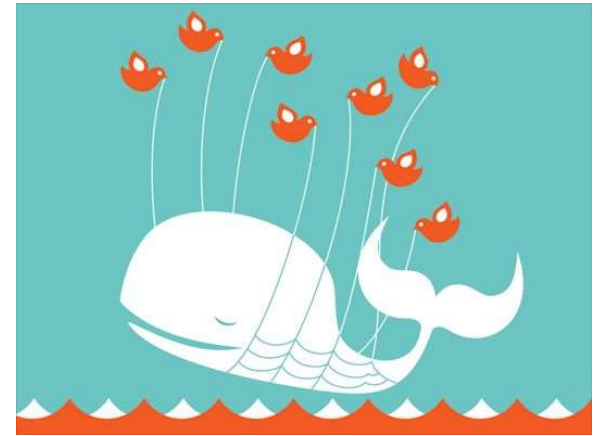


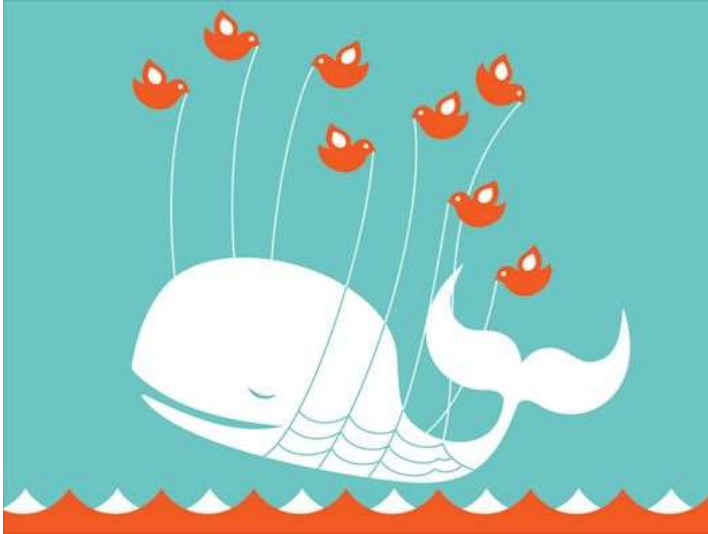
Ataques de Negação de Serviço – DoS e DDoS



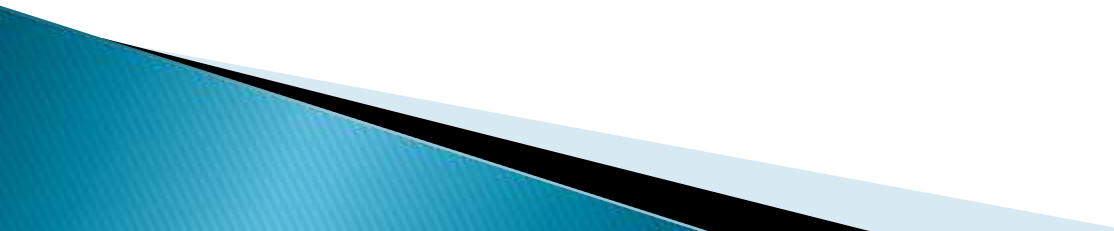
Carlos Henrique M. da Silva
carloshenrique.85@globocom

DoS

Um ataque de negação de serviço (também conhecido como DoS Attack, um acrônimo em inglês para *Denial of Service*), é uma tentativa em tornar os recursos de um sistema indisponíveis para seus utilizadores.

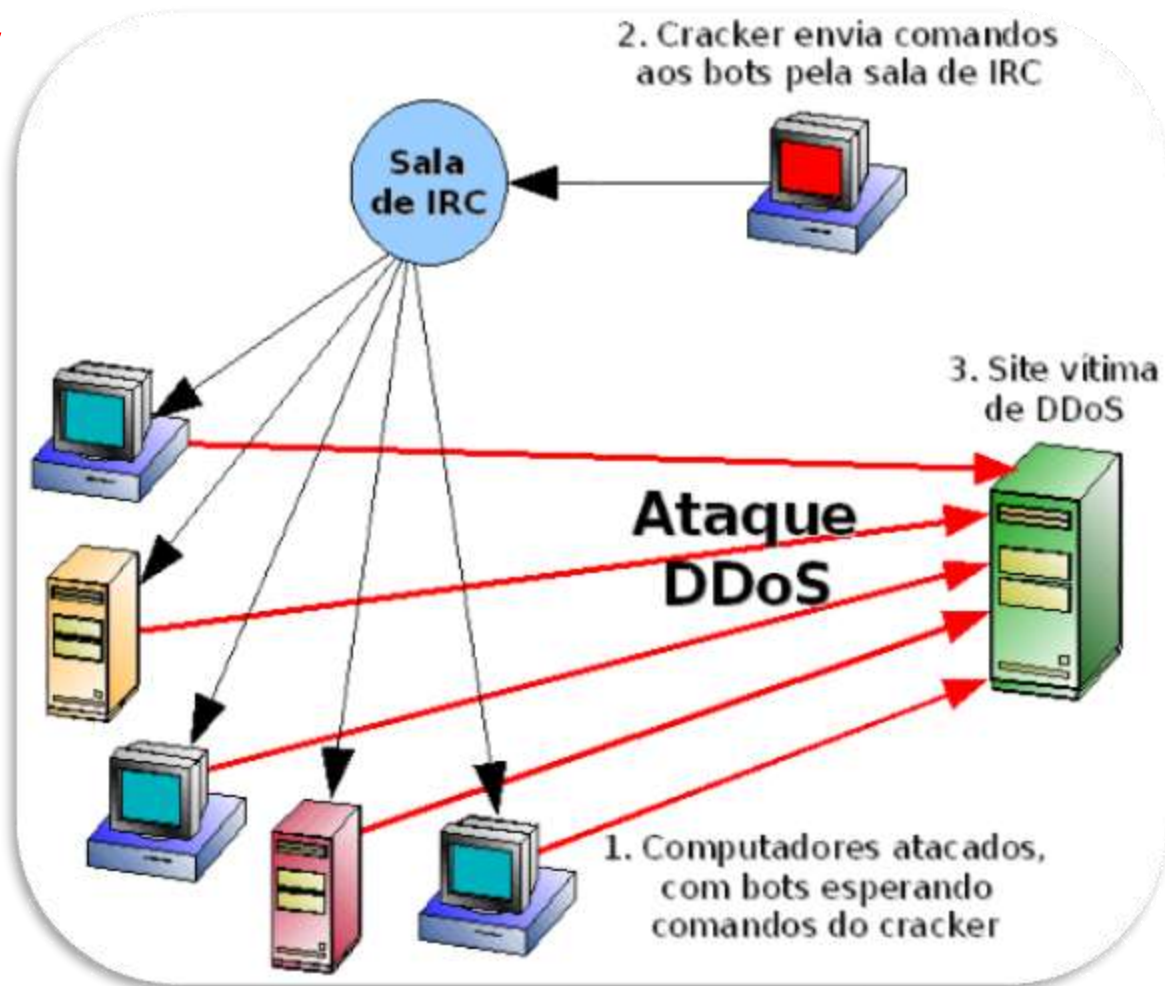


DoS

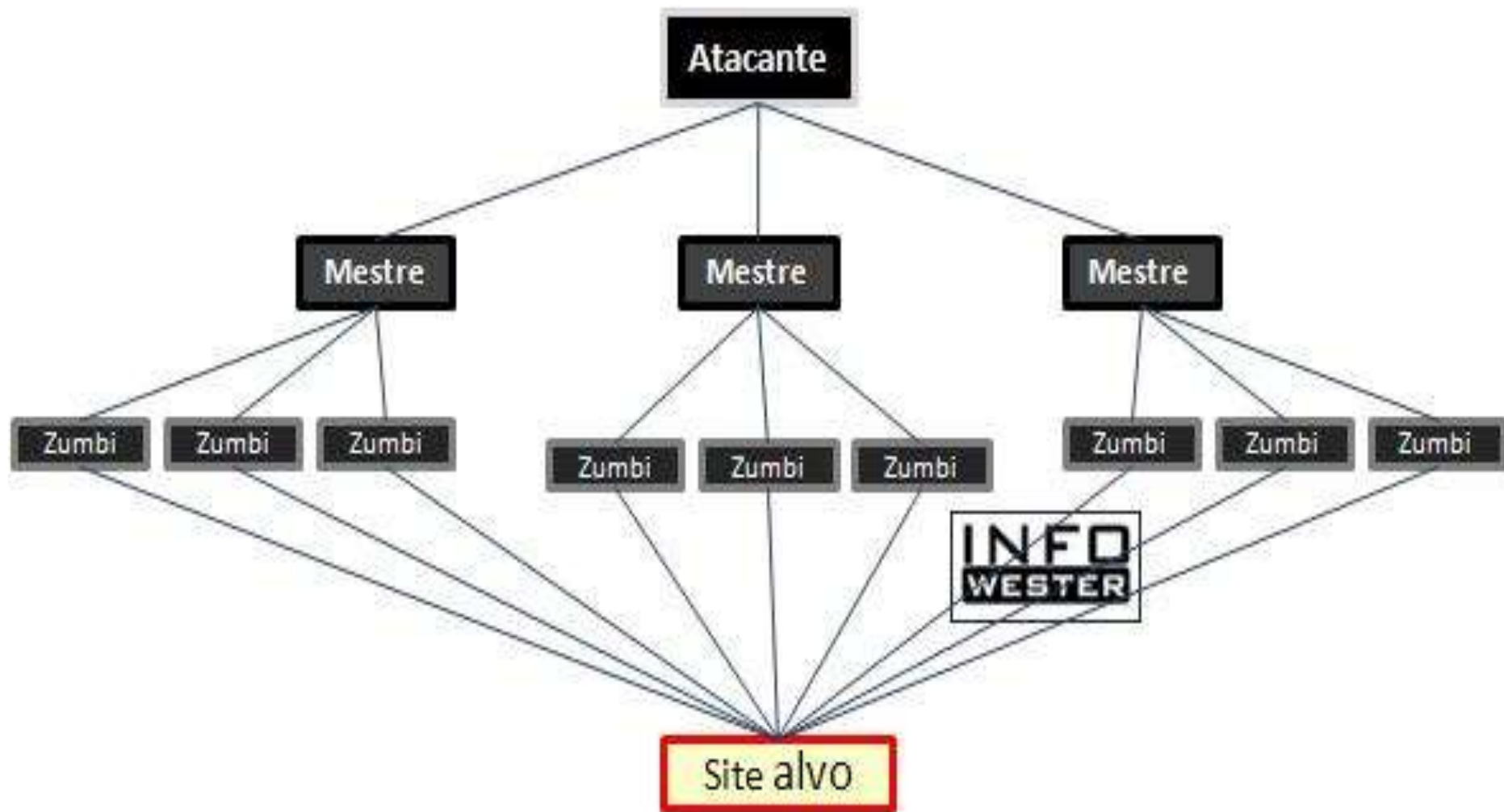
- ✗ Não visa invadir um computador para extrair informações.
 - ✗ Não modifica o conteúdo armazenado no computador.
 - ✓ Tornar inacessíveis os serviços providos pela vítima a usuários legítimos.
 - ✓ A vítima simplesmente para de oferecer o seu serviço aos clientes legítimos, enquanto tenta lidar com o tráfego gerado pelo ataque.
- 

DDoS

Distirbuted Denial of Service é como um super-DoS, onde várias pessoas se reúnem para atacar um servidor, onde uma só pessoa não vai fazer diferença.



DDoS



DDoS

Ataques por Inundação

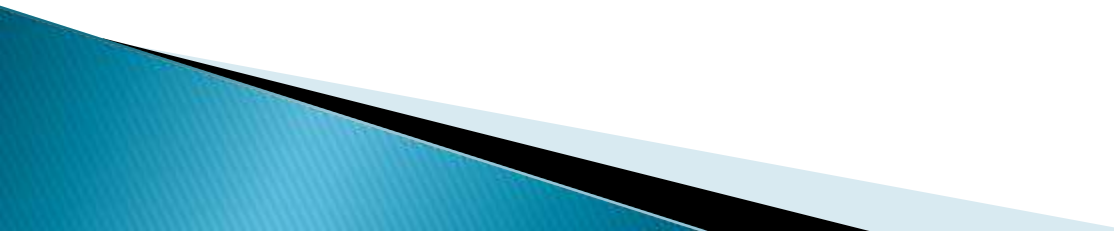


Se caracterizam por enviarem um grande volume de tráfego ao sistema da vítima primária de modo a congestionar sua banda. O impacto deste ataque pode variar entre deixar o sistema lento, derrubá-lo ou sobrecarregar a banda da rede da vítima. Ataques por inundação podem usar pacotes UDP (*User Datagram Protocol*) ou ICMP (*Internet Control Message Protocol*).

DDoS

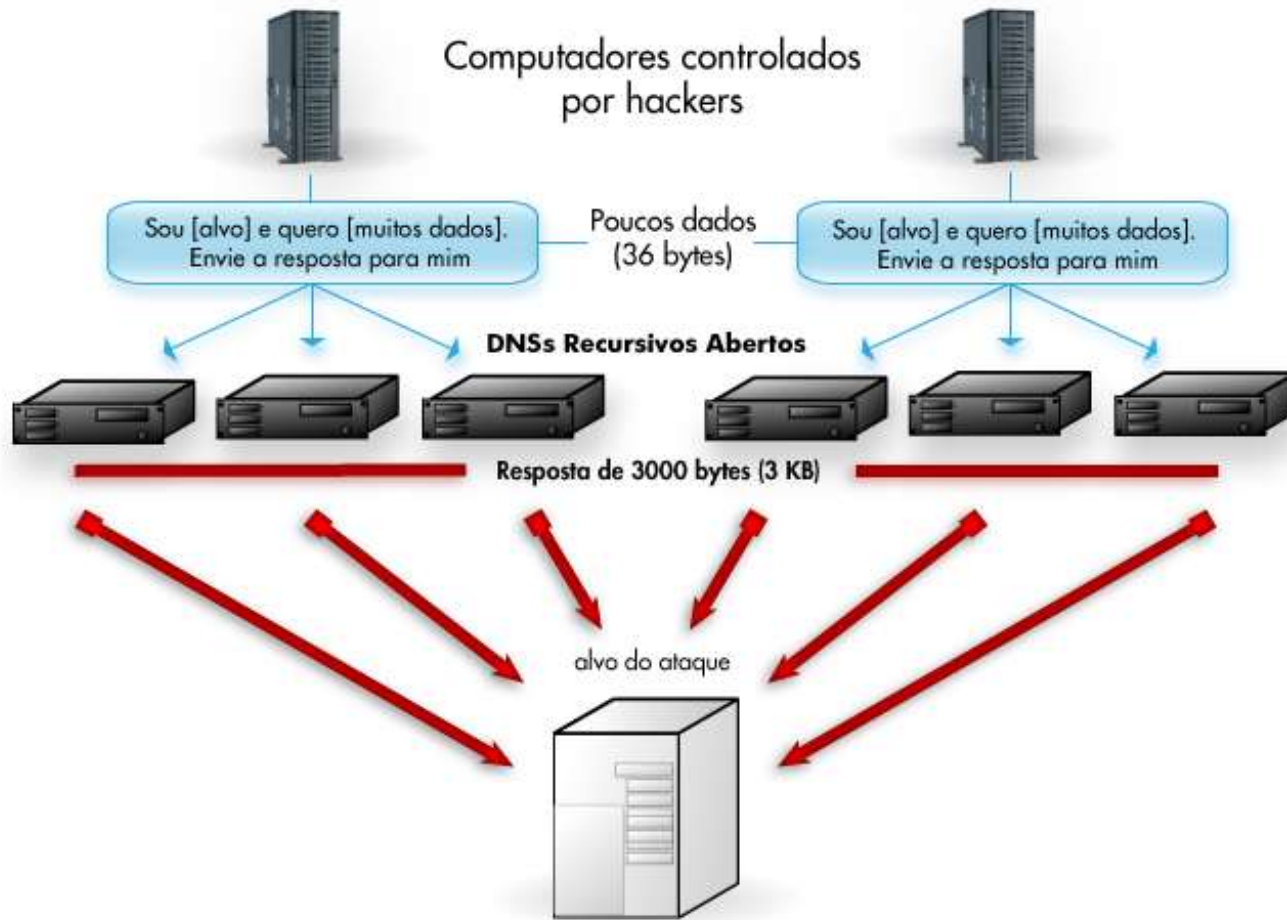
Ataques por Amplificação

Se caracterizam por enviarem requisições forjadas para uma grande quantidade de computadores ou para um endereço IP de broadcast, que por sua vez responderão às requisições. Forjando o endereço IP de origem das requisições para o endereço IP da vítima primária fará com que todas as respostas sejam direcionadas para o alvo do ataque.



DDoS por Amplificação

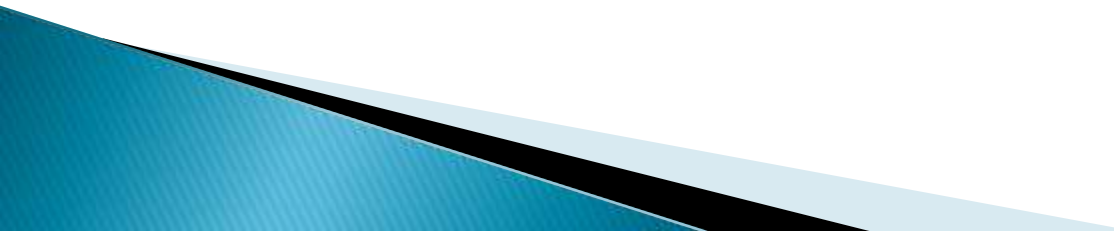
Ataque de negação de serviço distribuído refletido



DDoS

Ataques por Exploração de Protocolos

Se caracterizam por consumir excessivamente os recursos da vítima primária explorando alguma característica específica ou falha de implementação de algum protocolo instalado no sistema da vítima. Os principais ataques por exploração de protocolos são por uso indevido de pacotes TCP SYN (*Transfer Control Protocol Synchronize*) ou de pacotes TCP PUSH+ACK.



DDoS – Como se Proteger?


Combatendo ataques DoS ou DDoS

Como servidores podem ter estrutura e recursos diferentes, não há fórmula mágica que funcione em todas as implementações que consiga evitar ou combater ataques DoS. Cada caso é um caso, sem contar que, em boa parte das vezes, é difícil identificar o problema. Mas é possível contar com algumas armas para combatê-lo, embora nenhuma delas garanta 100% de proteção.



DDoS – Como se Proteger?

Dentre as estratégias recomendadas pode-se considerar as seguintes:

- Incrementar a segurança do host
 - Instalar *patches* de segurança
 - Aplicar filtros "anti-spoofing"
 - Limitar banda por tipo de tráfego
 - Prevenir que sua rede seja usada como "amplificadora"
 - Estabelecer um plano de contingência
- 

DDoS – Como detectar?

As ferramentas DDoS são muito furtivas no quesito detecção. Dentre as diversas propriedades que dificultam a sua detecção pode-se citar como mais significativa a presença de criptografia.

AUDITORIA – Comandos/Utilitários: Alguns comandos podem ser bastante úteis durante o processo de auditoria. Considerando os nomes padrões dos binários das ferramentas DDoS, é possível fazer uma auditoria por nome de arquivo binário usando o comando **find**.

DDoS – Como detectar?

O utilitário `lsof` pode ser usado para realizar uma auditoria na lista de processos em busca do processo *daemon* inicializado pelas ferramentas DDoS. Por último, se a sua máquina estiver sendo usada como master, o IP do atacante eventualmente poderia aparecer na tabela de conexões da sua máquina (`netstat`).

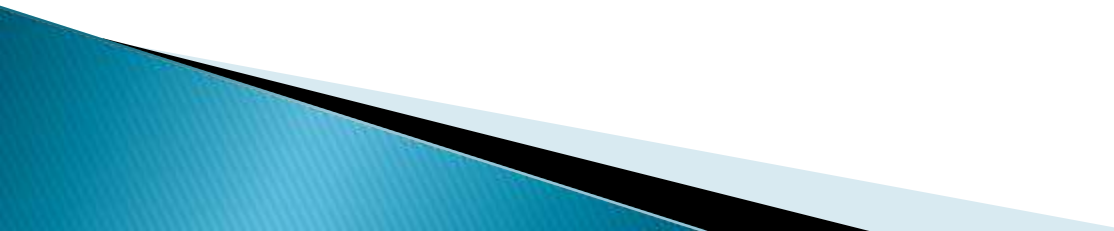
* Se tiver sido instalado previamente um *rootkit*, este IP não se revelará.



DDoS – Como detectar?

Ferramentas de auditoria de *host*: Ferramentas como o **Tripwire** podem ajudar a verificar a presença de *rootkits*.

Ferramentas de auditoria de rede: O uso de um *scanner de portas* pode revelar um eventual comprometimento da sua máquina. Lembre-se que as ferramentas DDoS utilizam portas padrões.



DDoS – Como detectar?

FERRAMENTAS DE DETECÇÃO ESPECÍFICAS

Uma variedade de ferramentas foram desenvolvidas para detectar ferramentas de ataque DDoS que, eventualmente, possam ter sido instaladas no seu sistema, dentre elas:

Linux

Find_ddos

Gag

DDS

Windows

Netstat – netstat –ano | find /c "80"

DDOs Tracer

Ataque DoS Simples

Exemplo:

```
ping IP -l 65500 -n 10000000 -w 0.00001
```

Onde:

-l = tamanho do buffer

-n = N° de requisições

-w = tempo limite para aguardar cada resposta (em milissegundos)

```
nslookup Nome do Site
```



Ferramenta de Ataque DoS

HttpDosTool



VIDA DE PROGRAMADOR

.COM.BR



#150

VOCÊ VIU ESSA ONDA DE ATAQUE
DE HACKERS?

ONDA? SEI...



É POR ISSO QUE EU MANTENHO
OS SERVIDORES DA EMPRESA
SEMPRE ATUALIZADOS!

VOCÊ ACHA MESMO QUE
OS SERVIDORES DAQUI
ESTÃO MAIS
ATUALIZADOS
QUE OS DO
GOVERNO?



CLARO! SAIU NA MÍDIA QUE O
PROBLEMA FOI UM ATAQUE
DE DOS*! AQUI TODOS SÃO
WINDOWS 2000, QUE
É BEM MELHOR!



*DDoS

OBRIGADO!

Carlos Henrique M. da Silva
carloshenrique.85@globo.com

- ▶ Formado em Análise de Sistemas
- ▶ Pós-Graduado em Auditoria em T.I.
- ▶ Gerente de TI da CLIOC – Coleção de *Leishmania* do Instituto Oswaldo Cruz – Fiocruz
- ▶ Certificado em Gestão de Segurança da Informação e Gerenciamento de T.I. pela Academia Latino-Americana (Microsoft TechNet / Módulo Security)

