Introdução a Segurança da Informação – Parte 7

13 de abril de 2015 / maximoz

Antivírus

O antivírus é um tipo de software que protege seu computador de todo tipo de programa malicioso que perpetra em seu computador sem seu consentimento. Tais programas maliciosos são intrusivos, hostis e irritantes. Os diferentes tipos de programas maliciosos podem ser:

1. **Vírus de computador:** Esse tipo de programa hostil age semelhante ao vírus que infecta humanos. Assim que ele entra em seu computador, se aconchega calmamente, até que encontra um software executável que o ajuda a se espalhar semelhante a um hospedeiro. Transmite-se ativamente até sobre todos os computadores que estão conectados na rede e destrói todos os softwares importantes.
2. **Worm:** Esse é bastante similar ao vírus mas ele não precisa de um executável para se espalhar. Ele se espalha automaticamente e destrói todos os softwares importantes também.
3. **Spyware:** Esse programa nocivo é bem diferente de vírus e cavalos de Tróia, mas é igualmente prejudicial. Ele não se espalha como vírus, mas ele mantém continuamente a aparição de pop-ups para convencer ao usuários a instalar sua versão paga que traiçoeiramente promete proteger seu computador, ou algo do tipo. Esse programa secretamente coleta informações pessoais como cartões de crédito, CPF, usuários e senhas do seu computador e as envia remotamente a outro computador quase que em tempo real.
4. **Adware:** Ele é pouco semelhante ao spyware, mas seu principal objetivo é anúncio publicitário. Podem até existir, mas, em geral não pode ser considerado um programa malicioso porque vem em seu computador com seu consentimento. No entanto, ele pode te encher de anúncios publicitários; com pop-ups e banners de propaganda.
5. **Grayware:** Esse software é amplamente utilizado para todos os programas de computador que são irritantes mas não necessariamente totalmente destrutivos. Ele inclui programas como o adware, programas de piadas, e dialers.

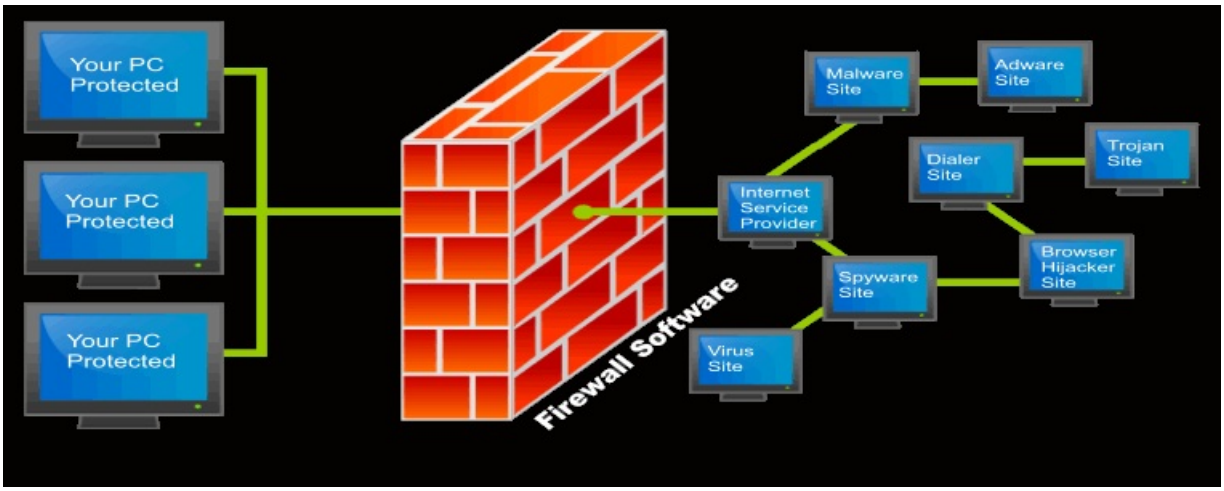
O antivírus precisa ser sempre atualiza com as últimas definições de vírus para continuar protegendo seu computador das novas ameaças que surgem periodicamente. É importante ressaltar que não importa quão bom seja o antivírus e que esteja sempre atualizado, se o usuário, inconsequentemente, baixa todo tipo de programa desconhecido sem certificados tendo em mente que o antivírus o está protegendo está agindo errado pois ainda há risco. Há muitos usuários que optam não usar antivírus algum pois sabem o que estão a baixar e instalar, mas é uma decisão pessoal, não recomendado para paranoicos.

O antivírus é agora uma exigência de todo computador/servidor que está interconectado em uma rede ou conectado através da internet. Mesmo um computador independente precisa de um antivírus instalado. Isso é porque o vírus não pode somente afetar seu computador através da internet mas também pode infectá-lo a partir de dispositivos de armazenamento externos conectados ao seu computador temporariamente.

Firewall

Um firewall pode ser tanto um software quanto um hardware. Um firewall hardware é um dispositivos que é plugado em sua rede fisicamente. É uma pequena caixa de metal com portas. Ele é ligado entre a rede e o computador. No entanto, ele é o mais adequado para empresas e grandes redes e não é utilizado comumente.

O firewall software é mais comumente usado para proteger dados através de constante inspeção de entrada e saída de pacotes IP. O firewall age como um porteiro entre uma rede seguran e uma desprotegida e permita ou nega a passagem de tráfego com base nas políticas de segurança configuradas no firewall. Ele garante que nada pessoal saia e nada malicioso entre.



O firewall requer uma compreensão adequada de endpoints de rede e operações do dia-a-dia da empresa, de como que ele possa ser configurado corretamente. Sem a configuração adequada, não há nenhum uso. Ele pode ser um ou mais dos seguintes tipos:

1. **Filtrador de pacotes:** Como o nome sugere, o firewall filtrador de pacotes inspeciona cada pacote que passa através dele por cinco características: endereço IP de origem, porta de origem, endereo IP de destino, porta de destino e protocolo IP. Você pode usar o filtrador de pacotes para bloquear tipos particulares de tráfego em uma particular porta. Por exemplo, você pode bloquear o tráfego web na porta 80 e o tráfego do Telnet na porta 23.
2. **Firewall Proxy:** A aplicação Firewall Proxy representa o servidor web interno e oculta o endereço de rede interno domundo exterior. Ele verifica cada pacote passando que seja contra as regras do firewall e se o pacote é permitido, então ele destrói e recria cada pacote para prevenir ataques deconhecidos baseado nas fraquezas do TCP/IP.
3. **Inspeção de Estado:** O firewall de filtragem de pacotes mantém uma faixa do estado de conexões de rede. Por exemplo, ele examina comunicações TCP/UDP que passam através dele e permite apenas os pacotes que combinam com um estado de conexão conhecida.

Detecção de Intrusão

A intrusão ou os ataques à sistemas ou redes de computadores podem ser detectados usando o Sistema de Detecção de Intrusão (IDS). Esses sistemas ficam monitorando a rede/sistema para atividades atividades maliciosas ou violações da política. Assim que o sistema percebe alguma atividade maliciosa, ou ele tenta impedí-las por si mesmo ou exerco outras atividades que estão configuradas no sistema para impedir a intrusão. Algumas das formas que um IDS pode desempenhar para impedir uma atividade maliciosa é reconfigurando os roteadores e firewalls para rejeitar o tráfego do mesmo endereço ou elaborando pacotes na rede para redefinir a conexão. Em alternativa, o sistema imediatamente informa as atividades maliciosas ao administrador do sistema, cria logs e relatórios.

Pode haver dois tipos de IDS:

1. **Baseado em Host:** Esses sistemas coletam e analisam dados que se originam a partir de um computador que hospeda um serviço como Serviço Web, Serviço DHCP ou DNS.
2. **Baseado em Rede:** Já esses coletam e analisam dados que se originam a partir de uma rede. Tais como pacotes de dados que viajam sob uma rede.

Em um bom sistema de detecção de intrusão os dois tipos de IDS trabalham em conjunto para proteger uma rede. Com tempo, os novos e desconhecidos ataques continuam aparecendo e não é possível manter-se com eles porque são muitos. Embora você não possa proteger seu sistema/rede contra todo tipo possível de ataque, você pode protegê-lo da maioria das maeaças usando um IDS.

Os sistemas IDS detectam intrusões por algumas formas. Algumas dessas formas são:

1. **Detecção de Anomalia:** O IDS detecta anomalias estatísticas do sistema definindo uma linha de base nas atividades do sistema/rede tal como a utilização de CPU, atividade no disco, logins e atividades em arquivos. Assim que há um desvio nessa linha de base, o sistema dispara um alarme.
2. **Reconhecimento de Assinatura:** O IDS examina o tráfego procurando por padrões conhecidos de ataque. Por exemplo, o sistema pode verificar todos os pacotes que tentam acessar o script padrão CGI vulnerável “/cgi-bin/phf” em um servidor web./li>
3. **Uso de banda:** Ele se mantém examinando o uso da banda no sistema. Um aumento inesperado no uso da banda pode levar a um evento suspeito.
4. **Ataques de Negação de Serviço:** Nesse tipo de ataque, o atacante sobrecarrega o servidor com

mensagens e o servidor para de responder a qualquer mensagem seja qual for o requisitor. Sendo assim, faz com que ninguém possa acessar o servidor. O atacante nesse tipo de ataque pode usar como vítima o roteador, firewall ou um servidor proxy e fazê-los ficarem sem uso.

Os tipos a seguir não são ataques propriamente ditos, eles têm como finalidade comente a obtenção de informações da vítima, ou seja, é uma etapa do processo de ataque, mas não ele em sua verdadeira forma. Esses "ataques" condizem com as seguintes etapas de um pentest: *coleta de informação, mapeamento de rede e enumeração de serviços*. Uma ferramenta conhecida para isso é o Nmap. Vejamos os tipos:

1. **IP Half Scan:** Nesse tipo de "ataque", o atacante repetidamente tenta se conectar a um computado destino e não envia pacotes ACK correspondentes. Ele tenta determinar exatamente quais oa as portas abertas para conexões, sem o computador de destino estar consciente dessa ação.
2. **Varredura de Portas (Port Scan):** Aqui o atacante faz uma tentativa de contar os serviços em execução em um computador fazendo a varredura por cada porta procurando uma resposta. Se o ataque tiver êxito, o atacante pode tomar conhecimento de portas ativas e explorar possíveis vulnerabilidades dos serviços das portas.

Os sistemas de detecção de intrusão são, na maioria das vezes, integrado aos firewalls. No entanto, se ele não for embutido, você precisará tanto de um firewall como um IDS para proteger seu sistema. O firewall deve ser configurado corretamente para habilitar o IDS, isso se o IDS for integrado ao seu firewall.

Próximo capítulo >>>

Traduzido e adaptado por: Maximoz Sec
Artigo original: http://learnthat.com/introduction-to-network-security