Cartilha de proteção contra o IP Spoofing

CAIS

RNP

Sumário

AQUI TEM PROTEÇÃO
ANTI-SPOOFING
APOIO RNP

AQUI TEM PROTEÇÃO
ANTI-SPOOFING
APOIO RNP

Há tempos, uma grande preocupação para a segurança da informação é garantir a disponibilidade de serviços conectados à internet.

Com isso, esta cartilha irá apresentar e sugerir *formas para mitigação da técnica conhecida como IP Spoofing*. O método pode, por exemplo, ser utilizado em ataques de negação de serviço (DoS), que podem gerar grandes impactos de sobrecarga e disponibilidade na rede.

O que é e por que se preocupar com o Spoofing?

AQUI TEM PROTEÇÃO ANTI-SPOOFING

APOIO RNP

O Spoofing ocorre quando um usuário malicioso falsifica as informações referentes à origem dos pacotes para obter acesso indevido, forjar informações ou prejudicar conexões confiáveis. Diversos tipos de ataques podem ser realizados com o uso dessa técnica, tais como: ataques de negação de serviço (DoS), ARP Spoofing, Web Spoofing, Mail Spoofing, entre outros.

Especificamente no caso do IP Spoofing, um atacante manipula intencionalmente as informações do campo “origem” no cabeçalho do protocolo IP. Dessa forma, o pacote chega ao destino com a informação do endereço IP de origem forjado, o que permite que o Spoofing ocorra.

Version	IHL	Type of Service	Total Length	
Identification			Flags	Fragment Offset
Time To Live		Protocol	Header Checksum	
Source IP Address				
Destination IP Address				
Options				
Data				

Cabeçalho do protocolo IPv4.

Exemplos de ataques provocados por técnicas de IP Spoofing

Ataque de Negação de Serviço Distribuído Reflexivo (DRDoS)

Por meio de redes que não validam ou que não realizam o controle de pacotes manipulados, usuários maliciosos exploram servidores vulneráveis na internet para realizar a combinação da técnica do IP Spoofing com o Ataque de Negação de Serviço (DoS), o que acarreta o Ataque de Negação de Serviço Distribuído Reflexivo (do inglês DRDoS).

AQUI TEM PROTEÇÃO ANTI-SPOOFING

APOIO RNP

Exemplos de ataques provocados por técnicas de IP Spoofing

Basicamente, esse ataque consegue potencializar o Ataque de Negação de Serviço Distribuído (DDoS). Por ele, os atacantes encaminham pequenas requisições UDP a servidores vulneráveis na internet. Por sua vez, esses servidores servem como amplificadores para o ataque ao receberem os pacotes manipulados (spoofados) e responderem às requisições para uma determinada vítima, que foi forjada inicialmente como origem da conexão pelo atacante. Isso gera um ataque direcionado, amplificado e de grande impacto.

Diante da vulnerabilidade do serviço, é possível conseguir um fator de amplificação de grande impacto, conforme a tabela a seguir:

Protocol	Bandwidth Amplification Factor	Vulnerable Command
DNS	28 to 54	see: TA13-088A [4]
NTP	556.9	see: TA14-013A [5]
SNMPv2	6.3	GetBulk request
NetBIOS	3.8	Name resolution
SSDP	30.8	SEARCH request
CharGEN	358.8	Character generation request
QOTD	140.3	Quote request
BitTorrent	3.8	File search
Kad	16.3	Peer list exchange
Quake Network Protocol	63.9	Server info exchange
Steam Protocol	5.5	Server info exchange
Multicast DNS (mDNS)	2 to 10	Unicast query
RIPv1	131.24	Malformed request
Portmap (RPCbind)	7 to 28	Malformed request
LDAP	46 to 55	Malformed request
CLDAP	56 to 70	-
TFTP	60	-

Fonte: US-CERT. https://www.us-cert.gov/ncas/alerts/TA14-017A

AQUI TEM PROTEÇÃO
ANTI-SPOOFING
APOIO RNP

Como se proteger?

Nesta cartilha, abordamos exclusivamente o **ataque de IP Spoofing**.
No entanto, mitigar ataques de IP Spoofing não se limita apenas às informações contidas nessa publicação.

Aplicar filtros e realizar o controle do tráfego dos roteadores de borda é uma prática adotada para mitigar o ataque de IP Spoofing, conforme os documentos de boas práticas publicados pela Internet Engineering Task Force (IETF):

BCP38
Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing;
https://tools.ietf.org/html/bcp38

BCP84
Ingress Filtering for Multihomed Networks.
https://tools.ietf.org/html/bcp84

AQUI TEM PROTEÇÃO ANTI-SPOOFING

APOIO RNP

Para auxiliar a disseminação de boas práticas em segurança da informação, o Centro de Atendimento a Incidentes de Segurança (CAIS) da RNP oferece tutoriais para a configuração dos controles Anti-Spoofing para os seguintes fabricantes:

Anexo A – Tutorial Juniper - **clientes** - **provedores**

Anexo B – Tutorial Cisco - **clientes** - **provedores**

Assista ao vídeo da campanha Aqui tem proteção Anti-Spoofing

http://url.rnp.br?campanhaantispoofing

Confira outras iniciativas e projetos de segurança da informação promovidos pela RNP em

http://www.rnp.br/servicos/seguranca

Referências:

Portal de Boas Práticas para a Internet no Brasil. Disponível em: <http://bcp.nic.br/>. Acesso em: 26/06/2017.

IETF Tools. Disponível em: <https://tools.ietf.org>. Acesso em 23/06/2017.

Team Cymru – Bogon Reference. Disponível em: <http://www.team-cymru.org/bogon-reference.html>. Acesso em 23/06/2017.

CAIS

RNP

MINISTÉRIO DA **DEFESA**

MINISTÉRIO DA **CULTURA**

MINISTÉRIO DA **SAÚDE**

MINISTÉRIO DA **EDUCAÇÃO**

MINISTÉRIO DA **CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES**

BRASIL
GOVERNO FEDERAL