Fatec
Jales

Sistemas para Internet

06 – Ataques na Internet

Uma visão geral dos ataques listados na Cartilha de Segurança para Internet do CGI – Comitê Gestor da Internet

Componente Curricular: **Bases da Internet**

Professor: Jorge Luís Gregório | e-**mail***: jorge.gregorio@fatec.sp.gov.br*


@jlgregorio81


Jorge Luís Gregório

Ataques na Internet

Ataques costumam ocorrer na Internet com diversos objetivos, visando diferentes alvos e usando variadas técnicas. Qualquer serviço, computador ou rede que seja acessível via Internet pode ser alvo de um ataque, assim como qualquer computador com acesso à Internet pode participar de um ataque.

Comitê Gestor da Internet, 2012, pág. 17

Motivações

- Demonstração de Poder
  - Suspender os serviços de uma empresa e chantageá-la
- Prestígio
  - Disputas entre atacantes
- Motivações financeiras
  - Roubar dados confidenciais afim de aplicar golpes financeiros
- Motivações ideológicas
  - Tornar inacessível ou descaracterizado, sites que representem ou divulguem conteúdo contrário à opinião pública
- Motivações comerciais
  - Espionagem industrial, tornar inacessível sites de concorrentes, etc

Exploração de vulnerabilidades

Uma vulnerabilidade é definida como uma condição que, quando explorada por um atacante, pode resultar em uma violação de segurança. Exemplos de vulnerabilidades são falhas no projeto, na implementação ou na configuração de programas, serviços ou equipamentos de rede.

Comitê Gestor da Internet, pág. 18

Varredura em Redes (Scan)

Varredura em redes, ou *scan*, é uma técnica que consiste em efetuar buscas minuciosas em redes, com o objetivo de identificar computadores ativos e coletar informações sobre eles como, por exemplo, serviços disponibilizados e programas instalados. Com base nas informações coletadas é possível associar possíveis vulnerabilidades aos serviços disponibilizados e aos programas instalados nos computadores ativos detectados.

Comitê Gestor da Internet,2012, pág. 18

As varreduras podem ser de dois tipos:

- Legítima: realizada por pessoas autorizadas
- Maliciosa: realizas por invasores

Falsificação de e-mail (E-mail spoofing)

Falsificação de e-mail, ou *e-mail spoofing*, é uma técnica que consiste em alterar campos do cabeçaalho de um e-mail, de forma a aparentar que ele foi enviado de uma determinada origem quando, na verdade, foi enviado de outra.

Comitê Gestor da Internet, 2012, pág. 18

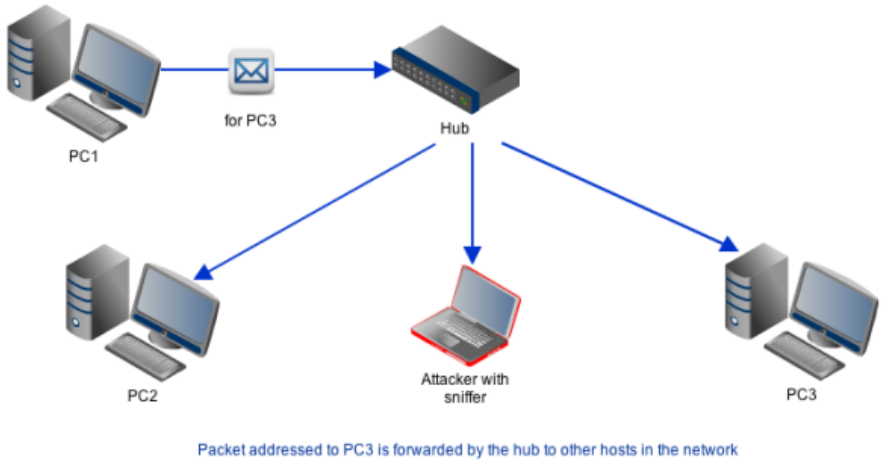
Interceptação de Tráfego (Sniffing)

Interceptação de tráfego, ou *sniffing*, é uma técnica que consiste em inspecionar os dados trafegados em redes de computadores, por meio do uso de programas específicos chamados de *sniffers*.

Comitê Gestor da Internet, 2012, pág. 19

Legítima: realizada por pessoas autorizadas para detectar problemas de tráfego, análise de dados e monitoramento de atividades maliciosas

Maliciosa: realizada por atacantes afim de capturar informações como senhas, números de cartões de créditos e outros conteúdos confidenciais que são transmitidos por conexões inseguras e/ou sem criptografia.



Força bruta (Brute force)

Um ataque de força bruta, ou *brute force*, consiste em adivinhar, por tentativa e erro, um nome de usuário e senha e, assim, executar processos e acessar sites, computadores e serviços em nome e com os mesmos privilégios deste usuário.

Comitê Gestor da Internet, 2012, pág. 20

???

Problemas com a Força Bruta

- Com a Força Bruta, o atacante pode:
  - Trocar sua senha
  - Invadir serviços de e-mail e perfis das redes sociais
  - Invadir computadores e outros dispositivos
- Mesmo que o atacante não consiga acesso, pode acontecer outros problemas:
  - Bloqueio de contas devido à sucessivas tentativas de acesso
- Podem ser realizados manualmente ou através do uso de ferramentas hackers

Desfiguração de página (Defacement)

Desfiguração de página, *defacement* ou pichação, é uma técnica que consiste em alterar o conteúdo da página Web de um site.

Comitê Gestor da Internet, 2012, pág. 21

Principais formas utilizadas

- Explorar erros de aplicações Web
- Explorar vulnerabilidades dos servidores Web
- Explorar vulnerabilidades das tecnologias usadas no desenvolvimento da aplicação Web;
- Invadir o servidor de páginas e alterar o arquivo HTML/CSS original

Site da **Nasa** é vítima de ataque de hackers brasileiro

Fonte: G1.com

DoS (Denial of Service)

Negação de serviço, ou DoS (Denial of Service), é uma técnica pela qual um atacante utiliza um computador para tirar de operação um serviço, um computador ou uma rede conectada à Internet.

Quando utilizada de forma coordenada e distribuída, ou seja, quando um conjunto de computadores ´ e utilizado no ataque, recebe o nome de negação de serviço distribuído, ou DDoS (Distributed Denial

of Service).

O objetivo destes ataques não é invadir e nem coletar informações, mas sim exaurir recursos e causar indisponibilidades ao alvo. Quando isto ocorre, todas as pessoas que dependem dos recursos afetados são prejudicadas, pois ficam impossibilitadas de acessar ou realizar as operações desejadas.

Comitê Gestor da Internet, 2012, pág. 21

Prevenção

- Mesmo não sendo 100% garantido, é possível se proteger (ou tentar) de ataques com simples ações:
  - Tenha um antivírus e um firewall instalados, ativos e atualizados nos seus dispositivos
  - Tome cuidado com suas senhas – use somente senhas fortes
  - Utilize recursos de criptografia para transmitir e armazenar dados
  - Atualize seus programas para as versões mais recentes, pois sempre há, além de melhoramentos, correções de falhas
  - Atualizações do Sistema Operacional

Referências

Comitê Gestor da Internet no Brasil. Cartilha de Segurança para Internet – Versão 4.0. 2 ed. São Paulo: 2012. Disponível em <http://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em 01 mar. 2014.

Bibliografia Recomendada.

BBC Brasil. Cinco pontos-chave para se proteger de ataques na internet. 02 nov. 2013. Disponível em <http://www.bbc.co.uk/portuguese/noticias/2013 /11/131101_dicas_proteger_ataque_ cibernetico_mm.shtml>

BBC Brasil. 'Maior ataque cibernético da História' atinge internet em todo o mundo. 27 mar. 2013. Disponível em <http://www.bbc.co.uk/portuguese/ultimas_ noticias/2013/03/130327_ataque_ cibernetico_ji.shtml> Acesso em 10 mai. 2014

G1. Hackers brasileiros desfiguram páginas da Nasa em protesto. 10 set. 2013. Disponível em <http://g1.globo.com/tecnologia/noticia/2013/09/hackers-brasileiros-desfiguram-paginas-da-nasa-em-protesto.html> Acesso em 11 mai. 2014.

Info Exame. Maior ataque DDoS da história atinge servidores da CloudFlare. 11 fev. 2014. Acesso em 11 mai. 2014. Disponível em < http://info.abril.com.br/noticias/ti/2014/02/maior-ataque-ddos-da-historia-atinge-servidores-da-cloudflare.shtml> Acesso em 11mai. 2014.