**BAB I PENDAHULUAN**

**1.1 Latar Belakang**

Indonesia sekarang masih menduduki peringkat sepuluh besar untuk kasus *cybercrime* (Kompas,2012). Kasus terakhir yang menimpa pemerintah indonesia sendiri adalah pengrusakan terhadap website POLRI oleh seorang hacker yang belum diketahui identitasnya sampai saat ini. Walaupun pemerintah indonesia sudah mengupayakan pencegahan terhadap kejahatan di dunia maya dengan membuat undang-undang tindak kejahatan dunia maya tetap saja mencari pelaku/penjahat dunia maya itu cukup sulit. Semua itu karena dunia maya tidak kenal batas wilayah maupun waktu. Yang bisa kita lakukan saat ini tidak lain adalah antisipasi degan cara mengamankan asset-asset kita yang ada di internet. Dan yang pasti kita tidak boleh menyepelekan masalah keamanan website.

Tidak hanya website pemerintah, website-website pendidikan pun juga terancam diserang oleh hacker baik dari dalam negeri maupun luar negeri. Zone –H yang mempunyai alamat domain [www.zone-h.org](http://www.zone-h.org) adalah sebuah website untuk mensubmit hasil dari *deface-an* suatu website, di website tersebut banyak ditemui website-website pendidikan yang sudah pernah di *deface* oleh attacker termasuk website UIN Sunan Kalijaga yang mempunyai domain [www.uin-suka.ac.id](http://www.uin-suka.ac.id). Website UIN Sunan Kalijaga telah di *deface* oleh **Gorontalo Defacer cr3w** pada tanggal 18/10/2008 pukul 15:44:02 seperti telihat pada gambar 1.1.



Gambar 1.1. Website UIN Sunan Kalijaga pernah di deface, archive di zone-h

Dan sampai saat ini website UIN Sunan Kalijaga masih mempunyai bug/celah yang sangat banyak. Padahal sebuah website akademik jelas harus memberikan informasi yang valid, seandainya ada attacker yang mempunyai maksud jahat bisa mengubah informasi yang ada pada website tersebut, tentu ini akan sangat membahayakan dan merugikan berbagai pihak.

Berikut ini adalah beberapa risiko yang bisa terjadi jika sebuah server sudah dimasuki oleh attacker:

1. Jika sebuah website pernah di *deface* jelas itu menunjukkan bahwa keamanan pada website tersebut kurang begitu diperhatikan, image dari pembuat maupun memilik website tersebut akan turun.
2. Seorang attacker bisa saja mengubah informasi yang ada pada website untuk mndapatkan keuntungan.
3. Seorang attacker bisa saja mencuri data-data penting yang ada di dalam server tersebut.
4. Seorang attacker bisa menjadikan server tersebut sebagai media penyimpanan file-file video, mp3, dan sebagainya.
5. Seorang attacker bisa menjadikan server tersebut sebagai kambing hitam atau batu loncatan untuk penyerangan ke server lain, sehingga seakan-akan penyerang tersebut berasal dari IP server yang dijadikan kambing hitam tersebut.
6. Attacker bisa menjadikan sever tesebut sebagai *zombie* untuk melakukan DOS (Denial of Service) pada server lain.

**1.2 Batasan Kerja Praktek**

Batasan masalah dalam kerja praktek ini adalah sebagai berikut:

1. Hanya melakukan penetration testing 1 server web yang mempunyai alamat domain [www.uin-suka.ac.id](http://www.uin-suka.ac.id).
2. Pencarian bug/celah pada web application dan sistem operasi server.

**1.3 Tujuan Kerja Praktek**

Adapun tujuan dari kerja praktek ini adalah sebagai berikut:

1. Mencari sebanyak mungkin bug/celah dalam website UIN Sunan Kalijaga.
2. Mendapatkan akses tertinggi sebagai superuser yaitu root di server UIN Sunan Kalijaga.
3. Memberikan rekomendasi dan *patch* kepada PKSI UIN Sunan Kalijaga.

**1.4 Manfaat Kerja Praktek**

Diharapkan dari pelaksanaan kerja praktek ini dapat membawa manfaat bagi berberapa pihak baik dari PKSI UIN Sunan Kalijaga maupun bagi mahasiswa sendiri.

1. Manfaat bagi PKSI UIN Sunan Kalijaga adalah:
2. Solusi dan *patch* dari hasil kerja praktek ini bisa digunakan untuk menutup celah/bug yang ada baik di sisi web application, server web maupun sistem operasi server.
3. Rekomendasi dari hasil kerja praktek bisa digunakan sebagai acuan pengamanan server Web UIN Sunan Kalijaga.
4. Manfaat bagi mahasiswa adalah:
5. Mahasiswa memperoleh pengalaman kerja sebelum memasuki dunia kerja.
6. Mahasiswa memperoleh kemampuan diri dalam penetration testing pada server.
7. Mahasiswa memperoleh kemampuan untuk menambal bug atau mem-*patch* suatu sistem.
8. Mahasiswa memperoleh kemampuan untuk mengamankan sebuah server dari serangan.

**BAB II TEMPAT KERJA PRAKTEK**

**2.1 Gambaran Umum Instansi**

Pusat Komputer dan Sistem Informasi Universitas Islam Negeri Sunan Kalijaga, sebagaimana tercantum dalam Keputusan Menteri Agama Republik Indonesia nomor 390 Tahun 2004 tanggal 3 September 2004 adalah gabungan dari dua lembaga sebelumnya yaitu Pusat Komputer dan Sistem Infromasi. Pusat Komputer (PUSKOM) adalah salah satu dari dua Unit Pelaksana Teknis atau unsur penunjang pada IAIN Sunan Kalijaga (Statuta IAIN Sunan Kalijaga Yogyakarta Tahun 2001 Pasal 121 ayat 3). Unit Pelaksana Teknis lainnya adalah Perpustakaan. Sistem Infromasi, semula merupakan sub bagian dari bagian Perencanaan dan Sistem Informasi (PSI).

Secara yuridis, Pusat Komputer sudah ada sejak diberlakukannya Keputusan Menteri Agama RI nomor 385 Tahun 1993 tanggal 29 Desember 1993, tentang Organisasi dan Tata Kerja IAIN Sunan Kalijaga Yogyakarta. Pasal 60 memuat tentang Pusat Komputer yang menjelaskan bahawa Pusat Komputer adalah unsur penunjang IAIN Sunan Kalijaga di bidang komputer (pasal 60 ayat 1). Pusat Komputer dipimpin oleh seorang kepala, yang ditunjuk di antara pranata komputer senior di lingkungan Pusat Komputer yang bertanggungjawab kepada Rektor dan pembinaannya dilakukan oleh Pembantu Rentor I (pasal 60 ayat 2).

Pusat Komputer sebagai unit pelasana teknis atau unsur penunjang di IAIN Sunan Kalijaga dimuat juga dalam Keputusan Menteri Agama RI Nomor 399 Tahun 1993 tentang statuta Institut Agama Islam Negeri Sunan Kalijaga Yogyakarta.

Dalam upaya meningkatkan kualitas pelayanan administrasi di IAIN Sunan Kalijaga Yogyakarta diperlukan adanya sarana pendukung berupa pusat komputer yang berkemampuan tinggi, teruji tingkat validitasnya, efisien, efektif dan didukung oleh keakuratan data, kecepatan pengolahan serta keamanan yang terjamin, maka Rektor, Prof. Dr. H.M. Atho Mudzhar, membentuk tim pelaksana penyiapan Program Pusat Komputer IAIN Sunan Kalijaga Yogyakarta.

Visi PKSI UIN Sunan Kalijaga Yogyakarta

Mewujudkan UIN Sunan Kalijaga Yogyakarta sebagai universitas digital (cyber campus)

Strategi

1. Otomasi proses administrasi (Akademik, Kemahasiswaan, dan Umum)

2. Digital lifestyle experience (e-learning, digital information dissemination, dan digital payment)

Prinsip PKSI UIN Sunan Kalijaga Yogyakarta

* + - 1. Layanan
* One Day Service
* One Stop Service
* 3S (Senyum, Salam, Sapa)
  + - 1. Teknis
* One Account for All Access
* One Entry for All Database
* ADAP (As Digital As Posible)
  1. **Ruang Ligkup Kerja Praktek.**

Staf pada UPT. PKSI UIN Sunan Kalijaga terdiri atas:

1. Kepala : Agung Fatwanto, S.Si., M.Kom., Ph.D

2. Divisi:

* 1. Divisi Infrastruktur: Hendra Hidayat, S.Kom.

Anggota: Rahmadhan Gatra, ST

* 1. Divisi Pengembangan Sistem Informasi: Mustaqim, MT.

Anggota:

* Salim Athari, S.Kom
* Adi Wirawan, S.Kom
* Prihanto Dwi Rahmanto, S.Kom.
  1. Divisi SDM: Ratna Windah Lestari, SIP

Anggota: Rohyati, S.Ag.

* 1. Divisi Media: M. Arif Wibisono

Anggota: Daru Prasetyawan, ST

* 1. Divisi Layanan IT: Siti Mutmainah, S.Kom.

Anggota:

* Novi Praci Putri
* Mellyana Cahya Ningrum

3. Bendahara: Ratna Windah Lestari, SIP

**BAB III HASIL DAN PEMBAHASAN**

* 1. **Analisis**

1. Kondisi Tempat Kerja

Gedung PKSI UIN Sunan Kalijaga terdiri dari tiga lantai dengan rincian sebagai berikut:

1. Lantai I

Lantai I terdiri dari dua ruangan utama yaitu ruangan pusat layanan dan ruangan server. Pada ruangan pusat layanan terdiri dari beberapa meja kerja devisi layanan IT PKSI dan devisi infrastruktur PKSI UIN Sunan Kalijaga. Kemudian di sebelah timur ruang layanan ada ruang server yang berisi seluruh server kampus UIN Sunan Kalijaga.

2. Lantai II

Lantai II terdiri dari satu ruangan utama yaitu ruang multimedia , Ruang multimedia ini digunakan untuk tempat pemotretan, meja kerja devisi Media PKSI UIN Sunan Kalijaga dan kontroling TV UIN Sunan Kalijaga.

1. Lantai III

Lantai III terdiri dari dua ruangan utama yaitu ruangan development dan ruangan rapat, staff PKSI yang bergerak di bidang development bekerja di ruangan ini.

Spesifikasi komputer yang digunakan di PKSI UIN Sunan Kalijaga adalah sebagai berikut:

Tabel 3.1. Spesifikasi Komputer yang digunakan di PKSI UIN Sunan Kalijaga

|  |  |  |
| --- | --- | --- |
| NO. | System | Keterangan |
| 1. | Operating System | Windows 7 Home Premium 64-bit (6.1, Build 7601) Service Pack 1 |
| 2. | System Manufacturer | Dell Inc. |
| 3. | System Model | Studio XPS 9100 |
| 4. | Processor | Intel(R) Core(TM) i7 CPU 960 @ 3.20GHz (8 CPUs), ~3.2GHz |
| 5. | Memory | 12288MB RAM |
| 6. | Card name | AMD Radeon HD 6700 Series |
| 7. | Display Memory | 2793 MB  Dedicated Memory: 1006 MB  Shared Memory: 1787 MB |

1. Kondisi SDM di PKSI UIN Sunan Kalijaga

Sumber daya manusia di PKSI UIN Sunan Kalijaga Yogyakarta terdiri dari limabelas orang, dengan empat orang merupakan tenaga kontrak yaitu:

* + - 1. Agung Fatwanto, S.Si., M.Kom., Ph.D (Kepala PKSI)
      2. Mustaqim, MT. (devisi pengembangan sistem informasi)
      3. Mellyana Cahya Ningrum (anggota devisi layanan IT)
      4. Novi Praci Putri (anggota devisi layanan IT)

Dengan demikian pegawai tetap PKSI UIN Sunan Kalijaga hanya terdiri dari sebelas orang.

**3.2 Kegiatan KP**

Metode standar penetation testing adalah sebagai berikut :

1. Footprinting
2. **Scanning Fingerprinting**
3. **Enumeration**
4. **Gaining Access**
5. **Privilege Escalation**
6. **Pilfering**
7. **Covering Tracks**
8. **Backdooring**
9. **Denial of Service**

Dibawah ini merupakan proses dan hasil penetration testing di server web UIN Sunan Kalijaga. Dalam kerja praktek ini dilakukan dua kali penetration testing dikarenakan terjadi migrasi server web UIN Sunan Kalijaga dari server yang menggunakan FreeBSD 8.0 kemudian pada akhir maret 2012 pindah server dan menggunakan sistem operasi FreeBSD 8.2.

1. **Footprinting**

Footprinting adalah proses menggali informasi sebanyak-banyaknya dari target (box). Hasil footprinting server UIN Sunan Kalijaga yang diperoleh adalah sebagai berikut :

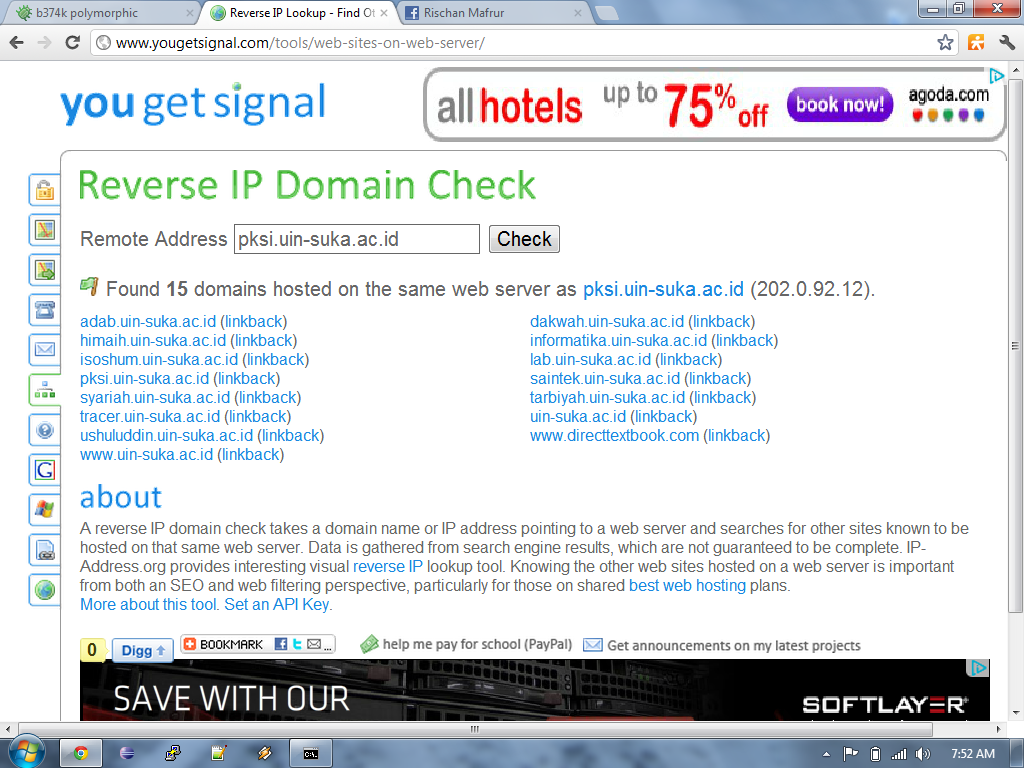
1. Check IP server target.

Pada penetration pertama IP Server web UIN Sunan Kalijaga adalah 172.16.4.201.

Kemudian untuk penetration yang kedua IP nya adalah 10.0.8.120.

1. Reverse IP domain check

Reverse IP domain check adalah mencari informasi website apa saja yang ada dalam host tersebut. Contoh aplikasi yang bisa digunakan adalah **You Get Signal** bisa di akses di [www.yougetsignal.com](http://www.yougetsignal.com) kemudian pilih menu reverse IP domain check, seperti terlihat pada gambar 3.1.



Gambar 3.1. Reverse IP Domain Check domain pksi.uin-suka.ac.id

Dari hasil reverse domain check bisa kita lihat bahwa server web UIN Sunan Kalijaga tidak hanya berisi satu website tapi ada duabelas website lain di dalamnya yaitu website Fakultas Adab, Fakultas Sosial dan Humaniora, Fakultas Syariah, Fakultas Dakwah, Fakultas Sains dan Teknologi, dan Fakultas Tarbiyah dan lain-lain.

Jadi untuk memasuki server web UIN Sunan Kalijaga bisa melalui berbagai pintu, bisa mencari bug/celah di website utama UIN Sunan Kalijaga, website PKSI, Fakulatas Tarbiyah, atau yang lain, yang pasti semakin banyak website yang ada dalam satu host/server akan semakin banyak memambah peluang seorang attacker berhasil melakukan penetration.

*Tips :*

*Penggunaan banyak domain dalam satu host merupakan tindakan yang cukup berbahaya, dikarenakan jika ada salah satu website ada yang mengandung bug kemudian attacker berhasil masuk dalam server web tersebut tentu attacker bisa melakukan* ***jumping****.*

***Jumping*** *adalah tindakan seorang attacker yang bisa meloncat ke direktori/home user lain(website lain yang ada dalam satu server tersebut).*

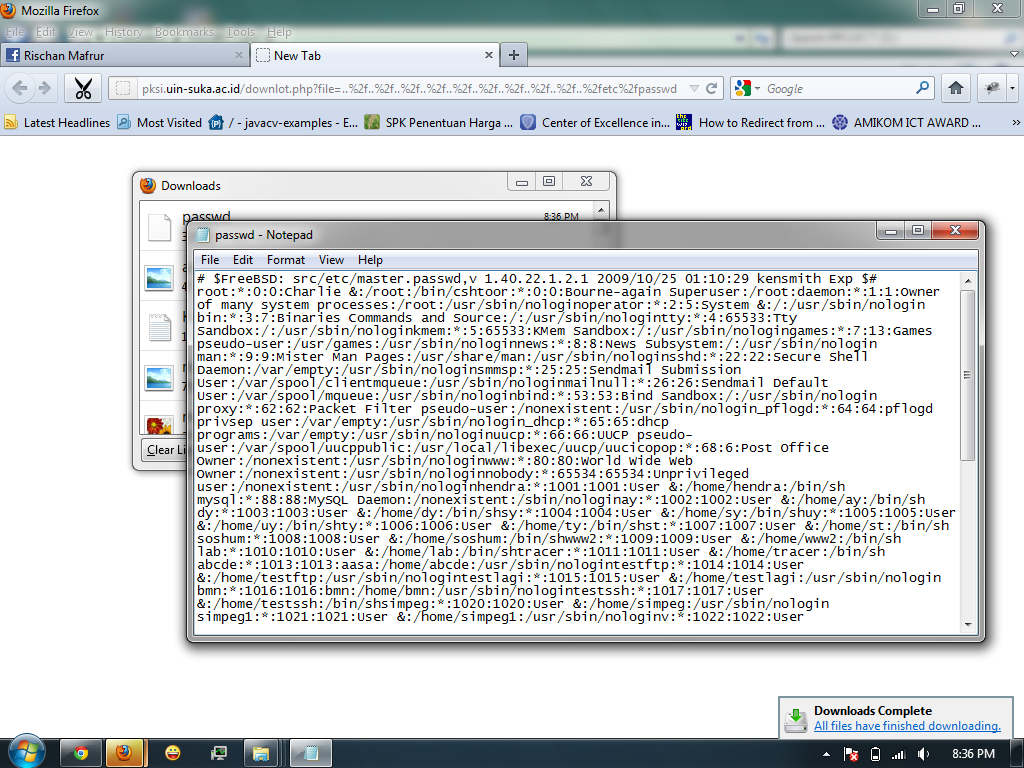
*Hal ini sebenarnya bisa diatasi dengan proteksi direktori yaitu dengan cara pengaturan permission direktori tersebut, karena sebenarnya proses* ***jumping*** *hanyalah mencari direktori yang bisa dibaca(readable) atau yang bisa ditulis (writable) dalam home user lain. Ketika ada direktori home user lain bisa dibaca atau mungkin bisa ditulis oleh attacker jelas attacker bisa mengakses direktori tersebut.*

1. Analisis Keamanan Website *(web application)*
2. LFI di Website PKSI UIN Sunan Kalijaga

Website dengan domain <http://pksi.uin-suka.ac.id> menggunakan CMS (Content Management Sistem) lokomedia yang mempunyai banyak bug/celah. Dalam proses penetration testing ternyata ditemukan bug LFI (Local File Inclusion). LFI merupakan bug yang bisa membuat seorang attacker bisa mengambil file yang berharga dari dalam server. Dengan bug LFI ini seorang attacker bisa mendownload file passwd dari server yaitu dengan mengetikan URL seperti ini:

[*http://pksi.uin-suka.ac.id/downlot.php?file=..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2fetc%2fpasswd*](http://pksi.uin-suka.ac.id/downlot.php?file=..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2fetc%2fpasswd)

Perintah tersebut adalah perintah untuk mendownload file passwd yang ada dalam server dan ternyata perintah tersebut bekerja dengan baik di server UIN Sunan Kalijaga, seperti telihat pada gambar 3.2.



Gambar 3.2. Download file passwd dari server UIN Sunan Kalijaga

File passwd adalah file yang sangat berharga didalam sistem operasi Linux, BSD dan keluarganya. File ini adalah file yang hanya bisa di *write (edit)* oleh root tapi bisa di baca oleh semua user yang ada didalam sistem. File ini berisi list user /semua user yang ada dalam server. Jika seorang attacker sudah mendapatkan file ini berarti sudah mengurangi setengah dari pekerjaannya karena dengan melihat file ini attacker akan mengetahui user apa saja yang ada dalam server dan tentu list user tadi bisa di gunakan sebagai *wordlist* username untuk bruteforce, dan biasanya admin memberikan password yang mudah ditebak atau password yang hampir sama dengan username sehingga mempermudah proses bruteforce.

Bug LFI ini sebenarnya berasal dari kesalahan script yang ada pada file downlot.php. File downlot.php dapat dilihat pada lampiran 1. Kesalahanya ada pada variable $filename.

*$direktori = "files/"; // folder tempat penyimpanan file yang boleh didownload*

$ *filename = $\_GET['file']*

Variable filename tidak difilter dengan bagus sehingga client bisa menginputkan semua karakter ke dalam URL, seperti pada kasus ini attacker menginputkan perintah untuk fetch file passwd dan ternyata perintah tersebut dijalankan dengan baik oleh sever.

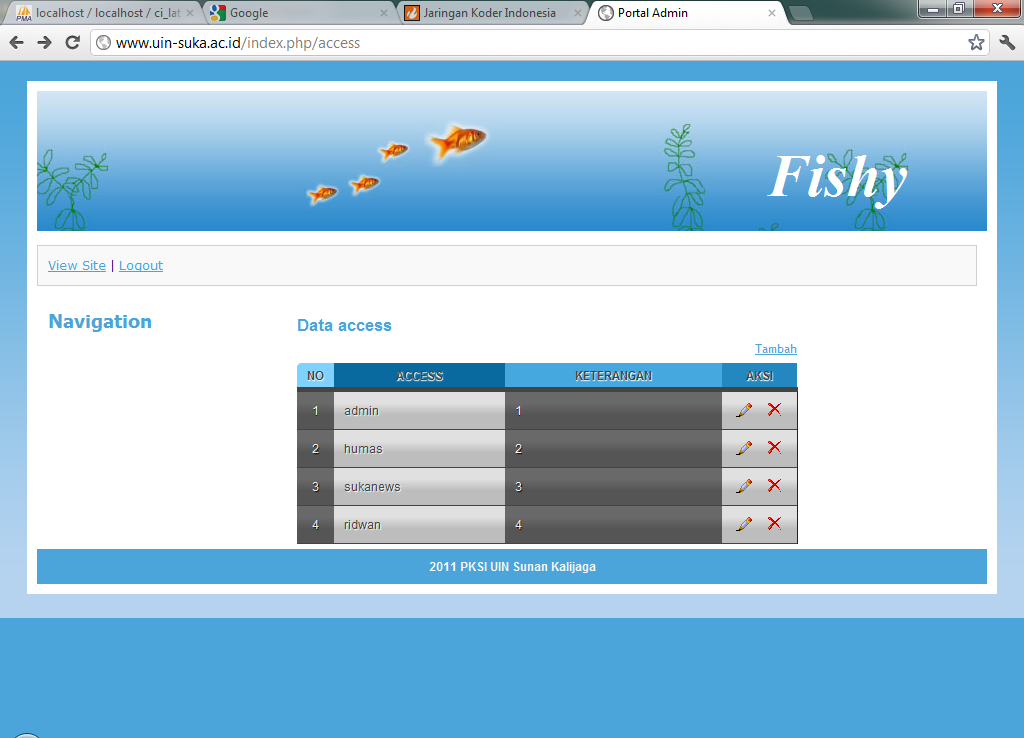
1. Multi Bug di Semua Website

Website utama UIN Sunan Kalijaga saat ini beserta semua website fakultas UIN Sunan Kalijaga menggunakan template yang sama yaitu menggunakan template yang dibuat dengan Framework Codeigniter.

Dalam penetration testing ini ditemukan beberapa bug yang cukup berbahaya yaitu :

1. Tidak ada session di <http://www.uin-suka.ac.id/index.php/access>
2. Ada menu import file excel di <http://www.uin-suka.ac.id/index.php/chapter>
3. Editor tanpa session di <http://www.uin-suka.ac.id/index.php/ckeditor>

Untuk bug kedua dan ketiga memang tidak begitu berakibat fatal, tapi bug yang pertama ini bisa berakibat fatal. Pada bug yang pertama ini jika attacker mengakses URL <http://www.uin-suka.ac.id/index.php/access> kita langsung akan diarahkan ke page admin tanpa proses login, kita bisa mengedit hak akses user bahkan bisa menambah user, seperti terlihat pada gambar 3.3.



Gambar 3.3. Masuk page admin tanpa menggunakan session di website UIN Sunan Kalijaga

*Tips:*

*Seorang admin web seharusnya melakukan testing terlebih dahulu sebelum mengonlinekan websitenya. Tanpa melakukan testing admin tak pernah tahu apakah website tersebut masih ada celah atau tidak.*

*Kesalahan sekecil apapun seperti lupa melakukan casting terhadap variable input, tidak ada filter dalam variable input, atau bahkan lupa memberikan session di salah satu page admin itu semua bisa berakibat fatal.*

*Coding yang terstruktur, bersih dan testing sebelum benar-benar di implementasikan adalah hal yang wajib dilakukan jika menginginkan website aman dari serangan.*

1. **Scanning Fingerprinting**

Selanjutnya adalah *Scanning Fingerprinting* yaitu identifikasi service apa saja yang berjalan di dalam server. Dalam *scanning fingerprinting* ini dibagi menjadi beberapa bagian yaitu:

1. Analisis dan scanning sistem operasi yang digunakan.
2. Analisis dan scanning service yang dijalankan.
3. Analisis dan scanning webserver yang digunakan.
4. Analisis dan scanning php beserta modul-modulnya yang digunakan.
5. Analisis dan scanning mysql yang digunakan.

Hasil dari analisis dan scanning sebagai berikut:

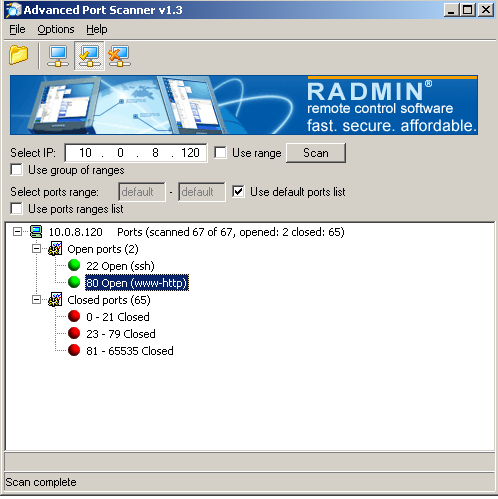


Gambar 3.4. Scanning Fingerprinting menggunakan php script.

Tabel 3.2 Table Fingerprinting

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **Fingerprinting** | **Hasil** | **Keterangan** |
| 1. | Sistem Operasi | Pentesting pertama:  FreeBSD web123.uin-suka.ac.id 8.0-RELEASE FreeBSD 8.0-RELEASE #1: Thu Oct 7 15:25:30 WIT 2012 hendra@web123.uin-suka.ac.id | Para proses pentesting yang pertama server UIN Sunan Kalijaga menggunakan sistem operasi FreeBSD 8.0 |
|  |  | Pentesting kedua:  FreeBSD pempek.uin-suka.ac.id 8.2-RELEASE FreeBSD 8.2-RELEASE #0: Fri Feb 18 02:24:46 UTC 2011 root@almeida.cse.buffalo.edu:/usr/obj/usr/src/sys/GENERIC i386 | Untuk pentesting yang kedua diperoleh hasil bahwa server UIN Sunan Kalijaga menggunakan sistem operasi FreeBSD 8.2. |
| 2. | **Web Server** | Pentesting pertama : Apache/2.2.17 | Versi Webserver yang digunakan, ini menjadi penting untuk diketahui karena bisa jadi webserver yang digunakan adalah webserver versi beta atau yang masih mempunyai bug. |
| Pentesting kedua :Apache/2.2.17 |
| 3. | **PHP** | Pentesting pertama : PHP 5.2.11  Safe Mode : Off | Safe Mode adalah mode aman PHP, safe mode off memberikan peluang lebih besar pada attacker untuk menguasai server. |
| Pentesting kedua : PHP 5.3.5  Safe Mode :Off |
| Modul Loaded:  core prefork http\_core mod\_so mod\_authn\_file mod\_authn\_dbm mod\_authn\_anon mod\_authn\_default mod\_authn\_alias mod\_authz\_host mod\_authz\_groupfile mod\_authz\_user mod\_authz\_dbm mod\_authz\_owner mod\_authz\_default mod\_auth\_basic mod\_auth\_digest mod\_file\_cache mod\_cache mod\_disk\_cache mod\_dumpio mod\_reqtimeout mod\_include mod\_filter mod\_charset\_lite mod\_deflate mod\_log\_config mod\_logio mod\_env mod\_mime\_magic mod\_cern\_meta mod\_expires mod\_headers mod\_usertrack mod\_unique\_id mod\_setenvif mod\_version mod\_ssl mod\_mime mod\_dav mod\_status mod\_autoindex mod\_asis mod\_info mod\_suexec mod\_cgi mod\_cgid mod\_dav\_fs mod\_vhost\_alias mod\_negotiation mod\_dir mod\_imagemap mod\_actions mod\_speling mod\_userdir mod\_alias mod\_rewrite mod\_php5 | Baik pentesting yang pertama maupun kedua ternyata sama saja semua modul PHP diload, ini jelas berbahaya dan tidak efisien, sebaiknya modul-modul yang sekirannya kurang penting di disable saja. |

**Port scanning**



Gambar 3.5. Port scanning server web UIN Sunan Kalijaga menggunakan RADMIN tool.

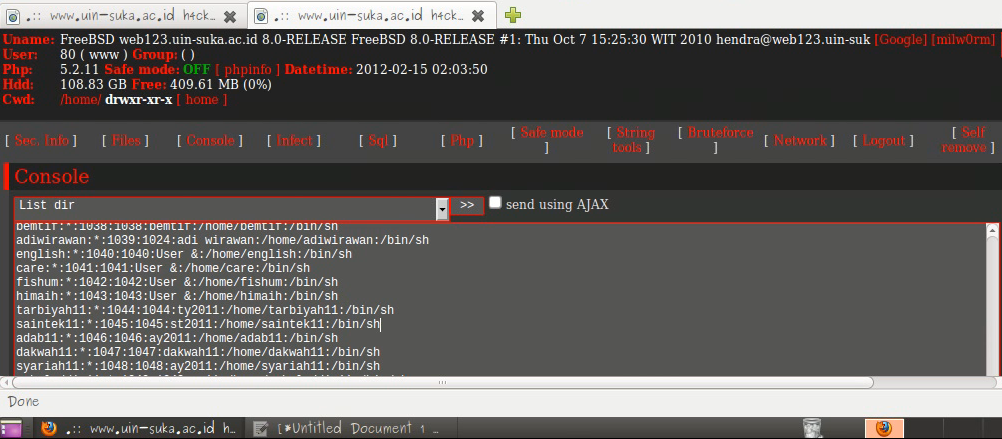
Untuk melihat port apa saja yang terbuka di Server UIN Sunan Kalijaga salah satu tool yang bisa di gunakan adalah RADMIN port scanner. Hasilnya adalah hanya dua port yang terbuka yaitu port 80 http dan port 22 ssh, seperti pada gambar 3.5.

Dengan port scanning seorang attacker bisa mengetahui port mana saja yang terbuka sehingga attacker juga akan tahu service apa saja yang dijalankan. Semakin banyak port yang terbuka jelas akan semakin menambah peluang attacker untuk bisa memasuki server tersebut.

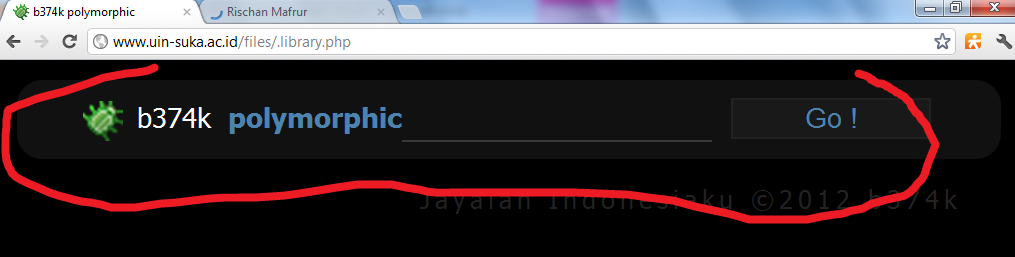
1. **Enumeration dan Gaining Access**

Metode *Enumeration* adalah mencari *poorly protected password* kemudian dilanjutkan dengan *Gaining Access* dan ketika proses footprinting saja sudah ditemukan page admin tanpa session yang sebenarnya itu adalah *Gaining Access*. Bagi seorang attacker akses page admin tidakalah cukup, karena page admin hanya bisa melihat, mengedit atau menambah berita, gambar dan lain-lain. Untuk melihat dan mengexploit server seorang attacker membutuhkan sebuah backdoor/webshell. Ketika seorang attacker bisa masuk ke halam admin biasanya yang mereka cari adalah form upload baik itu upload file maupun gambar. Dalam pentesting server UIN Sunan Kalijaga ternyata ditemukan form upload gambar tanpa menggunakan filter sehingga semua file bisa diupload termasuk file php. Dari sinilah seorang attacker menanamkan backdoor phpshell kedalam server.

Gambar 3.6 memperlihatkan phpshell yang ditanam di server web UIN Sunan Kalijaga pada pentesting I. Dan gambar 3.7 dan 3.8 adalah phpshell yang ditanam di server web UIN Sunan Kalijaga pada pentesting II (saat ini).



Gambar 3.6. Tampilan PHP Shell di server lama UIN Sunan Kalijaga pentesting I (FreeBSD 8.0)



Gambar 3.7. Jendela login webshell di server UIN Sunan Kalijaga pentesting II (FreeBSD 8.2)



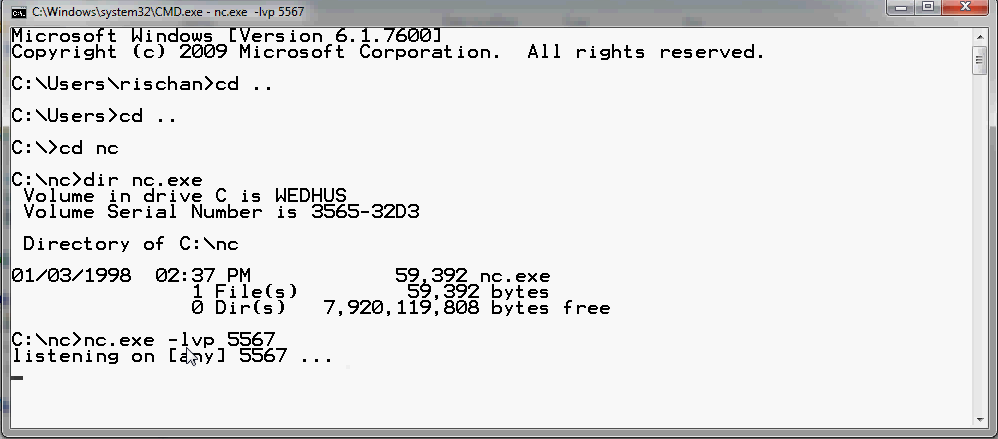
Gambar 3.8. Web Shell di server web UIN Sunan Kalijaga pentesting II (FreeBSD 8.2)

Phpshell bisa digunakan untuk memasukkan perintah-perintah linux selayaknya command line di linux. Seorang attacker adalah seorang yang tak kan pernah puas, menggunkan phpshell untuk menginputkan perintah-perintah linux jelas tidak nyaman. Solusinya adalah menggunakan back connect atau bind connection.

Untuk melakukan back connect jalankan netcat/nc di cmd menggunakan perintah sebagai berikut:

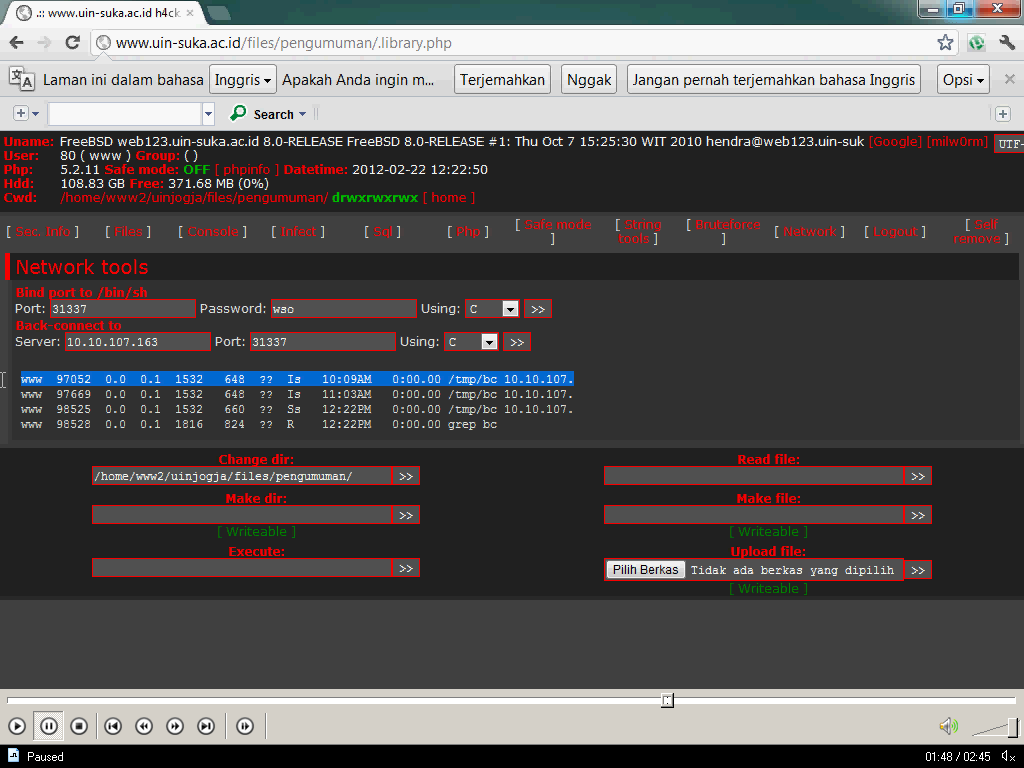
**nc.exe –lvp 5567**

parameter l adalah untuk listening, v untuk verbose (menampilkan kondisi yang terjadi saat itu), dan p adalah port, 5567 adalah port yang digunakan untuk melakukan back connect, seperti pada gambar 3.9.



Gambar 3.9. Back connect menggunakan netcat pentesting I

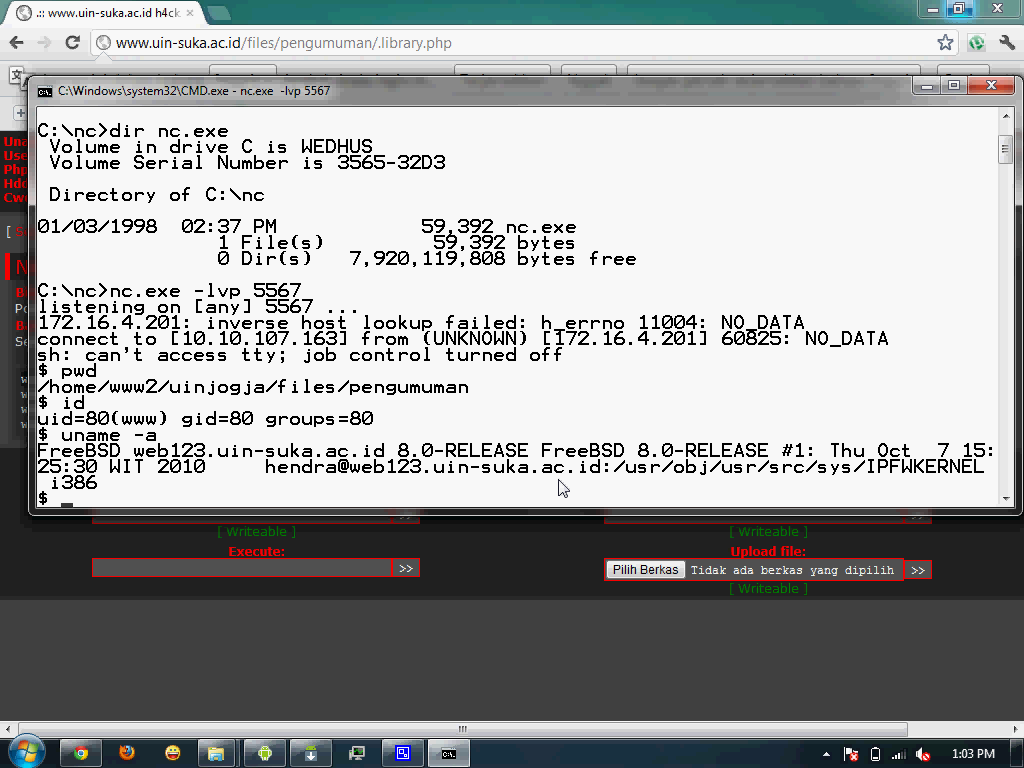
Setelah komputer local melakukan listening menggunakan netcat, jalankan script back connect di server target. Hampir di semua phpshell biasanya sudah di sertakan script back connect baik menggunakan perl, c, atau python. Jangan lupa untuk mengganti port sesuai dengan port yang sudah dilisten di komputer local yaitu 5567, seperti terlihat pada gambar 3.10.



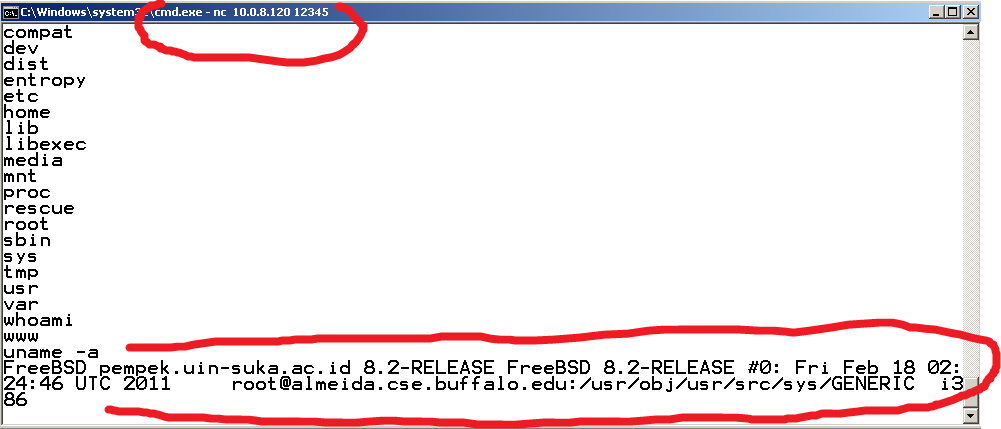
Gambar 3.10. Menjalankan script back connect di server web UIN Sunan Kalijaga pentesting I

Hasilnya bisa dilihat pada gambar 3.11 yaitu akses shell menggunakan back connect. Dengan back connect attacker bisa memperoleh akses shell selayaknya ssh shell dengan uid **www**, hanya saja setiap kali ingin mengakses server harus melakukan back connect menggunakan netcat. Pada pentesting yang kedua bisa terlihat pada gambar 3.12 yaitu menggunakan Bind connection pada IP 10.0.8.120 dan port 12345. Perbedaan bind connection dengan back connect adalah jika back connect komputer local (komputer attacker) yang melakukan proses listening kemudian attacker menjalankan script back connect di server, kalau bind connection attacker harus menjalankan script bind connection di dalam server sehingga server/target yang melakukan listening setelah server listening attacker akan melakukan koneksi menggunakan perintah sebagai berikut:

**nc <IP server> <port server yang listening>**



Gambar 3.11. Berhasil mendapatkan akses shell menggunakan back connect pentesting I



Gambar 2.12. Bind Connection menggunakan netcat pentesting II

*Bila seorang attacker sudah mendapatkan akses ke server menggunakan phpshell seorang attacker bisa melakukan apa saja yang dia inginkan, mendapatkan akses shell terminal/console menggunakan back connect atau bind dan sebagainya. Phpshell, phpbackdoor, bind connection, back connect dan sebagainya semua itu sebenarnya bisa diatasi dengan cara mematikan berbagai fungsi sistem di php. Sebaiknya admin hanya mengeload modul-modul atau fungsi-fungsi php yang memang benar-benar digunakan, untuk mendisable fungsi-fungsi yang cukup berbahaya yaitu dengan menambahkan baris berikut di dalam file php.ini.*

*disable\_functions = “shell\_exec, passthru, proc\_open, proc\_close, proc\_get-status, proc\_nice, proc\_terminate, exec, system, suexec, popen, pclose, dl, ini\_set, virtual, set\_time\_limit”.*

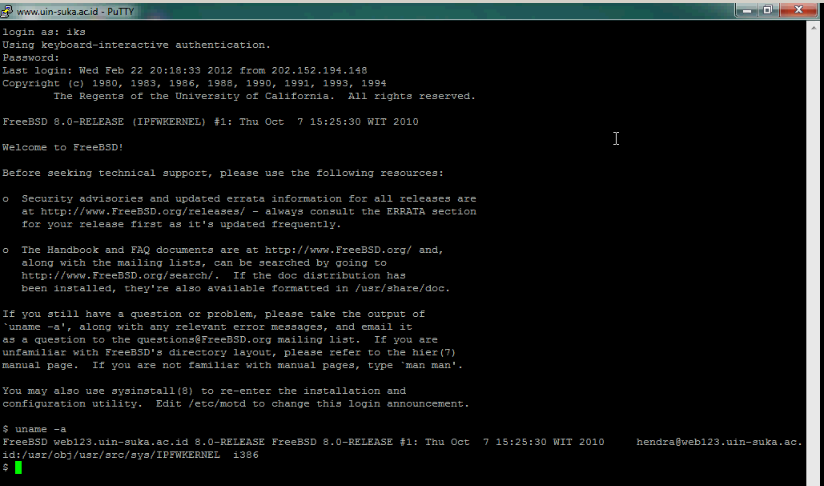
*Jika fungsi-fungsi di atas ini benar-benar di disable maka phpshell tidak akan bisa bekerja. Selain dengan cara tersebut admin juga bisa menggunakan cara lain yaitu mengaktifkan safe mode php.*

Pada tahap *enumeration* ini seorang attacker biasanya juga melakukan bruteforce username dan password ssh. Karena pada saat proses footprinting sudah diperoleh file passwd tentu file ini yang akan dijadikan wordlist proses bruteforce.

Pada pentesting yang pertama bruteforce membuahkan hasil yaitu ditemukan user yang menggunakan password cukup lemah yaitu user ssh dengan username “iks” dan password “iksiksiks” , kemudian ditemuakan lagi username “fishum” dengan password “fishum11”. Akan tetapi pada pentesting yang kedua proses bruteforce tidak membuahkan hasil.

Setelah mendapatkan username dan password ssh tentu attacker tidak memerlukan lagi akses bind atau back connect karena attacker bisa dengan leluasa masuk dan mengutak-atik server menggunakan account ssh yang diperolehnya.

Pada gambar 3.13 memperlihatkan attacker barhasil login ssh menggunakan username dan password yang diperoleh dari proses bruteforce.



Gambar 3.13. Login ssh menggunakan user dan password yang didapatkan dari bruteforce

*Tips:*

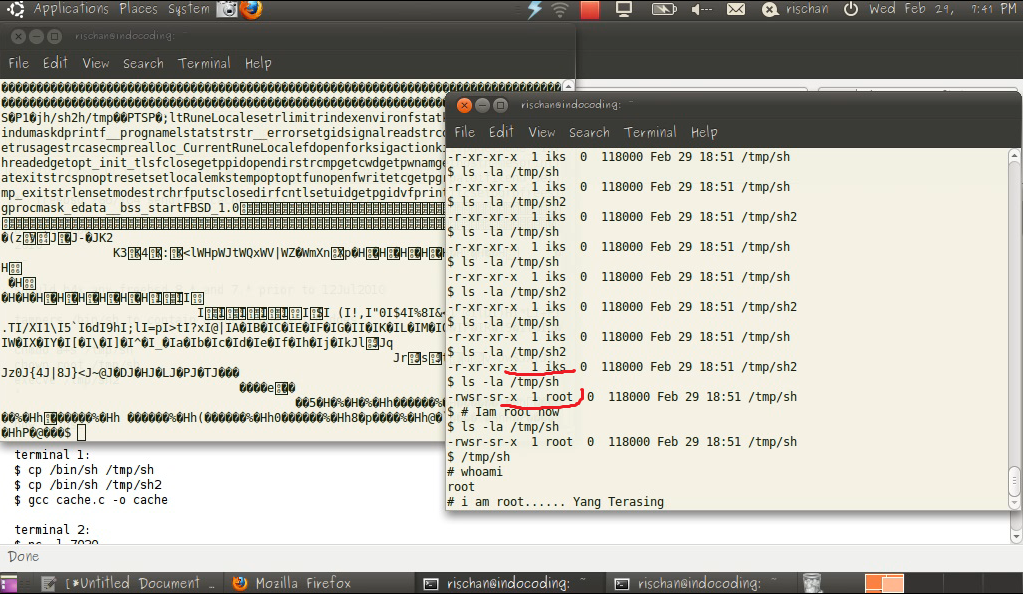
*Dalam pemberian password sebaiknya menggunakan kombinasi angka, huruf dan lambang, selain itu sebaiknya tidak semua user diberi hak akses ssh, lebih baik hanya user yang memang membutuhkan saja yang diberikan akses ssh. Kalau perlu gunakan rsa public key dan matikan autentifikasi dengan password sehingga hanya user yang sudah mengupload rsa public nya yang bisa masuk kedalam server. Gunakan aplikasi semacam ssh bruteforce blocker sehingga bila ada tanda-tanda bruteforce sistem akan langsung otomatis menolaknya dan melaporkan lognya ke administrator.*

1. **Privilege Escalation**

Pada tahap *enumeration dan gaining access* attacaker sudah berhasil mendapatkan akses ssh tetapi masih sebagai user biasa dan tentu untuk server BSD dan keluarganya user biasa tidak bisa menggunakan perintah “su” untuk menjadi root/ superuser.

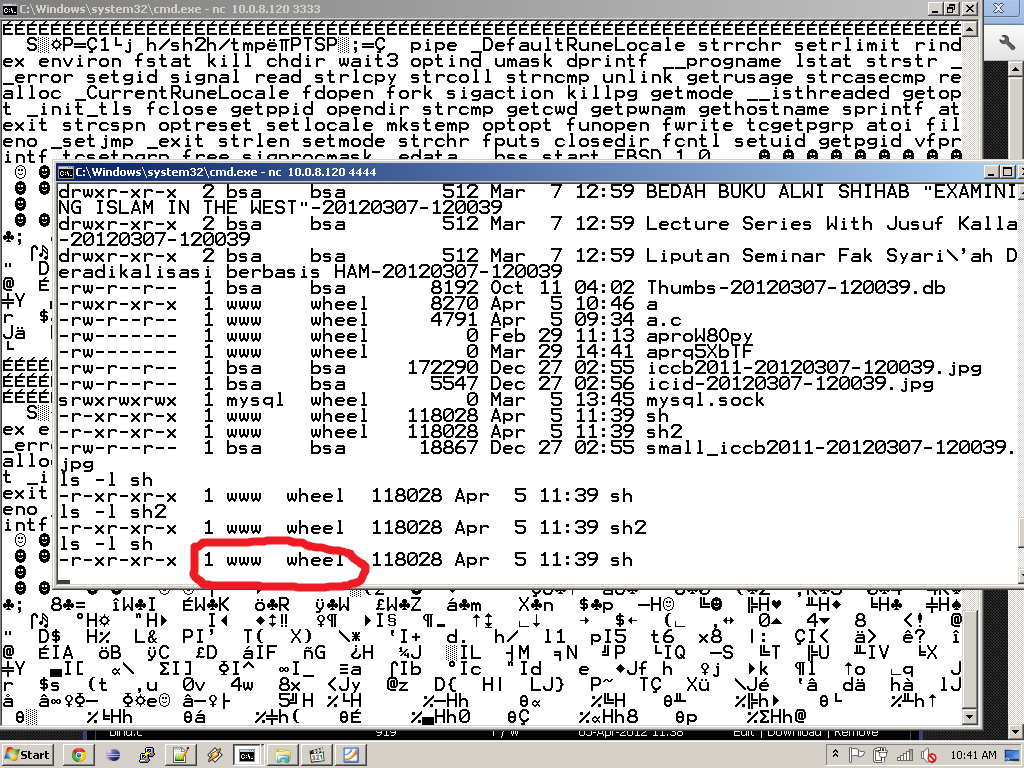
Pada tahap privilage escalation ini seorang attacker akan berusaha mencari exploit baik remote exploit maupun local exploit yang bisa menjadikan attacker mendapatkan akses tertinggi dalam server yaitu root.

Untuk pentesting yang pertama server UIN Sunan Kalijaga masih menggunakan sistem operasi FreeBSD 8 dan berhasil di root menggunakan local exploit *FreeBSD mbufs() sendfile cache poisoning local privilege escalation*. Pada Gambar 3.14 telihat attacker berhasil mendapatkan akses root server web UIN Sunan Kalijaga yang menggunakan sistem operasi FreeBSD 8.0. File local root exploit dapat dilihat pada lampiran 2.



Gambar 3.14. Berhasil mendapatkan akses root di server menggunakan local root exploit

Pada pentesting ke II server UIN Sunan Kalijaga menggunakan FreeBSD 8.2 dan gagal di exploit menggunakan local root exploit ini, seperti terlihat pada gambar 3.15.



Gambar 3.15. Gagal local root exploit pada FreeBSD 8.2 pentesting II

Untuk FreeBSD 8.2 ditemukan juga bug local exploit pada aplikasi ProFTPd yaitu aplikasi layanan FTP yang secara default sudah terinstall di FreeBSD 8.2. Local root exploit ini jelas bekerja di FreeBSD 8.2 akan tetapi server UIN Sunan Kalijaga mematikan service FTP, Server UIN Sunan Kalijaga hanya membuka port http dan ssh, sehingga memang untuk saat ini tidak bisa di exploit, akan tetapi jika suatu waktu layanan FTP dibuka, dan ada attacker yang berhasil masuk ke dalam server dan dia menggunakan local root exploit tersebut, kemungkinan besar server UIN Sunan Kalijaga akan berhasil di exploit. File local root ProFTPd dapat dilihat pada lampiran 3.

1. **Pilfering**

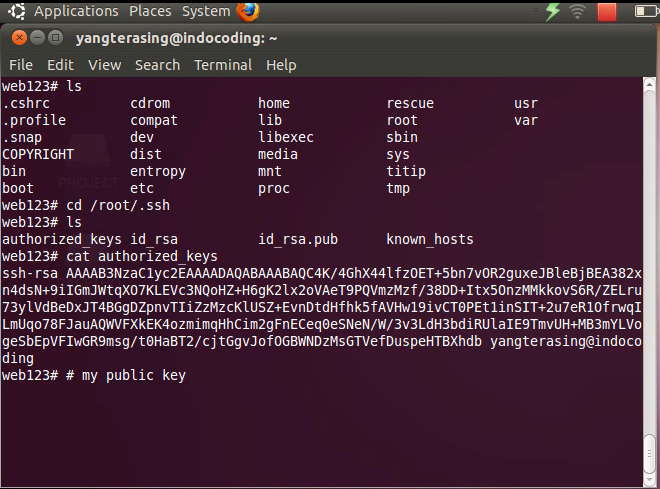
Pilfering adalah akses dengan user legal supaya tidak diketahui oleh admin yang sebenarnya. Langkah-langkah yang dilakukan dalam proses pentesting sebenarnya semuanya tergantung dari kondisi adminnya, kita bisa mengetahui bagaimana admin bekerja, apa saja yang biasanya di lakukan admin bahkan kita bisa menilai kemampuan admin dengan melihat log historynya.

Ketika memang admin kurang begitu tanggap terhadap perubahan-perubahan dalam server atau mungkin admin kurang mengerti mengenai hal seperti ini keamanan,serangan dan sebagainya tentu saja penangannya akan berbeda.

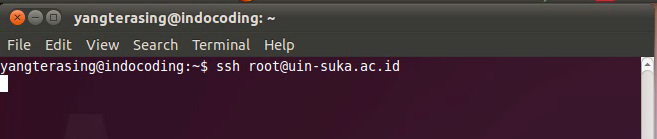
1. **Backdooring**

Backdooring adalah kegiatan untuk menanam sebuah pintu belakang, sehingga ketika attacker ingin mengakses server tidak perlu repot-repot seperti ketika awal mencari bug/celah kemudian mengexploitnya. Pada tahap backdooring ini juga tergantung dengan situasi dan kondisi. Seperti yang sudah disampaikan diatas kalau sang admin kurang begitu peduli atau kurang tahu dalam hal keamanan, backdooring, webshell dan kawan-kawannya jelas seorang attacker tidak perlu susah payah menanam rootkit, atau menyetting crontab untuk connect pada komputer pribadi setiap hari apa pukul berapa, semuannya jelas tergantung kondisi target.

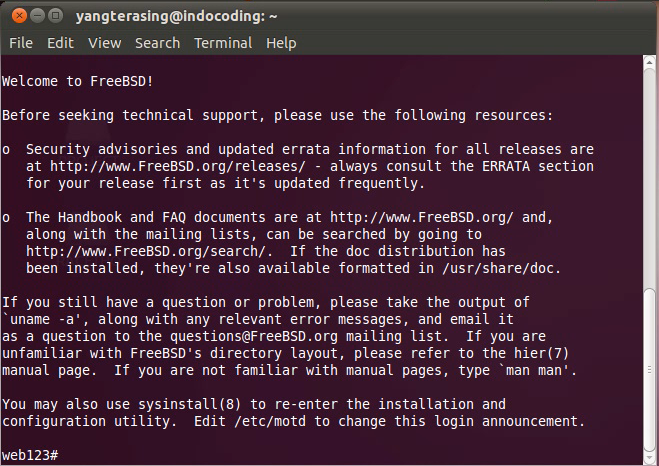
Dalam kerja praktek ini hanya digunakan backdoor phpshell yaitu c99 yang sudah dimodifikasi untuk server lama (pentesting pertama). Gambar backdoor c99 bisa di lihat pada gambar 3.6, dan untuk server yang baru ini FreeBSD 8.2 backdoor yang digunakan adalah b374k shell yang merupakan php shell karya anak indonesia bisa dilihat pada gambar 3.7 dan 3.8. Selain backdooring menggunakan phpshell bisa juga menanamkan public key kedalam home root server UIN Sunan Kalijaga seperti terlihat pada gambar 3.16 sehingga attacker bisa langung login root di server web UIN Sunan Kalijaga tanpa menggunakan password. Pada gambar 3.17,3.18,3.19 adalah bukti bahwa attacker mengakses root tanpa login password yaitu menggunakan rsa public key. Sebenarnya teknik ini juga bisa digunakan untuk pengamanan ssh, dengan menggunakan public key hanya komputer yang sudah mengupload public keynya di home server yang bisa login ke server.



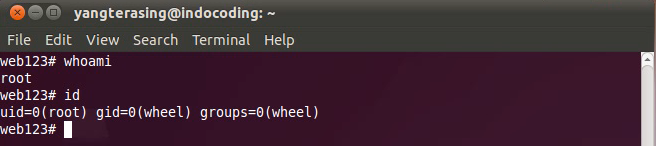
Gambar 3.16. Id\_rsa\_pub attacker yang ada di home root server UIN Sunan Kalijaga (pentesting I)



Gambar 3.17. Login ssh user root di server web UIN Sunan Kalijaga (pentesting I)



Gambar 3.18. Berhasil login user root di server web UIN Sunan Kalijaga menggunkan RSA key



Gambar 3.19. Whoami, menunjukkan bahwa web123 adalah user root

*Tips:*

*Root adalah user tertinggi dalam sistem keluarga \*NIX, jika seorang attacker sudah berhasil mendapatkan akses root, maka attacker sudah mempunyai hak akses tertinggi terhadap sistem, attacker bisa melakukan apa saja, termasuk mengubah konfigurasi sistem, bahkan meghapus file-file sistem atau memformat hardisk server dan sebagainya. Gunakan versi sistem operasi dan kernel yang memang benar-benar sudah stable, kalaupun menggunakan versi current atau rillis, admin harus selalu update informasi dan pathching jika ada bug.*

*FreeBSD 8.0, 8.2 yang digunakan sebagai sistem operasi server web UIN Sunan Kalijaga keduanya mempunyai bug.Versi FreeBSD paling STABLE adalah FreeBSD 6.2, FreeBSD merupakan proyek riset jadi sangat maklum jika ketika release masing sering ditemukan banyak sekali bug.*

1. **Covering Tracks**

Sebuah sistem pasti mempunyai log, log adalah sebuah file yang merekam apa saja yang dilakukan oleh sistem atau misalanya ketika terjadi error dalam sistem maka akan disimpan dalam error log.

Pada kerja praktek yang kami lakukan jelas kami tidak menghapus log, karena log ini nanti yang bisa kami jadikan sebagai bukti untuk ditunjukkan pada admin server web yang bersangkutan. Tapi ketika posisi kami memang sebagai attacker di suatu server jelas untuk mempertahankan akses kami pada server target dan tentu supaya tidak diketahui oleh admin kami harus berusaha dengan sekeras-kerasnya untuk membuat backdoor yang sulit terdeteksi dan pasti kami akan menghapus seluruh jejak-jejak yang sudah kami lakukan.

Biasanya file log dalam sistem operasi lunux, BSD dan keluarganya file log bisa dilihat pada /var/log/auth.log atau /var/log/apache2/access.log.

*Tips:*

*Tugas seorang network administrator adalah mengamati log, semua aktifitas dari sistem dan juga client yang mengakses server akan selalu tercatat dalam log misalnya seperti adakah yang mencoba bruteforce, adakah client / user yang mengakses file-file aneh berextensi php, dan sebagainya semuanya harus diwaspadai.*

*Bila ada file mencurigakan terutama berextensi php coba dibuka kemudian bila ternyata isinya dienkripsi coba untuk didekripsi bisa jadi itu adalah web shell atau backdoor.*

*Gunakan maldetect untuk pendeteksi malware, virus, shell, rootkit, backdoor dan sebagainya, maldetect adalah antivirus yang berjalan di sistem operasi Linux, BSD dan keluarganya. Aplikasi ini bisa mengenali php web shell, backdoor, spyware, Trojan dan berbagai jenis spyware.*

1. **Denial Of Service**

DOS atau Denial Of Servis adalah tindakan dari seorang attacker yang sudah putus asa karena gagal mendapatkan akses ke dalam sistem.

DOS sendiri merupakan tindakan merequest page yang secara terus menerus dan request tadi dikakukan oleh bot aplikasi yang ditanam attacker di dalam server lain. DOS atau DDOS jika dilakukan oleh banyak zombie komputer bisa menyebabkan sebuah sistem down/mati bahkan bisa menimbulkan kerusakan hardware karena beban kerja komputer jelas akan naik ketika request terlalu banyak yang liyani akhirnya komputer akan hang/freez, panas dan menyebabkan kerusakan hardware.

**BAB IV PENUTUP**

**4.1 Kesimpulan**

1. Saat ini website dan server web UIN Sunan Kalijaga masih mempunyai bug/celah yang sangat banyak (seperti yang sudah disampaikan pada bab pembahasan) yang harus di lakukan adalah membersihkan seluruh file yang mencurigakan (phpshell) kemudian menutup semua celah sesuai dengan yang rekomendasi diatas kemudian mengepatch/menambal bug yang ada dalam sistem operasi yang digunakan.
2. Server web UIN saat ini menggunakan sistem operasi FreeBSD 8 di akhir maret 2012 di ganti server dengansistem operasi FreeBSD8.2 yang keduanya ternyata mempunya bug/celah yang bisa menjadikan hacker/attacker mendapatkan akses tertinggi yaitu root, sebaikanya segera di patch, atau mengambil jalan aman dengan menggunakan sistem operasi yang stabil dan tidak mengandung bug/celah.
3. Semua celah itu berbahaya, baik itu celah di website yang timbul dari kesalahan coding, kesalahan atau ketidakpahaman dalam konfigurasi jaringan atau mungkin sistem operasi/aplikasi yang di gunakan mengandung bug/celah oleh karena itu sebagai seorang admin server harus mengantisipasi hal ini.
4. Untuk meminimalisir kesalahan coding yang bisa menimbulkan bug/celah seorang admin web dan admin server seharusnya melakukan testing dulu di komputer local kemudian ketika memang sudah bebas dari celah/bug website bisa di onlinekan
5. Tidak ada sistem yang benar-benar aman dan sempurna, sebagai seorang admin sebuah server hanya bisa mengupayakan untuk mengamankan server dengan semaksimal mungkin dan mengurangi risiko-risiko terbentuknya celah/bug yang bisa dimasuki oleh hacker.

**LAMPIRAN**

Lampiran 1 Script downlot.php yang ada di website PKSI UIN Sunan Kalijaga

Lampiran 2 Local root exploit FreeBSD *mbufs() sendfile cache poisoning local privilege escalation*

Lampiran 3 File local root ProFTPd

Lampiran 4 Table ringkasan bug list

Lampiran 1 Script downlot.php yang ada di website PKSI UIN Sunan Kalijaga

*<?php*

*include "config/koneksi.php";*

*$direktori = "files/"; // folder tempat penyimpanan file yang boleh didownload*

*// $filename = $\_GET['file'];*

*$filename ="./"$\_GET['file'];*

*$file\_extension = strtolower(substr(strrchr($filename,"."),1));*

*switch($file\_extension){*

*case "pdf": $ctype="application/pdf"; break;*

*case "exe": $ctype="application/octet-stream"; break;*

*case "zip": $ctype="application/zip"; break;*

*case "rar": $ctype="application/rar"; break;*

*case "doc": $ctype="application/msword"; break;*

*case "xls": $ctype="application/vnd.ms-excel"; break;*

*case "ppt": $ctype="application/vnd.ms-powerpoint"; break;*

*case "gif": $ctype="image/gif"; break;*

*case "png": $ctype="image/png"; break;*

*case "jpeg":*

*case "jpg": $ctype="image/jpg"; break;*

*default: $ctype="application/proses";*

*}*

if ($file\_extension=='php'){

echo "<h1>Access forbidden!</h1>

<p>Maaf, file yang Anda download sudah tidak tersedia atau filenya (direktorinya) telah diproteksi. <br /> Silahkan hubungi <a href='mailto:redaksi@bukulokomedia.com'>webmaster</a>.</p>";

exit;

}

else{

mysql\_query("update download set hits=hits+1 where nama\_file='$filename'");

header("Content-Type: octet/stream");

header("Pragma: private");

header("Expires: 0");

header("Cache-Control: must-revalidate, post-check=0, pre-check=0");

header("Cache-Control: private",false);

header("Content-Type: $ctype");

header("Content-Disposition: attachment; filename=\"".basename($filename)."\";" );

header("Content-Transfer-Encoding: binary");

header("Content-Length: ".filesize($direktori.$filename));

readfile("$direktori$filename");

exit();

}

?>

Lampiran 4 Tabel ringkasan bug list

|  |  |
| --- | --- |
| **No** | **Bug** |
| 1. | **Celah di Web Application** |
|  | LFI di website PKSI |
|  | Page Admin tanpa session di semua template web  a) Tidak ada session di http://www.uin-suka.ac.id/index.php/access  b) Ada menu import file excel di http://www.uin-suka.ac.id/index.php/chapter  c) Editor tanpa session di <http://www.uin-suka.ac.id/index.php/ckeditor> |
| 2. | **Password lemah** |
|  | a). PKSI username :"abeng" password:"daru"  Walaupun menggunakan md5(one way encription) tetap saja mudah di crack jika password begitu mudah.  b ). Ssh brutforce dengan wordlist dari file passwd membuahkan hasil |
|  | c). Ternyata password ssh sama dengan password database. Password database jelas akan di tampilkan pada file koneksi.php, atau di database configuration CI. |
| 3. | **php.ini** |
|  | a). Safe mode off |
|  | b). Exec semua berjalan  Sehingga semuanya perintah sistem bisa di jalankan menggunakan php web shell termasuk connect back dan bind shell. |
|  | c). Attacker bisa leluasa *jumping* ke direktori mana saja yang disukainya, ini karena safe mode off dan semua exec php di jalankan. |
| 4. | **Database** |
|  | a). Sungguh hal yang kurang bijak jika database seluruh dosen dan karyawan UIN Sunan Kalijaga diletakkan dalam server web yang penuh celah seperti ini, dan itu terjadi di server UIN Sunan Kalijaga (pentesting I). |
|  | b). Password root mysql jelas-jelas di tampilkan dalam file koneksi php. |
| 5. | **Susunan Directory** |
|  | Susunan direktori dan file kurang begitu terstruktur, tidak layak jika folder-folder tersebut merupakan file-file instansi akademik |
|  | Penamaan file yang tidak terstruktur pula, contoh nama folder a dan sebagainya. |
|  | .htaccess tidak dimanfaatkan dengan sebaik-baiknya, sehingga sering direktori yang tidak mempunyai index ketika diakses akan menampilkan semua file yang ada didalamnya, bisa diatasi dengan menggunakan .htaccess atau selau menambahkan index disetiap direktori |
| 6. | **Sistem Operasi dan Kernel** |
|  | Server pertama FreeBSD 8.0 dan server yang kedua FreeBSD 8.2 kedua duanya mempunyai bug yang cukup fatal. |