Uvod

Dobro došli u šesto izdanje knjige *Hakerske tajne za neupućene*. U njoj ćete pronaći trikove i tehnike za hakovanje računara, izložene na jednostavan način, koje možete koristiti za procenu bezbednosti informacionih sistema, pronalaženje ranjivosti i otklanjanje slabih mesta pre nego što ih iskoriste zlonamerni hakeri i drugi napadači. Ovde opisano hakovanje predstavlja pre svega profesionalan i legitiman način za testiranje bezbednosti, zbog čega ga ja u knjizi nazivam *etičko hakovanje*, odnosno *testiranje ranjivosti i neprobojnosti.*

Bezbednost računara i mreže složene su teme i stalne mete napadača. Morate biti dobro pripremljeni da biste zaštitili informacije od „loših momaka". U tome će vam pomoći tehnike i alatke iz ove knjige.

Čak i ako implementirate sve moguće bezbednosne tehnologije i najbolje postojeće prakse, to ne znači da je vaše mrežno okruženje potpuno bezbedno. Tek kada savladate način na koji razmišljaju zlonamerni napadači, primenite ta znanja i upotrebite prave alatke za procenu sistema koristeći njihov ugao posmatranja, steći ćete predstavu o tome koliko su zaista bezbedni vaši sistemi i informacije.

Etičko hakovanje (ili, jednostavnije, procena bezbednosti), koje podrazumeva formalno i sistematično testiranje ranjivosti i neprobojnosti, neophodno je za pronalaženje slabih mesta i potvrdu stalne bezbednosti informacionih sistema. Ova knjiga sadrži ono što vam je potrebno da biste uspešno realizovali program procene, obavili odgovarajuće provere bezbednosti, uveli prave mere zaštite i tako zadržali na odstojanju hakere i zlonamerne korisnike.

O knjizi

Knjiga Hakerske tajne za neupućene jeste priručnik o tome kako da hakujete sistem da biste poboljšali njegovu bezbednost i sveli poslovni rizik na minimum. Tehnike za testiranje bezbednosti zasnivaju se na pisanim pravilima za testiranje neprobojnosti računarskog sistema, testiranje ranjivosti i na najboljim praksama bezbednosti informacija. U knjizi je obuhvaćeno sve što je potrebno, od uspostavljanja plana testiranja, preko procene sistema i pronalaženja slabih mesta do upravljanja programom za testiranje bezbednosti koji se koristi.

U većini mreža, operativnih sistema i aplikacija koje se svakodnevno koriste postoje na hiljade mogućih ranjivosti. Ovde ću na različitim platformama i sistemima opisati samo one najvažnije, koje – po mom mišljenju – doprinose najvećem broju bezbednosnih problema u savremenom poslovanju. Obradiću osnovni *Pareto* princip, ili „pravilo 80/20", jer želim da vam pomognem da pronađete tih 20 procenata problema koji dovode do 80 procenata bezbednosnih rizika. Bez obzira na to da li bezbednosne ranjivosti procenjujete u maloj kućnoj profesionalnoj mreži, korporativnoj mreži srednje veličine ili u velikim poslovnim

sistemima, u knjizi *Hakerske tajne za neupućene* pronaći ćete sve informacije koje su vam potrebne.

Ova knjiga sadrži sledeće:

- različite tehničke i druge testove i njihove detaljno opisane metodologije.
- specifične kontra-mere za zaštitu od hakovanja i napada.

Pre nego što započnete testiranje sistema, upoznajte se sa informacijama iz dela 1, kako biste se pripremili za zadatke koji su pred vama. Izreka „ko ne planira uspeh, planira neuspeh" pokazala se kao tačna kada je reč o proceni bezbednosti – ako želite da uspete, morate napraviti solidan plan.

Pretpostavke

Odricanje od odgovornosti: Ova knjiga je namenjena isključivo stručnjacima iz oblasti informacionih tehnologija (IT) i bezbednosti koji imaju ovlašćenje da testiraju svoje sisteme ili sisteme svojih klijenata. Ako informacije iz ove knjige iskoristite za zlonamerno i neovlašćeno hakovanje ili provaljivanje u računarske sisteme, radite to na sopstvenu odgovornost. Ni ja (kao autor) ni bilo ko drugi povezan sa ovom knjigom nećemo biti odgovorni za neetička i kriminalna dela koja biste mogli počiniti uz pomoć metodologija i alata koji su ovde opisani.

Nadam se da je sada sve jasno: ova knjiga je za vas ako ste administrator sistema, menadžer za bezbednost informacija, konsultant ili revizor za bezbednost, menadžer za usklađenost ili ste na neki drugi način zainteresovani za procenu slabih mesta računarskih sistema, softvera i IT operacija, kao i za njihovo obezbeđivanje na duži rok.

Pretpostaviću da, kao stručnjak za IT ili bezbednost:

- poznajete osnovne koncepte i termine u vezi sa računarima, mrežama i bezbednošću informacija;
- imate pristup računaru i mreži na kojima ćete koristiti ove tehnike i alatke;
- imate odobrenje svog poslodavca ili klijenta za primenu tehnika za hakovanje koje se opisuju u ovoj knjizi.

Ikonice upotrebljene u knjizi

UPAMTITE

Značenja ikonica na marginama knjige.
Informaije vredne pamćenja.

UPOZORENJE

Informacije koje mogu imati negativan uticaj na testiranje ranjivosti i neprobojnosti – obavezno ih pročitajte!

Savet kojim se ističe ili objašnjava neka važna tema.

TEHNIČKI DETALJI

Tehničke informacije koje su zanimljive, ali ne i presudne za razumevanje teme o kojoj je reč.

Uz knjigu

Pre nego što nastavite, pogledajte *podsetnik* (engl. *cheat sheet*) priložen uz ovu knjigu. Možete mu pristupiti ako posetite veb lokaciju *dummies.com* i potražite naslov *Hacking For Dummies*. Podsetnik je odličan način da, u slučaju potrebe, prilikom primene programa za testiranje bezbednosti ostanete na pravom putu ili se na njega vratite.

Obavezno pogledajte i moju veb lokaciju `www.principlelogic.com`, a posebno stranicu sa izvorima informacija (*Resources*).

Kada završite sa čitanjem

Što više naučite o tome kako deluju spoljni hakeri i napadači, i kako vaš sistem treba da se testira, bolje ćete obezbediti računarske i mrežne sisteme. Ova knjiga sadrži osnove koje su vam potrebne za razvoj i održavanje uspešnog programa za upravljanje procenom bezbednosti i ranjivosti, a samim tim i za svođenje poslovnih rizika na minimum.

Zavisno od konfiguracije računara i mreže, možda ćete moći da preskočite određena poglavlja. Na primer, ako ne koristite Linux ili bežične mreže, ta poglavlja će vam biti suvišna. Međutim, budite oprezni: vi sami možda ne koristite određene sisteme, ali se oni mogu nalaziti na vašoj mreži, otvoreni za zloupotrebu.

Imajte na umu da se koncepti testiranja bezbednosti višeg nivoa neće menjati tako često kao ranjivosti za koje uspostavljate zaštitu. Testiranja ranjivosti i neprobojnosti uvek će predstavljati i nauku i umetnost u ovoj dinamičnoj oblasti. Morate biti u toku sa najnovijim hardverskim i softverskim tehnologijama, kao i sa različitim vrstama ranjivosti koje ih prate u stopu.

Za hakovanje sistema nećete pronaći samo jedan *najbolji način*, zato prilagodite ove informacije svojim potrebama. Srećno vam hakovanje!