Incidenti neovlašćenog pristupa
Vrsta: Seminarski | Broj strana: 15 | Nivo: Fakultet za poslovnu informatiku

Univerzitet Singidunum Fakultet za poslovnu informatiku
Seminarski rad
Tema:Incidenti neovlašćenog pristupa
Mr.Gojko Grubor
Dalibor Radovanović II-2/2005
Definicija incidenata
vršenje daljiskog ugrožavanja root-a nekog servera E-pošte oštećenje/brisanje Web-servera nagaĎanje i provaljivanje lozinki kopiranje baze podataka koja sadrži brojeve kreditnih kartica pregledanje osetljivih podataka, uključujući i evidencije platnih spiskova i medicinske informacije, bez ovlašćenja izvršavanje sniffer programa na radnoj stanici, da bi se uhvatila korisnička imena i lozinke korišćenje greške u pogledu dozvole na nekom anonimnom FTP serveru za distribuciju piratskog sotvera i muzičkih datoteka biranje brojeva u neosiguranom modemu i dobijanje pristupa internoj mreži glumljenje nekog rukovodioca, pozivanje službe za pomoć, resetovanje lozinke E-pošte tog rukovodioca i saznavanje nove lozinke korišćenje, bez dozvole, prijavljene radne stanice na kojoj nema operatera (ili automatizovane rande stanice).• • • • • • • • • •Neovlašćen pristup se javlja kada korisnik dobije pristup resursima koji nisu namenjeni tom korisniku. Neovlašćeni pristup se tipično dobija korišćenjem operativnog sistema ili usled ranjivosti aplikacije, pribavljanjem korisničkih imena i lozinki, ili društvenog inžinjeringa. Napadači mogu da dobiju ograničeni pristup kroz jednu ranjivu tačku i da upotrebe taj pristup da bi napadali druge ranjive tačke, da bi na kraju dobili pristup na višim nivoima. Primeri incidenata neovlašćenog pristupa uključuju sledeće:
Da bi rešavali incidente neovlašćenog pristupa, potrebno je obaviti sledeće postupke:
•
Konfigurisati IDS softver u mreži i glavnom računaru da bi smo identifikovali i dobili upozorenje o pokušajima da se dobije neovlašćeni pristup. Svaki tip softvera za otkrivanje uljeza može da otkrije napade koje drugi tipovi nisu u stanju da otkriju. Potrebno je da koristiti centralizovane servere dnevnika rada (log server), tako da se bitne informacije od glavnih računara širom organizacije memorišu na jednoj jedinoj osiguranoj lokaciji. Potrebno je da ustanoviti procedure po kojima treba postupati kada svi korisnici neke aplikacije, sistema, sigurnosnog domena ili organizacije treba da promene svoje lozinke zato što su lozinke ugrožene. Te procedure treba da se pridržavaju politike u pogledu lozinki date organizacije. Sa administratorima sistema potrebno je razgovarati o incidentima neovlašćenog pristupa, kako bi oni shvatili svoje uloge u procesu rešavanja incidenata.
•
•
•
2
Sprečavanje incidenata
Ako se primenjuju opšte smernice o sprečavanju incidenata, broj incidenata neovlašćenog pristupa bi trebalo uspešno da se smanji. Preporučena praksa za smanjenje incidenata jeste korišćenje jake slojevite strategije odbrane, sa nekoliko bezbednosnih slojeva izmeĎu

neovlašćenih korisnika i resursa koje oni pokušavaju da eksploatišu. Postupci za sprečavanje incidenata neovlašćenog pristupa za odreĎene kategorije su: 1. Bezbednost mreže - Potrebno je da konfigurišemo perimetar mreže, kako bismo odbili sav dolazni saobraćaj koji nije izričito dozvoljen. - Potrebno je valjano osigurati sve metode daljinskog pristupa, uključujući i modeme i VPN-ove. Jedan neosiguran modem može da omogući neovlašćeni pristup internim sistemima i mrežama. Kada osiguravamo udaljeni pristup, potrebno je da pažljivo razmotrimo kredibilnost klijenata; ako su oni izvan kontrole organizacije, onda im treba dati što je moguće manje pristupa resursima, a njihove postupke treba pomno pratiti. - Postaviti sve javno dostupne usluge na osigurane demilitarizovane zone (DMZ) segmenata mreže. Perimetar mreže onda može da se konfiguriše tako da spoljašnji glavni računari mogu da uspostave veze samo sa glavnim računarima na DMZ-i, a ne u internim segmentima mreže. - Koristiti privatne IP adrese za sve glavne računare na internim mrežama. Ovo će jako ograničiti mogućnost napadača da uspostave direktne veze sa internim glavnim računarima.
...