ATIVIDADE – SEGURANÇA E IPV6

REDES DE ALTA VELOCIDADE

CARLA BEATRIZ DA SILVA TEIXEIRA

1) Muitos têm apostado que o IPv6 é naturalmente mais seguro que o IPv4, se baseando, provavelmente, no suporte obrigatório que o IPv6 oferece ao IPsec. Entretanto, isto não é necessariamente verdade. Por que?

IPV6 traz funcionalidades as quais as equipes técnicas e os equipamentos ainda não estão preparados.

2) Em que ano a IANA (Internet Assigned Numbers Authority) distribuiu os últimos endereços IPv4 disponíveis para as entidades de registro regionais.

Em fevereiro de 2011, a IANA (Internet Assigned Numbers Authority) distribuiu os últimos endereços IPv4 (Internet Protocol version 4) disponíveis, alarmando a todos sobre a necessidade imediata de migração do IPv4 para uma versão mais nova do protocolo.

3) Além dos 128 bits no endereço, quais foram as outras preocupações suportadas pela versão 6 do IP?

preocupações com as questões relacionadas à segurança dos dados, pois, como diversos tipos de transações ocorrem por meio da infraestrutura suportada por estes protocolos, as informações podem ser capturadas e alteradas por usuários mal-intencionados.

4) Qual a área que traz maior preocupação no IPv6?

Segurança dos dados

5) Quais funcionalidades novas podem ser usadas como brechas para ataques no IPv6?

IP Spoofing: técnica que consiste no envio de pacotes com o endereço de origem adulterado. Desta maneira, os pacotes de retorno nunca regressam para o falsificador. No IPv6, o cabeçalho de extensão AH obriga o usuário mal-intencionado a calcular um hash (Nota DevMan 5) semelhante àquele que seria gerado entre a entidade falsificada e a vítima; no entanto, para a obtenção deste, seria necessário conhecer os parâmetros da AS, incluindo as chaves criptográficas e os algoritmos. Assim, caso a vítima receba um pacote com o hash incorreto, esta deve descartá-lo;

Sniffing: ataque em que os pacotes são capturados com o objetivo de verificar seu conteúdo, explorando aplicações que não utilizam nenhum tipo de criptografia no envio de seus dados, como FTP (transferência de arquivos), Telnet (acesso/login remoto), entre outras. Para evitar este tipo de ataque, pode-

se lançar mão do cabeçalho de extensão ESP, para criptografar os dados e promover a privacidade entre as partes envolvidas na comunicação.

6) Quais são as categorias de autoconfiguração de endereço?

Autoconfiguração stateless: possibilita a configuração automática dos endereços IPv6 unicast sem a necessidade de servidores DHCP. Para tanto, o host utiliza seu endereço link local (FE80::/64) para enviar uma mensagem multicast RS (Router Solicitation) para todos os roteadores do segmento – esta é parte do Neighbor Discovery Protocol (NDP). Desta maneira, é solicitado o prefixo IPv6 e o endereço a ser configurado como default gateway. O roteador responde às informações requisitadas em uma mensagem RA (Router Advertisement) – ver Nota DevMan 4. A seguir, o host combina o prefixo recebido com o endereço físico de sua interface (MAC Address), segundo o formato IEEE EUI-64. A Figura 14 ilustra o processo de autoconfiguração stateless;

Autoconfiguração stateful: técnica opcional à stateless que utiliza o protocolo DHCPv6 para obtenção do endereço IPv6, default gateway, servidores DNS (Domain Name System), NTP (Network Time Protocol), entre outros parâmetros para configuração da interface de rede. Os hosts clientes utilizam seu endereço link local para enviar e receber as mensagens DHCPv6, por intermédio de mensagens multicast.

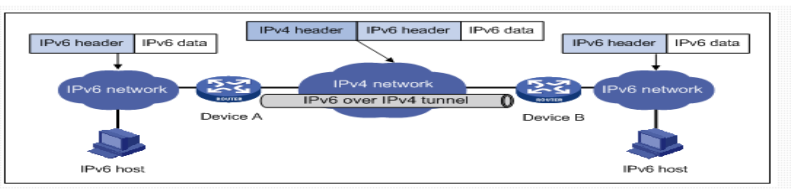
7) O que é o IPsec?

O IPSec é um conjunto de regras ou protocolos de comunicação para configurar conexões seguras em uma rede. O Protocolo da Internet (IP) é o padrão comum que determina como os dados trafegam pela Internet. O IPSec adiciona criptografia e autenticação para tornar esse protocolo ainda mais seguro.

O IPSec, suportado opcionalmente pelo IPv4, foi desenvolvido como parte integrante do IPv6, através dos cabeçalhos de extensão AH (Authentication Header) – usado para autenticar o emissor dos dados e assegurar a integridade dos mesmos – e ESP (Encapsulation Security Payload) – empregado para prover privacidade entre o originador e o receptor dos dados.

8) Qual a diferença entre modo túnel e modo transporte?

Túneis (Encapsulation): neste método, um pacote IPv6 é transmitido como parte dos dados de um pacote IPv4, criando um túnel entre os nós (Figura 16). No futuro, este túnel também suportará o inverso, ou seja, redes IPv4 conectadas por redes IPv6. É importante notar que, nos dois cenários, os nós nas extremidades do túnel devem ser compatíveis com ambos os protocolos.



9) Quais primeiros atributos que são novidade no IPv6 podem ser utilizados como brechas de segurança?

Já respondida anteriormente.

10) Como o ICMPv6 pode ser usado para ataques de segurança?

O ICMP é usado principalmente para determinar se os dados estão chegando ou não ao destino pretendido em tempo hábil.
Pode ser utilizado entre os pontos de maior vulnerabilidade do IPv6 estão a auto configuração, os cabeçalhos de extensão e o desafio de configurar e manter equipamentos como firewalls e sistemas de detecção de intrusão para defesa de duas redes simultaneamente: a rede IPv4 e a rede IPv6.