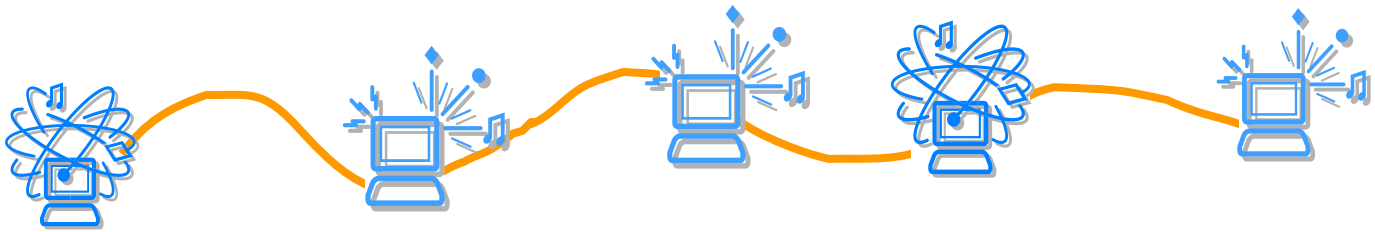
Segurança em Redes

Ameaças, vulnerabilidades e ataques



Redes de Comunicação de Dados

Departamento de Engenharia da Electrónica e das Telecomunicações e de Computadores

Instituto Superior de Engenharia de Lisboa

Tipos básicos de ataques na criptoanálise (PKCS 6)

Ataques de criptoanálise são geralmente classificadas em seis categorias que distinguem o tipo de informação que o criptoanalista tem disponível para montar um ataque. As categorias de ataque estão listadas aqui aproximadamente em ordem crescente da qualidade da informação disponível para o criptoanalista ou, equivalentemente, em ordem decrescente de nível de dificuldade para o criptoanalista. O objetivo do criptoanalista em todos os casos é ser capaz de decifrar os novos pedaços de texto codificado sem informações adicionais. O ideal para um criptoanalista é extrair a chave secreta.

- Um ataque somente ao texto cifrado (***ciphertext-only attack***) é um em que o criptoanalista obtém uma amostra do texto cifrado, sem o texto em claro associado a ele. Esses dados são relativamente fáceis de obter em muitos cenários, mas um ataque bem-sucedido apenas ao texto cifrado é geralmente difícil e requer uma amostra muito grande de texto cifrado.
- Um ataque com texto em claro conhecido (***known-plaintext attack***) é um ataque em que o criptoanalista obtém uma amostra do texto codificado e do texto em claro correspondente também.
- Um ataque com texto em claro escolhido (***chosen-plaintext attack***) é um no qual o criptoanalista é capaz de escolher uma quantidade de texto em claro e, em seguida, obter o correspondente texto cifrado criptografado.
- Um ataque adaptativo com texto em claro escolhido (***adaptive-chosen-plaintext attack***) é um caso especial de ataque com texto em claro escolhido onde o criptoanalista é capaz de escolher dinamicamente as amostras de texto em claro e alterar as suas escolhas com base nos resultados de criptografias anteriores.

Tipos básicos de ataques na criptoanálise (PKCS 6)

- Um ataque ao texto cifrado escolhido (***chosen-ciphertext attack***) é um no qual criptoanalista podem escolher um pedaço de texto cifrado e tentar obter o texto em claro correspondente. Este tipo de ataque é geralmente mais utilizado em criptosistemas de chave pública.
- Um ataque adaptativo ao texto cifrado escolhido (***adaptive-chosen-ciphertext attack***) é a versão adaptativa do ataque anterior. Um criptoanalista pode montar um ataque desse tipo num cenário em que tem a utilização gratuita de um equipamento de descodificação, mas é incapaz de extrair dele a chave usada.

Note-se que os ataques em criptoanálise podem ser montados não só contra os algoritmos de criptografia, mas também, de forma análoga, contra algoritmos de assinatura digital, algoritmos de MAC e geradores de números pseudo-aleatórios.

Tipos básicos de ataques na criptoanálise (PKCS 6)

Type of Attack	Known to Cryptanalyst
Ciphertext Only	• Encryption algorithm • Ciphertext
Known Plaintext	• Encryption algorithm • Ciphertext • One or more plaintext-ciphertext pairs formed with the secret key
Chosen Plaintext	• Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key
Chosen Ciphertext	• Encryption algorithm • Ciphertext • Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key
Chosen Text	• Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key • Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

Mas! A segurança é mesmo um grande problema?

Os ataques são reais ou apenas boatos?

- No âmbito do projecto Honeynet (http://honeynet.org) foi criada uma rede "*honeypot*" com um nome e conteúdos apelativos, em Julho de 2001, e verificaram que:
  - Um computador ligado Internet é "scanado" dúzias de vezes por dia;
  - Um servidor RedHat 6.2 sofre um ataque com sucesso ao fim de 72 horas (o tempo mínimo foi de 15 minutos!!);
  - Um máquina com Windows 98 "normal" foi atacada com sucesso 5 vezes em 4 dias.

Mas! A segurança é mesmo um grande problema?

- Mas porquê preocuparmo-nos com as máquinas dos “inocentes” que são infiltradas (“*hacked*”)?

- Não é um problema pessoal?

- Não nos devíamos preocupar apenas com os servidores?

- Nem por isso! **Máquinas infiltradas servem para realizar muitos tipos de ataques sob o controlo de, por exemplo, tróianos (*trojans*).** Ataques como, por exemplo, DDoS (*Distributed Denial of Service*). Podemos ser nós as próximas vitimas.

Maiores vulnerabilidades

Existem *sites* que se davam ao “luxo” de listar as maiores vulnerabilidades:

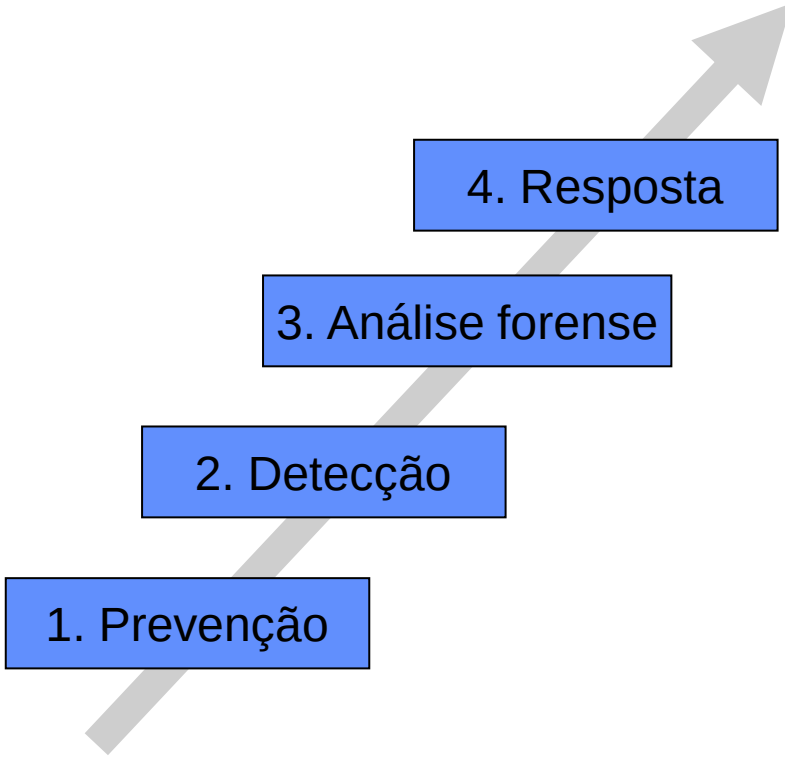
http://www.sans.org/top20/

Meia dúzias de perguntas para incrementar a segurança

Quem? O quê? Porquê? Onde? Como?

- As respostas às questões acima, no que diz respeito à segurança, varia de organização para organização.
  - **Quem** pode querer comprometer a nossa informação, fazer-nos mal, ter acesso aos nossos produtos e "por aí fora"?
  - **Que** é que os atacantes podem fazer e o que é que fizeram em outras organizações?
  - **Porque** é que a situação está como está agora?
  - **Quando** é que é mais provável os atacantes atacarem?
  - **Onde** é que o ataque se deve dirigir?
  - **Como** é que o irão realizar?

Quatro passos para o incremento da segurança



Categorias dos ataques

É muito difícil dividir os ataques conforme o tipo de técnica utilizada. Muitas delas são um misto de várias técnicas. A classificação aqui usada é mais uma possível:

- Técnicas para **obtenção de informações** (intrusão (***intrusion***))
- Técnicas de **negação de serviço** (**DoS** – ***Denial of Service***), distribuído (DDoS) ou não (DoS)
- Técnicas para **obtenção de acesso não autorizado** ("***control path***")

Categorias dos ataques

Os ataques também podem ser classificados de acordo com os seus efeitos:

- Ataques contra *routers*
- Ataques baseados em CGI (*Common Gateway Interface*)
- Ataques baseados em *browsers*

Obtenção de informações

Informações mais procuradas:

- Nome da máquina alvo
- Endereço IP da máquina alvo
- Topologia física ou lógica da rede
- Aplicações em execução no alvo
- Actualizações ou *patches* de correcção instalados
- Serviços disponíveis no alvo
- Portas em estado de escuta (*listening*)
- Senhas de utilizadores ou administradores do sistema

Obtenção de informações

Técnicas mais usadas:

- *Crack* de senhas
- *Varredura* (*scan*) de portas
- Utilização de utilitários

Crack de senhas

Este processo pretende:

- Obter a senha em texto claro
- Associar a senha ao respectivo utilizador

As formas de aceder às senhas são:

- Tentar aceder ao ficheiro de senhas, ou:
- Tentar obter as senhas através da captura na rede

Crack de senhas

As **técnicas para a quebra de senhas** podem utilizar:

- Método da força bruta
- Método do dicionário

- O **método da força bruta** testa todas as condições possíveis de caracteres até que uma combinação funcione.

- O **método do dicionário** emprega uma lista de palavras que pode ser geral, tipo dicionário, ou uma lista mais "trabalhada" tendo em conta o utilizador cuja senha se pretende descobrir.

Varredura de portas (*port scanning*)

Consiste em **testar os portos de uma máquina ou conjunto de máquinas** para verificar quais os portos que estão recetivos a estabelecerem ligações.

Objectivo: Saber quais as aplicações recetivas e qual o sistema operativo da máquina alvo

Existem algumas aplicações para tornarem esta tarefa mais simples, uma delas é o **SATAN** (*System Administrator Tool for Analyzing Networks*)

Varredura de portas (*port scanning*)

Existem várias formas de executar o *port scanning*:

Varredura padrão – Envio de TCP SYN para o alvo, é executado o *3-way handshake* completo e é estabelecida a ligação. Tem o inconveniente de deixar determinar a origem da varredura de forma fácil.

Varredura TCP SYN – É enviado um TCP SYN para o alvo mas a ligação não é terminada. O atacante a partir da resposta, TCP SYN/ACK ou TCP RST, pode tirar as conclusões sobre a porta. Este método de *scan* dificulta a descoberta da origem do ataque.

Stealth scanning – O pacote enviado simula uma ligação já existente. A forma como a máquina alvo responde dá as informações necessárias. Este método serve para tentar evitar os filtros afinados para os TCP SYN.

Utilização de utilitários

- Utilização de ferramentas de gestão para obter informações sobre o alvo.

- As ferramentas utilizadas são, por exemplo:
  - *Ping*
  - *Traceroute*
  - *Netstat e Nbtstat*
  - *Finger*

- As informações são mais limitadas mas as ferramentas são de uso fácil.

Sniffing passivo

- Necessita acesso à rede alvo.
- Técnica mais utilizada por atacantes internos
- Difícil de detectar
- Ferramentas, como o Wireshark, facilmente disponíveis
- Permite obter muitas informações implicando um elevado potencial de risco

- Entre as técnicas para minimizar os riscos contam-se:
  - Criptografia de dados e parâmetros
  - Utilização duma topologia de rede segura
  - Detecção de *sniffers* na rede

Nota: O Wireshark é mais um analisador de protocolos do que um *sniffer*

Ataques de negação de serviço (DoS e DDoS)

Tem, tipicamente, uma de duas intenções:

- Esgotar os recursos de uma máquina
- Esgotar a largura de banda de uma ligação em particular.

Em Fevereiro de 2000 um ataque DDoS "deitou abaixo" as ligações da eBay, Yahoo, CNN e outros durante várias horas.

Classificação dos ataques DoS

- Ataque à largura de banda
  - Inundar a rede e destruir a ligação
  - Necessários muitos recursos para ser lançado: ataque DDoS
- Ataque aos protocolos
  - Não tem de consumir toda a largura de banda
  - Exemplos: *SYN flood, smurf attack*
- Ataque à vulnerabilidade do software
  - São suficientes alguns pacotes
  - Exemplos: "*ping of death*" envia um super grande ICMP ECHO REQUEST e causa o *crash* dos computadores com protocolo mal implementado

Ataques de negação de serviço (DoS e DDoS)

Podem ser citadas as seguintes técnicas de negação de serviço:

- SYN *flood*
- *SSL request floods*
- LAND
- Ataques baseados em ICMP
- *Teardrop*
- *Ping o'Death*
- Ataques de dessincronização
- DDoS – *Distributed Denial of Service*
- SPAM: *Open mail relay*
- Controlo de congestão

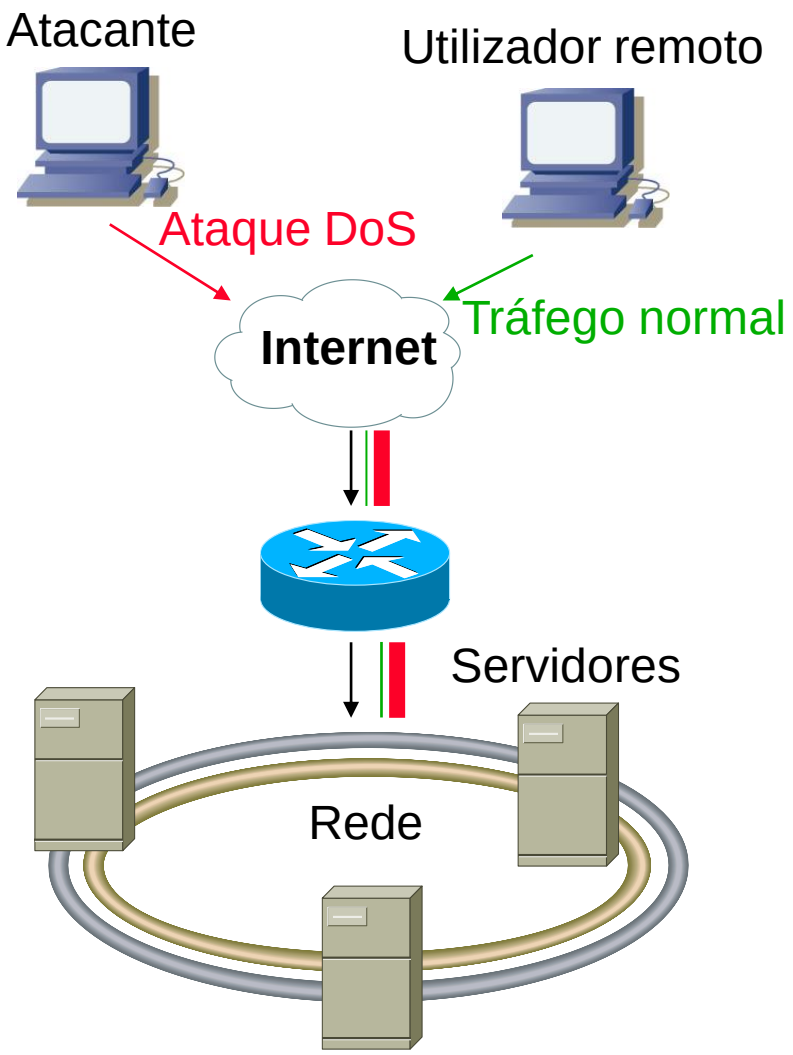
Ataques – SYN *flood*

Objectivo

Esgotar a capacidade de uma ligação através do envio de um "monte" de pacotes para uma determinada ligação.

Problema de implementação

O montar um ataque destes tem o problema dos recursos necessários ao ataque serem normalmente superiores aos que um utilizador doméstico possui.

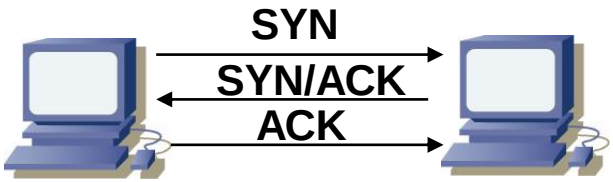


Ataques – SYN *flood*

Objectivo: Consumir recursos da máquina alvo.

Implementação mais comum:

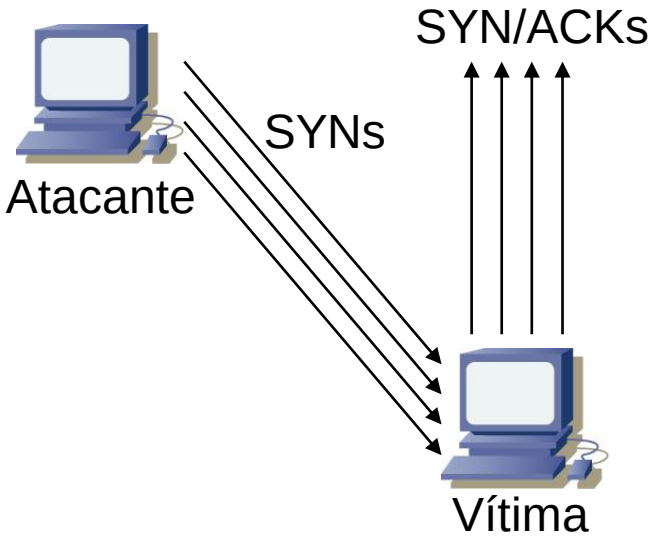
No SYN *floods* explora o *3-way handshake* do TCP.



O atacante envia pacotes SYN para a máquina vítima que vai para o estado SYN_RECD, devolve SYN/ACK e reserva recursos para poder estabelecer a ligação.

Ataques – SYN *flood*

Resultado: O atacante por cada pacote SYN enviado, quase sem custo algum, consegue que o destinatário reserve recursos. Se bombardear a vítima com pacotes SYN os recursos desta consomem-se rapidamente. Isto até que, por *timeout,* as ligações *half-open* comecem a ser fechadas.



Ataques – SYN *flood*

Eficiência:

Os **ataques mais eficazes de *flooding* utilizam muitos pacotes pequenos enviados o mais rapidamente possível**, dado que os *routers* não são tipicamente limitados pela largura de banda mas pelo ritmo de processamento de pacotes.

Existem muitas opções para efectuar ataques DDoS, nomeadamente utilizando UDP, ICMP, TCP SYN, etc.

Ataques – DoS: SSL *request floods*

Objectivo: Consumir recursos da máquina alvo.

Implementação mais comum:

Utilização do protocolo ***Secure Sockets Layer*** **(SSL)** utilizado para tornar as transações na Web seguras.

Da maneira como o SSLv3 está especificado, depois da mensagem ClientHello ser recebida pelo servidor, o servidor manda um certificado para o cliente e o cliente devolve um *pre-master secret* para a sessão, cifrado com a chave pública do servidor (do qual as chaves de sessão serão posteriormente derivadas). O objectivo do ataque é o cliente obrigar o servidor a realizar a tarefa de decifrar, utilizando o RSA (uma operação dispendiosa em termos de recursos), sem ele próprio ter de realizar trabalho a sério. Um estudo demonstrou que 800Kbps de tráfego era suficiente para colocar um servidor SSL fora de serviço.

Ataques – DoS: LAND ou *Loop*

Consiste no envio de um pacote TCP à máquina vítima com o endereço de origem igual ao endereço destino, portos de origem e de destino iguais e a *flag* de SYN activa.
Este ataque causa a exaustão de recursos.

O Windows Server 2003 e o Windows XP SP2, quando não utilizam o *firewall*, são vulneráveis a este tipo de ataque.

Existem outras versões deste ataque em que são alterados os campos de controlo do cabeçalho IP como os portos ou os bits de controlo.

Ataques – Baseados em ICMP

Implementação mais comum: *Spoofing* de endereços IP e ICMP

1. O mestre envia um comando para os escravos instruindo-os para iniciarem o ataque;

2. Os escravos enviam ICMP *echo requests* com o endereço de origem falsificado (*spoofed*) de forma a indicarem o endereço da máquina vítima;

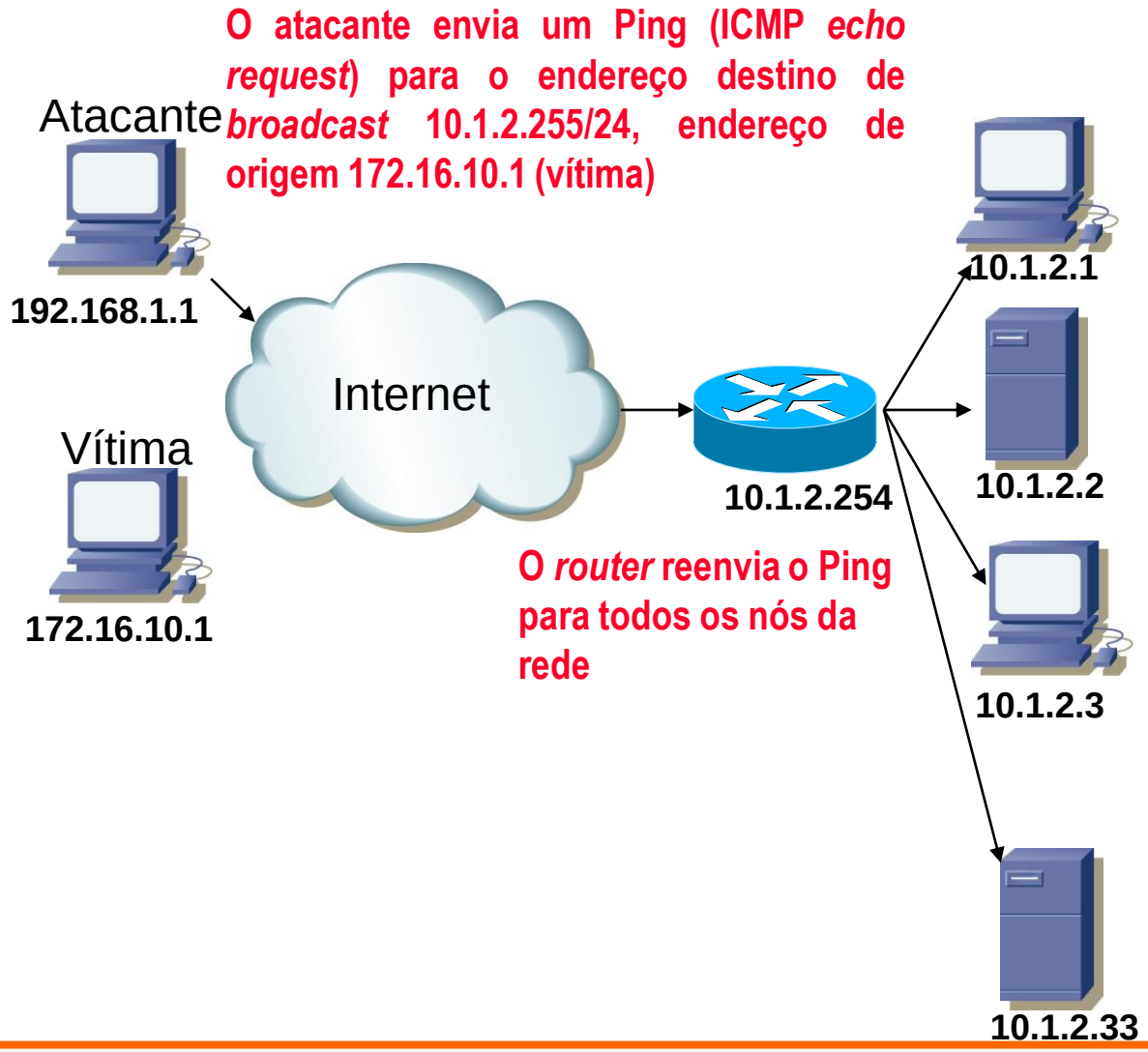
3. As máquinas destino dos ICMP *echo requests* enviados pelas máquinas escravas devolvem ICMP *echo reply* para a máquina vítima (cujo endereço constava no endereço de origem dos ICMP *echo requests*).

Ataques – Baseados em ICMP

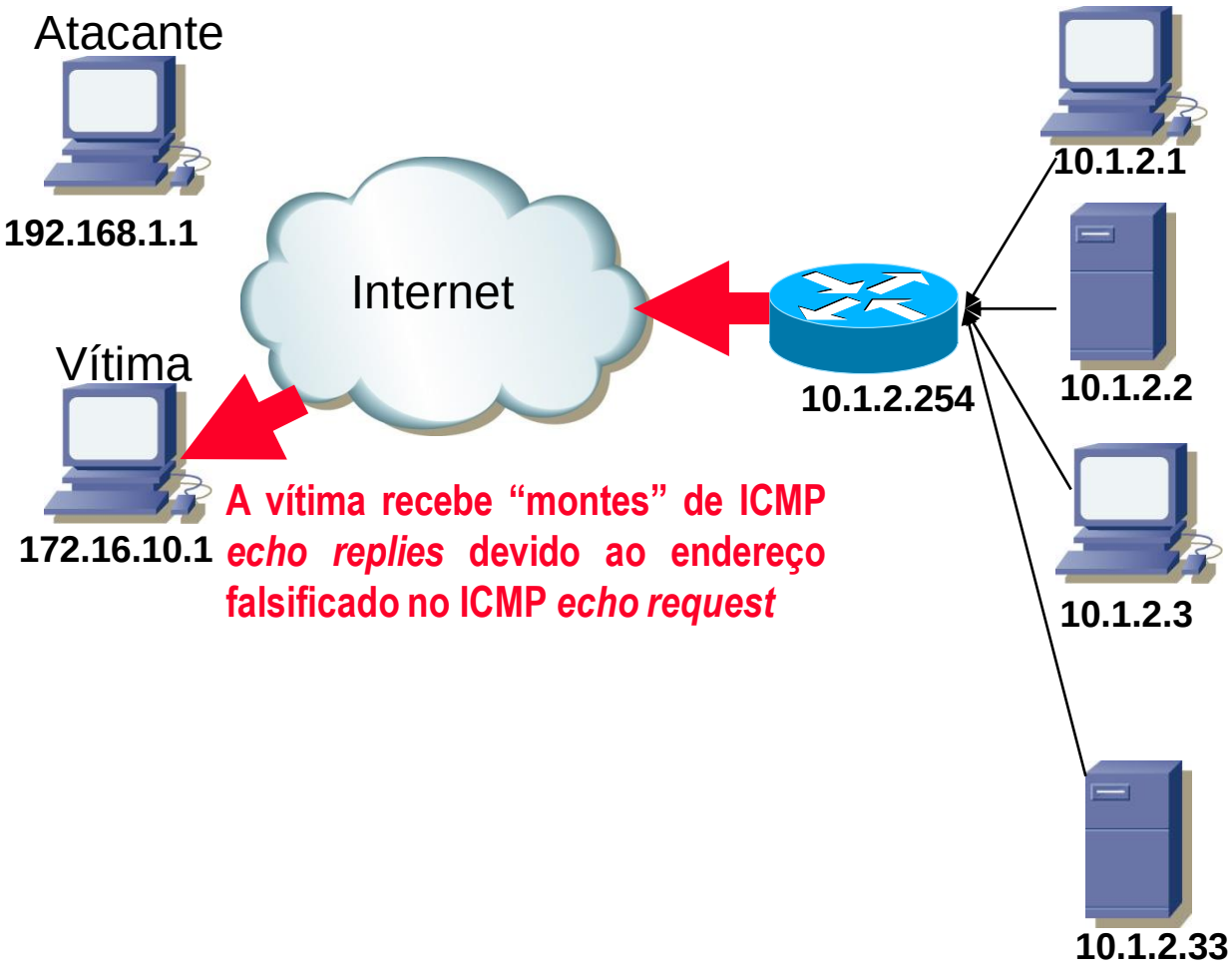
Formas mais eficazes deste ataque (???)

Algumas redes (*smurf amplifier networks*) respondem a ICMP *echo requests* enviados para o endereço de *broadcast*. Se o endereço de origem do ICMP *echo request* contiver o endereço da máquina vítima esta receberá muitos ICMP *echo replies* de resposta.

Ataques – Baseadas em ICMP: *Smurf amplifier networks*



Ataques – Baseadas em ICMP: *Smurf amplifier networks*



Ataques – Baseadas em ICMP: *Smurf amplifier networks*

Este tipo de ataque pode ser atenuado se nos *routers* que servem as várias redes se se colocar nas respetivas configurações algo como "***no ip directed-broadcast***".

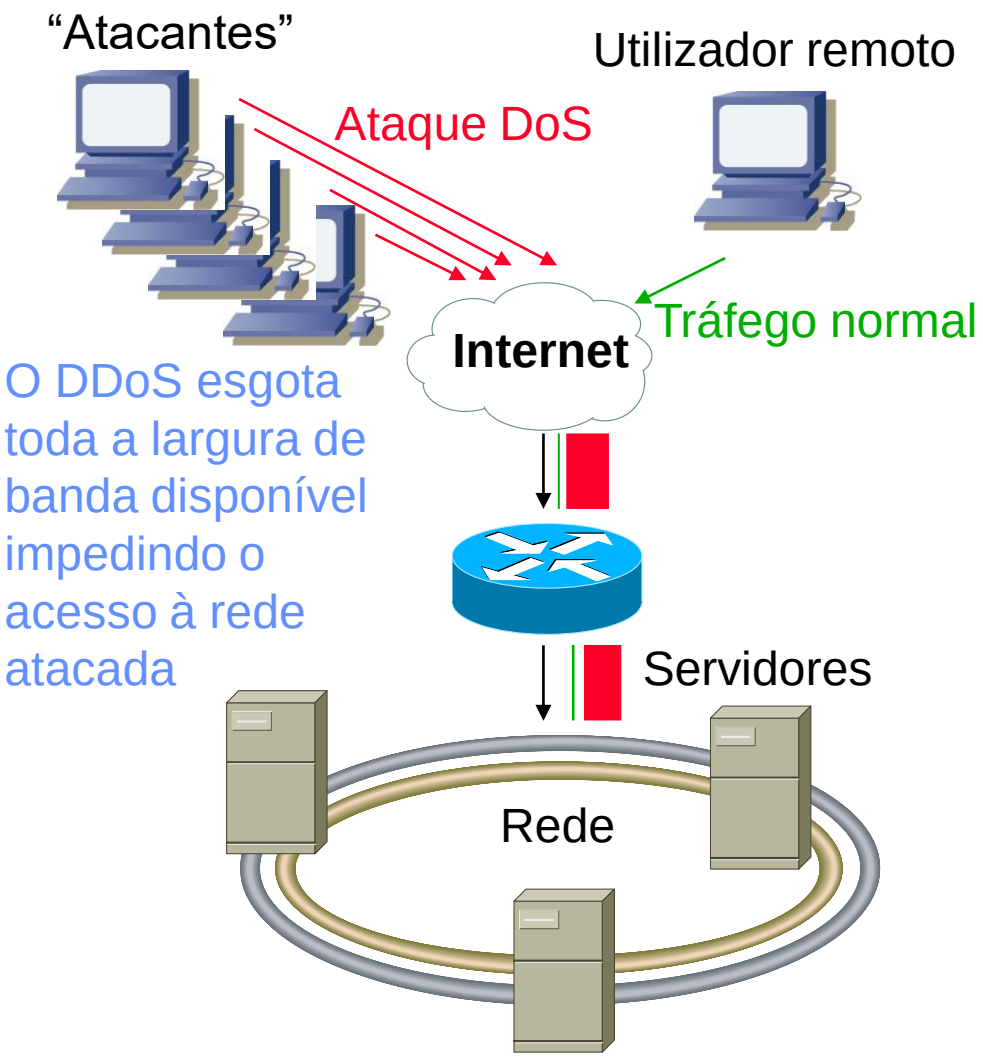
Existe também um movimento que tenta boicotar as redes que permitem a amplificação dos *broadcasts*. Tentam isto não permitindo que tráfego dessas redes passe para as redes que gerem, por exemplo:

> access-list 2 deny 128.118.0.0 0.0.255.255
> access-list 2 deny 129.24.0.0 0.0.255.255
> access-list 2 deny 129.111.0.0 0.0.255.255
> access-list 2 deny 129.100.0.0 0.0.255.255
> …….

Ataques – DDoS – "*Pong*"

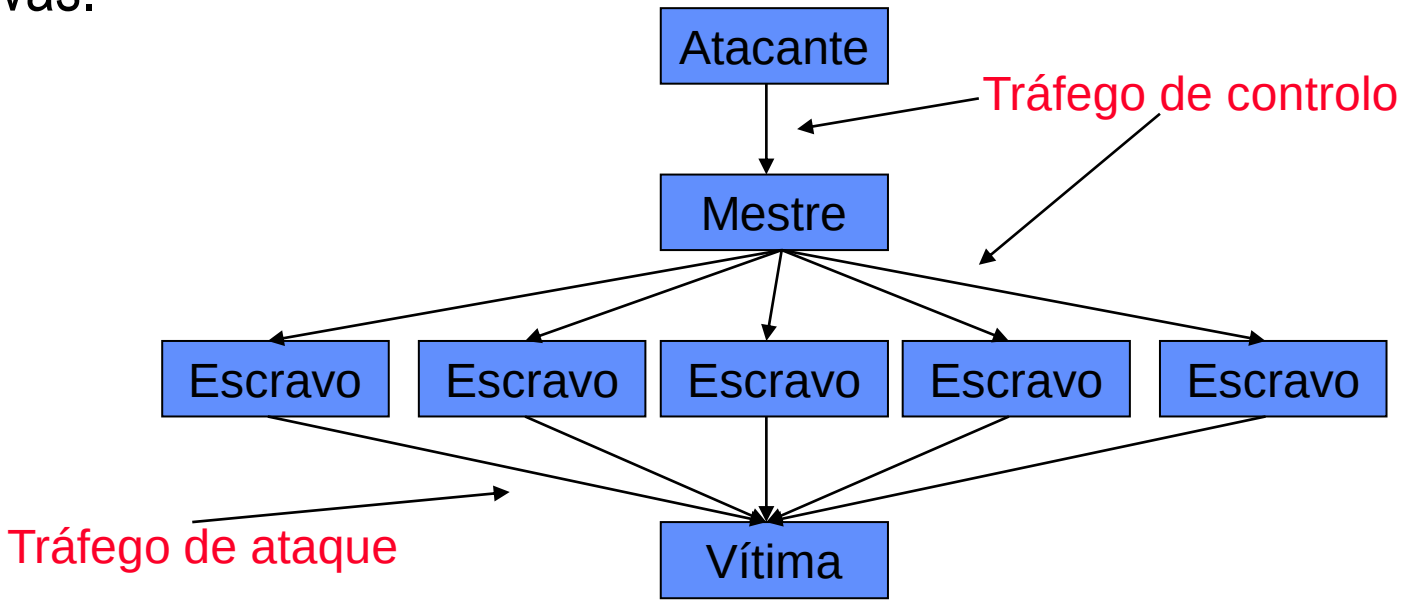
Um ataque DoS utiliza recursos limitados para realizar o ataque.

Um ataque DDoS tenta utilizar o maior número de recursos possível de maneira a amplificar os efeitos do ataque.



Ataques – DDoS – "*Pong*"

Solução: Obter o controlo de um grande número de máquinas para actuarem como "escravas".
Cada máquina escrava necessita enviar apenas uma pequena quantidade de tráfego para a máquina vítima. A ligação da vítima será ocupada por grandes quantidades de tráfego proveniente de todas as máquinas escravas.



Ataques – DoS: "*Teardrop*"

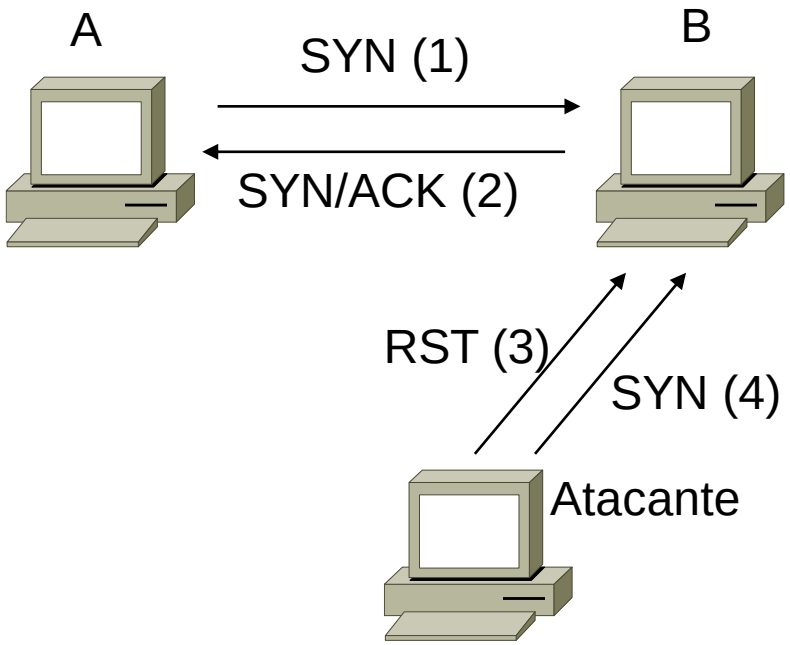
- Adulterar o cabeçalho de datagramas IP segmentados de maneira a causar problemas à máquina que os tenta refazer causando instabilidade e falhas.

Ataques – DoS: "*Ping o'Death*"

- É outra forma de utilizar o ICMP em ataques DoS.
- Consiste em enviar um ping com a dimensão além do limite máximo (65.535 bytes).
- É enviado em vários segmentos IP e o "problema" aparece quando a máquina destino tenta juntar os vários segmentos.

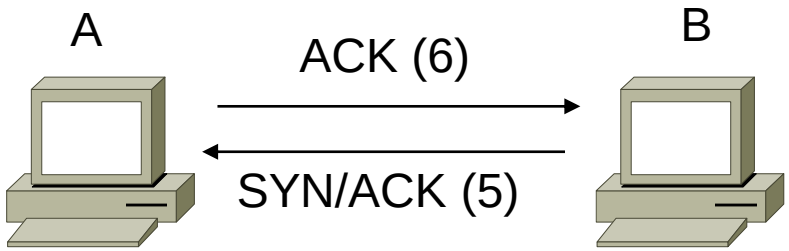
Ataques – DoS: Dessincronização

- Consiste em levar duas máquinas cuja ligação TCP está a ser monitorizada, a criarem um ligação dessincronizada. Ligação essa que não funciona mas que consome recursos.



Após a ligação entre as máquinas A e B, SYN (1) e SYN/ACK (2), o atacante envia um RST (3) seguido dum SYN (4) ambos com o endereço e o porto falsificados de A.

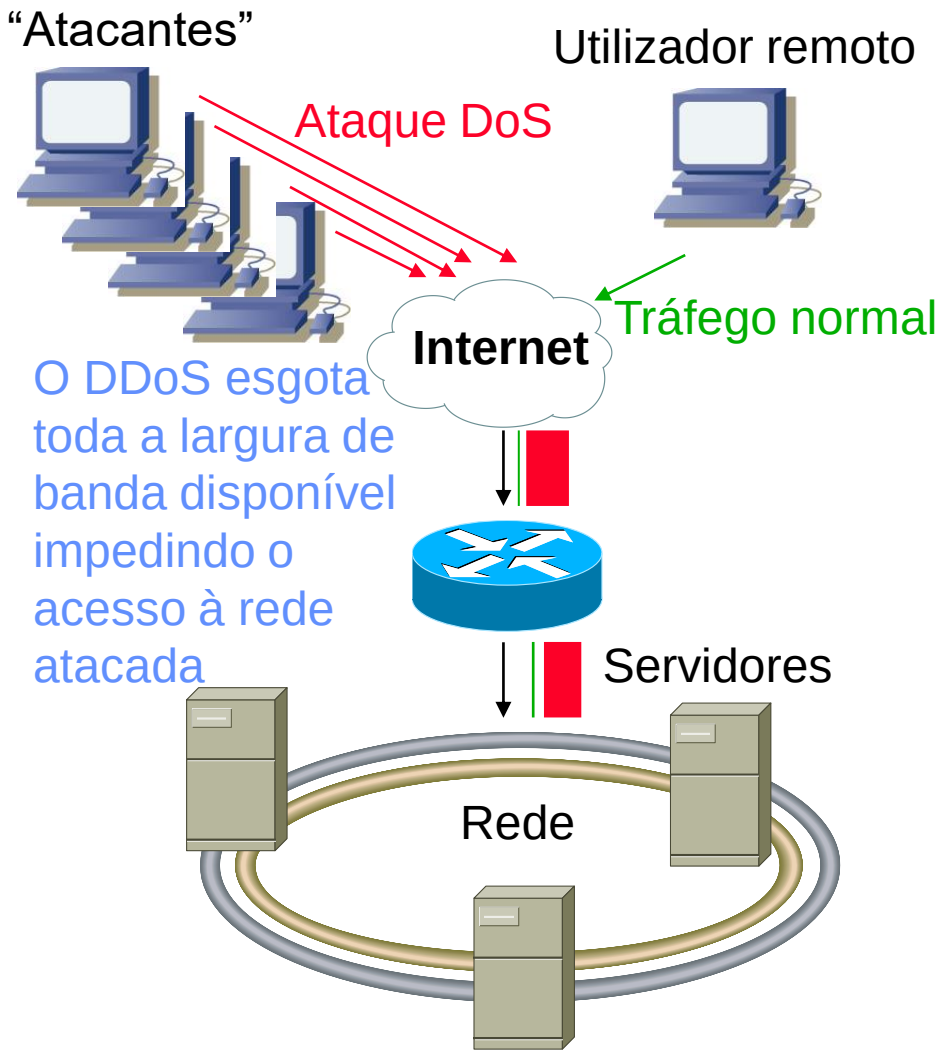
Ataques – DoS: Dessincronização



- Como resultado as máquinas estabelecem uma ligação que consome recursos mas que não pode funcionar dado os números de sequência não coincidirem.

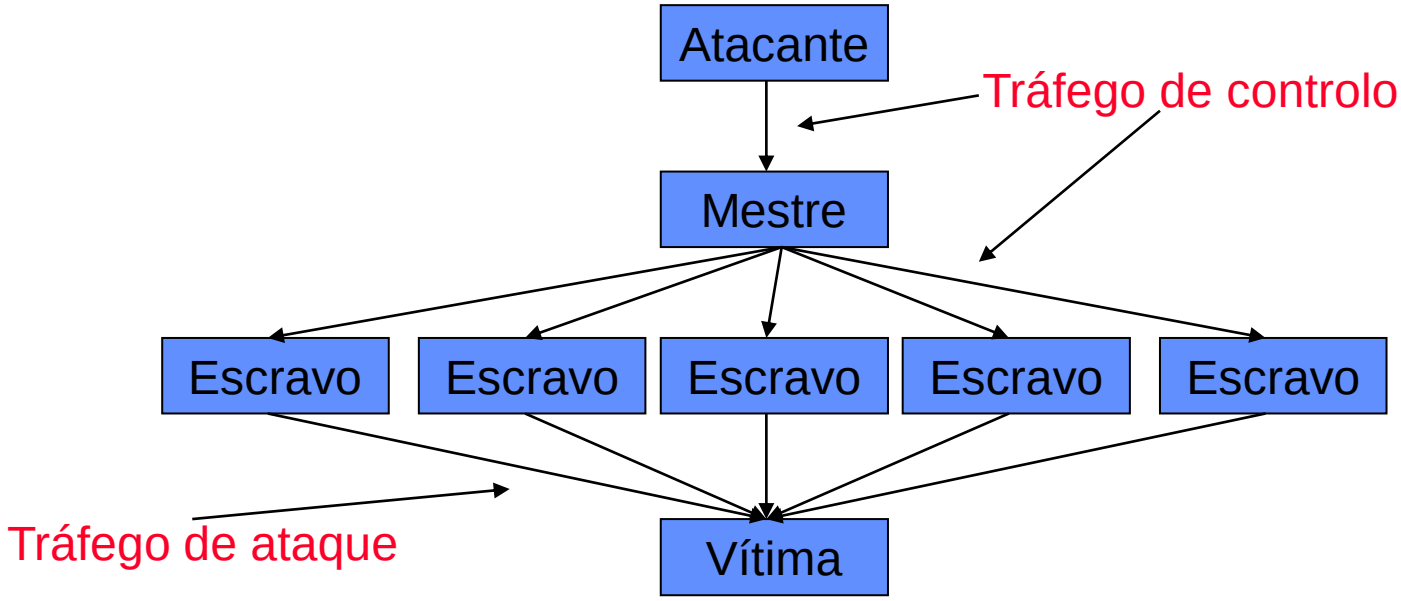
Ataques – DDoS: SYN *flood*

Ataque algo semelhante ao Pong mas em que os pacotes enviados são TCP SYN.



Ataques – DDoS: SYN *flood*

Solução: Obter o controlo de um grande número de máquinas para actuarem como "escravas".
Os recursos da máquina vítima esgotam-se rapidamente face ao grande número de pedidos de estabelecimento de ligação.



Ataques – DDoS: SYN *flood*

É colocado software específico no mestre e nos escravos para que estes fiquem prontos a "funcionar". Existe muito software que pode dar suporte a este tipo de ataque, entre ele o TFN, Stacheldraht e o Trinoo. Este software é colocado nas máquinas que irão servir de mestres e de escravos através de várias artimanhas como vírus, etc. Pode-se encontrar uma boa descrição da utilização de *Bots* em:

http://honeynet.org/papers/bots/

É díficil determinar a identidade do atacante dada a natureza distribuída do ataque DDoS.

Um exemplo deste tipo de ataque é narrado em:

http://web.stanford.edu/class/msande91si/www-spr04/readings/week1/grcdos.pdf

Ataques – DoS: SPAM: *Open mail relay*

De certa forma **o SPAM pode ser considerado um ataque do tipo DoS**.

Os *spammers* utilizam uma de várias formas para enviar *emails*. Uma das formas que era popular era a utilização de um ***open mail relay*** **(um servidor de emails que recebia emails de toda a gente e enviava para toda a gente**). A vantagem era que o *spammer* não necessitava ter uma ligação de alto débito bastando enviar uma mensagem com o número de destinatários que quisesse no campo To:. O servidor *relay* realizava o resto do trabalho. Como este tipo de servidores têm vindo a desaparecer os *spammers* têm de recorrer a recursos próprios adquirindo as próprias ligações de alto débito.

Ataques – DoS: Controlo de congestão

Quando um cliente TCP “desconfia” que existe congestão na rede pode utilizar os mecanismos de controlo de congestão para tentar diminuir a congestão na rede e recuperar alguma largura de banda. Isto pode implicar reduzir o seu tráfego de saída.

Um ataque possível é levar a máquina vítima a “pensar” que existe congestão de maneira a levá-la a diminuir o tráfego.

Técnicas para obtenção de acesso não autorizado (intrusão)

Técnicas utilizadas:

- *Spoofing*
- *Active sniffing*
- *Buffer overflow*
- Exploração de relacionamentos de confiança
- Ataques de fragmentação
- Ataques baseados em números de sequência
- *Trojans* (tróianos)

Ataques – Intrusão

Existem muitos ataques deste tipo os quais são resultado, na sua maioria, de má implementação da segurança nas máquinas (por exemplo, a exploração do *buffer overflow*).

Os ataques do tipo intrusão que serão aqui referidos são os relacionados com:

- **fraquezas dos protocolos de rede**, sobretudo no TCP
- **problemas de autenticação na Web**
- **ataques ao nível da camada de ligação** (*link layer*).

Técnicas de intrusão – *Spoofing* IP

Utilização de um endereço IP falso de maneira a fazer-se passar por outra máquina.

É usado para **explorar uma relação de confiança ou um mecanismo de autenticação baseados em endereços IP** como o NFS (*Network File System*) e os serviços de *proxy* do MS Windows NT.

Será mais fácil atingir os objectivos de intrusão se o atacante puder abrir uma ligação em vez de se inserir numa ligação já em curso. Este método é bastante complicado.

Estabelecer uma ligação fazendo-se passar por outro tem de prever que a máquina verdadeira não pode responder pelo que não deve estar activa ou deve estar ocupada com um ataque DoS.

Técnicas de intrusão – *Spoofing* IP

Este tipo de ataque é mais fácil de realizar quando aplicado sobre UDP. No TCP tem o problema dos números de sequência.

Este ataque é mais bem sucedido se for realizado da mesma rede local (mesmo prefixo de rede) que o da máquina alvo. Se for de outra rede a simulação do IP pode ser detetada pelo *router* ou por *firewalls* bem configurados.

https://www.iplocation.net/find-ip-address

Técnicas de intrusão – *Spoofing* DNS

Uma forma de *spoofing* utilizado é a alteração da base de dados dum servidor DNS para fazer corresponder um URL ao um determinado endereço IP, por exemplo o do atacante.

Se a página do atacante for forjada para se parecer com a de outra entidade por quem se está a tentar fazer passar (*phishing*) pode implicar que a vítima forneça informações sensíveis ou obtenha dados falsos.

Técnicas de intrusão – *Active sniffing*

Variação da técnica de *passive sniffing*. Consiste na captura, alteração e posterior envio de pacotes, sem interromper a comunicação.

As técnicas de prevenção são semelhantes às do *passive sniffing*.

Técnicas de intrusão – *Buffer overflow*

Métodos destinados a explorar vulnerabilidades de sistemas operativos e aplicações.

Princípio comum: Muitos processos são executados por contas que possuem direitos muito amplos, normalmente equivalentes aos direitos de administrador ou *root*. É o caso da conta SYSTEM do MS Windows NT ou da conta HTTPD em UNIX.

O estudo do software que corre numa máquina pode levar ao conhecimento de situações em que o enviar de mais parametros do que o software é capaz de tratar, ou está à espera, leva a uma situação de *buffer overflow* a qual, quando bem planeada, pode levar à execução de software do atacante.

https://www.owasp.org/index.php/Buffer_Overflow

Técnicas de intrusão – Relação de confiança

Relações de confiança que se estendem a vários sistemas. Disponível em sistemas UNIX e MS Windows NT. O objectivo é simplificar a gestão de sistemas.

O comprometimento de um sistema faz comprometer vários.

Por exemplo, no UNIX, um atacante que consiga aceder a **/etc/hosts.equiv** e **~/.rhosts** pode dizer que é de confiança ou que possui uma máquina de confiança (que irá servir para atacar as outras).

Técnicas de intrusão – Ataques de fragmentação

Servem para testar limitações nas funções de filtragem de pacotes em *routers* e outros dispositivos de rede.

Consiste no envio de pacotes fragmentados de maneira a que o bit de SYN não esteja activo no primeiro segmento, mas num dos seguintes. Isto para enganar os filtros de segurança.

Técnicas de intrusão – Ataques baseados em ISN ou TCP *connection hijacking*

São técnicas complexas.

O atacante pretende intrometer-se numa ligação fazendo-se passar por uma das máquinas envolvidas. Utilizam técnicas complexas.

O fundamento desta técnica é a previsão dos números de sequência iniciais (ISN). Uma vez este descoberto o resto é fácil.

Técnicas de intrusão – TCP *connection hijacking*

A maioria dos ataques ao TCP são deste tipo – o *spoofing* de endereços IP permite a uma máquina passar-se por outra.

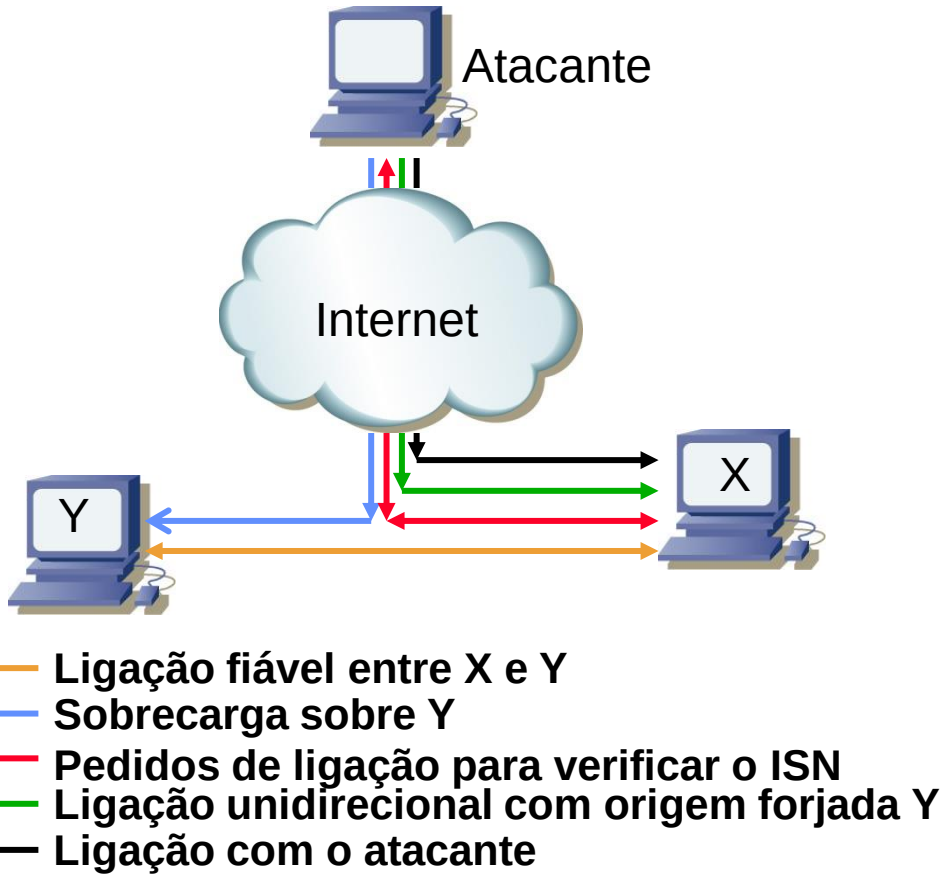
Serviços antigos como o *rsh* autenticavam uma máquina apenas pela origem dos pacotes.

Um ataque deste tipo permite utilizar uma ligação TCP de outro utilizador ou fazer parecer que a ligação está a ser estabelecida de outra origem qualquer.

Técnicas de intrusão – TCP *connection hijacking*

Para realizar um ataque deste tipo são necessários vários passos:

1. Fazer *spoofing* dos endereços IP dos pacotes;
2. Descobrir o número de sequência inicial (ISN) que o servidor enviará ao cliente no estabelecimento da ligação;
3. Ter a certeza que o cliente *spoofed* não responde ao servidor (por ex. enviando-lhe um pacote de FIN).



Técnicas de intrusão – TCP *connection hijacking*

O primeiro e o terceiro passo são relativamente fáceis de realizar, embora existam algumas defesas contra o primeiro). **A parte dificil é descobrir qual o número de sequência inicial (ISN)** que o servidor retorna ao endereço IP *spoofed*.

Como pode ser feito? **O atacante pode realizar algumas ligações TCP verdadeiras, legitimas, ao servidor e verificar qual o padrão pelo qual o ISN incrementa**, e assim tentar adivinhar de uma forma mais precisa qual o número de ISN retornado na ligação de que quer tentar fazer *hijacking*.

Anteriormente **este número era bastante previsível**. **Actualmente o ISN sofre um incremento aleatório** o que parece ser uma solução razoável para o tipo de ataque.

Técnicas de intrusão – TCP *connection hijacking*

Historicamente o aumento aleatório do ISN parece não resolver este problema.

A utilização de geradores de números aleatórios (PRG) maus leva a que seja possível prever qual o próximo número aleatório que vai ser "gerado" analisando alguns dos anteriormente gerados.

http://www.infosecwriters.com/text_resources/pdf/SKapoor_SessionHijacking.pdf

Técnicas de intrusão - Autenticação de clientes Web

Um estudo recente mostrou que, em muitos casos, se **utilizam meios muito fracos para a autenticação dos clientes**. Dado que o SSL/TLS é um pouco pesado para se ter a certeza de que alguém está autorizado a ler um jornal, por exemplo. Algumas empresas desenvolveram meios "caseiro" de "autenticação" mais leves os quais permitem as infiltrações com relativa facilidade. Muitos dos problemas relacionados com clientes Web têm a ver com o facto do HTTP ser um protocolo "*stateless*".

Técnicas de intrusão - Ataques ao nível 2

As redes *wireless* 802.11 transmitem dados através do rádio; os dados enviados podem ser protegidos através duma facilidade definida pela norma e que se designa por WEP (*Wireless Equivalent Privacy*) a qual cifra os dados antes de serem transmitidos.

Em Agosto de 2001 a cifra foi quebrada. A partir daí a utilização do WEP teve de ser repensada.

Ataques – Controlo

Os ataques descritos a seguir embora menos comuns podem ter consequências bem mais dramáticas que os anteriormente descritos.

Como é do conhecimento a Internet não funcionava sem protocolos de *routing* (por exemplo, OSPF e BGP) e de resolução de nomes (por exemplo, DNS). O ataque a estes mecanismos pode, em certos casos, resultar em sérios problemas.

Ataques – Controlo: Ataques à resolução de nomes

O ***Domain Name System*** **(DNS)** é utilizado para relacionar nomes (por exemplo, www.isel.pt) com endereços IP (por exemplo, 193.137.220.0). Um ataque que seja gerado para degradar o funcionamento do DNS pode ter consequências graves.

Como se pode implementar um ataque desses?
Uma forma é realizar um ataque aos servidores de domínios de topo (*top-level domain servers*) como, por exemplo, aqueles que mantêm os servidores com autoridade para os domínios .com, etc.
Existem 13 servidores DNS de topo, replicados utilizando anycast pelo que não é fácil efectuar um ataque DDoS aos mesmos.

Ataques – Controlo: Ataques ao *routing*

Estes ataques consistem em ataques aos protocolos de *routing* (BGP, OSPF, etc.). A segurança destes protocolos está ligada à segurança dos protocolos abaixo, por exemplo TCP, UDP e IP. Um ataque TCP *hijacking* a uma sessão BGP então o atacante pode inserir mensagens de *routing*. A autenticação das mensagens BGP pode minorar este problema.

Problemas mais graves advêm da validação de mensagens provenientes de sistemas autónomos (AS) vizinhos. É complicado, do ponto de vista administrativo, decidir quem pode ou não anunciar prefixos assim como validar todos os atributos nas mensagens BGP.

Ataques – Controlo: Ataques ao *routing*

O "*black holing*" (enviar para um "buraco negro") é um problema resultante da perda de conectividade por alguém anunciar que tem acesso a um prefixo que afinal não tem.

Solução: Utilizar antigas tecnologias como o telefone analógico para telefonar e "chamar nomes" ao "artista" que cometeu o erro e anunciar custos superiores para essa região de endereços até o problema ser resolvido.

Ataques – DoS: SPAM: *Drive-by*

Outra forma de ataque de SPAM é a utilização de ataques de intrusão e de "*control path*" para enviarem SPAM.

A técnica denominada "*drive-by*" tem vindo a ganhar popularidade: um *spammer* consegue largura de banda ligando-se a uma rede *wireless* sem protecção, enviando um "monte" de *emails* e saindo. Neste tipo de ataque é relativamente difícil descobrir-se a origem.

Para tornarem a origem dos ataques mais difíceis de descobrir os atacantes também podem utilizar as estruturas de *routing* a seu favor anunciando blocos de prefixos, enviando *emails* com endereço de origem nesses blocos e depois retirando os prefixos. Este método é utilizado igualmente noutros ataques.

Defesas: Ataques DoS/DDoS

- Existem dois tipos de defesas básicas para este tipo de ataques:
  - **Pro-activas**: Tentam principalmente evitar o ataque;
  - **Reactivas**: Tentam minimizar as consequências dos ataques após estes começarem.

Defesas pro-activas: Ataques DoS/DDoS

Defesas contra ataques SYN *flooding* e SSL *connection flooding*

O principal problema é que o atacante pode obrigar as vítimas a ter trabalho com um esforço mínimo da parte deste. Podem-se usar as seguintes soluções:

1. A vítima (servidor) pode atrasar a atribuição de recursos/efectuar trabalho até o mais tarde possível
2. Forçar o atacante (cliente) a efectuar algum trabalho antes do alvo efectuar qualquer trabalho

Defesas pro-activas: Ataques DoS/DDoS (1)

SYN *cookies*

Quando o servidor recebe um pacote SYN de uma máquina em particular, devolve um SYN/ACK a essa máquina, mas não passa ao estado SYN_RECD. Em vez disso calcula o número de sequência inicial (ISN) que deve ser utilizado nessa ligação baseando-se num *hash* das propriedades da ligação:

ISN=hash(src_addr, src_port, dst_addr, dst_port, key)

Onde *key* é uma chave secreta específica do servidor.

Defesas pro-activas: Ataques DoS/DDoS (2)

SYN *cookies* (cont.)

Quando o terceiro pacote no *3-way handshake* retorna o servidor apenas necessita testar se o *hash* dos parâmetros do ACK condiz com o ISN (mais um). Se assim for o servidor pode atribuir os recursos para dar suporte à ligação.

A chave secreta deve ser alterada com alguma frequência para prevenir a utilização do mesmo ISN da mesma origem posteriormente. Um tempo entre alterações próximo do máximo RTT possível parece uma boa escolha.

Defesas pro-activas: Ataques DoS/DDoS

Client puzzles

Uma forma semelhante de evitar os ataques a servidores SSL (e ataques SYN *flood*), conhecidos também como ***connection depletion attacks***, é requerer que o cliente faça algum trabalho antes do servidor concordar em estabelecer a ligação. O nome típico é ***client puzzle***. O *puzzle* é normalmente uma inversão parcial de uma função de *hash* criptográfica:

S->C: m',H(x **o** m')=h

C->S: x

Onde o número de bits de x pode ser escolhido conforme a dificuldade que se pretenda para o problema (mais bits -> mais tempo para a resolução).

[http://www.cs.jhu.edu/~fabian/courses/CS600.624/slides/week6.pdf]

Defesas pro-activas: Ataques DoS/DDoS

Prevenção de DDoS

Não é um problema com uma solução fácil.

Os operadores de rede podem ter uma palavra a dizer. Podem ser colocados ***ingress* e *outgress filters*** nos *routers* de fronteira para controlarem os endereços de origem dos pacotes que os atravessam. Isto dificulta o *spoofing* de endereços IP.

Uma defesa razoável contra **ataques de amplificação** é **não receber ou responder a tráfego de *broadcast***, excepto de origens especificas (por ex. clientes DHCP).

Defesas pro-activas: Ataques DoS/DDoS

***Prevenção de DDoS* (cont.)**

- Se o ISP conhecer os padrões de tráfego da sua rede pode aplicar ***traffic shaping*** a determinadas classes de tráfego, por exemplo os pacotes SYN e ICMP pdem ser limitados.
- **Sistemas de detecção de intrusões (IDS)** podem detectar anomalias em padrões de tráfego ou reconhecer certos tipos de ataques através das suas assinaturas. Não funciona para novos ataques cuja assinatura ainda não é conhecida.
- Defesas contra o **SPAM** são dificeis. A mais agressiva até agora é tentar **evitar que haja *relay mail servers*** activos. Algumas organizações como http://www.trendmicro.com/us/security-intelligence/current-threat-activity/global-spam-map/ mantêm informação sobre este tipo de tráfego. Esta técnica não ajuda no caso de técnicas de *spamming* diretas.
- Existem igualmente disponíveis listas de servidores que enviam SPAM.
- Pode testar o seu servidor de *email* aqui.

Defesas reactivas: Ataques DoS/DDoS

O **primeiro passo** de qualquer mecanismo de defesa reactiva a um ataque DoS é **classificar o tráfego** (de onde vem? De que tipo é? Está a ocorrer numa porta específica?).

Isto pode ser díficil de realizar. Um truque usual é utilizar ***Access Control Lists*** **(ACL)** que permitam os outros pacotes mas que classifique os pacotes do ataque. Uma vez feita a classificação podem ser executados os passos para **limitar o débito ou filtrar esse tráfego**.

O problema é que **o atacante pode alterar os padrões de tráfego** de ataque (endereço de origem, portos, etc.) pelo que o ato de classificar e bloquear um ataque pode ser algo como o **jogo do gato e do rato**.

Defesas reactivas: Ataques DoS/DDoS

Pushback

Uma forma de limitar o débito do atacante é realizar *pushback*. Para isto ser possível um *router* tem de poder pedir aos *routers* acima (*upstream*) que limitem um determinado tipo de tráfego.

Tem alguns problemas como a implementação, a autenticação das mensagens de *pushback* e o efeito desta técnica nos outros tipos de tráfego.

Defesas reactivas: Ataques DoS/DDoS

Traceback

Pode ser útil, para além de se minimizarem os efeitos de um ataque, descobrir qual a origem do mesmo. A ideia base é a de que uma rede vítima de um ataque pode dizer com relativa facilidade de que vizinho provem um ataque. O operador da rede atacada pode contactar o operador da rede vizinha para este realizar um *trace*, e assim sucessivamente até à rede de destino.

Existem tentativas de automatizar este processo.

Defesas reactivas: Ataques DoS/DDoS

Traceback

Porque é que o *traceback* é dificil? A razão principal é o facto dos endereços de origem serem normalmente *spoofed*, escondendo a origem real dos pacotes.

A auditoria das ligações pode consumir uma grande quantidade de recursos e os *logs* dos *routers* podem ocupar muito espaço.

Existem outros métodos utilizam a marcação probabilística de pacotes para seguirem os grandes fluxos.

Defesas reactivas: Ataques de intrusão

TCP *connection hijacking*

Como referido, o incremento aleatório do ISN do TCP não é suficiente. É necessário utilizar algoritmos mais eficientes para iniciarem aleatoriamente o ISN.

Aplicações de segurança

- **Antivírus**

  Faz o varrimento de ficheiros maliciosos disseminados pela Internet ou correio eletrónico. Basicamente, sua função está associada à ponta do processo, isto é, ao utilizador que envia e recebe dados. Uma das últimas tendências deste tipo de ameaça são os chamados "vírus polimórficos", que possuem a capacidade de mudar constantemente para enganar a vítima e dificultar sua remoção;

- **Balanceamento de carga**

  As ferramentas de balanceamento estão relacionadas à capacidade de operar de cada servidor da empresa. Elas permitem que, em horários de grande utilização da rede, se determine a hierárquia do que passa, bem como o equilíbrio da carga disseminada entre os servidores;

Aplicações de segurança

- ***Firewall***

  Cumprem a função de controlar os acessos. São soluções que, uma vez estabelecidas as suas regras, passam a gerir tudo o que deve entrar e sair da rede corporativa. Muitas vezes, recomenda-se a adopção do *firewall* para separar a intranet da companhia dos seus clientes externos ou de servidores e serviços públicos.

  Basicamente, o *firewall* é software, mas também pode incorporar hardware especializado;

- **Autenticações**

  São processos de identificação para disponibilizar acesso. A autenticação e consequente autorização de manipulação dos dados baseiam-se em algo que o indivíduo sabe (uma senha, por exemplo), algo que ele tem (dispositivos como *tokens*, cartões inteligentes, etc) e o que ele é (leitura de íris, linhas das mãos, etc);

Aplicações de segurança

- **Detector de Intrusão (IDS)**

  Estas ferramentas têm a função de monitorar o tráfego contínuo da rede, identificando ataques que estejam em execução. Como complemento do *firewall*, o IDS (*Intrusion Detection System*) baseia-se em dados dinâmicos para realizar sua varredura, como, por exemplo, pacotes de dados com comportamento suspeito, códigos de ataque e outros;

- **Varredura de vulnerabilidades**

  Produtos que permitem realizar verificações regulares em determinados componentes da rede como servidores e *routers*. O objetivo destas ferramentas é encontrar brechas de sistemas ou configurações;

Aplicações de segurança

- **Rede Privada Virtual (VPN)**

  Uma das alternativas mais adotadas pelas empresas na actualidade, as VPNs são canais que utilizam túneis para a transmissão de dados cifrados entre divisões de uma mesma companhia, parceiros de negócios etc;

- **Criptografia:** É utilizada para garantir a confidencialidade das informações. Trata-se de uma codificação que usa um processo de decifração para restaurar os dados ao seu formato original. As chaves criptográficas podem ser simétricas (secreta) ou assimétricas (privada/pública);

Aplicações de segurança

- **Integradores:** Permitem centralizar a gestão de diferentes tecnologias que protegem as operações da rede.

Mais que uma solução, trata-se de um conceito.

Ferramentas utilizadas em segurança

- **Testes de penetração/"*Scanning*" de vulnerabilidades**
  - Nessus
  - Shadow Security Scanner
  - NMAP
  - AMAP
  - WHOIS
  - hping
  - netcat
- **Segurança de aplicações Web**
  - Paros
  - Nikto
  - Exodus
  - Achilles

Ferramentas utilizadas em segurança

- **Análise forense**
  - The Coroner's Toolkit (TCT)
  - TASK
  - Autopsy
- **Várias**
  - Fragrouter
  - Firewalk
  - Stunnel
  - Brutus
  - ike-scan

http://sectools.org/

Ferramentas de ataque e de defesa

Site sobre segurança, um bom sítio para começar:

http://www.backtrack-linux.org/

Outrora famoso, apesar de desatualizado por falta de manutenção, permite ir para:

https://www.kali.org/

Aviso: Não esquecer que, se forem a alguns destes *sites*, devem ter a vossa máquina protegida com anti-vírus atualizado e o *firewall* activo. Cuidado com o software que carregarem e correrem.

Os vírus também contam enquanto ameaças

- Vírus famosos

- Vírus ao longo dos anos