PRIMENA *HONEYPOT* ARHITEKTURE U ANALIZI RANJIVOSTI INFORMACIONIH SISTEMA

Džigurski Ozren
Univerzitet u Beogradu, Fakultet bezbednosti
odzigurski@gmail.com

Abstrakt

U radu su prikazani različiti aspekti primene koncepta *honeypot* sistema u cilju zaštite informacionih sistema od nelegalnih pristupa i zlonamernih aktivnosti napadača. Postavljanjem kompjuterske zamke – *honeypot*-a, nakon upada napadača u zamku, moguće je otkriti zlonamerne podatke i aktivnosti napadača. Osim za pasivnu detekciju aktivnosti napadača i prikupljanja informacija, u novijim istraživanjima razmatraju se i mogućnosti primene *honeypot* sistema za aktivno delovanje na samog napadača u cilju onemogućavanja njegovog delovanja, kao i primena *honeypot* sistema u kompjuterskoj forenzici. Iz tog razloga i sami napadači razvijaju alate za detekciju postojanja *honeypot* sistema. Poseban problem u primeni *honeypot* sistema predstavlja problem legalnosti i etike upotrebe *honeypot* sistema s obzirom da princip primene zamke, u pravnoj nauci i kriminalistici nije opšte prihvaćen i opravdan.

***Ključne reči**: honeypot, honeypot arhitektura, anti-honeypot, kompjuterska forenzika, kompjuterska etika.*

APPLICATION OF THE *HONEYPOT* ARCHITECTURE IN VULNERABILITY ANALYSIS OF INFORMATION SYSTEMS

Džigurski Ozren
Universityof Belgrade, Faculty of Security Studies
odzigurski@gmail.com

Abstract

This paper presents various aspects of the concept of *honeypot* systems to protect information systems from illegal access and malicious activity attacker. Placing the computer traps - *honeypot*, after an intrusion into the trap, it is possible to detect malicious data and attacker activities. Except for the passive detection of activity and an information gathering, in recent studies are discussed possibilities of *honeypot* systems for active participation in order to prevent its action and the use of *honeypot* systems in computer forensics. For this reason and attackers are developing tools for the detection of the existence of *honeypot* systems. A special problem in the application of *honeypot* system is the legality and ethics of the its use, since the application of the principle of traps in jurisprudence and criminology is generally not well accepted and legitimate.

***Keywords**: honeypot, honeypot architecture, anti-honeypot, computer forensics, computer ethics.*

UVOD

Jedan od osnovnih bezbednosnih ciljeva u svakoj poslovnoj instituciji je da se smanji ili eliminiše rizik u kritičnim resursima organizacije. U idealnom slučaju, najbolje što se može uraditi je da se sprečavaju napadi, ali jedan od ključnih slogana o bezbednosti informacija je: "Prevencija je idealna, ali detekcija je obaveza". Mora se shvatiti da će ključni resursi organizacije sigurno biti napadnuti i da je zbog toga neophodno da se napadi na njih otkriju što

ranije moguće u njihovim ciklusima izvršavanja i tu mogućnost efikasno iskoristiti kada se napad pojavi. Jedan od načina da se to uradi je primena *honey-x* tehnologije, odnosno *honeypot* principa.

Generalno, *honeypot* je poseban resurs informacionog sistema čija pogodnost je u tome što omogućava otkrivanje neovlašćene ili nezakonite upotrebe tog resursa. U stvari, njegova vrednost je u njegovom zloupotrebljavanju.

Ovaj resurs informacionog sistema može da bude, [1]:

- namenski server,
- simulirani sistem,
- servis na izabranom serveru, kao što je jednostavan *honeypot* koji se koristi samo za praćenje portova koji nisu u legitimnoj upotrebi,
- virtuelni server, kao što su originalni *honeypot*-ovi ili njihove mreže *honeynet*, *honeyfarm*,
- određeni fajl sa posebnim *honeypot* atributima koji se uobičajeno naziva *honeytoken*.

Vrednost *honeypot* sistema potiče zbog ne postojanja bilo kakve ovlašćene aktivnosti na tom resursu. *Noneypot* resurs nikada nije namenjen za legitimnu upotrebu i zbog toga, svako korišćenje ovog resursa je nelegitimno i akcidentalno, ili neprijateljski po svojoj prirodi. U tom slučaju, moguće je koristiti *honeypot* za bolje razumevanje šta se dešava prilikom napada na kritične korporativne resurse.

Na tipičan veb server mogu se izvršiti izuzetno mnogo napada svakodnevno. Pokušaj da se identifikuju razlike između legitimnih pristupa i napadača je često nemoguće. Ovo je često slučaj, osim ako postoji jednostavan način da se prepozna tip saobraćaja napada, kao što je mogućnost korišćenja *honeypot* principa u te svrhe. U tom slučaju, *honeypot* je bezbedan kao i veb server i instalira se na istom segmentu mreže. U slučaju napada on se vrši istovremeno i na *honeypot* i na legitimni veb server. S obzirom da *honeypot* nema legitimnu upotrebu moguće je da se brzo identifikuje saobraćaj napada i da se iskoriste te informacije da bi se izgradila bolja zaštita ostatka sistema.

1. TIPOVI *HONEYPOT* SISTEMA

Honeypot sistemi mogu da se klasifikuju na osnovu njihove primene i na osnovu načina realizacije, [1]. Na osnovu oblasti primene, *honeypot* sistemi se mogu klasifikovati kao:

- Korporativni,
- Istraživački.

Korporativni *honeypot* sistemi su jednostavni za korišćenje, hvataju samo ograničene vrste informacija, i koriste se prvenstveno u okviru organizacija ili korporacija. Ovi sistemi se implementiraju unutar korporativne mreže sa drugim serverima organizacije i koriste se u cilju da poboljšaju opšte stanje bezbednosti mreže. Pored toga, ovi sistemi su *niske interakcije* tako da se lako implementiraju i zbog toga oni daju manje informacija o napadima ili napadačima nego istraživački sistemi.

Istraživački *honeypot* sistemi imaju za cilj prikupljanje informacija o motivima i taktikama napadača čije mete su različite kompjuterske mreže. Ovi sistemi direktno ne daju korisne

informacije za određenu organizaciju; umesto toga, oni se koriste za istraživanje pretnji kojima se organizacije suočavaju, kao i da ih nauče kako da se bolje zaštite od tih pretnji. Istraživački *honeypot* sistemi su složeni za primenu i održavanje, vrše prikupljanje širokog spektra informacija, a koriste se prvenstveno u cilju istraživanja kod bezbednosnih i vladinih organizacija.

Na osnovu kriterijuma za projektovanje, *honeypot* se može klasifikovati kao:

- jednostavan *honeypot*,
- *honeypot* niske interakcije,
- *honeypot* visoke interakcije.

Jednostavan *honeypot* se u glavnom primenjuje u korporativnim sistemima. Aktivnosti napadača se prate samo pomoću posebnog pristupa koji je instaliran kao *honeypot* link na mreži. Nijedan drugi softver na ovom linku ne treba da bude instaliran. Iako je upotreba jednostavnog *honeypot* korisna, skrivenost odbrambenih mehanizama, za praćenje napadača može se obezbediti i sa drugim boljim kontrolnim mehanizmima.

Honeypot niske interakcije simulira samo servise najčešće aktivirane od strane napadača. S obzirom da oni zahtevaju relativno malo resursa, višestruke virtuelne mašine mogu lako da budu instalirane na jednom fizičkom sistemu. Ovi virtuelni sistemi imaju kratko vreme odziva i potreban je manji programski kod, čime se smanjuju kompleksni zahtevi za bezbednost ovih sistema. (Primer *Honeyd*).

Honeypot visoke interakcije imitira aktivnosti realnih sistema koji izvršavaju razne servise i, stoga, napadačima može biti dozvoljeno izvršavanje mnogo različitih servisa, tako da napadači troše značajno vreme pri tome. Prema novim istraživanjima tehnologije *honeypot* visoke interakcije, upotrebom virtuelnih mašina, višestruki *honeypot* može biti instalirani na jednoj fizičkoj mašini. Zbog toga, čak i ako je *honeypot* kompromitovan, on može da se obnovi mnogo brže. U principu, *honeypot* visoke interakcije može da obezbediti više mogućnosti, time što je teško da se on otkrije, ali su oni veoma složeni za održavanje. Ako virtuelne mašine nisu na raspolaganju po jedan *honeypot* se mora instalirati za svaki fizički računar, što može biti dosta složeno i skupo. (Primer *Honeynet*).

Distribuirani *honeypot* sistemi predstavljaju nove tehnologije u oblasti arhitekture ovih sistema. *Honeynets* i *Honeyfarms* pripadaju klasi distribuiranih sistema koji se koriste za monitoring velikog skupa IP adresa kako bi *honeypot* sistemi bili što efikasniji.

Honeynets i *Honeyfarms* su imena dati grupama *honeypot*-ova, pri čemu su *Honeyfarms* više centralizovani. Grupisanje *honeypot*-ova omogućavaju mnoge aktivnosti koje pomažu da se ublaže neki od nedostataka tradicionalnih *honeypot*-ova. Na primer, obični *honeypot* često ograničava dolazni saobraćaj kako bi se izbegli napadi na ne-*honeypot* nodove. Međutim, ovo ograničenje omogućava da *honeypot* bude identifikovan od strane napadača. *Honeyfarm* se može koristiti kao čvor za preusmeravanje dolaznog saobraćaja za svaki pojedinačni *honeypot*. Ovi čvorovi preusmeravanja se takođe se ponašaju kao moguće žrtve napada.

Dve ili više *honeypot*-a na mreži formiraju *honeynet*. *Honeynet* je mreža *honeypot*-ova visoke interakcije koji simuliraju korporativnu mrežu i koja je konfigurisana tako da se sve aktivnosti prate, beleže i koja je u izvesnoj meri, diskretno upravljana. Tipično, *honeynet* se koristi za praćenje veće ili složenije mreže u kojime jedan *honeynet* ne može biti dovoljan. *Honeynet* i

honeypot-ovi se obično realizuju kao deo većih sistema za detekciju upada na mrežu, pri čemu je *Honeyfarm* centralizovani skup *honeypot*-ova i alata za analizu napada.

U oblasti informatičke bezbednosti, *honeytoken* je *honeypot* koji nije računarski sistem. Njihova vrednost ne leži u njihovoj upotrebi, nego u njihovoj zloupotrebi. *Honeytoken* može postojati u različitim oblicima, kao što je neaktivni ili lažni nalog za unos u baze podataka koji će biti selektovan samo od strane zlonamernih upita, čineći da je taj koncept pogodan za obezbeđivanje integriteta podataka, pri čemu je svaka upotreba ovih naloga sumnjiva, ali ne nužno i zlonamerna. U principu, oni ne moraju da sprečavaju bilo kakvu manipulaciju sa podacima, ali umesto toga oni mogu da daju administratoru uvid u neophodne dalje mere za postizanje integriteta podataka. Primer za *honeytoken* može biti i lažna *email* adresa koja se koristi za praćenje nelegalnih aktivnosti, kao što su na primer pokušaji da se *mailing* lista ukrade.

HoneyMonkey je istraživački *honeypot* firme Microsoft. Ova implementacija koristi mrežu računara u potrazi za sajtovima koji koriste internet pretraživače za instaliranje zlonamernog softvera na istom HoneyMonkey računaru. HoneyMonkey se zasniva na konceptu *honeypot*, sa tom razlikom što aktivno traži sajtove koji pokušavaju da ga eksploatišu. Projekat je zasnovao Microsoft 2005 godine. Sa *HoneyMonkey* moguće je naći bezbednosne propuste koji još nisu javno poznati, ali koje napadači iskorišćavaju.

2. ISTORIJA KONCEPTA *HONEYPOT*

Prvi radovi u kojima je prikazan *honeypot* koncept su bili radovi *The Cuckoo's Egg*, autor Clifford Stoll i *An Evening With Berferd*, autor Bill Cheswick, koji su objavljeni 1990 i 1991 godine, [2]. Prvi javno dostupan *honeypot* je bio u okviru projekta Deception ToolKit (DTK), autora Freda Koena, 1998 godine, [3]. U okviru ovog projekta realizovan je *honeypot* koji je imao za cilj da privuče napadače na način, kao da sistem DTK sadrži veliki broj široko poznatih ranjivosti. Posle toga, više *honeypot* sistema su postali javno i komercijalno dostupni tokom kasnih devedesetih godina dvadesetog veka.

Koncept *honeynet* se pojavio 1999 godine u okviru projekta: Honeynet Project.

Kako su kompjuterski crvi počeli masovno da se šire početkom 2000, pokazalo se da su *honeypot* sistemi postali imperativ u hvatanju i analiziranju crva.

Pojam *honeytoken* se prvi put pojavio 2003 godine.

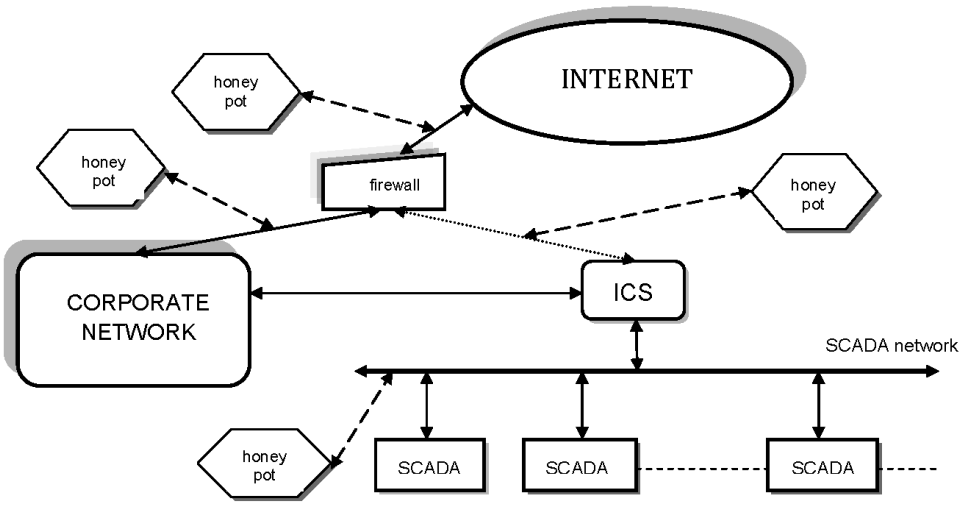
Godine 2004, prvi put su uvedeni virtuelni *honeypot* sistemi koji su omogućavali da više *honeypot* rade na jednom serveru. Hibridna arhitektura *honeypot* sistema koja objedinjuje *honeypot* niske interakcije i *honeypot* visoke interakcije uvedena je 2008 godine.

3. ARHITEKTURE *HONEYPOT* SISTEMA

Za analizu ranjivosti korporativnih informacionih sistema, u okviru metodologije sistema za detekciju napada (IDS), danas se široko primenjuje i princip informatičke zamke – *honeypot*, za detektovanje napada na sistem. Ovaj princip je naročito pogodan za primenu u okviru industrijskih i procesnih (ICS/SCADA) sistema [4].

Kao što je napomenuto, u računarskoj terminologiji *honeypot* je zamka za otkrivanje, odvraćanje, ili na neki način suprotstavljanje pokušajima neovlašćenog korišćenja resursa informacionih

sistema. Generalno, *honeypot* sitem se sastoji od računara, podataka i mreža koji izgledaju kao da su deo osnovne mreže, ali u stvari prestavljaju njihovu imitaciju i izolovano se prate, a koji pored toga izgledaju kao da sadrže podatke ili resurse od važnosti za napadače. *Honeypot* funkcioniše slično kao sistemi za detekciju napada (IDS), koji se obično implementiraju na svakoj instanci informacionog sistema, ali se u ovom slučaju koriste virtuelne a ne stvarne adrese, slika 1, [5]. *Honeypot* arhitektura je realizovana tako da u potpunosti imitira rad realnih komponenti sistema i koristi se za prikupljanje podataka o tome ko, kada i u koju svrhu napada realne sisteme.



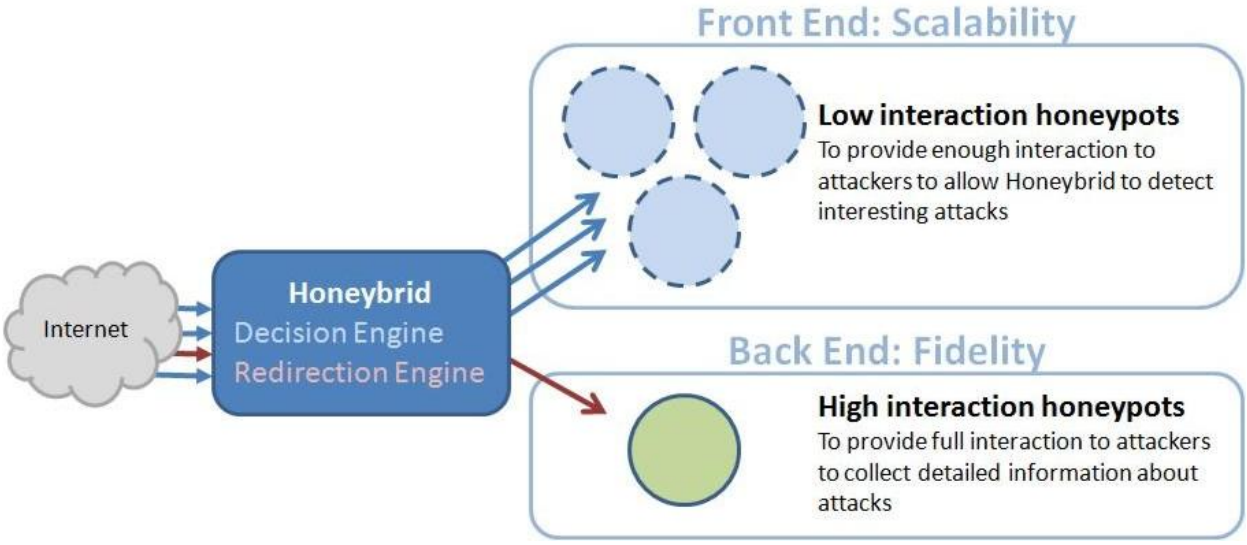
Slika 1. Generalna arhitektura honeypot sistema.

Hibridna honeypot arhitektura

Nove mogućnosti istraživanja i primene u oblasti *honeypot* sistema predstavljaju hibridne *honeypot* strukture, [6]. Kao što je pomenuto, *honeypot*-ovi niske interakcije nisu tako moćni, ali su mnogo bezbedniji i lakše se realizuju u odnosu na *honeypot* visoke interakcije. Pored toga, *honeypot* visoke interakcije su previše skupi, oni rade sa stvarnim servisima i iz tog razloga predstavljaju veći bezbednosni rizik. Kombinujući prednosti oba *honeypot*-a, može se koristiti *honeypot* niske interakcije kao server koji filtrira i preusmerava dolazni saobraćaj na *honeypot* visoke interakcije. Ova vrsta *honeypot* kombinacije naziva se hibridni *honeypot.* Osnovni cilj upotrebe hibridnih *honeypot*-ova je da se iskoristi skalabilnost *honeypot*-ova niske interakcije i mogućnosti kvalitetnog procesiranja *honeypot*-ova visoke interakcije, i to u cilju prikupljanja detaljnih napadačkih aktivnosti u velikim korporativnim mrežama, za potrebe da se oni uspešno analiziraju i da se procene mogućnosti za eventualnee nove napade.

U hibridnim *honeypot* sistemima, *honeypot* niske interakcije ima ulogu pristupne kapije (gateway) za *honeypot* visoke interakcije. *Honeypot* niske interakcije filtrira masovni dolazni saobraćaj i obezbeđuje prosleđivanje samo odabranih konekcija napadača ka *honeypot*-u visoke interakcije. U tom procesiranju hibridni *honeypot* se oslanja na dva modula. Jedan modul se koristi za izbor potencijalnih napadačkih aktivnosti i napadača, (Decision Engine), a drugi vrši preusmeravanje izabranih napadačkih aktivnosti na dalju obradu u *honeypot* visoke interakcije, (Redirection Engine), slika 2. Kombinovanjem ovih tehnika i komponenti, hibridni *honeypot* sistemi obezbeđuju efikasan metod za filtriranje napada u cilju fokusiranja samo na specifične

napadačke aktivnosti i tako se smanjuje vreme analize i ubrzava reagovanje na napade. Hibridni *honeypot* sistemi nalaze primenu u velikim korporativnim mrežama koje sadrže više stotina ili više hiljada računarskih komponenti.



Slika 2. Arhitektura hibridnih *honeypot* sistema.

4. IMPLEMENTACIJA *HONEYPOT* SISTEMA

Na osnovu implementacije *honeypot* sistema, oni mogu biti kategorizovani na sledeći način, [7],tabela 1:

***Honeypot* niske interakcije.**

Tipičan *honeypot* niske interakcije ima nekoliko otvorenih portova, tako da administrator zna na koje portove napadači pokušavaju da pristupe. Napadaču neće biti dozvoljeno da radi još nešto drugo osim toga. Dakle, *honeypot* niske interakcije je relativno manje rizičan. Iz tog razloga, *honeypot* niske interakcije ne daje više uvida u namere napadača, pa, se oni obično koriste kao korporativni *honeypot*-ovi.

***Honeypot* visoke interakcije**

Tipičan *honeypot* visoke interakcije ima nekoliko otvorenih portova, kao i nekoliko aktivnih realnih ali rizičnih servisa. Dakle, napadaču je dozvoljeno da zapravo izvrši upad u *honeypot* i njemu je dozvoljeno dozvoljeno da uradi ono što želi. Iz tog razloga, *honeypot* visoke interakcije se smatra relativno rizičnim. *Honeypot* visoke interakcije zato može da se koristi da se prikupi dosta znanja o alatima, tehnikama i metodama koje koriste napadači, i oni se obično koriste kao istraživački *honeypot*-ovi.

Honeypot klasifikacija	Honeypot kategorija	Primer
Nivo interakcije	Honeypot niske interakcije	Honeyd Specter KFSensor MWCollect
	Honeypot visoke interakcije	Honeynet Sebek Argos
Upotreba Honeypot-a	Istraživački Honeypot	Honeynets
	Korporativni Honeypot	Nepenthes

Tabela 1. Klasifikacija *honeypot*-ova prema načinu implementacije.

U nastavku su prikazani neke tipične realizacije *honeypot* sistema.

Honeyd

Honeyd je najpoznatiji *honeypot* niske interakcije, [8]. *Honeyd* je razvijen na Univerzitetu u Mičigenu i koristi se uglavnom kao korporativni *honeypot*. *Honeyd* je *open source* rešenje i projektovan je za *Unix* sisteme. On može da imitira preko 400 različitih operativnih sistema i hiljade različitih računara, sve u isto vreme. *Honeyd* se prvenstveno koristi za otkrivanje napada. Ona radi tako što prati IP adrese koje su neiskorišćene, koji nemaju dodeljenih sistemskih servisa. Jednom povezan, napadač veruje da je u interakciji sa realnim sistemom. Ne samo da *Honeyd* ima dinamičku interakciju sa napadačima, već može da otkrije i aktivnosti na svakom portu. Ove kombinovane mogućnosti identifikovanja i otkrivanja aktivnosti na svakom portu, daju *Honeyd*-u veliku vrednost kao sredstvo za detekciju neautorizovanih aktivnosti napadača.

Honeynets

Honeynets predstavljaju najviši domet istraživačkih *honeypot*-ova, [9]. Oni su *honeypot*-ovi visoke interakcije, koji imaju velike mogućnosti, ali oni takođe imaju najviši stepen rizika. Njihova glavna vrednost leži u mogućnostima istraživanja i dobijanju informacija o pretnjama koje postoje u internet domenu. *Honeynet* je mreža korporativnih *honeypot* sistema. To daje napadačima mogućnost u kompletan uvid u skup sistema, aplikacija i funkcionalnosti u cilju izvršavanja napada. Iz ovoga se može saznati mnogo, ne samo alate i taktike napadača, već i njihove načine komunikacije, organizacije grupa i motive za napade. Međutim, sa ovim mogućnostima dolazi i mnogo rizika. Moraju se preduzeti različite mere kako bi se osiguralo da, kada je ova mreža kompromitovana, ona ne može da se koristi da napadne druge sisteme. *Honeynet* su pre svega istraživački *honeypot*-ovi . *Honeynet* može da se koristi i kao korporativni *honeypot*, posebno za detekciju ili reagovanje na napade, ali je to dosta složeno.

Nepenthes

Nepenthes su niske ili srednje interakcije *honeypot*-ovi koji emuliraju nekoliko poznatih ranjivosti Microsoft sistema, putem više servisa, u pokušaju da se uhvate aktivni primeri zlonamernih programa, koji ih eksploatišu, [10]. U *Nepenthes* servisima se instaliraju poznate ranjivosti, oponašaju se interakcije sa servisima do faze eksploatacije i zatim se memorišu delovi programa koji izvršavaju zlonamerni sistemi.

Nepenthes kao *honeypot* niske interakcije sa definisanim skupom ranjivosti, mogu biti raspoređeni u korporativnu mrežu i može biti korisno upotrebljen za generisanje upozorenja

sistem administratorugu da se preduzmu neophodne mere za povećanje bezbednosti mreže. *Nepenthes honeypot* može biti i posebeno podešen da prati izvestan broj portova za koje se očekuje da ranjivi moduli dobijaju napade preko kompjuterskih crva.

Bežični *honeypot*

Bežični (*wireless*) *honeypot* je posebna vrsta *honeypot* sistema, koji se koriste da se prate dešavanja u korporativnim sistemima u bežičnom domenu i da se dobiju neke informacije i statistički podaci o mogućim napadima na sistem, [11]. Prime tome najviše se koristi tehnologija po standardu IEEE 802.11, a takođe su moguće i druge tehnologije kao što je *bluetooth*. *Honeyspot* je poznati bežični *Honeypot* projekat podržan od strane španskog *Honeynet* projekta. Termin *Honeyspot* je kombinacija termina *Honeypot* i *Hotspot*. U principu, *Honeyspot* je realizovan za praćenje napadača i njihovih napada na bežične mreže.

Privatni *honeypot*

Još jedna često u upotrebi *honeypot* je privatni (*homemade*) *honeypot*. Ovi *honeypot*-ovi su obično *honeypot*-ovi niske interakcije. Njihova svrha je obično da prati neku specifičnu aktivnost napadača, kao što su kompjuterski crvi ili kao što je skeniranje aktivnosti napadača na sistemu. To se može realizovati kao obični ili kao istraživački *honeypot*, u zavisnosti od njihove namene. S obzirom na realizaciju, nema mnogo mogućnosti za napadača da komunicira sa realnim sistemom, pa je time i rizik za moguću štetu smanjen. Jedan od uobičajenih primera je da se kreira servis koja prati port 80 (http), i da se vrši hvatanje celokupnog saobraćaja do i od porta. To se obično čini kada se prati napad pomoću kompjuterskog crva.

***Honeypot* za institucije malog obima**

Institucije i privredna preduzeća manjeg obima koji koriste kompjuterske mreže u svom poslovanju, moraju da obezbede visok nivo bezbednosti informacija i komponenti svojih mreža. *Honeypot* koji se projektuje za ove male institucije mora sadržavati informacije kompletnog sistema mreže i voditi evidenciju svih log fajlova mreže. Kompletne informacije o aktivnostima napadača moraju da se prikupljaju i memorišu u cilju povećanja bezbednosti sistema. Iz tog razloga, *honeypot* se realizuje tako da olakšava pristup svim zlonamernim korisnicima kako bi se što više prikupilo informacija o njihovim nelegalnim pokušajima. Zaštita kompletnog sistema je primarni cilj, tako da realni sistem ne sme biti kompromitovan, ni u kom slučaju. Zbog ovih strogih zahteva postoji mali broj realizovanih *honeypot*-ova ovog tipa koji ispunjavaju sve ove uslove.

Honeypot WordPress Plugin

Honeypot WordPress Plugin omogućava da se provere IP adrese klijenata koji se priključuju na odgovarajući blog. Honeypot WordPress Plugin omogućava da se brzo proveri da li je posetilac bloga skupljač mailova, komentar spamer ili bilo koji drugi zlonamerni napadač. Komunikacija sa serverom za verifikaciju vrši se putem *DNS-request* mehanizma, što čini upit i odgovor još bržim. Zahvaljujući *Honeypot WordPress Plugin* mnogi potencijalno zlonamerni korisnici odustaju od pokušaja da pristupe blogovima i da ih zloupotrebljavaju.

5. ANTI-*HONEYPOT* TEHNOLOGIJA

Kada su bezbednosne institucije počele da koriste *honeypots* i *honeynets* kao sredstva za informacionu zaštitu, sajber napadači su reagovali stvaranjem alata za detekciju i

onemogućavanje *honeypot*-ova. Stvaranje ove anti-*honeypot* tehnologije znači da su *honeypot*-ovi imali uticaja na aktivnosti i probleme napadača u vezi sa tim, [12].

Ako napadač otkrije *honeypot*, on će se uglavnom truditi da ga izbegne i da ide na neki drugi sistem koji će napadati. Međutim, postoji rizik da bi napadač mogao ugroziti *honeypot* i koristiti ga za napad na druge računare u lokalnoj mreži ili internetu. Napadač takođe može pokušati da ga onesposobi, izbriše podatke, formatira disk, ili da postavi njegovu adresu na hakerskim sajtovima da spreči druge napadače da budu uhvaćeni u zamku. U svakom slučaju, to može da dovede do problema u funkcionisanju *honeypot* sistema.

Većina napadača neće pokušavati da kompromituje *honeypot*, međutim, ako je *honeypot* visokog prioriteta za napad, kao meta, na primer u vojnim komandnim sistemima, a mogući napadač je iz strane države, onesposobljavanje tog *honeypot*-a može biti poželjno. Da bi se ostvarila takva manipulacija, postoji nekolika tehnika i alata koji uobičajeno koriste sajber napadači za snimanje i analiziranje sistema, a koji se mogu koristiti i prilagoditi za ove aktivnosti. Neki od ovih alata mogu da otkriju sumnjive *honeypot* alate, kao što su virtuelne mašine, detektore lozinki ili alate za debagovanje. Pored toga, postoji i dostupan komercijalni softver za *honeypot* detekciju, kao što je *Send-Safe Honeypot Hunter*.

6. AKTIVNI *HONEYPOT* SISTEMI

Problem koji proističe iz pasivne prirode *honeypot*-a, je u tome se on zasniva na sposobnosti da privuče i zadrži pažnju napadača, a koristi se malo da se zaustavi neposrednu opasnost od napada. Poseban problem je u tome što administrator nekada ne može biti dostupan, ili ne može adekvatno da reaguje u vreme napada. U cilju poboljšanja karakteristika i da bi se iskoristile prednosti *honeypot*-ova, moguće je realizovati aktivni *honeypot* sistem, koji bi mogao da izvrši automatizovati odgovor na napad, i to pomoću, [13]:

- kontra špijunaže,
- kontra merama,
- kontra ofanzivom.

Napadači ostavljaju puno informacija na sistem koji napadaju, međutim ove informacije ne mogu da se upotrebe za generisanje aktivnosti prema napadaču, jer bi to bilo neophodno da se ostvari pre nego što je napadač provalio u sistem. Zbog toga je neophodno da se dobije što više informacija o napadaču, za vreme dok on ispituje ciljni sistem. Postoje alati koji ne samo da pasivno prikupljaju podatke o aktivnostima napadača na *honeypot*, već mogu i aktivno da dobijaju informacije o svakom sistemu koji je povezan na njega. Mnogo informacija može da se dobije i dok je napad u toku. *Honeypot* može pokrenuti skeniranje porta napadača i pokušati da, na primer, uhvati *telnet baner* ili *finger* sistema napadača. Informacije koje se stiču pomoću ovih alata omogućavaju identifikaciju napadača i samim tim se poboljšava proces generisanja aktivnosti prema ciljnom napadaču.

Upotreba protivmera generalno omogućava sistem administratorima da izoluju napadnute sisteme i da zaustave napad. Na taj način, aktivni *honeypot*-ovi su u stanju da zaustavljanjem napada dodatno zaštite korporativnu mrežu.

Iako je ideja aktivnog *honeypot*-a veoma privlačna, ovo ne treba smatrati kao krajnje rešenje za bezbednosne probleme. Automatizovani i aktivni *honeypot* sistemi mogu da pomognu u

poboljšanju bezbednosti mreže, ali pravi posao mora ipak da se uradi od strane ljudi, tj. administratora sistema i eksperata.

7. *HONEYPOT* FORENZIKA

Honeypot je veoma efikasan za praćenje informatičkog okruženja, koji omogućava i da se lako prikupljaju i memorišu velike količine zlonamernih aktivnosti i podataka. Međutim, mali broj istraživanja se bave time da se iskoriste ovi bogati izvori informacija, već su radovi uglavnom posvećeni projektovanju i hardverskoj realizaciji honeypot-ova.

Tokom poslednjih godina, predloženo je mnogo različitih upotreba *honeypot*-ova. Neki od njih su predviđeni da troše vreme napadača, drugi da se smanje spam aktivnosti, ili za obmanjivanje napadača, kao i ostali koji se koriste za analiziranje postupaka napada napadača.

Postoji nekoliko načina na koje napadači mogu da ugrožavaju sistem. Oni najčešće koriste razne hakerske alate, skripta, kao i druga specifična sredstva. Poznati su načini kako se analiziraju aktivnosti alata i kako prikupiti podatke od njihovih aktivnosti. Analiziranje upotrebe skripti je takođe važno, pri čemu se mogu dobiti mnogo korisnih informacija. Ovi podaci se zatim uobičajeno koriste za poboljšanje zaštite i povećanje bezbednosti računarskih mreža i sistema.

Neki napadi na *honeypot*-ove su veoma česti i ponavljaju se. Pored toga, takvi napadi generišu veoma veliku količinu podataka. Iz tog razloga, neophodno je razmotriti opštu statistiku ovih podataka, sa dubinskom analizom različitih procesa koji su doveli do njihovog nastanka. Detaljna analiza, uz upotrebu statističkih metoda i forenzičkih softverskih alata, mogu da otkriju neke zakonitosti i skrivene fenomene koji se ne uočavaju direktno u prikupljenoj masi podataka iz *honeypot*-ova.

Honeypot forenzika predstavlja novi i interesantan pristup projektovanju i mogućim upotrebama *honeypot*-ova, ali za sada koliko je poznato, nema još mnogo rezultata u ovoj oblasti, [14]. Do sada prikazani rezultati potvrđuju da dublje i preciznije analize *honeypot* podataka omogućavaju dobro razumevanje zlonamernih aktivnosti napadača i njihovo otkrivanje. Međutim, za sada se *honeypot* forenzika pretežno koristi za proučavanje i razumenje strategije napadača i njihovih alata, ali ne i za njihovo procesuiranje.

8. LEGALNOST I ETIKA UPOTREBE *HONEYPOT* SISTEMA

Opšte je prihvaćeno da je hakerisanje nelegalno i neetički, međutim postavlja se pitanje da li hakeri koji proizvode internet kriminal, treba da budu namamljeni na *honeypot*-ove? Na ovo pitanje se ne može jednostavno odgovoriti, stoga etika i legalnost upotrebe *honeypot*-ova postaje i kontroverzna tema. Argument je da, pošto je nemoralno i nezakonito namamiti nekog na krađu raznih sredstava i stvari, zašto je pravno ili etički opravdano namamiti pojedince u izvršavanje kompjuterskog kriminala, [15]?

Bezbednosni stručnjaci su zaključili da postoje tri glavna pravna problema koji eventualno mogu imati uticaja na vlasnike *honeypot*-ova, naime to su: upotreba zamke, privatnost i odgovornost.

Mnoge države imaju različite zakone koji se odnose na zaštitu informacija. Ovi propisi se odnose na bezbednost podataka, praćenje nelegalnih aktivnosti i prikupljanje zlonamernih podataka. Na neki način ovi propisi bi mogli da definišu kako koristiti *honeypot*-ove u ove svrhe, ali se ne

može na osnovu toga postaviti jasna granica za šta *honeypot* može ili ne može da se koristi. Može se tvrditi da će vlasnici *honeypot*-ova biti pravno sigurni samo dok se *honeypot*-ovi koriste za direktnu zaštitu svoje mreže i da pri tome, nisu javno deklarisani kao kompjuterska zamka. Međutim, teško je naći dokaz protiv nekoga ko štiti svoju mrežu od zloupotrebe, da ne zloupotrebljava dobijene podatke, pri tome. To zavisi u velikoj meri od namere i načina korišćenja informacija koje su prikupljene.

9. PREDNOSTI I NEDOSTACI *HONEYPOT* SISTEMA

Postoji mnogo bezbednosnih rešenja za zaštitu korporativnih i drugih informacionih sistema, koja su dostupna na tržištu. Putem interneta moguće je izabrati najpovoljnije rešenje koje može da zadovolji razne zahteve. Ovde su navedeni neki od razloga zašto bi trebalo izabrati *honeypot* sisteme u te svrhe:

- *Honeypot* može da deluje u svrhu odvraćanja od napada. Znajući da je *honeypot* sistem podešen za snimanje i prijavljivanje svih zlonamernih aktivnosti, to može da učini da aktivnosti napadača postanu bezopasni.
- *Honeypot* je realizovan da prihvata samo zlonamerne aktivnosti. Ovi sistemi nisu predviđeni za legalan pristup, tako da se bilo koji podaci poslati na *honeypot* smatraju kao napad na ceo sistem.
- Na osnovu podataka o napadu na *honeypot*, administratori sistema mogu da saznaju metode napadača i da ih koriste za kontra mere u cilju poboljšanja bezbednosti celokupnog sistema.
- *Honeypot* može da detektuje unutrašnji napad. Mnogi bezbednosni problemi proizilaze kada zaposleni koji su angažovani u okviru organizacije, zloupotrebljavaju sistem.
- S obzirom da *honeypot* snima samo zlonamerni saobraćaj, nema potrebe za ogromnim skladištenje podataka. Svaki računar može da se koristi kao *honeypot* sistem i nema potrebe za uvođenjem nove tehnologije.
- Oni su jednostavni za razumevanje, za konfigurisanje i instaliranje i nemaju realizovane kompleksne algoritme. Nema potrebe za čestim ažuriranjem ili dogradnjama honeypot-a.
- Podaci iz *honeypot*-a mogu se u nekim slučajevima koristiti kao forenzički dokaz. Dokle god je legalno realizovan i nije deklarisan kao kompjuterska zamka, podaci iz *honeypot*-a mogu se eventualno koristiti kao pravni dokaz.

S obzirom da postoji nekoliko bitnih prednosti korišćenja *honeypot*-ova, postoje i neki njihovi nedostaci, kao što su:

- Napadači mogu u slučaju kompromitacije, upotrebiti *honeypot* da kompromituju i druge sisteme u organizaciji i na internetu. Ovo može dovesti do pravnih implikacija za organizacije koje poseduju *honeypot* sisteme.
- Realizacija *honeypot*-a povećava kompleksnost mreže. U zavisnosti od toga kako je realizovan, on može povećati kompleksnost za potrebe bezbednosti i povećati izloženost za napade.
- *Honeypot* se servisira isto kao celokupni sistem u korporaciji, što povećava administriranje u IT sektoru.
- Objavljivanje o postojanju *honeypot*-a ne mora da odvrati napadača, već ga može navesti da se potrudi da namerno kompromituje sistem.

- Aktivnosti *honeypot*-a ostavljaju tragove, što omogućava iskusnim napadačima da razlikuju da li napadaju *honeypot* sistem ili realni sistem.
- U slučaju kompromitacije *honeypot* može da se iskoristi kao tajno oružje, tj. da ga napadač iskoristi da pristupi drugim delovima sistema i da ih ugrozi, što može da izazove velike posledice po ceo sistem.

10. PRIMER UPOTREBE *HONEYPOT* SISTEMA

Za ilustraciju upotrebe *Honeypot* sistema može da posluži primer istraživanja efikasnosti ove arhitkure koji je realizovan na *Amazon EC2 cloud* veb servisu sa tri *honeypot* instance niske interakcije, [16]. Ove instance su imitirale rad realnih SCADA i PLC uređaja u sistemu za kontrolu pritiska vode u vodovodnom sistemu i koristile su se za prikupljanje statističkih podataka o napadima na njih. Pored toga, *honeypot* instance su prikazane kao deo realnog projekta u okviru vodovodnog sistema i optimizirane su za internet pretraživače i lansirane na *Google*, kako bi privukle pažnju i omogućile napadačima da ih lako pronađu.

Posle samo 18 sati od lansiranja na internet, nađeni su prvi znaci napada na jednoj od *honeypot* instanci. Dok su *honeypot* instance nastavljale da prikupljaju statističke podatke o napadima, dobijeni rezultati dobijeni statističkom obradom su se pokazali alarmantnim. Statistika iz ovog izveštaja sadrži podatke za 28 dana sa ukupno 39 napada iz 14 različitih zemalja. Od tih 39 napada, 12 bili su jedinstveni i mogu da se klasifikuju kao "ciljana", dok se 13 napada ponavljaju od nekoliko istih aktera, u periodu od nekoliko dana, i mogu se smatrati kao "ciljana" i/ili "automatizovana". Sve u svemu, Kina je činila većinu napada, sa pokušajima od 35% od ukupnog broja napada, slede SAD sa 19%, i Laos sa 12%. Ostali pokušaji napada, sa procentom manjim od 10, dolazili su iz sledećih zemalja: Velika Britanija, Holandija, Japan, Brazil, Poljska, Vijetnam, Rusija, Palestina, Čile, Hrvatska i Severna Koreja.

ZAKLJUČAK

U radu su prikazani različiti aspekti primene koncepta *honeypot* sistema u cilju zaštite informacionih sistema od nelegalnih pristupa i zlonamernih aktivnosti napadača. Primena *honeypot* sistema, simuliranjem delova realnog sistema, omogućava detekciju i otkrivanje ovih zlonamernih aktivnosti bez direktnog upada napadača u realni informacioni sistem. Na taj način, postavljanjem kompjuterske zamke – *honeypot*-a, nakon upada napadača u zamku, moguće je otkriti zlonamerne podatke i aktivnosti napadača. Pri tome, napadač nije svestan toga da ne napada realni sistem, već samo jedan njegov simulirani deo.

U zavisnosti od načina i kompleksnosti realizacije *honeypot* sistema zavisi opseg i kvalitet dobijenih detektovanih podataka, kao i mogućnost za njihovu upotrebu u svrhu poboljšanja zaštite realnih sistema. S druge strane, što je *honeypot* sistem kompleksniji on time postaje rizičniji po realni sistem, s obzirom da napadač na osnovu upada u *honeypot* može njegovom analizom da prepozna neke karakteristike realnog sistema. Iz tog razloga i sami napadači razvijaju alate za detekciju postojanja *honeypot* sistema.

Osim za pasivnu detekciju aktivnosti napadača i prikupljanja informacija, u novijim istraživanjima razmatraju se mogućnosti primene *honeypot* sistema za aktivno delovanje na samog napadača u cilju onemogućavanja njegovog delovanja. Pored toga, razmatraju se i

mogućnosti naknadne detaljne analize prikupljenih zlonamernih podataka napadača, primenom forenzičkih alata, za primenu u kompjuterskoj forenzici.

Poseban problem u primeni *honeypot* sistema predstavlja problem legalnosti i etike upotrebe *honeypot* sistema s obzirom da princip primene zamke u pravnoj nauci i kriminalistici nije opšte prihvaćen i opravdan. To se naravno odnosi i na kompjutersku zamku – *honeypot.* Iz tog razloga, pravna i etička pitanja primene *honeypot* sitema moraju u budućnosti biti predmet ozbiljnih istraživanja.

LITERATURA

[1] Spitzner L.: *Honeypots: Tracking Hackers*. Boston, MA: Addison-Wesley, 2003.

[2] Stoll, C.: *The cuckoo's egg: tracking a spy through the maze of computer espionage.* New York: Bantan Doubleday Dell Publishing Group Inc. 1990.

[3] Cohen, Fred. *The Deception ToolKit*. The Risks Digest 9 March 1998.

[4] Ronald Krutz: *Securing SCADA Systems*, Wiley Publishing Inc, USA, 2006, page 7-10.

[5] Džigurski O., Mandić G., Milošević M.: *Critical Infrastructure Securuty and Social Networks.*National Critical Infrastructure Protection, Regional Perspective, Belgrade, 2013.

[6] Masood Mansoori, Omar Zakaria, and Abdullah Gani: *Improving Exposure of Intrusion Deception System through Implementation of Hybrid Honeypot*,The International Arab Journal of Information Technology, Vol. 9, No. 5, September 2012.

[7] Peter, E., & Schiller, T.: *A Practical Guide to Honeypots*. www.cs.wustl.edu/~jain/cse571-09/ftp/honey.pdf, 2012.

[8] Provos, Niels: *A Virtual Honeypot Framework*. Proceedings of the 13th USENIX Security Symposium. 2004. 1-14.

[9] The Honeynet Project: *Know Your Enemy: Learning about Security Threats* (2nd ed.). Boston, MA: Addison-Wesley, 2004.

[10] Nepenthes project homepage: http//Nepenthes.sourceforge.net

[11] Siles, R.: *HoneySpot: The Wireless Honeypot*. http://flambers.com/papers/honeywifi.pdf, 2007.

[12] Krawtez N.: *Anti-Honeypot Technology*, IEEE Security and Privacy. Vol 2, Nb 1, p. 76-78, 2004.

[13] Kilgore W.: *Active Honeypot Systems Project.* University of Advancing Technology, Tempe, Arizona, 2005.

[14] F. Pouget, M. Dacier: *Honeypot-based Forensics.* Institut Eurécom France, 2005.

[15] Spitzner, L.: *Honeypots: Are They Illegal?* http://www.symantec.com/connect/articles/honeypots-are-they-illegal, 2010.

[16] Kyle Wilhoit: *Who's Really Attacking Your ICS Equipment*?, Trend Micro Incorporated, Research Paper, 2013.