virtualnih sustava i servisa, pri čemu su podržani TCP, UDP i ICMP mrežni protokoli. Jedna od najvećih prednosti Honeyd programa pred ostalim rješenjima ovog tipa je njegova mogućnost da, osim mrežnih servisa, simulira i TCP/IP stog različitih operacijskih sustava. Na ovaj način napadaču je otežana mogućnost da ciljni sustav prepozna kao *honeypot* te da odustane od svojih inicijalnih namjera.

Spomenuta emulacija TCP/IP stoga zasnovana je na bazi otisaka poznatog Nmap programskog paketa, koju on koristi prilikom identifikacije operacijskog sustava udaljenog računala. Prije slanja odgovora klijentskom računalu svi mrežni paketi prolaze kroz specijalan modul koji ih prilagođava sustavu koji se simulira.

Honeyd *honeypot* sustav podržava istovremenu simulaciju više različitih operacijskih sustava s različitim IP adresama. U tu svrhu potrebno je koristiti ili *Proxy ARP* funkcionalnost ili dodavanje novih ruta na mrežnom usmjerivaču iza kojeg se nalazi računalna mreža na kojoj je postavljen *honeypot* sustav.

Na sljedećoj slici prikazana je arhitektura Honeyd programskog paketa iz koje se može zaključiti način rada programa.



Slika 3 - Arhitektura Honeyd programskog paketa

Mrežno sučelje *honeypot* sustava paket prosljeđuje modulu za primanje i analizu paketa. Ovaj modul, ovisno o ciljnoj IP adresi, pretražuje bazu s konfiguracijom sustava na temelju čega se određuje o kojem se virtualnom poslužitelju radi. Ovisno o protokolu primljenog paketa (TCP, UDP, ICMP), paket se zajedno s pripadajućom konfiguracijom šalje upravljačkom programu odgovarajućeg protokola. Ovdje se obavljaju osnovne provjere nad paketom nakon čega se, ovisno o kojem se servisu radi, šalje odgovarajućem poslužiteljskom modulu. Poslužiteljski moduli su obični programi, pisani u nekom od skriptnih jezika, kojima se simuliraju različiti mrežni servisi, odnosno poslužitelji. Uz prosljeđivanje paketa simuliranoj inačici odgovarajućeg mrežnog servisa, program podržava i prosljeđivanje paketa na proizvoljno odredište. Na taj način moguće je bilo koji upit klijenta proslijediti na bilo koji drugi poslužitelj, čak i na adresu s koje je upit došao.

Nakon procesiranja upita od strane određenog poslužiteljskog modula on se prosljeđuje modulu za modificiranje paketa. Ovaj modul opet kontaktira bazu s konfiguracijom sustava, na temelju čega se

paket modificira na taj način da odgovara TCP/IP stogu simuliranog operacijskog sustava. Nakon toga paket se preko mrežnog sučelja vraća klijentskom računalu s kojeg je primljen upit.
Virtualni poslužitelji definiraju se u konfiguracijskoj datoteci Honeyd programskog paketa. Za svaki sustav potrebno je definirati parametre koji će opisati osnovne karakteristike sustava te servise koji su na njemu pokrenuti. Primjer konfiguracije dan je u nastavku:

```
reate router
et router personality "Cisco 7206 running IOS 11.1(24)"
et router default tcp action reset
dd router tcp port 23 "scripts/router-telnet.pl"


reate netbsd
et netbsd personality "NetBSD 1.5.2 running on a Commodore
miga (68040 processor)"
et netbsd default tcp action reset
dd netbsd tcp port 22 proxy $ipsrc:22
dd netbsd tcp port 80 "sh scripts/web.sh"


ind 10.0.0.1 router
ind 10.1.0.2 netbsd
```

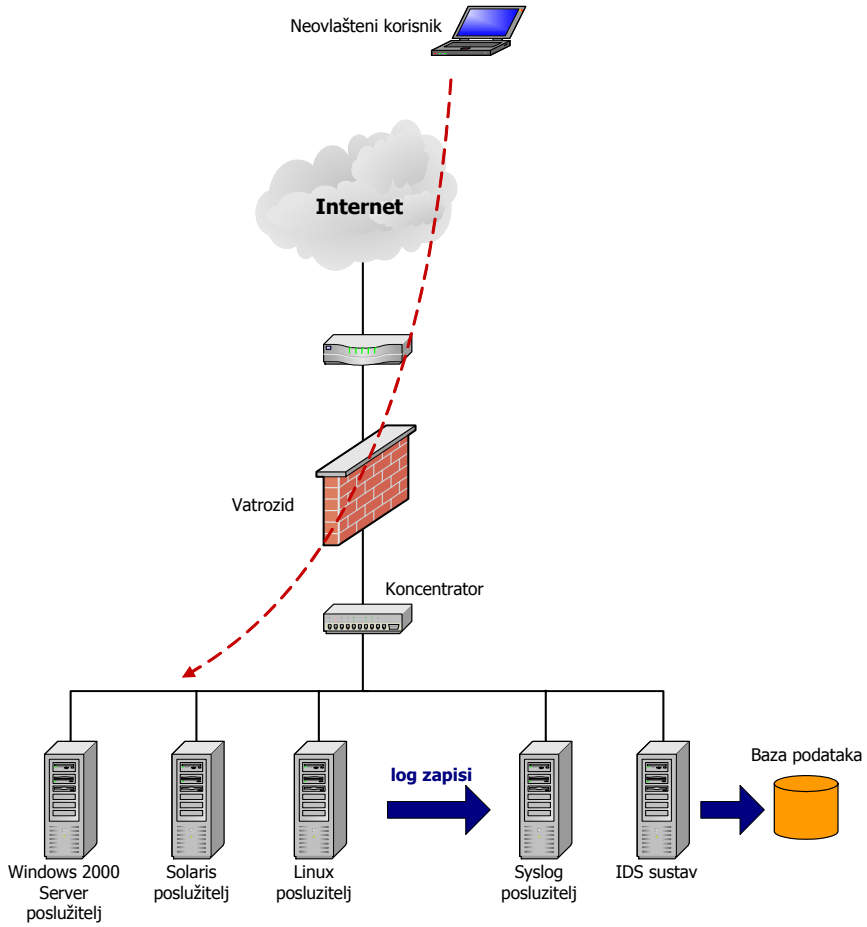
Ovom konfiguracijom definirana su dva virtualna poslužitelja: mrežni usmjerivač Cisco, serije 7206 s IOS 11.1(24) operacijskim sustavom te mrežni poslužitelj s NetBSD operacijskim sustavom. Na Ciscovom usmjerivaču simuliran je samo telnet servis za udaljeni terminalski rad, dok su na NetBSD poslužitelju omogućeni Web i SSH servisi. Web poslužitelj simuliran je skriptom ljuske `web.sh`, dok se SSH promet preusmjerava na izvorišnu adresu s koje je inicirana konekcija.

7. Honeynet sustavi

Za razliku od upravo opisanih *honeypot* sustava koji se u pravilu sastoje od jednog računala koje simulira određeni broj mrežnih servisa, odnosno poslužitelja, *honeynet* sustavi puno su kompleksniji i mogu se opisati kao napredniji model *honeypot* tehnologije. *Honeynet* sustavi najčešće se implementiraju kao kompletni računalni sustavi sa svim komponentama koje se koriste i u klasičnim implementacijama mrežnih okruženja (poslužitelji, vatrozidi, sustavi za detekciju neovlaštenih aktivnosti i sl.). Smisao i vrijednost *honeynet* implementacija isključivo je istraživačkog karaktera, s osnovnim ciljem prikupljanja novih spoznaja o tehnikama i alatima koje neovlašteni korisnici upotrebljavaju prilikom provođenja napada.
Značajnije razlike *honeynet* u odnosu na *honeypot* sustave su:

- radi se o složenijim računalnim sustavima s različitim komponentama kojima se simulira realno mrežno okruženje. Ovakva arhitektura omogućuje istovremenu simulaciju više tipova mrežnih uređaja (usmjerivači, preklopnici, vatrozidi...) i operacijskih sustava (Windows, Solaris, Linux,...), što omogućuje prikupljanje veće količine informacija o neovlaštenim korisnicima;
- mrežni servisi, poslužitelji i ostala mrežna oprema ne simuliraju se posebnim specijaliziranim programskim paketima (iako niti ova mogućnost nije isključena) kao u slučaju većine klasičnih *honeypot* sustava, već se koriste realni programi i uređaji koji se svakodnevno koriste u različitim mrežnim okruženjima;
- sustavi su znatno realniji od *honeypot* rješenja, što u velikoj mjeri smanjuje mogućnost njihove detekcije od strane neovlaštenih korisnika.
- *Honeynet* sustavi predstavljaju znatno veći sigurnosni rizik u odnosu na klasične *honeypot* sustave te zahtijevaju vrlo dobro poznavanje različitih mrežnih protokola, tehnologija i operacijskih sustava, kao i područja računalne sigurnosti.
- Potreban veći angažman oko postavljanja i održavanja sustava.

Na sljedećoj slici (Slika 4) prikazana je tipična arhitektura jednog *honeynet* sustava.



Slika 4 - Honeynet

U ovakvoj konfiguraciji potrebno je posebnu pažnju obratiti na sigurnosnu politiku vatrozida iza kojeg se nalazi *honeynet* sustav. Konfiguraciju je potrebno prilagoditi tako da se omogući prikupljanje što veće količine informacija o neovlaštenim korisnicima, a da se pritom neovlaštene aktivnosti ograniče isključivo na *honeynet* sustav. Površnom i nepažljivom konfiguracijom vatrozida situacija može vrlo lako izmaći kontroli, nakon čega kompromitirani *honeynet* sustav predstavlja ozbiljnu prijetnju i za legitimne računalne sustave. Ovu mogućnost uvijek treba svesti na minimum.

Kako je na slici prikazano, svi log zapisi prosljeđuju se udaljenom `syslog` poslužitelju, čiji je jedini zadatak prikupljanje i analiza log zapisa te obavješćivanje administratora pri detekciji sumnjivih događaja.

Komunikaciju prema `syslog` poslužitelju potrebno je ograničiti samo na komponente *honeynet* sustava koje imaju mogućnost bilježenja log zapisa putem `syslog` protokola i na UDP 514 mrežni port (SYSLOG). Ovo je moguće vrlo jednostavno korištenjem `iptables` programskog paketa. Primjer naredbi koje je u tu svrhu potrebno izvršiti je:

```
ptables -A INPUT -s honeynet --destination-port 514 ** -j ACCEPT
ptables -A INPUT -j DROP
```

Na računalima na kojima je podešeno prosljeđivanje log zapisa na udaljeni `syslog` poslužitelj potrebno ja maksimalno prikriti informacije o takovoj konfiguraciji. U suprotnom, neovlašteni korisnik može jednostavno prepoznati *honeypot* sustav te doći do adrese na koju se šalju log zapisi. Identifikacijom IP adrese `syslog` poslužitelja, napadač ga može ili pokušati kompromitirati ili pokrenuti neki od napada uskraćivanjem računalnih resursa (engl. ***D**enial **o**f **S**ervice – DoS*) koji će onemogućiti daljnje bilježenje log zapisa.

Postoje implementacije *honeynet* sustava slične opisanoj, u kojoj je jedna od ideja upravo ta da se neovlaštenog korisnika natjera na otkrivanje i pokušaj kompromitiranja udaljenog `syslog`

poslužitelja. Budući da IDS sustav ionako prati i bilježi cijeli promet na mreži ovakve metode omogućuju analizu postupaka naprednijih neovlaštenih korisnika.
Na samom `syslog` poslužitelju poželjno je instalirati neki od alata za periodičku analizu log zapisa i obavješćivanje administratora (npr. `logcheck` i `swatch`), kako bi se pri detekciji događaja administrator odmah obavijestio o tome.
IDS sustav potrebno je podesiti tako da bilježi sav promet na *honeynet* mreži. Na taj način moguća je detaljna analiza i rekonstrukcija svih događaja, što je jedna od osnovnih zadaća ovakvih sustava. Pohranjivanje u bazu podataka omogućiti će pretraživanje prema različitim kriterijima, što također može pomoći pri kasnijoj analizi, a vrlo je korisno i kod različitih statističkih obrada. Prikrivanje IDS sustava također je vrlo važan korak za pouzdanu implementaciju *honeynet* sustava. IDS sustav u ovakvoj arhitekturi predstavlja primarni izvor informacija o neovlaštenim aktivnostima i posebno je važno voditi računa o sigurnosti prikupljenih podataka. U tu svrhu moguće je IDS sustav postaviti u nevidljivom modu (engl. *stealth IDS*), ali ta tema izlazi van opsega ovog dokumenta.

8. Zaključak

Dokument opisuje tehnologiju *honeypot* sustava, relativno novu tehnologiju u području računalne sigurnosti, čiji je osnovni cilj detekcija neovlaštenih aktivnosti i prikupljanje novih spoznaja o tehnikama i alatima koje neovlašteni korisnici upotrebljavaju prilikom provođenja napada. Opisani su osnovni koncepti i ideje, navedena je osnovna podjela *honeypot* sustava prema njihovim svojstvima te su dani primjeri konkretnih implementacija.