GTER 36

Análise preliminar de dados de testes AntiSpoofing do SIMETBox

Fabrício Tamusiunas

NIC.br

Histórico dos sistemas para teste de AntiSpoofing

- Dez/2012 - Lançamento da versão para testes disponível pelo portal

  http://bcp.nic.br

- Março/2013 - Lançamento primeira versão para o SIMETBox
  - Baseada no hping

- Outubro/2013 - Atualização do SIMETBox com nova aplicação para testes desenvolvida pelo NIC.br
  - hping era muito grande (~ 120 kbytes)…

Como são feitas as medições

- São feitos 4 tipos de testes
- O usuário sabe o próprio IP através de WEB Service (HTTP)
  - Teste 1 - validação do próprio IP
    - O sistema envia um pacote com o IP externo no usuário como origem e o IP do usuário dentro do pacote
  - Teste 2 - spoofing da rede do usuário
    - O sistema pega outro IP da rede do usuário (imaginando ser um /24) e forja a origem como sendo este IP. O IP válido externo vai dentro do pacote.

Como são feitas as medições

- Teste 3 - spoofing de outra rede
  - O sistema envia um pacote forjando a origem como sendo de outra rede. O IP válido externo vai dentro do pacote.
- Teste 4 - spoofing usando endereço da RFC 1918
  - O sistema envia um pacote forjando a origem como sendo um IP privado. O IP válido externo vai dentro do pacote.

Como são feitas as medições

- Problemas encontrados na metodologia inicialmente adotada
  - O usuário pode usar proxy e o endereço pego via HTTP pode ser de outro ASN
  - O usuário pode estar atrás de NAT
    - 69% dos usuários do SIMETBox usam NAT!!
  - O usuário pode usar *multiwan*

Como são feitas as medições

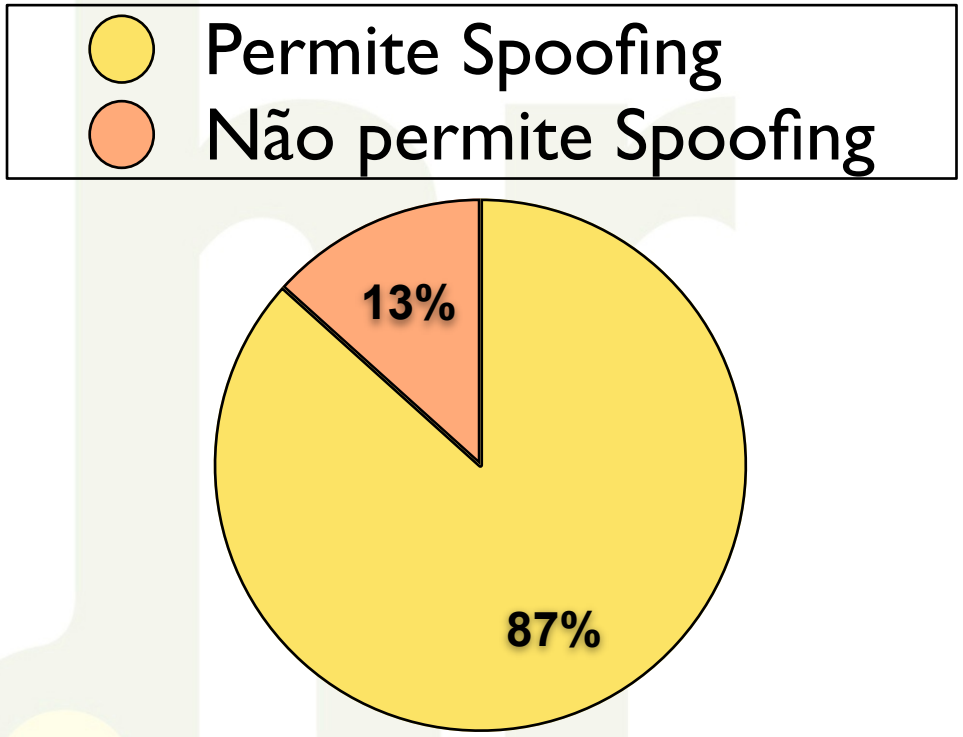
- Então como resolver estes problemas na metodologia atual?
  - Cruzando os dados dos testes do SIMETBox (sessão de testes de vazão, latência,etc.) com os dados do AntiSpoofing
    - O SIMET não usa HTTP nem porta 80, além disso, registra se o usuário está usando NAT durante o teste.

Como são feitas as medições

- Nova metodologia a ser aplicada
  - Para o teste AntiSpoofing, o SIMETBox se conectará primeiramente utilizando uma conexão TCP não HTTP (pelo socket local será possível pegar o IP em uso localmente). Através desta conexão saberá qual o IP público.
  - Após isso, serão feitos todos os testes, enviando dentro do pacote o endereço local e o público detectado.

Alguns resultados preliminares

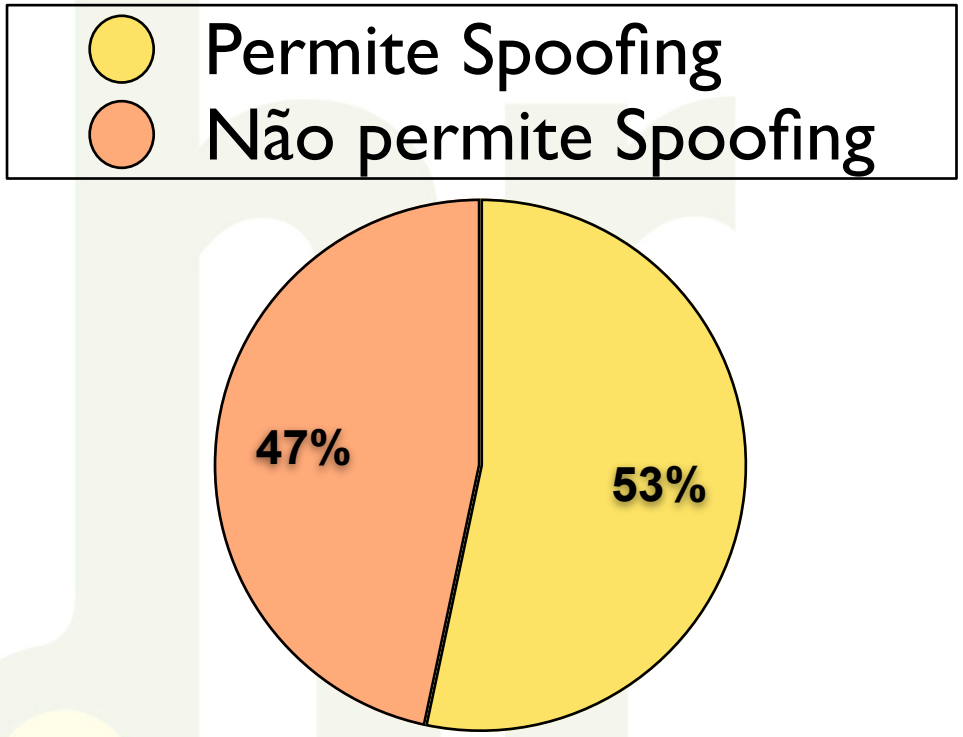
- Total de ASN que permitiram spoofing de IPs públicos em novembro/2013



Minas Gerais
Bahia
Paraná
São Paulo
Roraima
Espírito Santo
Paraná
Giânia
Ceará
Santa Caratina
Rio Grande do Sul

Alguns resultados preliminares

- Alguns ASN que permitem spoofing de endereços da RFC 1918 em novembro/2013



Minas Gerais
Paraná
Rio Grande do Sul
São Paulo
Goiás
Ceará
Santa Catarina

Por que filtrar?

- Muitos ataques de DoS (ou DDoS) só existem em caso de spoofing permitido
- Todos os ataques de reflexão só existem através de spoofing
- Mais informações e maiores motivações?
  - http://bcp.nic.br/entenda-o-antispoofing/
- Quer saber se o seu ASN está com os devidos filtros?
  - Venha conversar conosco !!

Por que filtrar?

- E o mais importante:

Ser um bom cidadão da Internet !!!

Próximas etapas

- Apresentar avanços nos próximos GTER
- Aplicação da nova metodologia
- Análise mais aprofundada dos casos com NAT para possível utilização dos dados gerados pelo SIMETBox
  - (66 com NAT X 30 sem NAT)

Quer testar a sua rede?

- Quer testar na sua rede automaticamente?
  - http://simet.nic.br/simetbox.html
- Quer saber mais?
  - http://bcp.nic.br

BCP.NIC.BR - EQUIPE

- Equipe BCP.NIC.BR
  - @CERT.BR
    - Klaus Steding-Jessen
    - Cristine Hoepers
  - @CEPTRO.BR
    - Milton Kaoru Kashiwakura
    - Fabrício Tamusiunas
    - Antonio M. Moreiras
    - Rodrigo Regis dos Santos
  - @REGISTRO.BR
    - Frederico A. C. Neves
    - Ricardo G. Patara
    - Hugo Koji Kobayashi

Perguntas?

fabricio@nic.br