O que são ataques

Ataque é uma tentativa de desabilitar computadores, roubar dados ou usar um sistema de computador violado para lançar ataques adicionais. Os criminosos virtuais usam diferentes métodos para lançar um ataque cibernético que incluem malware, phishing, ransomware, ataque man-in-the-middle ou outros métodos.

O que são códigos maliciosos

códigos maliciosos (*malware*) são programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador. Algumas das diversas formas como os códigos maliciosos podem infectar ou comprometer um computador são:

- pela exploração de vulnerabilidades existentes nos programas instalados;
- pela auto-execução de mídias removíveis infectadas, como *pen-drives*;
- pelo acesso a páginas *Web* maliciosas, utilizando navegadores vulneráveis;
- pela ação direta de atacantes que, após invadirem o computador, incluem arquivos contendo códigos maliciosos;
- pela execução de arquivos previamente infectados, obtidos em anexos de mensagens eletrônicas, via mídias removíveis, em páginas *Web* ou diretamente de outros computadores (através do compartilhamento de recursos).

Uma vez instalados, os códigos maliciosos passam a ter acesso aos dados armazenados no computador e podem executar ações em nome dos usuários, de acordo com as permissões de cada usuário.
Os principais motivos que levam um atacante a desenvolver e a propagar códigos maliciosos são a obtenção de vantagens financeiras, a coleta de informações confidenciais, o desejo de autopromoção e o vandalismo. Além disto, os códigos maliciosos são muitas vezes usados como intermediários e possibilitam a prática de golpes, a realização de ataques e a disseminação de *spam.*

O que códigos maliciosos podem fazer com seu computador?

Eles podem desencadear efeitos como:

- Deixar o desempenho lento ou com falhas;
- Corromper arquivos ou até mesmo exclui-los;
- Ocasionar pop-ups de adware constantemente;
- Panes no sistema operacional;
- HD que não para de girar;
- Aplicativos que travam ou param de funcionar;
- Lentidão geral nas ações;
- Mudanças inexplicadas nas configurações de conta e do dispositivo;
- Mau funcionamento de aplicativos, arquivos e outros programas.

Aplicativos para Prevenção, Detecção e Remoção de Vírus

Existem milhares de aplicativos para prevenção, detecção e remoção de vírus, porem aqui escolhemos alguns para apresentarmos. Logo abaixo apresentaremos alguns aplicativos para prevenção, detecção e remoção de vírus, que são eles:

1 – Scanner de Vulnerabilidade OpenVAS

Esta ferramenta abre a varredura em servidores e dispositivos de rede, incluindo endereço IP, serviço aberto, portas abertas, problemas com configuração e instalação de programas e aplicativos.

Em seguida, gera um relatório com as informações via e-mail para posterior retificação. Este scanner de vulnerabilidade pode ser usado a partir de um servidor externo.

2 – Tripwire IP360

Aqui, a verificação é feita de forma integrada com o gerenciamento de riscos, os usuários são mais capazes de identificar de forma autônoma todos os problemas de rede, que incluem ativos locais, na nuvem e em contêineres.

É um tipo de scanner capaz de realizar uma avaliação mais geral e sistêmica pelos profissionais de tecnologia da informação.

3 – Scanner de Vulnerabilidade Nessus

É um tipo de scanner de vulnerabilidade que funciona gerando um procedimento de segurança proativo em redes integradas, virtuais, físicas ou em nuvem. É mais adequado para uso por profissionais **especializados em segurança cibernética** no monitoramento de patches, software , identificação e exclusão de adware, malware e até mesmo aplicativos.

4. Comodo HackerProof

Atualizado diariamente, é muito utilizado pelas equipes de tecnologia da informação por apresentar prevenção de ataques drive-by, boa verificação de sites maliciosos e arquivos no sistema operacional do computador.

Com base em indicadores, a avaliação de segurança é monitorada pelos usuários, o que exige o aprimoramento do próprio software.

5. **Scanner de vulnerabilidade da comunidade Nexpose**

A novidade desse scanner de vulnerabilidade é **o código aberto** , o que se torna uma vantagem para os profissionais de tecnologia da informação. Dessa forma, é possível evoluir em melhorias constantes no momento em que um novo dispositivo se conecta à rede.

Também trabalha com critérios de avaliação de pontuação de risco entre as ameaças e garante a medição por **profissionais de segurança cibernética** .

6. Gerenciador de Vulnerabilidades Plus

A diferença aqui é que a verificação utiliza o mesmo mecanismo usado pelos hackers para que os profissionais de TI também saibam como os ataques estão sendo reelaborados e possam pensar em soluções de prevenção mais atualizadas.

O scanner é fornecido gratuitamente em até 25 dispositivos e oferece verificação automática, avaliação de risco e impacto, configurações incorretas de segurança, proteção de servidor da Web e muito mais.

7. Scanner de Vulnerabilidade Nikto

Neste scanner de vulnerabilidades, o profissional de TI tem a possibilidade de entender as versões e funcionalidades dos servidores, e atuar de forma mais direcionada a protocolos e malwares.

Permite checar diferentes portas de um mesmo servidor simultaneamente e é muito utilizado pela eficiência na proteção do servidor.

8. Wireshark

Este scanner é adequado para dispositivos Linux, macOS e Windows, e é amplamente utilizado em sistemas de rede de órgãos e serviços públicos.

Nesta ferramenta, a identificação de ameaças é feita off-line para avaliação e correção.

9. Aircrack-ng

É um scanner de vulnerabilidade amplamente utilizado para monitoramento de redes WiFi, utilizando aplicativos acessíveis em drives, cartões e ataques de replay. Cuida das chaves perdidas capturando pacotes de dados. Os sistemas operacionais suportados incluem NetBSD, Windows, OSX, Linux e Solaris.

10. Scanner de segurança de rede retina

A operação aqui é **um software de código aberto baseado na Web** a partir de um local central e inclui: aplicação de patches, conformidade, configuração e geração de relatórios.

Ele também fornece proteção garantida para bancos de dados, estações de trabalho, servidores e aplicativos da Web, com suporte total para integrações do VCenter e ambientes de digitalização de aplicativos virtuais.

https://www.unisys.com/pt/glossary/what-is-cyber-attack/

https://www.gov.br/fundaj/pt-br/centrais-de-conteudo/noticias-1/4-codigos-maliciosos-malware

https://blog.bling.com.br/codigos-maliciosos-ou-virus-tudo-sobre-eles-e-como-se-prevenir/

https://skyone.solutions/en/hub/vulnerability-scanner/