UNIVERSIDADE DO SAGRADO CORAÇÃO

JOÃO PEDRO VALARINI MORET BRANDÃO

ANÁLISE DE SOFTWARE DE ESCANEAMENTO DE VULNERABILIDADE EM REDE DE COMPUTADORES

BAURU
2016

JOÃO PEDRO VALARINI MORET BRANDÃO

ANÁLISE DE SOFTWARE DE ESCANEAMENTO DE VULNERABILIDADE EM REDE DE COMPUTADORES

Trabalho de Conclusão de Curso apresentado ao Centro de Ciências Exatas e Sociais Aplicadas da Universidade do Sagrado Coração como parte dos requisitos para obtenção do título de bacharel em Ciência da Computação, sob orientação do Prof. Dr. Elvio Gilberto da Silva.

BAURU
2016

Brandão, João Pedro Valarini Moret

B8191a

Analise de Software de Escaneamento de Vulnerabilidade em Redes de Computadores / João Pedro Valarini Moret Brandão. -- 2016.

64f. : il.

Orientador: Prof. Dr. Elvio Gilberto da Silva.

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

1. Redes de Computadores. 2. Vulnerabilidades. 3. Escaneamento. 4. Segurança. 5. Ferramentas. I. Silva, Elvio Gilberto da. II. Título.

JOÃO PEDRO VALARINI MORET BRANDÃO

ANÁLISE DE SOFTWARE DE ESCANEAMENTO DE VULNERABILIDADE EM REDE DE COMPUTADORES

Trabalho de conclusão de curso apresentado ao Centro de Ciências Exatas e Sociais Aplicadas da Universidade Sagrado Coração como parte dos requisitos para obtenção do título de Bacharel em Ciência da Computação sob orientação do Prof. Dr. Elvio Gilberto da Silva.

Banca examinadora:

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

_____
Prof. Me. Henrique Pachioni Martins
Universidade Sagrado Coração

_____
Prof. Me. Patrick Pedreira Silva
Universidade Sagrado Coração

Bauru, 06 de Dezembro de 2016.

AGRADECIMENTOS

Primeiramente agradeço a Deus por ter me abençoado e me dado força durante todo este período acadêmico e para a elaboração deste trabalho. Agradeço também meu irmão Diego, minha cunhada Anita, meus pais Eliane e Jansen, minha namorada Walkiria, meus familiares, amigos, professores e ao meu orientador Prof.Dr. Elvio Gilberto da Silva que tanto me ajudou e incentivou neste trabalho, tendo sempre paciência e confiança ao longo das supervisões das minhas atividades. É um prazer tê-lo como meu orientador.

Quero também agradecer à Universidade do Sagrado Coração com todos seus qualificados profissionais e pessoas acima de tudo.

“Tudo é considerado impossível, até acontecer.”

(NELSON MANDELA)

RESUMO

O crescente avanço tecnológico tornou o uso de computadores tanto no ambiente empresarial quanto para uso doméstico, indispensável. Assim como, o nível de conectividade a diferentes recursos é cada vez mais amplo. Esse cenário impacta em uma maior proliferação de ameaças a segurança da informação, esta que é um dos ativos mais importantes para qualquer organização, precisando estar protegida, garantindo seus princípios de confidencialidade, integridade e disponibilidade. Estabelecer um crescimento, com uma segurança equivalente, é para os profissionais da área de redes questão crucial nos dias de hoje.A utilização de *softwares* na prevenção de intrusão nas redes de computadores deve fazer parte da política de segurança das organizações que prezam pela segurança e sigilo das informações. A organização que não tem a preocupação com suas informações se torna um alvo fácil para que seus dados sejam roubados e utilizados por terceiros. Este estudo tem como finalidade por meio de um estudo de caso analisar os *softwares* R3x, Nmap, AdvancedPort Scanner, e SoftPerfect Network Scanner, ferramentas estas de grande utilidade no escaneamento de possíveis pontos suscetíveis a falhas ou ameaças, bem como, a contribuição que podem trazer para a área segurança de redes. Este trabalho foi desenvolvido em duas partes distintas, uma fase de investigação dos aspectos teóricos com ênfase na pesquisa e revisão literária e uma etapa prática através da utilização das ferramentas que foram estudadas, a fim de atingir o resultado proposto, onde foram realizados testes práticos em um ambiente com 1 computador, 1 máquina virtual, 1 roteador e 2 smartphones com o objetivo de analisar os resultados obtidos onde foi possível notar que através das 4 ferramentas estudadas foram identificados vários itens em diferentes tipos de equipamento, obtendo ótimos resultados e por fim foi elaborado um comparativo acerca da pesquisa.

Palavras-chave: Redes de computadores. Vulnerabilidades. Escaneamento. Segurança. Ferramentas.

ABSTRACT

Technological advance contributed for computers to become indispensable at homes as well as in companies. The same way, access to a variety of content became wider. This scenario increases the risk of threats to information security which is one of the most important assets for any organization and needs to be protected, ensuring its principles of confidenciality, integrity and availability. Establishing growth and an equivalent security is a crucial issue for professionals working with computer networks. The use of software to prevent breach of computer networks should be part of the security policy of organizations that have no concern with its informations become an easy target for data stealth by third parties. This case study aims to analyze the following softwares: Nmap, Advanced Port Scanner, SoftPerfect Network Scanner and R3x, very useful tools in scanning possible vulnerable points to security or threats, this contributing to the field of network security. This research was developed in two distinct parts, a phase of investigation of the theoretical aspects with emphasis in the research and literary revision, and a practical step through the use of the tools that were studied, in order to reach the proposed result, where practical tests were developed in a environment with 1 computer, 1 virtual machine, 1 router and 2 smartphones with the objective of analyze the results obtained where it was possible to notice that by 4 tools studied were identified several items in different types of equipments, getting excellent results and a comparative was elaborated based on the research.

Key-words: Computer Networks, Vulnerabilities, Scanning. Security. Tools.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ACLs	Access Control Lists
ARP	Address Resolution Protocol
DNS	Domain Name System
FTP	File TransferProtocol
HTTP	Hypertext Transfer Protocol
ISO	International Organization for Standardization
LAN	Local Area Network
MAC	Media Access Control
MAN	MetropolitanArea Network
OSI	Open Systems Interconnection
P2P	peer-to-peer
RARP	Reverse Address Resolution Protocol
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
TCP/IP	Transmission Control Protocol/ internet Protocol
WAN	Wide Area Network

SUMÁRIO

1 INTRODUÇÃO

Como resultado do grande avanço tecnológico, o modelo de um único computador atendendo a todas as necessidades computacionais dos usuários tanto domésticos quanto empresariais, tornou – se obsoleto, pois com o surgimento das redes de computadores, os trabalhos começaram a ser realizados por vários computadores separados, porém interconectados através da rede.

Existem vários tipos diferentes de redes como: pequenas, médias e grandes, domésticas ou empresariais; vários usuários com diferentes níveis de conhecimento, além de possuir diferentes objetivos, escalas e tecnologias tornando o assunto bem abrangente (TANENBAUM, 2003).

Por abranger muitos tipos diferentes de redes e vários tipos de usuários, tanto domésticos quanto organizacionais, existem vulnerabilidades que são exploradas por usuários mal intencionados que comprometem a segurança da informação, violando seus princípios básicos que são: confidencialidade, integridade e disponibilidade.

Uma vulnerabilidade é definida como uma condição que, quando explorada por um atacante, pode resultar em uma violação de segurança (PINHEIRO; KON, 2005 citado por MARTINELO; BELLEZI, 2014).

Se a rede estiver protegida com senhas *telnet* de difícil descoberta, nomes de comunidade SNMP, acesso e uso limitado, além de possuir registros dos logs, a rede estará menos vulnerável e o risco de invasões diminui (MCCLURE; SCAMBARY; KURTZ, 2003).

Dentre os vários tipos de vulnerabilidades, alguns exemplos são: senhas fracas e de fácil adivinhação, hosts rodando serviços desnecessários como FTP, DNS e SMTP, controle de acesso a roteadores inadequados, pontos de acesso remotos inseguros e não monitorados, contas de usuários com privilégios excessivos, falta de políticas de segurança adequadas, ACLs de roteador ou *firewall* mal configuradas, vazamento de informações e *softwares* desatualizados
(MCCLURE; SCAMBARY; KURTZ, 2003).

As vulnerabilidades em redes de computadores podem ser identificadas e investigadas através de *softwares* de escaneamento de portas e de verificação de segurança como o NMap, Advanced Port Scanner, SoftPerfect Network Scanner e R3x, que são baseadas em ambiente Windows. Com base no estudo e análise de

softwares de escaneamento de vulnerabilidades em redes de computadores, bem como, sua importância, com motivação do crescente aumento da conectividade tanto de usuários domésticos quanto de empresas, elaborar um quadro comparativo com os resultados obtidos a fim de incentivar estudos acerca do assunto.

Usuários tiram proveito desta tecnologia através da exploração das vulnerabilidades da segurança da informação, e tem como objetivo cometer crimes como roubo de senhas e dados pessoais, além de prejudicar a rede cujo ataque está voltado, enviando falsos pacotes e causando lentidão em seu alvo.

Através de testes com ferramentas de escaneamento de vulnerabilidade em redes de computadores, foi possível fazer uma análise comparativa entre os *softwares* utilizados, analisando qual software de escaneamento de vulnerabilidade melhor se adequa ao tipo de rede em questão, visando auxiliar usuários tanto do ambiente doméstico quanto corporativo, a fim de que obtenham mais conhecimento sobre o assunto estudado, já que é uma área que está em constante atualização e carece de pesquisas.

2 OBJETIVOS

2.1 OBJETIVO GERAL

Analisar *softwares* de escaneamento de vulnerabilidades em redes de computadores, bem como, sua importância, e por fim, apresentar um comparativo dos resultados obtidos a fim de incentivar estudos acerca do assunto.

2.2 OBJETIVOS ESPECÍFICOS

a) Investigar técnicas de segurança, com ênfase no escopo deste trabalho.
b) Pesquisar *softwares* que possibilitem a técnica de varredura de vulnerabilidades.
c) Efetuar um levantamento teórico sobre os *softwares* escolhidos.
d) Instalar *softwares* que possibilitem a realização da análise
e) Investigar técnicas de invasão.
f) Aplicar técnicas de escaneamento e varredura de vulnerabilidades.
g) Elaborar um quadro comparativo a fim de demonstrar as características das ferramentas.

3 REVISÃO DA LITERATURA

A seguir será apresentado um levantamento teórico, o qual norteou o desenvolvimento desta pesquisa

3.1 REDES DE COMPUTADORES

De acordo com Tanenbaum e Wetherhall (2011 citado por BITENCOURT 2014), rede de computadores é um conjunto de computadores interconectados que podem trocar informações através de uma única tecnologia. O compartilhamento de recursos tem como objetivo tornar o acesso a programas, equipamentos e dados ao alcance de todos os usuários da rede, independente de recursos ou localização física, promover a comunicação confiável entre os sistemas de informação, além de melhorar o fluxo e acesso às informações.

Torres (2001) destaca que devido à necessidade da troca de informações, surgiram as redes de computadores, que não é uma tecnologia que podemos chamar de nova, pois existe desde a época dos primeiros computadores e seus componentes básicos são:

a) Servidor: Tem a função é oferecer um recurso para a rede.
b) Cliente: Micro ou dispositivo que acessa os recursos disponibilizados pela rede.
c) Recurso: Impressoras, arquivos, unidades de disco e acesso à internet que são utilizados ou oferecidos aos clientes da rede.
d) Protocolo: Linguagem utilizada pelos dispositivos de rede, de modo que seja possível trocar informações entre si.
e) Cabeamento: Tem a função de transmitir os dados que serão trocados entre os diversos dispositivos de uma rede.
f) Placa de rede: Permite que os computadores sejam conectados à uma rede através da comunicação serial, onde é transmitido apenas um bit por vez.
g) Hardware de rede: Equipamentos utilizados para melhorar a comunicação da rede, como: switches, hubs e roteadores.

Existem diferentes tipos de redes, e podem ser definidas como: pequenas, médias, grandes, domésticas ou empresariais, sendo utilizadas por vários tipos de usuários com diferentes níveis de conhecimento, além de possuir diferentes objetivos, escalas e tecnologias tornando o assunto bem abrangente (TANENBAUM, 2003).

Baseado nos conceitos de Torres (2001), o universo das redes é composto por diversos acrônimos, os mais comuns que são usados para definir o tamanho de uma rede são:

a) LAN (Local Area Network): Rede local cuja capacidade abrange algumas centenas de metros.
b) MAN (Metropolitan Area Network): Redes metropolitanas que abrangem dimensões bem maiores que as da rede LAN.
c) WAN (Wide Area Network): Rede de área extensa, que possui dimensões geográficas incalculáveis, abrangendo milhares de quilômetros.

Segundo Mendes (2007), para resolver problemas de incompatibilidade entre fabricantes, na década de 1970 a ISO (International Organization for Stardardization) desenvolveu um modelo de referência chamado OSI (Open Systems Interconnection), para que os fabricantes pudessem criar protocolos como, por exemplo, o TCP/IP, à partir deste modelo que possui sete camadas, que de acordo com a definição de Torres (2001) são:

a) Camada 7 – Aplicação: Constrói a interface entre o protocolo de comunicação e o aplicativo que envia ou recebe informações através da rede.
b) Camada 6 – Apresentação: Conhecida como camada de tradução, converte o dado recebido através da camada de aplicação em um formato compreensível pelo protocolo usado.
c) Camada 5 – Sessão: Permite que aplicações em diferentes computadores se comuniquem, definindo a transmissão e marcando os dados em transferência.
d) Camada 4 – Transporte: Responsável por pegar os dados enviados pela camada de sessão e dividi-los em pacotes a serem transmitidos pela rede.

e) Camada 3 – Rede: Realiza o endereçamento dos pacotes, converte endereços lógicos em físico, de forma que os pacotes chegam ao seu destino.
f) Camada 2 – Link de Dados: Captura os pacotes de dados que são conhecidos como nós, recebidos através da camada de Rede, transformando-os em quadros a serem trafegados pela rede, adicionando informações como endereço da placa de rede de origem e destino.
g) Camada 1 – Física: Pega os quadros enviados pela camada de link de dados e transforma em sinais compatíveis com o meio de transmissão, convertendo-os em 0s e 1s de sinais elétricos quando o meio for elétrico, e sinais luminosos quando o meio é óptico.

"O protocolo TCP/IP atualmente é o protocolo mais usado em redes locais. Isso se deve basicamente à popularização da internet, a rede mundial de computadores, já que esse protocolo foi criado para ser usado na internet" (TORRES, 2001, p.64).

Torres (2001) ainda complementa que o protocolo TCP/IP se tornou o mais utilizado, que foi devido a sua arquitetura aberta, onde qualquer fabricante pode adotar sua própria versão do TCP/IP, e por isto foi transformado em um protocolo universal, possibilitando a comunicação de todos os sistemas. É um protocolo de quatro camadas distribuídos da seguinte maneira:

a) Camada de Aplicação: Equivalente às camadas 5,6,7 do modelo OSI, comunica-se com a camada de transporte através de uma porta, vários protocolos operam nesta camada de aplicação, os mais conhecidos são: HTTP (HyperText Transfer Protocol), SMTP Simple Mail Transfer Protocol), FTP (File Transfer Protocol), SNMP (Simple Network Management Protocol) e o DNS (Domain Name System).
b) Camada de Transporte: Equivale à camada 4 do modelo OSI, responsável por pegar os dados enviados pela camada de aplicação e transformá-los em pacotes, para que sejam repassados para a camada de internet.
c) Camada de Internet: Equivalente à camada 3 do modelo OSI, responsável pelo roteamento de pacotes, informações sobre o caminho a ser percorrido, vários protocolos operam nesta camada como o IP (Internet Protocol), ARP

(Addres Resolution Protocol), ARP (Address Resolution Protocol) e RARP (Reserve Address Resolution Protocol).

d) Camada de Interface com a Rede: Equivalente às camadas 1 e 2 do modelo OSI, é responsável por enviar o datagrama através da rede, recebido pela camada de internet .

Em consequência da queda do custo de implementação de redes, é praticamente impossível pensar em um ambiente com computadores, tanto domésticos quanto empresariais não terem uma rede implementada, pois com o surgimento da internet, a utilização das redes de computadores se tornou imprescindível (TORRES, 2001).

3.2 REDES SEM FIO

Uma rede sem fio refere se a uma rede de computadores sem a necessidade do uso de cabos, com a conexão sendo feita por meio de equipamentos que utilizam a radio freqüência e comunicação infravermelha, possibilitando a conexão dos dispositivos em uma rede.

O surgimento das redes sem fio ocorreu nos anos 90 baseadas em ondas de rádio, teve inicio como complemento das redes locais cabeadas expandindo a comunicação, possui facilidade física de instalação e utilização, pois não limita os usuários a ficarem apenas conectados via cabo de rede, desde que o aparelho utilizado possua conexão wireless (COZER, 2006).

O universo das redes sem fio é composto por:

a) WPAN: É definida pelo padrão Bluetooth, afim de que um usuário projete uma rede através do alcance de uma pessoa para que consigam trocar informações sem a utilização de cabos (TANEMBAUN 2011 citado por RIBEIRO; AMADIO; GAVILAN; SANTOS, 2012).

b) WLAN: É uma rede que pode ser comparada a rede cabeada, pois oferece os mesmos recursos, é composta por transmissores, receptores e estações

cliente ligada a pontos de acesso, porém possuem um tamanho restrito (BEZERRA 2004 citado por RIBEIRO; AMADIO; GAVILAN; SANTOS, 2012).

c) WMAN: Abrange um espaço maior do que a WLAN, este sistema cresceu a partir de sistema de televisão a cabo disponível em muitas cidades, onde uma grande antena era alocada próximo ao ponto de instalação para que o sinal chegasse a casa dos usuários.
d) WWAN: Redes de longa distância, podendo abrangir de estados até continentes, bastante utilizada operadores de celulares.

A principal desvantagem das redes sem fio é em relação à segurança, porém existe outra desvantagem como, por exemplo: interferência no meio físico devido a barreiras naturais composta por objetos, paredes e árvores, o que pode variar muito influenciando na propagação do sinal, sendo assim necessário avaliar as necessidades de implantação (MARQUES, 2001).

3.3 INTERNET

Segundo Fegan e Farouzan (2009 citado por LIBANO, 2014), a Internet é formada por redes que se comunicam entre si, um conjunto de dispositivos que trocam informações. Em 1969 surgiu uma rede formada por quatro universidades norte-americanas, o que deu início à atual rede mundial de computadores.

A Internet é uma rede mundial de computadores que interconecta milhões de dispositivos computacionais (KUROSE; ROSS, 2006).

Segundo os autores supracitados, a internet teve seus primórdios nos Estados Unidos, durante os anos 60 e 70, onde foi criada e utilizada para fins militares e acadêmicos. Era denominada ARPAnet, nos anos 80 surgiu o protocolo TCP/IP como padrão de comunicação das máquinas, porém nos anos 90 ocorreu uma grande revolução na história da Internet que foi o surgimento da World Wide Web, e a Internet deixou de ser exclusivamente acadêmica tornou-se comercial e então surgiram os primeiros navegadores, sistemas de busca, sites de compra, sistema de *download* de músicas, bate papo, popularização de correio eletrônico gratuito e blogs. Nos anos 2000 deve ser destacado o surgimento das redes P2P, aumento da conectividade e velocidade da conexão.

A internet tornou-se indispensável à grande maioria da população devido ao seu desenvolvimento ao longo das décadas. Ela é utilizada para realizar diversas atividades, como: transações bancárias, compras *online*, acesso às redes sociais, entre outras atividades.

O alto grau de conectividade além de grandes benefícios inseriu em ambientes virtuais incidentes que comprometem a segurança das redes, destacando o surgimento de vírus, técnicas utilizadas para roubo de informações, e emperramento de serviços da rede e internet. Foi a partir desta questão que a segurança da informação tornou-se de extrema importância, fazendo com que massivos investimentos em ferramentas de proteção contra invasores acompanhassem este crescimento, e então a segurança da informação tornou-se de extrema importância (KUROSE; ROSS, 2006).

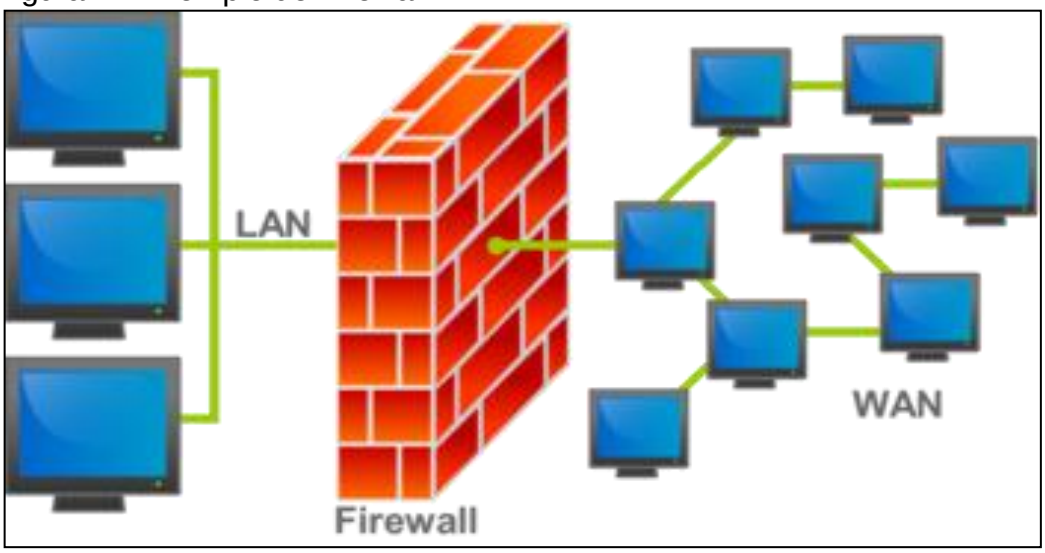
3.4 FIREWALL

De acordo com Jang (2003 citado por DUMONT, 2006), um *firewall* verifica todos os pacotes de dados que entram na rede, tomam decisões com base no tipo de dado ou serviço recebido, sendo possível ajustar diferentes níveis de proteção para diferentes computadores.

É o primeiro meio de defesa capaz de impedir a exposição das informações aos ataques externos.

Baseado nos conceitos de Teixeira e Mercer (2004), um *firewall* é composto por várias regras, geralmente é colocado no ponto de entrada da rede, sendo direcionado para uma ou mais interfaces da rede, além de controlar o acesso de serviços de toda a rede à partir de um único local, como pode ser observado na Figura 1.

Figura 1 - Exemplo de Firewall.



Fonte: Scmagazine(2016).

Analisando a Figura 1 percebe-se que ela ilustra o funcionamento de um firewall, que funciona como uma barreira, separando a rede local (LAN) da rede global (WAN).

3.5 INFORMAÇÃO

A informação é o dado trabalhado, tratado, útil e com valor significativo atribuído ou agregado a ele com um sentido natural e lógico a quem o utiliza (RESENDE, 2006).

Segundo Rezende e Abreu (2000 citado por LAUREANO, 2005), a informação é o dado com uma interpretação lógica ou natural, cujo valor é altamente significativo e pode representar grande poder para quem a possui. A informação contém valor, pois está integrada com processos, pessoas e tecnologias.

De acordo com Sêmola (2003), representa a inteligência competitiva dos negócios, e é reconhecida como um ativo crítico para a continuidade operacional da empresa.

3.6 SEGURANÇA DA INFORMAÇÃO

Conforme Beal (2005), a segurança da informação é definida como proteção dos ativos de informação e tem como objetivo evitar vazamentos, roubos, alteração,

perda e acesso indevido às informações. De acordo com o autor citado anteriormente, seus princípios básicos são:

a) **Disponibilidade:** Informação sempre disponível para acesso autorizado a quem necessite.
b) **Integridade:** É o requisito de segurança que visa à proteção da informação contra modificações não autorizadas.
c) **Confidencialidade:** Garante que a informação transmitida seja acessível somente a partes autorizadas.

Sêmola (2003), ainda complementa os princípios da segurança da informação com mais dois pontos importantes que são:

a) **Autenticidade:** Garante que em um processo de comunicação, a mensagem não sofra alterações e os remetentes não se passem por terceiros.
b) **Legalidade:** Informações produzidas de acordo com a legislação vigente.

De acordo com Melo (2010 citado por ALBUQUERQUE e SANTOS, 2013) a informação tornou-se de extrema importância para as organizações com o passar do tempo, sendo necessário o surgimento de um novo modelo de economia que tem como base, a informação.

A norma ABNT NBR ISO/IEC 17799:2005 define Segurança da informação como preservação dos conceitos apresentados acima. A Segurança da Informação deve ser vista como algo estratégico em uma empresa, pois é dependente de vários serviços como: *sites*, *e-mails*, videoconferência, telefonia e sistemas de informação.

Devido à importância da informação, foram elaboradas políticas, procedimentos e processos, para que as ações fossem orientadas no propósito de promover e implementar a segurança da informação. Baseados nos conceitos de Frangopoulos, Eloff e Venter (2008 citados por ALBUQUERQUE e SANTOS, 2013) eles complementam que embora do ponto de vista técnico a segurança da informação seja completa, é incompleta quando tratada por relações humanas que é reforçado por Mitnick (2003), que o homem é o maior causador de incidentes de segurança da informação.

Segundo Alexandria (2009), devido ao aumento do uso da internet, registros de incidentes relacionados à segurança, vulnerabilidades e falta de segurança física é essencial utilizar-se dos recursos da segurança da informação, pois existem vários

riscos relacionados à falta de segurança, que ocorre desde equipamentos mal configurados até vazamentos de informações que podem também ser danificadas por catástrofes naturais como incêndios, terremotos ou inundações.

A segurança na rede possui princípios básicos da comunicação segura que são a confidencialidade onde somente o remetente e o destinatário tenham acesso e entendam o conteúdo da mensagem sem que ela seja vista por outros usuários, autenticação na qual as entidades de comunicação confirmam se o conteúdo e remetente são legítimos e a integridade que significa a não alteração do conteúdo emitido ao destinatário (KUROSE; ROSS, 2006).

As informações devem ser bem gerenciadas tratadas de maneira adequada, esteja ela em meio físico ou eletrônico, devem ser armazenadas, transportadas e descartadas corretamente ao final de sua vida útil, portanto é necessário trabalhar uma boa gestão de segurança da informação.

3.7 GESTÃO DE SEGURANÇA

A Gestão da Segurança da Informação são práticas, procedimentos e mecanismos utilizados com a finalidade de evitar a exploração das vulnerabilidades, buscando defender os princípios da segurança da informação que são: integridade, disponibilidade, confidencialidade, autenticidade e legalidade (SÊMOLA, 2003).

De acordo com Sêmola (2003), a gestão da segurança da informação, pode ser classificada em três pontos: tecnológica, física e humana. As organizações acabam se preocupando apenas com a área tecnológica, focando-se em *firewalls* e antivírus, deixando de lado o aspecto físico e humano, sendo que esses acabam se tornando os pontos mais vulneráveis e suscetíveis a ataques.

A Gestão de Segurança deve ser utilizada como arma estratégica pelas organizações, pois seguindo corretamente os princípios da segurança da informação, é possível manter as informações de forma segura e íntegra, e esta prática de gestão de segurança da informação depende da atuação dos agentes humanos, pois um de seus maiores desafios é a engenharia social que é uma técnica usada para obter uma informação de usuários mal instruídos quanto à segurança da informação (NAKAMURA; GEUS, 2007).

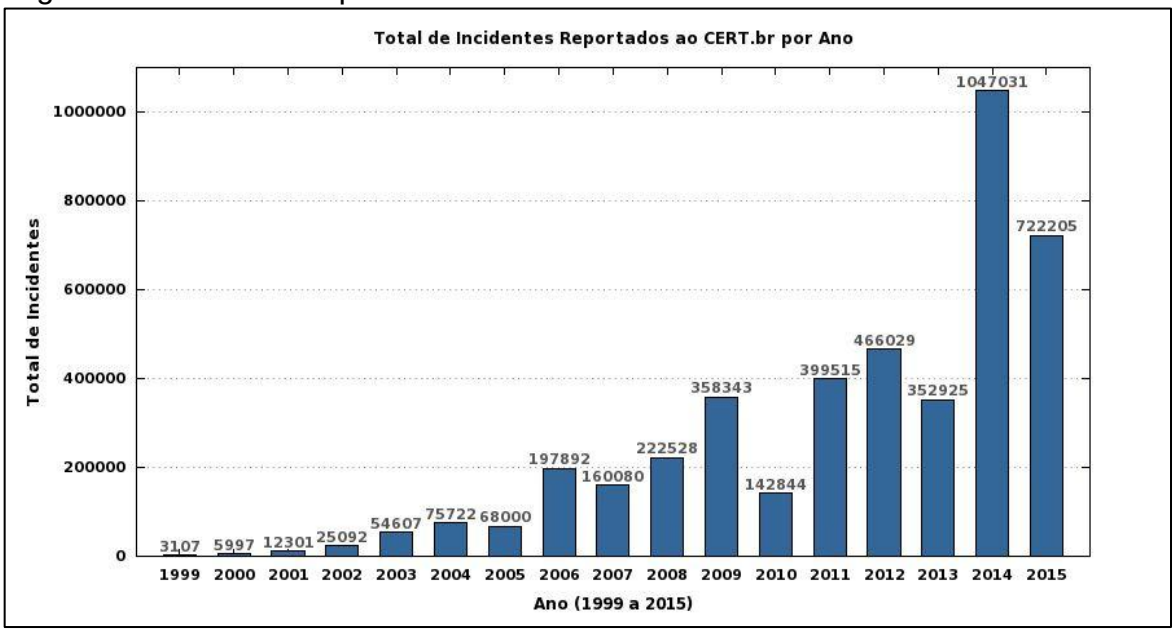
3.7.1 Ameaças à Segurança

Devido a falhas na segurança da informação e grande exploração das vulnerabilidades na segurança de rede, diariamente são relatados ataques e possíveis ameaças que podem ocorrer tanto em ambientes domésticos quanto corporativos. Geralmente os ataques que ocorrem nas organizações são feitos por usuários insatisfeitos que na maioria das vezes são da própria equipe de tecnologia. Pode ocorrer também, dificuldade para solucionar problemas como invasões não autorizadas ou desastres naturais, equipamentos de redes mal conFigurados, dados perdidos em mídias de armazenamento portátil, acessos indevidos à internet e servidores, *e-mails* maliciosos, divulgação de senhas, vazamento de informações e falhas na segurança física (MCCLURE; SCAMBARY; KURTZ, 2003).

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.BR, 2016), mantido pelo NIC.br do Comitê Gestor da Internet no Brasil é responsável por reportar incidentes de segurança em computadores que envolvam redes conectadas à Internet brasileira.

Estatísticas do CERT.BR comprovam o número elevado de incidentes reportados no ano de 2015 atingindo o número total de 722205, conforme mostra a Figura 2.

Figura 2 - Incidentes reportados ao Cert.br de 1999 a dezembro 2015.

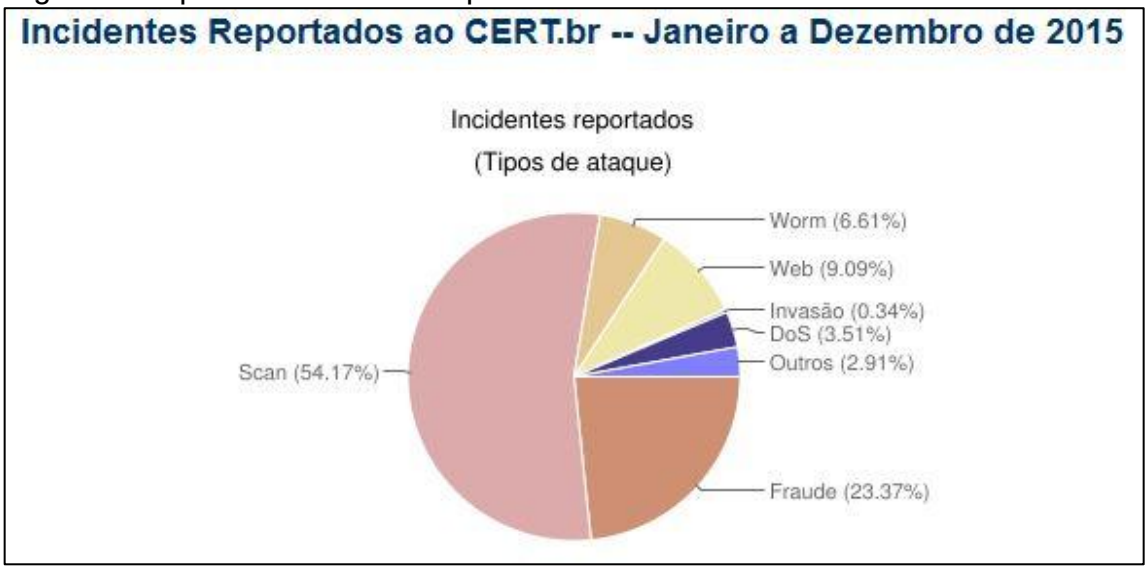


Fonte: Cert.br (2016).

Pode-se observar de acordo com a Figura 2 que devido ao aumento da conectividade ao longo dos anos, aumentou também o número de incidentes.

Dentre estes 54,17% são ataques do tipo Scan, que são notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles, os dados completos podem ser vistos na Figura 3.

Figura 3 - Tipos de incidentes reportados no ano de 2015.



Fonte: Cert.br (2016).

3.8 VULNERABILIDADE

De acordo com o Cert.org (2014 citado por BITENCOURT, 2014), uma vulnerabilidade é uma condição que quando bem explorada pelo atacante pode resultar em uma violação de segurança, ou seja, um ponto suscetível a ataques que tem várias origens devido a diversos tipos de falhas como: física, *hardware*, *software*, natural e humana.

Uma vulnerabilidade é definida por (PINHEIRO; KON, 2005 citado por MARTINELO; BELLEZI, 2014) como um ponto do sistema suscetível a ataques. Uma ameaça pode explorar uma vulnerabilidade para concretizar o ataque.

As vulnerabilidades são originadas de falhas que na maioria das vezes não são intencionais, estas falhas podem, ser: físicas, humanas, *hardware*, naturais e através de *softwares*. Muitas vulnerabilidades são criadas com utilização de *softwares* desenvolvidos para este fim.

3.8.1 Ameaça

Para Sêmola (2003), ameaça é a possibilidade de um agente, interno ou externo, explorar acidentalmente, através da falta de orientação de riscos à segurança aos funcionários e usuários, ou propositalmente, provocando invasões, fraudes e causando roubo de informações com objetivo de explorar vulnerabilidades específicas.

3.9 EXPLORAÇÃO DE VULNERABILIDADES

"À medida que o atacante avalia a rede, ele explora as vulnerabilidades para determinar precisamente como obter o controle dos valiosos bens de informação" (TOMAS, 2007, p.345). De acordo com McClure, Scambary e Kurtz (2003), toda informação está sujeita à vulnerabilidade, que é um ponto suscetível a ataques, existentes devido a falhas de conFiguração ou inexistência de medidas de proteção adequadas, sejam elas físicas, onde podem ocorrer vandalismo e catástrofes naturais, ou lógicas, que quando bem exploradas, resultam em vários tipos de ataque como: *dumpster diving* ou *trashing*, engenharia social, ataque físico, *packet sniffing*, port *scanning*, *scanning* de vulnerabilidades, *firewalking*, *worms* e *malwares* que quando bem sucedidos resultam na violação da segurança da informação.

3.9.1 Dumpster diving ou Trashing

De acordo com Harris (2010 citado por TENORIO, 2013), dumpster diving ou trashing refere-se ao conceito de vasculhar o lixo descartado referente aos arquivos e documentos da organização, onde o atacante teria que obter acesso físico ao local onde o lixo é mantido, que na maioria das vezes é uma área desprotegida, e não é uma técnica ética, porém não é ilegal.

Mitnick (2003) afirma que esta é uma das técnicas utilizadas para realizar um ataque, é eficiente e muito comum. Consiste em explorar o lixo com objetivo de obter informações como dados da empresa ou da rede, assim como senhas, informações pessoais e confidenciais, já que na maioria das vezes o descarte das informações ao final da vida útil é feito de maneira incorreta.

3.9.2 Engenharia social

Engenharia Social (ES) é a arte ou técnica que tem como objetivo obter informações como: senhas pessoais, IP de servidores, endereços de email, informações privilegiadas e sigilosas, explora as fraquezas humanas e sociais através da persuasão, influência e manipulação (MITNICK, 2003).

Segundo Granger (2002 citado por POPPER e BRIGNOLI 2003), existe várias técnicas de engenharia social, como: contato telefônico, onde o hacker soluciona todas suas dúvidas de maneira que o atendente por obrigação acaba passando informações; compartilhamento e uso de senhas consideradas fracas e de fácil adivinhação; invasão do *hacker* na empresa se passando por um técnico que fará manutenção de um problema causado por ele mesmo, na expectativa de resolução do problema, os funcionários fornecem informações valiosas sobre o funcionamento da rede, sistemas e informações sobre a empresa

Para que um ataque tenha sucesso, o atacante pode usar várias habilidades psicológicas como: poder e autoridade, reciprocidade, tendência natural para agradar e ser útil com o objetivo de que a informação seja extraída sem o levantamento de qualquer suspeita.

Deve-se ficar atento às ações da engenharia social, pois a maioria das soluções de segurança disponibiliza apenas dispositivos tecnológicos para o combate a essas ameaças, deixando uma lacuna nesta área que necessita de uma abordagem diferente.

Uma das formas de ataque realizado pelo engenheiro social é através da utilização de e-mail através do envio de spams e vírus nos anexos, segundo Tagiarol (2010 citado por MARTINELLO E BELLEZI 2014), no ano 2000 o vírus “I Love You” infectou milhões de usuários, na expectativa e curiosidade de descobrir que era o remetente, acabavam infectando o computador, neste caso podemos concluir que o ataque foi direcionado à parte psicológica do usuário.

Uma das técnicas de defesas e prevenção acerca da ES é orientar os funcionários a não passarem informações de nenhum caráter correspondente a empresa, bem como, a instalação de sistemas de monitoramento, seja telefônico ou *web*.

Podemos concluir que se não houver conscientização sobre esta técnica e as vulnerabilidades que podem ser descobertas através deste meio, a segurança da informação será afetada.

3.9.3 Ataque Físico

Tipo de ataque que visa danificar ou até mesmo furtar equipamentos que contém informações. É necessário tomar medidas de proteção e vigilância no perímetro em que os equipamentos se encontram através do controle de acesso, instalação de câmeras de segurança, fechaduras eletrônicas além da supervisão de visitantes e funcionários de outras áreas, a fim de evitar possíveis transtornos (MELLO, 2006).

3.9.4 Packet Sniffing

É um método que verifica cada pacote trafegado através de uma rede de computadores, por meio de ferramentas administrativas ou de rede, chamadas *sniffers*, na qual um usuário detecta os dados contidos nos pacotes pertencentes a outros usuários. Administradores de rede utilizam este método para monitorar atividades, diagnosticar problemas e analisar o desempenho da rede (ANSARI; RAJEEV; CHANDRASHEKAR, 2003).

3.9.5 Firewalking

Segundo Nakamura e Geus (2007), é uma técnica implementada em uma ferramenta similar ao *traceroute*, que pode ser utilizada para a obtenção de informações sobre uma rede protegida por *firewall*, permitindo que os pacotes passem por portas em um *gateway*, além de mapear roteadores encontrados antes do *firewall*.

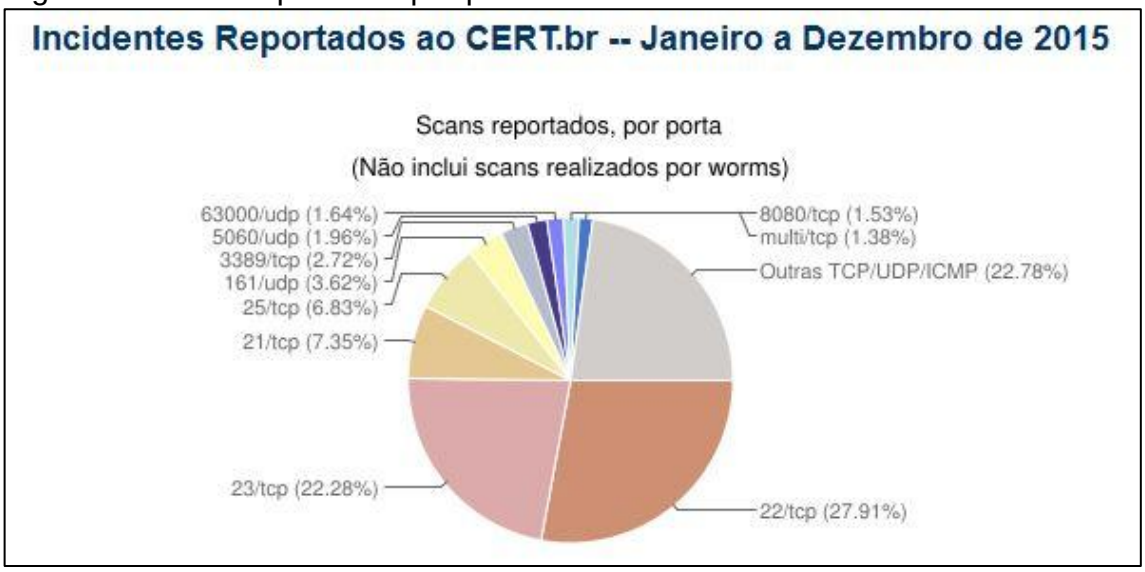
Permite a junção do *traceroute* com o *port scan*, pois utiliza elemento das duas técnicas. Para utilização do *firewalking* é necessário conhecer os endereços do último *gateway* e host atrás do *firewall*. Este tipo de ataque possui várias fases, e é bastante utilizado para descobrir se a rede possui portas abertas para que possibilite ao atacante fazer uma varredura nas aplicações ativas.

3.9.6 Port Scan

De acordo com a Cert.br (2016), é uma técnica que efetua buscas minuciosas em redes, com objetivo de identificar computadores ativos na rede, e coletar informações como, serviços e programas instalados para através desta coleta, associar possíveis vulnerabilidades nos computadores, e consequentemente na rede onde foi realizada a varredura por meio do mapeamento das portas TCP e UDP. Pode ser usada de maneira legítima, por pessoas devidamente autorizadas para verificar a segurança da rede, afim de tomar medidas preventivas, ou utilizada de maneira maliciosa por atacantes com o objetivo de explorar as vulnerabilidades encontradas nos serviços disponibilizados.

Baseado em estatísticas retratadas pelo CERT.br, pode se observar dados sobre Scans reportados por porta, conforme mostra Figura 4.

Figura 4 - Scans reportados por porta ao Cert.br de 1999 a Dezembro de 2015.



Fonte: Cert.br (2016).

3.9.7 Scanning de Vulnerabilidades

De acordo com Nakamura e Geus (2007), o *scanning* de vulnerabilidades realiza vários tipos de testes em uma rede, com objetivo de encontrar falhas de segurança em protocolos, serviços, aplicativos ou sistemas operacionais.

Quando esta técnica é efetuada por um atacante, pode prejudicar a segurança da informação, já quando utilizada pelo administrador da rede em

questão, pode evitar e prevenir futuros ataques ou danos a segurança da informação.

> Atacar as vulnerabilidades costumava ser um procedimento tempo-intensivo que exigia muito conhecimento por parte do atacante. Entretanto hoje, ferramentas automatizadas mudaram tudo isso. Já quase se foram os dias em que se tinha de adivinhar quais eram os códigos de exploração publicamente disponíveis e manter todos eles para ser efetivo (TOMAS, 2007, p. 345).

Para efetuar este escaneamento são utilizados *softwares* chamados de scanners de vulnerabilidades, que analisam riscos em roteadores, *switches*, *firewalls*, servidores, computadores, ou seja, equipamentos ligados à rede.

3.9.8 Malwares

De acordo com a CERT.br (2012), códigos maliciosos (*malwares*) são programas desenvolvidos para executar ações maliciosas em um computador, através da exploração de vulnerabilidades de programas instalados, arquivos obtidos em anexos de mensagens eletrônicas ou diretamente através de arquivos compartilhados pela rede.

3.9.9 Worms

É um programa capaz de se propagar automaticamente pelas redes. Envia cópias de si mesmo de computador para computador, explorando automaticamente as vulnerabilidades, são responsáveis por consumir muitos recursos devido a grande quantidade de cópias de si mesmo, como conseqüência, afetam o desempenho da rede (CERT.BR,2012).

3.10 IMPORTÂNCIA DA ANÁLISE DE VULNERABILIDADES

A Análise de Vulnerabilidades consiste em identificar e eliminar sistematicamente vulnerabilidades de um sistema (MÓDULO SECURITY, 2013).

Segundo Martinelo e Bellezi (2014 citado por BITENCOURT, 2014), em uma rede de computadores com diversos usuários ativos, manter a rede livre de vulnerabilidades é um trabalho minucioso e complexo para os administradores de

rede, pois as maiores dificuldades encontradas para manter a rede em segurança, é o fato da liberdade do usuário em instalar novos *softwares*, desconhecimento da prevenção contra *malwares* que através de e-mails falsos e mensagens em redes sociais instalam códigos maliciosos, diversidade de versões de *software* e sistemas operacionais, estes fatores citados acabam dificultando e impossibilitando os profissionais de TI a estarem cientes de todas as vulnerabilidades descobertas, principalmente as mais recentes.

Fatores como estes tornam indispensável ao administrador ferramentas que o auxilie a manter o ambiente computacional e consequentemente a rede o menos vulnerável possível.

3.11 FERRAMENTAS

Serão apresentadas a seguir algumas ferramentas para posterior análise.

3.11.1 Nmap

O Nmap é um software que possui versões suportadas para Unix, Windows e MacOS, é utilizado tanto por interface console como também interface gráfica, é um utilitário livre e de código aberto, usado para exploração de redes, segurança e auditoria, é capaz de examinar grandes redes ou apenas um host, oferece inúmeros recursos e funcionalidades, como detecção do Sistema Operacional remoto, MAC Adress, Internet Protocol (IP), rápido exame de multiportas por *ping* entre outras.

A função principal do Nmap é realizar uma varredura em portas (TCP) e o retorno dessa varredura é classificado em um dos seguintes estados: open (aberta), *closed* (fechada), *filtered* (filtrada), *unfiltered* (não filtrada) e a combinação de *open*/*filtered* ou *closed*/*filtered* (Lyon 2009 citado por LOPES, CARVALHO, COSTA, 2013).

O uso mais simples do Nmap é escanear diretamente uma máquina da rede, onde uma quantidade enorme de portas TCP será examinada na máquina alvo, e cada porta será classificada de acordo com seu estado.

Conforme Morimoto (2010 citado por LOPES, CARVALHO, COSTA, 2013), o Nmap não é especifico para uma aplicação e sim de uso geral. Vários outros

softwares que são utilizados para gerencia e controle de redes de computadores fazem uso do Nmap, ele é um dos componentes-base usados.

O *software* funciona através do envio pacotes IP aos hosts e através de requisições e respostas específicas capazes de determinar: hosts disponíveis na rede, serviços, aplicações e versões executadas, filtros de pacotes e firewalls em uso além de outros itens relacionados a rede. Em geral o Nmap opera nas camadas de rede e transporte, podendo também manipular dados na camada de enlace e aplicação.

3.11.2 R3x

O R3x é um *software* gratuito que fazia parte dos 5 *softwares* de segurança mais usados no mundo antes do lançamento de seu sucessor, o Languard Network Scanner que pode ser rodado em qualquer computador com o sistema operacional Windows que pode detectar uma série de itens como: *hosts* ativos, endereço IPV4, serviços rodados pelo sistema e informações detalhadas sobre os serviços, MAC address e grupo de trabalho.

Este programa, inicialmente chamado de Project R3x, destaca-se por detectar problemas nos sistemas com muita eficiência além de ser um *software* rápido e de fácil utilização.

3.11.3 Advanced Port Scanner

Segundo o próprio site da ferramenta, o Advanced Port Scanner é um *scanner* de rede gratuito que possibilita realizar o escaneamento de várias portas, é um *software* útil, rápido e de fácil utilização e interface gráfica bem desenvolvida, realiza o escaneamento através do *range* de IP pré-definido, por exemplo: de 192.168.1.0 até 192.168.1.255, através dele é possível verificar hosts ativos na rede, analisar portas, usuário, grupo de trabalho, sistema operacional, MAC address e obter acesso aos recursos encontrados como pastas compartilhadas, HTTP, HTTPS e FTP, realizar desligamento remoto e até mesmo obter acesso aos computadores via Radmin.

3.11.4 SoftPerfect Network Scanner

Segundo o próprio site da ferramenta, o SoftPerfect Network Scanner é um *software* gratuito que é capaz descobrir todos os equipamentos que estejam conectados em uma determinada rede apenas definindo a faixa de endereços a ser analisada e obter diversas informações úteis como: IP's dos dispositivos, pastas compartilhadas, portas abertas, sistemas operacionais e compartilhamentos administrativos.

4 TRABALHOS CORRELATOS

Este trabalho apresenta uma análise de aspectos correspondentes à segurança em redes de computadores, com ênfase no uso de *softwares* de escaneamento e descoberta de vulnerabilidades. Para realização da pesquisa, foram utilizados alguns estudos correspondentes e semelhantes ao escopo do trabalho.

A proposta de Bittencourt (2014) é bem semelhante ao trabalho que está em desenvolvimento, onde o mesmo equiparou as ferramentas Nessus e OpenVAS com objetivo de obter pontos positivos e negativos em relação a eficiência e usabilidade destes *softwares* afim de elaborar um quadro comparativo e através destes , foi observado diferentes características entre eles, como o tempo de escaneamento e tipo de sistema operacional em que a ferramenta melhor trabalha.

O escopo do trabalho realizado por Tenório (2013) foi muito importante para auxiliar nos tópicos propostos pela pesquisa, pois contém várias informações sobre técnicas de invasão, exploração de vulnerabilidades e métodos de análise e escaneamento de portas através de *scanners* e análise de pacotes com a utilização de ataques do tipo Fraggle, Synflood e Port Scan.

Dumont (2006) abordou vários conceitos relacionados à segurança da informação no ambiente de servidores Linux, que foram primordiais para realização da pesquisa e entendimento do assunto.

Foi concluído através da citação destes trabalhos, que o cenário computacional e tecnológico atual é muito propício a ataques e vulnerabilidades, devido a este rápido avanço, é necessário utilizar várias ferramentas a fim de investigar técnicas de segurança contribuir com a segurança da informação.

5 METODOLOGIA

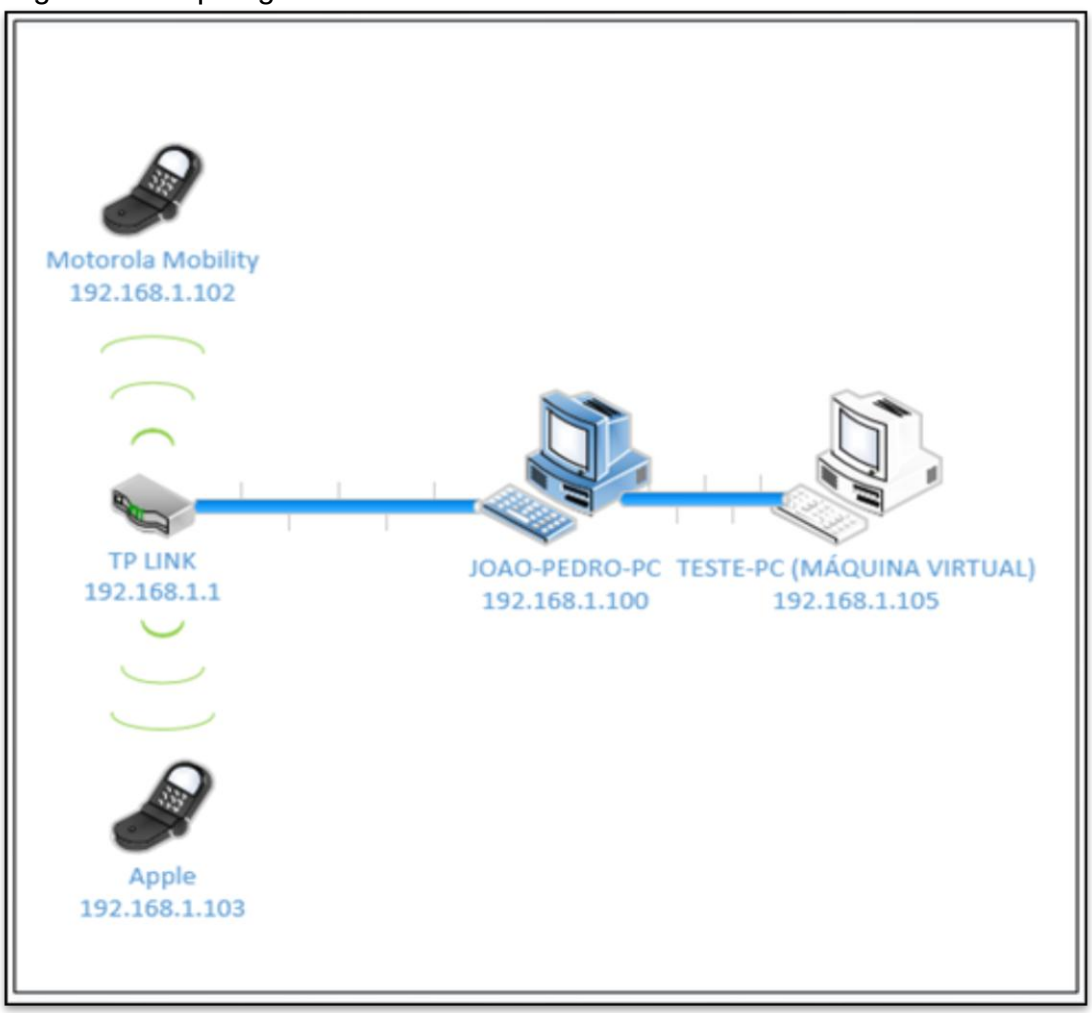
Este trabalho foi desenvolvido em duas partes distintas: uma fase de investigação dos aspectos teóricos e uma etapa prática de aplicação das técnicas de escaneamento e varredura de vulnerabilidades em redes de computadores.

Na primeira fase foi dada ênfase a pesquisa e revisão literária sobre os conceitos, definições e técnicas utilizadas para o roubo de informações e análise de vulnerabilidades, com estudos realizados na Internet através da pesquisa, leitura e coleta de informações de artigos científicos e livros relacionados à área de computação como redes, segurança e gestão. Essa pesquisa teve a finalidade de se obter conhecimento para que se possa ter uma visão geral tanto sobre o ambiente em que a segunda fase do trabalho atuará, quanto as ameaças existentes e a maneiras de encontrar e explorar vulnerabilidades existentes no ambiente de redes de computadores.

Foram abordados vários temas na pesquisa, como: redes de computadores, internet, segurança da informação que formam a base da pesquisa, além de assuntos relacionados às ameaças, ataques e vulnerabilidades que podem prejudicar o funcionamento de uma rede de computadores.

Foram pesquisados vários *softwares* que possibilitam realizar a análise de vulnerabilidades em redes de computadores. Os *softwares* que foram utilizados na segunda parte do projeto são: Nmap, R3x, Advanced Port Scanner e SoftPerfect Network Scanner. Para que a análise pudesse ser concluída foram realizados os testes em um ambiente com 5 equipamentos, sendo 1 computador com Windows SevenUltimate 64 *bits*, processador core i3 e 4GB de memória RAM, 1 máquina virtual com Windows Seven Professional 32 *bits* com a virtualização realizada através do Oracle Virtual Box e 2GB de memória RAM, 1 roteador TP-LINK 150Mbps de 3 portas, sendo 2 LAN’s e 1 WAN, 1 *smartphone* Motorola Moto G2 e 1 *smartphone* Iphone 3 da Apple, conforme ilustra a Figura 5.

Figura 5 – Topologia da rede.

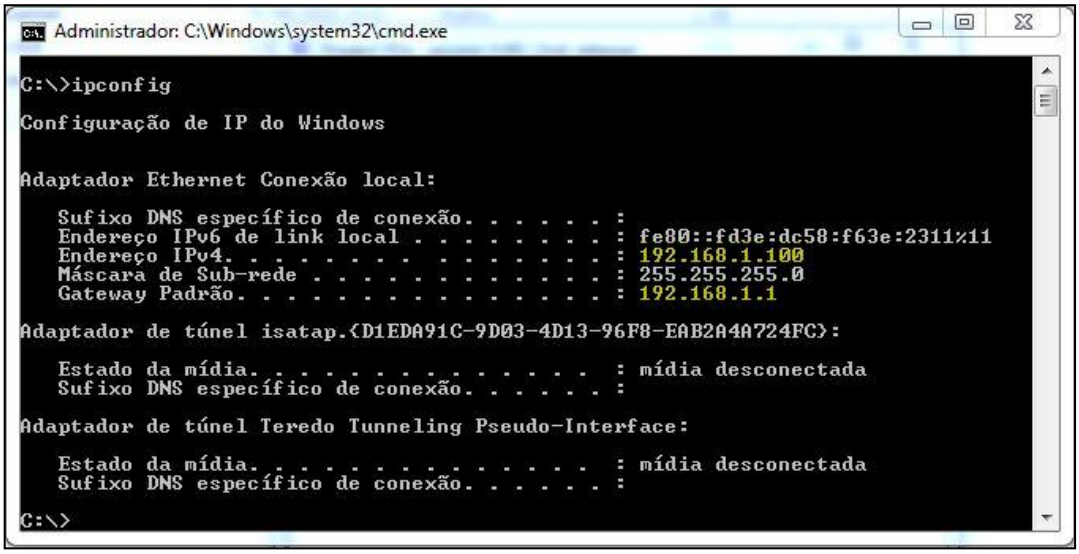


Fonte: Elaborada pelo autor

Foram utilizadas 4 ferramentas de escaneamento de rede, as quais permitam obter informações sobre os equipamentos que fazem parte da mesma, como: Endereço IPV4, *hostname, mac address*, *hosts* ativos, portas utilizadas, grupo de trabalho, compartilhamentos, última inicialização e tempo de resposta; e à partir destes dados explorar possíveis vulnerabilidades detectadas.

Em teste efetuado utilizando o comando “ipconfig” através do MS-DOS foi detectado que a rede ilustrada na Figura 5 pertence ao endereço IP atribuído por DHCP por meio do roteador, e sua terceira casa do endereço IP, por exemplo, 192.168.”1”.165 é 1, conforme pode ser visto na Figura 6.

Figura 6 – Comando ipconfig no MS-DOS.



Fonte: Elaborada pelo autor

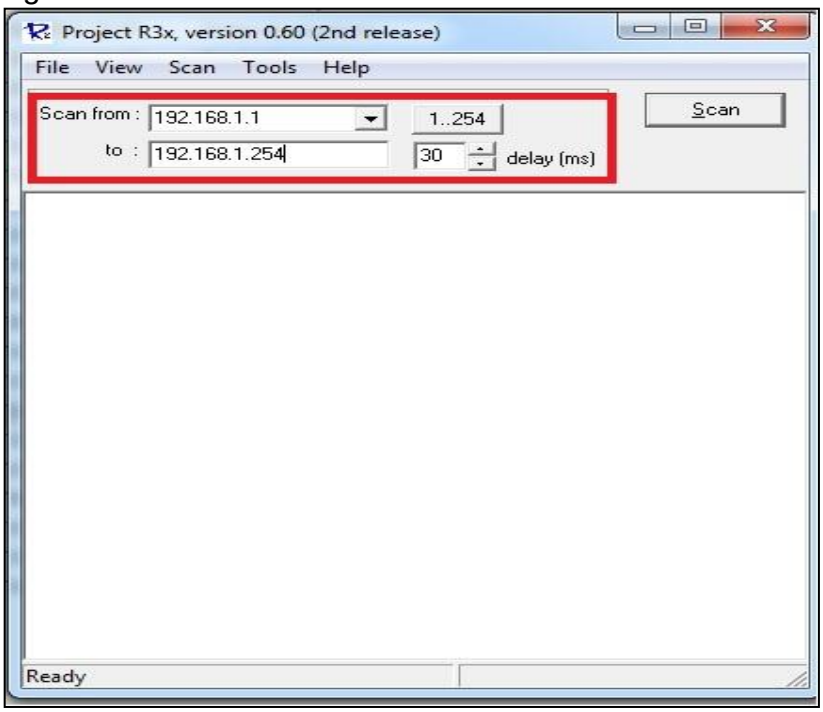
6 RESULTADOS

A seguir serão apresentadas as ferramentas utilizadas para atingir o objetivo proposto.

6.1 R3X

Para realizar o escaneamento através da ferramenta R3x, cuja interface é bem simples, foi necessário definir um intervalo de a ser escaneado baseado na descoberta do IP confome ilustrado na Figura 6, portanto, baseando-se na rede que é 192.168.1.0, foi inserido o seguinte endereço, 192.168.1.1 até 192.168.1.254, conforme ilustra a Figura 7.

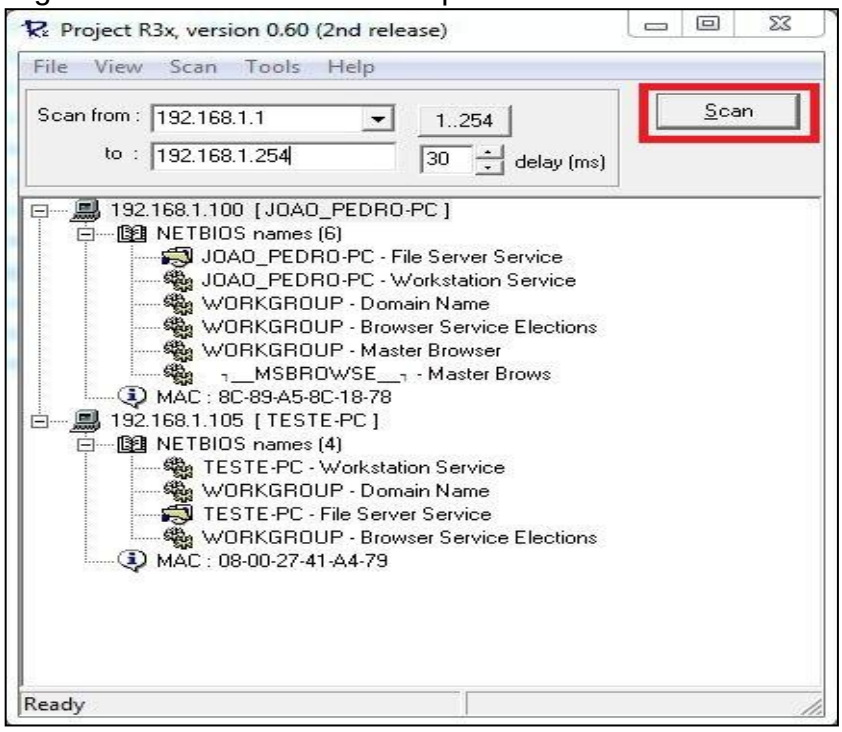
Figura 7 – Tela inicial ferramenta R3x.



Fonte: R3x (2016).

Para realizar a varredura foi necessário apenas clicar no botão “Scan”, o resultado obtido pode ser visualizado na Figura 8.

Figura 8 – Resultados obtidos pela ferramenta R3x.



Fonte: R3x (2016).

Como pode ser observado na Figura 8, foram obtidas algumas informações sobre os equipamentos na rede, como: hosts ativos, endereço IPV4, MAC address, hostname, grupo de trabalho, serviços e especificação dos serviços.

Conforme resultados obtidos através do escaneamento realizado, foram identificados 2 equipamentos na rede, 1 computador cujo endereço IPV4 é 192.168.1.100 e seu hostname é JOAO_PEDRO-PC, foram identificados alguns itens como: endereço IPV4, MAC address, hostname, grupo de trabalho, serviços e especificação dos serviços que também foram identificados no outro equipamento que faz parte da rede, que é 1 máquina virtual de endereço IPV4 192.168.1.105 e hostname TESTE-PC. Para ser concluído, o escanemento foi realizado em mais ou menos 45 segundos, que foi cronometrado através de um smartphone. Os itens detectados podem ser vistos com mais clareza no Quadro 1.

Quadro 1 – Análise por equipamento ferramenta R3x.

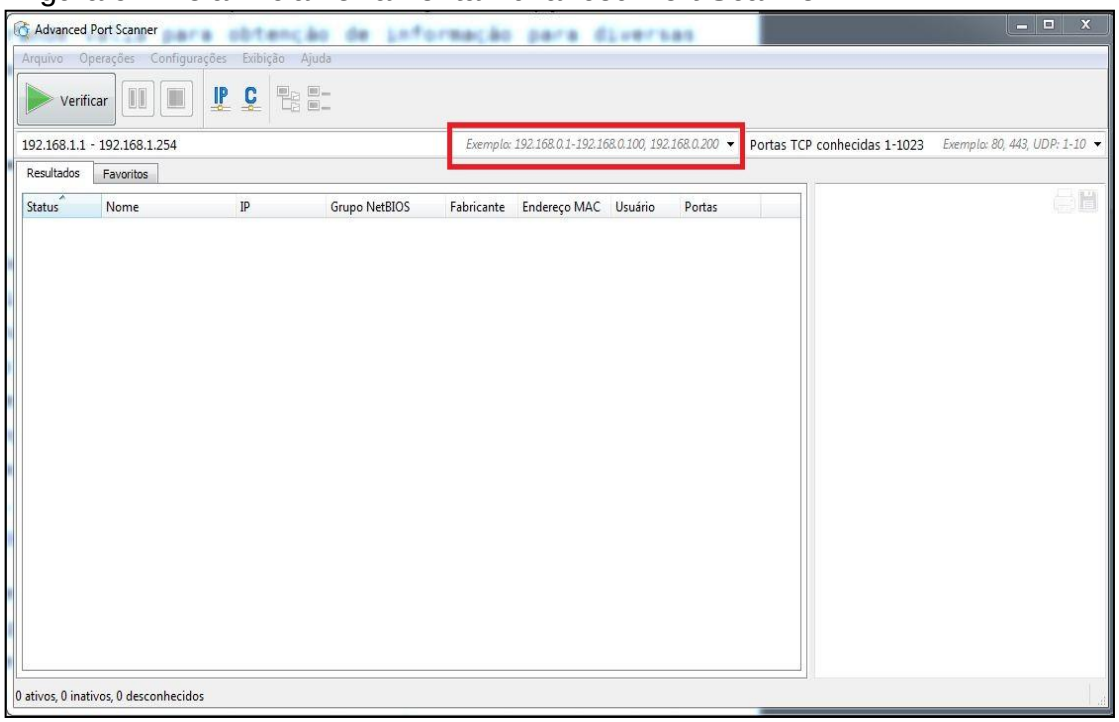
	R3x	
	EQUIPAMENTOS	
	COMPUTADOR	**MÁQUINA VIRTUAL**
	Hosts Ativos	Hosts Ativos
	Endereço IPV4	Endereço IPV4
	MAC address	MAC address
	Hostname	Hostname
	Grupo de trabalho	Grupo de trabalho
	Serviços	Serviços
	Especificação dos serviços	Especificação dos serviços
TOTAL	**7**	**7**

Fonte: Elaborada pelo autor

6.2 ADVANCED PORT SCANNER

O processo de escaneamento realizado através da ferramenta Advanced Port Scanner obteve ótimos resultados, detectou os 5 equipamentos presentes na rede e vários itens a serem analisados. A tela inicial do programa possui uma interface bem simples e intuitiva, contendo exemplos a serem aplicados no escaneamento.

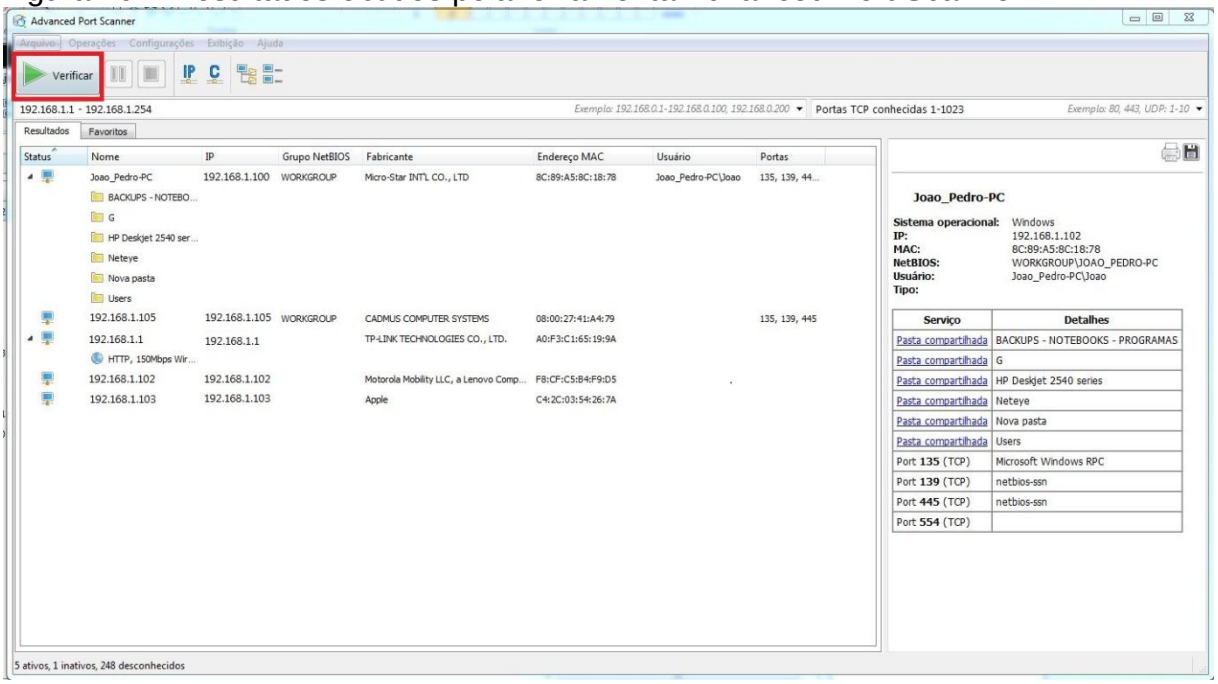
Figura 9 – Tela inicial ferramenta Advanced Port Scanner.



Fonte: Advanced Port Scanner (2016).

Possuindo conhecimento prévio da classe de IP e sub-rede obtido através da Figura 6, foi definido o escaneamento para procurar por hosts ativos do range de IP 192.168.1.1 até 192.168.1.254 e logo após a definição dos alvos, foi clicado no botão “Verificar” onde foi necessário cerca de 1 minuto e 50 segundos para o escaneamento ser concluído, este tempo foi obtido através do cronometro de um smartphone, o resultado pode ser observado na Figura 10.

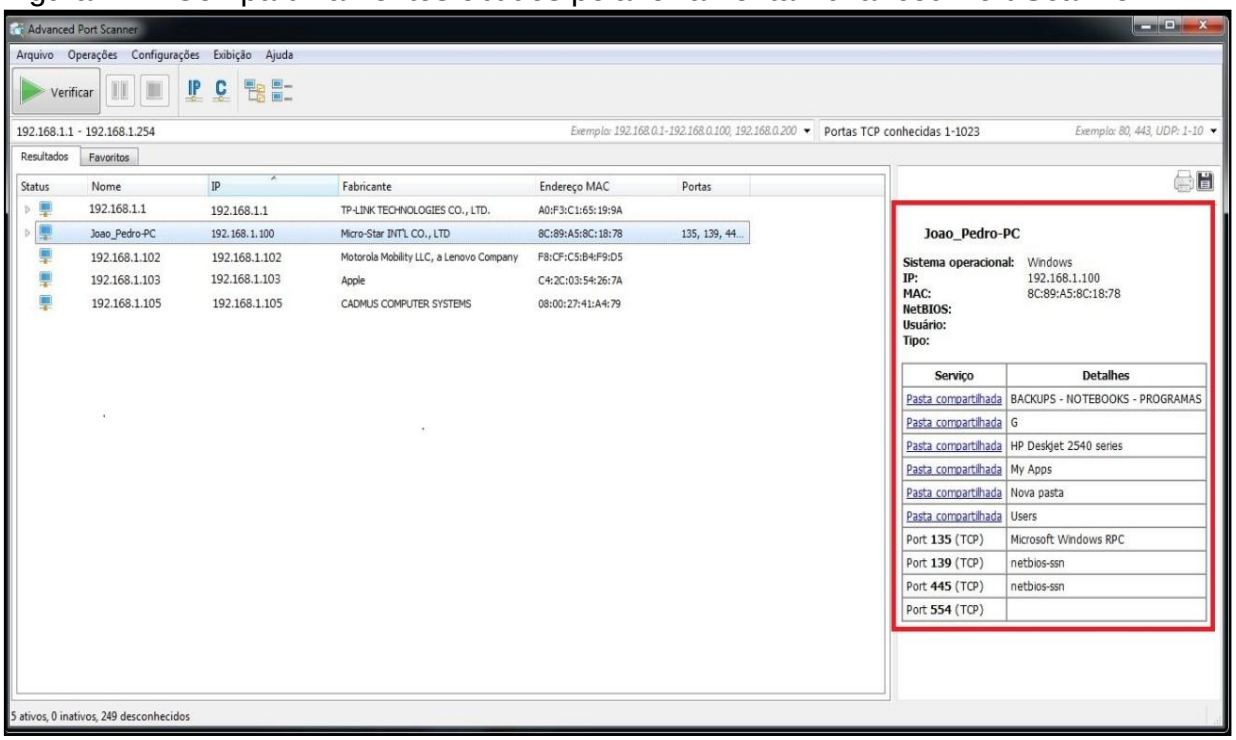
Figura 10 – Resultados obtidos pela ferramenta Advanced Port Scanner.



Fonte: Advanced Port Scanner (2016).

Foi observado que a ferramenta detectou os 5 equipamentos presentes na rede, roteador, computador, 2 smartphones e máquina virtual respectivamente. Foi obtido no geral informações como endereço IPV4, características dos aparelhos, MAC address, número de portas analisadas, portas abertas, sistema operacional, compartilhamentos, impressoras, fabricante dos aparelhos, hostname, grupo de trabalho e usuário. A ferramenta foi mais eficaz ao verificar o computador, onde detectou 11 itens, na máquina virtual e roteador foram obtidos 5 itens e nos smartphones apenas 4 itens. Pode ser observado que a ferramenta detalha os compartilhamentos conforme pode ser visto na Figura 11.

Figura 11 – Compartilhamentos obtidos pela ferramenta Advanced Port Scanner.



Fonte: Advanced Port Scanner (2016).

O equipamento de IP 192.168.1.100 e hostname Joao_Pedro-PC possui algumas pastas compartilhadas, para acessar essas pastas, basta apenas clicar na pasta selecionada na tabela à direita conforme visto na Figura 11, o equipamento de IP 192.168.1.1 também possui um compartilhamento via HTTP, que também pode ser acessado após o clique no link referente ao equipamento. Os itens detectados podem ser vistos com mais clareza no Quadro 2.

Quadro 2 – Análise por equipamento ferramenta Advanced Port Scanner.

	ADVANCED PORT SCANNER			
	EQUIPAMENTOS			
	COMPUTADOR	**MÁQUINA VIRTUAL**	**ROTEADOR**	**SMARTPHONES**
	Hosts Ativos	Hosts Ativos	Hosts Ativos	Hosts Ativos
	Endereço IPV4	Endereço IPV4	Endereço IPV4	Endereço IPV4
	MAC address	MAC address	MAC address	MAC address
	Portas abertas	Portas abertas	Fabricante	Fabricante
	Hostname	Fabricante	Serviços	
	Grupo de trabalho			
	Sistema Operacional			
	Compartilhamentos			
	Impressora			
	Fabricante			
	Usuário			
TOTAL	**11**	**5**	**5**	**4**

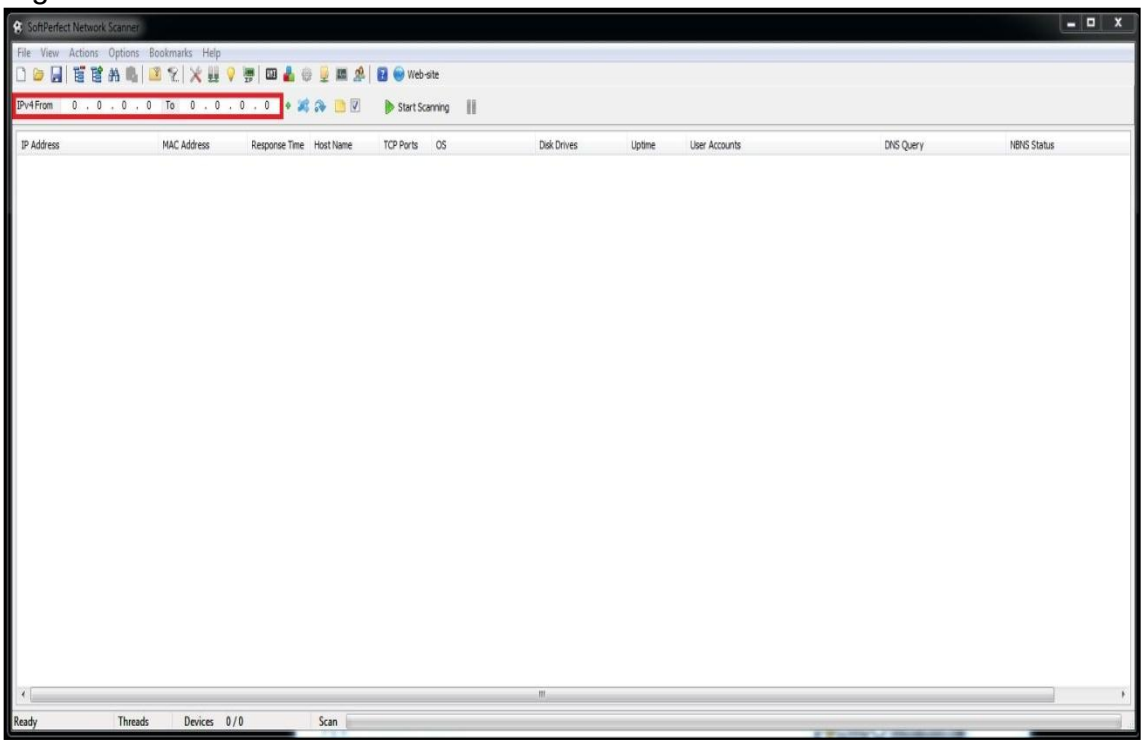
Fonte: Elaborada pelo autor

6.3 SOFTPERFECT NETWORK SCANNER

O escaneamento realizado através da ferramenta SoftPerfect Network Scanner detectou os 5 equipamentos presentes na rede, dando várias informações sobre cada um deles.

Na tela inicial do programa foi possível observar um campo vazio solicitando qual o range de IP a ser escaneado pela ferramenta, conforme ilustrado na Figura 6.

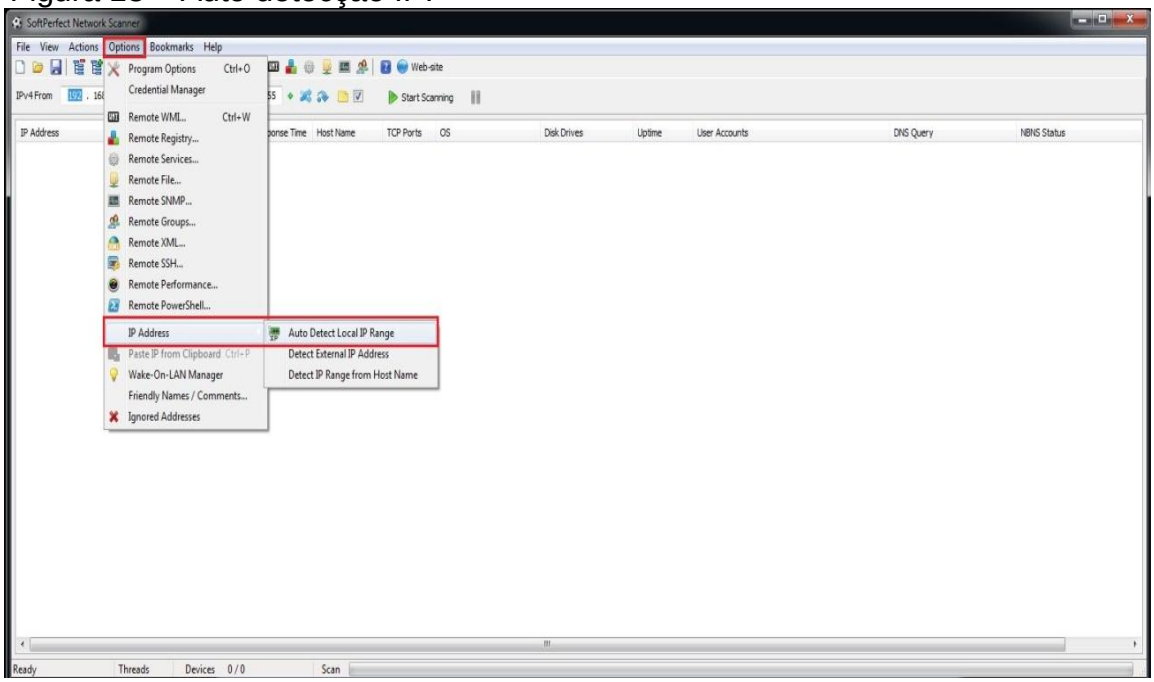
Figura 12 – Tela inicial ferramenta SoftPerfect Network Scanner.



Fonte: SoftPerfect Network Scanner (2016).

Porém na aba “Options” foi encontrado uma opção onde a ferramenta auto detectou a classe de IP, sub-rede e o range a ser escaneado, conforme ilustrado na Figura 13.

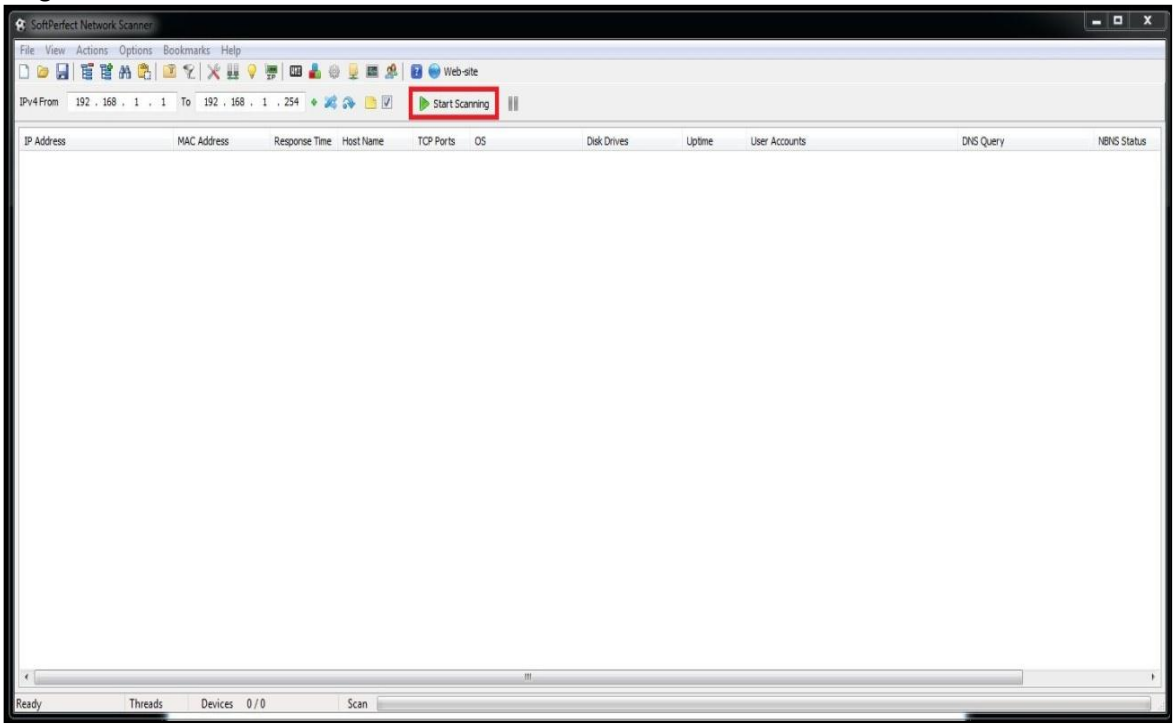
Figura 13 – Auto detecção IP.



Fonte: SoftPerfect Network Scanner (2016).

A ferramenta SoftPerfect Network Scanner tem uma função que auto detectou a classe de IP, sub-rede e o range a ser escaneado, conforme ilustrado na Figura 13. Foi clicado no botão “Start Scanning” para inicializar o escaneamento conforme ilustrado na Figura 14.

Figura 14 – Escaneamento ferramenta SoftPerfect Network Scanner.

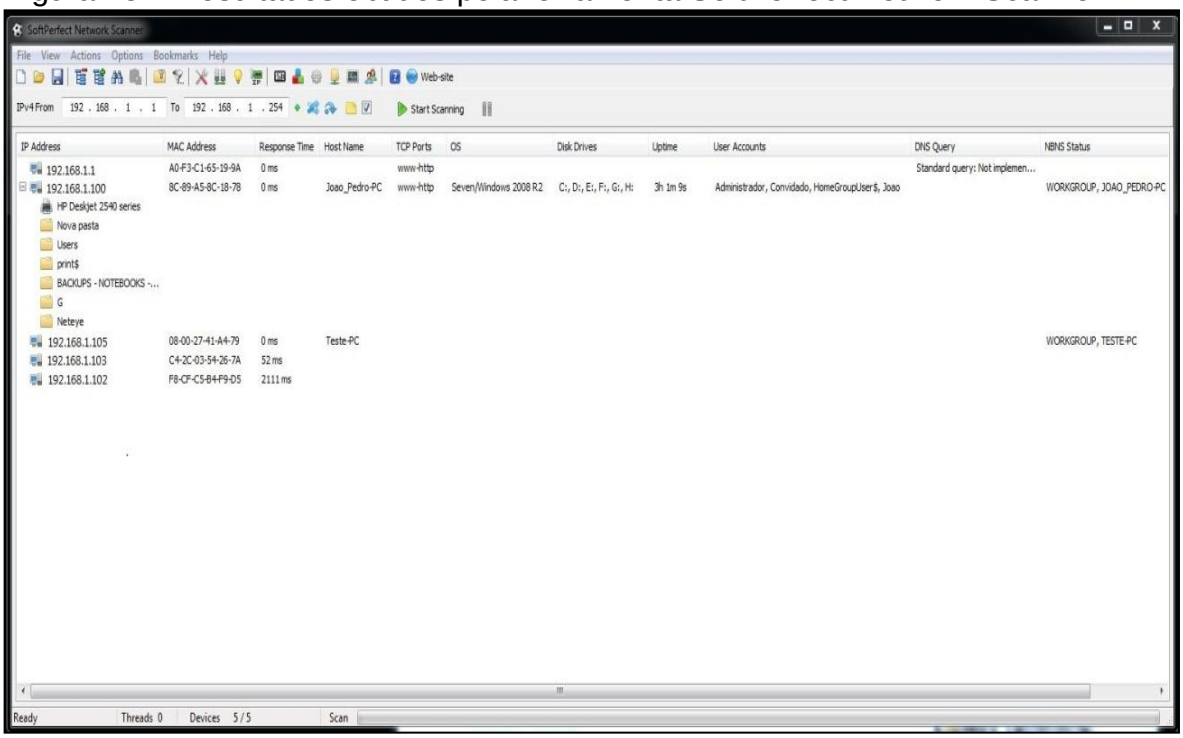


Fonte: SoftPerfect Network Scanner (2016).

Após a varredura, foram detectados os 5 equipamentos que fazem parte da rede, sendo 1 computador, 1 máquina virtual, 1 roteador e 2 smartphones. Foram obtidos vários itens em comum dos diversos equipamentos como: MAC address, endereço IPV4 e tempo de resposta. O software obteve melhor desempenho ao analisar o computador onde foram identificados 13 itens como: hosts ativos, endereço IPV4, MAC address, portas abertas, hostname, grupo de trabalho, sistema operacional, compartilhamentos, impressora, tempo ativo do host, discos rígidos, contas de usuário e tempo de resposta. Na máquina virtual foram obtidos itens como: hosts ativos, endereço IPV4, MAC Address, hostname, grupo de trabalho e tempo de resposta, totalizando 5 características. No roteador foi possível obter os hosts ativos, endereço IPV4, MAC address, portas abertas e tempo de resposta, já nos 2 smartphones detectados foram detectados apenas 4 itens, sendo: hosts

ativos, endereço IPV4, MAC address e tempo de resposta. Esta análise pode ser vista na Figura 15.

Figura 15 – Resultados obtidos pela ferramenta SoftPerfect Network Scanner.



Fonte: SoftPerfect Network Scanner (2016).

Os itens detectados podem ser vistos com mais clareza no Quadro 3.

Quadro 3 – Análise por equipamento ferramenta SoftPerfect Network Scanner.

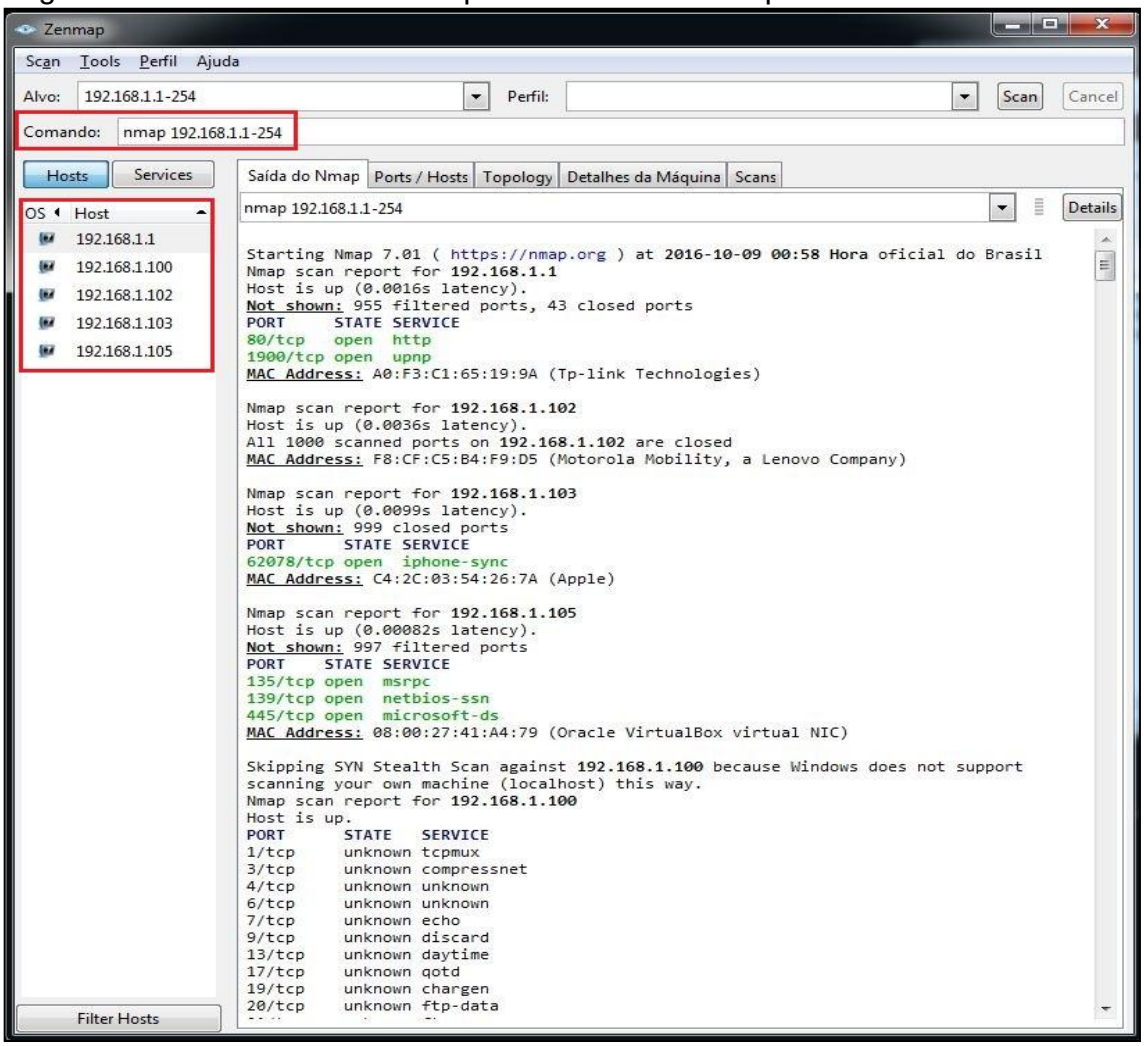
	SOFTPERFECT NETWORK SCANNER			
	EQUIPAMENTOS			
	COMPUTADOR	**MÁQUINA VIRTUAL**	**ROTEADOR**	**SMARTPHONES**
	Hosts Ativos	Hosts Ativos	Hosts Ativos	Hosts Ativos
	Endereço IPV4	Endereço IPV4	Endereço IPV4	Endereço IPV4
	MAC address	MAC address	MAC address	MAC address
	Portas abertas	Hostname	Portas abertas	Tempo de resposta
	Hostname	Grupo de trabalho	Tempo de resposta	
	Grupo de trabalho	Tempo de resposta		
	Sistema Operacional			
	Compartilhamentos			
	Impressora			
	Tempo ativo do Host			
	Discos Rígidos			
	Contas de usuário			
	Tempo de resposta			
TOTAL	**13**	**6**	**5**	**4**

Fonte: Elaborada pelo autor

6.4 NMAP

Na varredura realizada pela ferramenta Nmap, por meio do comando “nmap 192.168.1.1-254” foram identificados os 5 equipamentos presentes na rede conforme pode ser visto na Figura 16.

Figura 16 – Resultados obtidos pela ferramenta Nmap.



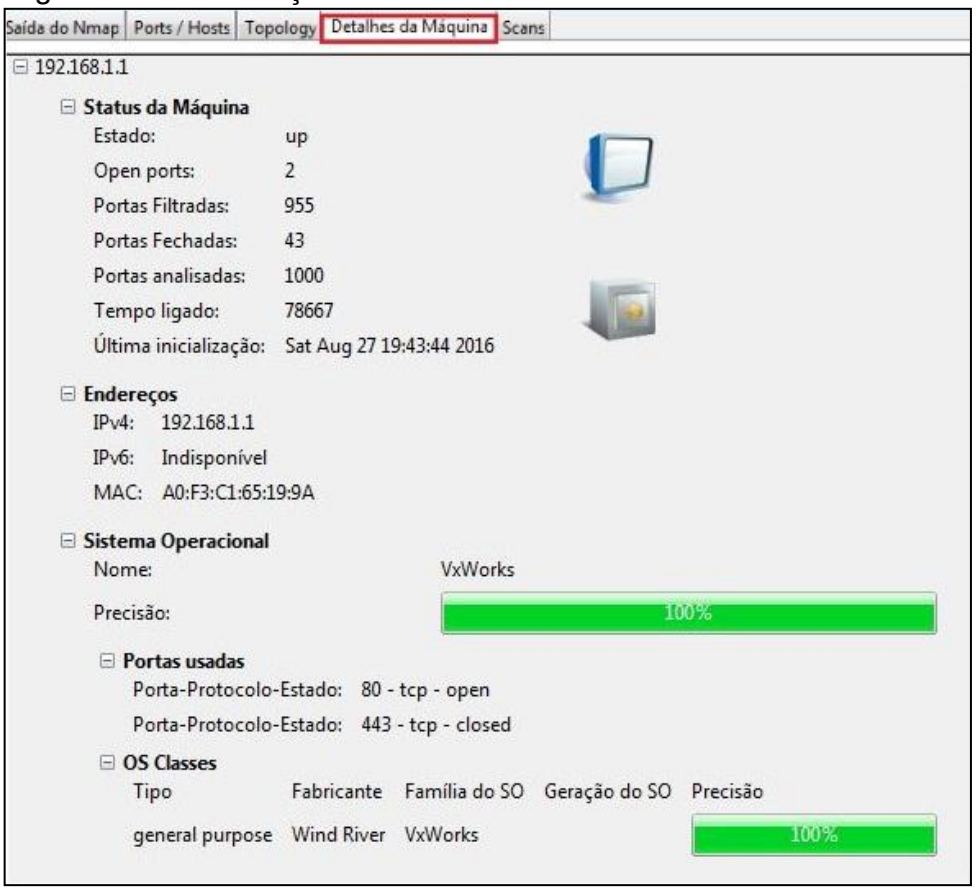
Fonte: Nmap (2016).

Teve seu melhor desempenho ao identificar vários itens no roteador, como: hosts ativos, endereço IPV4, MAC Address, número de portas analisadas, portas abertas e fechadas, tempo ativo do host, última inicialização, sistema operacional, fabricante e tempo de resposta, sendo 11 características no total, teve um bom desempenho na detecção de 8 itens nos 2 smartphones presentes como: hosts ativos, endereço IPV4, MAC address, fabricante, número de portas analisadas, portas abertas e fechadas e o tempo de resposta, identificou também alguns elementos no único computador e máquina virtual presentes na rede como: hosts ativos, endereço IPV4, fabricante, número de portas analisadas, portas abertas e fechadas e o tempo de resposta.

Através do comando “nmap –O 192.168.1-254” foram obtidas informações detalhadas sobre alguns equipamentos como:tempo ativo do host, última

inicialização, sistema operacional, portas abertas e fechadas do roteador conforme ilustra Figura 17.

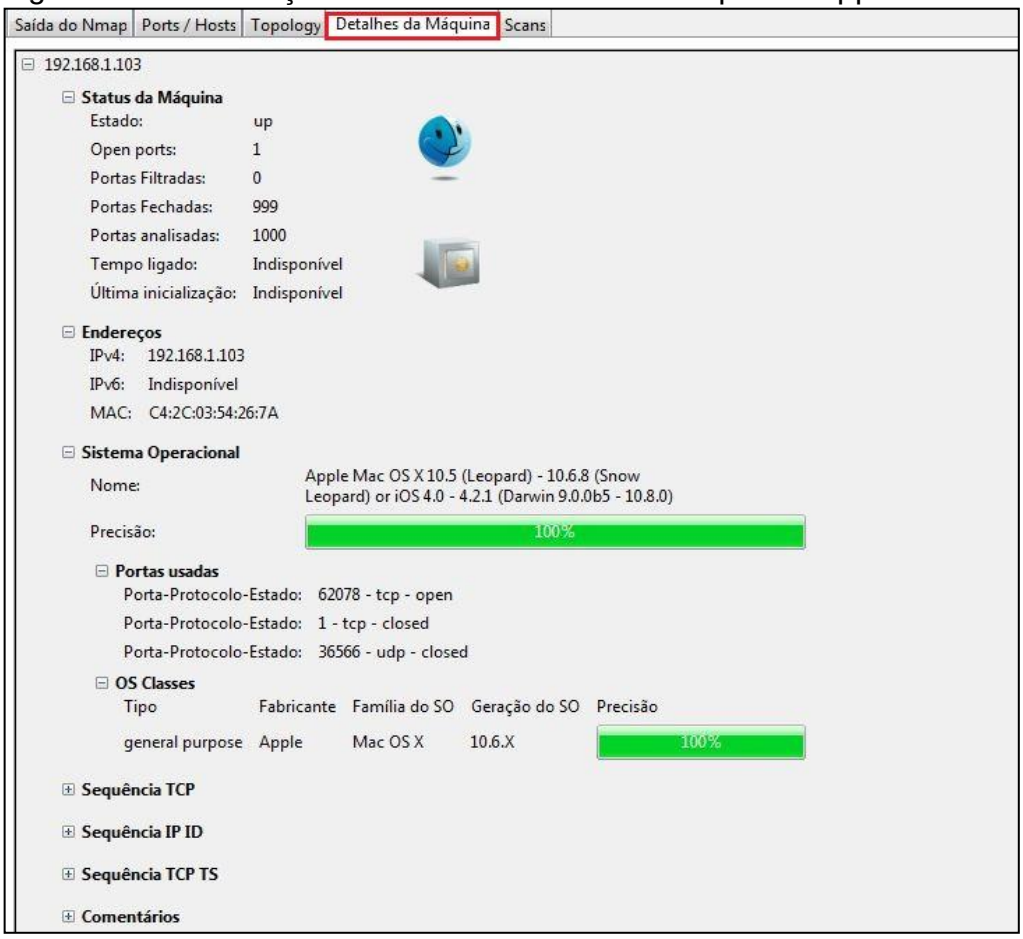
Figura 17 – Informações detalhadas sobre o roteador.



Fonte: Nmap (2016).

Foram obtidas informações detalhadas como: sistema operacional, portas abertas e fechadas do smartphone Apple de IP 192.168.1.103 conforme ilustra a Figura 18.

Figura 18 – Informações detalhadas sobre o smartphone Apple.



Fonte: Nmap (2016).

Os itens detectados podem ser vistos com mais clareza no Quadro 4.

Quadro 4 – Análise por equipamento ferramenta Nmap.

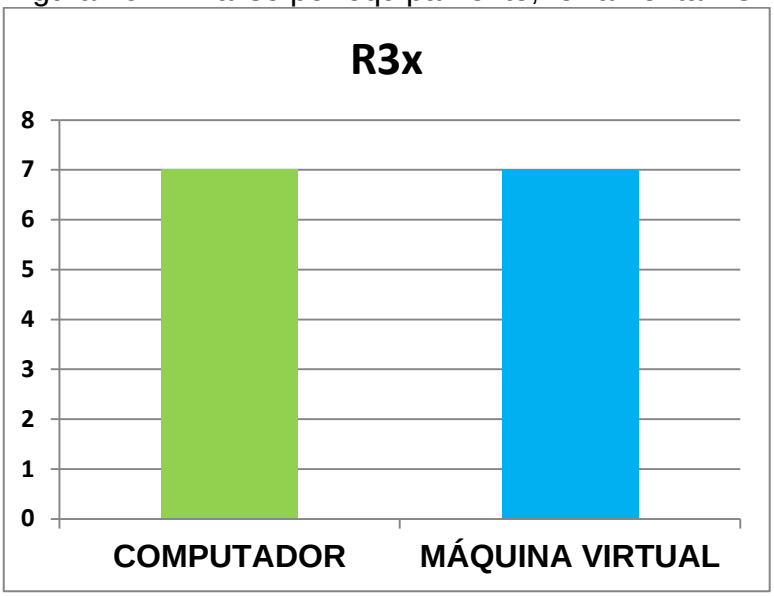
	NMAP			
	EQUIPAMENTOS			
	COMPUTADOR	**MÁQUINA VIRTUAL**	**ROTEADOR**	**SMARTPHONES**
	Hosts Ativos	Hosts Ativos	Hosts Ativos	Hosts Ativos
	Endereço IPV4	Endereço IPV4	Endereço IPV4	Endereço IPV4
	MAC address	MAC address	MAC address	MAC address
	Número de portas analisadas	Número de portas analisadas	Número de portas analisadas	Número de portas analisadas
	Portas abertas	Portas abertas	Portas abertas	Portas abertas
	Portas fechadas	Fabricante	Portas fechadas	Portas fechadas
	Fabricante	Tempo de resposta	Tempo ativo do Host	Fabricante
	Tempo de resposta		Última inicialização	Tempo de resposta
			Sistema Operacional	
			Fabricante	
			Tempo de resposta	
TOTAL	**8**	**7**	**11**	**8**

Fonte: Elaborada pelo autor

7 ANÁLISE GERAL

Após escaneamentos realizados na rede com 4 ferramentas diferentes, Nmap, Advanced Port Scanner, SoftPerfect Network Scanner onde foi possível detectar 4 tipos de equipamentos presentes na rede conforme ilustrado na Figura 6 que são: computador, máquina virtual, roteador e 2 *smartphones*, a ferramenta R3x detectou apenas o computador e máquina virtual, um dos fatores que contribuíram para o *software* identificar apenas 2 dos 5 equipamentos existentes na rede, foi devido seu lançamento ter ocorrido no ano de 2001, época em que a tecnologia que possuímos ainda estava se desenvolvendo, por exemplo, a baixa utilização de smartphones em relação aos dias atuais, porém se destacou-se perante as demais ferramentas na descoberta de itens tanto no computador quanto a máquina virtual, detectando itens exclusivos como serviços e especificação dos mesmos, totalizando 7 itens de cada conforme pode ser visto na Figura 19.

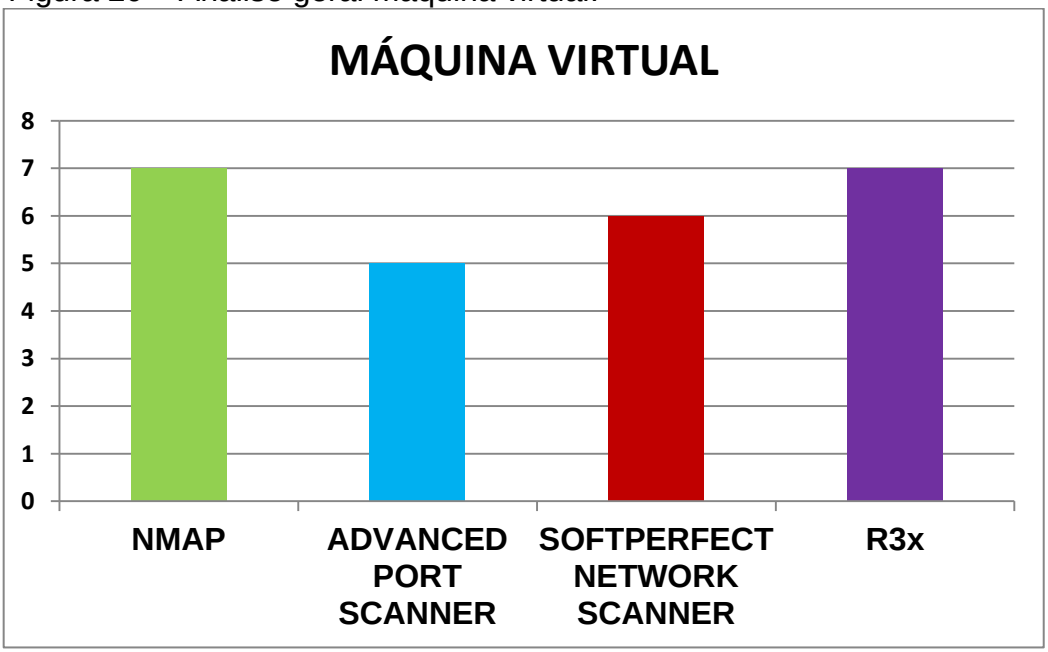
Figura 19 – Análise por equipamento, ferramenta R3x.



Fonte: Elaborada pelo autor

A Figura 20 comprova que a ferramenta R3x, mesmo sendo a mais antiga das ferramentas analisadas por não receber atualizações, foi bem eficiente em relação ao número de itens detectados através do escaneamento realizado na máquina virtual, pois detectou 7 itens, o mesmo número da ferramenta Nmap que apesar seu lançamento ter ocorrido no ano de 1997, recebe constantes atualizações.

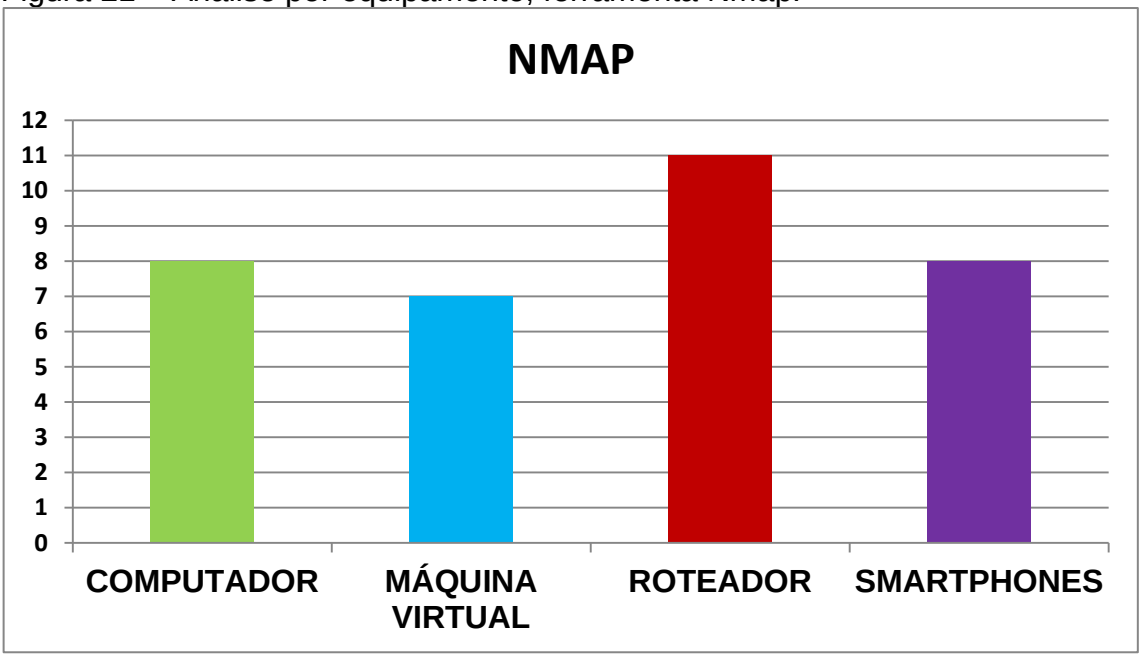
Figura 20 – Análise geral máquina virtual.



Fonte: Elaborada pelo autor

A ferramenta Nmap detectou todos os equipamentos presentes na rede que são 1 computador, 1 máquina virtual, 1 roteador e 2 smartphones que podem ser vistos na Figura 6, o escaneamento levou cerca de 2 minutos e 45 segundos para ser concluído. A Figura 21 ilustra a quantidade de itens detectados por equipamento através da ferramenta em questão.

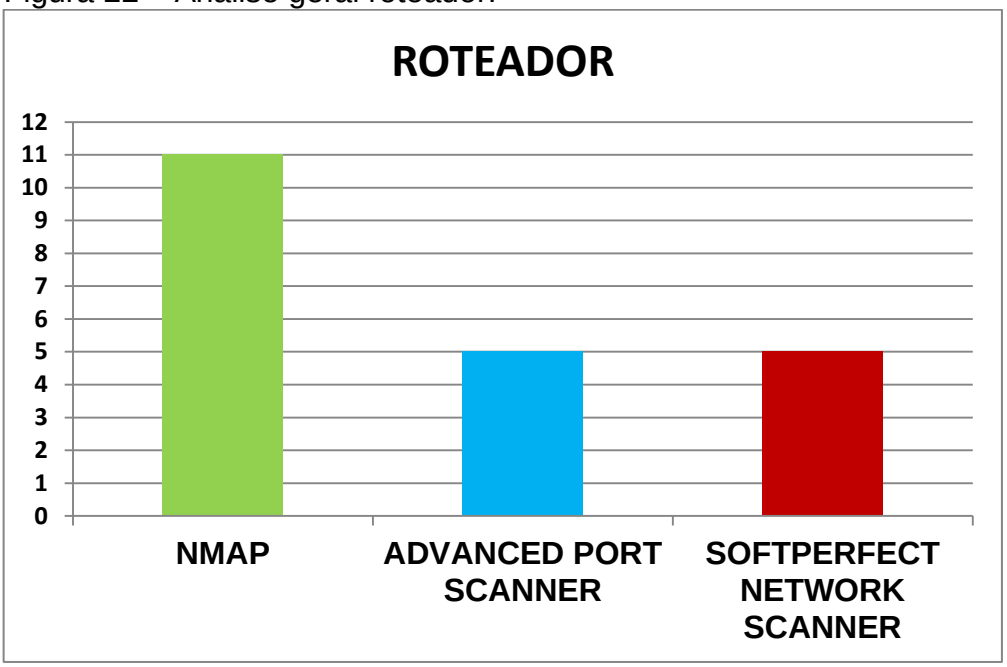
Figura 21 – Análise por equipamento, ferramenta Nmap.



Fonte: Elaborada pelo autor

A ferramenta Nmap, destacou-se perante as demais em relação a análise quanto ao roteador onde detectou 7 itens a mais do que as ferramentas Advanced Port Scanner e SoftPerfect Network Scanner, detectando itens exclusivos como: tempo ativo do host, última inicialização, sistema operacional e número de portas analisadas, totalizando 11 elementos, conforme podem ser vistos na Figura 22 que ilustra a quantidade de itens do roteador que foram detectados por todas as ferramentas e comprovar que o Nmap foi a que obteve melhor desempenho.

Figura 22 – Análise geral roteador.

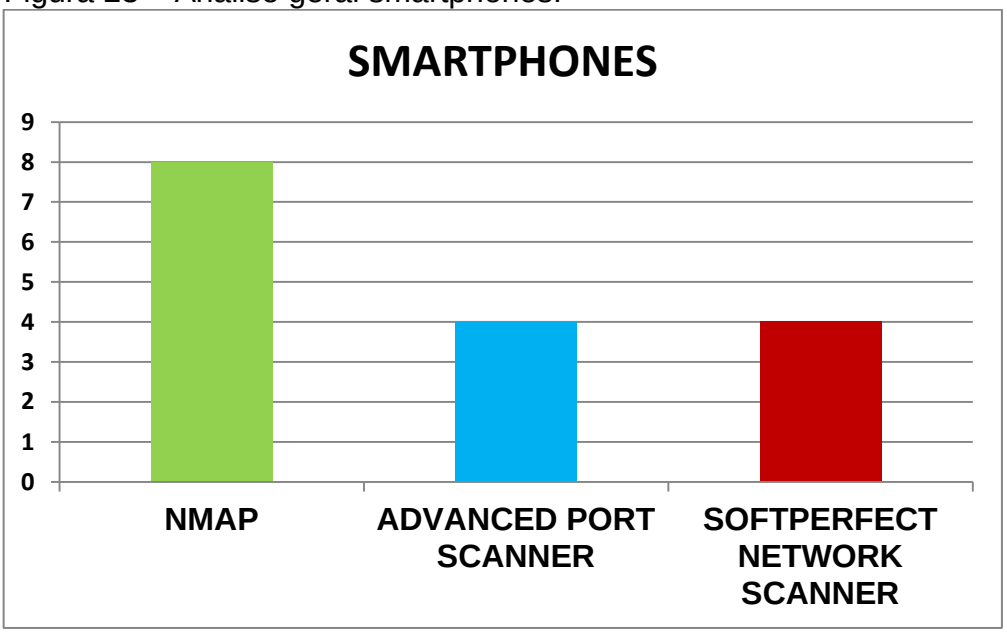


Fonte: Elaborada pelo autor

Além de se destacar em relação aos itens obtidos no roteador, a ferramenta Nmap teve o melhor desempenho quanto a descoberta de itens relacionados aos smartphones onde foi possível detectar 4 elementos a mais do que as demais ferramentas, com escaneamento realizado em cerca de 2 minutos e 45 segundos.

A Figura 23 ilustra a quantidade de itens nos smartphones que foram identificados pelas ferramentas Nmap, Advanced Port Scanner e SoftPerfect Network Scanner e comprovar que a ferramenta Nmap foi a melhor em relação a análise destes equipamentos detectando um total de 8 itens.

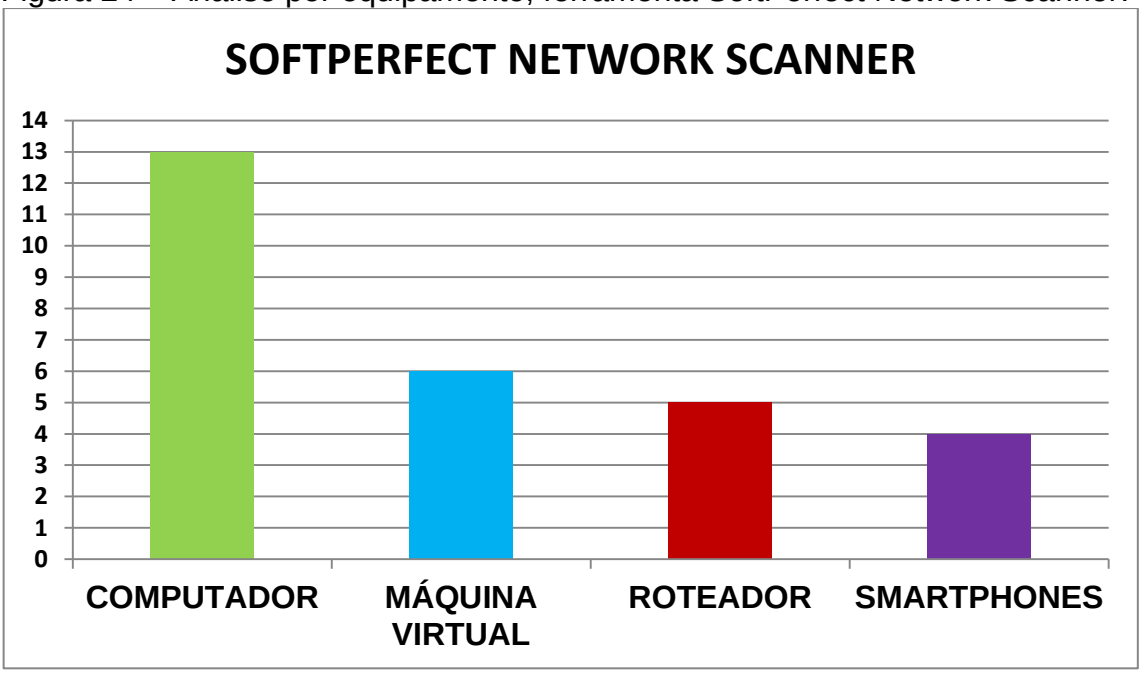
Figura 23 – Análise geral smartphones.



Fonte: Elaborada pelo autor

A ferramenta SoftPerfect Network Scanner obteve mais sucesso ao detectar os itens presentes no computador e só através do escaneamento realizado por meio desta, foi possível detectar itens como: discos rígidos, contas de usuário presentes no computador e tempo ativo do host, no total foram 13 itens identificados no computador, conforme pode ser visto na Figura 24 que também ilustra a quantidade de itens por equipamentos que foram identificados pela ferramenta em questão.

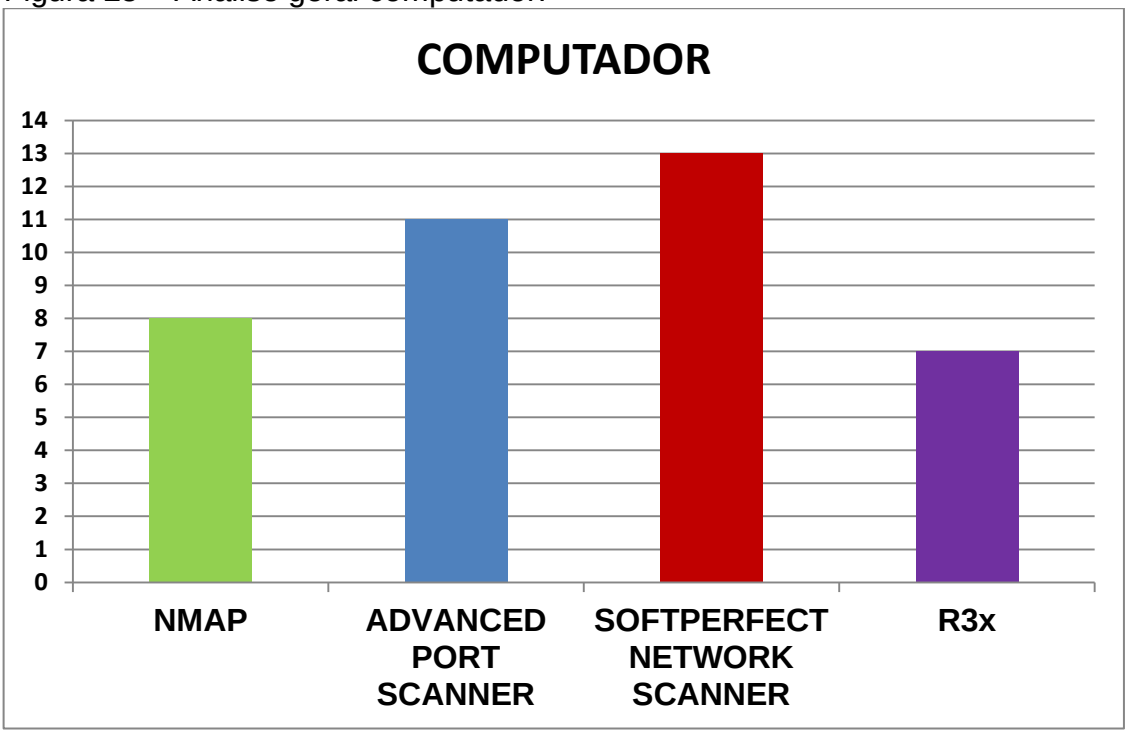
Figura 24 – Análise por equipamento, ferramenta SoftPerfect Network Scanner.



Fonte: Elaborada pelo autor

A Figura 24 ilustra o cenário onde a ferramenta SoftPerfect Network Scanner obteve seu melhor desempenho em relação a detecção dos itens relacionados ao computador, a Figura 25 comprova que a ferramenta em questão foi a melhor dentre as estudadas quanto a identificação dos itens relacionados ao computador, pode ser levado em consideração o tempo de escaneamento que foi de mais ou menos 1 minuto e 35 segundos e por ser o mais atual dos *softwares* analisados.

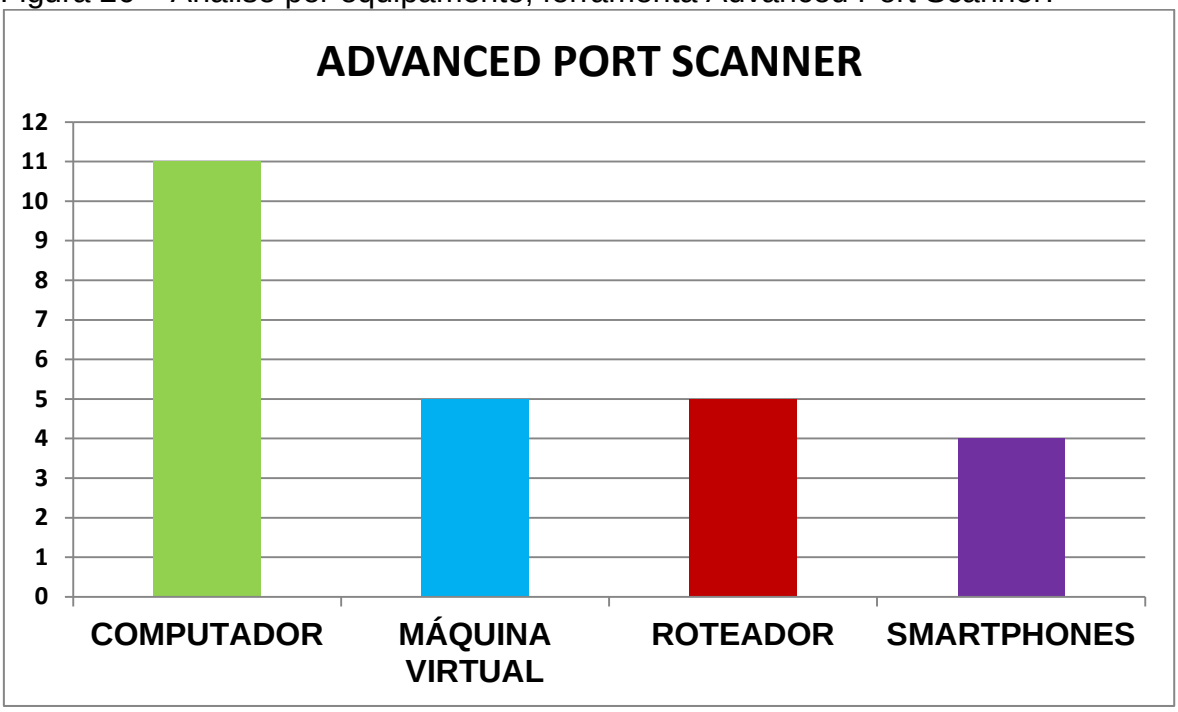
Figura 25 – Análise geral computador.



Fonte: Elaborada pelo autor

A ferramenta Advanced Port Scanner destacou-se perante a relação de itens obtidos no computador totalizando 11, conforme pode ser visualizado na Figura 26 que também ilustra a quantidade total de itens detectados nos demais equipamentos através da ferramenta destacada.

Figura 26 – Análise por equipamento, ferramenta Advanced Port Scanner.

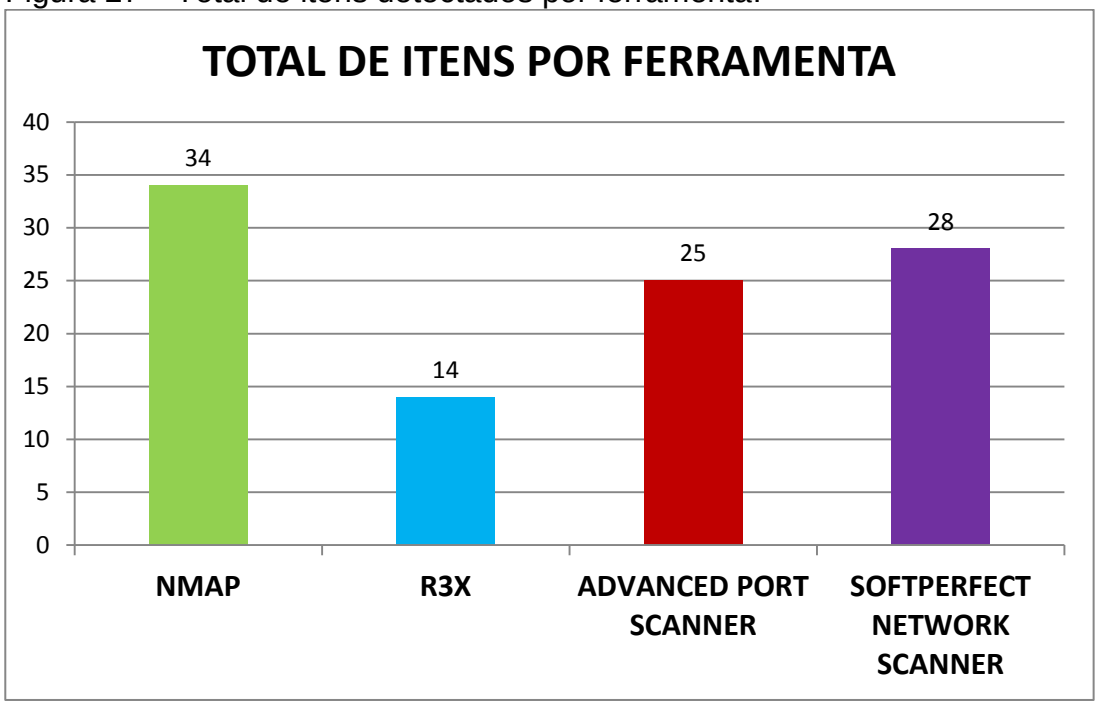


Fonte: Elaborada pelo autor

Em relação aos outros equipamentos, detectou 5 itens na máquina virtual e roteador e 4 itens nos smartphones, esta boa quantidade de itens identificados através do escaneamento em todos os equipamentos pode ser justificada pelo software ser do início do ano de 2016 e tendo um tempo médio de 1 minuto e 50 segundos, podendo ser comparada ao SoftPerfect Advanced Scanner que foi citado acima.

A Figura 27 mostra a totalidade de itens identificados por cada ferramenta, com destaque a ferramenta Nmap identificando um total de 34 itens entre computador, máquina virtual, roteador e smartphones. Destacam-se também as ferramentas SoftPerfect Network Scanner e Advanced Port Scanner identificando um total de 28 e 25 itens, respectivamente, tiveram desempenho bem parecido, a ferramenta R3x obteve um total de 14 itens, porém podemos levar em consideração a ferramenta detectar apenas itens do computador e da máquina virtual.

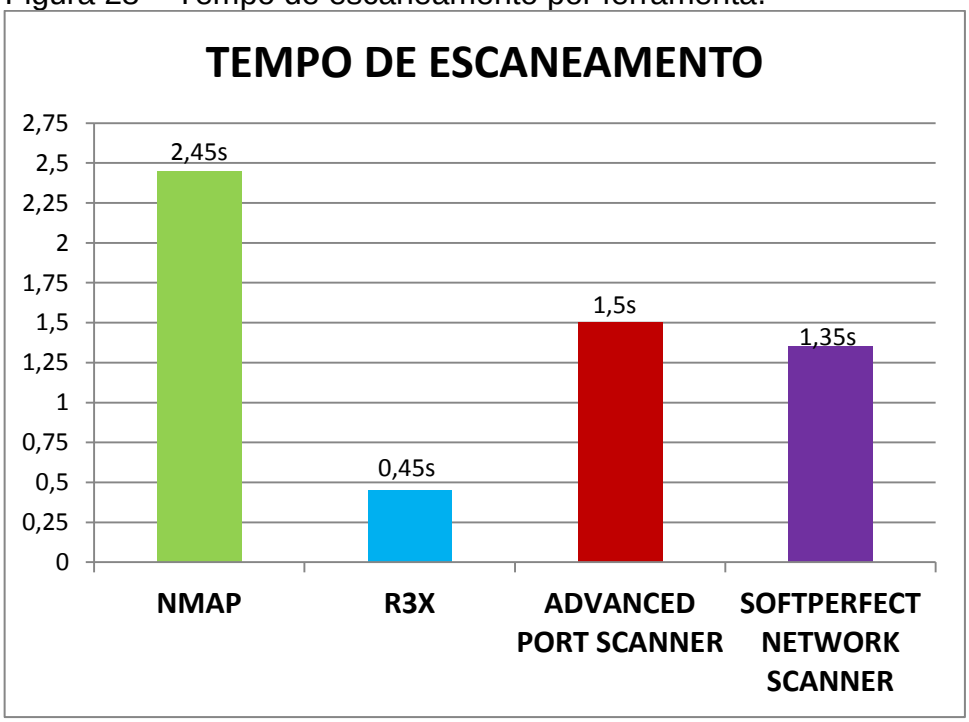
Figura 27 – Total de itens detectados por ferramenta.



Fonte: Elaborada pelo autor

A Figura 28 ilustra o tempo de escaneamento de cada ferramenta, que é um fator que pode ser levado em consideração quanto a quantidade de itens obtidos.

Figura 28 – Tempo de escaneamento por ferramenta.



Fonte: Elaborada pelo autor

7.1 VULNERABILIDADES

Quanto mais informações um atacante possuir sobre seu alvo, existe mais chances dele obter sucesso e através disso explorar as possíveis vulnerabilidades existentes por meio de portas TCP e UDP abertas explorando os compartilhamentos através da porta 445 e identificar serviços em execução através da porta 135, ter um conhecimento prévio do equipamento apenas pela descoberta do MAC Address que é um endereço físico representado por algarismos hexadecimais, sendo exclusivo de cada dispositivo, é utilizado para comunicação do dispositivo com a interface da rede, possui um padrão onde os 3 primeiro bytes são definidos pelo IEEE e os 3 últimos pelo próprio fabricante, descobrir o sistema operacional, serviços em execução, hostname, grupo de trabalho, usuários e tempo ativo do host.

Todas as informações obtidas são de extrema valia para um atacante planejar uma invasão, pois através destas descobertas ele terá mais chance de ser bem sucedido. O quadro 5 ilustra todas as vulnerabilidades encontradas nos diferentes equipamentos que fazem parte da rede que foram detectadas através do escaneamento realizado com as ferramentas estudadas.

Quadro 5 – Vulnerabilidades encontradas pelas ferramentas.

	VULNERABILIDADES			
	FERRAMENTAS			
	Nmap	**R3X**	**Advanced Port Scanner**	**SoftPerfect Network Scanner**
	Hosts Ativos	Hosts Ativos	Hosts Ativos	Hosts Ativos
	Endereço IPV4	Endereço IPV4	Endereço IPV4	Endereço IPV4
	Características dos aparelhos	MAC address	Características dos aparelhos	MAC address
	MAC address	Hostname	MAC address	Portas abertas
	Número de portas analisadas	Grupo de trabalho	Portas abertas	Tempo ativo do Host
	Portas abertas	Serviços	Sistema Operacional	Sistema Operacional
	Portas fechadas	Especificação dos serviços	Compartilhamentos	Compartilhamentos
	Tempo ativo do Host		Impressora	Impressora
	Última inicialização		Fabricante	Hostname
	Sistema Operacional		Hostname	Grupo de trabalho
	Fabricante		Grupo de trabalho	Discos Rígidos
			Serviços	Contas de usuário
			Usuário	Tempo de resposta
TOTAL	**11**	**7**	**13**	**13**

Fonte: Elaborada pelo autor

8 CONSIDERAÇÕES FINAIS

Como resultados do crescente avanço tecnológico surgiram as redes de computadores, a qual sua utilização é imprescindível, tanto ambiente doméstico quanto empresarial, possuindo vários tipos de usuário com diferentes níveis de conhecimento e objetivos,o que torna o assunto bem abrangente.

Por este motivo, o uso de técnicas e ferramentas de escaneamento de vulnerabilidades nas redes de computadores é de suma importância para o auxílio na análise de dados. Com isso, o objetivo desse estudo foi analisar *softwares* de escaneamento de vulnerabilidades em redes de computadores para expor os resultados através de uma análise e quadros comparativos.

Foi possível notar, através das ferramentas Nmap, R3x, Advanced Port Scanner e SoftPerfect Network Scanner vários itens em diferentes tipos de equipamentos, que podem ser explorados por usuários com um nível maior de conhecimento acerca do assunto, em relação aos itens pode levar-se em consideração o ano de lançamento do software, funcionalidades do software e tempo de escaneamento, foram obtidos ótimos resultados através das ferramentas em questão por ser possível identificar os equipamentos presentes na rede e itens e características dos mesmos, o que pode contribuir para um atacante obter mais sucesso em uma invasão, pois através destas descobertas, terá uma chance maior de ser bem sucedido.

Como trabalhos futuros, podem ser utilizadas outras ferramentas e detalhar o nível da vulnerabilidade encontrada nos itens explorados através do escaneamento realizado na rede, e através destas informações, realizar uma análise construída em quadros comparativos e ilustrar maneiras de se proteger destas ferramentas que realizam escaneamentos.

REFERÊNCIAS

BEAL, A. **Segurança da Informação: Princípios e Melhores Práticas para a Proteção dos Ativos de Informação nas Organizações**. São Paulo: Atlas, 2005.

BITENCOURT, A. C. **Análise de Software de Escaneamento de Vulnerabilidades em Redes de Computadores**. 2014. 44f. Curso Superior de Tecnologia em Redes de Computadores, Universidade Federal de Santa Maria, Santa Maria, RS, 2014.

CERT. BR – **Cartilha de segurança para internet** – CERT.br, 2 ed, Comitê Gestor da Internet no Brasil, São Paulo, 2012. Disponível em: <http://cartilha.cert.br/ > Acesso em: 19 abr. 2016.

CERT. BR – Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil. **Incidentes Reportados ao CERT. br – de 1999 a Dezembro de 2015**. Disponível em: <http://www.cert.br/stats/incidentes/> Acesso em: 19 abr. 2016.

CERT.BR – Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil. **Incidentes Reportados ao CERT.br – de 1999 a Dezembro de 2016**. Disponível em: <http://www.cert.br/stats/incidentes/2015-jan-dec/scan-portas.png> Acesso em: 19 abr. 2016.

CERT.BR – Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil. **Incidentes Reportados ao CERT.br – de 1999 a Dezembro de 2016**. Disponível em: <http://www.cert.br/stats/incidentes/2015-jan-dec/scan-portas.html> Acesso em: 19 abr. 2016.

DUMONT, C. E. S. **Segurança em Servidores Linux em Camadas.** 2006**.** 59f. Monografia de Pós-Graduação apresentada ao Departamento de Ciências da Computação da Universidade Federal de Lavras, Lavras, MG, 2006.

IV ENCONTRO DE ADMNISTRAÇÃO DA INFORMAÇÃO, 2013, Bento Gonçalves. **Produção Científica sobre Segurança da Informação em Anais de Eventos da ANPAD...** Bento Gonçalves, 2013. Disponível em: <http://www.anpad.org.br/diversos/trabalhos/EnADI/enadi_2013/2013_EnADI93.pdf> . Acesso em: 30 abr. 2016

KUROSE, J. ; ROSS, K. **Redes de Computadores e a Internet -** São Paulo, Editora Pearson Adison Wesley, 2006.

LIBANO, D. R. **Um estudo da Deep Web e suas principais vulnerabilidades.** 2014. 59f. Trabalho de conclusão de curso apresentado ao Centro de Ciências Exatas e Sociais Aplicadas da Universidade Sagrado Coração, Bauru, SP, 2014

LOPES, C.; CARVALHO, M.; MELO, R.; COSTA, K**. Análise de Vulnerabilidades em Redes de Computadores – Estudo de Caso com a Ferramenta Nmap.** 2013. 11f. Curso de Tecnologia em Redes de Computadores - Faculdade de Tecnologia de Bauru (FATEC), Bauru, SP, 2013

MARTINELO, C.; BELLEZI, M. **Análise de Vulnerabilidades com OpenVAS e Nessus.** São Carlos, jan-abr. 2014. T.I.S. São Carlos, v. 3, n. 1. Disponível em: <http://revistatis.dc.ufscar.br/index. php/revista/article/viewFile/74/68>. Acesso em: 30 abr. 2016

MARQUES, Alexandre Fernandez. **Segurança em rede IP.** Monografia de pós-graduação em Redes de Computadores e Comunicação de Dados. Londrina: ASIT, 2001.

MCCLURE. S; SCAMBARY.J; KURTZ. G .**Hackers Expostos: segredos e soluções para a segurança -** São Paulo: Editora Campus Ltda, 4ª Edição, 2003.

MENDES, Douglas Rocha. **Redes de Computadores: Teoria e Prática**. São Paulo: editora Novatec, 2007.

MITNICK, Kevin D.; SIMON, William L. **A arte de enganar: ataques de hackers: controlando o fator humano na segurança da informação**. São Paulo: Pearson Education, 2003.

NAKAMURA, E.; GEUS, P. **Segurança de Redes em ambientes cooperativos** - São Paulo : Novatec Editora, 2007.

RESENDE, D. ; ABREU, A. **Tecnologia da informação aplicada a sistemas de informação empresariais**. São Paulo: Atlas. 2006.

RIBEIRO, H.; AMADIO, R; GAVILAN, J.; SANTOS, H. **Segurança em Redes 802.11,** Jaciara, nov. 2012. Revista Científica Eletrônica de Ciências Sociais Aplicadas da Eduvale, Ano V, número 07. Disponível em: <http://eduvalesl.revista.inf.br/imagens_arquivos/arquivos_destaque/lxQN9quh6TtUkla_2015-12-19-2-36-3.pdf>. Acesso em: 30 abr. 2016

SÊMOLA, Marcos. **Gestão da segurança da informação: uma visão executiva**. Rio de Janeiro: Campus, 2003.

TANEMBAUN, Andrew. **Redes de Computadores** - Rio de Janeiro: Elsevier Editora Ltda, 4ª Edição, 2003.

TENÓRIO, D. F. **Detecção Cega de Tráfego Malicioso Através da Variação Temporal do Maior Autovalor**, 2013. 116f. Publicação PPGEE. DM - 548/2013, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 2013.

THOMAS, Tom. **Segurança de Redes - Primeiros passos** - Rio de Janeiro: Editora Ciência Moderna Ltda, 2007.

TORRES, G. **Redes de Computadores Curso Completo –** Rio de Janeiro: Axcel Books Editora do Brasil, 2001.