10ª Jornada Acadêmica da Jornada da UEG
"Integrando saberes e construindo conhecimento"
10 a 12 de Novembro de 2016
UEG - Câmpus Santa Helena de Goiás, GO

AS MELHORES FERRAMENTAS DE SEGURANÇA PARA SISTEMAS EM REDE

José Vitor Souza Silva[1]; João Vitor Rodrigues da Silva[1]; Paulo Ricardo Ribeiro Pereira[1]; Sergio Ricardo Belchior Filho[1]; Higor Pereira Delfino[1]; Thaiz Silva de Lima[1]; Glauco Vitor Pedrosa[2]

[1]Discentes do curso de Sistemas de Informação da UEG- Câmpus Santa Helena de Goiás, email: jose.vitor.s@hotmail.com; jvitorrs1831@outlook.com; pauloricardoribeiropereira@gmail.com; sergiobelchiorfilho@outlook.com; hygor.tec@gmail.com; thaiz_x3@hotmail.com

[2]Docente do curso de Sistemas de Informação da UEG- Câmpus Santa Helena, email: glaucovitor@ueg.com

RESUMO: Atualmente, a segurança tem sido uma das maiores preocupações quando o assunto são redes de computadores, com o crescimento da tecnologia e o surgimento de novas maneiras de comunicação e redes onde se pode compartilhar todo e qualquer tipo de dados e informação com qualquer dispositivo conectado. Graças a Internet as empresas, organizações e ambientes corporativos puderam expandir seus negócios e assim conseguirem mais lucro. Mas, também com a evolução dos sistemas em rede, os ataques (roubos, destruição, modificação ou deturpação de informação), aumentaram gradualmente. Por isso, as empresas e organizações que fazem uso destes sistemas investem cada vez mais em sua segurança, pois várias informações de alto valor tanto intelectual quanto material podem ser roubadas, sendo que alguns ataques podem até acabar com a integridade e confiança em uma corporação ou empresa. Através deste artigo serão apresentadas algumas ferramentas utilizadas para aumentar a segurança destes sistemas, que apesar de não serem perfeitas, ajudam a prevenir os mais variados tipos de ataque que possam ocorrer.

Palavras-chave: Segurança, ferramentas, redes de computadores.

THE BEST SAFETY TOOLS FOR NETWORK SYSTEMS

ABSTRACT: Currently, sefety has been one of the most concerns when the topic is computer network, with the growth of technology and the emergence of new ways of

communication and networks where you can share any type of data and information to any connected device. Due to Internet companies, organizations and corporate environments could expand their business and thus gain more profit. But also with the evolution of networked systems, attacks (theft, destruction, alteration or misrepresentation of information), increased gradually. So, to companies and organizations that make use of these systems are increasingly investing in their safety because several high-value information both intellectual and material can be stolen, and some attacks may even end up with integrity and trust in a corporation or company. Through this article we will present some tools used to enhance the security of these systems, although not perfect, help prevent various types of attacks that might occur.

Key-words: Safety, tools, computer network.

INTRODUÇÃO

Com o aumento do uso aos sistemas em redes ao redor do mundo e com o surgimento da Internet, a rede mundial de computadores, trouxe com ela vários benefícios não só às empresas, mas também no nosso dia-a-dia, podemos compartilhar todo tipo de coisa com qualquer um, basta estar conectado em uma rede, tudo de forma simples e rápida e acessível a todos.

Mas também é preciso ter cuidado ao disponibilizar qualquer tipo de informação importante na internet ou redes que não forem privadas. Estas informações podem estar vulneráveis a ataques externos, tendo a chance de serem roubadas ou em outros casos, alteradas e excluídas. E em caso de provedores de serviços, serem interrompidos de suas atividades, prejudicando a empresa.

Quando colocamos no ar um sistema e o conectamos a uma rede, devemos planejar a sua segurança que pode conter uso de variadas ferramentas para minimizar este problema. Nas próximas seções serão apresentadas algumas ferramentas que tem como a segurança de sistemas sua principal função, e como podem auxiliar no aumento da segurança dos dados e informações.

Sistemas de Detecção de Intrusos – IDS

Um sistema de detecção de intrusos geralmente detecta manipulações de sistema de computador indesejadas, normalmente através da internet. Essas manipulações normalmente vêm de ataques de hackers. Os IDS (Intruaion Detection Systems) são usados para detectar vários tipos de comportamentos maliciosos que podem comprometer a segurança e a confiabilidade de um sistema. Eles incluem ataques pela rede contra serviços vulnearaveis, ataque baseado em uma estação como aumento de privilegio, logins não autorizados e malware.

SNORT

Um sistema de detecção de intrusões (IDS) público para as massas, O Snort e uma ferramenta eficiente de detecção de intrusões, capaz de efetuar analises em tempo real de trafego capturado e registro de datagrama em redes IP. Permite analisar protocolos, procura de conteúdos e pode ser usado para detectar diversos ataques e sondas, nomeadamente transbordamentos de memória, levantamentos furtivos de portos de transporte, ataques usando CGI, sondas para SMB, tentativas de identificação de sistemas operativos, etc.

OSSEC

O Ossec e um sistema de detecção de intruso baseado em host, escalável, multi – plataforma, Open Source. Possui um poderoso mecanismo de correlação e análise, integrando análise de log, verificação de integridade de arquivos, monitoramento de registro do Windows, execução de políticas centralizadas, detecção de rootkits, alertas em tempo real e resposta ativa.

Samhain

Um Sistema de detecção de intruso baseado em host fornece verificação de integridade de arquivos e monitoramento e analise de arquivos de log, assim como detecção de rootkits, monitoramento de portas, detecção de executáveis SUID desonestos e processos ocultos.

NOME	PLATAFORMA	LICENCIAMENTO
SNORT	LINUX/UNIX, WINDOWS	GRATUITO
OSSEC	LINUX, OPENBSD, MacOS, SOLARIS,	GRATUITO

	WINDOWS	
SAMHAIN	UNIX, LINUX, CYGWIN/WINDOWS	GRATUITO

Tabela 1: Sistemas de Detecção de Intrusos – IDS

Criptografia

A criptografia é uma técnica de esconder informação original em uma outra ilegível. Essa técnica foi empregada na comunicação e transferência de dados por volta de 1940 com a Enigma, uma máquina de criptografia com rotores desenvolvida pelo alemão Arthur Scherbius. Por anos ela foi um grande problema para os inimigos das tropas alemãs, que por mais que interceptassem as mensagens não conseguia lê-las. Isso foi contornado com construção de outra máquina. A máquina de Turing, desenvolvida pelo britânico Alan Turing, considerada por muitos o primeiro computador. A maquina de Turing testava todas as combinações possíveis para decifrar a mensagem transformá-la em um texto legível, hoje essa técnica é conhecida por Brute Force ou Ataque de força bruta.

Para fazer a segurança com encriptação é utilizado complexos algoritmos, na Tabela1 podemos ver os melhores do mercado.

Nome	**Plataforma**	**Licença**
Data Encryption Standard (DES)	Win/Linux/MAC	FREE
Triple Data Encryption Standard (3DES)	Win/Linux/MAC	FREE
Advanced Encryption Standard (AES)	Win/Linux/MAC	FREE

Tabela 2: Criptografia

Data Encryption Standard (DES)

A chave consiste nominalmente de 64 bits, porém somente 56 deles são realmente utilizados pelo algoritmo. Os oito bits restantes são utilizados para checar a paridade e depois são descartados, portanto o tamanho efetivo da chave é de 56 bits, e assim é citado o tamanho de sua chave.

Triple Data Encryption Standard (3DES)

Os dados são encriptados com a primeira chave, descriptado com a segunda chave e finalmente encriptado novamente com a terceira chave. Isto faz do 3DES ser mais lento, mas oferece maior segurança.

Advanced Encryption Standard (AES)

Algoritmo padrão nos estados unidos, não possuir patentes, cifrar em blocos de 128 bits usando chaves de 128, 192 e 256 bits, pode ser implementado tanto em software quanto em hardware, ter maior rapidez em relação ao 3DES

VPN – Virtual Private Network

VPN como o próprio nome já diz é uma rede virtual privada que utiliza uma rede pública como tráfegos dos dados, esta rede privada usa o tunelamento e a criptografia para que somente as maquinas que acessam aquela rede possa ver os dados que estão sendo enviado assim mantendo-os seguros e fora de invasores.

Virtual Private Network (VPN)

Ferramenta	Descrição	Plataforma	Licença
ExpressVPN	Banda larga ilimitada e uma conexão rápida e criptografada com segurança SSL, permitindo a alteração de IP por cada localização de cidade espalhado no mundo acessando a qualquer website ou aplicação sem restrições geográficas ou censura.	Windows,Linux, Mac,IOS e Android	Gratuito
vyprVPN	Gerenciamento de servidores sem partes de terceiros, aplicativo fácil de usar, banda larga ilimitada, vários protocolos de criptografia e utiliza o chameleon uma tecnologia que derruba bloqueios de VPN. Existe a versão gratuita que oferece este serviço mas para um trafego de dados limitado que é 500 MB por mês, a versão paga não tem restrições a limite de dados.	Windows, Mac, Android, IOS, TV e Roteador	Gratuito e Pago
Steganos Online Shield	Exibe dispositivos em sua rede que poderiam ser ameaças, VPN anônima pela internet com servidores em muitos países e Criptografia AES de 256 bits. O	Windows e Android	Pago

	aplicativo Bloqueia anúncios e pop-ups para que a sua navegação não seja interrompida e assim o cliente navegue ser incomodado.		

Tabela 3: VPN – Virtual Private Network

Vulnerabilidade em Máquinas de Sistemas Distribuídos

Segundo Tanenbaum (2007) um sistema distribuído é aquele que se apresenta aos seus usuários como um sistema centralizado, mas que, na verdade, funciona de diversas CPUs independentes. Além disso um sistema distribuído não deve ter pontos críticos de falha.

Nmap

O Nmap é eficaz o suficiente para detectar dispositivos remotos, e na maioria dos casos identifica corretamente firewalls e roteadores, além de sua marca e modelo. Os administradores de rede podem usar o Nmap para verificar quais portas estão abertas, e também se essas portas podem ser exploradas ainda mais em ataques simulados. A saída é um texto claro e detalhado.

Metasploit

O Metasploit é uma ferramenta fantástica estruturada em código aberto, que realiza exames rigorosos contra um conjunto de endereços IP. Ao contrário de muitos outros enquadramentos, pode também ser usado para técnicas anti-forenses. Programadores experientes podem escrever uma peça de código explorando uma vulnerabilidade particular, e testá-lo com o Metasploit para ver se ele é detectado. Este processo pode ser invertido tecnicamente – quando um vírus ataca utilizando alguma vulnerabilidade desconhecida, o Metasploit pode ser usado para testar o "antídoto" para ele.

Vulnerabilidade em Máquinas de Sistemas Distribuídos

Vulnerabilidade é definida como uma condição que, quando explorada por um atacante, pode resultar em uma violação de segurança. Exemplos de vulnerabilidades são falhas no projeto, na implementação ou na configuração de programas, serviços ou equipamentos de rede. Um ataque de exploração de vulnerabilidades ocorre quando um atacante, utilizando-se de uma vulnerabilidade, tenta executar ações maliciosas, como invadir um sistema, acessar informações confidenciais, disparar ataques contra outros computadores ou tornar um serviço

inacessível.

Wireshark

O Wireshark (anteriormente chamado de Ethereal) funciona em modo promíscuo para capturar todo o tráfego de um domínio de broadcast TCP. Filtros personalizados pode ser ajustados para interceptar o tráfego específico, por exemplo, para capturar a comunicação entre dois endereços IP, ou capturar consultas DNS baseados na rede. Normalmente, o testador está à procura de endereços IP vadios, pacotes com endereços forjados, pacotes desnecessários, e geração de pacotes suspeitos a partir de um único endereço IP. O Wireshark dá uma visão ampla e clara do que está acontecendo na sua rede.

Ferramenta	**Plataforma**	**Licença**
Nmap	Windows, Mac, Linux	Gratuito
Metasploit	Windows, Mac, Linux	Grauito
Wireshark	Windows, Mac, Linux, BSD	Gratuito

Tabela 4: Vulnerabilidade em Máquinas de Sistemas Distribuídos

Firewall

Entre todas as grandes formas diferentes de segurança nos sistemas de redes, firewall é uma das que mais se destacam, segundo Gouveia, Magalhães (2007) Firewall trata-se de uma combinação de software e hardware que bloqueia a entrada de intrusos através de redes públicas, com isso ele é capaz de gerenciar as informações que entram e saem da rede.

Firewall

Ferramenta	**Descrição**	**Plataforma**	**Licença**
Iptables	O Iptables se encontra no Kernel do Linux e em algumas extensões do Windows e utiliza a filtragem de pacotes como estrutura básica, é uma ferramenta básica de interface com o usuário que permite a criação de regras de firewall.	Windows e Linux	Paga. A contratação custa R$ 72,00 e a renovação nos anos seguintes R$ 40,00.
AVG	O AVG Internet Security, criado pela Freeware e comercial controla todas as entradas de rede no PC, e verifica outras maquinas	Windows, Linux, Android e iOS.	Gratuita, embora há várias versões diferentes pagas.

	que queiram se conectar a esta, e caso não esteja na lista de permissão ele envia uma solicitação para o usuário se ele permite o acesso.		
Comodo Firewall	O Comodo Firewall é outra ferramenta que utiliza os conceitos de um firewall, esta monitora a rede *Wireless Fidelity* (Wi-Fi) e atualiza periodicamente os dados sobre malware, é capaz de criar códigos e regras independentes para se preparar para eventualidades de aplicações sobre.	Windows XP, Ubunto, Debian e Fedora.	Gratuita, embora há outras versões diferentes pagas.

Tabela 5: Firewall

RESULTADOS E DISCUÇÃO

Através do uso das ferramentas e dos softwares apresentados neste trabalho é esperada uma redução drástica no numero de invasões, roubo de dados e vírus, pois através destas ferramentas é possível fortificar a segurança de rede e dos dispositivos como um todo cobrindo várias falhas na segurança.

CONCLUSÃO

Com o finalização desde trabalho conclui-se que é sempre importante ter um nível de segurança razoável em qualquer dispositivo que faça contato com a Internet para evitar o máximo possível o roubo de dados e outros tipos de ataques.

Este trabalho teve como objetivo apresentar algumas ferramentas úteis para a segurança em redes, através de softwares e ferramentas especializadas nesta área, que estão em crescente uso e oferecem uma ótima qualidade em seus serviços e funcionalidades.

Além disso, a área de segurança em redes está sempre em constante crescimento, sendo um dos melhores setores para se investir, pois a segurança sempre será essencial em qualquer sistema, seja ela de grande ou médio porte.

REFERÊNCIAS

GOUVEIA, J. Magalhães A. **Redes de computadores**. 1. ed. Tradução e revisão Jorge Luís Machado do Amaral e José Franco Machado do Amaral. Rio de Janeiro: LTC. 2007. 264 p.

Netfilter, Iptables - O que é a Netfilter.org? Disponível em: < http://www.netfilter.org/>. Acesso em 20 de outubro de 2016.

TANENBAUM, Andrew S; STEEN, Maarten Van. **Sistemas Distribuídos**: princípios e paradigmas.2ªEd. São Paulo: Pearson Prentice Hall, 2007.382paginas.

Segurança de Sistemas. Disponível em:<http://pt.slideshare.net/JerryNeves/segurana-em-sistemas-distribuidos>. Acesso em 01 de Novembro de 2016.

Segurança em Redes Informáticas. Disponível em: <http://sejalivre.org/as-10-principais-ferramentas-open-source-de-seguranca/Segurança em Redes Informáticas - Formação.com.pt>. Acesso em 01 de Novembro de 2016.

Vyprvpn. Disponível em:< https://www.goldenfrog.com/BR/vyprvpn>. Acesso em 01 de Novembro de 2016.

Safervpn. Disponível em:< https://www.safervpn.com/pt/>. Acesso em 01 de Novembro de 2016.

Steganos online shield vpn. Disponível em:< https://www.steganos.com/en/steganos-online-shield-vpn>. Acesso em 01 de Novembro de 2016.

IP vanish vpn. Disponível em:< https://www.ipvanish.com>. Acesso em 01 de Novembro de 2016.

ExpressVPN. Disponível em:< http://www.techtudo.com.br/tudo-sobre/expressvpn-app.html>. Acesso em 01 de Novembro de 2016.