UNIVERSIDADE DO SAGRADO CORAÇÃO

GUILHERME LAVIER SANTOS GANDOLFI

ESTUDO DE FERRAMENTAS PARA ESCANEAMENTO E DETECÇÃO DE ATAQUES EM REDES DE COMPUTADORES

BAURU
2013

GUILHERME LAVIER SANTOS GANDOLFI

ESTUDO DE FERRAMENTAS PARA ESCANEAMENTO E DETECÇÃO DE ATAQUES EM REDES DE COMPUTADORES

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 Pachioni Martins

BAURU
2013

Gandolfi, Guilherme Lavier Santos

G1961a

Estudo de ferramentas para escaneamento e detecção de ataques em redes de computadores / Guilherme Lavier Santos Gandolfi -- 2013.

45f. : il.

Orientador: Prof. Esp. Henrique Pachioni Martins.

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

1. Redes de computador. 2. Segurança. 3. Ataques. 4. Varredura. I. Martins, Henrique Pachioni. II. Título.

GUILHERME LAVIER SANTOS GANDOLFI

ESTUDO DE FERRAMENTAS PARA ESCANEAMENTO E DETECÇÃO DE ATAQUES EM REDES DE COMPUTADORES

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 orientação do Profº Esp. Henrique Pachioni Martins.

Banca Examinadora:

_____
Prof. Esp. Henrique Pachioni Martins
Universidade do Sagrado Coração

_____
Prof. Dr. Elvio Gilberto da Silva
Universidade do Sagrado Coração

_____
Prof. Esp. André Luiz Ferraz Castro
Universidade do Sagrado Coração

Bauru, ____ de dezembro de 2013

DEDICATÓRIA

Dedico este trabalho a Deus, pois sem ele nada disto seria possível, ele é a razão de estarmos aqui vivendo e batalhando.

Dedico este trabalho também a minha mãe Sonia que sempre me proporcionou o melhor para pode chegar até aqui e também a meu pai Carlos Augusto que mesmo não estando mais entre nós, sempre me apoiou quando precisei e sempre estará ao meu lado onde quer que ele esteja.

AGRADECIMENTOS

Agradeço a todas as pessoas que me ajudaram e me apoiaram durante o desenvolvimento deste trabalho.

Ao Prof. Dr. Kelton Augusto Pontara da Costa, que foi meu orientador durante a primeira parte deste trabalho, pela ajuda no desenvolvimento teórico do trabalho.

Ao Prof. Esp. Henrique Pachioni Martins, que assumiu como meu orientador para a segunda parte do trabalho, pela ajuda proporcionada na parte prática do trabalho e tirando qualquer duvida que surgisse tornando a realização deste trabalho muito mais fácil.

RESUMO

Cada dia mais e mais pessoas vem sendo vítimas de ataques em suas de computadores privadas perdendo informações importantes por falta de conhecimento em segurança de redes. Pensando nisso este trabalho prevê a discussão rede de computadores, desde o básico de seu funcionamento passando por segurança em redes, mostrando os diferentes aspectos que ela abrange e as várias técnicas disponíveis para deixar seu ambiente mais seguro, e assim como as formas de ataques mais comuns que sua rede pode estar em risco se não tomado o devido cuidado. A introdução à ferramentas de varredura de rede que tem como função detectar os pontos onde sua rede pode estar aberta para ataques, para que você consiga proteger sua rede antes que alguém se aproveite destas falhas, foram utilizados os *softwares Nessus*, *Nmap* e *GFI LanGuard* com intuito de mostrar como eles funcionam, quais informações eles proporcionam para ajudar na proteção da sua rede e quais características um difere do outro

Palavras-Chave: Redes de Computador, Segurança, Ataques, Varredura.

ABSTRACT

Each Day more and more people end up being victims of attacks on their private computer network losing valuable information due the lack of knowledge on network security, with that on mind this project predicts the discussion about computer network, from the basic of your functionalities and going through network security, showing the different aspects that it covers and most of the available techniques to make your environment more secure, also cover the most commons forms of attacks that your network might be at risk if not taken care. Introduction to network sweeping tools which ones have the function to detect where your network might be open to attacks, so you can fix before anyone try to take advantage of those exploits, going to utilize the programs Nessus, Nmap and GFI LanGuard with the intention of showing how they work, which kind of information they grab to help you protecting your network and on what they differ from each other.

Key Words: Computer Network, Security, Attacks, Sweep.

LISTA DE ABREVIATURAS

ACK – Acknowledgment

DDoS – Distributed Denial of Service

DoS – Denial of Service

GUI – Graphical User Interface

IDS – Intrusion Detection System

IP – Internet Protocol

IPS – Intrusion Prevention System

MAC - Media Access Control

RST - Reset

SYN – Synchronicity

TCP – Transmission Control Protocol

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

Durante as primeiras décadas de sua existência, as redes de computadores foram usadas principalmente por pesquisadores universitários, com a finalidade de enviar mensagens de correio eletrônico, e também por funcionários de empresas para compartilhar impressoras. Sob essas condições a segurança nunca precisou de maiores cuidados. Porém, como milhões de cidadãos comuns atualmente usam as redes para executar operações bancárias, fazer compras e arquivar suas devoluções de impostos, tem surgido um ponto fraco atrás do outro, e a segurança vem se tornando um problema de grandes proporções. Este é um assunto abrangente e inclui inúmeros tipos de problemas. Em sua forma mais simples, preocupa-se em impedir que pessoas mal-intencionadas 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 não estão autorizadas a usar (TANENBAUM; WETHERALL, 2011).

Com isso, várias ferramentas de segurança em redes têm surgido a fim de tentar ajudar a manter sua rede livre de falhas e pontos fracos, porém se usadas por pessoas mal-intencionadas, tais ferramentas podem ajudá-lo a detectar as falhas que a rede possui, facilitando o ataque.

Através deste estudo foram analisados alguns *softwares* de escaneamento de rede para identificar falhas e vulnerabilidades em redes de computador. Os softwares escolhidos foram o *Nessus*, *Nmap* e *GFI LanGuard*, para coletar os dados sobre a rede a ser analisada e fazer as devidas comparações.

1.1 Objetivo Geral

Estudar ferramentas de varredura de rede para compreender sobre os conceitos de segurança, invasão e prevenção de ataques em redes de computadores.

1.2 Objetivos Específicos

- Estudar os conceitos de Segurança em redes de computadores
- Identificar ferramentas de escanemanto de rede para aplicação
- Identificar características de funcionamento das ferramentas de varredura de rede
- Fazer Comparação entre ferramentas de varredura de rede

1.3 Justificativa

Devido ao grande crescimento de usuários utilizando redes de computadores e com isso o grande aumento na preocupação de que seus dados estejam sempre seguros. Através da análise de programas de escaneamento de rede será possível observar e mostrar qual área da rede está vulnerável a ataques, ajudando usuários e empresas que as utilizam a detectarem tais falhas e tentar corrigi-las o mais rápido possível para que dados importantes não caiam nas mãos de pessoas mal intencionadas. Com isso este estudo tem por finalidade realizar um levantamento bibliográfico, demonstrar ferramentas de escaneamento e realizar análises das mesmas, para apoiar profissionais e acadêmicos sobre o assunto.

2 REFERENCIAL TEÓRICO

2.1 Redes de Computadores

Uma rede é um conjunto de dispositivos conectados por *links* de comunicação (denominados frequentemente de nós). Um nó pode ser um computador, uma impressora ou qualquer outro dispositivo capaz de enviar e/ou receber dados gerados noutros nós da rede. Uma rede é constituída de dois ou mais dispositivos juntos através de *links*. Um *link* é um caminho de comunicação por onde são transferidos dados de um dispositivo ao outro. Como mostra a Figura 1 podemos imaginar um *link* como uma linha que liga dois ou mais dispositivos, podendo ser feitas tanto através de cabos, como de ondas de radio. (FOROUZAN, 2006)

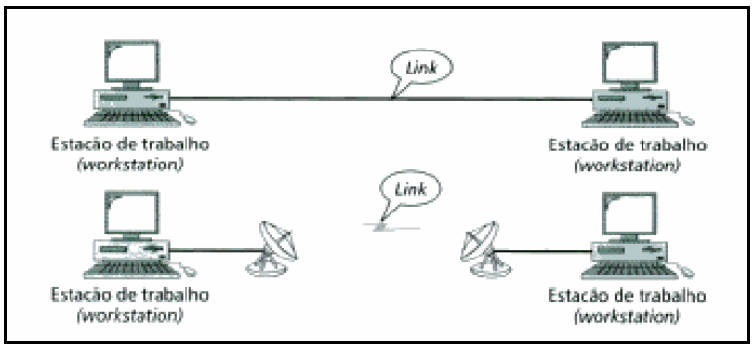

Figura 1 - Rede de Computador
Fonte: FOROUZAN (2006)

Segundo Kurose, e Ross, (2009, p. 3);

> A Internet pública é uma rede de computadores mundial, isto é, uma rede que interconecta milhões de equipamentos de computação em todo mundo. [...] A Internet pública é a rede a que normalmente nos referimos como Internet. Também há muitas redes privadas, tais como redes corporativas e governamentais, cujos hospedeiros não podem trocar mensagens com hospedeiros que estão fora da rede privada. Essas redes privadas são frequentemente denominadas intranets. .

Ainda Kurose e Ross diz que a *Internet* permite que aplicações distribuídas que executam em seus sistemas finais troquem dados entre si. Essas aplicações podem ser a navegação na *Web*, mensagem instantânea, áudio e vídeo em tempo real, telefonia para Internet, jogos distribuídos, compartilhamento de arquivos *peer-to-peer*(P2P), login remoto, correio eletrônico e mais, muito mais conforme mostra Figura 2.

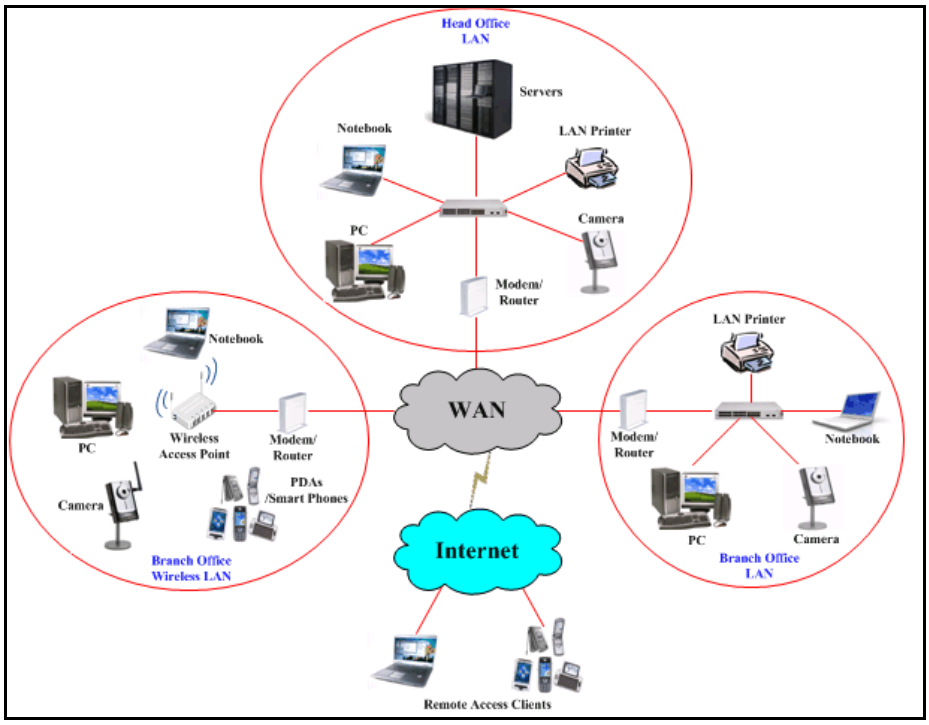

Figura 2 - Redes de Computador conectadas a Internet
Fonte: Infigro.sg (2013)

2.2 Segurança

A criptografia é o coração da segurança em rede. Se precisarmos estabelecer privacidade em uma rede, é de suma importância pensar como iremos criptografar a informação no transmissor e decodificá-la à forma original no receptor. (FOROUZAN, 2006)

Ainda Forouzan(2006) diz que em uma rede, embora seja possível manter um excelente nível de confiabilidade das mensagens, preservar a integridade, autenticar o transmissor e assegurar o não repúdio de informação, estes aspectos de segurança

sozinhos não impedem que uma pessoa mal-intencionada envie, deliberadamente, mensagens de modo a provocar danos em um sistema. Precisamos de recursos para filtrar mensagens de modo a permitir somente aquelas que nos interessam. O *firewall* é a tecnologia utilizada para esse fim. (FOROUZAN, 2006)

2.2.1 Criptografia

As mensagens a serem criptografadas, conhecidas como texto simples (ou *plaintext*) são transformadas por meio de uma função parametrizada por uma chave (*Encryption key*). Em seguida a saída do processo de criptografia, conhecida como texto cifrado (ou *ciphertext*), é transmitida. Essa mensagem cifrada pode ser alvo de intrusos passivos (*Passive Intruder*) que conseguem apenas ler a mensagem cifrada e intrusos ativos (*Active Intruder*) que podem alterar a mensagem cifrada. No entanto, ao contrário do destinatário pretendido, ele não conhece a chave para descriptografar o texto (*Decryption key*) e, portanto, mesmo lendo ou alterando parte da mensagem o intruso não sabe o real conteúdo dela como mostra a Figura 3 (TANENBAUM et all,2011).

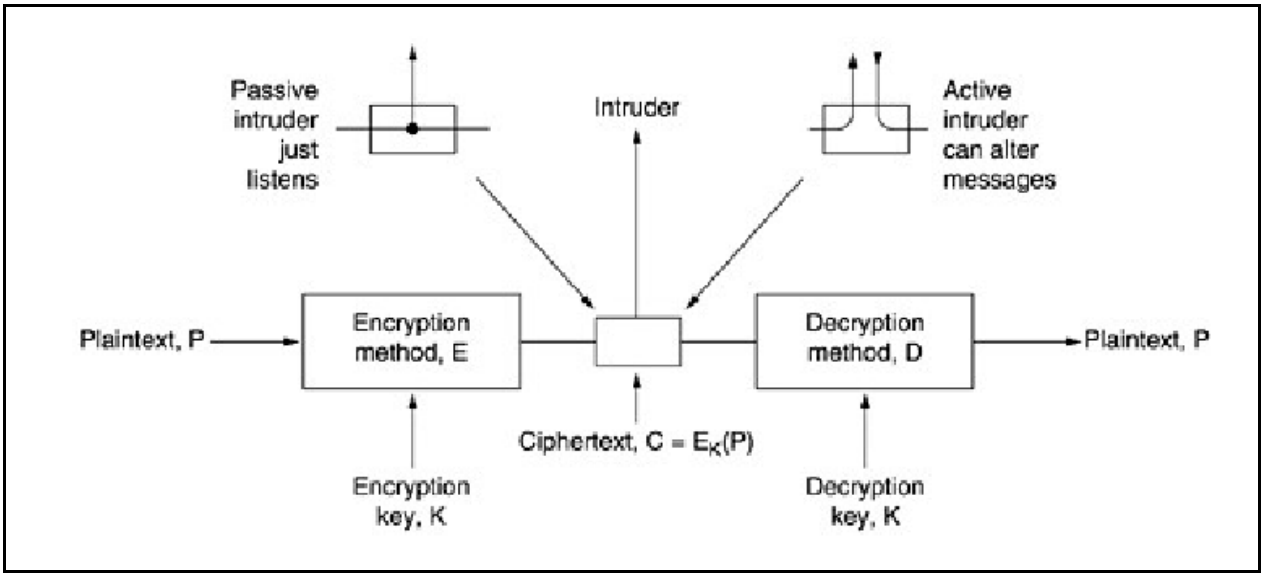

Figura 3 - Modelo de Criptografia
Fonte: TANEMBAUM et all (2011)

Técnicas criptográficas permitem que um remetente disfarce os dados de modo que um intruso não consiga obter nenhuma informação dos dados interceptados. O destinatário é claro deve estar habilitado a recuperar os dados originais a partir dos dados disfarçados (KUROSE et all,2009).

2.2.2 Firewall

Hoje em dia praticamente todas as estruturas de segurança de rede dependem do conceito de *firewall*. A ideia original do *firewall* era isolar a sua rede interna da Internet, por completo. Através da filtragem do trafego TCP/IP o firewall decide o que é permitido e o que não é. O *firewall* analisa os cabeçalhos dos pacotes de IP que passam por ele. Através desta análise, ele pode descobrir qual porta este pacote utilizará e ainda os endereços IP de origem e destino. Com base nesta informação, ele compara com uma lista de regras decide se o pacote pode prosseguir ou não (TORRES, 2001).

A Figura 4 mostra que normalmente um *firewall* é instalado no ponto onde a *Intranet* se conecta à Internet. Todo o fluxo de dados vindo da Internet ou indo passa pelo *firewall*. Existem alguns casos em que o *firewall* pode ser colocado dentro da *Intranet* para isolar servidores importantes (MARTIMIANO, 2006).

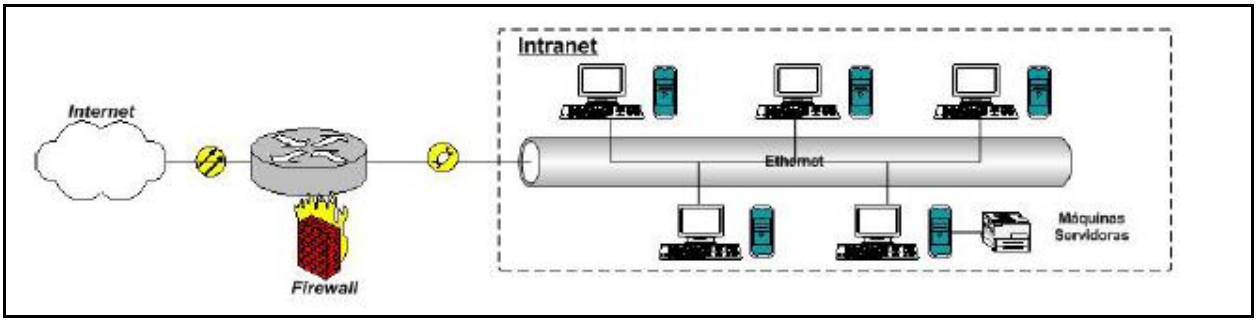

Figura 4 - Localização comum de um Firewall
Fonte: MARTIMIANO (2006)

2.2.3 Intrusion Detection System

Intrusões são difíceis de detectar porque existem muitas formas pelas quais elas podem acontecer. Pode utilizar-se de falhas na arquitetura ou como alto conhecimento em sistemas operacionais, e ao tentar corrigir algo você pode desproteger outra parte do sistema deixando o sistema vulnerável a novos ataques. As funcionalidades de um sistema de detecção tornam-se muito importantes na medida em que se pode analisar o conteúdo das conexões permitidas e detectar as que apresentem um comportamento suspeito ou não condizente com a política implantada (BERNARDES, 1999).

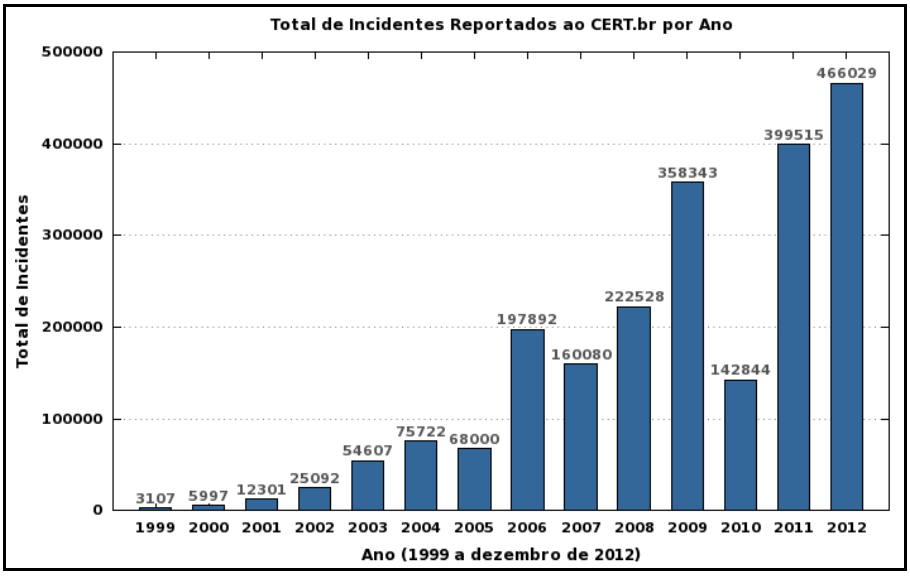

Figura 5 – Total de Incidentes Reportados
Fonte: CERT.br (2013)

Segundo PEREIRA, (2012, p5);

> Detectar uma intrusão significa identificar qualquer comportamento suspeito no tráfego de uma rede de computadores. Sistemas de detecção de intrusos (*Intrusion Detection Systems* – IDSs) monitoram esse trafego detectando comportamento e pacotes suspeitos que possam danificar ou ter acesso não autorizado a informações sigilosas que trafegam pela rede. [...] Sistemas de Detecção de Intrusos são aplicados como ferramentas complementares no processo de gestão de segurança em redes de computadores, pois apesar dos esforços empregados para automatizar a tarefa de detecção e respectivas respostas ainda é indispensável a participação humana para tomar as devidas providencias no caso de alertas e relatórios que são gerados pelos IDSs.

2.2.4 Intrusion Prevention System

Sistemas de Prevenção de Intrusos (*Intrusion Prevention System* – IPS) é uma solução ativa de segurança, capaz de fornecer segurança em todos os níveis, desde o núcleo do sistema operacional até os pacotes de dados da rede.O IPS provê políticas e regras para o tráfego de rede, trabalhando em conjunto com um IDS que emite alertas em casos de tráfego suspeito. Enquanto o IDS informa sobre um potencial ataque, o IPS promove tentativas de parar o ataque com capacidade de prevenir invasões com “assinaturas” conhecidas, ele também pode impedir alguns atques não conhecidos, devido a sua base de dados de ataque genéricos. Visto como uma combinação de IDS e uma “camada de aplicação Firewall” para proteção, IPS é considerado a geração seguinte do IDS (O..., 2010).

O IPS complementa um IDS bloqueando a intrusão e impedindo um dano maior para a rede. É uma ferramenta que detecta e bloqueia o invasor. Em uma comparação poderia dizer que o IDS é como um alarme de um carro que soa quando alguém abre a porta e o IPS dispara o alarme e também trava as rodas para que o invasor não leve o carro. Após a detecção, um IPS executara ações para interromper ataques e evitar ataques futuros, essas ações podem ser desde o cancelamento de conexão ate uma reconfiguração de firewall para interromper o ataque (EVANGELISTA, 2008).

2.3 Ataques em rede de computadores

Um ataque em rede de computador pode ser definido como qualquer método, processo ou meios utilizados na tentativa de comprometer maliciosamente a segurança da rede. As razoes para tais ataques são das mais variadas desde busca por reconhecimento, espionagem, ganância, terrorismo ate vingança. Existe também um grande numero de tipos de ataques tais como manipulação de dados, escutas, *spoofing*, ataques DoS, ataques DDoS, *sniffers*. (SPENCER, 2013)

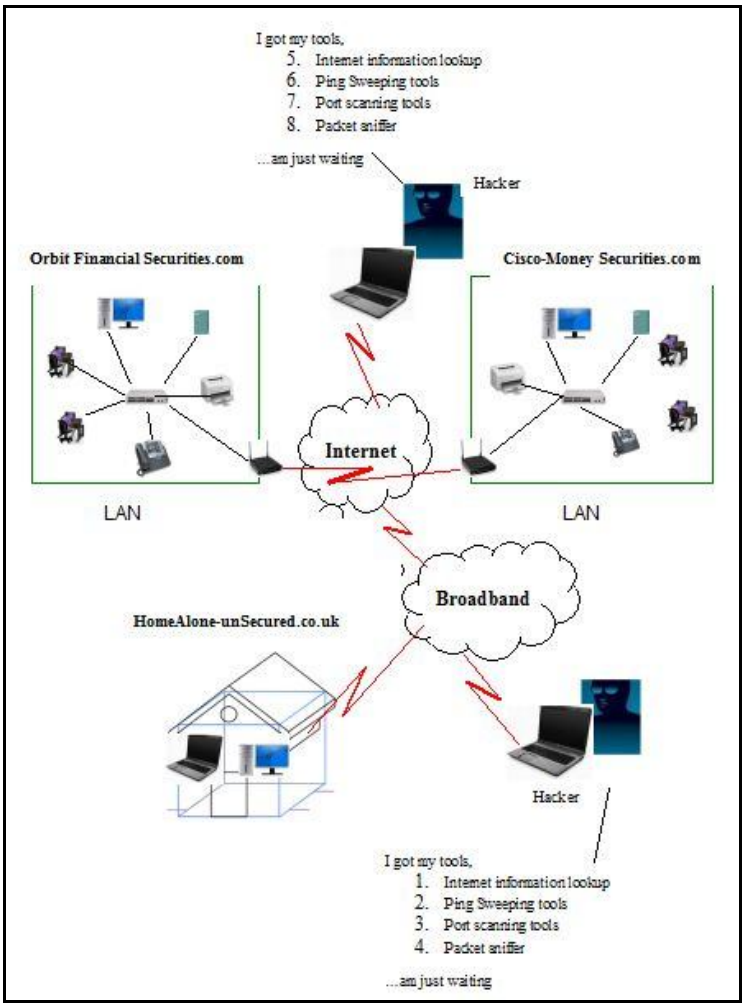

Figura 6 - Ataque de Reconhecimento
Fonte: Orbit-computer-solutions.com (2013)

O Ataque de reconhecimento conforme mostra a Figura 6 é utilizado para juntar informações sobre os sistemas e serviços de rede, possibilitando à pessoa por trás do ataque a descobrir vulnerabilidades ou fraquezas da rede. Tal pessoa utiliza de varias ferramentas para concluir seu reconhecimento, ferramentas de internet como *nslookup* e *whois* para descobrir o espaço de IP designado a certa rede, após utilizam programas para “pingar” todos os IPs dentro de certo raio ou subnet para descobrir quais estão ativos. Quando ele descobre os endereços ativos, começa a utilizar ferramentas de escaneamento de portas para descobrir quais serviços de rede e portas estão ativos. O *scanner*, então, consulta tais portas para determinar tipo e versão de aplicações e SO

que estão sendo utilizados no alvo. Baseando-se nessa informação, o hacker pode determinar se existe alguma vulnerabilidade ou fraqueza. (TYPES..., 2013)

Sniffer se refere ao processo que hackers usam para capturar e analisar o tráfego da rede. Os pacotes da rede são analisados e com isso os hackers conseguem monitorar e capturar informações que atravessam a rede como senhas ou informações confidenciais da organização. (SPENCER, 2013)

Um Ataque DoS, de uma forma resumida, é prevenir que usuários autorizados utilizem-se de um certo serviço, fazendo uso de todos os recursos do servidor. Em uma conexão comum, o usuário manda uma mensagem ao servidor, pedindo para autenticá-la. O servidor autentica-a e retorna-a ao usuário. Este recebe a confirmação da autenticação, então é permitido no servidor. Já em um ataque DoS, o usuário manda diversos pedidos de autenticação, fazendo com o servidor estoure sua capacidade de receber pedidos de autenticação. Além disso, todos os pedidos tem um endereço de retorno falso; com isso, o servidor não consegue retornar os pedidos de autenticação, fazendo com que o mesmo fique parado, esperando para fechar a conexão e quando finalmente ele fecha, o usuário responsável pelo ataque manda novos pedidos de autenticação, fazendo com que o servidor fique sempre cheio e que outros usuários não consigam ter acesso. (HOW..., 2000)

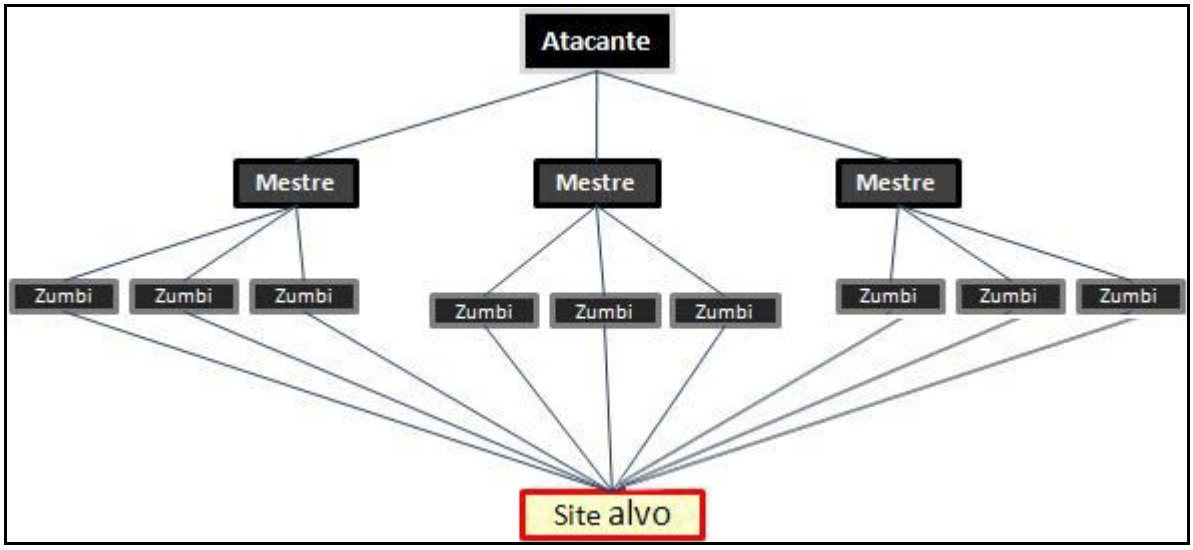

Figura 7 - Ataque DDoS
Fonte: Infowester (2012)

A Figura 7 mostra um ataque DDoS que segue basicamente os mesmos princípios de um ataque DoS porem utilizando-se de milhares de computadores. A pessoa por trás do ataque cria malwares com a intenção de disseminar pequenos programas de ataques DoS, quando tal malware contamina uma maquina ela fica disponível para fazer parte do ataque, sendo que na maior parte das vezes seu dono não tem nem ideia que esta fazendo parte deste ataque. Esta maquina, então, entra em uma rede chamada botnet, que nada mais é que uma rede formada por computadores infectados e que pode ser controlada remotamente pelo atacante. Uma vez na botnet a maquina contaminada passa a ser chamada de zumbi, que recebe ordem de máquinas mestres que estão sendo orientadas pelo computador atacante. Como existem varias maquinas envolvidas no ataque, torna-se muito difícil descobrir quem foi o responsável pelo ataque, fazendo com que esse se torne um dos mais comum e favorito de *hackers*. (ALECRIM, 2012)

2.4 Escaneamento em redes

Novas vulnerabilidades de rede estão constantemente sendo descobertas e ameaça contra redes corporativas tem ficado cada vez mais sofisticadas. O escaneamento por vulnerabilidades pode ajudar a identificar fraquezas antes que elas se tornem perigosas para o setor tecnológico. Scanners de vulnerabilidade são produtos que analisam a rede e dispositivos de rede e então apresentam ao usuário relatórios que permitem ao mesmo responder rapidamente a problemas em potencial. Tais scanners procuram por problemas como firewalls configurados incorretamente ou servidores que possam estar suscetíveis a fraquezas (VIOLINO, 2009).

Similar a *Sniffing* de pacotes, scanner de portas e outras “ferramentas de segurança”, *scanners* de vulnerabilidade podem ajudar a sua própria rede, ou podem ser utilizado por pessoas mal intencionadas a identificar as fraquezas de sua rede e preparar um ataque. Com isso a ideia é você utilizar tais ferramentas para identificá-las e concerta-las antes que alguém utilize as utilize contra você. (O’Donnell, 2013)

3 METODOLOGIA

A primeira parte da pesquisa foi o levantamento bibliográfico que foi realizado com a utilização de livros, teses, dissertações e artigos de *sites*.

Na segunda parte da pesquisa foi realizada a coleta de dados, utilizando os *softwares Nessus* em sua versão *trial*, *GFI LANGuard* também em sua versão *trial* e *Nmap*. Foi feito um escaneamento em uma rede doméstica de três computadores para encontrar possíveis falhas ou fraquezas que a rede poderia ter que poderiam ser utilizadas para invasão.

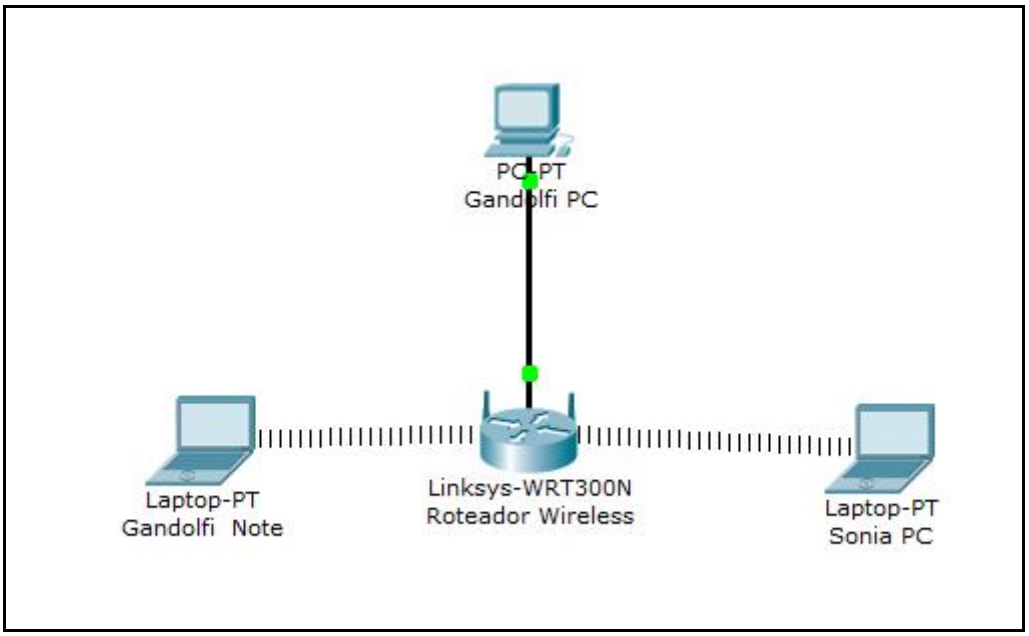

Figura 8 - Modelo Rede
Fonte: Elaborado pelo Autor (2013)

A Figura 8 mostra uma rede doméstica constituída de 3 computadores e 1 roteador wireless, 1 computador do tipo *desktop* ligado ao roteador através de cabos de rede e 2 notebooks ligados ao roteador utilizando tecnologia Wireless.

Todas as análises foram realizadas em computador do tipo Notebook com processador AMD Athlon TF-20, 1.6GHz, memória RAM de 2GB com o sistema operacional Windows 7 Professional 32 Bits.

Após análise de todos os IPs da rede mostrada na Figura 8 foram comparados os resultados obtidos nos três *softwares* para observar possíveis características positivas e negativas entre as análises para uma comparação entre os *softwares* descrever sua confiabilidade.

Por mais de uma década o *Nmap Project* vem catalogando ferramentas de segurança em rede de computadores preferidas da comunidade, com isso em mente as ferramentas *Nessus* e *GFI LANGuard* foram escolhidas utilizando este ranking criado pelo *Nmap Project* e também a ferramenta mantida por eles o *Nmap*

4 RESULTADOS

Nesta parte da pesquisa serão catalogados os resultados obtidos nos três *softwares* de varredura na rede proposta. Os resultados serão mostrados de forma que a primeira máquina analisada irá mostrar o maior numero de informação sobre o *software* e o seu funcionamento e as demais irão apenas mostrar diferenças entre as análises.

4.1 Nmap

Nmap é um *software gratis* e *Open Source* que foi desenvolvido para descobrir características de redes e auditoria de segurança. Para obtenção das informações necessárias foi utilizada a *GUI* oficial do *Nmap* que é chamada de *Zenmap.*

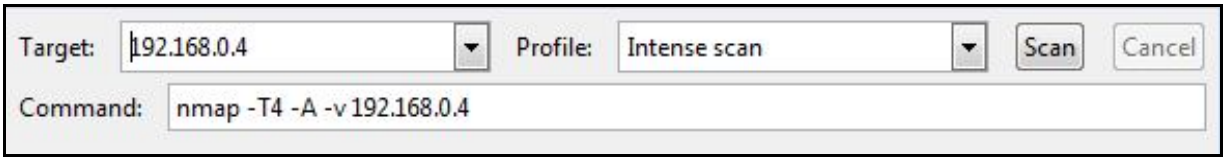

Figura 9 – Layout de Varredura Nmap
Fonte: Elaborado pelo Autor (2013)

Através da Figura 9 podemos ver que o programa possui uma *interface* simples proporcionando ao usuário uma fácil utilização, onde só é preciso colocar o IP da máquina a ser verificada no campo *Target* e selecionar o tipo de varredura a ser realizada no caso foi utilizado à opção *Intense Scan* e clicar no botão *Scan* ou ainda para usuários mais avançados eles proporcionam o campo *Command* onde você pode adicionar diretrizes extras para refinar seu escaneamento que estão no manual do programa.

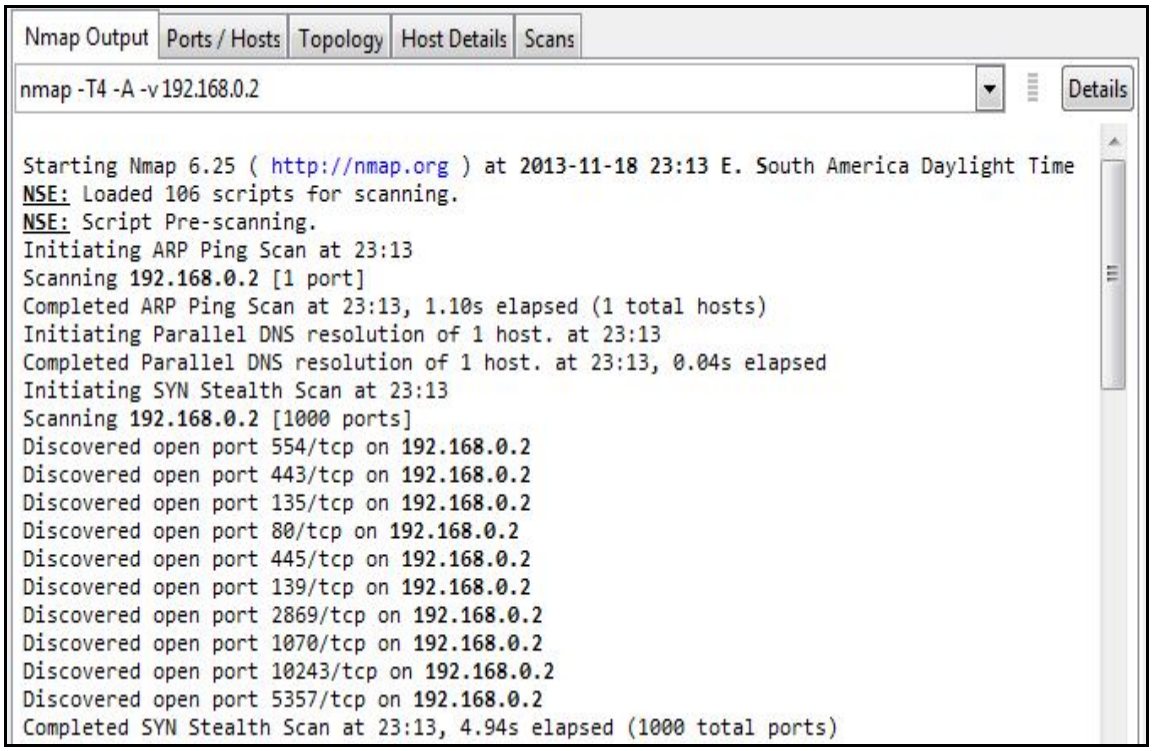

Figura 10 – Exemplo Output Desktop Gandolfi PC
Fonte: Elaborado pelo Autor (2013)

Na figura 10 podemos ver uma parte do passo a passo que o programa executa quando é iniciada a varredura, pode ver que foi utilizado processo de *SYN Stealth Scan* para detectar as portas que estão abertas na máquina, tal processo funciona de forma que é emitido um pacote de sincronização (SYN) para a porta e caso ela retorne tal pacote como sincronização (SYN) ou reconhecimento (ACK) significa que ela esta aberta, então o scanner envia um pacote de *reset* (RST) para que a conexão não seja estabelecida totalmente, caso o pacote retorne como reset (RST) é considerado que a porta esta fechada e se porta possuir filtros o pacote será perdido e não terá resposta.

```
Host script results:
| nbstat:
|   NetBIOS name: GANDOLFI-PC, NetBIOS user: <unknown>, NetBIOS MAC:
(Asustek Computer)
|   Names
|     GANDOLFI-PC<00>      Flags: <unique><active>
|     WORKGROUP<00>        Flags: <group><active>
|_    GANDOLFI-PC<20>      Flags: <unique><active>
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   NetBIOS computer name: GANDOLFI-PC
|   Workgroup: WORKGROUP
|_  System time: 2013-11-18T20:14:52-03:00
| smb-security-mode:
|   Account that was used for smb scripts: guest
|   User-level authentication
|   SMB Security: Challenge/response passwords supported
|_  Message signing disabled (dangerous, but default)
|_smbv2-enabled: Server supports SMBv2 protocol

TRACEROUTE
HOP RTT     ADDRESS
1   3.79 ms 192.168.0.2
```

Figura 11 Resultados do Host Gandolfi PC
Fonte: Elaborado pelo Autor (2013)

Na Figura 11 ainda na aba *Output* do escaneamento é mostrado um pequeno resumo de informações básicas sobre a máquina tal qual o nome dela na rede, o sistema operacional utilizado, o MAC *address* que neste caso foi retirado por questões de segurança e seu fabricante. É possível ver também o comando *Traceroute* sendo utilizado para descobrir o caminho na rede até a maquina escaneada.

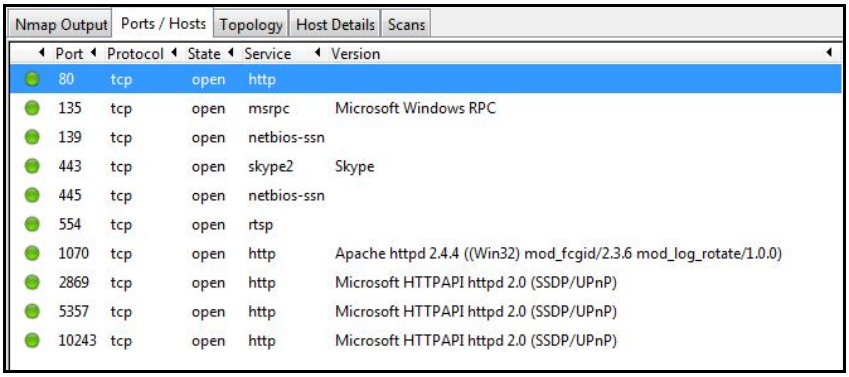

Figura 12 Aba Ports/Hosts Gandolfi PC
Fonte: Elaborado pelo Autor (2013)

Após o escaneamento ser finalizado o *software* irá preencher as demais abas com as informações obtidas para uma visualização mais fácil e rápida, a Figura 12 esta mostrando a aba *"Ports/Hosts"* que tem como utilidade mostrar as portas e hosts que foram encontradas abertas ou com filtros, é mostrado o numero da porta, qual protocolo de comunicação utilizado, qual o estado (aberta, fechada, filtrada), o serviço utilizado nesta porta e qual a versão.

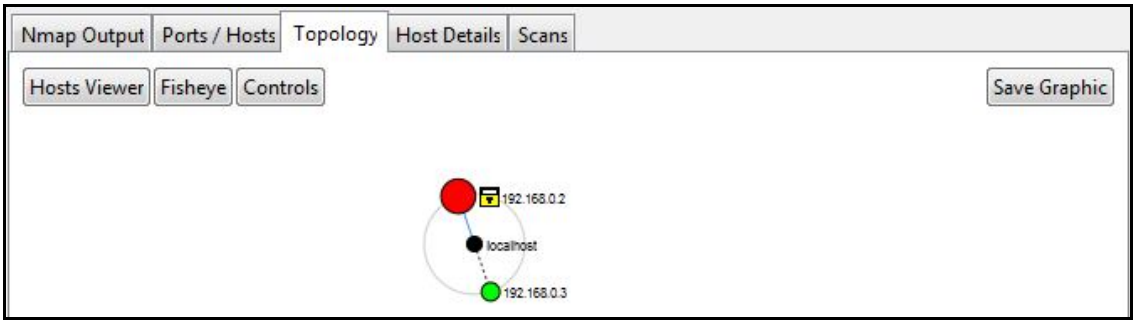

Figura 13 Aba Topology Gandolfi PC
Fonte: Elaborado pelo Autor (2013)

Na Figura 13 é possível ver a aba de Topologia onde o *software* mostra os pontos de conexão entra a maquina de escaneamento (*localhost*) e as máquinas que foram escaneadas nesta sessão do programa

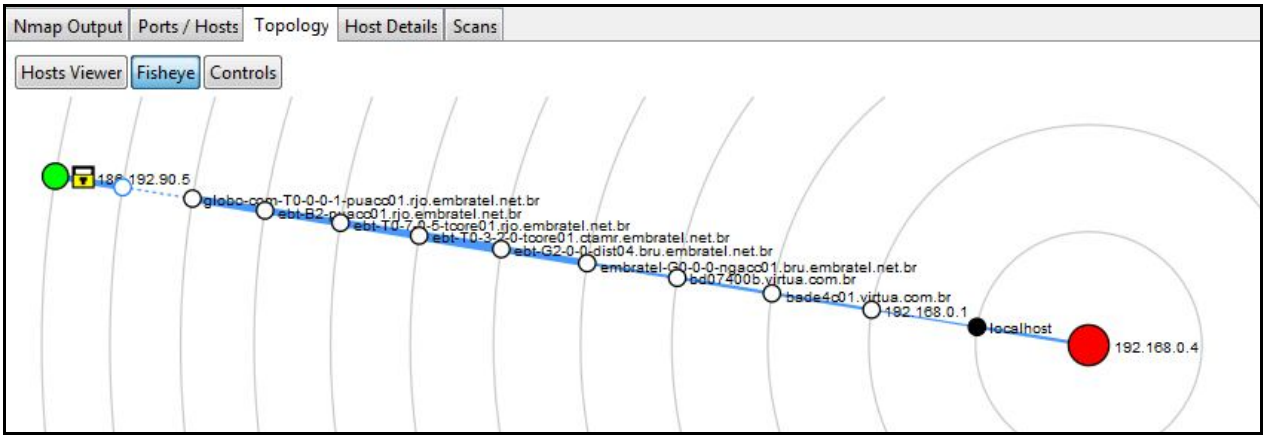

Figura 14 Exemplo Topologia Complexa
Fonte: Elaborado pelo Autor (2013)

Para um melhor visualização da aba topologia foi realizado um rápido *Traceroute* com o *website* globo.com para ver todos os pontos de conexão entre o *localhost* e o *website* e também para mostrar como o programa lida com conexões mais complexas. Também pode ser notado que o programa não mostra apenas a rota escaneada, todas os escaneamentos que estão em *background* vão ser incluídos na topologia, como se pode ver a topologia para o Notebook Gandolfi PC incluída.

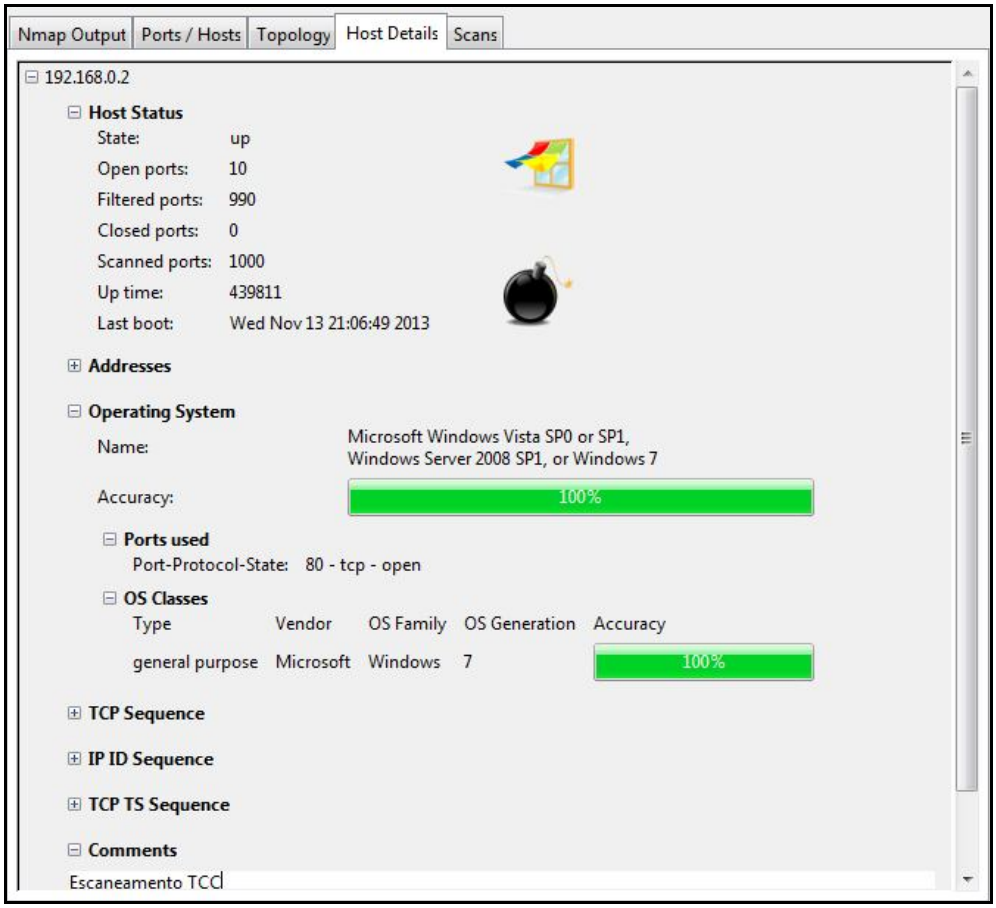

Figura 15 Aba Host Details Gandolfi PC
Fonte: Elaborado pelo Autor (2013)

Nesta aba o *software* coloca todas as informações mais básicas sobre sistema como o estado se está ligado ou desligado, quantas portas foram econtradas abertas, filtradas, fechadas, tal como o numero de portas escaneadas, o tempo que está ligado e o data de quando foi ligado. Mostrando os endereços desta maquina, ressaltando que o MAC *address* foi apagado por questões de segurança. O sistema operacional em

funcionamento e o grau de certeza que ele tem nessa afirmação e quais portas foram utilizadas para determinar.

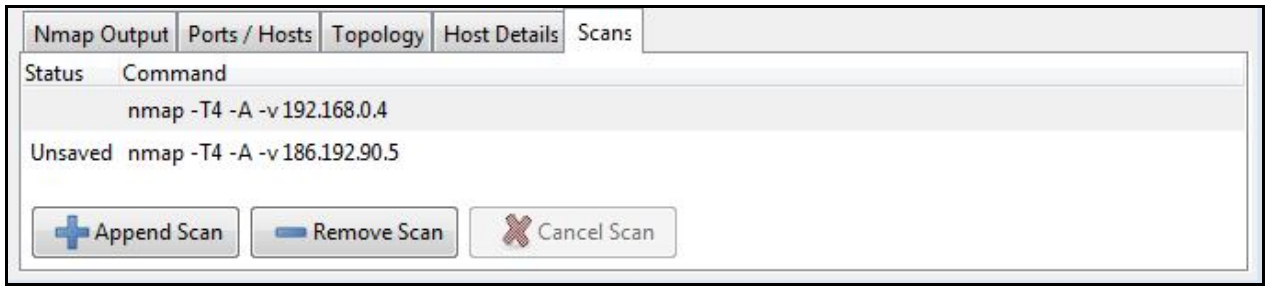

Figura 16 Aba Scans
Fonte: Elaborado pelo Autor (2013)

A aba *scans* mostrada na Figura 16 mostra todos os escaneamentos abertos nesta sessão de utilização do *software*. Mostrando o seu estado caso esteja em progresso (running), falhado (failed), não salvo (unsaved), esta aba pode também ser útil para saber quais topologias serão incluídas na aba *Topology*.

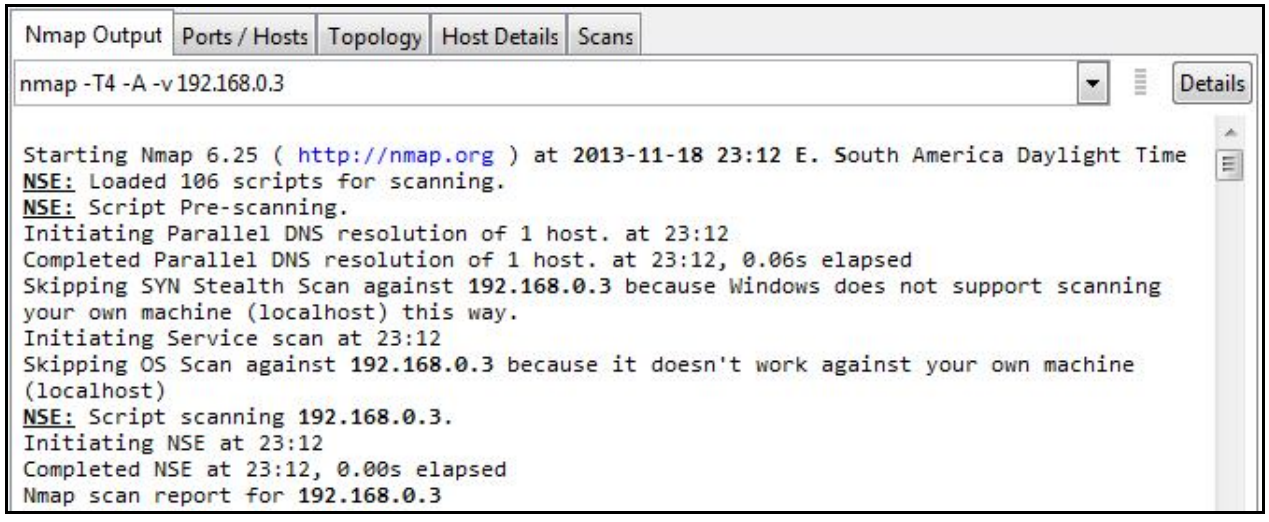

Figura 17 Exemplo Output Gandolfi Note
Fonte: Elaborado pelo Autor (2013)

Na Figura 17 pode ser visto o grande ponto fraco deste software enquanto ele é muito bom para escanear maquinas na sua rede, os métodos utilizados para captura de informação não funcionam se você estiver tentando escanear a maquina em que esta utilizando o programa, o *software* pula quase todas as fases do escaneamento por não estar conseguindo obter as informações.

Com base nisto é possível afirmar que o Software Nmap proporciona o esperado, porém não perfeitamente, seu uso seria muito aproveitado se utilizado por um encarregado do setor de computação de uma empresa, pois apesar de não proporcionar um escanemanto para a máquina em que está sendo executado, seria muito útil para as demais maquinas da rede ajudando a manter a rede muito mais segura contra ataques.

4.2 GFI Lan Guard

GFI Lan Guard é um software pago que porem possui uma versão *Trial* de 30 dias limitada para testes, seu preço varia de acordo com o numero de maquinas que você possui na rede para serem escaneadas, 30USD por máquina em uma rede de até 24 maquina chegando a 7.50USD por máquina em uma rede com mais de 2000 máquinas, alem da função de escaneamento de IPs ele ainda proporciona um escaneamento geral da maquina procurando falhas e *softwares* que não vem sendo atualizados corretamente que possam levar a rede a correr riscos.

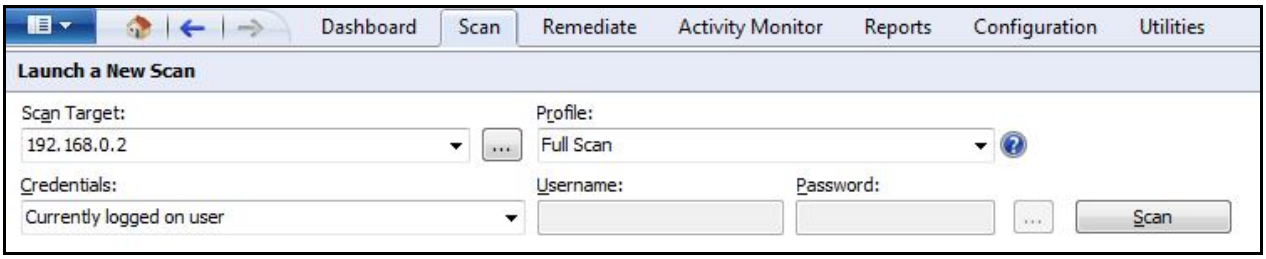

Figure 18 Layout de Varredura GFI LanGuard
Fonte: Elaborado pelo Autor (2013)

Assim como o *Nmap*, o *GFI LanGuard* possui uma aba de escaneamento bem intuitiva e fácil de se utilizar, só é necessário saber o IP da máquina que você deseja fazer o escaneamento e selecionar o tipo desejado, para este trabalho foi utilizado a opção *Full Scan.*

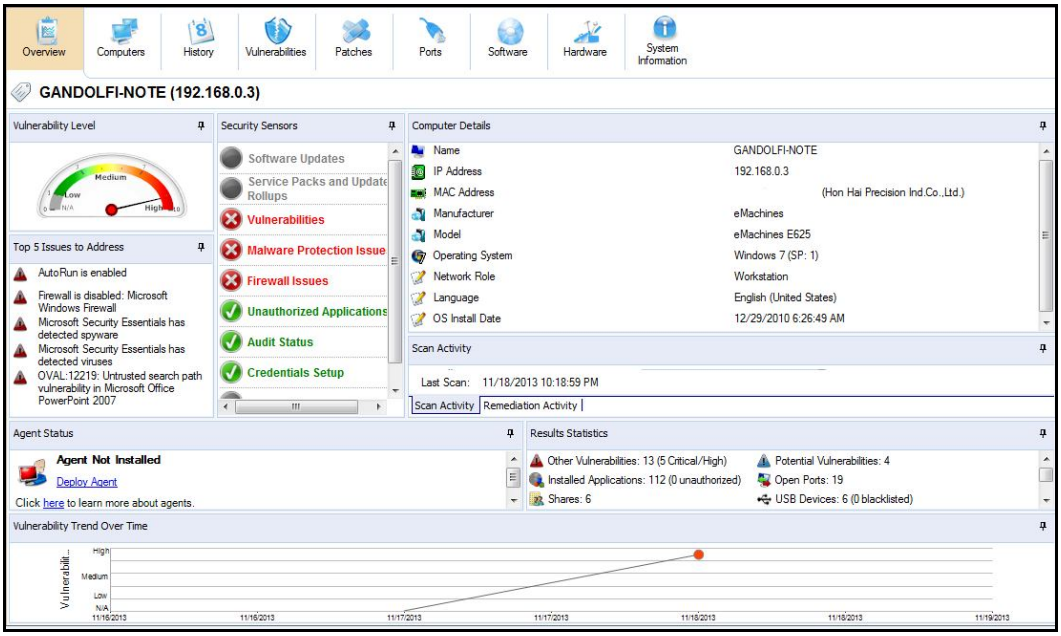

Figura 19 Overview Gandolfi Note GFI LanGuard
Fonte: Elaborado pelo Autor (2013)

A Figura 19 mostra a aba Overview que o programa cria após a realização do escaneamento na maquina desejada, diferentemente do Nmap que apresenta problemas quando tenta escanear a maquina em qual ele esta sendo executado o GFI LanGuard além de superar este problema ainda lhe traz adicionais problemas de vulnerabilidade que outros *softwares* podem vir a causar.

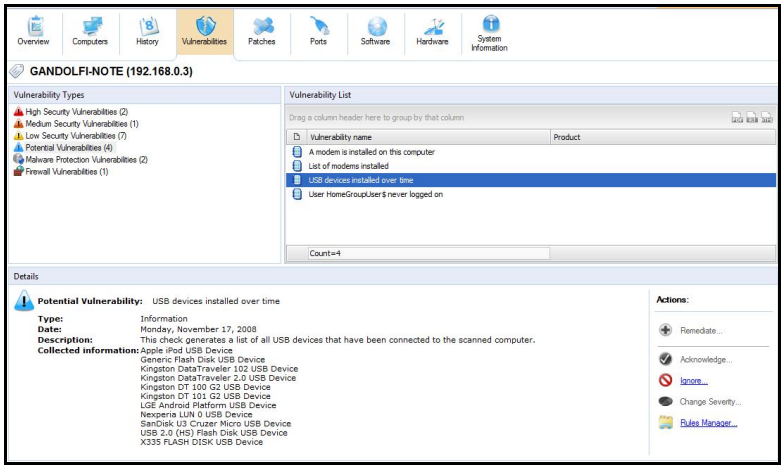

Figura 20 Aba Vulnerabilities Gandolfi Note GFI LanGuard
Fonte: Elaborado pelo Autor (2013)

Na Figura 20 temos a aba *vulnerabilities* que mostra com mais detalhes e separada por grau/tipo de vulnerabilidade que o seu computador esta sofrendo, a instância destacada na imagem mostra uma lista de todos os dispositivos que já foram conectados a esta maquina, uma informação muito importante para saber se alguém já tentou acessar sua maquina fisicamente para capturar informações.

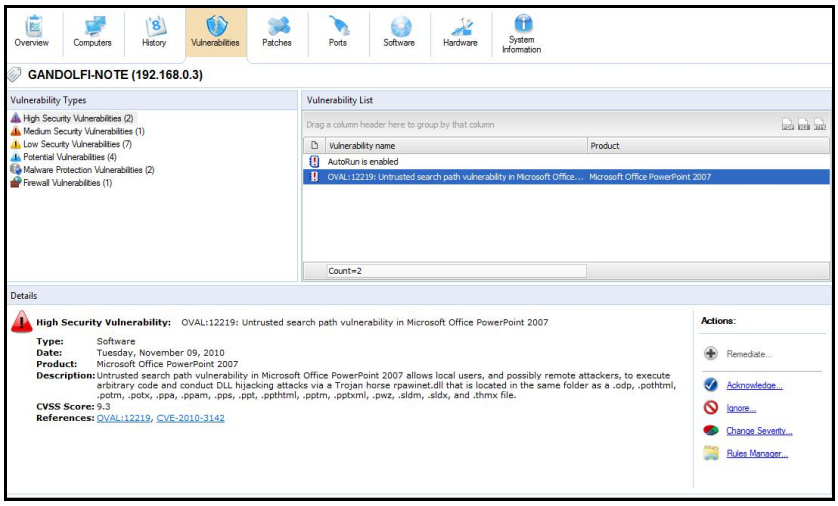

Figura 21 Aba Vulnerabilities Gandolfi Note
Fonte: Elaborado pelo Autor (2013)

Ainda na aba vulnerabilities, temos outra instância selecionada agora na parte de Vulnerabilidade de Alta Segurança. O programa não só mostra o que é, mas explica o porquê tal atributo é considerado de risco e o que pode acontecer se não tomar as devidas precauções.

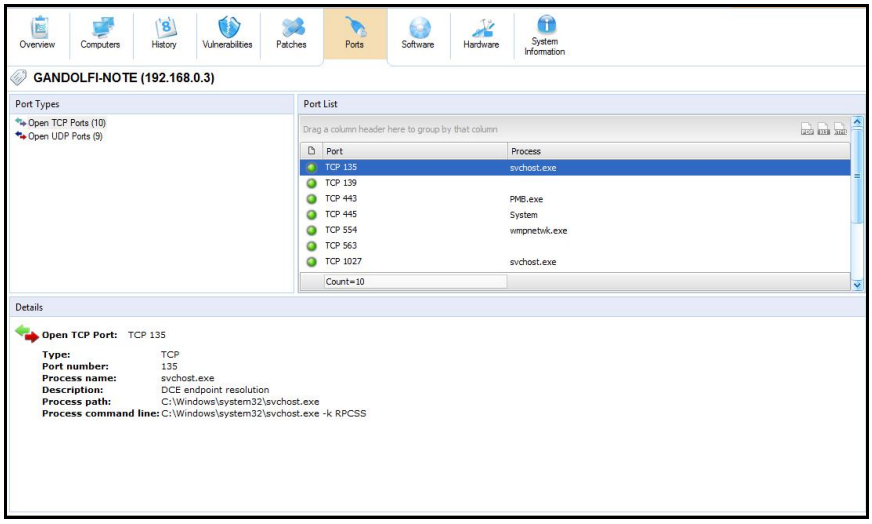

Figure 22 Aba Ports Gandolfi Note GFI LanGuard
Fonte: Elaborado pelo Autor (2013)

A aba *Ports* assim como no Nmap, mostra todas as portas que foram encontradas abertas na sua máquina porém com a descrição de qual processo as

utiliza, o tipo de porta, a descrição e qual o caminho até o processo que a utiliza e caso não reconheça o serviço irá proporcionar um aviso sobre possível *malware* que possa estar utilizando tal porta.

Outras abas como *Software*, *Hardware* e *System Information* apenas geram listas de *software* ou *hardware* instalado na maquina para uma fácil visualização.

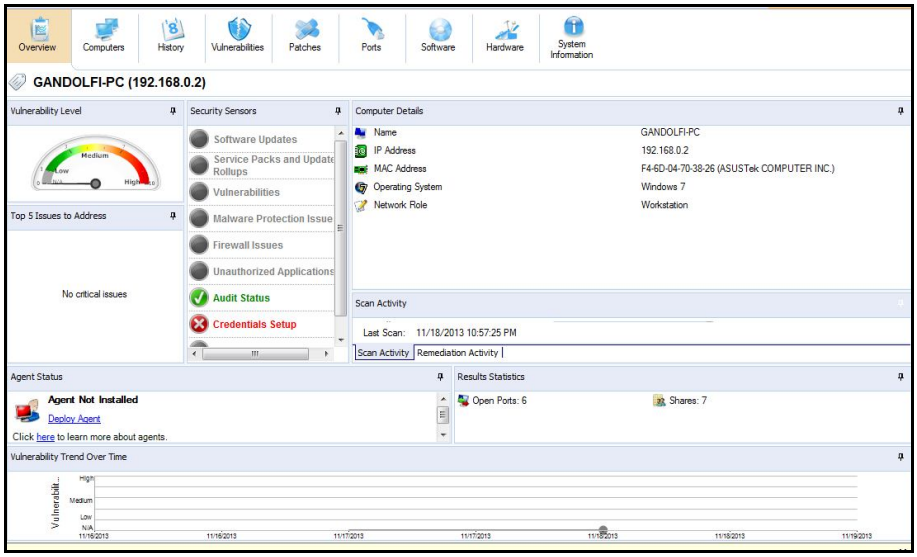

Figura 23 Overview Gandolfi PC GFI Lan Guard
Fonte: Elaborado pelo Autor (2013)

A Figura 23 mostra como é preenchida a aba overview quando é realizado o escaneamento em uma máquina que não é a que o *software* está instalado, pode-se notar que em relação à Figura 19 existe bem menos informação sendo apresentada isto porque o *software* não consegue captar informações sobre outros softwares instalados em maquinas diferentes, então quando realizado escaneamento em uma maquina que não é a que o *software* está instalado ele irá realizar apenas sua função primaria que é a de escanear portas e verificar se tem algo que possa lhe causar danos nesse quesito.

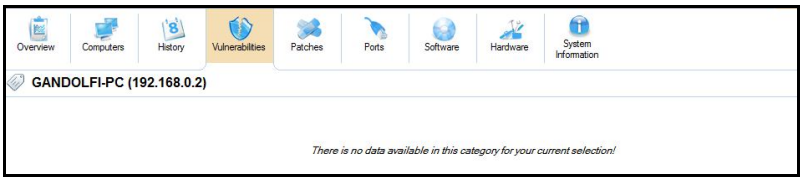

Figura 24 Aba Vulnerabilities Gandolfi PC GFI LanGuard
Fonte: Elaborado pelo Autor (2013)

Por não conseguir retrair as informações, a maioria das abas irá mostrar esta mensagem informando que não tem dados disponíveis como pode ser visto na Figura 24.

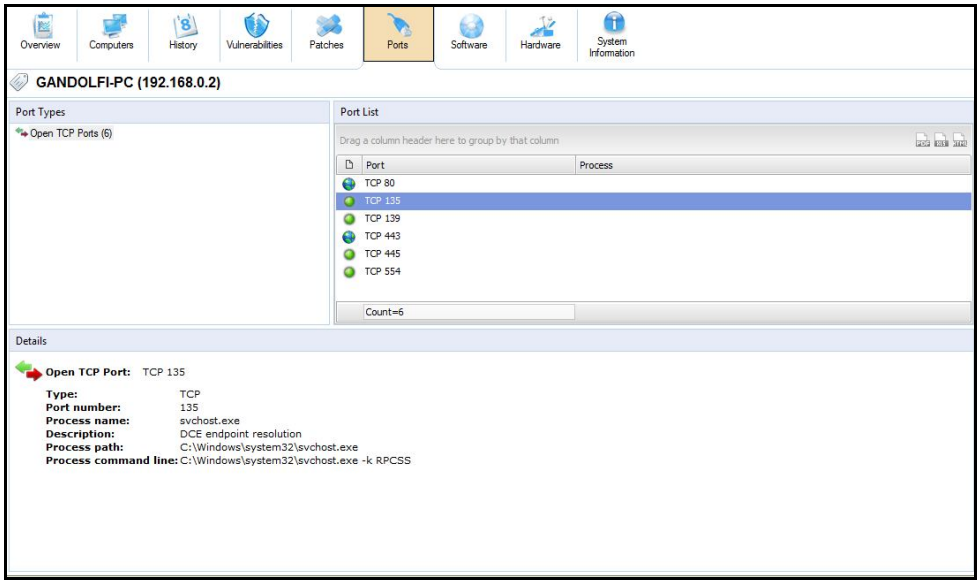

Figura 25 Aba Ports Gandolfi PC GFI LanGuard
Fonte: Elaborado pelo Autor (2013)

Porem a aba *Ports* será preenchida normalmente mostrando quais portas estão abertas e todas as informações disponíveis sobre elas na maquina escaneada como pode ser visto na Figura 25.

Após tal análise conclui-se que o *software* cumpre o esperado, pois diferentemente do Nmap consegue realizar o escaneamento de portas tanto de máquinas na rede, como da máquina em que o programa está sendo executado. Porém como o programa se propõe a também escanear ameaças causadas por outros

softwares pode se considerar a não habilidade de fazer tal escaneamento em outras maquinas um ponto fraco.

4.3 Nessus

Nessus é um software pago que possui uma versão *Trial* de 7dias limitada para testes, seus serviços são taxados por assinaturas sendo 1 ano cerca de 1500USD e 3 anos 3900USD, ele é constantemente atualizado e também permite que o usuário refine o método de escaneamento de diferentes formas, pois possui um vasto numero de *plug-ins*.

Ao contrario dos outros softwares o *Nessus* possui uma forma de garantir uma segurança interna de seus escaneamentos de forma que durante sua instalação você é forçado a criar um nome de usuário e senha para utilizar o programa, com isso somente quem possuir tais dados terá acesso as informações escaneadas.

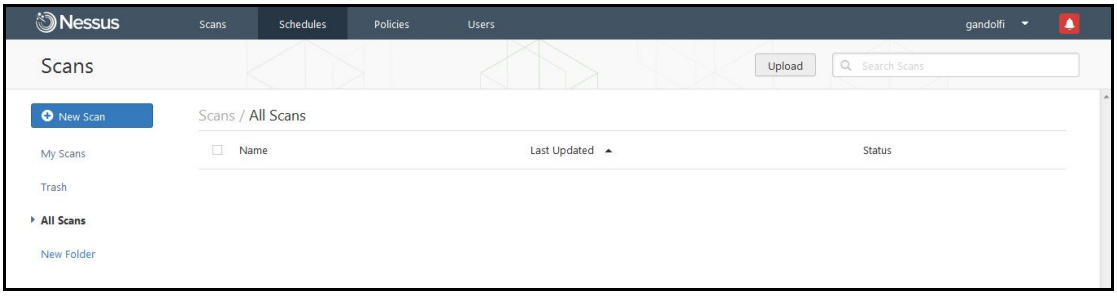

Figura 26 Tela Principal Nessus
Fonte: Elaborado pelo Autor (2013)

Depois de realizado o *login*, o programa abre sua tela principal, local onde ficam armazenados quaisquer escaneamentos realizados no passado e também a opção de realizar novos escaneamentos, note-se também que nesta tela é possível criar pastas para armazenar seus escaneamentos de forma mais organizada.

Figura 27 Aba Policies Nessus
Fonte: Elaborado pelo Autor (2013)

Diferentemente dos outros *softwares* o *Nessus* não possui métodos de escaneamento pré-programados, então se for a primeira vez que estiver utilizando antes de iniciar um escaneamento é necessário criar uma política de escaneamento na aba *Policies* como pode ser visto na Figura 28. Uma janela irá se abrir querendo saber o tipo de escaneamento desejado para configuração de parâmetros, para este trabalho foi utilizado política *Basic Network Scan*.

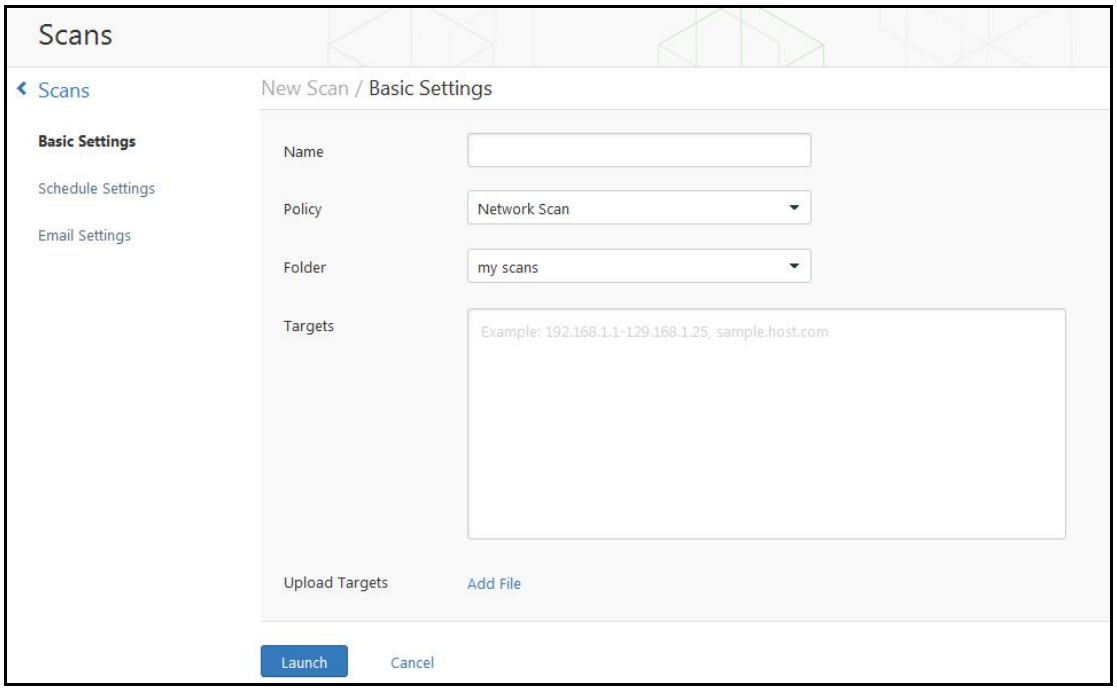

Figura 28 Layout Varredura Nessus
Fonte: Elaborado pelo Autor (2013)

Assim como nos outros *softwares* a parte de escaneamento é bem simples, só preciso criar um nome para o escaneamento para facilitar na hora de pesquisar, definir a política de escaneamento que foi previamente criada, a pasta em que será salvo o escaneamento e os alvos do escaneamento.

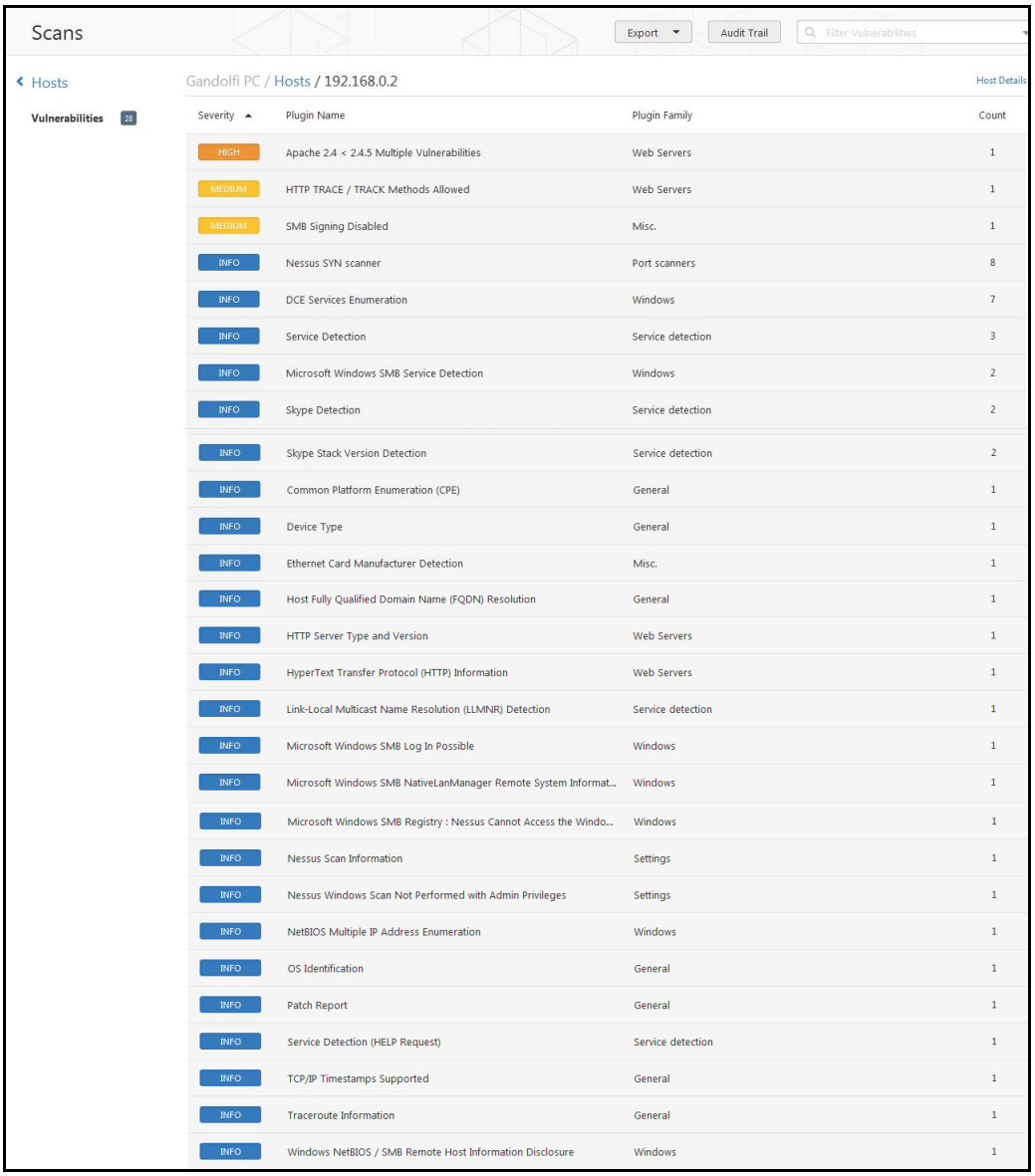

Figura 29 Overview Gandolfi PC Nessus
Fonte: Elaborado pelo Autor (2013)

Depois de realizado o escaneamento o programa irá separar todas as informações que ele considerar relevantes em tópicos de forma que o usuário pode selecionar para saber sobre tal assunto mais aprofundado. A Figura 30 mostra o escaneamento final da maquina Gandolfi PC onde se pode notar que foi classificado um tópico como alto risco, dois como médios riscos e o resto como informação sobre a máquina, a lista de portas abertas nesta máquina fica armazenada na opção "*Nessus SYN Scanner*", onde é listada quais portas estão abertas e quais serviços utilizam estas portas.

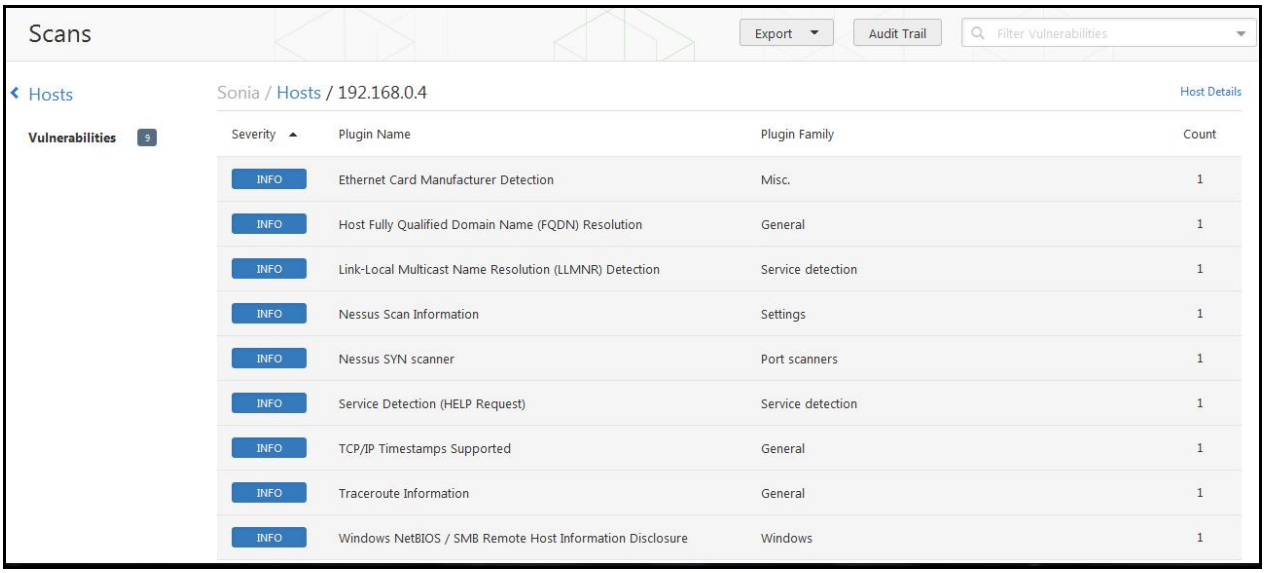

Figura 30 Overview Sonia PC Nessus
Fonte: Elaborado pelo Autor (2013)

A Figura 31 mostra o resultado da analise máquina Sonia PC, pode-se notar que o programa não encontrou nada que ele considera-se de risco nesta maquina, logo os atributos listados para essa maquina são apenas informações sobre sistema operacional, *traceroute*, lista de portas, etc.

Após visto como o programa funciona, pode-se concluir que o software Nessus cumpre o papel proposto, exibindo resultados de uma forma clara e organizada e sem muita poluição visual, com isso proporcionando ao usuário uma utilização bem mais simples e fácil.

5 CONSIDERAÇÕES FINAIS

Com a rápida evolução tecnológica evolução que estamos vivendo, é impossível garantir a segurança de seus dados sem a utilização de alguma ferramenta de segurança para seu computador ou redes de computadores.

Scanners de vulnerabilidade são ferramentas que ajudam a detectar possíveis falhas na sua rede através da analise das portas para detectar se existe alguma porta aberta em sua rede desnecessariamente que possa ser visada por alguém tentando acessar seus dados de forma indevida.

Os Softwares analisados *Nmap, GFI LanGuard e Nessus*, cumpriram seus papéis na analise da rede detectando falhas que precisavam ser checadas e concertadas

Após o estudo dos três *softwares,* acredito que o *Nessus* se saiu melhor em relação aos outros dois, pois além de fazer tudo o que foi proposto, conta com uma enorme gama de *plug-ins* em seu *website* oficial ajudando a refinar seus escaneamentos ajudando a isolar problemas específicos mais facilmente, porém caso sua empresa não esteja preparada para gastar tanto em uma licença do *Nessus,* o *Nmap* por ser *OpenSource* e consequentemente grátis é uma ótima saída.

Através deste trabalho é possível concluir-se que apesar de ajudar no combate contra invasões, scanners de vulnerabilidade apenas ajudam a proteger uma parte de sua rede, utilizar apenas essas ferramentas na grande maioria das vezes não será o bastante, então além de escanear sua rede sempre a procura de falhas é recomendado utilizar outras ferramentas de segurança como o Firewall para garantir ainda mais a segurança de suas informações.

REFERÊNCIAS

ALECRIM, E. Ataques DoS (Denial of Service) e DDoS (Distributed DoS). **Info Wester**, 2012. Disponível em: < http://www.infowester.com/ddos.php >. Acesso em: 20 maio 2013

BERNARDES, M. C**. Avaliação do uso de agentes móveis em segurança computacional**. 1999. Dissertação (Mestrado em Ciências de Computação e Matemática Computacional) - Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos, 1999. Disponível em: <http://www.teses.usp.br/teses/disponiveis/55/55134/tde-04022002-103542/>. Acesso em: 11 maio 2013.

EVANGELISTA, S. V. B. **Sistemas de Detecção de Intrusos e Sistemas de Prevenção de Intrusos: princípios e aplicação de entropia**. 2008. 74f. Trabalho de Conclusão de Curso (Tecnólogo em Tecnologia da Informação e da Comunicação), Instituto Superior de Tecnologia, Laboratório Nacional de Computação Cientifica, Petrópolis, 2008. Disponível em: <http://www.lncc.br/~borges/doc/IDS%20IPS%20e%20Entropia.TCC.pdf> Acesso em: 20 maio 2013

FOROUZAN, A. B. **Comunicação de dados e redes de computadores** 3ed Tradução: Glayson Eduardo de Figueiredo. Porto Alegre: Bookman,2006.

HOW a 'denial of service' attack works. **Cnet.com**. 2000. Disponível em < http://news.cnet.com/2100-1017-236728.html > Acesso em: 12 maio 2013

KUROSE, F. J.; Ross, W. K. **Redes de computadores e a Internet:** Uma abordagem top-down 3ed, Tradução: Arlete Simille Marques. São Paulo:PEARSON,2009.

MARTIMIANO, L. A. F. **Sobre a estruturação de informação em sistemas de segurança computacional: o uso de ontologias**. 2006. 185f. Tese (Doutorado Ciências de Computação e Matemática Computacional) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos, 2006. Disponível em: <http://www.teses.usp.br/teses/disponiveis/55/55134/tde-02102006-091853/>. Acesso em: 11 maio 2013.

O'Donnell, A. Introduction to Vulnerability Scanning. **About.com**, 2013. Disponível em < http://netsecurity.about.com/cs/hackertools/a/aa030404.htm >. Acesso em: 20 maio 2013

O que significam as siglas IPS e IDS, no contexto de redes de computadores?. **Núcleo de Processamento de Dados Universidade Federal do Espírito Santo,** 2010 Disponível em <http://www.npd.ufes.br/node/87> Acesso em: 18 maio 2013

PEREIRA, C. R. **Detecção de Intrusão em Redes de Computadores Utilizando Floresta de Caminhos Ótimos.** 2012. 76f. Dissertação(Mestrado Instituto de Biociências, Letras e Ciências Exatas) – Instituto de Biociências, Letras e Ciências Extas, Universidade Estadual Paulista, São José do Rio Preto, 2012. Disponível em < http://www.athena.biblioteca.unesp.br/F/XF2HYC6HFAH239X6VBMCFTILPR9676KNI2TXES4P9RLSKAQBM7-15036?func=full-set-set&set_number=004105&set_entry=000002&format=999>. Aceso em: 11 maio 2013

SPENCER, W. Network Attacks. **Tech-faqs.com**, 2013. Disponível em < http://www.tech-faq.com/network-attacks.html> Acesso em: 12 maio 2013

TANENBAUM, A. S.; WETHERALL, D. **Redes de Computadores.** 5ed Tradução: Daniel Vieira. São Paulo: PEARSON, 2011.

TORRES, A. **Redes de Computadores curso completo** Rio de Janeiro: Axcel,2001.

TYPES of Network Attacks. **Orbit-computer-solutions.com**, 2013. Disponível em < http://www.orbit-computer-solutions.com/Types-of-Network-Attacks.php> Acesso em: 12 maio 2013

VIOLINO, B. Scanning for Network Vulnerabilities. **CIO.com**, 2009. Disponível em: < http://www.cio.com/article/483744/Scanning_for_Network_Vulnerabilities >. Acesso em: 20 maio 2013

ESTUDO DE FERRAMENTAS PARA ESCANEAMENTO E DETECÇÃO DE ATAQUES EM REDES DE COMPUTADORES

Guilherme Lavier Santos Gandolfi, Henrique Pachioni Martins, Elvio Gilberto da Silva, André Luiz Ferraz Castro

Instituto de Informática – Universidade Do Sagrado Coração (USC) Bauru – SP

Centro de Ciências Exatas e Sociais Aplicadas– Universidade do Sagrado Coração, USC.

gandolfi3000@hotmail.com, henmartins@gmail.com

Abstract. This Article has as its objective the discussion about network security, from the basic of your functionalities and showing the different aspects that it covers and most of the available techniques to make your environment more secure, the introduction to network sweeping tools which ones have the function to detect where your network might be open for attacks, so you can fix before anyone try to take advantage of those exploits, will be utilized the programs Nmap, Nessus, GFI Languard to show how they work, their characteristics and on what they differ from each other.

Resumo. Este Artigo tem como objetivo a discussão sobre segurança em redes de computadores, desde seu básico até os diferentes aspectos que ela abrange e as varias técnicas disponíveis para deixar o seu ambiente mais seguro, a introdução a ferramentas de varredura de rede que tem como função detectar pontos onde sua rede pode estar aberta a ataques, para que você consiga concerta-los antes que alguém se aproveita de tais falhas, serão utilizados os softwares Nmap, Nessus e GFI Languard para mostrar como tais ferramentas funcionam, suas características e quais as diferenças de uma para a outra.

1. Introdução

Durante as primeiras décadas de sua existência, as redes de computadores foram usadas principalmente por pesquisadores universitários, com a finalidade de enviar mensagens de correio eletrônico, e também por funcionários de empresas para compartilhar impressoras. Sob essas condições a segurança nunca precisou de maiores cuidados. Porém, como milhões de cidadãos comuns atualmente usam as redes para executar operações bancárias, fazer compras e arquivar suas devoluções de impostos, tem surgido um ponto fraco atrás do outro, e a segurança vem se

tornando um problema de grandes proporções. Este é um assunto abrangente e inclui inúmeros tipos de problemas. Em sua forma mais simples, preocupa-se em impedir que pessoas mal-intencionadas 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 não estão autorizadas a usar. (TANENBAUM; WETHERALL, 2011).

Com isso, várias ferramentas de segurança em redes têm surgido a fim de tentar ajudar a manter sua rede livre de falhas e pontos fracos, porém se usadas por pessoas mal-intencionadas, tais ferramentas podem ajudá-lo a detectar as falhas que a rede possui, facilitando o ataque.

Através deste estudo serão analisados alguns softwares de escaneamento de rede para identificar falhas e vulnerabilidades em redes de computador. Entre eles é possível citar Nessus, Nmap e outros que serão descritos posteriormente, para coletar os dados sobre a rede a ser analisada e fazer as devidas comparações.

2. Segurança de Rede

A criptografia é o coração da segurança em rede. Se precisarmos estabelecer privacidade em uma rede, é de suma importância pensar como iremos criptografar a informação no transmissor e decodificá-la à forma original no receptor. (FOROUZAN, 2006)

Hoje em dia praticamente todas as estruturas de segurança de rede dependem do conceito de *firewall*. A ideia original do *firewall* era isolar a sua rede interna da Internet, por completo. Através da filtragem do trafego TCP/IP o firewall decide o que é permitido e o que não é. O *firewall* analisa os cabeçalhos dos pacotes de IP que passam por ele. Através desta análise, ele pode descobrir qual porta este pacote utilizará e ainda os endereços IP de origem e destino. Com base nesta informação, ele compara com uma lista de regras decide se o pacote pode prosseguir ou não. (TORRES, 2001)

2.1 Intrusion Detection System

Intrusões são difíceis de detectar porque existem muitas formas pelas quais elas podem acontecer. Podem utilizar-se de falhas na arquitetura ou como alto conhecimento em sistemas operacionais, e ao tentar corrigir algo você pode desproteger outra parte do sistema deixando o sistema vulnerável a novos ataques. As funcionalidades de um sistema de detecção tornam-se muito importantes na medida em que se pode analisar o conteúdo das conexões permitidas e

detectar as que apresentem um comportamento suspeito ou não condizente com a política implantada. (BERNARDES, 1999)

Segundo PEREIRA, C. R. (2012, p5),

> Detectar uma intrusão significa identificar qualquer comportamento suspeito no tráfego de uma rede de computadores. Sistemas de detecção de intrusos (Intrusion Detection Systems – IDSs) monitoram esse trafego detectando comportamento e pacotes suspeitos que possam danificar ou ter acesso não autorizado a informações sigilosas que trafegam pela rede. [...] Sistemas de Detecção de Intrusos são aplicados como ferramentas complementares no processo de gestão de segurança em redes de computadores, pois apesar dos esforços empregados para automatizar a tarefa de detecção e respectivas respostas ainda é indispensável a participação humana para tomar as devidas providencias no caso de alertas e relatórios que são gerados pelos IDSs.

2.2 Intrusion Prevention System

Sistemas de Prevenção de Intrusos(Intrusion Prevention System – IPS) é uma solução ativa de segurança, capaz de fornecer segurança em todos os níveis, desde o núcleo do sistema operacional até os pacotes de dados da rede.O IPS provê políticas e regras para o tráfego de rede, trabalhando em conjunto com um IDS que emite alertas em casos de tráfego suspeito. Enquanto o IDS informa sobre um potencial ataque, o IPS promove tentativas de parar o ataque com capacidade de prevenir invasões com “assinaturas” conhecidas, ele também pode impedir alguns atques não conhecidos, devido a sua base de dados de ataque genéricos. Visto como uma combinação de IDS e uma “camada de aplicação Firewall” para proteção, IPS é considerado a geração seguinte do IDS. (O..., 2010)

3. Escaneamento em redes

Novas vulnerabilidades de rede estão constantemente sendo descobertas e ameaça contra redes corporativas tem ficado cada vez mais sofisticadas. O escaneamento por vulnerabilidades pode ajudar a identificar fraquezas antes que elas se tornem perigosas para o setor tecnológico. Scanners de vulnerabilidade são produtos que analisam a rede e dispositivos de rede e então apresentam ao usuário relatórios que permitem ao mesmo responder rapidamente a problemas em potencial. Tais scanners procuram por problemas como firewalls configurados incorretamente ou servidores que possam estar suscetíveis a fraquezas. (VIOLINO, 2009)

Similar a *Sniffing* de pacotes, scanner de portas e outras “ferramentas de segurança”, *scanners* de vulnerabilidade podem ajudar a sua própria rede, ou podem ser utilizado por pessoas mal intencionadas a identificar as fraquezas de sua rede e preparar um ataque. Com isso a ideia é você utilizar tais ferramentas para identificá-las e concerta-las antes que alguém utilize as utilize contra você. (O’Donnell, 2013)

4. Metodologia

A primeira parte da pesquisa foi o levantamento bibliográfico que foi realizado com a utilização de livros, teses, dissertações e artigos de sites.

A segunda parte da pesquisa foi realizada a coleta de dados, utilizando os softwares Nessus em sua versão *trial*, Nmap e GFI Lan Guard também em sua versão *trial*. Foi feito um escaneamento em uma rede doméstica de três computadores para encontrar possíveis falhas ou fraquezas que a rede possui-se que poderiam ser utilizadas para invasão.

Todas as análises foram realizadas em computador do tipo Notebook com processador AMD Athlon TF-20, 1.6GHz, memória RAM de 2GB com o sistema operacional Windows 7 Professional 32Bits.

Após análise de todos os IPs da rede mostrada na figura 8 foram comparados os resultados obtidos nos três softwares para observar possíveis características positivas e negativas entre as análises para uma comparação entre os softwares descrever sua confiabilidade.

5. Resultados

Os resultados serão mostrados de forma que a primeira maquina analisada ira mostrar o maior numero de informação sobre o software e o seu funcionamento e as demais irão apenas mostrar diferenças entre as análises.

5.1 Nmap

Nmap é um software gratis e *Open Source* que foi desenvolvido para descobrir características de redes e auditoria de segurança, vários adiministradores de redes também acreditam ser muito útil para gestão de programação de updates e controlar o tempo que uma

maquina esta ligada. Para obtenção das informações necessárias foi utilizada sua GUI oficial do Nmap que é chamada de Zenmap.

O Software possui uma interface simples proporcionando ao usuário uma fácil utilização, onde você só precisa colocar o ip da maquina que deseja escanear e o tipo de escaneamento dentre as varias opções que o programa fornece. Após o escaneamento é finalizado o programa preenche suas abas com as informações coletadas como as portas que estão abertas, o sistema operacional, a topologia da rede em relação as maquinas escaneadas. Seu único problema é que ele não consegue obter informações da maquina em que esta sendo executado com isso ele seria melhor aproveitado em uma empresa onde só é necessário checar os computadores de seus funcionários.

5.2 GFI LanGuard

GFI Lan Guard é um software pago que porem possui uma versão *Trial* de 30dias limitada para testes, seu preço varia de acordo com o numero de maquinas que você possui na rede para serem escaneadas, alem da função de escaneamento de ips ele ainda proporciona um escaneamento geral da maquina procurando falhas e softwares que não vem sindo atualiazados corretamente que possam levar a rede a correr riscos.

Assim como o Nmap, o GFI LanGuard possui uma aba de escaneamento bem intuitiva e fácil de se utilizar, só é necessário saber o IP da maquina que você deseja fazer o escaneamento e selecionar o tipo de escaneamento que você deseja. Ao contrario do Nmap este software consegue detectar as portas e informações de sistema operacional independente de onde estiver em execução e ainda consegue colher infomações sobre outros softwares que possam estar deixando seu computador em risco, porem tal função só é possível na maquina em que o programa esta sendo executado.

5.3 Nessus

Nessus é um software pago que possui uma versão *Trial* de 7dias limitada para testes, é constantemente atualizado e também permite que o usuário refine o método de escaneamento de diferentes formas pois possui um vasto numero de *plug-ins.*

Assim como os demais softwares possui uma interface bem simples e de fácil utilização, onde após o escaneamento o programa separa as informações em tópicos para ajudar o usuário a encontrar o que procura mais facilmente. Outro ponto muito bom sobre o software é que possui

um sistema de login com isso ajudando na segurança interna onde apenas a pessoa encarregada terá acesso as informações escaneadas.

6. Referências

BERNARDES, M. C**. Avaliação do uso de agentes móveis em segurança computacional**. 1999. Dissertação (Mestrado em Ciências de Computação e Matemática Computacional) - Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos, 1999. Disponível em: <http://www.teses.usp.br/teses/disponiveis/55/55134/tde-04022002-103542/>. Acesso em: 11 maio 2013.

FOROUZAN, A. B. **Comunicação de dados e redes de computadores** 3ed Tradução: Glayson Eduardo de Figueiredo. Porto Alegre: Bookman,2006.

PEREIRA, C. R. **Detecção de Intrusão em Redes de Computadores Utilizando Floresta de Caminhos Ótimos.** 2012. 76f. Dissertação(Mestrado Instituto de Biociências, Letras e Ciências Exatas) – Instituto de Biociências, Letras e Ciências Extas, Universidade Estadual Paulista, São José do Rio Preto, 2012. Disponível em < http://www.athena.biblioteca.unesp.br/F/XF2HYC6HFAH239X6VBMCFTILPR9676KNI2TXES4P9RLSKAQBM7-15036?func=full-set-set&set_number=004105&set_entry=000002&format=999>. Aceso em: 11 maio 2013

O'DONNELL, A. Introduction to Vulnerability Scanning. **About.com**, 2013. Disponível em < http://netsecurity.about.com/cs/hackertools/a/aa030404.htm >. Acesso em: 20 maio 2013

O que significam as siglas IPS e IDS, no contexto de redes de computadores?. **Núcleo de Processamento de Dados Universidade Federal do Espírito Santo,** 2010 Disponível em <http://www.npd.ufes.br/node/87> Acesso em: 18 maio 2013

TANENBAUM, A. S.; WETHERALL, D. **Redes de Computadores.** 5ed Tradução: Daniel Vieira. São Paulo: PEARSON, 2011.

TORRES, A. **Redes de Computadores curso completo** Rio de Janeiro: Axcel,2001.

VIOLINO, B. Scanning for Network Vulnerabilities. **CIO.com**, 2009. Disponível em: < http://www.cio.com/article/483744/Scanning_for_Network_Vulnerabilities >. Acesso em: 20 maio 2013