Rad primljen:15.02.2010.
UDK: 343.983:004.623

IMPLEMENTACIJA HIBRIDNOG METODA PRIKUPLJANJA PODATAKA SA AKTIVNIH WINDOWS SISTEMA ZA POTREBE FORENZIČKE ANALIZE

IMPLEMENTATION OF THE HYBRID METHOD OF DATA COLLECTION WITH ACTIVE WINDOWS SYSTEM FOR FORENSIC ANALYSIS

Prof. dr Mladen Veinović
Univerzitet Singidunum

Mr Igor Franc
Univerzitet Singidunum

Rezime: U slučajevima bezbednosnih incidenata na aktivnim windows sistemima, pravilno prikupljanje relevantnih podataka može značajno povećati verovatnoću dolaženja do informacija-o tome ko, odakle, i na koji način je napad izvršio napad i sl. Kod nekih izvora, se načini prikupljanja potencijalnih dokaza, kategoriše se i na osnovu tačke sa koje se prikupljanje vrši (lokalna i udaljena metoda). U ovom radu se predstavljaju rezultati napora da se ode korak dalje i predlaže korišćenje kombinovane (hibridne) metode prikupljanja podataka sa aktivnih sistema. Reč je, dakle,o pribavljanja potencijalnih dokaza, i sakupljanju informacija o stanju sistema posle napada.

Ključne reči: (Live response), live acquisition, batch obrada, RFC3227, Locardov princip razmene, trajnost podataka, hibridna metoda, WDA, RAID...

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, etc. For some sources of the potential ways of collecting evidence and rank on the basis of points which made the collection of (local and remote methods). In this paper we present the results of efforts to go further and propose the use of hybrid methods of collecting data from the active system. In addition, beside gathering of potential evidences, information about the system after attack has also been gatered in this work.*

Keywords: *Live response, live acquisition, batch, RFC3227, LOCARD'S EXCHANGE PRINCIPLE, order of volatile, hybrid metod, WDA, RAID.*

1. 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, ako dva računara, na neki način, razmenjuju podatke, odnosno komuniciraju putem mreže u RAM memoriji jednog računara, naćiće se IP adresa drugog i obrnuto, u RAM memoriji drugog računara naći će se IP adresaonogprvog.

Primenom Lokardovog principa, na oblast računarske forenzike, postaje jasno da pravilnost sakupljanja podataka, sa određenog računarskog sistema, ima dva pretpostavljena razloga a to su:

1. obezbeđivanje relevantnih podataka na osnovu kojih se, forenzičkom analizom, mogu doneti tačni zaključci o svim značajnim aspektima incidenta i
2. sakupljanje podataka, uz minimalnije izmene u okruženju (računarskom sistemu), u cilju ne - ugrožavanja skupa podataka za korišćenje u daljoj forenzičkoj analizi.

2. AKTIVNI ODGOVOR I AKTIVNA AKVIZICIJA

U prikupljanju podataka, za potrebe forenzičke analize, računari, na kojima su identifikovani bezbednosni incidenti, ne smeju se isključivati, već treba da budu u aktivnom sistemu, koji obavlja svoje regularne zadatke. Za ovakve procese postoje dva pristupa:

1. Aktivniodgovor (Live response)
2. Aktivnaakvizicija (Live acquisition)

Proces 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 samodeo podataka, aktivnog sistema, relevantnih za potrebe forenzičke analize. Na suprot *njemu aktivna akvizicija ostvarenje* kompletne kopije spoljne memorije aktivnog računara. Fokus ovog rada je na metodu aktivnog odgovora je za razliku od metoda aktivne akvizicije koja izlazi iz njegovih okvira.

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

- na računarskim sistemima u vezi elektronskim novčanim transakcijama (e-commerce) koje su stalnoprisutne te se gašenje računara isključuje kao mogućnost,
- na računarskim sistemima kod kojih je aktivno šifrovanje sadržaja spoljne memorije (tzv. *whole disc encryption, wde*),
- kod računarskih sistema zaraženih malicioznim softverom, usko vezanim za prisutnu hardversku platformu i
- kod računarskih sistema koji poseduju ogromnu količinu spoljne memorije (npr. računari sa aktivnim RAID diskovima i sl.).

3. TRAJNOST PODATAKA U SISTEMU

Različiti podaci, koji se nalaze u sistemu, mogu nam duže ili kraće vreme biti dostupni [2]. Potrebno je napraviti određeni redosled za njihovo prikupljanje i čuvanje kako ne bi bili izgubljeni zbog protoka vremena.

Slika 1. Trajnost podatka u sistemu [3]

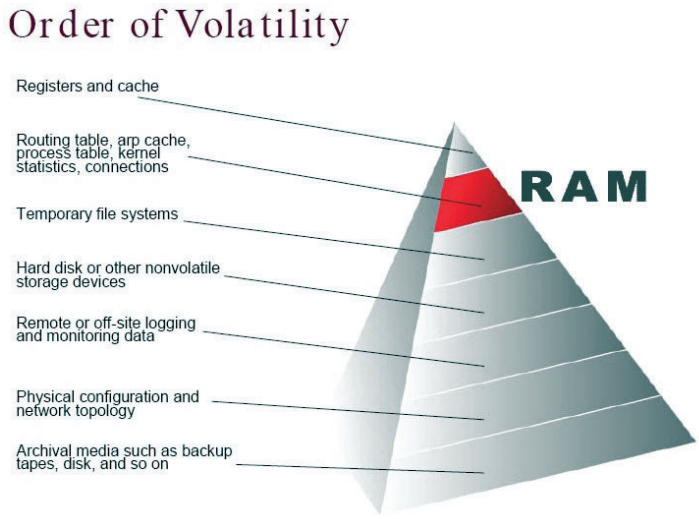

Tabela [4] pokazuje trajnost podataka u intervalima, od nekoliko mikrosekundi do nekoliko godina, a može se videti i koji metod analize je primenljiv za njihovo prikupljanje.

Tabela 1: Trajnost podataka

LOKACIJA	METOD ANALIZE	TRAJNOST	OPIS
CPU registri	live	milisekunde	Malo podataka koji nisu preterano korisni za istragu
CPU cache	live	sekunde	Instrukcije i podci koji mogu biti veliki i imati puno informacija
RAM	live	minuti	Informacije o trenutno i prethodno pokrenutim programima i podacima koji ne postoje vise ni na jednom drugom mestu
Disk cache	live/offline	sati	Predstavlja proširenje RAM-a kada se tamo nadje velika količina podataka, a koji se brišu ako se računar isključi, ovo je jedno od mesta u kome se mogu naći podaci vezani za istragu.
Temporary files	live/offline	sati	Sadrži podatke koje mnoge aplikacije, pisane za windows, kreiraju bez znanja korisnika, a čiji fajlovi predstavljaju bitne podatke za istragu.
Unallocated space	offline	dani	To je bilo koja lokacija koja trenutno nema pokazivač na fajlu, i ovde se mogu nalaziti delovi i celi fajlovi koji su ranije postojali, ali su izbrisani.
Permanent files	offline	godine	Ovo su stalni fajlovi, koji se ne gube ukoliko dodje do prestanka napajanja oni će biti dostupni dok ne budu izbrisani ili ne dodje do gubljenja medija

4. STANDARDIZOVANO PRIKUPLJANJE PODATAKA

Veoma je važno poznavati određene standarde i poštovati ih prilikom prikupljanja potencijalnih dokaza. Dva standarda, koja su kreirana od strane IETF grupe i direktno veza baza digitalnu forenziku, su RFC2828[5] i RFC3227 [6]. Prvi standard se odnosi na 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.

Prvo se prikupljaju dokaz koji su najćešće promenljivi, a zatim oni koji to nisu. Sledi 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)

4.1. Predlog redosleda prikupljanja podataka

Na osnovu tabele 1, kao i na osnovu datog primera u RFC3227 [6], predlaže se sledeći redosled prikupljanja podataka sa računara putem metodologije aktivnog odgovora. Akoji je nastao na osnovu analize velikog broja izveštaja koji generišu razni programi za digitalnu forenziku (FTK, EnCase...).

- Sistem 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
- Deljeni mrežni direktorijumi

5. HIBRIDNA METODOLOGIJA AKTIVNOG ODGOVORA

Za razliku od lokalnne, u udaljene metode, gde je bitno da li digitalni forenzičar ima ili nema fizički pristup računaru, sa kojeg se podaci prikupljaju i na osnovu toga se primenjuje jedna ili druga metoda, za hibridnu metodu nije od presudnog značaja da li digitalni forenzičar ima ili nema fizički pristup računaru sa kojeg je potrebno prikupiti podatke.

Kod ove metode postoje dva BATCH fajla koji se koriste u kombinaciji da bi se prikupljali potrebii podaci sa minimalnim izmenama na ciljnom sistemu.

Prvi fajl je **batchserver.bat** koga je potrebno pokrenuti na računaru forenzičara.

Listing 1 – Serverski fajl batchserver.bat

```
if_nc -v -l -p 1000 > date.log
if_nc -v -l -p 1001 > time.log
if_nc -v -l -p 1002 > netstat_ano.log
if_nc -v -l -p 1003 > fport.log
if_nc -v -l -p 1004 > openports.log
if_nc -v -l -p 1005 > nbtstat_c.log
if_nc -v -l -p 1006 > ipconfig_all.log
if_nc -v -l -p 1007 > promisc.log
if_nc -v -l -p 1008 > promqry.log
if_nc -v -l -p 1009 > nestat_rn.log
if_nc -v -l -p 1010 > psloggedon.log
if_nc -v -l -p 1011 > logonsessions.log
if_nc -v -l -p 1012 > pslist.log
if_nc -v -l -p 1013 > listdlls.log
if_nc -v -l -p 1014 > handle.log
if_nc -v -l -p 1015 > svc.log
if_nc -v -l -p 1016 > psservice.log
if_nc -v -l -p 1017 > psfile.log
if_nc -v -l -p 1018 > userdump.log
if_nc -v -l -p 1019 > memory.dd
if_nc -v -l -p 1020 > clipboard.log
if_nc -v -l -p 1021 > doskey_history.log
if_nc -v -l -p 1022 > shedule_job.log
if_nc -v -l -p 1023 > psinfo.log
if_nc -v -l -p 1024 > drives.log
if_nc -v -l -p 1025 > share.log
```

Drugi fajl je **batchclient.bat**, koji se pokreće na računaru i sa kojeg se prikupljaju podaci ali, obavezno, tek posle njegovog pokretanja na računaru forenzičara.

Listing 2– Klijentski fajl batchclient.bat

```
date /t | if_nc %1 1000 -w 1
time /t | if_nc %1 1001 -w 1
netstat -ano | if_nc %1 1002 -w 3
if_fport.exe | if_nc %1 1003 -w 2
if_openports.exe | if_nc %1 1004 -w 2
nbtstat -c | if_nc %1 1005 -w 2
ipconfig /all | if_nc %1 1006 -w 2
if_promiscdetect.exe | if_nc %1 1007 -w 2
if_promqry.exe | if_nc %1 1008 -w 2
netstat -rn | if_nc %1 1009 -w 2
if_psloggedon.exe | if_nc %1 1010 -w 2
if_logonsessions.exe | if_nc %1 1011 -w 2
if_pslist.exe | if_nc %1 1012 -w 3
if_listdlls.exe | if_nc %1 1013 -w 10
if_handle.exe | if_nc %1 1014 -w 3
if_svc.exe | if_nc %1 1015 -w 3
if_psservice.exe | if_nc %1 1016 -w 5
if_psfile.exe | if_nc %1 1017 -w 3
if_userdump.exe | if_nc %1 1018 -w 2
if_mdd.exe -o | if_nc %1 1019 -w 45
if_pclip > | if_nc %1 1020 -w 3
doskey /history | if_nc %1 1021 -w 1
at | if_nc %1 1022 -w 1
if_psinfo | if_nc %1 1023 -w 3
if_di.exe | if_nc %1 1024 -w 1
if_share.exe | if_nc %1 1025 -w 1
```

Prilikom pokretanja klijentskog fajla potrebno je navesti IP adresu računara forenzičara na kojem je pokrenut serverski fajl, i sve prikupljene podatkeposlati putem mreže, do računara digitalnog forenzičara (na laptop ili u forenzičku laboratoriju). Kao što se može videti, u ovom fajlu, većina komandi je iz sistema SysInternals [7], zatim sistema Fport Foundstones [8] a ima i generičkih (windows) komandi koje su sastavni deo operativnog sistema.

Prilikom korišćenja ove metode mogu se lako i brzo prrenositi podaci na računar forenzičara, a jedini problem može biti pri tome što je za neke elemente neophodno posedovati administratorske privilegije na računaru sa kojeg seuzimaju podaci. Takođe važno je da forenzičar koristi BATCH fajlove kako bi automatizovao i ubrzao proces prikupljanja podataka. Tabela 1 pokazuje da su neki podaci, prisutni u sistemu, dostupni za manje od jedne sekunde.

6. PRIMENA NA MS (WINDOWS) OPERATIVNIM SISTEMIMA

Zapotrebeovogradaizvršeno je testiranje batch fajlovanarazličitim (windows) sistemima (Win XP sp1, Win XP sp3, Win 2003 server, VISTA, Windows 7) i dobijen isuprilližnoistirezultati, štoznači da je ovajfajlprimenljivnasvim gore navedenim MS operativnimnačinimarada.

6.1. Windows XP

Pošto je ovo i dalje najčešće korišćeni operativni sistem, testiranje ju ovom radu je započeto baš na njemu. Instaliran je čist operativni sistem, a zatim su na njega instalirani svi standardni programi, koji se koriste u svakodnevnoj upotrebi, i pušten 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.

Prikupljen je, takođe, i kompletan sadržaj radne memorije, na računaru za testiranje, veličine 512 MB. Od posebnog je značaja istaći da forenzičar treba da ima administratorski nalog kako bi mogao u potpunosti prikupiti podatke. Pretestiranja,završena je, prekoadministratorskognaloga, i prikupljenisupotrebnipodaci,kaošto se moževidetinaslici 2 .Poštopostojerazličitevarijante Win XP sistema u zavisnostiodinstaliranog Service Pack-a, istifajl je pušten u sistemsa SP1 i SP3 i donjenirezultatisuidentični, štoznači da je fajlkreirantako da se bezproblemamožekoristinasvakom Win XP sistemu.

Slika 1,2: MS Windows XP – pokretanje

6.2 Win 2003 Server

Pošto Win 2003 i Win XP dele sličnu arhitekturu, izvršeno je i testiranje na ovom operativnom sistemu, koji se vrlo često koeristi u poslovanju. Instaliran je čist operativni sistem, a zatim su na njega instalirani svi standardni programi,za svakodnevnu upotrebu, i puštanje batch fajl koji je izvršen bez greške. Kao što se i očekivalo, testiranje je pokazalo da je batch fajl prošao bez problema i na taj način su kreirani fajlovi pokazali trenutno stanje sistema, odnosno njegovu sliku bezbednosnog aspekta.

Slika 3,4: MS Windows Server 2003 – pokretanje

Jedini problem koji se pojavio na ovom sistemu je program Fport koji nije mogao da se izvrši. Za testiranje 512MB prikupljen je, takođe i kompletan sadržaj radne memorije, i ono je izvršeno na čistom, tek instaliranom sistemu bez dodatnih programa i sa SP1 (Service Pack 1).

6.3 VISTA i Windows 7

S obzirom da na tržištu operativnih sistema postoje i ovi sistemi, koji trenutno još uvek nisu aktuelni, ali se očekuje njihova ekspanzija, izvršeni su testovi i na njima. Oni dele skoro identičnu arhitekturu i rezultati su potpuno identični. Instalacija čistog operativni sistem,na njemu su postavljenistandardni programi koji su u svakodnevnoj upotrebi, pušten je batch fajl i test je obaljen bez greške.

Testiranje je pokazalo da je batch fajl prošao bez problema i kreirani fajlovi, na računaru forenzičara, su pokazali trenutno stanje sistema, odnosno njegovu sliku sa bezbednosnog aspekta. Jedini nedostatak ovakvog proveravanja je bio u programu mdd1.3, koji nije mogao da isčita trenutno stanje radne memorije od 2GBb i da to upiše u fajl.

Slike 5; 6: Pokretanje MS Windows Vista i Windows 7 operativnih sistema

Pokazalo se još da je na ovim sistemima došlo do povećane kontrole korisnika. Međutim, ukoliko korisnik nema administratorski nalog, možeprikupiti samo elementarne podatke, koji, možda,nisu dovoljni za dalju istragu (tabela 2). Ovo stanje je prikazano u tabeli 3 i ako sedetaljno amačizra, može se videti da 7 različitih fajlova ne može da se izvrši ako korisnik nije imao administratorsku privilegije na sistemu.

Tabela 2: Izvršene komande sa admin privilegijama

ADMIN PRIVILEGES	Win XP SP1	Win XP SP3	Win 2003 Server	VISTA	Windows 7
date	x	x	x	x	x
time	x	x	x	x	x
netstat -ano	x	x	x	x	x
fport	x	x			
openports	x	x	x	x	x
nbtstat -c	x	x	x	x	x
ipconfig /all	x	x	x	x	x
promiscdetect	x	x	x	x	x

- nastavak na sledećoj strani -

ADMIN PRIVILEGES	Win XP SP1	Win XP SP3	Win 2003 Server	VISTA	Windows 7
promqry			x	x	x
netstat -rn	x	x	x	x	x
psloggedon	x	x	x	x	x
logonsessions	x	x	x	x	x
pslist	x	x	x	x	x
listdlls	x	x	x	x	x
handle	x	x	x	x	x
svc	x	x	x	x	x
psservice	x	x	x	x	x
psfile	x	x	x	x	x
userdump	x	x	x	x	x
mdd	x	x	x		
pclip	x	x	x	x	x
doskey /history	x	x	x	x	x
at	x	x	x	x	x
psinfo	x	x	x	x	x
di	x	x	x	x	x
share	x	x	x	x	x

Tabela 3: Izvršenekomandebez admin privilegija

NON ADMIN PRIVILEGES	Win XP SP1	Win XP SP3	Win 2003 Server	VISTA	Windows 7
date	x	x	x	x	x
time	x	x	x	x	x
netstat -ano	x	x	x	x	x
fport	x	x			
openports	x	x	x	x	x
nbtstat -c			x	x	x
ipconfig /all	x	x	x	x	x
promiscdetect	x	x	x	x	x
promqry			x	x	x
netstat -rn	x	x	x	x	x
psloggedon	x	x	x	x	x
logonsessions					
pslist	x	x	x	x	x
listdlls					
handle					
svc	x	x	x	x	x
psservice	x	x	x	x	x
psfile					
userdump	x	x	x	x	x
mdd					
pclip	x	x	x	x	x
doskey /history	x	x	x	x	x
at					
psinfo	x	x	x	x	x
di	x	x	x	x	x
share	x	x	x	x	x

ZAKLJUČAK

Ovde su dati osnovni faktori, koji mogu uticati na uspešnost sakupljanja podataka, za potrebe forenzičke analize. Korišćeni su aktuelni standardi, a za osnovu je uzet RFC 3227 dokument. Za fokus rada postavljena je metodologija *hibridnog aktivnog direktorijuma*, koja treba da omogući uspešno sakupljanje podataka, sa aktivnih računarskih sistema, iparalelno s timobavlja i svoje standardne zadatke. Ova metodologija, takođe omogućava pristup određenom skupu podataka kojima nije moguče pristupiti na drugi način osim onog, koji podrazumeva prikupljanje podataka posle isključivanja računarskih sistema.

Za osnovni smisao ovog rada može se uzeti primena metodologije *hibridnog aktivnog odgovora* na realnim, trenutno aktuelnim operativnim sistemima. Ovde su obrađeni MS Windows XP, MS Windows Server 2003, MS Windows Vista, MS Windows 7 operativni sistemi. Svi operativni sistemi su konfigurisani za upotrebu u realnom okruženju.

Na njih su instalirani softverski paketi koji se mogu očekivati na računarima u realnoj upotrebi. Takođe, izvršen je identičan set naredbi za prikupljanje podataka na svim MS operativnim sisitemima.

LITERATURA

[1] Windows Forensic Analysis, Harlan Carvey, Syngress 2007,
[2] Windows Forensics, Chad Steel, Wiley 2006.
[3] http://www.cert.org
[3] Real Digital Forensics, Keith J. Jones, Richard Bejtlich, Curtis W. Rose, Addison Wesley 2006
[4] Windows Forensics, Chad Steel, Wiley 2006
[5] RFC2828: Internet Securicy Glosary
[6] RFC3227: Guidelines for Evidence Collection and Archiving
[7] http://technet.microsoft.com/en-us/sysinternals/default.aspx
[8] www.foundstone.com

AUTORI:

Prof. dr Mladen Veinović
Univerzitet Singidunum,
Danijelova 32, Beograd

email:
mveinovic@singidunum.ac.rs

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

Mr Igor Franc
Univerzitet Singidunum,
Danijelova 32, Beograd

email:
ifranc@singidunum.ac.rs

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