Centar Informacijske Sigurnosti

Linux distribucije za penetracijsko ispitivanje

rujan 2012.

CIS-DOC-2012-09-062

Upozorenje

Podaci, informacije, tvrdnje i stavovi navedeni u ovom dokumentu nastali su dobrom namjerom i dobrom voljom te profesionalnim radom CIS-ovih stručnjaka, a temelje se na njihovom znanju i petnaestak godina iskustva u radu u informacijskoj sigurnosti. Namjera je da budu točni, precizni, aktualni, potpuni i nepristrani.

Ipak, oni su dani samo kao izvor informacija i CIS ne snosi nikakvu izravnu ili posrednu odgovornost za bilo kakve posljedice nastale korištenjem podataka iz ovog dokumenta.

Ukoliko primijetite bilo kakve netočnosti, krive podatke ili pogreške u ovom dokumentu, ili imate potrebu komentirati sadržaj molimo Vas da to javite elektroničkom poštom na adresu info@CIS.hr.

O CIS-u

CIS izrađuje pregledne dokumente (eng. white paper) na teme iz područja informacijske sigurnosti koji će biti korisni zainteresiranoj javnosti, a u svrhu **podizanje njezine svijesti o informacijskoj sigurnosti** i **sposobnosti za čuvanje i zaštitu informacija i informacijskih sustava**. Pored toga, CIS razvija i održava mrežni portal www.CIS.hr kao referalnu točku za informacijsku sigurnost za cjelokupnu javnost; izrađuje obrazovne materijale namijenjene javnosti; organizira događaje za podizanje svijesti o informacijskoj sigurnosti u javnosti i pojedinim skupinama te djeluje u suradnji sa svim medijima.

CIS **okuplja mlade** zainteresirane za informacijsku sigurnost i radi na njihovom pravilnom odgoju i obrazovanju u području informacijske sigurnosti te pripremu za **profesionalno bavljenje informacijskom sigurnošću**.

Centar informacijske sigurnosti [CIS] nastao je 2010. godine na poticaj Laboratorija za sustave i signale[LSS] Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu, a kao posljedica 15togodišnjeg rada na istraživanju, razvoju i primjeni informacijske sigurnosti. LSS je među ostalim potaknuo osnivanje CARNetovog CERTa i sudjelovao u izradi Nacionalnog programa informacijske sigurnosti RH.

Smisao CISa je da bude **referentno mjesto za informacijsku sigurnost** za javnost, informatičare i posebno za mlade te da sustavno podiže njihovu svijest i sposobnosti u području informacijske sigurnosti.

Rad CISa podržava Ministarstvo znanosti, obrazovanja i sporta Republike Hrvatske, a omogućuju sponzori.

Prava korištenja

Sadržaj

1. Uvod

U današnje vrijeme Linux jezgra (eng. *Linux kernel*) je jedna od najzastupljenijih jezgri operacijskog sustava. Nad Linux jezgrom se razvio čitav niz operacijskih sustava. Razlog tome je činjenica da sustav Linux spada u slobodnu programsku podršku, što znači da ga svatko može koristiti, proučavati i mijenjati njegov izvorni kod. Različite inačice operacijskih sustava zasnovanih na Linux jezgri nazivaju se Linux distribucije (eng. *Linux distribution, distro*). Distribucije se vrlo često međusobno razlikuju po mnogim kriterijima među kojima je i njihova namjena.

Jedno od područja namjene za koje se vrlo često razvijaju nove distribucije je sigurnost računalnih sustava. Kako je penetracijsko ispitivanje važna i često korištena metoda provjere sigurnosti računalnih sustava, tako se sve više Linux distribucija razvija upravo za tu namjenu. Penetracijsko ispitivanje (eng. *Penetration testing, Pen-testing*) je metoda kojom se sigurnost računalnih sustava ili mreža provjerava simulirajući akcije zlonamjernog napadača. Najčešće ga primjenjuju veće organizacije (banke, korporacije) koje su česta meta zlonamjernih napada. Iako postoje određene smjernice koje olakšavaju izvođenje ispitivanja, izbor alata i metoda koje se koriste ovisan je samo o osobi koja provodi ispitivanje. Zlonamjernom napadaču na rasploaganju stoji velik izbor alata i tehnologija, pa tako i osoba koja provodi ispitivanje često želi isprobati što više mogućnosti kako bi što kvalitetnije mogla ocijeniti sigurnost sustava.

Upravo iz tog razloga nastaju brojne Linux distribucije za penetracijsko ispitivanje. One olakšavaju rad sigurnosnih stručnjaka koji izvode ispitivanje. U takvim distribucijama bojni alati koji se koriste u penetracijskim ispitivanjima dolaze instalirani i organizirani u kategorije. Na taj način je sigurnosnim stručnjacima omogućeno da se posvete samom ispitivanju, a ne traženju i pripremi raznih alata. Također, vrlo često su takve distribucije dostupne na *Live* medijima, što znači da se mogu pokrenuti s bilo kojeg računala bez potrebe za instalacijom.

U ovom dokumentu je objašnjeno što su Linux distribucije te kako i zašto one nastaju. Također, opisano je penetracijsko ispitivanje, kada se provodi te koji alati i tehnike se pritom primjenjuju. Nadalje, ukratko je prikazan razvoj Linux distribucija za penetracijsko ispitivanje, a najpoznatije od njih su detaljnije analizirane i uspoređene. Za kraj je dan kratki uvid u daljnji razvoj takvih distribucija.

2. Linux distribucije

Linux distribucije su operacijski sustavi izrađeni na Linux jezgri. Svaki operacijski sustav ima svoju jezgru (eng. *kernel*), koja je programski element operacijskog sustava na najnižoj razini. To znači da ona komunicira izravno sa sklopovljem računala (Slika 1). Ostali programi koji se izvode mogu računalnim resursima (npr. memoriji) pristupati samo preko jezgre. Jezgra ima izravan pristup svim računalnim resursima, ona se brine za sinkronizaciju rada procesa, upravlja memorijom, vremenom izvođenja, mrežnim funkcionalnostima i slično.

Slika 1. *Odnos jezgre OS-a prema programima i sklopovlju*
Izvor: *Wikipedia*

Linux jezgra je dakle zajednička komponenta svih Linux distribucija. Napisao ju je 1991. godine finski student Linus Torvalds, a od tada je izmjenjena i nadograđivana velik broj puta od strane mnogih programera diljem svijeta.

Iako su Linux na početku koristili samo Linux programeri koji nisu imali potrebu za razvijanjem distribucija, one su se počele razvijati vrlo brzo nakon nastanka same jezgre. Njihova prednost je u tome što ih mogu koristiti i korisnici koji ne znaju mnogo o samoj jezgri.

Linux distribucije se međusobno razlikuju u mnogo pogleda. Dolaze s različitim skupom alata kao što su uređivači teksta, namjenski programi, baze podataka i sl. Mogu biti projektirani za različite namjene (specifične ili opće), sadržavati različite programske knjižnice (eng. libraries), razlikovati se u izvedbi korisničkog sučelja i dr. Mogu biti namijenjeni za klasična stolna računala, poslužitelje, mobilne uređaje (kao što su mobiteli i tableti), ili pak za ugradbene računalne sustave. Neke od distribucija su komercijalne, no većina ih je besplatna za uporabu. Trenutno postoji više od šest stotina različitih distribucija od kojih se preko stotinu i dalje aktivno razvija i izlazi u vidu novih inačica.

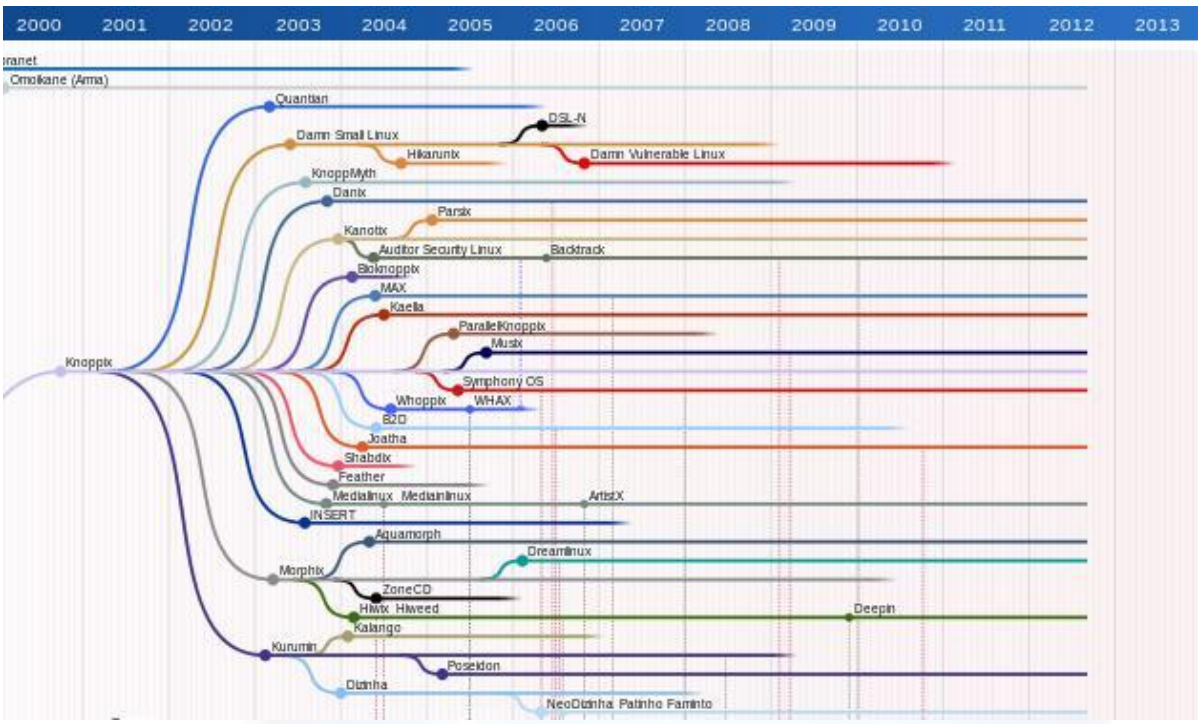
Tipične Linux distribucije namijenjene osobnim računalima sastoje se od nekoliko komponenti. Kao što je ranije spomenuto, svaka distribucija se sastoji od Linux jezgre. Iako se i dalje često koristi tekstualno sučelje (eng. *command line interface, CLI*), važan dio svake distribucije je njeno grafičko sučelje. Ono se može podijeliti na tri važne komponente:

1. **Sustav prozora** (eng. *windowing system*) - Sustav prozora pruža podršku za razne grafičke uređaje, brine se primjerice o iscrtavanju miša na ekranu, i što je najvažnije omogućuje istodoban rad više programa u različitim prozorima.
2. **Upravljanje prozorima** (eng. *windowing manager*) - Upravljanje prozorima služi za funkcije kao što su pomicanje prozora po ekranu, mijenjanje veličine prozora i slično.
3. ***Desktop* okruženje** (eng. *desktop enviroment*) -*Desktop* okruženje povezuje sustav prozora i kontrolu prozora. Ono je zapravo konkretna implementacija grafičkog sučelja. Dva najpoznatija *desktop* okruženja su *Gnome* i KDE.

Slika 2 prikazuje kako se nove distribucije rijetko razvijaju ispočetka. Većinom nastaju nadogradnjom i promjenom već postojećih. Vrlo često autori prilikom izrade nove distribucije koriste željene elemente iz nekoliko postojećih, ili se pak iz jedne distribucije razviju dvije ili više novih. Neke od glavnih distribucija iz kojih se razvijaju nove su Debian, Slackware Linux, Ubuntu, RedHat itd.

Cjelokupni dijagram razvoja Linux distribucija kroz vrijeme može se naći na sljedećoj web stranici:

http://upload.wikimedia.org/wikipedia/commons/8/8c/Gldt.svg



Slika 2. *Linux distribucije kroz vrijeme*
Izvor: *Wikipedia*

Jedan od razloga postojanja toliko velikog broja različitih Linux distribucija svakako je njihovo starenje. Kao što svakih nekoliko godina izlazi nova i unaprijeđena inačica operacijskog sustava Windows, tako je potrebno i Linux distribucije nadograđivati. Razlika je u tome što velik broj ljudi nezavisno radi na njihovom unaprjeđenju te ih tako nastaje više u kraće vremena.

Drugi razlog tako velikog broja distribucija je što se razvijaju za razne namjene. Osim operacijskih sustava opće namjene (npr. Ubuntu, Fedora, Debian, Slackware), postoje i brojne inačice specijalizirane za pojedinu namjenu. Te namjene mogu biti iz vrlo različitih područja. Sustav Joli OS služi za korištenje na malim prijenosnim računalima (eng. *netbook*) i za rad s različitim servisima u oblaku (eng. s*ervice in cloud*). Operacijski sustav ArtistX je namijenjen radu s multimedijom, i sadrži razne primjenske programe namijenjene obradi zvuka, slika i videa. Neke distribucije kao GParted namijenjene su za izradu particija diskova i ne sadrže uopće ostale primjenske programe, dok neke kao što je Parted Magic osim za particiju služe i za spašavanje podataka s oštećenih diskova. Neke distribucije oponašaju pojedine komercijalne operacijske sustave, teko primjerice PearOS svojim grafičkim sučeljem i funkcionalnostima vrlo podsjeća na sustav Mac OS X, dok Zorin OS izgleda kao sustav Windows (Slika 3). Jedno od područja za koje su često namijenjene Linux distribucije svakako je i penetracijsko ispitivanje. O ovim distribucijama više će biti riječi u nastavku dokumenta.

Slika 3. ZorinOS – *Linux distribucija koja oponaša Windowse*
Izvor: *Makeuseof*

Velik broj Linux distribucija nije namijenjen trajnoj instalaciji na tvrdi disk računala već se pokreće kao *Live CD*. *Live CD* je operacijski sustav koji se u potpunosti može pokrenuti s prijenosnog medija (umjesto s tvrdog diska računala). To je vrlo praktično kada se primjerice neka specijalizirana distribucija želi pokrenuti s drugog računala, ili kada se želi isprobati različite distribucije kako bi se odabrala najbolja. Nedostatak je činjenica da se prilikom svakog novog pokretanja postavke operacijskog sustava nanovo postavljaju na osnovne, pa ga je teško prilagoditi vlastitim potrebama (jer se to mora raditi svaki put iznova).

3. Penetracijsko ispitivanje

Penetracijsko ispitivanje (eng. *Penetration testing, Pentesting*) je metoda provjere informacijskih sustava i mreža. Osoba koja provodi ispitivanje zapravo oponaša zlonamjernog napadača koji sustav može napadati izvana (bez ikakvih ovlasti u sustavu) ili iznutra (s određenom razinom ovlasti). Upravo je zbog toga drugi naziv za takvu vrstu provjere i etičko hakiranje.

Prednost ovakve metode provjere nad metodama kojima je cilj samo navesti moguće ranjivosti sustava jest to da se ovakvim pristupom mogu mnogo bolje vidjeti stvarne posljedice napada koji bi se mogao dogoditi. Ovakva vrsta ispitivanja provodi se prvenstveno kako bi se dobio uvid u stvarnu sigurnost sustava. Naime, ukoliko i postoje razne metode obrane od napadača (kao što su vatrozidi (eng. *firewall*), IDS-ovi (eng. *Intrusion Detection System*) i sl., to ne mora nužno značiti da je sigurnost takvog sustava zagarantirana. Brojni sustavi za obranu zastarijevaju i često se otkrivaju njihove ranjivosti, tako da je vrlo bitno držati ih uvijek ažurnima.

U velikim organizacijama (kao što su banke) često je sigurnost podataka od ključne važnosti za poslovanje. Takve organizacije periodički provode penetracijsko ispitivanje. Iako ispitivanje mogu provoditi i sigurnosni stručnjaci u sklopu same organizacije, praksa pokazuje kako su rezultati bolji ukoliko ga provode vanjske organizacije. Razlog tome je to što se vanjska osoba može „bolje uživjeti“ u ulogu zlonamjernog napadača, ali i činjenica da stručnjaci koje provode penetracijsko ispitivanje na velikom broju različitih organizacija imaju više iskustva u takvom poslu.

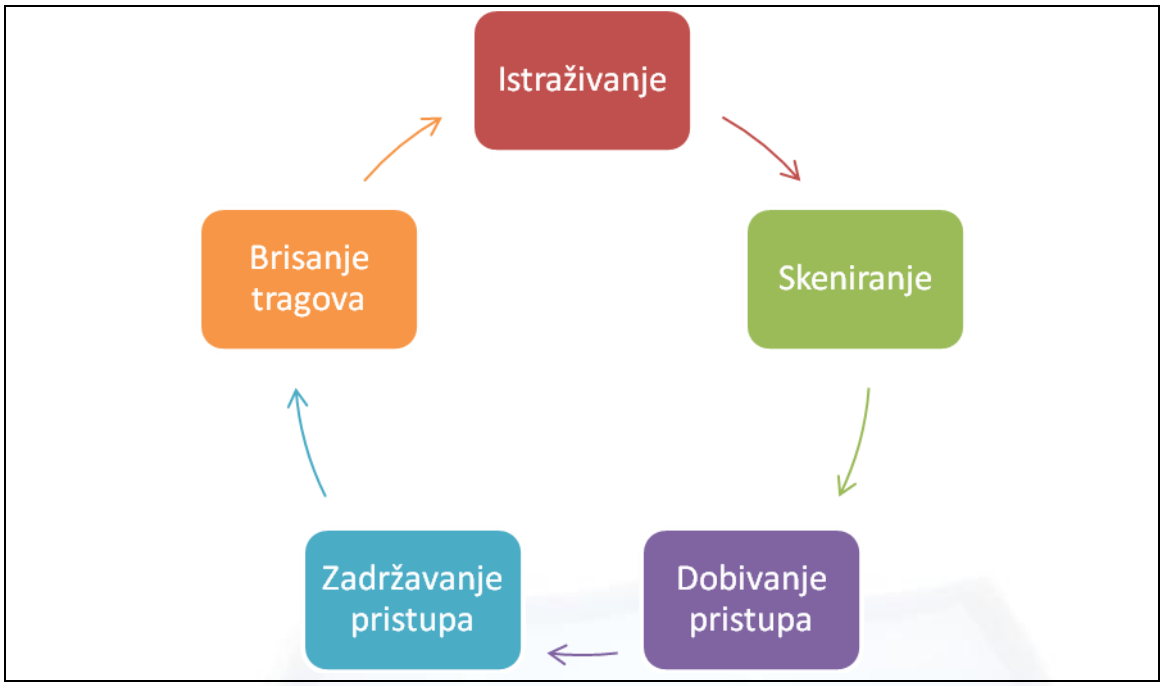
Alati i metode koje se koriste u penetracijskom ispitivanju izbor su same osobe ili organizacije koja provodi ispitivanje, no svejedno postoji nekoliko smjernica i dobrih praksi kojih se većina osoba koje provode ispitivanje pridržava. Slika 4 prikazuje tijek izvođenja penetracijskog ispitivanja. Penetracijsko ispitivanje provodi se u tri faze: planiranje, izvođenje i izvještavanje.

Slika 4. *Tijek izvođenja penetracijskog ispitivanja*
Izvor: *CIS*

Najčešće penetracijsko ispitivanje započinje planiranjem ispitivanja. Planiranje podrazumijeva određivanje opsega (koji dijelovi sustava će se ispitivati, od kakvih napadača i sl.). Ukoliko ispitivanje izvodi vanjska organizacija, u fazi planiranja obavljaju se dogovori s organizacijom koja je naručila ispitivanje.

Nakon toga slijedi izvođenje samog ispitivanja koje je prikazano na slici u nastavku (Slika 5). Izvođenje ispitivanja je, kao što je ranije rečeno, zapravo oponašanje samog zlonamjernog napadača, odnosno hakiranje. Dakle, faze su sljedeće:

1. **Istraživanje** - U ovoj fazi se prikupljaju informacije o organizaciji i sustavu koji se ispituje.
2. **Skeniranje**- U ovoj fazi se otkrivaju ranjivosti sustava koje se mogu iskoristiti.
3. **Dobivanje pristupa** -U ovoj fazi se iskorištavaju ranjivosti i pokušava se dobiti neovlašteni pristup sustavu, tj. odvija se sam napad na sustav i saznaju se povjerljive informacije.
4. **Zadržavanje pristupa** - Kako bi povjerljive informacije uvijek bile dostupne, potrebno je imati trajni pristup sustavu.
5. **Brisanje tragova** - Nakon obavljenog napada potrebno je ukloniti sve tragove kako napad ne bi bio otkriven.



Slika 5. *Ciklus izvođenja ispitivanja (hakiranje)*
Izvor: *CIS*

Nakon što je penetracijsko ispitivanje dovršeno, potrebno je o rezultatima izvijestiti organizaciju koja je naručila ispitivanje. Izvještaj sadrži popis svih ranjivosti koje je bilo moguće iskoristiti te često i savjete kako se zaštititi.

Postoje brojni alati namijenjeni penetracijskom ispitivanju. To su alati za skeniranje, ispitivanje ranjivosti, dobivanje i održavanje pristupa i sl. Pojedini alati služe samo jednoj od navedenih namjena, dok drugi objedinjuju više njih. Neki od najpoznatijih alata su:

- **Nmap**

  Alat za skeniranje otvorenih priključnica (eng. *port*) na računalima. Izdan je pod GNU GPL licencom i može se koristiti na različitim platformama. Osim samog skeniranja priključnica ima i mnogo drugih mogućnosti (otkrivanje operacijskih sustava, otkrivanje servisa pokrenutih na poslužiteljima uključujući i njihove inačice, pokretanje skripti, itd.).
- **Metasploit**

  Alat namijenjen pokretanju zlonamjernog koda (eng. *exploit*) na odredišnom računalu i iskorištavanju poznatih ranjivosti raznih programa i servisa.
- **Wireshark**

  Besplatan alat otvorenog koda namijenjen analizi informacijskih paketa u mreži. Može se koristiti na svim operacijskim sustavima sličnim sustavu UNIX te na operacijskom sustavu Windows.
- **Hydra**

  Jedan od najpoznatijih alata namijenjen probijanju autentikacije raznih servisa. Najčešće se koristi za probijanje lozinki. Postoje inačice za sve popularnije operacijske sustave.

No unatoč brojnim alatima koji olakšavaju proces penetracijskog ispitivanja, ono je ipak mukotrpan posao. Mnogi od alata za skeniranje pronalaze vrlo velik broj ranjivosti na sustavu, a mali broj njih se zaista može iskoristiti. Zadaća osobe koja provodi ispitivanje je provjeriti sve ranjivosti i pokušati ih iskoristiti.

Kako se alati za skeniranje ne mogu ažurirati jednakom brzinom kojom se nove ranjivosti pronalaze, osoba koja provodi ispitivanje trebala bi o njima biti informirana. Zato osim alata koji ispituju ranjivosti, na Internetu postoje i velike baze ranjivosti pojedinih sustava (operacijskih sustava, primjenskih programa i sl.) gdje se takve informacije mogu pronaći.

Unatoč činjenici da se penetracijsko ispitivanje ne svodi samo na puko korištenje alata, oni ipak ubrzavaju i olakšavaju proces samog ispitivanja. Takvih alata postoji vrlo velik broj. Kako osobe koje provode penetracijsko ispitivanje ne bi morale mnogo vremena trošiti na traženje, instalaciju i podešavanje takvih alata, one često koriste neke od brojnih Linux distribucija namijenjenih toj svrsi.

4. Linux distribucije za penetracijsko ispitivanje

Linux distribucije za penetracijsko ispitivanje služe ponajviše kako bi na jednom mjestu okupile širok spektar kvalitetnih alata dobro organiziranih u kategorije. Neke od takvih distribucija usko su orijentirane samo na penetracijsko ispitivanje, dok se neke često koriste i za druge namjene.

Ovakve distribucije međusobno se razlikuju u broju i kvaliteti alata, lakoći korištenja, korisničkom sučelju (kao i sve ostale Linux distribucije). Sve one imaju svoje prednosti i nedostatke, a izbor distribucije često ovisi o subjektivnom dojmu. Nekome će se svidjeti bogato korisničko sučelje jedne distribucije, dok će netko drugi više cijeniti brzinu rada i organiziranost neke druge distribucije. Upravo iz tog razloga u nastavku slijedi detaljniji osvrt na neke od najpoznatijih Linux distribucija namijenjenih penetracijskom ispitivanju, a nakon toga i njihova međusobna usporedba.

4.1. Razvoj Linux distribucija za penetracijsko ispitivanje

U samim počecima, kada se tek pojavila potreba za prvim Linux distribucijama namijenjenim penetracijskom ispitivanju, počelo se raditi na mnogo nezavisnih projekata i to je rezultiralo vrlo velikim brojem distribucija. Neke od njih s vremenom su postale popularne i prihvaćene od velikog broja korisnika, dok je druge koristio samo mali krug ljudi. Razloge zašto su neke distribucije postale popularne, a neke nisu, teško je navesti. Na to su, osim kvalitete samih distribucija, utjecali i brojni drugi čimbenici (npr. loša reklama i sl.).

Kako je vrijeme prolazilo, većina tih projekata počela se gasiti. To ne vrijedi samo za one manje popularne. Čak su se i neke od najpopularnijih distribucija prestale ažurirati, popravljati greške (eng. *bug*) i izdavati nove inačice. One distribucije koje su i dalje ostale aktivne, godinama su se razvijale te se danas uvelike razlikuju od onoga kako su u početku izgledale.

Iako su neke kvalitetne distribucije zamrle, njihovim udruživanjem nastale su druge, novije i modernije distribucije koje se danas koriste. Tako je, primjerice, popularni BackTrack nastao iz nekoliko starijih distribucija.

4.2. Najpoznatije distribucije

4.2.1. BackTrack

BackTrack je najpoznatija Linux distribucija specijalizirana za penetracijsko ispitivanje. Osim penetracijskog ispitivanja namijenjena je i računalnoj forenzici, no koristi se i za razne druge namjene povezane s računalnom sigurnošću. Ova distribucija zasnovana je na *Debian GNU/Linux* i *Ubuntu* distribucijama.

BackTrack je nastao iz ranih inačica *live* Linux distribucija *Whoopix*, IWHAX i Auditor. Prva, Beta inačica, izašla je u veljači 2006. godine. Od njegovog nastanka do danas redovito izlaze nove inačice, a njegova popularnost sve više raste. Na novim inačicama rade ljudi iz različitih dijelova svijeta, a osim rada na razvoju vrlo brzo popravljaju greške (eng. *bug*) koje prijavljuju korisnici. Ekipa programera koji razvijaju BackTrack potiče korisnike na korištenje novih inačica na način da prilikom izlaska novih inačica za starije više ne pružaju korisničku podršku.

Ova distribucija dostupna je u 32 i 64-bitnoj inačici, a može se preuzeti s Gnome ili KDE *desktop* okruženjem. BackTrack dolazi u *Live CD* izdanju, no moguće ga je i trajno instalirati na tvrdi disk računala. Također postoji i inačica koju je moguće instalirati na mobilni telefon ili tablet.

U načinu rada za forenziku, BackTrack se pokreće bez da ostavlja ikakve tragove na računalu na kojem je pokrenuto. Na taj način se osigurava da ništa, pa tako ni korisni dokazi, neće biti obrisani s računala.

Iako ga koriste i sigurnosni stručnjaci i osobe koje su se tek počele baviti računalnom sigurnošću, BackTrack je ipak namijenjen iskusnijim korisnicima. Onima s manje iskustva, a posebice onima kojima je to prvi susret sa sustavom Linux, za početak se preporuča neka druga distribucija.

Alati u distribuciji BackTrack organizirani su u deset kategorija i nekolicinu potkategorija (radi lakšeg snalaženja**Error! Reference source not found.**). Korisnici distribucije BackTrack nakon instalacije imaju na izbor preko tri stotine sigurnosnih alata (alata za skeniranje mreža, iskorištavanje ranjivosti, probijanje lozinki itd.) te naravno mogućnost instalacije dodatnih alata.

Kategorije u koje su organizirani alati su:

- prikupljanje informacija (eng. *Information Gathering*),
- otkrivanje ranjivosti (eng. *Vulnerability Assessment*),
- iskorištavanje ranjivosti (eng. *Exploitation tools*),
- povećanje prava pristupa (eng. *Privilege escalation*),
- održavanje pristupa (eng. *Maintaining Access*),
- reverzni inženjering (eng. *Reverse Engineering*),
- ispitivanje pod opterećenjem (eng. *Stress testing*),
- forenzika (eng. *Forensics*),
- alati za stvaranje izvještaja (eng. *Reporting tools*),
- ostali alati (eng. *Miscellaneous*).

Slika 6. *BackTrack izbornik*
Izvor: *BackTrack*

Jedan od nedostataka distribucije BackTrack je činjenica da pojedine inačice nisu međusobno kompatibilne, pa se tako na primjer teško prelazi primjerice s distribucije BackTrack 4 na 5. Također, nedostatak je taj da dokumentacija ponekad zna biti zastarjela ili manjkava. Neke korisničke upute na službenim stranicama vrijede samo za stare inačice operacijskog sustava, i nemoguće ih je primjeniti na novima. No, dokumentacija se iz dana u dan razvija i postaje sve detaljnija pa je realno za očekivati kako će ovaj problem u budućnosti biti sve manji i manj.

4.2.2. Blackbuntu

Blackbuntu je relativno nova Linux distribucija namijenjena penetracijskom ispitivanju. Nastala je iz distribucije *Ubuntu* 10.10.

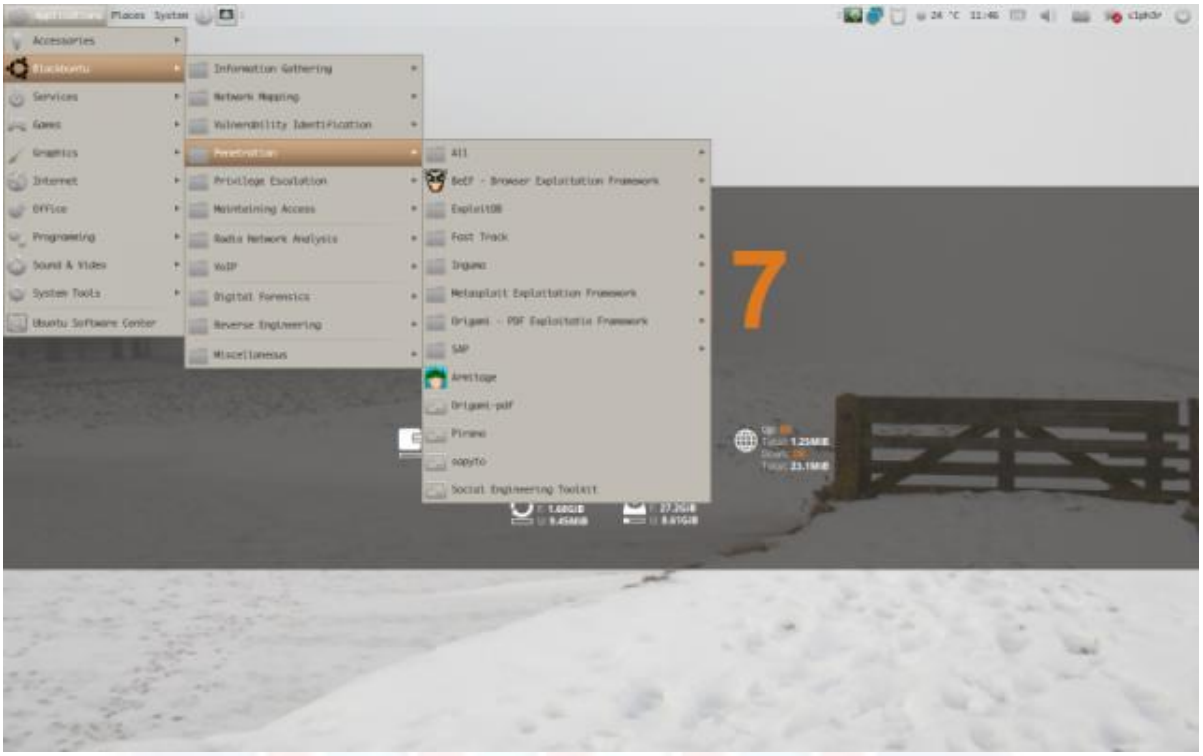
Iako je razvoj ove distribucije tek nedavno započeo, ona sve više dobiva na popularnosti u krugovima osoba koje se bave računalnom sigurnošću. Razlog tome je njegova jednostavnost i lakoća korištenja. Projekt razvoja ovog operacijskog sustava otvorenog je tipa i mogu mu se pridružiti svi koje to zanima. Trenutno na njemu sudjeluje dvadesetak ljudi iz Europe, Azije, Sjeverne i Južne Amerike.

Do inačice 0.3 Blackbuntu dolazi s Gnome *desktop* okruženjem, no u pripremi je i KDE okruženje, koja će sigurno biti dostupno u prvom izdanju (1.0).

Za razliku od distribucije Backtrack, Blackbuntu je prvotno namijenjen za osobe koje tek počinju učiti o informacijskoj sigurnosti, studente i općenito osobe zainteresirane za to područje. No to naravno nije pravilo te ga koriste i iskusni stručnjaci koji su procijenili da im ova distribucija odgovara više od ostalih.

Mnogi se slažu kako distribucija Blackbuntu vrlo nalikuje na BackTrack kad su u pitanju alati i način na koji su oni organizirani (Slika 7). Naime, oni su u ovoj distribuciji organizirani

u jedanaest kategorija gotovo identičnih onima u distribuciji BackTrack, s malo izmijenjenim nazivima. Neke dodatne kategorije su VoIP analiza (eng. *Voice over IP Analysis*) i radio analiza (eng. *Radio Network Analysis*).



Slika 7. *Blackbuntu izbornik*
Izvor: *Blackbuntu*

Blackbuntu se za sada ipak koristi mnogo manje nego BackTrack. Razlog tome je činjenica da je relativno nov i nije još dobro razvijen. Također, iako se jednak učinak može postići korištenjem obe distribucije, BackTrack za sada ima veću zajednicu korisnika te je mnogo lakše pronaći upute za istu stvar koristeći BackTrack nego koristeći Blackbuntu. Unatoč tome Blackbuntu ima potencijala postati vrlo moćna distribucija za penetracijsko ispitivanje ukoliko se i dalje nastavi razvijati.

4.2.3. NodeZero

NodeZero je još jedna Linux distribucija za penetracijsko ispitivanje zasnovana na Ubuntu.

Zanimljiva činjenica vezana za ovu distribuciju je što je njen autor Hrvat pa su iz tog razloga početne postavke tipkovnice namještene na Hrvatski jezik. Ova distribucija nastala je jer su njeni autori zaključili kako postojeće *Live* distribucije ne zadovoljavaju njihove potrebe.

NodeZero dolazi s Gnome *desktop* okruženjem. Namijenjen je prvenstveno trajnoj instalaciji na tvrdi disk računala iako ga je moguće pokrenuti i na *Live CD-u.*

Upravo zbog te činjenice, ova je distribucija namijenjena iskusnim korisnicima koji gotovo svakodnevno koriste operacijske sustave namijenjene penetracijskom ispitivanju. Na taj način oni distribuciju mogu prilagoditi svojim potrebama i navikama, a promjene se neće obrisati svakim ponovnim pokretanjem.

Ova distribucija brojem i količinom alata nimalo ne zaostaje za sličnim distribucijama iz tog područja (Slika 8). Broji preko 300 alata organiziranih u sljedeće glavne kategorije:

- mreža (eng. *Network*),
- web analiza i napadi (eng. *Web Analysis and Attack*),
- iskorištavanje ranjivosti (eng. *Exploiting*),

- povećavanje prava pristupa (eng. *Privilege Escalation*),
- dobivanje prava pristupa (eng. *Connect and Access*),
- anonimnost (eng. *Anonymity*),
- bežično i *Bluetooth* (eng. *Wireless and Bluetooth*),
- VoIP (eng. *Voice over IP*),
- reverzno inženjerstvo (eng. *Reverse Engineering*),
- računalna forenzika (eng. *Digital Forensics*).

Slika 8. *NodeZero izbornik*
Izvor: *NodeZero*

Neki smatraju kako je jedan od nedostataka ove distribucije činjenica da pojedini alati nakon instalacije operacijskog sustava nisu odmah spremni za uporabu nego ih je potrebno ručno konfigurirati. No to nije greška, nego su svi alati koje je potrebno dodatno postavljati ostavljeni da ih korisnici samostalno postave te da ih na taj način što bolje prilagode svojim potrebama.

4.2.4. Knoppix STD

Knoppix STD je, kao što i samo ime govori, distribucija zasnovana na Knoppix distribuciji. STD je kratica za distribuciju sigurnosnih alata (eng. *Security tools distribution*).

Prva inačica ove distribucije izašla je 2004. godine te, iako je često navođena kao jedna od najboljih Linux distribucija za penetracijsko ispitivanje, od tada pa sve do danas nije izašla nijedna nova inačica. Zbog činjenice da ova distribucija odavno nije ažurirana, sve češće se počinju javljati problemi prilikom njenog korištenja na novijim uređajima.

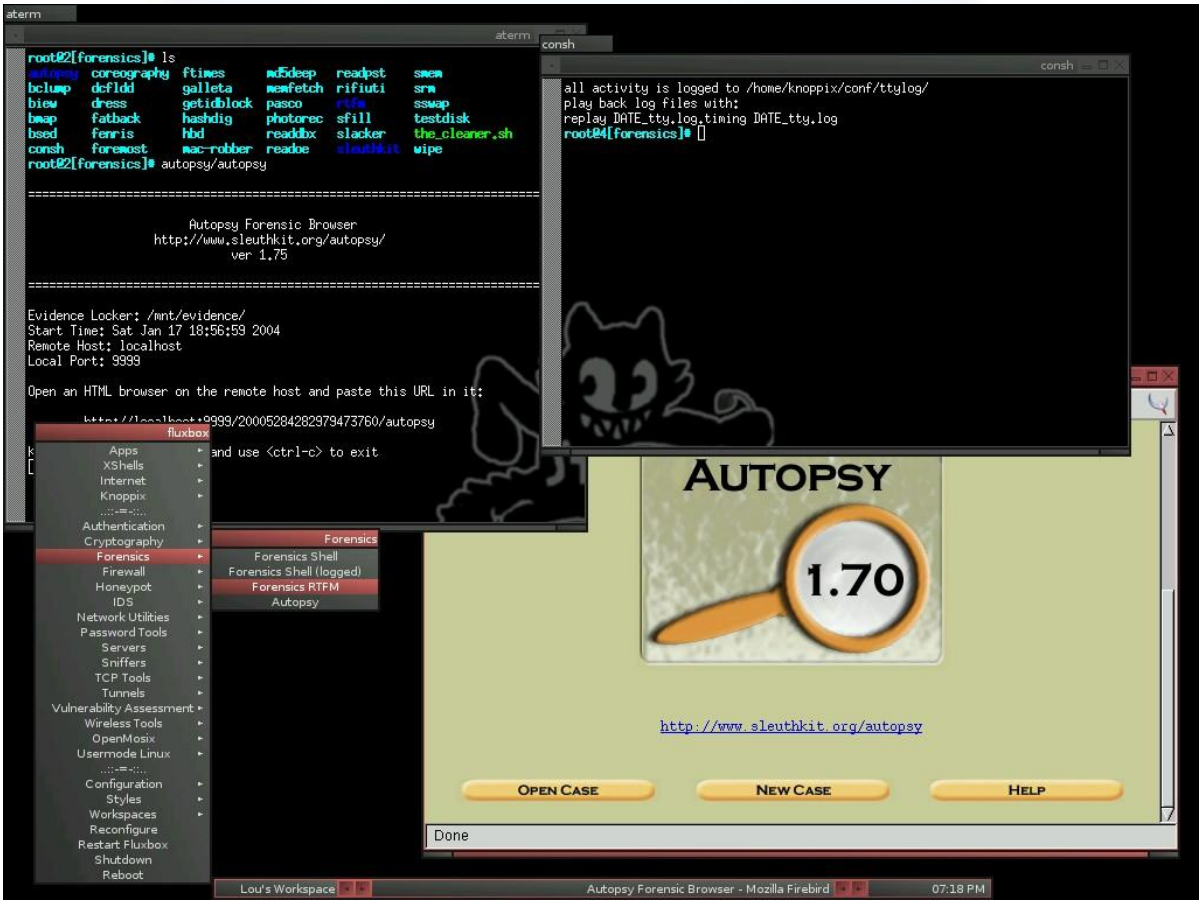
Za razliku od NodeZero, Knoppix STD dolazi samo u *Live CD* izdanju, bez mogućnosti instalacije na tvrdi disk računala. Jedino podržano *desktop* okruženje je Fluxbox.

Ova distribucija je namijenjena osobama dobro upoznatima s Linuxom. Osobe koje ga žele koristiti trebaju biti dobro upoznate s radom preko naredbene linije jer se većina alata koristi na taj način. Što se tiče samog područja računalne sigurnosti, mogu ga koristiti i početnici i stručnjaci.

Autori ove distribucije navode kako je jedina njena svrha korisnicima staviti na raspolaganje što veći broj sigurnosnih alata sa što ljepšim i jednostavnijim sučeljem. I zaista, jedan od

glavnih razloga zašto se Knoppix STD još uvijek uspoređuje sa novijim i ažurnijim distribucijama je upravo mnoštvo kvalitetnih alata. Alati su podijeljeni u sljedeće kategorije (Slika 9).

- autentikacija (eng. *Authentication*),
- kriptografija (eng. *Cryptography*),
- forenzika (eng. *Forensics*),
- vatrozidi (eng. *Firewall*),
- (eng. *Honeypots*),
- sustavi za otkrivanje napada (eng. *Intrusion Detection System*),
- mrežni alati (eng. *Network utilities*),
- alati za lozinke (eng. *Password tools*),
- poslužitelji (eng. *Servers*),
- alati za *sniffing* (eng. *Sniffers*),
- TCP alati (eng. *TCP tools*),
- alati za tuneliranje (eng. *Tunnels*),
- otkrivanje ranjivosti (eng. *Vulnerability Assessment*),
- alati za bežične mreže (eng. *Wireless tools*).



Slika 9. *Knoppix STD izbornik, alati za forenziku*
Izvor: *Knoppix STD*

Knoppix STD se i dalje koristi unatoč činjenici da njezin razvoj odavno stagnira. Iako se javljaju problemi prilikom korištenja ove distribucije na novijoj računalnoj opremi (eng. *hardware*), ona se može koristiti uz pomoć virtualizacijskih alata (npr. VMware, VirtualBox).

No ukoliko se uskoro razvoj ponovno ne pokrene, sve veći broj vrlo kvalitetnih novih distribucija mogao bi Knoppix STD u potpunosti istisnuti iz upotrebe.

4.2.5. Pentoo

Pentoo je također jedna od češće korištenih Linux distribucija za penetracijsko ispitivanje i općenito računalnu sigurnost. Zasnovana je na operacijskom sustavu Gentoo.

Prva inačica izašla je 2005. godine, a u prve dvije godine redovito su izlazile nadogradnje i nove inačice. Nakon toga se razvoj počeo polako usporavati, ali nije stao. Posljednja inačica izašla je 2012. godine. Za ovu distribuciju zaslužna su četvorica programera i sigurnosnih stručnjaka koji su ujedno i veliki ljubitelji distribucije *Gentoo*. Njihova želja bila je razviti distribuciju namijenjenu penetracijskom ispitivanju prilagođenu *Gentoo* korisnicima.

Kao i BackTrack, i ova je distribucija dostupna u 32 i u 64-bitnom izdanju. Koristi se kao *Live CD* te dolazi s *desktop* okruženjem Xfce.

Kao što je i ranije spomenuto, Pentoo je namijenjen korisnicima distribucije Gentoo, ali i svima ostalima koji se žele baviti računalnom sigurnošću. Iako prvotno nije namijenjen početnicima, pogotovo onima koji se prvi put susreću sa sustavom Linux, koriste ga i početnici i iskusniji korisnici. Alati su u Pentoo distribuciji organizirani u nešto više kategorija nego primjerice u *BackTrack* ili Knoppix STD distribucijama. Slika 10 prikazuje izbornik distribucije Pentoo.

U usporedbi s ostalim Linux distribucijama namijenjenim penetracijskom ispitivanju, za Pentoo se može reći da, iako možda nije najpopularnija, svakako je zaslužila da ju se isproba prilikom odabira distribucije. Njena velika prednost je što se za razliku od mnogih takvih distribucija još uvijek razvija i nadograđuje i to već dugi niz godina.

Slika 10. *Pentoo izbornik*
Izvor: *Beginlinux*

4.2.6. Ostale distribucije

Distribucije koje su detaljnije obrađene u ovom dokumentu zaista su neke od najčešće korištenih. Najpopularnija od njih svakako je BackTrack, no ne treba zanemariti ni ostale distribucije. Teško je suziti izbor na samo nekoliko jer svaka ima neko svoje svojstvo koja će nekome biti od ključne važnosti, dok drugome neće predstavljati nikakvu prednost. U nastavku će biti spomenute još neke istaknutije distribucije iz područja penetracijskog ispitivanja.

- **BackBox**
  - Osim ranije spomenutih distribucija, često se koristi i distribucija BackBox zasnovana na Ubuntu. Ova distribucija je brza, jednostavna za korištenje te uvijek opremljena najnovijim inačicama alata za penetracijsko ispitivanje.
- **PHALK**
  - Linux distribucija PHALK (eng. *Professional Hacker's Assault Kit*) također je među poznatijima u krugovima sigurnosnih stručnjaka. Odlikuje se mnoštvom alata i vrlo dobrom dokumentacijom.
- **Auditor**
  - Auditor, jedna od distribucija iz koje je nastao BackTrack, još uvijek se koristi i samostalno. Zasnovana je na *Knoppixu* te dolazi samo u *Live* izdanju bez mogućnosti trajne instalacije na tvrdi disk.
- **L.A.S Linux**
  - L.A.S Linux (eng. *Local Area Security Linux*) još je jedna *Live* distribucija. Odlikuje se time što zauzima vrlo malo memorije te stane na mini CD (180 MB), no razvoj na ovoj distribuciji stagnira.
- **nUbuntu**
  - nUbuntu je kao što samo ime kaže zasnovana na distribuciji Ubuntu. Glavna ideja autora ove distribucije bila je preoblikovati Ubuntu tako da se prilagodi potrebama penetracijskog ispitivanja. Dodani su specijalizirani alati, a izbačeni alati opće namjene (uređivači slika, teksta i sl.).

4.2.7. Usporedba distribucija

U ovom poglavlju bit će napravljena pregledna usporedba distribucija koje su detaljnije razrađene u dokumentu. Kao kriteriji usporedbe uzeti su pojedini parametri tehničke prirode, ali i oni netehnički.

Među tehničke kriterije spadaju Alati, *Desktop* okruženje i „Bazni OS“ (operacijski sustav koji se koristio kao temelj za izgradnju distribucije). Prilikom odabira distribucije za penetracijsko ispitivanje vrlo često se u obzir uzima broj kvaliteta i organiziranost alata koje ona nudi. Također, korisnicima koji su od ranije upoznati s operacijskim sustavima zasnovanim na Linuxu, važan kriterij mogu predstavljati *desktop* okruženje i bazni.

Netehnički kriteriji koji mogu biti važni pri odabiru distribucije su korisnici kojima je namijenjena distribucija te njezin razvoj. Neiskusni korisnici u potrazi za distribucijom na kojoj bi željeli naučiti i isprobati svoje umijeće često traže jednostavnost i lakoću korištenja, dok oni iskusniji često imaju drugačije želje i potrebe. Također ponekad je korisnicima vrlo bitno je li se distribucija koju koriste razvija i ažurira.

Distribucije	Alati	Desktop okruženje	Bazni OS	Korisnici	Razvoj
BackTrack	Preko 300 alata organiziranih u 10-ak kategorija	Gnome, KDE	Debian, Ubuntu	Početnici i iskusni pentesteri, ne preporuča se Linux početnicima	Izdaju se nove inačice i redovito ispravljaju greške
Blackbuntu	Alati organizirani u kategorije vrlo slične BackTracku	Gnome , KDE u pripremi	Ubuntu	Početnici, studenti i učenici	Izdaju se nove inačice
NodeZero	Preko 300 alata organiziranih u 10-ak kategorija	Gnome	Ubuntu	Iskusniji korisnici koji svakodnevno koriste ovakvu vrstu OS-a	Razvija se
Knoppix STD	Mnoštvo alata organiziranih u 15-ak kategorija	Fluxbox	Knoppix	Osobe dobro upoznate s Linuxom	Razvoj stao
Pentoo	20-ak kagetorija	Xfce	Gentoo	Prvenstveno Gentoo korisnici, općenito i iskusni i početnici	Izdaju se nove inačice (svakih nekoliko godina), razvoj malo usporeniji nego na početku

Tablica 1. *Usporedba distribucija*

4.3. Budućnost Linux distribucija za penetracijsko ispitivanje

Penetracijsko ispitivanje u posljednje vrijeme postaje sve popularnije. Sve se više organizacija odlučuje za takvu vrstu provjere sigurnosti svojih sustava. Iz tog se razloga u posljednje vrijeme povećava broj korisnika Linux distribucija specijaliziranih za penetracijsko ispitivanje, a sa sve većim brojem korisnika rastu i zahtjevi na takve distribucije.

Uz već postojeće Linux distribucije koje se razvijaju i nadograđuju duži niz godina, ponekad se znaju pojaviti i nove distribucije. Unatoč njihovoj kvaliteti, brzini ili broju alata koji sadržavaju, one ponekad vrlo teško uspiju pridobiti nove korisnike. Razlog tome je tromost ljudi koji su navikli koristiti određenu distribuciju i ne žele promjenu. Stoga nove distribucije moraju zaista biti vrlo dobre kako bi uspjele na današnjem tržištu. Dobra strana toga je što sve veća konkurencija ima za posljedicu sve brži razvoj ovih distribucija.

Popularnost ovih distribucija s vremenom će još više rasti. Stoga će distribucije koje žele zadržati svoje korisnike uvijek morati biti u korak s vremenom. Osim samih distribucija, sve se više razvijaju i alati koji se koriste u penetracijskom ispitivanju. Popularne distribucije već danas pažljivo odabiru svoje alate, a taj će se trend nastaviti i u budućnosti. Iako je važno da distribucija svojim korisnicima ponudi što veći broj alata, još je važnije da ti alati budu kvalitetni i stabilni kako bi korisnici bili što zadovoljniji.

5. Zaključak

Penetracijsko ispitivanje je, kao što je ranije spomenuto, metoda provjere sigurnosti računalnih sustava u kojoj se simulira zlonamjerni napadač. Ranjivosti sustava mogu biti brojne te postoje brojni alati i tehnike koje se koriste u penetracijskom ispitivanju. Za većinu područja penetracijskog ispitivanja postoje specijalizirani alati. Neki od njih postali su toliko popularni da ih koriste gotovo svi stručnjaci koji provode ispitivanje, dok su drugi manje popularni, ali ne nužno i manje kvalitetni.

Linux distribucije na jednom mjestu okupljaju sve alate potrebne za izvođenje penetracijskog ispitivanja i na taj način korisnika rješavaju brige oko instalacije i potrage za alatima. One pružaju korisniku jednostavno i organizirano radno okruženje.

Nažalost, postoji i loša strana ovih distribucija. Često je slučaj da osobe koje provode penetracijsko ispitivanje nisu jedini korisnici ovih distribucija. Koriste ih i zlćudni napadači za nedopuštene svrhe. Protiv toga se nije jednostavno boriti jer su distribucije dizajnirane kako bi osobe koje provode ispitivanje mogle što jednostavnije „napadati“ željene sustave. Pošto zlćudni napadači koriste iste alate i tehnike nemoguće je razlikovati etične od neetičnih hakera.

Nadalje, postoji i problem odabira distribucije. Mnoštvo je Linux distribucija specijaliziranih za penetracijsko ispitivanje. Na pitanje kako odabrati najbolju ne postoji jednostavan odgovor. Na Internetu je moguće pronaći brojne testove koji pomažu pri odabiru distribucije, no takvi su testovi često vrlo površni, a i orijentirani na distribucije opće namjene.

Odabir distribucije je vrlo subjektivan, te se nije preporučljivo oslanjati se na tuđe savjete. Ono što je nekome vrlo važno svojstvo, drugome ne mora predstavljati nikakvu prednost. Vrlo često je prije odluke za određenu distribuciju poželjno isprobati njih nekoliko.

Važno je također primijetiti kako se ove distribucije iz dana u dan razvijaju i nadograđuju. Osim toga izlaze i nove distribucije. Nakon uspješnog odabira distribucije svakako je važno i dalje pratiti novosti iz ovog područja jer danas izabrana distribucija sutra vrlo lako može zastarjeti.

6. Leksikon pojmova

Debian

Debian je besplatni operacijski sustav objavljen pod GPL licencom. Danas Debian, osim Linux jezgre, podržava i druge jezgre, poput jezgre BSD operacijskog sustava. Inačica Debian 4.0 nazvana Etch, objavljena je 8. travnja 2007. godine.

http://en.wikipedia.org/wiki/Debian
http://www.debian.org/

Exploit

Zloćudna informacija ili odsječak koda - Predstavlja odsječak programskog koda ili dio podataka koji iskorištava neispravnost ili aktivnu ranjivost određenog sustava kako bi se nanijela šteta, izazvalo neočekivano ponašanje ili omogućio neovlašten pristup.

http://searchsecurity.techtarget.com/definition/exploit
http://www.webopedia.com/TERM/E/exploit.html

Gnome

Gnome je desktop okruženje i grafičko sučelje za operacijske sustave. U potpunosti je otvorenog koda i izdano je pod GPL licencom. Može biti korišten sa bilo kojim operacijskim sustavom sličnim sustavu UNIX, a najpoznatije izdanje je za GNU/Linux.

http://www.gnome.org/

http://en.wikipedia.org/wiki/GNOME

KDE

KDE je međunarodna zajednica koja razvija programsku podršku otvorenog tipa namijenjenu različitim platformama (Linux, FreeBSD, Windows, Solaris, Mac OS X). Najpoznatiji proizvod je KDE desktop okruženje koje koristi velik broj Linux distribucija.
http://www.kde.org/

http://en.wikipedia.org/wiki/KDE

Linux

Linux je naziv za jezgru operacijskog sustava sličnu Unixu. Ime Linux potječe od imena prvog autora jezgre, Linusa Torvaldsa. Danas je Linux djelo mnogih programera diljem svijeta i jedna od najpoznatijih slobodnih programskih podrški.

http://www.linux.org/

http://en.wikipedia.org/wiki/Linux

Linux distribucije

Linux distribucije su operacijski sustavi nastali nad Linux jezgrom. Osim jezgre distribucija mora sadržavati grafičko sučelje, razne programe i alate. Distribucije mogu biti namijenjene stolnim i prijenosnim računalima, mobilnim uređajima, dlanovnicima i sl. Osim distribucija za opću namjenu postoji čitav niz specijaliziranih Linux distribucija (distribucije za multimediju, spašavanje podataka, sigurnost i sl.).

http://en.wikipedia.org/wiki/Linux_distribution

http://wiki.open.hr/wiki/Linux_distribucije

http://distrowatch.com/

Obrnuti inženjering - Reverzni inženjering

Otkrivanje tehnoloških principa i načina rada određenog entiteta. - Proces obrnutog inženjerstva podrazumijeva otkrivanje tehnoloških principa i načina rada određenog uređaja, objekta ili sustava analizom njegove unutrašnje strukture. Često uključuje fizičko otkrivanje unutrašnjih dijelova (npr., mehanički uređaj, elektronička komponente, računalni program) i detaljno analiziranje. Ovisno o primjeni ciljevi mogu biti različiti. Moguće je otkriti određenu poslovnu tajnu rada uređaja, otkrivanje tajnog algoritma koji se implementira i drugo. Prilikom analize programske potpore najčešće se žali zaobići određen dio koda koji implementira određenu sigurnosnu politiku. - Proces reverznog inženjerstva podrazumijeva otkrivanje tehnoloških principa i načina rada određenog uređaja, objekta ili sustava analizom njegove unutrašnje strukture. Često uključuje fizičko otkrivanje unutrašnjih dijelova (npr., mehanički uređaj, elektronička komponente, računalni program) i detaljno analiziranje. Ovisno o primjeni ciljevi mogu biti različiti. Moguće je otkriti određenu poslovnu tajnu rada uređaja, otkrivanje tajnog algoritma koji se implementira i drugo. Prilikom analize programske potpore najčešće se žali zaobići određen dio koda koji implementira određenu sigurnosnu politiku.
http://searchcio-midmarket.techtarget.com/definition/reverse-engineering
http://www.npd-solutions.com/reoverview.html
http://www.wisegeek.com/what-is-reverse-engineering.htm

Penetracijsko ispitivanje

Penetracijsko ispitivanje je metoda provjere sigurnosti računalnih sustava i mreža. Osobe koje provode testiranje simuliraju zlonamjernog napadača i na taj način pokušavaju narušiti sigurnost sustava.

http://en.wikipedia.org/wiki/Penetration_test
http://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2008-02-219.pdf

Ubuntu

Ubuntu je računalni operacijski sustav temeljen na Debian Linux distribuciji te je besplatno distribuiran, koji koristi vlastito *desktop* okruženje. Prema *online* istraživanjima Ubuntu je najpopularnija Linux distribucija na prijenosnim i osobnim računalima. No često se koristi i kod poslužitelja te računarstva u oblacima. Posljednja inačica 12.04 objavljena je 26.travnja 2012.
http://en.wikipedia.org/wiki/Ubuntu_(operating_system)
http://www.ubuntu.com/

Vatrozid – Firewall

Sigurnosna stijena (eng. *Firewall*) je skup komunikacijskih nakupina koji služe kako bi odvojili privatnu mrežu od javne. Sastoje se od programa koji služe kako bi pratili i upravljali promet između računala i mreža. Sigurnosne stijene mogu propuštati, blokirati, šifrirati promet na temelju pravila koja korisnik postavlja.
http://searchsecurity.techtarget.com/definition/firewall
http://kb.iu.edu/data/aoru.html

VoIP - Voice over IP

VoIP je skup internetskih tehnologija, komunikacijskih protokola i tehnologija prijenosa kako bi se ostvario prijenos govora preko IP mreže. VoIP koristi protokole za podršku sjednice poput SIP-a i SAP-a za uspostavljanje i raskid sjednica, tj. poziva.
http://voip.about.com/od/voipbasics/a/whatisvoip.htm
http://www.edinformatics.com/internet/voice_over_IP.htm
http://transition.fcc.gov/voip/

7. Reference

Za reference je potrebno koristiti stil Reference. Primjer je dan u nastavku.

[1] Koen Vervloesem:BackTrack 5 review – if you're serious about pentesting don't leave home without it!, http://www.linuxuser.co.uk/reviews/backtrack-5-review-if-youre-serious-about-pentesting-dont-leave-home-without-it/, rujan 2012.

[2] Makeuseof: Best Linux Distros, http://www.makeuseof.com/pages/best-linux-distributions, rujan 2012.

[3] 10 Pentesting Linux Distributions you should try http://blog.rootcon.org/2012/02/10-pentesting-linux-distributions-you.html, rujan 2012.

[4] Hak5: Blackbuntu vs. BackTrack, http://www.youtube.com/watch?v=zZVUb5A0HRw, rujan 2012.

[5] Philip Bailey: Linux Penetration testing distributions list, http://bailey.st/blog/2010/11/30/linux-penetration-testing-distributions-list/, rujan 2012.

[6] BackTrack Linux, http://www.backtrack-linux.org/, rujan 2012.

[7] Blackbuntu Linux, http://www.blackbuntu.com/, rujan 2012.

[8] NodeZero Linux, http://nodezero-linux.org/, rujan 2012.

[9] Pentoo, http://www.pentoo.ch/, rujan 2012.

[10] Knoppix STD, http://s-t-d.org/, rujan 2012.

[11] Wikipedia: Linux distributions, http://en.wikipedia.org/wiki/Linux_distribution, rujan 2012.

[12] Wikipedia: Penetration test, http://en.wikipedia.org/wiki/Penetration_test, rujan 2012.