Sistematizovano udaljeno prikupljanje podataka sa aktivnih sistema za potrebe forenzičke analize

Igor Franc, Mladen Veinović

***Sadržaj* — U slučajevima bezbednosnih incidenata na aktivnim sistemima, pravilno prikupljanje relevantnih podataka može značajno povećati verovatnoću dolaženja do informacija o tome ko je izvršilac napada, odakle je napad izvršen, na koji način je napad izvršen i sl. U ovom radu se predstavljaju rezultati napora da se postavljeni formalni standardi i metode automatizovano primene na trenuto aktuelne realne i operativne sisteme i okruženja. Dodatno, u radu se pored pribavljanja potencijalnih dokaza sakupljaju i informacije o stanju sistema posle napada. Kod nekih izvora načini prikupljanja potencijalnih dokaza se kategorišu i na osnovu tačke sa koje se prikupljanje vrši (lokalna i udaljena metoda). Ovde će biti obrađena udaljena metoda koja podrazumeva da digitalni forenzičar nema fizički pristup sistemu.**

***Ključne reči* — Aktivni odgovor, aktivna akvizicija, *batch* obrada, etički haking, otvoreni kod, RAID, RFC3227, *Locardov* princip razmene, NetCat, WDE**

I. UVOD

Prikupljanje podataka sa računarskih sistema, na kojima su identifikovani bezbednosni incidenti, predstavlja kompleksan zadatak čije pravilno izvođenje može u odlučujućoj meri uticati na uspešnost predstojećeg forenzičkog procesa. Lokardov princip razmene [1] kaže da u svakoj interakciji dva objekta dolazi do određene razmene, odnosno, promene stanja objekata učesnika. Na primer, u saobraćajnoj nesreći gde automobil udari pešaka doći će do razmene, tako što će se na automobilu naći krv, koza ili kosa udarenog pešaka i obrnuto pešak će zadobiti određene povrede koje zavise od površine koja ga je udarila (branik automobila, far) što može biti važan dokaz u toku forenzičke istrage.

Primenom Lokardovog principa razmene materije, na oblast računarske forenzike, postaje jasno da pravilnost sakupljanja podataka sa određenog računarskog sistema ima dva pretpostavljena cilja:

1. obezbeđenje relevantnih podataka na osnovu kojih se forenzičkom analizom mogu doneti tačni zaključci o svim značajnim aspektima incidenta
2. sakupljanje podataka uz minimalnije izmene u okruženju (računarskom sistemu) u cilju ne ugrožavanja skupa podataka koji će biti korišćeni u daljoj forenzičkoj analizi.

Problemom prikupljanja podataka iz računarskih sistema za potrebe forenzičke analize, bavile su se brojne radne grupe pri različitim vojnim i civilnim organizacijama. Međutim, ovaj problem ostaje aktuelan baš iz razloga što se utvrđene metode moraju stalno prilagođavati savremenim stanjima i trendovima u oblasti informacionih tehnologija.

II. LIVE RESPONSE I LIVE ACQUSITION

Jedan od izraženijih problema u prikupljanju podataka za potrebe forenzičke analize je u tome što se računari na kojima su identifikovani bezbednosni incidenti ne smeju isključiti već se prikupljanje podataka mora vršiti na aktivnom sistemu koji obavlja svoje regularne zadatke. Za potrebe ovakvih situacija razvijena su dva pristupa:

1. Aktivni odgovor *(Live response)* i
2. Aktivna akvizicija *(Live acquisition).*

Pristup *aktivnog odgovora* podrazumeva prikupljanje relevantnih promenljivih podataka aktivnog sistema sadržaja radne memorije, registara, aktivnih mrežnih komunikacija, aktivnih procesa i sl. Korišćenjem ovog pristupa, za potrebe analize, preuzima se samo deo podataka aktivnog sistema, relevantnih za potrebe forenzičke analize. Nasuprot pristupu aktivnog odgovora, *aktivna akvizicija* podrazumeva pravljenje kompletne kopije spoljne memorije aktivnog računara. Ovom metodom se, za razliku od metode aktivnog odgovora, ne preuzima kopija radne memorije (RAM-a). Fokus ovog rada je postavljen na metodu *aktivnog odgovora* dok metoda *aktivne akvizicije* izlazi izvan njegovih okvira.

Metoda *aktivnog odgovora* je široko prihvaćena u aktuelnim forenzičkim krugovima i najčešće se koristi:

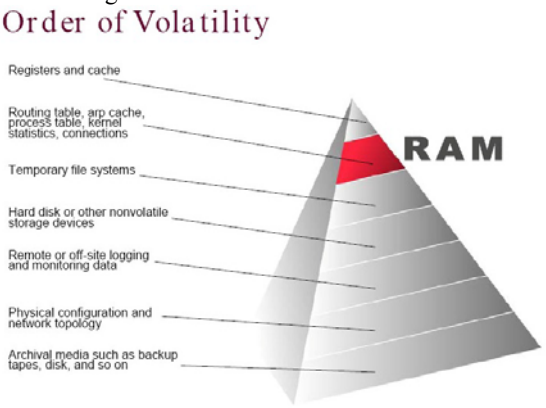
- na računarskim sistemima vezanim za elektronske novčane transakcije (e-commerce) koje moraju biti stalno omogućene, te se gašenje računara isključuje kao mogućnost;
- na računarskim sistemima kod kojih je aktivno šifrovanje sadržaja spoljne memorije (tzv. *whole disc encryption, WDE*);

Mr Igor Franc ifranc@singidunum.ac.rs
Prof. Dr Mladen Veinović mveinovic@singidunum.ac.rs

- kod računarskih sistema zaraženih malicioznim softverom, usko vezanim za prisutnu hardversku platformu;
- kod računarskih sistema koji poseduju ogromnu količinu spoljne memorije (npr. računari sa aktivnim RAID diskovima i sl.).

III. TRAJNOST PODATAKA U SISTEMU

Različiti podaci, koji se nalaze u sistemu, mogu nam duže ili kraće vreme biti dostupni. Potrebno je napraviti određeni redosled za njihovo prikupljanje kako ne bi bili izgubljeni zbog protoka vremena ili zbog akcija koje preduzima digitalni forenzičar.



Sl. 1. Trajnost podatka u sistemu [2]

TABELA 1: TRAJNOST PODATAKA [3]

LOKACIJA	TRAJNOST
CPU registri	milisekunde
CPU *cache*	sekunde
RAM	minuti
Disk cache	sati
Temporary files	sati
Unallocated space	dani
Permanent files	godine

IV. STANDARDIZOVANO PRIKUPLJANJE PODATAKA

Vrlo je bitno poznavati određene standarde i poštovati ih prilikom prikupljanja potencijalnih dokaza. Dva standarda koja su kreirana od strane IETF grupe i direktno su vezana za digitalnu forenziku su RFC2828[4] i RFC3227 [5]. Prvi standard je vezan za opštu bezbednost, a drugi, vrlo bitan za ovaj rad (posebno je važna sekcija 2.1), daje određeni redosled prikupljanja potencijalnih dokaza za tipičan sistem, i stoga je detaljno predstavljen u ovom radu.

Svrha RFC 3227 dokumenta je da sistem administratorima i digitalnim forenzičarima da smernice za prikupljanje i čuvanje podataka koji se mogu koristiti kao dokaz da se sigurnosni incident dogodio ili se sumnja u to. Od posebnog značaja je deo dokumenta 2.1. u kome je tačno dat redosled prikupljanja podataka.

Dokazi se prikupljaju tako da se prvo prikupe oni koji su najćešće promenljivi, a zatim onih koji to nisu. U nastavku je dat primer redosleda prikupljanja podataka za jedan tipičan sistem:

- Registri (*registers*), Keš (*cache*)
- Tabele rutiranja (*routing table*), arp keš (*arp cache*), tabela procesa (*process table*), statistika kernela (*kernel statistics*)
- Memorija (*memory*)
- Privremeni sistemski fajlovi (*temporary file systems*)
- Disk
- Udaljeno logovanje i kontrolisanje relevantnih podataka (*remote logging and monitoring data that is relevant*)
- Fizička konfiguracija (*physical configuration*), topologija mreže (*network topology*)
- Arhivski mediji (*archival media*)

A. *Predlog redosleda prikupljanja podataka*

Na osnovu Sl. 1, kao i na osnovu primera koji je dat u RFC3227 [5], predlaže se redosled prikupljanja podataka sa računara putem metodologije *aktivnog odgovora*. Predlog je nastao na osnovu analize velikog broja izveštaja koji generišu razni programi za digitalnu forenziku (FTK, EnCase...).

- Sistemski datum i vreme
- Mrežne konekcije
- Informacije o portovima
- Informacije o mreži (*Cached NetBIOS Name Table*)
- Status mreže (*promiscuous mode*)
- Interna tabela rutiranja
- Logovani korisnici
- Informacije o procesima
- Informacije o servisima i drajverima
- Otvoreni fajlovi
- Memorija (*process memory dumps, full system memory dumps*)
- Sadržaj CLIPBOARD memorije
- Istorijat izvršenih naredbi (engl. *command history*)
- Tempirani procesi (*Scheduled jobs*)
- Informacije o tipu i verziji operativnog sistema
- Mapirani drajvovi

V. UDALJENA LIVE RESPONSE METODOLOGIJA

Ova metoda se koristi kada digitalni forenzičar nema fizički pristup računaru. Podaci se prikuplaju kroz računarsku mrežu (NetCat, CryptCat) do računara u forenzičkoj laboratoriji ili do laptop računara forenzičara. Najveća mana ove metode jeste što digitalni forenzičar mora imati korisničko ime i šifru nekog od korisnika kompromitovanog računara, kao i to da na računaru ne sme biti aktivan firewall što podrazumeva da je za ovo neophodna saradnja sa sistem administratorom ukoliko je to moguće. Ukoliko to nije moguće neophodno je koristiti metode etičkog hakinga (*Ethical Hacking*) kako bi se došlo do korisničkog imena i lozinke ili kako bi se zaobišao na neki način firewall.

Prilikom korišćenja ove metode mogu se lako i brzo prikupiti podaci pod uslovom da je propusna moć konekcije dovoljno velika za prenos određene količine podataka, u suprotnom procedura prikupljanja podataka bi mogla dugo da traje. Za ovu metodu, takođe, je važno da forenzičar koristi BATCH fajlove kako bi automatizovao i ubrzao proces prikupljanja podataka.

VI. PRIMENA NA MS WINDOWS OS

Za potrebe ovog rada izvršeno je testiranje batch fajla na različitim Windows sistemima (Win XP sp1, Win XP sp3, Win 2003 server, VISTA, Windows 7) i dobijeni su približno isti rezultati, što znači da je ovaj fajl primenljiv na svim gore navedenim MS operativnim sistemima.

A. MS Windows XP

Pošto je ovo i dalje najčešće korišćeni operativni sistem, testiranje je započeto baš na njemu. Instaliran je čist OS, bez dodatnih programa i pušten je *batch* fajl koji je izvršen bez greške. Na taj način su kreirani fajlovi koji pokazuju kakvo je trenutno stanje sistema, odnosno kakva je njegova slika sa bezbednosnog aspekta.

Takođe, prikupljen je i kompletan sadržaj radne memorije, na računaru za testiranje, veličine 512 MB. Od posebnog je značaja istaći da forenzičar mora imati administratorski nalog kako bi mogao u potpunosti prikupiti podatke.

Prilikom testiranja, skripta je izvršena preko administratorskog naloga i prikupljeni su potrebni podaci. Pošto postoje različite varijante Win XP sistema u zavisnosti od instaliranog *Service Pack*-a isti fajl je pušten na sistem sa SP1 i SP3. Rezultati su bili identični, što znači da je fajl kreiran tako da se bez problema može koristi na svakom Win XP sistemu.

B. MS VISTA/Windows7

S obzirom da na tržištu operativnih sistema postoje i ovi sistemi koji trenutno još uvek nisu aktuelni, očekuje se njihova ekspanzija i već su vršeni testovi na njima. Oni imaju približno istu arhitekturu i skoro su potpuno identični. Testiranje je vršeno na čistim, tek instaliranim sistemima Windows 7 RC1 i VISTA SP1, bez dodatnih programa.

Testiranje je pokazalo da je *batch* fajl prošao bez problema i na taj način se pokazalo kakvo je trenutno stanje sistema, odnosno njegova slika sa bezbednosnog aspekta. Ovde se pojavio problem sa programom *mdd1*.3, koji nije mogao da isčita trenutno stanje radne memorije od 2GB i da to upiše u fajl.

Testiranje je pokazalo da je na ovim sistemima došlo do povećane kontrole korisnika. Važna napomena je da, ukoliko korisnik nema administrativni nalog, može prikupiti samo elementarne podatke koji možda neće biti dovoljni za dalju istragu. Ova situacija je prikazana u tabeli 3. Može se videti da 7 različitih fajlova nije moglo da se izvrši ako korisnik nije imao administratorske privilegije na sistemu.

C. MS Windows 2003 Server

Pošto Win 2003 i Win XP dele sličnu arhitekturu, izvršeno je i testiranje na ovom operativnom sistemu koji se vrlo često sreće u poslovnom okruženju. Kao što se očekivalo, testiranje je pokazalo da je *batch* fajl prošao bez problema i na taj način kreirani log fajlovi su pokazali kakvo je trenutno stanje sistema, odnosno njegova slika sa bezbednosnog aspekta.

Jedina smetnja koja se pojavila u ovom sistemu je program *Fport* koji nije mogao da se izvrši. Za testiranje 512MB na ovom računaru prikupljen je i kompletan sadržaj radne memorije. Proveravanje je vršeno na čistom, tek instaliranom sistemu, bez dodatnih programa i sa SP1 (*Service Pack 1*).

VII. BATCH FAJL

Tokom testiranja pokazalo se da je ovaj fajl potpuno primenljiv na svim trenutno aktuelnim MS Windows operativnim sistemima pa čak i na Windows 7. U zavisnosti od privilegija naloga po kome se vrši proveravanje, fajl dat na Sl. 2. prikuplja potencijalne dokaze koje dalje digitalni forenzičari mogu obrađivati i na taj način utvrditi ko je, odakle i šta uradio na aktivnom sistemu, bez potrebe da fizički budu prisutni kao i bez potrebe za isključivanjem istog.

```
md reportsr
psexec.exe \\%1 -u %2 -p %3 date /t > reportsr\date.log
psexec.exe \\%1 -u %2 -p %3 time /t > reportsr\time.log
psexec.exe \\%1 -u %2 -p %3 netstat -ano > reportsr\netstat_ano.log
psexec.exe \\%1 -u %2 -p %3 -c fport.exe > reportsr\fport.log
psexec.exe \\%1 -u %2 -p %3 -c openports.exe > reportsr\openports.log
psexec.exe \\%1 -u %2 -p %3 nbtstat -c > reportsr\nbtstat_c.log
psexec.exe \\%1 -u %2 -p %3 ipconfig /all > reportsr\ipconfig_all.log
psexec.exe \\%1 -u %2 -p %3 -c promiscdetect.exe >
reportsr\promisc.log
psexec.exe \\%1 -u %2 -p %3 -c promqry.exe > reportsr\promqry.log
psexec.exe \\%1 -u %2 -p %3 netstat -rn > reportsr\nestat_rn.log
psexec.exe \\%1 -u %2 -p %3 -c psloggedon.exe >
reportsr\psloggedon.log
psexec.exe \\%1 -u %2 -p %3 -c logonsessions.exe >
reportsr\logonsessions.log
psexec.exe \\%1 -u %2 -p %3 -c pslist.exe > reportsr\pslist.log
psexec.exe \\%1 -u %2 -p %3 -c listdlls.exe > reporter\listdlls.log
psexec.exe \\%1 -u %2 -p %3 -c handle.exe > reportsr\handle.log
psexec.exe \\%1 -u %2 -p %3 -c svc.exe > reportsr\svc.log
psexec.exe \\%1 -u %2 -p %3 -c psservice.exe > reportsr\psservice.log
psexec.exe \\%1 -u %2 -p %3 -c psfile.exe > reportsr\psfile.log
psexec.exe \\%1 -u %2 -p %3 -c userdump.exe > reportsr\userdump.log
psexec.exe \\%1 -u %2 -p %3 doskey /history >
reportsr\doskey_history.log
psexec.exe \\%1 -u %2 -p %3 at > reportsr\shedule_job.log
psexec.exe \\%1 -u %2 -p %3 -c psinfo -h -s -d > reportsr\psinfo.log
psexec.exe \\%1 -u %2 -p %3 -c di.exe > reportsr\drives.log
psexec.exe \\%1 -u %2 -p %3 -c share.exe > reportsr\share.log
```

Sl. 2. Listing batch fajla za udaljeno prikupljanje

Kao što se vidi u ovom fajlu, većina komandi je iz *SysInternals*-a [6], *Fport* je iz *Foundstones*-a [7], a ima i generičkih Windows komandi koji su sastavni deo operativnog sistema. Takođe na Sl. 2 se može videti da se komanda psexec.exe često ponavlja. Razlog za to je što je to ključna komanda za metodu udaljenog pristupa jer omogućava pokretanje komandi sa udaljene lokacije kao da se pokreću lokalno sa računara a rezultati se šalju putem mreže do određenog računara koji forenzičar odredi.

Ono što je ovde još bitno jeste da je za pokretanje ovog fajla potrebno proslediti tri parametra:

- Korisničko ime (*user name*) - %1
- Lozinku (*password*) – 2%

- IP adresu računara na koji se šalju padaci – 3%

TABELA 2: IZVRŠENE KOMANDE SA ADMINISTRATORSKOG NALOGA

ADMIN PRIVILEGES	Win XP SP1	VISTA/Win 7	Win 2003 Server
date	x	x	x
time	x	x	x
netstat -ano	x	x	x
fport	x		
openports	x	x	x
nbtstat -c	x	x	x
ipconfig /all	x	x	x
promiscdetect	x	x	x
promqry		x	x
netstat -rn	x	x	x
psloggedon	x	x	x
logonsessions	x	x	x
pslist	x	x	x
listdlls	x	x	x
handle	x	x	x
svc	x	x	x
psservice	x	x	x
psfile	x	x	x
userdump	x	x	x
mdd	x		x
pclip	x	x	x
doskey /history	x	x	x
at	x	x	x
psinfo	x	x	x
di	x	x	x
share	x	x	x

TABELA 3: IZVRŠENE KOMANDE BEZ ADMINISTRATORSKOG NALOGA

NON ADMIN PRIVILEGES	Win XP SP1	VISTA/Win 7	Win 2003 Server
date	x	x	x
time	x	x	x
netstat -ano	x	x	x
fport	x		
openports	x	x	x
nbtstat -c		x	x
ipconfig /all	x	x	x
promiscdetect	x	x	x
promqry		x	x
netstat -rn	x	x	x
psloggedon	x	x	x
logonsessions			
pslist	x	x	x
listdlls			
handle			
svc	x	x	x
psservice	x	x	x
psfile			
userdump	x	x	x
mdd			
pclip	x	x	x
doskey /history	x	x	x
at			
psinfo	x	x	x
di	x	x	x
share	x	x	x

VIII. ZAKLJUČAK

U ovom radu predstavljeni su osnovni faktori koji imaju uticaja na uspešnost prikupljanja podataka za potrebe forenzičke analize. Korišćeni su aktuelni standardi, a kao osnova uzet je RFC 3227 dokument. Kao osnovni fokus rada postavljena je metodologija *udaljenog aktivnog odgovora*, koja ima za cilj da omogući uspešno sakupljanje podataka sa aktivnih računarskih sistema, koji paralelno, sa procesom preuzimanja podataka obavljaju i svoje standardne zadatke. Takođe, ova metodologija omogućava pristup određenom skupu podataka kome je nemoguće pristupiti drugim metodama, odnosno, metodama koje podrazumevaju prikupljanje podataka posle isključivanja računarskih sistema ili fizičkog prisustva forenzičara.

LITERATURA

[1] Harlan Carvey, *Windows Forensic Analysis*. Syngress 2007.
[2] http://www.cert.org
[3] Chad Steel, *Windows Forensics*. Wiley 2006.
[4] RFC2828 – Internet Security Glossary
[5] RFC3227 - Guidelines for Evidence Collection and Archiving
[6] http://technet.microsoft.com/en-us/sysinternals/default.aspx
[7] www.foundstone.com

ABSTRACT

In case of security incidents in active systems, collection of relevant data can significantly increase the likelihood of discovering the information about who is the perpetrator of attacks, which carried out the attack, the way the offense performed, and the like. The results of efforts to set formal standards and methods for automatic application of the current actual and real operating systems and environments, are presented in this article. In addition, beside gathering of potential evidences, information about the system after attack has also been gatered in this work.

METHODICAL DATA COLLECTING FOR FORENSIC ANALYSIS PURPOSE FROM REMOTE LIVE SYSTEMS

Igor Franc, Mladen Veinović