

GUERRA AVANÇADA

Atenção: Apresento aqui algumas curiosidades unicamente para estudo e complemento profissional. O mau uso das informações a seguir é de responsabilidade do leitor deste documento.

Os scripts de guerra estão ficando cada vez mais avançados. Contudo, os servidores e os IRCops também estão ficando cada vez melhores. Muitos servidores incorporam o Clone Detection. Isso significa listar as pessoas comparando os IP's e notificando os IRCops. Isso pode tornar impossível fazer um número de clones suficientes para dar um flood em alguém. Alguns servidores tem proteção contra táticas de netsplit takeover. Esse tipo de coisa pode deter o hacking contra OPs durante um netsplit, permitindo somente tomar canais que não tenham OP. Anti Collide é também usado em muitos servidores. Fazendo com que os dois usuários sejam mortos numa colisão por troca de nick. Se alguém quiser te ferrar você vai deixar de brigar só porque não pode usar clones e etc??? NÃO!

1. Nuke

Nuke é uma grande arma para tirar alguém de IRC rápido! Funciona assim: O programa de nuke manda informação para pessoa no servidor e ela é ferrada por eles, causará erros como "dead Socket", "connection refused", "eof from client" e "machine is not on the network".

Para usar o nuke é preciso primeiro um modem rápido, 28.8 ou melhor. Você também precisa do Trumpet© Winsock. Programa dial up que se comunica rapidamente com o modem. Esse programa pode ser facilmente encontrado na web. Agora só é preciso de um programa de Nuke. Eu recomendo o Winuke 4 by CHAOS INC. ou Wnewk para maquinas windows, ou se você usa um mac, MAC NUKE. Depois de pegar esses programas, é fácil ter uma vingança, tomar canais, e matar gente rapidamente.

2. Bombas ICMP

ICMP é uma maneira extremamente poderosa de tirar a pessoa, não só de IRC, mas de sua conexão com a Internet. Funciona dessa maneira: ela manda mensagens ICMP, em uma taxa muito alta de velocidade, causando barulho na linha, e modem lag. Causa tanto lag, que seu ping aumenta terrivelmente e o joga pra fora do IRC server.

Para usar o ICMP você precisa de um Unix Shell account. Por que? Porque para usar o ICMP efetivamente você precisa de mais do que um modem pode oferecer. Você precisa de uma T1, pelo menos. Existem muitos programas de ICMP para Windows disponíveis, mas eles não trabalham muito bem. É a velocidade que importa nessa hora.

Aqui estão duas formas de usar ICMP num Unix shell:

```
ping -s (ip address) (packet size) (# of packets)
ping -s (packet size) -c (# of packets) <-f> (ip address)
```

(IP address) é o *!*@seja.la.oque.for

(packet size) é o tamanho de cada pacote a mandar, tente 30kb

(# of packets) é quantos pacotes mandar 3000 é um bom número

-f é opcional em segundo, e manda ppacotes a 20/seg

3. Botnet/Floodnet

É cada vez mais difícil usar clones sem ser pego. Você precisa de uma maneira de usar o flood sem ser detectado. Como fazer isso? Floodnet. Existem duas tipos diferentes de Floodnet. O primeiro é com Eggdrop bots, esses botnets são compreendidos como eggdrops ligados, e tem um script de flood comum. Existem botnets com muitas centenas de ligações. É muito difícil parar o flood deles. A outra maneira, é usar scripts individuais. Os scripts têm comandos comuns, e permitem que usuários com o mesmo script de se liguem, para juntos combinarem seus clones. Existem vantagens e desvantagens dos dois. As vantagens dos botnets é que estão sempre online porque estão em um Shell. Mas as desvantagens é que não são tão dinâmicos quanto um clone floodnet.

Autor: Yuri Bueno Fontenla

Contato: gold_fox1@hotmail.com