Redes de Computadores II – Resumo de Artigos

Daniel Veiga da Silva Antunes

1. As 10 principais ameaças comuns à segurança de rede explicadas

https://securitytrails.com/blog/top-10-common-network-security-threats-explained

Vírus de computador: Softwares projetados para serem transmitidos de um computador para outro. Conhecidos por enviar spam, desabilitar suas configurações de segurança, corromper e roubar dados do seu computador, incluindo informações pessoais, como senhas, chegando até mesmo a excluir tudo do seu disco rígido.

Software de segurança desonesto: Software malicioso que induz os usuários a acreditar que têm problemas de segurança, se oferecem para instalar ou atualizar as configurações de segurança dos usuários. Levam à instalação de malware real no seu computador.

Cavalo de Tróia: Também conhecido como Trojan, é um código malicioso ou software de ataque que engana os usuários para executá-lo voluntariamente, escondendo-se atrás de um programa legítimo.

Adware e Spyware: Adware consiste em um software projetado para rastrear dados de seus hábitos de navegação e, com base nisso, mostrar anúncios e pop-ups. O spyware funciona de forma semelhante ao adware, mas é instalado no seu computador sem o seu conhecimento.

Verme de computador: Os Worms (Vermes) de computador são programas de malware que se replicam rapidamente e se espalham de um computador para outro.

Ataque DOS e DDOS: DOS é realizado por uma máquina e sua conexão com a Internet, inundando um site com pacotes e impossibilitando que usuários legítimos acessem o conteúdo do site inundado. Um ataque DDOS é semelhante ao, mas é mais forte.

Phishing: Método de engenharia social com o objetivo de obter dados confidenciais, como senhas, nomes de usuário, números de cartão de crédito. Geralmente vêm na forma de mensagens instantâneas ou e-mails de phishing projetados para parecer legítimos. O destinatário do e-mail é então induzido a abrir um link malicioso, levando à instalação de malware.

Ataque de injeção de SQL: Usam códigos maliciosos para obter dados privados, alterar e até destruir esses dados, e podem chegar a anular transações em sites através de injeções de código SQL.

Ataques MIM: Ataques Man-In-The-Middle (Homem do meio) são ataques de segurança cibernética que permitem que o invasor escute a comunicação entre dois alvos. Ele pode ouvir uma comunicação que deveria, em configurações normais, ser privada.

A melhor coisa que todos nós podemos fazer é estarmos preparados. Não há como ter certeza de que um sistema é impenetrável por ameaças de segurança cibernética. Precisamos garantir que nossos sistemas sejam o mais seguros possível.

2. Prevenções a Ataques de Redes

https://www.cynet.com/network-attacks/network-attacks-and-network-security-threats/

Segregue sua rede: Uma parte básica para evitar ameaças à segurança da rede é dividir uma rede em zonas com base nos requisitos de segurança. A segmentação limita o impacto potencial de um ataque a uma zona e exige que os invasores tomem medidas especiais para penetrar e obter acesso a outras zonas da rede.

Regular o acesso à Internet via servidor proxy: Não permita que os usuários da rede acessem a Internet sem verificação. Passe todas as solicitações por meio de um proxy transparente e use-o para controlar e monitorar o comportamento do usuário. Coloque domínios na lista de permissões para garantir que os usuários corporativos possam acessar apenas os sites que você aprovou explicitamente.

Posicione os dispositivos de segurança corretamente: Coloque um firewall em cada junção de zonas de rede, não apenas na borda da rede. Se você não puder implantar firewalls completos em todos os lugares, use a funcionalidade de firewall integrada de seus switches e roteadores. Implante dispositivos anti-DDoS ou serviços em nuvem na borda da rede. Considere cuidadosamente onde colocar dispositivos estratégicos como balanceadores de carga – se estiverem fora da Zona Desmilitarizada (DMZ), eles não serão protegidos por seu aparato de segurança de rede.

Usar tradução de endereço: Permite traduzir endereços IP internos em endereços acessíveis em redes públicas. Você pode usá-lo para conectar vários computadores à Internet usando um único endereço IP. Isso fornece uma camada extra de segurança, porque qualquer tráfego de entrada ou saída precisa passar por um dispositivo NAT e há menos endereços IP, o que torna difícil para os invasores entenderem a qual host estão se conectando.

Monitore o tráfego de rede: Garanta que você tenha visibilidade completa do tráfego de rede de entrada, saída e interno, com a capacidade de detectar ameaças automaticamente e entender seu contexto e impacto. Combine dados de diferentes ferramentas de segurança para obter uma visão clara do que está acontecendo na rede, reconhecendo que muitos ataques abrangem vários sistemas de TI, contas de usuários e vetores de ameaças.