HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Damn Vulnerable Linux

CCERT-PUBDOC-2007-04-190

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument, koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, **www.lss.hr -** laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Zbog otvorenosti programskog koda, operacijski sustavi Linux doživjeli su mnoga različita izdanja (distribucije). Programeri i dizajneri programske podrške podijelili su se u grupe prema osobnim stavovima vezanim uz smjerove daljnjeg napretka i poboljšanja sustava u različitim kontekstima, uključujući i sigurnost.

Damn Vulnerable Linux jedna je od mnogih distribucija Linux sustava s vrlo važnom razlikom u odnosu na sve ostale. Ova distribucija načinjena je tako da sadrži što više sigurnosnih propusta u paketima od kojih je izgrađena.

Razumljivo, postavlja se pitanje zašto bi netko proizveo takvu distribuciju, ali i tko bi ju uopće koristio obzirom na njezinu neupotrebljivost u kontekstu računalne sigurnosti. Odgovor je vrlo logičan i nije neočekivan: upravo oni koji se bave sigurnošću računala odnosno sigurnošću operacijskih sustava i programske podrške. Edukacija budućih inženjera s područja sigurnosti računalnih sustava uz neizbježan teoretski mora imati i praktičan, većini zanimljiviji, dio. Stjecanje temeljnih znanja na ovaj način uvelike je otežano korištenjem stabilnih inačica sustava. Upravo je to razlog razvoju edukacijskih distribucija kao što je Damn Vulnerable Linux.

U ostatku dokumenta ukratko su opisane mogućnosti DVL sustava s kratkim osvrtom na konkretnu primjenu u području istraživanja sigurnosnih nedostataka. Jezgroviti opisi početnih koraka u svladavanju korištenja sustava popraćeni su i brojnim prikazima sučelja (eng. *screenshot*) radi lakšeg snalaženja. Konačno, korištenjem poznatih sigurnosnih alata izveden je sigurnosni pregled sustava te su prikazani rezultati.

2. Općenito o Damn Vulnerable Linux sustavu

Damn Vulnerable Linux (DVL) je sve što kvalitetna, sigurna i stabilna Linux distribucija nije. Razvojni tim stručnjaka koji je oblikovao sustav utrošio je mnogo truda na pronalaženje odgovarajućih paketa. Cilj je bio pronaći najranjivije među njima, kako bi početnici mogli načiniti svoje prve korake u razumijevanju sigurnosnih propusta, ali i kako bi napredniji korisnici mogli nadograditi svoja znanja i vještine. Za ovu namjenu bilo je potrebno pronaći odgovarajuće inačice paketa s najlošijim postavkama, sa zastarjelim dijelovima programa – sve što čini sustav i njegove aplikacije ranjivima u najvećoj mogućoj mjeri. DVL nije stvoren da bi se koristio svakodnevno kao uobičajena Linux distribucija, nego zato da bi se prvenstveno studentima s područja računalne sigurnosti omogućilo upoznavanje ove problematike.

DVL je dostupan u obliku ISO slike veličine oko 150MB, s koje se može pokrenuti bez potrebe za prethodnim instaliranjem, što s većinom ostalih distribucija nije moguće. Temelji se na popularnoj Linux distribuciji *Damn Small Linux* (DSL), ne samo zbog manje veličine nego i zato što je DSL izgrađen na jezgri inačice 2.4, koja je značajno ranjivija od inačice 2.6. Ovaj operacijski sustav sadrži starije, ranjivije verzije Apache+PHP, MySQL, FTP i SSH poslužitelja. Također, sadrži i alate kojima se omogućava prevođenje programskog koda i ispravljanje programskih pogrešaka. Tu su uključeni GCC, GDB, NASM, ELF Shell, DDD, LDasm, LIDa i drugi.

Na web stranicama posvećenim DVL sustavu moguće je preuzeti inicijalnu inačicu s oznakom 1.0. DVL Black Hat Edition (DVL 1.1) je nova inačica koja je trebala biti izdana u vrijeme pisanja dokumenta, ali je zbog različitih ispravaka njezino objavljivanje odgođeno. Slijedeći odlomci odnose se na DVL 1.0 inačicu vrlo zanimljivog i neobičnog operacijskog sustava.

2.1. Namjena sustava

Damn Vulnerable Linux je Linux distribucija ciljano načinjena tako da bude što ranjivija. Sadrži čitav niz sigurnosnih (eng. *IT-security*) i alata koji narušavaju sigurnost(eng. *IT-anti-security*), pri čemu su uvijek odabirane njihove najranjivije inačice. U distribuciju je uključen i čitav sustav za edukaciju koga se može koristiti na više načina. Jedna od primjena je osobno obrazovanje pojedinca zainteresiranog za područje računalne sigurnosti, ali postoje i druge, poput uporabe za održavanje akademskih predavanja.

Prilikom oblikovanja distribucije nastojalo se uključiti što je više moguće alata posvećenih praktičnom dijelu obuke i što više nastavnih materijala koji uključuju opise i rješenja danih zadataka. Ovdje se uglavnom radi o zadacima koje su stvorili članovi *crackmes.de* zajednice.

DVL distribucija namijenjena je jednako početnicima kao i profesionalcima na području računalne sigurnosti. Njezino korištenje pretpostavlja poznavanje Linux operacijskih sustava, budući da se većina rada i zadavanja naredbi svodi na naredbeni redak. Zato se korisnicima koji nisu imali prethodnog doticaja s Linux sustavima predlaže korištenje neke druge distribucije za prikupljanje temeljnih znanja.

DVL je izgrađen na Damn Small Linux (DSL) operacijskom sustavu koji implementira tzv. *LiveCD* način izvedbe. Ovaj koncept omogućuje pokretanje čitavog operacijskog sustava s CD ili sličnog medija, a pritom ne zahtijeva prethodnu instalaciju. Na taj je način čitav sustav prisutan u radnoj memoriji računala, a može ga se jednostavno koristiti u implementacijama virtualnih računala kao što su *VMWare* i *Qemu*.

2.2. Sudionici razvoja

Distribucija je razvijena inicijativom instituta IITEC (eng. *International Institute for Training, Assessment, and Certification*) i S^2E (eng. *Secure Software Engineering*) u suradnji s francuskim timom *The Reverse Engineering Community*. Na čelu razvojnog tima su Dr. Thorsten Schneider (IITAC, S^2E) i Kryshaam (*French Reverse Engineering Team*). S porastom korisnika sustava, raste i opseg njegova korištenja u područjima koja uključuju i akademske ustanove. U Njemačkoj su to *Leibnitz University of Hannover* i *University of Apllied Sciences and Arts Hannover*.

Slika 1: Povezanost Damn Vulnerable Linux sustava s ostalim organizacijama sličnog karaktera

DVL je uvelike potpomognut vanjskim organizacijama usmjerenim na pojedini segment sigurnosti. Značajnije su navedene u nastavku.

- *CrackMes.de* je web stranica skupine entuzijasta namijenjena obrnutom inženjerstvu i razbijanju sigurnosnih mehanizama aplikacija. Ova organizacija učestalo opskrbljuje DVL novim člancima i sigurnosnim izazovima.
- Web sjedište s nazivom *The CodeBreakers Journal* obrađuje teme iz računalne sigurnosti i teme vezane uz napade i obranu. Novi članci izdaju se učestalo, ali tek nakon isrcrpnih recenzija, što pridonosi njihovoj kvaliteti. Radi se o vrlo velikoj zajednici korisnika koja svoje članove broji u tisućama, a čija se veličina svakodnevno povećava.
- Već spomenuta organizacija IITAC osigurava nastavni materijal korišten u uslugama koje uključuju *eLectures*, *eTrainings*, *eSeminars* i *eCertifications*.
- *The Reverse Engineering Community* je forum na kojemu se mogu pronaći brojne upute, moguće je postaviti proizvoljne upite iz ove tematike te vrlo često i dobiti željene odgovore.

2.3. Alati i obrazovni materijali

Alati i upute te ostali edukacijski materijali Damn Vulnerable Linux sustava mogu se podijeliti u nekoliko cjelina prema usmjerenosti na određeni dio sigurnosti računalnih sustava. U nastavku slijedi kratak opis svih dijelova kao i vrsta materijala osiguranih u postojećim i nadolazećim distribucijama sustava.

Jedna od tematskih cjelina je *Practice of Shellcode development* koja se bavi proučavanjem iskorištavanja sigurnosnih ranjivosti aplikacija (eng. *binary exploit*). Slijedi *Practice of Reverse Code Engineering* tema koja sadrži niz aplikacija razvijenih upravo s namjerom omogućavanja praktičnog rada na području razbijanja sigurnosnih mehanizama aplikacija. *Practice of Atrack Web Surface Analysis* se bavi iskorištavanjem propusta vezanih uz web stranice poput umetanja proizvoljnih SQL kodova i iskorištavanja propusta dinamičkih web stranica. *Practice of Attack Surface Analysis and Forensic* se bavi forenzičkom analizom podataka. Konačno, *Practice of Scientific topics* uključuje znanstveni pristup računalnoj sigurnosti.

Obzirom na edukativnu orijentiranost čitave distribucije, navedene tematske cjeline zahtijevaju detaljnije pojašnjenje koje je dano u nastavku.

2.3.1 Iskorištavanje sigurnosnih propusta aplikacija (prepisivanje spremnika)

Pogreška prepisivanja spremnika (eng. *buffer overflow*, *buffer overrun*) je pogreška programa koja se očituje pokušajem pisanja po nedozvoljenim memorijskim lokacijama. Nakon prepisivanja uobičajeno slijedi nasilan prekid izvršavanja programa ili, u slučaju namjerno uzrokovane pogreške, nerijetko i povreda sigurnosti operacijskog sustava.

Ovdje se radi o nepredviđenom stanju sustava kada proces pokušava spremiti podatke izvan granica spremnika konačne veličine. Ishod toga je prepisivanje podataka koji se nalaze na memorijskim lokacijama smještenima neposredno iza samog spremnika. Prepisani podaci mogu biti drugi spremnici,

varijable ili naredbe programskog toka (eng. *program flow data*). Ove pogreške mogu uzrokovati prestanak rada (rušenje) ranjive aplikacije ili dati nepredviđene rezultate. Uzrok njihovoj pojavi može biti posebno oblikovan ulazni podatak, a pažljivo oblikovanje programskog koda namijenjenog provjeri graničnih vrijednosti parametara spremnika ili dobro oblikovan prevoditelj mogu ih ukloniti.
Tehnike za iskorištavanje opisanih ranjivosti ovise o arhitekturi sklopovskog dijela računalnog sustava, operacijskom sustavu i dijelu memorije u kome se ranjivi program nalazi. Iskorištavanje propusta u memorijskom spremniku gomile (eng. *heap*) uvelike se razlikuje od eksploatacije propusta na spremniku stoga (eng. *stack*).
Dva su načina na koja zlonamjeran korisnik može iskoristiti pogrešku prepisivanja spremnika stoga. Prvi način je prepisivanje lokalne varijable koja se nalazi u adresnom prostoru vrlo blizu spremnika. Na ovaj način mijenja se prvotno zamišljeno ponašanje aplikacije u smjeru povoljnom za napadača. Drugi način obuhvaća prepisivanje povratne adrese u okviru spremnika stoga. U tom slučaju aplikacija prilikom izlaska iz funkcije, umjesto da se vrati na dio programskog koda koji je funkciju pozvao, nastavlja sa izvođenjem od memorijske lokacije koja je zapisana na mjestu povratne adrese. Ukoliko je prepisivanje pažljivo izvedeno, povratna adresa će pokazivati na memorijski segment u kome se nalazi programski kod čije izvođenje napadač u konačnici i želi pokrenuti.
Zlonamjerne aktivnosti mogu se temeljiti i na pogreškama prepisivanja spremnika gomile. Memorija u ovom spremniku dinamički se zauzima tijekom izvođenja programa i uglavnom sadrži podatke vezane uz samu aplikaciju. Iskorištavanje je usmjereno na izmjenu postojećih programskih struktura poput pokazivača povezanih lista.

2.3.2 Propusti web aplikacija

U računalnom smislu, napad na sadržaj web stranica (eng. *website defacement*) najčešće se odnosi na izmjenu sadržaja postojećih web stranica. Najpoznatija arhiva takvih web stranica, žrtava napada, nalazi se na adresi http://www.zone-h.org. Ovaj oblik zlonamjernih aktivnosti može se shvatiti kao oblik elektroničkih grafita kojim se različite skupine *hakera* koriste kako bi obznanili vlastita uvjerenja. Radi se o različitim porukama počevši s politički orijentiranim, preko religijskih pa sve do osobnih, isključivo namijenjenih vlastitom probitku.
Za ovakve napade najčešće su odabrane stranice poznatih organizacija ili udruga. Mnogi napadači ostavljaju različite oblike potpisa kako bi dokazali svoje umijeće. Ovdje je potrebno spomenuti i postojanje niza natjecanja na kojima se najbolji mogu okušati u probijanju različitih sigurnosnih zapreka u zadanom vremenskom roku.
Web stranice velikih tvrtki često odražavaju njihov ugled pa je dostupnost i ispravan rad ovih usluga od velike važnosti. Ukoliko se neka institucija nađe pod napadom za koga nije pripremljena, velika je vjerojatnost za pojavu nemogućnosti ispravnog rada web stranica kroz određeno vrijeme. Kako bi se to spriječilo razvijeno je mnogo programskih i sklopovskih rješenja koje koristi većina sigurnosno osviještenih organizacija.
Opisani problem postao je jedan od značajnijih pa je budućim stručnjacima potrebno prenijeti znanja o načinima izvedbe ovakvih napada kako bi mogli uspješno razvijati strategije koje će ih spriječiti.

2.3.3 Reverzni inženjering

Skupina obrazovnih materijala s nazivom *CrackMe* izvorni je doprinos organizacije *crackme.de* u unaprjeđenju obuke vezane uz reverzni inženjering. Riječ je o metodama koje uključuju pretvaranje strojnog koda programa u nešto čitljiviji oblik za čovjeka, što omogućava analizu načina rada aplikacije s ciljem razbijanja zaštitnih mehanizama. Ovoj skupini programa pripadaju aplikacije s karakterističnim nazivima *crackmes*, *reversemes* i *keygenmes*. Mehanizam zaštite sličan je kod svih, a nalazi se u velikom broju komercijalnih proizvoda.
Crackme.de smatra se najvećom svjetskom organizacijom na ovom području računalne sigurnosti. Svi zainteresirani za ovakav oblik rada i provjere svojih sposobnosti pozvani su da se pridruže legalnim metodama dokazivanja svojeg znanja. Daljnje upute dostupne su na web stranicama koje se nalaze na adresi http://www.crackmes.de/.

2.3.4 Forenzička analiza

Riječ je o posebnim tehnikama koje se koriste u analizi elektroničkih podataka, poduzetih aktivnosti pri korištenju računala, rekonstrukcije djelomično ispravnih podataka i ostalim oblicima analize. Ovo područje pored stručnih zahtijeva i pravna znanja e budući da je u izravnom doticaju sa zakonima vezanim uz računalni kriminal i zakonima o privatnosti podataka. Postupak forenzičke analize izvodi se s ciljem otkrivanja načina korištenja računala, odnosno potencijalnih ilegalnih ili neautoriziranih postupaka. Sve poduzete aktivnosti istražitelja moraju biti u skladu s njihovim ovlastima jer se u protivnom pronađeni dokazi mogu odbaciti u sudskom postupku. Ova distribucija Linux operacijskog sustava u svojim budućim inačicama obuhvatit će i važne teme s ovog područja.

2.3.5 Edukacijski materijali

Edukacijski materijali podijeljeni su u nekoliko skupina navedenih u nastavku.

- *eLectures* obuhvaća prezentacije i video materijale koji se koriste na sveučilišnim predavanjima, a uključuje i komercijalne materijale. Za prikaz video sadržaja koristi se Flash tehnologija koja uključuje i zvuk te jednostavno kretanje kroz tijek prezentacije.
- *eTrainigs* su video sadržaji koji prikazuju primjere vezane uz pojedinu temu. Uz video materijal dostupan je i odgovarajući paket datoteka koji sadrži sav materijal prikazan u multimedijskom dijelu prezentacije. Na ovaj način omogućen je istovremeno praktičan rad korištenjem netom stečenih vještina i saznanja.
- *eSeminars* su zapravo virtualne učionice koje omogućuju interakciju korisnika s nastavnikom i ostalim sudionicima u realnom vremenu. Za prisustvovanje ovom obliku nastave nije potrebna nikakva specifična sklopovska niti programska podrška. Ovim je izbjegnuta i potreba za putovanjem na određenu fizičku lokaciju. Potrebno je samo u određeno vrijeme biti priključen na Internet.

2.4. Nadogradnje

Ovo izdanje DVL operacijskog sustava nikako nije i posljednje. Autori distribucije su najavili su čestoe nadogradnje. Plan nadogradnje dijeli se u tri faze kako bi se njegovo odvijanje moglo jednostavnije i preglednije pratiti.

Prva faza obuhvaća prikupljanje svih korisnih podataka i alata koji će sustav učiniti pogodnijim za učenje. Također, u ovoj fazi će se dodati i nekoliko video uradaka koji će novim korisnicima služiti kao upute kod prvih susreta s DVL operacijskim sustavom. Pored toga, proširit će se i opseg postojećih tekstualnih uputa dostupnih na web stranicama projekta.

Druga faza obuhvaća više programskih dodataka (eng. *binary plugins*) poput Crackmes, Exploitmes, usavršavanja preko Interneta (eng. *eTraining*) i novih predavanja putem Interneta (eng. *eLearning*). Nadalje, u ovoj će se fazi povećati opseg članaka i ostalih dokumenata te će se tako omogućiti lakše razumijevanje rada cijelog sustava. U zadnjoj, trećoj fazi, nastojati će se poboljšati napredniji dodaci poput PHP, SQL, CGI i drugih sličnih aplikacija. K tome, poraditi će se još na usavršavanju elemenata koji su inicijalno namijenjeni obradi u prve dvije faze.

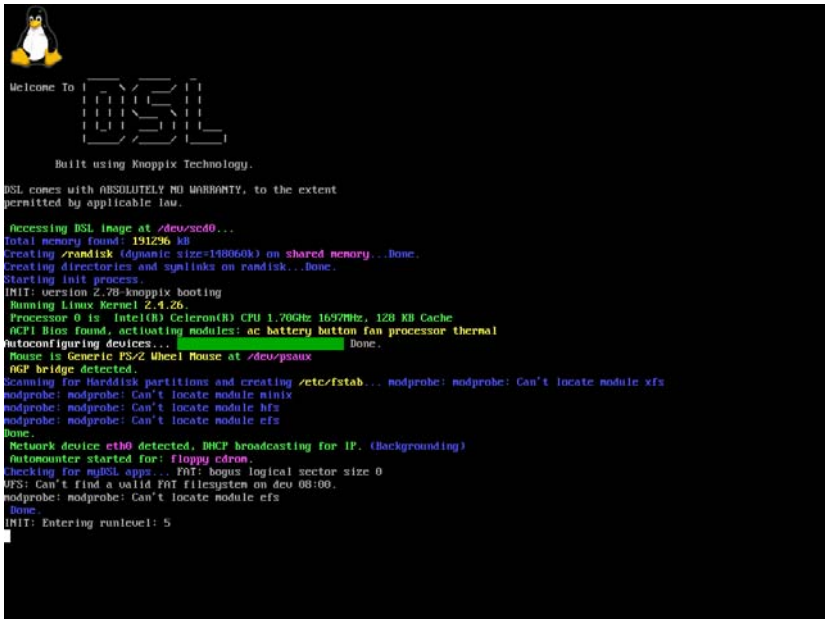
Dodaci (eng. *plugins*) pomažu u modularnoj orijentaciji razvoja DVL operacijskog sustava. Prvi strateški dio čini razvojni tim koji osigurava dostupnost ključnih elemenata sustava i temeljnog nastavnog materijala. Drugi dio je zajednica. Radi se o velikom broju suradnika koji su zaduženi za unapređenje različitih elemenata DVL sustava. Njihov doprinos očituje se stvaranjem zadataka za obuku koji mogu, ali i ne moraju uključivati pisanje izvornog koda. Osim toga, oni osiguravaju rješenja i opise postupaka te teoretsku podlogu. Svatko može pomoći i svatko je pozvan da pomogne. Jedan od ciljeva je izgraditi siguran programski okvir (eng. *framework*) koji će se moći koristiti za proces ispitivanja i otkrivanja sigurnosnih nedostataka. Pisanje novih nastavnih materijala s drugačijim pristupom također je dobrodošlo, kao i razvijanje lekcija vezanih uz konkretne probleme računalne sigurnosti. Konačno, kako navodi glavni autor, već i samo korištenje ovog sustava svojevrstan je doprinos zajednici.

3. Rad sa sustavom

Rad s Damn Vulnerable Linux sustavom svodi se na korištenje nekoliko alata dostupnih u inicijalnoj distribuciji. Među njima su ftp, web i ssh poslužitelji te klijenti za ove usluge. Ovdje su uključeni i alati namijenjeni programerima. Kao i svaka Linux distribucija, i DVL sadrži alate za postavljanje sustava, grafičkog korisničkog sučelja i sl.. U nastavku slijedi kratak opis temeljnih funkcionalnosti uz njihov istovremeni prikaz.

3.1. Pokretanje sustava

Kako je već pojašnjeno, DVL sustav se distribuira u obliku CD slike (eng. *image*) - live CD mediju. To znači da je pokretanje sustava gotovo istovjetno pokretanju bilo koje druge aplikacije, što kod većine Linux operacijskih sustava nije uobičajeno. Na taj se način čitav sustav nalazi u radnoj memoriji i ne zahtijeva nikakve modifikacije, a što je još važnije, nema opasnosti po postojeće podatke na diskovnim particijama. Također, čitav se sustav može pokretati na emulatorima računalnog sklopovlja, tj. virtualnim računalima. Tako se postiže istovremeno izvođenje operacijskog sustava domaćina (eng. *host*) i gosta (eng. *guest*). Na slijedećoj slici prikazan je inicijalni postupak pokretanja operacijskog sustava DSL:

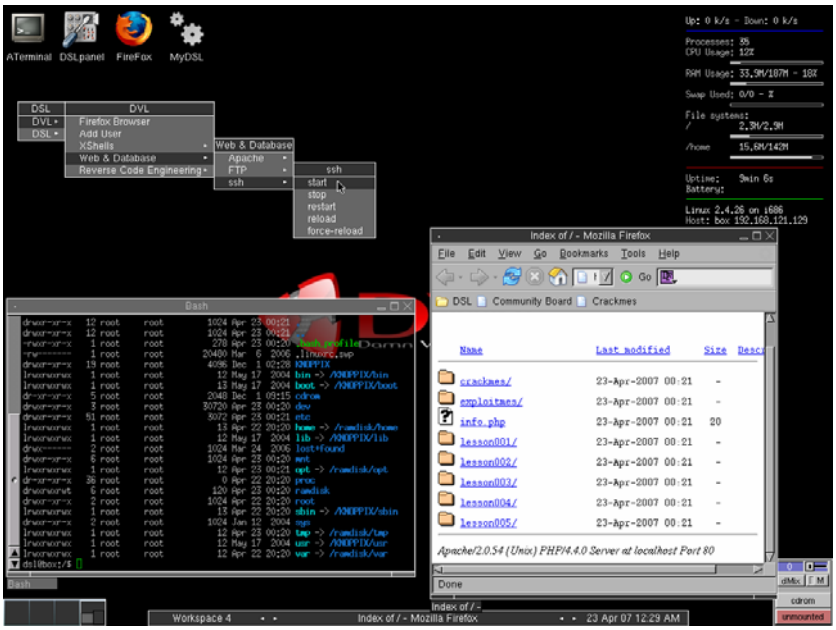


Slika 2: Pokretanje operacijskog sustava

3.2. Grafičko korisničko sučelje

Po završetku postupka pokretanja sustava (eng. *boot*) pojavljuje se grafičko korisničko sučelje s *fluxbox* upraviteljem prozora (eng. *window manager*). Uključeno je i grafičko sučelje minimalnih zahtjeva po resurse s nazivom *jwm* (*Joe's Window Manager*) pa korisnik može odabrati grafičko sučelje koje smatra prikladnijim za korištenje.

Pritiskom na desnu tipku miša, pojavljuje se glavni izbornik s dva podizbornika: DSL i DVL. Riječ je o izbornicima vezanim uz Damn Small Linux i Damn Vulnerable Linux, respektivno. DVL podizbornik se grana dalje na podizbornike koji između ostalog omogućuju pokretanje popularnog web preglednika Firefox, a sadrže i prečac do jednostavnog grafičkog sučelja aplikacije za dodavanje novih korisnika sustava – *Add User*. Ostali podizbornici vezani su uz različite inačice terminala (prozora naredbenih redaka) - *XShells*, web poslužitelj Apache, ftp i ssh poslužitelje. Posebno zanimljiv podizbornik je *Reverse Code Engineering* koji sadrži prečace do korisnih alata za reverzni inženjering. Izbornik i neke aplikacije prikazani su na sljedećoj slici:

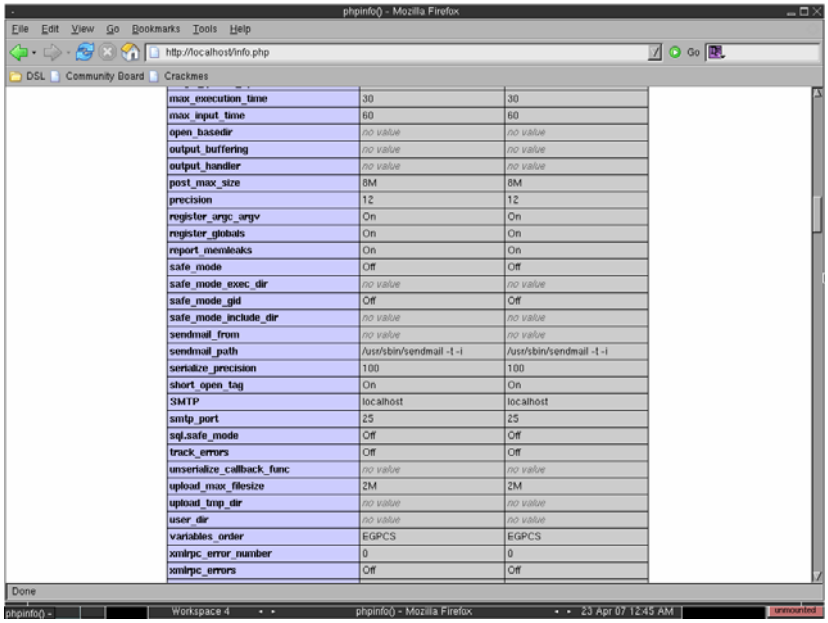


Slika 3: Prikaz glavnog izbornika

3.3. Alati

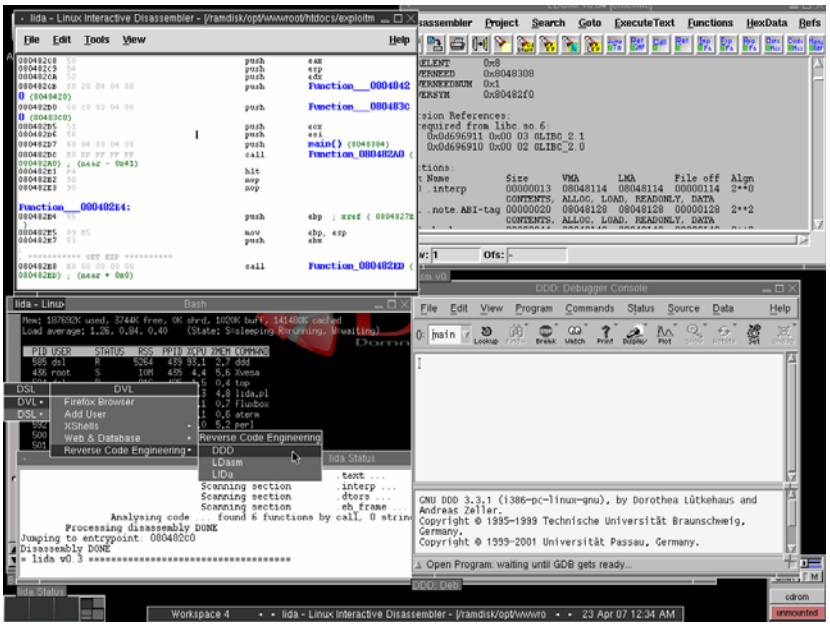
Odabirom kratice *Add User* otvara se aplikacija vrlo jednostavnog sučelja za dodavanje i brisanje korisnika sustava. Ona je korisna kod dodavanja korisnika za FTP ili neki drugi oblik *vanjskog* pristupa sustavu. Nadalje, postoji više implementacija terminalnih prozora koji se mogu koristiti prema korisnikovim preferencijama. Neke mogućnosti su već poznate iz Damn Small Linux sustava, ali umetnute su i neke nove poput terminalnog emulatora *For Light/Dark Blinded* kojim se ostvaruje veća preglednost teksta konzole, a to nerijetko povećava i produktivnost rada.

Moguće je korištenje različitih programskih poslužitelja, kao što su apache, ftp i ssh. Jednostavna manipulacija nad svakim od poslužitelja omogućena je korištenjem prečaca umjesto potrebe za upisivanjem naredbi u naredbeni redak – *start*, *restart* i *stop*. Nakon pokretanja Apache web poslužitelja upisivanjem „*localhost*" adrese u web preglednik dobiva se popis edukacijskih materijala. Ovo je ujedno i dobar način provjere ispravnosti rada Apache paketa. Edukacijski materijali prikazani na ovaj način opisani su u prethodnoj cjelini pa ih nije potrebno dodatno pojašnjavati. Dovoljno je navesti kako se radi o opisima web usmjerenih napada, iskorištavanja spremnika i tehnika reverznog inženjerstva. Omogućeno je učitavanje „info.php" datoteke koja daje tablicu s postavkama Apache poslužitelja vezanih uz interpretaciju PHP skripta. U spomenutoj tablici razvidne su vrlo nesigurne postavke sustava. Jedna od njih je i isključena *safe_mode* postavka. Ipak, u skladu s konačnim ciljem ove distribucije, nepravilnom konfiguracijom poput ove olakšava se uočavanje ranjivosti web poslužitelja i PHP interpretera. Prikaz spomenute tablice dan je na sljedećoj slici:



Slika 4: Ranjivo postavljen PHP interpreter

Posljednji podizbornik u DVL skupini je *Reverse Code Engineering*. Ovdje su sadržani prečaci do alata potrebnih za reverzni inženjering. Jedan od njih je i *Data Display Debugger* (*DDD*) – često korišteno grafičko sučelje prema aplikacijama namijenjenim otklanjanju programskih pogrešaka (eng. debugging). Radi se o alatima *GDB, DBX* i *XDB*. Sljedeća aplikacija je *LDasm* (*Linux Disassembler*), izrađena po uzoru na poznatu aplikaciju iz svijeta reverznog inženjerstva na Windows operacijskim sustavima, *W32Dasm*. Ovo je svakako jedan od nezaobilaznih alata vezanih uz reverzni inženjering. Posljednja aplikacija uključena u ovu distribuciju je *LIDa* (*Linux Interactive DisAssembler*).



Slika 5: Prikaz alata za obrnuti inženjering

Mogućnost korištenja MySQL poslužitelja baza podataka osigurana je i na ovom sustavu. Pozicioniranjem u direktorij `/opt/mysql` te pokretanjem naredbe `./configure` obavlja se inicijalno postavljanje svih potrebnih parametara i pokretanje samog poslužitelja. Terminalni prozor unutar kojeg je izvedena ova naredba dan je na sljedećoj slici. Ukoliko se želi koristiti MySQL klijent,

treba promijeniti tekući direktorij u `/opt/mysql/bin` te pokrenuti naredbu `mysql`. Za provjeru ispravnosti pokrenutog poslužitelja potrebno je pokrenuti naredbu

```
dsl@box:/opt/mysql/bin/$ mysql --version
```

Ispis bi trebao dati podatke vezane uz inačicu instaliranog MySQL paketa. U ovom slučaju to je 4.1.21, jedna od ranjivijih inačica MySQL sustava za upravljanje bazama podataka.

Slika 6: Prikaz pokretanja MySQL aplikacije

Na ovoj Linux distribuciji prisutan je i *gcc* prevoditelj. Prvi korak u provjeri ispravnosti instalirane inačice spomenutog prevoditelja je pokretanje naredbe:

```
dsl@box:/$ gcc --version
```

Ispis bi trebao odgovarati sljedećem sadržaju:

```
gcc (GCC) 3.3.4 (Debian 1:3.3.4-7)
Copyright (C) 2003 Free Software Foundation, Inc.
This is free software; see the source for copying donfitions. There is NO
Warranty; not even for MERCHANTABILITY or FITNESS FOR FOR A PARTICULAR
PURPOSE.
```

Riječ je o inačici prevoditelja koja ima ugrađene mehanizme provjere sigurnosnih pogrešaka temeljenih na prepisivanju spremnika pa je s te strane posebno korisna u kontekstu za koji je namijenjena distribucija.
S obzirom da korisnik nerijetko ima zahtjeve za razvojem programa ili programskih odsječaka u nižem programskom jeziku - asembleru, u DVL je integriran i paket HLA (eng. *High-Level Assembler*). Paket je posebno pogodan i za učenje asemblera pa nije potrebno napominjati da se radi o neizbježnom alatu za reverzni inženjering.

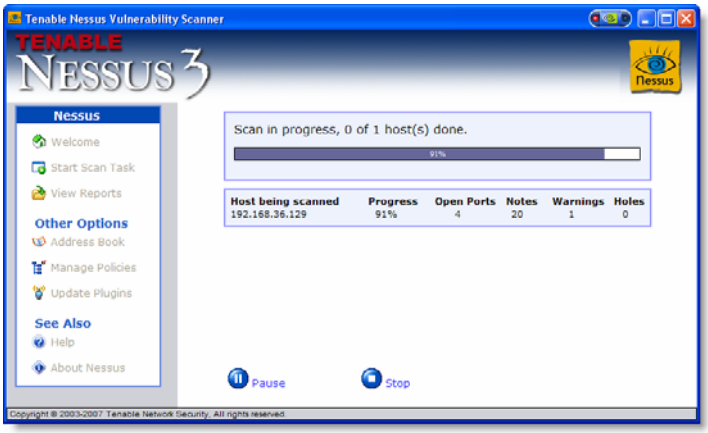
Slika 7: Prikaz pokretanja ***High-Level Assembler*** alata

Kao što je već spomenuto na početku poglavlja, glavni izbornik sadrži podizbornik s nazivom DSL, preuzet iz Damn Small Linux distribucije. Ovdje su sadržani brojni alati korišteni kod uobičajenih Linux distribucija pa ih u kontekstu ovog dokumenta nije potrebno posebno opisivati. Korisnicima se preporuča samostalno istraživanje ovog podizbornika, budući da sadrži prečace do različitih korisnih aplikacija kao i mogućnosti postavljanja različitih parametara grafičkog sučelja.

4. Sigurnosna ispitivanja DVL sustava

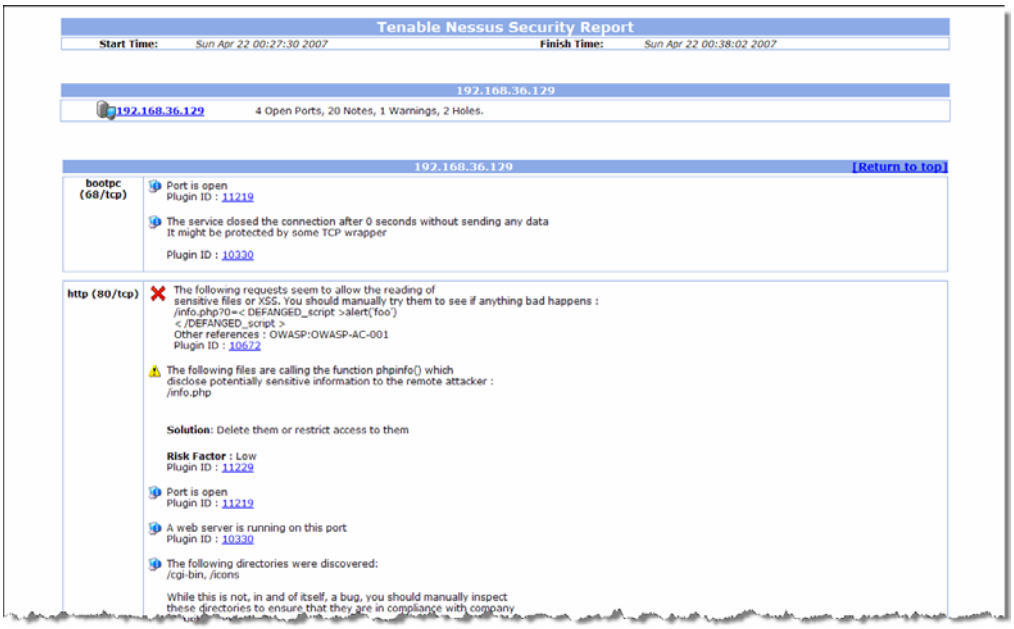
Za potrebe ovog dokumenta načinjen je jednostavan test sigurnosti DVL distribucije korištenjem *Nessus* alata. Nessus je jedan od često korištenih alata namijenjenih automatskoj detekciji otprije poznatih propusta u sustavu.

Pored Nessus alata, korišten je i Nmap, alat za pregled priključaka (eng. *port scan*) otvorenih na provjeravanom računalu. Korištenje alata za pregled otvorenih priključaka nije dozvoljeno na računalima korisnika koji to nisu eksplicitno odobrili, kao ni na bilo kojem drugom javno dostupnom računalu. Pregled za potrebe ovog dokumenta izveden je u kontroliranom okruženju na komu se DVL izvodi korištenjem emulatora virtualnog računala VMWare. Tijek izvođenja sigurnosne provjere prikazan je slijedećom slikom:



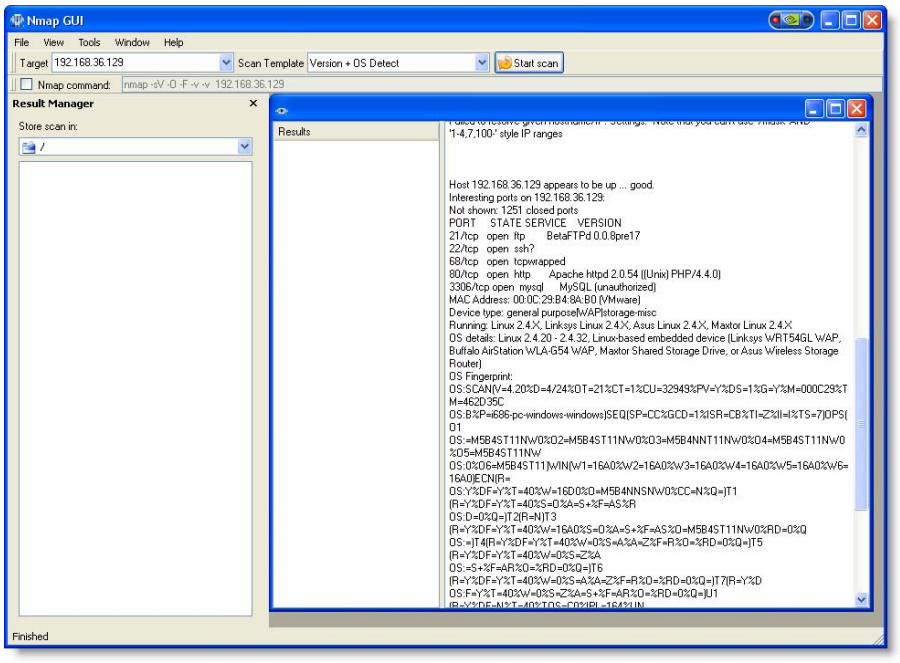
Slika 8: Izvođenje sigurnosne provjere DVL sustava

Prikaz rezultata vidljiv je na slijedećem ispisu.



Slika 9: Rezultati sigurnosne provjere Nessus alatom

Budući da je popis sigurnosnih nedostataka poveći, na prikazu je dan samo isječak s početka izvješća. Nessus je pronašao i one ranjivosti koje su opisane u početnim predavanjima iz web sigurnosti. Pregled otvorenih priključaka daje rezultate prikazane sljedećom slikom:



Slika 10: Rezultati pregleda Nmap alatom

Na popisu se pored nabrojanih priključaka mogu uočiti i inačice pozadinskih aplikacija koje ih koriste. Ova informacija je korisna napadaču jer se može usmjeriti na iskorištavanje propusta čije je postojanje dokumentirano, a ne mora trošiti vrijeme na ispitivanje svih mogućih propusta svojstvenih nekoj vrsti usluge. Primjerice, FTP poslužitelj korišten na DVL sustavu je BetaFTPd inačice 0.0.8pre17.

5. Zaključak

Damn Vulnerable Linux nije jedina Linux distribucija namijenjena edukaciji na području računalne sigurnosti, ali je krajnjem korisniku najjednostavnija za korištenje budući da ne zahtijeva kupovinu popratnog udžbenika niti je strogo orijentirana prema određenom segmentu sigurnosti kao neke druge distribucije. Uklapanjem čitavog niza vježbi i zadataka te popratnih opisa, DVL sustav omogućava prve korake i bez pristupa web stranicama projekta. Ipak, na web stranicama nalaze se i edukacijski video sadržaji zasada vezani uz temeljno korištenje sustava i neke specifične propuste. Ovi sadržaji nisu uključeni u distribuciju iz očitog razloga – drastičnog povećanja veličine ISO datoteke koju se preuzima s weba. Međutim, daljnji razvoj mogao bi se orijentirati prema dvjema inačicama – kompaktnoj, koja bi uključivala samo nužne pakete i edukacijske materijale, i potpunoj koja bi uključivala sve do tada izdane video i audio materijale te ostale oblike edukacijskih materijala.

Tema iskorištavanja ranjivosti računalnih programa obično se može podijeliti u tri cjeline koje uključuju:

- korištenje pogrešaka prepisivanja spremnika, pogrešaka obrade/formatiranja znakovnog niza i premjestivog programskog koda (eng. shellcode),
- iskorištavanje propusta vezanih uz web, primjerice umetanje SQL koda, modificiranje putova (eng. *path*) i korištenje propusta u implementaciji web stranica te
- obrnuto inženjerstvo koje obuhvaća analizu aplikacija na razini strojnog jezika (asembler), mehanizme zaštite od neovlaštenog kopiranja te pokazuje koliko su te zaštite uistinu jake.

DVL je usmjeren na pojašnjavanje sigurnosnih propusta prve i treće skupine – pogrešaka prepisivanja spremnika i obrnutog inženjerstva. Uz uključen velik broj članaka i dokumenata na ovu temu, DVL uključuje i sve alate potrebne za praktičnu primjenu znanja prikupljenih iz različitih obrazovnih materijala.

Na kraju je potrebno naglasiti da je DVL dobro osmišljen i koristan projekt čija je temeljna namjena edukacija pa se svim zainteresiranima za ovo područje računalne tehnologije savjetuje upoznavanje s ovom Linux distribucijom i svim njenim mogućnostima.

6. Reference

[1] International Institute for Training, Assessment, and Certification, http://www.damnvulnerablelinux.org/, 2007.

[2] International Institute for Training, Assessment, and Certification, http://www.secure-software-engineering.com/, 2007.

[3] Liberenix, http://librenix.com/?inode=10148, 2007.

[4] Kriptopolis, http://www.kriptopolis.org/damn-vulnerable-linux, ožujak 2007.

[5] Securing Linux by breaking it with Damn Vulnerable Linux, http://www.linux.com/article.pl?sid=07/02/15/1747220, 2007.

[6] International Institute for Training, Assessment, and Certification, http://www.iitac.org/, 2007.

[7] Nmap sigurnosni alat, http://insecure.org/, 2007.

[8] French Reverse Engineering Team, http://www.binary-reverser.org/, travanj 2007.

[9] Wikipedia, http://en.wikipedia.org/wiki/Reverse_engineering, travanj 2007.

[10] Analiza Nessus alata, CARNet CERT & LSS, CCERT-PUBDOC-2007-01-181.pdf, siječanj 2007.

[11] Damn VulnerableLinux, http://themostboringblogintheworld.wordpress.com/2007/04/17/damn-vulnerable-linux-the-live-cd-that-teaches-you-how-to-hack-download/, travanj 2007.

[12] Damn Vulnerable Linux, http://weldan.wordpress.com/2007/03/10/damn-vulnerable-linux/, ožujak 2007.

[13] Damn Vulnerable Blog, http://blog.damnvulnerablelinux.org/, travanj 2007.