Administração e Gerenciamento de Redes

Trabalho 02 – Ataque e Defesa DDoS

Cenário: Duas indústrias farmacêuticas estão participando de um processo de licitação para uma vacina que será vendida ao governo contra um novo tipo de gripe. De acordo com as novas regras de licitação, as informações deverão ser fornecidas exclusivamente via WebService. O vencimento da licitação está próximo e os WebServices deverão estar acessíveis durante meia hora para que o governo possa adquirir os dados. Se o WebService não estiver no ar, a empresa será considerada desistente do processo. A concorrência na área farmacêutica é violenta e fora a espionagem industrial, vencer a licitação é objetivo de todos os envolvidos e os concorrentes tentarão derrubar-se mutuamente para que a licitação não seja efetuada com sucesso.

Descrição: Os grupos terão de preparar seus laboratórios e irão utilizar a ferramenta trin00 e mais seus conhecimentos para realizar ataques na rede dos "concorrentes", atacando e defendendo simultaneamente pelo período de 1 hora.

Requisitos mínimos:

a. **Serviços fornecidos: Apache, SSH, DNS Próprio.**
b. **Mínimo de 3 computadores**
c. **Máximo de RAM por HOST virtual: 64 Mb**
d. **Consumo de RAM real (máximo):**
    a. **1024 Mb para o pc com o laboratório do grupo**
    b. **0512 Mb para os auxiliares**
e. **Todas as máquinas da rede virtual deverão estar com IP's devidamente configurado e serem acessíveis internamente**
f. **Os grupos poderão utilizar até 03 máquinas reais no experimento, mas apenas uma das máquinas poderá representar a rede da indústria**
g. **As outras máquinas poderão ter laboratórios preparados para atacar**

Regras de Ataque:

A.1. Os atacantes deverão usar o trin00 *E* poderão usar quaisquer outros conhecimentos que tenham para efetuar o ataque.
A.2. O ataque deverá ser dirigido exclusivamente aos concorrentes (considera-se que o ataque seria descoberto publicamente e a empresa impedida de participar da licitação)
    A.2.i Essa regra implica que não poderá ser feito ataque ao "governo", ao "ISP", os clientes e à infra-estrutura de rede.
    A.2.ii Caso o número de pacotes seja excessivo para a infra-estrutura do laboratório ou para o ISP, provocando DoS acidental na infra-estrutura, o poder de ataque deverá ser reduzido.

Regras de Defesa:

D.1. O grupo poderá utilizar quaisquer técnicas que conheça para evitar ser derrubado.
D.2. Durante todo o experimento, os defensores deverão manter seus serviços acessíveis para todos os clientes, ou o máximo de tempo possível.

Critério de pontuação:

Pontos negativos:

- **Não usar o trin00: -2pts**
- **Atacar a infra-estrutura, o governo, ISP ou os clientes: -3pts**
- **Não atingir os requisitos mínimos: -1pt**
- **Ultrapassar o consumo de memória: -3pts**

Pontuação positiva:

- **O grupo não for derrubado por méritos próprios: +1pt**
- **O grupo que conseguir derrubar um concorrente: +1pt**
- **O vencedor da licitação (último sobrevivente) +1pt**

Os grupos terão 15 minutos para o setup do laboratório e ao sinal, poderão começar o ataque aos demais concorrentes. O prazo máximo é de uma hora, ou até somente um atacante ficar de pé!

Entrega:

1. **Entregar o relatório compactado no formato .tar.gz ou .zip**
2. **Entregar também um relatório com as seguintes seções: nome do grupo e dos integrantes, descrição do laboratório, estratégia de ataque, estratégia de defesa, resultados obtidos.**

Forma de entrega:

Enviar PDF do relatório e o laboratório para os emails a seguir, até 12/11 as 23:59 hrs

- **kalinka@icmc.usp.br**
- **usp@paulogurgel.com.br**