SISTEMATIZOVANO PRIKUPLJANJE PODATAKA SA AKTIVNIH SISTEMA ZA POTREBE FORENZIČKE ANALIZE

Igor Franc
Univerzitet Singidunum
Danijelova 32, Beograd, Srbija
E-mail: ifranc@singidunum.ac.rs

Gojko Grubor
Univerzitet Singidunum
Danijelova 32, Beograd, Srbija
E-mail: ggrubor@singidunum.ac.rs

Sažetak: U slučajevima bezbednosnih incidenata na aktivnim sistemima, pravilno prikupljanje relevantnih podataka može značajno povećati verovatnoću otkrivanja informacija o tome ko je izvršilac napada, odakle je napad izvršen, na koji način je napad izvršen i sl. U okviru RFC 3227 dokumenata od strane IETF grupe date su okvirne ciljne grupe podataka koji se mogu iskoristiti za dobijanje informacija o napadu. Kod nekih izvora se načini prikupljanja potencijalnih dokaza kategoriše i na osnovu tačke sa koje se prikupljanje vrši (lokalna,udaljena i hibridna metoda). U ovom radu se predstavljaju rezultati napora da se postavljeni formalni standardi i metode automatizovano primene na trenutno aktuelne realne i operativne sisteme i okruženja. Dodatno, u radu se pored pribavljanja potencijalnih dokaza sakupljaju i informacije o stanju sistema posle napada.

Ključne reči: aktivni odgovor, akvizicija aktivnog sistema, *batch* obrada, otvoreni kod, SLA, WDE, RAID, RFC3227, *Locardov* princip razmene, NetCat.

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 [7] kaže da u svakoj interakciji dva objekta dolazi do određene razmene, odnosno, promene stanja objekata učesnika.

Evo nekoliko primera za to:

- Temperaturu vode nikada nije moguće tačno izmeriti jer bi za tako nešto bilo merenje vršiti toplomerom čija je temperatura ista kao i temperatura vode. U protivnom, samim postavljanjem toplomera (čija se temperatura razlikuje) u vodu dolazi do razmene, odnosno, promene temperatura vode i toplomera.
- 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
- Ako dva računara na neki način razmenjuju podatka odnosno komuniciraju putem mreže u RAM memoriji jednog računara naći će se IP adresa drugog

računara i obrnuto, u RAM memoriji drugog računara naći će se IP adresa onog prvog

Primenom *Lokardovog* principa 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 minimalne 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.

2. AKTIVNI ODGOVOR I AKVIZICIJA AKTIVNOG SISTEMA

Jedan od izražajnijih 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. *Akvizicija aktivnog sistema (Live acquisition)*

Pristup *aktivnog odgovora* na kompjuterski incident 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 kontekstualnih podataka aktivnog sistema, relevantnih za potrebe forenzičke analize. Nasuprot pristupa *aktivnog odgovora,* pristup *akvizicije aktivnog sistema* podrazumeva pravljenje kompletne kopije spoljne memorije (HD) aktivnog računara. Ovom metodom se, za razliku od metode aktivnog odgovora, ne preuzima kopija radne memorije. Fokus ovog rada je postavljen na metodu aktivnog odgovora dok metoda akvizicije aktivnog sistema izlazi izvan njegovih okvira.

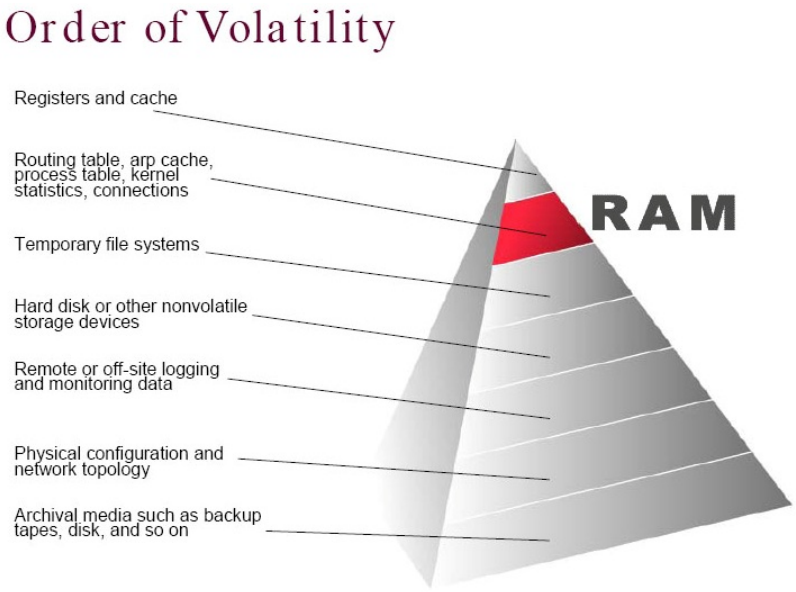
Metoda *aktivnog odgovora* je široko prihvaćena u aktuelnim forenzičkim krugovima i najčešće se koristi u sledećim situacijama:

- na računarskim sistemima vezanim za elektronske novčane transakcije (e-trgovina) 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);
- 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.).

3. TRAJNOST PODATAKA U SISTEMU

Različiti podaci, koji se nalaze u sistemu mogu nam duže ili kraće vreme biti dostupni [3]. Potrebno je napraviti određeni redosled za njihovo prikupljanje kako ne bi bili izgubljeni zbog protoka vremena (slika 1).

Slika 1. Trajnost podatka u sistemu [3]



Sledeća tabela [8] pokazuje trajnost podataka u intervalima, od nekoliko mikrosekundi do nekoliko godina, a može se videti i koji metod analize je primenljiv za njihovo prikupljanje:

LOKACIJA	METOD ANALIZE	TRAJNOST	OPIS
CPU registri	aktivna forenzika	mili-sekunde	Uglavnom sadrži malo podataka koji nisu preterano korisni za istragu
CPU keš	aktivna forenzika	sekunde	Sadrži instrukcije i podatke koji mogu biti veliki i imati puno informacija
RAM	aktivna forenzika	minuti	Sadrži informacije o trenutno i prethodno pokrenutim programima gde se mogu naći podaci koji ne postoje vise ni na jednom drugom mestu
Keš HD	aktivna forenzika/ *offline*	sati	Predstavlja proširenje RAM-a kada se tamo nađe velika količina podataka, bitna stvar je da se oni brišu ako se računar isključi, ovo je jedno od najbitnijih mesta u kome se mogu naći podaci vezani za istragu
Privremeni fajlovi	aktivna forenzika/ *offline*	sati	Sadrži podatke koje mnoge aplikacije pisane za *Windows* kreiraju bez znanja korisnika, a ti fajlovi predstavljaju bitne podatke za istragu
Nealocirani prostor	*offline*	dani	Predstavlja bilo koju lokaciju koja trenutno nema pokazivač na fajl, odnosno ovde se mogu nalaziti delovi i celi fajlovi koji su ranije postojali ali su izbrisani

Permanentni fajlovi	*offline*	godine	Ovo su stalni fajlovi, tj. ne dolazi do njihovog gubljenja ukoliko dođe do prestanka napajanja i oni ce biti dostupni dok god ne budu izbrisani ili ne dođe do gubljenja medija

Tabela 1: Trajnost podataka

4. 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 [5] i RFC3227 [6]. Prvi standard je vezan za opštu bezbednost, a drugi, vrlo bitan za ovaj rad (posebno je vazna 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 oni 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 (*processes table*), statistika kernela (*kernel statistics*);
- Radna memorija (*RAM memory*);
- Privremeni sistemski fajlovi (*temporary system's files*);
- Čvrsti disk (*Hard disk*);
- Udaljeno logovanje i monitorisanje 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 primera koji je dat u RFC3227 [6], 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,
- deljeni mrežni direktorijumi,

5. METODOLOGIJA LOKALNG AKTIVNOG ODGOVORA

Ova metoda se koristi kada digitalni forenzičar ima fizički pristup računaru. Sve prikupljene podatke čuva lokalno, direktno na hard disk ili na izmenjivom medijumu (*thumb drive, USB external drive*), a to zavisi od lokalnih resursa koje ima na raspolaganju. Ukoliko koristi ovu metodu digitalni forenzičar mora imati USB *Flash* ili CD disk sa alatima koje će koristiti tokom prikupljanja podataka.

Prilikom korišćenja ove metode mogu se lako i brzo prikupiti podaci pod uslovom da forenzičar ima fizički pristup sistemu, kao i da ima administratorske privilegije. Za ovu metodu, takođe, je važno 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.

5.1. BATCH fajl za lokalno prikupljane podataka

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 na kome se izvršava, ovaj fajl će prikupiti potencijalne dokaze koje će dalje digitalni forenzičari moći da obrađuju i na taj način utvrde ko je, odakle i šta uradio na aktivnom sistemu bez potrebe za isključivanjem istog.

```
md %1\reportsl
date /t > %1\reportsl\date.log
time /t > %1\reportsl\time.log
netstat -ano > %1\reportsl\netstat_ano.log
fport.exe > %1\reportsl\fport.log
openports.exe > %1\reportsl\openports.log
nbtstat -c > %1\reportsl\nbtstat_c.log
ipconfig /all > %1\reportsl\ipconfig_all.log
promiscdetect.exe > %1\reportsl\promisc.log
promqry.exe > %1\reportsl\promqry.log
netstat -rn > %1\reportsl\nestat_rn.log
psloggedon.exe > %1\reportsl\psloggedon.log
logonsessions.exe > %1\reportsl\logonsessions.log
pslist.exe > %1\reportsl\pslist.log
listdlls.exe > %1\reportsl\listdlls.log
handle.exe > %1\reportsl\handle.log
svc.exe > %1\reportsl\svc.log
```

```
psservice.exe > %1\reportsl\psservice.log
psfile.exe > %1\reportsl\psfile.log
userdump.exe > %1\reportsl\userdump.log
mdd.exe -o %1\reportsl\memory.dd
pclip > %1\reportsl\clipboard.log
doskey /history > %1\reportsl\doskey_history.log
at > %1\reportsl\shedule_job.log
psinfo –h -s -d > %1\reportsl\psinfo.log
di.exe > %1\reportsl\drives.log
share.exe > %1\reportsl\share.log
```

Listing 1. - Batch fajl za prikupljanje podataka na MS Windows operativnim sistemima.

Kao što se može videti u ovom fajlu većina komandi je iz *SysInternals* [2], zatim *Fport* iz *Foundstones* [4] a ima i generičkih Windows komandi koji su sastavni deo operativnog sistema.

6. METODOLOGIJA UDALJENOG AKTIVNOG ODGOVORA

Ova metoda se koristi kada digitalni forenzičar nema fizički pristup računaru. Podaci se prikupljaju 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.

6.1. *Batch* fajl za udaljeno prikupljane podataka

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 > reportsr\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
```

Listing 2. - *batch* fajla za udaljeno prikupljanje

Kao što se vidi u ovom fajlu, većina komandi je iz *SysInternals*-a [1], *Fport* je iz *Foundstones*-a [2], 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:

- IP adresu računara na koji se šalju padaci - %1
- Korisničko ime (*user name*)– 2%
- Lozinku (*password*) – 3%

7. HIBRIDNA LIVE RESPONSE METODOLOGIJA

Za razliku od lokalne i udaljene metode gde je vrlo bitno da li digitalni forenzičar ima ili nema fizički pristup računari sa koja se podaci prikupljaju i na osnovu toga se može primeniti ili jedna ili druga metoda, za hibridnu metodu nije od presudnog značaja da li digitalni forenzičar ima ili nema fizički pristup računaru sa kog je potrebno prikupiti podatke.

Kod ove metode postoje dva BATCH fajla koja se koriste u kombinaciji i na taj način se prikupljaju potrebni podaci sa minimalnim izmenama na ciljnom sistemu.

7.1. BATCH serverski fajl za hibridno prikupljanje podataka

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

```
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
```

Listing 3. – Serverski fajl batchserver.bat

7.2. BATCH klijentski fajl za hibridno prikupljanje podataka

Drugi fajl je **batchclient.bat** koji se pokreće na računaru sa koga se prikupljaju podaci ali obavezno tek posle pokretanja fajla batchserver.bat na računaru forenzičara.

```
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
```

Listing 4. – Klijentski fajl batchclient.bat

Prilikom pokretanja klijentskog fajla potrebno je navesti IP adresu računara forenzičara na kojem je pokrenut serverski fajl i na taj način se svi prikupljeni podaci šalju putem mreže do računara digitalnog forenzičara (laptop ili u forenzičku laboratoriju). Kao što se može

videti u ovom fajlu većina komandi je iz *SysInternals* [2], zatim *Fport* iz *Foundstones* [4] a ima i generičkih Windows komandi koji su sastavni deo operativnog sistema

Prilikom korišćenja ove metode mogu se lako i brzo prikupiti podaci i preneti na računar forenzičara, jedini problem može biti to što za neke elementi je neophodno posedovati administratorske privilegije na računaru sa koga se prikupljaju podaci. Za ovu metodu, takođe, je važno 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.

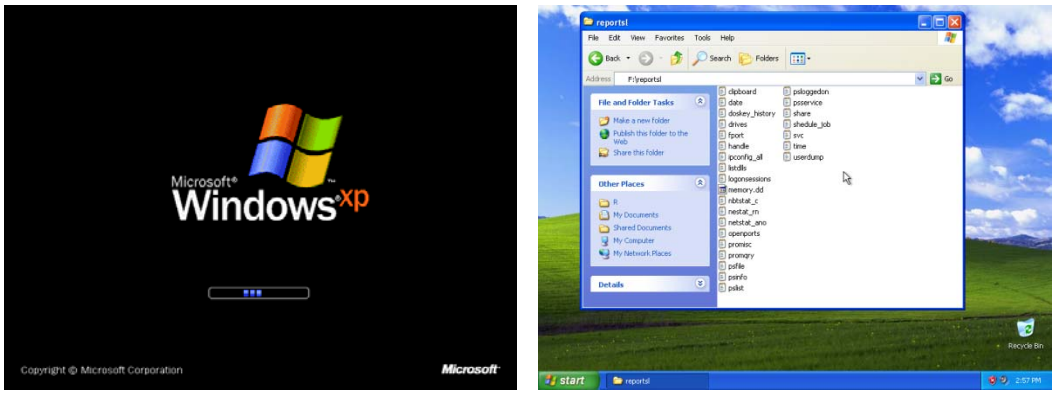
8. PRIMENA NA MS WINDOWS OPERATIVNIM SISTEMIMA

Za potrebe ovog rada izvršeno je testiranje svih *batch* fajlova 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 su ovi fajlovi primenljivi na svim dole navedenim MS operativnim sistemima.

8.1. Windows XP

Pošto je ovo i dalje najčešće korišćeni operativni sistem, testiranje je započeto baš na njemu. Instaliran je čist operativni sistem na virtuelnoj masini WMVare Workstation 6.5 sa standardnim programima koji se najčešče koriste na njemu su testirani svi *batch* fajlovi koji su izvršeni bez greške. Na taj način su kreirani fajlovi koji pokazuju kakvo je trenutno stanje sistema, odnosno kakva je njegova slika sa bezbednosnog aspekta.

Slika 2. MS Windows XP – pokretanje i rezultati



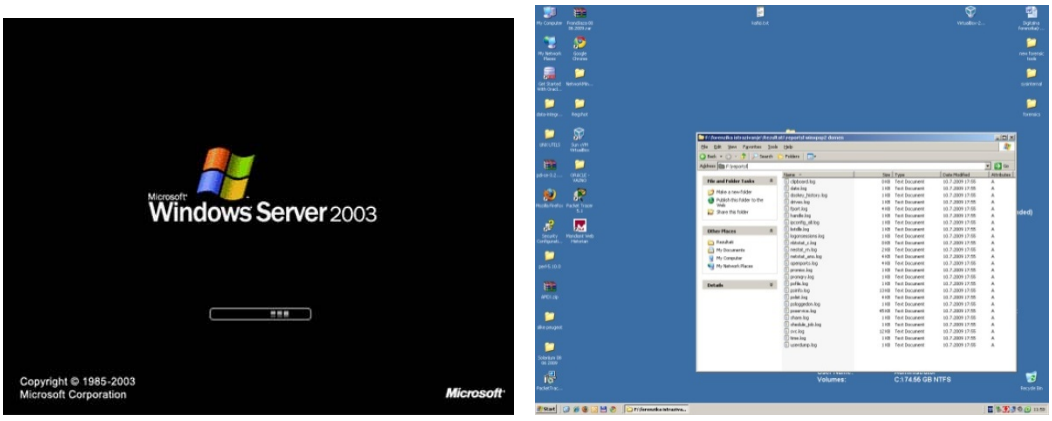
Takođe, prikupljen je i kompletan sadržaj radne memorije, na računaru za testiranje, veličine 512 MB. Od posebnog je značaja istaći da forenzičar mora imati administratorski nalog kako bi mogao u potpunosti prikupiti podatke.

Prilikom testiranja, skripta je izvršena preko administratorskog naloga i prikupljeni su potrebni podaci kao što se može videti na slici 2. 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.

8.2. Win 2003 Server

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

Slika 3. MS Windows Server 2003 – pokretanje i rezultati



Jedini problem koji se pojavio sa ovim sistemom jeste sa programom *Fport* koji nije mogao da se izvrši. Takođe prikupljen je i kompletan sadržaj radne memorije koji je na ovom računaru za testiranje 512MB. Testiranje je izvršeno na čistom, tek instaliranom Windows 2003 sistemu koji je instaliran kao virtuelna mašina u programu *WMVare* Workstation 6.5 sa standardnim programima koji se najčešće koriste i sa instaliranim SP1 (*Service Pack* 1). Rezultati sa kreiranim fajlovima dati su na slici 3.

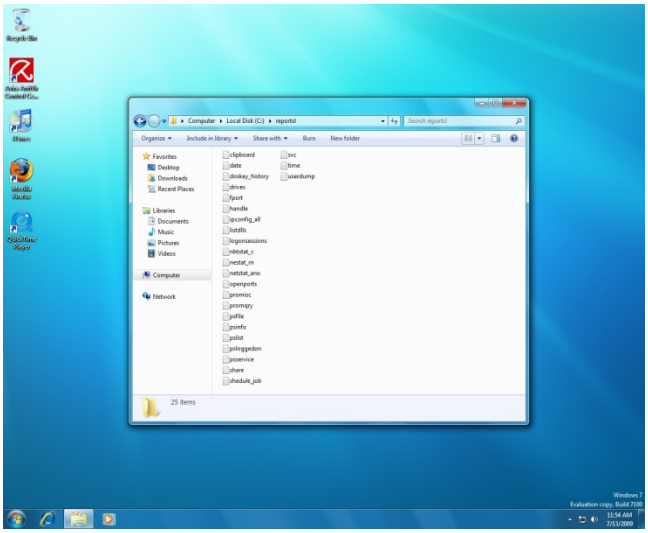
8.3. VISTA i Windows 7

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 ova dva sistema. Oni dele skoro identičnu arhitekturu tako da su rezultati potpuno identični. Testiranje je izvršeno na čistom, tek instaliranom sistemu Windows 7 Profesional i VISTA SP1 koji su instalirani kao virtuelna mašina u programu WMVare Workstation 6.5 sa standardnim programima koji se najčešće koriste (slika 4).

Slika 4. Pokretanje MS Windows Vista i Windows 7 operativnih sistema

Testiranje je i u ovom slučaju pokazalo da su svi *batch* fajlovi prošli bez problema i na taj način su kreirani fajlovi pokazali kakvo je trenutno stanje sistema, odnosno njegova slika sa bezbednosnog aspekta. Jedini problem koji se ovde pojavio jeste sa programom mdd1.3, koji nije mogao da isčita trenutno stanje radne memorije od 2GBb i da to upiše u fajl. Rezultati su dati na slici 5.

Slika 5. Windows 7 – rezultati procesa prikupljanja podataka



Testiranje je pokazalo da je na ovim sistemima došlo do povećane kontrole korisnika. Međutim ukoliko korisnik nema administratorski nalog, moći će da prikupi samo elementarne podatke koji možda neće biti dovoljni za dalju istragu. Ova situacija je prikazana u tabelama 2 i 3. Ako detaljno pogledamo tabelu može se videti da 7 različitih fajlova nije moglo da se izvrši ukoliko korisnik nije imao administratorske privilegije na sistemu.

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
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 2: Izvršene komande sa admin privilegijama

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

Tabela 3: Izvršene komande bez admin privilegija

9. IZBOR ADEKVATNE METODE ZA PRIKUPLJANE PODATAKA SA AKTIVNIH SISTEMA

U radu su prikazane sve tri metode prikupljana podataka sa živih sistema za potrebe dalje forenzičke analize. Kao ključni faktor prilikom izbora metode za prikupljane podatka potrebno je uzeti to da li postoji fizički pristup računaru sa koga je potrebno prikupiti podatke, zatim koliko je potrebno brzo prikupiti podataka kao i to o kolikoj se količini podataka radi jer propusni opseg mreže može onemogućiti prenošenje veće količine podataka od na primer nekoliko GB.

U sledećoj tabeli date su karakteristike svakog od tri metoda za prikupljane podataka

	lokalna metoda (*local response*)	udaljena metoda (*remote response*)	hibridna metoda (*hybrid response*)
fizički pristup	da	ne	da (lice od poverenja)
brzina prenosa	da	ne	ne
količina podataka	da	ne	ne

Tabela 4 – Karakteristike metoda za prikupljanje podataka

Kao što se u prethodnoj tabeli može videti najpogodniji način za prikupljanje podataka jeste lokalna metoda i nju je poželjno koristiti uvek kada je to moguće iz razloga što je najbrža i ne postoji ograničenje u količini podataka koje je potrebno prikupiti. Udaljenu metodu je neophodno koristiti u situaciji kada ne postoji nikakav fizički pristup računaru sa koga je potrebno prikupiti podatke u razumnom vremenskom roku, potrebno je samo na neki način saznati korisničko ime i šifru nekog korisnika tog računara (poželjno je da to bude nalog sa admin privilegijama). I na kraju hibridna metoda se koristi onda kada iz nekog razloga nije moguće udaljeno se konektovati na računar sa koga se podaci prikupljaju zbog nekih sigurnosnih mehanizama koji onemogućavaju taj proces i tada je potrebno da postoji lice od poverenja koje će uključiti USB disk ili ubaciti CD sa BATCH fajlom i pokrenuti ga dok ce se sve ostalo vršiti automatski i podaci će se prenositi putem mreže, ovde jedino ograničenje može biti brzina mreže za prenos podataka kao i količina podataka koje je potrebno preneti.

10. ZAKLJUČAK

U ovom radu predstavljeni su osnovni faktori koji imaju uticaj na uspešnost sakupljanja podataka za potrebe forenzičke analize. Korišćeni su trenutno aktuelni standardi a kao osnova uzet je RFC 3227 dokument. Kao osnovni fokus rada postavljena je metodologija aktivnog odgovora (*live response),* 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.

Kao osnovni doprinos ovog rada može se uzeti primena metodologije aktivnog odgovora na realnim, trenutno aktuelnim operativnim sistemima kao i uporedni prikaz sve tri metode prikupljana podataka sa živih sistema za potrebe forenzičke analize. U radu 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, odnosno, na njih su instalirani softverski paketi koji se mogu očekivati na računarima u realnoj upotrebi. Takođe, na svim MS operativnim sistemima izvršen je identičan set naredbi za prikupljanje podataka. U radu se nalaze i kompletni listinzi *Batch* fajlova za sve tri metode za prikupljanje podataka, a date su i karakteristike svake od tri metode u tabeli i dati su i faktori koje je potrebno uzeti u obzir prilikom izbora metode za prikupljanje podataka.

11. Literatura

[1] Computer Forensics and Investigations Third Edition, Bill Nelson, Amelia Phillips, Frank Enfinger, Christopher Steuart, Thomson 2008

[2] http://technet.microsoft.com/en-us/sysinternals/default.aspx

[3] http://www.cert.org

[4] http://www.foundstone.com

[5] RFC2828 – Internet Security Glossary

[6] RFC3227 - Guidelines for Evidence Collection and Archiving

[7] Windows Forensic Analysis, Harlan Carvey, Syngress 2007.

[8] Windows Forensics, Chad Steel, Wiley 2006.

METHODICAL DATA COLLECTING FOR FORENSIC ANALYSIS PURPOSE FROM LIVE SYSTEMS

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. In the RFC 3227 of the IETF group of the framework are the target group of data that can be used to obtain information about the attack. For some sources of the potential ways of collecting evidence and rank on the basis of points which made the collection of (local, remote and hibryd methods). 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.*

Keywords: *Live response, live acquisition, batch, open source, SLA, WDE, RAID, RFC3227, LOCARD'S EXCHANGE PRINCIPLE, NetCat*