UNIVERZITET SINGIDUNUM
FAKULTET ZA INFORMATIKU I MENADŽMENT

INTERNET BAZE PODATAKA – EVIDENCIJA ČLANOVA SAVEZA GEODETA SRBIJE

- Diplomski rad -

Mentor:
_____

Student:
_____

Br. indeksa:
_____

Beograd, 2009.

Beograd, 2007.

FAKULTET ZA POSLOVNU INFORMATIKU

UNIVERZITET SINGIDUNUM
FAKULTET ZA POSLOVNU INFORMATIKU
Beograd, Danijelova 32

Broj: _____/2005

Kandidat: _____

Broj indeksa: _____

Smer: Projektovanje i programiranje

Tema: INTERNET BAZE PODATAKA – EVIDENCIJA ČLANOVA SAVEZA GEODETA SRBIJE

Zadatak: Realizovati i opisati web aplikaciju za evidenciju članova SGS. Omogućiti prikaz, izmene i brisanje podataka iz baze. Sve strane, osim one za prikaz, zaštiti autorizacionim mehanizmom, uz beleženje podataka o tome ko je i kada vršio izmene. Izmene omogućiti članovima, a brisanje i izmene administratorima. Za rešenje zadatka primeniti programski jezik PHP, korišćenjem sistema za upravljanje relacionim bazama podataka MySQL za skladištenje podataka.

MENTOR

_____
Prof,dr Petrovic Petar

Datum odobrenja teme:
20.09.2007.
Beograd

DEKAN

_____
Prof. dr Marko Markovic

Sistemi za detekciju i prevenciju napada na računarske mreže

Abstrakt :

Uz standardne tehnike zaštite računarkih mreža često se koriste i sistemi čija je osnovna namena prepoznavanje ne legalnih aktivnosti i napada na mreži. Svrha ovog rada je da prikaže kako se i na koje načine može sve ugroziti rad u računarskim mrežama i da prikaže sve napade koji se mogu izvršiti. Detaljno će biti opisane arhitekture sistema za detekciju i sistema za prevenciju napada, kao i njihove tehnike za zaštitu mreža.

Ključne reći: računarska mreža, napad, detekcija upada, prevencija napada

Systems for detection and prevention from attacks on computer networks

Abstract :

In addition to standard techniques used for protecting the computer networks, systems which main goal is detection of attacks and illegal actions are also commonly used. Goal of this thesis is to elaborate how and on witch ways can work in computer networks be copromised and to show all attacs that can be executed. In detail will be described architectures of Intrusion Detection System and Instrusion Prevention System, as well as theirs techniques for protection of computer networks.

Key words: computer network, attack, intrusion detection, prevention system

Sadržaj :

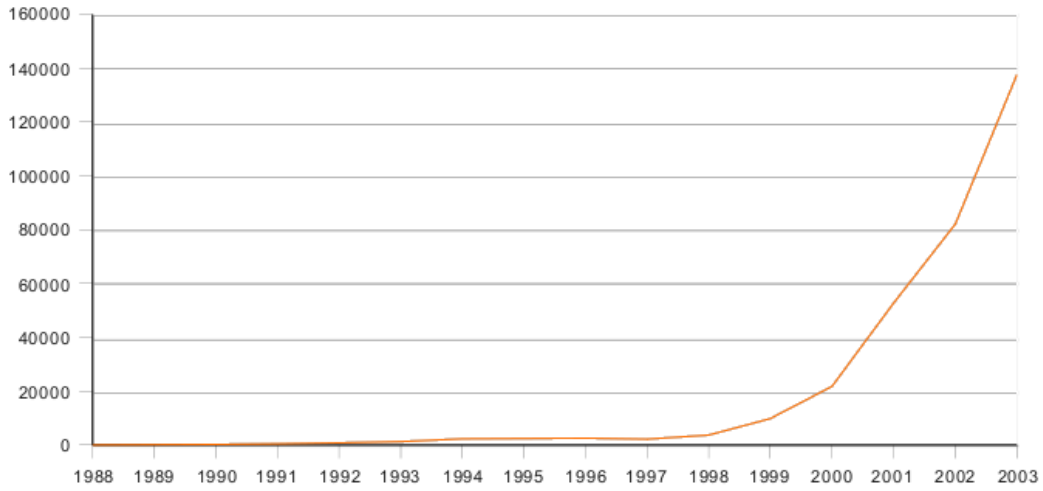
Slike :

1.Uvod

Pre svega nekoliko godina dovoljnu zaštitu za većinu korisnika personalnih računara pružao je kvalitetan antivirusni program. Takvi programi prepoznavali su i onemogućavali pokretanje zlonamernih programa i time činili računare koliko-toliko sigurnima. Međutim, već neko vreme antivirusni program sam po sebi ne predstavlja dovoljnu zaštitu računarskim sistemima koji su stalno ili privremeno spojeni na Internet. Iako ti programi i dalje dobro rade svoj posao, oni nas neće zaštiti od neželjene elektronske pošte (engl. spam), špijunskih programa (engl. spyware) ili napada sa Interneta.

Računarska sigurnost je, zahvaljujući sve bržem rastu računarske industrije, postala ne zaobilazna tema u projektovanju bilo kojeg informacionog sistema. Novi propusti i metode napada na razne sisteme otkrivaju se gotovo svakodnevno. Prema podacima preuzetih od CERT-a (eng. Computer Emergency Response Team) broj prijavljenih sigurnosnih incidenata u razdoblju od petnaest godina porastao je gotovo 1000 puta, kao što prikazuje slika 1.1, a praktično se udvostručuje svake sledeće godine. Razlozi za ovakav drastičan porast broja sigurnosnih incidenata su mnogobrojni. Poslednjih godina pristup Internetu je sve jednostavniji i jeftiniji, a broj korisnika se neprestano povećava. Tržištem trenutno dominira vrlo mali broj operativnih sistema, pa pronalaženjem propusta u bilo kojem od njih napadač automatski dobija veliki broj potencijalnih žrtava

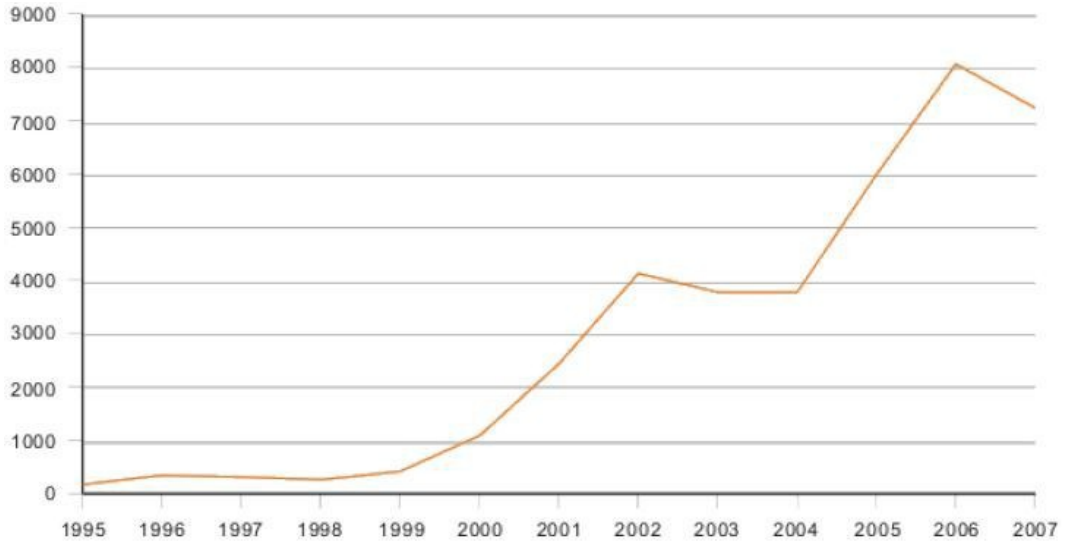
na kojima može iskoristiti pronađeni propust. Brzi razvoj tehnologije često izbacuje na tržište ne kompletna i ne proverena rešenja koja na kraju rezultuju velikim brojem sigurnosnih propusta. Često navođeni primer je slučaj WEP protokola (eng. Wired Equivalent Privacy) u bežičnim mrežama. Dve godine nakon objave pronađeni su ozbiljni propusti u protokolu, a u samo nekoliko narednih meseci pojavio se niz alata za iskorišćavanje njegovih nedostataka. Uza sve navedeno, popularizacijom Interneta informacije o novim propustima se trivijalno i vrlo brzo šire među velikim brojem ljudi, a pronalaženje alata za napade na razne informacione sisteme svodi se na jednostavno upisivanje ključnih reči u pretraživač , pa preuzimanje gotovih alata sa jedne od mnogobrojnih krakerskih stranica. Zbog toga znanje i veštine napadača postaju sve manje važni faktori, pa sve veći deo populacije napadača čine takozvani script kiddies, napadači koji koriste već gotove alate bez detaljnog znanja o alatu koji koriste ili o propustu koji iskorišćavaju.



Slika 1.1: Prijavljeni sigurnosni incidenti [CERT]

Struktura napada se tokom vremena takođe drastično promenila. Prema podacima iz CERT-a, pre desetak godina većinu prijavljenih incidenata su sačinjavale prijave vezane za štetno delovanje virusa, pogađanje korisničkih lozinki raznim metodama pretraživanja (eng. brute force password guessing) i iskorišćavanje dobro poznatih propusta u sistemima. Porastom kompleksnosti informacionih sistema uveliko se povećao i broj sigurnosnih propusta, što je jasno vidljivo i na slici 1.2. Danas većinu prijava CERT-u sačinjavaju razni tipovi napada sa mreže u rasponu od jednostavnog prikrivenog skeniranja pristupnih vrata (eng. stealth port scanning) pa sve do vrlo ozbiljnih napada poput raspodeljenih napada uskraćivanjem usluge (eng. distributed denial of service). U vreme kada je gotovo svaki računar priključen na Internet i zbog svih prethodno navedenih razloga, mrežna sigurnost i razvoj sigurnosnih rešenja za obranu od napada sa mreže čine jedno od najbrže razvijajućih područja računarske industrije. Posebnu ulogu u

tome ima i razvoj alata za obranu ranjivih mrežnih usluga, među kojima važnu ulogu imaju i sistemi za detekciju napada sa mreže.



Slika 1.2: Pronađeni sigurnosni propusti

5. Zaključak

Sistemi za detekciju napada na mreže su tehnologija koja se još uvek brzo razvija i poboljšava. Sa vremenom su postali ne zamenjivi deo celokupnog sigurnosnog sistema i toliko ih je uobičajeno naći koliko je uobičajeno da se koristi i sigurnosni zid. Međutim, brzim razvojem tehnologije NIDS-ovi se takođe moraju prilagođavati sve većim zahtevima tržišta i moraju odolevati sve lukavijim tehnikama napada. U samo dvadesetak godina koliko postoje evoluirali su od najprimitivnijih metoda nadziranja do današnjih nevidljivih distribuiranih sistema za rad u stvarnom vremenu koji mogu nadzirati i gigabitne mreže sa izrazito velikom količinom prometa.

Literatura :

1. Northcutt, Stephen; Novak, Judy: Network Intrusion Detection, Third Edition, New Riders Publishing, 2002.

2. J. McGibney, Intrusion Detection Systems & Honeypots, Waterford Institute of Technology, Ireland, Prezentacija sa konferencije INET/IGC, Barcelona, 2004

3. B. Laing, Implementing a Network Based Intrusion Detection System, Sovereign House,Reading, 2000.

4. Carter, Earl; Hogue, Jonathan: Intrusion Prevention Fundamentals, Cisco Press, 2006

5. Wikipedia
   Intrusion Detection System,
   http://en.wikipedia.org/wiki/Intrusion_detection_system
   http://en.wikipedia.org/wiki/Buffer_overflow
   http://en.wikipedia.org/wiki/Denial-of-service
   Intrusion Prevention System,
   http://en.wikipedia.org/wiki/Intrusion-prevention_system

6. Sans Institute, Intrusion Detection FAQ,
   http://www.sans.org/ resources /idfaq

7. Carnegie Melon University, CERT/CC Statistics 1998 – 2006,
   http://www.cert.org/ stats