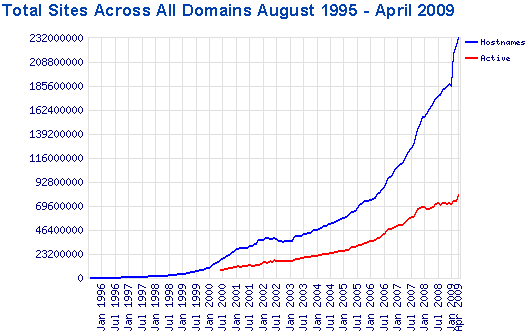
**BAB I PENDAHULUAN**

**1.1 Latar Belakang**

Sekarang adalah era digital dimana manusia sudah tidak bisa dipisahkan lagi dengan dunia maya/internet. Salah satu bagian dari internet adalah website. Data dari Monemy.com bahwa saat ini jumlah website di dunia sudah mencapai 232.000.000. Berikut grafik jumlah website dari tahun 1995 sampai 2009.



Gambar 1. Pertumbuhan Jumlah website di dunia

Hal itu dikarenakan saat ini tidak hanya instansi pemerintah atau perusahaan yang mempunyai website, kita pribadi saja bisa mempunyai website apalagi dengan adanya teknologi blog dan CMS. Dengan menggunakan blog atau CMS kita bisa membuat website hanya dengan melakukan beberapa klik. Website menjadi begitu popular karena website mudah dibuat dan banyak menawarkan keuntungan. Dengan menggunakan website kita bisa menampilkan informasi yang dapat diakses oleh siapa saja, dimana saja dan kapan saja. Bahkan saat ini banyak pula perusahaan-perusahaan yang menyediakan transaksi melalui website mereka. Website telah dijadikan satu bagian penting untuk promosi atau layanan kepada pelanggan. Berkaitan dengan perkembangan ini, maka keamanan website mulai menjadi masalah penting. Lebih lagi dengan kemunculan website-website *e-commerce*. Demikian juga dengan penggunaan website oleh perusahaan-perusahaan sebagai tempat promosi dan layanan mereka yang tentunya membutuhkan jaminan keamanan. Keamanan website menjadi lebih lagi dibutuhkan dengan adanya kasus-kasus pencurian kartu kredit (*carding*) melalui website, penipuan (*scam*), virus, worm, malware, perusakan website (*deface*) dan lain-lain. Karena pentingnya masalah kemanan ini maka bagi perusahaan atau seseorang yang ingin mengembangkan websitenya sudah selayaknya memperhatikan hal ini. Apalagi jika website yang akan dikembangkan itu berhubungan dengan transaksi atau bisnis, maka keamanan yang baik pada website kita akan menghindarkan kerugian yang jumlahnya mungkin bisa sangat besar, baik secara material maupun non-material.

Sebuah prestasi yang cukup bagus yang dimiliki Negara kita yaitu Indonesia menempati ranking 10 besar untuk kasus cybercrime di dunia. Dibawah ini saya kutipkan berita dari kompas.com.

*“JAKARTA, KOMPAS.com - Ada kabar tak mengenakkan datang dari Symantec terkait hasil monitornya tentang aktivitas ancaman di Internet yang dipaparkan di hotel Grand Hyatt, Jakarta kemarin (29/4). Indonesia kini sudah termasuk dalam peringkat Top 10. Begitu tercantum dalam laporan bertajuk Internet Security Threat Report XV perioda Januari – Desember 2009.”* Ditulis oleh Wiek pada hari Jumat, 30 April 2010 pukul 10:24 WIB.

*Sumber: http://tekno.kompas.com/read/2010/04/30/10240384/Peringkat.Indonesia.di.CyberCrime.Naik*

Apa dampak dari prestasi tersebut?. Jelas prestasi ini menjadikan Indonesia menjadi negara yang rawan untuk bisnis *e-commers* yang jelas membutuhkan transaksi online. Sehingga banyak perusahaan, penjual atau penyedia jasa asing enggan mengijinkan transaksi ke Indonesia bahakan yang tak segan-segan untuk *memblacklist* indonesia. Dengan kondisi seperti ini jelas sangat merugikan bagi Indonesia.

Sebuah aksi pencurian kartu kredit *(carding),* pencurian data dan sebagainya, itu semua berawal dari suatu celah/bug yang ada pada website atau server yang bersangkutan. Jika seorang attacker sudah bisa masuk dalam sebuah server dan dia sudah memperoleh akses untuk membuka, mengambil, atau menulis data itulah malapetaka. Attacker bisa dengan mudah mengubah informasi yang ada sehingga pembaca website/pelanggan akan tertipu. Atau kalau yang dibobol oleh attacker itu adalah sebuah server *e-commers* jelas ini lebih dari malapetaka karena attacker bisa mengambil seluruh data *customer* yang pernah bertransaksi di website tersebut dan yang pasti di sana pasti ada data-data penting seputar kartu kredit yang seharusnya hanya boleh di ketahui oleh orang yang mempunyainya.

Tidak cukup sampai kasus pencurian kartu kredit (*carding*). Indonesia juga dikenal sarang peretas website (*defacer*), seperti kasus yang terakhir ini adalah website polri yang di hack dan diubah tampilanya (*deface*). Dibawah ini saya kutipkan berita dari kompas.com mengenai kasus tersebut.

*"Saya menyayangkan sikap-sikap yang terlalu mengabaikan bahaya serangan yang terjadi di dunia maya dan hal ini sudah merupakan masalah serius di seluruh dunia," ujar Tifatul dalam siaran pers yang diterima Kompas, Selasa (19/7/2011).*

*Ia mengatakan, semua pihak harus menyadari dan siaga, serta membangun sistem pertahanan cyber. Ini tanggung jawab kita semua," ujarnya.*

*Dalam penelusuran Kemkominfo, masih banyak lembaga dan kementerian negara yang belum membangun sistem keamanan komputer yang baik, bahkan cenderung mengabaikan aspek keamanan sistem informasi ini.*

*Tifatul juga mengingatkan bahwa serangan dunia maya dapat berskala yang lebih luas karena tanpa batas. Lemahnya pengamanan dapat mengakibatkan kejadian fatal. Di tingkat negara, bisa mengakibatkan lumpuhnya sistem komputer pemerintah dan lembaga penting lainnya.* Ditulis oleh Imam Prihadiyoko pada hari Selasa, 19 Juli 2011 pukul 13:05 WIB

*Sumber:*

*http://nasional.kompas.com/read/2011/07/19/13054473/Tifatul.Website.Pemerintah.Gencar.Di.Hack*

Walaupun pemerintah indonesia sudah mengupayakan pencegahan dengan membuat undang-undang IT tetap saja mencari pelaku/penjahat dunia maya itu sulit di lakukan. Semua itu karena dunia maya/internet 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.

Tidak hanya website pemerintah, website-website pendidikan pun juga terancam diserang oleh hacker baik dari dalam negeri maupun luar negeri. Seperti bisa kita lihat di [www.zone-h.org](http://www.zone-h.org) yaitu website untuk mensubmit hasil dari *deface-an* suatu website, di website tersebut banyak sekali 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). Saya mencoba mencari domain UIN Sunan Kalijaga di situs tersebut dan ternyata 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.



Gambar 2. Website UIN Sunan Kalijaga pernah di deface, archive di zone-h

Dan yang lebih miris lagi 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 punya maksud jahat bisa mengubah informasi yang ada pada website tersebut, tentu ini akan sangat membahayakan. Oleh karena itu saya mencoba untuk kerja praktek di PKSI yaitu penetration testing server web dan mencari celah/bug sebanyak-banyaknya kemudian mencoba untuk memberikan solusi dan rekomendasi. Semoga bisa memberikan banyak masukan untuk keamanan website dan server web di kampus UIN Sunan Kalijaga.

**1.2 Batasan Kerja Praktek**

Batasan kerja praktek yang saya lakukan adalah hanya penetration testing 1 server yang merupakan host dari domain utama website UIN Sunan Kalijaga. Tapi karena 1 server itu tidak hanya di gunakan untuk website UIN Sunan Kalijaga melainkan juga sebagai host website semua Fakultas di UIN Sunan Kalijaga jadi tentu semua isi yang ada pada server web tersebut adalah objek pekerjaan saya.

Yang saya uji keamanannya meliputi web application (php), system operasi yang di gunakan server dan service yang berjalan pada server.

**1.3 Tujuan Kerja Praktek**

1. Mencari sebanyak mungkin bug/celah dalam website UIN Sunan Kalijaga.
2. Berusaha untuk mendapatkan akses tertinggi yaitu root di server UIN Sunan Kalijaga.

**1.4 Manfaat Kerja Praktek**

1. Laporan Kerja Praktek ini bisa digunakan sebagai acuan pembenahan celah/bug di server Web UIN Sunan Kalijaga.
2. Dalam laporan kerja praktek ini saya juga memberikan solusi/*patch* dan rekomendasi untuk menutup celah/bug yang ada baik di sisi web application maupun server web.

**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.

*sumber: http://pksi.uin-suka.ac.id/statis-4-tentangpksi.html*

**2.2 Ruang Ligkup Kerja Praktek.**



Gambar 3. Rapat Ketua dan para devisi PKSI

Staf pada UPT. PKSI terdiri atas:

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

2. Divisi:

Divisi Infrastruktur: Hendra Hidayat, S.Kom.

Anggota: Rahmadhan Gatra, ST

Divisi Pengembangan Sistem Informasi: Mustaqim, MT.

Anggota:

Salim Athari, S.Kom

Adi Wirawan, S.Kom

Prihanto Dwi Rahmanto, S.Kom.

Divisi SDM: Ratna Windah Lestari, SIP

Anggota: Rohyati, S.Ag.

Divisi Media: M. Arif Wibisono

Anggota:Daru Prasetyawan, ST

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**

1. Kondisi Tempat Kerja

Kondisi tempat kerja instansi yaitu PKSI Uin sunan kalijaga cukup bagus. Lantai 1 PKSI adalah tempat layanan dan tempat admin website bekerja yaitu mas hendra dan juga tempat semua server kampus UIN SUnan Kalijaga. Di Awal saya Kerja Praktek saya biasanya bekerja di Lantai satu bersama dua teman saya yang sedang KP juga. Saat ini di Lantai satu memang penuh dengan anak-anak SMK yang sedang PKL jadi memang agak penuh.

Untuk Lantai II adalah ruang multimedia, saya malah lebih kerasan di lantai II ini, karena memang enak, nyaman dan penuh dengan mac. Lantai III dibagi menjadi dua ruangan, ruangan yang pertama dipakai oleh banyak pegawai PKSI dan sering di pakai untuk seminar juga, untuk ruang yang kedua biasanya di pakai untuk rapat.

Untuk kondisi tempat kerja saya rasa bagus, karena memang dari segi komputer yang digunakan cukup update.

1. Kondisi SDM di PKSI UIN Sunan Kalijaga

Kondisi SDM di PKSI menurut saya sedikit memperihatinkan, bukan dari kemampuan pagawai PKSI tapi dari jumlah pegawai PKSI yang menurut saya terlalu sedikit. Dengan SDM yang sangat terbatas PKSI harus melayani semua urusan di kampus UIN sunan kalijaga yang berhubungan dengan layanan IT.

Mungkin juga karena hal ini sehingga server web di UIN tidak begitu terpelihara. Seperti yang kita lihat di atas untuk devisi Infrastruktur hanya terdiri dari Mas Hendra dan Mas Gatra. Tapi untuk kinerja SDM di PKSI saya tahu mereka sudah bekerja keras dan maksimal.

**3.2 Kegiatan KP**

Metode standar penetation testing adalah:

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

Berikut akan saya uraikan tahap-tahap pentesting yang saya lakukan beserta *screenshootnya.*

1. **Footprinting**

Footprinting adalah proses menggali informasi sebanyak-banyaknya dari target. Hasil Footprinting yang saya lakukan sbb:

1. Mengecek IP dari server target.

IP Server 172.16.4.201 yang sejak tanggal 20 maret sudah diganti menjadi 10.0.8.120.

1. Reverse IP domain check

Reverse IP domain check adalah melihat website apa saja yang ada dalam host tersebut. Contoh saya menggunakan aplikasi di [www.yougetsignal.com](http://www.yougetsignal.com) kemudian menu revers IP domain check. Seperti terlihat pada Gambar 4.



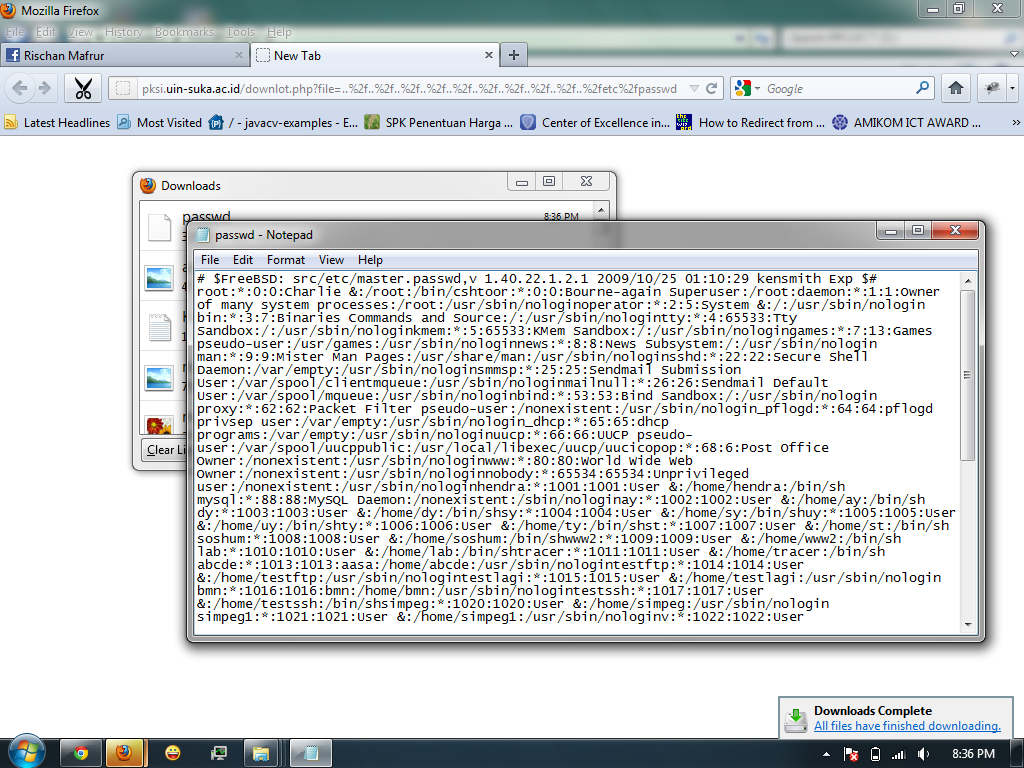
Gambar 4. Reverse IP Domain Check domain www.uin-suka.ac.id

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

Website dengan domain <http://pksi.uin-suka.ac.id> menggunakan CMS lokomedia yang rawan akan bug/celah. Dan ternyata saya menemukan celah di dalamnya yaitu LFI (Local File Inclusion). LFI merupakan bug yang bisa membuat seorang attacker bisa mengambil file yang berharga dari dalam server. Dengan bug LFI ini saya bisa mendownload suatu file passwd dari server dengan menggunakan celah ini 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>

Perintah tersebut adalah perintah untuk mendownload file passwd yang ada dalam server dan ternyata perintah tersebut bekerja dengan baik. Seperti telihat pada Gambar 5.



Gambar 5. Download file passwd dari server UIN Sunan Kalijaga

File passwd adalah file yang sangat berharga di system operasi Linux, BSD dan keluarganya. File ini adalah file yang hanya bisa di *write* oleh root tapi bisa di baca oleh siapa saja dan file berisi list user apa saja yang ada dalam server. Dengan menggunakan file ini itu sudah mengurangi setengah dari pekerjaan attacker karena dengan melihat file ini attacker menjadi tahu user apa saja yang ada dalam server, list user tadi bisa di gunakan sebagai wordlist username untuk bruteforce. Dan yang lebih parahnya biasanya admin memberikan password yang mudah di tebak.

Bug LFI ini sebenarnya berasal dari kesalahan script yang ada pada file downloat.php. File downloat.php bisa di lihat di lampiran. Kesalahanya berada pada variable $filename

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

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

Variable filename tidak di filter dengan bagus jadi client bisa menginputkan semua karakter ke dalam URL, jelas ini sangat berbahaya.

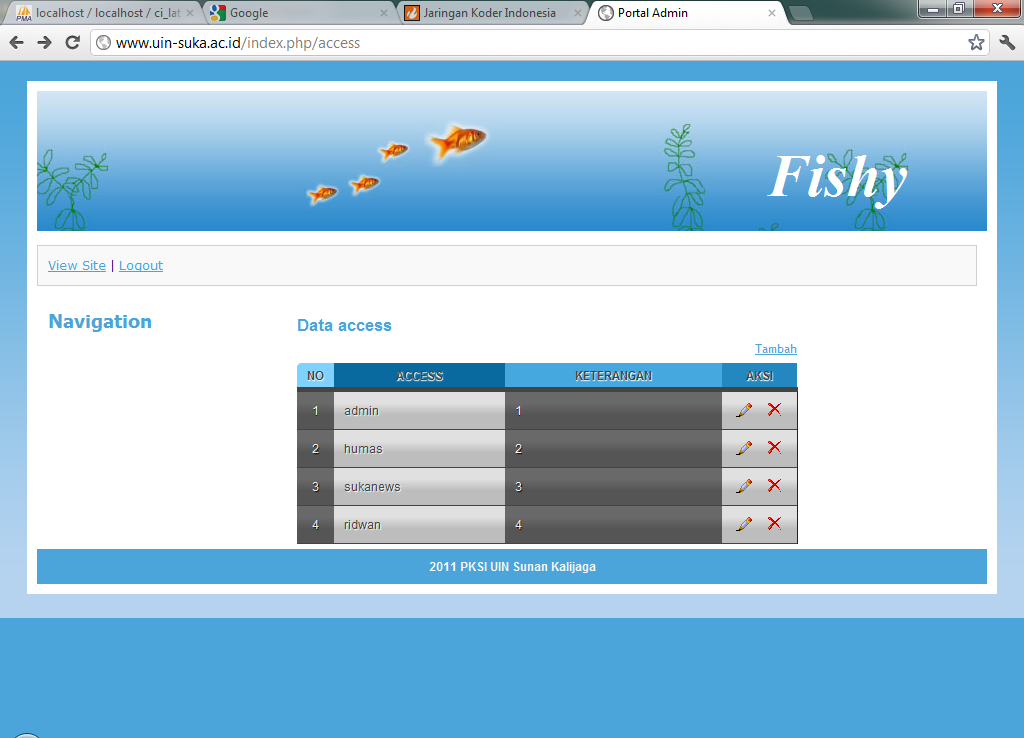
1. Multi Bug di Semua Website

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

Katika saya menguji keamanan di website utama UIN Sunan Kalijaga saya cukup kaget karena menemukan beberapa bug yang cukup berbahaya.

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 kalau untuk bug yang pertama jelas ini sangat fatal. Pada bug yang pertama ini jika kita mengakses URL <http://www.uin-suka.ac.id/index.php/access> kita langsung akan di hadapkan page admin tanpa login, kita bisa mengedit hak akses user bahkan kalau dulu saya bisa menambah user. Seperti terlihat pada gambar 6.



Gambar 6. Masuk page admin tanpa menggunakan session di website UIN Sunan Kalijaga

1. **Scanning Fingerprinting**

Saat saya melakukan footprinting saja sudah menemukan banyak sekali celah/bug bahkan langsung bisa mempunyai akses admin ke website UIN Sunan Kalijaga.

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

1. Analisis dan scanning sistem operasi yang digunakan.
2. Analisis dan scanning service apa saja 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 saya sebagai berikut:



Gambar 7. Scanning Fingerprinting menggunakan php script.

**Versi Sistem Operasi**

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

kemudian tanggal 20 maret di pindah server dan system operasinya diganti menjadi

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

**Web Server**

Apache/2.2.17 (FreeBSD) mod\_ssl/2.2.17 OpenSSL/0.9.8q DAV/2 PHP/5.3.5 with Suhosin-Patch webmaster@uin-suka.ac.id

**About PHP**

PHP safemode OFF

PHP module 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

**About Hash**

Hash support enabled

Hashing Engines

md2 md4 md5 sha1 sha224 sha256 sha384 sha512 ripemd128 ripemd160 ripemd256 ripemd320 whirlpool tiger128,3 tiger160,3 tiger192,3 tiger128,4 tiger160,4 tiger192,4 snefru snefru256 gost adler32 crc32 crc32b salsa10 salsa20 haval128,3 haval160,3 haval192,3 haval224,3 haval256,3 haval128,4 haval160,4 haval192,4 haval224,4 haval256,4 haval128,5 haval160,5 haval192,5 haval224,5 haval256,5

**MySQL & etc**

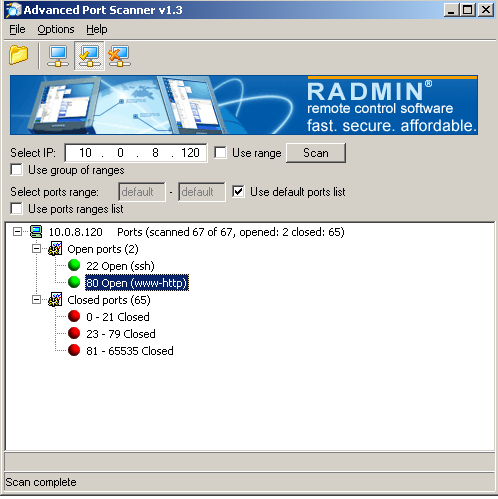
mysqlnd 5.0.7-dev - 091210 - $Revision: 304625 $

OpenSSL support enabled

OpenSSL Library Version OpenSSL 0.9.8q 2 Dec 2010

**Port scanning**

Untuk melihat port apa saja yang terbuka di Server UIN hanya dua port yang dibuka yaitu port 80 http dan port 22 ssh. Seperti pada gambar 8 sebagai berikut:

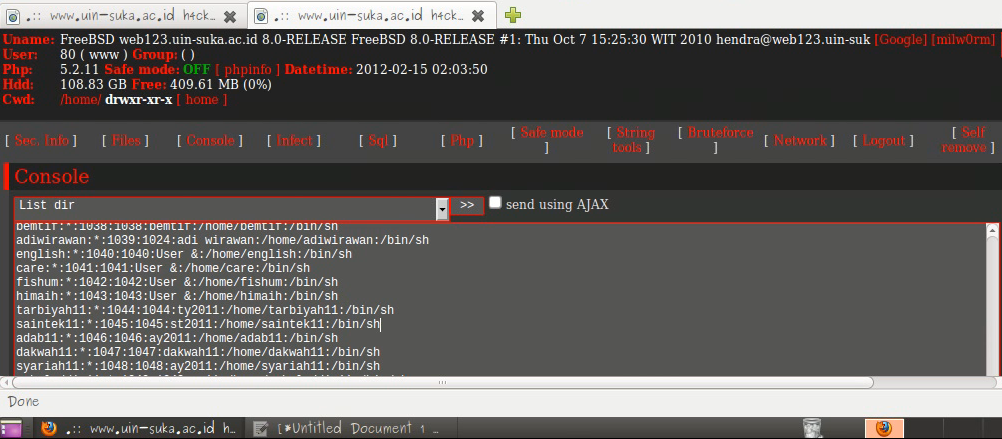


Gambar 8. Port scanning server web UIN Sunan Kalijaga menggunakan RADMIN tool

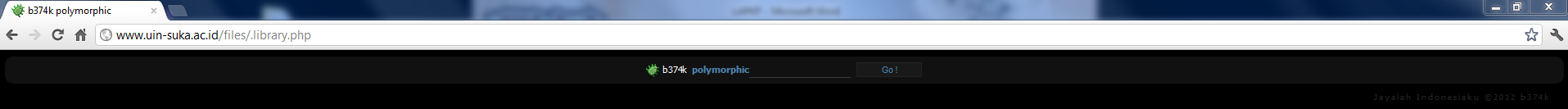
1. **Enumeration dan Gaining Access**

Metode *Enumeration* adalah mencari *poorly protected password* kemudian dilanjutkan dengan *Gaining Access* dan ternyata ketika saya melakukan footprinting saja saya sudah bisa menemukan page tanpa session yaitu bisa mengakses page admin tanpa login yaitu *Gaining Access*. Page admin tidakalah cukup, karena page admin hanya bisa melihat dan mengedit atau menambahkan berita, gambar dan lain-lain. Untuk melihat dan mengexploit server kita membutuhkan webshell. Dan ada bug yang cukup fatal yaitu image upload tanpa filtering. Jadi pada page upload image berita saya bisa mengupload file php kemudian saya bisa mengakses file php tersebut.

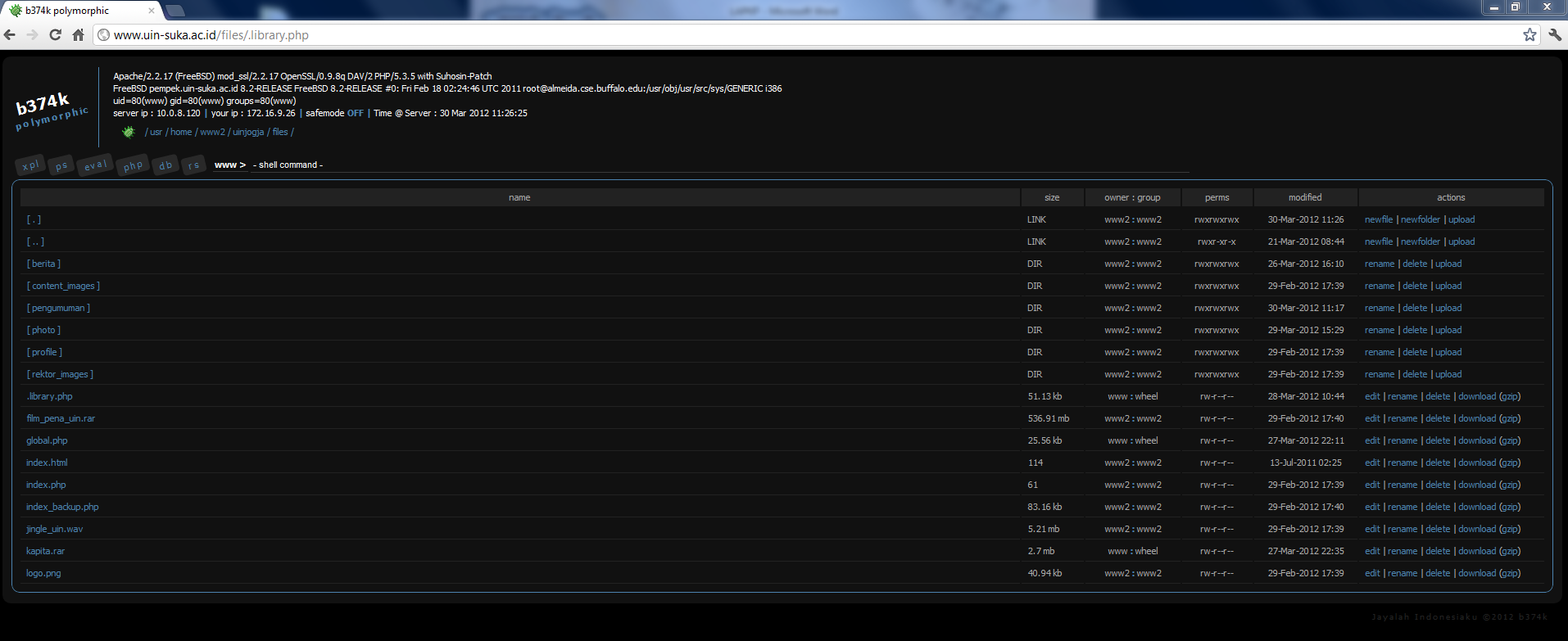
Gambar 9,10, dan 11 memperlihatkan php shell yang saya tanam dalam server web UIN Sunan Kalijaga.



Gambar 9. Tampilan PHP Shell yang saya tanam di server lama UIN Sunan Kalijaga (FreeBSD 8.0)



Gambar 10. Jendela login webshell yang saya tanam di server UIN Sunan Kalijaga sekarang (FreeBSD 8.2)



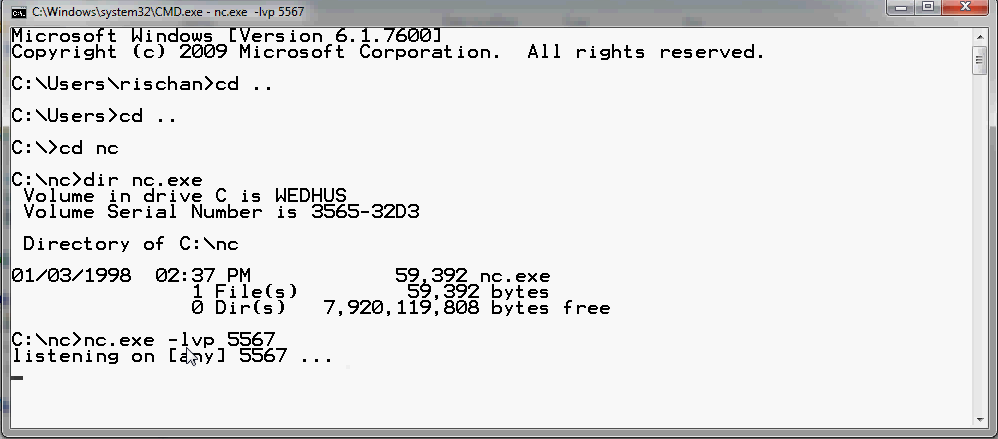
Gambar 11. Web Shell yang saya tanam di server web UIN Sunan Kalijaga sekarang (FreeBSD 8.2)

Ketika kita menggunakan php web shell kita bisa memasukkan perintah-perintah linux di dalamnya, tapi jelas sangat tidak nyaman karena kita tidak mendapatkan akses shell seperti ssh misalanya. Solusinya adalah kita melakukan backconnect1 atau Bind connection2. (catatan kaki).

Saya memilih Back connect, yang pertama saya lakukan adalah menjalankan *nc/ netcat* 3 (catatan kaki). Netcat kita jalankan di cmd dengan mengetikkan perintah sbb:

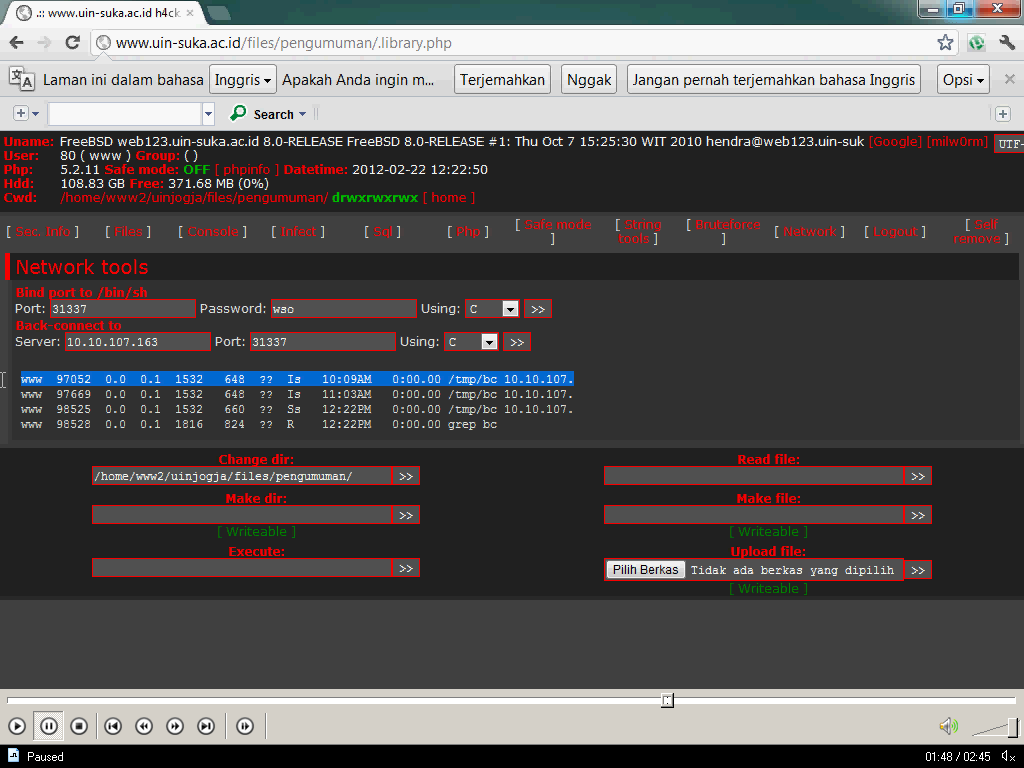
nc.exe –lvp 5567

parameter l adalah untuk listening, v untuk verbose (menampilkan kondisi yang terjadi saat itu), dan p adalah port, 5567 adalah port yang saya gunakan untuk melakukan back connect. Bisa di lihat di gambar



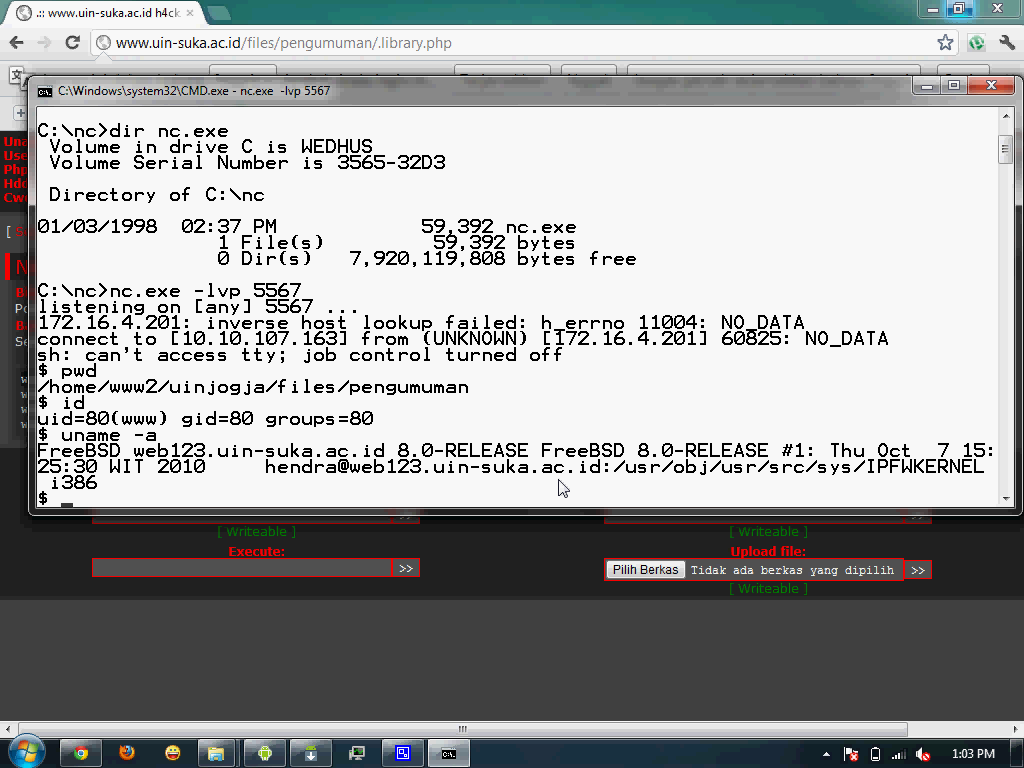
Gambar 12. Back connect menggunakan netcat

Setelah computer kita melakukan listening menggunakan netcat, saatnya menjalankan script back connect di server. Kita tidak perlu repot-repot mencari script back connect karena di dalam web shell biasanya script back connect sudah di sertakan. Begitu juga dengan web shell c99 yang saya gunakan, secript back connect ada di menu network. Jangan lupa untuk mengganti port sesuai dengan port yang sudah kita listen di netcat kita yaitu 5567. Seperti terlihat pada gambar 13.



Gambar 13. Menjalankan script back connect di server web UIN Sunan Kalijaga

Hasilnya bisa di lihat pada gambar 14 yaitu saya memperoleh akses shell menggunakan back connect. Pada gambar 14 setelah saya mendapatkan akses shell saya mencoba beberapa perintah shell seperti pwd, id, dan uname –a.

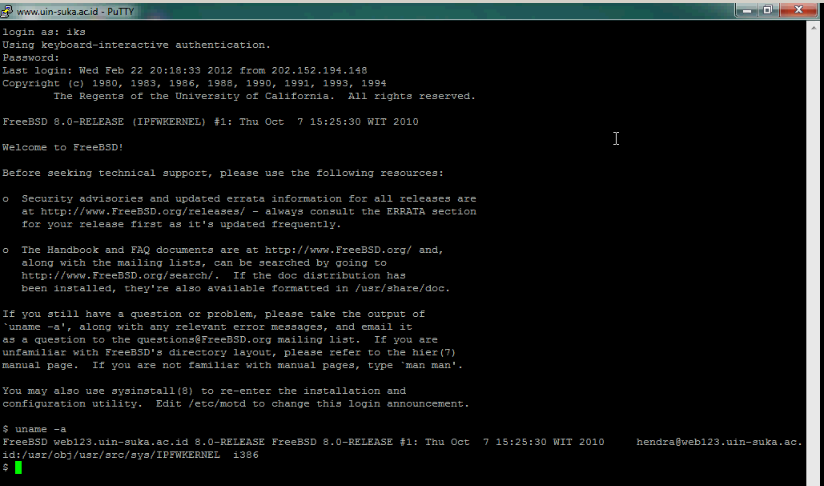


Gambar 14. Berhasil mendapatkan akses shell menggunakan back connect

Akses shell menggunakan back connect tenyata belum membuat saya puas, akhirnya saya mencoba untuk menggunakan file passwd yang saya peroleh untuk mengelist user yang ada kemudian mencoba untuk *membruteforce* ssh.

Dan ternyata usaha saya tidak sia-sia bruteforce yang saya lakukan membuahkan hasil yaitu saya mendapatkan akses ssh user “iks” dengan password “iksiksiks” tentu password yang begitu mudah untuk di brutefoce dengan userlist yang saya dapatkan dari bug LFI yang sudah saya temukan sebelumnya.

Gambar 15. Menunjukkan saya login ssh menggunakan user “iks” dan password “iksiksiks” dan akhirnya saya memperoleh akses ssh ke server walaupun masih sebagai user biasa.

. 

Gambar 15. Saya berhasil login ssh menggunakan user dan password yang saya dapatkan dari bruteforce

1. **Privilege Escalation**

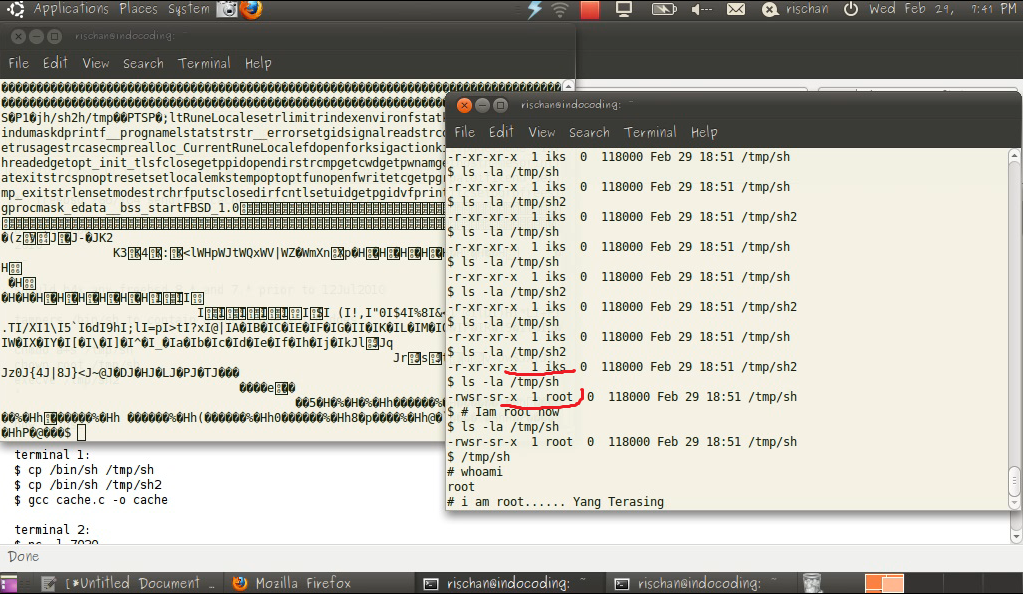
Pada tahap sebelumnya *enumeration dan gaining access* saya sudah berhasil memperoleh akses ssh tapi masih sebagai user biasa dan tentu tidak bisa menggunakan perintah “su” untuk menjadi root/ superuser.

Pada tahap privilage escalation ini saya berusaha mencari exploit baik itu remote exploit atau local exploit yang bisa menjadikan saya mempunyai akses tertinggi dalam server yaitu root.

Untuk pentesting server sebelum tanggal 20 Maret 2012 server UIN Sunan Kalijaga masih menggunakan sistem operasi FreeBSD 8 dan saya menemukan local root exploit yang berhasil saya jalankan di server web UIN Sunan Kalijaga sehingga saya bisa memperoleh akses root. Local root exploit itu adalah

FreeBSD mbufs() sendfile cache poisoning local privilege escalation exploit that throws a setuid shell in /tmp. Works on 7.x and 8.x builds prior to 12Jul2010. Untuk cara bagaimana saya melakukan local root exploit ini bisa kita lihat di video demo yang sudah saya buat. Yaitu di <http://youtube.com/sdad>.

Pada Gambar 16 telihat saya berhasil mendapatkan akses root server web UIN Sunan Kalijaga.



Gambar 16. Saya berhasil mendapatkan akses root di server menggunakan local root exploit

1. **Pilfering**

Pilfering adalah akses dengan user legal supaya tidak di ketahui oleh admin yang sebenarnya. Semua tahap-tahap tadi yang saya lakukan sebenarnya juga 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 tanggap dan mengerti masalah hal seperti ini tentu saya sebagai attacker santai-santai saja.

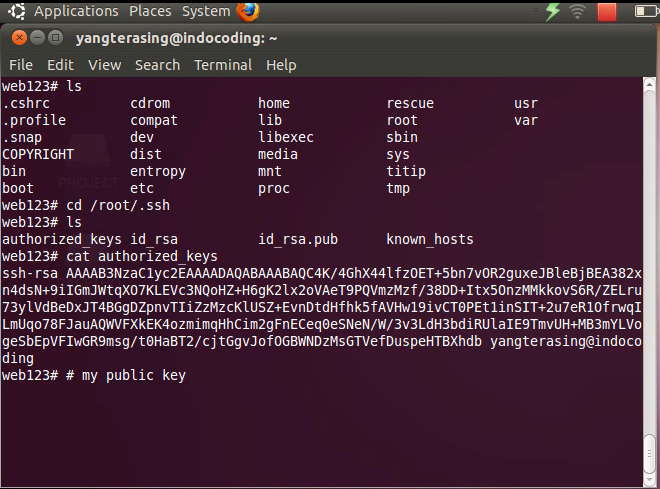
Dalam sistem operasi FreeBSD yang diijinkan untuk menjalankan perintah su hanyalah user yang berada dalam group wheel, sehingga dalam tahap ini saya menjadikan user fishum menjadi group wheel kita bisa mengedit file di /etc/group dan menjadikan fishum anggota dari group wheel. Tapi yang saya lakukan ini sama saja, saya tidak mengetahui password root yang sebenarnya walaupun saya bisa mengakses root melalui exploit /tmp/sh yang saya punyai. Sebenarnya saya bisa mengganti password root dari server tapi itu merupakan tindakan yang melanggar etika dan sangat mengundang risiko. Dan saya berpikir untuk menggunakan cara lain yaitu backdooring. Backdooring bisa dilakukan dengna berbagai cara seperti ssh backdoor yang langsung ke user root, crontab bindshell, atau karena saya tahu admin kurang begitu tanggap saya menanan public key komputer saya ke dalam server di home rootnya sehingga saya bisa langsung akses root server melalui komputer saya tanpa login password jadi dengan demikian walaupun saya tidak tahu password root saya bisa langsung mengakses root tanpa repot-repot menjalankan exploit saya dan tentunya tanpa harus mengganti password root sang admin.

1. **Backdooring**

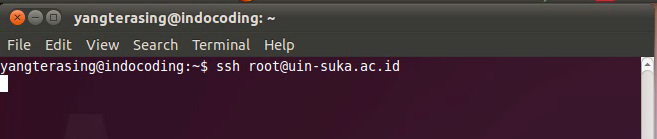
Backdooring adalah kegiatan untuk menanam sebuah pintu belakang, sehingga ketika kita ingin mengakses ke server kita tidak perlu repot-repot seperti ketika awal mencari bug/celah kemudian mengexploitnya. Dalam tahap backdooring ini juga tergantung dengan situasi dan kondisi. Seperti yang saya sampaikan diatas kalau sang admin kurang begitu peduli atau kurang tahu dalam hal keamanan, backdooring, webshell dan kawan-kawannya jelas kita tidak perlu susah-susah menanam rootkit yang bisa kita akses, atau mensetting crontab untuk connect pada host kita setiap hari apa pukul berapa, semuannya jelas tergantung kondisi target.

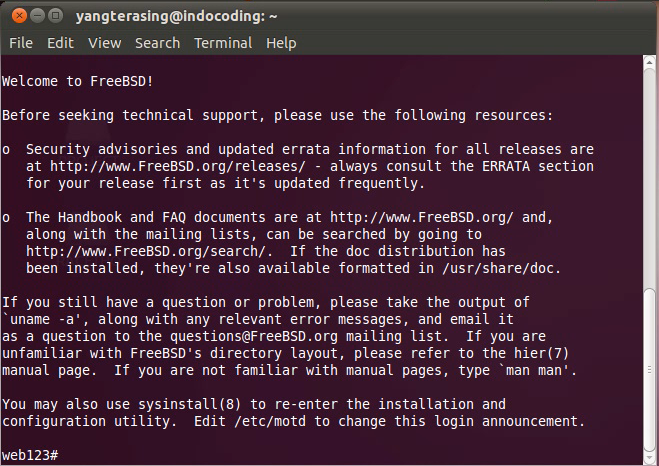
Dalam kerja praktek ini saya hanya menggunakan backdoor phpshell yaitu c99 yang sudah saya modifikasi untuk server lama, dan untuk server yang baru ini FreeBSD82 saya menggunakan phpshell b374k yang merupakan hasil kreasi dari anak bangsa yang mendunia. Backdoor webshell saya sudah saya tampilakan di gamabar 9,10 dan 11 di tahap gaining access.

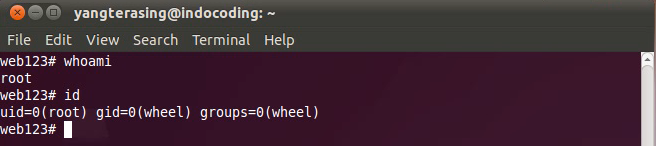
Selain backdooring menggunakan php web shell saya juga menanamkan public key id rsa saya kedalam home root server UIN Sunan Kalijaga seperti gambar 17 sehingga saya bisa langung login root di server web UIN Sunan Kalijaga tanpa password.



Gambar 17. Id\_rsa\_pub saya copikan ke home root server UIN Sunan Kalijaga







Sekali lagi saya tekankan untuk masalah backdooring ini perlakuan terhadap server tergantung dengan kondisi target. Kalau admin server cepat tanggap seperti yang pernah saya lakukan ketika pentesting sebuah server di Jakarta saya menggunakan sshdoor. Saya menginstall sshdoor dalam server dan menjalankan sshdoor ini sebagai *daemon* yang tidak diketahui oleh admin. Atau saya juga pernah menggunakan configurasi crontab agar setiap pukul 10 hari sabtu server listening untuk IP komputer saya dan saya langsung otomatis bisa login ke server. Tapi itu semua tidak saya lakukan di Kerja Praktek penetration testing di server web UIN Sunan Kalijaga ini karena semuanya tergantung dengan kondisi target.

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

Biasaya file log dalam system operasi lunux, BSD dan keluarganya file log bisa kita lihat pada /var/log/auth.log atau /var/log/apache2/access.log.

1. **Denial Of Service**

DOS atau Denial Of Servis adalah tindakan dari seorang attacker yang sudah putus asa melakukan serangan untuk 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 akhirnya akan hang/freez dan bisa panas dan menyebabkan kerusakan hardware.

Jelas dalam Kerja Praktek saya hal ini tidak saya lakukan, tujuan KP saya adalah mencari bug/celah sebanyak-banyaknya kemudian mencoba untuk mendapatkan akses tertinggi dalam server yaitu root. Selain itu di bab rekomendasi sudah saya sertakan rekomendasi beserta patch untuk menambal beberapa celah yang ada dalam website maupun sistem operasi.

**List Bug/Celah di server web UIN Sunan Kalijaga**

|  |  |
| --- | --- |
| **No** | **Bug** |
| 1. | **Celah di Web Application** |
|  | LFI ada 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 yang sangat 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 |
| 4. | **Database** |
|  | a). Sungguh hal yang kurang bijak jika database seluruh dosen dan karyawan UIN Sunan Kalijaga di letakkan dalam server web yang penuh celah seperti ini, dan itu terjadi di server UIN Sunan Kalijaga. |
|  | 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 |
| 6. | **Sistem Operasi dan Kernel** |
|  | Server pertama FreeBSD 8.0 dan server yang kedua FreeBSD 8.2 kedua duanya mempunyai bug yang cukup fatal. |

Table . Table list bug/celah di server web UIN Sunan Kalijaga

**3.3 Rekomendasi**

1. Web Application seharusnya di test terlebihdahulu sebelum di onlinekan.
2. Satu server sebaiknya jangan digunakan untuk banyak website, bisa di gunakan banyak website dengan syarat proteksi file dan konfigurasi php.ini yang bagus sehingga jika ada attacker masuk dalam satu website dia tidak bisa melakukan *jumping* ke home user lain(website lain yang ada dalam satu server).
3. Hati-hati penggunaan variable dalam php atau asp, mayoritas bug sebuah website adalah sql inejction, LFI(local file inclusion) dan RFI(remote file inclusion), XSS yang semuanya itu disebabkan kesalahan script.
4. Bila seorang superuser memberikan authority untuk admin web, pada halaman admin jangan sampai ada form upload tanpa filtering yaitu yang mengijinkan upload semua file, cukup untuk upload dokumen atau gambar saja, sekali lagi harus berhati-hati dalam coding.
5. Password yang bagus adalah password yang cukup panjang dan mengandung karakter-karakter yang tidak biasa kalau perlu password sering diganti untuk mengantisipasi bruteforce.
6. Jangan mudah percaya atau memberikan password kepada orang lain.
7. Minimalisir login di komputer umum dan di jaringan yang tidak secure (wifi, hub dsb).
8. Apa saja fungsi-fungsi php yang sekiranya perlu di enable bisa di load/di enable, jika ada fungsi yang memang tidak perlu sebaiknya di disable saja, apalagi seperti fungsi-fungsi yang bisa mengakses sistem.
9. Gunakan .htaccess secara maksimal, file ini sebenarnya sangat sakti.
10. Jangan sampai dalam setiap direktory tidak ada index, sehingga isi dari direktory itu bisa di tampilkan, dengan file .htaccess ini bisa di konfigurasi.
11. Sebaiknya server database dan server web dipisah itu akan mengurangi resiko.
12. Gunakan versi system operasi dan kernel yang memang benar-benar sudah stable, kalaupun kita menggunakan versi current atau rillis, siap-siaplah untuk selalu update informasi dan pathching jika ada bug.
13. Tugas seorang network administrator adalah mengamati log, semua aktifitas dari system 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, dsb semuanya harus diwaspadai.
14. Sekarang sudah ada aplikasi yang bisa memonitoring log dengan bagus, bahkan bisa mengirimkan log via email pada admin jika terjadi apa-apa pada server.
15. Bila ada file mencurigakan terutama berextensi php coba di buka kemudian bila ternyata isinya dienkripsi coba untuk didekripsi bisa jadi itu adalah web shell atau backdoor.
16. Gunakan maldetect untuk pendeteksi malware, virus, shell, rootkit, backdoor dsb, maldetect adalah antivirus yang berjalan di system operasi Linux, BSD dan keluarganya. Aplikasi ini bisa mengenali php web shell, backdoor, spyware, Trojan dsb.
17. Sebaiknya hak akses ssh dibatasi hanya untuk IP tertentu atau group user tertentu saja, atau akses ssh sama sekali tidak di ijinkan menggunakan username dan password hanya boleh menggunakan public key yang sudah ditanam dalam server web, ini cukup untuk mengurangi risiko keamanan, semua ini bisa di konfigurasi di sshd config.

**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 saya utarakan di bab Pembahasan) solusi yang harus di lakukan adalah membersihkan seluruh file yang mencurigakan (phpshell) kemudian menutup semua celah sesuai dengan yang saya rekomendasikan diatas dan 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**

Sherman, Chris. "Everything You Ever Wanted to Know About URL." *SearchEngineWatch*. Ed. Danny Sullivan.   
24 Aug. 2004. 4 Sept. 2004 http://searchenginewatch.com/searchday/article.php/3398511.

lampiran gambar, lampiran patch dan lampiran link video youtube..

<http://www.moneyma.com/tech-news/internet/total-number-of-websites-in-this-world/>

<http://packetstormsecurity.org/filedesc/freebsd-cache.c.html>

patch

<http://security.freebsd.org/advisories/FreeBSD-SA-10:07.mbuf.asc>