LUIZ GONZAGA FONSECA MOTA
ESCOLA ESTADUAL DE EDUCAÇÃO PROFISSIONAL

SEDUC | SECRETARIA DA EDUCAÇÃO
GOVERNO DO ESTADO DO CEARÁ

Tópicos Especiais - Segurança da Informação

Segurança em rede e Comunicação

A Segurança de Redes e de Comunicações é um ramo da ciência da computação dedicado a proteger os dados e recursos transmitidos ou armazenados em redes de computadores. Redes de computadores consistem em conjuntos de dispositivos interconectados que trocam informações através de protocolos padronizados.

As redes estão expostas a ameaças tanto internas quanto externas. Ameaças internas originam-se dentro da própria rede e incluem usuários mal-intencionados, dispositivos infectados, erros humanos e falhas técnicas. Por outro lado, as ameaças externas, originárias fora da rede, incluem hackers, crackers, espiões, terroristas, vírus, worms, trojans, ransomware e spyware. Todas essas ameaças podem comprometer a confidencialidade, integridade e disponibilidade dos dados e recursos da rede, resultando em danos financeiros, operacionais e reputacionais.

Para mitigar esses riscos, a Segurança de Redes e de Comunicações emprega uma variedade de técnicas e ferramentas categorizadas principalmente em medidas preventivas, detectivas e corretivas. Medidas preventivas, como controle de acesso, criptografia, assinatura digital, firewall e antivírus, visam evitar ou dificultar ataques. Medidas detectivas, como auditoria e análise de tráfego, focam na identificação e monitoramento de ataques. Já as medidas corretivas, como backup e restauração, buscam recuperar ou restaurar dados e recursos comprometidos após um ataque.

Para mitigar esses riscos, a Segurança de Redes e de Comunicações emprega uma variedade de técnicas e ferramentas categorizadas principalmente em medidas preventivas, detectivas e corretivas. Medidas preventivas, como controle de acesso, criptografia, assinatura digital, firewall e antivírus, visam evitar ou dificultar ataques. Medidas detectivas, como auditoria e análise de tráfego, focam na identificação e monitoramento de ataques. Já as medidas corretivas, como backup e restauração, buscam recuperar ou restaurar dados e recursos comprometidos após um ataque.

Protocolos em Rede e suas Vulnerabilidades

TCP/IP - Basicamente composta por 4 Camadas.

Aplicação, Transporte, Rede e Enlace.

Ataque de Ataque de spoofing: O spoofing é um método em que pacotes de dados TCP/IP ou UDP/IP são enviados com um endereço de remetente falso. O atacante usa o endereço de um sistema autorizado e confiável para injetar seus próprios pacotes no sistema estrangeiro que, de outra forma, seriam bloqueados por um sistema de filtro.

Prevenção: A prevenção pode ser feita através do uso de firewalls para filtrar pacotes indesejados.

Ataque de hijacking: O hijacking do TCP/IP é uma forma de ataque do tipo man-in-the-middle. O intruso pode determinar os endereços IP dos dois participantes da sessão, tornar um deles inacessível usando um ataque DoS e se conectar ao outro falsificando o ID de rede do primeiro.

A detecção e prevenção desses ataques podem ser realizadas com IDS/IPS.

Ataque de flooding: O ataque de inundação SYN é um tipo de ataque DDoS que explora parte do handshake (aperto de mãos) normal do TCP para consumir recursos no servidor alvo e torná-lo irresponsivo. Com o SYN flood DDoS, o ofensor envia solicitações de conexão TCP mais rápido do que a máquina alvo pode processá-las, causando saturação da rede.

Novamente, IDS/IPS podem ser úteis para detectar e prevenir esses ataques.

Ataque de sniffing: Um ataque de sniffing ocorre quando um invasor usa um sniffer de pacotes para interceptar e ler dados sensíveis que passam por uma rede. Alvos comuns para esses ataques incluem mensagens de email não criptografadas, credenciais de login e informações financeiras.

A criptografia IPsec pode ser usada para proteger a comunicação em uma rede IP contra esses ataques.

Em resumo, as medidas de segurança para o UDP incluem limitação de taxa ICMP, filtragem de pacotes UDP no nível da rede (exceto DNS) e uso de firewalls e IDS/IPS.

O UDP (User Datagram Protocol) é um protocolo de transporte que oferece um serviço não confiável e sem conexão. Ele é usado para aplicações que exigem rapidez e baixo consumo de recursos, como streaming de áudio e vídeo, jogos online, VoIP, entre outros. No entanto, o UDP é vulnerável a vários tipos de ataques.

Ataque de amplificação: Um ataque de amplificação é uma forma de ataque DDoS (Distributed Denial of Service) que explora a natureza sem estado do protocolo UDP. Os atacantes podem forjar o endereço IP de origem em um pacote UDP, fazendo com que um servidor intermediário envie uma resposta amplificada para o alvo do ataque. Isso pode resultar em uma quantidade significativa de tráfego indesejado sendo direcionado para o alvo.

A limitação da taxa ICMP pode ser uma medida eficaz para mitigar esse tipo de ataque.

Ataque de reflexão: Este ataque explora o fato de que o UDP é um protocolo sem estado. Os atacantes podem criar um pacote de solicitação UDP válido listando o endereço IP do alvo do ataque como o endereço IP de origem do UDP. Isso faz com que o servidor intermediário envie seus pacotes de resposta UDP para a vítima alvo em vez de retornar ao endereço IP do atacante.

A filtragem de pacotes UDP no nível da rede pode ajudar a prevenir esses ataques.

Ataque de inundação (flooding): Ataque de inundação (flooding): Este é um tipo de ataque DDoS no qual um grande número de pacotes UDP são enviados para um servidor alvo com o objetivo de sobrecarregar a capacidade desse dispositivo de processar e responder.

O uso de firewalls e IDS/IPS pode ser útil para detectar e prevenir esses ataques.

Ataque de falsificação (spoofing): Em um ataque de falsificação, os atacantes enviam pacotes UDP com um endereço IP remetente falsificado para portas aleatórias no sistema alvo. Como o UDP é um protocolo sem conexão, o servidor usa o Protocolo de Mensagens de Controle da Internet (ICMP) para informar ao remetente que o pacote não pôde ser entregue. Isso pode resultar em uma inundação de pacotes ICMP “destino inatingível” sendo enviados para algum espectador aleatório.

A limitação da taxa ICMP pode ser uma medida eficaz para mitigar esse tipo de ataque.

ICMP (Internet Control Message Protocol)

O ICMP (Internet Control Message Protocol) é um protocolo de rede que é usado para enviar mensagens de controle e de erro entre dispositivos na rede. Ele é usado para testar a conectividade, diagnosticar problemas e informar sobre falhas na rede. No entanto, o ICMP é vulnerável a vários tipos de ataques.

Vamos explorar alguns desses ataques e as estratégias correspondentes de prevenção e mitigação:

Ataque ping da morte (Ping of Death): Este ataque visa interromper uma máquina alvo enviando um pacote maior que o tamanho máximo permitido, fazendo com que a máquina alvo congele ou trave.

A limitação da taxa de respostas ICMP pode ser uma medida eficaz para mitigar esse tipo de ataque.

Ataque ping flood: Este ataque tenta sobrecarregar um dispositivo alvo com pacotes de solicitação de eco ICMP, fazendo com que o alvo se torne inacessível para o tráfego normal.

O uso de firewalls e IDS/IPS pode ser útil para detectar e prevenir esses ataques.

Ataque ping sweep: Este ataque ocorre quando um invasor envia solicitações de eco ICMP (pings) para vários endereços de destino. Se um host alvo responder, a resposta revelará o endereço IP do alvo ao invasor.

A filtragem de pacotes ICMP no nível do firewall pode ajudar a prevenir esses ataques.

Ataque smurf: Este ataque envolve o envio de solicitações de eco ICMP a partir de um endereço IP falsificado para vários nós da rede, resultando em uma sobrecarga de respostas que inundam o sistema da vítima.

A limitação da taxa de respostas ICMP pode ser uma medida eficaz para mitigar esse tipo de ataque.

Ataque fraggle: Este ataque é semelhante a um ataque smurf, mas usa o protocolo UDP em vez do ICMP. Ambos visam inundar seu sistema com tráfego indesejado. A filtragem de pacotes UDP no nível do firewall pode ajudar a prevenir esses ataques.

Em resumo, as medidas de segurança para o ICMP incluem limitação da taxa de respostas ICMP, filtragem de pacotes ICMP no nível do firewall e uso de IDS/IPS.

Ataque fraggle: Este ataque é semelhante a um ataque smurf, mas usa o protocolo UDP em vez do ICMP. Ambos visam inundar seu sistema com tráfego indesejado. A filtragem de pacotes UDP no nível do firewall pode ajudar a prevenir esses ataques.

Em resumo, as medidas de segurança para o ICMP incluem limitação da taxa de respostas ICMP, filtragem de pacotes ICMP no nível do firewall e uso de IDS/IPS.

ARP (Address Resolution Protocol)

O ARP (Address Resolution Protocol) é um protocolo de enlace que é usado para resolver endereços IP em endereços MAC (Media Access Control). Ele permite que os dispositivos se comuniquem na mesma sub-rede local. No entanto, o ARP é vulnerável a vários tipos de ataques. Vamos explorar alguns desses ataques e as estratégias correspondentes de prevenção e mitigação:

Ataque de envenenamento (poisoning): Um ataque bem-sucedido de envenenamento de ARP permite que um invasor altere o roteamento em uma rede, permitindo efetivamente um ataque do tipo man-in-the-middle. Em redes de computadores, o envenenamento de ARP, spoofing de ARP ou roteamento venenoso de ARP, é uma técnica pela qual um invasor envia mensagens do Protocolo de Resolução de Endereços (ARP) falsificadas para uma rede local.

Novamente, a implementação do DAI pode ser útil para prevenir esses ataques.

Ataque de spoofing: O spoofing de ARP, também conhecido como envenenamento de ARP, descreve ataques do tipo man-in-the-middle realizados em tabelas ARP de rede local. Este tipo de ataque resulta em hackers enviando pacotes ARP falsos que se inserem entre dois sistemas que se comunicam sem serem notados, para que possam ouvir ou manipular seu tráfego de dados.

A implementação do DAI (Dynamic ARP Inspection) pode ajudar a verificar a autenticidade das mensagens ARP e prevenir o envenenamento de ARP.

Ataque de inundação (flooding): O flooding de ARP é um ataque em que os hackers inundam a rede com um alto volume de solicitações ou respostas ARP, causando confusão e congestionamento. Ele cria um ambiente caótico, comprometendo a privacidade da rede ao expor o tráfego da rede a todos os dispositivos no mesmo segmento de rede.

A implementação do DAI também pode ser útil para prevenir esses ataques.

Em resumo, a segurança do protocolo ARP pode ser melhorada através da implementação do DAI (Dynamic ARP Inspection), que ajuda a verificar a autenticidade das mensagens ARP e prevenir o envenenamento e inundação ARP.

DHCP (Dynamic Host Configuration Protocol)

O DHCP (Dynamic Host Configuration Protocol) é um protocolo de aplicação que é usado para atribuir endereços IP dinamicamente aos dispositivos na rede. Ele permite que os dispositivos se configurem automaticamente na rede, sem a necessidade de intervenção manual. No entanto, o DHCP é vulnerável a vários tipos de ataques. Vamos explorar alguns desses ataques:

Ataque de exaustão (Exhaustion Attack): Em um ataque de exaustão DHCP, um invasor transmite um grande número de mensagens DHCP REQUEST com endereços MAC de origem falsificados. Se o servidor DHCP legítimo na rede começar a responder a todas essas mensagens DHCP REQUEST falsas, os endereços IP disponíveis no escopo do servidor DHCP serão esgotados em um curto espaço de tempo. Isso pode resultar em um ataque bem-sucedido de negação de serviço (DoS) no servidor DHCP; assim, nenhum novo cliente DHCP será capaz de obter um endereço IP e, portanto, eles não serão capazes de realizar qualquer tipo de comunicação baseada em IP.

O uso de switches gerenciados cientes do protocolo pode ajudar a bloquear respostas DHCP de servidores não autorizados e prevenir esse tipo de ataque.

Ataque de falsificação (Spoofing Attack): O ataque de falsificação DHCP ocorre quando um invasor tenta responder às solicitações DHCP e tenta se listar (falsifica) como o gateway padrão ou servidor DNS, iniciando assim um ataque do tipo man-in-the-middle.

Novamente, o uso de switches gerenciados cientes do protocolo pode ser útil para prevenir esses ataques.

Ataque de negação de serviço (Denial of Service Attack): Durante um ataque DHCP, um ator hostil inunda um servidor DHCP com pacotes DISCOVER falsos até que o servidor DHCP esgote seu suprimento de endereços IP. Uma vez que isso acontece, o invasor pode negar o serviço aos usuários legítimos da rede, ou até mesmo fornecer uma conexão DHCP alternativa que leva a um ataque do tipo man-in-the-middle.

O uso de switches gerenciados cientes do protocolo pode ajudar a bloquear respostas DHCP de servidores não autorizados e prevenir esse tipo de ataque.

Ataque de roubo de identidade (Identity Theft Attack): Em um ataque de roubo de identidade DHCP, os invasores configuram um servidor DHCP falso e usam isso para enviar respostas DHCP forjadas para dispositivos em uma rede. Os invasores costumam usar esse ataque para substituir os endereços IP do Gateway Padrão e dos servidores DNS e, assim, desviar o tráfego para servidores maliciosos.

Novamente, o uso de switches gerenciados cientes do protocolo pode ser útil para prevenir esses ataques.

Em resumo, a segurança do protocolo DHCP pode ser melhorada através do uso de switches gerenciados cientes do protocolo, que ajudam a verificar a autenticidade das mensagens DHCP e prevenir ataques.