

Segurança:

Windows

E

Linux

Uma visão geral.

Por: Jonas Monteiro Carreira (Cunsultor em segurança da informação)
e-mail: j3l15@hotmail.com

Ao instalarmos o sistema operacional Linux e usarmos os seus recursos, logo podemos citar vários recursos com o qual podemos comparar com o sistema operacional Windows. Bem, o assunto seria algo abrangente nas diversas tecnologias usadas por ambos os sistemas. O assunto com o qual gostaria de discutir é sobre a segurança desses sistemas operacionais, por isso estou escrevendo este artigo sobre uma visão desses sistemas abordando a área de segurança.

Quando escolhemos um sistema operacional que vise exclusivamente a segurança, de forma em que não queremos adquirir vírus e suas variantes, logo pensamos no Linux. Mas se formos pensar, podemos dizer que o Linux pode ter a fama de seguro contra vírus e worms ou podemos, também, dizer que todos os sistemas de código aberto podem ser inseguros, simplesmente por possuírem o código livre. Afinal, o “cracker” pode muito bem ler o código e descobrir falhas e, com isso, criar um grande ciclo de “crackers” mal-intencionados, dispostos a prejudicar o Linux. Bem, existem adeptos do Linux que dizem que empresas e desenvolvedores estão sempre alerta para se prevenir bem antes dessas vulnerabilidades serem expostas no mundo virtual. Enquanto a Microsoft estaria sozinha com seus desenvolvedores, tentando “tampar” os “buracos” feitos por eles mesmos. Isso leva a usuários “céticos” pensarem: Será que os desenvolvedores Windows são tão bons assim para tampar a brechas que eles mesmos fizeram?

Podemos observar que o Windows é um sistema bastante alvo de “crackers”, simplesmente por sua popularidade, principalmente por usuários domésticos. Um “cracker” que desenvolve vírus e worms não teria o mínimo interesse em Linux. Sendo que, 80% dos usuários usam sistema Windows, mas pelo outro lado da moeda, podemos observar também o crescimento de uma internet repleta de redes rodando Linux e servidores Web Apache rodando PHP com Banco de dados mysql. E por que um “cracker” não se interessaria por uma arquitetura desse tipo? sendo que, logicamente, uma rede desse tipo, com certeza, estaria rodando informações sigilosas. No meio disso tudo, podemos descartar o tipo vulnerável de vírus e começar a se preocupar com vulnerabilidades mais importantes do que uma simples destruição do sistema (o roubo de informações financeiras), e invasões mais sofisticadas. É só pensarmos como uma “cracker” potencial: “Se o administrador escolheu um sistema seguro como o Linux. Logicamente, ele estaria protegendo informações sigilosas”. Não podemos esquecer também que existem aqueles “crackers” que só estão à procura de fama para ele invadir um Linux. Seria a glória.

Bem, ao observamos sistemas Linux, os vírus ficam de lado e damos atenção a falhas do tipo:

BufferOverflow: Falhas de BufferOverflows têm deixado muitos administradores preocupados com sua rede, não somente administradores, mas também Linus Tovalds (desenvolvedor do Linux), que tem implementado projetos que visam a segurança dos processos de memória do Linux. O primeiro foi o OpenWall e depois veio o tão falado Pax (Sobre os Pax ficará para o próximo artigo), que promete a segurança total do sistema. Recentemente, o bugado IIS em sua nova versão 6.0 tem sido bastante “seguro” em comparação ao seu “companheiro” Apache. Esse tipo de coisa faz pensarmos: “Será que os crackers de plantão estão deixando o IIS de lado e indo de encontro ao Apache por sua popularidade na internet?”.

A vantagem do Linux sobre o Windows ainda é bastante grande, isso temos que afirmar. A todos os meios e técnicas mais comuns de invasão, o Windows ainda é falho e o Linux ainda tem a vantagem de que para você e o seu grupo executar determinado arquivo tem que ter os devidos privilégios. Algo que complicaria a vida de um vírus dentro do Linux. E o usuário Root é o administrador do sistema que controla todos os outros usuários e grupos, fazendo com que o administrador se sinta mais seguro em suas informações. Para um vírus básico entrar no Windows, basta ter uma extensão Bat, Exe e apenas dois cliques. Além disso, quando ocorre uma falha no Linux, o que vemos é que, no Máximo, em 24 horas o Patch já esta disponível. Já no Windows, isso demora até meses.

No meio de tantas especulações de qual sistema é o mais seguro. Nós, profissionais de segurança, temos de levar em conta que o crescimento da plataforma Linux é uma realidade e devemos começar a nos preocupar, até mesmo, em como proteger de ataques de vírus no Linux. Mas mesmo assim, o Linux ainda continua sendo um sistema fascinante para se aprender e para saber o que estamos fazendo, como estamos fazendo e de que maneira nós queremos que seja feito. Por outro lado está o Windows, que também é o sistema operacional que a maioria de nós aprendemos a usar e a quebrar a cabeça e uma coisa eu não posso negar: Que no Windows eu aprendir a programar e até hoje eu o uso para estudar.

Cordial Abraço!

Jonas Monteiro Carreira.