FACULDADE DE ADMINISTRAÇÃO E NEGÓCIOS
SERGIPE - FANESE
NÚCLEO DE PÓS GRADUAÇÃO E EXTENSÃO – NPGE
CURSO DE PÓS GRADUAÇÃO “LATO SENSU”
ESPECIALIZAÇÃO EM REDES DE COMPUTADORES

JOSÉ EDUARDO NASCIMENTO FIGUEIREDO

SEGURANÇA EM REDES DE COMPUTADORES

Aracaju – SE
2010

JOSÉ EDUARDO NASCIMENTO FIGUEIREDO

SEGURANÇA EM REDES DE COMPUTADORES

Trabalho de Conclusão de Curso apresentado ao Núcleo de Pós-Graduação e Extensão da FANESE, como requisito para obtenção do título de Especialista em Redes de Computadores

Aracaju – SE
2010

JOSÉ EDUARDO NASCIMENTO FIGUEIREDO

SEGURANÇA EM REDES DE COMPUTADORES

Trabalho de Conclusão de Curso apresentado ao Núcleo de Pós-Graduação e Extensão – NPGE, da Faculdade de Administração de Negócios de Sergipe, como requisito para a obtenção do título de Especialista em Redes de Computadores

_____

Prof. Especialista Ricardo Torres

_____

Prof. Me. Sérgio Luiz Elias de Araújo

_____

José Eduardo Nascimento Figueiredo

Aprovado (a) com média: _____

Aracaju (SE), _____ de _____ de 2010

RESUMO

Este artigo consiste em demonstrar de forma conceitual as principais características de Segurança das Redes de Computadores, pois a necessidade crescente em disponibilizar produtos e serviços na internet, traz uma preocupação maior em garantir a segurança das informações. Há atualmente diversas técnicas de invasão, danos e roubos de dados, é pensando nisso que cada vez mais aparecem novas soluções para proteger as redes coorporativas e residenciais.

Palavras-chave: Segurança. Redes de Computadores. Ameaças. Ataques. Criptografia. Protocolo. Integridade.

ABSTRACT

This article is to demonstrate to the main conceptual features of Security of Computer Networks, as the growing need in providing products and services on the Internet, brings a major concern in the security of information. There are currently several techniques of invasion, damage and theft of data, is thinking about that more and more appear new solutions to protect corporate networks and residential.

LISTA DE FIGURAS

SUMÁRIO

CAPÍTULO I

1. INTRODUÇÃO

Com relação a redes de computadores é importante salientar que as informações pessoais e corporativas devem ser tratadas com o máximo de segurança possível.

A tendência das grandes, médias e pequenas empresas em distribuir informações como produtos e serviços diretamente na internet, com o intuito de aproximar a empresa dos seus clientes em potencial, faz com que haja uma necessidade especial em aplicar técnicas de segurança da informação a seus serviços, protegendo assim, a empresa e seus clientes de possíveis danos processuais, financeiros, de imagem, entre outros.

Para garantir o máximo de segurança possível nas redes de computadores é necessário conhecer bem as principais ameaças, métodos e ataques, bem como as técnicas existentes de controle e prevenção.

O objetivo principal deste projeto de pesquisa é adquirir, demonstrar e disseminar conhecimento, tanto no meio acadêmico quanto profissional, a respeito das principais características dos protocolos.

Durante o desenvolvimento do projeto será apresentada uma breve introdução sobre segurança de redes de computadores, os conceitos básicos das principais ameaças de risco e as principais técnicas utilizadas pelas redes corporativas, utilizando-se de pesquisas bibliográficas e estudos conceituais.

CAPÍTULO II

2. SEGURANÇA EM REDES DE COMPUTADORES

Desde o início da utilização das redes de computadores nunca houve uma preocupação tão grande em relação à segurança da informação como hoje em dia, isto ocorre principalmente devido ao crescimento constante de usuários conectados à rede e a grande disponibilidade de serviços na internet, principalmente transações bancárias.

Segundo Tanebaum (2003), como milhões de cidadãos comuns atualmente estão usando as redes para executar operações bancárias, fazer compras e arquivar sua devolução de impostos, a segurança das redes está despontando no horizonte como um problema potencial.

Uma Rede de Computadores para ser considerada segura deve-se garantir quatro características principais:

- Confidencialidade – Determinadas informações devem estar armazenadas de forma confiável e de acesso restrito, como informações pessoais dos clientes, contas bancárias etc.
- Integridade – Deve haver garantias de que as informações não foram modificadas de forma maliciosa.
- Disponibilidade - Garantir que todos os serviços estejam disponíveis conforme necessidade da empresa.
- Autenticidade - Garantir que as informações contidas no site, email ou serviço disponível seja verdadeiramente da empresa ou pessoa em questão e não uma falsificação.

2.1 Ameaças e Métodos de Ataques

Ameaças e ataques às redes de computadores e aos sistemas de informação consistem na utilização de técnicas específicas para se obter acesso as redes e sistemas restritos, informações sigilosas e fraudes.

Os ataques e ameaças podem ser classificados por:

- Modo de Atuação

  - Passivo – Consiste apenas na interceptação da informação durante o trajeto dos pacotes entre a origem e o destino.
  - Ativo – Consiste na atuação de forma direta sobre a informação, como adulteração de sites, roubo de informações sigilosas, bloqueio de serviços, entre outros.
- Objetivo
  - Interrupção – Ataca principalmente a disponibilidade de um serviço ou de um sistema.
  - Interceptação – Ataca a confidencialidade das informações.
  - Modificação – Ataca a integridade das informações.
  - Fabricação – Ataca a autenticidade das informações.

2.1.1 Malwares

Os Malwares consistem em códigos maliciosos desenvolvidos com a finalidade de roubar informações ou danificar serviços e sistemas operacionais, tais ameaças são originadas principalmente de arquivos infectados distribuídos em anexos de emails, computadores infectados na rede e os mais diversos tipos de mídias removíveis.

Os principais Malwares disseminados na internet são:

- Vírus – Programas maliciosos que infectam outros aplicativos ou áreas restritas do sistema operacional do computador do usuário.
- Worms – São vírus que se replicam no computador infectado e se propagam principalmente por uso de emails, arquivos e pastas compartilhadas, com o intuito de explorar vulnerabilidades nos sistemas operacionais e em aplicativos instalados para proporcionar invasões e roubo de dados.
- Bots – Programas similares aos worms cuja finalidade principal é abrir comunicação com invasores para que o mesmo possa realizar ataque de acesso, envio de spam, e phishing, roubo de dados entre outros danos.
- Botnets – Redes formadas por diversos Bots.

- Trojans (Cavalo de Tróia) e BackDoors – Programas maliciosos que tentam se passar por programa de uso corriqueiro do usuário com o intuito de roubo de informações.
- KeyLoggers – Programas maliciosos que infectam os computadores com o intuito de registrar tudo o que é digitado no teclado pelo usuário.
- ScreenLoggers - Programas maliciosos que infectam os computadores com o intuito de capturar a imagem da tela no momento em que o usuário clicar com o mouse em algum botão.
- Spywares – Programas maliciosos que infectam as máquinas com o intuito de modificar configurações no sistema operacional, bem como coletar informações importantes.

> Spyware é o termo usado para descrever software que executa determinados comportamentos, como publicidade, recolhimento de informações pessoais ou alteração da configuração do computador, normalmente sem o seu consentimento prévio. (Microsoft, 2006)

- RootKits – Trojan que utiliza de técnicas de programação avançadas para evitar a detecção e remoção do mesmo, bem como de outros programas maliciosos.

> O objetivo do rootkit é esconder a si mesmo e de outro software para não ser visto. Isso é feito para prevenir que um usuário identifique e remova potencialmente um software de ataque. Um rootkit pode se esconder em quase todos os softwares, incluindo servidores de arquivos, keyloggers, botnets e remailers. Muitos rootkits podem até esconder grande quantidade de arquivos, permitindo assim que um atacante armazene diversos arquivos, invisivelmente, em seu computador. (Microsoft, 2005)

2.1.2 DOS (Denial of Service – Negação de Serviço)

Segundo Tanebaum (2003), Os ataques em que o objetivo do intruso é desativar o destino em vez de roubar dados são chamados ataques DoS (Denial of Service — negação de serviço).

Este modo de ataque consiste na utilização de técnicas específicas para sobrecarregar um determinado servidor com inúmeras solicitações até causar a indisponibilidade do serviço.

2.1.3 Ataques a Camada 2 (Enlace)

a) MAC (Media Access Control) Spoofing

Técnica utilizada principalmente para roubo de informações e acessos restritos para determinados endereços MAC, esta técnica consiste em um computador tentar se passar por outro, alterando o endereço MAC e com isso obter acessos a redes e informações restritas.

b) ARP (Address Resolution Protocol) Poisoning

Técnica utilizada pelos hackers em redes Ethernet com o intuito de roubar dados, tentando se passar por outro computador para receber os pacotes e reenviar para o computador correto, intermediando toda a transmissão de informações.

> *ARP-Poisoning* ou *ARP Spoofing* é um tipo de ataque no qual uma falsa resposta ARP é enviada à uma requisição ARP original. Enviando uma resposta falsa, o roteador pode ser convencido a enviar dados destinados ao computador 1 para o computador 2, e o computador por último redireciona os dados para o computador 1.(Vieira, 2005)

Para evitar este tipo de ataque é necessária a utilização de switchs com a opção MAC Binding disponível e ativada, isto evita que o endereço MAC configurado a uma determinada porta do switch não seja modificado.

Há diversos programas para realizar o ARP Poisoning como ARPoison e o Parasite, para detectar uma tentativa de ataque utiliza-se de programas como o Arpwatch para monitorar e detectar se houve alguma mudança na tabela ARP e avisa o técnico responsável, outra é o RARP (Reverse Arp) para solicitar o endereço IP de um determinado endereço MAC.

c) DHCP (Dynamic Host Configuration Protocol) Starvation

Esta técnica consiste em inundar o servidor DHCP com requisições de IPs geradas aleatoriamente com o intuito de realizar um DOS (Negação do Serviço) ao esgotar todos os IPs disponíveis.

d) DHCP (Dynamic Host Configuration Protocol) Rogue Server

Esta técnica consiste em anular um servidor DHCP causando uma negação do serviço e disponibilizar uma máquina com o mesmo serviço na rede.

O invasor configura o serviço da nova máquina de forma como lhe convêm, com o intuito de gerenciar e capturar determinadas informações, bem como possibilitar brechas na rede, tudo isto de forma transparente para o usuário.

2.1.4 Ataques a Camada 3 (Rede)

a) IPSpoofing

Técnica utilizada pelos hackers utilizando-se de pacotes com IPs forjados com o intuito de quebrar a segurança das redes com autenticação apenas por IP e não por usuário.

> Spoofing is a technique where an intruder attempts to gain unauthorized access by altering a packet's IP address to make it appear as though the packet originated in a part of the network with higher access privileges. (CHECKPOINT, 2003)[1]

2.1.5 Ataques a Camada 4 (Transporte)

a) SYN Flood

Esta técnica consiste na utilização do protocolo TCP, que é orientado à conexão, onde a máquina do invasor envia diversos pacotes *SYN*, solicitando

[1] Spoofing é uma técnica onde um intruso tenta obter acesso não autorizado por alteração de endereço de um pacote IP para fazer parecer que o pacote foi originado em uma parte da rede com mais privilégios de acesso

abertura de conexão, o servidor responde com o pacote *SYNACK* e aguarda a resposta *ACK* da máquina do invasor, que nunca irá responder.

Como cada computador tem suas limitações, a máquina atacada vai chegar ao limite, causando assim um DOS, decorrente da não disponibilidade de comunicação.

2.1.6 Ataques a Camada 7 (Aplicação)

a) DNS Poisoning

Esta técnica consiste no envenenamento do cache de servidores DNS com informações maliciosas, isto é, o invasor pode realizar no servidor DNS a inclusão ou alteração de uma determinada informação com o intuito de redirecionar os acessos de um determinado site para um da sua autoria, muitas vezes cópias de sites bancários e de lojas virtuais (Phishing) ou arquivos infectados com malwares.

b) PortScan

O invasor utiliza determinados programas pra detectar possíveis brechas de sistemas operacionais ou serviços para realizar tentativas de invasões nas portas que estiverem abertas.

2.1.7 Ataques de Tentativas de Acesso

a) Password Crack

Esta técnica consiste na tentativa de quebra de senhas utilizando-se de técnicas específicas como força bruta, dicionário de dados ou tabelas hash.

2.1.8 Técnicas de Fraude e Roubo de Informações

a) Phishing

Baseia-se principalmente na utilização de sites e emails falsos para que o usuário digite senhas e dados pessoais, principalmente cartões de créditos e dados bancários.

> Phishing é basicamente um golpe on-line de falsificação, e seus criadores não passam de falsários e ladrões de identidade especializados em tecnologia. Eles usam spams, websites maliciosos, mensagens instantâneas e de e-mail para fazer com que as pessoas revelem informações sigilosas, como números de contas bancárias e de cartões de crédito (Symantec, 2005)

Os sites falsos normalmente são direcionados principalmente por um DNS envenenado ou por links enviados por email, os mais copiados são sites de bancos, e-commerce entre outros.

b) Engenharia Social

Este modo de ataque consiste em utilizar de técnicas de convencimento para que os usuários forneçam informações valiosas como CPF, endereço, datas, entre outras, ou instalar programas maliciosos no computador.

Tais informações podem ser usadas para cadastros em sites de compras, cartões de créditos e acessos a sistemas restritos.

2.2 Técnicas de Segurança

2.2.1 Criptografia

Segundo Torres (2002), Criptografia é o ato de codificar dados em informações aparentemente sem sentido, para que pessoas não consigam ter acesso às informações que foram cifradas.

A utilização de criptografia consiste em transformar um texto em outro inelegível para que se possa garantir confidencialidade e autenticação na troca das informações.

Esta técnica de segurança utiliza-se de chaves de codificação e decodificação para cifrar os dados, estas chaves podem ser do tipo simétrica (chave privada) e assimétrica (chave pública e privada).

2.2.1.1 Criptografia Simétrica

A Criptografia Simétrica consiste basicamente na utilização de uma chave única privada para criptografar e descriptografar as informações. Tal chave é compartilhada entre a origem e o destino.

O grande problema na utilização de Criptografia Simétrica é o compartilhamento da chave, pois, um hacker ao conseguir uma chave privada compartilhada pode-se decifrar as informações de ambos os lados.

Abaixo estão alguns exemplos de algoritmos de Criptografia Simétrica:

- DES
- IDEA
- AES
- RC2, RC4 e RC5

A figura a seguir mostra o funcionamento da criptografia de chave simétrica.

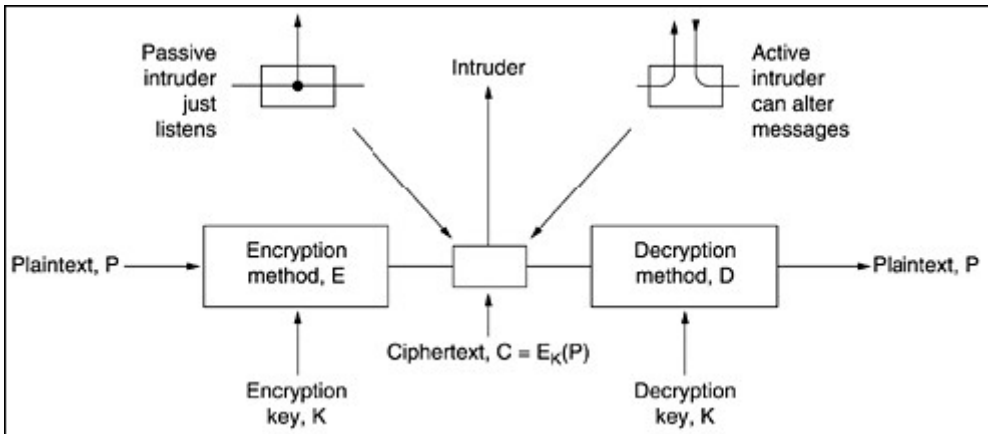

Figura 1: Criptografia Simétrica
Fonte: Redes de Computadores, Tanenbaum

2.2.1.2 Criptografia Assimétrica

A Criptografia Assimétrica consiste na utilização de duas chaves, uma pública e outra privada, onde apenas a partir da chave privada é possível a geração de uma chave pública.

Seguem alguns exemplos de algoritmos de Criptografia Assimétrica:

- RSA
- DSA
- Diffie-Hellman

A figura abaixo mostra o funcionamento da criptografia de chave assimétrica, onde se utiliza algoritmo de encriptação com chave pública e decriptação com chave privada conhecida apenas pelo destinatário.

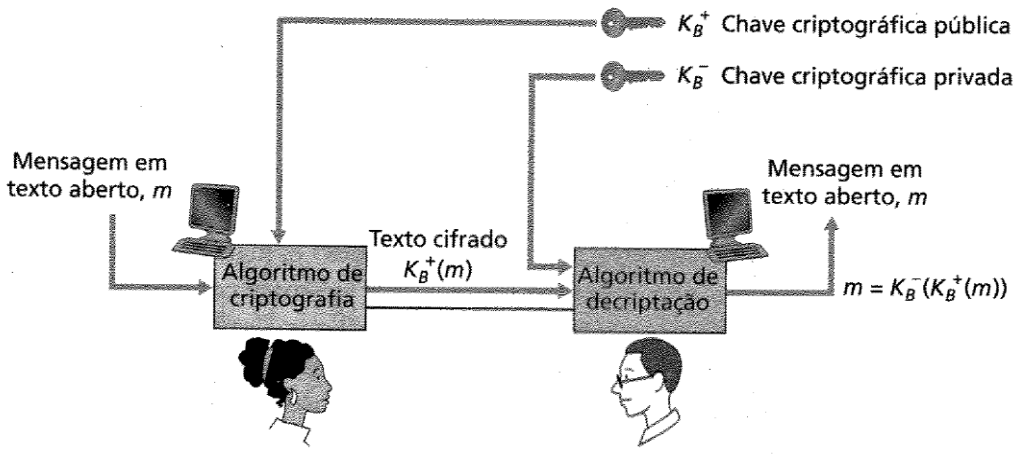

Figura 2: Criptografia Assimétrica
Fonte: Redes de computadores e a Internet, Kurose

2.2.1.3 Assinatura Digital

Segundo Tanebaum (2003) autenticidade de muitos documentos legais, financeiros e outros documentos é determinada pela presença de uma assinatura autorizada.

A assinatura digital utiliza-se de uma assinatura eletrônica para garantir a autenticidade e integridade da informação, a assinatura eletrônica consiste em um

resumo da informação gerada a partir de cálculos matemáticas, denominado função *hash*.

Após a geração do *hash*, é realizada a criptografia da informação, juntamente com o *hash* utilizando-se da chave privada.

Para garantir o não repudio das informações é acrescentado ao pacote um Certificado Digital referente à origem, tal certificado é vendido por unidades certificadoras.

A assinatura digital juntamente com o Certificado, são bastante utilizados por empresas que disponibilizam produtos e serviços na internet para evitar principalmente o Phishing.

2.2.2 Firewalls

Segundo Kurose (2006) um Firewall é uma combinação de hardware e software que isola a rede interna de uma organização da internet em geral, permitindo que alguns pacotes passem e bloqueando outros.

Os Firewalls podem ser divididos basicamente em duas categorias de acordo com sua finalidade, filtragem de pacotes ou filtragem de aplicação.

A figura a seguir demonstra a disposição de um firewall em gerenciar a comunicação, bloqueando e/ou liberando o acesso entre as redes local Alaska_LAN, DMZ Alaska_DMZ.LAN e a rede internet.

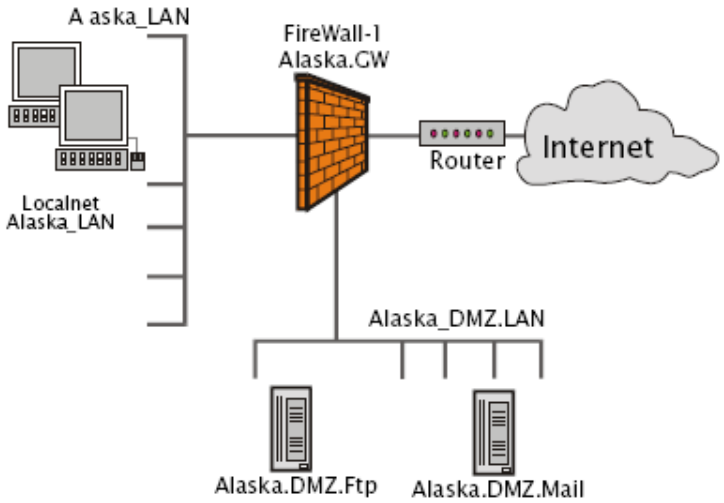

Figura 3: Firewall
Fonte: Firewall-1 and SmartDefense, CheckPoint

a) Filtro de Pacotes

O filtro de pacotes consiste em analisar os pacotes trafegados entre as redes interna e externa até a camada de transporte, levando-se em consideração endereços MAC, IPs de origem e destino, Protocolos, entre outras informações.

Todos os pacotes que após a análise não estiverem de acordo com as regras estipuladas pelo administrador serão descartados.

b) Filtro de Aplicação

O filtro de aplicação, também conhecido como Proxy / Gateway, consiste em analisar os pacotes até a camada de aplicação, estipulando se um determinado serviço / aplicação está disponível para trafegar entre as redes.

Os Firewalls podem ser de Software, Hardware ou ambos, dependendo do fabricante e da implementação necessária à empresa.

2.2.3 IPSec

Segundo Microsoft (2006), a segurança IPSec baseia-se em um modelo de segurança ponto a ponto, estabelecendo relações de confiança e a segurança entre um endereço de origem e um de destino.

O IPSec cria um túnel de comunicação entre as partes, de forma transparente para o usuário, utilizando-se de criptografia para garantir a segurança das informações trafegadas, cujos os principais algoritmos são:

- Diffie-Hellman;
- DES;
- SHA1;
- MD5;
- Entre outros.

A segurança do IPSec se aplica principalmente na camada de Rede, onde são realizados a proteção básica das camadas de transporte e aplicação (Modo Transporte) e o tunelamento dos pacotes IPs (Modo Túnel).

Em se tratando de redes TCP/IP, o IPV6 obrigatoriamente deve trabalhar com o IPSec, já no IPV4 é compatível, mas vai de acordo com a necessidade de cada empresa.

2.2.4 SSL – Secure Sockets Layer

Com o avanço da internet e a disponibilização de transações financeiras em comércio eletrônico, a *Netscape Communications Corp* desenvolveu um protocolo de segurança denominado SSL.

O protocolo SSL consiste em estabelecer uma conexão segura entre a origem e o destino, com autenticação, criptografia e integridade dos dados transferidos.

Segundo Tanebaum (2003) efetivamente, trata-se de uma nova camada colocada entre a camada de aplicação e a camada de transporte, aceitando solicitações do navegador e enviando-as ao TCP para transmissão ao servidor.

O SSL utiliza-se de alguns algoritmos de criptografia, cada um para sua especialidade como comércio eletrônico, transações financeiras etc.

2.2.5 VPN

> As Redes Privadas Virtuais tornaram-se um marco na comunicação dentro de uma empresa e entre empresas. Utilizando técnicas de tunelamento e segurança, elas permitem a utilização da Internet, uma rede pública e compartilhada, para a conexão de filiais, usuários remotos e parceiros/clientes à rede interna de uma companhia. (RAPOPORT, 2003)

A utilização de VPN nas empresas possibilita diversas vantagens, entre elas a redução de custo, pois para interconectar a matriz com as filiais e funcionários remotos não é necessário pagar por links dedicados, utilizando-se da própria rede pública, a internet. Outra vantagem é a segurança, já que se utiliza protocolos para criptografar os dados e garantir a integridade, confidencialidade e autenticidade das informações.

A VPN utiliza determinados protocolos para estabelecer a segurança devida em cada camada do modelo OSI. Na camada de enlace são aplicados os PPTP, L2F e L2TP, na camada de rede aplica-se o IPSEC e na de aplicação o SSL, todos estes protocolos são responsáveis pelo tunelamento e criptografia dos pacotes em suas respectivas camadas.

2.2.6 IPS (Intrusion Prevention System)

Para proteger a rede de ataques, as grandes empresas utilizam ferramentas como o IDS (Intrusion Detection System) para detectar uma possível ameaça.

> O IDS, Sistema de Detecção de Intrusão, detecta e notifica as tentativas de intrusão, analisando e capturando os pacotes que estão trafegando na rede procurando identificar as evidencias de um ataque em andamento, podendo emitir alarmes, ou executando uma ação automática, como por exemplo, a desativação do *link*, a depender da ferramenta. (JUNIOR, 2006).

As principais ferramentas IDS disponíveis no mercado podem ser de Hardware ou de Software, dependendo do fabricante. Ambos podem ser implementados juntamente com Firewalls e Proxies.

O grande problema do IDS é que ao detectar um possível comportamento malicioso, o IDS só informa ao administrador da rede. Fora isso também há os falsos positivos, isto é, pacotes nocivos que podem ser detectados como intrusão e vice-versa. Pensando nisso o IDS evoluiu para IPS, onde além de detectar uma atividade anormal e informar ao administrador, o IPS descarta os pacotes e bloqueia as conexões suspeitas, tornando-se assim uma ferramenta proativa.

Segundo Nobrega (2009), os sistemas de prevenção de intrusões na rede (IPS, Intrusion-Prevention Systems) são equipamentos de segurança online que desempenham inspeção de pacotes para identificar e bloquear tráfego malicioso.

CAPÍTULO III

3. SEGURANÇA EM REDES SEM FIO

Em se tratando de redes de computadores não se pode deixar de falar nas redes sem fio, cujas principais ameaças são as mesmas das redes de computadores convencionais.

Levando-se em consideração os avanços tecnológicos e a popularidade das redes sem fio, tanto no meio coorporativo como residencial, há a necessidade crescente em garantir a segurança das informações.

Pensando nisso, foram criados protocolos específicos para redes sem fio, utilizando-se principalmente de criptografia de pacotes, tais pacotes são: WEP, WPA, WPA-PSK, WPA2, WPA2-PSK e WPA-Radius.

3.1 WEP (Wired Equivalent Privacy)

Segundo Rufino (2007), WEP é um protocolo que utiliza algoritmos simétricos, portanto existe uma chave secreta que deve ser compartilhada entre as estações de trabalho e o concentrador, para cifrar e decifrar as mensagens trafegadas.

Por utilizar uma criptografia simétrica, este protocolo é o mais fraco em questão de segurança, já que está sujeito a quebra da chave por ataque de dicionário e força bruta, pensando nisso aconselha-se a troca das chaves de criptografia WEP com frequência para evitar descoberta por parte dos invasores.

3.2 WPA (Wi-Fi Protect Access)

O WPA foi criado basicamente para substituir o WEP, corrigindo as falhas de segurança encontradas, as principais diferenças são a utilização de autenticação de usuários e a forma como é liberada a chave de criptografia.

> Dentre as novidades do WPA há o protocolo TKIP (Temporal Key Integrity Protocol), responsável pela gerência de chaves temporárias usadas pelos equipamentos em comunicação, possibilitando a preservação do segredo mediante a troca constante da chave. (RUFINO, 2007)

Isto significa que a troca de chaves é realizada de forma dinâmica, sendo executada de tempos em tempos.

Outra forma de autenticação utilizada no WPA é a EAP (Extensible Authentication Protocol).

Segundo Rufino (2007), o EAP utiliza o padrão 802.11x e permite vários métodos de autenticação, incluindo a possibilidade de certificação digital.

3.3 WPA-PSK

É uma variante do WPA, que utiliza o protocolo TKIP para criptografia, bastante utilizada em redes domésticas pela sua facilidade de configuração e compatibilidade com placas de redes mais antigas.

3.4 WPA2

O WPA2 consiste numa evolução do WPA, lançado em 2004, robusto, uma das maiores diferenças são a utilização do protocolo CCMP em vez do TKIP, mas utilizando o mesmo conceito de chaves temporárias.

3.5 WPA2-PSK

O WPA2-PSK é uma variante do WPA2, onde utiliza criptografia AES, uma criptografia mais forte e confiável.

Utilizado principalmente em redes domésticas e pequenos escritórios.

3.6 RADIUS

Além de utilizar criptografia para garantir a transferência de informações em redes sem fio no meio coorporativo, o ideal é a autenticação de usuários e hosts, o método mais utilizado atualmente é o uso de servidores Radius, preferencialmente integrados a um servidor LDAP.

O protocolo de segurança utilizado em conjunto com o servidor Radius é o WPA.

CONSIDERAÇÕES FINAIS

Durante a elaboração do artigo pôde-se analisar as principais ameaças às redes de computadores, tanto cabeadas quanto redes sem fio, e o que é aconselhável como solução para evitar os possíveis ataques.

Analisando todas as informações contidas no artigo pôde-se concluir que as redes de computadores, tanto domésticas como empresarial, necessitam cada vez mais de segurança, utilizando algoritmos e protocolos de criptografia, firewalls, VPN, IPS, entre outras técnicas. Tudo isso visando garantir a integridade, autenticidade e confidencialidade das informações, bem como a disponibilidade dos serviços.

REFERÊNCIAS

TANENBAUM, Andrew S. **Redes de Computadores**. 4ª Ed. Rio de Janeiro: Elsevier, 2003.

KUROSE, James F. **Redes de Computadores e a Internet**. 3ª Ed. São Paulo: Pearson, 2006.

RUFINO, Nelson Murilo de O. **Segurança em Redes sem Fio**. 2ª d. São Paulo: Novatec, 2007.

Microsoft. **O que é o Spyware?** 2006. Disponível em: <http://www.microsoft.com/portugal/athome/security/spyware/spywarewhat.mspx>. Acessado em: 29 de Dezembro de 2010;

Microsoft. **Rootkit: O Obscuro Ataque do Hacker** 2005. Disponível em: < http://technet.microsoft.com/pt-br/library/dd459016.aspx>. Acessado em: 06 de Janeiro de 2010;

VIEIRA, Luiz. **ARP Poisoning: compreenda os princípios e defenda-se** 2005. Disponível em: < http://www.vivaolinux.com.br/artigo/ARP-Poisoning-compreenda-os-principios-e-defendase?pagina=1>. Acessado em: 06 de Janeiro de 2010;

Symantec. Phishing: **Como eles atacam** 2005. Disponível em: <http://www.symantec.com/pt/br/norton/security_response/phishing.jsp>. Acessado em: 07 de Janeiro de 2010;

Microsoft. **Apresentando o IPSec** 2006. Disponível em: < http://technet.microsoft.com/pt-br/library/cc757786%28WS.10%29.aspx>. Acessado em: 09 de Janeiro de 2010;

NÓBREGA, João. **Intrusion Prevention Systems** 2009. Disponível em: < http://www.computerworld.com.pt/2009/05/13/intrusion-prevention-systems/>. Acessado em: 15 de Janeiro de 2010;

JUNIOR, Francisco Vieira. **Estudo de caso em segurança de redes usando como ferramenta de IDS (Intrusion Detection System) o SNORT.** 2006. Disponível em: < http://www.fieb.org.br/iel/bitec/Arquivos/2006/FRANCISCO_VIEIRA_JUNIOR.pdf> Acessado em: 15 de Janeiro de 2010;

TORRES, Gabriel. **Criptografia.** 2002. Disponível em: < http://www.clubedohardware.com.br/artigos/667>. Acessado em: 17 de Janeiro de 2010;

CHECKPOINT. **Firewall-1 and SmartDefense**, 2003. Disponível em: <http://hills.ccsf.edu/~lbaca/FireWall-1_and_SmartDefense.pdf>. Acessado em: 18 de janeiro de 2010.

RAPOPORT, Eduardo. **VPN – Virtual Private Network.** 2003. Disponível em: < ht http://www.gta.ufrj.br/~rezende/cursos/eel879/trabalhos/vpn/>. Acessado em: 18 de Janeiro de 2010;

LINHARES, André Guedes. **Uma Análise dos Mecanismos de Segurança de Redes IEEE 802.11: WEP, WPA, WPA2 e IEEE 802.11w.** Disponível em: < ht http://www.unibratec.com.br/jornadacientifica/diretorio/UFPEAGL.pdf >Acessado em: 18 de Janeiro de 2010;

CREDENCIAIS DO AUTOR

Dados do autor: Especialista em Redes de Computadores, Gestor RM – SEBRAE/SE, forma de contato com o autor por e-mail (jenfigueiredo@yahoo.com.br) ou telefone celular ((79) 9801-0304).