ANCELMO BOTEON

ANÁLISE DE FERRAMENTAS PARA SEGURANÇA DE REDES

Universidade Federal de Santa Catarina
Departamento de Informática e Estatística

FLORIANÓPOLIS, 2007.

ANCELMO BOTEON

ANÁLISE DE FERRAMENTAS PARA SEGURANÇA DE REDES

Universidade Federal de Santa Catarina
Departamento de Informática e Estatística

Trabalho de conclusão de curso apresentado à Universidade Federal de Santa Catarina, como parte dos requisitos para a obtenção do grau de bacharel em Sistemas de Informação.

Professor João Bosco Mangueira Sobral

FLORIANÓPOLIS, 2007.

ANCELMO BOTEON

ANÁLISE DE FERRAMENTAS PARA SEGURANÇA DE REDES

Monografia aprovada em ___ / ___ / 2007,
como requisito para a obtenção do grau de bacharel
em Sistemas de Informação.

Banca Examinadora

_____

Professor João Bosco Mangueira Sobral

Orientador

_____

Professor Fernando Augusto da Silva Cruz

Membro

_____

Clythia Higa Tamashiro

Membro

AGRADECIMENTOS

Gostaria de agradecer aos meus pais, que sempre me incentivaram a estudar para ter um futuro melhor, e por estarem ao meu lado, em todos os momentos.

Gostaria também de agradecer a minha noiva, Cláudia, por me incentivar e esclarecer minhas dúvidas, com sinceridade, honestidade e senso de justiça.

Com certeza não poderia esquecer de agradecer os meus grandes amigos, que fizeram e fazem parte da minha vida.

Não poderia faltar o meu agradecimento ao professor João Bosco Mangueira Sobral, meu orientador, e aos membros da banca professor Fernando Augusto da Silva Cruz e a Clytia Higa Tamashiro, por aceitarem fazer parte deste projeto.

Enfim, gostaria de agradecer a todos que de alguma forma contribuíram para eu atingir meus objetivos.

Sumário

LISTA DE FIGURAS

LISTA DE SIGLAS

ARP *Address Resolution Protocol*

TCP *Transmission Control Protocol*

IP	*Internet Protocol*
LAN	*Local Area Network*
DoS	Denial of Service
HTTP	*HyperText Transfer* protocol
HTTPS	*HyperText Transfer protocol Secure*)
SSL	*Secure Sockets Layer*
DNS	*Domain Name System*
ICMP	*Internet Control Message Protocol*
POP	Post Office Protocol

RESUMO

Muito se fala em segurança da informação, e nesse sentido o presente trabalho tem por objetivo a segurança de rede, como parte do contexto de proteger a informação. Segurança de rede faz uso de muitas ferramentas que um administrador pode utilizar. Muitas vezes essas ferramentas são usadas no sentido do atacante, entretanto, neste trabalho são selecionadas algumas mais importantes, para que um administrador possa ter uma fonte de avaliação quanto à utilização, desempenho, pontos positivos e pontos negativos das ferramentas

estudadas. Foram abordadas as seguintes ferramentas: Ethereal - captura de tráfego em redes, para análise dos pacotes que trafegavam em redes Ethernet utilizando Hubs; Ettercap - análise de pacotes em redes usando *switchs* , e ferramenta muito poderosa para ataques de homem-do-meio; Nessus - análise de vulnerabilidades, resultando em uma análise e possíveis soluções para as falhas de segurança encontradas; John the Ripper – para auditoria de senhas, servindo para analisar o poder das senhas dos usuários da rede; *honeyd*, simulador de hosts na rede para que o mesmo seja atacado para análise do comportamento dos atacantes; *hydra*, uma ferramenta de ataque de força bruta. O trabalho mostra os requisitos de instalação, configurações, resultado dos testes realizados e também uma análise das ferramentas.

ABSTRACT

Much is said in security of the information, and in this direction the present work has for objective the net security, as part of the context to protect the information. Security of net makes use of many tools that an administrator can use. Many times these tools are used in the direction of the aggressor, however, in this work are selected the some most important ones, so that a positive administrator can have a source of evaluation how much to the use, performance, points and negative points of the studied tools. The following tools had been boarded: Ethereal - capture of traffic in nets, for

analysis of the packages that passed through in nets Ethernet using Hubs; Ettercap - analysis of packages in nets using switchs, and very powerful tool for attacks of man-in-the-middle; Nessus - analysis of vulnerabilities, resulting in an analysis and possible solutions for the joined imperfections of security; John the Ripper - for auditorship of passwords, serving to analyze the power of the passwords of the users of the net; honeyd, simulator of hosts in the net so that the same it is attacked for analysis of the behavior of the aggressors; hydra, a tool of attack of rude force. The work shows the requirements of installation, configurations, result of the carried through tests and also an analysis of the tools.

1. INTRODUÇÃO

No contexto atual da denominada “Sociedade da Informação”, faz-se uso assíduo das redes de computadores, pois sem elas as informações, em uma organização, não fluiriam na velocidade necessária para a eficiência organizacional. Aliado às redes de

computadores temos o fator segurança, que muitas vezes não existe na rede, num nível aceitável, tanto pelo fato da empresa não investir em tecnologia, quanto pela falta de conhecimento, ou mesmo o foco. Muitas vezes as informações na rede trafegam de uma maneira não sigilosa, e nesse sentido os computadores podem estar vulneráveis a ataques, informações sigilosas podem ser obtidas por alguém com conhecimentos em informática, e de alguma maneira prejudicar o fluxo correto da organização.

Essas informações podem ser obtidas através de sniffers, que servem para capturar todo o tráfego que chega à placa de rede do computador. Além desse tipo de ferramenta, pode-se encontrar também os chamados *port scanner*, que vasculham nos computadores vulnerabilidades, para dessa forma obterem dados importantes referentes a organização ou mesmo informações sobre senhas de bancos, entre outros.

Neste sentido, o presente trabalho tem por objetivo analisar algumas das ferramentas mais importantes para análise de segurança nas redes de computadores, onde pode-se encontrar informações sobre requisitos para instalação, histórico da ferramenta, arquivos de configurações, assim como exemplos de testes e análise das mesmas, de maneira a identificar e corrigir as possíveis vulnerabilidades encontradas.

Este trabalho é organizado da seguinte forma: **o capítulo 2** apresenta algumas formas de ataques as quais estamos sujeitos. **Os capítulo 3,4,5,6,7 e 8** apresentam, respectivamente, um estudo sobre as ferramentas Ettercap, Ethereal, Nessus, John the Ripper, Honeyd, e Hydra, onde pode-se encontrar informações sobre pré-requisitos para instalação, informações sobre configurações, os testes realizados com as ferramentas, e uma análise sobre as mesmas. Por fim apresenta-se as conclusões referentes aos testes realizados comparando as ferramentas utilizadas.

2. FORMAS DE ATAQUES

Muita coisa mudou desde o surgimento dos computadores, e uma das maiores invenções já feitas pelo homem, além do computador, é o conceito de redes de computadores.

Esse conceito surgiu no meio militar, pois havia a necessidade de troca de informações.

Algum tempo depois de criadas, as redes passaram a ser utilizadas por todos, ocasionando o que hoje podemos chamar de “Sociedade da Informação”, devido ao rápido e fácil acesso as informações.

O conceito de redes pode variar de autor para autor, porém um ponto em comum nos conceitos é o de **compartilhamento de recursos**, ou seja, a criação de uma maneira simples e prática para o compartilhamento de periféricos (como impressoras, scanners, etc.) e informações.

Com este conceito, surgiu a necessidade da segurança computacional, onde temos como principais objetivos: manter a autenticidade (garantia da origem) , confidencialidade (informação ao alcance apenas a pessoas autorizadas) , integridade (garantia de que a informação originada não se alterou ao longo da rede) e disponibilidade de informações (garantia de que a informação sempre estará disponível quando for necessária).

2.1 Tipos de Ataques

Nesta seção, estão descritos alguns tipos de ataques aos quais os computadores pertencentes a uma rede estão expostos.

2.1.1 Ataques Internos

Segundo Tanenbaum (2003):

> “Uma vez que um cracker tenha tido acesso a um computador, ele pode começar a causar dano. Se o computador tiver um bom sistema de segurança, só será possível prejudicar o usuário cuja conta foi usada para invadir, mas muitas vezes o acesso inicial pode servir de trampolim para outras contas”.

Neste tipo de ataque, é necessário que o atacante tenha acesso direto ao computador atacado, para tentar realizar o que for importante e também o que lhe for permitido.

Nesta categoria de ataques, pode-se encontrar alguns exemplos como os mencionados por Tanembaum (2003):

- **Cavalo de Tróia**: consiste em um programa aparentemente inocente contendo código que realiza uma função inesperada e indesejável. Esta função pode modificar, remover ou criptografar os arquivos do usuário, copiando-os para algum local onde possa ser acessado posteriormente pelo atacante.
- **Conexão Impostora**: relacionada a cavalo de tróia, funciona simulando uma tela de login igual a do sistema operacional. Ao entrar com seu usuário e senha, esta tela some, e a verdadeira tela de login aparece. Desta forma são capturados o nome de usuário e a senha, para tentativas de conexões futuras por parte do atacante.
- **Bombas Lógicas**: tipo de ataque ocasionado pela alta rotatividade de funcionários, onde consiste em uma parte de dados dentro do sistema de produção da empresa, inserida pelo programador. O caso mais famoso de bomba lógica consiste em verificar se no sistema de folha de pagamento do identificador pessoal do programador aparece em dois períodos consecutivos, se caso não aparecer, a bomba explode.

- **Transbordo de Buffer**: procedimento utilizado pois geralmente são usadas *buffers* de tamanhos fixos para cadeias de caracteres como nome de arquivos. Consiste em escrever no *buffer* mais do que ele suporta, ultrapassando os limites da própria área de dados do processo, podendo sobrescrever a área onde continha o endereço de retorno do programa com algum endereço previamente calculado para que se concretizem as intenções do atacante.

2.1.2 Ataques externos

Esse tipo de ataque, segundo Tanembaum (2003, p. 463) “consiste em algum código sendo transmitido pela rede para uma máquina alvo e lá executado causando algum dano”.

Tanembaum, em seu livro *Sistemas Operacionais Modernos* (2003), focaliza neste tipo de ataque os vírus, vermes, códigos móveis e applets java.

A seguir apresenta-se uma descrição breve de cada um destes tipos de ataques, para que posteriormente se expliquem algumas ferramentas que analisam as vulnerabilidades dos hosts na rede para eventual invasão.

2.1.2.1 Vírus

Segundo Tanembaum (2003, p. 463)

> “**vírus** é um programa capaz de se reproduzir anexando seu código a um outro programa, do mesmo modo como os vírus biológicos se reproduzem. Mais ainda, os vírus podem fazer também outras coisas além de se reproduzirem”.

Os vírus podem ser distribuídos de diversas maneiras, geralmente chegam através de e-mail ou mesmo junto com algum programa distribuído na internet.

Existem vários tipos de vírus, dentre eles podemos destacar os vírus residentes em memória, vírus de setor de boot, vírus de drivers de dispositivo, vírus de macro, entre outros.

2.1.2.2 Vermes

Conforme Tanembaum (2003, p. 463) “Vermes são como os vírus, porém se auto-replicam”.

Isso equivale a dizer que os vermes necessitam trafegar de máquina em máquina sozinhos, através de conexões de redes. Os vermes podem ter partes rodando em diferentes máquinas ao mesmo tempo, e mesmo não modificando outros programas, podem carregar com eles o código de um vírus, por exemplo.

2.1.2.3 Código Móvel

Código móvel, é um código que tem sua fonte em um sistema remoto porém executado em um sistema local.

A tecnologia de código móvel é fundamental para o compartilhamento de construções digitais complexas no cyberespaço, que servem como "tijolos" para o desenvolvimento de várias outras tecnologias e aplicações, como por exemplo, as aplicações da tecnologia JAVA, sendo um bloco fundamental nas construções de

plataformas e aplicações para agentes móveis em software, educação e treinamento interativos na *Web*, bibliotecas digitais, mundos virtuais 3D e comércio eletrônico, segundo informações do site da Universidade de Brasília.

O código móvel denomina um conjunto de tecnologias de linguagens e plataforma de sistemas distribuídos que suportam a construção de programas de computador que são instalados nos servidores, transferidos sob demanda para os computadores clientes e automaticamente executados da forma mais segura possível, sobre a plataforma dos computadores clientes.

A utilização de códigos móveis preocupa grande parte dos especialistas de informática que são unânimes em afirmar que sempre existirão brechas de segurança a serem exploradas, qualquer que seja o sistema dos computadores.

Como exemplos desta categoria, temos:

- JavaScript;
- Applet Java;
- Flash;
- Atualizações de software;
- Agentes móveis;
- *Middlewares* de computação em *grid*, etc.

Pode-se notar que a idéia do código móvel é muito interessante, porém deve-se estar atento aos *patches* (correções) relativos as aplicações que utilizam-se desta idéia, para que se evitem danos causados por um eventual ataque ou exploração da falha.

2.1.2.4 Applet JAVA

Applets são pequenos programas Java que são instalados em servidores Web e referenciados através de páginas HTML. Quando um *browser* acessa esta página HTML que referencia o applet, ele automaticamente também transfere o código do applet e o executa.

Este código é intermediário, pois roda em uma máquina virtual Java disparada pelo navegador com diversas limitações de segurança.

Segundo site da Wikipedia (2007), na maioria dos browsers, os applets são executados dentro de uma “caixa de areia” (sandbox), impedindo-os de acessarem os dados da máquina no qual estão sendo executados.

2.2 Técnicas de Ataques

Neste capítulo, encontraremos algumas técnicas utilizadas para se obter acesso a informações privilegiadas das possíveis vítimas de ataques através da manipulação de pacotes na rede.

São técnicas interessantes, utilizadas para conseguir, de alguma maneira, capturar o tráfego da rede, mesmo que switches sejam usados.

2.2.1 Arp Poisoning

O protocolo ARP é o responsável pela resolução de um endereço IP em um endereço MAC. Um outro protocolo, o RARP (ARP reverso), resolve o endereço MAC em endereço IP.

Para que o arp e rarp entrem em ação, são utilizadas quatro mensagens que são:

- Arp request: solicitação do endereço MAC de quem utiliza um determinado IP;
- ARP reply: computador com o ip solicitado no arp request retorna para a rede seu endereço MAC;
- RARP request: um computador pergunta a rede qual o IP de um determinado MAC e,
- RARP reply (o computador que reconhece o endereço MAC retorna seu IP).

De acordo com o exposto, fica claro que para um computador comunicar-se com outro, ele deverá usar estas requisições anteriores, porém, por motivos de eficiência, fica inviável ficar solicitando os endereços MAC e IP a cada comunicação, e por esse motivo os sistemas operacionais possuem uma cache onde são encontrados o IP e seu correspondente endereço MAC, na chamada de tabela arp.

Neste sentido, devido à maneira como alguns sistemas operacionais são desenvolvidos, onde eles aceitam um arp reply sem o ter solicitado (com a mensagem arp request), pode acontecer de um computador A mandar um arp reply com o IP da máquina B para o computador C. Este por sua vez atualiza sua cache com o novo endereço MAC para o IP de B, e quando o computador C quiser se comunicar com a máquina B esse tráfego será direcionado para a máquina A.

Esse tipo de ataque pode ser usado para desvio de sessão e ataque do tipo denial of service.

No caso do ataque de sessão, mais conhecido *como ataque de homem-do-meio*, um computador invasor intermedeia a troca de informações entre um computador A e um computador C, dizendo para rede que os endereços IP de A e de C correspondem ao seu endereço MAC, com isso, toda informação que vai de A para C ou vice-versa, é passada pelo computador B que tem acesso irrestrito aos pacotes, podendo até modificá-los.

A anatomia de um ataque desse tipo é realizado quando temos as estações com suas tabelas arp contendo o endereço IP e o seu respectivo endereço MAC.

Para uma estação B se colocar no meio da comunicação entre uma máquina A e uma máquina C, ela deve enviar pacotes arp adulterados para A e C dizendo que endereço IP de C e o endereço IP de A estão associados ao seu endereço MAC.

Depois que a estação B fez o ataque, se a estação A quiser mandar um pacote para a estação C ou vice-versa, os pacotes passarão pela estação B que só tem que encaminhar os pacotes, e antes de encaminhá-los pode ver o conteúdo ou até mesmo modificá-lo.

Na figura 1, podemos verificar o funcionamento desse ataque, onde a flecha em vermelho corresponde ao computador A enviando dados ao computador C e a flecha azul indica o computador C enviando dados ao computador A.

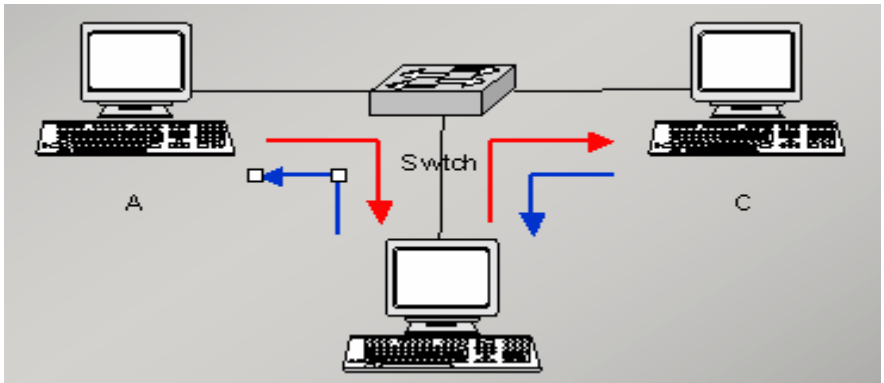

Figura 1 – Fonte http://www.fe.up.pt

Com esta estrutura montada, é possível verificar a troca de informações entre os computadores. Além disso, com o auxílio da ferramenta *ettercap*, é possível realizar diversos ataques sob estes dois computadores.

Nesse sentido, pode ser feito um desvio http ou https para um servidor forjado, ataque este conhecido como DNS spoofing, onde o ettercap coloca-se entre o cliente e qualquer outra estação de forma a capturar as suas informações.

Ao ser feita uma requisição ao servidor DNS (DNS request) para saber o IP de um determinado site, o ettercap detecta essa resposta e altera o endereço IP da resposta para o endereço IP desejado (o de outro servidor criado para capturar dados).

Assim que o cliente recebe o DNS reply (resposta com o IP do servidor forjado), faz o pedido de página web ao servidor, e o ataque do *homem-do-meio* pode continuar ou não. O *homem-do-meio* pode continuar ou não, se sim, no caso de usar https, o certificado que o cliente vai receber, serão do *homem-do-meio*, se não, recebe o certificado do servidor forjado.

Para direcionar a vítima para o endereço IP desejado, deve ser editado o arquivo etter.dns, localizado no diretório de instalação do Ettercap.

Vale lembrar que para ataques desse gênero, o plugin que possibilita o dns spoofing deve estar ativado.

2.2.2 Redirecionamento ICMP

Técnica utilizada por roteadores para comunicar que existe um outro roteador em melhores condições para enviar um pacote de uma máquina para um destino.

Sua utilização é notada quando um roteador recebe um pacote, e este pode retornar ao emissor uma mensagem de redirecionamento (*ICMP redirect)*, caso o roteador conheça um outro roteador que possa fazer a entrega com menor custo. Há que se dizer, que isso pode acontecer apenas quando o transmissor, o receptor e o roteador estão na mesma rede local.

Pelo fato dos pacotes ICMP ficarem encapsulados dentro de um datagrama IP, os primeiros 3 campos são iguais para todos os tipos de mensagens ICMP, resultando num total de 4 bytes. A estrutura de um pacote ICMP é mostrada no capítulo 3, seção 3.3.

De posse dessa informação, um atacante pode desviar todas as seções para a máquina que desejar, e para fazer isso, é necessário criar uma mensagem de redirecionamento ICMP composta pelo cabeçalho IP de 64 bits do *payload* do pacote escutado (pacote capturado) e o endereço IP para o qual se quer desviar o tráfego.

Após isso, é necessário ficar monitorando a chegada dos pacotes de redirecionamento IP e fazer o que o atacante achar melhor sobre os dados.

Para esclarecer o redirecionamento ICMP, segue anatomia deste tipo de ataque:

- Uma máquina A envia um pacote para uma máquina B cujo endereço Ip está fora da sua sub-rede, e por este motivo, é enviado através de um roteador R1;
- O roteador R1 possui uma rota para B através de um roteador R2;
- Se o endereço de R2 pertence a mesma sub-rede de A, o roteador R1 envia uma mensagem de redirecionamento ICMP informando a máquina A que R2 é a melhor rota para se chegar a B.
- O roteador R1 envia depois os pacotes para R2, para que este os entregue a B.

Recebendo a mensagem de R1 (redirecionamento ICMP), a máquina A atualiza a sua tabela de roteamento com a informação recebida na mensagem, de maneira a deixar armazenada que R2 é a rota para se chegar a B, evitando o caminha A envia para R1, R1 envia para R2 e R2 envia para B.

2.2.3 Port Stealing

Em redes interligadas por switches, a troca de informações entre os computadores é feita pela análise do endereço MAC pelo switch, e como no switch existe uma tabela interna onde nela consta o registro de todos os endereços MAC com suas respectivas portas, cada pacote é direcionado especificamente para o computador de destino, o que não ocorre nos hubs.

Uma maneira de conseguir capturar tráfego alheio, enganando o switch, chama-se *port stealing*, que é realizado da seguinte forma:

- O atacante envia muitos pacotes para camada 2 com o endereço de origem igual ao do host da vítima e destino igual ao endereço MAC do atacante.
- Em algum momento, o atacante rouba a porta da vítima, pois o switch atualizará sua tabela interna com as informações. A partir da atualização da tabela interna do switch, todos os pacotes destinados a vítima, serão direcionados para o atacante;
- Quando o atacante receber um pacote que estava destinado a uma de suas vítimas, ele gera uma requisição arp (arp request) para o IP da vítima;
- Quando o atacante receber a resposta arp (arp reply) da vítima, a porta no switch é “devolvida” para a vítima da mesma maneira que estava antes do ataque começar;
- O atacante pode agora encaminhar o pacote para vítima e reiniciar o ataque port stealing, porém, antes de ele encaminhá-lo, ele pode ver o conteúdo e modificá-lo se for o caso.

Este tipo de ataque se encaixa no perfil *ataque homem-do-meio*.

2.2.4 DoS

Ataque caracterizado por tirar de atividade um serviço ou um servidor por completo.

A idéia geral é consumir todos os recursos da máquina, de maneira a fazer com que o computador atacado não consiga atender a mais nenhuma solicitação, caracterizando nesse caso a negação de serviço.

Como exemplos desse tipo de ataque podemos encontrar o *estouro de partição*, onde é necessário estar logado no sistema, e desta forma uma determinada partição é

lotada com dados inúteis. Outro tipo de ataque DoS, é o de enviar para a rede um número de pacotes superior ao limite que o destino é capaz de absorver.

Além destes temos vários outros, e podemos encontra-los em (MELO, 2004).

2.2.5 DHCP spoof e DNS spoof

Esta técnica pode ser usada para causar indisponibilidade ao host, pois são passados para os computadores que solicitarem os endereços de IP e servidores DNS, e nesse caso, pode-se passar endereços inalcançáveis ou mesmo inexistentes.

Além desse objetivo, também pode-se desviar sessões para obter senhas e outras informações (um ataque conhecido como de DNS *spoof*), pois ao realizar-se um ataque desse tipo pode-se redirecionar os domínios para onde quiser, bastando para isso montar a estrutura de servidores e páginas.

3. FERRAMENTA ETTERCAP

Pelo exposto na documentação (Ornaghi, Valleri, 2000) que acompanha o software

> "Ettercap é um *sniffer* que inicialmente foi projetado para operar em redes locais de computadores utilizando switches (e *hubs* por conseguinte*)*, porém ao longo do seu desenvolvimento foram sendo agregadas muitas funcionalidades, sendo otimizado para ataques de homem-do-meio".

Segundo Melo (2004, p. 171) "Ettercap [...] é uma ferramenta que reúne recursos de várias técnicas de exploração de vulnerabilidades".

Esta ferramenta faz parte de um projeto em constante atualização, e traz como destaque recursos para execução de DoS, *Scanners* (varredura na rede em busca de portas abertas), *FingerPrint* (técnica de descoberta do sistema operacional da vítima através da análise da pilha tcp/ip, onde os dados são analisados e comparados com uma base de dados previamente construída para a identificação do sistema operacional), *Spoofing* (técnica para se fazer passar por outro computador na rede), ataques MITM (*Man in the Middle* – ataque de homem do meio) customizados.

O modo como opera não é muito "oculto", pois envia um ARP REQUEST para toda a faixa de IP da LAN, considerando o IP corrente e a respectiva máscara da rede, como pode-se ver na figura abaixo, e uma vez que receba os ARP REPLIES, cria uma lista dos hosts que estão na rede, mapeando-a.

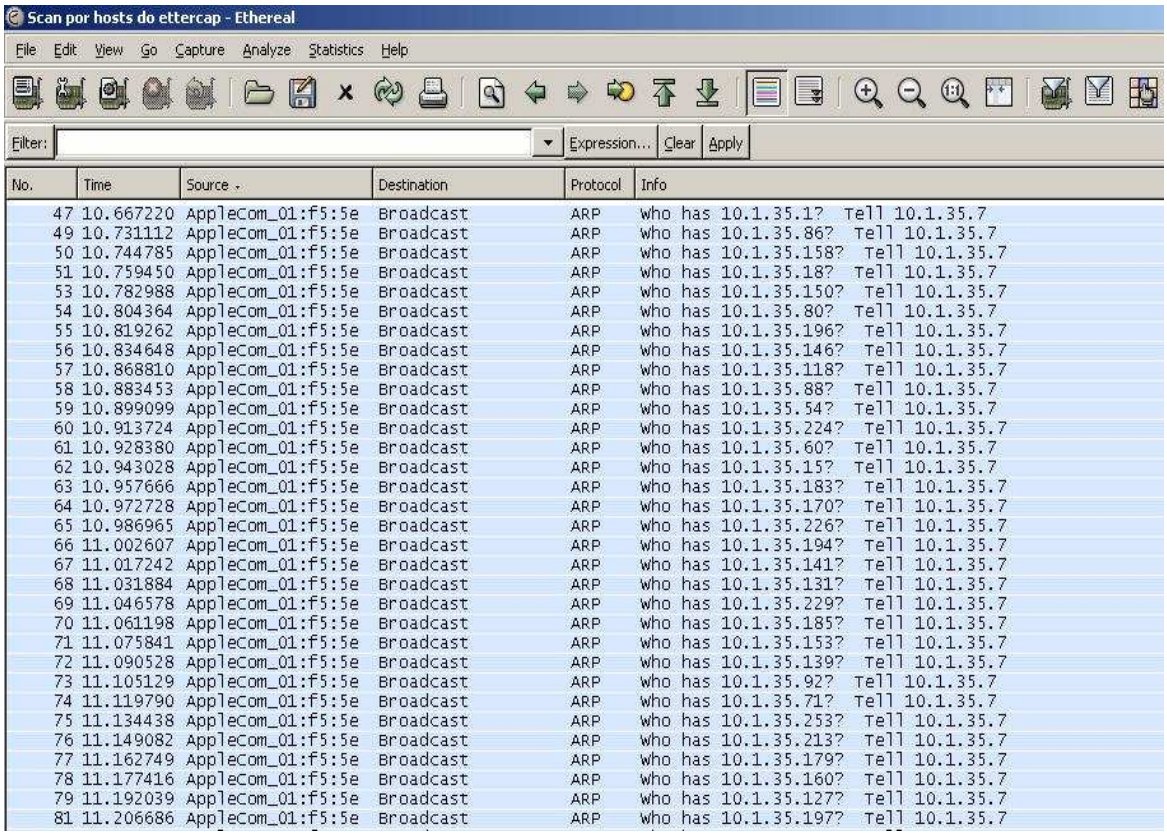

Figura 2 Ethereal capturando tráfego no instante que o Ettercap procura hosts

O Ettercap atua na camada 2 do modelo OSI, passando muitas vezes despercebido pelos administradores de rede, pois poucos usam monitoramento ou métodos para quantificar atividades nessa camada.

Para interagir com esse software, são fornecidas 3 opções de interfaces que são :

- Text Mode: modo texto clássico, ideal para os puristas mais radicais;
- Ncurses: interface bem organizada utilizando o mesmo layout que a GTK;
- GTK: interface gráfica baseada em GTK ;

Por ser uma poderosa ferramenta, possui inúmeros parâmetros de configuração, os quais podem ser encontrados pela internet, ou mesmo na obra *Exploração de Vulnerabilidades em Redes TCP/IP* (MELO, 2004). Com esta ferramenta é possível serem utilizados os ataques de ARP poisoning, ICMP redirect, DHCP spoofing, port Stealing e dns spoofing.

Nos capítulos posteriores, serão detalhados aspectos referentes à instalação e configuração dessa ferramenta, utilizando, praticamente, alguns de seus recursos de maneira a explorar da melhor forma a ferramenta.

3.1 Instalação

Esta ferramenta pode ser utilizada em diversas plataformas como, por exemplo Windows , OpenBSD, FreeBSD, Solaris, Mac OS X e linux.

Porém nesse trabalho, esta ferramenta foi instalada no sistema operacional Windows XP e em uma distribuição Linux chamada Fedora Core 4.

Em ambiente Windows, a instalação foi super simples, bastando apenas a execução do programa fonte, porém em ambiente Linux, foi preciso a instalação das bibliotecas adicionais como o libpcap, libnet, libpthread, zlib e o GCC (compilador da linguagem C) para que o software pudesse ser instalado.

3.2 Configuração

Esta ferramenta é muito fácil de ser configurada, bastando para isso que o usuário modifique as configurações contidas no arquivo etter.conf localizado no subdiretório *share* da pasta onde foi instalada ferramenta.

Além deste arquivo, podemos também modificar o arquivo etter.dns, pois é neste arquivo que encontramos dados de quais domínios serão direcionados. Por padrão, este arquivo já vem com domínios da microsoft apontando para sites do linux.

Nos testes realizados apenas o arquivo etter.dns foi modificado para a inserção de mais domínios com o objetivo de aumentar as chances de um ataque do tipo *dns spoofing*.

3.3 Testes práticos com a ferramenta

Os testes realizados com essa ferramenta, foram aplicados em um prédio residencial, onde existe uma rede interligada por switches.

Esta rede é composta por um servidor que tem como funções manter um servidor dhcp, e um *gateway* para a internet.

Devido à quantidade de ataques possíveis de se realizar com esta ferramenta, começamos por colocar em prática o chamado redirecionamento ICMP. Com este ataque foi possível enviar para rede as informações necessárias para que os computadores enviassem pacotes por outra rota (a do computador atacante), tornando dessa forma a informação ao alcance do atacante.

Porém, para um maior aproveitamento desse ataque, foi necessário utilizar o Ethereal (nome empresa ou autores e ano) para capturar os pacotes redirecionados, como pode ser visto na figura 3:

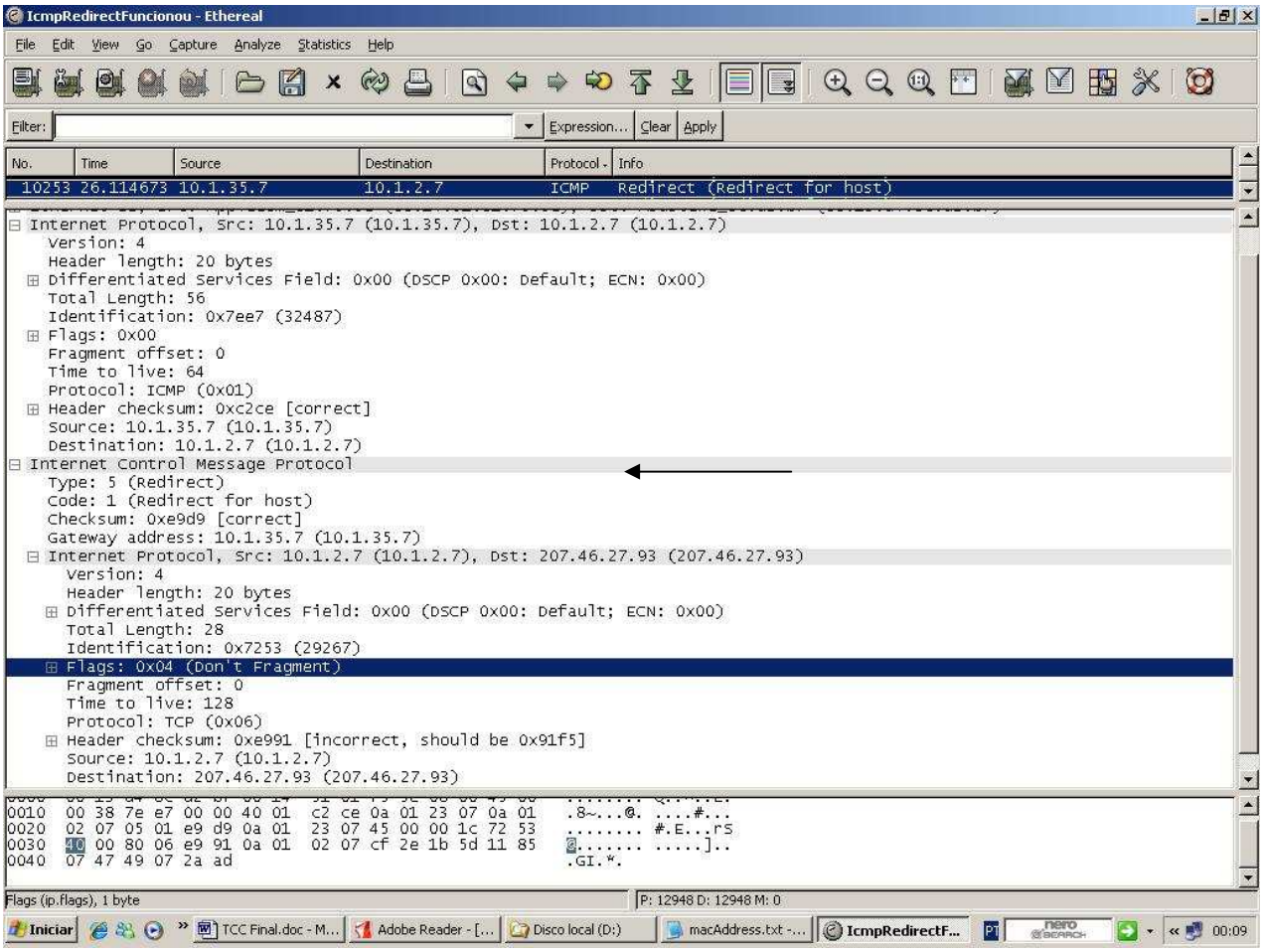

Figura 3 – redirecionamento IP.

Pode-se verificar na figura acima, na direção da seta, o campo *type* do cabeçalho contendo o número 5, indicando redirecionamento ICMP. Abaixo segue descrição do cabeçalho completo de um pacote ICMP:

- Type (8 bits) : Identifica a mensagem determinando pelo valor desse campo, o formato do datagrama. Para informações dos valores, vide Melo (p.41, 2004);
- Code: fornece mais informações sobre o tipo de mensagem Nosso exemplo o número 1 indica que o datagrama foi redirecionado para o host alcançável. Para maiores informações, consultar: http://www.faqs.org/rfcs/rfc792.html.
- Checksum (16 bits): verifica a integridade do cabeçalho (*header*).

Nos testes realizados com esta ferramenta, foi analisado o potencial do ataque DNS spoofing. Para redirecionar um domínio, são necessárias algumas alterações no arquivo etter.dns, pois é lá que encontram-se os nomes dos domínios e os respectivos IP´s que devem ser convertidos. Vale lembrar que mudanças são para personalizar ou mesmo aumentar o número de redirecionamentos, pois por padrão o domínio microsoft já vem redirecionado.

Nos testes realizados, foram redirecionados os domínios da Microsoft para IP's do Linux, conforme abaixo:

- microsoft.com A 198.182.196.56;
- *.microsoft.com A 198.182.196.56;

Isso equivale a dizer que tudo o que contiver a string Microsoft.com será direcionado para o IP: 198.182.196.56 , ou seja, o site http://www.linux.org/ .

Além destes dois ataques, o dhcp spoofing foi utilizado, onde se forja um servidor dhcp, indicando aos computadores que solicitarem IP que o *gateway* ou servidor DNS é o IP do atacante. Com isso, todas as informações que trafegarem do computador da vítima para internet, passarão pelo computador do atacante, que pode ter acesso a informações privilegiadas da vítima, como número do cartão de crédito, senha de e-mail, entre outros.

Comprovando que esta ferramenta funciona como sniffer na rede com switch, vários *logins* e senhas foram coletados, tanto de sites não seguros, como de tentativas de conexões POP.

.

3.4. Avaliação da ferramenta

Esta ferramenta mostrou-se muito eficaz no ambiente testado, onde foi possível realizar ataques do tipo *dns spoof*, redirecionamento *ICMP* e o *DHCP spoof*, sendo que este último foi facilitado, pois todos os computadores (exceto servidores) obtêm endereço *IP* via dhcp, porém possui muitos outros ataques interessantes, como por exemplo, o de poder realizar um ataque homem-do-meio em uma conexão segura (https) ou não segura.

Este *sniffer* se distingue de outros pelo fato de não ser obrigatoriamente passivo, como é o caso do Ethereal, pois o ettecap pode atuar de modo ativo inserindo dados entre as conexões existentes na rede ou mesmo matando uma conexão. Aliado a isso, é possível utilizá-lo em ambientes onde a rede é interligada por *switches*, o que não ocorre na maioria dos *sniffers*, tornando-o mais vantajoso que o Ethereal, por exemplo.

Por outro lado, o ponto negativo encontrado nessa ferramenta, refere-se ao fato de como ela mapea a rede, porque esse processo não é oculto, pois são enviados pacotes com requisições *ARP* para toda a faixa de *IP*'s da rede de acordo a faixa e máscara IP do computador do atacante.

4. ETHEREAL

É uma ferramenta *open source* e atualmente está disponível para diversas plataformas unix, linux e Windows, enquadrando-se na categoria de sniffers, sendo portanto um analisador de pacotes da rede, ou seja, ele pode capturar o tráfego de pacotes que chegam até a interface de rede do computador, mesmo que os pacotes não sejam para a estação em análise (modo promíscuo), tentando mostrar o maior número de detalhes possíveis.

Para que tenha condições de capturar informações destinadas a outros computadores, é necessário que a rede seja interligada por hubs[1], no caso da tecnologia ethernet, pois caso esteja interligada por switch[2], este *sniffer* não conseguirá capturar o tráfego destinado a outros computadores, pois o *switch* já direcionada os dados para a porta onde o computador de destino esta ligado, evitando dessa maneira que a informação se propague para todos os computadores da rede, ficando dessa forma, a ferramenta monitorando apenas o tráfego destino ao computador com o Ethereal instalado.

4.1 Instalação

Esta ferramenta foi instalada em ambiente Windows, e para que a mesma funcione, é necessário instalar o libpcap, capturador de pacotes que o etheral utiliza, e o kit de ferramentas GTK, utilizado para criar os gráficos do programa.

A instalação feita não apresentou problemas, e dessa forma foi possível utilizá-lo em seu mais perfeito funcionamento.

---

[1] Hub: equipamento de interconexão de computadores que recebe dados em uma porta específica de um computador e o entrega em todas as portas.

[2] Switch: interconecta computadores como o hub, porém a diferença é que o switch ao receber os dados de um computador de origem, o entrega diretamente na porta onde se encontra o computador destino.

4.2.Configuração

Esta ferramenta já vem previamente configurada para coletar os pacotes mais utilizados nas redes, porém de acordo com a necessidade do usuário, torna-se necessário à utilização de alguns filtros.

Algumas modificações feitas são apresentadas na seção seguinte.

4.3. Testes com a ferramenta

Este *sniffer* possui vários parâmetros de configuração, mostrando por completo o conteúdo dos pacotes.

Nos testes realizados, foi possível analisar o cabeçalho IP para a demonstração de como é um pacote de redirecionamento ICMP, atuando em conjunto com a ferramenta ettercap que enviou os pacotes com a instrução de redirecionamento.

Devido a rede possuir a interconexão com os switches, não foi possível capturar informações particulares nos pacotes enviados.

Para esclarecer o seu uso, serão mostradas as telas e algumas funcionalidades.

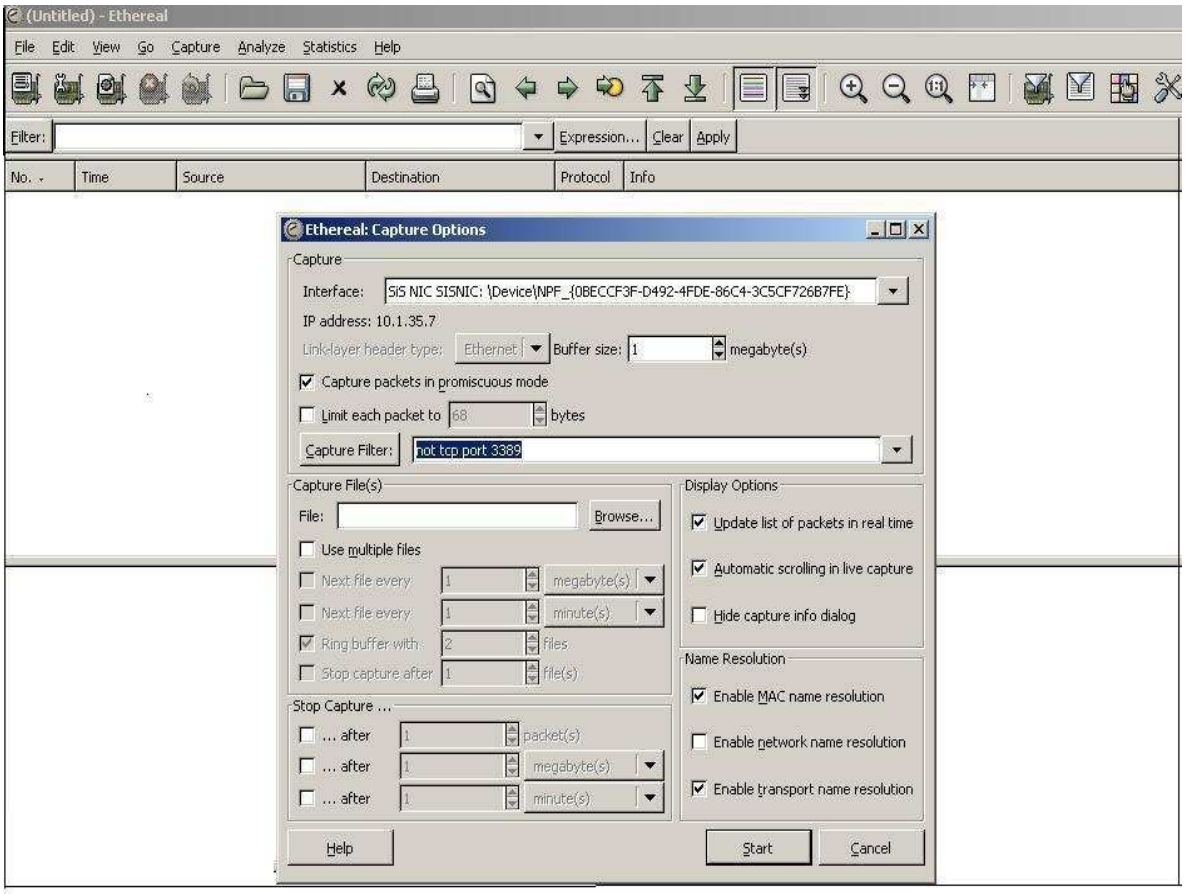

Figura 4 - Tela de configuração para determinar o modo da escuta

Na figura 4, podem ser verificadas as opções para iniciar uma escuta no tráfego da rede. No campo filtro de captura, podemos introduzir o que queremos verificar, sendo que este pode ser o IP do computador desejado, o endereço MAC de um computador, mensagem broadcast ou multicast, somente tráfego na porta 80, filtrar apenas pacotes TCP, ou UDP, entre outros filtros.

Nos testes realizados, foram aplicados filtros para determinados hosts (ip), e pacotes (TCP,UDP, ARP, ICMP..), para que a análise ficasse mais clara, porém para efeito de análise, será mostrado apenas a tela onde o filtro aplicado foi do protocolo arp, muito utilizado em redes, pois o mesmo faz a associação entre o endereço IP e o endereço MAC, como mostrado na figura 5.

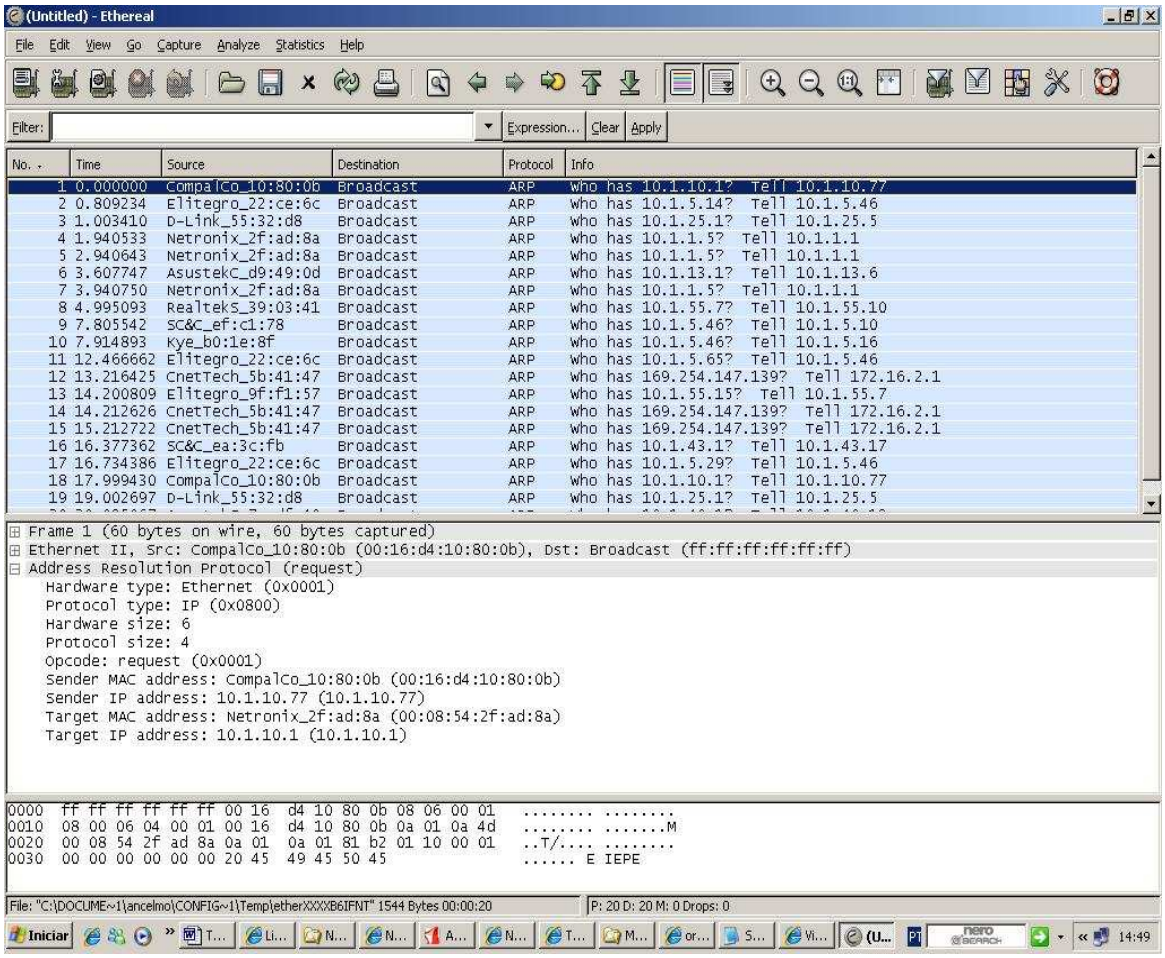

Figura 5 – Exemplo de requisição arp

Como pode ser visto, na parte intermediária da figura 5, pode ser encontrado o cabeçalho de um pacote arp. Para facilitar o entendimento, segue o formato de um pacote arp:

Hardware type: especifica o tipo de hardware, ou seja, a tecnologia usada. Nesse caso temos o valor Ethernet;

Protocol type: especifica o tipo de protocolo ao qual o endereço lógico se refere. Nesse caso temos o valor IP;

Hardware size: determina o comprimento em bytes do endereço MAC. No nosso exemplo acima são 6 bytes (exemplo: 00:16:d4:10:80:0b);

Protocol size: determina o comprimento em bytes do endereço do protocolo. Nesse caso 4 bytes (exemplo: 10.1.10.77);

Opcode : tipo da operação, valor booleano (request ou reply) No nosso caso, a operação foi de requisição.

Sender MAC address : possui o endereço MAC do solicitante;

Sender IP address: possui o endereço IP do silicitante;

Target MAC address: endereço MAC de um computador ao qual se deseja estabelecer comunicação. Em pacotes arp normais, este campo vem com o valor zerado.

Target IP address: endereço IP ao qual deseja-se saber o endereço físico, ou seja, endereço IP do computador ao qual se quer comunicar.

A ênfase no protocolo arp, é devida a utilização massiva pela ferramenta ettercap, onde através da técnica arp poisoning, ela consegue capturar tráfego em redes interconectadas com switches.

4.4. Avaliação da ferramenta

De acordo com o exposto, podemos verificar que esta ferramenta possui inúmeras funcionalidades.

Como pontos fortes dessa ferramenta, podemos encontrar a quantidade de formatos dos arquivos de saída gerados, onde podemos salvar uma varredura em um formato que seja legível por outros programas como o tcpdump, Novel LANalyzer, sun snoop, entre outros, porém o Ethereal também consegue ler arquivos de logs capturados por estas ferramentas como sun snoop, tcpdump, Novel LANalyzer, microsoft network monitor, H-UX´s nettl entre outras.

Além disso, mostra a estrutura completa dos pacotes que trafegam na rede, é muito fácil de utilizar, possui uma interface amigável diferenciando os tipos de pacotes pela cor em que os apresenta, e funciona capturando tráfego de muitas tecnologias, como por exemplo ethernet, token ring, 802.11, ATM.

Como pontos negativos, pode ser citado o fato de não funcionar em redes ethernet interligadas com *switchs*.

5. NESSUS

O Nessus é uma ferramenta de auditoria muito usada para detectar e indicar uma maneira de solucionar as possíveis vulnerabilidades encontradas nos computadores.

Essa ferramenta era open-source até a versão 2.2.8, e passou a ser código fechado, porém continua sendo uma ferramenta de uso gratuito e é distribuída através do site: <http://www.Nessus.org>. Sua versão atual é a 3.0.

Seus recursos são muito avançados, e uma grande vantagem que possui em relação a outras ferramentas desse gênero, é que o Nessus varre todas as portas TCP´s detectando servidores ativos e simula invasões para detectar vulnerabilidades.

Para executar as varreduras de portas, o Nessus utiliza o Nmap, um portScan muito poderoso.

Esta ferramenta possui uma facilidade que se refere ao usuário não precisa ter o servidor do Nessus instalado no seu computador, ou seja, precisa apenas do cliente instalado, pois ele permite a estrutura cliente-servidor para que vários pontos da rede possam ser analisados. Nessa arquitetura, vários clientes podem controlar os servidores. Nesse sentido, a parte servidora executa os testes e a parte cliente configura e emite os relatórios.

Ao término de uma varredura, são apontadas as possíveis vulnerabilidades, e de uma maneira sucinta, é explicado de que forma o host pode ser atacado e como se proteger para corrigir essa vulnerabilidade. Além disso, nos relatórios do escaneamento são criados links para uma página específica de acordo com o plugin encontrado na vulnerabilidade, onde podemos encontrar mais detalhes sobre os riscos envolvidos, como o tipo de acesso (como exemplo: remoto), complexidade de ataque (indefinido, baixo ou alto), modo de autenticação (indefinido, requerido ou não requerido), o impacto

sobre a confidencialidade (indefinido, nenhum, parcial, completo), disponibilidade (indefinido, nenhum, parcial ou completo) e a integridade (nenhum, parcial ou completo).

5.1. Instalação

A instalação dessa ferramenta foi em ambiente Windows, e o processo de instalação consistiu em obter o arquivo fonte, instala-lo, e para finalizar o processo de instalação é necessária uma chave de liberação do produto.

Ainda após este procedimento, ao ser inicializado, o Nessus precisa atualizar seus arquivos de dados, os quais possuem mais dados referentes a mais serviços ou sistemas operacionais agregados a ferramenta para aumentar seu poder de atuação.

5.2. Configuração

Esta ferramenta, assim como outras, já possui um modo padrão de escaneamento, porém, caso seja necessária alguma configuração adicional, servirá apenas para customizá-la de acordo com as necessidades do usuário.

5.3. Testes com a ferramenta

Este capítulo tem por objetivo demonstrar o uso da ferramenta Nessus, e na figura 6 abaixo, encontramos a tela inicial do Nessus, onde podemos escolher entre as opções de fazer um scan ou analisar os relatórios de scans já realizados anteriormente.

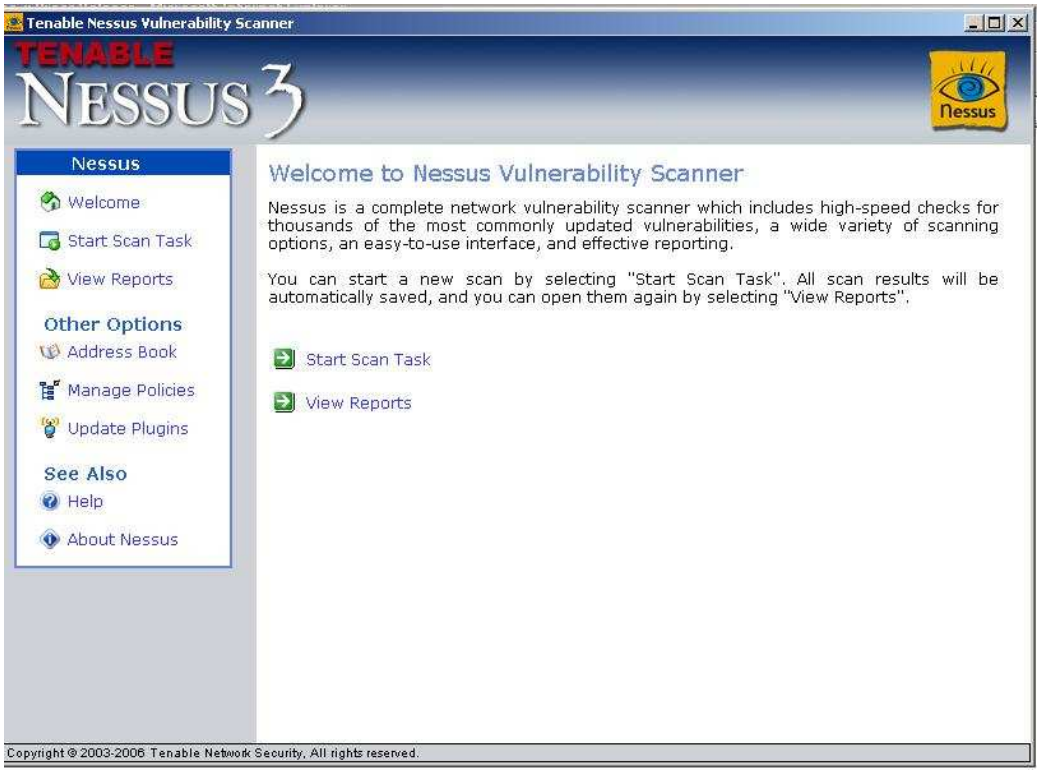

Figura 6 - Tela inicial Nessus

Caso a escolha seja a de fazer um scan, a figura 7 aparecerá:

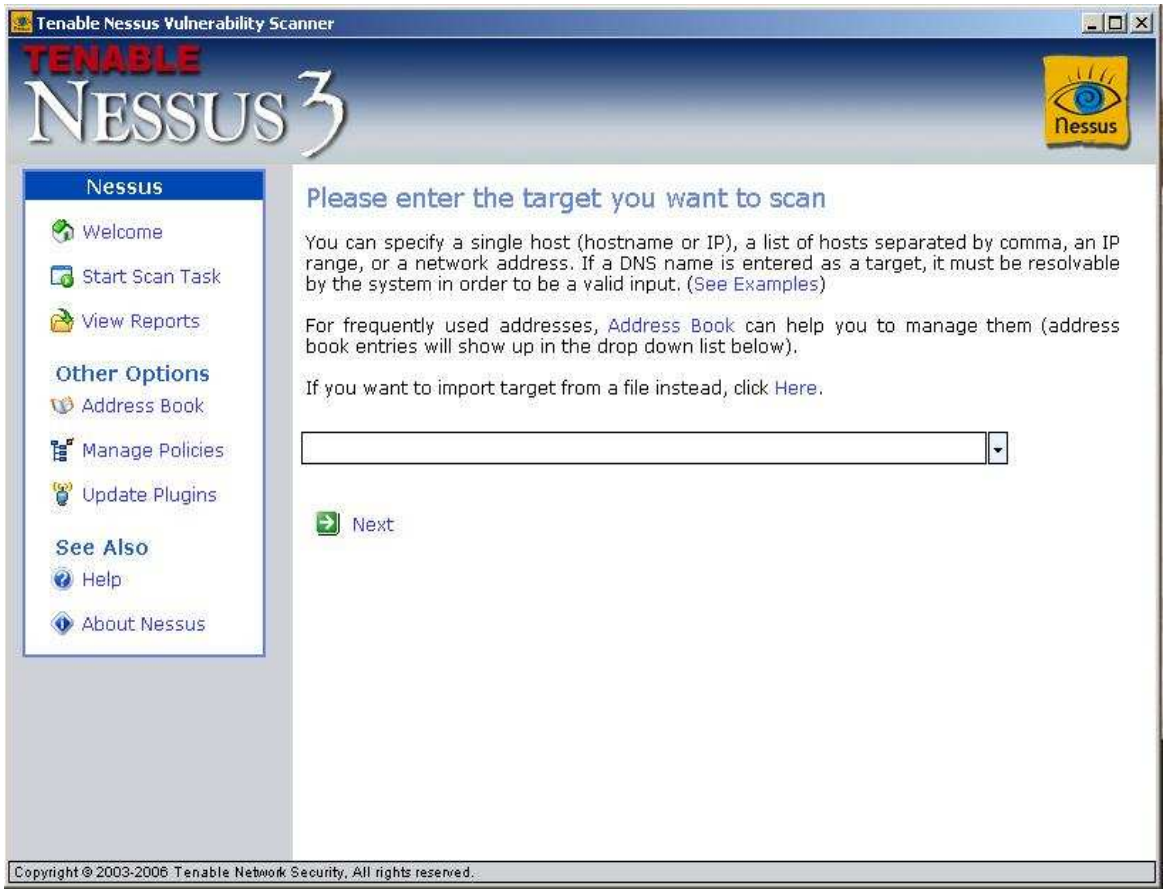

Figura 7 - Tela de escolha do host através do IP ou o nome.

Após a inserção da identificação do servidor (pelo IP ou o nome), o Nessus apresenta uma tela onde o usuário pode escolher quais plugins deseja usar em sua varredura.

Para se ter uma idéia do poder dessa ferramenta, existem hoje algo em torno de 13608 plugins (retirados de: <http://www.Nessus.org/plugins/index.php?view=all>), sendo que a cada dia surgem inúmeros outros, pois o processo de aquisição de plugins é cooperativo, e a ferramenta contempla isso, pois quando ela não reconhece a

vulnerabilidade ou alguma outra informação sobre o host, é perguntado ao utilizador se ele tem as informações sobre aquela vulnerabilidade, para que seja enviado para o setor do desenvolvimento testar e comprovar a veracidade das informações, e se for o caso inseri-la como um novo plugin.

Comprovando o que foi dito na frase anterior, nos testes realizados, a ferramenta não conseguiu identificar o sistema operacional de um dos hosts varrido, e solicitou informações sobre ele, porém não se tinha conhecimento de qual era o sistema operacional, e portanto, nada foi enviado a fábrica do software.

O próximo passo, refere-se a escolha dos plugins.

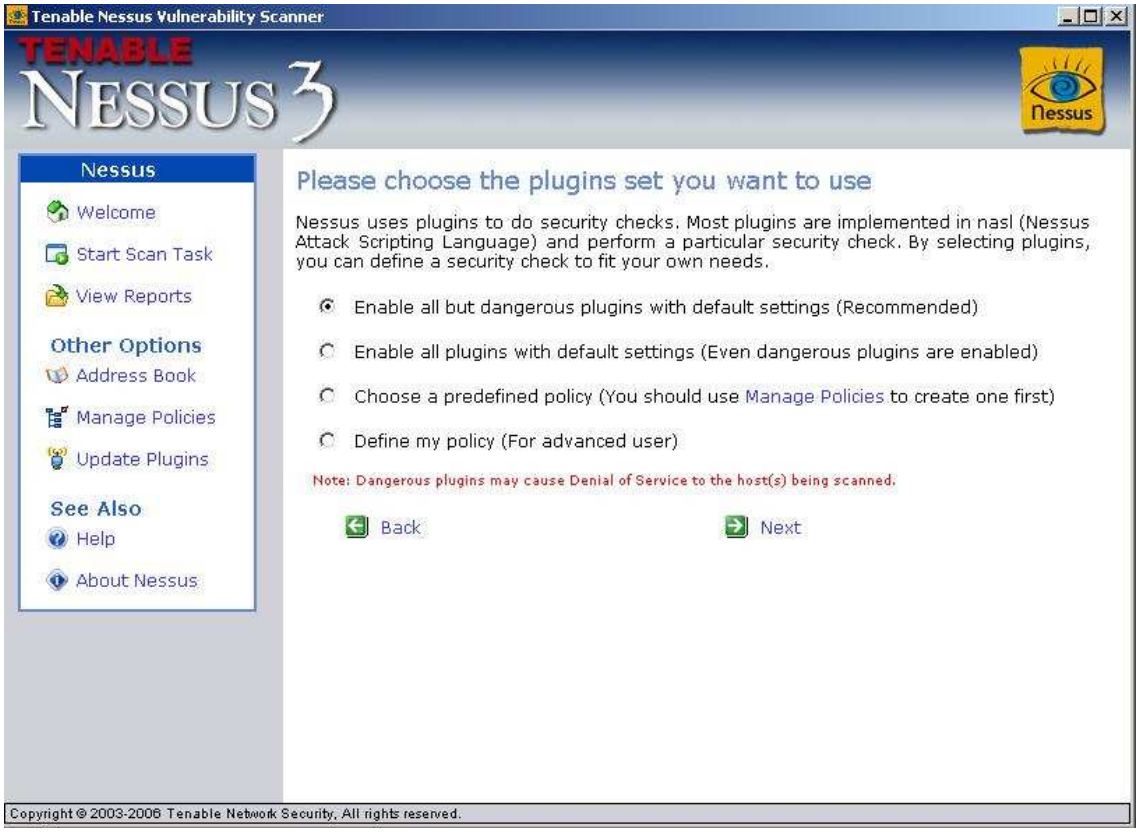

Figura 8 - Escolha dos plugins para a varredura.

Nas varreduras realizadas, foram ativados todos os plugins mais perigosos com as configurações padrões.

A próxima e última tela antes do diagnóstico apresenta a funcionalidade de realizar a varredura através do computador local ou de um servidor, sendo que nos testes realizados foram utilizadas varreduras através de um único computador.

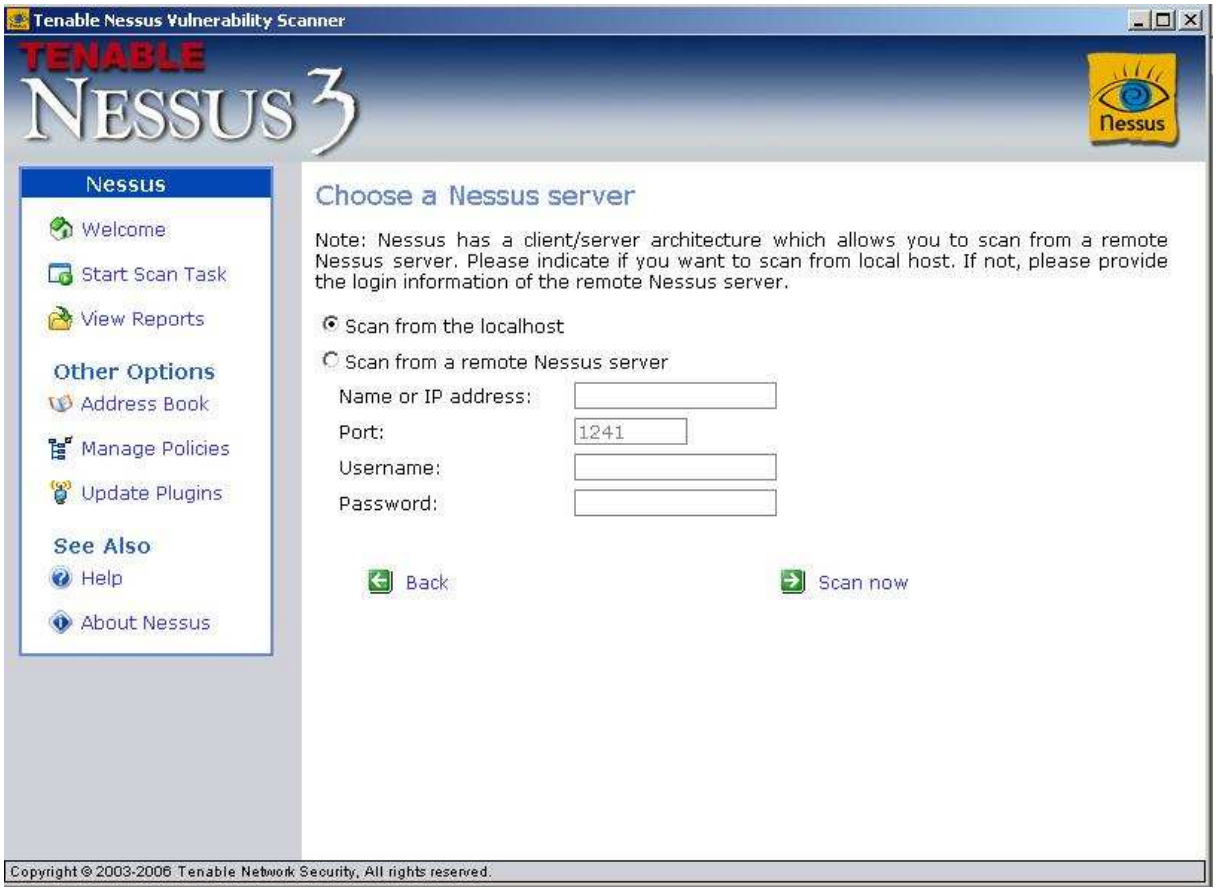

Figura 9 - Escolha do ponto de partida da varredura.

Após a varredura, tem-se o resultado da mesma no formato de uma página Web, onde podemos encontrar o diagnóstico da ferramenta. Na figura 9 tem-se um esboço do que pode-se encontrar após uma varredura.

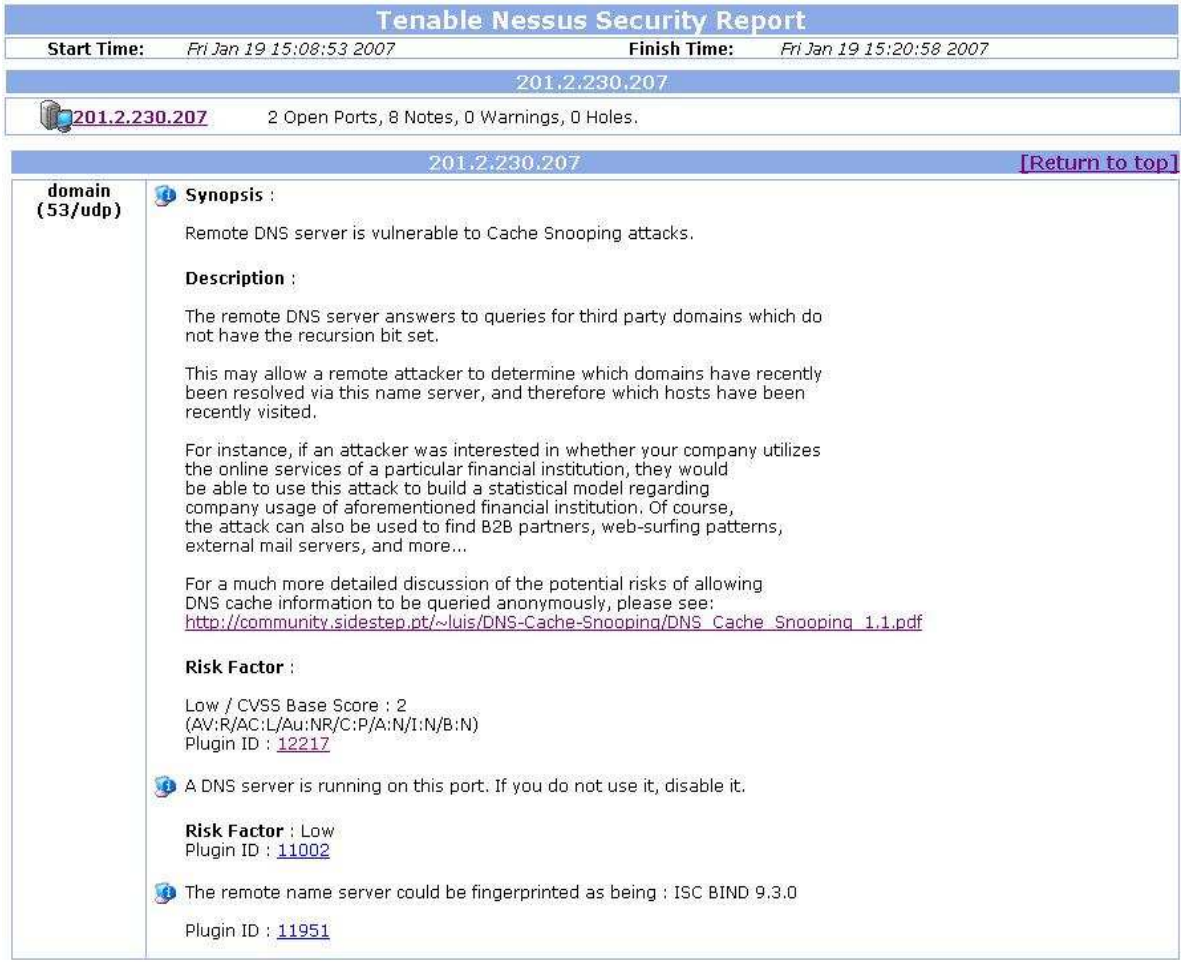

Figura 10 - Esboço de uma parte do relatório de uma varredura

Nesta parte do relatório da ferramenta, pode-se verificar na primeira linha a data e hora de início e de fim da varredura. Já na segunda linha, pode-se verificar qual o IP ou nome do computador escaneado assim como a quantidade de portas abertas (nesse caso 2) e as notas (que neste caso são 8) e os possíveis avisos referentes aos resultados coletados, porém para efeito de análise nesse momento, apenas a mais importante foi mostrada.

Neste caso acima, ele alerta para o fato de um servidor DNS estar rodando, e além disso, ele explica que o hosts está vulnerável a ataques do tipo cache spoofing, onde é possível determinar os últimos sites de acessos desse servidor, podendo dessa

forma traçar um perfil sobre navegação na Web, ou mesmo identificar relações entre a empresa e uma instituição financeira.

Além das facilidades citadas acima, pode-se selecionar na primeira tela a opção de ver os relatórios de todas as varreduras feitas, onde pode-se encontrar as opções de apagar um relatório salvo, importar um relatório ou comparar 2 relatórios, conforme Figura 10.

Figura 11 - Escolha por ver os relatórios do Nessus.

Nesta tela do programa, para apagar um ou mais relatórios, basta que sejam selecionados os relatórios que se desejam apagar e clicar em *delete selected report*(s). Caso tenha-se um relatório a ser importado, pode-se optar pelo menu *Import report* (desse modo pode-se inserir um relatório obtido de outra máquina e colocá-lo na base

do Nessus local, e caso seja necessário comparar duas varreduras, basta escolhê-los). A saída dessa última funcionalidade mostra o conteúdo de um relatório na direita e outro na esquerda, sendo que a análise fica por conta do usuário.

5.4 Análise da ferramenta

Esta ferramenta é eficiente na identificação dos serviços e sistemas rodando nos micros da rede.

Características importantes da ferramenta: a facilidade de utilização, interface amigável, relatórios bem detalhados dos serviços rodando no computador, assim como procedimentos a serem realizados no caso de alguma vulnerabilidade ser detectada,

Como pontos negativos, um problema encontrado é que não é possível trocar endereço IP da máquina do atacante, possibilitando a identificação da origem da varredura, e uma restrição encontrada na ferramenta, foi a de que não é possível estipular um tempo de alternância entre as portas do computador alvo, podendo dessa forma a ferramenta ser detectada por anti-portscanners, como o portsentry, por exmeplo.

6. JOHN THE RIPPER

Este software é um poderoso decifrador de senhas. Inicialmente desenvolvido para sistemas Unix-like, porém atualmente ele pode ser utilizado em ambientes DOS, Windows, BSD e linux. Ele pode fazer ataques de força-bruta nas senhas armazenadas no formato DES, MD4 e MD5, entre outros.

Ele pode atuar nos arquivos de senhas com o método de ataque de dicionário, onde são lidas as palavras de um *wordlist* (lista de palavras), e nesse modo de operação, quanto maior for a *wordlist*, mais chances de se obter sucesso na descoberta das senhas; pode operar também por combinações dos nomes e das iniciais dos usuários ou ele mesmo pode gerar suas próprias combinações, sendo que esta última consome muitos recursos da máquina, e a mesma deve ser usada com cautela, principalmente no modo diferente do *single*, pois consome muito tempo de CPU, podendo derrubar outros serviços.

Este aplicativo, pode ser de grande utilidade para um administrador de redes, pois com ele é possível analisar a complexidade das senhas que os usuários utilizam, e com base nessa análise, cabe ao responsável pela rede orientar o usuário quanto ao uso de senhas fracas, deixando claro os riscos aos quais o mesmo estará exposto.

6.1 Instalação

Devido a forma como foi produzido, este software não precisa ser instalado, bastando apenas para isso utilizar seu executável para que o mesmo funcione.

A ferramenta foi utilizada tanto em ambiente Windows, como em linux, e nenhum problema foi encontrado para que a mesma funcionasse no seu perfeito estado.

6.2 Configuração

Esta ferramenta já vem configurada para funcionar de uma maneira padrão e eficaz, porém, caso seja e interesse do usuário, arquivos de saídas, tempo para gravação de logs, alerta para senha descoberta, *wordlist* (lista de palavras) padrão, entre outros parâmetros podem ser configurados no arquivo John.ini.

O arquivo padrão para as senhas gravadas é o John.pot, e nele estão contidas todas as senhas quebradas por ele.

Para maiores informações sobre essa ferramenta e suas inúmeras funcionalidades e modos de operação, consultar site oficial da ferramenta: <http://www.openwall.com/john/>, ou mesmo a documentação completa que vem junto com o software.

6.3. Testes com a ferramenta

Os testes realizados com o John de ripper, foram feitos obtendo arquivos de senhas de sistemas linux, e nestes testes, a maioria das senhas, algo em torno de 90%, foram quebradas.

Para um melhor desempenho da ferramenta, vale lembrar que é bom sempre estar incrementando a lista de palavras (*wordlist*), pois dessa maneira a quebra torna-se muito mais ágil e quem sabe eficaz.

6.4.Avaliação

Esta ferramenta mostrou-se muito eficaz, pois quebrou inúmeras senhas, mesmo tendo poucas palavras no dicionário chamado de *wordlist*, indicando que seu algoritmo de geração de senhas é eficaz.

Um ponto negativo associado a esta ferramenta, é que quando em execução, a mesma consome muito processamento, e em um dos testes realizados, chegou a travar o computador, derrubando outros aplicativos abertos no momento em que o software atuava.

7. HONEYD

Este software encaixa-se na categoria de honeypots, que são simuladores de ambientes virtuais para encurralar um atacante. Conforme CERT (centro de estudos,respostas e tratamento de incidentes de Segurança no Brasil), “honeypot é recurso de segurança preparado especificamente para ser sondado, atacado ou comprometido e para registrar essas atividades."

Aliado ao conceito de honeypot tem-se o conceito de honeynet, que segundo CERT é definida como “uma rede projetada especificamente para ser comprometida e utilizada para observar os invasores. Essa rede normalmente é composta por sistemas reais e necessita de mecanismos de contenção eficientes e transparentes, para que não seja usada como origem de ataques e também não alertar o invasor do fato de estar em uma honeynet.”

Existem dois tipos de honeypots, que são os honeypots de baixa interação e os honeypots de alta interação, sendo que essa divisão ocorre porque o primeiro emula serviços e sistemas operacionais não permitindo que o atacante interaja com o sistema, e o segundo possui serviços e sistemas operacionais reais, e permitem que o atacante interaja com o sistema.

Segundo informações obtidas do ISTF (infosecuruty task force: <http://www.istf.com.br>), honeypots “são proibidos por lei em diversos países, pois induzem as pessoas a cometerem invasões”, porém no Brasil não existe nenhuma restrição até o momento, inclusive, de acordo com o CERT, a internet brasileira possui uma honeynet, contendo honeypots de alta interação, porém com algumas modificações que permitem a captura de todos os dados, inclusive os criptografados.

Este projeto é criado e mantido em parceria com especialista do INPE (Instituto Nacional e Pesqusias Espaciais) e o grupo brasileiro de resposta a incidentes de segurança.

Muitas universidades fazem parte desse projeto no Brasil, inclusive a UFSC, no departamento DAS (departamento de automação e sistemas).

No presente trabalho, devido à falta de experiência do acadêmico, foi melhor utilizar um honeypot de baixa interação para não colocar um computador em perigo, e a ferramenta utilizada foi o honeyd.

Com este software é possível emular diversos sistemas operacionais, os quais podemos citar a família Windows, Linux, Sistemas de roteadores (Cisco).

7.1. Instalação

A instalação desta ferramenta foi em uma distribuição Linux, chamada Fedora Core 4.0, porém de acordo com o que foi visto, não é muito fácil a instalação da mesma, pois quatro bibliotecas devem ser instaladas para que este software trabalhe corretamente, que são o libpcap, o libevent, libdnet e arpd.

Além de não estarem todas em um único pacote, cada biblioteca é encontrada em um site diferente.

Muitos problemas ocorreram na instalação, pois o código fonte do software adicional arpd estava com problemas na sintaxe de um arquivo chamado arpd.c, porém com o apoio do fórum responsável por manter a ferramenta, alguns ajustes foram feitos e foi possível a instalação das bibliotecas e da ferramenta.

7.2. Configuração

A configuração dessa ferramenta, consiste em descrever qual sistema operacional será simulado, e quais portas e/ou serviços estarão disponíveis.

Para isso, o arquivo honeyd.conf deve ser editado para que ele possa simular o sistema operacional desejado pelo usuário, assim como os serviços e portas disponíveis para um eventual ataque.

7.3. Testes

Os testes realizados foram feitos na distribuição Linux Fedora Core 4.0. Nele foram simulados ambientes windows e linux para os testes, porém só foram feitos testes do próprio computador, pois não havia infra-estrutura necessária para a simulação da intrusão.

Pelos testes feitos, foi possível verificar que a máquina emula bem um sistema operacional, podendo ser confundida com uma máquina real por atacantes novatos (como é o caso do acadêmico).

7.4 Avaliação

Esta ferramenta apresenta como ponto positivo apenas apenas a sua capacidade de simular serviços, ou seja, não são sistemas reais rodando, o que provê uma certa segurança pois nenhum serviço real será afetado, com isso, limita as ações dos atacantes, e além disso pode simular diversos hosts ao mesmo tempo.

Como pontos negativos tem-se um consumo elevado do processamento devido a criação de processos para emulação dos diversos serviço. Além disso, esse tipo de honeypot não chama a atenção de atacantes avançados, ou seja, possivelmente apenas atacantes com pouca experiência o utilizarão, não contribuindo muito para defesas futuras no sistema.

8. HYDRA

Esta ferramenta encaixa-se no conceito de ataques de força bruta, onde inúmeras conexões com parâmetros diferentes são utilizadas para a tentativa de acesso a recursos com acesso controlado.

Hydra foi desenvolvida por Van Hauser, e hoje é uma das ferramentas mais bem conceituadas nessa categoria devido à quantidade de ataques que a mesma permite. Como exemplo, podemos citar ataques de força bruta a serviços como telnet, ftp, ssh2, snmp, vnc, pop3, smtp, imap, dentre outros.

8.1 Instalação

Esta ferramenta foi instalada no Fedora Core 4, e os problemas encontrados, foram as dependências de outras bibliotecas. Mesmo conhecendo-se as bibliotecas, o processo de instalação é difícil para usuários leigos.

Mesmo com todas as dificuldades encontradas, foi possível a instalação desse software no ambiente linux, para a realização de testes.

Conforme documentação que acompanha a ferramenta, é possível utilizar o hydra em ambiente Windows através de um programa auxiliar chamado Cgywin, um software que emula um ambiente linux em um sistema operacional Windows, porém, não foi possível a instalação devido à não geração dos arquivos necessários para todo o processo de compilação.

8.2 Configuração

Devido a grande quantidade de ataques possíveis de serem realizados com esta ferramenta, as configurações dos ataques resumem-se a parâmetros da linha de comando.

Porém, é bom lembrar que para que todos os tipos de ataques funcionem, são necessárias as respectivas bibliotecas, como por exemplo, para ataques a servidores de ssh, temos que ter a bilbioteca libssl assim como os módulos do ssh instalados.

8.3 Testes

Esta ferramenta é muito versátil, possibilitando inúmeras formas de configurações de ataques. Seu potencial aumenta de acordo com o número de palavras contidas em seu dicionário, tanto de possíveis nomes de usuários, como para possíveis senhas.

É bom lembrar,que este tipo de ataque de força bruta, já é bem antigo, o que pode levar as tentativas ao fracasso devido à proteção aplicada nos servidores.

Mesmo assim, ataques deste gênero funcionam em grande parte dos servidores e os testes realizados em laboratório foram feitos através de contas já conhecidas a servidores como uol, bol, entre outros, porém, a ferramenta permite que lista de usuários e lista de senhas sejam utilizadas nos ataques, visando uma maior eficácia.

8.4 Avaliação da ferramenta

Ferramenta eficaz em seus ataques, porém a eficácia depende muito dos parâmetros utilizados. Neste caso enquadram-se a lista de senhas e a lista de usuários (caso não se conheça nenhum usuário em potencial), pois a ferramenta fica tentando as conexões com as palavras contidas nestas listas.

Esta ferramenta mostrou-se de fácil utilização, mesmo em linha de comando, porém, devido ao fato de o dicionário de senhas utilizado nos testes conter poucas palavras, a maioria dos ataques não retornou sucesso.

Embora a ferramenta possua ataques a servidores de diretório como o LDAP, smb e roteadores, não foi possível utilizar esta facilidade, devido a característica da rede testada, porém os testes mais utilizados foram aos servidores pop3, devido a grande quantidade desse tipo de servidores na rede.

CONCLUSÃO

De acordo com o exposto, pode-se verificar que existem vários tipos de ataques e técnicas que podem tornar as informações trafegando na rede de fácil acesso a pessoas mal intencionadas.

Após o desenvolvimento do presente trabalho, foi possível analisar o potencial de algumas das ferramentas mais conhecidas no mercado no que se refere a segurança de redes.

Dessa forma, foi verificado como analisar o que trafega pela placa de rede de um computador através da ferramenta Ethereal, assim como entender a estrutura dos pacotes que circulam na rede. Além disso, pode-se verificar que esta ferramenta pode capturar tráfego destino a outros computadores da rede quando esta não for interligada por switch (no caso de redes Ethernet), caso contrário, seu potencial restringe-se apenas ao tráfego do computador local.

Outra ferramenta que chamou a atenção foi a Ettercap, cuja qual consegue capturar tráfego em redes interligadas por *switchs*, pois esta ferramenta atua na camada 2 do modelo OSI, onde poucos administradores de redes têm o hábito de monitorar, porém mesmo dessa forma, o modo como ela mapeia a rede não é muito oculto, pois envia requisições arp para toda a faixa de IP's de sua sub-rede. . Este software mostrou-se muito eficaz, pois foram efetivados ataques de *dns spoof*, *dhcp spoof* e redirecionamento *ICMP*, permitindo dessa forma acesso a informações alheias.

No ramo da segurança dos hosts na rede, pode-se constatar através da ferramenta Nessus, que é importante tomar certos cuidados ao disponibilizar serviços na rede, pois varreduras de portas podem identificar o serviço e as possíveis vulnerabilidades que podem deixar o sistema indisponível. Essa ferramenta é muito útil

para essa identificação, e seu modo de utilização é bem simples. O que chama a atenção nessa ferramenta é o resultado das varreduras, onde é explicado que tipo de risco o computador possui e como se defender. Sua potencialidade diminui ao se deparar com *firewalls* ou *anti port scanners*, pois alguns parâmetros não podem ser modificados para uma varredura mais oculta.

No entanto, para um administrador de rede não pode faltar a ferramenta John the Ripper, pois é com ela que ele poderá analisar o potencial das senhas da rede, e verificar se a política de senhas que a empresa adota é uma boa política, pois este software consegue quebrar vários formatos de arquivos de senhas. Sua eficácia depende muito do dicionário de senhas utilizado como base para quebrar as senhas, mas a ferramenta não fica restrita a esse dicionário, pois ela mesma cria senhas de acordo com o nome do usuário. Um cuidado especial com esta ferramenta refere-se ao fato dela consumir muito processamento, podendo dessa forma derrubar serviços com computador que a utiliza.

Na mesma linha de raciocínio, tem-se a ferramenta Hydra, muito popular para ataques de força bruta, porém sua eficácia restringe-se a listas de senhas e nomes de usuários enormes, pois seu modo de operação é com base nelas. Devido a grande difusão de ataques desse gênero, muitos administradores se previnem desse tipo de ataques com monitoramento de controle de acessos com intuito de inibi-los, fazendo com que este tipo de ataque não funcione.

Finalmente, com o objetivo de colher o maior número possível de informações sobre ataques, foi apresentado o Honeyd, um *honeypot* capaz de simular sistemas operacionais e serviços única e exclusivamente para que sejam atacados, com o objetivo de coleta de logs e rastros deixados pelos invasores. É um software muito interessante pois consegue simular inúmeros sistemas operacionais, porém devido ao

fato de criar hosts virtuais, o processamento é muito pesado, podendo comprometer o rendimento do sistema como um todo.

Foi verificado nos testes que cada detalhe da gerência da rede pode ser crucial para se ter ou não segurança.

O presente trabalho poderia se estender mais no que diz respeito aos testes com as ferramentas, mas fatores como espaço físico e infra-estrutura tecnológica não contribuíram para a criação de um ambiente operacional.

Espera-se que este trabalho possa servir de base para administradores de redes tornarem-nas mais seguras, de maneira a evitar que pessoas mau intencionadas façam mau uso das informações entre outros malefícios que podem ser causados.

SUGESTÕES PARA FUTURAS PESQUISAS

Como sugestão para trabalhos futuros, poderia ser montada uma equipe para criar um laboratório para testar estas ferramentas, criando um ambiente operacional, de maneira a colocá-las em prática no mais alto nível.

Poderia ter por exemplo, um servidor web capaz de atender o tráfego encaminhado através de ataques de redirecionamento *ICMP* ou mesmo de *DNS spoofing*, de maneira a comprovar a eficácia dos ataques da ferramenta Ettercap.

Já para a ferramenta John the Ripper, pode-se criar listas de senhas na ordem de mega bytes para ampliar o seu poder de atuação, assim como aumentar o dicionário de usuários e senhas para a ferramenta Hydra.

Em paralelo a isso, desenvolver técnicas de maneira a inibir a atuação destes ataques, para garantir efetivamente um ambiente de comunicação seguro.

REFERÊNCIAS BIBLIOGRÁFICAS

BASE 64. Disponível em: <http://www.base64.com.br/article.php?recid=60>. Acesso em 15 de Janeiro de 2007.

Cunha, Leonardo Godinho da. **Segurança em Códigos Móveis. Monografia**. 2005.

CYGWIN. Disponível em: <http://www.cygwin.com/mirrors.html>. Acesso em 20 de fevereiro de 2007.

DUARTE, Ricardo. Análises e exploração de vulnerabilidade. Disponível em: <http://Web.fe.up.pt/~jaime/0506/SSR/tp1/duarte.pdf>. Acesso em 20 de dezembro de 2006.

ETHEREAL. The world's most popular network protocol analyzer. Disponível em: <http://www.Ethereal.com/>. Acesso em 20 de outubro de 2006.

ETTERCAP. Disponível em: <http://ettercap.sourceforge.net/>. Acesso em 05 de Janeiro de 2007.

HONEYNET.BR. Disponível em: <www.honeynet.org.br/>. Acesso em 12 de fevereiro de 2007

INSECURE.ORG. Disponível em: http://insecure.org/nmap/ - Acesso em 06 de Janeiro de 2007.

LINUX NA REDE: Disponível em: <http://www.linuxnarede.com.br/tutoriais/post_art/fullnews.php?id=view&f_act=fullnews&f_id=16>. Acesso em 06 de janeiro de 2007.

LUIS, João Carlos Mendes. Disponível em: <http://www.jonny.eng.br/trabip/arp.html>. Acesso em 04 de janeiro de 2007.

MELO, Sandro. **Exploração de Vulnerabilidades em Redes TCP/IP**. Rio de Janeiro: Editora Alta Books, 2004.

NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR. DISPONÍVEL EM: <http://www.cert.br/docs/reportagens/2003/2003-06-24.html>. Acesso em 20 de fevereiro de 2007.

OPENWALL PROJECT: Disponível em: <http://www.openwall.com/john/>. Acesso em 25 de Janeiro de 2006.

ORNAGHI, Alberto; VALLERI, Marco. Man in the middle attacks demos. Disponível em: <http://ettercap.sf.net/devel/bh-us-03-ornaghi-valleri.pdf>. acesso em 23 de dezembro de 2006.

PALADION. Disponível em: <www.paladion.net>. Acesso em 13 de fevereiro de 2007.

TANEMBAUM, Andrew S. **Sistemas Operacionais Modernos**. 2ª edição. São Paulo: Prentice Hall 2003.

TRABALHO 7: SSL/TLS. Disponível em: <http://www.fe.up.pt/~jvv/Assuntos/Apresentacoes/TLS.ppt>. Acesso em: 20 de dezembro de 2006.

UNIVERSIDADE DE BRASILIA. Departamento de Ciência da Computação. Disponível em: <http://www.cic.unb.br/docentes/jhcf/MyBooks/ciber/doc-ppt-html/CodigoMovel.html>. Acesso em setembro de 2006.

VIVA O LINUX. Disponível em: <http://www.vivaolinux.com.br/artigos/verArtigo.php?codigo=2481#>. acesso em 20 de Janeiro de 2007.

WIKIPÉDIA. A enciclopédia livre. Disponível em: http://pt.wikipedia.org/wiki/Applet_Java - Acesso em 10 de setembro de 2006.

Ornaghi, Alberto; Valleri, Marco. Ettercap MG-0.7.3. Ettercap.pdf. Ano 2000.

ANEXOS

ANÁLISE DE FERRAMENTAS PARA SEGURANÇA DE REDES

Ancelmo Boteon
ancelmo@inf.ufsc.br

Abstract

Much is said in security of the information, and in this direction the present work has for objective the net security, as part of the context to protect the information. Security of net makes use of many tools that an administrator can use. Many times these tools are used in the direction of the aggressor, however, in this work are selected the some most important ones, so that a positive administrator can have a source of evaluation how much to the use, performance, points and negative points of the studied tools. The following tools had been boarded: Ethereal - capture of traffic in nets, for analysis of the packages that passed through in nets Ethernet using Hubs; Ettercap - analysis of packages in nets using switchs, and very powerful tool for attacks of man-in-the-middle; Nessus - analysis of vulnerabilities, resulting in an analysis and possible solutions for the joined imperfections of security; John the Ripper - for auditorship of passwords, serving to analyze the power of the passwords of the users of the net; honeyd, simulator of hosts in the net so that the same it is attacked for analysis of the behavior of the aggressors; hydra, a tool of attack of rude force. The work shows the requirements of installation, configurations, result of the carried through tests and also an analysis of the tools.

Index Terms – security , network, tool for analysis of security on the network.

1. Introdução

O Hoje em dia com o uso difundido das redes de computadores, nos deparamos com um problema grave que é a segurança das informações que trafegam na rede.

Muitos nem importam com ela, porém se pararmos para pensar, muita informação importante trafega na rede, como senhas de banco, aplicações financeiras, número do cartão de crédito

Nesse sentido, o presente artigo tem o objetivo de analisar algumas ferramentas que serão utilizadas para análise da segurança nas redes de computadores.

Serão estudadas as ferramentas Ettercap, Ethereal, Nessus, John the Ripper, honeyd e Hydra., e serão esplanadas de acordo com seu histórico e análise dos testes.

2. Formas de ataques

Podemos dividir os ataques em internos e externos, onde o primeiro para acontecer necessita que o atacante tenha esteja logado no sistema, e o segundo, conforme Tanembaum (2003) é “algum código sendo transmitido pela rede para uma máquina alvo e lá executando causando algum dano”.

Como exemplo de ataques internos, podemos citar cavalo de tróia, conexão impostora, bombas lógicas, e transbordo de buffer. Já os ataques externos podem ser exemplificados com vírus, vermes, código móvel e applet Java.

3. Técnicas de ataques

Para um melhor entendimento do que algumas ferramentas utilizam, seguem descrições de alguns ataques utilizados por elas.

3.1 Arp poisoning

Técnica utiliza para ataques de desvio de sessão (também conhecido como ataque de homem do meio) ou mesmo ataque de negação de serviço. Seu funcionamento em um ataque que desvia a sessão, ocorre quando temos estações querendo se comunicar. Cada estação possui sua tabela arp contendo o endereço IP e o seu respectivo endereço MAC.

Para uma estação B se colocar no meio da comunicação entre uma máquina A e uma máquina C, ela deve enviar pacotes arp adulterados para A e C dizendo que endereço IP de C e o endereço IP de A estão associados ao seu endereço MAC.

Depois que a estação B fez o ataque, se a estação A quiser mandar um pacote para a estação C ou vice-versa, os pacotes passarão pela estação B que só tem que encaminhar os pacotes, e antes de encaminhá-los pode ver o conteúdo ou até mesmo modificá-lo.

Com esta estrutura montada, é possível verificar a troca de informações entre os computadores. Além disso, com o auxílio da ferramenta *ettercap*, é possível realizar diversos ataques sob estes dois computadores.

Nesse sentido, pode ser feito um desvio http ou https para um servidor forjado, ataque este conhecido como DNS spoofing, onde o ettercap coloca-se entre o cliente e qualquer outra estação de forma a capturar as suas informações.

Ao ser feita uma requisição ao servidor DNS (DNS request) para saber o IP de um determinado site, o ettercap detecta essa resposta e altera o endereço IP da resposta para o endereço IP desejado (o de outro servidor criado para capturar dados).

Assim que o cliente recebe o DNS reply (resposta com o IP do servidor forjado), faz o pedido de página web ao servidor, e o ataque do *homem-do-meio* pode continuar ou não. O *homem-do-meio* pode continuar ou não, se sim, no caso de usar https, o certificado que o cliente vai receber, serão do *homem-do-meio*, se não, recebe o certificado do servidor forjado.

Para direcionar a vítima para o endereço IP desejado, deve ser editado o arquivo etter.dns, localizado no diretório de instalação do Ettercap.

3.2 Redirecionamento ICMP

Técnica utilizada por roteadores para comunicar que existe um outro roteador em melhores condições para enviar um pacote de uma máquina para um destino.

Sua utilização é notada quando um roteador recebe um pacote, e este pode retornar ao emissor uma mensagem de redirecionamento (*ICMP redirect)*, caso o roteador conheça um outro roteador que possa fazer a entrega com menor custo. Há que se dizer, que isso pode acontecer apenas quando o transmissor, o receptor e o roteador estão na mesma rede local.

Pelo fato dos pacotes ICMP ficarem encapsulados dentro de um datagrama IP, os primeiros 3 campos são iguais para todos os tipos de mensagens ICMP, resultando num total de 4 bytes. A estrutura de um pacote ICMP é mostrada no capítulo 3, seção 3.3.

De posse dessa informação, um atacante pode desviar todas as seções para a máquina que desejar, e para fazer isso, é necessário criar uma mensagem de redirecionamento ICMP composta pelo cabeçalho IP de 64 bits do *payload* do pacote escutado (pacote capturado) e o endereço IP para o qual se quer desviar o tráfego.

Após isso, é necessário ficar monitorando a chegada dos pacotes de redirecionamento IP e fazer o que o atacante achar melhor sobre os dados.

Para esclarecer o redirecionamento ICMP, segue anatomia deste tipo de ataque:

- Uma máquina A envia um pacote para uma máquina B cujo endereço Ip está fora da sua sub-rede, e por este motivo, é enviado através de um roteador R1;
- O roteador R1 possui uma rota para B através de um roteador R2;
- Se o endereço de R2 pertence a mesma sub-rede de A, o roteador R1 envia uma mensagem de redirecionamento ICMP informando a máquina A que R2 é a melhor rota para se chegar a B.
- O roteador R1 envia depois os pacotes para R2, para que este os entregue a B.

Recebendo a mensagem de R1 (redirecionamento ICMP), a máquina A atualiza a sua tabela de roteamento com a informação recebida na mensagem, de maneira a deixar armazenada que R2 é a rota para se chegar a B, evitando o caminha A envia para R1, R1 envia para R2 e R2 envia para B.

3.3 port Stealing

Em redes interligadas por switches, a troca de informações entre os computadores é feita pela análise do endereço MAC pelo switch, e como no switch existe uma tabela interna onde nela consta o registro de todos os endereços MAC com suas respectivas portas, cada pacote é direcionado especificamente para o computador de destino, o que não ocorre nos hubs.

Uma maneira de conseguir capturar tráfego alheio, enganando o switch, chama-se *port stealing*, que é realizado da seguinte forma:

- O atacante envia muitos pacotes para camada 2 com o endereço de origem igual ao do host da vítima e destino igual ao endereço MAC do atacante.
- Em algum momento, o atacante rouba a porta da vítima, pois o switch atualizará sua tabela interna com as informações. A partir da atualização da tabela interna do switch, todos os pacotes destinados a vítima, serão direcionados para o atacante;
- Quando o atacante receber um pacote que estava destinado a uma de suas vítimas, ele gera uma requisição arp (arp request) para o IP da vítima;
- Quando o atacante receber a resposta arp (arp reply) da vítima, a porta no switch é "devolvida" para a vítima da mesma maneira que estava antes do ataque começar;
- O atacante pode agora encaminhar o pacote para vítima e reiniciar o ataque port stealing, porém, antes de ele encaminhá-lo, ele pode ver o conteúdo e modificá-lo se for o caso.

Este tipo de ataque se encaixa no perfil *ataque de homem do meio.*

3.4 DoS

Ataque caracterizado por tirar de atividade um serviço ou um servidor por completo.

A idéia geral é consumir todos os recursos da máquina, de maneira a fazer com que o computador atacado não consiga atender a mais nenhuma solicitação, caracterizando nesse caso a negação de serviço.

Como exemplos desse tipo de ataque podemos encontrar o *estouro de partição*, onde é necessário estar logado no sistema, e desta forma uma determinada partição é lotada com dados inúteis. Outro tipo de ataque DoS, é o de enviar para a rede um número de pacotes superior ao limite que o destino é capaz de absorver.

Além destes temos vários outros, e podemos encontra-los em (MELO, 2004).

3.5 DHCP spoof e DNS spoof

Esta técnica pode ser usada para causar indisponibilidade ao host, pois são passados para os computadores que solicitarem os endereços de IP e servidores DNS, e nesse caso, pode-se passar endereços inalcançáveis ou mesmo inexistentes.

Além desse objetivo, também pode-se desviar sessões para obter senhas e outras informações (um ataque conhecido como de DNS *spoof*), pois ao realizar-se um ataque desse tipo pode-se redirecionar os domínios para onde quiser, bastando para isso montar a estrutura de servidores e páginas.

4. Ferramenta Ettercap

Esta ferramenta faz parte de um projeto em constante atualização, e traz como destaque recursos para execução de DoS, *Scanners* (varredura na rede em busca de portas abertas), *FingerPrint* (técnica de descoberta do sistema operacional da vítima através da análise da pilha tcp/ip, onde os dados são analisados e comparados com uma base de dados previamente construída para a identificação do sistema operacional), *Spoofing* (técnica para se fazer passar por outro computador na rede), ataques MITM (*Man in the Middle* – ataque de homem do meio) customizados.

O modo como opera não é muito "oculto", pois envia um ARP REQUEST para toda a faixa de IP da LAN, considerando o IP corrente e a respectiva máscara da rede, como pode-se ver na figura abaixo, e uma vez que receba os ARP REPLIES, cria uma lista dos hosts que estão na rede, mapeando-a.

Por ser uma poderosa ferramenta, possui inúmeros parâmetros de configuração, os quais podem ser encontrados pela internet, ou mesmo na obra *Exploração de Vulnerabilidades em Redes TCP/IP* (MELO, 2004). Com esta ferramenta é possível serem utilizados os ataques de ARP poisoning, ICMP redirect, DHCP spoofing, port Stealing e dns spoofing.

4.1 Avaliação da ferramenta

Esta ferramenta mostrou-se muito eficaz no ambiente testado, onde foi possível realizar ataques do tipo *dns spoof*, redirecionamento *ICMP* e o *DHCP spoof*, sendo que este último foi facilitado, pois todos os computadores (exceto servidores) obtêm endereço *IP* via dhcp, porém possui muitos outros ataques interessantes, como por exemplo, o de poder realizar um ataque homem-do-meio em uma conexão segura (https) ou não segura.

Este *sniffer* se distingue de outros pelo fato de não ser obrigatoriamente passivo, como é o caso do Ethereal, pois o ettecap pode atuar de modo ativo inserindo dados entre as conexões existentes na rede ou mesmo matando uma conexão. Aliado a isso, é possível utilizá-lo em ambientes onde a rede é interligada por *switches*, o que não ocorre na maioria dos *sniffers*, tornando-o mais vantajoso que o Ethereal, por exemplo.

Por outro lado, o ponto negativo encontrado nessa ferramenta, refere-se ao fato de como ela mapea a rede, porque esse processo não é oculto, pois são enviados pacotes com requisições *ARP* para toda a faixa de *IP*'s da rede de acordo a faixa e máscara IP do computador do atacante.

5. Ethereal

É uma ferramenta *open source* e atualmente está disponível para diversas plataformas Uunix, Linux e Windows, enquadrando-se na categoria de sniffers, sendo portanto um analisador de pacotes da rede, ou seja, ele pode capturar o tráfego de pacotes que chegam até a interface de rede do computador, mesmo que os pacotes não sejam para a estação em análise (modo promíscuo), tentando mostrar o maior número de detalhes possíveis.

Para que tenha condições de capturar informações destinadas a outros computadores, é necessário que a rede seja interligada por hubs[3], no caso da tecnologia ethernet, pois caso esteja interligada por switch[2i] este *sniffer* não conseguirá capturar o tráfego destinado a outros computadores, pois o *switch*[2] já direcionada os dados para a porta onde o computador de destino esta

[3] Hub: equipamento de interconexão de computadores que recebe dados em uma porta específica de um computador e o entrega em todas as portas.

[2] Switch: interconecta computadores como o hub, porém a diferença é que o switch ao receber os dados de um computador de origem, o entrega diretamente na porta onde se encontra o computador destino.

ligado, evitando dessa maneira que a informação se propague para todos os computadores da rede, ficando dessa forma, a ferramenta monitorando apenas o tráfego destino ao computador com o Ethereal instalado.

Nos testes realizados, foi possível analisar o cabeçalho IP para a demonstração de como é um pacote de redirecionamento ICMP, atuando em conjunto com a ferramenta ettercap que enviou os pacotes com a instrução de redirecionamento.

Devido a rede possuir a interconexão com os switches, não foi possível capturar informações particulares nos pacotes enviados.

Nos testes realizados, foram aplicados filtros para determinados hosts (ip), e pacotes (TCP,UDP, ARP, ICMP..), para que a análise ficasse mais clara, porém para efeito de análise, será mostrado apenas a tela onde o filtro aplicado foi do protocolo arp, muito utilizado em redes, pois o mesmo faz a associação entre o endereço IP e o endereço MAC.

5.1 Avaliação da ferramenta

De acordo com o exposto, podemos verificar que esta ferramenta possui inúmeras funcionalidades.

Como pontos fortes dessa ferramenta, podemos encontrar a quantidade de formatos dos arquivos de saída gerados, onde podemos salvar uma varredura em um formato que seja legível por outros programas como o tcpdump, Novel LANalyzer, sun snoop, entre outros, porém o Ethereal também consegue ler arquivos de logs capturados por estas ferramentas como sun snoop, tcpdump, Novel LANalyzer, microsoft network monitor, H-UX´s nettl entre outras.

Além disso, mostra a estrutura completa dos pacotes que trafegam na rede, é muito fácil de utilizar, possui uma interface amigável diferenciando os tipos de pacotes pela cor em que os apresenta, e funciona capturando tráfego de muitas tecnologias, como por exemplo ethernet, token ring, 802.11, ATM.

Como pontos negativos, pode ser citado o fato de não funcionar em redes ethernet interligadas com *switchs*.

6. Nessus

O Nessus é uma ferramenta de auditoria muito usada para detectar e indicar uma maneira de solucionar as possíveis vulnerabilidades encontradas nos computadores.

Essa ferramenta era open-source até a versão 2.2.8, e passou a ser código fechado, porém continua sendo uma ferramenta de uso gratuito e é distribuída através do site: <http://www.Nessus.org>. Sua versão atual é a 3.0.

Seus recursos são muito avançados, e uma grande vantagem que possui em relação a outras ferramentas desse gênero, é que o Nessus varre todas as portas TCP´s detectando servidores ativos e simula invasões para detectar vulnerabilidades.

Para executar as varreduras de portas, o Nessus utiliza o Nmap, um portScan muito poderoso.

Esta ferramenta possui uma facilidade que se refere ao usuário não precisa ter o servidor do Nessus instalado no seu computador, ou seja, precisa apenas do cliente instalado, pois ele permite a estrutura cliente-servidor para que vários pontos da rede possam ser analisados. Nessa arquitetura, vários clientes podem controlar os servidores. Nesse sentido, a parte servidora executa os testes e a parte cliente configura e emite os relatórios.

Ao término de uma varredura, são apontadas as possíveis vulnerabilidades, e de uma maneira sucinta, é explicado de que forma o host pode ser atacado e como se proteger para corrigir essa vulnerabilidade. Além disso, nos relatórios do escaneamento são criados links para uma página específica de acordo com o plugin encontrado na vulnerabilidade, onde podemos encontrar mais detalhes sobre os riscos envolvidos, como o tipo de acesso (como exemplo: remoto), complexidade de ataque (indefinido, baixo ou alto), modo de autenticação (indefinido, requerido ou não requerido), o impacto sobre a confidencialidade (indefinido, nenhum, parcial, completo), disponibilidade (indefinido, nenhum, parcial ou completo) e a integridade (nenhum, parcial ou completo).

6.1 Análise da ferramenta

Esta ferramenta é eficiente na identificação dos serviços e sistemas rodando nos micros da rede.

Características importantes da ferramenta: a facilidade de utilização, interface amigável, relatórios bem detalhados dos serviços rodando no computador, assim como procedimentos a serem realizados no caso de alguma vulnerabilidade ser detectada,

Como pontos negativos, um problema encontrado é que não é possível trocar endereço IP da máquina do atacante, possibilitando a identificação da origem da varredura, e uma restrição encontrada na ferramenta, foi a de que não é possível estipular um tempo de alternância entre as portas do computador alvo, podendo dessa forma a ferramenta ser detectada por anti-portscanners, como o portsentry, por exemplo.

7. John the ripper

Este software é um poderoso decifrador de senhas. Inicialmente desenvolvido para sistemas Unix-like, porém atualmente ele pode ser utilizado em ambientes DOS, Windows, BSD e linux. Ele pode fazer ataques

de força-bruta nas senhas armazenadas no formato DES, MD4 e MD5, entre outros.

Ele pode atuar nos arquivos de senhas com o método de ataque de dicionário, onde são lidas as palavras de um *wordlist* (lista de palavras), e nesse modo de operação, quanto maior for a *wordlist*, mais chances de se obter sucesso na descoberta das senhas; pode operar também por combinações dos nomes e das iniciais dos usuários ou ele mesmo pode gerar suas próprias combinações, sendo que esta última consome muitos recursos da máquina, e a mesma deve ser usada com cautela, principalmente no modo diferente do *single*, pois consome muito tempo de CPU, podendo derrubar outros serviços.

Este aplicativo, pode ser de grande utilidade para um administrador de redes, pois com ele é possível analisar a complexidade das senhas que os usuários utilizam, e com base nessa análise, cabe ao responsável pela rede orientar o usuário quanto ao uso de senhas fracas, deixando claro os riscos aos quais o mesmo estará exposto

.

7.1 Avaliação

Esta ferramenta mostrou-se muito eficaz, pois quebrou inúmeras senhas, mesmo tendo poucas palavras no dicionário chamado de *wordlist*, indicando que seu algoritmo de geração de senhas é eficaz.

Um ponto negativo associado a esta ferramenta, é que quando em execução, a mesma consome muito processamento, e em um dos testes realizados, chegou a travar o computador, derrubando outros aplicativos abertos no momento em que o software atuava.

8. Honeyd

Este software encaixa-se na categoria de honeypots, que são simuladores de ambientes virtuais para encurralar um atacante. Conforme CERT (centro de estudos,respostas e tratamento de incidentes de Segurança no Brasil), “honeypot é recurso de segurança preparado especificamente para ser sondado, atacado ou comprometido e para registrar essas atividades."

Aliado ao conceito de honeypot tem-se o conceito de honeynet, que segundo CERT é definida como “uma rede projetada especificamente para ser comprometida e utilizada para observar os invasores. Essa rede normalmente é composta por sistemas reais e necessita de mecanismos de contenção eficientes e transparentes, para que não seja usada como origem de ataques e também não alertar o invasor do fato de estar em uma honeynet.”

Existem dois tipos de honeypots, que são os honeypots de baixa interação e os honeypots de alta interação, sendo que essa divisão ocorre porque o primeiro emula serviços e sistemas operacionais não permitindo que o atacante interaja com o sistema, e o segundo possui serviços e sistemas operacionais reais, e permitem que o atacante interaja com o sistema.

Segundo informações obtidas do ISTF (infosecuruty task force: <http://www.istf.com.br>), honeypots “são proibidos por lei em diversos países, pois induzem as pessoas a cometerem invasões”, porém no Brasil não existe nenhuma restrição até o momento, inclusive, de acordo com o CERT, a internet brasileira possui uma honeynet, contendo honeypots de alta interação, porém com algumas modificações que permitem a captura de todos os dados, inclusive os criptografados.

Este projeto é criado e mantido em parceria com especialista do INPE (Instituto Nacional e Pesqusias Espaciais) e o grupo brasileiro de resposta a incidentes de segurança.

Muitas universidades fazem parte desse projeto no Brasil, inclusive a UFSC, no departamento DAS (departamento de automação e sistemas).

No presente trabalho, devido à falta de experiência do acadêmico, foi melhor utilizar um honeypot de baixa interação para não colocar um computador em perigo, e a ferramenta utilizada foi o honeyd.

Com este software é possível emular diversos sistemas operacionais, os quais podemos citar a família Windows, Linux, Sistemas de roteadores (Cisco).

8.1 Avaliação do Honeyd

Esta ferramenta apresenta como ponto positivo apenas a sua capacidade de simular serviços, ou seja, não são sistemas reais rodando, o que provê uma certa segurança pois nenhum serviço real será afetado, com isso, limita as ações dos atacantes, e além disso pode simular diversos hosts ao mesmo tempo.

Como pontos negativos tem-se um consumo elevado do processamento devido a criação de processos para emulação dos diversos serviço. Além disso, esse tipo de honeypot não chama a atenção de atacantes avançados, ou seja, possivelmente apenas atacantes com pouca experiência o utilizarão, não contribuindo muito para defesas futuras no sistema.

9. Hydra

Esta ferramenta encaixa-se no conceito de ataques de força bruta, onde inúmeras conexões com parâmetros diferentes são utilizadas para a tentativa de acesso a recursos com acesso controlado.

Hydra foi desenvolvida por Van Hauser, e hoje é uma das ferramentas mais bem conceituadas nessa categoria devido à quantidade de ataques que a mesma permite. Como exemplo, podemos citar ataques de força bruta a serviços como telnet, ftp, ssh2, snmp, vnc, pop3, smtp, imap, dentre outros.

9.1 Avaliação da ferramenta

Ferramenta eficaz em seus ataques, porém a eficácia depende muito dos parâmetros utilizados. Neste caso enquadram-se a lista de senhas e a lista de usuários (caso não se conheça nenhum usuário em potencial), pois a ferramenta fica tentando as conexões com as palavras contidas nestas listas.

Esta ferramenta mostrou-se de fácil utilização, mesmo em linha de comando, porém, devido ao fato de o dicionário de senhas utilizado nos testes conter poucas palavras, a maioria dos ataques não retornou sucesso.

Embora a ferramenta possua ataques a servidores de diretório como o LDAP, smb e roteadores, não foi possível utilizar esta facilidade, devido a característica da rede testada, porém os testes mais utilizados foram aos servidores pop3, devido a grande quantidade desse tipo de servidores na rede.

10. CONCLUSÃO

De acordo com o exposto, pode-se verificar que existem vários tipos de ataques e técnicas que podem tornar as informações trafegando na rede de fácil acesso a pessoas mal intencionadas.

Após o desenvolvimento do presente trabalho, foi possível analisar o potencial de algumas das ferramentas mais conhecidas no mercado no que se refere a segurança de redes.

Dessa forma, foi verificado como analisar o que trafega pela placa de rede de um computador através da ferramenta Ethereal, assim como entender a estrutura dos pacotes que circulam na rede. Além disso, pode-se verificar que esta ferramenta pode capturar tráfego destino a outros computadores da rede quando esta não for interligada por switch (no caso de redes Ethernet), caso contrário, seu potencial restringe-se apenas ao tráfego do computador local.

Outra ferramenta que chamou a atenção foi a Ettercap, cuja qual consegue capturar tráfego em redes interligadas por *switchs*, pois esta ferramenta atua na camada 2 do modelo OSI, onde poucos administradores de redes têm o hábito de monitorar, porém mesmo dessa forma, o modo como ela mapeia a rede não é muito oculto, pois envia requisições arp para toda a faixa de IP's de sua sub-rede. . Este software mostrou-se muito eficaz, pois foram efetivados ataques de *dns spoof*, *dhcp spoof* e redirecionamento *ICMP*, permitindo dessa forma acesso a informações alheias.

No ramo da segurança dos hosts na rede, pode-se constatar através da ferramenta Nessus, que é importante tomar certos cuidados ao disponibilizar serviços na rede, pois varreduras de portas podem identificar o serviço e as possíveis vulnerabilidades que podem deixar o sistema indisponível. Essa ferramenta é muito útil para essa identificação, e seu modo de utilização é bem simples. O que chama a atenção nessa ferramenta é o resultado das varreduras, onde é explicado que tipo de risco o computador possui e como se defender. Sua potencialidade diminui ao se deparar com *firewalls* ou *anti port scanners*, pois alguns parâmetros não podem ser modificados para uma varredura mais oculta.

No entanto, para um administrador de rede não pode faltar a ferramenta John the Ripper, pois é com ela que ele poderá analisar o potencial das senhas da rede, e verificar se a política de senhas que a empresa adota é uma boa política, pois este software consegue quebrar vários formatos de arquivos de senhas. Sua eficácia depende muito do dicionário de senhas utilizado como base para quebrar as senhas, mas a ferramenta não fica restrita a esse dicionário, pois ela mesma cria senhas de acordo com o nome do usuário. Um cuidado especial com esta ferramenta refere-se ao fato dela consumir muito processamento, podendo dessa forma derrubar serviços com computador que a utiliza.

Na mesma linha de raciocínio, tem-se a ferramenta Hydra, muito popular para ataques de força bruta, porém sua eficácia restringe-se a listas de senhas e nomes de usuários enormes, pois seu modo de operação é com base nelas. Devido a grande difusão de ataques desse gênero, muitos administradores se previnem desse tipo de ataques com monitoramento de controle de acessos com intuito de inibi-los, fazendo com que este tipo de ataque não funcione.

Finalmente, com o objetivo de colher o maior número possível de informações sobre ataques, foi apresentado o Honeyd, um *honeypot* capaz de simular sistemas operacionais e serviços única e exclusivamente para que sejam atacados, com o objetivo de coleta de logs e rastros deixados pelos invasores. É um software muito interessante pois consegue simular inúmeros sistemas operacionais, porém devido ao fato de criar hosts virtuais, o processamento é muito pesado, podendo comprometer o rendimento do sistema como um todo.

Foi verificado nos testes que cada detalhe da gerência da rede pode ser crucial para se ter ou não segurança.

O presente trabalho poderia se estender mais no que diz respeito aos testes com as ferramentas, mas fatores como espaço físico e infra-estrutura tecnológica não contribuíram para a criação de um ambiente operacional.

Espera-se que este trabalho possa servir de base para administradores de redes tornarem-nas mais

seguras, de maneira a evitar que pessoas mau intencionadas façam mau uso das informações entre outros malefícios que podem ser causados.

11. Referências Bibliográficas

BASE 64. Disponível em: <http://www.base64.com.br/article.php?recid=60>. Acesso em 15 de Janeiro de 2007.

Cunha, Leonardo Godinho da. **Segurança em Códigos Móveis. Monografia**. 2005.

CYGWIN. Disponível em: <http://www.cygwin.com/mirrors.html>. Acesso em 20 de fevereiro de 2007.

DUARTE, Ricardo. Análises e exploração de vulnerabilidade. Disponível em: <http://Web.fe.up.pt/~jaime/0506/SSR/tp1/duarte.pdf >. Acesso em 20 de dezembro de 2006.

ETHEREAL. The world's most popular network protocol analyzer. Disponível em: <http://www.Ethereal.com/>. Acesso em 20 de outubro de 2006.

ETTERCAP. Disponível em: <http://ettercap.sourceforge.net/>. Acesso em 05 de Janeiro de 2007.

HONEYNET.BR. Disponível em: <www.honeynet.org.br/>. Acesso em 12 de fevereiro de 2007

INSECURE.ORG. Disponível em: http://insecure.org/nmap/ - Acesso em 06 de Janeiro de 2007.

LINUX NA REDE: Disponível em: <http://www.linuxnarede.com.br/tutoriais/post_art/fullnews.php?id=view&f_act=fullnews&f_id=16>. Acesso em 06 de janeiro de 2007.

LUIS, João Carlos Mendes. Disponível em: <http://www.jonny.eng.br/trabip/arp.html>. Acesso em 04 de janeiro de 2007.

MELO, Sandro. **Exploração de Vulnerabilidades em Redes TCP/IP**. Rio de Janeiro: Editora Alta Books, 2004.

NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR. DISPONÍVEL EM: <http://www.cert.br/docs/reportagens/2003/2003-06-24.html>. Acesso em 20 de fevereiro de 2007.

OPENWALL PROJECT: Disponível em: <http://www.openwall.com/john/>. Acesso em 25 de Janeiro de 2006.

ORNAGHI, Alberto; VALLERI, Marco. Man in the middle attacks demos. Disponível em: <http://ettercap.sf.net/devel/bh-us-03-ornaghi-valleri.pdf>. acesso em 23 de dezembro de 2006.

PALADION. Disponível em: <www.paladion.net>. Acesso em 13 de fevereiro de 2007.

TANEMBAUM, Andrew S. **Sistemas Operacionais Modernos**. 2ª edição. São Paulo: Prentice Hall 2003.

TRABALHO 7: SSL/TLS. Disponível em: <http://www.fe.up.pt/~jvv/Assuntos/Apresentacoes/TLS.ppt>. Acesso em: 20 de dezembro de 2006.

UNIVERSIDADE DE BRASILIA. Departamento de Ciência da Computação. Disponível em: <http://www.cic.unb.br/docentes/jhcf/MyBooks/ciber/doc-ppt-html/CodigoMovel.html>. Acesso em setembro de 2006.

VIVA O LINUX. Disponível em: <http://www.vivaolinux.com.br/artigos/verArtigo.php?codigo=2481#>. acesso em 20 de Janeiro de 2007.

WIKIPÉDIA. A enciclopédia livre. Disponível em: http://pt.wikipedia.org/wiki/Applet_Java - Acesso em 10 de setembro de 2006.

Ornaghi, Alberto; Valleri, Marco. Ettercap MG-0.7.3. Ettercap.pdf. Ano 2000.