Rad primljen: 01.09.2010.

UDK: 343.983:004.8

IZOLOVANJE FAZE INCIDENTA PROAKTIVNE DIGITALNE FORENZIKE KORIŠĆENJEM ADAPTIVNOG VIRTUALNOG OKRUŽENJA

ISOLATION OF THE PROACTIVE DIGITAL FORENSICS INCIDENT PHASE USING THE ADAPTIVE VIRTUAL ENVIRONMENT

Prof. dr Mladen Veinović
Univerzitet Singidunum

Mr Aleksandar Jevremović
Univerzitet Singidunum

Mr Igor Franc
Univerzitet Singidunum

Nenad Stanić, master
Univerzitet Singidunum

Rezime: U ovom radu obrađuje se problem ublažavanja štete nastale tokom faze incidenta koju definiše proaktivna digitalna forenzika. Sama proaktivna digitalna forenzika podrazumeva umanjenje štete izazvane napadom kroz proaktivno pripremu okruženja, pre faze incidenta, a u cilju postizanja spremnosti organizacije za digitalnu forenzičku istragu. Osnovni rezultat ovakvog pristupa jeste brzo reagovanje na incident, ublažavanje njegovih posledica i podizanje kvaliteta zaključaka forenzičke analize. Naš pristup podrazumeva potpuno eliminisanje štete izazvane incidentom njegovim izolovanjem u adaptivno virtualno računarsko okruženje. Pored eliminisanja štete, ovaj pristup nudi bolji kvalitet informacija sakupljenih za potrebe digitalne forenzičke istrage kroz profilisanje napada i napadača. U radu su, pored koncepta, predstavljeni i koraci za formiranje virtualnog okruženja, kao i primer forenzičke analize podataka prikupljenih na predloženi način.

Ključne reči: proaktivna digitanla forenzika, adaptivno virtualino okruženje, izolovanje faze napada.

Abstract: *This paper deals with the problem of mitigating the damage incurred during the phase of the incident, defined by proactive digital forensics. The very proactive digital forensics involves reducing the damage caused by the attack through proactive preparation environment, before the phase of the incident, with the aim of the organization's readiness for digital forensic investigations. The main result of this approach is a rapid response to an incident, mitigating its effects and improving the quality of the conclusions of forensic analysis. Our approach is a complete elimination of damage caused by the incident to his isolation in adaptive virtual computing environment. In addition to eliminating the damage, this approach provides a higher quality of information collected for the purpose of digital forensic investigations in profiling attacks and attackers. The paper also describes the steps for forming a virtual environment, as an example of forensic analysis of data collected in the manner proposed.*

Key words: *proactive digital forensics, adaptive virtual environment, isolation of incident phase.*

1. UVOD

Problemom prikupljanja podataka iz računarskih sistema za potrebe forenzičke analize bavile su se brojne radne grupe pri različitim vladinim, vojnim i civilnim organizacijama. Međutim, ovaj problem ostaje aktuelan baš zbgo toga što se utvrđene metode moraju stalno prilagođavati savremenim stanjima i trendovima u oblasti informacionih tehnologija. Različiti podaci, koji se nalaze u sistemu, mogu nam duže ili kraće vreme biti dostupni za prikupljanje.

Prikupljanje podataka sa računarskih sistema, na kojima su identifikovani bezbednosni incidenti, predstavlja kompleksan zadatak čije pravilno izvođenje može u odlučujućoj meri uticati na uspeh predstojećeg forenzičkog procesa. Međutim, kao problem javlja se česta situacija u kojoj neophodne podatke nije moguće prikupiti iz različitih razloga. Rešenje ovog problema nalazi se u proaktivnoj digitalnoj forenzici (ProDF).

Biti proaktivan definiše se kao kontrolisanje situacije pre nego što se ona dogodi [Soanes C, H.S., 2005]. Savremeni proaktivni sistemi za detekciju i sprečavanje upada u sistem (Intrusion Prevention Systems, IPS) obezbeđuju inteligentnu tehniku za hvatanje napadača, poznatu kao ćup meda (honypot). Ove tehnike omogućavaju „zarobljavanje" hakera u napadnutom sistemu, nakon utvrđivanja njegovog prisustva.

U ovom radu predlaže se korišćenje virtualizovanog računarskog okruženja za potrebe eliminisanja štete nastale u fazi incidenta i obezbeđivanje podataka potrebnih za proces digitalne forenzičke analize. U prvom delu rada date su opšte karakteristike proaktivne digitalne forenzike, njene dimenzije, faze i interni odnosi. Naredni deo rada obrađuje principe i tehnologije za kreiranje i korišćenje virtualnih računarskih sistema i okruženja. U nastavku rada predstavljen je model predloženog rešenja, kao simbioza principa i tehnologija virtualizacije i potreba proaktivne digitalne forenzike. Identifikovani su ključni principi, tehnologije i tačke realizacije rešenja. Takođe, dat je i proces modelovanja za potrebe praktične primene predloženog rešenja, kao i principi i karakteristike na kojima se može postići njegova adaptivnost. U završnim delovima rada obrađuju se otvorena pitanja i identifikovani dalji pravci razvoja, i revidira se ostvareni doprinos. Fokus rada je postavljen na izolovanje faze incidenta u virtualno računarsko okruženje, uz omogućavanje prikupljanja sveobuhvatnih digitalnih podataka (CDE) za potrebe faze digitalne forenzičke analize.

2. PROAKTIVNA DIGITALNA FORENZIKA, ProDF

Proaktivna digitalna forenzika (ProDF) predstavlja proširenje standardne digitalne forenzičke istrage čiji je osnovni cilj da se organizacija pripremi za digitalnu forenzičku istragu (internu ili kriminalnu) ili za testiranje otpornosti sistema na napad, i to pre nego što se napad dogodi. Proaktivna digitalna forenzika (ProDF), koja je definisana u ovom radu teži da podstakne organizacije kako bi započele uvođenje odgovarajućih mera da bi bile spremne za digitalnu forenzičku istragu, uz omogućavanje mehanizma za procenu i poboljšanje IT upravljačkog okruženja date organizacije.

Neophodno je istaći da mnoge organizacije potcenjuju potrebu za digitalnim dokazima [Sommer, P., 2005] u toku svog poslovanja. Kasnije, kada je dokaz neophodan za dokazivanje incidenta ne postoji dovoljno poverljivih digitalnih dokaza koji bi povezali incident sa napadačem. Većina organizacija ulaže mnogo resursa, kao što su vreme, novac i rad za razvijanje odgovora na incident (incident response), povratak posle uništenja (disaster recovery), i na plan kontinuiteta poslovanja što jeste najbolji način da se spreči incident ili da se oporavi od njega i nastavi sa poslom što je brže moguće. Međutim, veoma malo se razmislja o identifikaciji i čuvanju potencijalnih digitalnih dokaza [Clark, A., 2006] i ispravnog struktuiranja procesa za moguće tužbe koje su prihvatljive na sudu.

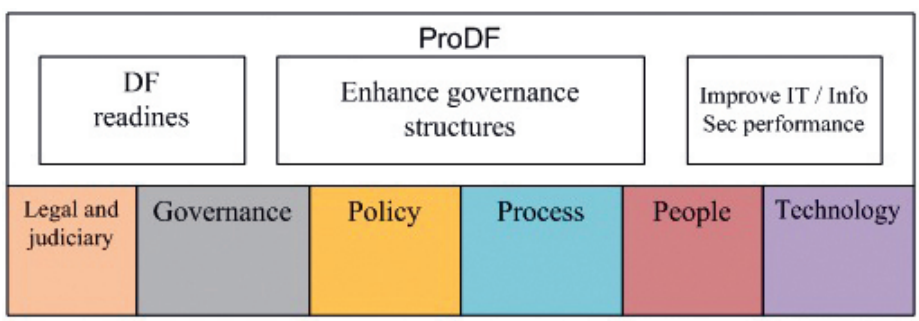
Glavni cilj istrage kompjuterskog kriminala je, kao i u slučaju klasičnog kriminala, izgraditi za pravosudne organe neoboriv, ili čvrst dokaz krivice, i/ili dokaz za oslobađanje osumnjičenog, i/ili pravedno sankcionisanje učinjenog dela. Autori ovog rada predlažu termin: Sveobuhvatan digitalni dokaz (Comprehensive Digital Evidence). CDE predstavlja digitalni dokaz koji je potpun, pouzdan, prihvatljiv na sudu, ima težinu dokaza na sudu za profilisanje incidenta i neosporno povezuje napadača kao počinioca incidenta.

Proaktivna digitalna forenzička istraga (ProDF) obezbeđuje neophodne procese, procedure, tehnologije i sveobuhvatne digitalne dokaze (CDE). Neophodno je razmotriti sledeće ciljeve proaktivne digitalne forenzičke istrage:

- Spremnost za digitalnu forenzičku istragu.
- Poboljšanje upravljačke strukture (IT i Information Security (Info Sec)) u organizacijama.
- Poboljšanje Info Sec / IT performansi sa korišćenjem odgovarajućih alata digitalne forenzike za poboljšanje efektivnosti i efikasnosti u organizaciji.

U literaturi [Ieong, R. and H. Leung, 2007] [Guldentops, E., 2005] [Grobler, C.P., 2004] se često spominje da su ljudi, procesi i tehnologija osnova mnogih upravljačkih modela. Model digitalne forenzičke istrage se takođe često pominje i predlažu se različite dimenzije elemenata i većina modela se koncentriše na pitanja ko, šta, zašto, kako, kada i gde. Autori su uporedili razne modele i predlažu sledeće dimenzije za digitalnu forenzičku istragu:

Slika 1 – Veza između ciljeva i dimenzija



- upravljanje - odgovor na pitanje „Zašto”, razmatra upravljanje objektima, partnerima, i bavi se upravljanjem rizika i operativnim rizicima,
- pravo - odgovor na pitanje „Zašto” i bavi se saglasnošću,
- ljudi - odgovor na pitanje „Ko”,
- politika - odgovor na pitanj „Šta”, „Kada” i „Ko”,
- procesi - odgovor na pitanja „Šta”, „Kada”, „Kako”, „Gde” i „Ko” i
- tehnologija - odgovor na pitanja „Kako”, „Kada” i „Gde” i povezuje korišćene aplikacije i tehnologije.

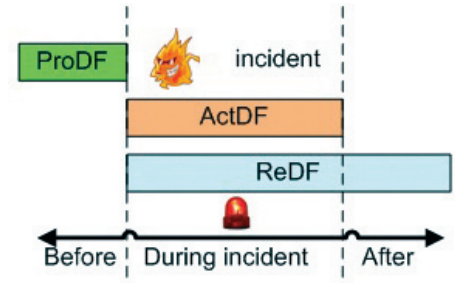
Pored proaktivne digitalne forenzičke istrage postoje još dve komponente digitalone forenzičke istrege [Garcia, J, 2005] istrage a to su:

Aktivna ili „live” digitalna forenzička istraga (ActDF) koja prestavlja sposobnost organizacije da prikupi relevantne i žive sveobuhvatne digitalne dokaze (CDE), zatim da se umanje efekti incidenta koji je u toku i omogući uspešna istraga.

Reaktivna ili „dead” digitalna forenzička istraga (ReDF) sastoji se od analitičkih i istražnih tehnika koje se koriste za zaštitu, identifikaciju, ekstrakticu, dokumentaciju, analizu i interpertaciju digitalnih medija koji su digitalno sačuvani i sakupljeni kao dokaz za olakšnje ili pomoć u rekonstrukciji incidenta.

Potrebno je istaći da se aktivna i reaktivna komponenta digitalne forenzičke istrage razlikuju po načinu upravljanja dokazima, procesima, alatima i primenjenim protokolima istrage. Fokus ovog rada je na proaktivnoj komponenti digitalne forenzičke istrage.

Slika 2 – Veza između komponenata



3. VIRTUALNO RAČUNARSKO OKRUŽENJE

Savremene virtualizacione tehnologije omogućavaju kreiranje kompletnog virtualnog umreženog računarskog okruženja na standardnim računarskim platformama. Koncept virtualnih mašina omogućava izvršavanje više nemodifikovanih operativnih sistema na jednom fizičkom računaru, a noseći softver za virtualizaciju omogućava umrežavanje virtualnih mašina različitim topologijama. Sama virtualizaciona tehnologija jedan je od glavnih fokusa vodećih proizvođača enterprise-level softvera: Microsoft, Red Hat, VMWare, Oracle i sl. Danas postoji veliki broj stabilnih rešenja, od kojih su mnoga i besplatna za korišćenje. Podrška za virtualizaciju integrisana je i u savremene verzije MS Windows Server i Linux operativnih sistema. U poslovnim sistemima virtualizaciona tehnologija se prvenstveno koristi za smanjivanje troškova pri kupovini hardvera.

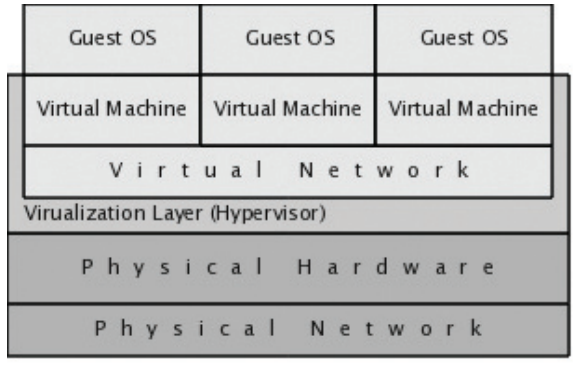
Pored ušteda na hardveru, u osnovne prednosti virtualnih računarskih okruženja spadaju fleksibilnost, skalabilnost i brz oporavak sistema. Fleksibilnost pri

korišćenju virtualnih računara ogleda se, pre svega, u mogućnosti lake migracije virtualizovanog računara sa jedne hardverske platforme na drugu. Ova mogućnost omogućava skalabilno proširivanje snage virtualnih računara u skladu sa potrebama. Proširivanje se vrši dodavanjem hardverskih resursa, a zatim migracijom na savremenije i moćnije hardverske platforme. Takođe, korišćenjem virtualizacionih tehnologija smanjuje se i vreme potrebno za uspostavljanje i oporavak računarskih sistema. S obzirom na to da eksternu memoriju virtualnih računara najčešće predstavljaju fajlovi na nosećim, realnim računarima, kreiranje zaštitnih kopija je u ogromnoj meri olakšano. Sa druge strane, na osnovu takvih kopija eksterne memorije, vreme potrebno za oporavak virtualnih računara se svodi na sekunde ili minute. Dodatno, korišćenjem ovih kopija virtualizovani računari se mogu lako multiplikovati, odnosno, može se lako kreirati složeno umreženo računarsko okruženje.

Za potrebe digitalne forenzičke analize posebno je značajna mogućnost jednostavnog spoljašnjeg nadgledanja virtualizovanog okruženja. Jedna od ključnih komponenata virtualizacione tehnologije jesu hipervizori, softverske komponente koje nadgledaju rad virtualnih mašina. Osim što hipervizori upravljaju korišćenjem resursa deljenih od strane virtualnih mašina, oni omogućavaju preuzimanje aktuelnih informacija o njihovom stanju i radu. Ovo je posebno značajno kada su u pitanju IDS/IPS sistemi i digitalna forenzika jer se na taj način može utvrditi i aktivnost (napadača) a podaci značajni za forenzičku analizu se mogu aktivno kopirati van domašaja napadača.

Virtualizovana računarska okruženja mogu se jednostavno povezati sa realnim računarskim okruženjem organizacije. Ova karakteristika je za koncept, opisan u ovom radu, posebno značajna jer omogućava migriranje napada sa realnog u virtualno računarsko okruženje. Tačku u kojoj će se migracija izvršiti trebalo bi da čini firewall sistem kroz koji napadač pokušava da pristupi realnom privatnom okruženju organizacije. Ispravna realizacija funkcionalnosti ove tačke od ključne je važnosti, jer propusti u njoj dovode do ulaska napadača u realno, umesto u virtualno okruženje. Odluka o preusmeravanju na-padača u virtualno okruženje samo je posledica uspešnog prepoznavanja da je u pitanju napad a ne regularan mrežni saobraćaj. Ona se može doneti na osnovu

Slika 3 – Arhitektura virtualizacije



zaključka IDS/IPS sistema ali su mogući i jednostavniji koncepti.

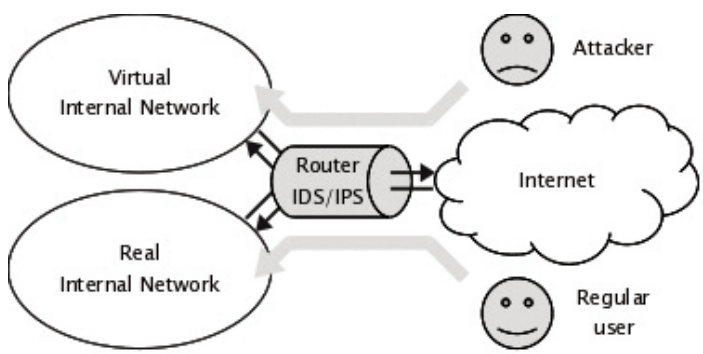
4. MODEL PREDLOŽENOG REŠENJA

Osnovnu ideju predloženog rešenja čini prepoznavanje napada i njegovo preusmeravanje u virtualno računarsko okruženje. Na taj način se štiti realna interna mreža, eliminiše se šteta nastala u fazi incidenta, ali se obezbeđuju odgovarajući podaci, potrebni za fazu aktivne i reaktivne digitalne forenzičke analize. Virtualno računarsko okruženje sadrži virtualnu internu mrežu, odnosno mrežu koja poseduje slične karakteristike kao i realna interna mreža, ali kompromitovanje njenih članova ne nanosi štetu organizaciji.

Teoretski, model se može iskoristiti i u slučajevima kada interna mreža organizacije nije povezana sa spoljnim svetom. Ovaj scenarijo je moguć u situacijama kada organizacija želi da ispita realne mogućnosti i karakteristike eventualnih napada i napadača, pre povezivanja svoje interne mreže sa Internetom. Međutim, danas su u praksi sve ređe interne računarske mreže čiji klijenti nemaju mogućnost pristupa Internetu. Dodatno, sve aktivnije uvođenje Internet protokola verzije 6 u upotrebu otvara i nova bezbednosna pitanja jer se gubi, često, neophodna funkcionalnost prevođenja mrežnih adresa kao jedan od sistema zašite.

Kritičnu tačku predloženog sistema čini ruter, odnosno IDS/IPS sistem. Ovaj sistem ima zadatak da na osnovu dostupnih parametara zahteva sa spoljne mreže utvrdi da je u pitanju napad a ne regularan zahtev. Na primer, ukoliko klijenti sa Interneta vrše pristup Web aplikaciji za elektronsko poslovanje koja se izvršava na serveru u realnoj internoj mreži organizacije, onda se veoma lako može posumnjati na zahteve sa protokolima namenjenim za udaljenu administraciju računara (Remote Desktop, SSH i sl.). S druge strane, u opisanoj situaciji i zahtevi pod HTTP protokolom (ali koji su usmereni na ispitivanje karakteristika Web servera i aplikacije), mogu se preusmeriti u virtualizovano računarsko okruženje, i to upravo ka virtualizovanim instancama Web servera na kojima su namerno napravljeni

Slika 4 – Preusmeravanje napada na internu virtualnu mrežu



bezbednosni propusti (koji odgovaraju identifikovanim tipovima napada) sa svrhom da prikupljaju podatake o cilju, izvoru i karakteristikama napada. Uspešno prepoznavanje napada i preusmeravanje napadača u virtualno okruženje predstavlja izolovanje potencijalne faze incidenta.

Članove virtualne interne mreže čine virtualizovani računari koji simuliraju članove realne interne mreže. Virtualna interna mreža se organizuje tako da po sadržaju i arhitekturi manje ili više odgovara realnoj internoj mreži organizacije, ali tako da napadač prilikom upada u mrežu i njene sisteme stekne utisak da je pristupio realnoj mreži organizacije. S druge strane, virtualna interna mreža može biti i podeljenja tako da se u različitim fragmentima nalaze već pomenuti sistemi koji odgovaraju različitim tipovima napada, u cilju preventivnog profilisanja napadača i utvrđivanje nivoa njegovog znanja i zainteresovanosti za izvršavanje upada. Suprotan koncept podrazumeva blisko uvezivanje karakteristika virutalne interne mreže sa karakteristikama realne interne mreže organizacije, u cilju posrednog utvrđivanja bezbednosnih propusta realne mreže.

Fizički gledano, virtualizovano okruženje u koje se preusmerava napad nalazi se na jednom ili više računara koji mogu, ali i ne moraju biti članovi realne interne mreže. Pretpostavka je da odvajanje računara na kojima se izvršava virtualno okruženje od realne interne mreže može podići nivo bezbednosti. Argument tome jesu i skoro identifikovani eksploiti koji omogućavaju pristup nosećem računaru putem virtualne mašine koja se na njemu izvršava.

5. MODELOVANJE I ADAPTIVNOST

Jedan od prvih i osnovnih koraka u realizaciji virtualnog računarskog okruženja, za potrebe izolovanja faze incidenta i obezbeđivanje podataka za digitalnu forenzičku istragu, jeste njegovo modelovanje. Modelovanje virtualnog računarskog okruženja predstavlja proces u kome se određuju karakteristike virtualnog okruženja koje će biti formirano. Sa druge strane, model kao apstraktan prikaz omogućava proaktivnu analizu i uspostavljanje bezbednosnih politika, i čini osnovu za buduća prilagođavanja virtualnog okruženja realnom.

Modelovanje virtualnog računarskog okruženja vrši se u skladu sa realnim okruženjem organizacije. Postoji više dimenzija po kojima se određuju paralele između realnog i virtualnog okruženja: topologija mreže, broj i tipovi računarskih sistema, softverske komponente i njihove verzije, strukture baza podataka, setovi podataka, i t.d. Bliskim preslikavanjem realnog u virtualno okruženje smanjuje se mogućnost da će napadač shvatiti da je izolovan u okruženje različito od realnog. Dodatno, analizom ponašanja napadača u blisko preslikanom virtualnom okruženju dobijaju se i kvalitetne informacije o realnim ciljevima napada, a takođe se mogu utvrditi i potencijalne slabosti realnog okruženja. Sa druge strane, opasnosti koja leži u bliskom preslikavanju realnog okruženja jeste odavanje previše informacija o samom realnom okruženju, ili čak omogućavanje potpunog uspeha izolovanog napada koji za cilj imaju prikupljanje preslikanih informacija.

Model virtualnog okruženja čini osnovni dokument i preduslov za njegovo formiranje. Na osnovu modela vrši se nabavka potrebnih instalacija softvera (operativnih sistema, softverskih paketa, i sl.), virtualizovanje određenih realnih računarskih sistema, kopiranje određenih setova podataka (šema baza podataka, tabela, fajlova i sl.) sa realnih sistema, i kopiranje bezbednosnih polisa primenjenih na realnim sistema. Takođe, ukoliko je model virtualnog okruženja blizak realnom okruženju, u njemu treba navesti i značajne razlike između realnog i virtualnog okruženja. Ove razlike su značajne u fazi forenzičke analize jer se na osnovu njih, samog modela i prikupljenih podataka mogu utvrditi slabosti sistema zaštite u realnom okruženju.

Na osnovu modela virtualnog okruženja utvrđuje se hardverska platforma na kojoj će se virtualno okruženje izvršavati. Ova platforma mora da poseduje adekvatnu količinu resursa za izvršavanje svih virtualnih mašina definisanih u modelu, a može je činiti jedan ili više fizičkih računara. Postoje određeni pristupi koji omogućavaju da se na jednom fizičkom računaru izvršava veći broj virtualnih računara, odnosno, da ukupan zbir njima dodeljenih resursa bude veći od ukupne količine resursa na fizičkom računaru. Na primer, Linuks operativni sistem počev od verzije 2.6.32 podržava deljenu memoriju jezgra [M. Tim Jones, 2010] što omogućava efikasnije korišćenje dostupne radne memorije. U ovom radu se predlaže drugačiji pristup štednji resursa formiranjem adaptivnog virtualnog računarskog okruženja.

Adaptivnost virtualnog okruženja u ovakvoj primeni ogleda se u mogućnosti aktiviranja određenih delova virtualnog okruženja u zavisnosti od dela okruženja u kome je napadač prisutan. Za postizanje ovakve adaptivnosti podrazumeva se držanje aktivnih svega nekoliko inicijalnih sistema u virtualnom okruženju. Nakon evidentiranja aktivnosti napadača na nekom od njih aktiviraju se direktno povezani sistemi. Veze sistema se određuju u zavisnosti od mrežne topologije virtualnog okruženja a za evidentiranje aktivnosti napadača mogu se koristiti različiti indikatori. Na primer, moguće je iskoristiti razlike u opterećenju procesora procesima virtualne mašine [John Lim, 2009], ukoliko je konfugiracija takva da je razlika u opterećenju pri pristupu napadača primetna. Takođe, moguće je koristiti i druge indikatore kao što su mrežna aktivnost, pokretanje novih procesa, i t.d. Za smanjenje vremena potrebnog za aktiviranje pasivnih članova virtualne računarske mreže, za njih je potrebno čuvati snimak stanja radne memorije. Na taj način se vreme potrebno za učitavanje operativnog sistema i servisa zamenjuje vremenom potrebnim za učitavanje slike radne memorije aktivne varijante sistema.

Prednosti ovakve adaptivnosti virtualnog računarskog okruženja odnose se, pre svega, na ekonomski aspekt noseće hardverske platforme. Za opisani pristup važna je pretpostavka da napadač neće istovremeno pristupati svim sistemima u virtualnom računarskom okruženju, odnosno, da neće biti istovremeno biti aktivne sve grane grafa kojim bi virtualno okruženje bilo opisano. U protivnom, prevazišla bi se dostupna količina resursa i ne bi mogli da se aktiviraju potrebni delovi virtualnog okruženja. Sa druge

strane, stavljanje dovoljne količine resursa za taj slučaj eliminiše potrebu za komplikovanjem sistema adaptibilnim funkcijama jer omogućava istovremenu aktivnost svih sistema u virtualnom računarskom okruženju.

6. OTVORENA PITANJA I DALJI PRAVCI ISTRAŽIVANJA

Jedno od najznačajnijih pitanja koje se otvara korišćenjem opisanog virtualnog okruženja jeste upravo mogućnost da napadač detaljnim ispitivanjem okruženja utvrdi da se ne nalazi u realnom već u virtualizovanom, izolovanom okruženju. Do pomenutog zaključka napadač može doći pre svega kroz analizu hardverskih parametara sistema kojem je ostvario pristup, odnosno, analizom modula jezgra kojima je ostvaren pristup spoljnoj memoriji, mrežnim interfejsima i sl. U praksi su aktivnosti napadača usmerene pre svega ka ispitivanju mrežne topologije i softverskih parametara sistema, odnosno, propusta u njima. Međutim, adekvatnim izmenama virtualizacione platforme, ili operativnih sistema virtualizovanih sistema, mogu se simulirati i hardverske komponente na osnovu kojih će napadač steći utisak da se nalazi na fizičkom sistemu, bez supervizora.

Sledeće značajno pitanje odnosi se na bezbednosne politike vezane za upravljanje virtualnim okruženjem. Tim dokumentima moraju se jasno definisati, pre svega sledeći aspekti primene predloženog rešenja:

- proces i nadležnosti u uspostavljanju virtualnog okruženja
- segmenti i stepeni poklapanja virtualnog okruženja sa realnim
- setovi i ažurnost podataka koji se kopiraju u virtualno okruženje

Pravilnim razvojem bezbednosnih polisa koje se odnose na upravljanje virtualnim okruženjem, i njihovom adekvatnom primenom, doprinosi se postizanju cilja predloženog u ovom radu, izolovanje faze incidenta, eliminisanje štete koja je u njoj izazvana, i prikupljanje adekvatnih podataka za potrebe digitalne forenzičke analize.

7. ZAKLJUČAK

Rešenje predloženo u ovom radu omogućava izolovanje faze incidenta, definisane u proaktivnoj digitalnoj forenzici, u virtualno računarsko okruženje. Prvi cilj koji se postiže primenom predloženog pristupa jeste eliminisanje negativnih posledica faze incidenta, štete izazvane napadom. Ne manje važan očekivani rezultat je i obezbeđivanje sveobuhvatnih digitalnih dokaza za potrebe digitalne forenzičke istrage.

Kao osnova realizacije predloženog rešenja podrazumevana je virtualizaciona tehnologija. Njenom primenom se obezbeđuje neophodna fleksibilnost predloženog rešenja i drastično smanjuju troškovi za kreiranje virtualnog računarskog okruženja u koje se izoluju napadi. Pored toga, opisana adaptivnost predloženog rešenja, kao osnova efikasnijeg korišćenja resursa i preciznijeg profilisanja napadača, zasnovana je na određenim jedinstvenim karakteristikama virtualizovanih računarskih sistema i mreža.

S obzirom na aktuelnost proaktivne digitalne forenzike i virtualizacionih

tehnologija, postoji veliki broj otvorenih pitanja i prostora za unapređivanje u ob-lasti kojom se ovaj rad bavi. Međutim, smatramo da se u ovom pravcu mogu postići značajni rezultati u pogledu podizanja bezbednosnog nivoa računarskih sistema, kao i broj uspešnih forenzičkih istraga.

Literatura

[1] [Soanes C, H.S., 2005] Oxford Dictionary, in Compact Oxford English Dictionary of Current English 2005, Oxford University press

[2] [Sommer, P., 2005] Directors and Corporate Advisors' Guide to Digital Investigations and Evidence. Information Assurance Advisory Council, http://www.iaac.org.uk, accessed 3 June 2010

[3] [Clark, A., 2006] Are you ready for Forensics? http://www.inforenz.com/press/20060223

[4] [leong, R. and H. Leung, 2007] Deriving Case-specific Live Forensics Investigation Procedures from FORZA. in Symposium on Applied Computing archive Proceedings of the 2007 ACM symposium on Applied computing 2007. Seoul, Korea: ACM Press New York, NY, USA.

[5] [Guldentops, E., 2005] et al., Aligning COBIT, ITIL and ISO 17799 for Business Benefit. 2005, The IT Governance Institute

[6] [Grobler, C.P., 2004] A model to assess Information Security in an organisation - specific reference to the Policy dimension, in Academy of IT. 2004, RAU: Johannesburg

[7] [Garcia, J, 2005] Proactive and Reactive Forensics. http:rediris.es/cert/doc/reuniones/af05/proactive_n_reactive_forens ics.pdf, accessed 5 Maj 2010

[8] [M. Tim Jones, 2010] Anatomy of Linux Kernel Shared Memory, M. Tim Jones 2010., http://www.ibm.com/developerworks/linux/library/l-kernel-shared-memory/index.html

[9] [John Lim, 2009] Monitoring and logging CPU Utilization of Virtual Machines in Xen, John Lim 2009., http://phplens.com/phpeverywhere/?q=node/view/266

Autori

Mr Igor Franc
Univerzitet Singidunum
Danijelova 32, Beograd

e-mail:
ifranc@singidunum.ac.rs

Oblast istraživanja:
digitalna forenzika, bezbednost inormacionih sistema, računarske mreže, internet tehnologije, smart kartice, elektronsko poslovanje.

Mr Aleksandar Jevremović
Univerzitet Singidunum
Danijelova 32, Beograd

e-mail:
ajevremovic@singidunum.ac.rs

Oblast istraživanja:
računarske mreže, baze podataka, zaštita informacija, elektronsko poslovanje, Internet tehnologije.

Prof. dr Mladen Veinović
Univerzitet Singidunum
Danijelova 32, Beograd

e-mail:
mveinovic@singidunum.ac.rs

Oblast istraživanja:
računarske mreže, baze podataka, zaštita informacija, elektronsko poslovanje, digitalna obrada signala, identifikacija sistema.

Nenad Stanić, master
Univerzitet Singidunum
Danijelova 32, Beograd

e-mail:
nstanic@singidunum.ac.rs

Oblast istraživanja:
baze podataka, zaštita informacija, elektronsko poslovanje, Internet tehnologije.