U OVOM POGLAVLJU

- Ciljevi hakera i zlonamernih korisnika
- Kako se odvija testiranje bezbednosti
- Šta ugrožava računarske sisteme
- Pokretanje postupka za testiranje bezbednosti

Poglavlje 1

Uvod u testiranje ranjivosti i neprobojnosti

U ovoj knjizi se govori o testiranju bezbednosne ranjivosti računara i mreža, kao i o otklanjanju slabih mesta koja se pronađu kako napadači ne bi dobili priliku da ih zloupotrebe.

Terminologija

Svi su čuli za hakere i zlonamerne korisnike, a mnogi su i na sopstvenoj koži osetili posledice njihovih kriminalnih aktivnosti. Ko su ti ljudi i zašto treba da ih upoznamo? U sledećim odeljcima pronaći ćete kratke opise ovih napadača.

U knjizi koristim sledeću terminologiju:

UPAMTITE

- **Hakeri** (ili *spoljni napadači)* pokušavaju da, kao neovlašćeni korisnici i najčešće spolja, pristupe računarima, osetljivim informacijama ili čak celim mrežama da bi na nepošten način ostvarili neki cilj. Hakeri napadaju gotovo svaki sistem koji im se učini dostupnim. Neki više vole reprezentativne i dobro zaštićene sisteme, ali svako hakovanje i svaki sistem podižu rejting napadača u hakerskim krugovima.

- **Zlonamerni korisnici** (*spoljni* ili *unutrašnji napadači)* pokušavaju da pristupe računarima i osetljivim informacijama spolja (kao klijenti ili poslovni partneri) ili iznutra (kao ovlašćeni i pouzdani korisnici). Zlonamerni korisnici napadaju sisteme koje mogu da iskoriste za ostvarivanje nepoštenih ciljeva, jer mogu imati pristup takvim sistemima ili znanja o njima.

  Zlonamerni napadači su, uopšteno govoreći, i hakeri i zlonamerni korisnici. Da bi sve bilo jednostavnije, i jedne i druge ću nazivati *hakerima*, a na *hakere* i *zlonameme korisnike* razdvajaću ih samo onda kada treba da istaknem neku razliku ili detaljnije opišem njihove specifične alatke, tehnike i načine razmišljanja.
- **Etički hakeri** (ili *„dobri momci"*) hakuju sisteme da bi otkrili njihove ranjivosti i zaštitili ih od neovlašćenog pristupa, zloupotrebe ili pogrešne upotrebe. U ovu kategoriju spadaju istraživači, konsultanti i interno osoblje u oblasti bezbednosti informacija.

Haker

Termin haker (engl. *hacker*) ima dva značenja:

- U tradicionalnom značenju, hakeri vole da petljaju sa softverskim ili elektronskim sistemima, uživaju u tome da istražuju i uče kako rade računarski sistemi. Vole da otkrivaju nove načine rada, kako mehaničkim tako i elektronskim putem.
- Poslednjih godina, terminom *haker* obuhvataju se i oni koji koji zlonamerno provaljuju u sisteme iz lične koristi. Tehničkim žargonom rečeno, ovi hakeri kriminalci su provalnici (engl. *crackers*) koji zlonamerno provaljuju u sisteme da bi stekli slavu, intelektualnu svojinu, profit ili to čak rade iz osvete. Provalnici menjaju, brišu i kradu najvažnije informacije, ili isključuju čitave mreže iz funkcije, što često nanosi veliku štetu korporacijama i vladninim službama.

  Napominjem da savremena pop-kultura i mediji uveliko svojataju termin *hakovanje* i uvode ga u razne oblasti. Stručnjaci za marketing, političari imedijski stratezi znaju da većina ljudi ne razume termin *hakovanje* pa ga često koriste onako kako im odgovara da bi postigli svoje ciljeve, ali ne dozvolite da vas to zbuni.

UPOZORENJE

Dobri hakeri, ili hakeri *sa belim šeširom* (engl.*white-hat)*, ne žele da budu u istoj kategoriji sa lošim hakerima, ili hakerima *sa crnim šeširom (engl. black-hat*). (Ako vas zanima, termini *beli šešir* i *crni šešir* potiču iz starih vestern filmova, u kojima su „dobri momci" nosili bele kaubojske šešire, a „loši momci" crne.) Hakeri sa *sivim šeširom* (engl. *gray-hat*) imaju osobine i jednih i drugih. U svakom slučaju, većina ljudi terminu *haker* pripisuje negativno značenje.

Mnogi zlonamerni hakeri tvrde da oni zapravo ne nanose štetu nego pomažu drugima za opštedruštveno dobro. Ja se s tim ne bih složio. Zlonamerni hakeri su negativci i zaslužuju da snose posledice za ono što rade.

Pazite samo da ne pomešate hakere kriminalce sa istraživačima bezbednosti. Istraživači hakuju dobronamerno, razvijaju sjajne alatke koje možemo da koristimo, a najčešće i sa punom odgovornošću preduzimaju korake da se njihovi rezultati i programski kôdovi objave.

Zlonamerni korisnik

Pod terminom zlonamerni korisnik (engl. *malicious user*) – koji se često koristi u bezbednosnim krugovima i pojavljuje u naslovima o ugrožavanju informacija – podrazumevaju se zlonamerni zaposleni, ugovarači, pripravnici ili drugi korisnici koji zloupotrebljavaju dodeljene privilegije. Problem ne mora biti to što su korisnici hakovali interne sisteme, nego što su zloupotrebili privilegije za pristup računarima koje su im poverene. Korisnici se uvlače u najvažnije sisteme baza podataka da bi prikupili osetljive informacije, poslali poverljive informacije klijenta e-poštom konkurenciji ili na neko drugo mesto u oblaku, odnosno da bi sa servera obrisali osetljive datoteke kojima nije trebalo da imaju pristup.

Ponekad neki korisnik – bez ikakvog znanja, slučajno i bez loše namere – može dovesti do bezbednosnih problema ako premesti, obriše ili ošteti osetljive informacije. U poslovnom svetu čak i nedužan pritisak prsta na tastaturu može imati dalekosežne posledice. Zamislite samo sve mogućnosti inficiranja ucenjivačkim softverom i kako to može da utiče na poslovanje širom sveta. Potreban je samo jedan pritisak mišem da nepažljivi korisnik inficira celu mrežu.

Zlonamerni korisnici su najčešće najgori neprijatelji stručnjaka za informacione tehnologije i bezbednost informacija, jer oni tačno znaju kuda treba da idu po ono što im je potrebno i ne moraju biti stručnjaci za računare da bi ugrozili osetljive informacije. Ovi korisnici mogu da pristupe onome što im treba, a uprava kompanije im veruje i ne postavlja suvišna pitanja.

A šta ćemo sa Edwardom Snowdenom, bivšim službenikom američke Agencije za nacionalnu bezbednost, koji je „otkucao“ sopstvenog poslodavca? Ovo je složena tema (o motivaciji hakera govoriću u poglavlju 2). Šta god mislili o Snowdenu, on je zloupotrebio svoja ovlašćenja i prekršio uslove ugovora o poverljivosti. Isto važi za svaku drugu osobu koja, iz bilo kojih razloga, stekne slavu na sličan način.

Zlonamerni napadači i etički hakeri

Od hakera prevaranata potrebna vam je zaštita – morate biti jednako vešti kao i momci koji pokušavaju da napadnu vaše sisteme. Pravi stručnjak za procenu bezbednosti ima veštine, mentalni stav i alatke hakera, ali je pouzdan. Hakuje sistem da bi testirao bezbednost, na osnovu toga kako haker razmišlja i deluje.

UPAMTITE

Etičko hakovanje (poznato i kao testiranje ranjivosti i neprobojnost) obuhvata iste alatke, trikove i tehnike koje koriste hakeri kriminalci, sa jednom važnom razlikom: obavlja se uz dozvolu za ciljni sistem i u profesionalnom okruženju. Svrha ovog testiranja je otkrivanje ranjivosti sa aspekta zlonamernog napadača i poboljšanje bezbednosti sistema. Testiranje ranjivosti i neprobojnosti deo je ukupnog programa upravljanja rizikom u oblasti informacija, koji omogućava stalna poboljšanja bezbednosti. Ovakvim testiranjem može se obezbediti legitimnost izjava proizvođača o bezbednosti njihovih proizvoda.

TEHNIČKI DETALJI

SERTIFIKATI ZA TESTIRANJE BEZBEDNOSTI

Ako testirate ranjivost i neprobojnost i želite da dodate novi sertifikat svojim ovlašćenjima, razmislite o mogućnosti da postanete *sertifikovani etički haker* (engl. *Certified Ethical Hacker*, C|EH) preko programa sertifikacije koji finansira Savet EZ (više informacija potražite na veb lokaciji `www.eccouncil.org`). Poput *sertifikata za stručnjake u oblasti bezbednosti informacionih sistema* (engl. *Certified Information Systems Security Professional*, CISSP), sertifikat C|EH je opštepoznat i priznat u ovoj oblasti, a ima i akreditaciju *Američkog nacionalnog instituta za standarde* (engl. *American National Standards Institute*, ANSI 17024).

Druge opcije obuhvataju program *sertifikacije za globalnu bezbednost informacija* (engl. *Global Information Assurance Certification*, GIAC) instituta SANS, program za *sertifikovanog ispitivača neprobojnosti* (engl. *Certified Penetration Tester*, CPT) *Odbora za reviziju sertifikacije za bezbednost informacija* (engl. Information Assurance Certification Review Board, IACRB) i program kompanije *Offensive Security* za stručnu sertifikaciju (engl. *Offensive Security Certified Professional*, OSCP), što zapravo predstavlja sertifikaciju za testiranje bezbednosti u praksi. Volim ovaj pristup, jer se često dešava da oni koji obavljaju ovaj posao nemaju odgovarajuće praktično iskustvo sa alatkama i tehnikama da bi ih koristili na pravi način (više informacija potražite na veb lokaciji `www.giac.org` i `www.offensive-security.com`).

Testiranje ranjivost i neprobojnosti i provera bezbednosti

Testiranje bezbednosti pomoću testa ranjivosti i neprobojnosti često se meša sa proverom bezbednosti, ali razlika je velika kad je reč o ciljevima. Provera bezbednosti se odnosi na poređenje bezbednosnih smernica kompanije (ili zahteva o usklađenosti) sa onim što se stvarno dešava u praksi. Cilj provere bezbednosti jeste da se utvrdi da li postoje kontrole bezbednosti, najčešće tako što se koristi pristup sa aspekta rizika. Ova provera često obuhvata procenu poslovnih procesa i ponekad nije previše tehnički orijentisana; štaviše, provere bezbednosti se mogu svoditi na podsetnike u obliku liste kojima treba da se ispuni određeni zahtev o usklađenosti.

UPAMTITE

Ne odvijaju se sve provere na višim nivoima, ali mnoge koje sam video prilično su jednostavne, posebno one koje se odnose na usklađenost sa *Standardom za bezbednost podataka platnih kartica* (engl. *Payment Card Industry Data Security Standard*, PCI DSS) i *Sigurnosnim pravilom Zakona o prenosivosti i odgovornosti zdravstvenog osiguranja* (engl. *Health Insurance Portability and Accountability Act*, HIPAA). Često ih obavljaju lica koja nemaju tehnička znanja o računarima, mrežama odnosno aplikacijama, ili čak lica koja nemaju nikakve veze sa informacionim tehnologijama!

Nasuprot tome, procene bezbednosti koje se zasnivaju na etičkom hakovanju usmerene su na ranjivosti koje se mogu iskorišćavati. Ovim pristupom testiranju potvrđuje se da bezbednosne kontrole *ne postoje* ili da su neefikasne. Ovo formalno testiranje ranjivosti i neprobojnosti može biti i tehničko i netehničko, a često je (iako podrazumeva korišćenje formalne metodologije) manje strukturirano od formalne provere. Ako je provera u vašoj organizaciji obavezna (npr. za sertifikacije SSAE 16, SOC 1/2/3 ili ISO 27001), razmislite o integrisanju tehnika za testiranje ranjivosti i neprobojnosti o kojima govorim u ovoj knjizi sa sopstvenim programom za proveru informacionih tehnologija ili bezbednosti. Provera bezbednosti i testiranje ranjivosti i neprobojnosti veoma se dobro dopunjavaju.

Smernice za testiranje bezbednosti

Ako odlučite da testiranje ranjivosti i neprobojnosti uvrstite u program upravljanja rizikom u oblasti informacija svoje kompanije, morate imati dokumentovane smernice za testiranje bezbednosti. U njima treba da se navede ko sprovodi testiranje, koji se opšti tip testiranja obavlja i koliko često. Specifične procedure za testiranje mogu da sadrže metodologije koje se opisuju u ovoj knjizi. Možete razmisliti i o izradi dokumenta o bezbednosnim standardima u kome bi se navele specifične alatke za testiranje bezbednosti koje se koriste i lica koja sprovode testiranja. U skladu sa potrebama poslovanja, možete utvrditi standardne datume za testiranje – na primer, jednom u tri meseca za eksterne sisteme i dva puta godišnje za interne.

Usklađenost i regulatorna pitanja

Internim smernicama može se odrediti kako uprava posmatra testiranje bezbednosti, ali treba da uzmete u obzir i državne, lokalne i međunarodne zakone i propise koji utiču na vaše poslovanje. Poseban strah u kosti istraživačima uteruje *Zakon o autorskom pravu u digitalnoj eri* (engl. *Digital Millennium Copyright Act*, DMCA). Na veb lokaciji `www.eff.org/issues/dmca` potražite šta sve sadrži DMCA.

Mnogim federalnim zakonima i propisima u Sjedinjenim Državama — kao što su HIPAA i povezani akt *Health Information Technology for Economic and Clinical Health* (HITECH), *Gramm-Leach-Bliley Act* (GLBA), *North American Electric Reliability Corporation* (NERC) *Critical Infrastructure Protection* (CIP) i PCI DSS – zahtevaju se jake kontrole i dosledne procene bezbednosti. Od toga se ne razlikuju ni povezani međunarodni zakoni – npr. *Personal Information Protection and Electronic Documents Act* (PIPEDA) u Kanadi, *Uredba o zaštiti podataka o ličnosti* (engl. *General*

Data Protection Regulation, GDPR) u Evropskoj uniji i *Japan's Personal Information Protection Act* (JPIPA) u Japanu. Usklađivanje testova bezbednosti sa ovim zahtevima predstavlja odličan način za poštovanje državnih i lokalnih propisa, kao i za sprovođenje programa opšte bezbednosti informacija i zaštite privatnosti.

Zašto treba da hakujete svoje sisteme

Da biste uhvatili lopova, morate da razmišljate kao lopov – to je osnova testiranja ranjivosti i neprobojnosti. Poznavanje neprijatelja je ključno, a zakon verovatnoće radi protiv bezbednosti. Zbog sve većeg broja hakera i njihovih sve širih znanja, kao i zbog sve većeg broja ranjivosti sistema i drugih nepoznanica, svi računarski sistemi i aplikacije će, pre ili kasnije, biti hakovani na neki način. Ono što postaje sve važnije jeste zaštita sistema od „loših momaka", a ne samo pronalaženje najbolje opšte bezbednosne prakse. Kada upoznate hakerske trikove, otkrićete koliko su vaši sistemi zaista ranjivi.

Hakovanje se oslanja na slabe bezbednosne prakse i neotkrivene ranjivosti. Najnovija istraživanja, kao što je godišnji izveštaj *Data Breach Investigations Report* (DBIR) kompanije *Verizon* (`www.verizonenterprise.com/verizon-insights-lab/dbir`), pokazuju da se cilja i na dugotrajne i *poznate* ranjivosti. Mrežne barijere, šifrovanje i druge moderne (i skupe) bezbednosne tehnologije često vode do lažnog osećaja sigurnosti. Ovi bezbednosni sistemi su uglavnom usmereni na ranjivosti višeg nivoa, kao što su kontrola pristupa i zaštita informacija u prolazu, bez uticaja na to kako zlonamerni hakeri deluju. Ako svoje sisteme napadnete da biste otkrili njihove ranjivosti – posebno one koje su na dohvat ruke i uvaljuju u nevolju najveći broj korisnika – moći ćete bolje da ih obezbedite. Testiranje ranjivosti i neprobojnosti dokazana je metoda za jačanje odbrane sistema od napada. Ako ne identifikujete slabosti, samo je pitanje vremena kada će one biti zloupotrebljene.

Dok hakeri proširuju svoja znanja, i vi treba da radite isto. Morate da razmišljate i radite kao oni da biste od njih zaštitili svoje sisteme. Kao etički haker, morate poznavati aktivnosti koje obavljaju neetički hakeri i načine kojima se zaustavljaju njihovi pokušaji. Ako znate šta tražite i kako da upotrebite ove informacije, sprečićete hakere u njihovim namerama.

SAVET

Sisteme ne morate zaštititi od *svega, niti je tako nešto moguće.* Jedina potpuna zaštita bila bi ta da isključite napajanje računarskih sistema i stavite ih pod ključ tako da niko ne može da im priđe (čak ni vi sami), ali to ne bi bio dobar pristup sa aspekta bezbednosti, a još manje sa apsekta poslovanja. Najvažnije je da sisteme zaštitite od poznatih ranjivosti i najčešćih napada – onih čuvenih 20 procenata problema koji dovodi do 80 procenata rizika, a koji se u većini organizacija pokazuju kao slabosti koje se najčešće previđaju.

Nećete moći da predvidite sve ranjivosti koje će se pojavljivati u sistemima i poslovnim procesima. Ne možete da pravite planove za sve tipove napada,

posebno za one nepoznate; međutim, što više kombinacija budete isprobavali i što češće budete testirali cele sisteme a ne samo njihove pojedinačne delove, imaćete veće šanse da otkrijete ranjivosti koje utiču na informacione sisteme u celini.

Nemojte pri tome ići predaleko sa testiranjem – jačanje odbrane sistema od napada koji su malo verovatni (pa čak i onih koji su *manje* verovatni) nema mnogo smisla.

UPAMTITE

Vaši opšti ciljevi pri testiranju bezbednosti treba da budu sledeći:

- Dodelite prioritete sistemima kako biste mogli da se usmerite na ono što je zaista važno.
- Testirajte sisteme na nedestruktivan način.
- Nabrojte ranjivosti i, ako je potrebno, dokažite upravi da postoje poslovni rizici.
- Primenite rezultate kako biste pronašli ranjivosti i ojačali bezbednost sistema.

Opasnosti sa kojima se suočavaju sistemi

Jedno je uopšteno znati da su vaši sistemi moguća meta napada hakera iz celog sveta i lokalnih zlonamernih korisnika, a nešto sasvim drugo poznavati specifične potencijalne napade na sisteme. U ovom poglavlju ćemo govoriti o nekim najpoznatijim napadima, ali to nipošto neće biti konačan spisak.

Mnoge bezbednosne ranjivosti nisu kritične pojedinačno, ali iskorišćavanje nekoliko ranjivosti istovremeno može da nanese štetu sistemskom ili mrežnom okruženju. Unapred zadata (engl. *default*) konfiguracija operativnog sistema Windows, slaba lozinka administratora SQL Servera ili server koji se izvršava na bežičnoj mreži sami po sebi ne moraju predstavljati glavne bezbednosne probleme; međutim, ako bi neko iskorišćavao sve ove ranjivosti istovremeno, mogao bi (između ostalog) omogućiti neovlašćeni udaljeni pristup i obelodaniti osetljive informacije.

UPAMTITE

Složenost je neprijatelj bezbednosti.

Ranjivosti i napadi su poslednjih godina sve češći zbog virtuelizovanja, računarstva u oblaku pa čak i društvenih medija. Ove tri oblasti znatno usložnjavaju vaše radno okruženje.

Netehnički napadi

Zloupotrebe u koje spada manipulisanje ljudima – krajnjim korisnicima ili čak vama – predstavljaju najslabiju tačku u svakoj računarskoj ili mrežnoj infrastrukturi. U prirodi ljudi je da veruju drugima, zbog čega često dolazi do iskorišćavanja slabosti ljudske prirode kako bi se došlo do informacija (često preko pecanja e-poštom) i mogućnosti njihove zloupotrebe. Ovo nazivamo socijalni inženjering

(engl. *socijal engineering*). U poglavlju 6. naći ćete više informacija o socijalnom inženjeringu i kako da od njega odbranite svoje sisteme.

Drugi česti i delotvorni napadi na informacione sisteme jesu fizički. Hakeri provaljuju u zgrade, prostorije sa računarima ili na druga mesta koja sadrže najvažnije informacije, odnosno imovinu, da bi ukrali računare, servere i drugu vrednu opremu. U fizičke napade spada i *kopanje po smeću* (engl. *dumpster diving*) – pretraživanje kontejnera i kanti za otpatke u potrazi za intelektualnom svojinom, lozinkama, mrežnim dijagramima i drugim informacijama.

Napadi na mrežnu infrastrukturu

Napadi na mrežnu infrastrukturu mogu se lako izvesti, jer se mnogim mrežama preko interneta može pristupiti sa bilo kog mesta u svetu. Primeri napada na mrežne infrastrukture su sledeći:

- Povezivanje sa mrežom preko neobezbeđene bežične pristupne tačke povezane iza mrežne barijere.
- Iskorišćavanje slabosti mrežnih protokola, kao što su *File Transfer Protocol* (FTP) i *Secure Sockets Layer* (SSL).
- Preplavljivanje mreže prevelikim brojem zahteva i korišćenje *napada uskraćivanjem usluga* (engl. *denial of service*, DoS) za legitimne zahteve.
- Instaliranje analizatora mreže na mrežnom segmentu i hvatanje svakog paketa koji se kreće preko njega, pri čemu se otkrivaju poverljive informacije u obliku čistog teksta.

Napadi na operativne sisteme

Hakovanje operativnog sistema je metoda koju „loši momci“ najčešće koriste, zato što svaki računar ima operativni sistem. Operativni sistemi su podložni mnogim poznatim iskorišćavanjima i sadrže slaba mesta koja godinama ostaju bez zakrpa.

Povremena meta napada su i neki operativni sistemi koji su se u praksi pokazali bezbednim – kao što su stari ali još upotrebljivi Novell NetWare, OpenBSD i IBM serija i – pri čemu se i u njima pojavljuju slaba mesta; međutim, izgleda da hakeri više vole da napadaju Windows, Linux i Mac OS jer se najviše koriste.

Sledi nekoliko primera za napade na oprativne sisteme:

- Iskorišćavanje zakrpa koje nedostaju
- Napadanje ugrađenih sistema za proveru identiteta
- Provaljivanje bezbednosti sistema datoteka
- Provaljivanje lozinki i implementacija slabih šifrovanja