****

**Faculdade de Ciências e Tecnologias**

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

**4º Ano – Laboral**

**Cadeira: Segurança de Redes**

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

**Discente:**

Esmeralda Malumane

**Docente:**

Dr. Sérgio Simbine

Maputo, Abril 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.

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 foi modificado em trânsito

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

Os tipos de ataques pela internet precisam ser também ser estudado para ser capaz de detectar e proteger contra eles. Os sistemas de detecção de intrusão são estabelecido com base nos tipos de ataques mais comumente usado. 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

• 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. As outras razões mencionados precisam ser frustrados também.

**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 ados para transmissão. Mesmo que isso seja ininteligível dados são interceptados, uma chave é necessária para decodificar o mensagem. Este método de segurança é eficaz para um certo grau. Criptografia forte no passado pode ser facilmente quebrado hoje. Métodos criptográficos tem que continuar a avançar devido ao avanço dos hackers também. Ao transferir texto cifrado em uma rede, é útil ter uma rede segura. Isso permitirá o texto cifrado a ser protegido, de modo que seja menos provável que muitas pessoas até tentem quebrar o código. Uma rede segura também evitará alguém de inserir mensagens não autorizadas na rede. Portanto, as cifras rígidas são necessários, bem como redes de ataque rígido.

**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 ARPANET é um sucesso desde o início. Embora originalmente projetado para permitir que os cientistas compartilhar dados e acessar computadores remotos, e‐mail rapidamente se torna o aplicativo mais popular. O A ARPANET torna-se uma agência postal digital de alta velocidade como as pessoas o usam para colaborar em projetos de pesquisa e discutir temas de vários interesses.

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.

**Arquiteturas IPv4 e IPv6**

O IPv4 foi projetado em 1980 para substituir o NCP protocolo da ARPANET. O IPv4 exibiu muitos limitações após duas décadas. O protocolo IPv6 foi projetado com as deficiências do IPv4 em mente. O IPv6 não é um superconjunto do protocolo IPv4; em vez de é um novo projeto.

O design do protocolo de internet é tão vasto e não pode ser totalmente coberto. As principais partes da arquitetura relacionados à segurança são discutidos em detalhes.

**Ataques pela Internet Atual**

|  |  |  |
| --- | --- | --- |
| **Atributos da Segurança da informacao** | **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 |