/*

Linux Security Banners

*/

---

1) Security Faq

- O que são os banners da Rede ?

(Comentário Infeliz : A tá isso eu sei eu troco banners toda semana ...)

Os banner da rede são mensagens de entrada e saída apresentados por diversos]
serviços como o SendMail, Telnet, FTP, SSH à um usuário. Ou seja é a mensagem de boas
vindas ao usuário, que normalmente indica a versão de tal servico, o nome do host entre
outra coisas do servidor.

- Mais quais riscos corre o meu site apresentar estes banners ao usuário ?

Em torno de 88% dos defacers do mundo inteiro exploram os banners da rede, talvez
a maioria deles não saibam que estão explorando tal coisa, porém sabem quem com tal
exploração o ataque se resume apenas em rodar seu exploit ou semelhante ferramenta.

- Mais pra que eles precisam do banner ?

É simples, suas ferramentas são para determinadas versões de tipos diferentes de
servicos , como por exemplo o exploit para wu-ftp 2.6.0 , esse exploit teve foi muito
utilizado em certo tempo. Bom vamos ao que interessa, esse exploit era apenas para a
versão 2.6.0 do wu-ftp portanto se fosse explorado a versão 2.6.1 isso resultaria em
nada, o que não interessava ao defacer, mais a solução era verificar o banner do wu-ftp
que mostrava sua versão , era simples ele se conecta ao servidor a ser atacado pela porta
21 e simplesmente esperava o banner de rede, assim anotava os servidores vulneráveis
e descartavas os demais, ainda assim era muito trabalho para os coitadinhos, eles
simplesmente criavam um scanner de banners, que se conectava a porta 21 e salvava aqueles
que apareciam em semelhança a wu-ftp 2.6.0, facilitando assim em 99% seus ataque pois
não gastariam seu tempo com a procura.

- Se eu mudasse o banner de rede adiantaria muito ?

Simplesmente você deixaria o defacer doido pois a maioria deles se baseiam em Scaners
para efetuar o ataque e como eles não chekam os sites pessoalmente , com o banner trocado

seu servidor passaria desapercebido ou seja seria descartado da tentativa do ataque

2) Alterando os Banners

- Telnet Banner

Localização : /etc/issue

Basta alterar este arquivo e inventar algo para tornar seu servidor um pouco mais seguro. Em algumas máquinas este arquivo se auto reconstitui após reiniciado então será necessário executar o comando chattr +i /etc/issue , no momento em que realizara tal coisa desabilite seu servicod e telnet , pode até habilitar o ssh em seu lugar (faça tal procedimento apenas se o banner se auto reconstituir após a renicialização da máquina.

- SendMail Banner

Localização : /etc/sendmail.cf

Edite a opção contida neste arquivo desta maneira :

* Opção Atual: O SmtpGreetingMessage=$j Sendmail $v/$Z; $b
* Altere Para: O SmtpGreetingMessage=$j Privative 1.00.33; $b

(Se quise altere para algo mais divertido)

- Qmail Banner

Localização : /etc/qmail-smtpd (Provavel localizaçao do arquivo qmail-smtp)

As modificções do Qmail se resumem em alterar a variável SmtpGreeting do arquivo qmail-smtp para uma msg qualquer

- Wu-FTP Banner

Localização : /etc/ftpaccess

Neste arquivo define toda as opções de configuração dos banner do wu-ftp que são:

* greeting full (Msg completa de boas vindas - Nome, host, versão)
* greeting brief (Nome do Host)
* greeting brief (Exibe somente a msg - FTP Server ready)
* greeting txt Olá (Exibe a mensagem Olá)
* hostname www.shit.com (Define o nome do host a ser mostrado na entrada quanto na saida)

- ProFTP Banner

    Localização : /etc/proftp.conf

    Basta alterar a variável ServerName que está como o padrão "ProFTP Default Installation" para uma outra qualquer como :

      * ServerName "Seu acceso não é autorizado, seu IP será gravado. Agora Saia"

    Ou seja a escolha é simplesmente sua. Se eu servidor for responsável pela hospedagem de diversos sites não se esqueça de alterar o ServerName de todos eles
no arquivo httpd.conf

 3) Outros

   As daemons acima são as mais populares caso possua algum tipo de daemon que queira alterar e que não esteja acima basta nos contactar (nossos dados estarão sendo impressos no final)

 4) About

   Author : drwxr - john

   Contatos :

     * E-Mail   -> john@drwxr.org

     * Site   -> www.drwxr.org

   Mais textos :

     * www.drwxr.org
