Sadržaj

UVOD 1
O knjizi 1
Pretpostavke 2
Ikonice upotrebljene u knjizi 2
Uz knjigu 3
Kada završite sa čitanjem 3

DEO 1: POSTAVLJANJE TEMELJA ZA TESTIRANJE BEZBEDNOSTI 5

POGLAVLJE 1: **Uvod u testiranje ranjivosti i neprobojnosti** 7
Terminologija 7
Haker 8
Zlonamerni korisnik 9
Zlonamerni napadači i etički hakeri 9
Testiranje ranjivost i neprobojnosti i provera bezbednosti 10
Smernice za testiranje bezbednosti 11
Usklađenost i regulatorna pitanja 11
Zašto treba da hakujete svoje sisteme 12
Opasnosti sa kojima se suočavaju sistemi 13
Netehnički napadi 13
Napadi na mrežnu infrastrukturu 14
Napadi na operativne sisteme 14
Aplikacije i drugi specijalizovani napadi 15
Poštovanje principa procene bezbednosti 15
Poštovanje hakerske etike 15
Poštovanje privatnosti 16
Bez padova sistema 16
Pokretanje testa ranjivosti i neprobojnosti 17
Izrada plana 17
Izbor alatki 19
Sprovođenje plana 20
Procena rezultata 22
Primena preporuka 22

POGLAVLJE 2: **Kako razmišljaju hakeri** 23
Protiv čega se borite 23
Ko provaljuje u računarske sisteme 26
Tehnička znanja i veštine hakera 26
Motivacija hakera 27
Zašto to rade 28
Planiranje i izvođenje napada 31
Čuvanje anonimnosti 33

POGLAVLJE 3: **Priprema plana za testiranje bezbednosti** . . . 35
Definisanje ciljeva . . . 35
Biranje sistema za testiranje . . . 38
Definisanje standarda testiranja . . . 40
Pravi trenutak za testiranje . . . 40
Posebni testovi . . . 41
Procena sistema sa informacijama o njemu ili bez njih . . . 42
Izbor lokacije . . . 43
Odgovor na pronađene ranjivosti . . . 43
Pretpostavke . . . 44
Izbor alatki za procenu bezbednosti . . . 44

POGLAVLJE 4: **Metodologija hakovanja** . . . 47
Priprema za testiranje . . . 47
Posmatranje iz perspektive drugih . . . 49
Sistemi za skeniranje . . . 50
Hostovi . . . 50
Otvoreni priključci . . . 51
Šta se izvršava na otvorenim priključcima . . . 51
Procenjivanje ranjivosti . . . 54
Iskorišćavanje ranjivosti . . . 55

DEO 2: TESTIRANJE NA DELU . . . 57

POGLAVLJE 5: **Prikupljanje informacija** . . . 59
Prikupljanje javnih informacija . . . 59
Društveni mediji . . . 60
Pretraživanje veba . . . 60
Programi tragači . . . 61
Veb lokacije . . . 62
Mapiranje mreže . . . 62
WHOIS pretraživanje . . . 62
Pravilnik o privatnosti . . . 64

POGLAVLJE 6: **Socijalni inženjering** . . . 65
Šta je socijalni inženjering . . . 65
Testiranje pomoću socijalnog inženjeringa . . . 66
Zašto napadači koriste socijalni inženjering . . . 67
Posledice . . . 68
Sticanje poverenja . . . 69
Iskorišćavanje odnosa . . . 69
Napadi socijalnim inženjeringom . . . 72
Definisanje cilja . . . 72
Potraga za informacijama . . . 72
Mere protiv socijalnog inženjeringa . . . 77
Pravila . . . 77
Podizanje svesti i obuka korisnika . . . 77

POGLAVLJE 7: **Fizička bezbednost** 81
Najvažnije slabe tačke fizičke bezbednosti 82
Pronalaženje fizičkih ranjivosti u poslovnom prostoru 83
Infrastruktura objekta 83
Instalacije 84
Raspored u poslovnom prostoru i kako se koristi 86
Komponente mreže i računari 88

POGLAVLJE 8: **Lozinke** 93
Ranjivost lozinki 94
Organizacione ranjivosti lozinki 94
Tehničke ranjivosti lozinki 95
Provaljivanje lozinki 96
Provaljivanje lozinki na tradicionalan način 96
Provaljivanje lozinki pomoću alatki visoke tehnologije 99
Provaljivanje datoteka zaštićenih lozinkom 107
Ostali načini za provaljivanje lozinki 108
Opšte mere protiv provaljivanja lozinki 113
Čuvanje lozinki 114
Definisanje pravila o lozinkama 114
Ostale mere zaštite 115
Zaštita operativnih sistema 117
Windows 117
Linux i Unix 118

DEO 3: HAKOVANJE MREŽNIH HOSTOVA 119

POGLAVLJE 9: **Sistemi mrežne infrastrukture** 121
Šta su ranjivosti mrežne infrastrukture 122
Biranje alatki 123
Programi za skeniranje i analizatori 123
Procenjivanje ranjivosti 124
Skeniranje i provociranje mreže 124
Priključci za skeniranje 125
Skeniranje SNMP protokola 130
Otimanje zaglavlja 132
Testiranje pravila mrežnih barijera 133
Analiziranje mrežnih podataka 135
MAC-daddy napad 141
Testiranje napada uskraćivanjem usluga 146
Otkrivanje najčešćih slabosti rutera, komutatora i mrežnih barijera . . . 149
Pronalaženje neobezbeđenih interfejsa 149
Otkrivanje problema sa protokolima SSL i TLS 150
Uspostavljanje opšte odbrane mreže 150

POGLAVLJE 10: **Bežične mreže** 153
Posledice ranjivosti bežičnih mreža 153
Biranje alatki 154
Otkrivanje bežičnih mreža 156
Provera globalnog prepoznavanja 156
Skeniranje lokalnih vazdušnih talasa 157
Otkrivanje napada na bežičnu mrežu i sprovođenje mera zaštite 158
Šifrovani saobraćaj 160
Mere protiv napada na šifrovani saobraćaj 164
Zaštićeno podešavanje Wi-Fi mreže 165
Mere protiv ranjivosti WPS PIN-a 167
Piratski bežični uređaji 168
Mere protiv piratskih bežičnih uređaja 171
Lažiranje MAC adresa 172
Mere protiv lažiranja MAC adresa 175
Problemi fizičke bezbednosti 175
Mere protiv problema fizičke bezbednosti 176
Ranjive bežične radne stanice 176
Mere protiv ranjivosti bežičnih radnih stanica 177
Unapred zadati parametri 177
Mere protiv iskorišćavanja unapred zadatih parametara 177

POGLAVLJE 11: **Mobilni uređaji** 179
Merenje ranjivosti mobilnih uređaja 179
Provaljivanje lozinki laptop računara 180
Biranje alatki 180
Primena mera zaštite 184
Provaljivanje lozinki telefona i tablet računara 185
Provaljivanje iOS lozinki 186
Primena mera protiv provaljivanja lozinki 189

DEO 4: HAKOVANJE OPERATIVNIH SISTEMA 191

POGLAVLJE 12: **Windows** 193
Uvod u ranjivosti Windows sistema 194
Biranje alatki 195
Besplatne Microsoft alatke 195
Univerzalne alatke za procenu 196
Alatke za posebne namene 196
Prikupljanje informacija o ranjivostima Windows sistema 197
Skeniranje sistema 197
NetBIOS 199
Otkrivanje anonimnih sesija 202
Mapiranje 202
Prikupljanje informacija 203
Mere protiv hakovanja anonimnih sesija 205

Provera dozvola za deljene resurse 206
Unapred zadate vrednosti za Windows. 207
Testiranje 208
Iskorišćavanje nezakrpljenih propusta 208
Korišćenje alatke Metasploit 211
Mere protiv iskorišćavanja ranjivosti nastalih zbog nezakrpljenih propusta 215
Pokretanje skeniranja sa proverom identiteta 216

POGLAVLJE 13: **Linux i macOS** 219
Razumevanje Linux ranjivosti 220
Izbor alatki 220
Prikupljanje informacija o ranjivosti sistema 221
Skeniranje sistema 221
Mere protiv skeniranja sistema 224
Nalaženje nepotrebnih i nesigurnih servisa 225
Skeniranje sistema 225
Mere protiv napada na nepotrebne usluge 227
Zaštita datoteka .rhosts i hosts.ekuiv 229
Hakovanje korišćenjem datoteka hosts.equiv i .rhosts. 229
Mere protiv napada na datoteke .rhosts i hosts.equiv 230
Procena bezbednosti NFS 232
NFS hacks. 232
Mere protiv napada NFS-a. 232
Provera ovlašćenja datoteka. 233
Hakovanje dozvola datoteka. 233
Mere protiv hakovanja dozvola datoteka 233
Pronalaženje ranjivosti prepunjavanjem bafera 234
Napadi 234
Mere protiv napada prepunjenog bafera 235
Provera fizičke sigurnost 235
Fizičko ugrožavanje sigurnosti 235
Mere protiv fizičkih napada na bezbednost 236
Izvršavanje opštih sigurnosnih testova 237
Krpljenje 238
Ažuriranje distribucija 239
Višeplatfomski menadžeri ažuriranja 239

DEO 5: HAKERSKE APLIKACIJE 241

POGLAVLJE 14: **Sistemi za komunikaciju i razmenu poruka** 243
Uvod u ranjivosti sistema za razmenu poruka. 243
Prepoznavanje i borba protiv napada na e-poštu 244
Bombardovanje e-poštom 244
Zaglavlja 248
Napadi na SMTP 249
Opšti najbolji postupci za smanjivanje rizika po sigurnost pošte . . . 258

Razumevanje VoIP protokola 259
VoIP ranjivosti 260
Mere protiv VoIP ranjivost 264

POGLAVLJE 15: **Veb aplikacije i aplikacije za mobilne uređaje** 265
Izbor alata za testiranje sigurnosti na vebu 266
Traženje Web ranjivosti 267
Pregled direktorijuma 267
Mere protiv pregleda direktorijuma 270
Napadi filtriranja ulaza 271
Mere protiv napada preko polja za upis 278
Unapred zadati script napad 278
Mere protiv unapred zadatih skript napada 280
Nesigurni mehanizmi prijavljivanja 280
Mere za nezaštićene sisteme za prijavu 283
Izvršavanje opštih sigurnosnih skeniranja za proveru ranjivosti veb aplikacije 284
Smanjivanje veb sigurnosnih rizika 284
Sigurnost pomoću nevidljivosti 285
Postavljanje mrežne barijere 286
Analiziranje izvornog koda 286
Otkrivanje mana mobilne aplikacije 287

POGLAVLJE 16: **Baze podataka i sistemi skladištenja** 289
Zaronimo u baze podataka 289
Izbor alata 290
Pronalaženje baza podataka na mreži 290
Provaljivanje lozinki baze podataka 291
Skeniranje baza podataka na ranjivosti 292
Sledimo najbolje postupke za smanjivanje sigurnosnih rizika 293
O sistemima za skladištenje 294
Izbor alata 294
Pronalaženje sistema za skladištenje na mreži 295
Iskorenjivanje poverljivih sadržaja u datotekama na mreži 296
Držimo se najboljih postupka za smanjivanje rizika za skladištenje podataka 297

DEO 6: POSLE TESTIRANJA SIGURNOSTI 299

POGLAVLJE 17: **Izveštavanje o rezultatima** 301
Sakupljanje podataka 302
Određivanje prioriteta ranjivosti 303
Izrada izveštaja 304

POGLAVLJE 18: **Zatvaranje sigurnosnih rupa** 307
Pretvorite izveštaje u akciju 307
Krpljenjem do savršenstva 308

Upravljanje zakrpama 309
Automatizacija 309
Jačanje sistema 310
Procena sigurnosne infrastrukture 311

POGLAVLJE 19: **Upravljanje sigurnosnim procesima** 313
Automatizacija procene sigurnosti. 313
Nadgledanje zlonamerne upotrebe. 314
Angažovanje spoljnih saradnika za procenu sigurnosti 316
Podizanje svesti o sigurnosti. 317
Održati korak sa sigurnosnim naporima drugih 319

DEO 7: DEO SA DESET SAVETA 321

POGLAVLJE 20: **Deset saveta kako da budete prihvaćeni kao stručnjak za sigurnost** 323
Stvorite saveznika i podršku 323
Ne budite katastrofičar 324
Pokažite da organizacija ne može priuštiti sebi da bude hakovana 324
Istaknite opšte koristi testiranja sigurnosnosti 325
Pokažite kako testiranje sigurnosti na specifičan način može da pomogne vašoj organizaciji 325
Uključite se u posao 326
Uspostavite svoj kredibilitet 326
Razgovarajte jezikom uprave 326
Prikažite vrednost vašeg truda 327
Budite fleksibilni i prilagodljivi 327

POGLAVLJE 21: **Deset razloga zašto je hakovanje jedini uspešan način za testiranje** 329
Loši momci misle loše, koriste dobre alatke i razvijaju nove metode. . . 329
IT upravljanje i usaglašavanje 330
Ranjivost i detaljni testovi dopunjuju kontrolne i sigurnosne procene . . . 330
Klijenti i partneri će vas pitati koliko su sigurni vaši sistemi. 330
Zakon o proseku funkcioniše protiv kompanija. 331
Sigurnosne procene poboljšavaju razumevanje pretnji za poslovanje . . . 331
Ako se dogodi sigurnosni proboj, morate imati nešto na šta se možete osloniti. 331
Detaljno testiranje iznosi ono najgore u sistemima 332
Kombinovano testiranje ranjivosti i neprobojnosti 332
Odgovarajuće testiranje može da otkrije slabosti koje ste prevideli. . . . 332

POGLAVLJE 22: **Deset smrtnih grešaka** 333
Nedobijanje odobrenja 333
Pretpostavka da možete pronaći sve ranjivosti 334
Pretpostavka da možete ukloniti sve ranjivosti 334
Jednokratno testiranje 334
Mislite da sve znate 335
Testiranje bez gledanja na stvari iz perspektive hakera 335

Ne testirate prave sisteme 335
Ne koristite dobre alatke 335
Testiranje proizvodnih sistema u pogrešno vreme 336
Angažovanje spoljnih saradnika za testiranje 336

DODATAK: SPISAK ALATA I KORISNIH VEB STRANA 337

SPISAK TERMINA KORIŠĆENIH U KNJIZI 351

INDEKS 353

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!

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 *zlonamerne 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.

SERTIFIKATI ZA TESTIRANJE BEZBEDNOSTI



TEHNIČKI DETALJI

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

U OVOM POGLAVLJU

- Šta je socijalni inženjering
- Kakve su posledice socijalnog inženjeringa
- Testiranje pomoću socijalnog inženjeringa
- Zaštita vaše organizacije od socijalnog inženjeringa

Poglavlje 6
Socijalni inženjering

Socijalnim inženjeringom (engl. *social engineering*) iskorišćava se jedna od najslabijih karika u odbrani bezbednosti informacija svake organizacije – ljudi. Socijalni inženjering je zapravo hakovanje osoba, jer podrazumeva zloupotrebu ljudske lakovernosti kako bi se dobile informacije za ostvarivanje lične koristi.

Socijalni inženjering spada u one vrste hakovanja koje je najteže izvršiti, jer treba da budete prilično samouvereni i vešti da bi vas potpuni stranac doživeo kao osobu od poverenja. Od takvog hakovanja ćete se najteže zaštititi, jer su njime obuhvaćena i osobe koje donose odluke o bezbednosti.

U ovom poglavlju ćemo se baviti posledicama socijalnog inženjeringa, vašim sopstvenim tehnikama za testiranje bezbednosti u ovoj oblasti i posebnim merama za odbranu od socijalnog inženjeringa.

Šta je socijalni inženjering

U scenariju socijalnog inženjeringa, zlonamerni napadači se predstavljaju kao druge osobe, kako bi došli do informacija koje bi teško dobili na neki drugi način. Informacije koje su dobili od svojih žrtava koriste za pustošenje mrežnih resursa, krađu ili brisanje datoteka, čak i za korporativnu špijunažu ili neki drugi oblik prevare organizacije koju napadaju. Socijalni inženjering se razlikuje od iskorišćavanja *fizičke bezbednosti*, kao što su špijuniranje preko ramena ili kopanje po smeću, ali ova dva tipa hakovanja su povezana i često se koriste zajedno.

Sledi nekoliko primera socijalnog inženjeringa:

- „**Osoblje za podršku“**, koje tvrdi da mora da instalira zakrpu ili novu verziju softvera na računaru korisnika, nagovara korisnika da preuzme softver i tako dobija kontrolu nad sistemom.
- **„Proizvođači“**, koji tvrde da moraju da ažuriraju računovodstveni ili telefonski sistem organizacije, traže lozinku od administratora i dobijaju neograničen pristup.
- **„Zaposleno lice“**, koje obaveštava službu obezbeđenja da je izgubilo propusnicu za centar podataka, dobija ključeve od obezbeđenja, a time i neovlašćeni pristup fizičkim i elektronskim informacijama.
- **„E-pošta za pecanje“**, koja se šalje zbog prikupljanja identifikatora i lozinki od primalaca, ili zato da bi se na njihove računare instalirao zlonamerni softver. Ovi napadi po svojoj prirodi mogu biti opšti ili ciljani – ovi drugi se ponekad nazivaju podvodni ribolov (engl. *spearphishing*). Ovlašćenja za prijavljivanje ili zlonamerni softver kriminalci koriste za pristup mreži ili intelektualnoj svojini, za šifrovanje datoteka zbog traženja otkupa i slično.

Ponekad se ovakvi napadači predstavljaju kao pouzdani i upućeni rukovodioci ili stručnjaci, a ponekad glume neobaveštene i naivne zaposlene. Mogu da nastupe i kao spoljni saradnici – na primer, IT konsultanti ili radnici službe za održavanje. Socijalni inženjeri vešto se prilagođavaju svojim ciljnim grupama. Za ovako nešto potrebna je posebna vrsta ličnosti, a u ekstremnim slučajevima reč je o sociopatama.



UPAMTITE

Efikasna bezbednost informacija – posebno ona koja je neophodna za zaštitu od socijalnog inženjeringa – često počinje i završava se korisnicima. Druga poglavlja ove knjige sadrže savete o tehničkoj kontroli koja vam može pomoći u borbi protiv socijalnog inženjeringa, ali nemojte zaboraviti da osnovna ljudska komunikacija i interakcija u svakom trenutku imaju veoma važan uticaj na nivo bezbednosti organizacije. Ako napravimo poređenje sa reklamama u kojima se slatkiši opisuju kao „*tvrdi i hrskavi spolja, a mekani iznutra*“, onda taj „tvrdi i hrskavi“ deo predstavlja sloj mehanizama (mrežnih barijera, sistema za sprečavanje upada, filtriranja sadržaja itd.) na koje se organizacije najčešće oslanjaju dok štite svoje informacije. „Mekani“ deo su ljudi i procesi unutar organizacije. Ako „loši momci“ prodru kroz tvrdi sloj, ugroziće unutrašnji sloj koji je najčešće bez zaštite.

Testiranje pomoću socijalnog inženjeringa

U ovom poglavlju imam drugačiji pristup metodologijama testiranja od onoga koji ću prikazati u narednim poglavljima. Socijalni inženjering je i umetnost i nauka. Potrebna je zavidna veština da se predstavite kao stručnjak za bezbednost, što u dobroj meri zavisi od vaše ličnosti i opštih znanja o organizaciji.



SAVET

Ako socijalni inženjering za vas nije prirodno, informacije iz ovog poglavlja da biste o njemu nešto naučili i pronašli najbolji način da se od njega odbranite. Ne ustručavajte se da angažujete treću stranu za ovo testiranje ako tako nešto za vas ima poslovnog smisla.



UPAMTITE

Socijalni inženjering može imati štetne posledice za poslove i reputaciju ljudi, a može da izazove i curenje informacija, naročito kod izvođenja testova pecanjem. Sve dobro isplanirajte i radite pažljivo.

Napade socijalnim inženjeringom možete izvesti na mnogo načina: od toga da uđete na neka vrata i predstavite se kao druga osoba do toga da pokrenete sveobuhvatne kampanje pecanja putem e-pošte. Sve je moguće. Iz tog razloga, a i zato što bi bilo nemoguće opisati sva specifična ponašanja u jednom poglavlju, ovde neću davati uputstva za izvođenje napada socijalnim inženjeringom. Umesto toga ću opisati posebne scenarije za socijalni inženjering koji su bili korisni meni i drugima. Možete da iskoristite neke trikove i tehnike za svoju specifičnu situaciju.

Lice koje nije zaposleno u organizaciji može uspešno da primeni određene tehnike socijalnog inženjeringa, kao što su tehnike fizičkog upada. Ukoliko ove testove sprovodite za svoju organizaciju, biće teško da se predstavljate kao spoljno lice ako vas svi poznaju. Ovaj rizik od prepoznavanja ne mora biti problem u velikim organizacijama, ali ako imate malu i spregnutu kompaniju, ljudi će sve brzo shvatiti.



UPAMTITE

Možete angažovati specijalizovanu kompaniju ili pouzdanog kolegu da izvrši napad socijalnim inžejeringom.

Zašto napadači koriste socijalni inženjering

Napadači koriste socijalni inženjering da bi provalili u sisteme i pristupali informacijama, jer je to obično najlakši način da dobiju ono što im treba. Oni više vole da im neko otvori vrata organizacije, nego da u nju fizički provaljuju i rizikuju da budu uhvaćeni na delu. Bezbednosne tehnologije, kao što su mrežne barijere i kontrole pristupa, neće zaustaviti napadače koji su čvrsto rešili da uspeju.

Mnogi socijalni inženjeri svoje napade izvode polako, da ne bi izazvali sumnju. Oni postepeno prikupljaju male količine informacija i koriste ih da bi formirali što detaljniju sliku o organizaciji koju pokušavaju da prevare. Njihovo najvažnije sredstvo za rad je – vreme. Oni nemaju ništa osim vremena i zato će se potruditi da ga sebi obezbede u dovoljnoj meri kako bi njihovi napadi bili uspešni. Ovakvi napadi mogu se izvoditi i kratkim telefonskim pozivima ili e-poštom. Korišćene metode zavise od stila i sposobnosti napadača. U svakom slučaju, vi ste u lošijoj poziciji.

Socijalni inženjeri znaju da mnoge organizacije nemaju zvanične programe za klasifikaciju podataka, sisteme za kontrolu pristupa, planove za odgovore na incidente niti programe za podizanje svesti o bezbednosti, i koriste ove slabosti.

Oni obično znaju po malo o svemu – kako unutar tako i izvan ciljnih organizacija – jer im takva znanja koriste za ono što rade. Zahvaljujući platformama

društvenih medija kao što su LinkedIn i Facebook, ali i mnogim drugim resursima na mreži o kojima sam govorio u poglavlju 5, svaka informacija potrebna ovakvim napadačima često im je i na raspolaganju. Što više informacija o organizaciji dobiju, lakše im je da se predstave kao zaposlena lica ili druge pouzdane osobe unutar organizacije. Znanje i rešenost socijalnih inženjera omogućava im prednost u odnosu na upravu i zaposlene, koji ne prepoznaju vrednost informacija za koje su ovakvi napadači zainteresovani.

Posledice

Mnoge organizacije imaju neprijatelje koji žele da im stvore probleme socijalnim inženjeringom. To mogu biti aktuelna ili bivša zaposlena lica koja žele osvetu, konkurenti koji žele prednost ili hakeri koji žele da se dokazuju.

Bez obzira na to ko predstavlja uzrok problema, svaka organizacija je izložena riziku – pogotovo ako je u većoj meri prisutna na internetu. Velike kompanije koje obuhvataju više lokacija često su ranjivije zbog svoje složenost, ali i male kompanije mogu biti mete napada. Svako – od recepcionera, preko čuvara službe obezbeđenja do IT osoblja – može biti potencijalna žrtva socijalnog inženjeringa. Osoblje službi za tehničku podršku i službi za informacije posebno je ranjivo, jer su predusretljivost i pružanje informacija sastavni deo njihovog posla.

Socijalni inženjering ima ozbiljne posledice. Budući da je u ovom slučaju cilj napadača da nekog prevari i dobije informacije za ostvarivanje lične koristi, sve je moguće. Delotvornim socijalnim inženjeringom mogu se dobiti sledeće informacije:

- Korisničke lozinke.
- Propusnice ili ključevi za objekat, čak i za sale sa računarima.
- Intelektualna svojina, kao što su specifikacije projekata, izvorni kôd i druga istraživačka i razvojna dokumentacija.
- Poverljivi finansijski izveštaji.
- Privatne i poverljive informacije o zaposlenima.
- Lični podaci za identifikaciju (PII), kao što su zdravstveni kartoni i podaci sa kreditnih kartica.
- Spisak kupaca i planovi prodaje.

Ako bilo koja od navedenih informacija procuri, može doći do finansijskih gubitaka, pada morala zaposlenih i lojalnosti klijenata, čak i problema sa zakonskom i regulatornom usklađenošću. Mogućnosti su neograničene.

Iz različitih razloga, teško je zaštititi se od napada socijalnim inženjeringom. Prvo, o njima ne postoji odgovarajuća dokumentacija. Drugo, ovakve napadače može da ograniči samo nedostatak mašte. Pored toga, teško je obezbediti oporavak i zaštitu posle napada jer postoje brojne metode, a spoljašnji zidovi mrežnih

barijera i sistema za sprečavanje upada pružaju lažni osećaj sigurnosti, čime se problem samo dodatno pogoršava.

Kad je reč o socijalnom inženjeringu, nikada se ne zna sledeća metoda napada. Najbolje što možete jeste da budete na oprezu, razumete motive ovakvih napadača i zaštitite se od najčešćih napada pomoću stalne bezbednosne budnosti u organizaciji. U nastavku ovog poglavlja govoriću o tehnikama za to.

Sticanje poverenja

Poverenje – koje je tako teško steći, a lako izgubiti – predstavlja suštinu socijalnog inženjeringa. Većina ljudi veruje drugima, sve dok zbog situacije ne bude prisiljena na suprotno. Ljudi žele da pomognu jedni drugima, pogotovo nema očiglednog razloga za nepoverenje i ako zahtev za pomoć deluje opravdano. Oni najčešće vole timski rad na poslu i ne shvataju šta se sve može desiti ako otkriju previše informacija nepouzdanom izvoru. To poverenje omogućava da socijalni inženjeri postignu svoje ciljeve. Za sticanje poverenja obično je potrebno vreme, ali veštim napadačima je dovoljno i nekoliko minuta ili sati. Kako im to uspeva?

- **Dopadljivost:** Ko može da odoli prijateljskom ponašanju? Ljubaznost prija svima. Što su ovakvi napadači pristojniji – pod uslovom da u tome ne preteruju – veće su im šanse da dobiju ono što žele. Napad socijalnim inženjeringom često počinje tako što se odnos uspostavlja na osnovu zajedničkih interesa. Napadači obično koriste informacije do kojih su došli u fazi istraživanja, kako bi utvrdili šta žrtva voli i pretvarali se da i oni vole isto. Mogu da pozovu žrtvu telefonom ili se s njom sretnu uživo i da, na osnovu informacija koje su o toj osobi otkrili, započnu razgovor o lokalnim sportskim timovima ili o tome kako je divno ponovo biti samac. Nekoliko dobro izabranih i odmerenih komentara može predstavljati početak zanimljivog novog odnosa.
- **Uverljivost:** Sposobnost uveravanja se delimično zasniva na tome koliko znanja imaju napadači koji koriste socijalni inženjering, kao i na tome koliko su dopadljivi. Oni igraju određene uloge – na primer, predstavljaju se kao novi zaposleni ili kao kolege sa posla koje žrtve još nisu srele. Mogu se čak predstavljati i kao prodavci koji posluju sa organizacijom, a često sebi daju slobodu da utiču na druge. Najčešći trik u napadima socijalnim inženjeringom jeste da se učini nešto lepo za žrtvu, kako bi ona osećala obavezu da uzvrati, ili da se učestvuje u timskom radu organizacije.

Iskorišćavanje odnosa

Kada napadači pomoću socijalniog inženjeringa dobiju informacije od svojih naivnih žrtava, oni nastavljaju da ih navode da im otkrivaju sve više. To rade u direktnom kontaktu, ili putem elektronske komunikacije koju žrtve rado koriste, odnosno tehnologije kojom se žrtva lako navodi da otkrije informacije.

Obmanjivanje rečima i delima

Lukavi socijalni inženjeri dobijaju informacije od svojih žrtava na brojne načine. Često započinju i usmeravaju konverzaciju tako da žrtve nemaju dovoljno vremena da razmisle o onome o čemu govore. Međutim, ako su napadači suviše nepažljivi ili nestrpljivi, može ih odati sledeće:

- Prenaglašeno prijateljsko ponašanje ili entuzijazam.
- Pominjanje imena istaknutih osoba u organizaciji.
- Hvalisanje sopstvenim ovlašćenjima u organizaciji.
- Ukazivanje na negativne posledice ako se njihovi zahtevi ne ispune.
- Ispoljavanje nervoze ako im se postave pitanja – grimase i vrpoljenje, a naročito nevoljni pokreti šaka i stopala (jer je teže svesno kontrolisati delove tela koja su udaljeniji od lica).
- Preterivanje u detaljima.
- Fiziološke promene, kao što su širenje zenica ili promene visine glasa.
- Užurbanost.
- Odbijanje pružanja informacija.
- Dobrovoljno davanje informacija i odgovaranje na nepostavljena pitanja.
- Poznavanje informacija kojima lice izvan organizacije ne bi trebalo da raspolaže.
- Korišćenje načina govora ili žargona zaposlenih u organizaciji, iako je poznato da osoba u njoj nije zaposlena.
- Postavljanje čudnih pitanja.
- Pogrešno napisane reči u pisanoj komunikaciji.

Dobar socijalni inženjer neće na očigledan način ispoljiti navedene reakcije, ali ovi znakovi mogu da pokažu da je reč o zlonamernom ponašanju. Naravno, ako je osoba sociopata ili psihopata, iskustvo sa njima može biti i drugačije. (*Psihologija za neupućene*, 2. izdanje autora Adama Casha [John Wiley & Sons, Inc.] dobar je izvor informacija o takvim složenostima ljudskog uma.)

Socijalni inženjeri često nekome učine uslugu, a odmah zatim tu osobu mole da pomogne njima. Ovakvi trikovi iz oblasti socijalnog inženjeringa veoma dobro funkcionišu. Ovi napadači koriste i nešto što se naziva *obratni socijalni inženjering* (engl. *reverse social engineering*). Često nude pomoć u slučaju da nastane neki problem, a kada problem nakon izvesnog vremena zaista i nastane (često tako što ga izazovu sami napadači), oni pomažu žrtvi da ga reši. Može se desiti da ispadnu i heroji, što im dodatno poboljšava poziciju – mogu odmah da traže protivuslugu od naivnog zaposlenog, što će sigurno i učiniti. Mnogi ljudi padaju u takve zamke.

Igranje uloge zaposlenog je lako. Socijalni inženjer može da nosi sličnu uniformu, lažnu identifikacionu oznaku ili se naprosto oblači kao pravi zaposleni, jer zna da će zbog toga ostali prirodno pomisliti da je i on jedan od njih. Ovakvi napadači se mogu pretvarati i kao zaposleni koji zovu sa spoljne telefonske linije, što

je posebno popularan način za iskorišćavanje osoblja tehničke podrške i pozivnih centara. Napadači znaju da ovi zaposleni rutinski obavljaju zadatke i izgovaraju rečenice koje se ponavljaju.

Obmanjivanje pomoću tehnologije

Tehnologija može mnogo da olakša posao ili ga učini zabavnijim socijalnom inženjeru. Zlonamerni zahtev za informacije često stiže sa računara ili drugih elektronskih uređaja za koje žrtve veruju da mogu da ih identifikuju. Lažiranje imena računara, e-adrese, broja faks uređaja ili mrežne adrese nije teško. U sledećem odeljku biće opisano nekoliko merama protiv ovakvih tipova napada.

Hakeri mogu da vas prevare preko tehnologije slanjem e-poruke u kojoj se od žrtava traže važne informacije. Takvom e-poštom najčešće se šalje hiperveza koja žrtve usmerava na profesionalne veb lokacije, koje izgledaju kao prave i na kojima se „ažuriraju“ informacije o nalogu, kao što su korisnički identifikator, lozinka i broj socijalnog osiguranja. Ovo može da se izvodi i na lokacijama društvenih mreža, kao što su Facebook i Twitter.

Ovaj trik se koristi i u mnogim neželjenim e-porukama i e-porukama za pecanje. Većina korisnika preplavljena je neželjenom poštom do te mere da oni često spuštaju gard i otvaraju e-poruke i priloge koje ne bi trebalo da otvaraju. Ove e-poruke često izgledaju profesionalno i uverljivo, a primaoce navode da – u zamenu za neki poklon – otkriju osetljive informacije. Ovako nešto se može primeniti kada haker, koji je već provalio u mrežu, šalje poruke ili pravi lažne iskačuće prozore na internetu. Isti trikovi se primenjuju u trenutnom razmenjivanju poruka ili razmeni poruka preko pametnih telefona.

U nekim poznatim incidentima, hakeri su svojim žrtvama slali e-poruke sa zakrpom za koju se tvrdilo da ju je napravio Microsoft ili neki drugi poznati proizvođač. Međutim, takva poruka nije ono što korisnik misli – poslao ju je haker koji želi da korisnik instalira zakrpu, a sa njom i trojanski program koji krade lozinke ili pravi tajna vrata za računare i mreže. Ova tajna vrata hakeri koriste za hakovanje sistemâ organizacije, ili da bi računare žrtava (poznate pod nazivom *zombiji*) koristili kao odskočnu dasku za napade na druge sisteme. Čak i virusi i crvi mogu da izvode napade socijalnim inženjeringom. Na primer, crv LoveBug uverava korisnike da imaju tajne obožavaoce. Kada žrtve otvore e-poruku, već je prekasno za sve – računari su im zaraženi, a od tajnih obožavalaca ni traga ni glasa.

Mnoge računarske taktike socijalnog inženjeringa mogu se sprovoditi anonimno sa interneta preko proksi servera, anonimizatora, anonimnih servera za prosleđivanje pošte i osnovnih SMTP servera koji imaju otvoren relej. Kada se ljudi odazovu na zahtev za pružanje poverljivih ličnih ili korporativnih informacija, izvorima ovih napada socijalnog inženjeringa nemoguće je ući u trag.

U OVOM POGLAVLJU

- **Biranje alatki**
- **Skeniranje mrežnih hostova**
- **Procenjivanje bezbednosti pomoću analizatora mreže**
- **Sprečavanje uskraćivanja usluga i ranjivosti infrastrukture**

Poglavlje 9
Sistemi mrežne infrastrukture

Da bi operativni sistemi i aplikacije bili bezbedni, mora biti bezbedna mreža. Zbog toga u okviru testiranja bezbednosti morate da procenite uređaje kao što su ruteri, mrežne barijere, pa čak i generički mrežni hostovi (uključujući servere i radne stanice).

Postoji na hiljade mogućih ranjivosti mreže, kao i podjednako mnogo alatki i još više tehnika za testiranje. Verovatno nemate dovoljno vremena i sredstava da biste testirali sve moguće ranjivosti svojih sistema mrežne infrastrukture i koristili svaku moguću alatku ili metodu. Zato treba da se usmerite na one testove kojima se dobija dobra opšta procena mreže. Upravo takve testove opisujem u ovom poglavlju.

Mnoge poznate ranjivosti karakteristične za mrežu možete ukloniti tako što ćete svoje mrežne hostove ažurirati najnovijim softverom i firmverom proizvođača. Budući da mnogi sistemi mrežne infrastrukture nisu javno dostupni, velika je verovatnoća da vaši mrežni hostovi neće biti napadnuti spolja. Brojne druge slabe tačke možete ukloniti tako što ćete na svojoj mreži poštovati neke dobre bezbednosne prakse, koje opisujem u ovom poglavlju. Među testovima, alatkama i tehnikama iz ovog poglavlja pronaći ćete gotovo sve što vam je potrebno za procenu bezbednosti.



SAVET

Što bolje razumete mrežne protokole, biće vam lakše da testirate ranjivosti mreže, jer mrežni protokoli predstavljaju osnovu za većinu bezbednosnih koncepata. Ako vam nije do kraja jasno kako mreža radi, preporučujem da pročitate

knjigu *TCP/IP For Dummies*, 6. izdanje, autora Candace Leiden i Marshall Wilensky (John Wiley & Sons, Inc.), koja je i meni pomogla da savladam koncepte umrežavanja. Kao dobra referenca može da posluži i lista zahteva za komentare (engl. *Request for Comments*, RFC) na stranici Official Internet Protocol Standards (`www.rfc-editor.org/standards`).

Šta su ranjivosti mrežne infrastrukture

Ranjivosti mrežne infrastrukture uzrok su većine tehničkih problema u informacionim sistemima. Ove ranjivosti niskog nivoa utiču na gotovo sve što se izvršava na mreži, zbog čega morate da testirate sistem i proveravate da li postoje, i da ih uklanjate kad god je to moguće.

Testovi bezbednosti u mrežnoj strukturi moraju se usmeriti na to da se pronađu slabosti koje i drugi vide na mreži, kako bi mogao da se proceni i obradi nivo izloženosti mreže.



UPAMTITE

Mnogi problemi su povezani sa bezbednošću mrežne infrastrukture. Neki su tehničke prirode i za njihovu ispravnu procenu potrebne su različite alatke; ostale možete procenjivati samo pažljivim posmatranjem i donošenjem logičnih zaključaka. Neke probleme je lakše uočiti sa spoljašnje strane mreže, a druge sa unutrašnje.

Kada procenjujete bezbednost mrežne strukture svoje kompanije, morate da posmatrate sledeće:

- Gde se na mreži nalaze uređaji, kao što su mrežna barijera ili sistem za sprečavanje upada (IPS), i kako su konfigurisani.
- Šta vide spoljni napadači dok pretražuju priključke i kako mogu da iskoriste ranjivosti na vašim mrežnim hostovima.
- Projektovanje mreže, kao što su veze sa internetom, mogućnosti za daljinski pristup, slojevita odbrana i razmeštaj hostova na mreži.
- Interakcija instaliranih bezbednosnih uređaja, kao što su mrežne barijere, sistemi za sprečavanje upada i antivirusni programi.
- Koji se protokoli koriste, uključujući one za koje se zna da su ranjivi – na primer, Secure Sockets Layer (SSL).
- Priključci koji se najčešće napadaju i koji su nezaštićeni.
- Konfiguracije mrežnih hostova.
- Nadzor i održavanje mreže.

Ako neko iskoristi ranjivosti sa prethodnog spiska, ili ranjivost bilo kog drugog dela bezbednosti mreže, posledice mogu biti sledeće:

- Napadač može da izvede napad uskraćivanjem usluga (DoS), što može da prekine vezu sa internetom ili obori celu mrežu.
- Zlonamerno zaposleno lice koje koristi analizator mreže može da ukrade poverljive informacije iz e-poruka i datoteka i pošalje ih preko mreže.
- Haker može da konfiguriše pristup mreži na tajna vrata.
- Privremeni saradnik može da napadne posebne hostove iskorišćavanjem lokalnih ranjivosti na mreži.



SAVET

Pre procene bezbednosti mrežne infrastrukture, ne zaboravite da uradite sledeće:

- Testirajte sisteme spolja i iznutra (to jest, u internim mrežnim segmentima i demilitarizovanim zonama [DMZ], kao i između njih).
- Pribavite dozvolu od partnerskih mreža da proverite postojanje ranjivosti na njihovim sistemima (kao što su otvoreni priključci, nedostatak mrežnih barijera ili pogrešno konfigurisani ruter), koje mogu da utiču na bezbednost *vaše* mreže.

Biranje alatki

Kao i kod svih procena bezbednosti, za testiranje bezbednosti mreže potrebne su prave alatke: programi za skeniranje priključaka, analizatori protokola i alatke za procenu ranjivosti. Postoje odlične komercijalne, javne i besplatne alatke, a u narednim odeljcima ću opisati neke koje su mi omiljene. Imajte na umu da ćete morati da koristite više alatki, jer nijedna od njih ne radi sve što vam je potrebno.



SAVET

Ako tražite bezbednosne alatke koje se lako koriste i imaju sve neophodne funkcije, uglavnom ćete dobijati ono što ste platili, naročito na Windows platformi. Veliki broj stručnjaka za bezbednost veliča kvalitete raznih besplatnih alatki, pogotovo onih koje se izvršavaju u Linuxu i drugim operativnim sistemima srodnim Unixu. Mnoge od tih alatki su veoma korisne ako imate dovoljno vremena, strpljenja i volje da se bavite njihovim prednostima i nedostacima. Ako se uporede rezultati besplatnih i komercijalnih alatki za ovu namenu, mislim da će se izvesna prednost pokazati na strani korišćenja komercijalnih alatki.

Programi za skeniranje i analizatori

Ovi programi obavljaju gotovo sva skeniranja priključaka i testiranja mreže koja su vam potrebna:

- **Cain & Abel** (`www.oxid.it/cain.html`) za analizu mreže i trovanje ARP protokola.
- **Essential NetTools** (`https://www.tamos.com/products/nettools`) sa velikim brojem funkcija za skeniranje mreže.

- **NetScanTools Pro** (`https://www.netscantools.com`) sa velikim brojem funkcija za procenu bezbednosti mreže, uključujući skeniranje signalom ping, skeniranje priključaka i testiranje SMTP releja.
- **Getif** (`www.wtcs.org/snmp4tpc/getif.htm`), stara dobra alatka za pretraživanje SNMP protokola.
- **Nmap** (`https://nmap.org`) ili **NMapWin** (`https://sourceforge.net/projects/nmapwin`), čeoni grafički korisnički interfejs (GUI) sa programom Nmap u pozadini, za testiranje hostova i priključaka, kao i za identifikovanje (engl. *fingerprint*) operativnih sistema (OS).
- **Savvius Omnipeek** (`https://www.savvius.com`) za analizu mreže.
- **TamoSoft CommView** (`https://www.tamos.com/products/commview`) za analizu mreže.
- **Wireshark** (`http://wireshark.org`) za analizu mreže.

Procenjivanje ranjivosti

Ove alatke za procenu ranjivosti omogućavaju da, između ostalog, testirate da li mrežni hostovi sadrže različite poznate ranjivosti, kao i potencijalne probleme konfiguracije koji mogu dovesti do zloupotrebe:

- **GFI LanGuard** (`https://www.gfi.com/products-and-solutions/network-security-solutions/gfi-languard3`) za skeniranje priključaka i testiranje ranjivosti.
- **Nexpose** (`https://www.rapid7.com/products/nexpose`), sveobuhvatna alatka za detaljno testiranje ranjivosti.

Skeniranje i provociranje mreže

Testiranje bezbednosti mrežne infrastrukture, koje se opisuje u sledećim odeljcima, obuhvata sledeće korake hakovanja:

1. **Prikupljanje informacija i mapiranje mreže.**
2. **Skeniranje sistema da bi se proverilo koji je dostupan.**
3. **Utvrđivanje šta se izvršava na sistemima koje ste otkrili.**
4. **Pokušaj proboja u sisteme koje ste otkrili (ako se za to opredelite).**



SAVET

Svaki upravljački program mrežne kartice i svaka implementacija TCP/IP protokola u većini operativnih sistema – uključujući Windows, Linux, pa čak i mrežne barijere i rutere – imaju osobenosti koje dovode do različitog ponašanja tokom skeniranja i provociranja sistema. Zbog tih razlika u ponašanju može doći

do različitih odgovora sistema, od lažnih uzbuna do DoS uslova. U svojim vodičima za administratore ili na veb lokacijama proizvođača potražite detalje o svim poznatim problemima i zakrpama za njihovo rešavanje. Ako ste zakrpili sve svoje sisteme, ne bi trebalo da imate probleme, ali imajte na umu da je sve moguće.

Priključci za skeniranje

Program za skeniranje priključaka (engl. *port scanner*) pokazuje vam šta je šta na vašoj mreži, i to tako što je pretražuje da bi uočio šta je aktivno. Ovim programima se obezbeđuje osnovni prikaz rasporeda mreže, što vam može pomoći da identifikujete neovlašćene hostove ili aplikacije, kao i greške u konfiguraciji mrežnih hostova koje mogu da dovedu do ozbiljnih bezbednosnih ranjivosti.

Širom perspektivom programa za skeniranje priključaka često se otkrivaju bezbednosni problemi koji bi na neki drugi način ostali neprimećeni. Ovi programi se lako koriste i mogu da testiraju mrežne hostove bez obzira na operativne sisteme i aplikacije koji se izvršavaju. Testovi se izvršavaju relativno brzo i bez potrebe za obradom pojedinačnih mrežnih hostova (što može biti više nego zamorno).

Pri proceni opšte bezbednosti mreže važno je tumačenje rezultata koje dobijate iz skeniranja priključaka. Na primer, možete da dobijete lažne uzbune na otvorenim priključcima pa ćete morate da idete korak dalje. Skeniranja protokola za korisničke datagrame (engl. *User Datagram Protocol*, UDP), kao i sam protokol, manje su pouzdani od skeniranja protokola za upravljanje prenosom (engl. *Transmission Control Protocol*, TCP) i često dovode do lažnih uzbuna, jer mnoge aplikacije ne znaju kako da odgovore na nasumične dolazne UDP zahteve.

Program za skeniranje sa velikim brojem funkcija, kao što je Nexpose, može da identifikuje priključke i prikaže šta se izvršava u jednom koraku.



UPOZORENJE

Skeniranja priključaka mogu da oduzmu dosta vremena, zavisno od toga koliko hostova imate, koliko priključaka skenirate, koje alatke koristite, kakve su mogućnosti obrade sistema koji testirate i kolika je brzina mrežnih veza.



UPAMTITE

Po pravilu treba da skenirate više važnih hostova. Nemojte ništa izostaviti, jer sistemi koje zanemarite mogu kasnije da vam se osvete. Pored toga, izvršavajte iste testove različitim uslužnim programima, kako biste videli da li dobijate različite rezultate. Neće sve alatke pronaći iste otvorene priključke i ranjivosti – što nije dobro, ali je realna činjenica testiranja ranjivosti i neprobojnosti.

Ako testirate sistem pomoću više alatki i ne dobijete iste rezultate, možete dodatno da istražite problem. Ako nešto ne izgleda ispravno (na primer, pronašli ste čudan skup otvorenih priključaka), onda najverovatnije i nije. Pokrenite test ponovo, a ako ste sumnjičavi, upotrebite drugu alatku zbog drugačije perspektive.



SAVET

Ako je to moguće, treba da testirate svih 65.534 TCP priključaka na svakom mrežnom hostu koji pronađe vaš program za skeniranje. Ako pronađete sumnjive priključke, potražite u dokumentaciji da li je aplikacija poznata i odobrena. Ne bi bilo loše da pretražite svih 65.534 UDP priključaka. Imajte na umu da ovaj proces može znatno da produži vreme skeniranja.

Da bi sve bilo brže i jednostavnije, možete da pretražite najčešće hakovane priključke koji se navode u tabeli 9-1. Ne zaboravite da mnoge od tih priključaka koriste i zlonamerni programi..

TABELA 9-1 **Najčešće hakovani priključci**

Broj priključka	Usluga	Protokol(i)
7	Echo	TCP, UDP
19	Chargen	TCP, UDP
20	FTP data (File Transfer Protocol)	TCP
21	FTP control	TCP
22	SSH	TCP
23	Telnet	TCP
25	SMTP (Simple Mail Transfer Protocol)	TCP
37	Time	TCP, UDP
53	DNS (Domain Name System)	UDP
69	TFTP (Trivial File Transfer Protocol)	UDP
79	Finger	TCP, UDP
80	HTTP (Hypertext Transfer Protocol)	UDP
110	POP3 (Post Office Protocol version 3)	TCP
111	SUN.RPC (remote procedure calls)	TCP, UDP
135	RPC/DCE (endpoint mapper) for Microsoft networks	TCP, UDP
137, 138, 139, 445	NetBIOS over TCP/IP	TCP, UDP
161	SNMP (Simple Network Management Protocol)	TCP, UDP
443	HTTPS (HTTP over TLS)	TCP
512, 513, 514	Berkeley r-services and r-commands (such as `rsh`, `rexec`, and `rlogin`)	TCP
1433	Microsoft SQL Server (ms-sql-s)	TCP, UDP
1434	Microsoft SQL Monitor (ms-sql-m)	TCP, UDP
1723	Microsoft PPTP VPN	TCP
3389	Windows Terminal Server	TCP
8080	HTTP proxy	TCP

U OVOM POGLAVLJU

- Napad na sisteme e-pošte
- Napad na trenutno razmenjivanje poruka
- Napad na aplikacije protokola za prenos glasa (VOIP)

Poglavlje **14**

Sistemi za komunikaciju i razmenu poruka

Sistemi i protokoli za komunikaciju, poput e-pošte i protokola za prenos glasa preko Interneta, često su nosioci slabih tačaka koje se lako previde. Zašto? Prema sopstvenom iskustvu, komunikacioni softver – kako kod servera, tako i kod klijenta – ranjiv je jer administratori mreže često veruju da su mrežna barijera i softver za zaštitu od zlonamernih programa sve što im je potrebno da se izbegnu problemi ili jednostavno zaborave da zaštite ove sisteme.

U ovom poglavlju, pokazaću vam kako da testirate uobičajene probleme sa e-poštom i VoIP (engl. *voice over internet protocol, VoIP*). Takođe ću istaći i prikaz ključnih mera zaštite koje će vam pomoći da sprečite hakovanje ovih sistema.

Uvod u ranjivosti sistema za razmenu poruka

Gotovo sve aplikacije za prenos poruka predstavljaju metu za hakere na vašoj mreži. Imajući u vidu sve širu upotrebu e-pošte, kao i to koliko poslovanje zavisi od iste, sve vrlo lako može postati meta. Isto važi i za VoIP. Potpuno je zastrašujuće šta ljudi sa zlom namerom mogu da učine sa ovim alatkama.

Kod sistema za razmenu poruka, jedna od osnovnih slabosti je ta što većina protokola za podršku nije osmišljena uzimajući zaštitu u obzir – posebno oni koji su se pojavili pre nekoliko decenija kada sigurnost nije bila ni blizu značajna kao u današnje vreme. Zanimljivo je da su čak i moderni sistemi za razmenu poruka – ili barem primena protokola – *još uvek* podložni ozbiljnim sigurnosnim rizicima. Sem toga, pogodnost i upotrebljivost često prevagnu nad potrebom za sigurnošću.

Mnogi napadi na sisteme za razmenu poruka su samo blage neprijatnosti; ostali mogu da nanesu ozbiljnu štetu podacima i ugledu vaše organizacije. Zlonamerni napadi na sisteme za razmenu poruka su sledeći:

- Prosleđivanje zlonamernih programa (softvera).
- Rušenje servera.
- Zadobijanje daljinske kontrole nad radnim stanicama.
- Hvatanje informacija koje putuju mrežom.
- Pažljivo proučavanje e-pošte sačuvane na serveru i u radnim stanicama.
- Prikupljanje informacija o razmeni poruka preko dnevničkih datoteka ili analizatora mreže, a to napadaču može da pruži informacije o razgovorima između ljudi i organizacija (što se često naziva analizom saobraćaja ili analizom društvenih mreža).
- Preuzimanje i preslušavanje telefonskih razgovora.
- Prikupljanje informacija o unutrašnjoj konfiguraciji mreže, kao što su ime računara i *IP* adrese.

Ovakvi napadi mogu dovesti do problema kao što je neovlašćeno – a moguće i protivzakonito – otkrivanje poverljivih informacija, kao i gubitak istih.

Prepoznavanje i borba protiv napada na e-poštu

Napadi koje predstavljam u ovom odeljku koriste najčešće ranjivosti e-pošte za koje znam. Dobra vest je da većinu možete ukloniti ili ublažiti do te mere da ne predstavljaju rizik za informacije. Neki od ovih napada zahtevaju poznavanje osnovnih metodologija hakovanja: prikupljanje javnih informacija, skeniranje i popisivanje sistema, pronalaženje i korišćenje ranjivosti. Ostali napadi se mogu izvesti slanjem e-pošte ili preuzimanjem mrežnog saobraćaja.

Bombardovanje e-poštom

Bombardovanje elektronskim pismima (engl. *email bombs*) napada tako što stvara uslove za uskraćivanje usluge (engl. *denial of service*, DoS) na vašem softveru za e-poštu, čak i na mreži i Internet konekciji jer zauzimaju veliki deo propusnog opsega, a ponekad i skladišnog prostora. Bombe u vidu e-pošte mogu da dovedu

do pada servera i omoguće neovlašćeni administratorski pristup – da, čak i uz današnje naizgled beskrajne kapacitete memorije.

Priložena datoteka

Napadač može izvesti napad pretrpavanjem priloženim datotekama tako što će poslati na stotine ili hiljade pisama sa izuzetno velikim prilozima za jednog ili više primaoca na vašoj mreži.

NAPADI PRILOŽENIM DATOTEKAMA E-POŠTE

Napadi priloženim datotekama imaju dva cilja:

- **Server za poštu može biti meta sa ciljem** potpunog prekida rada na sledeće načine:
  - *Prepunjenost memorije:* Više velikih poruka mogu brzo da popune kapacitet servera pošte. Ako se poruke ne obrišu automatski putem servera ili ručno od strane pojedinačnih korisničkih naloga, server neće biti u mogućnosti da primi nove poruke.

    Ovakav napad može da dovede do ozbiljnog *DoS* problema po vaš sistem pošte, pri čemu će doći ili do pada sistema ili ćete dobiti zahtev za prekidanje veze sa internetom da biste očistili nagomilanu poštu (engl. *junk*). 100MB priložene datoteke koja se pošalje deset puta za stotinu korisnika može da zauzme 100GB skladišnog prostora, a može i više!

    UPOZORENJE
  - *Blokiranje propusnog opsega:* Napadač može da vam nagomilanom poštom potpuno zaustavi ili uspori prijem pošte. Čak i ako vaš sistem automatski prepoznaje i odbacuje očigledne napade prilozima, lažne poruke troše resurse i usporavaju prenos validnih poruka.
- **Napad na pojedinačnu adresu e-pošte** može imati ozbiljne posledice ako adresa pripada bitnom korisniku ili grupi.

MERE PROTIV NAPADA PRILOŽENIM DATOTEKAMA

Sledeće mere zaštite mogu pomoći u sprečavanju napada pretrpavanjem priloženim datotekama:

- **Ograničavanje veličine pošte ili priloženih datoteka.** Potražite ovu opciju u podešavanjima konfiguracije servera pošte (ima ih u *Microsoft Exchange-u*), u delu za filtriranje poruka ili u podešavanju klijenta.
- **Ograničavanje prostora svakog korisnika na serveru ili u oblaku** (engl. *cloud*)**.** Ova mera zaštite sprečava upisivanje velikih priloženih datoteka na disk. Ograničite veličinu poruka za dolazne, pa čak i odlazne poruke ako imate za cilj da sprečite korisnika da izvrši ovaj napad unutar vaše mreže. Smatram da je nekoliko gigabajta dobro ograničenje, ali ono zavisi od veličine vaše mreže, raspoloživosti skladištenja, kulture poslovanja i tako dalje. Razmislite pažljivo o ograničenju pre nego što ga zadate.



SAVET

Razmotrite korišćenje *SFTP*, *FTPS* ili *HTTPS* umesto pošte za prenos velikih datoteka. Dostupne su mnoge usluge za prenos datoteka u oblaku, kao na primer *Dropbox for Business*, *OneDrive for Business* i *Sharefile*. Takođe možete podstaći korisnike da koriste zajedničke ili javne foldere. Na taj način možete sačuvati kopiju datoteke na serveru, a primalac može da preuzme datoteku na svojoj radnoj stanici.



UPOZORENJE

Suprotno uvreženom verovanju i upotrebi, sistem pošte *ne treba* da bude spremište informacija, ali se pošta upravo u to razvila. Server pošte koji se koristi za ovu svrhu može dovesti do bespotrebnih nezakonitih i regulatornih rizika i pretvoriti se u veliku noćnu moru ako vaša organizacija primi zahtev za uvid u vaš sistem pošte od nadležnih organa. Važan deo vašeg sistema bezbednosti je raspodela i upravljanje podacima. Ali ne bavite se time sami. Aganžujte advokata, menadžera za ljudske resurse i šefa informativne službe. To vam omogućava da pravi ljudi budu prisutni i da vaš posao ne upadne u nevolju zbog posedovanja previše – ili premalo – elektronskih podataka u slučaju da dođe do tužbe ili istražnog postupka.

Veze

Haker može istovremeno poslati ogroman broj pisama na vaš sistem pošte. Zlonamerni program prisutan na vašoj mreži može isto to da uradi iz unutrašnjosti mreže ako mreža ima otvoren jednostavan protokol za prenos pošte (*Simple Mail Transfer Protocol*, *SMTP* protokol), što često i jeste slučaj. Ovi napadi na veze mogu dovesti do toga da server odustane od obrade svih dolaznih ili odlaznih zahteva za protokol za kontrolu prenosa (*Transmission Control Protocol*, *TCP* protokol). U ovom slučaju može doći do zaključavanja ili pada servera, a to omogućava napadaču da dobije administratorski ili korenski (engl. *root*) pristup sistemu ili da pristupi kao administrator.

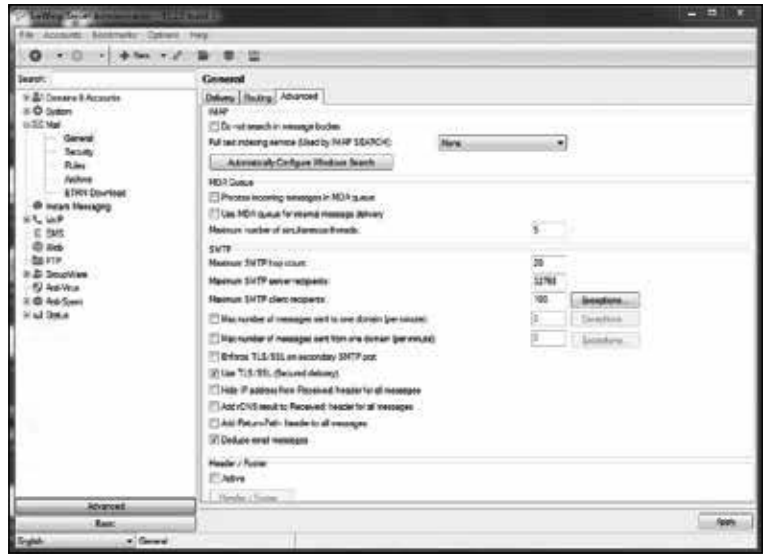
NAPADI PUTEM PREPLAVLJIVANJA E-POŠTOM

Napad pri kojem se koristi preplavljivanje e-poštom često se izvodi kao napad neželjenom poštom (engl. *spam*) i ostalim vrstama *DoS* napada.

MERE PROTIV NAPADA NA VEZE

Treba sprečiti napade na poštu što je moguće više po obodu mreže, najbolje u oblaku. Što više mrežnog saobraćaja ili zlonamernog ponašanja držite podalje od servera pošte i klijenata, utoliko bolje.

Mnogi serveri e-pošte imaju opciju ograničavanja broja resursa koji se koriste za dolazne veze, kao što je prikazano na Slici 14-1 kod podešavanja maksimalnog broja istovremenih programskih niti za *IceWarp* server pošte. Ovo podešavanje ima različite nazive za različite servere pošte i mrežne barijere, te je dobro proveriti šta piše u dokumentaciji. Potpuno zaustavljanje neograničenog broja dolaznih zahteva može biti nemoguć zadatak, ali možete ublažiti uticaj napada. Ovo podešavanje ograničava vreme serverskog procesa što pomaže za vreme *DoS* napada.



SLIKA 14-1: Ograničavanje broja resursa koji obrađuju dolazne poruke.

Čak i u velikim kompanijama ili prilikom korišćenja servisa za poštu u oblaku, kao što su *G Suite* ili *Office 365*, gotovo da nema razloga da na hiljade dolaznih pisama bude neophodno u kratkom vremenskom periodu.



UPOZORENJE

Serveri e-pošte mogu da se programiraju da dostavljaju pisma serveru za automatizovane funkcije, na primer *napravite ovu porudžbinu vezanu za e-trgovinu kada primite poruku sa ovog naloga*. Ako DoS zaštita nije deo sistema, napadač može srušiti i server i aplikaciju koja prima te poruke i tada postoji mogućnost da dođe do zakonskih prekršaja kod e-trgovine. Ovaj tip napada lakše se sprovodi na veb lokacijama e-trgovine koje u obrascima ne koriste znakovni test *CAPTCHA* (*Completely Automated Public Turing test to tell Computers and Humans Apart*), test koji otkriva da li je posetilac čovek ili program. To može biti problem kada vršite skeniranje ranjivosti na vebu preko veb obrazaca koji su vezani za adrese e-pošte u pozadini. U takvoj situaciji nije neuobičajeno da se dobije na hiljade, ako ne i milion, pisama. Isplati se biti pripremljen i obavestiti sve koji su uključeni u to da rizik postoji. U Poglavlju 15 ću objasniti zaštitu veb aplikacija..

Automatizovanje kontrole sigurnosti e-pošte

Možete primeniti sledeće mere kao dodatnu zaštitu sistema e-pošte:

- **Zadrška:** Zadrška (engl. *tarpitting*) prepoznaje dolazne poruke namenjene nepoznatim korisnicima. Ako vaš server pošte podržava zadršku, može vam pomoći u sprečavanju napada na server u vidu neželjene pošte ili kod *DoS* napada. Ako se prekorači unapred definisan prag – recimo, više od 100 poruka u minuti – funkcija zadrške uspešno zaustavlja saobraćaj sa *IP* adrese pošiljaoca na određeni period.

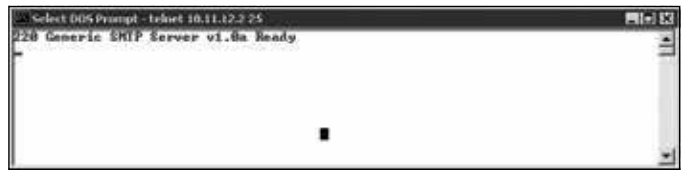
- **Mrežna barijera e-pošte:** Mrežne barijere pošte i aplikacije za filtriranje na osnovu sadržaja kupljene od firmi kao što su *Symantec* i *Barracuda Networks* dosta pomažu u sprečavanju različitih napada na poštu. Ove alatke štite gotovo sve aspekte sistema pošte.
- **Zaštita na obodu:** Iako nisu karakteristični za e-poštu, mnoge mrežne barijere i sistemi za sprečavanje upada mogu da prepoznaju različite napade na poštu i zaustave napadača u realnom vremenu, što dobro dođe za vreme napada.
- **CAPTCHA:** Korišćenje *CAPTCHE* kod veb obrazaca e-pošte pomaže pri umanjivanju uticaja automatizovanih napada i smanjuje šanse za prenatrpavanje poštom i DoS, čak i kada obavljate naizgled bezazleno skeniranje ranjivosti mreže. Ove prednosti dobro dođu prilikom testiranja veb lokacija i aplikacija, o čemu govorim u Poglavlju 15.

Zaglavlja

Prilikom hakovanja servera e-pošte, prioritet hakera je da otvori zaglavlje (engl. *banner*) da bi video da li može da otkrije koji softver koristi server pošte. Ovakva provera je jedna od najkritičnijih da bi se saznalo koje informacije javnost ima o vašim *SMTP*, *POP3* i *IMAP* serverima.

Prikupljanje informacija

Na slici 14-2 prikazano je zaglavlje na serveru pošte kada se ostvari osnovna *Telnet* veza na priključku 25 (*SMTP*). Da biste ovo dobili na komandnoj liniji unesite **telnet** ip ***ili_ime_vašeg_servea* 25**. Ova komanda otvara *Telnet* sesiju na *TCP* priključku 25.



SLIKA 14-2: *SMTP* zaglavlje koje prikazuje informacije o verziji servera.

Vrsta softvera e-pošte i verzija servera su često prilično očigledni i hakerima pružaju ideje o mogućim napadima, pogotovo ako pretražuju bazu podataka da bi pronašli ranjivosti koje su već poznate u toj verziji softvera. Slika 14-3 prikazuje isti server pošte sa *SMTP* zaglavljem koje je promenjeno iz unapred zadatog (u redu, i prethodno je takođe) da bi se prikrile informacije verzije servera pošte.



SAVET

Možete prikupiti informacije o *POP3* i *IMAP* uslugama pošte koristeći *Telnet* za priključak 143 110 (*POP3*) ili priključak 143 (*IMAP*).

U OVOM POGLAVLJU

- Koje ranjivosti treba prvo obraditi
- Krpljenje sistema
- Sigurnost sagledana u novom svetlu

Poglavlje 18
Zatvaranje sigurnosnih rupa

Pošto ste završili testiranje, želite da krenete putem ka većoj sigurnosti. Ali, pronašli ste neke sigurnosne ranjivosti – stvari koje treba obraditi (nadam se, ipak, ne mnogo ozbiljnih!). Zapušavanje ovih sigurnosnih rupa pre nego što ih neko iskoristi će zahtevati nešto truda. Potrebno je da smislite plan igre i odlučite koje sigurnosne ranjivosti treba prvo obraditi. Nekoliko zakrpa može biti prikladno, verovatno i povećanje sigurnosti sistema. Možda će biti potrebno da kupite neke nove sigurnosne tehnologije i da ponovo procenite dizajn vaše mreže kao i sigurnosnu infrastrukturu. U ovom poglavlju ću se dotaći nekih od ovih kritičnih oblasti.

Pretvorite izveštaje u akciju

Može vam se učiniti da je prva ranjivost koju treba obraditi očigledna, ali ne mora da bude tako. Prilikom pregledanja ranjivosti koje ste pronašli, razmotrite sledeće promenljive:

- Koliko kritičan je dati ranjivi sistem
- Koje osetljive informacije ili poslovni procesi su ugroženi
- Da li ranjivost može biti uklonjena

- Koliko je lako ukloniti datu ranjivost
- Da li treba da isključite sistem da biste rešili problem
- Koliko vremena, novca i truda bi trebalo uložiti u kupovinu novog hardvera ili softvera ili u prepravku postojećih radnih procesa da bi se zapušile rupe

U poglavlju 17 obradio sam osnovne probleme prilikom donošenja odluke koliko je važan ili hitan određeni sigurnosni problem. Na sigurnost bi takođe trebalo da gledate iz perspektive upravljanja vremenom i da rešite probleme koji su ujedno i važni (od velikog uticaja) i hitni (imaju veliku verovatnoću). Verovatno ne želite da pokušate da rešite ranjivosti koje su *samo* od velikog uticaja ili koje *samo* imaju veliku verovatnoću. Možete imati neke ranjivosti od velikog uticaja koje verovatno nikada neće biti iskorišćene. Slično tome, verovatno ćete imati neke ranjivosti sa velikom verovatnoćom da budu iskorišćene a koje ne bi napravile veliku promenu u vašem poslu. Ovakav pristup vam pomaže da se izdvojite od načina testiranja koje izvodi većina i koji će vam obezbediti buduća angažovanja.

Usmerite se na zadatke koji se najviše isplate na početku – oni koji su od velikog uticaja *i* sa velikom verovatnoćom. Ovi zadaci će verovatno biti u manjini. Pošto zapušite najkritičnije sigurnosne rupe, možete se usredsrediti na manje važne, manje hitne zadatke kada vreme i novac to dozvole. Pošto zapušite takve kritične rupe kao što je SQL injektovanje u veb aplikacijama i zakrpe koje nedostaju na važnim serverima, možda ćete želeti da ponovo napravite sigurnosne kopije i zaštitite lozinkom (ako šifrovanje nije dovoljno jako) da biste se zaštitili od radoznalih očiju u slučaju da vaše sigurnosne kopije dospeju u pogrešne ruke.

Krpljenjem do savršenstva

Da li ikada osećate da je sve što radite krpljenje sistema da biste sredili sigurnosne ranjivosti? Ako je vaš odgovor potvrdan, blago vama; vi makar obavljate posao! Ako osećate pritisak da zakrpite sisteme na pravi način ali nemate vremena, makar je taj posao nešto što znate da vas čeka. Mnogi profesionalci u IT-u i njihovi menadžeri ne misle o krpljenju sistema sve dok se ne dogodi proboj u sistem. (Pogledajte istraživanje u Verizon Data Breach Investigations Report [`https://www.verizonenterprise.com/verizon-insights-lab/dbir/`], na primer.). Rad sa zakrpama je veliki problem u mnogim firmama. Ako čitate ovu knjigu vi ste očigledno zabrinuti za sigurnost i nadam se, daleko ste od neadekvatnog rada sa zakrpama.



UPAMTITE

Štagod da uradite, koju god alatku da izaberete, i koje god procedure funkcionišu najbolje u vašem okruženju, neka vaši sistemi budu zakrpljeni! Ovo pravilo važi za operativne sisteme; veb servere; baze podataka; mobilne aplikacije; i čak i za upravljački softver (engl. *firmware*) na mrežnoj barijeri: usmerivačima (engl. *rooters*) i skretnicama (engl. *switches*). Posebno važne su softverske zakrpe prodavaca kao što su Oracle (Java) i Adobe (Reader, Flash itd.) Ove zakrpe se češće previde nego većina, a ipak one donose značajan rizik koji ostaje nerešen.

Krpljenje se može izbeći ali je neophodno. Jedini način da se eliminiše potreba za krpljenjem jeste da se na prvom mestu razvije siguran softver, ali to se neće

skoro desiti, ako se ikada i desi. Softver je isuviše kompleksan da bi mogao da bude savršen. Veliki broj sigurnosnih incidenata se može sprečiti valjanim krpljenjem, tako da prosto nemate nikakav razlog da izbegavate rad sa zakrpama.

Upravljanje zakrpama

Ako ne možete da se izborite sa poplavom zakrpa za sisteme, ne očajavajte; još uvek možete da savladate problem. Ovo su moji osnovni principi za primenu zakrpa da bi sistem ostao siguran:

- Budite sigurni da svi ljudi i odeljenja uključeni u primenu zakrpa u sistemima vaše organizacije misle slično i prate slične procedure.
- Obezbedite zvanične procedure za ove procese od kritičke važnosti:
  - Obezbedite upozorenja o zakrpama od prodavaca, uključujući i zakrpe trećih strana
  - Procenite koje zakrpe utiču na sistem
  - Odlučite kada da primenite zakrpe
- Uvedite pravila i procedure za testiranje zakrpa *pre* nego što ih primenite na server za javni pristup. Testiranje zakrpa pošto ih primenite nije toliko važno u radnim stanicama, ali serveri su potpuno druga priča. Mnoge zakrpe imaju nedokumentovane karakteristike i prateće posledice, koje sam iskusio. Netestirana zakrpa je poziv za prekid rada sistema.

Automatizacija

Sledeći odeljci opisuju raznovrsne alatke za rad sa zakrpama.

Komercijalne alatke

Preporučujem otpornu aplikaciju za automatizaciju zakrpa, pogotovo ako su sledeći faktori uključeni:

- Velika mreža.
- Mreža sa više operativnih sistema (Windows, Linux, Mac OS itd.)
- Puno softverskih aplikacija od treće strane, kao što su Adobe i Java.
- Više od nekoliko desetina kompjutera.



SAVET

Obratite pažnju na ova rešenja za automatizaciju rada sa zakrpama

- :Ecora Patch Manager (`www.ecora.com/ecora/products/patchmanager.asp`)
- GFI LanGuard (`www.gfi.com/products-and-solutions/network-security- solutions/gfi-languard`)
- PDQ Deploy (`https://www.pdq.com/pdq-deploy`)

Besplatne alatke

Upotrebite jednu od ovih besplatnih alatki koje će vam pomoći u automatskom krpljenju:

- Windows Server Update Services (`https://technet.microsoft.com/en-us/library/cc539281.aspx` or System Center Configuration Manager (`https://www.microsoft.com/en-us/cloud-platform/system-center-configuration-manager`)).
- Windows Update, koji je ugrađen u Microsoft Windows operativni sistem
- Microsoft Baseline Security Analyzer (`https://www.microsoft.com/en-us/download/details.aspx?id=7558`).
- Ugrađene alatke za rad sa zakrpama za sisteme zasnovane na Linuxu (kao što su Yellowdog Updater, Modified i YaST Online Update).

Jačanje sistema

Pored primene zakrpa na vašim sistemima, budite sigurni da su vam sistemi obezbeđeni (zaključani) od ranjvosti koje zakrpe ne mogu da poprave. Otkrio sam da mnogi ljudi stanu kad obave proces sa zakrpama, misleći da su njihovi sistemi obezbeđeni, ali to nije tako. Tokom godina, viđao sam administratore mreže kako ignorišu preporuke takvih organizacija kao što su Nacionalni institut za standarde i Tehnološko-kompjuterski centar za sigurnosne resurse (`http://csrc.nist.gov/publications/PubsSPs.html)i` Centar za sigurnost na internetu (`www.cisecurity.org`), ostavljajući mnoge sigurnosne rupe širom otvorene. Ipak, verujem da ni sistemi za osnaživanje protiv zlonamernih napada nisu pouzdani. Zato što je svaki sistem drugačiji i potrebe svake organizacije su drugačije, nema rešenja koje odgovara svim situacijama, tako da morate da pronađete ravnotežu a da se previše ne oslanjate ni na jedno rešenje.



UPAMTITE

Pošto primenite zakrpe, dobra je ideja da ponovo proverite sisteme na ranjivosti da potvrdite da su se zakrpe primile.

Ova knjiga predstavlja kontramere za jačanje koje možete da primenite na mreži, kompjuterima, pa čak i fizičkim sistemima i ljudima. Pronašao sam da ove kontramere najbolje funkcionišu.

Primena makar osnovnih sigurnosnih postupaka je od kritične važnosti. Bilo da instalirate mrežni bedem ili zahtevate od korisnika da imaju jake lozinke putem Windows active direktorijuma domen GPO, morate obratiti pažnju na osnove ako želite da imate bilo kakav delić sigurnosti. Osim zakrpa, ako pratite kontramere koje sam zabeležio, dodajete druge dobro poznate sigurnosne postupke za mrežne sisteme (rutere, servere, radne stanice itd.) koji su slobodno dostupni na internetu i izvodite tekuće sigurnosne testove, možete biti uvereni da dajete sve od sebe da održite sigurnost organizacije.

PLAĆANJE GREŠAKA

Jednom sam bio uključen u projekat koji je bio odgovor na incident gde je bilo uključeno više od 10 000 Windows servera i radnih stanica zaraženih ciljanim zlonamernim programom. Još napredniji zlonamerni program je uzeo maha. Kompanija je zarazu pronašla brzo i mislili su da je IT tim sve očistio. Neko vreme je prošlo, a posle godinu i više u kompaniji su shvatili da nisu sve očistili. Taj zlonamerni program se osvetnički vratio, do te mere da je čitava njihova mreža bila pod nadzorom stranih, kriminalnih hakera, sponzorisanih od strane države.

Pošto je više od desetine ljudi provelo sate da dođu do korena problema, bilo je odlučeno da odeljenje IT-a nije uradilo ono što je trebalo da uradi što se tiče krpljenja i jačanja sistema. Takođe je došlo do ozbiljnog prekida u komunikaciji između odeljenja IT-a i drugih odeljenja, uključujući bezbednost, pomoć klijentima i radnih odeljenja. Ovaj slučaj gde je bilo „isuviše malo, isuviše kasno" uvukao je veliku kompaniju u veliku nevolju. Lekcija koja se može naučiti iz ovoga je da neadekvatno osigurani sistemi mogu da stvore ogromanu muku u poslu..

Procena sigurnosne infrastrukture

Pregled sigurnosne infrastrukture na sledeće načine može da obezbedi snagu vašim sistemima:

- **Pogledajte kako je sveukupna mreža dizajnirana.** Razmotrite organizacione stavke da li su sva pravila uspostavljena, da li se održavaju ili čak da li se ozbiljno prihvataju.. Odredite da li članovi uprave prihvataju informacionu sigurnost i usaglašavanje sa njom ili prosto odgurnu date mere kao nepotrebni trošak ili prepreku u poslovanju.
- **Mapirajte mrežu koristeći informacije koje dobijete iz sigurnosnih testova u ovoj knjizi.** Ažuriranje postojeće dokumentacije je od velike važnosti. Iscrtajte IP adrese, servise koji rade i sve drugo što možete da otkrijete. Nacrtajte dijagram mreže. Dizajn mreže i sigurnosne probleme je mnogo lakše proceniti kada radite sa njima vizuelno. Iako više volim da koristim tehnički program za crtanje kao što je Microsoft Visio ili Cheops (`http://cheops-ng.sourceforge.net`) da napravim mrežne dijagrame, takva alatka nije neophodna. Možete nacrtati svoju mapu na tabli.

  Ažurirajte dijagrame kada se mreža promeni ili jedanput godišnje i sl.



UPAMTITE

- **Razmišljajte o pristupu kako da smanjite ranjivosti i da povećate sveukupnu sigurnost organizacije .** Da li ste usmerili sav vaš napor na sporedne stvari a ne na složeni sigurnosni pristup? Mislite o tome kako su većina prodavnica i banaka zaštićene. Bezbednosne kamere su usmerene na kase, kompjutere blagajnika i okolinu - ne samo na parking i ulaze. Posmatrajte sigurnost iz perspektive odbrane koja zadire u dubinu. Primenite više slojeva bezbednosti tako da napadač mora da pređe preko drugih prepreka da bi izvršio uspešan napad.
- **Razmišljajte o sigurnosnim i poslovnim procesima na višem nivou vaše kompanije.** Zabeležite koji sigurnostni postupci i pravila postoje i da li se primenjuju. Odredite koji rizici postoje na način da sigurnost bude nadgledana i sprovedena. Nijedna organizacija nije imuna na praznine u ovoj oblasti. Posmatrajte ukupnu sigurnosnu kulturu u vašoj organizaciji da biste videli kako izgleda iz perspektive spoljašnjeg posmatrača. Posmatrajte je i kroz oko unutrašnjeg posmatrača. Otkrijte šta vaši klijenti ili poslovni partneri misle o tome kako se vaša organizacija odnosi prema osetljivim informacijama. Mogu reći, sa sto posto sigurnosti, da nešto – i to nekoliko stvari - može biti poboljšano vašem sistemu.



SAVET

Pružanje podrške sigurnosti nije samo pitanje zakrpa i drugih tehničkih sigurnosnih kontrola. Ponekad IT i program upravljanja sigurnošću treba poboljšati. Ponekad je potrebno da započnete nešto novo. Ponekad je prosto potrebno da prestanete da radite određene stvari. Tokom godina sam naširoko pisao o pogrešnom i pravilnom korišćenju IT-a i sigurnosnih programa i veći deo tog sadržaja možete naći na mojoj veb stranici `https://www.principlelogic.com/management.html`.

Sagledavanje vaše sigurnosti sa višeg nivoa i iz netehničke perspektive daje vam novi uvid u sigurnosne rupe i ukupne poslovne rizike. Taj proces zahteva vreme i trud, ali pošto ste utvrdili osnovnu liniju sigurnosti, upravljanje novim pretnjama i ranjivostima postaje mnogo lakše.