UNIVERSIDADE DO SAGRADO CORAÇÃO

CESAR GERALDI LOPES FILHO

# MÉTODOS DE IDENTIFICAÇÃO E ANÁLISE DE VUNERABILIDADE EM REDES SEM FIO

BAURU

2013

**CESAR GERALDI LOPES FILHO**

# MÉTODOS DE IDENTIFICAÇÃO E ANÁLISE DE VULNERABILIDADE EM REDES SEM FIO

Trabalho de conclusão de curso apresentado ao Centro de Ciências Exatas e Sociais Aplicadas como parte dos requisitos para obtenção do titulo de bacharel em Ciência da Computação, sob a orientação do Profº. Esp.Henrique Pachione Martins

**BAURU**

**2013**

Lopes Filho, Cesar Geraldi
L8641m

Métodos de identificação e análise de vulnerabilidade em redes sem fio / Cesar Geraldi Lopes Filho -- 2013.
64f. : il.

Orientador: Prof. Esp. Henrique Pachioni Martins.

Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) – Universidade do Sagrado Coração – Bauru – SP.

1. Vulnerabilidade. 2. Port scanner. 3. Segurança. 4. Invasão. 5. Redes sem fio. I. Martins, Henrique Pachioni. II. Título.

**CESAR GERALDI LOPES FILHO**

# Métodos de identificação e análise de vulnerabilidade em redes sem fio

Trabalho de Conclusão de Curso apresentado ao Centro de Ciências Exatas e Sociais Aplicadas como parte dos requisitos para obtenção do título de bacharel em Ciência da Computação, sob orientação do Prof. Esp. Henrique Pachione Martins.

Banca examinadora:

_____
Prof. Esp. Henrique Pachione Martins

_____
Prof. Esp. André Luiz Ferraz Castro

_____
Prof. Dr. Elvio Gilberto da Silva

Bauru, novembro de 2013.

## AGRADECIMENTOS

Agradeço primeiramente a Deus por sempre guiar meu caminho e abençoar minha vida.

Aos meus pais Cesar e Elaine por darem o dom da vida, a oportunidade de estudar e hoje ter uma formação profissional assim com o todos os cuidados necessários para ter uma vida saudável e sem faltar nenhuma necessidade.

A minha família que sempre me ajudou e apoiou, e teve presente acreditando que tudo seria realizado com sucesso.

Em especial um muito obrigado a noiva Ana Carolina que esteve ao meu lado todos os momentos principalmente nos de dificuldades, quando estive desanimado, nos dias em que parecia que não iria conseguir realizar todas minhas tarefas de certa forma me ajudou sempre me colocando e fazendo que eu pensasse de forma positiva a tais dificuldades e assim concluir os mesmos.

A todos meus amigos que sempre acreditaram em minhas escolhas e de alguma forma participaram para que tudo desse certo.

A todos meus professores pelo ensinamento realizado que também contribuíram para que chegasse a minha formação de ensino superior.

Ao meu orientador que acreditou em meu potencial ao escolher realizar este trabalho e que a cada passo concretizado deste, sempre esteve disposto e disponível a me ajudar e orientar no que fosse necessário.

**RESUMO**

Este trabalho apresenta algumas ferramentas para a detecção de vulnerabilidades em redes de computadores sem fio. Os *Port Scanners* permitem verificar em uma rede, informações sobre os computadores e outros dispositivos nela conectados, como portas TCP abertas e serviços ativos. Profissionais de segurança em redes costumam empregar estas ferramentas como um mecanismo auxiliar na avaliação da segurança interna da rede. A lista de portas abertas fornecidas pode ser utilizada por um invasor que, com o auxílio de um *Exploit*, pode conseguir acesso total ou parcial à máquina com a falha de segurança.

**Palavra Chave:** Vulnerabilidade, port scanner, segurança, invasão, redes sem fio.

**ABSTRACT**

This paper presents some tools to detect vulnerabilities in computer networks wirelessly. The Port Scanner allows you to check on a network information about computers and other devices connected to it, such as open TCP ports and active services. Professional security networks usually employ these tools as an aid in the assessment of internal network security mechanism. The list of open ports provided can be used by an attacker who, with the aid of an Exploit, can achieve full or partial access to the machine with the security flaw.

Key Word: Vulnerability, port scanner, security, invasion, wireless network

**LISTA DE FIGURAS**

## LISTA DE SIGLAS

ABNT: Associação Brasileira de Normas Técnicas.

AES: Advanced Encryption Standard.

DHCP: Dynamic Host Configuration Protocol

DoS: Denial of Service.

DNS: Domain Name System.

IEEE: Institute of Electrical and Electronics Engineers.

HTML: HyperText Markup Language.

IDS: Intrusion Detection System.

IPS: Intrusion Prevention System.

IP: Internet Protocol.

ISO/OSI: International Organization for Standardization/ Open System Interconnection.

LAN: Local Area Network.

MAC: Media Access Control.

MAN: Metropolitan Area Network.

PHP: PHP Hypertext Preprocessor.

SSID: Service Set identifier.

TCP: Transmission Control Protocol.

TCP/IP: Transmission Control Protocol/Internet Protocol.

TKIP: Temporal Key Integrity Protocol.

UDP: User Datagram Protocol.

WAN: Wide Area Network.

WEP: Wired Equivalent Privacy.

Wi-fi: Wireless fidelity.

WPA: Wi-Fi Protected Access.

**SUMÁRIO**

# 1 INTRODUÇÃO

As redes de computadores tiveram um grande crescimento nos últimos anos. Existem estudos que indicam a existência de pelo menos um computador pessoal para cada cidadão em todo o mundo.

Com o passar do tempo surgiram grandes novidades como, por exemplo, novos meios de transmissão, ferramentas administrativas e tecnologia de equipamentos. Mesmo em ambientes residenciais é comum o armazenamento e compartilhamento de dados e, conseqüentemente, o uso de redes de computadores se torna mais comum. Rede de computadores consiste na utilização de dois ou mais computadores conectados entre si podendo assim fazer o compartilhamento de impressora, dados, serviços e mensagens (TANENBAUM, 2003).

As redes de computadores são visadas de ataques que podem comprometer a segurança da informação e prejudicar o ambiente empresarial. Os ataques podem ser divididos de três formas: externo, interno e físico. Os ataques externos são os que possuem fatores externos interferindo na rede, por meio da internet utilizando técnicas maliciosas como vírus ataques internos ocorrem quando funcionários de uma empresa acessam dados para os quais não possuem permissões e os ataques físicos são as invasões de acesso físico à rede no contato ao ponto de acesso de uma rede sem fio ou em uma rede cabeada no rearranjo do cabeamento.

Uma das ameaças mais reportadas, a automação e a programação de códigos maliciosos na rede, são os chamados *worms*. Há também os ataques específicos da *web*, com a desfiguração de paginas na internet e comprometimento de serviços. Os ataques de negação de serviço (*DoS*), que é um conjunto de computadores para derrubar um computador ou um serviço na rede. A invasão em um computador bem sucedida na rede também é considerada ameaça.

Com o crescimento da *internet* aliado ao crescimento de tarefas executadas *online*, há abertura para incidentes que podem comprometer a segurança.

Em redes sem fio, as ameaças são ainda maiores, pois além da preocupação da segurança lógica da informação, tem também a preocupação de como as informações são transmitidas na rede. O tráfego de dados nesse tipo de rede é feito por meio de ondas de rádio freqüência que se propagam pelo ar, com isso não é possível fazer o direcionamento desse tráfego, já que o sinal se propaga para todos os lados podendo ser receptado por qualquer usuário que esteja conectado no mesmo ambiente físico da rede, mesmo não tendo a permissão para isso.

Outra característica em redes sem fio, é que não há a possibilidade de determinar a área de alcance do sinal, sendo que este pode ultrapassar paredes e os dados serem transmitidos erroneamente ou serem capturados por outros usuários, não sendo possível o controle de quem pode ou não ter acesso à esta informação. Uma solução possível para isso seria a criptografia, que nada mais é que proteger os dados de forma que apenas que somente o pessoal autorizado a acessar possa receber. Em segurança de redes sem fio, a criptografia é considerada muito importante, pois embaralha os dados enviados para quem o acesso não é autorizado e mantém o sentido para o receptor permissionado.

Fazendo tais considerações pode-se notar a importância de estudar os métodos de invasão com objetivo de proteger a rede.

## 1.1 OBJETIVOS GERAL

Apresentar as técnicas de identificação de possíveis vulnerabilidades em redes sem fio, e propor possíveis correções para criar uma transmissão mais segura.

## 1.2 OBJETIVOS ESPECIFICOS

- Mostrar tipos de identificação de vulnerabilidade;
- Apresentar a utilização de ferramentas *portscaners* para obtenção de informações e análise da rede;
- Verificar possíveis vulnerabilidades em pontos de acesso em redes sem fio;
- Mostrar formas de verificação dos serviços disponíveis na rede para o usuário e estabelecer quais dos serviços são necessários e quais não deveriam ser disponibilizados;

## 1.3 JUSTIFICATIVA

As tecnologias de redes sem fio estão sendo cada vez mais utilizada no cotidiano das pessoas, por proporcionar mobilidade, praticidade, conexões mais rápidas e estáveis e preços mais acessíveis. As organizações estão sujeitas a riscos, ataques executados em data e hora não estipulados, sendo diversos os métodos e técnicas utilizados. Alguns cuidados devem ser tomados para que as atividades e negócios das organizações não sejam interrompidos.

Assim, o estudo de caso desse trabalho justifica-se por auxiliar no entendimento e utilização do software de detecção de vulnerabilidades em redes sem fio, utilizando softwares livres, sem custo de implantação, suportado por praticamente todos os sistemas operacionais. Ao mesmo tempo apresenta-se confiável e de fácil aprendizagem, incentivando sua utilização por profissionais da Tecnologia da Informação (TI), bem como oferecendo um material didático para auxiliar profissionais e acadêmicos da área de redes de computadores.

# 2 REFERENCIAL TEÓRICO

## 2.1 REDES DE COMPUTADORES

As redes de computadores estão sempre passando por processos evolutivos chegando aos padrões utilizados atualmente (MORIMOTO, 2008). A rede criada em 1960 para o uso exclusivo dos militares, hoje tomou um rumo bem diversificado: como forma de diversão em *lanhouses* e jogos *on-line*, até como forma de administrar uma empresa fazendo o monitoramento da produção e emitindo notas.

Segundo Tanenbaum (2003), as redes de computadores podem ser utilizadas de duas maneiras: de forma comercial e de forma residencial. A forma comercial é muito utilizada para informações computadorizadas como estoque, registro de clientes e contas a receber, além da possibilidade de compartilhamento para vários locais distantes graças às redes de computadores. Para se ter uma rede é necessário um computador robusto para ser o servidor, no qual serão armazenados os bancos de dados com as informações devidamente registradas.

Geograficamente as redes de computadores podem ser divididas em três categorias (ROCHA, 2007), *LAN* (*Local Area Network*), que é responsável por fazer a interligação de computadores de um prédio, casa, ou campus com a finalidade de compartilhar software e hardware; *MAN* (*Metropolitan Area Network*) que é utilizada para interligar computadores de várias áreas de uma cidade ou até mesmo de cidades vizinhas, onde não é possível ser implementada com a tecnologia *LAN*, *WAN* (*Wide Area Network*) que é uma rede de longo alcance que interliga redes maiores que as *LAN's* possibilitando o transporte de dados em um segmento de rede muito maior (MORIMOTO, 2008).

Quanto ao meio de transmissão, as redes são classificadas em dois tipos: cabeadas e sem fio.

### 2.1.1 REDES CABEADAS

As redes interligadas por cabos são as mais utilizadas, seja através de cabo par trançado, coaxial ou fibra ótica (MORIMOTO, 2008).

O par trançado por conseguir alcançar uma velocidade de até 100 *Mbps*, substituiu boa parte dos coaxiais a partir da década de 1990. Além de serem flexíveis e de fácil instalação, os cabos par trançado são de baixo custo, tanto na instalação quanto na manutenção. Esses cabos são classificados em categorias,que indicam a qualidade do cabo e a freqüência máxima que pode ser suportada (ROCHA, 2007).

Existem os coaxiais que foram bastante utilizados nas redes de computadores devido à sua blindagem, gerando um isolamento e assim não perdendo sua potência. Sua pouca

flexibilidade nas instalações, sua velocidade de transmissão de dados, que pode somente chegar a até 10 *Mbps* e por ser propenso a mau contato é cada dia menos utilizado (TITTEL, 2003).

A fibra ótica é uma alternativa ao uso dos cabos de par trançado. A fibra ótica envia os sinais por feixes de luz, e por esse motivo a quantidade e velocidade de dados trafegados são mais altas comparando-se com as de par trançado. Outra vantagem em se usar a fibra ótica é o seu alcance que pode chegar a até 80 km sem nenhum tipo de repetidor. A grande desvantagem desse tipo de cabo é o seu preço muito elevado devido a sua dificuldade de fabricação (MORIMOTO, 2008).

Independente do tipo, todos os cabos servem para o mesmo fim, conectar vários equipamentos e assim formar uma rede de comunicação e transmissão de dados. Em geral, cada uma das máquinas da rede, chamadas de estações, são conectadas em um *hub* ou *switch,* responsável por encaminhar os dados entre os computadores da rede.

As redes de computadores podem gerar duas arquiteturas: ponto-a-ponto e cliente/servidor (TITTEL, 2003).

Na arquitetura ponto-a-ponto, mostrada na figura 1, cada estação pode ser um servidor ou cliente que pode facilmente compartilhar *hardware* e criar, ler e escrever arquivos em outros computadores. Esse tipo de implementação pode ser utilizada independente do sistema operacional, desde que este forneça suporte para ponto-a-ponto.

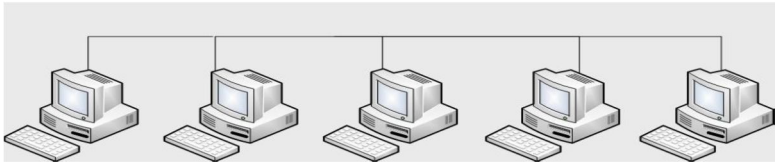


Figura 1 – Arquitetura de uma rede Ponto-a-Ponto.

Fonte: próprio autor

Arquitetura Cliente / Servidor - Nessa arquitetura o servidor fornece serviços específicos aos computadores clientes, como pode ser observado na figura 2. Indicada para redes com cinco ou mais computadores, ou quando se deseja obter mais segurança de uma rede (TITTEL, 2003).

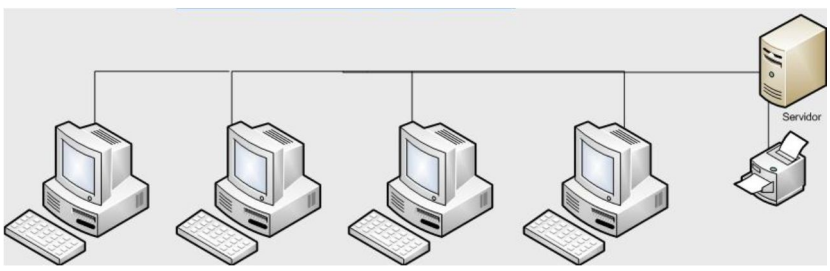



Figura 2 – Arquitetura de uma rede Cliente Servidor.

Fonte: próprio autor.

Para efetuar a transmissão de dados entre as interfaces de rede é necessário que ambas falem a mesma língua, ou seja, implementem o mesmo protocolo de transmissão de dados. O protocolo mais utilizado em redes é o *TCP/IP* (RUSSEL, 2002).

### 2.1.2 REDES SEM FIO

Utilizar cabeamento em uma rede é, geralmente, a maneira mais rápida de transferir dados. O cabo mais utilizado, o par trançado, pode alcançar a velocidade de até 1 *Gbps*. Entretanto, a utilização de uma rede cabeada tem suas desvantagens, o custo do cabeamento cresce conforme o número de computadores e distância da cobertura da rede (MORIMOTO, 2008).

Implementar uma rede doméstica, de cerca de cinco computadores, é tanto simples como barato, basta comprar um *switch* e o comprimento de cabo necessário. Porém montar uma rede empresarial com 200 computadores torna-se muito mais caro, pois além de todo o cabeamento das estações é preciso efetuar o cabeamento estruturado por vários andares do prédio. Outro problema é a pouca flexibilidade dessa tecnologia. Caso sejam necessárias mudanças de locais de alguns computadores seria preciso refazer o cabeamento desses computadores (RUSSEL, 2002).

Em algumas situações não é viável a implementação de cabeamento, como em prédios antigos onde não existem passagens exclusivas para cabos, conectar escritórios de dois edifícios diferentes ou em construções consideradas patrimônio público onde não é permitido furar paredes. O uso de redes sem fio é uma alternativa para solucionar esses problemas. Trata-se de rede bastante flexível, permitindo que se alterem os computadores de local sem nenhuma mudança. Devido ao seu baixo custo, torna-se acessível à maioria da população (MORIMOTO, 2008).

Muitos estabelecimentos utilizam redes sem fio como uma forma de marketing. Estabelecimentos como aeroportos, *shopping centers* e bares disponibilizam *Internet* para seus clientes através dessa tecnologia, o que é um grande atrativo para o público. Apesar das vantagens, fazer a configuração de uma rede sem fio envolve muitos detalhes como potência da antena do roteador, tipo de criptografia utilizada, além de configurações no ponto de acesso a fim de otimizar a conexão (TITTEL, 2003).

Em redes sem fio, também chamadas de redes *wireless*, a transmissão de dados é feita por ondas de radiofreqüência que se propagam pelo ar. Logo, as camadas 1 e 2 do modelo *ISO/OSI*, camada física e de enlace respectivamente, são diferentes das redes cabeadas (TANENBAUM, 2003).

Outra diferença das redes sem fio em relação às cabeadas são os padrões de seus dispositivos elaborados pelo instituto de Engenheiros Eletricistas e Eletrônicos IEEE (IEEE, 2009). O IEEE é uma organização responsável por, entre outras atribuições, estabelecer normas para diferentes tipos de dispositivos. A norma referente às redes de computadores é o IEEE 802, que engloba LAN`s e MAN`s, e as principais utilizadas em redes sem fio são as 802.11, 802.15, 802.16.

- 802.11 – Padrão que trata de conexões de redes locais sem fio (WLANs). Muito difundido nos últimos anos, esse padrão é responsável pela conectividade da maioria dos computadores portáteis, o que explica o fato da maioria deles saírem de fábrica com dispositivos receptores para esse tipo de freqüência.
- 802.15 – Padrão que trata da tecnologia *Bluetooth*, destinada a conexão sem fio de dispositivos utilizando baixa potência e curto alcance. São muito usadas em acessórios de dispositivos móveis como celulares e para transferências de dados em equipamentos próximos.
- 802.16 – Também conhecido como padrão WiMAX, trata de redes sem fio metropolitanas (WMANs). Ainda em desenvolvimento, esse padrão é similar ao 802.11, porém é destinado a longas distâncias, com objetivo de oferecer conectividade.

O mais utilizado em redes locais sem fio é o IEEE 802.11. Com o passar do tempo, ele vem cada vez mais aumentando seu alcance e velocidade (LOUREIRO, 2004). Atualmente os padrões existentes são mostrados no quadro 1 :

| PADRÃO | VELOCIDADE | FREQUENCIA |
|---|---|---|
| 802.11b | 11 Mbps | 2.4 Ghz |
| 802.11a | 54 Mbps | 5Ghz |
| 802.11g | 54 Mbps | 2.4 Ghz |
| 802.11n | 300 Mbps | 2.4/ ou 5Ghz |

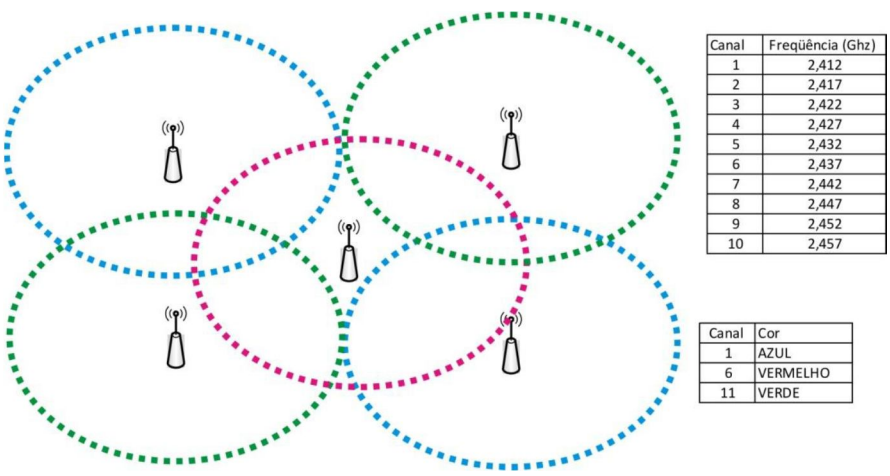
Figura 3 - Tecnologias de redes sem fio.
Fonte: próprio autor

Em uma rede sem fio, os dados são transmitidos através de sinais de radiofreqüência por um ou mais pontos de acesso, também chamado de *Access point*, para os computadores que estiverem conectados na mesma rede. Os pontos de acesso podem tanto emitir os dados para estações sem fio como para estações com fio(IEEE, 2009).

Algumas vezes é preferível por em questão o custo de uma implementação de redes sem fio. Imagine uma empresa que tenha um setor de informática com 300 computadores: pelos padrões da ABNT NBR 14565 (ABNT, 2002), o servidor da rede deve ficar em um ambiente diferente das estações, e os cabos de rede não devem ultrapassar o comprimento

de 100 metros entre o servidor e o computador, o que significa que apenas nesse setor seriam necessários até 30 km de cabos para manter a rede. Com a tecnologia de redes sem fio, essa grande quantidade de fios não existiria. Cada computador teria sua placa de rede receptora que receberia o sinal de um ponto de acesso, o equipamento responsável por transmitir os dados da rede para os computadores.

No entanto essa implementação deve ser efetuada mediante a algumas considerações, pois existem limitações físicas e lógicas (SOUSA, 2002). A largura da banda da rede deve ser suficiente para suprir toda a demanda e evitar possíveis problemas de lentidão. Um ponto de acesso não suportaria requisições de 500 computadores, e uma boa prática para se evitar “gargalos” é a utilização de, em média, um para cada vinte computadores, podendo variar de acordo com a tecnologia do equipamento. Além disso, o canal de operação deve ser bem distribuído a fim de se evitar interferências de outro canal, como mostra a figura 3.



| Canal | Freqüência (Ghz) |
|---|---|
| 1 | 2,412 |
| 2 | 2,417 |
| 3 | 2,422 |
| 4 | 2,427 |
| 5 | 2,432 |
| 6 | 2,437 |
| 7 | 2,442 |
| 8 | 2,447 |
| 9 | 2,452 |
| 10 | 2,457 |

| Canal | Cor |
|---|---|
| 1 | AZUL |
| 6 | VERMELHO |
| 11 | VERDE |

Figura 4 – Distribuição de pontos de acesso.

Fonte: próprio autor

Como não é possível definir a área de alcance da rede e bloquear acesso de usuários fora do ambiente, uma técnica foi desenvolvida para confundir as informações enquanto são trafegadas, de modo que um usuário não autorizado não entenda as informações, essa técnica é chamada de criptografia. A primeira forma de criptografia para redes sem fio foi a *WEP*, *Wireless Equivalent Privacy*. Criada em 1999, esse método de criptografia é considerado inseguro e recomenda-se que seja utilizado apenas em equipamentos antigos que não suportam outras criptografias. Apresenta algumas vulnerabilidades como o tamanho da chave que é composta de apenas 40 bits, podendo ser facilmente quebrada por força bruta utilizando ferramentas como *Aircrack* (LINHARES, GONÇALVES, 2007).

Para solucionar as vulnerabilidades encontradas no WEP foi criado, em 2003, o padrão WPA, *Wi-Fi Protected Access*, que trouxe vários mecanismos com o intuito de solucionar as falhas de segurança do protocolo anterior. Esse objetivo foi alcançado, porém

o WPA também apresentou algumas vulnerabilidades com o passar do tempo, como uma fraqueza em seu algoritmo de combinação de chaves, e isso resultou, em 2004, a criação do *WPA*2, que em relação ao anterior evoluiu basicamente os algoritmos de criptografia e integridade (SOUSA 2002).

## 2.2 SERVIÇOS DE REDES

De acordo com a necessidade do usuário se deu a existência de serviços de redes para a melhoria do desempenho de uma rede. O serviço de rede nada mais é que uma aplicação executada em vários computadores que estão conectados no mesmo ambiente (MORIMOTO, 2008). Para ter um serviço é necessário um aplicativo para executar, podendo utilizar vários serviços quando executado.

Os serviços, utilizados em uma arquitetura *TCP/IP*, que utiliza uma porta *TCP/UDP* para comunicação, com isso o serviço pode receber ou enviar informações, existindo 65535 (sessenta e cinco mil quinhentos e trinta e cinco) portas disponíveis. O *TCP* para garantir a entrega reduz o seu desempenho, diferente do protocolo *UDP*, que é considerado um protocolo de transmissão mais rápido, mas não é tão seguro por não garantir a entrega de certos pacotes. E a grande vantagem do protocolo *TCP* sobre o *UDP*, com a entrega garantida através de um mecanismo que estabelece uma conexão de envio junto com uma mensagem de confirmação ao enviar o pacote, e caso algum dado nessa transação seja perdida ou danificada ele envia novamente. Temos também outros protocolos como os *VoIP*, o *DNS*, que são baseados em *UDP* pois a tolerância de algumas perdas ou restrições de desempenho (TITTEL, 2003).

No protocolo *TCP* existem os *overheads*, que dentro dele esta o *three-way hand-shake*nas conexões, quando se deseja estabelecer uma conexão de algum serviço em qualquer porta *TCP*, é enviado imediatamente um pacote "*SYN*", caso a porta acionada esteja fechada o servidor responde com um pacote "*ACK*" assim sendo encerrada a transmissão, se a porta estiver disponível o servidor responde com um pacote "*SYN+ACK*" assim que recebe a resposta o cliente envia um pacote "*ACK*" e a conexão estabelecida (MORIMOTO, 2008). No Quadro 2, alguns serviços de redes com suas portas e protocolos.

| Protocolo | Porta | Serviço |
|---|---|---|
| TCP | 20 | Stream Control Transmission Protocol |

| | | |
|---|---|---|
| TCP | 21 | File Transfer Protool |
| TCP | 22 | SSH (Secure Shell) |
| TCP | 23 | Telnet |
| TCP | 25 | SMTP |
| UDP | 53 | Domain Name System |
| TCP | 80 | HTTP |
| TCP | 110 | POP3 |

Figura 5 - Principais serviços de rede

Fonte: próprio autor

Para que a estações de trabalho tenham as suas funcionalidades básicas, a rede oferece vários serviços, alguns deles precisam estar ativos como *Web, E-Mail*, *DNS* e *DHCP* independentemente do sistema que está sendo utilizado.

### 2.2.1 SERVIÇO WEB

Servidores *Web* fazem uma parte importante da *internet*, pois eles que criam ambientes para executar as aplicações *Web* e fazem a hospedagem de páginas, agora com o conceito de nuvens está virando tendência na computação, onde as aplicações *online* estão substituindo as aplicações *desktop*, a partir dai vemos a importância do crescimento desse serviço (SOUSA , 2002).

SOUSA (2002) relata que na década passada, quando as páginas de internet utilizavam somente *HTML* estático e não possuía quase nenhum *script (atu*almente as paginas são feitas de *scripts* em *PHP)*, estão fazendo acessos a banco de dados entre outros recursos.

Para que os recursos tenham uma utilidade os ambientes precisam ter uma combinação de aplicações do sistema operacional, sendo um gerenciador de banco de dados, um servidor web e um interpretador de linguagem. Existem algumas combinações utilizadas uma delas que é usada em ambiente *Windows* como *Wamp* (Windows + Apache + MySQL + PHP) e no *Linux* é conhecida como *LAMP* ( Linux + Apache + MySQL + PHP). Para que as estações tenham acesso a sites é necessário ter um servidor *Web* na rede (SOUSA, 2002).

### 2.2.2 SERVIÇO DNS

Para facilitar para os usuários os endereços da *Internet*, foi criado o serviço de *DNS* (*Domain Name System*) servindo para deixar eles mais legíveis. Por exemplo, um site com o endereço www.enderecoweb.com.br que é acessado pelos usuários, mas para a internet o endereço mandado é 200.221.2.45. Seria complicado se os usuários tivessem que lembrar

da seqüência de números do que palavras separadas por ponto, assim sendo o papel do servidor *DNS*.

O servidor *DNS* possui uma tabela de nomes, que dentro dela tem os nomes do endereço conhecidos na rede com seus nomes de domínio, o maior problema é manter a tabela sempre atualizada. É comum sempre a utilização de dois servidores de *DNS*, o primário e o secundário, caso um fique indisponível o outro assume imediatamente (ROSS, 2009).

As solicitações feitas de um computador para a rede de forma padrão é fornecida pelo provedor, mas também é possível instalar e configurar um servidor *DNS* na rede local. Ocorrem varias solicitações ao servidor *DNS* para o reconhecimento do nome de um domínio, que tem uma grande base de dados na *Internet* (MORIMOTO, 2008), e por conta disso o processo pode demorar. Existem 14 grandes servidores espalhados pelo mundo, os famosos *rootservers,* que recebem as requisições e direcionam para servidores menores responsáveis pelo domínio, eles são lidos da esquerda para direita, podendo ser primários (.br, .ar, .uk) ou secundários (.com, .edu, .net). A figura 4 explica o funcionamento desse processo.

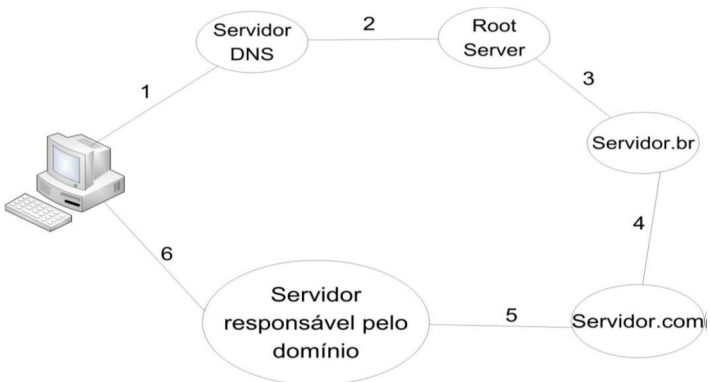



Figura 6– Funcionamento do servidor DNS

Fonte: próprio autor

O computador faz o envio de uma solicitação, através de um *browser,* para acessar o endereço enviado www.enderecoweb.com.br, que vai para o servidor *DNS* especificado na configuração da rede (1). Esse servidor encaminha para um *rootserver* (2), que encaminha para o servidor primário (3), caso registro.br. Em seguida passa para o servidor secundário (4), por exemplo o *.com.* Agora é encaminhado ao servidor responsável pelo domínio (5) e finalmente encaminhada para a estação (6).

### 2.2.3 SERVIÇO DHCP

Para que os computadores da rede recebam as configurações por um servidor, sem a necessidade de configurar manualmente cada um, existe o serviço de *DHCP* (*Dynamic Host*

*Configuration Protocol),* que fornece a permissão de acesso para os computadores. Para que uma rede trabalhe usando *DHCP* é muito importante que esse servidor *DHCP* esteja sempre disponível, caso não esteja as máquinas ficarão sem conseguir conectar automaticamente. Ele não necessita de um servidor dedicado, por consumir pouca memória e processamento (ROCHA et al,2007).

Quando a estação não tem as informações necessárias para acessar uma rede como DSN, numero de IP e *Gateway*, para que ele consiga essas informações a estação cliente de IP número 0.0.0.0 faz um *brodcast* na porta 68 UDP para o endereço 255.255.255.255 que faz a transmissão para todos os computadores da rede. O servidor *DHCP* de *IP* número 192.168.0.1 faz a concessão na porta 67 *UDP* para o cliente com *IP* 192.168.0.2 na mesma porta. Com isso é adquirido um pacote contendo todas as informações necessárias e que não tinham, essas informações serão armazenadas temporariamente e a estação tentará fazer a renovação de suas informações. Caso isso não aconteça serão feitas novas tentativas ate alcançar 87.5% do *lease time,* caso ele não renove no final de seu tempo a estação ficará fora da rede e serão feitas novas solicitações de cinco em cinco minutos (MORIMOTO, 2008).

### 2.2.4 SERVIÇO DE E-MAIL

Considerado de grande importância em uma rede, pois envia e recebe *e-mails* de usuários de uma rede. O seu funcionamento é simples, o problema acontece quando falamos de segurança tornando sua configuração bem complexa, pois para tentar bloquear *e-mails* automáticos contendo programas, vírus em anexo e *spams* é necessário fazer varias configurações, como antivírus, atualizações, *DNS* reverso, filtro de *AntiSpam* entre outros. O foco principal do servidor de *e-mail* é permitir que as mensagens sejam enviadas com sucesso de seu correio eletrônico (ROSS, 2009).

## 2.3 FERRAMENTAS PARA ANALISE DE ANOMALIAS

A correta configuração dos serviços e o uso seguro por parte dos usuários são fundamentais para a segurança de uma rede. Contudo, paralelamente a esses fatores, ferramentas de segurança podem ser utilizadas para monitorar a rede para detectar possíveis problemas e, conseqüentemente, suas respectivas formas de correções. As ferramentas de segurança podem ser dividas em várias categorias (GRAVES 2007). A seguir são apresentadas algumas delas:

### 2.3.1 SCANNER DE VULNERABILIDADE

Um *scanner* de vulnerabilidades é um aplicativo que permite gerar relatórios sobre as vulnerabilidades de um computador ou uma rede (GASPAR, JESUS e SILVA, 2008). Em sua base de dados constam informações sobre ataques, vulnerabilidades, falhas e atualizações, e baseando-se nessas informações são elaborados os relatórios. A contribuição dessa ferramenta para um administrador de rede é a capacidade de prevenir ataques efetuando as correções propostas por esses relatórios. São exemplos dessas ferramentas o *OpenVAS* e o *Nessus*.

*OpenVAS* (*Vulnerability Assessment System)*, o *OpenVAS* é uma ferramenta muito utilizada por administradores de redes que desejam encontrar vulnerabilidades na rede ou em estações. Com atualizações disponíveis em grandes freqüências, o aplicativo inclui um servidor central e uma interface gráfica. É possível efetuar diferentes tipos de testes para verificar as vulnerabilidades da rede (OPENVAS, 2010).

E o *Nessus* que é considerada uma ferramenta de auditoria, muito usada para detectar vulnerabilidades nos computadores da rede local e suas respectivas correções. Realiza uma varredura de portas e detecta servidores ativos, simulando invasões para detectar vulnerabilidades. Um diferencial dessa ferramenta é que ela procura por servidores ativos não apenas nas portas padrões, mas em todas as portas TCP (NESSUS, 2010).

### 2.3.2 PORT SCANNER

Segundo LEE, ROEDEL e SILENOK (2003), os *port scanners* são ferramentas que podem auxiliar na descoberta de vulnerabilidades em computadores da rede, sendo muito utilizada por profissionais de segurança, esse tipo de ferramenta efetua um teste nas portas lógicas em um determinado computador ou em vários computadores de uma determinada rede e informa quais estão abertas e fechadas. Usuários mal intencionados também fazem uso desse tipo de ferramenta para planejar uma invasão à rede, e uma varredura de portas dessa natureza pode trazer como conseqüência congestionamento na rede e futuros ataques. Em um teste efetuado por um *port scanner* o usuário pode determinar o tipo de teste, que são classificados em *scan* vertical, que é a varredura de várias portas de um determinado computador, *scan* horizontal, varredura de uma única porta em vários computadores da rede, e os *scan s*em blocos, que é a combinação dos dois tipos anteriores. São exemplos desse tipo de ferramenta o *Nmap* e o *Zenmap*

O *Nmap* é uma ferramenta das mais utilizadas quando se fala em segurança de redes. É um *port scanner* multi-plataforma que pode detectar várias informações sobre uma

estação, como o sistema operacional, serviços ativos, *uptimes*, entre outras, além de verificar quais portas estão abertas e fechadas (NMAP, 2010).

Já o *Zenmap* é a versão do *Nmap* com interface gráfica. Desenvolvido para facilitar o uso por parte de usuários iniciantes, usuários avançados também o utilizam devido a sua eficiência em elaborar relatórios estatísticos baseados nos resultados do teste, além de proporcionar ao usuário o gerenciamento de testes, como salvá-los e imprimi-los (ZENMAP, 2010).

### 2.3.3 IDS

A maior parte das empresas ignora o uso de sistemas de detecção de intrusão devido ao uso de soluções preventivas como *firewalls*, antivírus, controle de acesso e criptografia (GASPAR, JESUS e SILVA, 2008). Porém há fatores que mostram que apenas esses métodos não são suficientes, como o fato de ser praticamente impossível implementar uma rede totalmente segura. Um sistema IDS efetua o monitoramento de estações objetivando identificar ações não autorizadas.

Essa identificação ocorre nos padrões de atividades que sugerem a ocorrência de ataques ou usos indevidos de um sistema, de uma estação ou no tráfego da rede.

Segundo (GASPAR et al 2008), o objetivo de um sistema IDS é detectar e alertar, preferencialmente em tempo real, sobre o uso indevido de sistemas em decorrência de ameaças lógicas. Uma das ferramentas IDS mais utilizadas é o Snort.

O *Snort* é um detector de intrusão na rede que desenvolve análise de tráfego em tempo real e registro de pacotes em redes *IP* (SNORT, 2010).

### 2.3.4 IPS

Os *IPS*, sistemas de prevenção de intrusão, podem ser considerados uma evolução dos sistemas *IDS* agregando funcionalidades de prevenção de ataques (CHERON, PADILHA, 2010). Podendo ser utilizado como complemento dos sistemas *IDS*, esse sistema identifica uma intrusão, faz sua análise de relevância e bloqueia determinados eventos. Com isso, um sistema *IPS* pode agir sobre uma tentativa de intrusão de forma a impedir que essa obtenha sucesso e diminua possíveis prejuízos. Além de possuir os mesmos mecanismos de um sistema de detecção de intrusão, os sistemas de prevenção de intrusão podem impedir um evento malicioso em tempo real. O sistema *HLBR* (*hungwash light br*), é um exemplo de sistema *IPS*, pois trata-se de um *IPS* no qual é possível filtrar pacotes diretamente na camada 2 do modelo *OSI*. A detecção de tráfego indevido é feita através de regras simples, onde o próprio usuário pode configurá-las. Bastante eficiente e versátil esse

sistema é considerado “invisível” para outras máquinas na rede e por atacantes, já que não utiliza a pilha *TCP/IP* (HLBR, 2010).

### 2.3.5 SNIFFER

Uma vez implementada, uma rede permite que computadores compartilhem o mesmo meio de comunicação, e com isso pode permitir que um deles "escute" o tráfego dela. Os *Sniffers* são ferramentas que capturam pacotes de informações trafegados na rede (CASAGRANDE, 2003). São ferramentas passivas, isto é, apenas coletam os dados. Toda a comunicação de uma rede se faz a partir do endereço *MAC* dos computadores e cada um deles apenas "escuta" e responde aos pacotes cujo endereço corresponde a ele, ignorando o restante do tráfego. No entanto é possível configurar uma interface de modo a capturar todos os pacotes restantes que são ignorados. Esse é o funcionamento de um *sniffer*, muito utilizado por administradores que desejam monitorar o tráfego de sua rede e possibilitar o descobrimento de falhas e possíveis problemas de performance. Também é utilizada por usuários maliciosos que desejam roubar informações sigilosas como senhas e nomes de usuários. O *Wireshark* e *Tcpdump* são exemplos de ferramentas *sniffers*.

*Wireshark* considerada ferramenta de auditoria, que executa a análise de tráfego de uma rede. Sua função é verificar todos os pacotes que são enviados pelas placas de rede dos computadores da rede. Também pode ser utilizado para detectar problemas na rede e localizar conexões suspeitas (WIRESHARK, 2010).

O *Tcpdump* é um dos mais conhecidos *sniffers* para sistemas *Linux*. Com essa ferramenta é possível efetuar análises na rede a fim de solucionar possíveis problemas. Seu uso é muito simples, bastando apenas que o usuário tenha conhecimentos básicos sobre TCP/IP (TCPDUMP, 2010).

## 2.4 SEGURANÇA

A maioria da população mundial utiliza a rede mundial para fazer compras, controlar a movimentação bancaria e pagar contas, enviar e receber mensagens e as organizações também usam as redes de computadores e a internet para transferências de dados, documentos e informações, manter contato com as filiais em lugares diversos, até mesmo em outro país e, a proteção dos dados e informações se faz necessária.

Em sua forma mais simples, a segurança se preocupa em garantir que pessoas mal-intencionadas não leiam ou, pior ainda, modifiquem secretamente mensagens enviadas a outros destinatários. Outra preocupação da segurança são as pessoas que tentam ter acesso a serviços remotos que elas não estão autorizadas a usar (TANENBAUM, 2003).

Conforme Comer (2006), proteger a informação requer proteger recursos físicos e abstratos. Os físicos são dispositivos passivos, discos e *cd roms* e também dispositivos ativos, que são os computadores dos usuários e, em ambiente de rede devem ter proteção também os cabos, *bridges* e roteadores que compõe a estrutura da rede, nem sempre lembrada, mas a segurança física da rede normalmente deve ser levada em conta na segurança geral.

As organizações, para alcançarem o sucesso, cada vez mais dependem da informática e das telecomunicações, devem estar conectadas na internet para poder competir no mercado globalizado, ter velocidade, qualidade e eficiência nas decisões para oferecer o melhor produto e nas melhores condições. Surgiu um novo ambiente, o cooperativo, com isso novos problemas passam a ocorrer nesses ambientes com relação à segurança de recursos. Conforme Geus; Nakamura (2010), “a complexidade de conexões e a heterogeneidade do ambiente também devem ser consideradas”.

Os ataques são classificados como ataques passivos e ataques ativos. Para Stallings (2008), “um ataque passivo tenta descobrir ou utilizar informações do sistema, mas não afeta recursos. Um ataque ativo tenta alterar os recursos do sistema ou afetar sua operação”.

De acordo com o mesmo autor, ataques passivos apenas monitoram transmissões com o objetivo de obter informações, com análise do trafego e liberação do conteúdo da mensagem, já ataques ativos vão tentar modificar o fluxo de dados ou criar um fluxo falso e são divididos em quatro categorias: disfarce e repetição, negação de serviço e adulteração de mensagem.

Entre os componentes de segurança de uma rede o *firewall* é um dos principais e mais lembrado pelos profissionais de redes.

Segundo Geus; Nakamura (2010), *firewall* é um ponto entre duas ou mais redes, que pode ser um componente ou um conjunto de componentes, por onde passa todo o tráfego, permitindo que o controle, a autenticação e os registros de todo o tráfego sejam realizados.

Em uma organização que preza pela segurança não fará uso somente do *firewall* para proteção de sua rede e nos acessos a internet. O *firewall* de certo modo e a primeira linha de defesa controlando os acessos na rede, mas a autenticação aos serviços também e importante no controle de acesso a rede. O *IDS* (Sistema de Detecção de Intrusão), e importante para monitorar o ambiente, da rede e dos servidores.

Além de ser crucial para a segurança interna, o *IDS* pode detectar ataques que são realizados por meio de portas legítimas permitidas e que, portanto não podem ser protegidas, pelo *firewall* (GEUS; NAKAMURA, 2010).

A detecção de intrusão é baseada na suposição de que o comportamento do intruso difere daquele de um usuário legítimo de maneira que podem ser quantificadas. Naturalmente, não podemos esperar que haverá uma distinção clara, exata, entre um ataque de um intruso e o uso normal dos recursos por um usuário autorizado. Em vez disso, devemos esperar que haja alguma sobreposição (STALLINGS, 2008).

# 3 MATERIAIS E MÉTODOS

Para este estudo foi realizado, a identificação de vulnerabilidades em ambientes de redes sem fio, sendo realizados testes nos ambientes de rede sem fio utilizando o notebook com as seguintes configurações mostrada no quadro 3 :

| | |
|---|---|
| Processador | Intel core i7 q740 |
| Memória | 8GB |
| Adaptador de rede | QuacommAtheros ar5bwb222 |
| Sistema operacional | *BackTrack* 5 r3 *Released* |

Figura 7 - Descrição do notebook

Fonte: próprio autor

Foram escolhidos três locais da cidade de Bauru – SP com rede sem fio para que os testes fossem efetuados. Para garantir que as análises fossem efetuadas apenas nos computadores pertencentes à rede foram efetuados testes em dois dias diferentes em cada ambiente e apenas as estações presentes nos dois dias foram consideradas. Os testes utilizando o scanner de vulnerabilidade foram efetuados somente nas estações mais importantes.

O sistema operacional utilizado foi o *BackTrack* 5 r3 *Released* com versão disponibilizada em 13 de agosto de 2012 obtida em *http://www.backtrack-linux.org/downloads.* Para garantir que a versão instalada é a mais atualizada usei no terminal os comando #*aptitude* upgrade, que serve para verificar quais os pacotes que podiam ser atualizados no sistema, e *o #aptitude updade*, que faz as atualizações de acordo com a verificação do comando anterior.

Para gerenciar as conexões será utilizado o *Wicd*, um gerenciador de rede que possibilita se conectar à rede e diversas alternativas de configuração, pois com ele será possível obter informações sobre as redes disponíveis, tanto cabeadas como as sem fio. Como a utilização foi em apenas redes sem fio, será exibido o nome da rede, a intensidade do sinal, o tipo de criptografia e o *Mac Address* do ponto de acesso, com esse gerenciador, ao estar conectado em uma rede no rodapé aparecerá qual o IP que o computador recebe ao se conectar nela, com isso é possível indicar uma faixa de *IP's* a ser varrida pelos métodos, uma vez conectado a rede foram executados as seguintes ferramentas *Nmap, Zemap, OpenVAS*, *Script* em *Shell*, conforme descrito pelo levantamento bibliográfico.

Os testes foram divididos em 3 formas: o primeiro teste de vulnerabilidades foi do ponto de acesso: O objetivo desse teste é verificar possíveis vulnerabilidades no ponto de acesso das redes analisadas. Para efetuá-lo será utilizadas as informações fornecidas pelos

*port scanners Nmap* e *Zenmap*. Após a análise dessas informações foram efetuadas tentativas de acesso às configurações do ponto de acesso. A figura 5 ilustra o alvo do teste:

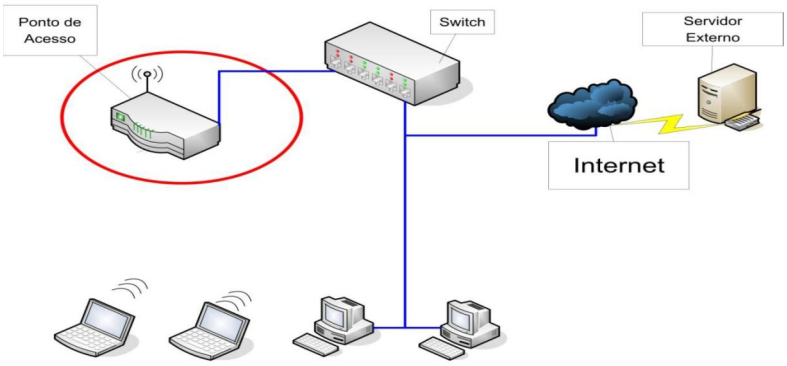



Figura 8 - Teste de vulnerabilidade do ponto de acesso

Fonte: próprio autor

O segundo teste de vulnerabilidades nos computadores da rede: O objetivo desse teste é encontrar vulnerabilidades nos computadores encontrados na rede. Para efetuá-lo foram utilizadas as ferramentas *Nmap, Zenmap* e *OpenVAS*. Com os *port scanners, Nmap e Zenmap* foram obtidas informações gerais de todas as estações encontradas na rede, e em seguida serão escolhidas as estações mais importantes para efetuar relatórios de vulnerabilidades utilizando o *scanner* de vulnerabilidades *OpenVAS*. A figura 6 ilustra o objetivo do teste:

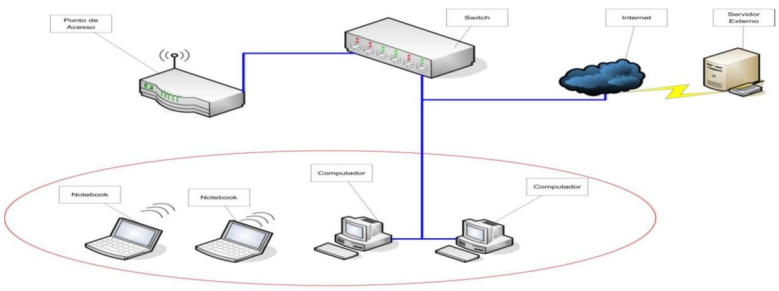


Figura 9 - Teste de vulnerabilidade dos computadores da rede.

Fonte: próprio autor

O terceiro e último teste foi aplicado em um acesso a um servidor externo. O objetivo desse teste é verificar quais serviços a rede permite que uma estação conectada a ela possa ser cliente. Para efetuá-lo será utilizado um servidor ativo na Internet com um IP roteável, sistema operacional *Ubuntu* e todas as 1024 portas *TCP* e *UDP* abertas pelo *shellscript*. Depois de conectado na rede serão efetuados testes de

acesso a esse servidor utilizando o *port scanner Zenmap*. A figura 7 ilustra o processo do teste:

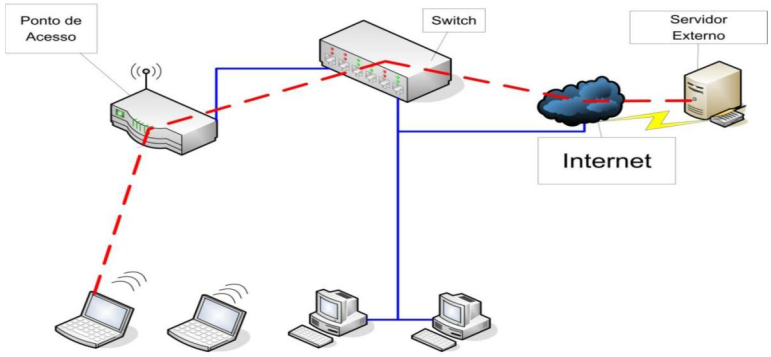



Figura 10 - Teste de acesso a um servidor externo

Fonte: próprio autor

Para que o servidor tivesse suas 1024 portas *TCP* e *UDP* abertas foram desenvolvidos códigos na linguagem *Shell Script*. A forma apresentada para efetuar essa ação é a alteração de dois arquivos de configuração do sistema *Linux* em questão. O primeiro deles é o arquivo "/etc/services", responsável para associar o nome de um serviço a um número de porta. O segundo arquivo a ser configurado é o „/etc/inetd.conf‟, que orienta o *daemon* „inetd‟ sobre a ação que deve ser efetuada quando uma conexão for recebida.

A seguir é apresentado o código para edição do arquivo „/etc/services‟: #!/bin/bash

for i in $(seq 1024) *// Início do laço que irá até 1024, número da última porta a ser aberta*

do

echo porta_tcp$i" "$i/tcp" "p$i" #Porta tcp"$i >>/etc/services *//A cada passagem pelo laço de repetição será escrita uma linha responsável pela abertura de cada uma das 1024 portas TCP*

done

for j in $(seq 1024) *// Início do laço que irá até 1024, número da última porta a ser aberta*

do

echo porta_udp$j" "$j/udp" "p$j" #Porta udp"$j >>/etc/services *//A cada passagem pelo laço de repetição será escrita uma linha responsável pela abertura de cada uma das 1024 portas UDP*

done

O código para edição do arquivo „/etc/inetd.conf‟ é apresentado a seguir: #!/bin/bash

for i in $(seq 1024) *// Início do laço que irá até 1024, número da última porta a ser aberta*

do

echo porta_tcp$i" "stream" "tcp" "nowait" "root" "/bin/bash" "/bin/bash -i >>/etc/inetd.conf *// A cada passagem pelo laço sera escrita uma linha no arquivo inetd.conf de forma a estabelecer uma conexão com a respectiva porta TCP do arquivo /etc/services*

done

for j in $(seq 1024) *// Início do laço que irá até 1024, número da última porta a ser aberta*

do

echo porta_udp$j" "dgram" "udp" ”wait" "root" "/bin/bash" "/bin/bash -i >>/etc/inetd.conf *// A cada passagem pelo laço sera escrita uma linha no arquivo inetd.conf de forma a estabelecer uma conexão com a respectiva porta UDP do arquivo /etc/services*

done

### 3.1 NMAP

Uma vez conectado à rede e sabendo a faixa de IP‟s a ser analisada já é possível efetuar um teste com o port scanner Nmap 5.21. O Nmap já está disponível na instalação padrão das principais distribuições Linux. Para utilizar todos os recursos disponíveis do Nmap é preciso executá-lo como root.

A sintaxe do uso do programa é #nmap <<PARÂMETROS>> <<ALVO_DO_TESTE>>. A utilização de parâmetros é opcional, porém é indicada quando se deseja personalizar o teste. O alvo do teste pode ser um número de IP ou uma faixa deles.

Existem vários parâmetros que podem ser inseridos em um teste do Nmap. A seguir são apresentados os que foram utilizados nos testes:

-T4: O parâmetro –T serve para estabelecer um padrão de temporalização do teste. São especificados seguidos de um número de 0 a 5 que correspondem ao tempo de execução do teste, onde quanto maior o número mais rápido é sua execução. Esses valores são classificados como paranóico (0), furtivo (1), educado (2), normal (3), agressivo (4) e insano (5). Os métodos paranóico e furtivo correspondem as execuções mais lentas e são indicados para evitar um sistema IDS. O método educado diminui o ritmo da varredura causando assim um menor uso da banda e recursos do alvo. O modo normal é o padrão do Nmap, portanto o parâmetro –T3 não tem nenhuma influência sobre o teste. O valor escolhido para os testes foi o –T4, padrão agressivo. Esse padrão acelera a varredura e é indicado para redes razoavelmente rápidas e confiáveis. Por fim, o método insano efetua a varredura da forma mais rápida possível, e caso a rede não seja rápida o suficiente pode causar imprecisões no teste.

-F: Ativa a opção de varredura rápida, verificando apenas as portas listadas no arquivo “nmap-services”.

-sV: Habilita a detecção da versão do serviço ativo.

-O: Habilita a detecção do sistema operacional utilizado em cada uma das estações. Tal identificação é útil para diferenciar sistemas como Windows, Linux e Mac-OS, mas não é eficiente para identificar qual distribuição Linux ou qual a versão do Windows está sendo utilizada.

-Pn: Esta opção desconsidera se a estação está em funcionamento testando todo o arranjo de IP‟s especificado no escopo do teste. Se em uma varredura for especificado o parâmetro /24 serão efetuados 255 testes ignorando o estado das estações.

Para a definição da faixa de IP‟s a ser verificada utilizou-se o parâmetro “192.168.0.1/24”, que significa a verificação de todos os endereços de IP da classe que o computador está conectado. O comando a ser utilizado para verificação da rede em questão seria:

#nmap –T4 –F –sV –O 192.168.0.1/24

Com esse comando, é possível efetuar uma rápida varredura do IP 192.168.0.1 até 192.168.0.254 sem a utilização de ping, buscar quais portas estão abertas em cada uma das estações, seus respectivos serviços e uma suposição do Sistema Operacional utilizado.

## 3.2 ZENMAP

Baseado nas mesmas informações utilizadas para efetuar os testes com o Nmap, pode-ser fazer o teste com o Zenmap. Para iniciá-lo, utiliza-se o comando:

#zenmap

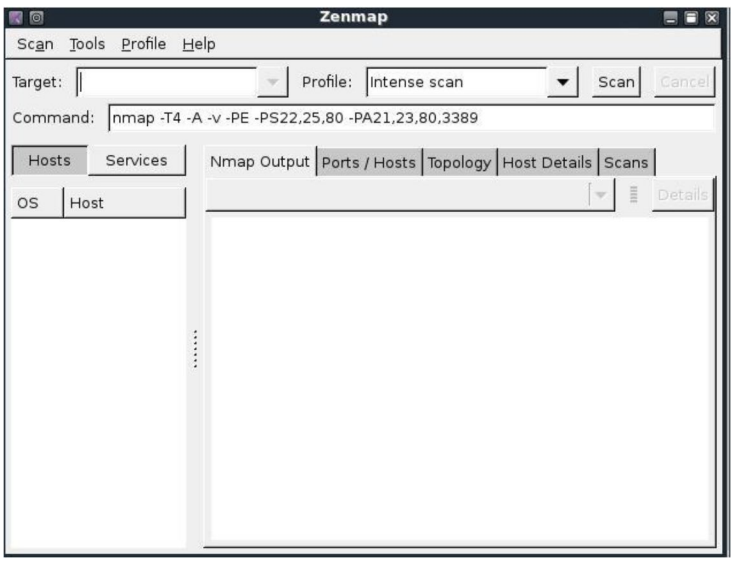



Figura 11 - Tela inicial do Zenmap.

A interface do Zenmap é apresentada na figura 11. No campo “target” é inserido o alvo das análises, ou seja, o mesmo valor do teste efetuado com o Nmap, 192.168.0.1/24. Em “profile” é selecionado o tipo de varredura a ser efetuada, equivalente aos parâmetros do Nmap. A opção utilizada nos testes foi a “Quick Scan Plus” para uma verificação inicial da rede, e “Intense scan” para possíveis servidores já que esse método oferece uma verificação mais detalhada.

Um teste efetuado no Zenmap apresenta os seguintes resultados:

• Hosts: Exibe todas as estações ativas na rede.

• Services: Apresenta os serviços encontrados na rede.

• Nmap Output: Exibe a saída do teste Nmap.

• Ports/hosts: Exibe informações sobre as portas abertas encontradas e seus respectivos serviços.

• Topology: Apresenta a topologia sugerida da rede.

• Hosts Details: Detalhes encontrados de cada uma das estações.

• Scans: Exibe um histórico dos scans efetuados.

Nota-se que o Zenmap oferece o mesmo resultado que o Nmap, porém com opções gráficas que podem auxiliar na elaboração de relatórios. Com todas as informações das estações encontradas, a próxima etapa é escolher uma delas e fazer a localização de vulnerabilidades com o auxílio da ferramenta OpenVAS.

### 3.3 OPENVAS

Para a utilização da ferramenta OpenVAS deve-se primeiramente iniciar o servidor usando o comando **#openvasd.** Após a entrada do comando, serão carregados todos os *plugins* do aplicativo, que correspondem a brechas de segurança conhecidas pelo banco de dados de vulnerabilidades do OpenVAS e que podem ser exploradas, Quando todos os *plugins* forem carregados será apresentada a frase “All plugins loads”, o que significa que já é possível abrir o cliente do OpenVAS com o comando: #OpenVAS-Client. Com a ferramenta aberta já é possível efetuar a criação de uma nova tarefa e seus respectivos escopos. Para efetuar o teste basta um duplo clique no escopo escolhido. Será solicitado o *login* e a senha para a conexão com o servidor OpenVAS, como mostra a figura 12.

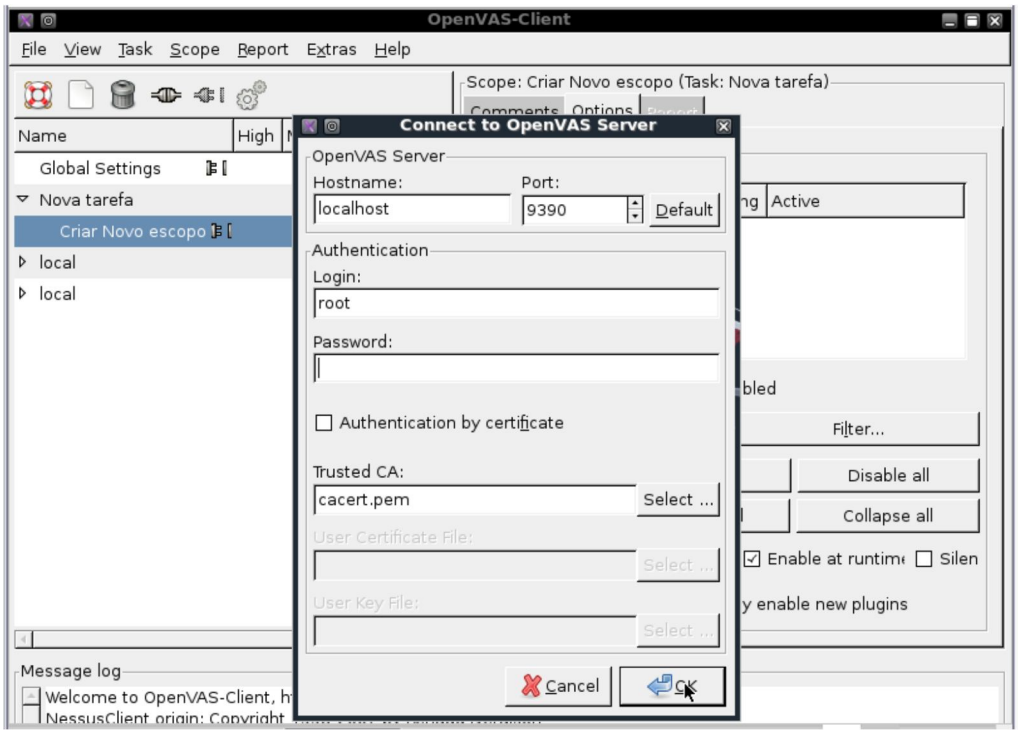



Figura 12 - **Conexão com o servidor do OpenVAS.**

O próximo passo é selecionar quais *plugins* serão utilizados durante o teste. Cada *plugin* corresponde a um determinado conjunto de falhas e para um teste completo, ou seja, uma busca por todas as falhas conhecidas é necessária a utilização de todos os *plugins* clicando na opção "*Enable all*" conforme apresenta a figura 13.

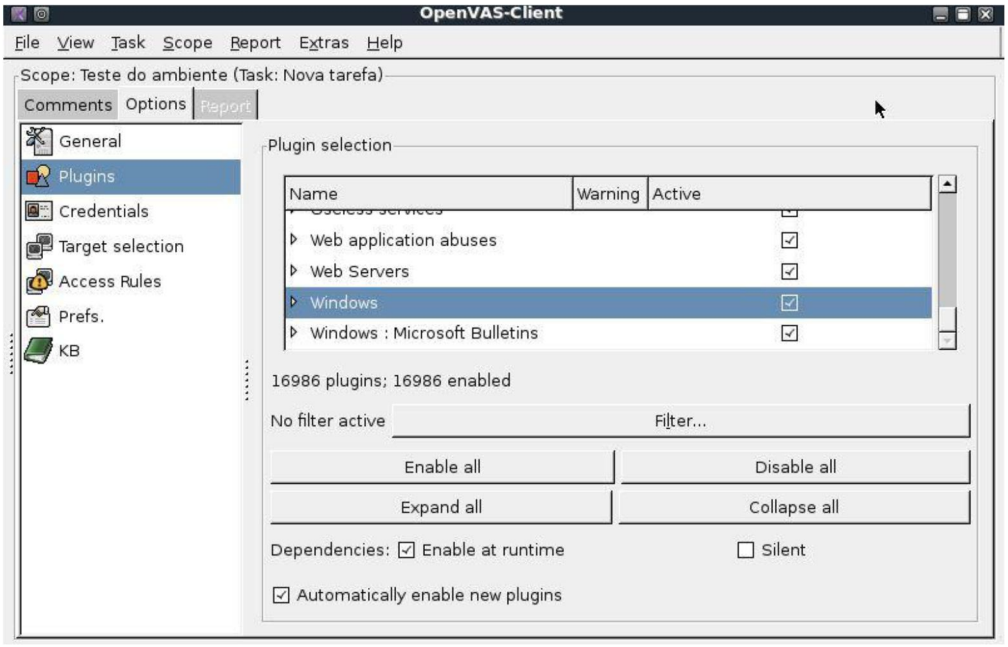



Figura 13 - **Selecionando plugins no OpenVAS.**

Com todos os *plugins* selecionados deve-se informar à ferramenta qual o número do IP da estação escolhida para verificar vulnerabilidades. Com o alvo inserido e todos os *plugins* selecionados já é possível efetuar o teste. Para isso basta selecionar a opção "Execute" do menu "Scope".

Ao final do teste é gerado o relatório das vulnerabilidades encontradas. O OpenVAS atualmente disponibiliza relatórios apenas no idioma Inglês, porém está em andamento um projeto de tradução da ferramenta promovido pela comunidade Back Track Brasil.

# 4 Resultados

Nas próximas subseções do capítulo serão apresentados os três tipos de testes efetuados em cada um dos ambientes: O primeiro foi o teste de vulnerabilidades encontradas no ponto de acesso da rede. O segundo foi o teste de vulnerabilidades encontradas nos computadores pertencentes à rede. O terceiro foi o teste de acesso a um servidor externo através da rede.

## 4.1 ESTABELECIMENTO A

Os resultados dos testes efetuados no *estabelecimento* A são apresentados a seguir:

### 4.1.1 TESTE DE VULNERABILIDADES DO PONTO DE ACESSO

O teste efetuado no ponto de acesso da rede do *estabelecimento* A não detectou nenhuma vulnerabilidade.

### 4.1.2 TESTE DE VULNERABILIDADES NOS COMPUTADORES DA REDE

O teste efetuado utilizando as ferramentas de *port scanner* Nmap e *Zenmap* encontrou seis estações ativas na rede. A topologia da rede sugerida é apresentada na figura 8:

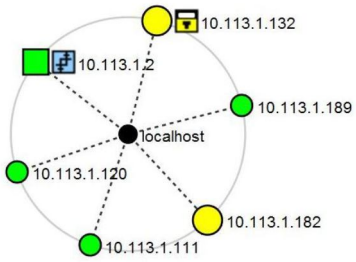



Figura 14 - Topologia de rede sugerida para o Estabelecimento A.

Após a análise dos resultados anteriores, foi efetuado um teste de vulnerabilidades pelo *OpenVAS* na estação de número 10.113.1.182. Foi constatado que se trata possivelmente de um servidor com o sistema operacional *RedHat* apresentando as seguintes especificações:

| Porta | Protocolo | Estado | Serviço | Versão |
|---|---|---|---|---|
| 113 | tcp | open | Tcpwrapped | |
| 139 | tcp | open | netbios-ssn | Samba smbd 3.x(*workgroup*) |
| 445 | tcp | open | netbios-ssn | Samba smbd 3.x(*workgroup*) |
| 6000 | tcp | open | X11 | |

Figura 15 - Serviços de rede encontrados na estação 10.113.1.182 do estabelecimento A.

As portas da estação que se encontram abertas são apresentadas no quadro 5. A porta 113 pode ser explorada pelos *trojans* "*Invisible Identd Deamon*" e "*Kazimas*", e a porta 6000 pelo *trojan* "*The Thing*". A porta 6000 é utilizada pelo serviço "*Open* X 11" e pode ser explorada por um invasor e quase sempre obtendo acesso ao servidor sem ser feita nenhuma autenticação.

O fato da porta 6000 estar aberta não necessariamente indica que o sistema está vulnerável. Um invasor pode não invadir o sistema, mas pode tentar enviar pacotes e requisições ao servidor para causar uma ataque de *DoS*.

As falhas apresentadas pelo *OpenVAS* podem ser corrigidas seguindo as referências apresentadas por órgãos regulamentadores, como o "*CVE Common Vulnerabilities and Exposures*", "*OpenVAS ID*" e "*BID Security Focus*". Essas entidades são mantidas por profissionais de segurança em redes. A "*OpenVAS ID*" é uma comunidade destinada a programadores profissionais que divulgam códigos em diversas plataformas a fim de se corrigir as falhas detectadas. Para cada falha existe uma correção, por isso é recomendado que o administrador da rede consulte suas soluções logo que uma nova falha for detectada.

As portas *TCP* 139 e 445 podem ser usadas para obter informações sobre o sistema operacional do servidor, e com isso facilitar o ataque e reduzir a margem de erros das ferramentas existentes, aumentado a chance de sucesso de um ataque. Tais portas estão abertas porque o servidor tem instalado o aplicativo Samba que permite o gerenciamento e compartilhamento de recursos de uma rede com computadores de sistemas operacionais *Windows*.

O Samba em versões anteriores a 4.3 são vulneráveis a ataques de diretório de passagem caso não seja atualizado periodicamente. Esse tipo de ataque permite ao invasor ter acesso como convidado, utilizando uma conta de usuário limitada, a arquivos e diretórios compartilhados com permissão restrita. O desenvolvedor do *software* recomenda também que os administradores corrijam a falha de configuração no arquivo *smb.conf* e troque o valor da variável por *wide links = no' in the '[global].* Feito isso basta reiniciar o serviço para que a correção entre em vigência. A outra falha referente à porta 139 *UDP* pode ser solucionada utilizando uma regra de *firewall* para filtrar todo o tráfego dessa porta.

### 4.1.3 TESTE DE ACESSO A UM SERVIDOR EXTERNO

O teste de acesso ao servidor externo revelou uma falha na proteção dos serviços disponibilizados ao usuário, que deveria ser feita através de regras de *firewall*. Com isso, um invasor poderia efetuar ataques a servidores externos sem a possibilidade de ser identificado, pois não existiu nenhum cadastro que permitisse a identificação do usuário na rede.

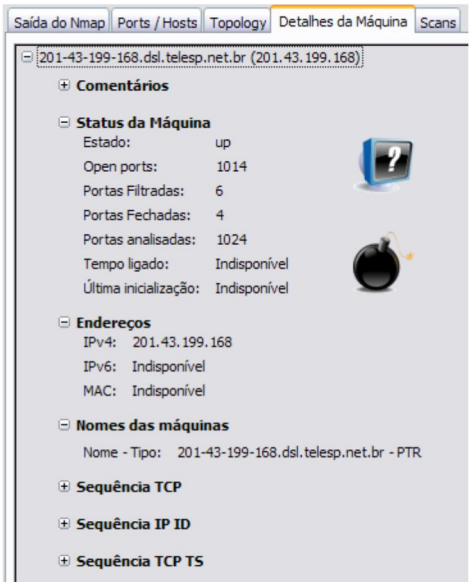



Figura 16– Estatística do estado das portas *TCP* em um acesso externo no estabelecimento A.

Como pode ser visto na figura 9, das 1024 portas analisadas apenas seis foram filtradas e 1014 estavam desprotegidas. Outras quatro portas se encontravam fechadas pelo servidor. Na varredura efetuada nas portas *UDP* foram detectadas nove portas abertas, como mostra a figura 10:

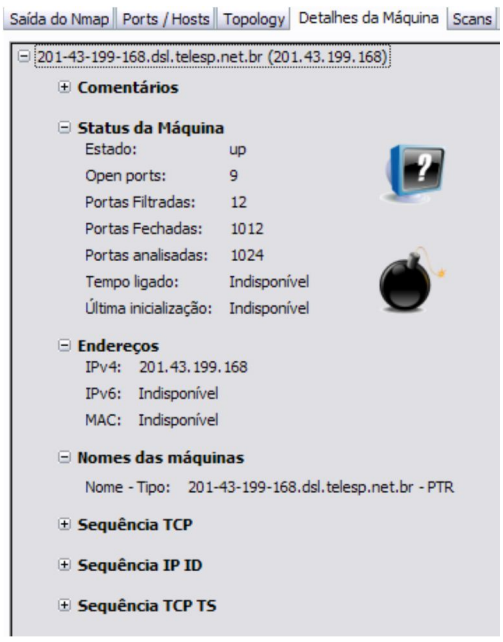



Figura 17 – Estatística do estado das portas *UDP* em um acesso externo no estabelecimento A.

## 4.2 ESTABELECIMENTO B

Os resultados dos testes efetuados no estabelecimento B são apresentados a seguir:

### 4.2.1 TESTE DE VULNERABILIDADES DO PONTO DE ACESSO

O nome do *SSID* da rede foi alterado para não despertar a curiosidade de nenhum invasor. Não foi possível acessar as configurações do painel de controle do ponto de acesso, pois as configurações padrões foram alteradas.

### 4.2.2 TESTE DE VULNERABILIDADES NOS COMPUTADORES DA REDE

Os testes efetuados pelos *port scanners* apresentaram resultados diferentes nos dois dias. No primeiro dia foi possível utilizar as ferramentas para analisar a rede e os computadores pertencentes a ela. Foram encontrados dois possíveis servidores com algumas vulnerabilidades uma do tipo *XSS* e outra na versão do serviço samba que estava desatualizado, ou seja, a versão era 4.3. No segundo dia a rede não permitiu efetuar os mesmos testes. Isso pode ter ocorrido devido o uso de ferramentas *IDS* por parte do administrador da rede, que ao detectar as ações efetuadas pelos *port scanners* bloqueou esse tipo de procedimento.

### 4.2.3 TESTE DE ACESSO A UM SERVIDOR EXTERNO

As regras de *firewall* estão bem configuras, pois apenas permitem tráfego nas portas TCP 80 e 53, como mostra a figura 11:

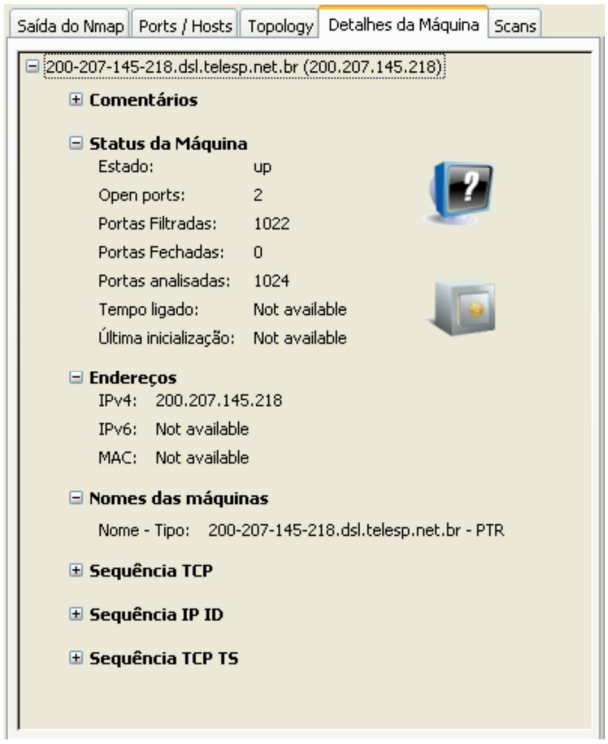



Figura 18 – Estatísticas de portas disponíveis em acesso externo do estabelecimento B.

Esta rede pode ser considerada segura nos quesitos de avaliação propostos pelo presente Trabalho. Segundo os testes foi possível apenas acessar a Internet. Contudo, não houve nenhum tipo de cadastro que identificasse o usuário em uma futura investigação.

## 4.3 ESTABELECIMENTO C

Os resultados dos testes efetuados no *estabelecimento* C são apresentados a seguir:

### 4.3.1 TESTE DE VULNERABILIDADES DO PONTO DE ACESSO

A rede do *estabelecimento* C apresentou as configurações básicas de fábrica em seu ponto de acesso, cujo nome era “linksys” e o IP 192.168.1.1. Nesse dispositivo foi possível acessar o centro de controle como mostra a figura 12.

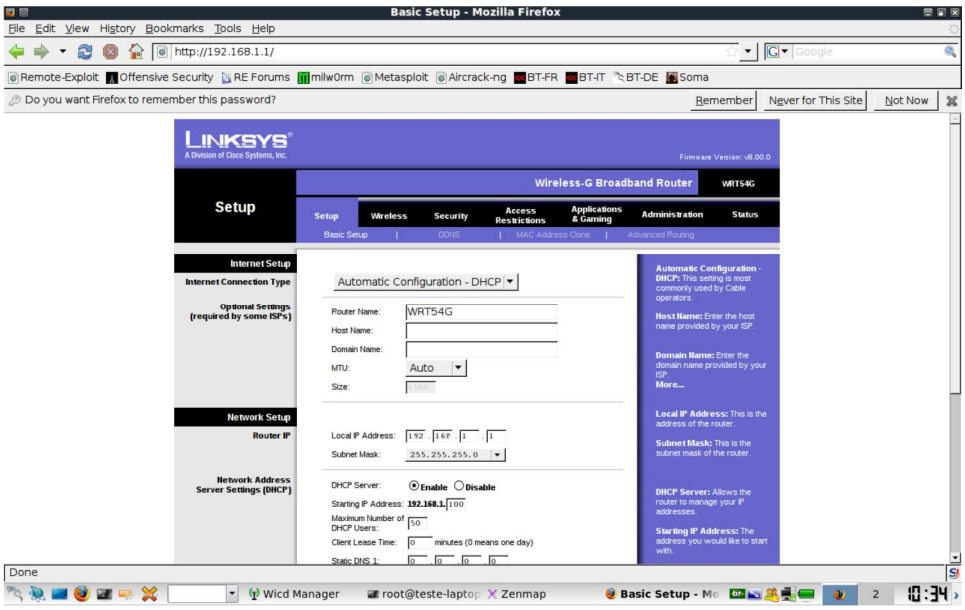



Figura 19– Tela do centro de controle do roteador do estabelecimento C.

A partir do centro de controle foi possível ter acesso às demais áreas de configuração do ponto de acesso da rede. A figura 13 mostra a interface que possibilita as configurações da rede sem fio, podendo efetuar ações como alterar o canal de freqüência, alterar o *SSID* da rede e deixá-lo oculto ou disponível:

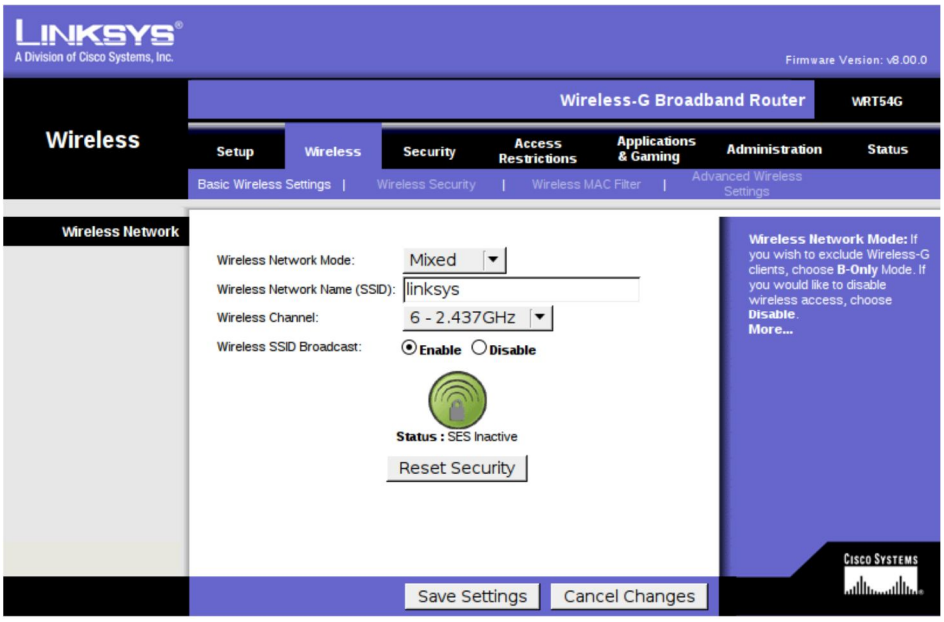



Figura 20– Tela de configuração da rede wireless do estabelecimento C.

Também foi possível ter acesso às configurações de segurança do dispositivo, sendo possível a alteração de filtros e de regras de *firewall*, mostrados na figura 14.

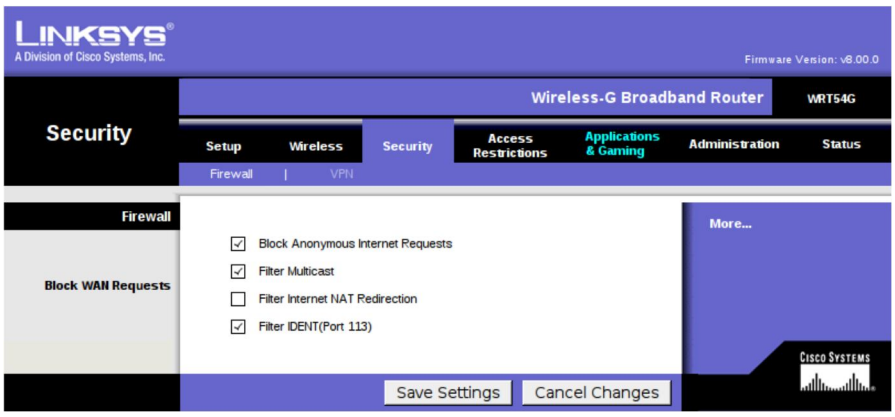



Figura 21 – Tela de configurações de segurança do do estabelecimento C.

### 4.3.2 TESTE DE VULNERABILIDADES NOS COMPUTADORES DA REDE

Nesta rede não foi encontrado nenhum servidor para efetuar o teste com o OpenVAS.

### 4.3.3 TESTE DE ACESSO A UM SERVIDOR EXTERNO

Além das graves vulnerabilidades encontradas em seu ponto de acesso, a rede do *estabelecimento* C não apresentou nenhuma proteção dos serviços disponibilizados através de seu *firewall*. Das 1024 portas verificadas em um servidor externo 905 estavam disponíveis para acesso, como pode ser visto na figura 15

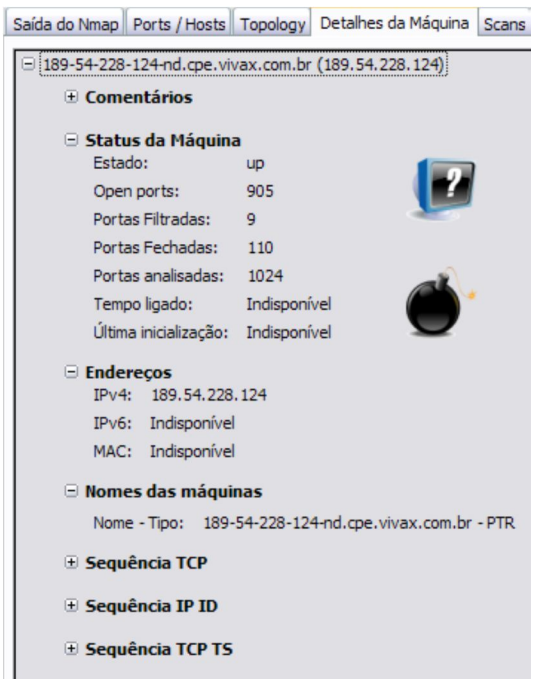



Figura 22 – Estatísticas de portas disponíveis em acesso externo do estabelecimento C.

## 4.4 CONSIDERAÇÕES FINAIS

Os testes efetuados revelaram que grande parte das redes analisadas não apresenta configurações de segurança em seu ponto de acesso, e algumas vulnerabilidades encontradas poderiam ser solucionadas seguindo alguns procedimentos básicos que servem para configurar redes sem fio em geral.

A configuração do ponto de acesso, que foi ignorada em algumas das redes verificadas, é de extrema importância para garantir a integridade e bom funcionamento da rede. Ao manter o *SSID* padrão o administrador permite que um invasor já tenha noção de várias combinações de *login* e senha para se conectar ao ponto de acesso, por isso sempre deve ser alterado sempre que a rede for implementada. Por esse motivo também se faz necessária a alteração de *login* e senha padrões dos equipamentos. Apesar de parecer um procedimento óbvio, algumas das redes analisadas não fizeram esse procedimento, o que permitia que um usuário mal intencionado efetuasse várias configurações prejudiciais a rede, podendo inclusive atualizar o *firmware* para uma versão que inutilizasse o equipamento.

Foi constatado também que nas redes analisadas foi possível ter acesso à rede em locais externos aos estabelecimentos. Com isso pode-se concluir que a escolha do local do ponto de acesso não foi planejada de forma a evitar que o sinal se irradiasse para além do ambiente previsto. Para efetuar essa verificação o administrador da rede poderia verificar a intensidade do sinal nas proximidades externas do estabelecimento utilizando *notebooks* com *softwares* de monitoramento, como o gerenciador de redes *Wicd*, que exibe a intensidade do sinal de uma rede.

Em apenas uma das redes analisadas apresentavam algum tipo de cadastro para permitir o acesso do usuário à rede. Com esse cadastro é possível que o administrador tenha maior controle da sua rede, permitindo uma eventual identificação de usuários que utilizaram a rede. Paralelamente a isso, é recomendado que a rede possua um sistema de *log*, que permita a visualização posterior de ações efetuadas pelos usuários.

Foi observado que a maioria das redes não apresentavam proteção por *firewall* adequada. As redes analisadas não apresentavam uma proteção externa, ou seja, regras de *firewall* entre a Internet e o roteador, e também não possuíam uma proteção adequada entre o ponto de acesso e o roteador. A figura 16 apresenta essa topologia verificada:

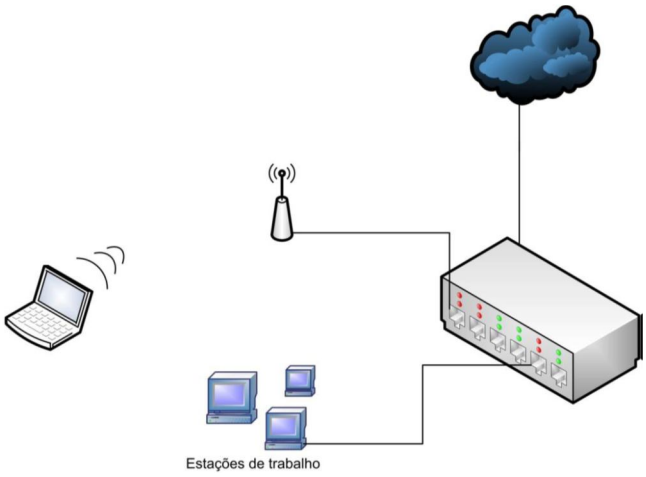



Figura 23– Topologia existente nas redes analisadas.

Para aperfeiçoar essa implementação é sugerida a criação de uma zona desmilitarizada na rede de forma que ela forneça aos usuários acesso a Internet protegido externamente isolando o tráfego da rede utilizando um *firewall* como *gateway* e que os usuários não tenham acesso direto ao roteador e outros dispositivos da rede, como mostra a figura 17:

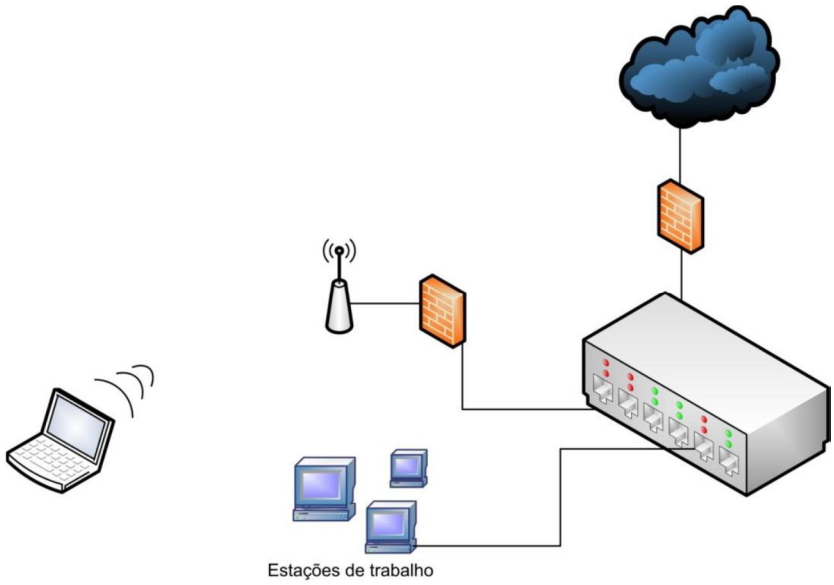



Figura 24 – Topologia sugerida para uma rede sem fio implementada com segurança.

Com isso este trabalho apresentou métodos de identificação e análise de possíveis vulnerabilidades de uma rede e como o administrador de redes pode efetuar as devidas correções a fim de criar um ambiente mais seguro.

## 4.5 TRABALHOS FUTUROS

As contribuições alcançadas com este trabalho não encerram as pesquisas relacionadas à segurança de redes de computadores, mas abrem oportunidades para alguns trabalhos futuros, como um estudo mais aprofundado sobre a responsabilidade do

uso de redes sem fio aberta; realizar analise de ferramentas de detecção de intrusões; a exploração de vulnerabilidade através do uso do *exploits*; analise de ferramentas de prevenção de intrusão.

**REFERÊNCIAS**


ABNT. ABNT/NBR14565. **Procedimento básico para elaboração de projetos de cabeamento de telecomunicações para rede interna estruturada**. Associação Brasileira de Normas Técnicas, 2002.

CASAGRANDE, Rogério Antônio, Técnicas de Detecção de Sniffers, Universidade Federal do Rio Grande do Sul, 2003.

CHERON, Maristela; PADILHA, Fauston Samuel, Estudo da ferramenta de Prevenção de Intrusão HLBR, 2010, PUC-PR.

Comer, Douglas.,**Interligação de redes com TCP/IP**, vol. 1, 5ª edição., Rio de Janeiro: Elsevier Editora Ltda., 2006.

Forouzan, Behrouz A; Sophia ChungFegan.**Protocolo TCP/IP**. 3. Ed. São Paulo: McGraw-Hill, 2008.

GASPAR, Antonio E. de O.; JESUS, Karla L. S; SILVA, Milene C. Um Estudo Sobre Sistemas De Detecção De Intrusão, 2008, Universidade Federal do Pará.

Gordon, Lyon. **Exame de redes com Nmap**. Rio de Janeiro: Editora Ciência Moderna Ltda., 2009, edição original 2008.

GRAVES, K. CEH Official Certified Ethical Hacker Review Guide (1st ed.), 2007. Indianapolis, In: Wiley Publishing, Inc..

HLBR. Disponível em <http://hlbr.sourceforge.net/>. Acesso em 01 de maio. 2010.

HOUAISS, Antônio, **Dicionário Houaiss Da Língua Portuguesa**, Objetiva, Rio de janeiro, 1ª edição - 2009.

KROPIWIEC, Diogo Ditzel, **Paradigmas de segurança em sistemas operacionais**, Universidade Estadual de Campinas, Campinas, 2008.

LEE, Cynthia Bailey; ROEDEL, Chris; SILENOK, Elena., Detection and Characterization of Port Scan Attacks, 2003, disponível em http://www.csd.uoc.gr/gvasil/stuff/papers/PortScans.pdf.

MORIMOTO, Carlos E. **Redes – Guia Prático.** Porto Alegre, Sul Editores 2008.

MORIMOTO, Carlos E. **Servidores Linux - Guia prático.** Porto Alegre, Sul Editores. 2008.

Nakamura, Emilio Tissato;Geus, Paulo Licio de., **Segurança de redes em ambientes cooperativos**. São Paulo: Novatec Editora, 2007.

NESSUS. Disponível em <http://www.nessus.org>. Acesso em 25 de abril. 2013.

NMAP. Disponível em <http://nmap.org>. Acesso em 27 de abril. 2013.

OLIVEIRA, Sérgio. **Um modelo de gerenciamento em redes de sensores sem fio**, Universidade Federal de Minas Gerais, Belo Horizonte, 2008.

OPENVAS. Disponível em <http://www.openvas.org/>. Acesso em 27 de abril. 2013.

ROCHA, Douglas R. Mendes. **Redes de Computadores - Teoria e Prática,** Novatec, São Paulo, 2007.

ROSS, Jonh**. O Livro do Wireless: Um Guia Definitivo para Wi-Fi - Redes Sem Fio**. São Paulo: Alta Books Paulo 2009.

RUSSELL, Ryan et al. Rede Segura: Network. 2.ed. Traduzido por Marcos Vieira. Rio de Janeiro: Alta Books, 2002.c

SNORT. Disponível em <http://www.snort.org>. Acesso em 28 de abril. 2013.

SOUSA, Maxuel Barbosa. **Wireless - Sistemas de Rede sem Fio.** Brasport, 2002.

STALLINGS, WILLIAN. Redes e sistemas de comunicação de dados. 5. ed. Rio

TANENBAUM, Andrew S. **Redes de computadores,** 15.ed Rio de Janeiro, Elsevier, 2003.

TCPDUMP. Disponível em <http://www.tcpdump.org>. Acesso em 13 de fevereiro. 2010.

TITTEL, Ed **. Redes de computadores,** Porto Alegre, Bookman 2003.

WIRESHARK. Disponível em <http://www.wireshark.org>. Acesso em 28 de abril. 2013.

ZENMAP. Disponível em <http://nmap.org/zenmap/>. Acesso em 12 de fevereiro. 2010.

Anexo

Estabelecimento A

Teste com Nmap

Starting Nmap 5.21 ( http://nmap.org ) at 2010-04-07 11:33 BRT

Nmap scan report for 10.113.1.2

Host is up (0.0080s latency).

Not shown: 98 closed ports

PORT STATE SERVICE

80/tcp open http

515/tcp open printer

MAC Address: 00:19:5B:BC:33:ED (D-Link)

Device type: WAP|broadband router

Running: D-Link embedded, SMC embedded, ZyXEL embedded

OS details: D-Link DI-524 or DI-604, SMC SMC7004VBR, or ZyXEL Prestige 320W broadband router

Network Distance: 1 hop

Nmap scan report for 10.113.1.3

Host is up (0.0028s latency).

Not shown: 99 closed ports

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 00:24:01:D0:8E:23 (D-Link)

Device type: WAP

Running: Linux 2.6.X

OS details: OpenWrt Kamikaze 7.09 (Linux 2.6.17 - 2.6.21)

Network Distance: 1 hop

Nmap scan report for 10.113.1.111

Host is up (0.000026s latency).

All 100 scanned ports on 10.113.1.111 are closed

Too many fingerprints match this host to give specific OS details

Network Distance: 0 hops

Nmap scan report for 10.113.1.120

Host is up (0.0023s latency).

All 100 scanned ports on 10.113.1.120 are closed

MAC Address: 00:26:BB:12:81:35 (Apple)

Device type: phone|media device|general purpose|specialized

Running: Apple iPhone OS 1.X|2.X|3.X, Apple Mac OS X 10.5.X, VMware ESX Server 3.X

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop

Nmap scan report for 10.113.1.182

Host is up (0.0025s latency).

PORT STATE SERVICE

113/tcp open tcpwrapped

139/tcp open netbios-ssn

445/tcp open netbios-ssn

6000/tcp open X11

MAC Address: 00:22:5F:DF:A6:D1 (Liteon Technology)

Device type: general purpose

Running: Linux 2.4.X

OS details: Linux 2.4.21 (Red Hat Enterprise Linux 3)

Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .

Nmap done: 256 IP addresses (4 hosts up) scanned in 25.62 seconds

Teste com Zenmap

Estações encontradas: 6.

Serviços: printer, HTTP, tcowrapped, X11, netbios-ssn e alguns serviços desconhecidos.

A topologia sugerida é apresentada a seguir:

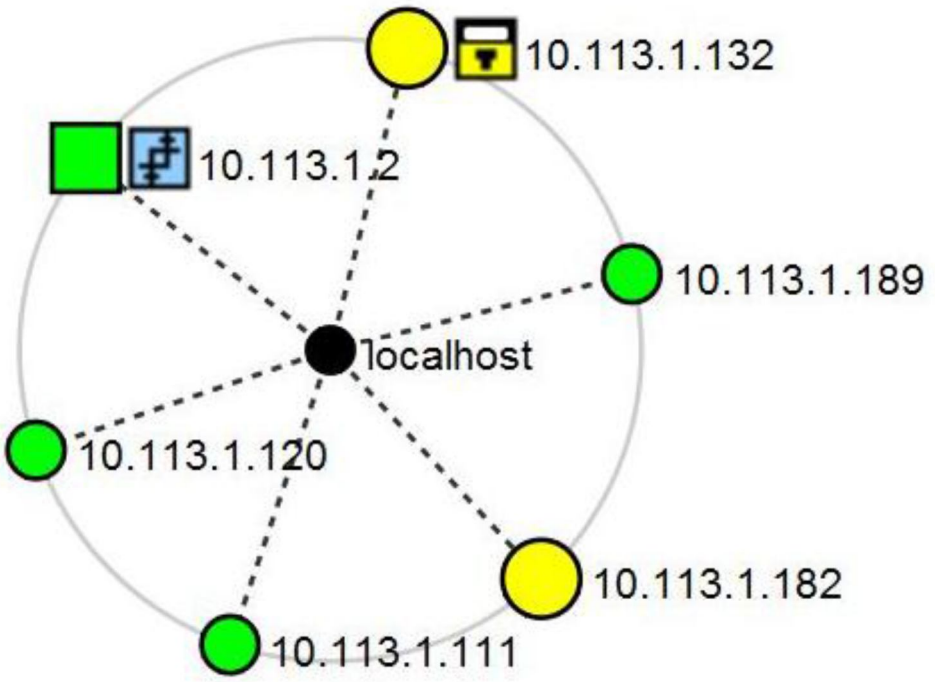



**Figura 1 – Topologia de rede sugerida do shopping center A.**

Teste com OpenVAS

| **Relatório da Varredura do OpenVAS** | | |
|---|---|---|
| Este relatório mostra em detalhes as estações que foram testadas e os problemas que foram encontrados. Por favor, siga as recomendações e procedimentos para erradicar essas ameaças. | | |
| **Detalhes da varredura** | | |
| Estações que responderam aos testes e estavam disponíveis | 1 | |
| Número de falha(s) de segurança | 2 | |
| Número de alerta(s)de segurança encontrada(s) | 5 | |
| Número de nota(s) de segurança encontrada(s) | 11 | |
| Número de falso(s) positivo(s) encontrado(s) | 0 | |
| **Lista de estações** | | |
| **Estação** | **Possíveis falhas** | |
| 10.113.1.182 | Falha de segurança encontrada | |
| **Analise da Estação c** | | |
| **Endereço da estação** | **Porta/Serviço** | **Falha a respeito da porta** |
| 10.113.1.182 | ssh (22/tcp) | Nota de segurança encontrada |
| 10.113.1.182 | microsoft-ds (445/tcp) | Nota de segurança encontrada |
| 10.113.1.182 | netbios-ssn (139/tcp) | Nota de segurança encontrada |
| 10.113.1.182 | netbios-ns (137/udp) | Alerta de segurança encontrada |
| 10.113.1.182 | general/tcp | Falha de segurança encontrada |
| 10.113.1.182 | xdmcp (177/udp) | Alerta de segurança encontrada |
| 10.113.1.182 | x11 (6000/tcp) | Nota de segurança encontrada |
| 10.113.1.182 | ldap (389/tcp) | Sem informação |
| 10.113.1.182 | http (80/tcp) | Sem informação |
| 10.113.1.182 | general/SMBClient | Nota de segurança encontrada |
| 10.113.1.182 | general/CPE | Sem informação |
| **Falhas de segurança e suas correções :10.113.1.182** | | |
| **Tipo** | **Porta** | **Falha e correção** |
| Informação | ssh (22/tcp) | Sem o uso das chaves para análise SLAD. As verificações SLAD serão desativadas. OpenVAS ID : |

| | | |
|---|---|---|
| | | 1.3.6.1.4.1.25623.1.0.90003 |
| Informação | ssh (22/tcp) | Sem o uso das chaves para análise SLAD. As verificações SLAD serão desativadas. OpenVAS ID : 1.3.6.1.4.1.25623.1.0.90002 |
| Vulnerabilidade | microsoft-ds (445/tcp) | Visão global: O Samba é propenso a uma vulnerabilidade de elevação de privilégios local no utilitário 'mount.cifs'. Atacantes locais podem explorar esta falha para obter privilégios elevados em computadores afetados. Solução: Atualizações estão disponíveis. Por favor, consulte as referencias para maiores informações. Referencias: http://www.securityfocus.com/bid/37992 http://www.samba.org Fator de risco: Alto CVE : CVE-2009-3297 BID : 37992 OpenVAS ID : 1.3.6.1.4.1.25623.1.0.100476 |
| Alerta | microsoft-ds (445/tcp) | Visão Geral: Samba é propenso a múltiplas vulnerabilidades, incluindo uma vulnerabilidade que pode permitir que atacantes contornem restrições de segurança determinadas, uma divulgação de informações de vulnerabilidade e um controle remoto de negação de serviço. Uma exploração bem sucedida pode permitir que atacantes ganhem acesso aos recursos que não é suposto serem compartilhado, permitindo que os atacantes obtenham sensíveis informações que podem ajudar em ataques a distancia e fazer com que a aplicação consuma recursos de CPU excessivos, negando serviço a usuários legítimos. |
| Versões do Samba 3.4.2, 3.3.8, 3.2.15, e 3.0.37 são vulneráveis. Solução: Atualizações estão disponíveis. Por favor, consulte as referencias para maiores informações. Referencias: http://www.securityfocus.com/bid/36363 http://www.securityfocus.com/bid/36573 http://www.securityfocus.com/bid/36572 http://www.samba.org/samba/security/CVE-2009-2813.html http://www.samba.org/samba/security/CVE-2009-2948.html http://www.samba.org/samba/security/CVE-2009-2906.html http://www.samba.org/samba/history/security.html http://us1.samba.org/samba/ Risk factor : Medium CVE : CVE-2009-2813, CVE-2009-2948, CVE-2009-2906 BID : 36363, 36572, 36573 OpenVAS ID : 1.3.6.1.4.1.25623.1.0.100306 | | |
| Alerta | microsoft-ds (445/tcp) | Visão Geral: O Samba é propenso a vulnerabilidade de DOS remota. Um atacante remoto pode explorar esta falha para causar um travamento da aplicação, negando serviço para usuários legítimos. Samba 3.4.5 e as versões anteriores. Referencias: |

| | | |
|---|---|---|
| | | http://www.securityfocus.com/bid/38326<br>http://git.samba.org/?p=samba.git;a=commit;h=a065c177dfc8f968775593ba00dffafeebb2e054 http://us1.samba.org/samba/<br>Fator de risco: Médio. CVE : CVE-2013-0547 BID : 38326 OpenVAS ID : 1.3.6.1.4.1.25623.1.0.100499 |
| Alerta | microsoft-ds (445/tcp) | Visão Geral:<br>Samba é propenso a uma vulnerabilidade de diretório de passagem porque a aplicação não limpa suficientemente a entrada fornecida pelo usuário.<br>Exploits podem permitir que um invasor acesse arquivos de fora do diretório de usuário administrador do Samba e permitir obter informações confidenciais e planejar futuros ataques.<br>Para explorar essa falha, é requerido o acesso autenticado para um diretório de arquivos compartilhados. Note que essa falha pode ser explorada através de um compartilhamento gravável acessível por usuários com privilégios de convidado.<br>NOTA: O desenvolvedor informa que esse problema decorre de uma falha de segurança na configuração padrão. A equipe do projeto Samba aconselha os administradores configurarem " 'wide links = no' in the global" no arquivo "smb.conf".<br>Solução: O desenvolvedor comentou sobre o problema afirmando que ela decorre de uma falha na configuração padrão. A equipe de desenvolvedores do Samba aconselha os administradores a estabelecerem " 'wide links = no' " no arquivo "smb.conf" e em seguida, reiniciar o serviço para completar a correção. Por favor, consulte as referências para mais informações.<br>Referências:<br>http://www.securityfocus.com/bid/38111<br>http://www.samba.org/samba/news/symlink_attack.html<br>http://archives.neohapsis.com/archives/fulldisclosure/2013-02/0100.html<br>http://www.samba.org<br>http://lists.grok.org.uk/pipermail/full-disclosure/2013-February/072927.html |
| Fator de risco : Médio BID : 38111 OpenVAS ID : 1.3.6.1.4.1.25623.1.0.100488 | | |

| | | |
|---|---|---|
| Informação | microsoft-ds (445/tcp) | Um servidor CIFS está em execução nesta porta OpenVAS ID : 1.3.6.1.4.1.25623.1.0.11011 |
| Informational | microsoft-ds (445/tcp) | Pode ser possível efetuar a autenticação remota na estação usando as seguintes combinações de login/password: OpenVAS ID : 1.3.6.1.4.1.25623.1.0.10394 |
| Informação | microsoft-ds (445/tcp) | Visão geral:<br>É possível extrair o as informações do Sistema Operacional e do servidor SMB da sessão e da instalação. Foi gerado um pacote durante a autenticação NTLM. Fator de risco: Nenhum.<br>Grupo de trabalho detectado: WORKGROUP Servidor SMB detectado: Samba 3.0.24 Sistema Operacional detectado: Unix OpenVAS ID : 1.3.6.1.4.1.25623.1.0.102011 |
| Informação | netbios-ssn (139/tcp) | Um servidor SMB esta respondendo nesta porta. OpenVAS ID : 1.3.6.1.4.1.25623.1.0.11011 |
| Alerta | netbios-ns (137/udp) | Os seguintes nomes NetBIOS foram recolhidos:<br>SATUX = Este é o nome do computador para os serviços de estação de trabalho registrados por um cliente WINS. SATUX = Este é o logado atualmente no usuário registrado para esta estação de trabalho. SATUX = Nome do computador. __MSBROWSE__ WORKGROUP WORKGROUP = Grupo de trabalho /Nome do domínio WORKGROUP = Grupo de trabalho /Nome do domínio Se você não quer que qualquer um encontre o nome NetBios do seu computador, você deverá filtrar todo o trafico nesta porta. Fator de risco: Médio. CVE : CAN-1999-0621 OpenVAS ID : 1.3.6.1.4.1.25623.1.0.10150 |
| Vulnerabilidade | general/tcp | Visão geral: O hospedeiro tem um ANI parser que no Windows é propenso a falha de Negação de Serviço DoS.<br>Vulnerabilidade:<br>Devido uma falha de verificação dos limites do processamento .Ani, um processo que é criado com essa flag quando um usuário é induzido a abrir um arquivo que contêm um código malicioso. Isso leva o sistema a consumir uma quantidade muito grande de memória |

| | | |
|---|---|---|
| | | causando lentidão no servidor ou fora do ar. Impacto: negação de serviço a usuários legítimos. Nível de Impacto: Aplicação Sistema Operacional afetado por essa falha: Microsoft Windows 2000 SP4 e versões anteriores. Microsoft Windows XP SP3 e versões anteriores. Microsoft Windows 2003 SP2 e versões anteriores. Correção: Sem solução ou patch disponível em 29 de março de 2013.Informações sobre a correção da falha e quando estará disponível para para consulta: http://www.microsoft.com/en/us/default.aspx Referências: http://xforce.iss.net/xforce/xfdb/56756 |
| http://code.google.com/p/skylined/issues/detail?id=3 http://skypher.com/index.php/2013/03/08/ani-file-bitmapinfoheader-biclrused-bounds-check-missing/ CVE : CVE-2013-1098 BID : 38579 OpenVAS ID : 1.3.6.1.4.1.25623.1.0.902033 | | |
| Informação | general/tcp | ICMP baseado nas impressões digitais do Sistema Operacional: Linux Kernel 2.6.11 (accuracy 100%) Linux Kernel 2.6.10 (accuracy 100%) Linux Kernel 2.6.9 (accuracy 100%) Linux Kernel 2.6.8 (accuracy 100%) Linux Kernel 2.6.7 (accuracy 100%) Linux Kernel 2.6.6 (accuracy 100%) Linux Kernel 2.6.5 (accuracy 100%) Linux Kernel 2.6.4 (accuracy 100%) Linux Kernel 2.6.3 (accuracy 100%) Linux Kernel 2.6.2 (accuracy 100%) Linux Kernel 2.6.1 (accuracy 100%) Linux Kernel 2.6.0 (accuracy 100%) Linux Kernel 2.4.30 (accuracy 100%) Linux Kernel 2.4.29 (accuracy 100%) Linux Kernel 2.4.28 (accuracy 100%) Linux Kernel 2.4.27 (accuracy 100%) Linux Kernel 2.4.26 (accuracy 100%) Linux Kernel 2.4.25 (accuracy 100%) Linux Kernel 2.4.24 (accuracy 100%) Linux Kernel 2.4.23 (accuracy 100%) Linux Kernel 2.4.22 (accuracy 100%) Linux Kernel 2.4.21 (accuracy 100%) Linux Kernel 2.4.20 (accuracy 100%) Linux Kernel 2.4.19 (accuracy 100%) Linux Kernel 2.0.36 (accuracy 100%) Linux Kernel 2.0.34 (accuracy 100%) Linux Kernel 2.0.30 (accuracy 100%) OpenVAS ID : 1.3.6.1.4.1.25623.1.0.102002 |

| | | |
|---|---|---|
| Informação | general/tcp | Informações sobre esta varredura : OpenVAS versão : 2.0.1 Plugin feed version : 201304091315 Type of plugin feed : OpenVAS NVT Feed Scanner IP : 10.113.1.111 Port range : default Thorough tests : no Experimental tests : no Paranoia level : 1 Report Verbosity : 1 Safe checks : yes Max hosts : 20 Max checks : 4 Scan duration : unknown (ping_host.nasl not launched?) OpenVAS ID : 1.3.6.1.4.1.25623.1.0.19506 |
| Alerta | xdmcp (177/udp) | A estação remota esta executando o XDMCP.<br>Este protocolo é usado por provedores de janelamento para conexões com terminais.<br>XDMCP é completamente inseguro, uma vez que todo o trafego não é encriptado.<br>Podendo expor informações de login ou senha.<br>Um atacante pode usar essa falha para capturar todas as teclas de uma estação através de seu terminal X, incluindo senhas.<br>XDMCP também é um mecanismo de login adicionais que você pode ou não estar ciente foi habilitado. Solução : Desativa XDMCP Fator de risco : Médio OpenVAS ID : 1.3.6.1.4.1.25623.1.0.10891 |
| Informação | x11 (6000/tcp) | O servidor X não permite a conexão de clientes no servidor<br>Porém é recomendado filtrar as conexões desta porta. Um atacante poderá enviar dados inúteis reduzindo o desempenho de sua sessão X ou até causar uma queda do servidor. Aqui está a versão do servidor : 11.0 Solução : filtrar o trafego nas portas do intervalo 6000-6009. Fator de risco : Baixo. OpenVAS ID : 1.3.6.1.4.1.25623.1.0.10407 |
| Informação | general/SMBClient | Versão do Sistema Operacional = UNIX Dominio = WORKGROUP Verção do Samba= SAMBA 3.0.24 OpenVAS ID : 1.3.6.1.4.1.25623.1.0.90011 |

Teste de acesso a um servidor externo

```
Starting Nmap 5.21 ( http://nmap.org ) at 2010-05-05 21:13 BRT
Nmap scan report for 201-43-199-168.dsl.telesp.net.br (201.43.199.168)
Host is up (0.091s latency).
```

PORT STATE SERVICE

1/tcp open tcpmux
2/tcp open compressnet
3/tcp open compressnet
4/tcp open unknown
5/tcp open unknown
6/tcp open unknown
7/tcp open echo
8/tcp open unknown
9/tcp open discard
10/tcp open unknown
11/tcp open systat
12/tcp open unknown
13/tcp open daytime
14/tcp open unknown
15/tcp open netstat
16/tcp open unknown
17/tcp open qotd
18/tcp open unknown
19/tcp open chargen
20/tcp open ftp-data
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
24/tcp open priv-mail
25/tcp filtered smtp
26/tcp open rsftp
27/tcp open nsw-fe
28/tcp open unknown
29/tcp open msg-icp
30/tcp open unknown
31/tcp open msg-auth
32/tcp open unknown
33/tcp open dsp
34/tcp open unknown
35/tcp open priv-print
36/tcp open unknown
37/tcp open time
38/tcp open rap
39/tcp open unknown
40/tcp open unknown
41/tcp open unknown
42/tcp filtered nameserver
43/tcp open whois
44/tcp open mpm-flags
45/tcp open mpm
46/tcp open unknown
47/tcp open ni-ftp
48/tcp open auditd
49/tcp open tacacs
50/tcp open re-mail-ck
51/tcp open la-maint
52/tcp open xns-time
53/tcp open domain
54/tcp open xns-ch
55/tcp open isi-gl
56/tcp open xns-auth
57/tcp open priv-term
58/tcp open xns-mail
59/tcp open priv-file
60/tcp open unknown
61/tcp open unknown
62/tcp open unknown
63/tcp open unknown
64/tcp open unknown
65/tcp open tacacs-ds
66/tcp open sqlnet
67/tcp open dhcps
68/tcp open dhcpc
69/tcp open tftp
70/tcp open gopher
71/tcp open netrjs-1
72/tcp open netrjs-2
73/tcp open netrjs-3
74/tcp open netrjs-4
75/tcp open priv-dial
76/tcp open deos
77/tcp open priv-rje
78/tcp open unknown
79/tcp open finger
80/tcp open http
81/tcp open hosts2-ns
82/tcp open xfer
83/tcp open mit-ml-dev
84/tcp open ctf
85/tcp open mit-ml-dev
86/tcp open mfcobol
87/tcp open priv-term-l
88/tcp open kerberos-sec
89/tcp open su-mit-tg
90/tcp open dnsix
91/tcp open mit-dov
92/tcp open npp
93/tcp open dcp
94/tcp open objcall
95/tcp open supdup
96/tcp open dixie
97/tcp open swift-rvf
98/tcp open linuxconf
99/tcp open metagram
100/tcp open newacct
101/tcp open hostname
102/tcp open iso-tsap
103/tcp open gppitnp
104/tcp open acr-nema
105/tcp open unknown
106/tcp open pop3pw
107/tcp open unknown
108/tcp open snagas
109/tcp open pop2
110/tcp open pop3
111/tcp open rpcbind
112/tcp open mcidas
113/tcp open auth
114/tcp open audionews
115/tcp open sftp
116/tcp open ansanotify
117/tcp open uucp-path
118/tcp open sqlserv
119/tcp open nntp
120/tcp open cfdptkt
121/tcp open unknown
122/tcp open smakynet
123/tcp open ntp
124/tcp open ansatrader
125/tcp open locus-map
126/tcp open unknown
127/tcp open locus-con
128/tcp open gss-xlicen
129/tcp open pwdgen
130/tcp open cisco-fna
131/tcp open unknown
132/tcp open cisco-sys
133/tcp open statsrv
134/tcp open unknown
135/tcp filtered msrpc
136/tcp open profile
137/tcp open netbios-ns
138/tcp open netbios-dgm
139/tcp filtered netbios-ssn
140/tcp open unknown
141/tcp open emfis-cntl
142/tcp open bl-idm
143/tcp open imap
144/tcp open news
145/tcp open unknown
146/tcp open iso-tp0
147/tcp open unknown
148/tcp open cronus
149/tcp open aed-512
150/tcp open sql-net
151/tcp open hems
152/tcp open unknown
153/tcp open unknown
154/tcp open unknown
155/tcp open unknown
156/tcp open unknown
157/tcp open knet-cmp
158/tcp open pcmail-srv
159/tcp open unknown
160/tcp open unknown
161/tcp open snmp
162/tcp open snmptrap
163/tcp open cmip-man
164/tcp open unknown
165/tcp open unknown
166/tcp open unknown
167/tcp open unknown
168/tcp open rsvd
169/tcp open unknown
170/tcp open unknown
171/tcp open unknown
172/tcp open unknown
173/tcp open xyplex-mux
174/tcp open mailq
175/tcp open unknown
176/tcp open genrad-mux
177/tcp open xdmcp
178/tcp open unknown
179/tcp open bgp
180/tcp open ris
181/tcp open unify
182/tcp open audit
183/tcp open unknown
184/tcp open ocserver
185/tcp open remote-kis
186/tcp open unknown
187/tcp open unknown
188/tcp open unknown
189/tcp open qft
190/tcp open gacp
191/tcp open prospero
192/tcp open osu-nms
193/tcp open srmp
194/tcp open irc
195/tcp open unknown
196/tcp open dn6-smm-red
197/tcp open unknown
198/tcp open unknown
199/tcp open smux
200/tcp open src
201/tcp open at-rtmp
202/tcp open at-nbp
203/tcp open unknown
204/tcp open at-echo
205/tcp open at-5
206/tcp open at-zis
207/tcp open unknown
208/tcp open unknown
209/tcp open tam
210/tcp open z39.50
211/tcp open 914c-g
212/tcp open anet
213/tcp open ipx
214/tcp open vmpwscs
215/tcp open unknown
216/tcp open atls
217/tcp open dbase
218/tcp open unknown
219/tcp open uarps
220/tcp open imap3
221/tcp open fln-spx
222/tcp open rsh-spx
223/tcp open cdc
224/tcp open unknown

```
225/tcp open unknown
226/tcp open unknown
227/tcp open unknown
228/tcp open unknown
229/tcp open unknown
230/tcp open unknown
231/tcp open unknown
232/tcp open unknown
233/tcp open unknown
234/tcp open unknown
235/tcp open unknown
236/tcp open unknown
237/tcp open unknown
238/tcp open unknown
239/tcp open unknown
240/tcp open unknown
241/tcp open unknown
242/tcp open unknown
243/tcp open unknown
244/tcp open unknown
245/tcp open unknown
246/tcp open unknown
247/tcp open unknown
248/tcp open bhfhs
249/tcp open unknown
250/tcp open unknown
251/tcp open unknown
252/tcp open unknown
253/tcp open unknown
254/tcp open unknown
255/tcp open unknown
256/tcp open fw1-
secureremote
257/tcp open fw1-mc-
fwmodule
258/tcp open fw1-mc-gui
259/tcp open esro-gen
260/tcp open openport
261/tcp open nsiiops
262/tcp open arcisdms
263/tcp open unknown
264/tcp open bgmp
265/tcp open maybe-fw1
266/tcp open unknown
267/tcp open unknown
268/tcp open unknown
269/tcp open unknown
270/tcp open unknown
271/tcp open unknown
272/tcp open unknown
273/tcp open unknown
274/tcp open unknown
275/tcp open unknown
276/tcp open unknown
277/tcp open unknown
278/tcp open unknown
279/tcp open unknown
280/tcp open http-mgmt
281/tcp open unknown
282/tcp open unknown
283/tcp open unknown
284/tcp open unknown
285/tcp open unknown
286/tcp open unknown
287/tcp open unknown
288/tcp open unknown
289/tcp open unknown
290/tcp open unknown
291/tcp open unknown
292/tcp open unknown
293/tcp open unknown
294/tcp open unknown
295/tcp open unknown
296/tcp open unknown
297/tcp open unknown
298/tcp open unknown
299/tcp open unknown
300/tcp open unknown
301/tcp open unknown
302/tcp open unknown
303/tcp open unknown
304/tcp open unknown
305/tcp open unknown
306/tcp open unknown
307/tcp open unknown
308/tcp open
novastorbakcup
309/tcp open unknown
310/tcp open unknown
311/tcp open asip-webadmin
312/tcp open unknown
313/tcp open unknown
314/tcp open unknown
315/tcp open dpsi
316/tcp open decauth
317/tcp open unknown
318/tcp open unknown
319/tcp open unknown
320/tcp open unknown
321/tcp open unknown
322/tcp open unknown
323/tcp open unknown
324/tcp open unknown
325/tcp open unknown
326/tcp open unknown
327/tcp open unknown
328/tcp open unknown
329/tcp open unknown
330/tcp open unknown
331/tcp open unknown
332/tcp open unknown
333/tcp open unknown
334/tcp open unknown
335/tcp open unknown
336/tcp open unknown
337/tcp open unknown
338/tcp open unknown
339/tcp open unknown
340/tcp open unknown
341/tcp open unknown
342/tcp open unknown
343/tcp open unknown
344/tcp open unknown
345/tcp open unknown
346/tcp open zserv
347/tcp open unknown
348/tcp open unknown
349/tcp open unknown
350/tcp open matip-type-a
351/tcp open matip-type-b
352/tcp open dtag-ste-sb
353/tcp open ndsauth
354/tcp open unknown
355/tcp open datex-asn
356/tcp open unknown
357/tcp open unknown
358/tcp open shrinkwrap
359/tcp open unknown
360/tcp open scoi2odialog
361/tcp open semantix
362/tcp open srssend
363/tcp open unknown
364/tcp open aurora-cmgr
365/tcp open unknown
366/tcp open odmr
367/tcp open unknown
368/tcp open unknown
369/tcp open rpc2portmap
370/tcp open codaauth2
371/tcp open unknown
372/tcp open unknown
373/tcp open legent-1
374/tcp open unknown
375/tcp open unknown
376/tcp open unknown
377/tcp open unknown
378/tcp open unknown
379/tcp open unknown
380/tcp open is99s
381/tcp open unknown
382/tcp open unknown
383/tcp open hp-alarm-mgr
384/tcp open unknown

385/tcp open unknown
386/tcp open unknown
387/tcp open unknown
388/tcp open unidata-ldm
389/tcp open ldap
390/tcp open unknown
391/tcp open synotics-
relay
392/tcp open synotics-
broker
393/tcp open unknown
394/tcp open unknown
395/tcp open unknown
396/tcp open unknown
397/tcp open mptn
398/tcp open unknown
399/tcp open iso-tsap-c2
400/tcp open work-sol
401/tcp open ups
402/tcp open genie
403/tcp open decap
404/tcp open nced
405/tcp open unknown
406/tcp open imsp
407/tcp open timbuktu
408/tcp open prm-sm
409/tcp open unknown
410/tcp open decladebug
411/tcp open rmt
412/tcp open synoptics-
trap
413/tcp open smsp
414/tcp open infoseek
415/tcp open bnet
416/tcp open silverplatter
417/tcp open onmux
418/tcp open hyper-g
419/tcp open ariel1
420/tcp open smpte
421/tcp open unknown
422/tcp open ariel3
423/tcp open opc-job-start
424/tcp open unknown
425/tcp open icad-el
426/tcp open unknown
427/tcp open svrloc
428/tcp open ocs_cmu
429/tcp open unknown
430/tcp open unknown
431/tcp open unknown
432/tcp open iasd
433/tcp open unknown
434/tcp open mobileip-
agent
435/tcp open mobilip-mn
436/tcp open unknown
437/tcp open comscm
438/tcp open dsfgw
439/tcp open dasp
440/tcp open sgcp
441/tcp open decvms-sysmgt
442/tcp open cvc_hostd
443/tcp open https
444/tcp open snpp
445/tcp filtered
microsoft-ds
446/tcp open ddm-rdb
```

```
447/tcp open ddm-dfm
448/tcp open ddm-ssl
449/tcp open as-servermap
450/tcp open tserver
451/tcp open sfs-smp-net
452/tcp open sfs-config
453/tcp open
creativeserver
454/tcp open contentserver
455/tcp open unknown
456/tcp open macon
457/tcp open scohelp
458/tcp open appleqtc
459/tcp open unknown
460/tcp open skronk
461/tcp open unknown
462/tcp open
datasurfsrvsec
463/tcp open unknown
464/tcp open kpasswd5
465/tcp open smtps
466/tcp open digital-vrc
467/tcp open unknown
468/tcp open unknown
469/tcp open unknown
470/tcp open scx-proxy
471/tcp open unknown
472/tcp open ljk-login
473/tcp open hybrid-pop
474/tcp open unknown
475/tcp open tcpnethaspsrv
476/tcp open unknown
477/tcp open unknown
478/tcp open unknown
479/tcp open iafserver
480/tcp open loadsrv
481/tcp open dvs
482/tcp open unknown
483/tcp open unknown
484/tcp open unknown
485/tcp open powerburst
486/tcp open sstats
487/tcp open saft
488/tcp open unknown
489/tcp open unknown
490/tcp open unknown
491/tcp open go-login
492/tcp open ticf-1
493/tcp open ticf-2
494/tcp open unknown
495/tcp open unknown
496/tcp open pim-rp-disc
497/tcp open retrospect
498/tcp open unknown
499/tcp open unknown
500/tcp open isakmp
501/tcp open stmf
502/tcp open asa-appl-
proto
503/tcp open unknown
504/tcp open unknown
505/tcp open mailbox-lm
506/tcp open unknown
507/tcp open crs
508/tcp open unknown
509/tcp open snare
510/tcp open fcp
511/tcp open passgo
512/tcp open exec
513/tcp open login
514/tcp open shell
515/tcp open printer
516/tcp open videotex
517/tcp open unknown
518/tcp open ntalk
519/tcp open unknown
520/tcp open unknown
521/tcp open unknown
522/tcp open ulp
523/tcp open ibm-db2
524/tcp open ncp
525/tcp open timed
526/tcp open tempo
527/tcp open unknown
528/tcp open custix
529/tcp open unknown
530/tcp open courier
531/tcp open unknown
532/tcp open unknown
533/tcp open netwall
534/tcp open unknown
535/tcp open iiop
536/tcp open opalis-rdv
537/tcp open unknown
538/tcp open gdomap
539/tcp open unknown
540/tcp open uucp
541/tcp open uucp-rlogin
542/tcp open commerce
543/tcp open klogin
544/tcp open kshell
545/tcp open ekshell
546/tcp open unknown
547/tcp open unknown
548/tcp open afp
549/tcp open unknown
550/tcp open unknown
551/tcp open unknown
552/tcp open deviceshare
553/tcp open pirp
554/tcp open rtsp
555/tcp open dsf
556/tcp open remotefs
557/tcp open openvms-
sysipc
558/tcp open unknown
559/tcp open unknown
560/tcp open rmonitor
561/tcp open monitor
562/tcp open unknown
563/tcp open snews
564/tcp open 9pfs
565/tcp open unknown
566/tcp open unknown
567/tcp open unknown
568/tcp open ms-shuttle
569/tcp open ms-rome
570/tcp open meter
571/tcp open umeter
572/tcp open sonar
573/tcp open unknown
574/tcp open unknown
575/tcp open unknown
576/tcp open unknown
577/tcp open vnas
578/tcp open ipdd
579/tcp open unknown
580/tcp open unknown

581/tcp open unknown
582/tcp open scc-security
583/tcp open philips-vc
584/tcp open unknown
585/tcp open unknown
586/tcp open unknown
587/tcp open submission
588/tcp open unknown
589/tcp open unknown
590/tcp open unknown
591/tcp open http-alt
592/tcp open unknown
593/tcp filtered http-rpc-
epmap
594/tcp open unknown
595/tcp open unknown
596/tcp open smsd
597/tcp open unknown
598/tcp open sco-
websrvrmg3
599/tcp open acp
600/tcp open ipcserver
601/tcp open unknown
602/tcp open unknown
603/tcp open mnotes
604/tcp open unknown
605/tcp open unknown
606/tcp open urm
607/tcp open nqs
608/tcp open sift-uft
609/tcp open npmp-trap
610/tcp open npmp-local
611/tcp open npmp-gui
612/tcp open unknown
613/tcp open unknown
614/tcp open unknown
615/tcp open unknown
616/tcp open unknown
617/tcp open sco-dtmgr
618/tcp open unknown
619/tcp open unknown
620/tcp open unknown
621/tcp open unknown
622/tcp open unknown
623/tcp open unknown
624/tcp open unknown
625/tcp open apple-xsrvr-
admin
626/tcp open apple-imap-
admin
627/tcp open unknown
628/tcp open qmqp
629/tcp open unknown
630/tcp open unknown
631/tcp open ipp
632/tcp open unknown
633/tcp open unknown
634/tcp open ginad
635/tcp open unknown
636/tcp open ldapssl
637/tcp open lanserver
638/tcp open unknown
639/tcp open unknown
640/tcp open unknown
641/tcp open unknown
642/tcp open unknown
643/tcp open unknown
644/tcp open unknown
645/tcp open unknown
646/tcp open ldp
647/tcp open unknown
648/tcp open unknown
649/tcp open unknown
650/tcp open unknown
651/tcp open unknown
652/tcp open unknown
653/tcp open unknown
654/tcp open unknown
655/tcp open unknown
656/tcp open unknown
657/tcp open unknown
658/tcp open unknown
659/tcp open unknown
660/tcp open mac-srvr-
admin
661/tcp open unknown
662/tcp open unknown
663/tcp open unknown
664/tcp open secure-aux-
bus
665/tcp open unknown
666/tcp open doom
```

```
667/tcp open unknown
668/tcp open unknown
669/tcp open unknown
670/tcp open unknown
671/tcp open unknown
672/tcp open unknown
673/tcp open unknown
674/tcp open acap
675/tcp open unknown
676/tcp open unknown
677/tcp open unknown
678/tcp open unknown
679/tcp open unknown
680/tcp open unknown
681/tcp open unknown
682/tcp open unknown
683/tcp open corba-iiop
684/tcp open unknown
685/tcp open unknown
686/tcp open unknown
687/tcp open unknown
688/tcp open unknown
689/tcp open unknown
690/tcp open unknown
691/tcp open resvc
692/tcp open unknown
693/tcp open unknown
694/tcp open unknown
695/tcp open unknown
696/tcp open unknown
697/tcp open unknown
698/tcp open unknown
699/tcp open unknown
700/tcp open unknown
701/tcp open unknown
702/tcp open unknown
703/tcp open unknown
704/tcp open elcsd
705/tcp open unknown
706/tcp open silc
707/tcp open unknown
708/tcp open unknown
709/tcp open
entrustmanager
710/tcp open unknown
711/tcp open unknown
712/tcp open unknown
713/tcp open unknown
714/tcp open unknown
715/tcp open unknown
716/tcp open unknown
717/tcp open unknown
718/tcp open unknown
719/tcp open unknown
720/tcp open unknown
721/tcp open unknown
722/tcp open unknown
723/tcp open omfs
724/tcp open unknown
725/tcp open unknown
726/tcp open unknown
727/tcp open unknown
728/tcp open unknown
729/tcp open netviewdm1
730/tcp open netviewdm2
731/tcp open netviewdm3
732/tcp open unknown
733/tcp open unknown
734/tcp open unknown
735/tcp open unknown
736/tcp open unknown
737/tcp open unknown
738/tcp open unknown
739/tcp open unknown
740/tcp open netcp
741/tcp open netgw
742/tcp open netrcs
743/tcp open unknown
744/tcp open flexlm
745/tcp open unknown
746/tcp open unknown
747/tcp open fujitsu-dev
748/tcp open ris-cm
749/tcp open kerberos-adm
750/tcp open kerberos
751/tcp open
kerberos_master
752/tcp open qrh
753/tcp open rrh
754/tcp open krb_prop
755/tcp open unknown
756/tcp open unknown
757/tcp open unknown
758/tcp open nlogin
759/tcp open con
760/tcp open krbupdate
761/tcp open kpasswd
762/tcp open quotad
763/tcp open cycleserv
764/tcp open omserv
765/tcp open webster
766/tcp open unknown
767/tcp open phonebook
768/tcp open unknown
769/tcp open vid
770/tcp open cadlock
771/tcp open rtip
772/tcp open unknown
773/tcp open submit
774/tcp open rpasswd
775/tcp open entomb
776/tcp open wpages
777/tcp open unknown
778/tcp open unknown
779/tcp open unknown
780/tcp open wpgs
781/tcp open hp-collector
782/tcp open hp-managed-
node
783/tcp open spamassassin

784/tcp open unknown
785/tcp open unknown
786/tcp open concert
787/tcp open qsc
788/tcp open unknown
789/tcp open unknown
790/tcp open unknown
791/tcp open unknown
792/tcp open unknown
793/tcp open unknown
794/tcp open unknown
795/tcp open unknown
796/tcp open unknown
797/tcp open unknown
798/tcp open unknown
799/tcp open controlit
800/tcp open mdbs_daemon
801/tcp open device
802/tcp open unknown
803/tcp open unknown
804/tcp open unknown
805/tcp open unknown
806/tcp open unknown
807/tcp open unknown
808/tcp open ccproxy-http
809/tcp open unknown
810/tcp open unknown
811/tcp open unknown
812/tcp open unknown
813/tcp open unknown
814/tcp open unknown
815/tcp open unknown
816/tcp open unknown
817/tcp open unknown
818/tcp open unknown
819/tcp open unknown
820/tcp open unknown
821/tcp open unknown
822/tcp open unknown
823/tcp open unknown
824/tcp open unknown
825/tcp open unknown
826/tcp open unknown
827/tcp open unknown
828/tcp open unknown
829/tcp open unknown
830/tcp open unknown
831/tcp open unknown
832/tcp open unknown
833/tcp open unknown
834/tcp open unknown
835/tcp open unknown
836/tcp open unknown
837/tcp open unknown
838/tcp open unknown
839/tcp open unknown
840/tcp open unknown
841/tcp open unknown
842/tcp open unknown
843/tcp open unknown
844/tcp open unknown
845/tcp open unknown
846/tcp open unknown
847/tcp open unknown
848/tcp open unknown
849/tcp open unknown
850/tcp open unknown
851/tcp open unknown
852/tcp open unknown
853/tcp open unknown
854/tcp open unknown
855/tcp open unknown
856/tcp open unknown
857/tcp open unknown
858/tcp open unknown
859/tcp open unknown
860/tcp open unknown
861/tcp open unknown
862/tcp open unknown
863/tcp open unknown
864/tcp open unknown
865/tcp open unknown
866/tcp open unknown
867/tcp open unknown
868/tcp open unknown
869/tcp open unknown
870/tcp open unknown
871/tcp open supfilesrv
872/tcp open unknown
873/tcp open rsync
874/tcp open unknown
875/tcp open unknown
876/tcp open unknown
877/tcp open unknown
878/tcp open unknown
879/tcp open unknown
880/tcp open unknown
881/tcp open unknown
882/tcp open unknown
883/tcp open unknown
884/tcp open unknown
885/tcp open unknown
886/tcp open unknown
887/tcp open unknown
888/tcp open accessbuilder
889/tcp open unknown
890/tcp open unknown
891/tcp open unknown
892/tcp open unknown
893/tcp open unknown
```

```
894/tcp open unknown
895/tcp open unknown
896/tcp open unknown
897/tcp open unknown
898/tcp open sun-
manageconsole
899/tcp open unknown
900/tcp open unknown
901/tcp open samba-swat
902/tcp open iss-
realsecure
903/tcp open iss-console-
mgr
904/tcp open unknown
905/tcp open unknown
906/tcp open unknown
907/tcp open unknown
908/tcp open unknown
909/tcp open unknown
910/tcp open unknown
911/tcp open unknown
912/tcp open unknown
913/tcp open unknown
914/tcp open unknown
915/tcp open unknown
916/tcp open unknown
917/tcp open unknown
918/tcp open unknown
919/tcp open unknown
920/tcp open unknown
921/tcp open unknown
922/tcp open unknown
923/tcp open unknown
924/tcp open unknown
925/tcp open unknown
926/tcp open unknown
927/tcp open unknown
928/tcp open unknown
929/tcp open unknown
930/tcp open unknown
931/tcp open unknown
932/tcp open unknown
933/tcp open unknown
934/tcp open unknown
935/tcp open unknown
936/tcp open unknown
937/tcp open unknown
938/tcp open unknown
939/tcp open unknown
940/tcp open unknown
941/tcp open unknown
942/tcp open unknown
943/tcp open unknown
944/tcp open unknown
945/tcp open unknown
946/tcp open unknown
947/tcp open unknown
948/tcp open unknown
949/tcp open unknown
950/tcp open oftep-rpc
951/tcp open unknown
952/tcp open unknown
953/tcp open rndc
954/tcp open unknown
955/tcp open unknown
956/tcp open unknown
957/tcp open unknown
958/tcp open unknown
959/tcp open unknown
960/tcp open unknown
961/tcp open unknown
962/tcp open unknown
963/tcp open unknown
964/tcp open unknown
965/tcp open unknown
966/tcp open unknown
967/tcp open unknown
968/tcp open unknown
969/tcp open unknown
970/tcp open unknown
971/tcp open unknown
972/tcp open unknown
973/tcp open unknown
974/tcp open unknown
975/tcp open securenetpro-
sensor
976/tcp open unknown
977/tcp open unknown
978/tcp open unknown
979/tcp open unknown
980/tcp open unknown
981/tcp open unknown
982/tcp open unknown
983/tcp open unknown
984/tcp open unknown
985/tcp open unknown
986/tcp open unknown
987/tcp open unknown
988/tcp open unknown
989/tcp open ftps-data
990/tcp open ftps
991/tcp open unknown
992/tcp open telnets
993/tcp open imaps
994/tcp open ircs
995/tcp open pop3s
996/tcp open xtreelic
997/tcp open maitrd
998/tcp open busboy
999/tcp open garcon
1000/tcp open cadlock
1001/tcp open unknown
1002/tcp open windows-icfw
1003/tcp open unknown
1004/tcp open unknown
1005/tcp open unknown

1006/tcp open unknown
1007/tcp open unknown
1008/tcp open ufsd
1009/tcp open unknown
1010/tcp open unknown
1011/tcp open unknown
1012/tcp open unknown
1013/tcp open unknown
1014/tcp open unknown
1015/tcp open unknown
1016/tcp open unknown
1017/tcp open unknown
1018/tcp open unknown
1019/tcp open unknown
1020/tcp open unknown
1021/tcp closed unknown
1022/tcp closed unknown
1023/tcp closed
netvenuechat
1024/tcp closed kdm
Nmap done: 1 IP address (1
host up) scanned in 18.60
seconds
```

ESTABELECIMENTO B

Teste com Nmap
Nome da rede: GuestLan

```
Starting Nmap 5.21 ( http://nmap.org ) at 2013-04-05 13:56 BRT
Nmap scan report for 150.163.64.50
Host is up (0.0072s latency).
Not shown: 99 filtered ports
PORT STATE SERVICE
80/tcp open http
MAC Address: 00:1F:5B:B7:FE:1E (Apple)
Nmap scan report for 150.163.64.198
Host is up (0.000015s latency).
All 100 scanned ports on 150.163.64.198 are closed
Nmap scan report for 150.163.64.253
Host is up (0.0096s latency).
Not shown: 99 filtered ports
PORT STATE SERVICE
80/tcp open http
MAC Address: 00:21:A0:37:DD:E7 (Cisco Systems)
Nmap scan report for 150.163.64.254
Host is up (0.013s latency).
Not shown: 98 filtered ports
PORT STATE SERVICE
53/tcp closed domain
80/tcp open http
MAC Address: 00:1A:30:FB:44:00 (Cisco Systems)
Nmap done: 256 IP addresses (4 hosts up) scanned in 10.80 seconds
```

Teste com Zenmap

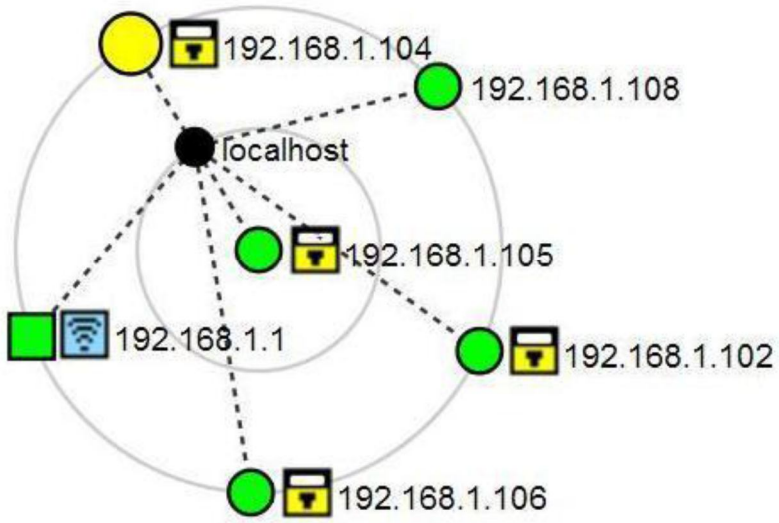



**Figura 2 – Topologia sugerida para a estabelecimento**

Teste de acesso a um servidor externo

```
Starting Nmap 5.21 ( http://nmap.org ) at 2013-05-10 14:24 BRT
Initiating Parallel DNS resolution of 1 host. at 14:24
Completed Parallel DNS resolution of 1 host. at 14:24, 3.39s elapsed
Initiating SYN Stealth Scan at 14:24
Scanning 200-207-145-218.dsl.telesp.net.br (200.207.145.218) [1024 ports]
Discovered open port 80/tcp on 200.207.145.218
Discovered open port 53/tcp on 200.207.145.218
Completed SYN Stealth Scan at 14:25, 15.02s elapsed (1024 total ports)
Nmap scan report for 200-207-145-218.dsl.telesp.net.br (200.207.145.218)
Host is up (0.046s latency).
Not shown: 1022 filtered ports
PORT STATE SERVICE
53/tcp open domain
80/tcp open http
Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 18.55 seconds
Raw packets sent: 2055 (90.420KB) | Rcvd: 38 (1672B).
```

ESTABELECIMENTO C

Teste com Nmap

```
Starting Nmap 4.85BETA10 ( http://nmap.org ) at 2013-04-03 13:04 BRT
Interesting ports on 192.168.1.1:
Not shown: 97 filtered ports
PORT STATE SERVICE
21/tcp closed ftp
23/tcp closed telnet
80/tcp open http
MAC Address: 00:1A:70:7C:B8:FA (Cisco-Linksys)
Device type: WAP|broadband router
Running: Linksys embedded, Netgear embedded, Netgear VxWorks 5.X
OS details: Linksys WRT54G or WRT54G2, or Netgear WGR614 or WPN824v2
wireless broadband router, Netgear WGT624 WAP, Netgear WGR614v7,
WGT624v3, or WPN824v2 WAP (VxWorks 5.4.2)
Network Distance: 1 hop
All 100 scanned ports on 192.168.1.103 are filtered
MAC Address: 00:1D:7D:FF:0A:21 (Giga-byte Technology Co.)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
All 100 scanned ports on 192.168.1.132 are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops
OS detection performed. Please report any incorrect results at
http://nmap.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 11.81 seconds
```

Teste com Zenmap

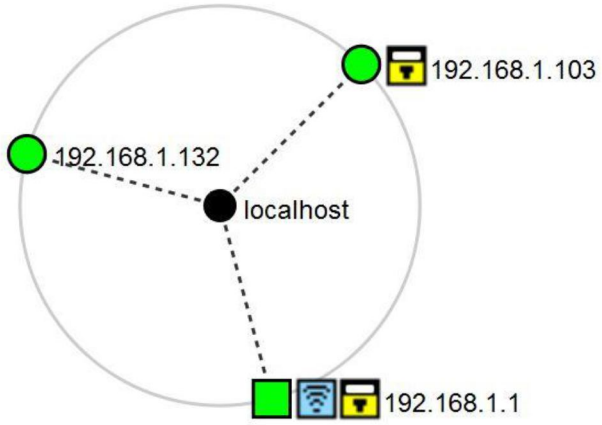



**Figura 3 – Tologia lógica sugerida da rede do estabelecimento C.**

Teste de acesso a um servidor externo

```
Starting Nmap 5.21 ( http://nmap.org ) at 2013-05-08 11:16 BRT
Nmap scan report for 189-54-228-124-nd.cpe.vivax.com.br (189.54.228.124)
Host is up (0.062s latency).
                          Not shown: 110 closed ports
```

```
1/tcp open tcpmux
3/tcp open compressnet
4/tcp open unknown
6/tcp open unknown
8/tcp open unknown
9/tcp open discard
10/tcp open unknown
11/tcp open systat
13/tcp open daytime
14/tcp open unknown
15/tcp open netstat
16/tcp open unknown
18/tcp open unknown
19/tcp open chargen
20/tcp open ftp-data
21/tcp filtered ftp
22/tcp open ssh
23/tcp open telnet
24/tcp open priv-mail
25/tcp filtered smtp
26/tcp open rsftp
27/tcp open nsw-fe
28/tcp open unknown
29/tcp open msg-icp
30/tcp open unknown
32/tcp open unknown
33/tcp open dsp
34/tcp open unknown
35/tcp open priv-print
36/tcp open unknown
37/tcp open time
38/tcp open rap
39/tcp open unknown
40/tcp open unknown
41/tcp open unknown
42/tcp open nameserver
43/tcp open whois
44/tcp open mpm-flags
45/tcp open mpm
46/tcp open unknown
47/tcp open ni-ftp
48/tcp open auditd
49/tcp open tacacs
50/tcp open re-mail-ck
52/tcp open xns-time
53/tcp open domain
54/tcp open xns-ch
55/tcp open isi-gl
56/tcp open xns-auth
58/tcp open xns-mail
59/tcp open priv-file
60/tcp open unknown
61/tcp open unknown
62/tcp open unknown
63/tcp open unknown
64/tcp open unknown
65/tcp open tacacs-ds
66/tcp open sqlnet
67/tcp open dhcps
68/tcp open dhcpc
69/tcp open tftp
70/tcp open gopher
71/tcp open netrjs-1
72/tcp open netrjs-2
73/tcp open netrjs-3
74/tcp open netrjs-4
75/tcp open priv-dial
77/tcp open priv-rje
78/tcp open unknown
79/tcp open finger
80/tcp filtered http
81/tcp open hosts2-
ns
82/tcp open xfer
83/tcp open mit-ml-dev
84/tcp open ctf
86/tcp open mfcobol
87/tcp open priv-term-l
88/tcp open kerberos-sec
89/tcp open su-mit-tg
91/tcp open mit-dov
92/tcp open npp
94/tcp open objcall
95/tcp open supdup
97/tcp open swift-rvf
98/tcp open linuxconf
99/tcp open metagram
100/tcp open newacct
101/tcp open hostname
102/tcp open iso-tsap
104/tcp open acr-nema
105/tcp open unknown
108/tcp open snagas
109/tcp open pop2
110/tcp open pop3
111/tcp open rpcbind
112/tcp open mcidas
113/tcp open auth
114/tcp open audionews
115/tcp open sftp
116/tcp open ansanotify
117/tcp open uucp-path
118/tcp open sqlserv
119/tcp open nntp
120/tcp open cfdptkt
121/tcp open unknown
123/tcp open ntp
124/tcp open ansatrader
125/tcp open locus-map
126/tcp open unknown
127/tcp open locus-con
128/tcp open gss-xlicen
129/tcp open pwdgen
130/tcp open cisco-fna
131/tcp open unknown
132/tcp open cisco-sys
133/tcp open statsrv
134/tcp open unknown
135/tcp filtered msrpc
136/tcp filtered profile
137/tcp filtered netbios-
ns
138/tcp filtered netbios-
dgm
139/tcp filtered netbios-
ssn
140/tcp open unknown
141/tcp open emfis-cntl
143/tcp open imap
144/tcp open news
145/tcp open unknown
147/tcp open unknown
148/tcp open cronus
149/tcp open aed-512
150/tcp open sql-net
151/tcp open hems
152/tcp open unknown
153/tcp open unknown
154/tcp open unknown
155/tcp open unknown
156/tcp open unknown
157/tcp open knet-cmp
158/tcp open pcmail-srv
159/tcp open unknown
160/tcp open unknown
161/tcp open snmp
162/tcp open snmptrap
163/tcp open cmip-man
164/tcp open unknown
165/tcp open unknown
166/tcp open unknown
167/tcp open unknown
168/tcp open rsvd
169/tcp open unknown
170/tcp open unknown
171/tcp open unknown
172/tcp open unknown
173/tcp open xyplex-mux
174/tcp open mailq
175/tcp open unknown
177/tcp open xdmcp
178/tcp open unknown
179/tcp open bgp
180/tcp open ris
181/tcp open unify
182/tcp open audit
183/tcp open unknown
184/tcp open ocserver
185/tcp open remote-kis
186/tcp open unknown
188/tcp open unknown
189/tcp open qft
190/tcp open gacp
191/tcp open prospero
192/tcp open osu-nms
194/tcp open irc
195/tcp open unknown
196/tcp open dn6-smm-red
198/tcp open unknown
199/tcp open smux
201/tcp open at-rtmp
202/tcp open at-nbp
203/tcp open unknown
204/tcp open at-echo
205/tcp open at-5
206/tcp open at-zis
207/tcp open unknown
208/tcp open unknown
209/tcp open tam
210/tcp open z39.50
211/tcp open 914c-g
212/tcp open anet
213/tcp open ipx
214/tcp open vmpwscs
215/tcp open unknown
216/tcp open atls
218/tcp open unknown
219/tcp open uarps
220/tcp open imap3
221/tcp open fln-spx
222/tcp open rsh-spx
223/tcp open cdc
224/tcp open unknown
225/tcp open unknown
226/tcp open unknown
227/tcp open unknown
228/tcp open unknown
229/tcp open unknown
230/tcp open unknown
231/tcp open unknown
232/tcp open unknown
233/tcp open unknown
234/tcp open unknown
235/tcp open unknown
236/tcp open unknown
237/tcp open unknown
238/tcp open unknown
239/tcp open unknown
240/tcp open unknown
241/tcp open unknown
242/tcp open unknown
244/tcp open unknown
245/tcp open unknown
246/tcp open unknown
247/tcp open unknown
249/tcp open unknown
250/tcp open unknown
252/tcp open unknown
253/tcp open unknown
254/tcp open unknown
255/tcp open unknown
```

```
256/tcp open fw1-
secureremote
257/tcp open fw1-mc-
fwmodule
258/tcp open fw1-mc-gui
259/tcp open esro-gen
260/tcp open openport
261/tcp open nsiiops
262/tcp open arcisdms
263/tcp open unknown
264/tcp open bgmp
265/tcp open maybe-fw1
266/tcp open unknown
267/tcp open unknown
268/tcp open unknown
269/tcp open unknown
270/tcp open unknown
271/tcp open unknown
272/tcp open unknown
273/tcp open unknown
274/tcp open unknown
275/tcp open unknown
276/tcp open unknown
277/tcp open unknown
278/tcp open unknown
279/tcp open unknown
281/tcp open unknown
282/tcp open unknown
283/tcp open unknown
284/tcp open unknown
285/tcp open unknown
286/tcp open unknown
287/tcp open unknown
289/tcp open unknown
290/tcp open unknown
291/tcp open unknown
292/tcp open unknown
293/tcp open unknown
295/tcp open unknown
296/tcp open unknown
297/tcp open unknown
298/tcp open unknown
299/tcp open unknown
300/tcp open unknown
301/tcp open unknown
302/tcp open unknown
303/tcp open unknown
304/tcp open unknown
305/tcp open unknown
306/tcp open unknown
307/tcp open unknown
308/tcp open
novastorbakcup
309/tcp open unknown
310/tcp open unknown
311/tcp open asip-webadmin
312/tcp open unknown
313/tcp open unknown
314/tcp open unknown
315/tcp open dpsi
316/tcp open decauth
317/tcp open unknown
318/tcp open unknown
319/tcp open unknown
320/tcp open unknown
321/tcp open unknown
322/tcp open unknown
323/tcp open unknown
324/tcp open unknown
325/tcp open unknown
326/tcp open unknown
328/tcp open unknown
329/tcp open unknown
331/tcp open unknown
332/tcp open unknown
333/tcp open unknown
334/tcp open unknown
335/tcp open unknown
336/tcp open unknown
337/tcp open unknown
338/tcp open unknown
339/tcp open unknown
340/tcp open unknown
341/tcp open unknown
342/tcp open unknown
345/tcp open unknown
347/tcp open unknown
348/tcp open unknown
349/tcp open unknown
351/tcp open matip-type-b
352/tcp open dtag-ste-sb
353/tcp open ndsauth
354/tcp open unknown
355/tcp open datex-asn
356/tcp open unknown
357/tcp open unknown
358/tcp open shrinkwrap
359/tcp open unknown
360/tcp open scoi2odialog
361/tcp open semantix
363/tcp open unknown
364/tcp open aurora-cmgr
365/tcp open unknown
366/tcp open odmr
367/tcp open unknown
368/tcp open unknown
369/tcp open rpc2portmap
370/tcp open codaauth2
371/tcp open unknown
372/tcp open unknown
374/tcp open unknown
375/tcp open unknown
376/tcp open unknown
377/tcp open unknown
378/tcp open unknown
379/tcp open unknown
380/tcp open is99s
381/tcp open unknown
382/tcp open unknown
383/tcp open hp-alarm-mgr
384/tcp open unknown
385/tcp open unknown
386/tcp open unknown
387/tcp open unknown
389/tcp open ldap
390/tcp open unknown
391/tcp open synotics-
relay
392/tcp open synotics-
broker
393/tcp open unknown
394/tcp open unknown
395/tcp open unknown
396/tcp open unknown
397/tcp open mptn
398/tcp open unknown
399/tcp open iso-tsap-c2
400/tcp open work-sol
401/tcp open ups
402/tcp open genie
403/tcp open decap
404/tcp open nced
405/tcp open unknown
406/tcp open imsp
407/tcp open timbuktu
408/tcp open prm-sm
409/tcp open unknown
410/tcp open decladebug
411/tcp open rmt
412/tcp open synoptics-
trap
413/tcp open smsp
414/tcp open infoseek
415/tcp open bnet
416/tcp open silverplatter
417/tcp open onmux
419/tcp open ariel1
420/tcp open smpte
421/tcp open unknown
422/tcp open ariel3
423/tcp open opc-job-start
424/tcp open unknown
425/tcp open icad-el
426/tcp open unknown
427/tcp open svrloc
428/tcp open ocs_cmu
430/tcp open unknown
431/tcp open unknown
432/tcp open iasd
433/tcp open unknown
434/tcp open mobileip-
agent
435/tcp open mobilip-mn
436/tcp open unknown
437/tcp open comscm
438/tcp open dsfgw
439/tcp open dasp
440/tcp open sgcp
441/tcp open decvms-sysmgt
442/tcp open cvc_hostd
443/tcp open https
444/tcp open snpp
445/tcp filtered
microsoft-ds
446/tcp open ddm-rdb
447/tcp open ddm-dfm
448/tcp open ddm-ssl
449/tcp open as-servermap
450/tcp open tserver
452/tcp open sfs-config
454/tcp open contentserver
455/tcp open unknown
456/tcp open macon
458/tcp open appleqtc
459/tcp open unknown
461/tcp open unknown
462/tcp open
datasurfsrvsec
463/tcp open unknown
464/tcp open kpasswd5
465/tcp open smtps
466/tcp open digital-vrc
467/tcp open unknown
468/tcp open unknown
469/tcp open unknown
470/tcp open scx-proxy
471/tcp open unknown
472/tcp open ljk-login
473/tcp open hybrid-pop
474/tcp open unknown
475/tcp open tcpnethaspsrv
476/tcp open unknown
477/tcp open unknown
478/tcp open unknown
479/tcp open iafserver
480/tcp open loadsrv
481/tcp open dvs
482/tcp open unknown
483/tcp open unknown
484/tcp open unknown
485/tcp open powerburst
486/tcp open sstats
487/tcp open saft
488/tcp open unknown
489/tcp open unknown
490/tcp open unknown
491/tcp open go-login
492/tcp open ticf-1
493/tcp open ticf-2
494/tcp open unknown
495/tcp open unknown
```

```
496/tcp open pim-rp-disc
497/tcp open retrospect
498/tcp open unknown
499/tcp open unknown
500/tcp open isakmp
501/tcp open stmf
502/tcp open asa-appl-
proto
506/tcp open unknown
507/tcp open crs
508/tcp open unknown
509/tcp open snare
510/tcp open fcp
511/tcp open passgo
512/tcp open exec
513/tcp open login
514/tcp open shell
515/tcp open printer
517/tcp open unknown
518/tcp open ntalk
519/tcp open unknown
520/tcp open unknown
521/tcp open unknown
522/tcp open ulp
523/tcp open ibm-db2
524/tcp open ncp
525/tcp open timed
526/tcp open tempo
527/tcp open unknown
531/tcp open unknown
532/tcp open unknown
533/tcp open netwall
534/tcp open unknown
536/tcp open opalis-rdv
537/tcp open unknown
538/tcp open gdomap
539/tcp open unknown
540/tcp open uucp
541/tcp open uucp-rlogin
542/tcp open commerce
543/tcp open klogin
544/tcp open kshell
545/tcp open ekshell
546/tcp open unknown
547/tcp open unknown
548/tcp open afp
549/tcp open unknown
550/tcp open unknown
551/tcp open unknown
552/tcp open deviceshare
553/tcp open pirp
554/tcp open rtsp
555/tcp open dsf
556/tcp open remotefs
557/tcp open openvms-
sysipc
558/tcp open unknown
559/tcp open unknown
560/tcp open rmonitor
561/tcp open monitor
562/tcp open unknown
563/tcp open snews
564/tcp open 9pfs
565/tcp open unknown
566/tcp open unknown
567/tcp open unknown
568/tcp open ms-shuttle
569/tcp open ms-rome
570/tcp open meter
571/tcp open umeter
572/tcp open sonar
573/tcp open unknown
574/tcp open unknown
575/tcp open unknown
576/tcp open unknown
577/tcp open vnas
578/tcp open ipdd
579/tcp open unknown
580/tcp open unknown
581/tcp open unknown
582/tcp open scc-security
584/tcp open unknown
585/tcp open unknown
586/tcp open unknown
587/tcp open submission
588/tcp open unknown
589/tcp open unknown
590/tcp open unknown
591/tcp open http-alt
592/tcp open unknown
593/tcp open http-rpc-
epmap
594/tcp open unknown
596/tcp open smsd
597/tcp open unknown
598/tcp open sco-
websrvrmg3
600/tcp open ipcserver
601/tcp open unknown
602/tcp open unknown
607/tcp open nqs
608/tcp open sift-uft
609/tcp open npmp-trap
610/tcp open npmp-local
611/tcp open npmp-gui
612/tcp open unknown
613/tcp open unknown
614/tcp open unknown
615/tcp open unknown
616/tcp open unknown
617/tcp open sco-dtmgr
618/tcp open unknown
619/tcp open unknown
620/tcp open unknown
621/tcp open unknown
622/tcp open unknown
625/tcp open apple-xsrvr-
admin
626/tcp open apple-imap-
admin
627/tcp open unknown
629/tcp open unknown
630/tcp open unknown
632/tcp open unknown
633/tcp open unknown
634/tcp open ginad
635/tcp open unknown
636/tcp open ldapssl
637/tcp open lanserver
638/tcp open unknown
639/tcp open unknown
640/tcp open unknown
641/tcp open unknown
642/tcp open unknown
644/tcp open unknown
645/tcp open unknown
646/tcp open ldp
647/tcp open unknown
648/tcp open unknown
649/tcp open unknown
650/tcp open unknown
651/tcp open unknown
652/tcp open unknown
654/tcp open unknown
655/tcp open unknown
656/tcp open unknown
657/tcp open unknown
658/tcp open unknown
659/tcp open unknown
660/tcp open mac-srvr-
admin
661/tcp open unknown
662/tcp open unknown
663/tcp open unknown
664/tcp open secure-aux-
bus
665/tcp open unknown
666/tcp open doom
667/tcp open unknown
669/tcp open unknown
670/tcp open unknown
671/tcp open unknown
672/tcp open unknown
673/tcp open unknown
674/tcp open acap
675/tcp open unknown
677/tcp open unknown
678/tcp open unknown
679/tcp open unknown
680/tcp open unknown
681/tcp open unknown
682/tcp open unknown
683/tcp open corba-iiop
684/tcp open unknown
685/tcp open unknown
686/tcp open unknown
687/tcp open unknown
688/tcp open unknown
689/tcp open unknown
690/tcp open unknown
691/tcp open resvc
692/tcp open unknown
693/tcp open unknown
694/tcp open unknown
695/tcp open unknown
697/tcp open unknown
698/tcp open unknown
699/tcp open unknown
700/tcp open unknown
701/tcp open unknown
702/tcp open unknown
704/tcp open elcsd
705/tcp open unknown
706/tcp open silc
707/tcp open unknown
708/tcp open unknown
710/tcp open unknown
711/tcp open unknown
712/tcp open unknown
714/tcp open unknown
715/tcp open unknown
716/tcp open unknown
718/tcp open unknown
719/tcp open unknown
720/tcp open unknown
721/tcp open unknown
723/tcp open omfs
724/tcp open unknown
725/tcp open unknown
726/tcp open unknown
727/tcp open unknown
728/tcp open unknown
729/tcp open netviewdm1
730/tcp open netviewdm2
731/tcp open netviewdm3
732/tcp open unknown
733/tcp open unknown
734/tcp open unknown
736/tcp open unknown
738/tcp open unknown
739/tcp open unknown
740/tcp open netcp
741/tcp open netgw
742/tcp open netrcs
743/tcp open unknown
744/tcp open flexlm
745/tcp open unknown
746/tcp open unknown
747/tcp open fujitsu-dev
748/tcp open ris-cm
749/tcp open kerberos-adm
```

```
750/tcp open kerberos
752/tcp open qrh
753/tcp open rrh
754/tcp open krb_prop
755/tcp open unknown
756/tcp open unknown
757/tcp open unknown
758/tcp open nlogin
759/tcp open con
760/tcp open krbupdate
761/tcp open kpasswd
762/tcp open quotad
763/tcp open cycleserv
764/tcp open omserv
765/tcp open webster
766/tcp open unknown
767/tcp open phonebook
768/tcp open unknown
769/tcp open vid
770/tcp open cadlock
771/tcp open rtip
772/tcp open unknown
775/tcp open entomb
776/tcp open wpages
777/tcp open unknown
778/tcp open unknown
779/tcp open unknown
780/tcp open wpgs
781/tcp open hp-collector
782/tcp open hp-managed-
node
783/tcp open spamassassin
784/tcp open unknown
785/tcp open unknown
786/tcp open concert
787/tcp open qsc
788/tcp open unknown
789/tcp open unknown
791/tcp open unknown
792/tcp open unknown
793/tcp open unknown
794/tcp open unknown
795/tcp open unknown
797/tcp open unknown
798/tcp open unknown
799/tcp open controlit
800/tcp open mdbs_daemon
801/tcp open device
802/tcp open unknown
803/tcp open unknown
805/tcp open unknown
806/tcp open unknown
807/tcp open unknown
808/tcp open ccproxy-http
809/tcp open unknown
810/tcp open unknown
811/tcp open unknown
812/tcp open unknown
813/tcp open unknown
814/tcp open unknown
816/tcp open unknown
817/tcp open unknown
820/tcp open unknown
821/tcp open unknown
822/tcp open unknown
823/tcp open unknown
824/tcp open unknown
825/tcp open unknown
826/tcp open unknown
827/tcp open unknown
828/tcp open unknown
830/tcp open unknown
831/tcp open unknown
832/tcp open unknown
833/tcp open unknown
834/tcp open unknown
835/tcp open unknown
836/tcp open unknown
837/tcp open unknown
838/tcp open unknown
839/tcp open unknown
840/tcp open unknown
841/tcp open unknown
842/tcp open unknown
844/tcp open unknown
846/tcp open unknown
847/tcp open unknown
848/tcp open unknown
850/tcp open unknown
851/tcp open unknown
852/tcp open unknown
853/tcp open unknown
854/tcp open unknown
856/tcp open unknown
857/tcp open unknown
858/tcp open unknown
859/tcp open unknown
860/tcp open unknown
861/tcp open unknown
862/tcp open unknown
863/tcp open unknown
864/tcp open unknown
865/tcp open unknown
866/tcp open unknown
867/tcp open unknown
868/tcp open unknown
869/tcp open unknown
870/tcp open unknown
871/tcp open supfilesrv
872/tcp open unknown
873/tcp open rsync
875/tcp open unknown
876/tcp open unknown
877/tcp open unknown
878/tcp open unknown
880/tcp open unknown
881/tcp open unknown
882/tcp open unknown
885/tcp open unknown
886/tcp open unknown
887/tcp open unknown
888/tcp open accessbuilder
889/tcp open unknown
890/tcp open unknown
891/tcp open unknown
892/tcp open unknown
893/tcp open unknown
894/tcp open unknown
895/tcp open unknown
896/tcp open unknown
897/tcp open unknown
899/tcp open unknown
901/tcp open samba-swat
902/tcp open iss-
realsecure
903/tcp open iss-console-
mgr
904/tcp open unknown
906/tcp open unknown
907/tcp open unknown
908/tcp open unknown
909/tcp open unknown
910/tcp open unknown
911/tcp open unknown
912/tcp open unknown
913/tcp open unknown
915/tcp open unknown
916/tcp open unknown
917/tcp open unknown
918/tcp open unknown
919/tcp open unknown
920/tcp open unknown
921/tcp open unknown
922/tcp open unknown
923/tcp open unknown
924/tcp open unknown
925/tcp open unknown
926/tcp open unknown
929/tcp open unknown
930/tcp open unknown
931/tcp open unknown
932/tcp open unknown
933/tcp open unknown
934/tcp open unknown
935/tcp open unknown
936/tcp open unknown
937/tcp open unknown
938/tcp open unknown
939/tcp open unknown
940/tcp open unknown
941/tcp open unknown
942/tcp open unknown
943/tcp open unknown
944/tcp open unknown
945/tcp open unknown
946/tcp open unknown
947/tcp open unknown
948/tcp open unknown
949/tcp open unknown
950/tcp open oftep-rpc
951/tcp open unknown
952/tcp open unknown
953/tcp open rndc
954/tcp open unknown
955/tcp open unknown
956/tcp open unknown
957/tcp open unknown
958/tcp open unknown
959/tcp open unknown
960/tcp open unknown
961/tcp open unknown
962/tcp open unknown
963/tcp open unknown
964/tcp open unknown
965/tcp open unknown
966/tcp open unknown
967/tcp open unknown
969/tcp open unknown
970/tcp open unknown
971/tcp open unknown
972/tcp open unknown
973/tcp open unknown
974/tcp open unknown
975/tcp open securenetpro-
sensor
977/tcp open unknown
978/tcp open unknown
979/tcp open unknown
980/tcp open unknown
981/tcp open unknown
982/tcp open unknown
983/tcp open unknown
984/tcp open unknown
985/tcp open unknown
986/tcp open unknown
987/tcp open unknown
988/tcp open unknown
989/tcp open ftps-data
990/tcp open ftps
991/tcp open unknown
993/tcp open imaps
994/tcp open ircs
995/tcp open pop3s
996/tcp open xtreelic
997/tcp open maitrd
998/tcp open busboy
999/tcp open garcon
1000/tcp open cadlock
1001/tcp open unknown
1002/tcp open windows-icfw
1003/tcp open unknown
```

```
1004/tcp open unknown
1005/tcp open unknown
1006/tcp open unknown
1007/tcp open unknown
1008/tcp open ufsd
1009/tcp open unknown
1010/tcp open unknown
1011/tcp open unknown
1012/tcp open unknown
1013/tcp open unknown
1014/tcp open unknown
1015/tcp open unknown
1016/tcp open unknown
1017/tcp open unknown
1020/tcp open unknown
```