****

**Faculdade de Ciências e Tecnologias**

**Licenciatura em Engenharia em Tecnologias e Sistemas de Informação**

**4º Ano – Laboral**

**Cadeira: Segurança de Redes**

**Tema: Resumo sobre Segurança de Redes e Internet**

**Discente:**

Damuge Leonardo Francisco

**Docente:**

Dr. Sérgio Simbine

Maputo, Fevereiro de 2023

**SEGURANÇA DE REDE**

A tecnologia de sistema e rede é uma tecnologia chave para uma ampla variedade de aplicações. A segurança é crucial para redes e aplicativos. Embora, rede a segurança é um requisito crítico em países emergentes redes, há uma falta significativa de segurança métodos que podem ser facilmente implementados. Existe uma “lacuna de comunicação” entre o desenvolvedores de tecnologia de segurança e desenvolvedores de redes. O projeto de rede é um bem desenvolvido processo baseado nos Sistemas Abertos Modelo de interface (OSI). O modelo OSI tem vários vantagens ao projetar redes. Oferece modularidade, flexibilidade, facilidade de uso e padronização de protocolos. Os protocolos de diferentes camadas podem ser facilmente combinadas para criar pilhas que permitem o desenvolvimento modular.

Ao considerar a segurança da rede, deve-se enfatizou que toda a rede é segura. A segurança da rede não diz respeito apenas ao segurança nos computadores em cada extremidade da cadeia de comunicação.

Protegendo a rede é tão importante quanto proteger os computadores e criptografando a mensagem. Ao desenvolver uma rede segura, os seguintes precisam ser considerados:

**1.** **Acesso** - os usuários autorizados recebem o significa comunicar de e para um rede particular.

**2.** **Confidencialidade** – Informação na rede permanece privado.

**3.** **Autenticação** – Certifique-se de que os usuários do rede são quem dizem ser.

**4.** **Integridade** – Certifique-se de que a mensagem não modificado em trânsito.

**5.** **Não-repúdio** - Certifique-se de que o usuário não refutar que ele usou a rede.

Para diminuir a vulnerabilidade do computador na rede existem muitos produtos disponíveis. Esses ferramentas são criptografia, mecanismos de autenticação, detecção de intrusão, gerenciamento de segurança e firewalls. As empresas em todo o mundo estão usando uma combinação de algumas dessas ferramentas. “Intranets” estão conectadas à internet e razoavelmente protegido dela.

As invasões de rede consistem em pacotes que são introduzidos para causar problemas para as seguintes razões: Consumir recursos inutilmente, para interferir com qualquer recurso do sistema função pretendida e para obter conhecimento do sistema que pode ser explorado em ataques posteriores.

A última razão para uma invasão de rede é mais comumente guardado e considerado pela maioria como o único motivo de invasão.

**DIFERENCIANDO SEGURANÇA DE DADOS E SEGURANÇA DE REDE**

A segurança dos dados é o aspecto da segurança que permite os dados do cliente sejam transformados em ininteligíveis dados para transmissão. A segurança da rede está principalmente contida no camada física.

**BREVE HISTÓRIA DA INTERNET**

- O nascimento da interna acontece em 1969, quando Rede de agências para projetos de pesquisas avançadas (ARPANet) é encomendado pelo departamento de defesa (DOD) para pesquisa em redes.

- A metade dos anos 80 marca um boom na vida pessoal indústrias de computadores e superminicomputadores.

- Na década de 1990, a internet começou a se tornar disponível ao público. A World Wide Web foi nascer. Netscape e Microsoft foram ambos competindo no desenvolvimento de um navegador para o Internet. A Internet continua a crescer e a navegar a internet tornou-se equivalente a assistir TV para muitos usuários.

**LINHA DO TEMPO DE SEGURANÇA**

- Criptógrafos poloneses criaram uma máquina de enigmas em 1918 que converteu mensagens simples em texto criptografado.

- Em 1930, Alan Turing, um brilhante matemático decifrou o código do Enigma. Proteger as comunicações era essencial no mundo Guerra II.

- Na década de 1960, o termo “hacker” é cunhado por um casal do Instituto de Tecnologia de Massachusetts (MIT). O Departamento de Defesa começou a ARPANet, que ganha popularidade como canal para a troca eletrônica de dados e informações.

- Durante a década de 1970, o protocolo Telnet foi desenvolvido. Isso abriu a porta para o uso público de redes de dados originalmente restritas a contratados do governo e pesquisadores acadêmicos.

- Durante a década de 1980, os hackers e os crimes relacionadosaos computadores estavam começando a surgir.

- A Lei de Fraude e Abuso de Computador de 1986 foi criado por causa do crime de Ian Murphy roubar informações de computadores militares.

**ARQUITETURA IPV4**

O protocolo contém alguns aspectos que causou problemas com seu uso. Esses problemas fazem nem todos estão relacionados à segurança. Eles são mencionados para obter uma compreensão abrangente do protocolo de internet e suas deficiências. As causas dos problemas com o protocolo são: Espaço de Endereçamento, roteamento, configuração, segurança e qualidade do Serviço. A arquitetura IPv4 tem um endereço de 32 bits largo.

**ARQUITETURA IPV6**

Quando o IPv6 estava sendo desenvolvido, a ênfase era colocados sobre os aspectos do protocolo IPv4 que precisavam ser melhorado. Os esforços de desenvolvimento foram colocados nas seguintes áreas: Roteamento e endereçamento, arquitetura multiprotocolo, arquitetura de segurança e controle de tráfego.

O espaço de endereços do protocolo IPv6 foi estendido por suportando endereços de 128 bits. Com 128 bits endereços, o protocolo pode suportar até 3.41038 máquinas. Os bits de endereço são usados menos eficiente neste protocolo porque simplifica configuração de endereçamento.

**ATAQUES CIBERNÉTICOS NA ACTUALIDADE**

Existem quatro atributos principais de segurança do computador. Eles foram mencionados antes de uma forma ligeiramente diferente forma, mas são reapresentados por conveniência e ênfase. Esses atributos de segurança são confidencialidade, integridade, privacidade e disponibilidade.

|  |  |  |
| --- | --- | --- |
| **ATRIBUTOS DA SEGURANÇA DA INFORMAÇÃO** | **MÉTODOS DE ATAQUE** | **TECNOLOGIA PARA SEGURANCA NA INTERNET** |
| Confidencialidade | Espionagem, Ilacking, phishing, DoS e falsificação de IP | IDS, Firewall, Sistemas criptografados, IPSec e SSL |
| Integridade | Virus, worms, trojas, DoS e falsificação de IP | IDS, Firewall, Software Anti-Malware, IPSec e SSL |
| Privacidade | Bombardeio de email, spamming, hacking DoS e Cookies | IDS, Firewall, Software Anti-Malware, IPSec e SSL |
| Disponibilidade | DoS, bombardeio de email, spamming e infecções no resgitro do sistema de boot | IDS, Software Anti-Malware, IPSec e Firewall |