Trabalho final de Teleinformática e Redes 2

André Bezerra Marinho (13/0005827)
Andressa Valadares (13/0042943)
Aurora Li Min de Freitas Wang (13/0006408)
Jessica da Silva Oliveira (13/0028983)
Rafael Neiva da Cunha (13/0016594)
Renato Estevam Nogueira (13/0036579)

20 de Junho de 2017

Sumário

Mecanismo dos ataques

- Sincronismo:
  - Comunicação via *Multicast*
  - Cada instância do programa poderá receber argumentos para acordar/adormecer o grupo de processos
  - O tipo do ataque e a vítima serão passados como argumento para uma instância e propagados pela mesma
- Distribuição:
  - Supõe-se que o código malicioso já está distribuído nas máquinas
  - A instância pode ser executada em cada máquina tanto vinculada a um processo pai quanto desvinculada (como *deamon*, executando com o parâmetro &)

SYN Flood

- Descrição: Ataque de negação de serviço que manda uma sucessão de requisições do tipo SYN de modo a tornar o servidor indisponível por fazê-lo tentar um *three-way handshake* que nunca será finalizado
- Como é evitado em servidores reais:
  - Cookies SYN
  - *Backlog* crescente
  - *Retries* limitados
  - Reduzir o *timeout* do *three-way handshake*
  - Cache SYN
  - Firewall e Proxy

HTTP Post

- Descrição: Estabelece numerosas conexões via HTTP com o servidor, cada conexão contendo um *content length* de valor alto. Entretanto, em vez de mandar todos os dados de uma vez, manda-os de um em um caracter durante um longo período de tempo.
- Como é evitado em servidores reais:
  - Negando conexão ao cliente que parece ser malicioso (problema: pode ser um cliente não-malicioso lento)
  - Combinação de métodos de *profiling*: verificando reputação do IP, monitorando atividade incomum, adicionando métodos de segurança na camada de aplicação

Servidor

- Definição: Servidor HTTP Apache
- Características: Software livre, *cross-platform*, estável
- Funcionalidades: Taxa de processamento de requisições limitada, número de conexões simultâneas limitado, limitação de largura de banda, etc
- Restrições: Tanto o servidor quanto a máquina ao qual será executado deverão desabilitar todas as proteções usualmente implementadas em casos reais para os ataques a serem feitos (mostradas nos slides anteriores)

Organização do grupo

Metodologia XP (*eXtreme Programming*)

- Papéis:
  - Cliente
  - Programador
  - *Coach*
  - *Tracker*
- Práticas:
  - Projeto Simples
  - Refatoração
  - Programação em Pares
  - Propriedade Coletiva
  - Padrões de programação

Referências

- Bogdan Calin. *HTTP Post Denial Of Service: more dangerous than initially thought*. Out. de 2014. URL: https://www.acunetix.com/blog/articles/http-post-denial-service/.
- *SYN Flood DOS Attack with C Source Code (Linux)*. URL: http://www.binarytides.com/syn-flood-dos-attack/.
- Hiep Nguyen Duc. *SYN Flood Attacks- "How to protect?- article*. Set. de 2014. URL: https://hakin9.org/syn-flood-attacks-how-to-protect-article/.
- *HTTP Flood*. URL: https://www.incapsula.com/ddos/attack-glossary/http-flood.html.
- tutorialspoint.com. *Extreme Programming Roles*. URL: https://www.tutorialspoint.com/extreme_programming/extreme_programming_roles.htm.