UDC: 004.7.056.53

ZAŠTITA RAČUNARSKIH MREŽA MINISTARSTVA ODBRANE I VOJSKE SRBIJE PRIMENOM VIRTUELNOG HONEYNETA

Kapetan *Zoran* Bobar, dipl. inž., zoran.bobar@mod.gov.rs,
Uprava za odnose sa javnošću MO

Rezime:

U ovom radu obrađena je zaštita računarskih mreža u Ministarstvu odbrane i Vojsci Srbije primenom virtuelnog honeyneta. Zaštita je obrađena sa aspekta arhitekture računarskih mreža koje imaju pristup internetu. Predloženi koncept primene virtuelnog honeyneta uzima u obzir dostignuća nauke u ovoj oblasti u svetu, ostale primenjene metode i tehnike zaštite, mogućnosti i potrebe korisnika i elemente delova računarskog sistema Ministarstva odbrane i Vojske koji bi mogli biti meta napada sa udaljenih mesta globalne (internet) mreže.

Ključne reči: *zaštita, bezbednost, računarske mreže, honeypot, honeynet.*

SECURITY OF COMPUTER NETWORK OF THE MINISTRY OF DEFENCE AND THE SERBIAN ARMED FORCES USING VIRTUAL HONEYNETS

Summary:

This paper covers the proposed solution for security of computer network in the Ministry of Defence and the Serbian Armed Forces using virtual honeynets. The security is covered from the aspect of the architecture of computer networks with Internet access. The proposed usage of virtual honeynets for protection takes into account the accomplishments of science in this field as well as security methods and techniques, users' needs and opportunities along with the computer network components of the MoD and the SAF that can be targets for attack.

Key words: *protection, security, computer network, honeypot, honeynet.*

Uvod

Proporcionalno sa razvojem informacionih tehnologija i telekomunikacionih sistema raste složenost sistema i široka primena, ali i broj incidenata na javnim mrežama. Napadači vrlo brzo pronalaze propuste u

zaštiti novih sistema, razvijaju sopstvene alate i tehnike kojima se zaobilaze definisane sigurnosne mere. Vreme za reagovanje pri upadu u računarski sistem znatno je skraćeno. Imajući u vidu ove pretnje, pri razvoju novih računarskih mreža studiozno se pristupa projektovanju sistema zaštite. Međutim, i pored svih preduzetih mera, značajan je negativan učinak malicioznih programa koji se svakodnevno pojavljuju – tipa virusa, crva, trojanaca, itd.

Bilo koji napad na sistem karakterišu sledeći elementi [1]:

– metod: veština, znanje, alat i druga sredstva kojima se vrši napad,

– prilika: vreme i raspoloživost sistema za napad i

– motiv: razlog zbog kog neko napada sistem.

Sa stanovišta zaštite računarskih sistema izuzetno je bitno praćenje i poznavanje karaktera napada sa svim njegovim elementima. Mehanizmi za detekciju napada nisu u mogućnosti da preventivno deluju na sve vrste napada. Česti su napadi koji nisu poznati i predstavljaju novinu, te se nameće potreba za pravovremenim otkrivanjem i izučavanjem njihove prirode u fazi dok nisu kompromitovani ciljni sistemi.

Tehnike, metode, sredstva i motivi svakodnevno poprimaju nove nepoznate dimenzije. Da bi se prikupili podaci i izučila priroda napada koji sigurno predstoje, primenjuju se različite tehnike. Relativno nova, ali svakim danom sve popularnija tehnika, namenjena prvenstveno svim vrstama napadača, jeste i honeypot.

Honeypot obuhvata sve računarske resurse (hardverski, aplikativni i mrežni) koji služe kao mamac, a predviđeni su da budu napadnuti ili kompromitovani od neovlašćenih korisnika. Načini implementacije i primena honeypota je raznolika, što ovaj sistem zaštite čini fleksibilnim i primenjivim u različitim područjima zaštite računarskih sistema.

Zaštita računarskih sistema je trajni proces celokupnog životnog ciklusa sistema, koja treba da obezbedi:

– *prevenciju* (prevention) – postupak preduzetih radnji pri projektovanju računarskih sistema na preventivnom delovanju zaštite računarskih resursa,

– *detekciju* (detection) – postupak praćenja saobraćaja i uočavanja sigurnosnih propusta u procesu prevencije, obaveštavanje o neovlašćenim pristupima i mogućim napadima na računarski sistem, i

– *reakciju* (reaction) – način na koji organizacija reaguje na detekciju neovlašćenog pristupa.

Honeypot se može svrstati u sve tri faze zaštite (što zavisi od tipa). Mogućnost detekcije neovlašćenih aktivnosti, te prikupljanje novih spoznaja o tehnikama i alatima koje napadači koriste, a koji se kasnije koriste za razvoj novih sigurnosnih rešenja, karakteristike su koje to potvrđuju.

Pojam, definicija i arhitektura

Prvi korak u razumevanju honeypota je njegova definicija. Za razliku od firewolla i mehanizma za prevenciju napada (IPS – Intrusion Prevention System), honeypot ne može da spreči maliciozne aktivnosti u sistemu. Njegova svrha je, prvenstveno, da te aktivnosti registruje. Ovaj resurs može da registruje bilo koji nekriptovani napad u mrežama, što ga čini fleksibilnim, pa time i popularnim i sve češće primenjivanim.

Definicija da je „honeypot resurs informacionih sistema namenjen neovlašćenim korisnicima“ [2] ukazuje na mogućnost njegove široke primene u svim tipovima distribuiranih informacionih sistema sa velikim mogućnostima detekcije. Postavlja se pitanje same prirode honeypota kao arhitekture koja beleži samo neautorizovane aktivnosti i na sebi ne sme imati korisne resurse za sam informacioni sistem na koji je postavljen.

Teoretski, honeypot ne bi trebao da vidi saobraćaj u mreži, jer on nema legitimne aktivnosti. Svaka interakcija produkcionih uređaja sa honeypotom je nelegitimna aktivnost i tako se i registruje u njemu. Zamisao je da je potrebno obmanjivati napadača da radi na legitimnom sistemu iako je on na honeypotu koji samo simulira rad pravog. Tako napadač troši dragoceno vreme i resurse, dok će honeypot pratiti i snimati sve njegove aktivnosti. Tako honeypot prikuplja dovoljno informacija o napadaču, a da, u stvari, ne raspolaže legitimnim podacima kompanije.

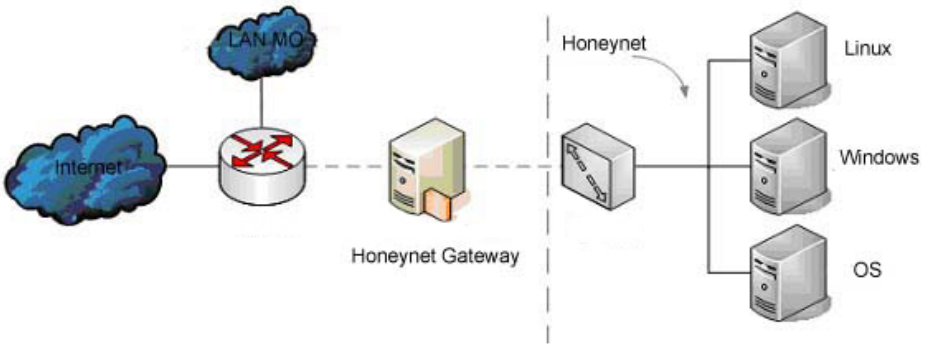
Složenija rešenja honeypota, koja simuliraju čitave mreže sa svim komponentama klasičnih računarskih mreža (server, firewall, switch, mehanizmi za detekciju i prevenciju napada i dr.) nazivaju se honeynetom i prvenstveno su primenjeni u svrhu istraživanja, tj. prikupljanja informacija o napadaču. Honeynet nije proizvod, ne instalira se nikakav softver, to je arhitektura koja se sastoji od niza honeypotova. Ova arhitektura treba da bude dobro kontrolisana kako bi se moglo pratiti šta se dešava u mreži. Ovakva arhitektura postavlja se u ciljni sistem.

Za uspešno postavljanje arhitekture honeyneta ključna su tri zahteva:

– kontrola podataka (data control), koja definiše koje aktivnosti se kontrolišu honeynetom, kako bi se minimizirao rizik;

– snimanje podataka (data capture) koji su usmereni ka honeynet aktivnosti napadača;

– zbirka podataka (data collection). Ovaj zahtev karakterističan je samo za organizacije koje imaju više honeynet platformi u distribuiranom okruženju, kao što je *Honeynet istraživačko udruženje*. Ove organizacije sve snimljene podatke prikupljaju na jedno mesto, kako bi se ukrstili i poredili.



Slika 1 – Honeynet druge generacije [3]

U prvoj generaciji honeyneta firewall je postavljen na trećem nivou gde se lako detektuje. Ovaj problem je rešen postavljanjem gatewaya sa dva uređaja koji se teško detektuje. Firewall radi u bridge modu i kontroliše sve konekcije spolja i iznutra nalik prvoj generaciji honeyneta. Prednosti gatewaya u drugoj generaciji je ugradnja IPS-a, koji omogućava iste funkcije kao i mehanizam za detekciju napada (IDS – Intrusion Decetion System), ali za razliku od IDS-a ima sposobnost da blokira i modifikuje napade [4]. Ova osobina pomaže u razdvajanju legitimnih i malicioznih aktivnosti. Ukoliko napadač pokuša da napadne mrežne resurse van honeypota IPS će takav pokušaj blokirati ili modifikovati. On registruje poznate napade, a nepoznati napadi prolaze. Ova generacija honeyneta je teža za detekciju s obzirom na to da realnije simulira računarske mreže.

Virtuelni honeynet sve funkcionalnosti honeyneta izvršava na jednom računaru. Razvijen je softver koji kreira više virtuelnih mašina i radi na različitim operativnim sistemima. Ova tehnologija je dobra ukoliko su ograničeni resursi. Takođe, virtuelni honeynet je lakše održavati u poređenju sa klasičnim, jer se sve izvršava na jednom računaru. Virtuelni honeynet ima nekoliko ograničenja u pogledu tipa arhitekture i operativnog sistema koji se može korisititi, što je uslovljeno konkretnim rešenjem [5].

Analiza realnog sistema

Ministarstvo odbrane i Vojska Srbije imaju razvijene informacione sisteme usklađene sa organizacionom strukturom. Pojedini delovi sistema funkcionišu zasebno u organizacijskim celinama kao lokalne računarske mreže. Uprava za telekomunikacije i informatiku je nadležna za razvoj, opremanje i projektovanje računarskih mreža u Vojsci i Ministarstvu [6].

U skladu sa materijalnim mogućnostima i raspoloživim sredstvima vrši se integracija računarskih mreža radi realizacije jedinstvenog infor-

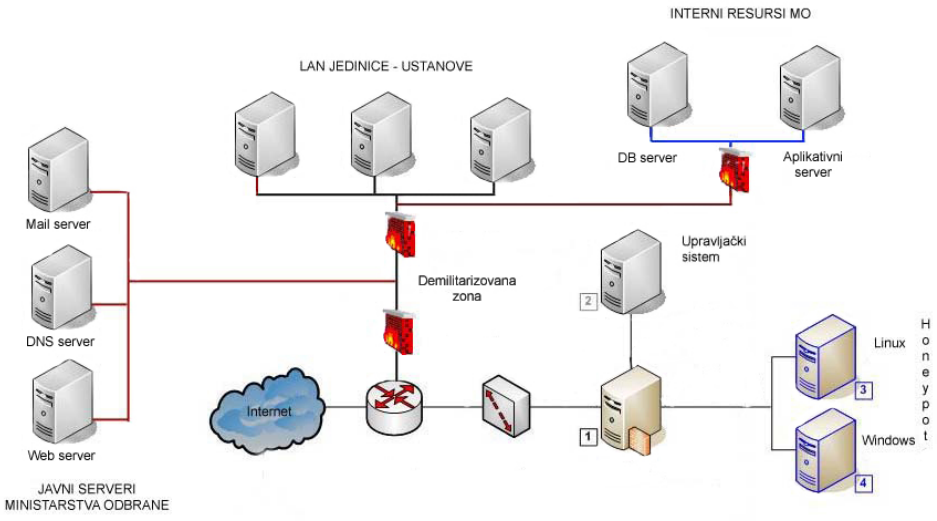
macionog sistema. Integrisanje delova ovog sistema karakterišu poprečne veze internog karaktera, ali zbog fizičkog razmeštaja velikog broja organizacionih celina neophodna je upotreba i delova javnih mreža. Poseban aspekt kome se pristupa planski u svim fazama projektovanja informacionih sistema u Vojsci i Ministarstvu je zaštita računarskih sistema. Primenom svih poznatih hardverskih i softverskih rešenja sprečava se neovlašćeni pristup računarskim mrežama spoljnjeg ili internog karaktera. Obavezna je primena firewalla, mehanizma za detekciju i prevenciju napada, a prenos podataka se vrši kriptovano. Pretnje koje se nameću razvojem i otvaranjem pojedinih delova sistema ka javnoj mreži (internetu) postaju svakim danom sve veće, posebno imajući na umu znanja i metode napadača. Imajući u vidu značaj informacija koje se nalaze u računarskim resursima Ministarstva odbrane i Vojske, nameće se potreba kontinuiranog praćenja i dogradnje zaštite informacionih sistema. Dosadašnja primenjena rešenja zasnivaju se na prevenciji, detekciji i otklanjanu malicioznih aktivnosti napadača koji deluju poznatim metodama i tehnikama. Metode zaštite spadaju u pasivne, te do sada nepoznate metode i tehnike napada nesmetano inficiraju sistem i prete nanošenjem štete nesagledivih posledica. Radi efikasne zaštite potrebno je raspoloživim sredstvima preuzeti aktivnu ulogu u zaštiti računarskih sistema Ministarstva odbrane i Vojske.

Primena virtuelnog honeyneta u zaštiti računarskih sistema Ministarstva odbrane i Vojske

Imajući u vidu razvojne mogućnosti, potrebe i preduzete mere zaštite, značajno unapređenje zaštite računarskog sistema u Ministarstvu odbrane i Vojsci predstavlja uvođenje virtuelnog honeyneta, što je varijanta koja omogućava da se honeynet sa više operativnih sistema postavi na jednom računaru. Ova solucija ima svoje prednosti kao što su moguća implementacija sa relativno malim angažovanjem resursa i jednostavna administracija.

Predloženo rešenje u potpunosti podržava honeynet treće generacije, osnovne module druge generacije honeyneta (data control, data capture), a unapređenja se odnose na integrisanu analizu podataka (data analysis) i grafički interfejs sa administriranjem na daljinu.

Internet računarska mreža Ministarstva odbrane i Vojske Srbije je preko jedinstvene pristupne tačke (ruter) povezana sa javnom (internet) mrežom. Neposredno iza rutera moguća je instalacija arhitekture virtuelnog honeyneta i to preko switcha na jednom host računaru. Svi virtuelni honeypotovi se rutiraju kroz honeywall koristeći VMWare interfejs.



Slika 2 – Arhitektura zaštite računarskih sistema Ministarstva odbrane i Vojske primenom virtuelnog honeyneta

VMWare je programski paket koji podržava kreiranje virtuelnih komponenti mreže za zamišljenu računarsku mrežu. To je, u stvari, virtuelna mreža koju će honeynet videti nakon instalacije. Honeynet je konfigurisan kao virtuelna mašina koja koristi tri interfejsa: dva *bridge* i jedan *host-only.* Honeypot 3 i 4 su konfigurisani preko jednog *host-only* interfejsa, dok napadač koristi *bridge* interfejs. Bridge interfejs nam služi da honeypot konektujemo na računarsku mrežu preko host računara. Pomoću bridgea vrši se konekcija virtuelne mrežne kartice u virtuelnom honeypotu na mrežnu karticu host računara. Host-only virtuelni eternet adapter omogućava vezu sa host operativnim sistemom. Tako se uspostavlja komunikacija između host računara i virtulnog honeypota na istom računaru.

Po pravilu, na host računar se uvek prvo instalira VMWare, a zatim različiti operativni sistemi za honeypot (3 – Linux i 4 – Windows). Nakon instaliranja operativnog sistema instalira se honeywall, što uključuje razvoj, konfigurisanje i upravljanje honeynet gatewayom. Honeynet je na drugom nivou zaštite, a prima i kontroliše sve podatke koji pristižu od napadača.

Arhitektura virtuelnog honeyneta, iako deo globalne računarske mreže Ministarstva odbrane i Vojske Srbije, ne sadrži legitimne podatke i nije deo redovnog protoka informacija, pa je bilo koji zahtev upućen ovoj komponenti sistema nelegalan, bio to zahtev sa javne mreže ili interni – od organa i institucija Ministarstva odbrane.

Prednosti primene honeypota

Za razliku od IDS-a koji prijavljuje kada i ko od napadača pristupa mreži, honeypot je odvojen od mreže, ne vodi računa o preopterećenju saobraćaja na mreži niti razdvajanje legitimnih od nelegitimnih paketa podataka. Honeypot prati samo podatke koji pristižu na njega. Obično je ta količina podataka mala, ali vrlo važna, jer nosi informacije o napadaču. Honeypot daje mogućnost administratorima da brzo uče o nedozvoljenim pristupima, a ako je honeypot napadnut i onesposobljen daje mogućnost administratoru da u realnom vremenu spreči napad na računarske resurse Ministarstva, te može služiti i kao svojevrsni alarm.

Prednosti ove metode mogu biti [5]:

– *mogućnost prikupljanja informacija o tehnikama i alatima* koje napadač koristi;

– *mali broj lažnih upozorenja* s obzirom na to da honeypot registruje samo neovlašćene aktivnosti; za legalne aktivnosti realnog sistema nije namenjen; ukoliko se honeypot koristi kao IDS ovo je velika prednost imajući u vidu da klasični IDS često šalje niz lažnih upozorenja (što zavisi od kvaliteta IDS-a);

– *relativno mala količina prikupljanih podataka* – za razliku od sigurnosnih rešenja, kao što su mrežni (network based) i host (host based) sistemi za detekciju neovlašćenih aktivnosti, honeypot beleži znatno manje količine podataka, ali s obzirom na prirodu tih podataka oni su najčešće korisni podaci;

– *fleksibilnost* – brojne mogućnosti i vrlo široko područje primene;

– *skromni zahtevi za računarskim resursima* – s obzirom na to da su namenjeni da beleže maliciozne aktivnosti nisu potrebni resursi za implementaciju zahtevnih aplikacija;

– *mogućnost analize kriptovanih protokola* – bez obzira na to o kom se servisu ili protokolu radi honeypot beleži napade koji su usmereni ka njemu;

– *jednostavnost* – projektovanje arhitekture jeste jednostavno, ali se ne može reći da je implementacija trivijalan zadatak, imajući u vidu da je potrebno solidno znanje o principima zaštite računarskih sistema. Za implementaciju nisu potrebni složeni algoritmi ili tablice stanja i sl., kao što je to slučaj sa drugim tehnologijama koje su namenjene za detekciju i identifikaciju neovlašćenih korisnika.

Zaključak

Honeypot je relativno nova koncepcija zaštite računarskih sistema sa velikim potencijalom detekcije neovlašćenih aktivnosti i prikupljanja informacija o novim nepoznatim napadima. Kao koncept motivisan novim

mogućnostima, honeypot se kroz honeynet arhitekturu vrlo brzo razvijao, kroz tri generacije, čime su određivani pravci razvoja. Predloženo rešenje primene virtuelnog honeyneta u sistemu zaštite računarskih sistema obuhvata najnovija dostignuća u ovoj oblasti, uvažavajući postojeći sistem zaštite i zahtevane potrebe koje nameće dalji razvoj i otvaranje računarskih mreža Ministarstva odbrane i Vojske Srbije ka javnim mrežama, uz minimalna ulaganja i rizik.

Primarna namena honeyneta jeste prikupljanje što više informacija o napadima na sistem. Honeynet je arhitektura koja simulira bilo koju realnu mrežu. Pomoću nje može se razviti bilo koji sistem, po želji. Ako je arhitektura honeyneta dobro postavljena moguće je prezentovati jedinstvene i veoma korisne podatke o raznim vrstama napada. Razni mehanizmi koji su implementirani u honeynet preuzimaju rizike koje upućuju napadači.

Današnja rešenja virtuelnog honeyneta imaju karakteristike dobrih simulacija koje napadači teško otkrivaju. Ona simuliraju više operativnih sistema na jednom računaru, sa mehanizmima za analizu podataka, i imaju mogućnost upravljanja na udaljenim lokacijama preko javne mreže. To su rešenja koja u svakom slučaju treba imati u vidu pri projektovanju i implementaciji zaštite računarskih sistema u sistemu odbrane.

Literatura

[1] Pfleeger, C., Lawrence, S., Security in Computing, Third Edition, Prentice Hall PTR, New Jersey, 2002.

[2] Honeynet Research Alliance, http://www.honeynet. org – Honeypot, Honeynet, Honeywall, VMWare [27.01.2009]

[3] Shuja, F., Virtual Honeynet: Deploying Honeywall using Vmware, Pakistan Honeynet Project, 2006.

[4] Dulanović, N., Hinić, D., Simić, D., An intrusion prevention mecahnism in Network Infrastructure, YUJOR, 2006.

[5] Honeynet Research Alliance, Know your enemy – learning about security threats, 2nd Ediition, The honeynet project, 2006.

[6] Uputstvo o korišćenju interneta u Ministarstvu odbrane i Vojsci Srbije i Crne Gore, „Službeni vojni list“ br. 1/2006.