Računalna forenzika

Sirovica, Vlatko

Undergraduate thesis / Završni rad

2022

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Rijeka / Sveučilište u Rijeci**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:195:908722

Sveučilište u Rijeci – Fakultet informatike i digitalnih tehnologija

Preddiplomski jednopredmetni studij informatike

Vlatko Sirovica

Računalna forenzika

Završni rad

Mentor: izv. prof. dr. sc. Božidar Kovačić

Rijeka, kolovoz 2022.

Sadržaj

Zadatak završnog rada

FAKULTET INFORMATIKE I DIGITALNIH TEHNOLOGIJA
SVEUČILIŠTE U RIJECI

Rijeka, datum

Zadatak za završni rad

Pristupnik: Vlatko Sirovica

Naziv završnog rada: Računalna forenzika

Naziv završnog rada na eng. jeziku: Computer forensics

Sadržaj zadatka:

Računalna forenzika je znanost koja se bavi sakupljanjem, pretraživanjem, analizom i prezentacijom podataka. Nakon opisa vrsta računalnih kriminala, potrebno je definirati pojam sigurnosnog incidenta, a zatim slijedi opis vrsta računalne forenzike. Na kraju je potrebno opisati forenzičku istragu.

Mentor

dr.sc. Božidar Kovačić

Voditelj za završne radove

Doc. dr. sc. Miran Pobar

Zadatak preuzet: 05.05.2021.

Vlatko Sirovica

(potpis pristupnika)

1. Uvod

U današnje vrijeme računalne mreže su raširene toliko da su sveprisutne u našim životima i zapravo ovisimo o njima. S razvitkom računalnih mreža razvio se i novi oblik kriminala, a to je računalni kriminal. Računalne mreže su toliko ranjive i nesigurne zbog sve većeg broja korisnika. Stručnjaci govore kako je ovo najbrže rastuća prijetnja jer u ovoj novoj vrsti kriminala dolazi do sve više inovativnih vrsta napada na korisnike računalnih mreža. Kako bi se otkrili i sankcionirali napadači potreban je razvoj stručnjaka koji će računalnom forenzikom neprekidno analizirati takvu vrstu kriminala i onda na temelju analize represivno djelovati na napadače.

Kad ljudi čuju za riječ forenzika neki će odmah pomisliti na televizijsku seriju CSI. Ali što je zapravo forenzika? Forenzika je općenito primjena znanstvenih metoda u kriminalističkoj istrazi. To je jedinstveno polje studija koje prolazi kroz sva područja znanosti od entomologije do genetike preko geologije do matematike sve uz jedinstveni cilj, a to je rješavanje misterija.

Računalna forenzika proučava kako su računala uključena u nastanak zločina. U slučajevima koji uključuju računovodstvene prijevare, ucjene, krađu identiteta… U okviru računalne sigurnosti forenzika se odnosi na procese kojima se identificiraju računalni ili digitalni dokazi te se oni onda čuvaju, analiziraju, tumače i prezentiraju. Povijest nam pokazuje kako situacije koje uključuju ljude i novac brzo privlače kriminal. Takav je slučaj i s Internetom. Nažalost, temeljni protokoli koji upravljaju internetskim prometom nisu dizajnirani za rješavanje problema neželjene pošte, virusa i tako dalje. Internetska forenzika prebacuje fokus s pojedinačnog stroja na Internet u cjelini. Uz jednu masivnu mrežu koja se proteže cijelim svijetom izazov identificiranja kriminalnih aktivnosti i ljudi koji stoje iza njih postaje ogroman. Često je nemoguće provjeriti izvor poruke ili kreatora web stranice. U tim slučajevima sitni detalji postaju važni. Tada raspored datoteka na web stranici ili način na koji su krivotvorena zaglavlja e-pošte mogu odigrati istu ulogu kao otisak prsta na mjestu zločina.

Ovaj završni rad podijeljen je na 4 poglavlja. U prvom poglavlju opisati će se i navesti vrste računalnog kriminala. Drugo poglavlje opisuje incidente i kako oni nastaju. U trećem poglavlju navesti će se i opisati tipovi računalne forenzike. Četvrto poglavlje prikazat će način istrage i tehnike rada forenzike.

2. Vrste računalnog kriminala

U ovom poglavlju opisati će se vrste računalnog kriminala koje najčešće predstavljaju opasnost za korisnika računala i nude potencijal za rad računalnog forenzičara. Također opisati će se vrsta napadača odnosno kriminalaca koje računalni forenzičari nastoje ili su ih već otkrili.

2.1. Hakiranje

Hakiranje kao jedna od najpoznatijih vrsta računalnog kriminala predstavlja aktivnost kojom individualno ili grupno se neovlašteno pristupa računalnom sustavu s ciljem dobivanja nezakonitog pristupa podacima i informacijama pohranjenima na napadnutom računalnom sustavu. Takve pojedince koji izvode takve napade ljudi nazivaju hakerima, ali zapravo te osobe se nazivaju krekeri (crackeri). Njima su prethodili tzv. frikeri koji su u šezdesetim godinama prošlog stoljeća preko zviždaljke koja stvara zvuk od 2600 Hz i puhanja u slušalicu pronašli način za besplatno korištenje telefonskih usluga. Pojam hakiranja javlja se u šezdesetim godinama prošlog stoljeća gdje su studenti sa sveučilišta MIT izrađivali programske prečace kako bi nešto na brži i jednostavniji način riješili. U to vrijeme tehnologija nije bila toliko razvijena stoga i nije bilo toliko mogućnosti kako bi netko svoje intelektualne sposobnosti iskoristio na nezakonit način. Hakere su prije smatrali osobama koje znaju puno o računalima. To je bilo tako sve dok u osamdesetim godinama prošlog stoljeća nisu krenuli uključivati script kiddies-e među hakere. Script kiddies-i su osobe koje upadaju u tuđe računalne sustave koristeći softvere trećih strana za koje su slabo znali na koji način rade. Od tada se riječ haker koristi s dva značenja. S obzirom na motive razlikuju se hakeri i krekeri. Hakeri su zapravo osobe koje iz znatiželje upadaju u tuđe računalne sustave bez namjere nanijeti štetu dok su krekeri osobe s većim stupnjem znanja koje svjesno provaljujući u računalne sustave pokušavaju izvući u većini slučajeva vlastitu korist i nanijeti štetu. Njihovom napadu su izloženi svi i sebe smatraju superiornijima od ostale populacije što se tiče inteligencije. Krekere dijelimo na bijele, crne i sive. Bijeli su osobe koje na temelju svog znanja testiraju i poboljšavaju softver u suradnji s proizvođačima softvera. Crni su kriminalci koji s namjerom uništavaju računalne sustave. Sivi su zapravo kombinacija crnih i bijeli pa ih se može nazvati špijunima [1].

2.1.1. Najpoznatiji hakeri

Za početak hakerstva se navodi 1969. godina kad su Dennis Ritchie i Ken Thompson napisali prvu verziju UNIX otvorenog operativnog sustava za mikroračunala. Njih se smatra prvim hakerskim dvojcem. Također vrijedno je navesti Richarda Stallmana koji je napravio GNU operativni sustav i Linusa Torvaldsa koji je izradio operativni sustav LINUX. Važno je napomenuti kako za razliku od ostalih koji će biti navedeni u ovom poglavlju ovi ljudi zaslužuju sve pohvale jer su ovim podhvatima iskoristili svoje sposobnosti i znanje za ostvarenje povijesnih prekretnica u računalnoj tehnologiji. Hakersko znanje se počelo zloupotrebljavati već sedamdesetih godina prošlog stoljeća kad je John Draper otkrio mogućnost besplatnog telefoniranja na telefonskoj govornici. Abbie Hoffman je zajedno s njim stvorio bibliju o načinu dobivanja besplatnih telefonskih usluga. S tehnologijom se usporedno razvijala i mogućnost hakera. Već u osamdesetim godinama prošlog stoljeća došlo je i do prvih hakerskih ratova i hakerskih grupa. Prva grupa sa eltinim hakerskim genijalcima bila je „Legion of Doom“, a među njima je bio i Mark Abene pod nazivamo Phiber Optik koji je nakon nesuglasica s vođom osnovao svoju grupu „Masters of Deception“ koja se sukobljavala s prvom navedenom. Dvogodišnji rat završio je nakon što su bili otkriveni i privedeni. Ali oni nisu prvi koji su završili iza rešetaka zbog hakiranja. Prvi optuženi haker je bio Robert Morris koji je napravio Internet crva 1988. S Internet crvom zarazio je i srušio preko 6000 računala. Kevin Mitnick je prvi haker koji je završio na FBI-evoj tjeralici „Most Wanted“ 1995. godine jer je ukrao 20000 brojeva kreditnih kartica. Prije toga je 1990. optužen na godinu dana zatvora jer je provalio u računalnu mrežu Digital Equipmenta. No, nisu samo u SAD-u zbog hakerskih aktivnosti bili na radaru vlasti. Ruski haker Vladimir Levin je 1994. provalio u računalo CitiBank-a i ukrao 10 milijuna dolara. Iduće godine ga je uhitio Interpol u Londonu [1].

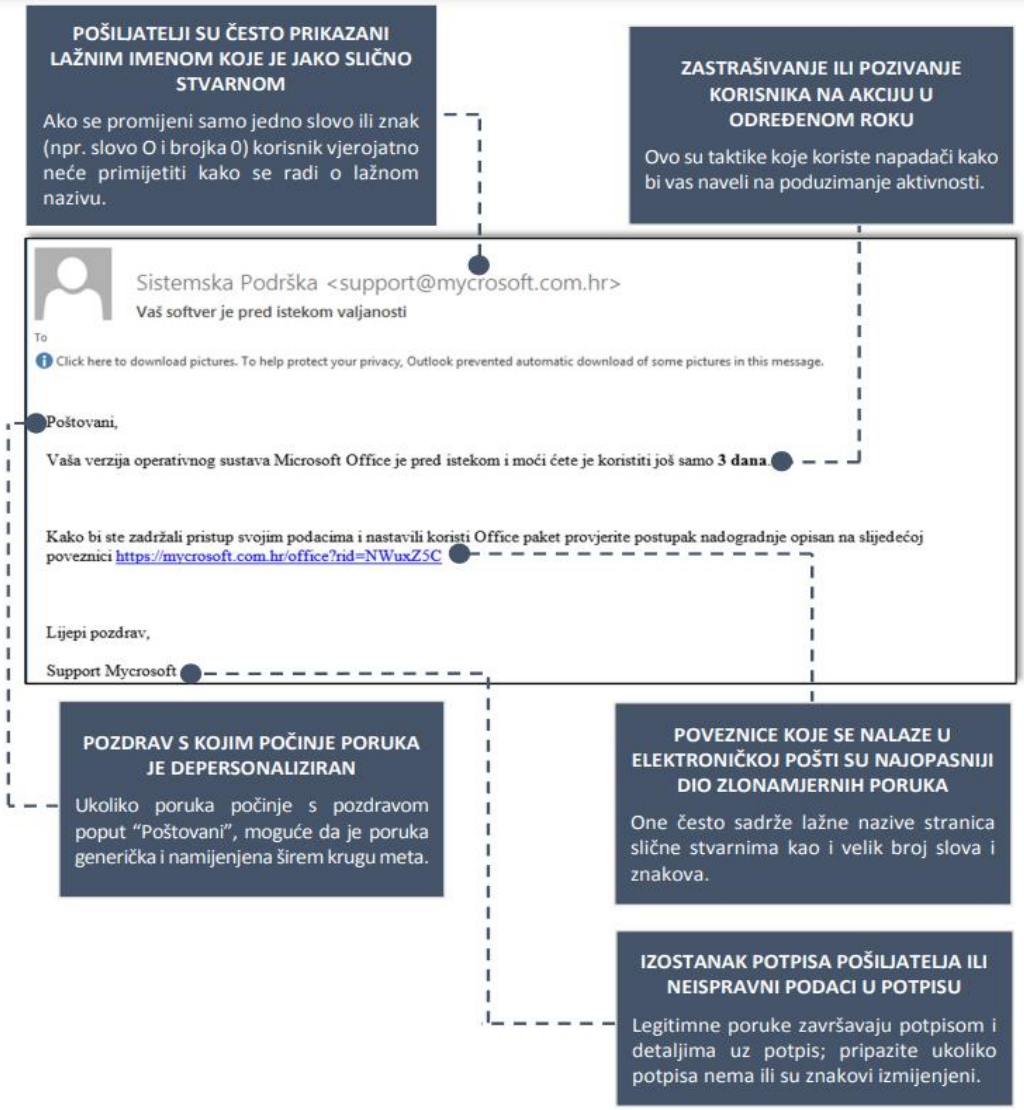
2.2. Phishing

Phishing ili mrežna krađa identiteta predstavlja način na koji napadač nastoji doći do povjerljivih informacija korisnika usluga. Pod to spadaju korisnička imena, podaci o kreditnim karticama, osobni podaci, lozinke itd. Ciljane skupine napadača mogu biti šira javnost, korisnici usluga i informacijski sustavi organizacija. Široj javnosti se nastoje prezentirati određene informacije što većem broju korisnika elektroničke pošte. Tu spadaju neželjene poruke odnosno spam (junk mail),

zlonamjerno oglašavanje odnosno malvertising i poruke neistinitog sadržaja odnosno hoax. Spam je zapravo elektronička pošta koja zatrpava elektronički sandučić kod primljenih poruka korisnika i bezvrijedna je, a vrlo često sadrži prijevaru ili zarazu virusom. Dobio je ime po skupini Monty Python jer su reklamirali mesni doručak Spam. Malvertising je korištenje online oglašavanja za širenje zlonamjernog softvera. Obično uključuje ubacivanje zlonamjernih reklama u legitimne web stranice. Hoax je poruka u električnoj pošti kojoj je cilj zastrašivanje krajnjeg primatelja. Primatelji ih onda prosljeđuju drugima misleći kako time rade ispravnu stvar. Dobra stvar kod hoax-a je da ne može direktno uzrokovati oštećenja na računalnom sustavu. Korisnicima usluga neovlašteno se izmjenjuje podatke i nastoji se preko osobnih podataka doći do financijske koristi. Informacijski sustavi organizacije su pod opasnosti kad napadač napadom na pojedinca odnosno zaposlenika želi ostvariti napad na samu organizaciju. Najčeći razlozi korištenja phishing napada su: niska cijena napada, niska razina svijesti korisnika, sve veća dostupnost osobnih podataka korisnika, jednostavnost napada zbog relativno visoke dostupnosti znanja i alata i oslanjanje napadača na zakon velikih brojeva. Ova vrsta računalnog kriminala može se podijeliti u tri kategorije(literatura):

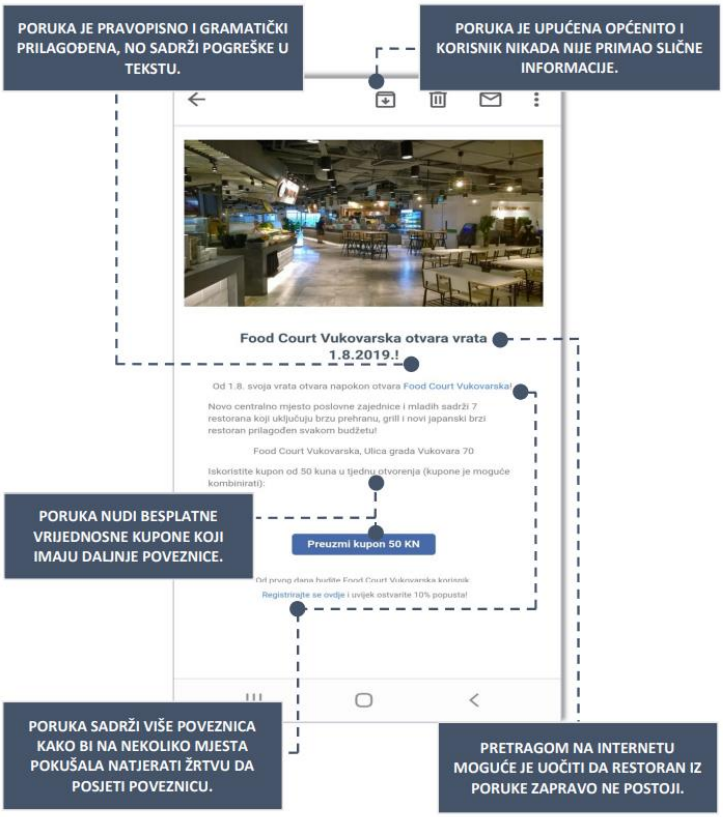
1. *Phishing* napadi putem poruka elektroničke pošte slanjem na ogroman broj adresa bez neke selekcije. U pravilu je te napade lako za prepoznati.
2. *Spear phishing* su napadi koji su precizno ciljani na određenog korisnika i teško je izbjeći takvu vrstu napada ukoliko korisnik nema dovoljnu razinu znanja o *phishing* napadima.
3. *Whaling* je podskupina *spear phishing-a* gdje je ciljani napad na upravljačke pozicije organizacije kako bi se došlo do povjerljivih podataka. Ovu vrstu napada također je teško izbjeći ukoliko korisnik nema dovoljnu razina znanja o *phishing* napadima.

U nastavku ovog poglavlja su prikazani i objašnjeni primjeri opasnih poruka prilikom *phishing* napada. Važno je obratiti pozornost na slijedeće pokazatelje kako bi se otkrio pokušaj napada [2].



Slika 1 Primjer phishing poruke poslane putem elektroničke pošte

Izvor: [2]



Slika 2 Primjer phishing poruke prilagođene mobilnom telefonu

Izvor: [2]

Slika 3 Primjer phishing poruke koja pokušava navući korisnika preko lažnih vijesti

Izvor: [2]

2.3. Računalni virusi

Računalni virus je računalni program kojemu je cilj zaraziti računalo i raširiti se samo-umnažanjem. Inficiranje se događa na način da ugrađuje svoj kod na računalo odnosno na datoteke na disku. Za pokretanje tog računalnog programa potrebno je pokrenuti datoteku u kojoj se nalazi. Naposlijetku računalni virus ima za cilj zaraziti i raširiti se na što više računala. Najčešće se širi prilikom slanja elektroničke pošte gdje se virus nalazi u datoteci koja se nalazi u privitku poruke i prijenosom preko USB stick-a. Za repliciranje potrebne su mu privilegije za izvođenje koda i zapisivanje u memoriju. Iz tog razloga su računalni virusi vezani uz izvršne datoteke. Postoji više vrsta zloćudnog softvera kojeg nazivamo virusom, a to su:

1. Crv koji automatski se pokušava širiti na druga računala na mreži na temelju sigurnosne slabosti sustava.
2. Spyware koji pokušava prikupljati osobne podatke o korisniku računala i onda ih slati bez pristanka trećoj osobi.
3. Trojanski konj koji lažno pokušava se prikazati kao program koji koristi računalu, a zapravo je maliciozan softver. Većina njih ima slične nazive uobičajenim programima, a za razliku od ostalih virusa nema sposobnost samo-umnažanja.
4. Adware koji pokušava automatski s mreže preuzimati reklame na korisnikovo računalo.
5. Rootkit koji osigurava pravo pristupa računalnom sustavu bez administratorskog znanja [1].

2.3.1. Mjere opreza i zaštite od računalnih virusa

Ukoliko je računalo zaraženo računalnim virusom najučinkovitija metoda je reinstalacija operacijskog sustava, ali postoje i ostale metode za oporavak sustava. Preporučuje se ne otvarati i prosljeđivati sumnjive poruke elektroničke pošte sumnjivih pošiljatelja i redovito ažurirati sigurnosne zakrpe operacijskog sustava. Za zaštitu od virusa i ostalih zloćudnih programa koriste se antivirusni program i vatrozid koji kao dio računalnog sustava sprječava neautorizirani pristup računalu. Antivirusni program koristi se za otkrivanje i uklanjanje malicioznog softvera što uključuje i računalne viruse. Ovaj program se najčešće oslanja na potpis virusa, a ukoliko je riječ o virusu za kojeg nije poznat potpis upotrebljavaju se heurističke metode. Aktivno pregledavajući operacijski sustav ovaj program pronalazi

zaražene datoteke i nakon obavljenog pregleda daje korisniku izvještaj o zaštićenosti njegovog sustava. Ukoliko ima zaraženih datoteka daje obavijest o tome i omogućuje korisniku daljnje akcije vezano uz rezultate. Problem jedino predstavlja činjenica što svakim novim danom nastaju novi virusi i potrebno je usporedno s nastajanjem novih virusa ažurirati bazu podataka potpisa virusa te automatski od strane korisnika i ažurirati program [1].

3. Incidenti

Računalni sigurnosni incident je svaki događaj koji krši implicitna ili eksplicitna pravila. To znači da se svaka radnja koja se ne bi smjela dogoditi, bilo da je ta radnja izričito dokumentirana ili ne, mogla smatrati incidentom. To može uključivati, ali nije ograničeno na radnje kao što su eskalacija privilegija, pokušaj neovlaštenog pristupa sustavima, skeniranje resursa mrežne infrastrukture (tj. poslužitelja, mrežnih preklopnika, usmjerivača itd.), učitavanje mrežnih njuškala ili keylogging[1] softvera na sustave i napadi uskraćivanja usluge (DoS). Incidenti imaju nekoliko karakteristika. Razumijevanje ovih karakteristika može uvelike pomoći administratoru sustava u planiranju sigurnosti poslužitelja ili cijele infrastrukture, ali isto tako može pomoći istražitelju otkriti korijenski uzrok incidenta. Ovisno o vrsti incidenti mogu biti lokalni ili udaljeni i ručni ili automatski. Ručne incidente najbolje je opisati kao one koji nastaju kao rezultat ljudske interakcije. Najčešće su lokalni incidenti ručni, ali i udaljeni incidenti mogu biti ručni incidenti. Automatski incidenti se događaju mnogo brže od ručnih incidenata jer nije potrebna ljudska interakcija nakon početnog pokretanja napada. Karakteristike incidenata ne samo da će odrediti kako se trebate pripremati za njih već će također određivati kako ćete reagirati [3].

3.1. Lokalni incidenti

Lokalni incident nastaje dok počinitelj ima izravan fizički pristup računalnom sustavu. Počinitelj može biti legitimni korisnik koji je napravio pogrešku posjetivši pogrešnu web stranicu ili premjestivši važan dokument s poslužitelja datoteka umjesto da ga kopira. Incident također može uzrokovati napadač koji želi izazvati probleme ili krađu podataka. Lokalni

[1] računalni program za bilježenje svakog pritiska na tipku od strane korisnika računala, posebno radi dobivanja lažnog pristupa lozinkama i drugim povjerljivim informacijama

incident je slučajan kada se dogodi pogreška korisnika kao što je klikanje na privitak e-pošte ili instaliranje jednog od klijenata za dijeljenje glazbenih datoteka koji također instalira nekoliko oblika špijunskog softvera. Namjerni, zlonamjerni lokalni incidenti nastaju kada je počinitelj pokrenuo svoj napad s vrlo određenim ciljem što može rezultirati neovlaštenim pristupom sustavu ili uzrokovati uskraćivanje usluge tog sustava. Lokalni incidenti mogu uključivati neku vrstu prijevare ili krađu vlasničkih podataka tvrtke koju je počinio nezadovoljni zaposlenik. Lokalni incidenti mogu biti u rasponu od jednostavnih (špijunski softver, network backdoor ili instalacije virusa) do onih incidenata koji mogu izložiti organizaciju vrlo ozbiljnom riziku (krađa vlasničkih podataka tvrtke, zlouporaba mrežnih resursa itd.). Lokalne incidente također može uzrokovati zlonamjerni softver. Iako se infekcija zlonamjernim softverom općenito može smatrati udaljenim incidentom postoje slučajevi kada se infekcija može dogoditi čak i ako mreža nema veze s internetom. Zlonamjerni softver kao što su virusi, crvi, trojanci i network backdoor mogu zaraziti sustave radnjama korisnika kao što su klikanje na privitke e-pošte ili preuzimanjem i pokretanjem izvršnih datoteka s nepouzdanih web stranica. Bilo što od toga može se dogoditi jednostavno zato što je korišten zaraženi CD ili USB stick tako da se čak i zatvorene mreže (mreže računalnih sustava bez fizičkog ili logičkog pristupa Internetu) mogu zaraziti. U drugim slučajevima korisnici mogu preuzimati i pokretati programe koji imaju štetne učinke na sustav kao što su instaliranje keystroke logger-a ili mrežnih sniffera, brisanje legitimnih programa i zaraza drugih sustava na mreži. To se sve još smatra lokalnim incidentima. Idući primjer lokalnog incidenta koji se može dogoditi je eskalacija privilegija. Eskalacija privilegija nastaje kada korisnik s pravima i povlasticama niže razine može podići svoje privilegije na višu razinu, poput onih povezanih s računom administratora ili sustava. To se općenito događa kada se iskorištava poznata ranjivost u sustavu. Na primjer, mana otkrivena u alatu za otklanjanje pogrešaka u sustavu Windows 2000 dovela je do izdavanja DebPloit-a. DebPloit (DEBugger exPLOIT) je naziv koji se daje programu koji se koristi za iskorištavanje propusta u autentifikaciji u Windows alatu za ispravljanje pogrešaka. Kako bi iskoristio ovu ranjivost napadač se mora moći prijaviti na sustav i pokrenuti programe. Međutim, objavljivanje koda DebPloit čini iskorištavanje ove ranjivosti iznimno jednostavnim, u tolikoj mjeri da je izvršni kod bio u nosivosti crva Masy, dopuštajući automatiziranom kodu da izvršava programe na zaraženim sustavima na povišenim razinama privilegija. Ako napadač ima fizički pristup sustavu Windows kojem želi pristupiti to može učiniti pomoću posebnog diska za podizanje sustava Linux. Ovaj disk za podizanje sustava sadrži minimalnu instalaciju i uslužni program Linuxa koji će omogućiti korisniku promjenu bilo koje lozinke na sustavu bez poznavanja izvorne lozinke. Nakon što je disk za podizanje sustava stvoren prema uputama

dostupnim na web stranici, napadač će ga koristiti za pokretanje Windows sustava. Sustav će se pokrenuti na Linux i pokrenuti će se uslužni program vođen izbornikom. Slijedeći izbornik, napadač može odabrati korisničku lozinku koju želi promijeniti tako da jednostavno unese novu lozinku, a zatim nastavi slijediti upute dok uslužni program ne završi svoj posao. Nakon što se sustav ponovno pokrene na Windows, napadač se može prijaviti na korisnički račun koristeći novu lozinku. Sve što treba je fizički pristup sustavu. Kada se dogodi lokalni incident i pod pretpostavkom da je odgovarajuća revizija konfigurirana na sustavu, tragovi incidenta mogu biti vidljivi u zapisniku sigurnosnih događaja (Event Viewer). Osim prijava, ako je administrator konfigurirao sustav za praćenje procesa može postojati neka naznaka kada je određeni program izvršen ili pokrenut proces. Ovo možda neće biti od pomoći jer se izvršni programi na Windows sustavima mogu imenovati gotovo bilo čime, ali uvijek postoji mogućnost da se nešto pronađe. Ako se sumnja na krađu korporativnih vlasničkih podataka ili zlouporabu mreže, istražitelj može pronaći informacije koje se odnose na incident provjeravajući Event Viewer za unose s ID-om događaja 134. Takvi unosi s nazivom događaja "Removable Storage Service" označavaju da je prijenosni uređaj za pohranu bio priključen na sustav provjeravajući Event Viewer za unose s ID-om događaja 134. Ako je zapisnik sistemskih događaja obrisan, istražitelj može provjeriti sadržaj ključa registra HKEY_LOCAL_MACHINE\System\MountedDevices. Prema Microsoftu, ovaj se ključ koristi za održavanje baze podataka montiranih uređaja. Ako je napadač i izbrisao preglednik događaja i dalje će bit prisutan ID događaja 517. Obrana od lokalnih incidenata uključuje poduzimanje odgovarajućih fizičkih sigurnosnih mjera za zaštitu sustava, instaliranje antivirusnog softvera, postavljanje i provođenje računalnih sigurnosnih mjera (kao što je jaka lozinka), konfiguriranje sustava u skladu s dokumentiranom politikom i nadzor sustava za usklađenost s politikom i za neuobičajene aktivnosti. Administratorima i upraviteljima treba biti jasno koju bi razinu privilegija korisnici trebali imati, a zatim konfigurirati sustave za provođenje ove razine [3].

3.2. Udaljeni incidenti

Udaljeni incident nastaje kao rezultat radnji poduzetih na mreži. Incident na daljinu može se dogoditi zbog nečeg tako bezopasnog kao što je upisivanje netočnog URL-a u svoj preglednik. Mnogo puta, međutim, udaljeni sigurnosni incidenti su rezultat toga da netko namjerno pokušava izazvati probleme ili dobiti pristup sustavu. Primjeri udaljenih incidenata uključuju pokušaj iskorištavanja ranjivosti web poslužitelja korištenjem posebno izrađenih

URL-ova, pokušaj daljinske prijave u sustav i druge pokušaje dobivanja neovlaštenog pristupa. Udaljeni incidenti ciljaju na određeni port na sustavu obično kao rezultat činjenice da se određena usluga izvodi na tom portu. Na primjer, web poslužitelji se obično mogu pronaći kako rade na TCP portu 80. Mrežni promet napada usmjerenih na ranjive web poslužitelje bit će usmjeren na ovaj port. Napadi na FTP poslužitelje usmjeravaju se na TCP port 21. Mrežni perimetarski uređaji, kao što su usmjerivači i vatrozidi, mogu se koristiti za ograničavanje ili ograničavanje nepotrebnog prometa, ali u mnogim slučajevima pristup web i FTP poslužiteljima je dopušten ili potreban. Ako je to slučaj, same usluge moraju se konfigurirati što je više moguće i moraju se nadzirati za moguću nepredvidljivu aktivnost. Kao i kod lokalnih incidenata, dokazi o udaljenim incidentima također se mogu pronaći u Event Viewer-u. Neuspješni pokušaji daljinske prijave u Windows pojavit će se u Event Viewer-u s ID-om događaja 529, a opis događaja će ukazivati na događaj tipa 3 prijave. Ako se napadač uspije daljinski prijaviti na sustav Windows 2000 ili noviji, ID događaja bit će 540, a događaj tipa prijave ostat će 3. Udaljeni incidenti će se, u mnogim slučajevima dogoditi prema obrascu aktivnosti. Napadači mogu prethoditi stvarnom napadu skeniranjem portova i aktivnostima prikupljanja informacija prije pokušaja iskorištavanja određene ranjivosti. Postoji niz besplatnih skenera portova dostupnih za preuzimanje na Internetu. Jedan od najpoznatijih je nmap. Nmap omogućuje korisniku izvođenje različitih vrsta skeniranja portova i pokušaja identificiranja verzije ciljnog operativnog sustava i svih usluga otkrivenih na određenim portovima. Značajke Nmapa uključuju: identificiranje hostova na mreži, skeniranje portova, otkrivanje verzije, TCP/IP stack fingerprinting i skriptabilna interakcija s ciljem. Nakon što su otvoreni portovi identificirani, napadač može pokušati prikupiti više informacija prije pokušaja eksploatacije. Ako je port 80 otvoren, mnogi napadači mogu unaprijediti svoje aktivnosti prikupljanja informacija i jednostavno pokrenuti skenere ranjivosti web poslužitelja protiv njih. Iako to ne zahtijeva veliki napor od strane napadača, može potrajati. Neki će napadači uzeti konzervativniji pristup i pokušati dobiti dodatne informacije iz sustava prije pokretanja konkretnijeg napada. Jedna od metoda identificiranja potencijalno ranjivih sustava je hvatanje bannera. Hvatanje bannera uključuje slanje legitimnog upita usluzi kao što je web ili FTP poslužitelj i gledanje kako se ta usluga ili aplikacija identificira. Mnoge aplikacije će pružiti ove informacije putem neke vrste bannera. Npr. kada vaš preglednik zatraži web stranicu od poslužitelja i prikaže rezultate, općenito zanemaruje informacije zaglavlja koje se vraćaju. Ove informacije zaglavlja mogu se vidjeti kako bi se odredila vrsta i broj verzije web poslužitelja. Napadač može koristiti ove informacije da cilja svoj napad i izbjegne gubljenje vremena na upite ili napade za koje zna da neće uspjeti protiv identificiranih ciljnih sustava. Provodeći

hvatanje bannera kod otvorenih portova, napadač može izgraditi sliku o tome kakvu je vrstu sustava pronašao i prema tome prilagoditi svoje napade. Druga metoda koju napadači mogu koristiti za identifikaciju potencijalno ranjivih web poslužitelja je korištenje web-mjesta kao što je NetCraft. Odlaskom na ovu stranicu napadač može slati upite putem "Što se radi na toj stranici?" polja. Na taj način napadač može suziti koje web poslužitelje skenirati ograničavajući svoju izloženost i vrijeme koje provodi skenirajući. Dodatna prednost korištenja NetCraft-a je ta što se IP adresa napadača nikada ne pojavljuje u zapisnicima web poslužitelja prije njegovog stvarnog napada. Nakon što su potencijalni ciljevi identificirani, napadač može koristiti druge vrste skenera koji će ispitivati određene aplikacije umjesto da jednostavno traže otvorene portove. Obrana protiv udaljenih incidenata je slična obrani protiv lokalnih incidenata. Administratori bi trebali imati uspostavljenu sigurnosnu politiku koja opisuje kako konfigurirati i nadzirati svoje sustave [3].

4. Tipovi računalne forenzike

Postoje razne vrste računalnih forenzičkih ispitivanja. Svako ispitivanje se bavi određenim aspektom informacijske tehnologije. Glavni tipovi računalne forenzike su: forenzika za bazu podataka, e-mail forenzika, forenzika za malware, forenzika za memoriju, mobilna forenzika i mrežna forenzika.

4.1. Forenzika za bazu podataka

Forenzika za bazu podataka je područje digitalne forenzičke znanosti koje se bavi forenzičkim ispitivanjem baza podataka i podataka unutar njih. Korištenjem elektroničkih podataka pohranjenih u bazi podataka za rekonstrukciju tragova otkrivaju se zločini i rješavaju slučajevi. Ovaj tip računalne forenzike slijedi standardnu forenzičku metodu i koristi istražne tehnike o sadržaju baze podataka i podacima. Forenzička analiza baze podataka može uključivati provjeru valjanosti vremenskih oznaka povezanih s vremenom ažuriranja retka u relacijskoj tablici kako bi se potvrdile radnje korisnika baze podataka. Forenzika baze podataka počela se široko primjenjivati među organima za provedbu zakona posljednjih godina. Forenzička istraga baze podataka može biti usmjerena na otkrivanje transakcija unutar sustava baze podataka ili aplikacije koje sugeriraju dokaz nezakonite aktivnosti kao što je prijevara.

Kako bi se olakšala obrada i upiti prema podacima najraširenije vrste baza podataka koje se danas koriste često se modeliraju u retke i stupce u nizu tablica. Dakle, podacima se može pristupiti, njima se može upravljati, mijenjati ih, ažurirati, kontrolirati i organizirati s lakoćom. Većina baza podataka piše i traži podatke koristeći jezik strukturiranih upita (SQL).

Forenzika baze podataka ispituje tko dobiva pristup bazi podataka i koje su poduzete radnje, te istražitelji iz toga pokušavaju doći do relevantnih informacija. Odgovornosti forenzičkih stručnjaka za baze podataka uključuju:

1. Istraživanje računalnih sustava i drugih digitalnih uređaja za pohranu u potrazi za dokazima.
2. Istraživanje korištenjem forenzičkih alata za diskove i baze podataka kao i čitača datoteka i mrežnog forenzičkog softvera.
3. Korištenje softvera za ispitivanje e-pošte, računalnih registara i datoteka kao i mobilnih uređaja.
4. Oporavak važnih dokumenata koji su uništeni ili šifrirani.
5. Otkrivanje i pružanje digitalnih dokaza tijelima za provedbu zakona [4].

4.1.1. Forenzički alati za baze podataka

Na neki način rad s forenzičkim alatima baze podataka ključan je za sve istražne subjekte, bez obzira radi li se o digitalnim forenzičkim istražiteljima, policajcima ili obavještajnim agencijama kada se bave dokazima baze podataka. Srećom, postoje alati koji će pomoći da ovaj postupak se učini brzim i jednostavnim. Ovi programi pružaju sveobuhvatna izvješća koja se mogu koristiti u sudskim postupcima.

1. DBR for MySQL je sposoban vratiti pokvarene, oštećene ili nedostupne MySQL baze podataka, uključujući tablice baze podataka, poglede, funkcije i pohranjene procedure. Osim što može dohvaćati, može i skenirati izbrisane podatke iz baze podataka.
2. DBR for SQLServer je robustan i učinkovit alat za popravak baze podataka SQLServera koji može popraviti oštećene ili nedostupne SQLServer baze podataka, uključujući tablice baze podataka, poglede, funkcije i pohranjene procedure.
3. ProDiscover Forensics je alat koji vam omogućuje da pronađete sve podatke na tvrdom disku. Za pravne postupke može zaštititi dokaze i pružiti visokokvalitetna

izvješća. Ovaj program možete koristiti za izvlačenje JPEG EXIF podataka iz formata slikovne datoteke.

4. Sleuth Kit (+Autopsy) je uslužni paket temeljen na sustavu Windows koji pojednostavljuje forenzičku istragu računalnih sustava. Ova aplikacija vam omogućuje da pregledate sadržaj vašeg tvrdog diska i pametnog telefona.
5. FTK Imager je forenzički alat koji se može koristiti za dobivanje dokaza. Bez diranja u izvorne dokaze, može napraviti kopije podataka. Kako biste ograničili količinu nebitnih podataka, ovaj program vam omogućuje odabir veličine datoteke i kriterija veličine piksela.
6. EnCase je program koji pomaže u preuzimanju podataka s tvrdih diskova putem enkripcije. Može se provesti dubinska istraga u spisima kako bi se prikupili dokazi kao što su dokumenti i fotografije.

   System for Interfacing with Financial Transactions (SIFT) izgrađen je na Ubuntu. Što se tiče digitalne forenzike i odgovora na incidente, to je jedan od najizvrsnijih dostupnih računalnih forenzičkih alata [4].

4.2. E-mail forenzika

E-pošta ima vrlo važnu ulogu u poslovnoj komunikaciji. Ona je prikladan način za slanje poruka kao i dokumenata, ne samo s računala već i s drugih elektroničkih naprava kao što su mobilni telefoni i tableti. Negativna strana e-pošte je da kriminalci mogu preko nje izvući važne informacije o tvrtki ili pojedincu. Stoga je uloga e-pošte u digitalnoj forenzici posljednjih godina povećana. Forenzika e-pošte uključuje proučavanje izvora i sadržaja e-pošte kao dokaza za identifikaciju stvarnog pošiljatelja i primatelja poruke zajedno s nekim drugim informacijama kao što su datum odnosno vrijeme prijenosa i namjera pošiljatelja. Uključuje istraživanje metapodataka, skeniranje portova kao i pretraživanje ključnih riječi. Neke od uobičajenih tehnika koje se mogu koristiti za e-mail forenzičku istragu su: analiza zaglavlja, istraga poslužitelja, istraživanje mrežnih uređaja, otisci pošiljatelja, usporedba teksta i softverski ugrađeni identifikatori [5].

4.3. Forenzika za malware

Forenzika za malware se odnosi na način pronalaženja, analiziranja i istraživanja različitih svojstava zlonamjernog softvera kako bi se pronašli krivci i razlozi napada. Metoda također uključuje zadatke poput provjere zlonamjernog koda, utvrđivanja njegovog unosa, metode širenja, utjecaja na sustav, portova koje pokušava koristiti itd. Istražitelji provode forenzičku istragu koristeći različite tehnike i alate. Postoje dva načina pristupa procesu analize zlonamjernog softvera, a to su pomoću statičke analize ili dinamičke analize. Kod statičke analize komponente i svojstva zlonamjernog softvera analiziraju se bez pokretanja koda dok se kod dinamičke analize zlonamjerni softver zapravo izvršava u kontroliranom, izoliranom okruženju i promatra se njegovo ponašanje. Statička analiza zlonamjernog softvera temelji se na potpisu tj. potpis binarne datoteke zlonamjernog softvera određuje se izračunavanjem kriptografskog hasha. Ona uključuje skeniranje virusa, uzimanje otisaka prstiju, itd. Može se učiniti neučinkovitim protiv nepoznatih ili novih vrsta zlonamjernog softvera ili u sofisticiranijim scenarijima napada. Dinamička analiza zlonamjernog softvera ima pristup otkrivanju i analizi zlonamjernog softvera koji se temelji na ponašanju unutar virtualnog okruženja. Dinamička analiza zlonamjernog softvera uključuje promjene registra, API pozive, upisivanje u memoriju itd. Ova analiza je učinkovitija i pruža veću stopu detekcije od statičke analize [6].

4.3.1. Četiri faze analize malwarea

Postoje četiri faze analize zlonamjernog softvera, često ilustrirane pomoću piramidalnog dijagrama koji postaje sve složeniji kako se ulazi dublje u proces. Radi jednostavnosti raščlaniti će se svaka od četiri faze analize malwarea, a to su:

1. Automatizirana analiza se odnosi na oslanjanje na modele detekcije formirane analizom prethodno otkrivenih uzoraka malwarea. Ovo je najprikladnija metoda za obradu zlonamjernog softvera u velikoj mjeri i brzu procjenu posljedica uzorka na mrežnu infrastrukturu. Potpuno automatizirana analiza može se obaviti pomoću alata kao što je Cuckoo Sandbox. To je platforma za automatiziranu analizu malwarea otvorenog koda koja se može podesiti za pokretanje prilagođenih skripti i

generiranje sveobuhvatnih izvješća. Postoji i nekoliko drugih alternativnih alata, komercijalnih i besplatnih koji su dostupni na tržištu.

2. Analiza statičkih svojstava uključuje gledanje metapodataka datoteke bez uklanjanja malwarea. Ovaj je proces obično nešto što se radi unutar izoliranog okruženja kao što je virtualni stroj koji nije povezan s internetom. Jedan od besplatnih alata koji bi mogao biti koristan u tu svrhu je PeStudio. Ovaj alat označava sumnjive artefakte unutar izvršnih datoteka i dizajniran je za automatsku analizu statičkih svojstava. PeStudio predstavlja hasheve datoteka koji se mogu koristiti za pretraživanje VirusTotal, TotalHash ili drugih spremišta zlonamjernog softvera kako bi se provjerilo je li datoteka prethodno analizirana. Štoviše, može se koristiti za ispitivanje ugrađenih nizova, knjižnica, uvoza i drugih pokazatelja kompromisa (IOC) i usporedbu svih neobičnih vrijednosti koje se razlikuju od onih koje se obično vide u običnim izvršnim datotekama. Provođenje statičke analize svojstava idealno bi trebalo ostaviti analitičaru malwarea ideju o tome treba li nastaviti s istragom ili prekinuti istragu.
3. Interaktivna analiza ponašanja gdje se uzorak malwarea izvršava izolirano dok analitičar promatra kako on stupa u interakciju sa sustavom i promatra promjene koje čini. Često se dio malwarea može odbiti izvršiti ako otkrije virtualno okruženje ili može biti dizajniran da izbjegne izvršenje bez ručne interakcije (tj. u automatiziranom okruženju). Postoji nekoliko vrsta radnji koje bi odmah trebale podići crvenu zastavu, uključujući: dodavanje ili izmjena novih ili postojećih datoteka, instaliranje novih usluga ili procesa i promjena registra ili promjena postavki sustava. Neke vrste zlonamjernog softvera mogu se pokušati povezati sa sumnjivim IP-ovima hosta koji ne pripadaju okruženjima. Drugi bi također mogli pokušati stvoriti mutex objekte kako bi izbjegli zarazu istog hosta više puta (kako bi se očuvala operativna stabilnost). Ovi su nalazi relevantni pokazatelji kompromisa. Neki od alata koje možete koristiti uključuju: Wireshark za promatranje mrežnih paketa, Process Hacker za promatranje procesa koji se izvršavaju u memoriji, Process Monitor za promatranje datotečnog sustava u stvarnom vremenu, registra, aktivnosti procesa za Windows i ProcDot koji pruža interaktivni i grafički prikaz svih snimljenih aktivnosti. Može se provesti dodatna istraživanja o novim podacima koji se prikupe korištenjem bilo koje baze podataka za analizu malwarea. Isto tako, dodatna analiza mreže može otkriti pojedinosti o infrastrukturi naredbi i upravljanja uzorkom malwarea, količini i vrsti podataka koje curi, itd.

4. Ručno mijenjanje koda gdje obrnuti inženjering koda uzorka malwarea može pružiti vrijedne uvide. Ovaj proces može: otkriti logiku i algoritme koje malware koristi, razotkriti skrivene mogućnosti i tehnike iskorištavanja koje malware koristi i daje uvid u komunikacijski protokol između klijenta i poslužitelja na strani naredbi i upravljanja. Obično da bi ručno poništili kod, analitičari koriste alate za ispravljanje pogrešaka. Iako su preokreti koda iznimno dugotrajan proces i iako vještine za njihovo izvođenje nisu osobito uobičajene, ovaj korak može pružiti mnogo važnih uvida [7].

4.4. Forenzika za memoriju

Forenzika memorije odnosi se na analizu privremenih podataka u memoriji računala. Stručnjaci za informacijsku sigurnost provode forenziku memorije kako bi istražili i identificirali napade ili zlonamjerna ponašanja koja ne ostavljaju lako uočljive tragove na podacima tvrdog diska. Privremeni podaci su podaci pohranjeni u privremenoj memoriji na računalu dok ono radi. Kada se računalo isključi, privremeni podaci gube se odmah. Privremeni podaci nalaze se u kratkoročnoj memoriji računala i mogu uključivati podatke poput povijesti pregledavanja, poruka čavrljanja i sadržaja međuspremnika. Ako se npr. radi na dokumentu u programu Word koji još nije spremljen na tvrdi disk ili neki drugi izvor trajne memorije tada se gubi taj rad ako je računalo ostalo bez struje prije nego što je spremljeno. Memory dump ili ispis memorije je snimka podataka memorije računala iz određenog trenutka. Ispis memorije može sadržavati vrijedne forenzičke podatke o stanju sustava prije incidenta kao što je pad ili ugrožavanje sigurnosti. Ispisi memorije sadrže RAM podatke koji se mogu koristiti za utvrđivanje uzroka incidenta i druge ključne pojedinosti o tome što se dogodilo. Forenzika memorije može pružiti jedinstveni uvid u aktivnosti sustava za vrijeme izvođenja uključujući otvorene mrežne veze i nedavno izvršene naredbe ili procese. U mnogim će slučajevima kritični podaci koji se odnose na napade ili prijetnje postojati isključivo u memoriji sustava, a to su: mrežne veze, vjerodajnice računa, poruke chata, ključevi za šifriranje, pokrenuti procesi, umetnuti fragmenti koda i internetska povijest koja se ne može predmemorirati. Bilo koji program bio on zlonamjeran ili ne mora se učitati u memoriju kako bi se mogao izvršiti što forenziku memorije čini važnom za prepoznavanje inače prikrivenih napada. Kako metode napada postaju sve sofisticiranije, alati i vještine za forenziku memorije danas su u velikoj potražnji jer mnoga mrežna sigurnosna rješenja poput vatrozida i antivirusnih alata ne mogu otkriti zlonamjerni softver zapisan izravno u fizičku memoriju ili RAM računala [8].

4.4.1. Forenzički alati za memoriju

Forenzički alati za memoriju također pružaju neprocjenjive podatke o prijetnjama koji se mogu prikupiti iz fizičke memorije vašeg sustava. Artefakti fizičke memorije uključuju sljedeće: korisnička imena i lozinke, dešifrirani programi (svaka šifrirana zlonamjerna datoteka koja se pokrene morat će se dešifrirati kako bi se pokrenula) i otvoreni sadržaj međuspremnika ili prozora (ovo može uključivati informacije koje su kopirane ili zalijepljene, sesije instant chata, unose u polje obrasca i sadržaj e-pošte). Postoji niz komercijalnih alata i alata otvorenog koda dizajniranih isključivo za provođenje forenzike memorije.

1. BlackLight je jedan od najboljih forenzičkih alata za memoriju. Pruža detalje korisničkih radnji i izvješće o analizi memorijske slike. Učinkovito organizira različite memorijske lokacije kako bi pronašao tragove potencijalno važnih korisničkih aktivnosti. Blacklight analizira nekoliko vrsta memorijskih datoteka uključujući datoteke hibernacije, pagefile.sys, raw dumpove i crash dumpove. Također može izvoditi skupno pretraživanje sadržaja ekstrakcije za razne stavke kao što su telefonski brojevi, adrese, URL-ovi itd. Blacklight dolazi s pregledom filtra datoteka i puno je brži od ostalih forenzičkih alata otvorenog koda. Ovaj alat se može koristiti za analizu podataka na 4 operacijska sustava (Android, Windows, iOS i MacOS X).
2. Volatility je još jedan forenzički alat za memoriju koji je za razliku od Blacklighta besplatan u punom izdanju. Pomaže stručnjacima za sigurnost da naprave analize stanja rada sustava pomoću podataka pronađenih u ispisima radne memorije (RAM). To je višeplatformska, modularna i proširiva platforma koja omogućuje izvlačenje korisnih informacija o mrežnim vezama, otvorenim socketima, pokrenutim procesima, procesima DLL-ova procesa, predmemoriranim registrima i još mnogo toga. Volatility je dostupan za operacijske sustave Windows, MacOS X i Linux.
3. SANS Investigative Forensic Toolkit (SIFT) popularan je alat za digitalnu forenziku koji dolazi sa svim bitnim značajkama. To je alat otvorenog koda i poznat je po izvođenju dubinske forenzičke istrage ili istrage odgovora na incidente. Podržava Advanced Forensic Format (AFF), RAW (dd) formate dokaza i Expert Witness Format za duboku analizu. SANS SIFT dolazi sa korisnički prilagođenim sučeljem. Može pokrenuti tražene alate s gornje trake izbornika ili koristiti tradicionalni način korištenja prozora terminala. Također uključuje druge korisne alate kao što je Rifiuti

za ispitivanje koša za smeće, log2timeline za generiranje vremenske trake temeljene na dnevnicima sustava i „skalpel za rezbarenje“ podatkovne datoteke. SANS SIFT nudi bolju iskoristivost memorije, najnovije forenzičke tehnike, ažuriranje Auto-DFIR paketa i unakrsnu kompatibilnost između Linuxa i Windowsa [9].

4.5. Mobilna forenzika

Mobilna forenzika je proces prikupljanja i analize elektronički pohranjenih informacija za potporu ili osporavanje pretpostavke u sudskim postupcima te građanskim ili kaznenim istragama. Mobilna forenzika dio je digitalne forenzike, ali ima neke svoje važne značajke koje uključuju: zapljenu i izolaciju mobilnog uređaja, ekstrakciju i oporavak te analizu izdvojenih podataka. Uglavnom se treba usredotočiti na uobičajene podatke kao što su mediji, pozivi i poruke, kontakti i pregledavanje povijesti sadržaja. Oporavak dokaza s mobilnih uređaja kao što su pametni telefoni i tableti u fokusu je mobilne forenzike. Budući da se pojedinci oslanjaju na mobilne uređaje za velik dio slanja, primanja i pretraživanja podataka razumno je pretpostaviti da ti uređaji sadrže značajnu količinu dokaza koje bi istražitelji mogli iskoristiti. Mobilni uređaji jedna su od stvari koje se danas najbrže razvijaju. Iako se tehnologija koja se koristi u mobilnim uređajima brzo razvija koncepti mobilne forenzičke istrage ostaju isti, a to je identificiranje i prikupljanje relevantnih dokaza u obliku koji pomaže otkriti istinu i koji ostaje prihvatljiv na sudu. Vojska koristi mobilne uređaje za prikupljanje obavještajnih podataka prilikom planiranja vojnih operacija ili terorističkih napada. Korporacija može koristiti mobilni dokaz ako se boji da je njezino intelektualno vlasništvo ukradeno ili da zaposlenik čini prijevaru. Poznato je da tvrtke prate osobnu upotrebu poslovnih uređaja od strane zaposlenika kako bi otkrile dokaze o nezakonitim aktivnostima. S druge strane, policija bi mogla iskoristiti prednost mobilne forenzike korištenjem elektroničkog otkrića za prikupljanje dokaza u različitim slučajevima od krađe identiteta do ubojstva. Proces mobilne forenzike uključuje:

1. Zapljenu i izolaciju gdje prema digitalnoj forenzici dokaze treba uvijek adekvatno čuvati, analizirati i predstaviti na sudu. Zapljene mobilnih uređaja praćene su nizom pravnih poteškoća i to predstavlja problem kod ovog koraka.
2. Identifikacija kod koje je svrha dohvaćanje informacija s mobilnog uređaja. S odgovarajućim PIN-om, lozinkom, uzorkom ili biometrijom može se otvoriti

zaključani zaslon. Šifre su zaštićene, ali otisci prstiju nisu. Aplikacije, fotografije, SMS-ovi i messengeri mogu imati slične značajke zaključavanja. Enkripcija, s druge strane pruža sigurnost koju je teško nadmašiti na softverskoj i/ili hardverskoj razini.

3. Akvizicija kod koje je kontrola podataka na mobilnim uređajima teška jer su sami podaci pokretni. Nakon što se poruke ili podaci pošalju s pametnog telefona kontrola nestaje. Unatoč činjenici da su različiti uređaji sposobni pohraniti ogromne količine podataka, sami podaci mogu biti pohranjeni negdje drugdje. Npr. sinkronizacija podataka između uređaja i aplikacija može se izvršiti izravno ili putem oblaka. Korisnici mobilnih uređaja često koriste usluge kao što su Appleov iCloud i Microsoftov One Drive, što izlaže mogućnost prikupljanja podataka. Kao rezultat toga, istražitelji bi trebali paziti na sve znakove da bi podaci mogli prijeći mobilni uređaj iz fizičkog objekta, budući da bi to moglo utjecati na prikupljanje podataka, pa čak i na proces očuvanja.
4. Ispitivanje i analizu mobilnog uređaja.
5. Izvještavanje kod kojeg dokument ili papirnati trag koji pokazuje zapljenu, čuvanje, kontrolu, prijenos, analizu i raspolaganje fizičkim i elektroničkim dokazima naziva se forenzičkim izvješćem. To je proces provjere kako je bilo koja vrsta dokaza prikupljena, praćena i zaštićena [10].

4.6. Mrežna forenzika

Mrežna forenzika je tip računalne forenzike koja se odnosi na praćenje i analizu računalnog mrežnog prometa u svrhu prikupljanja informacija, pravnih dokaza ili otkrivanja upada. Općenito ima dvije namjene. Prva se odnosi na sigurnost i uključuje praćenje mreže u potrazi za nepravilnim prometom i prepoznavanjem upada. Napadač bi mogao izbrisati sve datoteke dnevnika na kompromitiranom hostu stoga dokazi temeljeni na mreži mogu biti jedini dokazi dostupni za forenzičku analizu. Drugi oblik odnosi se na provedbu zakona. U ovom slučaju analiza snimljenog mrežnog prometa može uključivati zadatke poput ponovnog sastavljanja prenesenih datoteka, traženja ključnih riječi i analiziranja ljudske komunikacije poput e-pošte ili chata. Za prikupljanje mrežnih podataka obično se koriste dva sistema, a to su:

1. grubom silom "hvataj što možeš" gdje se svi paketi koji prolaze kroz određenu prometnu točku hvataju i zapisuju u pohranu, a analiza se naknadno provodi u skupnom načinu rada. Ovaj pristup zahtjeva velike količine prostora za pohranu.
2. inteligentnijom metodom "stani,gledaj,slušaj" gdje se svaki paket analizira na početni način u memoriji i samo se određene informacije spremaju za buduću analizu. Ovaj pristup zahtijeva brži procesor kako bi držao korak s dolaznim prometom.

U usporedbi s ostalim računalnim forenzikama gdje se dokazi obično čuvaju na disku, mrežni podaci su nestalniji i nepredvidljiviji. Istražitelji često imaju samo materijal za ispitivanje ako su filtri paketa, vatrozidi i sustavi za otkrivanje upada postavljeni da predvide povrede sigurnosti [11].

4.6.1. Mrežna forenzika na Ethernet sloju

Prikupom podataka na ovom sloju korisniku se omogućuje filtriranje različitih događaja. Web stranica, privici e-pošte i drugi mrežni promet mogu se rekonstruirati samo ako se prenose ili primaju nekriptirani. Prednost prikupljanja ovih podataka je ta što su oni izravno povezani s hostom. Ako je npr. poznata IP adresa ili MAC adresa glavnog računala u određeno vrijeme, svi podaci poslani na ili s te IP ili MAC adrese mogu se filtrirati. Tablice Address Resolution Protocol (ARP) navode MAC adrese s odgovarajućim IP adresama. Za prikupljanje podataka na ovom sloju mrežna kartica (NIC) glavnog računala može se staviti u "promiskuitetni način rada". Pritom će sav promet biti proslijeđen procesoru, a ne samo promet namijenjen hostu. Međutim, ako je uljez ili napadač svjestan da se njegova veza može prisluškivati, mogao bi upotrijebiti enkripciju da osigura svoju vezu. Danas je gotovo nemoguće probiti enkripciju, ali činjenica da je veza osumnjičenika s drugim hostom cijelo vrijeme šifrirana može značiti da je drugi host suučesnik osumnjičenika. Uobičajeni alat koji se koristi za praćenje i snimanje mrežnog prometa je Wireshark [11].

4.6.2. Mrežna forenzika na TCP/IP sloju

Na mrežnom sloju internetski protokol (IP) odgovoran je za usmjeravanje paketa koje generira TCP kroz mrežu (npr. Internet) dodavanjem informacija o izvoru i odredištu koje

usmjerivači diljem mreže mogu interpretirati. Mobilne digitalne paketne mreže poput GPRS-a koriste slične protokole poput IP-a tako da metode opisane za IP rade i s njima. Za ispravno usmjeravanje, svaki posredni usmjerivač mora imati tablicu usmjeravanja kako bi znao kamo poslati sljedeći paket. Ove tablice usmjeravanja jedan su od najboljih izvora informacija ako se istražuje digitalni kriminal i pokušava se pronaći napadača. Kako bi se to učinilo potrebno je pratiti pakete napadača, obrnuti rutu slanja i pronaći računalo s kojeg je paket došao [11].

4.6.3. Analitika šifriranog prometa

S obzirom na širenje TLS enkripcije na internetu procjenjuje se da polovica svih zlonamjernih programa koristi TLS kako bi izbjegla otkrivanje. Analiza kriptiranog prometa provjerava promet kako bi identificirala kriptirani promet koji dolazi od zlonamjernog softvera i drugih prijetnji otkrivanjem sumnjivih kombinacija karakteristika TLS-a, obično prema neuobičajenim mrežama ili poslužiteljima. Drugi pristup analizi šifriranog prometa koristi generiranu bazu podataka otisaka prstiju, iako su te tehnike kritizirane jer hakeri ih lako zaobilaze i netočne su [11].

4.6.4. Mrežna forenzika na Internetu

Internet može biti bogat izvor digitalnih dokaza uključujući pregledavanje weba, e-poštu, grupe za diskusije, chat i peer-to-peer promet. Na primjer, zapisi web poslužitelja mogu se koristiti za prikaz kada ili ako je osumnjičenik pristupio informacijama koje se odnose na kriminalnu aktivnost. Računi e-pošte često mogu sadržavati korisne dokaze. Zaglavlja e-pošte lako se krivotvore pa se mrežna forenzika može koristiti za dokazivanje točnog podrijetla inkriminirajućeg materijala. Mrežna forenzika također se može koristiti kako bi se otkrilo tko koristi određeno računalo izdvajanjem podataka o korisničkom računu iz mrežnog prometa [11].

5. Forenzička istraga

Cilj svake istrage računalnog sigurnosnog incidenta je utvrditi je li se incident dogodio i ako je kako se dogodio. Istražitelj bi trebao biti siguran da je prikupio dovoljno informacija kako bi utvrdio je li se incident dogodio ili nije. Trebao bi biti siguran da je prikupio što je moguće više zloćudnih informacija iz sustava bez izazivanja bilo kakvih nepotrebnih promjena u samom sustavu. Alati koje istražitelj koristi ne bi trebali stvarati ključeve registra ili datoteke na sustavu koji se istražuje jer to može štetiti istrazi. Informacije se mogu izvući iz fizičke memorije (tj. RAM-a), a sadržaj ključeva registra i datoteka također se može dohvatiti. Stoga, prije nego što se datoteke otvore ili kopiraju iz sustava koji se istražuje treba zabilježiti podatke koji će biti izmijenjeni, a aktivnost koja se provodi nad datotekom treba dokumentirati. Jednom kada se nađe u sustavu, zlonamjerni softver će općenito ostaviti trag ili neki dokaz koji ukazuje na njegovu prisutnost. Kada se zlonamjerni softver instalira, u sustavu se stvaraju datoteke. Mogu se dodati ključevi registra ili se može dodati vrijednost postojećem ključu registra. Da bi zlonamjerni softver bio aktivan i učinkovit, mora postojati u nekom trenutku kao pokrenuti proces, čak i nakratko. Konačno, mnogi oblici zlonamjernog softvera otvorit će portove na sustavu. Network backdoors i trojanci će općenito otvoriti portove u načinu rada za slušanje kako bi omogućili napadaču da se poveže s njima i preuzme kontrolu nad sustavom žrtve. IRC botovi će s druge strane, otvoriti port klijenta kako bi se povezali na IRC poslužitelj na Internetu. Napadač tada može kontrolirati velik broj sustava slanjem jedne naredbe na IRC kanal na koji su botovi spojeni. Ne ostavlja svaki zlonamjerni softver sve gore navedene tragove, iako će većina ostaviti neke [3].

5.1. „Infekcijski vektori“

Da bi otkrio zlonamjerni softver na Windows sustavu, istražitelj prvo mora razumjeti kako zlonamjerni softver dospijeva u sustav i što radi nakon što se aktivira na tom sustavu. Put koji može donijeti zlonamjerni softver na sustav odnosno „infekcijski vektor“ može biti nešto jednostavno kao CD-ROM. U danima prije nego što su internetske veze bile sveprisutne kao danas, jedan od „infekcijskih vektora“ virusima bila je razmjena datoteka putem disketa. Korisnici bi uzeli datoteke iz jednog sustava i kopirali ih na disketu. Ako su datoteka ili datoteke bile zaražene virusom, kada bi se disketa stavila u pogon drugog sustava i datoteke kopirale na taj sustav, virus bi također bio kopiran. Nagli rast interneta devedesetih godina prošlog stoljeća

pružio je još jedan vektor infekcije. Svrha interneta bila je brzo i učinkovito dijeljenje datoteka i informacija između geografski udaljenih lokacija. Vektori infekcije počeli su uključivati privitke e-pošte, internetska preuzimanja, itd. Svaki komunikacijski put koji omogućuje legitiman pristup sustavu postao je potencijalni vektor infekcije. U današnje vrijeme zlonamjerni softver može biti postavljen na kompromitirani sustav od strane napadača različitim mehanizmima. Taj napadač može biti neka osoba koja sjedi za svojim računalom tisućama kilometara daleko i pristupa sustavu zbog slabe ili lako pogodljive administratorske lozinke ili bi isto tako lako mogao biti legitimni korisnik koji sjedi za konzolom sustava. Preglednik i drugi mehanizmi osim e-pošte mogu pružiti puteve zlonamjernom softveru za zarazu sustava. Napadač može prevariti korisnika da posjeti web stranicu koja iskorištava ranjivost u sigurnosnoj konfiguraciji preglednika ili u samom pregledniku i preuzima kod u sustav korisnika [3].

5.2. Rootkit

Rootkit je zbirka alata i uslužnih programa koje napadač koristi kako bi prikrio svoju prisutnost na kompromitiranom sustavu i osigurao potreban pristup za svoje ponovne posjete. Na Windows sustavima rootkit-ovi povezuju API pozive i filtriraju output kako bi sakrili prisutnost napadača i njegove aktivnosti. Funkcionalnost u stilu Rootkita i sami rootkit-i postaju sve prisutniji kako vrijeme prolazi. Postoje dva načina rootkit-a za Windows sustave: kernel i korisnički rootkit način. Kernel rootkit-ovi potkopavaju temeljnu funkcionalnost operativnih sustava upotrebom sistemskih poziva i pristupa pozivima API funkcija. To se može učiniti učitavanjem upravljačkog programa uređaja (datoteke koje završavaju nastavkom .sys) koji presreće ili modificira kod koji izvršavaju procesi sustava. Kernel rootkit-ovi potkopavaju i ruše pouzdanu računalnu bazu sustava. Rootkit-ovi u korisničkom načinu rada na Windows sustavima općenito rade prepisivanjem datoteka na samom sustavu kao i korištenjem tehnika kao što su ubacivanje DLL-a i API spajanje. Ovi rootkit-ovi rade na isti način i u istom kontekstu kao i korisnik na sustavu. Rootkit-ovi se mogu otkriti preko Perl skripti, pogotovo one koji koriste tehnike ubacivanja DLL-a [3].

5.3. Datoteke i mape

Kada trojanski konj ili network backdoor zarazi sustav datoteke se stvaraju na žrtvinom sustavu. U mnogim slučajevima sustavu se dodaju nove mape. U drugim slučajevima, datoteke koje čine zlonamjerni softver dodaju se u direktorije koji se već nalaze u sustavu kao što je %WINDIR%\system32. Osim postavljanja datoteka u sustav, trojanci i backdoori moraju imati sredstva za osiguravanje postojanosti koja osiguravaju da se pokreću kada se sustav ponovno pokrene ili da nastave s radom kada se korisnik odjavi. Zlonamjerni softver ostaje skriven jer se pokreće automatski bez ikakve interakcije korisnika. Jedno mjesto na kojem zlonamjerni softver ostavlja trag su mape za polazne programe. Do te mape se može doći desnim klikom na gumb starta u sustavu Windows i onda lijevim klikom na opciju *Pokreni.* Prilikom ulaska u tu opciju upiše se naredba shell:common startup koja nas odvede u mapu za polazne programe. Programi Autoruns i AutoStartViewer su izvrsni alati za pregled ovih područja pokretanja programa. Obadva programa su alati koji se mogu koristiti za pregled sadržaja direktorija i ključeva registra gdje se može sakrivati malware. Oba alata korisniku pružaju grafičko korisničko sučelje što ih čini lakima za pregled, ali teškima za korištenje tijekom aktivnosti odgovora na incidente. Posebno se to odnosi u slučajevima kada istražitelj ne želi praviti datoteke na tvrdi disk lokalnog sustava. Autoruns ipak pruža zanimljivu mogućnost za nadvladavanje ovog problema. Umjesto pružanja opcije Spremi ili Spremi kao… pruža opciju kopiraj u međuspremnik. Koristeći pomoćni program kao što je netcat, istražitelj bi mogao pokrenuti Autoruns s CD-a s alatima za odgovor na incidente, a zatim upotrijebiti drugu mogućnost za slanje sadržaja međuspremnika netcat slušatelju na drugom sustavu. Ipak treba pripaziti da se dohvate svi podaci iz međuspremnika prije izvoza podataka iz Autorunsa u njega. AutoStart Viewer pruža mogućnost spremanja prikazanih informacija u datoteku ili njihovog ispisa. Ako se datoteke dodane u sustav ne nalaze na ovim lokacijama za pokretanje može biti teško pronaći ih. Dvije tehnike za lociranje novododanih ili nedavno pristupanih datoteka su pretraživanje na temelju datuma stvaranja ili zadnjeg pristupa datotekama ili osnovno skeniranje sustava kada je u dobrom odnosno neinficiranom stanju. Prva tehnika uključuje skeniranje svih datoteka na sustavu i prikupljanje njihove posljednje izmjene, zadnjeg pristupa i datuma stvaranja (zajednički naziv "MAC vremena") za analizu. Alternativna metoda traženja nedavno pristupanih datoteka je korištenje alata kao što je afind.exe iz FoundStonea za traženje datoteka kojima je posljednji put pristupljeno unutar određenog vremenskog okvira. Alati kao što su afind.exe, mac-match.exe ili posebno dizajnirane Perl skripte sa sličnim funkcijama omogućit će istražitelju da locira datoteke u sustavu s zadnjim vremenima pristupa unutar

određenih parametara kao što je pristup u posljednjih deset minuta ili posljednja dvadeset i četiri sata. Bez neke vrste alata za pokretanje osnovnog skeniranja (tj. prikupljanje MAC vremena, hash datoteka, drugih informacija iz datoteka u određenom trenutku) datoteka u sustavu teško se može utvrditi jesu li nove datoteke dodane u sustav. Alati koji izvode ovu funkciju mogu jednostavno dobiti popis datoteka zajedno s njihovim MAC vremenima ili mogu biti dovoljno sofisticirani da izračunaju hashove datoteka. Izračunavajući hash datoteke tijekom osnovnog skeniranja i uspoređujući ga s hashovima izračunatim tijekom kasnijih skeniranja, administrator bi mogao odrediti koje su se datoteke na neki način promijenile. Matematički algoritmi koji se koriste za izračunavanje hashova datoteke proizveli bi različite hashove za istu datoteku ako se promijeni samo jedan bit. Mogu se razviti alati za snimanje snimke sustava, grupiranje datoteka zajedno s njihovim veličinama, verzijama i hashovima koji se nalaze na sustavu kada je taj sustav prvi put instaliran. Međutim, nedostaci takvog alata su da bi te alate trebalo redovito pokretati, a osnovne informacije o legitimnim datotekama u sustavu trebale bi se ažurirati kad god se instalira zakrpa ili nova aplikacija. Ovo bi moglo dobro funkcionirati na maloj mreži koja se sastoji od nekoliko sustava, ali ne bi bilo dobro na mreži s mnogo sustava raštrkanih po različitim uredima, gradovima ili državama. Perl skripte koje se povezuju s udaljenim sustavima i skeniraju područja pokretanja sustava uključujući datoteke, direktorije i ključeve registra mogu se kreirati i redovito pokretati za skeniranje kritičnih poslužitelja ili pokrenuti tijekom razdoblja niske aktivnosti na sustavu za skeniranje manje kritičnih sustava kao što su korisničke radne stanice. Informacije prikupljene takvim skriptama mogu se pohraniti na središnjoj lokaciji, a zatim povezati i pregledati prema potrebi. Još jedan način kako se datoteke mogu dodati u sustav odnosi se na planirane zadatke. Planirani zadaci mogu se dodati u sustav putem at.exe. Zadaci koji se dodaju u sustav izvršit će se u svoje zakazano vrijeme što planirane zadatke čini izvrsnim mjestom za održavanje postojanosti malwarea i backdoora na zaraženom sustavu. Kada se planirani zadatak doda u sustav kreira se datoteka u direktoriju %WINDIR%\Tasks s nastavkom .job [3].

5.4. Ključevi registra

Trojanski konji i network backdoors-i često ostavljaju tragove svoje prisutnosti u ključu registra jer moraju ostati aktivni bez interakcije korisnika kada se sustav ponovno pokrene. Takav malware najčešće će stvoriti vrijednost u sveprisutnom ključu "Run": HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run. Vrijednosti stvorene u ovom ključu pokrenut će se prilikom pokretanja Windowsa i to je vrlo popularna vrijednost koju koriste autori softvera za stvaranje postojanosti svojih proizvoda. Na primjer, na većini sustava mogu se vidjeti unosi za RealPlayer, WinAmp i druge softvere instalirane na sustavu. Postoje i drugi ključevi registra koji pružaju sličnu funkcionalnost kao prethodno navedeni ključ ako su prisutni u registru sustava, a to su: HKEY_LOCAL_MACHINE\Sofware\Microsoft\Windows\CurrentVersion\RunOnce, HKEY_LOCAL_MACHINE\Sofware\Microsoft\Windows\CurrentVersion\RunOnceEx i HKEY_LOCAL_MACHINE\Sofware\Microsoft\Windows\CurrentVersion\RunServices. Isti skupovi ključeva koji se nalaze u HKEY_CURRENT_USER također će pružiti neke od istih funkcionalnosti. Skriptirano rješenje koristeći Perl ili reg.exe može brzo i jednostavno dohvatiti sadržaj ovih ključeva. Uz ove ključeve registra trebalo bi i ostale ključeve registra provjeriti. HKEY_CLASS_ROOT\exefile\shell\open\command je ključ registra koji govori sustavu kako se treba ponašati kada je datoteka sa .exe ekstenzijom pokrenuta. Neki malware-i točnije backdoori izmijene ovaj ključ na način da su pokrenuti kad god je izvršna datoteka pokrenuti. Sličnu funkcionalnost kao ovaj ključ imaju ključevi: HKEY_CLASS_ROOT\batfile\shell\open\command
HKEY_CLASS_ROOT\comfile\shell\open\command

Ovi ključevi registra odnose se na datoteke s ekstenzijama .bat i .com. Sveukupno gledano kada broj mjesta u registru koje istražitelj treba pregledati što se tiče malwarea dosta je mal. Postoji ograničen broj ključeva koji će osigurati potreban stupanj postojanosti malwarea tijekom ponovnih pokretanja i prijava [3].

5.5. Procesi

Svaki malware na sustavu mora biti pokrenut kao proces kako bi ga napadač mogao upotrijebiti ili iskoristiti. Ako je binarni program za malware u sustavu on je neučinkovit i bezopasan dok se ne pokrene i izvodi kao proces. Dok se to ne dogodi nema otvorenih portova

niti bilo čega drugog sumnjivog ili zlonamjernog osim niza 1 i 0 koji ispunjavaju neke sektore na disku. Međutim, napadač će poduzeti sve korake kako bi osigurao da onaj tko koristi sustav ne primijeti da se proces pokreće ili izvodi. Skrivanje procesa od administratora ili korisnika nije toliko teško i moglo bi se usporediti se preimenovanjem datoteka na sustavu. Važno je napomenuti kako upravitelj zadataka ne prikazuje potpuni put do slike procesa koji se izvodi ili naredbenog retka koji se koristi za pokretanje procesa. Vidjet će se sumnjivi procesi gdje su nazivi datoteka pogrešno napisani, ali morat će se koristiti alate kao što je tlist.exe da se vidi naredbeni redak korišten za pokretanje procesa i punu stazu do izvršne slike procesa [3].

5.6. Otvoreni portovi

Još jedno područje gdje neki malware ostavlja trag svoje prisutnosti su mrežne veze. Network backdoors otvorit će priključak za napadača na koji se može spojiti i preuzeti kontrolu nad sustavom. To će se pojaviti u izlazu netstat.exe programa kao krajnja točka u načinu slušanja. Jedan posebno poznati network backdoor bio je NetBus, a prema zadanim postavkama slušao bi port 12345 u verzijama 1.4 i 1.5. Od verzije 2.0 NetBus je postao legitiman alat za daljinsko upravljanje, a autori su lobirali kod antivirusnih tvrtki da se uklone otisci programa za novije verzije alata. Drugi backdoori kao što su Back Orifice i SubSeven bi slušali zadane portove. Međutim, ovi se backdoor-i mogu konfigurirati pomoću aplikacije koju su dostavili njihovi autori tako da napadač može promijeniti portove na koje se veže i na kojima čeka veze. Unatoč tome, network backdoors će općenito otvoriti priključak poslužitelja kojeg sluša i čekati da se napadač poveže. Ovo će se pojaviti u izlazu netstata kao aktivna veza sa stanjem navedenim kao slušanje. Korištenje alata kao što su openports.exe ili fport.exe omogućuje istražitelju da izvede mapiranje procesa na priključak kako bi odredio koji je proces vezan za priključak. Ostali malware-i, poput IRC bota, također će biti vidljivi u odlaznim mrežnim vezama. Botovi će otvoriti port klijenta kako bi se povezali s poslužiteljem na Internetu. Ova klijentska veza pojavit će se kao aktivna veza navedena kao uspostavljena i izgledat će slično drugim takvim klijentskim vezama kao što su one napravljene putem preglednika ili klijenata e-pošte. Jedino što IRC poslužitelji općenito slušaju veze na portu 6667. Odlazne veze na IRC poslužitelj će se pojaviti sa stranom IP adresom i portom 6667 navedenim kao port [3].

5.7. Servisi

Mnogo puta autori malwarea dizajniraju neke svoje male stvari da se instaliraju kao usluga. Instaliranje malwarea kao usluge je još jedan način da se održi postojanost zlonamjernog softvera, bez obzira na to što se događa u sustavu. Ako network backdoor radi kao usluga korisnici se mogu odjaviti, ali sve dok sustav radi backdoor će biti aktivan i dostupan napadaču. Osim toga, backdoor će raditi sa svim privilegijama lokalnog sustava dajući mu veću razinu pristupa sustavu. Nakon što se backdoor instalira kao usluga nije potrebna nikakva interakcija korisnika kako bi se sustav otvorio za iskorištavanje od strane napadača odnosno backdoor usluga će raditi sve dok sustav radi. Jedan od načina instaliranja backdoor-a kao usluge je korištenje uslužnog programa srvany.exe koji omogućuje pokretanje bilo koje Windows aplikacije kao usluge. Kad se backdoor instalira kao servis, on se pojavi u HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services ključu registra. Ovdje se pohranjuju informacije o uslugama kao što su postavke pokretanja sustava. Umjesto da koristi uređivač registra za stvaranje ovih vrijednosti registra, napadač može jednostavno skriptirati potrebne naredbe u batch datoteci pomoću alata kao što je reg.exe. Sve potrebne aplikacije tada se mogu uključiti i pokrenuti pomoću izvršnog povezivača kao što je Elite Wrap. Lociranje backdoor-a instaliranih kao usluga može biti trivijalan zadatak sve dok imate dostupne prave alate. Jedna metoda je korištenje uređivača registra za ručno pretraživanje registra dok druga uključuje povezivanje s API-jem upravitelja kontrole usluge korištenjem odgovarajućeg applet-a upravljačke ploče ili desnim klikom na ikonu Ovaj PC na radnoj površini i odabirom opcije „Upravljanje“ iz padajućeg izbornika. Druga mogućnost je korištenje Perl skripti za dohvaćanje usluga instaliranih na sustavu, bez obzira na njihovo stanje pomoću SCM API-ja [3].

5.8. Forenzičko poslužiteljski projekt alat

Forenzičar treba metodologiju i alate koji će mu omogućiti brzo i učinkovito prikupljanje podataka iz više sustava ako je potrebno tako da može donositi odluke i dati smjernice u vezi s daljnjim radnjama. Svrha forenzičko poslužiteljskog projekt alata je pružiti okvir za izvođenje forenzički ispravnog prikupljanja podataka iz potencijalno kompromitiranih sustava. Projekt to postiže prikupljanjem podataka i njihovim prijenosom na poslužitelj koji čeka putem mrežnog sučelja sustava. Na ovaj način datoteke se ne zapisuju u potencijalno ugroženi sustav jer će to potencijalno ugroziti kasniju istragu. Forenzičko poslužiteljski projekt alat se sastoji od komponente poslužitelja koja se nalazi na sustavu kojim upravlja istražitelj i

klijentskih komponenti koje istražitelj stavlja na vanjsku memoriju za korištenje na sustavima žrtve. Komponente klijenta dohvaćaju informacije iz sustava žrtve i šalju ih poslužitelju. Komponente klijenta komuniciraju s poslužiteljem pomoću ključnih riječi. Kada klijent želi da poslužitelj poduzme određenu radnju, poslat će ključnu riječ, a poslužitelj će izvesti skup unaprijed definiranih radnji na temelju te ključne riječi. Forenzičko poslužiteljski projekt alat koristi sljedeće ključne riječi:

1. PODACI - komponenta klijenta šalje ključnu riječ podatak poslužitelju kada želi poslati podatke, kao što su podaci prikupljeni iz datoteke, izlaz vanjske naredbe ili podaci prikupljeni pomoću Perl funkcija. Nakon što su podaci zapisani u datoteku, poslužitelj će izračunati MD5 i SHA-1 hashove na datoteci i zabilježiti ih u datoteku dnevnika slučaja.
2. DATOTEKA - Ključna riječ datoteka koristi se da serveru javi kako se datoteka kopira iz klijentskog sustava, a prethodi joj naredba podaci. Podaci o datoteci koje šalje naredba podaci uključuju puni put datoteke, MAC vremena, vlasnika te MD5 i SHA-1 hashove. Nakon slanja naredbe datoteka poslužitelj odgovara s OK. Kada se primi taj odgovor, klijent će kopirati datoteku na poslužitelj. Nakon što se datoteka kopira, poslužitelj će ponovno izračunati MD5 i SHA-1 hashove za datoteku i usporediti ih s hashovima izračunatim prije kopiranja datoteke. Poslužitelj to čini kako bi provjerio kako nije bilo pogrešaka ili promjena u datoteci tijekom prijenosa.
3. LOG - Klijent šalje ovu naredbu poslužitelju kada želi dodati unos u datoteku dnevnika slučaja.
4. CLOSELOG - Ovo je posljednja naredba koju klijent šalje poslužitelju, govoreći poslužitelju da više nema podataka za slanje. Kada primi ovu naredbu, poslužitelj će dodati jedan posljednji unos u datoteku dnevnika slučaja i zatim izračunati MD5 i SHA-1 hashove za datoteku dnevnika slučaja.

Komponente klijenta komuniciraju s poslužiteljem koristeći TCP/IP kako bi pružile veću razinu fleksibilnosti u različitim mrežnim okruženjima [3].

5.9. Skeneri portova i analizatori mrežnog protokola

Skeneri portova omogućuju istražitelju da odredi koji su portovi otvoreni na udaljenom sustavu. Oni se mogu koristiti usporedno s istragom kako bi se utvrdilo postoje li otvoreni portovi koji se ne pojavljuju u izlazu netstat.exe programa ili alata za mapiranje procesa u port

kao što je openports.exe. Ako istražitelj otkrije otvorene portove pomoću skenera portova, ali ne pronađe nikakve naznake da je taj isti port otvoren i koristi alate na samom sustavu, to može ukazivati na sumnjivu aktivnost na sustavu. Ako istražitelj otkrije neobičan port otvoren na sustavu, to može ukazivati na prisutnost špijunskog softvera ili uljeza. Portovi za koje je skener portova otkrio da su otvoreni općenito su u načinu rada slušanja, što znači da se neki softver na sustavu vezao za port i čeka veze s udaljenih sustava. Mnogi skeneri portova šalju TCP ili SYN paket kako bi započeli trosmjerno TCP rukovanje. Ako je port otvoren, on će odgovoriti s potvrdom sinkronizacije odnosno SYN-ACK paketom, pokazujući da je port spreman prihvatiti vezu. Skener portova će zatim poslati natrag potvrdu odnosno ACK paket nakon čega slijedi završni odnosno FIN paket. Neki skeneri portova će poslati samo SYN paket, a nakon što prime SYN-ACK paket od udaljenog glavnog računala što ukazuje na otvoreni port će poslati natrag paket za resetiranje odnosno RST. Ako je port zatvoren, udaljeni host će poslati natrag paket sa skupom RST i ACK paketa. Skeneri portova ne samo da mogu otkriti istražitelju koji su portovi otvoreni, već također mogu pružiti informacije o ciljnom operativnom sustavu i servisima koji slušaju otvorene portove. Najpoznatiji skeneri portova su netcat, portqry i nmap. Analizator mrežnog protokola ili sniffer radi tako da kopira sve pakete koji prolaze žicom. Analizator mrežnog protokola omogućuje istražitelju da kopira sav promet s mreže i analizira ga kako bi vidio što različiti sustavi govore jedni drugima. Istražitelj može upotrijebiti mrežni sniffer kad reagira na incident na način ako sumnja da žrtvin sustav ima npr. instaliran virus trojanca tada istražitelj može odlučiti uhvatiti pakete kako bi utvrdio je li netko povezan s trojancem i ako jest, koje naredbe šalje. Treba napomenuti da su analizatori mrežnog protokola izvrsni alati kada se koriste u svrhu rješavanja problema i za određivanje postoje li neki drugi pogođeni sustavi na mreži. Oni se mogu koristiti za utvrđivanje problema s protokolom ili vremenom vezanim uz mrežni promet i za lociranje određenih vrsta prometa. Najpoznatiji analizatori mrežnog protokola su NetMon, Netcap, Windump, Analyzer i Ethereal [3].

6. Zaključak

Sve dok računalni sustavi i mreže budu dizajnirani, instalirani i upravljani od strane ljudi događati će se incidenti. Mnogi su sigurnosni incidenti rezultat djelovanja pojedinca ili grupe, pa će bez obzira na to što se dogodi ljudi uvijek biti uključeni u incident. Kao posljedica toga računalna forenzika će biti nužna u otkrivanju kriminalnog djelovanja putem Interneta. Složenost operativnih sustava i aplikacija je porasla kako bi se zadovoljile potrebe korisnika, ali napor i vještina potrebni za napad na stotine sustava u isto vrijeme dramatično su se smanjili. Svatko s internetskom vezom može preuzeti i pokrenuti kod zlonamjernog softvera, obično ne radeći ništa osim pritiskanja običnog gumba. Sredstva napada mogu se sastojati od zlonamjernih web stranica usmjerenih na ranjivosti web preglednika, zlonamjernih privitaka e-pošte ili izravnih, ručnih pokušaja pojedinca da iskoristi poznate ranjivosti. Kada napadač pristupi udaljenom Windows sustavu elementi napadačevog sustava postaju vidljivi na žrtvinom sustavu. Nakon što je napadač uspješno dobio pristup sustavu, imat će vidljivu sesiju s udaljenim sustavom. Napadačeve aktivnosti mogu biti vidljive u njegovim vlastitim zapisima. Sve datoteke koje su kopirane sa sustava žrtve ostaju vidljive na računalu napadača osim ako se ne poduzmu posebni koraci da se osigura njihovo potpuno brisanje. Kopiranje datoteke također ostavlja trag na sustavu žrtve kao barem promjena u posljednjem vremenu pristupa datotekama. Imati to na umu iznimno je važno kada istražujete incident. Jednako je važno razumjeti tehničku prirodu sustava, kako funkcionira i gdje tražiti dokaze. Napadači i zlonamjerni korisnici poduzimaju i poduzimati će korake kako bi osigurali da njihove aktivnosti ostanu skrivene od pogleda vlasnika sustava i istražitelja, posebno od alata sustava kao što su Event Viewer i Upravitelj zadataka jer ne prikazuju potpuni put do izvršne slike za svaki proces. Ove informacije su dostupne pomoću dodatnih alata s kojima većina ljudi možda nije upoznata. Stoga, istražiteljima će biti zadatak otkriti pokušaje napada putem takvih alata. Kada se incidenti dogode, može se provesti čitav spektar aktivnosti odgovora na incident. Nakon što se podaci prikupe, te podatke treba analizirati i koristiti za razvoj slike aktivnosti u sustavu. Zbog sveprisutnosti Windows operativnih sustava i aplikacija, Windows sustavi su posebno sve više izloženi napadima i ugrožavanju. Iz svega zaključno moramo shvatiti kako je računalni kriminal sveprisutan i treba biti oprezan na svakom koraku pri korištenju računalnog sustava.

7. Literatura

[1] A. Brkić, Š. Babić i A. Blažević, »Računalni kriminal / cyber kriminal,« 20 Siječanj 2013.. [Mrežno]. Available: https://security.foi.hr/wiki/index.php/Ra%C4%8Dunalni_kriminal/cyber_kriminal.html. [Posljednji pristup 5 Srpanj 2022.].

[2] Z. s. s. i. s. R. Hrvatske, »Ministarstvo obrane Republike Hrvatske,« Listopad 2019.. [Mrežno]. Available: https://www.morh.hr/wp-content/uploads/2019/10/sigurnost-komunikacije-elektronickom-postom.pdf. [Posljednji pristup 10. srpanj 2022.].

[3] H. Carvey, Windows Forensics and Incident Recovery, Addison-Wesley, 2005.

[4] »Salvation Data Technology,« [Mrežno]. Available: https://www.itbusinessedge.com/security/digital-forensic-tools/. [Posljednji pristup 15 Srpanj 2022.].

[5] R. Jones, Internet Forensics, O´Reilly, 2005.

[6] »Infosavvy,« [Mrežno]. Available: https://info-savvy.com/what-is-malware-forensics/#:~:text=It%20is%20a%20way%20of,and%20reason%20for%20the%20attack.. [Posljednji pristup 22 Srpanj 2022.].

[7] L. Mukherjee, Sectigo store, 23 Kolovoz 2020. [Mrežno]. Available: https://sectigostore.com/blog/malware-analysis-what-it-is-how-it-works/. [Posljednji pristup 25 Srpanj 2022.].

[8] N. Lord, »Digital Guardian,« 29 Rujan 2020.. [Mrežno]. Available: https://digitalguardian.com/blog/what-are-memory-forensics-definition-memory-forensics#:~:text=Memory%20forensics%20(sometimes%20referred%20to,tracks%20on%20hard%20drive%20data.. [Posljednji pristup 30 Srpanj 2022.].

[9] S. Kapiswe, »https://www.technotification.com/,« 27 Ožujak 2019. [Mrežno]. Available: https://www.technotification.com/2019/03/best-memory-forensics-tools.html. [Posljednji pristup 30 Srpanj 2022.].

[10] »https://www.geeksforgeeks.org/,« 04 Ožujak 2022.. [Mrežno]. Available: https://www.geeksforgeeks.org/mobile-forensics-definition-uses-and-principles/. [Posljednji pristup 2 kolovoz 2022.].

[11] K. Afifi-Sabet, 7 prosinac 2021. [Mrežno]. Available: https://www.itpro.com/cyber-attacks/31660/what-is-network-forensics. [Posljednji pristup 3 kolovoz 2022.].