Zaštita

od zlonamernih programa

Istražite koncepte, alatke i tehnike za analizu i ispitivanje Windows zlonamernih programa

kompjuter biblioteka

Packt›

Monnappa K A

Zaštita

od zlonamernih programa

Monnappa K A

kompjuter biblioteka

Packt›

Izdavač:

kompjuter biblioteka

Obalskih radnika 4a, Beograd

Tel: 011/2520272

e-mail: kombib@gmail.com

internet: www.kombib.rs

Urednik: Mihailo J. Šolajić

Za izdavača, direktor:
Mihailo J. Šolajić

Autor: Monnappa K A

Prevod: Biljana Tešić

Lektura: Miloš Jevtović

Slog: Zvonko Aleksić

Znak Kompjuter biblioteke:
Miloš Milosavljević

Štampa: „Pekograf“, Zemun

Tiraž: 500

Godina izdanja: 2019.

Broj knjige: 515

Izdanje: Prvo

ISBN: 978-86-7310-538-3

Learning Malware Analysis

Monnappa K A

ISBN 978-1-78839-250-1

CIP - Каталогизација у публикацији
Народна библиотека Србије, Београд,
се добија на захтев

O AUTORU

Monnappa K A je zaposlen u kompaniji „CiscoSystems“ kao istražitelj za informacionu bezbednost - fokusira se na obaveštajne informacije o pretnjama i istraživanje naprednih napada na Internetu. Član je istražnog odbora BlackHat, autor bezbednosnog programa LimonLinux, pobednik takmičenja „VolatilityPluginContest 2016“ i jedan od osnivača istraživačke zajednice za računarsku bezbednost „Cysinfo“. Organizovao je programe obuke na različitim konferencijama o bezbednosti, uključujući BlackHat, FIRST, OPCDE i DSCI. Redovno sprovodi treninge na konferenciji o bezbednosti BlackHat u Sjedinjenim Američkim Državama, Aziji i Evropi.

Izražavam zahvalnost DanieluCuthbertu i dr Michaelu Spreitzenbarthu, jer su u rasporedu svojih ogromnih obaveza odvojili vreme da bi pregledali moju knjigu. Hvala Sharonu Raju, Prashantu Chaudhariu, Shrilekhai Inaniji i ostatku „Packt“ tima za podršku. Hvala Michaelu Schecku, Chrisu Friu, Scottu Heideru i mojim kolegama iz kompanije „Cisco CSIRT“ na ohrabrenju. Hvala Michaelu Haleu, Andreu Caseu, Jamieju Leviju, Aaronu Valtersu, Mattu Suicheu, Ilfaku Guilfanovu i Lenniju Zeltseru koji su me inspirisali i motivisali svojim radom. Hvala Sajanu Shettiu, Vijai Sharma, Gavinu Reidu, Leviu Gundertu, Joanni Kretovicz, Marti Strzelec, Venkateshu Murthiu, Amitu Malikuu i Ashvinu Patilu za beskrajnu podršku. Hvala autorima drugih knjiga, veb stranica, blogova i alatki koji su dali doprinos mom znanju, a, samim tim, i pisanju ove knjige

O RECENZENTIMA

Daniel Cuthbert je direktor za istraživanje bezbednosti u kompaniji „BancoSantander“. U svojoj karijeri dugoj više od 20 godina na napadačkoj i odbrambenoj strani video je evoluciju hakovanja, od malih grupa znatiželjnih umova, do današnjih organizovanih kriminalnih mreža i nacionalnih država. Član je odbora „BlackHatReviewBoard“ i jedan od autora projekata OWASP Testing Guide (2003) i OWASP Application Security Verification Standard (ASVS).

Dr Michael Spreitzenbarth je zaposlen u sektoru IT bezbednosti već nekoliko godina, od završetka diplomskog rada na temu forenzike mobilne telefonije. Doktorat iz oblasti Android forenzike i analize zlonamernih programa stekao je 2013. godine. Zatim se zaposlio u međunarodnoj kompaniji CERT i internom RED timu. Svakodnevno se bavi bezbednošću mobilnih sistema i forenzičkom analizom pametnih telefona i sumnjivih mobilnih aplikacija, ali i ispitivanjem bezbednosnih incidenata i simuliranjem napada na sajber bezbednost.

„PACKT“ TRAŽI AUTORE KAO ŠTO STE VI

Ako ste zainteresovani da postanete autor za „Packt“, posetite stranicu authors.packtpub.com i prijavite se. Mi smo radili sa hiljadama programera i profesionalaca i pomogli smo im da podele svoje mišljenje sa globalnom tehničkom zajednicom. Možete da popunite uopštenu prijavu, da se prijavite za specifičnu temu za koju tražimo autore ili da nam pošaljete neke svoje ideje.

Kratak sadržaj

Sadržaj

POGLAVLJE 5

POGLAVLJE 6

POGLAVLJE 7

POGLAVLJE 8

POGLAVLJE 9

POGLAVLJE 10

UVOD

Napredak računarske i internet tehnologije je promenio naše živote i način na koji se u organizacijama vodi poslovanje. Međutim, evolucija tehnologije i digitalizacija su dovele i do razvoja sajber kriminala. Sve veća opasnost od sajber kriminala za važne infrastrukture, centre podataka i privatne/javne, odbrambene, energetske, vladine i finansijske sektore predstavlja jedinstveni izazov za svakoga - od pojedinca, do velikih korporacija. U ovakvim sajber napadima koristi se zlonamerni softver (poznat i kao Malware) za finansijske krađe, špijunaže, sabotaže, krađu intelektualne svojine i problematične političke motive.

S obzirom da su napadači postali sofisticirani i da vrše napredne zlonamerne napade, otkrivanje i ispitivanje takvih upada i reakcija na njih su od ključne važnosti za stručnjake informacione bezbednosti. Analiza zlonamernih programa je veština koju morate da posedujete u borbi protiv naprednih zlonamernih programa i ciljanih napada. Drugim rečima, da biste naučili da vršite analizu zlonamernih programa, potrebni su vam vreme i strpljenje.

U ovoj knjizi ćete kroz analizu zlonamernih programa naučiti koncepte, alatke i tehnike za razumevanje ponašanja i karakteristika Windows zlonamernih programa. Upoznaćete osnovne koncepte analize zlonamernih softvera, a zatim ćete postepeno preći na naprednije koncepte analize koda i forenzike memorije. Da biste bolje mogli da razumete koncepte, u knjizi se koriste uzorci zlonamernih programa iz realnog sveta, zaražene slike memorije i vizuelni grafikoni. Osim toga, dato je dovoljno informacija koje će vam pomoći da razumete potrebne koncepte i, gde god je moguće, obezbeđeni su dodatni izvori za dalje čitanje.

Ako ste početnik u oblasti analize zlonamernih programa, ova knjiga će vam pomoći da započnete analizu, a ako ste iskusni u ovoj oblasti, da poboljšate svoje dodatno znanje. Ukoliko učite analizu zlonamernih programa da biste izvršili forenzičko ispitivanje, da biste reagovali na incident ili zbog zabave, ova knjiga omogućava da ostvarite svoje ciljeve.

ZA KOGA JE OVA KNJIGA

Ako ste osoba čiji je posao da reaguje na incidente, istražitelj za sajber bezbednost, administrator sistema, analitičar zlonamernih programa, forenzičar, student ili znatiželjni stručnjak za bezbednost koji je zainteresovan da nauči ili poboljša veštine za analizu zlonamernih programa, ova knjiga je za vas.

ŠTA OBUHVATA OVA KNJIGA

U Poglavlju 1, Uvod u analizu zlonamernih programa, predstavićemo čitaocima koncept analize zlonamernih programa, tipove analize zlonamernih programa i kreiranje izolovanog laboratorijskog okruženja za analizu tih programa.

U Poglavlju 2, Statička analiza, upoznaćete alatke i tehnike za ekstrahovanje informacija o metapodacima iz zlonamernih binarnih datoteka. Videćete kako se upoređuju i klasifikuju uzorci zlonamernih programa. Naučićete kako se utvrđuju različiti aspekti binarnih datoteka bez izvršavanja tih datoteka.

U Poglavlju 3, Dinamička analiza, upoznaćete alatke i tehnike za utvrđivanje ponašanja zlonamernih programa i interakciju tih programa sa sistemom. Naučićete kako se pribavljaju indikatori mreže i indikatori zasnovani na hostu koji su povezani sa zlonamernim programima.

U Poglavlju 4, Asemblerski jezik i osnove disasembliranja, objašnjen je osnovni asemblerski jezik, a naučićete i veštine koje su potrebne za izvršenje analize koda.

Poglavlje 5, Disasembliranje pomoću alatke IDA, obuhvata funkcije IDA Pro disasemblera. Naučićete kako se ovaj disasembler koristi za izvršavanje analize statičkog koda (disasembliranje).

U Poglavlju 6, Debagiranje zlonamernih binarnih datoteka, naučićete tehnike debagiranja binarnih datoteka pomoću debagera x64dbg i IDA Pro. Takođe ćete naučiti kako se koristi debager za kontrolu izvršenja programa i manipulaciju ponašanjem programa.

U Poglavlju 7, Funkcije i postojanost zlonamernih programa, opisane su različite funkcije zlonamernih programa primenom obrnutog inženjeringa. Ovo poglavlje obuhvata i različite metode postojanosti koje koriste zlonamerni programi.

U Poglavlju 8, Umetanje koda i hooking tehnika, naučićete uobičajene tehnike injektovanja koda koje koriste zlonamerni programi za izvršenje zlonamernog koda u kontekstu legitimnog procesa. U ovom poglavlju su opisane i hooking tehnike koje koriste zlonamerni programi za preusmeravanje kontrole na zlonamerni kod, radi nadgledanja, blokiranja ili filtriranja izlaza API-a. Naučićete kako se analiziraju zlonamerni programi koji koriste injektovanje i hooking tehnike.

Poglavlje 9, Tehnike maskiranja zlonamernih programa, obuhvata kodiranje, šifrovanje i tehniku pakovanja koji se u zlonamernim programima koriste za sakrivanje informacija.

Naučićete različite strategije za dekodiranje/dešifrovanje podataka i raspakivanje zlonamernih datoteka.

U Poglavlju 10, „Hvatanje“ zlonamernih programa korišćenjem forenzike memorije, naučićete detektovanje zlonamernih komponenata korišćenjem forenzike memorije. Upoznaćete različite Volatility plaginove za detektovanje i identifikovanje forenzičkih artefakata u memoriji.

U Poglavlju 11, Detektovanje naprednih zlonamernih programa korišćenjem forenzike memorije, upoznaćete tehnike koje se u naprednim zlonamernim programima koriste za sakrivanje od forenzičkih alatki. Naučićete da ispitujete i detektujete komponente administratorskog paketa korisničkog režima i zaštićenog režima rada.

Da biste dobili maksimum iz ove knjige:

Poznavanje programskih jezika C i Python bilo bi korisno (posebno da biste razumeli koncepte koji su predstavljeni u poglavljima 5, 6, 7, 8 i 9). Ako ste napisali nekoliko linija koda i posedujete osnovno znanje o programskim konceptima, moći ćete da izvučete maksimum iz ove knjige.

Ako nemate znanja iz oblasti programiranja, ipak ćete moći da shvatite osnovne koncepte analize zlonamernih programa koji su predstavljeni u poglavljima 1, 2 i 3. Međutim, možda ćete malo teže razumeti koncepte koji su predstavljeni u ostalim poglavljima. Da biste bolje razumeli koncepte, dato je dovoljno informacija i dodatnih izvora u svakom poglavlju.

PREUZIMANJE KOLORNIH SNIMAKA

Takođe smo obezbedili PDF datoteku sa kolornim slikama ekrana/dijagrama. Možete da je preuzmete na adresi https://www.packtpub.com/sites/default/files/downloads/LearningMalwareAnalysis_ ColorImages.pdf.

Upotrebljene konvencije

Postoji veliki broj konvencija teksta koje su upotrebljene u ovoj knjizi.

`CodeInText` - Ukazuje na primere koda, nazive datoteka, nazive direktorijuma, registre i vrednosti ključeva, ekstenzije datoteka, nazive putanje, skraćene URL-ove, korisnički unos i Twitter postove. Evo i primera: „Instalirajte preuzetu datoteku slike diska `WebStorm-10*.dmg` kao drugi disk u vaš sistem.“

Svaki unos komandne linije će biti prikazan na sledeći način:

```
$ sudo inetsim
INetSim 1.2.6 (2016-08-29) by Matthias Eckert & Thomas
Hungenberg Using log directory: /var/log/inetsim/
Using data directory: /var/lib/inetsim/
```

Kada želimo da privučemo pažnju na određeni deo bloka koda ili ispis, relevantne linije ili stavke će biti ispisane zadebljanim slovima:

```
$ python vol.py -f tdl3.vmem --profile=WinXPSP3x86 ldrmodules -p 880
Volatility Foundation Volatility Framework 2.6
Pid Process Base InLoad InInit InMem MappedPath
--- ----------- -------- ----- ------- ----- ----------------------------
880 svchost.exe 0x10000000 False False False \WINDOWS\system32\TDSSoiqh.dll
880 svchost.exe 0x01000000 True False True \WINDOWS\system32\svchost.exe
880 svchost.exe 0x76d30000 True True True \WINDOWS\system32\wmi.dll
880 svchost.exe 0x76f60000 True True True \WINDOWS\system32\wldap32.dll
```

Iskošena slova - Ukazuju na novi izraz, važnu reč ili reči, naziv zlonamernog programa i kombinaciju tastera. Evo i primera: „Pritisnite *Ctrl* + *C* za kopiranje."

Tekst na ekranu - Reči u menijima ili okvirima za dijalog se prikazuju ovakvim tekstom. Evo i primera: „Izaberite **System info** u kartici **Administrator**."

Napomene ili važna obaveštenja prikazani su ovako.

Saveti i trikovi su prikazani ovako.

KONTAKTIRAJTE SA NAMA

Povratne informacije od naših čitalaca su uvek dobrodošle.

Osnovne povratne informacije - Pošaljite e-mail na adresu informatori@kombib.rs i u naslovu poruke napišite naslov knjige. Ako imate bilo kakva pitanja o bilo kom aspektu ove knjige, pošaljite nam e-mail na adresu informatori@kombib.rs.

Štamparske greške - Iako smo preduzeli sve mere da bismo obezbedili tačnost sadržaja, greške mogu da se potkradu. Ako pronađete grešku u ovoj knjizi, bili bismo zahvalni ako biste nam to prijavili. Posetite stranicu http://www.packtpub.com/submit-errata, kliknite „Ostavite komentar" i unesite detalje.

Piraterija - Ako na Internetu pronađete ilegalnu kopiju naših knjiga, u bilo kojoj formi, molimo vas da nas o tome obavestite i pošaljete adresu lokacije ili naziv web sajta. Kontaktirajte sa nama na adresi informatori@kombib.rs i pošaljite nam link ka sumnjivom materijalu.

Ako ste zainteresovani da postanete autor - Ako postoji tema za koju ste specijalizovani i zainteresovani ste da pišete ili sarađujete na nekoj od knjiga, pogledajte vodič za autore na adresi authors.packtpub.com.

RECENZIJA

Kada pročitate i upotrebite ovu knjigu, zašto ne biste napisali vaše mišljenje na sajtu sa kojeg ste je poručili? Potencijalni čitaoci tada mogu da iskoriste vaše mišljenje da bi odlučili o kupovini, mi u „Packtu“ možemo da saznamo šta mislite o našim proizvodima, a naši autori mogu da imaju povratne informacije o svojoj knjizi.

1

Uvod u analizu zlonamernih programa

Broj sajber napada koji su usmereni na vlade, vojsku i javni i privatni sektor je nesumnjivo u porastu. Ovi napadi se fokusiraju na targetiranje pojedinaca ili organizacija da bi se izdvojile vredne informacije. Ponekad su navodno povezani sa sajber kriminalom ili sa grupama koje sponzorišu države, ali ih mogu vršiti i pojedinačne grupe radi postizanja svojih ciljeva. U većini tih napada koristi se zlonamerni softver (koji se naziva i malware) da bi se zarazile mete. Za otkrivanje i istraživanje sajber napada i odbranu od njih potrebni su znanje, veštine i alatke.

U ovom poglavlju ćete naučiti sledeće:

- šta su zlonamerni programi i koja je njihova uloga u sajber napadima
- analiza zlonamernih programa i njihov značaj u digitalnoj forenzici
- različite vrste analiza zlonamernih programa
- kreiranje laboratorijskog okruženja
- različiti izvori za dobijanje uzoraka zlonamernih programa

1. ŠTA SU ZLONAMERNI PROGRAMI?

Zlonamerni programi su kodovi koji izvršavaju zlonamerne radnje. Oni mogu biti u obliku izvršive datoteke, skripta, koda ili nekog drugog softvera. Napadači koriste zlonamerne programe za krađu poverljivih informacija, špijuniranje zaraženog sistema ili preuzimanje kontrole nad sistemom. Ovi programi obično uđu u sistem bez vašeg pristanka, a mogu se isporučiti pomoću različitih kanala za komunikaciju, kao što su e-mail, Veb ili USB drajver.

Ovo su neke od zlonamernih radnji koje izvršavaju zlonamerni programi:

- prekid računarskih operacija
- krađa poverljivih informacija, uključujući lične, poslovne i finansijske podatke
- neovlašćeni pristup sistemu žrtve
- špijuniranje žrtava
- slanje neželjene e-pošte
- distribuirani napadi radi blokiranja usluga (DDOS – Distributed Denial of Service)
- zaključavanje datoteka na računaru i njihovo zadržavanje radi iznude otkupa

Malware je širok pojam koji se odnosi na različite vrste zlonamernih programa, kao što su „trojanci“, virusi, „crvi“ i administratorski paketi (rootkits). Postoje različite vrste zlonamernih programa. Neki od tih programa su kategorizovani na osnovu svojih funkcija i vektora napada kao što je navedeno ovde:

- **Virus ili „crv“** – Zlonamerni program koji se može umnožiti i širiti na druge računare. Virus zahteva korisničku intervenciju, dok „crv“ može da se širi bez korisničke intervencije.
- **„Trojan“** – Zlonamerni program koji se „prerušava“ u neki uobičajeni program da bi ga korisnici na prevaru instalirali na svoje sisteme. Kada je zlonamerni program instaliran, on može da izvrši zlonamerne radnje, kao što su krađa poverljivih informacija, otpremanje datoteka na server napadača ili nadgledanje veb kamera.
- **Backdoor / Remote Access Trojan (RAT)** – Ovo je vrsta zlonamernog programa **„Trojan“** koja omogućava napadaču da pristupi komandama na kompromitovanom sistemu i da ih izvrši.
- **Adware** - Zlonamerni program koji korisniku prikazuje neželjene reklame (oglase) - one se, obično, isporučuju besplatnim preuzimanjem sadržaja sa Interneta i mogu prisilno da instaliraju softver na vaš sistem
- **Botnet** - Ovo je grupa računara zaraženih istoimenim zlonamernim programima (pod nazivom *botovi*). Botovi čekaju da prime instrukcije sa servera za upravljanje i kontrolu koji kontroliše napadač. Napadač može da izda komandu ovim botovima da izvrše zlonamerne radnje, kao što su DDOS napadi ili slanje nepoželjne e-pošte.
- **Information stealer** - Zlonamerni program koji je dizajniran za krađu poverljivih podataka sa zaraženog sistema, kao što su podaci o klijentima banaka ili uneti pritisci na taster. Neki od ovih zlonamernih programa su programi za beleženje pritisnutih tastera (key loggers), špijunski programi (spyware), „njuškala“ (sniffers) i „hvataljke“ oblika (form grabbers).

- **Ransomware** - Zlonamerni program zadržava sistem radi iznude otkupa, tako što korisnicima ne dozvoljava pristup računarima ili tako što šifrira datoteke.
- **Rootkit** - Zlonamerni program koji napadaču obezbeđuje privilegovani pristup zaraženom sistemu i prikriva svoje prisustvo ili prisustvo drugog softvera
- **Downloader ili dropper** - Zlonamerni program koji je dizajniran za preuzimanje ili instaliranje dodatnih zlonamernih komponenata

Korisni podaci koji će vam pomoći da razumete terminologiju i definicije zlonamernih programa dostupni su na adresi https://blog. malwarebytes. com/glossary/.

Klasifikacija zlonamernih programa zasnovana na funkcijama možda nije uvek izvodljiva, zato što jedan zlonamerni program može da sadrži više funkcija koje mogu da pripadaju različitim prethodno pomenutim kategorijama. Na primer, zlonamerni program može da sadrži komponentu „crva“, a taj „crv“ može da skenira mrežu, tražeći sisteme koji su podložni napadima, i da „ispusti“ drugu zlonamernu komponentu nakon uspešne eksploatacije, kao što su *backdoor* ili *ransomware*.

Klasifikacija zlonamernih programa se može izvršiti i na osnovu motiva napadača. Na primer, ako se zlonamerni program koristi za krađu ličnih, poslovnih ili vlasničkih informacija, može se klasifikovati kao *crimeware* ili *comoddity malware*. Ako se zlonamerni program koristi za targetiranje određene organizacije ili industrije radi krađe/prikupljanja informacija za špijunažu, može se klasifikovati kao *targeted* ili *espionage malware*.

2. ŠTA JE ANALIZA ZLONAMERNIH PROGRAMA?

Analiza zlonamernih programa je proučavanje „ponašanja“ ovih programa. Cilj je da se shvati rad tih programa i da se oni otkriju i eliminišu. Analiza obuhvata analiziranje sumnjive binarne datoteke u bezbednom kruženju da bi bile identifikovane karakteristike i funkcije te datoteke, tako da bi se mogla izgraditi bolja zaštita organizacione mreže.

3. ZAŠTO TREBA VRŠITI ANALIZU ZLONAMERNIH PROGRAMA?

Osnovni motiv izvršenja analize je izdvajanje informacija iz uzoraka zlonamernih programa. Te informacije mogu da pomognu u reagovanju na incident koji je izazvao takav program. Cilj je da se analizom zlonamernih programa utvrde mogućnosti tih programa i

da se oni detektuju i izoluju. Te informacije takođe pomažu u utvrđivanju prepoznatljivih obrazaca koji se mogu koristiti za „lečenje“ i sprečavanje budućih infekcija. Ovo su neki od razloga zbog kojih ćete izvršiti analizu zlonamernih programa:

- Utvrđivanje karakteristika i namene zlonamernih programa. Na primer, to vam može pomoći da utvrdite da li je zlonamerni program kradljivac informacija, HTTP bot, spam bot, rootkit, keylogger ili RAT i tako dalje.
- Bolje razumevanje kako je sistem kompromitovan i kakav je njegov uticaj
- Identifikovanje indikatora mreže povezanih sa zlonamernim programom, koji onda mogu da se koriste za detekciju sličnih infekcija nadgledanjem mreže. Na primer, ako tokom analize utvrdite da zlonamerni program kontaktira sa određenim *domenom/IP adresom*, možete koristiti ovaj domen/IP adresu za kreiranje potpisa i nadgledanje mrežnog saobraćaja da bi bili identifikovani svi hostovi koji su uspostavili kontakt sa domen/IP adresom.
- Izdvajanje indikatora zasnovanih na hostovima, kao što su nazivi datoteka i ključevi registratora, koji se mogu koristiti za utvrđivanje sličnih infekcija praćenjem zasnovanim na hostu. Na primer, ako saznate da zlonamerni program kreira ključ registratora, možete koristiti taj ključ registratora kao indikator za kreiranje potpisa ili za skeniranje mreže da biste identifikovali hostove koji imaju iste ključeve registratora.
- Utvrđivanje namere i motiva napadača. Na primer, ako tokom analize otkrijete da zlonamerni program krade podatke o klijentima banaka, možete zaključiti da je motiv napadača novčana dobit.

Timovi za špijunažu vrlo često koriste indikatore koji su utvrđeni analizom zlonamernih programa da bi klasifikovali napad i pripisali te indikatore poznatim pretnjama. Analiza zlonamernih programa može pomoći da dobijete informacije ko bi mogao da bude napadač (konkurencija, napadačka grupa koju sponzoriše određena država i tako dalje).

4. VRSTE ANALIZA ZLONAMERNIH PROGRAMA

Da biste razumeli rad i karakteristike zlonamernih programa i procenili njihov uticaj na sistem, često ćete koristiti različite tehnike analize. Ovo je klasifikacija tehnika analize:

- **Statička analiza** - Ovo je proces analiziranja binarnih datoteka bez njihovog izvršavanja. Ova analiza je najlakša za izvršavanje, a omogućava da izdvojite metapodatke koji su povezani sa sumnjivom binarnom datotekom. Statička analiza možda neće otkriti sve potrebne informacije, ali ponekad može obezbediti

zanimljive informacije koje pomažu da odredite gde da usmerite vaše naknadne analize. U Poglavlju 2, *Statička analiza*, predstavićemo alatke i tehnike za izdvajanje korisnih informacija iz zlonamernih binarnih datoteka pomoću statičke analize.

- **Dinamička analiza (analiza ponašanja) -** Ovo je proces izvršenja sumnjive binarne datoteke u izolovanoj sredini i nadgledanja njenog ponašanja. Ova tehnika analize je jednostavna za izvođenje i daje vredan uvid u aktivnost binarne datoteke tokom izvršenja. Korisna je, ali ne otkriva sve funkcije neprijateljskog programa. U Poglavlju 3, *Dinamička analiza*, biće reči o alatkama i tehnikama za određivanje ponašanja zlonamernih programa pomoću dinamičke analize.
- **Analiza koda -** Ovo je napredna tehnika koja se fokusira na analiziranje koda radi razumevanja načina na koji funkcinonišu binarne datoteke. Ona otkriva informacije koje se ne mogu utvrditi samo pomoću statičkih i dinamičkih analiza. Analiza koda se dalje deli na *statičku analizu koda* i *dinamičku analizu koda*. Statička analiza obuhvata rastavljanje sumnjive binarne datoteke i pregled koda radi razumevanja ponašanja programa, dok dinamička obuhvata kontrolisano debagovanje sumnjive binarne datoteke da biste razumeli funkcionalnost te datoteke. Za analiziranje koda potrebno je da razumete koncepte programskog jezika i operativnog sistema. U poglavljima 4, 5, 6, 7, 8 i 9 predstavićemo znanje, alatke i tehnike koji su potrebni za izvršavanje analize koda.
- **Analiza memorije (forenzika memorije) -** Ovo je tehnika analiziranja RAM memorije računara radi otkrivanja forenzičkih artefakata. Ovo je obično forenzička tehnika, ali integracija sa analizom zlonamernih programa će vam pomoći da razumete ponašanje tih programa nakon inficiranja. Analiza memorije je posebno korisna za utvrđivanje prikrivenih mogućnosti zlonamernih programa i mogućnosti koje treba izbegavati. Kako se izvršava analiza memorije naučićete u *poglavljima 10 i 11*.

Ako integrišete različite tehnike analize tokom izvršavanja analize zlonamernih programa, možete da otkrijete mnoštvo kontekstualnih informacija koje će se pokazati kao dragocene u ispitivanju zlonamernih programa.

5. KREIRANJE LABORATORIJSKOG OKRUŽENJA

Analiza neprijateljskog programa zahteva bezbedno i sigurno laboratorijsko okruženje da ne biste inficirali vaš sistem ili proizvodni sistem. Laboratorija za zlonamerne programe može biti veoma jednostavna ili kompleksna, u zavisnosti od resursa koji su vam dostupni

(hardver, softver za vizuelizaciju, Windows licenca i tako dalje). U ovom odeljku su data uputstva za kreiranje jednostavne lične laboratorije na jednom fizičkom sistemu koji se sastoji od *virtuelnih mašina (VM-ova)*. Ako želite da kreirate slično laboratorijsko okruženje, pratite instrukcije u nastavku ili pređite na sledeći odeljak (*Odeljak 6: Izvori zlonamernih programa*).

5.1 Laboratorijski zahtevi

Pre nego što počnete da kreirate laboratoriju, potrebno je da obezbedite *fizički sistem* koji pokreće osnovni operativni sistem *Linux*, *Windows* ili *macOS X* i instalirani softver za virtuelizaciju (kao što su *VMware* ili *VirtualBox*). Prilikom analiziranja izvršavaćete zlonamerne programe na virtuelnoj mašini koja se zasniva na Windowsu (Windows VM). Nakon što analizirate zlonamerne programe, virtuelnu mašinu možete da vratite u čisto stanje.

VMware Workstation za Windows i Linux možete preuzeti na adresi https://www.vmware.com/products/workstation/workstationevaluation.html, a VMware Fusion za macOS X na adresi https://www.vmware.com/products/fusion/fusionevaluation.html. VirtualBox za različite operativne sisteme možete preuzeti na adresi https://www.virtualbox.org/wiki/Downloads.

Radi kreiranja bezbednog laboratorijskog okruženja, treba da preduzmete neophodne mere predostrožnosti da biste sprečili da zlonamerni programi izađu iz virtuelizovanog okruženja i inficiraju fizički (host) sistem. Sledećih nekoliko napomena treba da imate na umu kada podešavate virtuelizovanu laboratoriju:

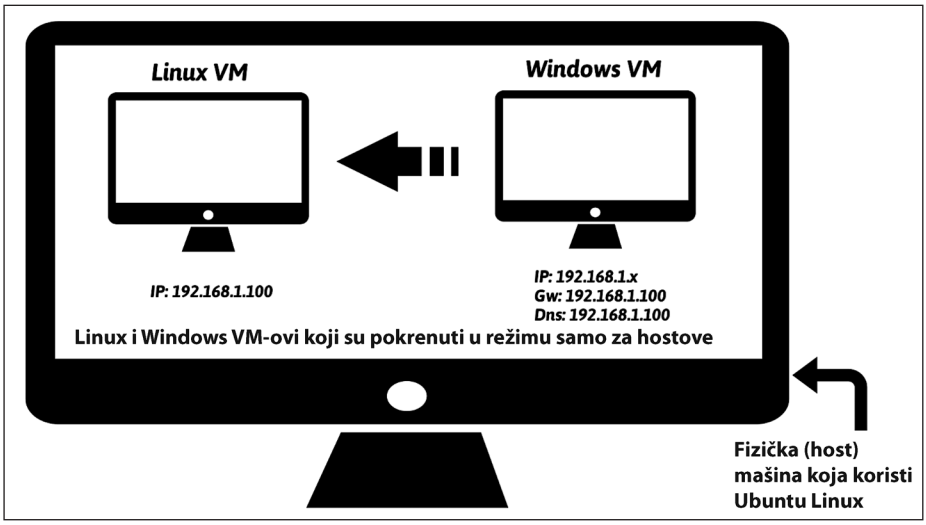
- Ažurirajte softver za virtuelizaciju. Ažuriranje je neophodno, jer zlonamerni programi mogu da iskoriste osetljivost softvera za virtuelizaciju, da izađu iz virtuelnog okruženja i da inficiraju host sistem.
- Instalirajte najnoviju kopiju operativnog sistema unutar virtuelne mašine (VM) i nemojte skladištiti nikakve osetljive informacije na virtuelnoj mašini.
- Ako tokom analiziranja zlonamernih programa ne želite da oni pristupe Internetu, treba da koristite režim mrežne konfiguracije *host-only* ili da ograničite mrežni saobraćaj u okviru laboratorijskog okruženja korišćenjem simuliranih servisa.
- Nemojte povezivati prenosive medijume koji se kasnije mogu koristiti na fizičkoj mašini, kao što su USB drajveri.
- Pošto ćete da analizirate Windows zlonamerne programe (obično Executable ili DLL), preporučuje se da izaberete osnovni operativni sistem, kao što su Linux ili macOS X, umesto Windowsa. Ako izaberete osnovni operativni sistem, Windows zlonamerni programi neće moći da zaraze host mašinu, čak i ako izađu iz virtuelne mašine.

5.2 Pregled laboratorijske arhitekture

Laboratorijska arhitektura koja će biti upotrebljena u ovoj knjizi sastoji se od *fizičke mašine (pod nazivom host mašina)* koja koristi Ubuntu Linux sa instancama *Linux virtual machine (Ubuntu Linux VM)* i *Windows virtual machine (Windovs VM)*. Ove virtuelne mašine će biti konfigurisane tako da budu deo iste mreže i da koriste režim mrežne konfiguracije *host-only*, pa zlonamernim programima nije dozvoljen kontakt sa Internetom, a mrežni saobraćaj je sadržan u izolovanom laboratorijskom okruženju.

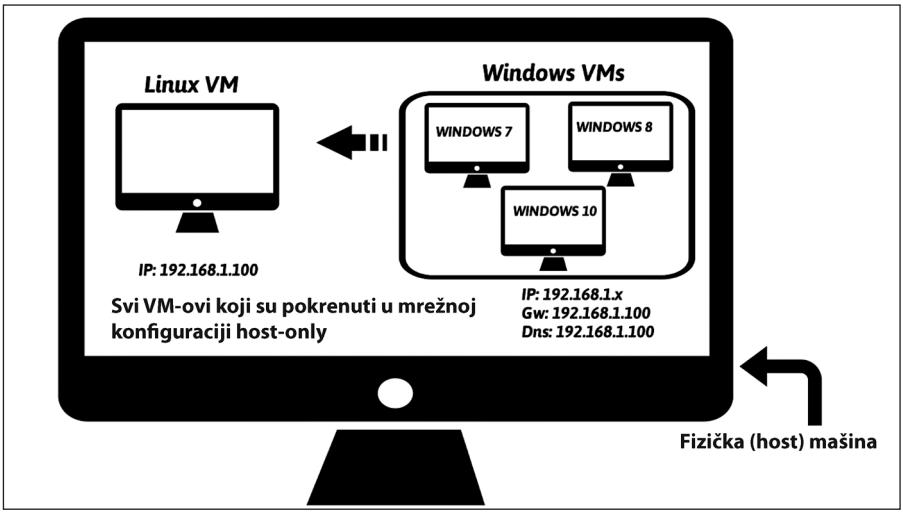
Windows VM je mesto na kome će zlonamerni programi biti izvršeni tokom analize, a *Linux VM* se koristi za nadgledanje mrežnog saobraćaja i biće konfigurisan da simulira internet servise (DNS, HTTP i tako dalje) da bi bio obezbeđen odgovarajući odgovor kada zlonamerni programi zahtevaju ove servise. Na primer, Linux VM će biti konfigurisan tako da obezbedi odgovarajući DNS odgovor kada zlonamerni programi zahtevaju servis DNS. Ovaj koncept je detaljno opisan u Poglavlju 3, *Dinamička analiza*.

Na sledećoj slici prikazana je jednostavna laboratorijska arhitektura koja će biti upotrebljena u ovoj knjizi. U ovom podešavanju *Linux VM* će biti unapred postavljen na IP adresu `192.168.1.100`, a IP adresa *Windows VM-a* će biti postavljena na `192.168.1.x` (gde je x broj od `1` do `254`, osim `100`). Podrazumevani mrežni prolaz (gateway) i DNS Windows VM će biti postavljeni na IP adresu Linux VM-a (to jest, na `192.168.1.100`), tako da se sav Windows mrežni saobraćaj usmerava kroz Linux VM. U sledećem odeljku ćete naučiti kako da podesite Linux VM i Windows VM u skladu sa ovim podešavanjem.



Ne morate se ograničavati na laboratorijsku arhitekturu koja je prikazana na prethodnoj slici. Dostupne su različite laboratorijske konfiguracije, ali ne možemo navesti uputstva o svakoj mogućoj konfiguraciji. U ovoj knjizi biće prikazano kako se podešava i koristi laboratorijska arhitektura koja je prikazana na prethodnoj slici.

Takođe je moguće podesiti laboratoriju sa više VM-ova koji koriste različite verzije Windowsa; to će vam omogućiti da analizirate uzorke zlonamernih programa na različitim verzijama operativnog sistema Windows. Primer konfiguracije koja sadrži više Windows VM-ova će biti sličan primeru prikazanom na sledećem dijagramu.



5.3 Podešavanje i konfiguracija Linux VM-a

Da bismo podesili Linux VM, koristićemo Linux distribuciju *Ubuntu 16.04.2 LTS* (`http://releases.ubuntu.com/16.04/`). Izabrao sam Ubuntu zato što je većina alatki razmatranih u ovoj knjizi unapred instalirana ili dostupna pomoću upravljača paketa *apt-get*. Ovo je postupak korak-po-korak za konfigurisanje distribucije Ubuntu 16.04.2 LTS na softverima *VMware* i *VirtualBox*. Pratite instrukcije koje su date ovde u skladu sa softverom za virtuelizaciju (*VMware* ili *VirtualBox*) koji je instaliran na vaš sistem.

Ako vam nisu poznati instaliranje i konfigurisanje virtuelnih mašina, pogledajte vodič za VMware na adresi http://pubs.vmware.com/workstation-12/topic/com.vmware.ICbase/ PDF/ workstation-pro-12-user-guide.pdf ili VirtualBox korisničko uputstvo (https://www.virtualbox.org/manual/UserManual.html).

1. Preuzmite Ubuntu 16.04.2 LTS sa adrese `http://releases.ubuntu.com/16.04/` i instalirajte ga na VMware Workstation/Fusion ili VirtualBox. Možete da instalirate neku drugu verziju Ubuntu Linuxa ukoliko znate da instalirate pakete i da rešavate probleme koji se odnose na zavisnost (dependency).
2. Instalirajte *Virtualization Tools* (alatke za virtuelizaciju) na operativni sistem Ubuntu, pa će se rezolucija Ubuntu ekrana automatski prilagoditi da odgovara geometriji monitora i da obezbedi dodatna poboljšanja, kao što je mogućnost deljenja sadržaja klipborda i kopiranja/lepljenja datoteka ili prevlačenja i otpuštanja datoteka na osnovnu *host mašinu* i *Linux virtuelnu mašinu*. Da biste instalirali alatke za virtuelizaciju na VMWare Workstation ili VMWare Fusion, možete da pratite postupak koji je naveden na adresi `https:/ kb.vmware.com/selfservice/microsites/search.do?language= en_US cmd=displayKC externalId=1022525` ili da pogledate video na adresi `https://youtu.be/ueM1dCk3o58`. Kada su alatke za virtuelizaciju instalirane, ponovo pokrenite sistem.
3. Ako koristite VirtualBox, morate da instalirate *Guest Additions softver* - da biste ga instalirali, u VirtualBox meniju izaberite **Devices | Insert guest additions CD image**. To će otvoriti Guest Additions Dialog Window. Zatim, kliknite na **Run** da biste aktivirali program za instalaciju sa virtuelnog diska. Potvrdite identitet pomoću lozinke kada se to od vas zatraži i ponovo pokrenite sistem.
4. Kada su instalirani operativni sistem Ubuntu i alatke za virtuelizaciju, pokrenite Ubuntu VM i instalirajte sledeće alatke i pakete.
5. Instalirajte *pip* – sistem za upravljanje paketima, koji se koristi za instaliranje paketa koji su napisani na Python jeziku i za upravljanje njima. U ovoj knjizi ćemo pokrenuti nekoliko Python skriptova. Neki od njih se zasnivaju na nezavisnim bibliotekama. Da biste automatizovali instalaciju nezavisnih paketa, treba da instalirate *pip*. Pokrenite sledeću komandu u terminalu da biste instalirali i nadgradili *pip*:

```
$ sudo apt-get update
$ sudo apt-get install python-pip
$ pip install --upgrade pip
```

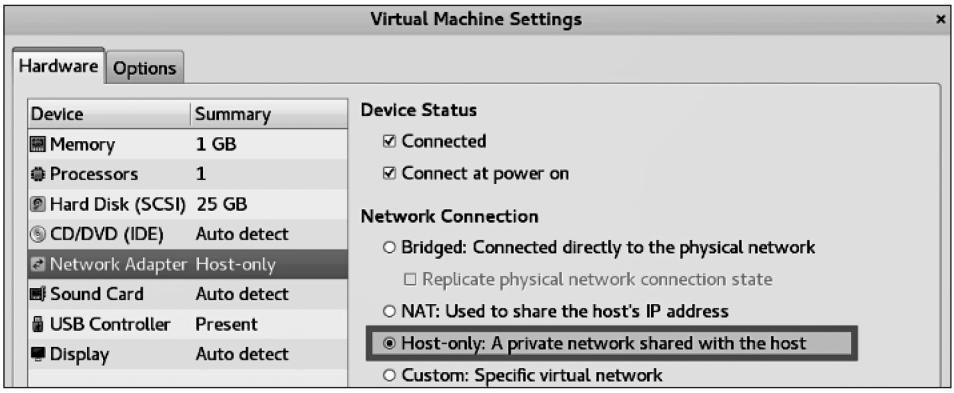
Ovo su neke od alatki i Python paketi koji ćemo koristiti u ovoj knjizi. Da biste ih instalirali, pokrenite sledeće komande u terminalu:

```
$ sudo apt-get install python-magic
$ sudo apt-get install upx
$ sudo pip install pefile
$ sudo apt-get install yara
$ sudo pip install yara-python
$ sudo apt-get install ssdeep
$ sudo apt-get install build-essential libffi-dev
python python-dev
\ libfuzzy-dev
$ sudo pip install ssdeep
$ sudo apt-get install wireshark
$ sudo apt-get install tshark
```

6. *INetSim* (`http://www.inetsim.org/index.html`) je moćan uslužni program koji omogućava simuliranje različitih internet servisa (kao što su DNS i HTTP) sa kojima će zlonamerni programi verovatno često komunicirati. Kasnije ćete shvatiti kako se konfiguriše INetSim za simuliranje servisa. Da biste instalirali INetSim, koristite komande koje su prikazane u sledećem kodu. Upotreba INetSima će biti detaljno razmatrana u Poglavlju 3, *Dinamička analiza*. Ako imate poteškoće prilikom instaliranja INetSima, pogledajte dokumentaciju (`http://www.inetsim.org/packages.html`):

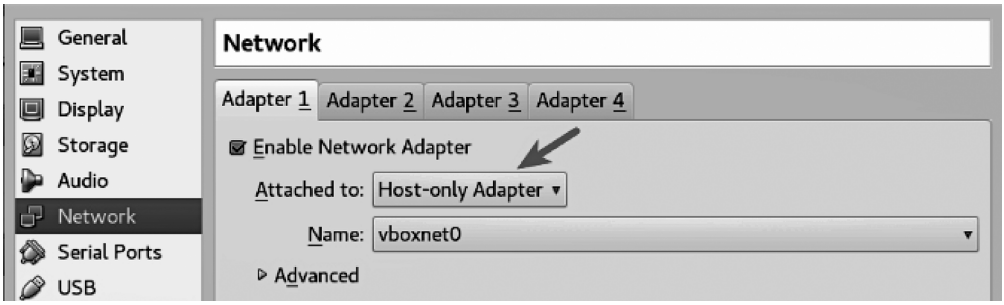
```
$ sudo su
# echo "deb http://www.inetsim.org/debian/ binary/" > \
/etc/apt/sources.list.d/inetsim.list
# wget -O - http://www.inetsim.org/inetsim-archive-signing-key.asc
| \
apt-key add -
# apt update
# apt-get install inetsim
```

7. Sada možete da instalirate Ubuntu VM u okviru laboratorije konfigurisanjem virtuelnog uređaja da biste mogli da koristite mrežni režim *samo za hostove*. Na VMWare softveru za virtuelizaciju pristupite opciji **Network Adapter Settings** i izaberite **Host-only mode,** kao što je prikazano na sledećoj slici. Sačuvajte postavke i ponovo pokrenite sistem.



U VirtualBoxu zatvorite *Ubuntu VM*, a zatim pristupite meniju **Settings**. Izaberite **Network** i promenite postavke adaptera u **Host-only Adapter,** kao što je prikazano na sledećem dijagramu. Kliknite na **OK**.

Kada u VirtualBoxu izaberete opciju Host-only adapter, naziv interfejsa ponekad može da se pojavi kao Not selected (Nije izabrano). U tom slučaju je potrebno prvo da kreirate najmanje jedan interfejs samo za hostove, tako što ćete pristupiti opcijama File | Preferences | Network | Host-only networks | Add host-only network. Kliknite na OK, a zatim pristupite meniju Settings. Izaberite Network i promenite postavke adaptera u Host-only Adapter, kao što je prikazano na sledećem snimku ekrana. Kliknite na OK.



8. Sada ćemo dodeliti statičku IP adresu `192.168.1.100` Ubuntu Linux VM-u. Da biste je dodelili, pokrenite Linux VM, otvorite terminalski prozor, ukucajte komandu `ifconfig` i zapišite naziv interfejsa. Moj naziv interfejsa je `ens33`, a vaš može biti drugačiji. Ako je drugačiji, potrebno je da izmenite sledeće korake u skladu sa tim nazivom. Otvorite datoteku `$sudogedit/etc/network/interfaces` pomoću sledeće komande:

```
$ sudo gedit /etc/network/interfaces
```

Dodajte sledeći unos na kraju datoteke (promenite `ens33` u naziv interfejsa na vašem sistemu) i memorišite ga:

```
auto ens33
iface ens33 inet static
address 192.168.1.100
netmask 255.255.255.0
```

Datoteka `/etc/network/interfaces` treba da izgleda kao ova koja je prikazana u sledećem kodu. Ovde je istaknut unos koji je upravo dodat:

```
# interfaces(5) file used by ifup(8) and ifdown(8)
auto lo
iface lo inet loopback

auto ens33
iface ens33 inet static
address 192.168.1.100
netmask 255.255.255.0
```

Zatim, restartujte Ubuntu Linux VM. U ovom trenutku IP adresa Ubuntu VM-a treba da je postavljena na `192.168.1.100`. Da biste proverili adresu, pokrenite sledeću komandu:

```
$ ifconfig
ens33 Link encap:Ethernet HWaddr 00:0c:29:a8:28:0d
inet addr:192.168.1.100 Bcast:192.168.1.255
Mask:255.255.255.0
inet6 addr: fe80::20c:29ff:fea8:280d/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:21 errors:0 dropped:0 overruns:0 frame:0
TX packets:49 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:5187 (5.1 KB) TX bytes:5590 (5.5 KB)
```

9. Sledeći korak je da konfigurišete *INetSim* da može da „osluškuje“ i da simulira sve servise na konfigurisanoj IP adresi `192.168.1.100`. Podrazumevano „osluškuje“ servise na lokalnom interfejsu (`127.0.0.1`) čija IP adresa treba da se promeni u `192.168.1.100`. Da biste je promenili, otvorite konfiguracionu datoteku koja se nalazi na adresi `/etc/inetsim/inetsim.conf` pomoću sledeće komande:

```
$ sudo gedit /etc/inetsim/inetsim.conf
```

Pristupite odeljku `service_bind_address` u konfiguracionoj datoteci i dodajte unos koji je prikazan ovde:

```
service_bind_address   192.168.1.100
```

Dodati (istaknuti) unos u konfiguracionoj datoteci treba da izgleda ovako:

```
# service_bind_address
#
# IP address to bind services to
#
# Syntax: service_bind_address <IP address>
#
# Default: 127.0.0.1
#
#service_bind_address 10.10.10.1
service_bind_address 192.168.1.100
```

DSN server INetSima će podrazumevano razrešiti sve nazive domena u `127.0.0.1`. Umesto toga, mi želimo da se naziv domena razreši u `192.168.1.100` (IP adresu Linux VM-a). Da biste razrešili naziv domena, pristupite odeljku `dns_default_ip` u konfiguracionoj datoteci i dodajte unos, kao što je prikazano ovde:

```
dns_default_ip  192.168.1.100
```

Dodati unos (koji je istaknut u sledećem kodu) u konfiguracionoj datoteci treba da izgleda ovako:

```
# dns_default_ip
#
# Default IP address to return with DNS replies
#
# Syntax: dns_default_ip <IP address>
#
# Default: 127.0.0.1
#
#dns_default_ip 10.10.10.1
dns_default_ip 192.168.1.100
```

Kada ste izmenili konfiguraciju, memorišite konfiguracionu datoteku i pokrenite glavni program INetSim. Proverite da li su svi servisi pokrenuti i da li `inetsim` „osluškuje“ `192.168.1.100`, kao što je istaknuto u sledećem kodu. Možete da prekinete servis pritiskom kombinacije tastera *CTRL+C*:

```
$ sudo inetsim
INetSim 1.2.6 (2016-08-29) by Matthias Eckert & Thomas Hungenberg
Using log directory: /var/log/inetsim/
Using data directory: /var/lib/inetsim/
Using report directory: /var/log/inetsim/report/
Using configuration file: /etc/inetsim/inetsim.conf
=== INetSim main process started (PID 2640) === Session ID: 2640
Listening on: 192.168.1.100
Real Date/Time: 2017-07-08 07:26:02
Fake Date/Time: 2017-07-08 07:26:02 (Delta: 0 seconds)
 Forking services...
 * irc_6667_tcp - started (PID 2652)
 * ntp_123_udp - started (PID 2653)
 * ident_113_tcp - started (PID 2655)
 * time_37_tcp - started (PID 2657)
 * daytime_13_tcp - started (PID 2659)
 * discard_9_tcp - started (PID 2663)
 * echo_7_tcp - started (PID 2661)
 * dns_53_tcp_udp - started (PID 2642)
 [..........REMOVED.............]
 * http_80_tcp - started (PID 2643)
 * https_443_tcp - started (PID 2644)
 done.
Simulation running.
```

10. U jednom trenutku biće potrebno da prenesete datoteke sa hosta na virtuelnu mašinu. Da biste omogućili prenos datoteka na *VMware*, isključite virtuelnu mašinu i pristupite meniju **Settings**. Izaberite **Options | Guest Isolation** i potvrdite izbor opcija **Enable drag and drop** i **Enable copy and paste**. Kliknite na **Save** da biste memorisali postavke.

    U VirtualBoxu isključite virtuelnu mašinu i izaberite **Settings | General | Advanced**, a zatim postavite **Shared Clipboard and Drag ‚n‘ Drop** na vrednost **Bidirectional**. Kliknite na **OK.**

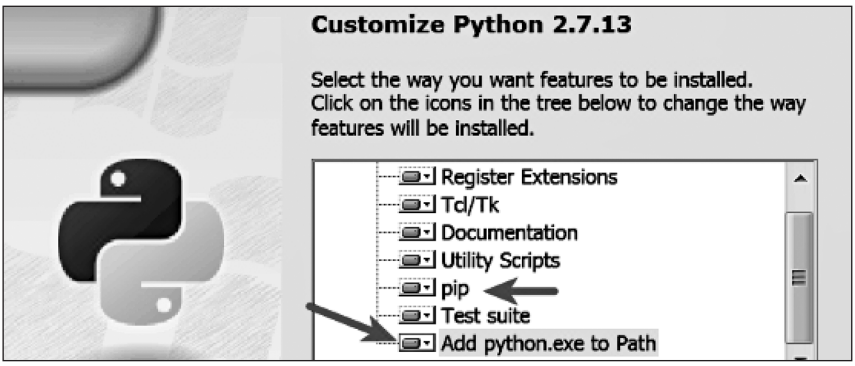
11. Sada je Linux VM konfigurisan da koristi režim *host-only*, a INetSim je podešen da simulira sve servise. Poslednji korak je da napravite snimak (čist snimak) i da mu dodelite naziv po vašem izboru da biste mogli da vratite virtuelnu mašinu u čisto stanje kada je potrebno. Da biste napravili snimak, na **Wmware workstationu** kliknite na **VM | Snapshot | Take Snapshot**, a na **Virtualboxu** na **Machine | Take Snapshot**.

Osim pomoću funkcije drag and drop, prenos datoteka možete izvršiti sa host mašine na virtuelnu mašinu i pomoću deljenih fascikli – pogledajte sledeću stranicu za VirtualBox (https://www.virtualbox.org/manual/ch04.html#sharedfolders), a za VMWare (https://docs.vmware.com/en/VMware-Workstation-Pro/14.0/com.vmware.ws.using.doc/GUID-AACE0935-4B43-43BA-A935-FC71ABA17803.html).

5.4 Podešavanje i konfiguracija Windows VM-a

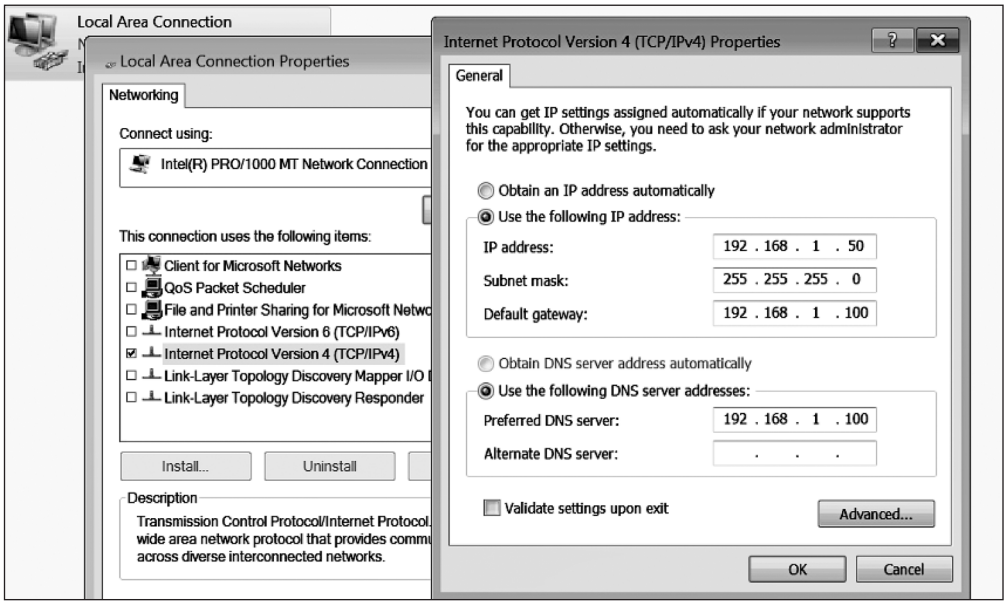
Pre podešavanja Windows VM-a potrebno je da prvo instalirate operativni sistem Windows (Windows 7, Windows 8 i tako dalje) po vašem izboru na softver za virtuelizaciju (kao što su VMware ili VirtualBox). Nakon što instalirate Windows, pratite sledeće korake:

1. Preuzmite Python sa adrese `https://www.python.org/downloads/`. Pobrinite se da preuzmete *Python 2.7.x* (kao što je 2.7.13); veći deo skriptova koji su upotrebljeni u ovoj knjizi su napisani za Python 2.7 verziju i možda neće pravilno funkcionisati u Python 3 verziji. Nakon što preuzmete datoteku, pokrenite program za instalaciju. Pobrinite se da izaberete opcije **pip** i **Add python.exe to Path**, kao što je prikazano na sledećem snimku ekrana. Instaliranje sistema pip će olakšati instaliranje nezavisnih Python biblioteka, a dodavanje Pythona putanji će olakšati pokretanje Pythona sa bilo koje lokacije.



2. Konfigurišite Windows VM tako da se pokrene u mrežnom konfiguracionom režimu **Host-only**. Da biste izvršili konfiguraciju u **VMwareu** ili **VirtualBoxu**, pristupite meniju **Network Settings** i izaberite opciju **Host-only mode**. Memorišite postavke i ponovo pokrenite sistem (ovaj korak je sličan koraku koji je opisan u odeljku *Podešavanje i konfiguracija Linux VM-a*).

3. Konfigurišite IP adresu Windows VM-a na `192.168.1.x` (izaberite bilo koju IP adresu, osim `192.168.1.100`, zato što je Linux VM podešen da koristi tu IP adresu) i podesite opcije **Default gateway** i **DNS server** na IP adresu Linux VM-a (to jest, na `192.168.1.100`), kao što je prikazano na sledećem snimku ekrana. Ova konfiguracija je potrebna da biste sav mrežni saobraćaj preusmerili kroz Linux VM kada izvršavate neprijateljski program na Windows VM-u.

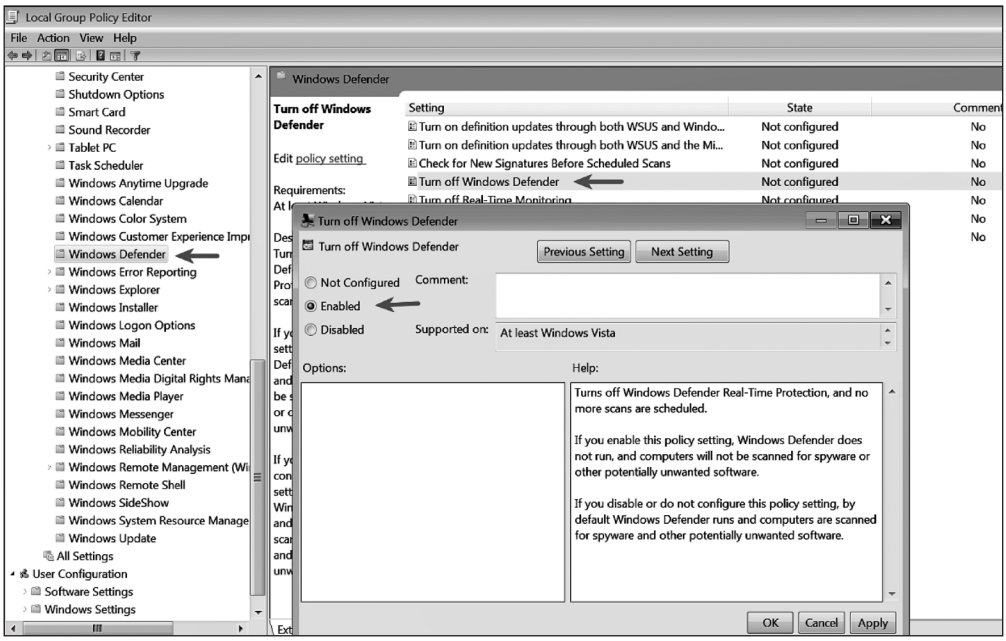


4. Pokrenite softvere **Linux VM** i **Windows VM**, a zatim se pobrinite da komuniciraju jedan sa drugim. Možete da proverite da li su ovi softveri povezani, tako što ćete pokrenuti komandu ping, kao što je prikazano na sledećem snimku ekrana:

```
C:\Users\test>ping 192.168.1.100

Pinging 192.168.1.100 with 32 bytes of data:
Reply from 192.168.1.100: bytes=32 time<1ms TTL=64
Reply from 192.168.1.100: bytes=32 time<1ms TTL=64
Reply from 192.168.1.100: bytes=32 time<1ms TTL=64
Reply from 192.168.1.100: bytes=32 time<1ms TTL=64
```

5. Windows Defender Service treba da bude onemogućen na Windows VM-u, jer može da ometa izvršavanje uzoraka zlonamernih programa. Da biste ga onemogućili, pritisnite kombinaciju *Windows taster* + R radi otvaranja menija Run, a zatim unesite *gpedit.msc* i pritisnite taster **Enter** da biste pokrenuli **Local Group Policy Editor**. U kartici sa leve strane **Local Group Policy Editora** pristupite stavkama **Computer Configuration | Administrative Templates| Windows Components | Windows Defender**. U kartici sa desne strane dva puta kliknite na opciju **Turn off Windows Defender policy** da biste je izmenili, a zatim izaberite **Enabled** i kliknite na **OK**:



6. Da biste mogli da prenesete datoteke (pomoću opcije drag and drop) i da kopirate sadržaj klipborda sa host mašine na Windows VM, pratite instrukcije koje su navedene u *koraku 7 u* odeljku *Podešavanje i konfiguracija Linux VM-a*.

7. Napravite čist snimak da biste mogli da vratite virtuelnu mašinu u čisto stanje nakon svake analize. Postupak za pravljenje snimka je naveden u *koraku 10 u* odeljku *Podešavanje i konfiguracija Linux VM-a*.

U ovom trenutku vaše laboratorijsko okruženje bi trebalo da bude spremno. Linux i Windows VM na čistom snimku treba da budu u mrežnom režimu **Host-only** i da komuniciraju jedan sa drugim. U ovoj knjizi će biti razmatrane različite alatke za analizu zlonamernih programa. Ako želite da koristite te alatke, možete ih kopirati na čist snimak virtuelne mašine. Radi ažuriranja, samo prenesite/instalirajte te alatke na virtuelne mašine i napravite novi čist snimak.

6. IZVORI ZLONAMERNIH PROGRAMA

Nakon što kreirate laboratoriju, biće vam potrebni uzorci zlonamernih programa da biste izvršili analizu. U ovoj knjizi su korišćeni različiti primeri zlonamernih programa, a pošto su ti uzorci iz stvarnih napada, odlučio sam da ih ne distribuiram, jer mogu da postoje pravni problemi koji se odnose na tu distribuciju. Ove uzorke (ili slične) možete pronaći tako što ćete pretražiti različita spremišta zlonamernih programa. U nastavku su navedeni neki izvori iz kojih možete dobiti uzorke zlonamernih programa za analizu. Neki od tih izvora omogućavaju da besplatno preuzmete uzorke zlonamernih programa (ili nakon besplatne registracije), a za druge izvore je potrebno da kontaktirate sa vlasnicima da biste kreirali nalog, nakon čega možete da dobijete uzorke:

- *Hybrid Analysis*: `https://www.hybrid-analysis.com/`
- *KernelMode.info*: `http://www.kernelmode.info/forum/viewforum.php?f=16`
- *VirusBay*: `https://beta.virusbay.io/`
- *Contagio malware dump*: `http://contagiodump.blogspot.com/`
- *AVCaesar*: `https://avcaesar.malware.lu/`
- *Malwr*: `https://malwr.com/`
- *VirusShare*: `https://virusshare.com/`
- *theZoo*: `http://thezoo.morirt.com/`

Možete da pronađete linkove za različite druge izvore zlonamernih programa na blogu Lennya Zeltsera `https://zeltser.com/malware-sample-sources/`.

Ako ni jedan od navedenih metoda ne funkcioniše, a želite da dobijete uzorke zlonamernih programa koji su korišćeni u ovoj knjizi, uspostavite kontakt sa autorom.

REZIME

Pre analiziranja zlonamernih programa važno je da kreirate izolovano laboratorijsko okruženje. Tokom izvršavanja analize zlonamernih programa obično ćete pokrenuti neprijateljski kod da biste posmatrali kako se on „ponaša“, tako da izolovano laboratorijsko okruženje sprečava slučajno širenje zlonamernog koda na vaš sistem ili proizvodne sisteme na mreži. U sledećem poglavlju ćete upoznati alatke i tehnike za izdvajanje vrednih informacija iz uzoraka zlonamernih programa korišćenjem *statičke analize*.