Aplikasi Model Sistem Keamanan Jaringan Berbasis *De-Militarised Zone*

ADDY SUYATNO

Program Studi Ilmu Komputer, FMIPA Universitas Mulawarman
Jl. Barong Tongkok Kampus Gunung Kelua Sempaja Samarinda 75119

Abstrak

De-Militarized Zone (DMZ) is a "sacrificial lamb" for hackers applied to protect internal system relating to hack attack (hack attack). DMZ works for all service base of network requiring access to network "external world" to part of network the other. That way, all " open port" is relating to external world will stay at network, so that if a hacker did attack and does crack at server using system DMZ, the hacker will only can access its(the host is only, not at internal network. In General DMZ is built based on three fruit of concept, that is: NAT (Network Address Translation), PAT (Port Addressable Translation), and Access List. NAT functions to show again coming packages "real address" to internal address. For example: if wes own "real address" 203.8.90.100, we can form a direct NAT automatically at data coming to 192.168.100.1 (an internal network address). Then PAT functions menunjukan data to coming at particular port, or range a port and protocol (TCP/UDP or other) and address IP to a particular port or range a port to an internal address of IP. While access list functions to control in precise what is coming and going out from network in a question. For example: we can refuse or enables all ICMP is coming to all address IP except for an undesirable ICMP.

***Keywords**: NAT, real address, PAT, Access List, Port, Protocol, DMZ, ICMP*

1. Pendahuluan

Pada umumnya berbagai perusahaan menggunakan Internet untuk hosting web server, komunikasi e-mail dan memberikan akses web kepada karyawannya. Pemisahan jaringan Internet dan IntraNet umumnya dilakukan dengan menggunakan teknik/software Firewall dan Proxy server. Melihat kondisi penggunaannya, kelemahan sistem umumnya dapat di tembus misalnya dengan menembus mailserver external yang digunakan untuk memudahkan akses ke mail keluar dari perusahaan. Selain itu, dengan menggunakan agressive-SNMP scanner dan program yang memaksa SNMP *community string* dapat mengubah sebuah *router* menjadi *bridge* (jembatan) yang kemudian dapat digunakan untuk batu loncatan untuk masuk ke dalam jaringan internal perusahaan (IntraNet).

Hacker biasanya memiliki keahlian dapat melihat kelemahan perangkat lunak pada komputer dalam suatu jaringan, kemudian mempublikasikan secara terbuka di Internet atau media lain untuk memancing agar sistem diperbaiki menjadi lebih baik. Namun teknologi informasi tidak saja membawa pengaruh baik, informasi tersebut menjadi sebuah tindak kejahatan –biasanya disebut cracker. Dunia *hacker* dan *cracker* tidak berbeda dengan dunia seni, pada makalah ini akan dibahas tentang seni keamanan jaringan internet menggunakan De-Militarised Zone.

2. Teori

2.1. Konsep Dasar De-Militarised Zone (DMZ)

DMZ merupakan mekanisme untuk melindungi sistem internal dari serangan hacker atau pihak-pihak lain yang ingin memasuki sistem tanpa mempunyai hak akses. Sehingga karena DMZ dapat diakses oleh pengguna yang tidak mempunyai hak, maka DMZ tidak mengandung rule. Secara esensial, DMZ memindahkan semua layanan suatu jaringan ke jaringan lain yang berbeda. DMZ terdiri dari semua port terbuka, yang dapat dilihat oleh pihak luar. Sehingga jika hacker menyerang dan melakukan *cracking* pada server yang mempunyai DMZ, maka hacker tersebut hanya dapat mengakses host yang berada pada DMZ, tidak pada jaringan internal.

Misalnya jika seorang pengguna bekerja di atas server FTP pada jaringan terbuka untuk melakukan akses publik seperti akses internet, maka hacker dapat melakukan cracking pada server FTP dengan memanfaatkan layanan *Network Interconnection System (NIS)*, dan *Network File System(NFS)*. Sehingga hacker tersebut dapat mengakses seluruh sumber daya jaringan, atau jika tidak, akses jaringan dapat dilakukan dengan sedikit upaya, yaitu dengan menangkap paket yang beredar di jaringan, atau dengan metoda yang lain. Namun dengan menggunakan lokasi server FTP yang berbeda, maka hacker hanya dapat mengakses DMZ tanpa mempengaruhi sumber daya jaringan lain.

Dengan melakukan pemotongan jalur komunikasi pada jaringan internal, trojan tidak dapat memasuki jaringan.

2.2. Konsep NAT, PAT, dan Daftar Akses

Network Address Translation (NAT) berfungsi untuk mengarahkan alamat riil, seperti alamat internet, ke bentuk alamat internal. Misalnya alamat riil 203.8.90.100 dapat diarahkan ke bentuk alamat jaringan internal 192.168.0.1 secara otomatis dengan menggunakan NAT. Namun jika semua informasi secara otomatis ditranslasi ke bentuk alamat internal, maka tidak ada lagi kendali terhadap informasi yang masuk. Oleh karena itu maka muncullah PAT.

Port Address Translation (PAT) berfungsi untuk mengarahkan data yang masuk melalui port, sekumpulan port dan protokol, serta alamat IP pada port atau sekumpulan post. Sehingga dapat dilakukan kendali ketat pada setiap data yang mengalir dari dan ke jaringan.

Daftar Akses melakukan layanan pada pengguna agar dapat mengendalikan data jaringan. Daftar Akses dapat menolak atau menerima akses dengan berdasar pada alamat IP, alamat IP tujuan, dan tipe protokol.

3. Analisis dan Perancangan Kerja DMZ

DMZ bekerja dengan mekanisme yang terstruktur melalui langkah-langkah strategis sebagai berikut :

Langkah 1: Sebaran IP Baru dan memindahkan Layanan Web

- Organisasi XYZ juga didukung dengan server RedHat Linux dan dilengkapi dengan kartu ISDN. Semua routing pada server ini di non-aktifkan dan hanya berfungsi sebagai gateway aplikasi yang bekerja dengan melakukan monitoring pada port-port tertentu, dan mengaktifkan program lain yang dapat melayani arus informasi pada jaringan internal.
- Langkah pengamanan pertama yang dilakukan adalah dengan membenahi alamat IP sehingga dapat digunakan sebagai alamat global. Jika terdapat serangan hacker, maka jaringan internal tidak akan terganggu.
- Lakukan setup DNS pada Windows NT4.0, karena layanan DNS pada NT relatif mudah dikonfigurasi, cukup aman untuk DNS internal, dan mendukung registrasi dinamis. Versi terbaru dari BIND mendukung registrasi dinamis untuk upgrade ke Windows 2000, sehingga sistem membutuhkan layanan DNS Windows 2000 untuk ekstensi direktori aktif.
- Kemudian dilakukan modifikasi pada semua alamat IP pada Server dan Print Server, mengubah konfigurasi aplikasi gateway pada Linux, dan membentuk sebaran DHCP baru. Langkah berikutnya adalah memindahkan halaman web dari jaringan lokal ke ISP karena halaman page tidak harus diubah setiap saat.

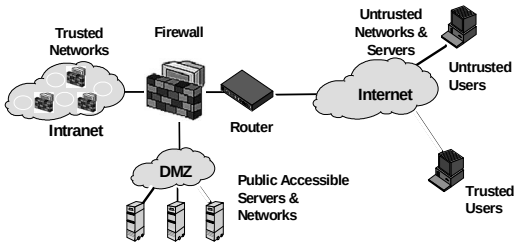
Langkah 2 – Menentukan Perangkat Keras Pendukung

- Perangkat keras yang digunakan meliputi koneksi ADSL, implementasi Firewall, dan implementasi DMZ. Pada perangkat keras yang digunakan menggunakan sistem operasi Windows atau Linux. Windows mempunyai kelemahan:
- Meskipun Windows NT/2000 cukup sulit di hack, namun mudah diserang Denial Of Service (DOS) atau service yang crash. Banyak sekali pihak yang melakukan hack pada lingkungan Windows.
- Sedangkan kelemahan Linux adalah karena Linux merupakan sistem operasi yang dibangun oleh hacker sehingga source code Linux mudah didapat. Oleh karena itu dengan menggunakan Linux, maka tingkat keamanan semakin rendah.
- Perangkat keras yang dibutuhkan terdiri dari perangkat komputer beserta paket keamanannya, koneksi ADSL dan firewall, serta switch layer Data Link.

Langkah 3 – Implementasi Jalur ADSL dan Firewall PIX

- Setelah perangkat keras tersedia, maka berikutnya adalah melakukan pemetaan alamat perangkat keras, misalnya:
  - ADSL – 209.15.20.34
  - Ethernet0 pada ADSL – 192.1.10.5/30 (255.255.255.252)
  - Ethernet0 pada firewall PIX.
- Berikutnya dibangun translasi NAT untuk melakukan panggilan forward ke 192.168.10.6. Biarkan router menjadi data route, dan biarkan Firewall menentukan konfigurasi yang diperlukan untuk pengelolaan resiko.

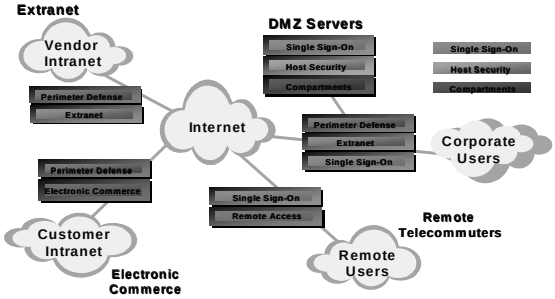
Firewall merupakan sistem yang menyediakan konektifitas yang aman antar jaringan baik internal maupun eksternal dalam beberapa lapis keamanan dengan fungsi yang berbeda. Pengertian firewall yang lain adalah sistem yang mengimplementasikan aturan keamanan untuk komunikasi antar jaringan komputer. Bagan keamanan digambarkan sebagai berikut:



Gambar 1. Bagan Keamanan Firewall

Langkah 4 – Instalasi dan Konfigurasi pada DMZ

Sampai pada langkah ini maka bagian eksternal jaringan telah terbentuk, dan dapat dikenali sebagai bagian *semi-trusted* (DMZ). Namun dengan catatan bahwa pada jaringan, koneksi ISDN telah dipisahkan dan dapat berjalan seperti yang diharapkan. Namun biarkan koneksi ADSL offline, hingga pengujian kinerja sistem telah dilakukan. Langkah ini dilakukan untuk meyakinkan bahwa sistem tidak terganggu selama proses instalasi dan konfigurasi. Sebelumnya arsitektur keamanan yang akan dibangun digambarkan sebagai berikut:



Gambar 2. Arsitektur Sistem Keamanan Jaringan Internet

Langkah yang perlu dilakukan adalah sebagai berikut:

- Pertama adalah menentukan subnet yang akan digunakan pada DMZ. 192.100.100.0/24 merupakan tebaran IP yang digunakan pada jaringan. Selain itu dilakukan juga pengujian pada tebaran IP. Tebaran IP harus mempunyai ruang lingkup yang sama.
- Ethernet1 pada PIX mempunyai alamat IP 192.100.100.6/24, untuk tetap berhubungan dengan antarmuka Ethernet. Switch juga ditentukan alamat IP-nya. Hal ini dilakukan untuk mencegah hacker memasuki dan melakukan sniffing pada sistem. Langkah ini merupakan proses inspeksi dan antispoofing pada firewall PIX.
- Setelah langkah diatas dilakukan, maka semua mesin telah terhubung dan online berdasar pada alamat IP dan layanan jaringan komputer yang dibutuhkan. Mesin tersebut dapat dikonfigurasi dengan berbagai spesifikasi keamanan.
- Firewall PIX juga dapat menerima permintaan VPN yang masuk, untuk memberi kemungkinan bagi pengguna jarak jauh untuk melakukan otentikasi pada sistem. Pembatasan akses pada server VPN menggunakan daftar akses yang menolak semua permintaan koneksi untuk mengakses VPN sampai diverifikasi sebagai salah satu kantor cabang atau dari kantor utama. Akses SSH pada mesin DMZ dapat dikontrol dari komputer lokal dengan menggunakan kantor. Sehingga dimungkinkan mengakses mesin melalui SSH, namun port scan dari internet tidak pernah melihat port SSH terbuka.
- Langkah berikutnya adalah melakukan redirect layanan DNS dari koneksi ADSL. Translasi alamat port dilakukan pada firewall PIX untuk meneruskan pengiriman setiap permintaan UDP/TCP port 53. Kemudian aktifkan filter paket pada firewall PIX untuk mengizinkan input koneksi TCP port 53 dari NamaServer secondary(umumnya milik ISP), permintaan UDP port 53 yang masuk, dan permintaan UDP port 53 yang keluar dari server DNS. Konfigurasi ini harus diselesaikan untuk semua layanan pada semua server dengan layanan yang munkin berbeda-beda per server.
- Setelah melalui semua langkah diatas, maka koneksi ADSL dapat dikonfigurasi dengan tingkat keamanan yang dibutuhkan oleh semua daftar akses dan PAT. Aturan dasarnya adalah jika tidak membutuhkan akses layanan tertentu, maka akses akan ditolak. Hacker hanya dapat menyerang layanan yang disediakan oleh host DMZ, oleh karena itu upaya yang harus dilakukan adalah meminimalisasi jumlah layanan yang dapat diakses lewat internet, serta melengkapi layanan tersebut dengan keamanan yang tinggi. Sedangkan pada dasarnya semua layanan dapat diakses lewat internet. Lakukan pengujian pada setiap layanan, memindai semua port dan yakinkan anda mempunyai akses yang terbatas, sebanyak kemungkinan layanan spesifik.
- Langkah terakhir adalah melakukan konfigurasi antarmuka ethernet pada firewall PIX ke dalam jaringan internal. Pastikan semua lalu lintas diblok melalui daftar akses dari jaringan internal, sehingga tidak ada orang maupun apapun yang dapat akses keluar.

Langkah 5 – Konfigurasi Chaining / PassThrough

Perancangan DMZ membutuhkan proxy untuk semua layanan yang mungkin, sehingga server exchange tidak mengirim dan menerima mail secara langsung, namun dengan proxy semua yang berkaitan dengan mail akan melalui server sendmail. Hal ini berarti bahwa tidak ada pengguna internet yang dapat langsung mengakses melalui layanan internal apapun. Selain itu, kita dapat mengeksekusi multi nilai pada perangkat yang berbeda untuk meningkatkan proteksi. Misalnya dengan mengaktifkan pemindai virus sendmail pada mail server DMZ dan Norton AntiVirus untuk exchange dan servernya.

Daftar akses mempunyai kompleksitas yang bervariasi tergantung pada layanan yang diaktifkan. Misalnya permintaan untuk menyediakan informasi web untuk kepentingan umum, membutuhkan persetujuan dari Proxy pada DMZ hanya dari proxy internal, dan Proxy DMZ dan menginisilisasi semua koneksi ke luar. Proxy DMX tidak perlu menerima request persetujuan dari sumber yang lain, sehingga hacker seharusnya tidak dapat mengakses server.

Langkah 6 – Alarm dan Tripwire

Terdapat banyak metode untuk mencegah hacker, namun masih terlalu banyak wilayah komputerisasi yang dapat dijelajahi. Sehingga, adu kekuatan antara administrator dan hacker tidak akan reda dalam waktu singkat, bahkan diperkirakan akan terus berjalan seiring dengan perkembangan teknologi. Terdapat tiga metode utama yang dapat digunakan, yaitu SysLog Logging, pendeteksi serangan Tripwire dan Cron Jobs

Langkah 7 – Aktifkan Sistem

Setelah melalui langkah-langkah diatas, maka sistem dapat diaktifkan, dengan tetap selalu mencatat perubahan-perubahan yang terjadi. Hal lain yang diperlukan sistem adalah ubah nama record, konfigurasi ulang layanan internal dan siap untuk digunakan.

4. Implementasi

Protokol TCP/IP merupakan protokol yang banyak digunakan pada lingkungan internal jaringan, bahkan merupakan protokol standard yang digunakan pada komunikasi internet. Berkaitan dengan pembangunan sistem keamanan, maka selain melakukan pencegahan dengan DMZ, diperlukan pula pengetahuan teknik pemrograman jaringan (*Network Programming*), sehingga dengan semikian diharapkan administrator lebih mengenal bagaimana cara kerja hacker dan kelompok penyerang yang lain.

Network Programming menggunakan bahasa C++ untuk beberapa metoda akses jaringan komunikasi data, yaitu dengan cara mengetahui nama sebuah komputer dan alamat IP-nya, melakukan pendeteksian dan penutupan koneksi pada TCP/IP, mengetahui nama komputer lain dan alamat IP masing-masing, melakukan pendeteksian port pada TCP/IP, melakukan operasi ping pada TCP/IP dan terakhir melakukan pendeteksian alamat MAC.

4.1. Mengetahui Nama Sebuah Komputer dan Alamat IP-nya

Kode program dan langkah-langkah berikut dapat digunakan untuk mengetahui nama komputer dan alamat IP pada komputer yang mengeksekusi program tersebut.

```
#include <winsock2.h>
{  WORD wVersionRequested;
   WSADATA wsaData;
   char name[255];
   CString ip;
   PHOSTENT hostinfo;

wVersionRequested = MAKEWORD( 2, 0 );
if ( WSAStartup( wVersionRequested,
&wsaData ) == 0 )
{ if( gethostname ( name, sizeof(name))
== 0)
  { if((hostinfo = gethostbyname(name))
!= NULL)
    { ip=inet_ntoa(*(struct in_addr
*)*hostinfo->h_addr_list);}}
WSACleanup( ); }}
```

4.2. Pendeteksian, dan Penutupan Koneksi Pada TCP/IP

Langkah-langkah pada fungsi tersebut adalah:

(i) Cek apakah socket dapat dibaca
(ii) Jika Ya, deteksi data yang masuk
(iii) Cek nilai data dan error untuk menentukan apakah koneksi jaringan masih terjaga.

Berikut adalah kode fungsi yang telah dimodifikasi:

```
BOOL CClientSocket::HasConnectionDropped(
void )
{
 BOOL bConnDropped = FALSE;
 INT iRet = 0;
 BOOL bOK = TRUE;

 struct timeval timeout = { 0, 0 };
 fd_set readSocketSet;
 FD_ZERO( &readSocketSet );
 FD_SET( m_hSocket, &readSocketSet );

 iRet = ::select( 0, &readSocketSet, NULL,
NULL, &timeout );
 bOK = ( iRet > 0 );
```

```
 if( bOK )
 {bOK = FD_ISSET( m_hSocket,
&readSocketSet );}

 if( bOK )
 { CHAR szBuffer[1] = "";
   iRet = ::recv( m_hSocket, szBuffer, 1,
MSG_PEEK );
   bOK = ( iRet > 0 );
   if( !bOK )
   { INT iError = ::WSAGetLastError();
     bConnDropped = ( ( iError ==
WSAENETRESET ) ||
     ( iError == WSAECONNABORTED ) ||(
iError == WSAECONNRESET ) ||
      ( iError == WSAEINVAL ) ||( iRet ==
0 ) );
   }
 }

 return(bConnDropped );
}
```

4.3. Mengetahui Informasi Mengenai Workstation

Program berikut digunakan untuk mengetahui informasi mengenai workstation baik yang aktif maupun yang tidak, tanpa mengubah konfigurasi server. Fasilitas ini cocok digunakan untuk aplikasi monitoring jaringan secara real time.

```
#include <what_you_need.h>
#include <lmcons.h>
#include <lmwksta.h>
#include <lmserver.h>
#include <lmerr.h>*/

//Network API job - obtain network info
about selected machine.
BOOL
_GetWkstaInformation100()
{ LPBYTE lpBuf;
  LPCSTR lpcstrWkstaName =
(LPCSTR)m_strWkstaName;
  int iwLength = 2 *
(MAX_COMPUTERNAME_LENGTH + 1);
  WCHAR lpwWkstaName[2 *
(MAX_COMPUTERNAME_LENGTH + 1)];
  lpwWkstaName[0] = '\0';
  MultiByteToWideChar(CP_ACP,0,lpcstrWksta
  Name,-1,lpwWkstaName, iwLength);

typedef NET_API_STATUS (NET_API_FUNCTION
*NETWKPROC)(LPWSTR, DWORD, LPBYTE *);

NETWKPROC _procNetWkstaGetInfo =
(NETWKPROC)
 (GetProcAddress(theApp.m_hNetDLL,
_T("NetWkstaGetInfo")));
if(_procNetWkstaGetInfo)
{  NET_API_STATUS nasRetVal =
   (*_procNetWkstaGetInfo)(lpwWkstaName,
   100, (LPBYTE*)&lpBuf);

  if(nasRetVal == NERR_Success)
  { WKSTA_INFO_100 *pWkstaInfo =
(WKSTA_INFO_100 *)lpBuf;
    DWORD dwPlatformId = pWkstaInfo-
>wki100_platform_id;
    if(dwPlatformId != PLATFORM_ID_NT)
    { return FALSE;}
    else return TRUE; }
  else {return FALSE;}}
else {return FALSE;}
}
```

4.4. Mengetahui nama komputer lain dan alamat IP masing-masing

Program ini dapat digunakan untuk mendapatkan informasi mengenai terminal-terminal yang berkoneksi dengan jaringan TCP/IP. Fungsi ini sama dengan fungsi Network Neighbourhood pada MsWindows.

Langkah-langkah yang dilakukan adalah sebagai berikut:

1. Include winsock2.h
2. Pada Menu, pilih Project-Setting dan pada tab Link, pilih Object/Library Modules
3. Tambahkan ws2_32.lib dan mpr.lib pada daftar link sebelumnya
4. Kompilasi kode program berikut tanpa membuat linker error

```
CString strTemp;
struct hostent *host;
struct in_addr *ptr;         // To
retrieve the IP Address

DWORD dwScope = RESOURCE_CONTEXT;
NETRESOURCE *NetResource = NULL;
HANDLE hEnum;
WNetOpenEnum( dwScope, NULL, NULL, NULL,
&hEnum );

WSADATA wsaData;
WSAStartup(MAKEWORD(1,1),&wsaData);

if ( hEnum )
{
  DWORD Count = 0xFFFFFFFF;
  DWORD BufferSize = 2048;
  LPVOID Buffer = new char[2048];
  WNetEnumResource( hEnum, &Count, Buffer,
&BufferSize );
  NetResource = (NETRESOURCE*)Buffer;

  char szHostName[200];

  for ( unsigned int i = 0; i <
BufferSize/sizeof(NETRESOURCE);

i++, NetResource++ )
  {
    if ( NetResource->dwUsage ==
RESOURCEUSAGE_CONTAINER &&
                  NetResource->dwType ==
RESOURCETYPE_ANY )
    {
      if ( NetResource->lpRemoteName )
      {
         CString strFullName =
NetResource->lpRemoteName;
         if ( 0 ==
strFullName.Left(2).Compare("\\\\") )
         strFullName =
strFullName.Right(strFullName.GetLength()-
2);
```

```
        gethostname( szHostName, strlen(
szHostName ) );
        host =
gethostbyname(strFullName);
        if(host == NULL) continue;
        ptr = (struct in_addr *) host-
>h_addr_list[0];

        // Eg. 211.40.35.76 split up like
this.
        int a = ptr->S_un.S_un_b.s_b1;
// 211
        int b = ptr->S_un.S_un_b.s_b2;
// 40
        int c = ptr->S_un.S_un_b.s_b3;
// 35
        int d = ptr->S_un.S_un_b.s_b4;
// 76

        strTemp.Format("%s -->
%d.%d.%d.%d",strFullName,a,b,c,d);
        AfxMessageBox(strTemp);
      }
    }
  }
  delete Buffer;
  WNetCloseEnum( hEnum );
}

WSACleanup();
```

4.5. Pendeteksian Port Pada TCP/IP

Kode program dibagi menjadi 2 bagian yaitu CPropertySheet dalam bentuk aplikasi MFC dan class untuk antarmuka WinSock.

File **CPropertySheetDialog.cpp/.h** dan **CPropertyPageDialog.cpp/.h** terdiri dari semua class yang dibutuhkan pada mekanisme Property Sheet dan digunakan sebagai basis aplikasi MFC. File **TcpPropertySheet.cpp/.h** terdiri dari kade untuk aplikasi utama, sedangkan semua file **Tcp[...]Page.cpp/.h** terdiri dari kode untuk halaman sheet. Kode antarmuka WinSock API terdapat pada file **CWinsock.cpp/.h** dan **CSock.cpp/.h**. File **CAsyncSock.cpp/.h** terdiri dari class yang digunakan untuk mengakses Winsock API dalam mode asyncronous, sedangkan kode program yang lain digunakan secara internal untuk menangani daftar kontrol, konfigurasi program, dan sebagainya.

Class pembangun antarmuka Winsock adalah CWinsock yang berfungsi untuk memetakan semua layanan WinSock ke library atau dummy inplementation tergantung pada definisi makro _DEBUGSOCKET, karena class CwinSock terdiri dari kode program untuk menangani layanan minimal server SMTP/POP3, yang dapat digunakan untuk menguji protokol SMTP/POP3 tanpa membutuhkan koneksi internet.

```
BOOL CTcpScanApp::InitInstance(void)
{
  CScanPage ScanPage;
  CConnectPage ConnectPage;
  CServicesPage ServicesPage;
  CPropertyPageList* pPropertyPageList =
new CPropertyPageList();

  if(pPropertyPageList)
  {
     PROPERTYPAGE* p;

     p = new PROPERTYPAGE(IDD_PAGE_SCAN,
&ScanPage,

RUNTIME_CLASS(CScanPage));
     pPropertyPageList->Add(p);
     p                =                new
PROPERTYPAGE(IDD_PAGE_CONNECT,&ConnectPage
,

RUNTIME_CLASS(CConnectPage));
     pPropertyPageList->Add(p);
     p                =                new
PROPERTYPAGE(IDD_PAGE_SERVICES,&ServicesPa
ge,

RUNTIME_CLASS(CServicesPage));
     pPropertyPageList->Add(p);

     CTcpScanPropertySheet*
pPropertySheetDialog =
              new
CTcpScanPropertySheet(NULL,
              pPropertyPageList);
     if(pPropertySheetDialog)
     { if(pPropertySheetDialog->Create())
       {            m_pMainWnd           =
pPropertySheetDialog;
         pPropertySheetDialog->DoModal();
       }
       delete pPropertySheetDialog;
    }
    delete pPropertyPageList;
  }
  Return(FALSE);
}
```

4.6. Melakukan operasi ping pada TCP/IP

Masalah umum pada TCP/IP adalah bagaimana melakukan ping pada Windows dengan menggunakan stack MS-TCP. Masalah tersebut dapat ditangani dengan menggunakan ICMP DLL.

Masalah implementasi adalah jika ditentukan nama komputer, atau alamat IP, maka lakukan ping yang dapat mengembalikan informasi waktu response ping. Fungsi ini membutuhkan ICMP.DLL dan beberapa struktur socket pada Csocket. Sebelum melakukan percobaan, file ICMPAPI.H, ICMP.LIB, dan IPEXPORT.H dari Microsoft, diletakkan pada direktori lib. Class terdiri dari 4 fungsi publik:

4.7. Pendeteksian alamat MAC

Alamat MAC dapat dilakukan dengan berbagai cara, salah satunya adalah dengan melakukan queri driver miniport NDIS. Mekanisme miniport dapat dibagi dilakukan melalui beberapa metode, namun salah satu metode yang paling sederhana adalah Metode Uuid Create (Uuid sekuensial). Langkah yang

dilakukan adalah melihat byte ke-2 hingga ke-8. Kode program sebagai berikut:

```
// Fetches the MAC address and prints it
static void GetMACaddress(void)
{
  unsigned char MACData[6];

  UUID uuid;
  UuidCreateSequential( &uuid );    // Ask
OS to create UUID
  for (int i=2; i<8; i++)  // Bytes 2
through 7 inclusive
                           // are MAC
address
    MACData[i - 2] = uuid.Data4[i];
  PrintMACaddress(MACData);         //
Print MAC address
}
```

Metode ini hanya dapat dieksekusi pada PC dengan NIC tunggal.

5. Kesimpulan

Tidak ada sebuah keamanan yang benar-benar fix dan menjamin untuk mengamankan suatu jaringan atau website. Keamanan adalah suatu proses, bukan produk. Jika anda memasang firewall, IDSes(instrusion detection system), routers dan honeypots (system untuk jebakan) mungkin dapat menyediakan lapisan-lapisan untuk bertahan, tetapi sekali lagi peralatan paling canggih di dunia tidak akan menolong suatu organisasi sampai organisasi tersebut mempunyai proses untuk mengupgrade system, memakai patch, mengecek security pada system sendiri dan metode lain. Telah banyak perusahaan yang memakai IDSes tetapi tidak memonitor file log, mereka menginstall firewall, tetapi tidak mengupgradenya. Jalan terbaik untuk melindungi website maupun network dari serangan adalah mendekatkan keamanan sebagaimana tantangan yang sedang terjadi terhadap keamanan itu sendiri.

6. Daftar Pustaka

[1] Spitzner, Lance, 1999, *A Passive Approach to Your Network Security, "The Secrets of Snoop"* Intrusion Detection within a Secured Network, *Secure System Administrating Research.*

[3] Marek,2000, *Building Secure Network with DMZ's*.

[4] Zuliansyah, Mochammad, 2002, *Teknik Pemrograman Network Interface Card pada Protokol TCP/IP*, ITB.