CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Računala mamci i ponašanje napadača

CCERT-PUBDOC-2008-09-241

+CERT.hr u suradnji s LSS

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

Rezultat toga rada je i ovaj 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

Računala mamci (eng. *decoy computers*) su sustavi koji omogućuju otkrivanje potencijalnog udaljenog napada. Napadači koriste sigurnosne propuste u operativnim sustavima ili programima koji se nalaze na tom računalu kako bi uzrokovali štetu na sadržajima, preuzeli povjerljive ili osobne informacije (brojeve kreditnih kartica, lozinke, i sl.), dobili kontrolu nad računalom ili ga učinili potpuno neupotrebivim.

Proizvođači programskih paketa aktualiziraju svoje proizvode izdavanjem zakrpi (eng. *patch*) kako bi ispravili poznate sigurnosne propuste. Usprkos stalnom trudu proizvođača da svoje proizvode učine sigurnijim, napadači pronalaze nove sigurnosne propuste i grade alate za njihovo iskorištavanje (eng. *exploit*) i tako ugrožavaju sigurnost podataka na računalu. Računala mamci su izvrstan način za nadgledanje, praćenje i rano otkrivanje pokušaja napadača da iskorištavanjem sigurnosnih propusta dobije ovlasti na računalu.

Konvencionalne zaštite na računalu (vatrozidi, antivirusni programi, zakrpe,...) često nisu dovoljne kako bi se spriječili ovakvi napadi. Ovim dokumentom čitatelju će biti objašnjena razlika između zlonamjernih napadača koji provaljuju u računalne sustave s ciljem nanošenja štete, te onih koji to čine kako bi unaprijedili računalnu sigurnost. Nadalje, bit će navedeni i pobliže opisani načini napada i zlonamjerni programski kodovi (virusi, crvi, trojanski konji, itd.) upravo kako bi se upozorilo korisnike računala na oprez. Kao važan dio obrane od zlonamjernih napada u nastavku dokumenta razrađena je cjelina računala mamaca u kojoj su pobliže opisane vrste i njihova namjena, princip rada, te postupak postavljanja jednog *honeypot* sustava.

2. Definicija i vrste napadača

Napadačem se smatra osoba koja svoje računalno znanje koristi kako bi ugrozila sigurnost računala ili podataka pohranjenih na računalu, a često ih se naziva hakerima (eng. *hacker*). Treba naglasiti da se napadači koji provode zlonamjerne ili kriminalne aktivnosti nazivaju „crackerima" kako bi se napravila jasna razlika među njima i hakerima koji djeluju prema etičkim načelima. Haker nema namjeru nanošenja zla i štete ljudima i računalnim sustavima.

Hakera se može definirati kao:

- osobu koja uživa istraživati detalje programskih sustava, te kako povećati njihove kapacitete i poboljšati učinkovitost
- nekoga tko programira s puno entuzijazma (ponekad fanatizma), te mu je sam posao programiranja ispred bilo koje druge aktivnosti
- osobu koja uživa u intelektualnom izazovu rješavajući ga koristeći inteligenciju i kreativnost

Crackerom se smatra osobu koja pokušava provaliti u računalo drugog korisnika pri tome koristeći sve dostupne metode i alate (crve, trojanske konje, rootkitove, sigurnosne propuste, društveni inženjering, i sl.) kako bi ga oštetila ili ukrala informacije. Postoje dvije vrste *crackera*:

1. oni koji posjeduju računalna znanja koja su potrebna da bi sami napisali zlonamjerne programe i
2. oni koji se samo znaju koristiti tim alatima.

2.1. Vrste napadača

Kada je u pitanju računalna sigurnost, postoji nekoliko skupina u koje se napadači mogu podijeliti. Podjela se temelji na uzorcima ponašanja i ciljevima koje žele postići. U nastavku su prikazane četiri osnovne skupine napadača podijeljene prema etičkim načelima.

2.1.1. White Hat hakeri

Ovim imenom se naziva hakere koji pronalaze sigurnosne propuste iz nesebičnih ili dobronamjernih razloga. White Hat hakere obično zapošljavaju tvrtke s ciljem osiguravanja i zaštite IT sustava. Tvorci su velikog broja inovativnih načina zaštite računala i računalnih sustava poput antivirusnih programa i zaštita na samom Internetu.

2.1.2. Black Hat hakeri

U najvećoj mogućoj mjeri narušavaju sustave računalne sigurnosti bez odobrenja. Osobe koje koriste tehnologiju (najčešće računalo ili Internet) za terorističke radnje, vandalizam (zlonamjerno uništavanje), prijevare sa kreditnim karticama, krađu identiteta, krađu intelektualnog vlasništva i/ili mnogih drugih oblika zločina. Također su poznati kao *crackeri*, često tvorci zlonamjernih programa (virusa, crva, trojanaca,...) čiji je cilj ukrasti podatke ili oštetiti računalne sustave. Njihove radnje ponekad nisu rezultat želje za materijalnom koristi već rezultat čiste zabave.

2.1.3. Grey Hat hakeri

Grey Hat hakeri su osobe koje posjeduju iznimna računalna znanja, ali isto tako i dvosmislena etička načela. Predstavljaju mješavinu između White Hat i Black Hat hakera. Najčešće nemaju zle namjere i ne napadaju radi stjecanja materijalne koristi, ali ponekad počine zločin tijekom iskorištavanja sigurnosnih propusta. Proboje u računalne sustave koje izvodi ova vrsta hakera smatra se manje destruktivnom i ne uzrokuje štetu. Ciljane aktivnosti su ispitivanje i nadgledanje sustava u koje su provalili.

2.1.4. Blue Hat hakeri

Velike tvrtke ih unajmljuju da pronađu sigurnosne propuste kako bi ih mogli zatvoriti prije izdavanja programskih paketa. Jedan od takvih primjera je Microsoft koji organizira konferenciju po nazivom Blue Hat Microsoft Hacker Conference gdje znanja izmjenjuju Microsoftovi inženjeri i Blue Hat hakeri radi poboljšanja sigurnosti Microsoftovih proizvoda. Konferencija se održava od 2004. godine dva puta godišnje, na proljeće i jesen u Microsoftovim prostorima u Redmondu.

3. Etička načela korištenja računala

Pri korištenju računalne opreme potrebno se pridržavati nekih etičkih načela. Kako bi zaštitili samoga sebe, a i pružili sigurnost drugima, američki Computer Ethics Institute je predstavio: „Deset zapovjedi računalne etike“ (eng. *Ten Commandments of Computer Ethics*). Ova pravila predstavljaju vrlo važan dio računalne kulture, pa ih se navodi u nastavku kako bi ih svaki korisnik pri korištenju računalne opreme imao na umu.

3.1. Deset zapovjedi računalne etike

1. Računalo se ne smije koristiti da bi se naudilo drugima.
2. Ne smije se uplitati u računalne poslove drugih ljudi.
3. Ne smije se neovlašteno pristupati dokumentima na računalima drugih ljudi.
4. Računalo se ne smije koristiti za krađu.
5. Računalo se ne smije koristiti za lažno predstavljanje.
6. Na računalu se ne smije umnožavati ili koristiti zakonom zaštićene programske pakete koje korisnik nije platio.
7. Nije dozvoljeno upotrebljavati računalne resurse drugih ljudi bez dozvole ili odgovarajuće naknade.
8. Nije dozvoljeno prisvajanje intelektualnog vlasništva drugih ljudi.
9. Potrebno je misliti o društvenim posljedicama programa koji pišemo ili sustava koji razvijamo.
10. Računalo se uvijek mora koristiti na načine koji osiguravaju uvažavanje i poštovanje drugih.

Pri svakoj upotrebi računala potrebno je savjesno i odgovorno ponašanje upravo kako ne bi napravili štetu drugima, kompromitirali sigurnost njihove računalne opreme i podataka na njoj. Isto tako je potrebno voditi računa o sigurnosti vlastitih podataka i pravovremeno se zaštititi od moguće krađe ili gubitka podataka. Često se događa u praksi da se ljudi ne pridržavaju ovih etičkih načela, što je upravo i razlog koji dovodi u pitanje računalnu sigurnost. Kako bi se korisnici ipak uspjeli obraniti potrebno je razvijati sustave poput računala mamaca, antivirusnih programa, vatrozida i njima sličnih.

4. *Honeypot* sustavi

Honeypot su sustavi koji služe za otkrivanje, uklanjanje i u jednoj mjeri suzbijanje pokušaja neovlaštene upotrebe računalnih sustava. Konstruirani su na način da oponašaju sustave koji su od nekog interesa napadaču, ali ograničavaju napadaču pristup cijelom mrežnom sustavu. Honeypot sustavi su obično nezaštićeni i omogućuju promatranje napadača i njegovih postupaka.

Svrhe honeypot sustava:

- promatranje načina na koji napadač iskorištava propuste i time naučiti gdje se nalaze i koje su ranjivosti sustava koje je potrebno ispraviti
- uloviti i zaustaviti napadača dok pokušava dobiti ovlasti administratora na sustavu (umjesto da se to radi dok provaljuje u „pravi" sustav)
- proučavanjem aktivnosti napadača projektanti mogu napraviti sustave koji su otporniji na proboje

Honeypot sustavi su najvrjedniji u funkciji alata za nadgledanje napadača i rano otkrivanje napada. Mogu se naći u obliku računala, datoteka ili podatkovnih zapisa, pa čak i neupotrebljenih IP adresa. Ne koristi ih se za normalne radnje (poslovanje, edukaciju, zabavu i sl.), tako da se za sve što otkriju može pretpostaviti da je zlonamjerno ili nije dozvoljeno. Jedna vrlo praktična prednost ovakvih sustava je da svu neželjenu poštu (eng spam) filtriraju sa velikom učinkovitošću. Ukoliko se honeypot sustavima ne rukuje ispravno, postoji veliki rizik da napadač provali i u ostala računala, pa se savjetuje veliki oprez u instalaciji, podešavanju i korištenju samih honeypot sustava.

Honeypot sustavi su klasificirani s obzirom na upotrebu i razinu interakcije.

4.1. Klasifikacija prema namjeni

4.1.1. Honeypot sustavi za zaštitu radne infrastrukture

Honeypot sustavi za obradu podataka rade tako da oponašaju programe i operativne sustave koji su zanimljivi napadačima. Obično ih koriste tvrtke kako bi umanjile rizik od zlonamjernih napada prema računalima koja koriste u poslovanju. Jedina im je mana što mogu uhvatiti samo određenu količinu informacija. Postavljaju se unutar mreže zajedno s drugim poslužiteljima kako bi podigli razinu sigurnosti (navodeći napadača na lažni trag). Ovakvi honeypot sustavi pripadaju vrsti koja ima nižu razinu interakcije s napadačem i stoga ih je lakše koristiti, ali daju manju količinu informacija o napadaču i napadu. Za zaštitu radne infrastrukture koriste se gotovo sve vrste honeypot sustava opisane u poglavlju 4.2.

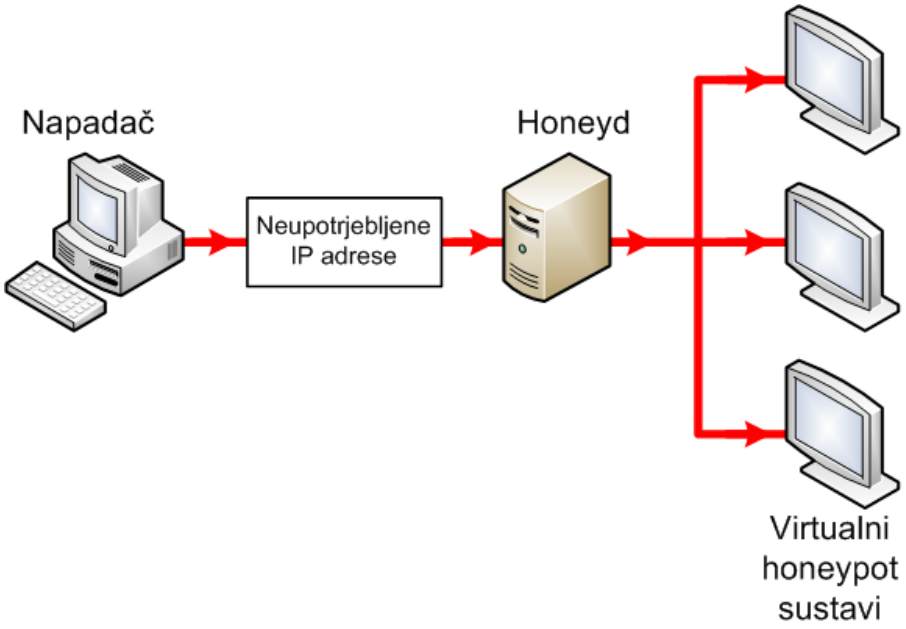
4.1.2. Istraživački honeypot sustavi

Kao što i sam naziv kaže, upotrebljava ih se za istraživanje „Black Hat" organizacija, njihovih namjera i načina na koji provaljuju u sustave. Pokreću ih volonteri, neprofitne organizacije ili obrazovne ustanove i služe kako bi se unaprijedili načini zaštite od provale napadača u računalne sustave. Istraživački honeypot sustavi su vrlo složeni za održavanje i nadgledanje, ali daju velike količine informacija.

4.2. Klasifikacija s obzirom na razinu interakcije

4.2.1. *Honeyd* alati

Honeyd alat je honeypot sustav niske razine interakcije s napadačem. Razvijen primarno za rad na Unix operativnim sustavima, radi na principu nadgledanja neupotrjebljenih IP adresa. Svaki put kada uoči pokušaj spajanja na neku od neupotrijebljenih IP adresa, presretne taj pokušaj i potom uspostavlja vezu s napadačem, pretvarajući se da je žrtva. Uobičajeno je postavljen tako da otkrije i zapiše svako spajanje na bilo koji UDP (eng. *User Datagram Protocol*) ili TCP (eng. *Transmission Control Protocol*) port.



Slika 1. Prikaz rada Honeyd sustava

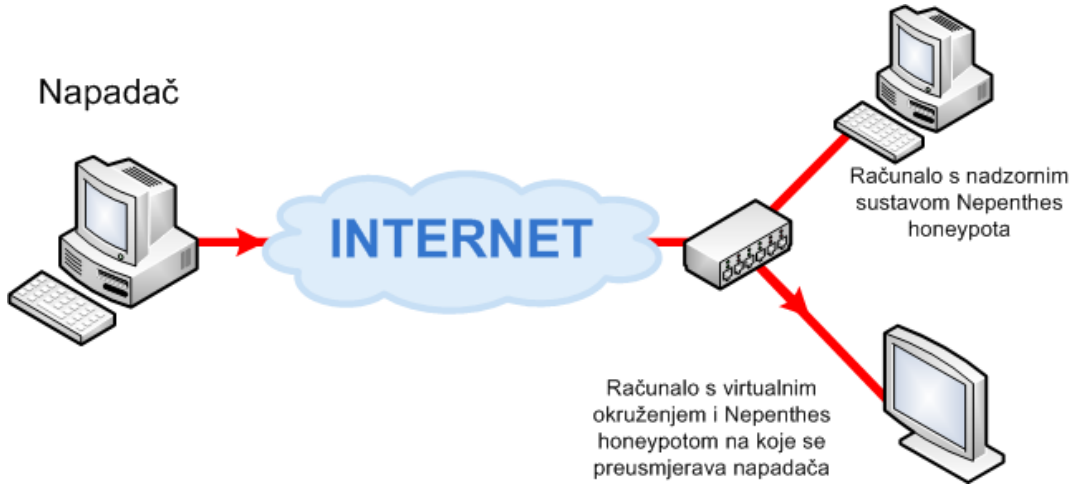
Kada se napadač spoji na imitirani servis, „honeyd“ otkriva i zapisuje svu interakciju napadača s tim servisom. „Honeyd“ potom stvara virtualne honeypot sustave u koje će napadač „provaliti“. U slučaju imitiranog FTP (eng. *File Transfer Protocol*) poslužitelja, moguće je otkriti napadačevo korisničko ime i lozinku kojima provaljuje u sustav, naredbe koje zadaje, što traži, pa čak i u posebnim slučajevima napadačev identitet.

Na sličan način radi i većina imitiranih servisa: očekuju određeno ponašanje, a potom odgovaraju na način kako su programirani. Korisnik „honeyd“ alata definira parove „napad – reakcija“ kojima definira reakciju sustava na određenu vrstu napada. Ograničenje ove metode je da ako napadač učini nešto neočekivano (nešto što nije definirano parom napad - reakcija), „honeyd“ ne zna pravilno odgovoriti. Ukoliko „honeyd“ nepravilno odgovori na upit, napadač shvaća da se radi o mamcu i odustaje od napada.

„Honeyd“ može imitirati operativne sustave ili programe, tj. može imitirati usmjeritelje, „Windows“ web poslužitelje, Linux DNS (eng. *Domain Name System*) poslužitelje i dr.

4.2.2. *Mwcollect*, *nepenthes* i *honeytrap* alati

„Mwcollect“ i „nepenthes“ alati se koriste za otkrivanje zlonamjernih programa koji se sami šire s računala na računalo. Napadi se zapisuju, a potom se izlučuje zlonamjerni programski kod unaprijed određenim tehnikama. Dakako napad se odvija u virtualnom okruženju koje honeypot sustav podmeće napadaču, tako da korisnikov sustav zapravo ne biva zaražen zlonamjernim programom.



Slika 2. Prikaz rada *nepenthes* honeypot sustava

„Honeytrap" alat stvara priključnice (eng. *port*) kojima osluškuje pokušaje TCP spajanja i izdvaja ih iz mreže. Nakon izdvajanja „Honeytrap" sustav odmah preuzima zlonamjerne programe. Ovaj pristup omogućuje otkrivanje novih vrsta napada koje nisu uspjeli detektirati antivirusni alati.

Poznato je da većina zlonamjernih programa iskorištava sigurnosne propuste programa ili operativnih sustava. Sva tri prethodno nabrojana sustava rade na način da dopuštaju zlonamjernim programima iskorištavanje sigurnosnih propusta unutar izdvojenog - virtualnog okruženja. Svi alati su podešeni tako da kada zamijete da je neki od sigurnosnih propusta iskorišten, bilježe kod zlonamjernog programa i na neki način obavještavaju administratora sustava. Ovi alati u sebi sadrže module kojima zapisuju, analiziraju i zaustavljaju izvršavanje zlonamjernog programskog koda koji se mogu proizvoljno uključivati ili isključivati.

4.2.3. Spam i e-mail honeypot sustavi

Spam honeypot sustavi se upotrebljavaju kako bi se otkrile aktivnosti spammera (autora neželjenih poruka elektroničke pošte). Mogu otkriti e-mail adrese na koje spammeri šalju test poruke. Napadač test porukama provjerava da li sustavi prosljeđuju poruke, a rezultat provjere se vraća na adresu napadača. Kada spam honeypot zabilježi takvu poruku, šalje test poruku na adresu napadača sa informacijom da je sustav pogodan za ovakvu vrstu aktivnosti. Napadač tada šalje velike količine elektroničkih poruka nedopuštenog sadržaja. Honeypot sustav na temelju adrese iz test poruke prepoznaje da se radi o elektroničkim porukama koje šalje napadač, te ih zaustavlja. Adresa napadača može biti jedan od zloupotrebljenih sustava pod nadzorom napadača, tako da može biti teško otkriti početnu točku napadača. Spam honeypot sustavi su od velike pomoći pri filtriranju spam pošte i u praksi su se pokazali kao dobro rješenje.

E-mail honeypot sustavi u principu imaju istu namjenu, primanje spam e-mail pošte. Napadači skupljaju adrese elektroničke pošte na Internetu, te šalju velike količine poruka nedopuštenog sadržaja. E-mail honeypot sustavi stvaraju lažne adrese elektroničke pošte i postavljaju ih na Internet kako bi ih napadač dodao u svoju bazu podataka. Kada napadač pošalje poruku nedopuštenog sadržaja na lažnu adresu, honeypot bilježi adresu i zapisuje ju na listu napadača. Napadači zloupotrebljavaju adrese stvarnih korisnika, tako da je teško odmah zabilježiti stvarnu adresu napadača.

4.3. Kako postaviti honeypot sustav

Najpopularniji virtualni honeypot sustav koji radi u Windows okruženju je *honeyd*. Kada napadač istraži honeypot sustav vrlo je važno da se čini da je u pitanju pravi korisnik. Postavljanje honeyd sustava u Windows okruženju naizgled se čini jednostavnim, svodi se na postavljanje programa i servisa koji će oponašati stvarne korisnike. U praksi je međutim potrebno poprilično dobro poznavanje problematike kako bi se uspjelo zavarati napadača da se radi o honeypot sustavu, a ne korisničkom računalu.

Prije postavljanja honeypot sustava potrebno je poznavati nekoliko stvari:

- koje TCP i UDP priključnice postaviti u status osluškivanja kako bi oponašale željeno računalo

- tekst koji bi se trebao prikazati napadačima kada pošalju upit honeyd sustavu
- detalje o servisima i programima koje se žele simulirati

Pri postavljanju honeypot sustava potrebno je obratiti pozornost na nekoliko odluka koje bi mogle biti važne pri odvlačenju napadačeve pozornosti na mamac. To su:

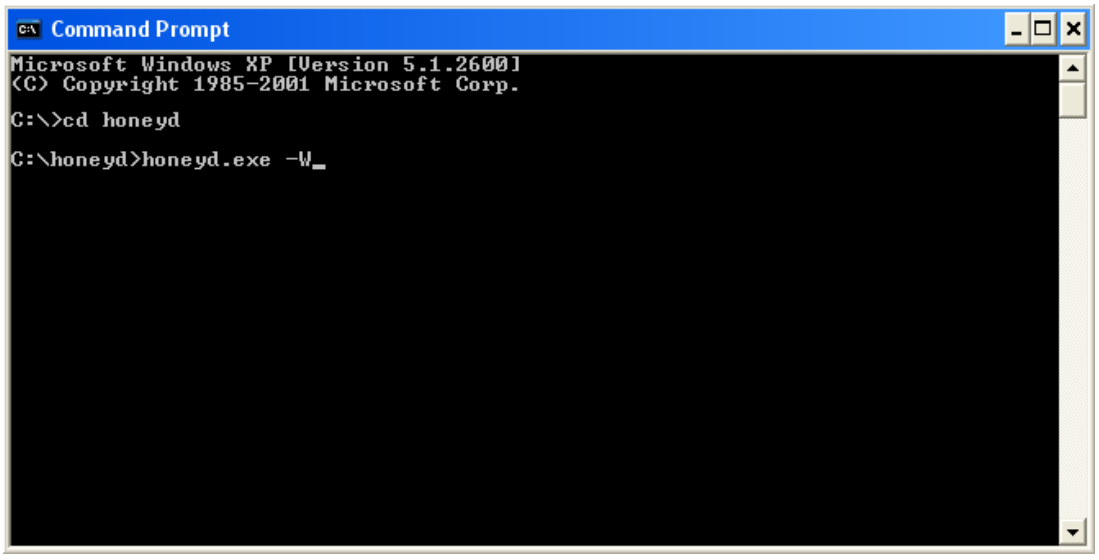
- potreba za honeypotom sa visokom razinom interakcije,
- upotreba operativnog sustava ili virtualnog okruženja,
- koji operativni sustav bi bio najpogodniji,
- da li aktualizirati operativni sustav,
- koje servise i programe postaviti na honeypot,
- koji su operativni sustavi pogodniji napadačima,
- koje alate za održavanje postaviti i
- kakvo će računalo biti potrebno za pokretanje željenog honeypot sustava

Koliko će honeypot sustav biti uspješan u skretanju pozornosti napadaču ovisi o gore navedenim stavkama. Potrebno je posvetiti pozornost svakoj od ovih stavki jer, ukoliko se dogodi propust, napadač može zaobići honeypot i izvršiti napad na računalo korisnika.

4.3.1. Instalacija honeyd alata

„Honeyd" je besplatni *open-source* honeypot alat sa niskom razinom interakcije. Razvijen je 2002. godine za istraživanje načina napada i metoda kojima se služe napadači. Međutim, zbog karakteristika ušao je i u komercijalnu uporabu. „Honeyd" ima veliki broj mogućnosti, ali pregršt konfiguracijskih postavki (eng. *configuration settings*) može zbuniti korisnika početnika pri prvoj upotrebi. Ova vrsta honeypot sustava je vrlo prilagodljiva i s te strane korisniku je omogućeno da ga postavi na željeni način.

Prvo je potrebno preuzeti „honeyd" program sa web stranice tvrtke netVigilance. Nakon preuzimanja datoteke potrebno je napraviti mapu na lokaciji C:\ sa imenom honeyd (C:\honeyd). Potom je potrebno izdvojiti datoteke iz preuzete arhive u prethodno napravljenu mapu. „Honeyd" se pokreće putem komandnog upita (eng. *Command prompt*) i to tako da se upiše naredba „honeyd.exe –W".



Slika 3. Naredbe za pokretanje „honeyd" programa

Kako bi se korisniku olakšalo postavljanje „honeyd" programa postoje već napravljene konfiguracijske skripte koje je moguće preuzeti i s Interneta. Konfiguracijske skripte omogućuju korisniku postavljanje načina na koji želi da njegov „honeyd" radi, servisa koje koristi, koliko

detaljne bilješke o napadaču da radi i sl. Nakon preuzimanja skripte je potrebno izdvojiti u mapu u „honeyd“ mapi (C:\honeyd\scripts\). Kao dodaci „honeyd“ programu korisni su programi poput Snort-a i/ili Ethereal-a koji služe za praćenje paketa koje „honeyd“ primi ili pošalje.

Također postoji i Linux/Unix inačica, a korisnici tih operacijskih sustava detalje o instalaciji i korištenju mogu pronaći na službenim stranicama proizvođača.

4.3.2. Nadgledanje honeyd programa

Kako bi korisniku bilo lakše nadgledati „honeyd“ program, korisno je zabilježiti slijedeće podatke vezane uz sustav:

- postavljena korisnička imena i lozinke
- ovlasti korisnika
- postavke tvrdog diska, ukupnu veličinu, broj diskova ili particija, slobodan prostor
- datoteke i direktorije
- pravila pristupa datotekama na datotečnom sustavu
- *ovlasti nad pojedinim dijelovima registry* sustava
- programe i procese na honeyd sustavu
- programe koji se automatski pokreću pri pokretanju sustava

Iako se navedeno čini kao velik broj podataka koje je potrebno zabilježiti, korisno je za napraviti kako bi se vidjelo kojim je datotekama napadač rukovao ili promijenio. Za prikupljanje podataka moguće je koristiti automatizirane programe, što je mnogo brže nego ručno zapisivanje. Postoji nekoliko besplatnih i komercijalnih programa koji zapisuju podatke, npr. Tripwire, Sysdiff, Windiff, i slični.

Također je potrebno pratiti izmjenu podataka na mrežnom sustavu, kako bi se razlučio koje su mrežne karakteristike normalne, a koje nisu. U samom honeypot sustavu je lako zamijetiti kada je napadač prisutan, pojavljuje se povećanje broja otvaranje, izmjena ili premještanja datoteka. Za nadgledanje ove vrste korisniku je dostupno nekoliko programskih rješenja poput Netmon, Netstat ili TCPView alata.

„Honeyd“ samostalno bilježi podatke o napadačevoj aktivnosti, tako da nije potrebno dodavati nikakve alate. Sakuplja ih u bazu i potom organizira po raznim kriterijima (vrijeme napada, adresa napadača, lokacije koje je napadač oštetio ili izmijenio,…).

4.4. Kako sakriti honeypot sustav

Autori zlonamjernih programa su se uspjeli othrvati protiv ove zaštite na način da su napravili sustave za otkrivanje honeypotova. Sustavi za otkrivanje rade na način da pronalaze određene karakteristike honeypot sustava i tako ih identificiraju. Međutim, kako postoji mnogo vrsta honeypot sustava, što rezultira s mnogo karakteristika koje treba uzeti u obzir, pa je zato i efikasnost ovih alata smanjena. To je jedan od neobičnih primjera kod programa, kada je veliki broj programa koji se malo razlikuju koristan. Prednost je također, postaviti i jedan honeypot sustav koji je lako otkriti jer će većina napadača odustati kada shvate da se radi o računalu mamcu zato što će pretpostaviti visoki nivo sigurnosti u dotičnoj mreži (kao kod banke: 90% pljačkaša će odustati kada vidi nadzorne kamere u poslovnici).

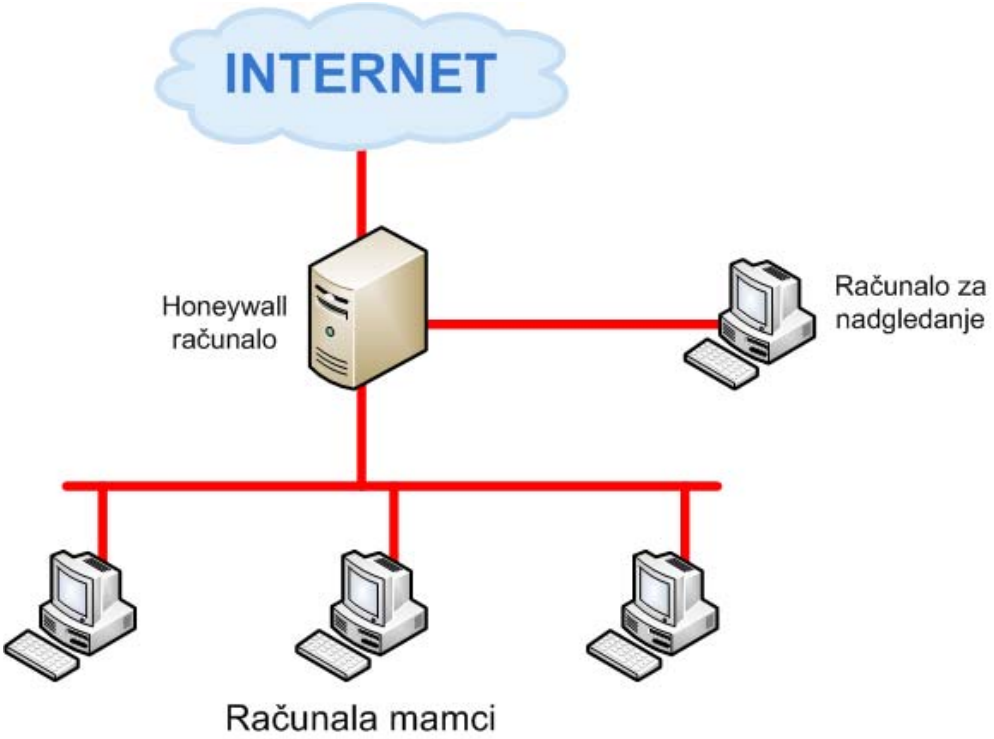
Od svih honeypot sustava najteže je sakriti one s niskom razinom interakcije jer ne sadrže operativni sustav. Očito, teško ih je sakriti jer ne sadrže napadačima zanimljive ili komplicirane servise, ali i zbog činjenice da niska razina interakcije brzo otkriva kako se radio o „automatu“ a ne o pravom sustava. Glavna razina komunikacije je putem mreže što znači da se honeypot nalazi na računalu sa stvarnim operativnim sustavom. Zbog toga se preporuča korištenje honeypota više razine interakcije (ali to od administratora zahtjeva i bolje poznavanje problematike).

Za otkrivanje honeypot sustava su razvijeni čak i posebni alati kojima se napadači koriste (Send-Safe Honeypot Hunter, Sebek.c alati, wmware_honeypot.c alati, Kebes,…). Posebne metode otkrivanja rijetko izađu na vidjelo. Moguće ih je otkriti prema programima za virtualna okruženja koje koriste (npr. VMware programski paket). Napadači najčešće iskoriste propuste tih programa kako bi ih identificirali. Zbog činjenice da se honeypot sustavi nadograđuju, napadačima je otežan posao jer su sve bolje i bolje sakriveni.

5. *Honeynet* sustavi

Ovi su sustavi najbolji primjer sustava s visokom razinom interakcije. Sastoje se od mreže fizičkih računala na kojima su postavljeni virtualni mamci sa stvarnim programima i podacima čija je namjena namamiti napadača. Mogu kontrolirati i zapisivati sav promet koji se događa unutar infrastrukture. Napadači traže, napadaju i provaljuju u ove sustave ne shvaćajući da se zapravo nalaze u honeynetu. Sva aktivnost napadača, od e-mailova do učitavanja datoteka se prati bez da su svjesni toga.

Honeynet sustavi su dodatno zaštićeni jedinicom koja se naziva *honeywall*. Honeywall je najčešće fizičko računalo s programima za zapisivanje, praćenje i ograničavanje napada, te osiguranje računala za nadgledanje koje je spojeno na honeynet mrežu. Honeywall ograničava mogućnosti napadača na način da kontrolira količinu izlaznih podataka koja se vraća napadaču.



Slika 4. Prikaz *honeynet* sustava

Smatra se da je svaki pokušaj spajanja na honeynet zlonamjeran, jer na njemu ne postoje stvarni korisnici. Sav promet koji se zabilježi na honeynet mreži je nedopušten pa je stoga osoba koja nadgleda honeynet sigurna da se radi o nedopuštenom spajanju na honeynet mrežu. Ova činjenica uvelike olakšava posao osobama koje nadgledaju: nije potrebno pretraživati velike količine podataka kao kod konvencionalnih načina zaštite (vatrozid, antivirusnih programa, sustava za otkrivanje nedopuštenog spajanja, itd.). Kako bi se privukla pažnja napadača datoteke na računalima mamcima koja se nalaze unutar honeyneta se najčešće nazivaju imenima „Financije“, „Osobni podaci“ i sl.

Pri postavljanju honeyneta potrebno je obratiti pozornost na slijedeće funkcije:

- kontrola podataka koja služi za sputavanje napadačeve aktivnosti kako ne bi upotrijebio honeynet da ugrozi druge sustave,
- nadgledanje podataka kojim se zapisuju sve napadačeve aktivnosti unutar honeynet mreže, što može poslužiti u shvaćanju načina provale, alata koje napadač koristi te njegovih motiva,
- analiza podataka iz prikupljenih informacija o napadu i
- prikupljanje podataka ukoliko je u pitanju više honeynet sustava na različitim lokacijama (svi prikupljeni podaci se šalju u bazu podataka u centralnoj lokaciji)

6. Krađa identiteta

U današnjem računalnom okruženju korisnici računala mnogo slušaju o slučajevima krađe identiteta pri čemu je u interesu kriminalaca steći materijalnu dobit. Stručnjaci za računalnu sigurnost već duže vrijeme upozoravaju korisnike na tajne napade lukavih kriminalaca. Iako običan korisnik takve napade obično ne zamijeti, događaju se. Postoji velik broj kriminalaca, a većina njih se kradomice bogati zbog greški tvrtki, njihovih kupaca i korisnika. Jedan način krađe identiteta je krađa podataka iz baza banaka, Internet trgovina i posrednika, te ostalih ustanova koje pohranjuju podatke o identitetu korisnika. Drugi način je prijevarom dobiveni podaci od korisnika. Krađa identiteta se u gotovo svim zemljama svijeta smatra kaznenim djelom.

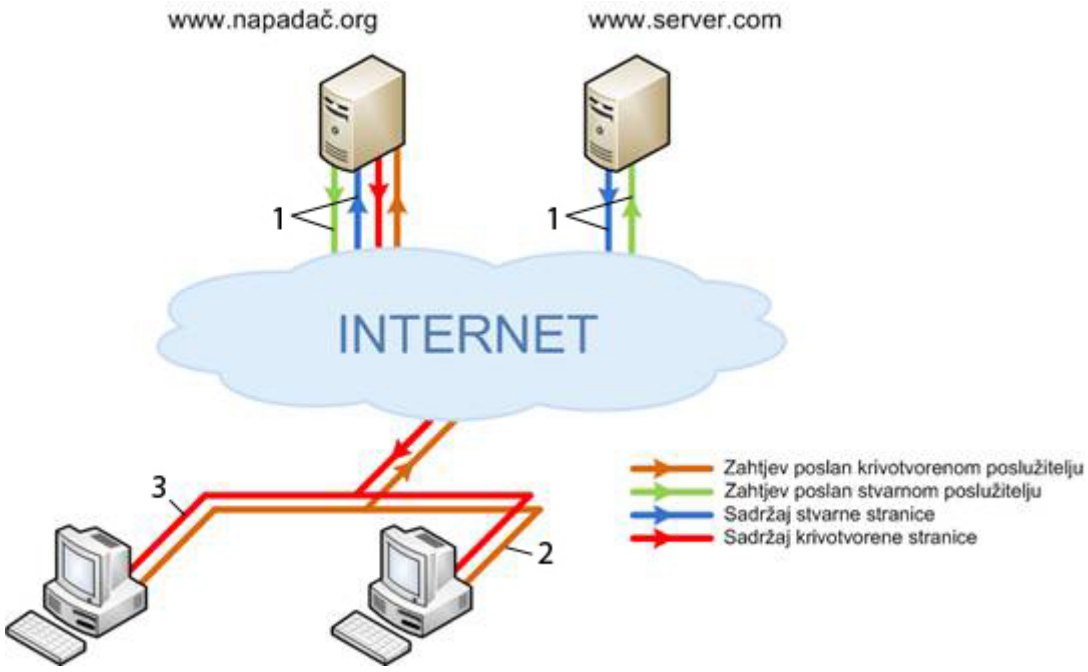
Važno je napomenuti da broj prijavljenih napada iz godine u godinu raste. Prema statistikama ITRC-a (eng. *Identity Theft Resource Center*), samo u zadnjih godinu dana bilježi se značajan porast broja napada. U 2007. godini je zabilježen broj od 446 prijavljenih napada dok je u prvih devet mjeseci 2008. godine prijavljeno 449 napada.

6.1. Spoofing

Zavaravanje (eng. *spoofing*) je slučaj krađe identiteta kada napadač ili program lažnim predstavljanjem dolazi do traženih podataka o žrtvi (brojeva kreditnih kartica, brojeva osiguranja, itd.). Dakle, napadač ili program se lažno predstavlja žrtvi kao neka druga osoba krivotvoreći podatkovne pakete i na taj način pokušava ugroziti sigurnost ili ukrasti podatke od žrtve. Napadač žrtvu vara promjenom zaglavlja paketa koje šalje, a ovisno o vrsti napada kojom se služi to mogu biti promijenjena zaglavlja IP (eng. *Internet Protocol*) paketa ili zaglavlja elektroničke pošte. Poznato je više metoda zavaravanja kojima se stječe ovlast nad ukradenim identitetom.

6.1.1. Man-in-the-middle napad

Ovaj napad je vrsta aktivnog prisluškivanja u kojem napadač stvara zasebne veze među žrtvama i šalje im poruke, zavaravajući ih da razgovaraju direktno jedan s drugim na privatnoj vezi, dok u stvarnosti cijeli razgovor kontrolira napadač. Napadač mora biti sposoban presresti sve poruke dviju žrtava i ubaciti nove. Napad je uspješan jedino kada napadač uspije oponašati svaku žrtvu bez da bude zamijećen.



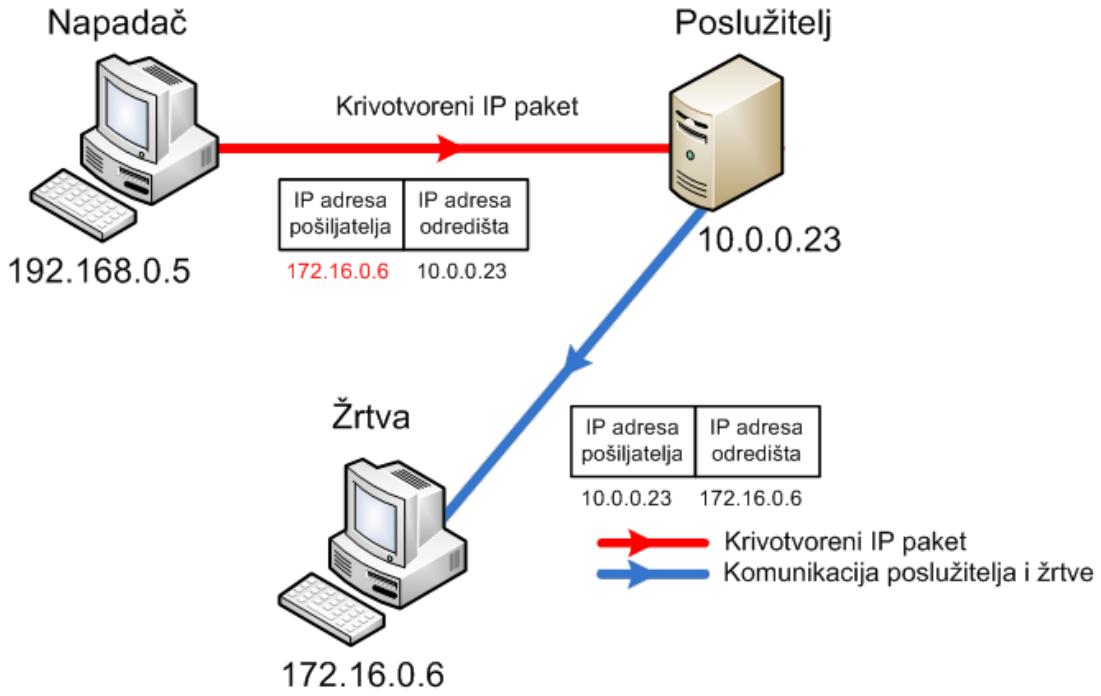
Slika 5. Prikaz principa *Man-in-the-middle* napada

1. Korisnik šalje zahtjev web poslužitelju, pri čemu napadač presreće zahtjev i stvara krivotvorinu istog sadržaja koji izgleda kao na web poslužitelju

2. Napadač preusmjerava korisnika na krivotvorenu web stranicu
3. Korisnik prima sadržaj krivotvorene web stranice

6.1.2. Napad korištenjem Internet skupine protokola

Ova vrsta zavaravanja odnosi se na stvaranje IP paketa sa krivotvorenom IP adresom s ciljem sakrivanja identiteta pošiljatelja ili oponašanja računalnog sustava. Osnovni protokol za slanje podataka putem Interneta i mnogih drugih računalnih mreža je Internet Protokol. Zaglavlje svakog IP paketa sadrži, među ostalim, numeričku adresu pošiljatelja i primatelja. Krivotvorenjem zaglavlja tako da sadrži drugu adresu, napadač može zavarati primatelja da je paket poslan s druge adrese.



Slika 6. Prikaz principa IP napada

IP zavaravanje se najčešće koristi pri DoS (eng. *Denial of Service*) napadima. U slučaju takvog napada cilj napadača je zatrpati žrtvu velikim količinama podataka. Paketi s krivotvorenim adresama su pogodni za takve napade i imaju određene prednosti - napad sa krivotvorenim IP paketima teže je filtrirati jer se čini da svaki paket dolazi sa različite adrese. Napadači često koriste ovu metodu kako bi onemogućili ispravan rad mrežnih sustava. Međutim, ova metoda može biti izuzetno zahtjevna s obzirom da je potrebno izmijeniti velik broj IP paketa u malo vremena.

Napad je učinkovit kod računala koja su povezana sigurnosnim odnosima, npr. u nekim mrežnim sustavima korisniku je omogućeno udaljeno spajanje s jednog na drugo računalo u istoj mreži bez upisivanja korisničkog imena i lozinke. Zavaravajući ciljano računalo lažnim IP paketima, napadač mu može pristupiti bez potvrde identiteta.

U Windows operativnom sustavu postoji nekoliko servisa koji su podložni ovakvim napadima:

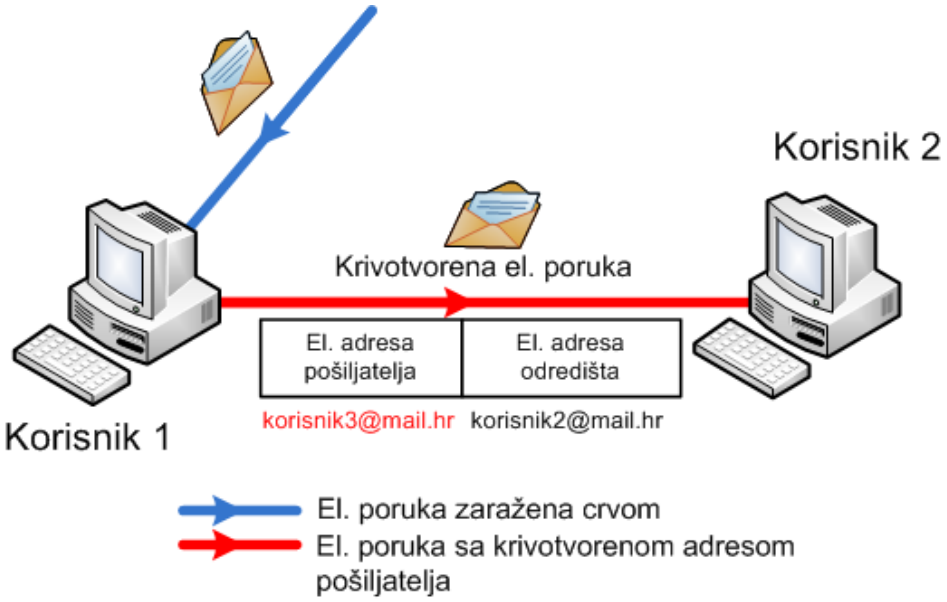
- RPC (Remote Procedure Call services)
- Svi servisi koji koriste IP potvrdu (npr. komunikacijski i servisi za preuzimanje podataka)
- X Window sustav
- Paket R servisa (rlogin, rsh, ...)

Zaštita od ovakve vrste napada je upotreba vatrozida (eng. *firewall*) koji će filtrirati IP pakete. Također je korisno, u mrežnim sustavima, konstruirati mrežne protokole i servise na način da se ne oslanjaju na izvornu IP adresu za identifikaciju i potvrdu.

6.1.3. Napad putem elektroničke pošte

Termin se koristi za opisivanje prijevarne aktivnosti u kojoj adresa pošiljatelja i drugi dijelovi zaglavlja elektroničke poruke bivaju izmijenjeni da bi se činilo da je poruka došla sa neke druge adrese. Promjenom određenih svojstava elektroničke poruke napadač postiže da se prikazuje lažni identitet. Često se koristi pri zatrpavanju korisnika elektroničkom poštom (eng. *e-mail spamming*) i krađi osobnih informacija (eng. *phishing*).

Mnogo pošiljatelja zlonamjerne elektroničke pošte (eng. *spammers*) koristi posebno razvijene programe koji stvaraju nasumično odabrane e-mail adrese, upravo kako ih ne bi otkrili. Slanje neželjene elektroničke pošte se koristi za masovno širenje crva (eng. *worms*) koji nakon što zaraze računalo pokušavaju pronaći e-mail adrese unutar adresara e-mail klijenta. Ukoliko uspije pronaći adrese, crv ih koristi kako bi se lažno predstavljao. Primjer napada prikazan je na slici 3.



Slika 7. Prikaz principa napada putem elektroničke pošte

- *Korisniku 1* je poslan e-mail koji je zaražen crvom, čije otvaranje rezultira zarazom računala
- Crv potom pronalazi e-mail adrese *Korisnika 2* i *Korisnika 3* u adresaru *Korisnika 1*
- Sa računala *Korisnika 1* crv šalje zaraženi e-mail *Korisniku 2*, pri čemu se čini da je e-mail poslan sa adrese *Korisnika 3*

6.1.4. Login napad

Zavaravanje pri prijavi (eng. *login spoofing*) je metoda koju napadači koriste kako bi dobili lozinku korisnika. Korisniku je prikazan normalan obrazac za prijavu, koji je ustvari zlonamjeran program, najčešće trojanac kojeg kontrolira napadač. Do proboja sigurnosti dolazi kada korisničko ime (eng. *username*) i lozinka (eng. *password*) bivaju uneseni. Unos se zapisuje i potom šalje napadaču.

Jedan od načina zaštite je korištenje kombinacija tipki prije same prijave, npr. *Ctrl-Alt-Delete* kod operativnog sustava Windows. Ukoliko se dogodi da korisnike operativni sustav ne traži da unesu kombinaciju tipki, potrebno je prijaviti grešku. Jezgra (eng. *kernel*) operativnog sustava nadgleda da li je kombinacija tipki unesena, tako da je nemoguće da neki trojanac presretne informaciju. Presretanje je moguće jedino u slučaju kada je i sama jezgra ugrožena nekim zlonamjernim programom. Programi koji inače nemaju sredstva za direktno upravljanje operativnim sustavom i samim komponentama računala kod zaraze jezgre mogu upravljati istima. Zaštita se temelji na zabrani udaljenog pristupa računalu sa ovlastima administratora i vatrozidu.

6.2. Keystroke logging napad

Pamćenje udaraca na tipku (eng. *Keystroke logging ili Keylogging*) je metoda pamćenja onog što je korisnik utipkao. Programe napisane s ciljem izvršavanja ove vrste napada nazivamo *Keyloggerima*, a najčešće se šire računalnim svijetom kao dio trojanca ili virusa. Ova vrsta napada ne predstavlja veliku opasnost jer je napadačima iznimno teško postići da se keylogger neprimjetno ugradi u operativni sustav. Napad je moguće izvesti na nekoliko razina:

- keyloggeri lokalne primjene na programe
- keyloggeri udaljene primjene na programe
- keyloggeri koji djeluju na sklopovlje računala
- keyloggeri udaljene primjene na sklopovlje računala
- keyloggeri osluškivači za bežičnu primjenu
- akustički keyloggeri

Neki od načina zaštite od ovakvih napada su:

- nadgledanje programa koji su pokrenuti
- anti-spyware programi
- vatrozid
- nadglednici mrežnog prometa
- automatski filtri
- lozinke za jednu upotrebu
- smart kartice

7. Zlonamjerni programski kodovi

Zlonamjerni programski kodovi (eng. *malware*) su programi čiji je zadatak ubaciti se u računalo bez korisnikovog pristanka ili ga pak oštetiti. Programi se smatraju zlonamjernim s obzirom na namjeru napadača, tj. što želi postići njime, a ne s obzirom na programske značajke. Zlonamjerni programski kodovi uključuju viruse, crve, trojance, rootkit-ove, spyware te druge zlonamjerne i nepoželjne programe.

U počecima računalnog doba zlonamjerni programi su pisani kao eksperimenti ili šale koje bi smetale korisniku više nego činile ozbiljnu štetu na računalu. Mladi su programeri pisali zlonamjerne programe kako bi vidjeli koliko se daleko dogurati njihov rad. Međutim, sa daljnjim razvojem računalne tehnologije pojavljivalo se sve više i više ovakvih primjera. Od pojavljivanja širokopojasnog Interneta (eng. *broadband Internet*) cilj napadača je postao profit, nezakonito oglašavanje i kriminal.

7.1. Virusi

Virusi su računalni programi koji mogu sami sebe kopirati i zaraziti korisnikovo računalo bez njegova znanja. Širenje virusa je moguće putem Interneta, mrežne strukture ili preko prijenosnih medija. Jednom kada računalo biva zaraženo virusom, isti se može kopirati i izmijeniti samog sebe kako bi ga se teže otkrilo. Najčešće se ubacuju u pokretačke datoteke programa (eng. *executables*) i pri pokretanju zaražene datoteke šire se na druge.

Da bi se virus umnožio, mora moći pokrenuti svoj kod i pisati u radnu memoriju. Iz ovog razloga se virusi ubacuju u pokretačke datoteke. Ukoliko korisnik pokrene zaraženi program, virus se učitava u memoriju. Viruse se dijele u dvije skupine, na temelju ponašanja i na temelju trenutka kada se učitavaju u memoriju.

7.1.1. Virusi koji nisu smješteni u radnoj memoriji

Viruse koji nisu smješteni u radnoj memoriji (eng. *Non-Resident viruses*) je mnogo teže za pronaći jer jednom kada zaražena datoteka biva pokrenuta, traže nove žrtve i ubacuju svoj kod. Sastoje se od dva modula, modula za traženje i modula za umnožavanje. Modul za traženje pri pokretanju zaražene datoteke traži nove pokretačke datoteke koje bi mogao zaraziti. Kada nađe takav slučaj signalizira modul za umnožavanje koji potom ubacuje zlonamjeran kod virusa u datoteku.

7.1.2. Virusi smješteni u radnoj memoriji

Virusi smješteni u radnoj memoriji (eng. *Resident viruses*) imaju modul za umnožavanje sličan nerezidentnima, jedina je razlika da rezidentni (virusi smješteni u radnoj memoriji) nemaju modul za traženje već kada bivaju učitani u radnu memoriju računala zaraze sve moguće pokretačke datoteke. Dijele se još na one koji brzo šire zarazu i one koji sporo šire zarazu. Rezidentne viruse koji brzo šire zarazu je teško ukloniti sa antivirusnim alatom. Oni koji sporo šire zarazu se čak mogu proširiti određenim naredbama koje korisnik upotrebljava, npr. kopiranjem datoteka.

7.1.3. Vektori napada i datoteke nositelji

Virusi su usmjereni na nekoliko vrsta prijenosnih medija i datoteka na računalima:

- binarne pokretačke datoteke (u Windows sustavu - COM, EXE; u Linux sustavu - ELF)
- Boot Recorde disketa i particija tvrdih diskova
- Master Boot Record tvrdog diska
- skripte opće namjene u operativnim sustavima
- razne sigurnosne propuste u operativnom sustavu i programima

7.2. Crvi

Crv (eng. *worm*) je računalni program koji također ima sposobnost umnožavanja samog sebe. Crvi koriste mrežne sustave kako bi se umnožili i zarazili računala. Za razliku od virusa, crvi ne ubacuju svoj programski kod u neki od programa na računalu. Poznato je iz prijašnjih iskustava da mogu izbrisati datoteke sa zaraženog računala, zapakirati podatke napadima ili čak poslati podatke putem e-mail

poruke. Obično sadržavaju dio koda „stražnja vrata“ (eng. *backdoor*) koji omogućuje napadačima da korisnikovu IP adresu koriste za *phishing* ili kako bi prikrili web adresu svoje stranice. Otvaranjem backodoor-a također se omogućuje lakša zaraza drugim vrstama zlonamjernih programa.

Velika su pomoć pri otkrivanju crva antivirusni i antispyware alati, te redovito aktualiziranje operativnog sustava i programa na računalu. Uz ovu pomoć, potrebno je još obratiti pozornost na elektroničku poštu označenu kao *spam*, te web stranice za čiji sadržaj nismo sigurni da je autentičan.

7.3. Trojanski konji (trojanci)

Naziv „Trojanski konj“ ova vrsta programa dobila je po poznatom grčkom osvajanju grada Troje. To su programi za koje se čini da obavljaju poželjne funkcije na računalu, a ustvari obavljaju korisniku neobjavljene zlonamjerne radnje. Obično se sastoje od dva dijela, klijenta i poslužitelja. Poslužitelj se pokreće na računalu žrtve i otvara napadaču mogućnost da načini štetu ili ukrade podatke. Da bi napadač uspio pristupiti računalu žrtve mora poznavati IP adresu istog. Neki trojanci čim zaraze računalo zapisuju IP adresu zaraženog računala i prosljeđuju je napadaču putem e-mail poruke ili nekog drugog oblika komunikacije nakon čega se napadač spaja na zaraženo računalo. Trojanski konji šire se kada ljudi zagrizu tzv. mamac i otvore program, misleći da on dolazi iz povjerljivog izvora.

Novija vrsta ovih zlonamjernih programa ne zahtjeva da se napadač mora spojiti na računalo, već se ono nakon zaraze spaja na napadača.

Postoji šest grupa podijeljenih s obzirom na način proboja u sustav i štete koju prouzrokuju:

1. Trojanci za udaljeni pristup
2. Trojanci za uništavanje podataka
3. Trojanci koji skidaju sadržaj sa Interneta
4. Server trojanci (Proxy, FTP , IRC, E-mail, HTTP/HTTPS, ...)
5. Trojanci koju onesposobe zaštitne programe
6. Trojanci za pokretanje DoS napada

Kako postoji mnogo različitih vrsta trojanaca, nemoguće ih se riješiti jednom metodom. Velika pomoć pri rješavanju ovog problema su antivirusni i antispyware alati. Moguće ih je također odstraniti čišćenjem privremenih Internet datoteka (eng. *Temporary Internet* files) i ručnim brisanjem.

7.4. Rootkitovi

Rootkit je program ili skup programa čija je svrha omogućiti napadaču da preuzme kontrolu nad zaraženim računalom. Vrlo ih je teško otkriti jer izbjegavaju sigurnosne zamke operativnih sustava. Često preoblikuju dijelove operativnih sustava, instaliraju se kao upravljački programi ili kao moduli jezgre sustava i najčešće se ne šire poput virusa.

Napadaču je na zaraženom računalu omogućen pristup svemu, tako da ova vrsta zlonamjernih programa predstavlja vrlo veliku opasnost. Moguće ih je otkriti jer, kao što je prije napomenuto, preoblikuju dijelove operativnih sustava, pa ih antivirusni alati koji koriste heurističke module vrlo lako otkrivaju.

8. Razine zlouporabe ovlasti

Kao što je prije izloženo, napadaču je na raspolaganju velik broj načina i alata kojima može ugroziti računala, mrežne sustave, pa čak i web stranice. Upotrebom bilo kojeg od njih može naštetiti korisniku čije je računalo napadnuto.

Kada je u pitanju osobno računalo korisnika, koji ujedno ima i ovlasti administratora računala, napadač će se poslužiti jednom od navedenih metoda kako bi upio provaliti u računalo i time steći ovlasti na istom. Zaštićeni podaci postaju dostupni napadaču i time se otvara mogućnost krađe identiteta, stvaranja financijske štete korisniku, preuzimanja i uništavanja povjerljivih i osobnih podataka, onesposobljavanja računala za normalan rad ili preuzimanje potpune kontrole nad računalom. Kod mrežnih sustava napadač podiže razinu ovlasti koristeći se propustima kako bi došao do razine administratora. Većina napadača ne uspijeva odmah dobiti ovlasti administratora mrežnog sustava, pa je potrebno koristiti više sigurnosnih propusta u programima ili operativnom sustavu. Korištenjem svakog propusta, ovlasti napadača eskaliraju. Usprkos zaštitama poznati su primjeri gdje je napadač dobio sve ovlasti i time kompromitirao sigurnost korisnika i povjerljivih podataka. Ukoliko se napad ne uoči pravovremeno, kompletan mrežni sustav biva ugrožen. Napadač može pokretati proizvoljne programske kodove i napade sa preuzete računalne opreme.

9. Zaključak

Uslijed velikog broja načina provale u osobna i poslovna računala koja sadrže podatke potrebno je osigurati sustave primjerenom zaštitom s obzirom na funkciju koju obavljaju. Kao što je ranije navedeno, gotovo svaki programski paket u sebi ima barem jedan sigurnosni propust, no to je i više nego dovoljno napadaču da se okoristi.

Honeypot sustavi omogućuju primjerenu zaštitu u računalnom svijetu. Svakim danom razvija se sve više sredstava kojima bi se moglo korisniku ukrasti vrijedne podatke ili na neki način nanijeti štetu. Ne treba zaboraviti da također omogućuju praćenje postupaka napadača i u nekim slučajevima hvatanje napadača. Honeypot sustavi su neka vrsta garancije da će novi i stari sigurnosni propusti za koje bude uočeno da napadači koriste, biti uklonjeni.

Općenito, honeypot sustavi korisnicima osobnih računala nisu potrebni jer će usporiti rad njihova računala. Mjere opreza i zaštite koje bi korisnici osobnih računala trebali koristiti su programska rješenja poput antivirusnih i antispyware programa,te vatrozida. Redovitim aktualiziranjem operativnog sustava i programa koji se nalaze na računalu pridonijeti će zaštiti svojih podataka.

Ova vrsta zaštite primjerenija je velikim mrežnim sustavima kakve koriste tvrtke i institucije. Kako bi zaštitili podatke i korisnike unutar mrežnog sustava administratori sustava postavljaju *e-mail* i *spam*, *mwcollect* sustave. U institucijama koje pohranjuju velike količine podataka na svojim računalima najčešće su postavljeni *honeynet* sustavi u koje je zbog njihove složenosti vrlo teško „provaliti“.

Razvoj honeypot sustava je nužan jer računala postaju baza osobnih i povjerljivih podataka. Napadači stalno pronalaze nove načine kako bi otuđili podatke, pa će se i honeypot sustavi morati razvijati ukorak sa metodama napadača. Upravo honeypot sustavi omogućuju zajednici da prate postupke napadača, tako da proizvođači programskih paketa mogu pravovremeno reagirati na nađene sigurnosne propuste.

10. Reference

[1] Napad zavaravanjem, http://en.wikipedia.org/wiki/Spoofing_attack, svibanj 2007.

[2] Krađa identiteta, http://hr.wikipedia.org/wiki/Krađa_identiteta, kolovoz 2006.

[3] Statistički podaci o krađama identiteta, http://www.idtheftcenter.org/artman2/publish/lib_survey/ITRC_2008_Breach_List.shtml, rujan 2008.

[4] Zlouporaba ranjivosti računalnih sustava, http://os2.zemris.fer.hr/ns/malware/2007_zelanto/, rujan 2008.

[5] Hakeri, http://hackersrule.blog.hr/, srpanj 2006.

[6] Hakeri, http://en.wikipedia.org/wiki/Hacker_(computer_security), kolovoz 2008.

[7] Sprječavanje napada, http://www.hellboundhackers.org/articles/819-preventing-the-hack-part-1.html, svibanj 2008.

[8] Internet protokol, http://en.wikipedia.org/wiki/OSI_model, kolovoz 2008.

[9] Keystroke logging napad, http://en.wikipedia.org/wiki/Keylogging, travanj 2008.

[10] Zlonamjerni programski kodovi, http://en.wikipedia.org/wiki/Malware, lipanj 2008.

[11] Honeypot sustavi, http://en.wikipedia.org/wiki/Honeypot_(computing), prosinac 2007.

[12] Što su honeypot sustavi, http://www.webopedia.com/TERM/H/honeypot.html, rujan 2008.

[13] Honeypot sustavi, http://www.tracking-hackers.com/papers/honeypots.html, svibanj 2003.

[14] Alati za otkrivanje honeypot sustava, http://www.ecs.csun.edu/~btimmer/COMP595SEC/antihoneypot.htm, rujan 2008.

[15] Korištenje honeypota, http://l0t3k.org/security/docs/honeypotting/en/, 2004. - 2007.

[16] Roger A. Grimes: „Honeypots for Windows“, Apress 2005.

[17] Preuzimanje honeyd sustava, http://www.netvigilance.com/, 2008.

[18] Honeyd skipte, http://www.honeyd.org/contrib.php, listopad 2004.

[19] Snort, http://www.snort.org/, 2008.

[20] Tripwire, http://www.tripwiresecurity.com/, 2008.

[21] Windiff, http://www.grigsoft.com/download-windiff.htm, 1996. - 2006.

[22] Netmon, http://www.netmon.ca, 2008.

[23] TCPView, http://technet.microsoft.com/en-us/sysinternals/bb897437.aspx, 2008.

[24] Honeyd sustav za Linux, http://www.honeyd.org/release.php, svibanj 2007.