



Segurança de Redes 2

TCP

Terminação de ligações

Não existe qualquer garantia de quem enviou um pacote na camada de transporte. Isto é devido a como o protocolo IP funciona.


Neste sentido, qualquer pessoa pode afirmar ter um determinado IP, quando na verdade não tem.

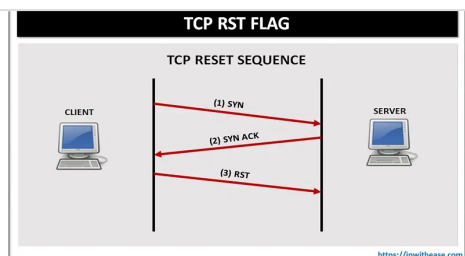
Por isso, há um tipo de ataque em que alguém pode fingir ser o nó com quem está a se comunicar e enviar um pacote com a **flag reset ativa (RST)**. Esta flag é uma forma de terminar a comunicação (funciona como um exit).

Esta flag é posta na camada TCP. Geralmente ocorre quando um dos computadores encerra a comunicação (lado A) e o outro lado volta numa tentativa de continuar a comunicação (lado B). Neste caso o lado A quando voltasse a ficar online enviaria um RST afirmando que não deseja mais continuar a ligação.

TCP RST FLAG - IP With Ease

TCP connections can be terminated in 2 ways - In this article, we will understand more about TCP RST Flag and its related nuances. TCP RST is more of a hard way which immediately terminates the

 <https://ipwithease.com/tcp-rst-flag/>



Great firewall

Este é um ataque feito pelo governo da China (TCP reset attacks). Numa tentativa de aceder um IP proibido, o governo da china envia um RST. Para fazer este ataque numa

grande escala e com certa rapidez, há a necessidade de ter o controle da estrutura.

Great Firewall - Wikipedia


The Great Firewall (GFW; simplified Chinese: 防火长城; traditional Chinese: 防火長城; pinyin: Fáng huǒ Cháng chéng) is the combination of legislative actions and technologies enforced by the

W https://en.wikipedia.org/wiki/Great_Firewall#Active_filtering



Deconstructing the Great Firewall of China

In our last post on censorship, we surveyed a range of countries around the world that engaged in content filtering on the Internet. Among them was one system of censorship whose sophistication

 <https://www.thousandeyes.com/blog/deconstructing-great-firewall-china/>



Spoofing às cegas (off path)

Se os pacotes de redes entre dois nós não passa pela nossa máquina, ou seja, não estamos na path de comunicação, conseguimos estabelecer um sessão com um dos computadores em nome de uma origem que não controlamos?

Poderíamos enviar um SYN inicial para o alvo, mas como não estamos na path, não conseguiríamos ver o número de sequência na resposta. Podemos tentar adivinhar o número de sequência. Se o número de sequência for baseado no relógio, prevê-lo já não é tão difícil. A mitigação é usar números de sequência aleatórios.

TCP Session Hijacking

Se alguém está na path de comunicação, o atacante pode fazer um TCP Session Hijacking.

Depois de uma troca inicial de mensagens para estabelecer a comunicação, o atacante já não precisa ter credenciais. Podemos aproveitar o estado dessa sessão para trocar mensagens com a vítima.

Diferente do spoofing, porque o spoofing tentamos nos passar por alguém desde o início.

Este tipo de ataque é feito em três partes:

- Tracking
- Des-sincronização
- Injeção

Des-sincronização

Enviamos um pacote para uma das partes e isto faz com que o numero de sequência aumente em uma delas. Durante o tempo em que as duas partes tentam estabelecer uma comunicação, abre-se uma janela para que atacante possa fazer uma injeção.

Porque é eficaz

- TCP/IP é intrinsecamente vulnerável a este simples ataque
- Não há contra-medidas eficazes (a não ser criptografia)
- Permite fazer bypass aos processos de autenticação.

Dificuldade

As dificuldade estão relacionadas a **preparação para realizar o ataque.**

- Precisamos estar no meio da comunicação
- Precisamos conhecer quem são as entidades que estão a comunicar
- Ainda precisamos intervir no momento do certo

UDP hijacking

No UDP não há tanto controle de tráfego, portanto fazer um hijacking é ligeiramentemente vai fácil.

Seconddate


Redireciona o tráfego para onde é desejado que ele seja interceptado. Este tipo de ataque usa os protocolos web para explorar as fraquezas.

A criptografia é uma medida de mitigação muito forte. Às vezes há muitos interesses de impedir com que pessoas façam criptografia

forte, porque permite com que o governo possa usar técnicas como estas para espionar pessoas e massa.

How the NSA Plans to Infect 'Millions' of Computers with Malware

Top-secret documents reveal that the National Security Agency is dramatically expanding its ability to covertly hack into computers on a mass scale by using automated systems that reduce the level of human

 <https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/>



Defesas - solução típica

A firewall define uma fronteira entre o que está sobre o nosso controle o fora dele.

- Firewall
- Network Address Translation
- Proxies de aplicações específicas
- Network intrusion detection system

Estes sistemas são utilizados para proteger a rede interna.

Firewalls

- Há as **firewalls locais** (hostbased) que possuem regras específicas para a máquina.
- Há também as **firewalls da rede** que filtra os pacotes. Elas tentam eliminar as comunicações que são identificadas como maliciosas. Proxies por outro lado, trabalham ao nível de uma aplicação.

A firewall é muito flexível em comunicações que vem de dentro pra fora, mas muito restrita à comunicação de fora pra dentro.

Políticas simples

- Permitir todos os acessos de dentro pra fora (obvio 😊)
- Restringir o acesso de fora pra dentro: permitir acesso a serviços apenas de exposição (não fazem

Como controlar o tráfego que não é especificado nas políticas?

- **Default allow** ⇒ permitir todos os acessos exceto problemas específicos.
- **Default deny** ⇒ Permitir apenas alguns acessos comuns a todos os sistemas. Esta é a escolha mais conservadora (proteção por omissão). Podemos começar com esta escolha e adicionar exceções.

Filtragem de pacotes

Utiliza-se informação das camadas de rede e de transporte.

Um exemplo é bloquear endereços DNS e pedidos HTTP.

- **Filtragem sem estado** ⇒ não tenta-se perceber o contexto do pacote. São sistemas mais eficientes, porém mais permissivos.
- **Filtragem com estado** ⇒ mais difícil de implementar. Tenta perceber o contexto da mensagem. Mas é difícil de fazer para contextos elaborados. Queremos manter um registo de ligações ativas e verificamos se um determinado pacote recebido faz sentido no contexto da ligação.

Contornar filtragem de pacotes

Podemos tentar utilizar portas que estão atribuídas a um serviço qualquer. Usamos um túnel para realizar a comunicação. Um túnel é encapsular um protocolo dentro de outro. Por exemplo: ssh, vpn, etc.

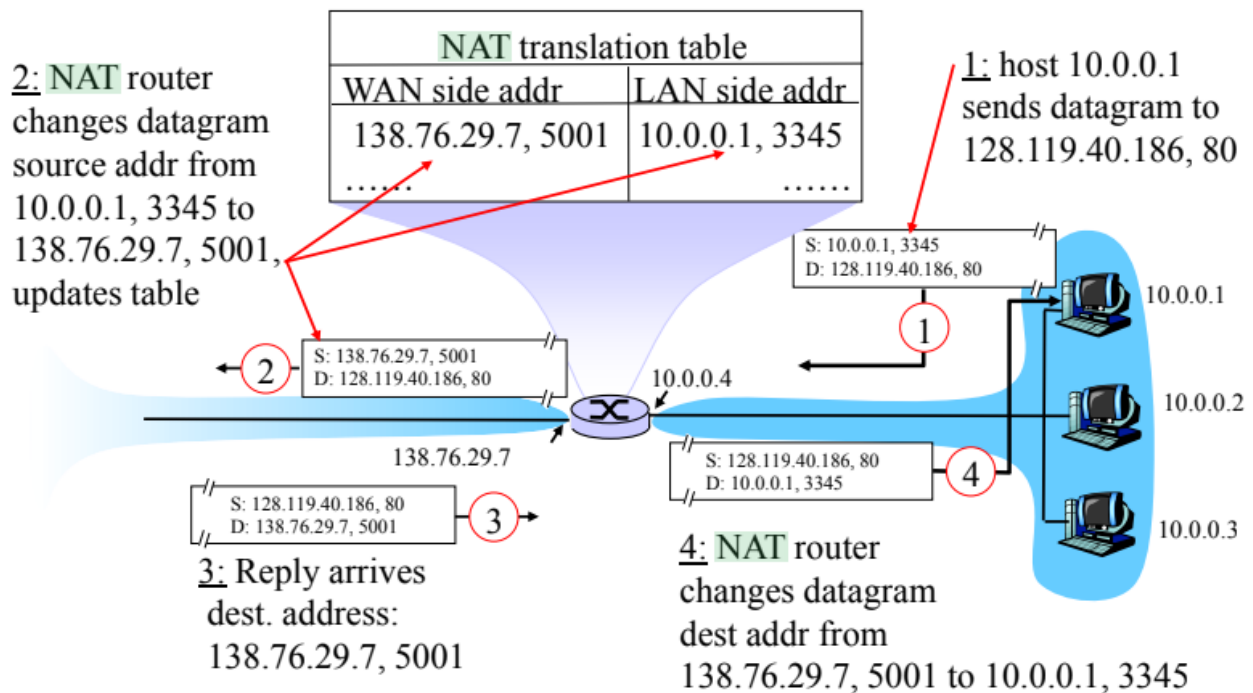
Túnel: tentar utilizar canais que estão abertos nestes mecanismos de filtragem de pacotes, utilizando canal disponível para enviar mensagens do protocolo que o corresponde, mas enviando dentro dos pacotes outro protocolo.

É como criar uma camada adicional.

NAT

Como funciona

O NAT possui uma tabela que possui o endereço IP mapeado a uma porta na rede pública: a translation table.



Se a mensagem do exterior não contém uma porta

- **Vantagens:** reduz exposição ao exterior (apenas um endereço IP) e ligações externas são descartadas a não ser que tenham sido iniciadas internamente.
- **Desvantagens:** pode deturbar o funcionamento de alguns protocolos. Fácil de fazer bypass para um adversário ativo (splitstream).

Network IDS/IPS

Vantagem: não precisamos alterar a máquina.

Desvantagens:

- É exigente em termos de processamento, já que precisamos analisar todo o tráfego.
- É menos preciso. Para tentar reduzir o número de falso negativos (que são o grande problema), há muitos falso positivos.
- Não consegue lidar com ataques a todo o sistema
- Como lidar com código cifrado?

Host-based IDS/IPS

Defesa em profundidade. Faz uma deteção mais agressiva em algumas máquinas.

É possível fazer deteção após a remoção da camada criptográfica. Ainda é possível procurar por padrões de ataque específicos para servidores web.

Análise de logs

O problema dessa estratégia é que vamos analisar o conteúdo depois que o ataque já aconteceu e o atacante ainda é capaz de modificar os próprios logs.

Pen-testing

É simular um ataque e ver como o sistema reage a ele.

Vantagens:

- Proativo: uma falha não causa perda de valor e permite corrigir o sistema
- Otimização: permite melhorar o sistema/reduzir falso positivos.

Desvantagens:

- Fazer pen-testing pode ter um custo caro.
- Por vezes um ataque pode causar danos (e.g down time).

Perguntas

- 1) O que é o RST? Como a China aplica um ataque usando esta flag?
- 2) O que é o TCP Session Hijacking? Qual a diferença deste para um off path? Quais são as fases? Qual a dificuldade?
- 3) O que é um seconddate?
- 4) Quais são as tarefas de uma firewall?