Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"

OTÁVIO BRISOLLA POLATTO SILVA

ESTUDO DAS TÉCNICAS E APLICABILIDADE DA FERRAMENTA BACKTRACK 5 R3 LINUX

Assis
2014

OTÁVIO BRISOLLA POLATTO SILVA

ESTUDO DAS TÉCNICAS E APLICABILIDADE DA FERRAMENTA BACKTRACK 5 R3 LINUX

Trabalho de Conclusão do Curso de Bacharelando em Ciência da Computação apresentado ao Instituto Municipal de Ensino Superior - IMESA, e a Fundação Educacional do Município de Assis - FEMA, como requisito para o Certificado de Conclusão do Curso.

Orientando: Otávio Brisolla Polatto Silva
Orientador: Me. Douglas Sanches da Cunha

Área de Concentração: Informática

Assis
2014

FICHA CATALOGRÁFICA

SILVA, Otávio Brisolla Polatto Silva

Estudo das Técnicas e Aplicabilidade da Ferramenta Backtrack 5 R3 Linux / Otávio Brisolla Polatto Silva. Fundação Educacional do Município de Assis – FEMA – Assis, 2.014.

67 pág.

Trabalho de Conclusão do Curso de Ciências da Computação – Instituto Municipal de Ensino Superior de Assis – IMESA.

Orientador: Prof. Me. Douglas Sanches da Cunha.

1.Invasão de Sistemas 2. Testes de Vulnerabilidade.

CDD:005.8

Biblioteca da FEMA

ESTUDO DAS TÉCNICAS E APLICABILIDADE DA FERRAMENTA BACKTRACK 5 R3 LINUX

OTÁVIO BRISOLLA POLATTO SILVA

Trabalho de Conclusão do Curso de Bacharelando em Ciência da Computação apresentado ao Instituto Municipal de Ensino Superior - IMESA, e a Fundação Educacional do Município de Assis - FEMA, como requisito para o Certificado de Conclusão do Curso.

Orientador: Me. Douglas Sanches da Cunha

Analisador: Esp. Celio Desiro

Assis

2014

DEDICATÓRIA

Dedico este trabalho aos meus pais José Hélio da Silva e Maria Cristina Brisolla Polatto que sempre me estimularam a estudar e correr atrás de meus objetivos.

AGRADECIMENTOS

Agradeço aos meus familiares que me acompanharam e apoiaram durante toda a vida, ao professor Douglas Sanches da Cunha que me orientou durante todo o projeto, e aos colegas de classe que diretamente ou indiretamente contribuíram para a realização deste trabalho.

All our dreams can come true - If we have the courage to pursue them

Walt Disney

RESUMO

A Distribuição Linux Backtrack 5 R3 reúne poderosas ferramentas para testes de penetração e testes de vulnerabilidade em sistemas computacionais e em redes de computadores. Estas ferramentas podem ser utilizadas para práticas benéficas como correções de falhas e vulnerabilidades, ou para práticas maliciosas como invasão de sistemas computacionais. Este trabalho foi desenvolvido em um ambiente local composto por dois computadores e máquinas virtuais, todos interligados em rede e com acesso a Internet. As técnicas demonstradas neste trabalho tem um objetivo profissional e acadêmico, servindo apenas para conhecimento, e o uso delas para fins maliciosos consiste em crime virtual, com penas previstas no código de lei.

Palavras Chave: Backtrack; Ferramentas; Testes de Penetração; Testes de Vulnerabilidade; Sistemas Computacionais; Redes de Computadores; Invasão de Sistemas; Conhecimento; Crime Virtual.

ABSTRACT

The Backtrack 5 R3 Linux distribution concentrates powerful tools for penetration testing and vulnerability testing in computer systems and computer networks. These tools can be used for beneficial practices such as bug fixes and vulnerabilities fixes, or malicious practices such as hacking computer systems. This work was developed in a local environment composed by two computers and virtual machines, all of them network connected and Internet access. The techniques demonstrated in this work has a professional and academic purpose, serving only to knowledge, and the use of them for malicious purposes consists of virtual crime, with punishment provided in the law code.

Keywords: Backtrack; Tools; Penetration Testing; Vulnerability Testing; Computers Systems; Computer Networks; Hacking; Knowledge, Virtual Crime.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1- INTRODUÇÃO

Com o crescente uso de dispositivos eletrônicos tais como Computadores, *Notebooks*, *Tablets* e *Smartphones*, conectados a Internet, e com o aumento da inclusão digital, existe uma demanda por segurança e privacidade, uma vez que a partir da Internet é possível realizar vários tipos de operações como transações bancárias, por meio de '*Internet Banking*', troca de e-mails, participar de redes sociais, realizar compras através do comércio eletrônico etc .

Além de tudo isso ainda tem-se os crimes virtuais, praticados geralmente por *crackers*, que quebram sistemas de segurança, com o objetivo de roubo de informações para benefício próprio, roubos ou outros ataques.

Neste cenário faz-se necessário o desenvolvimento de ferramentas de segurança, com a finalidade de serem utilizadas para testes de vulnerabilidade e testes de penetração, por analistas de segurança, analista de redes, e também na computação forense.

Neste trabalho será abordado o uso da ferramenta Backtrack 5 R3, demonstrando técnicas utilizadas pelos invasores, técnicas de detecção e técnicas de proteção contra ataques.

1.1. OBJETIVOS

Este trabalho tem como principal objetivo abordar técnicas de uso de ferramentas como Nmap, Nslookup, Dnsenum, Netifera , xHydra, Medusa, Metasploit Framework, dentre várias outras contidas na ferramenta Backtrack 5 R3, a fim de realizar testes de vulnerabilidade em um sistema computacional e demonstrar formas de prevenção contra estes tipos de ataque.

1.2. RELEVÂNCIA E JUSTIFICATIVA

Com o crescente uso da Tecnologia da Informação existe uma demanda cada vez maior de profissionais da área de computação voltada para a Segurança da Informação, tais como Administradores de Rede, Analistas de Segurança e Especialistas em Segurança da Informação. Por meio da ferramenta Backtrack 5 R3 é possível efetuar auditoria em segurança e testes de vulnerabilidade.

1.3. REVISÃO DA LITERATURA

Existem inúmeros artifícios além da ferramenta Backtrack 5 R3 e todas as ferramentas contidas nela, que possuem a mesma ou uma semelhante finalidade de efetuar Teste de Vulnerabilidade e Auditorias de Segurança em sistemas computacionais. Cita-se como exemplo a distribuição Linux sucessora do Backtrack 5 R3 chamada Kali Linux e a distribuição Linux baseada em Ubuntu Linux BackBox, e as ferramentas que as compõem.

Além do uso das ferramentas citadas neste Trabalho, referências bibliográficas como Backtrack Linux – Auditoria e Revisão em Segurança, Backtrack 5 *Cookbook* e endereços eletrônicos de *sites*, são de grande utilidade para aprofundar-se o conhecimento sobre ferramentas como o Backtrack 5 R3.

1.4. METODOLOGIA

Para a realização deste trabalho foram consultados artigos de outros escritores, tais como os livros Backtrack Linux – Auditoria e Revisão em Segurança, Backtrack 5 *Cookbook*, Trabalhos de Conclusões de Cursos e endereços eletrônicos. O estudo e a aplicabilidade das ferramentas foram realizadas a partir de um computador com a distribuição Linux Backtrack 5 R3 em execução, interligado via rede com outros computadores utilizando-se múltiplos sistemas operacionais.

1.5. MOTIVAÇÃO

A principal motivação para este trabalho é estimular o leitor e o profissional da área de segurança a buscar novos conhecimentos e conceitos na área de Tecnologia da Informação, bem como o entendimento das técnicas demonstradas aqui.

1.6. ESTRUTURA DO TRABALHO

Este trabalho é dividido em sete capítulos, onde este primeiro capítulo aborda a Introdução, Objetivos, Relevância,Justificativa, Revisão da Literatura, Metodologia, e a Motivação deste trabalho. É elaborado também um breve resumo sobre os conteúdos de cada capítulo.

O segundo capítulo demonstra um breve resumo sobre a ferramenta Backtrack 5 R3, técnicas *Hacking*, apresenta e exemplifica o uso de ferramentas como Genlist, Hping3, Nmap e Zenmap, a versão gráfica do Nmap. O terceiro capítulo apresenta um conceito básico sobre Servidores *DNS* e demonstra algumas ferramentas para Detecção de *Banners DNS*, tais como Nslookup, Dnsenum, Fierce e Netifera.

O quarto capítulo introduz o conceito de Quebra de Senhas e *Wordlists*, o que são e para que servem. São demonstradas as ferramentas Crunch, John The Ripper e Ophcrack. O quinto capítulo demonstra conceitos sobre invasão de sistemas, vulnerabilidades e obtenção de acesso. Uma exemplificação é realizada através das ferramentas xHydra e Medusa.

O sexto capítulo introduz e define o conceito de Metasploits. É abordada a ferramenta Metasploit Framework demonstrando-se um processo de invasão a partir de uma vulnerabilidade existente em uma máquina. O sétimo e último capítulo demonstra a conclusão sobre todo o estudo realizado, e uma possível previsão para trabalhos futuros, com foco na área de segurança.

2 – TÉCNICAS DE ATAQUE, BACKTRACK 5 R3 E DETECÇÃO DE SISTEMAS ATIVOS

2.1. INTRODUÇÃO

Este capítulo tem como intuito apresentar a ferramenta Backtrack 5 R3 e ressaltar suas formas de utilização, além de abordar o conceito sobre *Penetration Testing* e *Hacking*, demonstrar passos de como ocorre a efetivação de um ataque e apresentar e exemplificar as ferramentas Genlist, Hping3, Nmap e Zenmap.

2.2. BACKTRACK 5 R3 LINUX

Backtrack 5 R3 é uma distribuição Linux baseada no Debian GNU/Linux que conforme GIAVAROTO et al. (2013) informa, é uma ferramenta voltada para testes de penetração muito utilizada por auditores, analistas de segurança de redes e sistemas, *hackers* éticos etc. Sua primeira versão é de 26 de maio de 2006, seguida pelas versões [2] de 6 de março de 2007 [3] de 19 de junho de 2008, [4] de 22 de Novembro de 2010 e [5] de 2011.

A utilização do Backtrack 5 R3 Linux pode ser feita através da instalação em uma máquina virtual ou computador compatível, um DVD ou até mesmo a partir de um *pen drive bootavel* com uma imagem da distribuição para ser carregada na memória ou instalada.

2.3. PENETRATION TESTING E HACKING

GIAVAROTO et al.(2013) informa que *Penetration Testing*, ou *Pentest*, é um método para testar e descobrir vulnerabilidades em uma rede ou sistemas operacionais, onde são inseridos métodos de avaliação de segurança em um sistema computacional ou rede, aplicando-se simulações de ataques, de forma a simular uma invasão a partir de um estranho mal intencionado.

Hacking consiste do processo da utilização de ferramentas e técnicas, a partir da ferramenta Backtrack 5 R3 ou qualquer outra que possua a mesma finalidade, de invadir um sistema alvo definido com o intuito de roubo de senhas, informações e até mesmo práticas maléficas como a inserção de *malwares* que prejudiquem o sistema alvo em questão, atos que caracterizam a prática de crimes virtuais.

GIAVAROTO et al. (2013) ressalta que *Pentest* é o oposto de *Hacking*, e que apesar de ambos utilizarem as mesmas ferramentas de análises e raciocínios aplicados, o objetivo do *Pentest* é puramente aplicar as melhores técnicas de segurança a fim de proteger o maior patrimônio que existe, seja na forma de reparo de *hardwares* com *bugs* presentes, aplicando-se *patches* de segurança, otimizando-se *softwares*, políticas de senhas, entre outros, logo após o reconhecimento total do alvo analisado.

2.4. COMO OCORRE A EFETIVAÇÃO DE UM ATAQUE

PRITCHETT et al. (2012) informa que um dos mais importantes passos para a efetivação de um ataque é a concentração de informações, quanto maior for o número de informações reunidas, maior será a probabilidade de sucesso na efetivação do ataque.

Enumeração é o primeiro passo na efetivação de um ataque, e conforme PRITCHETT et al. (2012) define é o processo onde são descobertas informações sobre a rede de computadores de uma determinada empresa ou alvo, bem como a detecção de sistemas de proteção e os sistemas ativos que a compõem. PRITCHETT et al. (2012) aborda ainda conceitos sobre Enumeração *DNS*, que consiste da identificação de todos os servidores *DNS* de uma determinada organização alvo.

Após este princípio o segundo passo é a concentração de informações sobre o alvo escolhido, que pode ocorrer a partir das técnicas de *Footprinting* (Reconhecimento) e *Fingerprinting* (Impressão Digital).

Reconhecimento, ou *Footprinting*, conforme GIAVAROTO et al. (2013) diz é o método

utilizado para a obtenção de informações a respeito de um determinado alvo, ou organização. GIAVAROTO et al. (2013) informa ainda que o reconhecimento advém de táticas militares em que o terreno deve ser estudado de forma estratégica antes que seja atacado, e que este reconhecimento pode ser feito a partir de técnicas como a de engenharia social, informações disponíveis a partir de serviços públicos na Internet, ou a partir de ferramentas que possuam esta finalidade.

Ainda concentrando informações sobre o alvo o próximo e terceiro passo a ser seguido é a Impressão Digital, ou *Fingerprinting*, técnica que de acordo com GIAVAROTO et al. (2013) consiste no processo de concentração de informações a respeito de versões, que pode ser realizado a partir da Detecção de *Banners* sobre o sistema operacional ativo e serviços em execução como *SSH*, *Telnet*, *Apache*, dentre outros, a respeito do alvo escolhido dentro da rede.

A identificação de portas que se encontram abertas, a presença de *firewalls* ou qualquer outro sistema de proteção ativo, em conjunto com as informações reunidas nos processos acima são de grande relevância para o sucesso de um ataque.

Uma vez que informações foram reunidas, o próximo e quarto passo para a efetivação do ataque é a obtenção de acesso ao alvo escolhido. Para isto é necessária a definição da ferramenta a ser utilizada, que pode ser escolhida de acordo com o tipo de falha ou vulnerabilidade encontrada anteriormente. Este passo é descrito nos próximos capítulos, exemplificando assim o uso das ferramentas a serem apresentadas nos próximos capítulos.

2.5. GENLIST

De acordo com GIAVAROTO et al. (2013) Genlist é uma ferramenta simples, que tem como finalidade identificar *hosts* ativos dentro de uma sequência de endereços IP's. Seus principais parâmetros são:

- **-s ou --scan**: parâmetro que define a sequência alvo a ser escaneada.
- **-h**: retorna um manual de ajuda sobre o comando genlist.

Exemplo de execução:

Figura 1 - Varredura executada pelo Genlist.

No exemplo da Figura 1 o comando genlist -s retorna todos os *hosts* ativos da sequência de ip's 192.168.1.0.

2.6. HPING3

Hping3 é uma poderosa ferramenta que possibilita detectar *hosts*, regras de *firewall* e também efetuar varredura de portas. Dispõe dos modos TCP, UDP, ICMP, *Raw* IP e *Scan* **(**GIAVAROTO et al. 2013) . De acordo com (SALVATORE, 2014), autor da ferramenta Hping, é possível utilizar a ferramenta em vários modos, por pessoas que não se importam com segurança para testar redes e *hosts*. Seu modo *default* é o TCP e seus principais parâmetros e modos são:

• **-h**: retorna uma lista de referências sobre o comando.

• **-v**: retorna a versão utilizada.

• **-V**: ativa o modo verboso.

• **-S ou –syn**: ativa o modo furtivo SYN, que retorna informações mais completas sobre a varredura, como as *flags* SA e RA que significam respectivamente disponível e indisponível.

• **--icmp**: ativa o modo icmp, que utiliza o protocolo icmp. Neste caso o comando funciona como um simples comando ping.

• **--scan**: ativa o modo *scan*, que escaneia portas, cabendo ao usuário apenas informar o parâmetro *scan* e o número da porta. Exemplo: "--*scan* 80".

No exemplo seguinte é bloqueado o protocolo ICMP, que é responsável pelo retorno de pacotes de dados através do comando ping. Uma vez que o mesmo esteja bloqueado não é possível uma comunicação a partir do comando ping. Na figura seguinte é exibida uma regra de *firewall* do *iptables* onde é feito o bloqueio do protocolo ICMP.

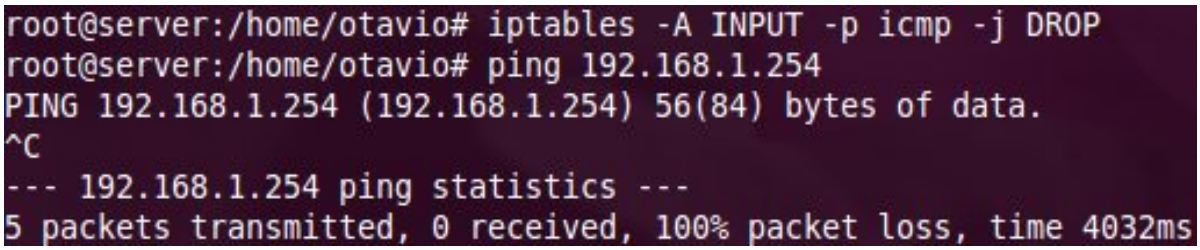

Figura 2 - Bloqueio do protocolo ICMP no computador alvo.

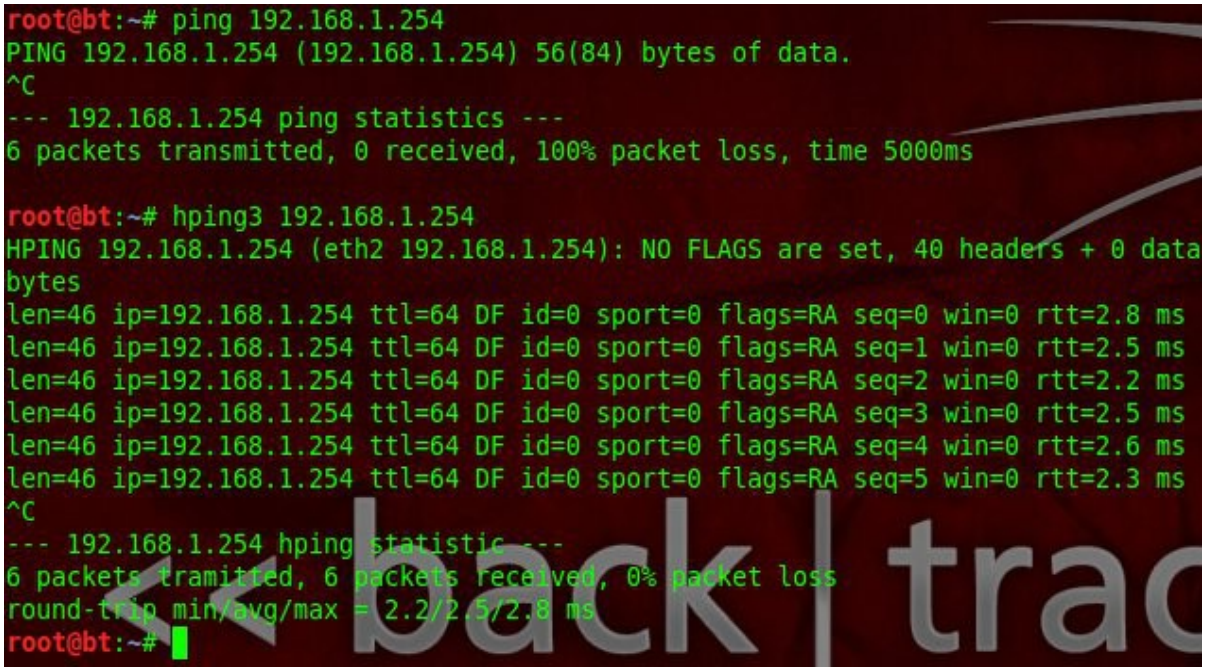

Figura 3 - Teste com o comandos ping e a ferramenta Hping3.

Na Figura 3 é possível notar uma falha tentativa de comunicação utilizando-se o comando ping para o *host* 192.168.1.254, que conforme exibido na Figura 2 se encontra com o protocolo ICMP bloqueado. Porém ao utilizar-se a ferramenta Hping3, a mesma retorna como resposta a flag RA, que significa que o *host* está indisponível.

2.7. NMAP

Criada em setembro de 1997 por Gordon Fyodor Lyon, a ferramenta NMAP, conhecida também como *Network Mapper*, é uma ferramenta para varreduras de portas, descoberta de serviços e detecção de versões. Existem versões de utilização tanto para Unix quanto para Windows, e também versões com interface gráfica como o Zenmap. Conforme (LYON, 2014) ressalta, seus principais parâmetros e modos são:

• **TCP SYN (-sS)**: parâmetro onde são examinadas portas de maneira rápida e de modo invisível, ou seja, possui uma difícil detecção por *firewalls* ou IDS.

• **TCP Connect (-sT)**: parâmetro onde é executada uma varredura utilizando-se o *Three-Way Handshake*. É facilmente detectada.

• **UPD (-sU)**: parâmetro onde é efetuada uma varredura utilizando-se o protocolo UDP.

• **TCP FIN (-sF, -sX, -sN)**: parâmetros utilizados na tentativa de travessia de *firewalls*.

• **TCP ACK (-sA)**: parâmetro utilizado como tática para detecção de regras de *firewall*.

• **-A**: parâmetro que ativa a detecção da versão do sistema operacional, detecção de versões, detecção de *scripts* e rotas de tráfego.

• **-O**: parâmetro que ativa a detecção da versão do sistema operacional.

• **-sV**: parâmetro que ativa a detecção de versão dos programas utilizados.

• **-sP**: parâmetro que habilita a verificação de hosts ativos em uma determinada sequência de ip's.

• **-p** : parâmetro onde é possível informar uma ou mais portas a serem escaneadas.

É recomendado ao leitor ler o arquivo de ajuda da ferramenta Nmap, por meio do comando “nmap -h”, a ser digitado no terminal de comandos, para um melhor entendimento dos parâmetros e do funcionamento da ferramenta. No exemplo seguinte é mostrada a utilização da ferramenta Nmap:

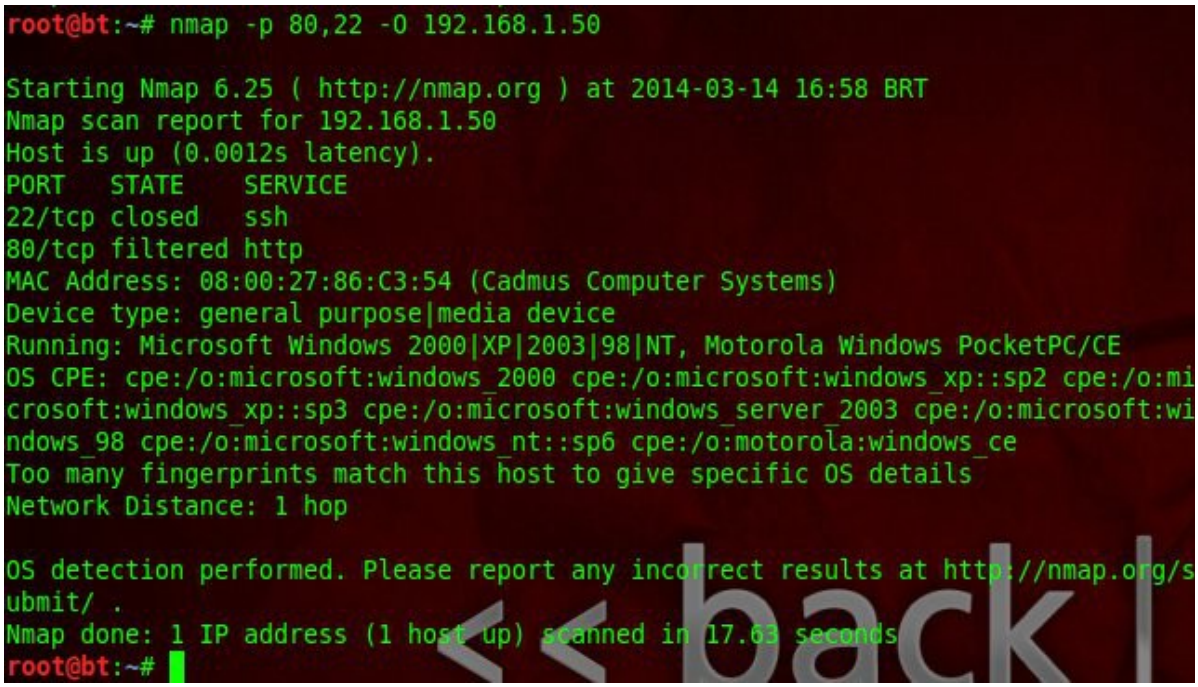

Figura 4 – Exemplo de utilização da ferramenta NMAP.

No exemplo da Figura 4 é utilizada a ferramenta nmap com os parâmetros “-p”, para as portas 80 e 22 serem verificadas, e o parâmetro “-O” para a detecção do sistema operacional utilizado no *host*. Observe que é retornada a informação de que a porta 22 se encontra fechada, que a porta 80 se encontra filtrada pelo *firewall*, e que o sistema operacional pode ser o Microsoft Windows nas versões 2000, XP, 2003, 98 ou NT.

2.8. ZENMAP

Conforme GIAVAROTO et al. (2013) informa a ferramenta Zenmap é a versão gráfica da poderosa ferramenta NMAP, onde são exibidos resultados de forma organizada, é possível a exibição de detalhes mesmo com um escaneamento e ainda é retornado um mapa topológico da rede em questão.

Na ferramenta Backtrack 5 R3 o Zenmap pode ser encontrado através do seguinte caminho: *Applications* > *BackTrack* > *Information Gathering* > *Network Analysis* >

Identify Live Hosts > zenmap. Sua interface é bem simples, e é exibida na figura seguinte:

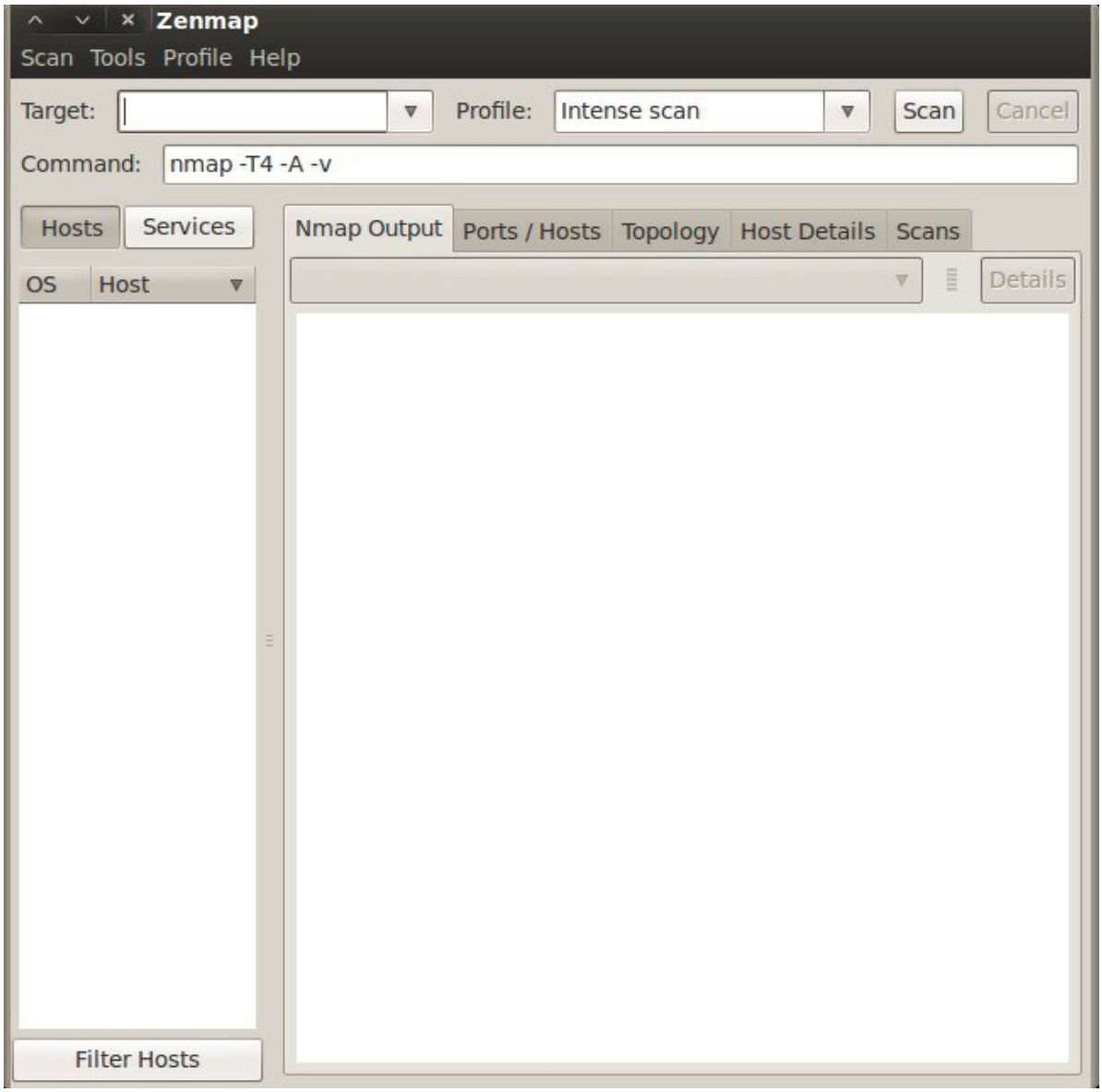

Figura 5 – Interface gráfica da ferramenta Zenmap.

O campo correspondente ao "*Target*" da interface gráfica é onde deve-se especificar o endereço IP do alvo definido, "*Profile*" é onde é possível selecionar o nível de intensidade de informações que se deseja obter com o escaneamento. Preenchidos estes campos basta apenas selecionar a opção "*Scan*" para dar início a um escaneamento.

No campo correspondente ao “*Command*” é possível especificar alguns parâmetros utilizados no Nmap que forem desejados. A reposta final do escaneamento é exibida em “*Nmap/Output”* e em suas barras laterais. Na figura seguinte é exibido um exemplo de utilização da ferramenta.

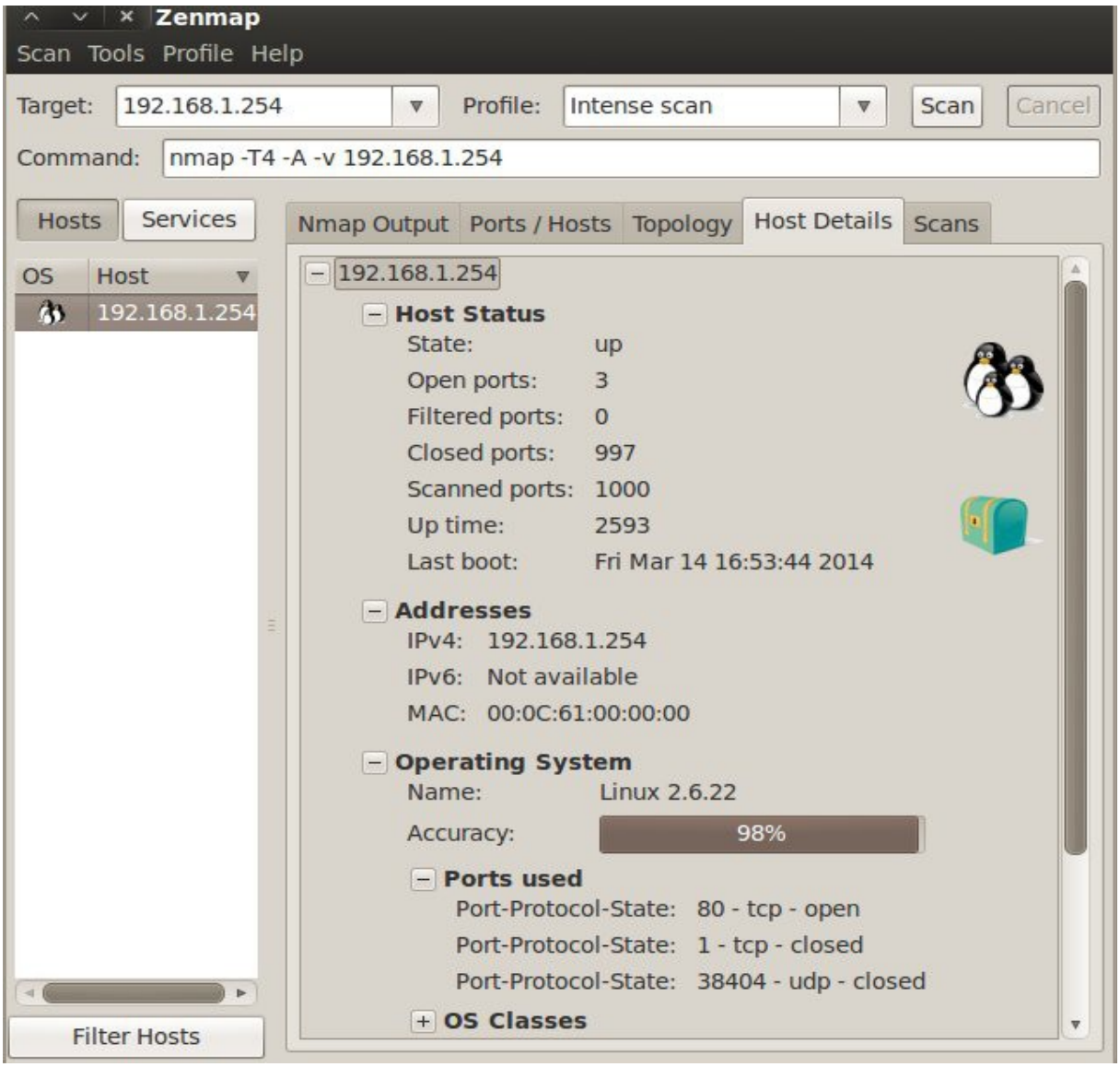

Figura 6 – Demonstração de uso da ferramenta Zenmap.

No exemplo da Figura 6 é possível constatar a implementação de uma verificação do *host* com endereço IP “192.168.1.254”, e com a exigência de uma alta intensidade de informações utilizando-se os parâmetros “-T4”, “-A” e “-v”, onde são retornadas

informações sobre o status, sistema operacional, versões, portas utilizadas e abertas, e outras informações sobre o *Host* de endereço IP “192.168.1.254”.

Caso selecionadas as opções laterais disponíveis na Figura 6, também seriam retornadas informações mais detalhadas, como topologia de rede, saída no modo verboso do comando, portas e *Hosts* ativos, dentre várias outras informações descobertas sobre o *Host* em questão.

2.9. ETHERAPE

Conforme GUETTA et al. (2014) informa EtherApe é um monitor gráfico de rede para Unix que utilizando-se da camada de enlace e do protocolo TCP/IP, efetua análises de rede em modo gráfico. Com ela é possível identificar *Hosts* ativos, a comunicação entre eles, os protocolos que estão sendo utilizados em conjunto com todo o tráfego de dados e toda a atividade de rede.

O acesso a ferramenta pode ser realizado por meio do menu *Applications* > *Internet* > *EtherApe*, ou em modo *root* por meio do mesmo caminho anterior porém selecionando “*EtherApe as root* “como opção final.
No exemplo seguinte é exibida uma análise de rede utilizando-se a ferramenta EtherApe.

Para dar início a uma análise utilizando-se a ferramenta EtherApe basta apenas clicar sobre o botão “*Start*”, e em seguida é demonstrado graficamente uma análise de tráfego da rede em questão, os protocolos em utilização e os ativos de rede presentes na mesma. Conforme GUETTA et al. (2014) declara, *hosts* e *links* mudam de tamanho em modo gráfico, e cada protocolo é demonstrado com uma respectiva cor. A seguir é exibida uma ilustração sobre uma análise de rede utilizando-se a ferramenta EtherApe.

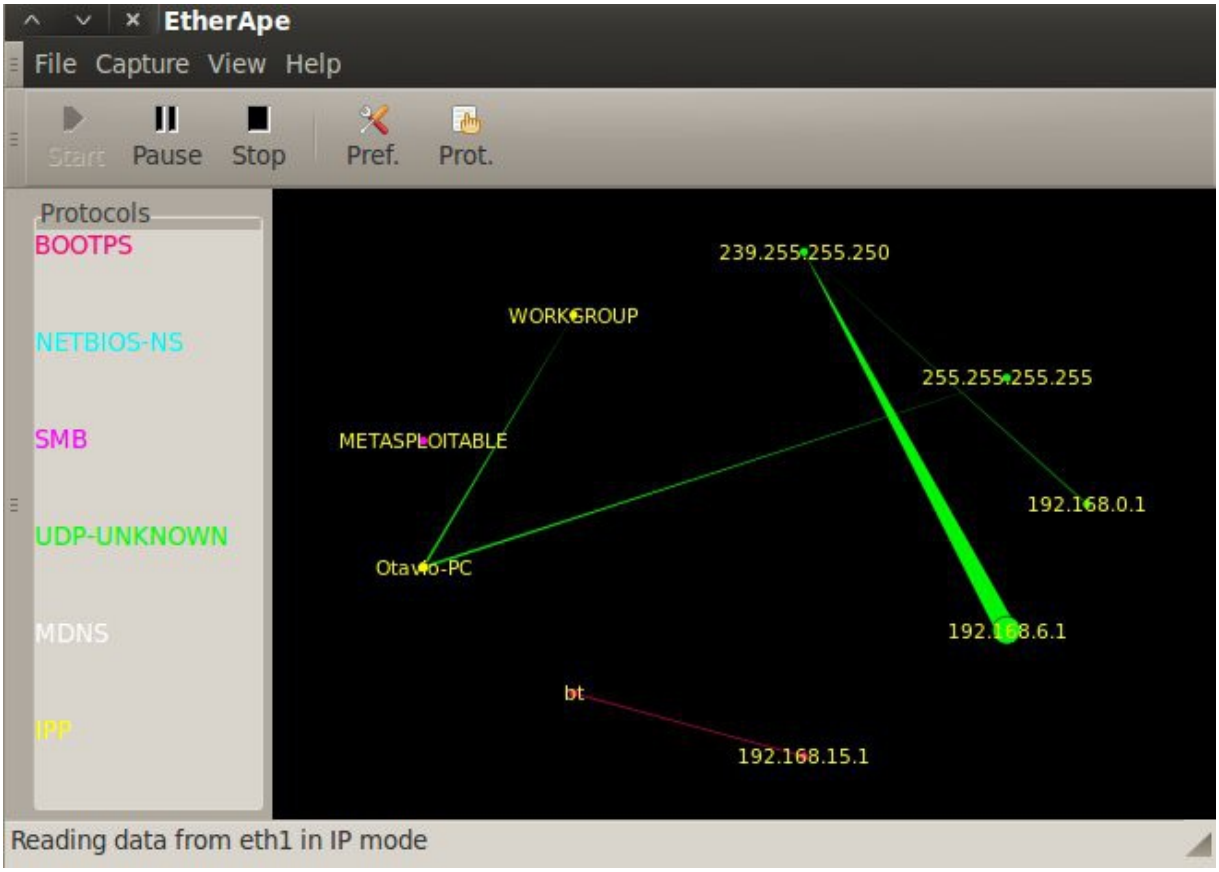

Figura 7 – Análise de Rede utilizando-se a ferramenta EtherApe.

É possível notar no exemplo da Figura 7 a detecção dos ativos de rede presentes, a comunicação entre eles e a utilização dos protocolos UDP e BOOTPS na rede. É possível ainda alterar a cor de cada protocolo para uma melhor visualização da análise de rede, ao selecionar o menu "*File*", a opção "*Preferences*", restando apenas a edição das cores de acordo com a preferência desejada na janela em exibição.

Ao final deste capítulo é possível concluir o quão importante é a busca de informações sobre a rede e o alvo a que se deseja obter acesso em questão, e o quanto a aplicabilidade das técnicas e ferramentas demonstradas neste capítulo simplificam e facilitam a realização deste trabalho.

3 – DETECÇÃO DE BANNERS SOBRE DNS (DOMAIN NAME SYSTEM)

3.1. INTRODUÇÃO

Este capítulo tem como propósito a definição do conceito sobre Servidores de Domínio ou Domain Name System (DNS), Detecção de Banners sobre DNS e a demonstração sobre como esta detecção de banners e informações podem ser feitas. Estas informações são detectadas com base nos conceitos de Reconhecimento e Impressão Digital, explicados anteriormente no capítulo 2. A Detecção de Banners sobre DNS pode ser realizada a partir de ferramentas contidas no Backtrack 5 R3 como Nslookup, Dnsenum, Fierce e Netifera, ou a partir de ferramentas do gênero que possuam a mesma finalidade e também por meio de serviços públicos disponibilizados na Internet.

3.2. DEFINIÇÃO SOBRE DOMAIN NAME SYSTEM (DNS)

DNS ou Domain Name System é definido por GIAVAROTO et al. (2013) como um banco de informações utilizado na resolução de nomes que traduz endereços de IP em nomes de domínios . Este banco de informações necessita sempre estar bem configurado, o menos vulnerável possível, pois em caso de vulnerabilidades, informações de uma determinada organização ou companhia podem correr riscos. Além disso no caso de erros de configuração podem ocorrer erros de associações.

GIAVAROTO et al. (2013) declara ainda a importância de estar ciente sobre alguns conceitos que um servidor DNS pode oferecer, conforme será mostrado a seguir:

- Registro SOA: responsável pelo domínio, versão, atualização, expiração e valorTTL.

- Registro NS: servidores responsáveis pelo domínio.

• Registro A: corresponde ao endereço dos servidores.

• Registro CNAME: usado como alias ou apelido, utilizando o CNAME, vários nomes poderão ser atribuídos a um mesmo servidor.

• Registro HINFO: fornecem informações sobre o servidor.

• Registro MX: informações relativas ao serviço de e-mail.

• Registro PTR: associa endereços a nome de servidores.

3.3. NSLOOKUP

GIAVAROTO et al. (2013) informa que a ferramenta Nslookup não é caracterizada por ser uma ferramenta, e sim um comando que está presente não só no Backtrack 5 R3 Linux, mas em várias outras distribuições Linux e também no ambiente Windows. Este comando pode ser executado em modo simples de usuário, não precisando estar em modo *root*, e sua função é descobrir informações simples a respeito de um determinado domínio *DNS*. É importante destacá-lo justamente por sua simplicidade.

No exemplo seguinte da Figura 8 é exibido um exemplo onde é retornado o endereço IP da página *WEB* da Fundação Educacional do Município de Assis.

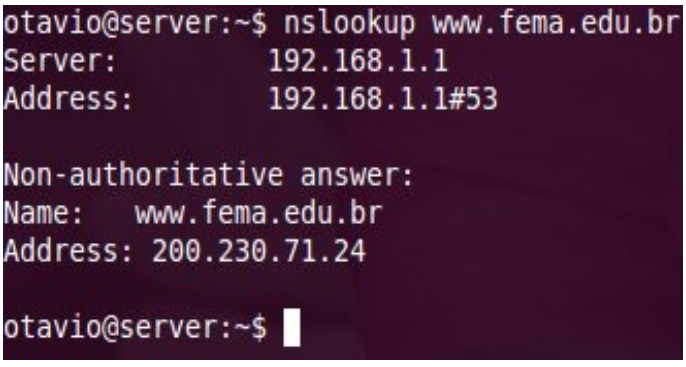

Figura 8 – Exemplo de utilização do comando Nslookup.

Utilizando-se o comando Nslookup é possível obter-se informações ainda mais relevantes. No exemplo a seguir é demonstrado que o comando Nslookup pode retornar mais informações, tais como transferências de zona de *DNS* e transferência de zona reversa de *DNS*.

Figura 9 – Obtenção de informações do servidor 192.168.1.254 utilizando-se o comando Nslookup.

No exemplo anterior da Figura 9 é possível notar a utilização do comando Nslookup, especificando como parâmetro o servidor “192.168.1.254”. Após isso é solicitada a informação sobre quem são os servidores responsáveis pelos domínios “www.otaviopolatto.com.br”, “ftp.otaviopolatto.com.br”, “smtp.otaviopolatto.com.br” e “pop.otaviopolatto.com.br”, e é retornado o endereço IP “192.168.1.254” que corresponde a todos os domínios solicitados.

É possível concluir que o comando Nslookup pode nos retornar informações sobre transferência de zona sobre o servidor local “192.168.1.254”, configurado especialmente para este teste. Porém é importante estar ciente de que isto só foi possível devido ao fato de o servidor está configurado para efetuar transferência de zonas e retornar este tipo de informação.

No exemplo a seguir é exibida a obtenção de informações de transferência de zona reversa, pertinentes ao servidor “192.168.1.254”.

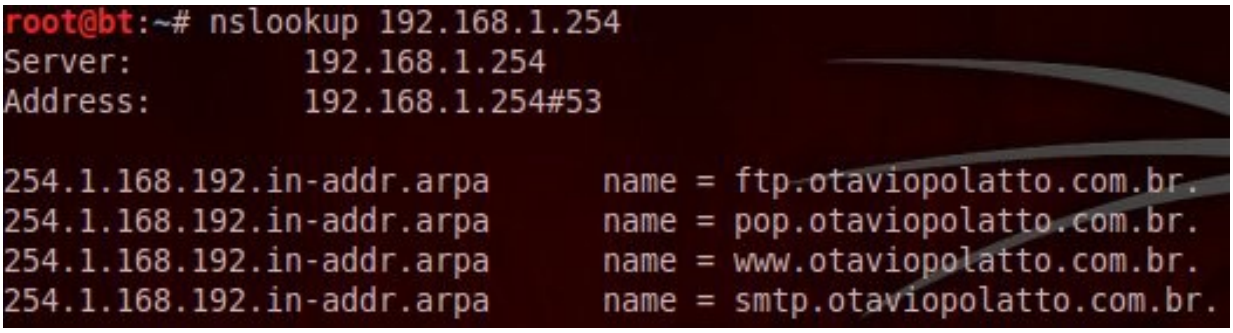

Figura 10 – Obtenção de informações de zona reversa do servidor 192.168.1.254 utilizando-se o comando Nslookup.

No exemplo anterior da Figura 10 é possível perceber ainda como foi possível a obtenção de informações de zona reversa pertinentes ao servidor “192.168.1.254”, fato que só foi possível em função de o servidor estar configurado para aceitar este tipo de requisição.

3.4. DNSENUM

Conforme GIAVAROTO et al. (2013) informa a ferramenta Dnsenum permite a pesquisa de hosts, nomes de servidores, registros MX, IPs, dentre vários outros. Sua localização na ferramenta Backtrack 5 R3 está localizada no diretório “/pentest/enumeration/dnsenum” e sua execução pode ser realizada por meio do seguinte comando : “./dnsenum.pl “www.meudominio.com.br” “, onde www.meudominio.com.br é o parâmetro alvo a se obter informações.

A seguir é exibida uma demonstração de utilização da ferramenta Dnsenum que tem como finalidade a obtenção de informações relevantes sobre o domínio "http://www.sitiobrasil.com.br".

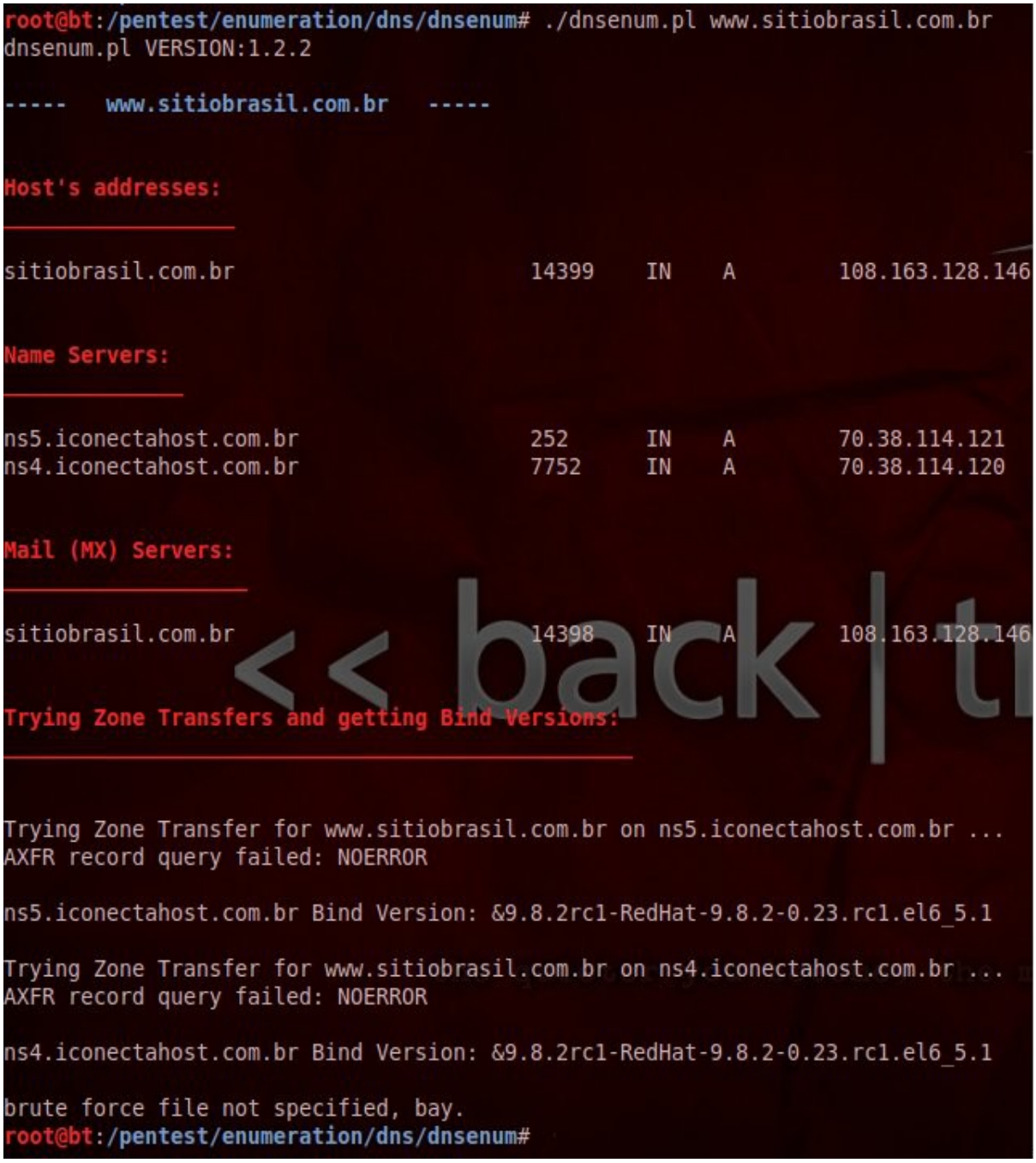

Figura 11 - Teste da ferramenta Dnsenum contra o domínio "http://www.sitiobrasil.com.br".

É possível observar no exemplo anterior da Figura 11 que no teste realizado contra o domínio “http://www.sitiobrasil.com.br” é possível a descoberta de informações sobre o endereço IP do *host* e sua respectiva porta em utilização, o sistema operacional em utilização Red Hat Linux, o nome dos servidores que respondem pelo domínio e seus respectivos endereços IP e portas utilizadas.

É importante ressaltar que o levantamento de informações a partir de ferramentas como Dnsenum depende do modo como o servidor em questão está configurado. No exemplo anterior por exemplo é possível notar que não é possível efetuar a transferência de zonas relacionada ao domínio alvo, pois o domínio em questão esta configurado de forma a preservar esta informação.

3.5. FIERCE

A ferramenta Fierce assim como a Dnsenum possui a mesma finalidade de levantar informações sobre o servidor alvo. Porém a Fierce merece destaque por seu excelente desempenho e pela possibilidade de descobrir informações relevantes no modo de força bruta, munindo-se de *Wordlists* que a própria ferramenta oferece.

No exemplo seguinte a ferramenta Fierce realiza um levantamento de informações contra o domínio “http://www.sitiobrasil.com.br” assim como no exemplo anterior.

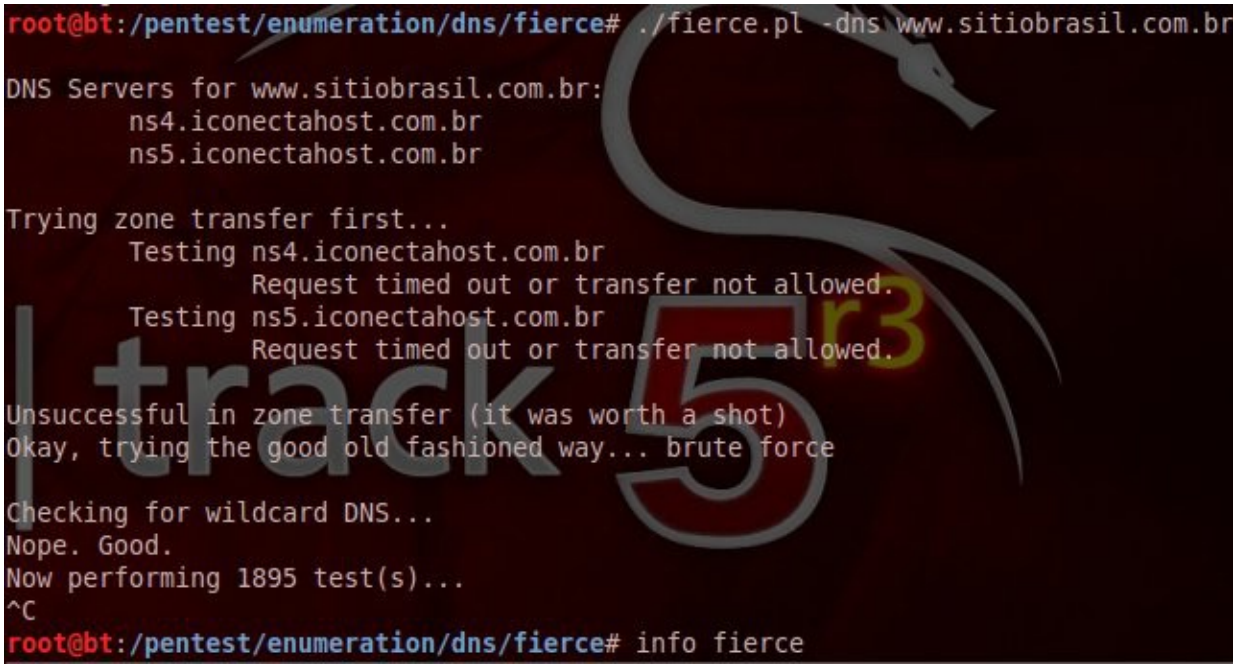

Figura 12 – Teste da ferramenta Fierce contra o domínio “http://www.sitiobrasil.com.br”.

No exemplo acima da Figura 12 é possível observar a identificação do nome dos servidores que respondem pelo domínio “http://www.sitiobrasil.com.br” e uma tentativa no levantamento de informações de transferência de zonas do domínio em questão. Esta transferência de zonas não foi realizada pois conforme no exemplo anterior da Figura 11, os servidores do domínio em questão não estão configurados para aceitar transferência de zonas.

É possível observar ainda que ao perceber que não foi possível realizar a transferência de zonas, a ferramenta Fierce inicia tentativas no modo de força bruta. Esta obtenção de informações de transferência de zonas no modo de força bruta pode ser um processo muito demorado, podendo levar horas e até mesmo dias para a descoberta destas informações. Este procedimento não foi concluído até o fim, para que informações sobre o domínio em questão fossem preservadas.

3.6. NETIFERA

Conforme GIAVAROTO et al. (2013) informa Netifera é uma ferramenta *open source* que possui a finalidade de levantar informações DNS *Lookup* sobre alvos, e descobertas sobre serviços TCP e UDP. O diferencial desta ferramenta é que ela possui um modo gráfico atrativo e de simples manuseio. Sua execução é realizada a partir do acesso ao menu *Applications* > *BackTrack* > *Information Gathering* > *Network Analysis* > *Identify Live Hosts* > *Netifera.*

Para a efetivação de uma busca sobre um domínio utilizando-se a ferramenta Netifera, deve-se selecionar o campo de endereço, informar o nome do domínio alvo, e clicar sobre o botão +, que dará início as buscas. É possível realizar mais de um teste ao mesmo tempo, devendo-se apenas clicar sobre o menu *File* > *New Space* e repetir os procedimentos anteriores de efetivação de buscas. No exemplo da Figura a seguir é demonstrado um exemplo de busca utilizando-se a ferramenta Netifera.

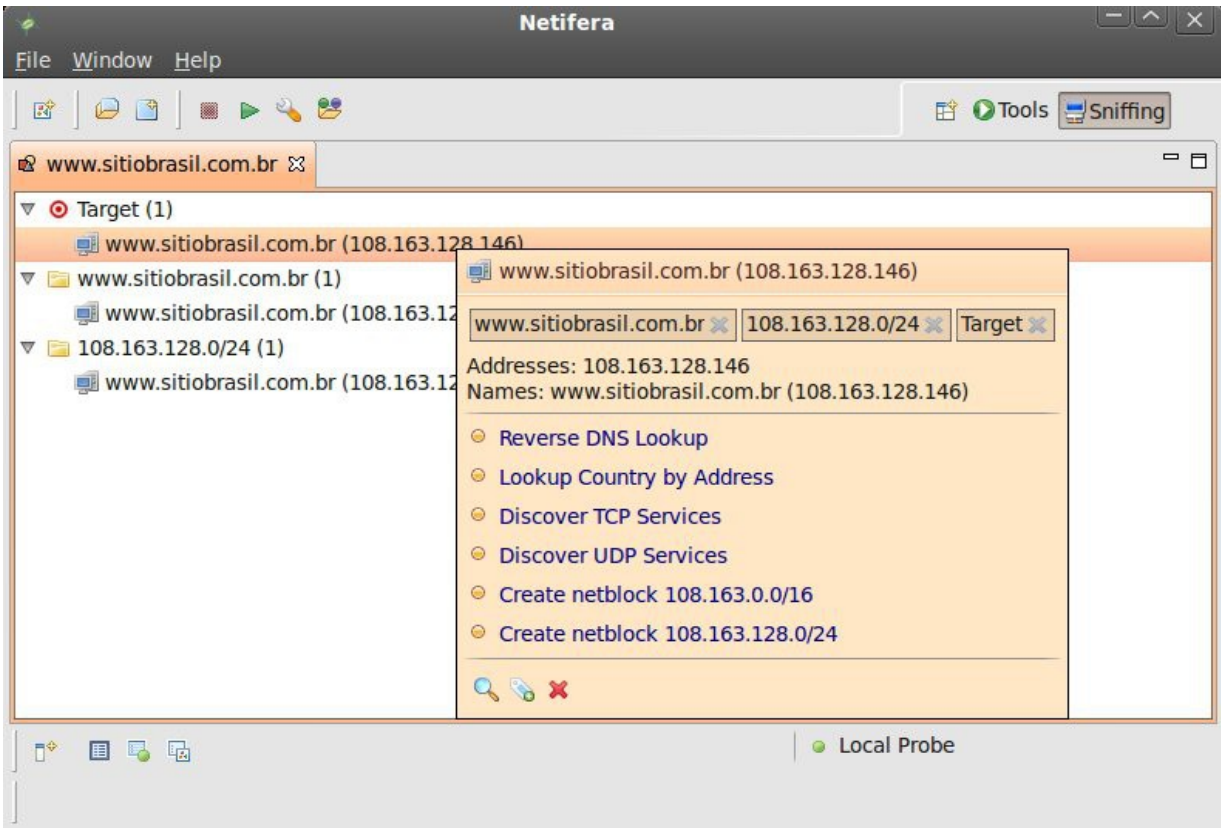

Figura 13 – Exemplo de utilização da ferramenta Netifera.

É possível observar no exemplo anterior da Figura 13 a realização de uma busca de informações contra o domínio "http://www.sitiobrasil.com.br", e o retorno de informações pela ferramenta Netifera como endereço IP do domínio e a possibilidade da realização de vários outros levantamentos de informações sobre o domínio, tais como teste de DNS Reverso, descobrimento de serviços TCP e UDP, descobrimento do país a partir do endereço IP, dentre outras.

3.7. BUSCAS DE DOMÍNIOS DNS A PARTIR DA INTERNET E NETCRAFT

GIAVAROTO et al. (2013) informa que apesar dos métodos de pesquisas sobre DNS utilizando-se ferramentas contidas no Backtrack 5 R3, deve-se deixar claro que isto é possível também por meio de serviços públicos na Internet. Na tabela a seguir são demonstrados alguns dos vários serviços públicos disponíveis:

Ferramentas	Endereços
Netcraft – endereços fora do Brasil	http://news.netcraft.com/
Domaintools – whois, lookup, IP, etc.	http://www.domaintools.com/
Registro BR – endereços no Brasil	https://registro.br/cgi-bin/whois/
Arin – endereços fora do Brasil	https://www.arin.net/
Apnic- endereços Ásia e Pacífico	http://www.apnic.net/apnic-info/search
Whois – endereços fora do Brasil	http://new.whois.net/
Ripe – endereços europeus	http://www.ripe.net/

Tabela 1 - Fontes de consultas DNS (In: GIAVAROTO et al., 2013, p.47)

Com o intuito de salientar a declaração de GIAVAROTO et al. (2013), no exemplo a seguir é efetuado um levantamento de informações a respeito do domínio "http://www.sitiobrasil.com.br" a partir do *site* "http://www.netcraft.com".

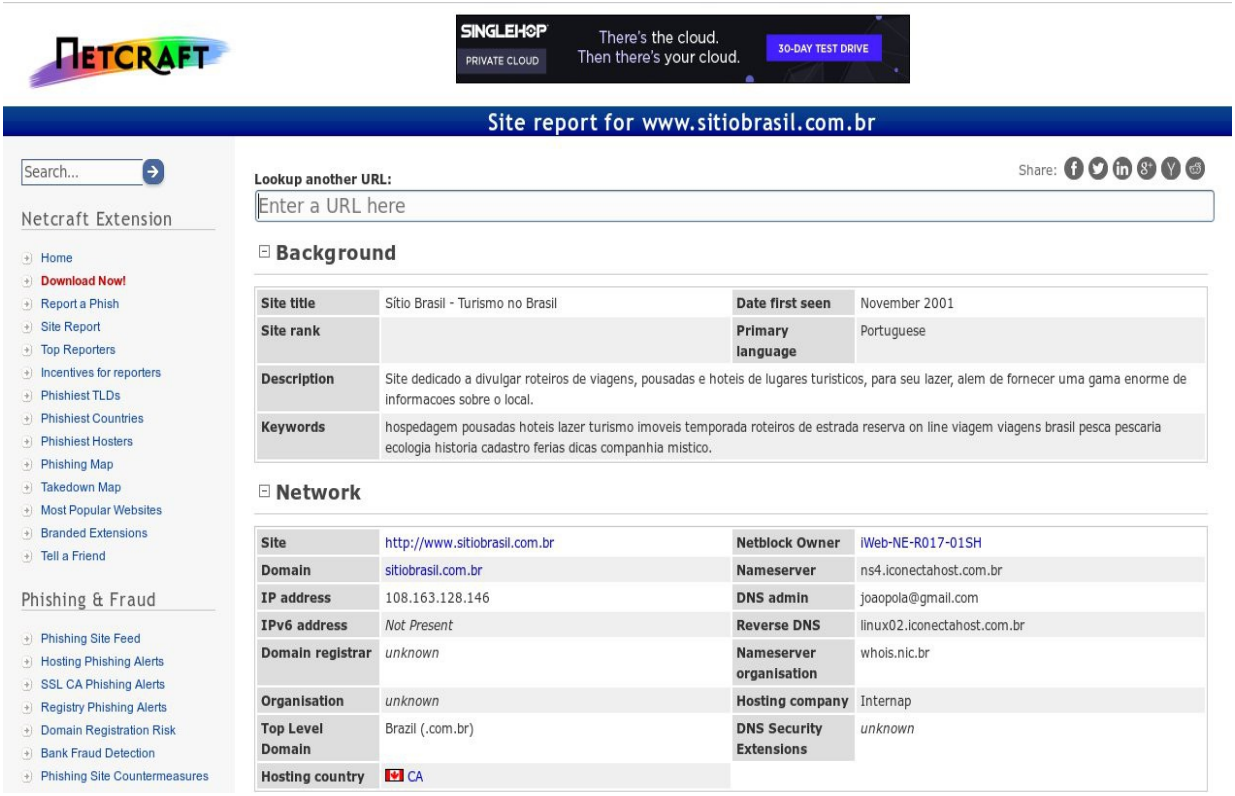

Figura 14 – Levantamento de informações a partir do *site* "http://www.netcraft.com".

É possível observar no exemplo anterior da Figura 14 que quase todas as informações obtidas anteriormente a partir das ferramentas Dnsenum e Fierce, são obtidas com facilidade a partir do *site* "http://www.netcraft.com", e que informações complementares como descrição e tipo do *site* também são obtidas. É possível ainda obter informações sobre a verdadeira origem do servidor hospedeiro do domínio "www.sitiobrasil.com.br" que, conforme relatado acima se encontra na Califórnia.

Finaliza-se este capítulo ressaltando a importância da aplicabilidade das técnicas e ferramentas utilizadas neste capítulo, e ainda a necessidade de que um servidor *DNS* esteja sempre bem configurado, para que não seja possível a revelação de informações relevantes por meio da transferência de zonas.

4 – QUEBRA DE SENHA E WORDLISTS

4.1. INTRODUÇÃO

Este capítulo tem como finalidade abranger o conceito sobre Quebra de Senhas e *Wordlists*, o que são e para que servem. É exemplificado aqui também a quebra de senhas de sistemas Windows utilizando-se o conceito de Tabelas *Rainbow* e os modos convencionais de quebras de senhas.

4.2. LISTA DE PALAVRAS OU WORDLISTS

Segundo DRAVET (2010), *Wordlists* ou Lista de Palavras, como o próprio nome sugere é uma lista constituída a partir de palavras, números ou caracteres especiais que fazem parte de um cotidiano geral e tem algum sentido para o alvo em questão. Esta lista de palavras é constituída a partir de informações obtidas a respeito do alvo e pode ser gerada manualmente utilizando-se a criatividade de seu autor, ou por meio de ferramentas desenvolvidas especificamente para esta finalidade, como a ferramenta a ser exemplificada neste capítulo Crunch.

Wordlists são formuladas geralmente em um formato de arquivo texto simples, para que possa ser reconhecido por qualquer ferramenta.

4.3. QUEBRA DE SENHAS

O processo de quebra de senha pode ocorrer a partir de dois modos: *online* e *offine*. De acordo com SHAKEEL et al. (2011), caracteriza-se quebra de senha *online* quando são efetuadas tentativas de quebra de senha a uma máquina de destino; E quebra de senha *offine* caracteriza-se quando é obtido um arquivo criptografado de senhas da máquina alvo, restando apenas a quebra de senhas utilizando-se ferramentas que possuam esta finalidade, a partir da máquina do atacante. Para

obtenção de acesso a um específico sistema protegido, rede *wireless*, ou aplicação protegida por login, é necessária a descoberta de um nome de usuário e senha do determinado alvo em questão. É possível munir-se de técnicas de engenharia social ou até mesmo ferramentas específicas para a quebra de senhas.

Conforme GIAVAROTO et al. (2013) diz a técnica de quebra de senhas pode ocorrer a partir de duas maneiras, por ataque de dicionário ou ataque de força bruta. No ataque por dicionário são utilizadas duas *Wordlists*, uma de possíveis usuários e outra de possíveis senhas e o software responsável encarrega-se de fazer os testes de combinações a fim de obter-se o usuário e senha corretos.

No ataque utilizando-se a técnica de força bruta o software responsável utiliza um algoritmo de combinação que se encarrega de fazer tentativas de quebra da senha, onde são realizados testes de combinação de caracteres até que seja descoberta a senha. Este método é mais difícil e demorado, pois, dependendo da complexidade da senha, torna-se quase impossível. As ferramentas para quebra de senhas a serem exemplificadas neste capítulo são a John The Ripper e a Ophcrack.

4.4. CRUNCH

A ferramenta Crunch tem como objetivo a criação de *Wordlists* a partir de parâmetros passados pelo usuário. A *Wordlist* a ser gerada conterá todas as combinações possíveis de acordo com os caracteres passados como parâmetro para sua criação. A execução da ferramenta Crunch no Backtrack 5 R3 pode ser realizada a partir do acesso ao diretório “/pentest/passwords/crunch” ao digitar-se o comando “./crunch” informando-se os parâmetros necessários para a criação da *Wordlist*. Um manual de ajuda sobre o uso da ferramenta Crunch pode ser visualizado através do comando “*info* crunch”. No exemplo da Figura a seguir, elaborado com base no exemplo de PAES (2014), demonstra-se a criação de uma *Wordlist* numérica a partir da ferramenta Crunch.

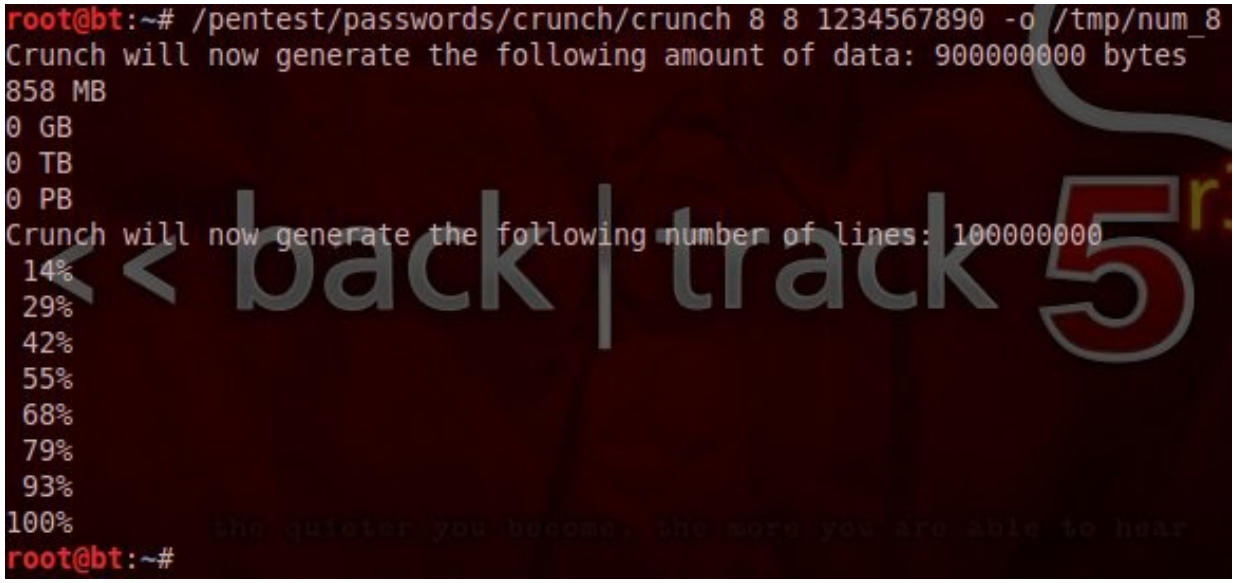

Figura 15 – Criação de *Wordlist* de 8 caracteres numéricos de 0-9 com a ferramenta Crunch.

No exemplo da Figura 15 acima é possível reparar a criação de uma *Wordlist* cujo tamanho final é de 858 MB com o tamanho mínimo e máximo de 8 caracteres numéricos 1234567890. A partir do parâmetro -o é possível observar também que a *Wordlist* é armazenada no diretório /tmp e que seu nome de saída é “num_8”.

A ferramenta Crunch disponibiliza para auxílio na criação de *Wordlists* um arquivo de dicionário de caracteres que pode ajudar muito no processo de criação da *Wordlist*. O arquivo responsável por este dicionário é o “charset.lst”, que também está localizado no diretório da ferramenta Crunch. No exemplo a seguir é elaborada a demonstração de criação de uma *Wordlists* utilizando-se a dicionário “charset.lst”.

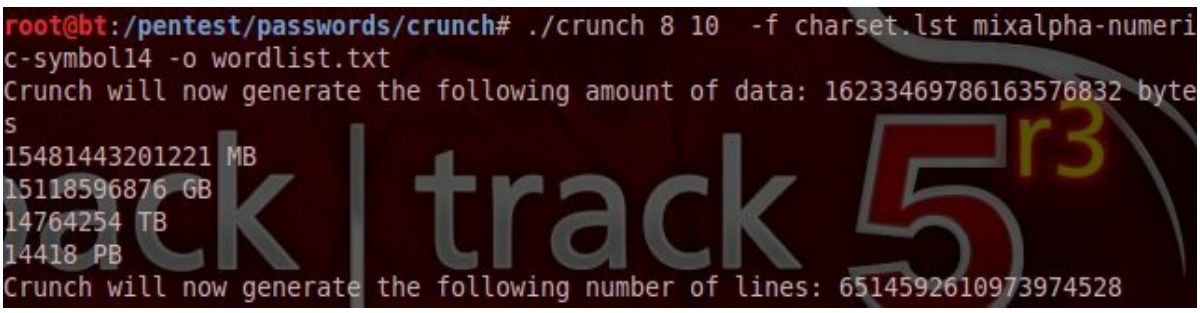

Figura 16 – Criação de *Wordlist* utilizando-se o dicionário de palavras charset.lst.

No exemplo anterior da Figura 16 é exibido o comando para a criação de uma *Wordlist* com tamanho mínimo de 8 caracteres e no máximo 10 caracteres, em seguida é especificado a partir do parâmetro “-f” o uso do dicionário de palavras “charset.lst” indicando-se os tipos de caracteres a serem utilizados na *Wordlist*; E por fim o parâmetro “-o” especifica a saída e o nome da *Wordlist* a ser gerada.

É importante ter ciência de que a criação de *Wordlists* com uma ampla variedade de caracteres e com um amplo número de caracteres pode gerar arquivos muito grandes, resultando em um processo muito demorado, podendo levar horas, dias e até meses dependendo da complexidade especificada.

4.5. JOHN THE RIPPER E A QUEBRA DE SENHAS DO WINDOWS

A ferramenta John The Ripper tem a função de quebrar senhas no modo de força bruta, e conforme GIAVAROTO et al. (2013) informa o software utiliza um algoritmo de combinação que se encarrega de efetuar as tentativas de quebra da senha, fato que pode resultar em um trabalho difícil e demorado, as vezes até impossível, dependendo do nível de complexidade da senha.

Esta ferramenta pode ser utilizada para quebrar-se vários tipos de senhas, com várias criptografias de vários sistemas operacionais. No exemplo a seguir é demonstrada a quebra de senha de usuários do sistema operacional Windows XP, a partir do arquivo SAM, que contém informações sobre senhas de usuário do Windows.

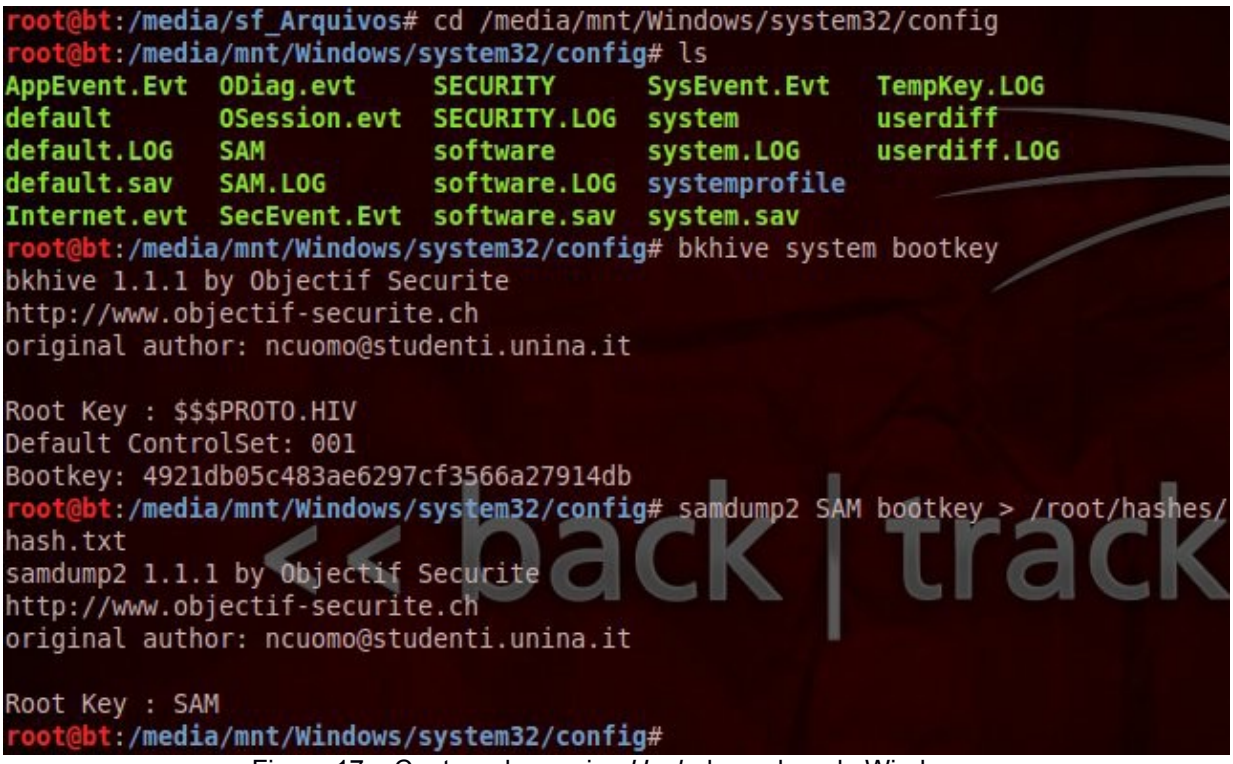

Figura 17 – Captura do arquivo *Hash* de senhas do Windows.

No exemplo acima da Figura 17 é possível observar o acesso a estrutura de arquivos do Sistemas Windows, e sua pasta *config*, encontrada no diretório "/media/mnt/Windows/system32/config". Em seguida utilizando-se o comando "bkhive system bootkey" é capturada a *system bootkey*, uma característica do Windows responsável pela implementação de uma camada de criptografia adicional para os Hashs de senhas armazenados no arquivo SAM. Em seguida é efetuada a captura do arquivo *Hash* de senhas SAM utilizando-se a ferramenta samdump2, e são armazenados os *Hashs* de senha no arquivo hash.txt, encontrado no diretório "/root/hashes".

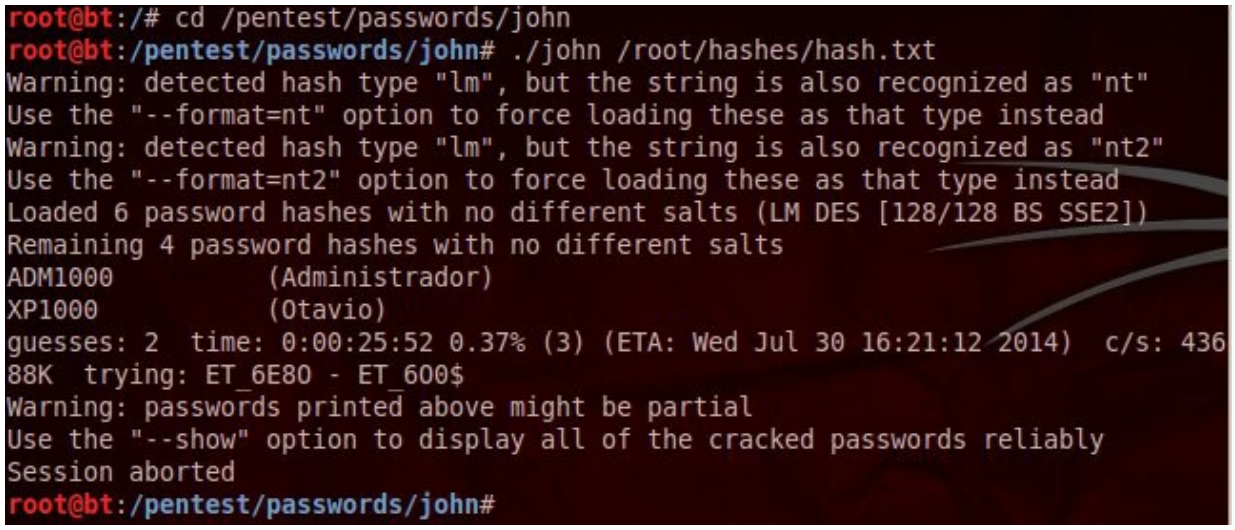

Figura 18 – Quebra de senha do Windows utilizando-se a ferramenta John The Ripper.

Em sequência aos passos anteriores da Figura 17, na Figura 18 exibida acima é possível efetuar a quebrar as senhas do arquivo *Hash* de senhas do Windows. Observa-se que para tal ação é efetuado o acesso ao diretório "/pentest/passwords/john", diretório da ferramenta John The Ripper, e em seguida é realizada a execução do comando "./john /root/hashes/hash.txt", onde é passado como parâmetro o diretório e o arquivo com os *Hashs* de senha gerados anteriormente pela ferramenta samdump2.

É importante ter ciência de que os procedimentos realizados anteriormente podem variar de acordo com a versão de utilização do Windows em questão, pois a criptografia utilizada para a proteção do arquivo *Hash* de senhas pode ser diferente a cada versão. Neste caso é necessário um maior aprofundamento sobre as técnicas e funcionalidades da ferramenta John The Ripper, devendo-se saber especificar corretamente o tipo de criptografia correta como parâmetro ao comando a ser utilizado.

Informações adicionais sobre as ferramentas John The Ripper, bkhive e samdump2 podem ser visualizadas ao digitar os comandos "*info* john", "*info* bkhive" e "*info* samdump2" no terminal de comandos do Backtrack 5 R3.

4.6. OPHCRACK

Ophcrack é uma ferramenta livre para quebra de senhas de sistemas operacionais Windows baseando-se no conceito de Tabelas *Rainbow*, que segundo PRITCHETT et al. (2012) são tabelas de dicionário especiais que utilizam valores *Hash*, ao invés de *Wordlists* com senhas convencionais. Estas tabelas são previamente criadas, fato que possibilita que a descoberta da senha ocorra de um modo muito mais rápido do que no modo de força bruta convencional.

Para a execução desta ferramenta é necessário efetuar o download das Tabelas *Rainbow* de acordo com a versão do Windows que se deseja quebrar a senha. O download destas tabelas pode ser efetuado através do link oficial do *site* da ferramenta Ophcrack: http://ophcrack.sourceforge.net/tables.php.

Um ponto forte desta ferramenta é que ela possui uma interface gráfica para execução, que pode ser executado acessando o menu *Applications* > *Backtrack* > *Privilege Scalation* > *Password Attacks* > *Ophcrack-GUI*. Além da interface gráfica a ferramenta possui também o modo texto, que pode ser acessado seguindo-se os mesmos passos anteriores, porém o atalho a ser executado será o Ophcrack. É possível ainda a consulta a um manual de ajuda oferecido pela ferramenta ao digitar o comando “ophcrack –help” no terminal de comandos do Backtrack 5 R3.

No exemplo seguinte é demonstrado o processo de quebra de senhas de um arquivo *Hash* de senhas do sistema operacional Windows XP, utilizando-se a tabela *rainbow* disponibilizada no link anterior “XP free small”.

O funcionamento da ferramenta Ophcrack é bem simples, para começar basta clicar sobre o botão “*Load*” e selecionar a opção “*Encrypted* SAM”, então a ferramenta irá carregar o arquivo criptografado de senhas do Windows.

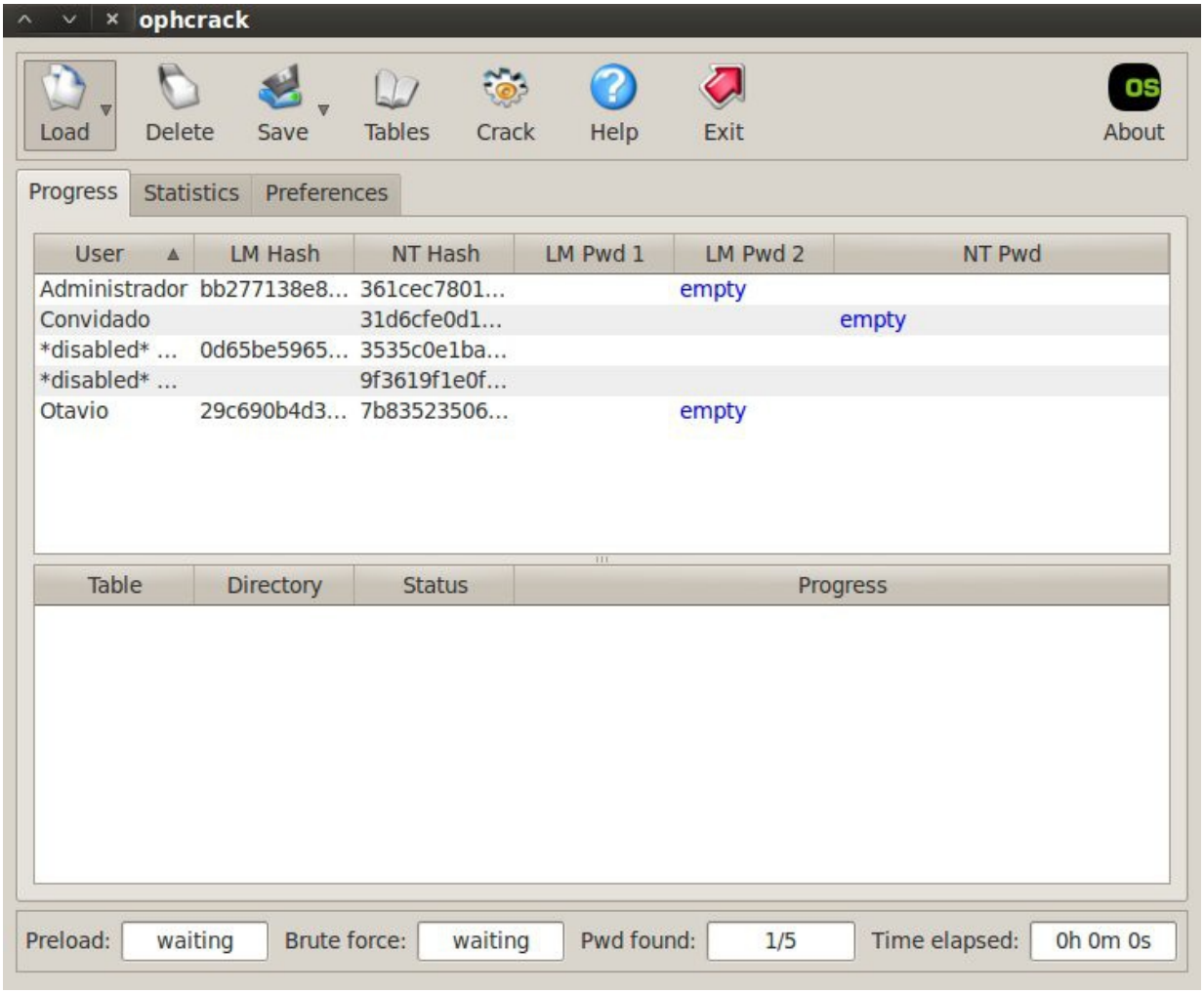

Figura 19 – Ferramenta Ophcrack com o arquivo *Hash* de senhas do Windows carregado.

Em seguida o próximo passo é carregar a tabela *rainbow* a ser utilizada. Para carregar a tabela basta clicar sobre o botão Tables, selecionar a tabela correspondente, neste caso a tabela “XP Free Small”, selecionar o arquivo correspondente a tabela, clicar sobre o botão “*Install*” e em seguida em “OK”.

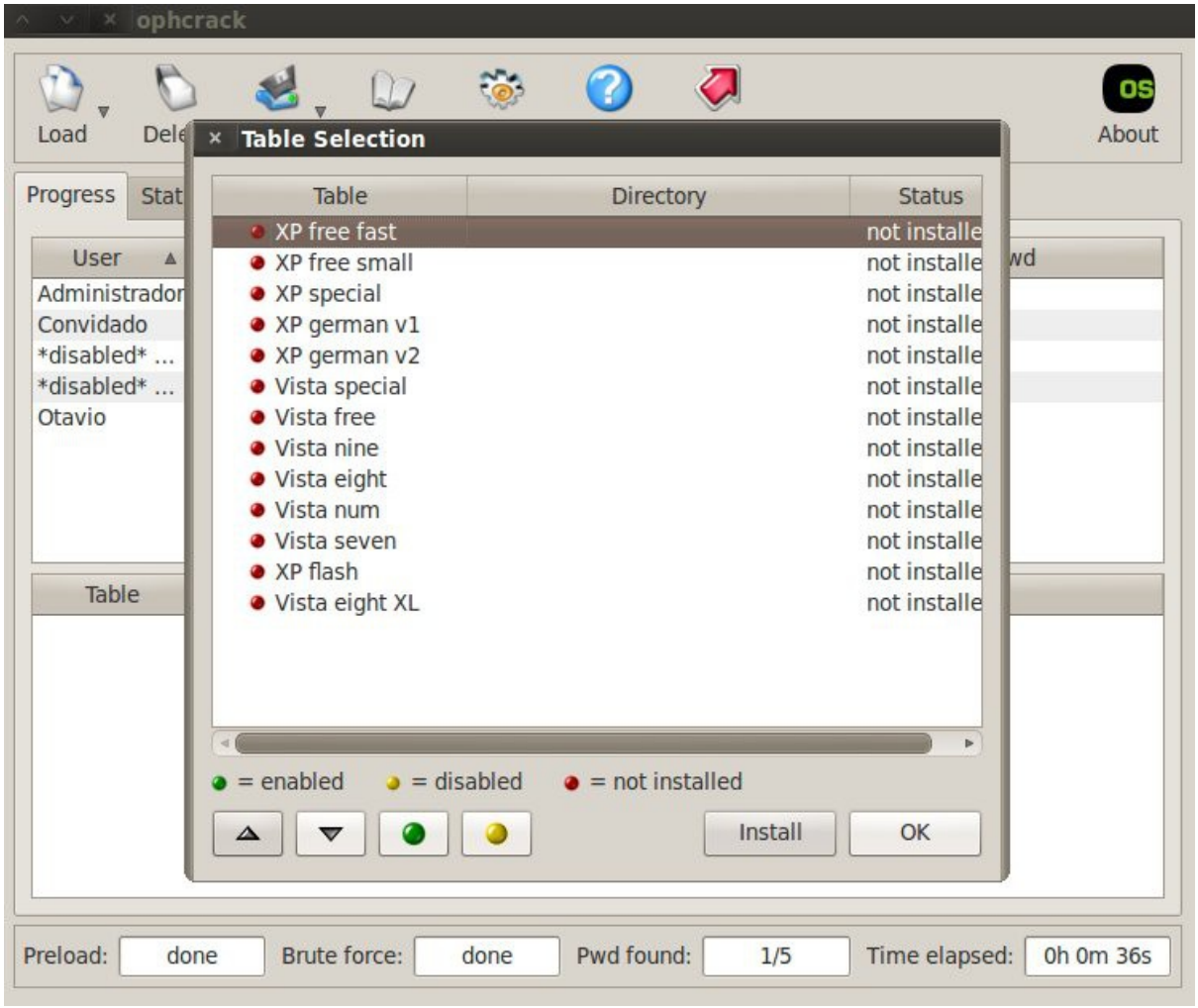

Figura 20 – Menu de seleção de Tabelas *Rainbow* da ferramenta Ophcrack.

Com o arquivo *Hash* de senhas do Windows carregado e a tabela *rainbow* correspondente a versão do Windows instalada, o próximo e último passo é clicar sobre o botão Crack e aguardar até que a senha seja quebrada pela ferramenta.

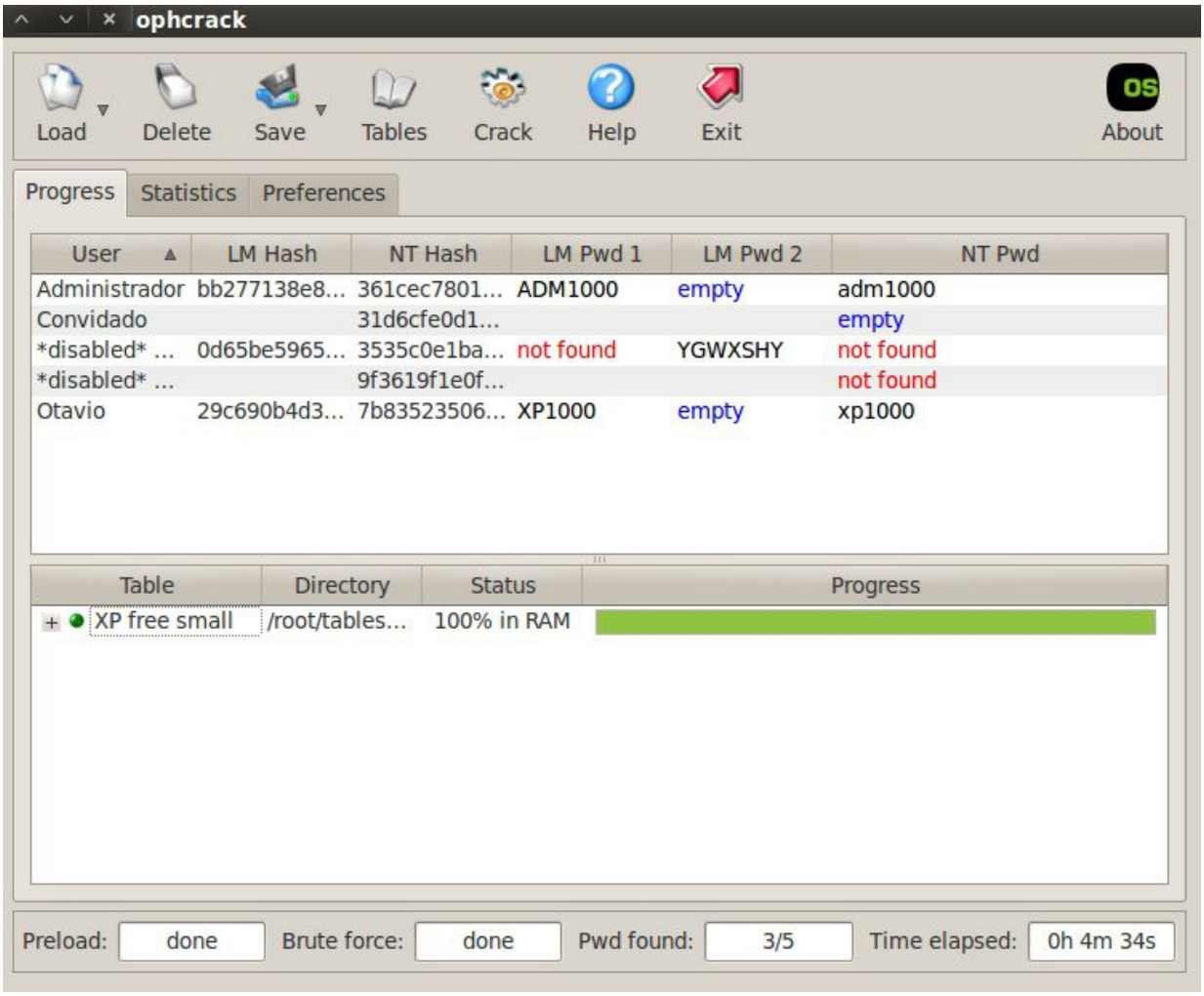

Figura 21 – Quebra de senha do Windows XP utilizando-se a ferramenta Ophcrack.

Observa-se acima na Figura 21 que a senha dos usuários “Administrador” e “Otávio” do Windows XP foi quebrada, e correspondem respectivamente á “adm1000” e “xp1000”. É possível perceber também que o processo todo durou apenas quatro minutos e trinta e quatro segundos. Conclui-se ao final deste processo que a ferramenta Ophcrack obteve uma alta precisão na quebra de senhas do Windows, mais rápida do que no modo convencional utilizando-se o modo de força bruta.

Ao final deste capítulo é possível concluir que para uma maior proteção e segurança, é sempre importante a utilização de senhas grandes e de ampla variedade, contendo números e caracteres especiais. Quanto maior o tamanho e o nível de complexidade da senha, maior é o tempo e a dificuldade para ela ser quebrada.

5 – VULNERABILIDADES E OBTENÇÃO DE ACESSO

5.1. INTRODUÇÃO

Nos capítulos anteriores foram demonstrados como ocorrem a efetivação de um ataque, técnicas de enumeração e impressão digital, obtenção de informações de servidores DNS e conceitos sobre quebra de senhas e *Wordlists*. Dando sequência ao conteúdo exposto anteriormente, o conceito de obtenção de acesso se faz presente, e o meio mais fácil para obter-se acesso é por meio da detecção de Vulnerabilidades.

5.2. VULNERABILIDADES

Pode ser definida uma Vulnerabilidade uma simples porta que se encontra aberta, uma falha de algum componente do sistema operacional do alvo, um arquivo de configuração que não esteja configurado de forma correta etc. Conforme PRITCHETT et al. (2012) informa, identificar e escanear as vulnerabilidades de um alvo é sempre considerada uma das tarefas mais entediantes por Analistas de Segurança e Hackers Éticos, porém é uma das fases mais importantes. Uma vez que vulnerabilidades sobre o alvo sejam identificadas, é possível obter-se acesso com maior precisão.

5.3. DETECÇÃO DE VULNERABILIDADES COM O BACKTRACK 5 R3

PRITCHETT et al. (2012) declara que a ferramenta Backtrack 5 R3 dispõe de ferramentas para a detecção de vulnerabilidades, sendo que as principais são a Nessus e OpenVAS, que possuem em comum a possibilidade de escanear e detectar vulnerabilidades em sistemas operacionais Windows e Linux, em seu sistema local em utilização e em serviços de rede. PRITCHETT et al. (2012) informa ainda que a ferramenta OpenVAS é caracterizada sobre o tipo de licença GNU, podendo ser classificada como um software livre, merecendo destaque em relação a ferramenta

Nessus que é paga.

Neste capítulo é abordado o uso das ferramentas xHydra e Medusa, que embora possuam a finalidade de quebrar senhas de modo a obter-se acesso ao sistema, efetuam este procedimento somente a partir da identificação de uma vulnerabilidade ou brecha, como a de uma falha no sistema ou a identificação de uma porta aberta.

5.4. XHYDRA

A ferramenta xHydra é bastante robusta, prática e apresenta um bom desempenho. GIAVAROTO et al. (2013) destaca que a ferramenta possui uma interface gráfica amigável e de fácil manuseio e é muito eficiente quando o assunto é quebra de senhas online. O acesso a ferramenta pode ser feito através do menu *Applications* > *BackTrack* > *Privilege Scalation* > *Password Attacks* > *Online Attacks* > *hydra-gtk*. Uma versão no modo texto também pode ser acessada, seguindo-se o mesmo caminho do passo anterior porém devendo-se selecionar como opção final a opção hydra.

No exemplo a seguir é demonstrada a obtenção de acesso a um servidor ftp de um alvo que encontra-se com a vulnerabilidade de estar com a porta 21 (ftp) aberta.

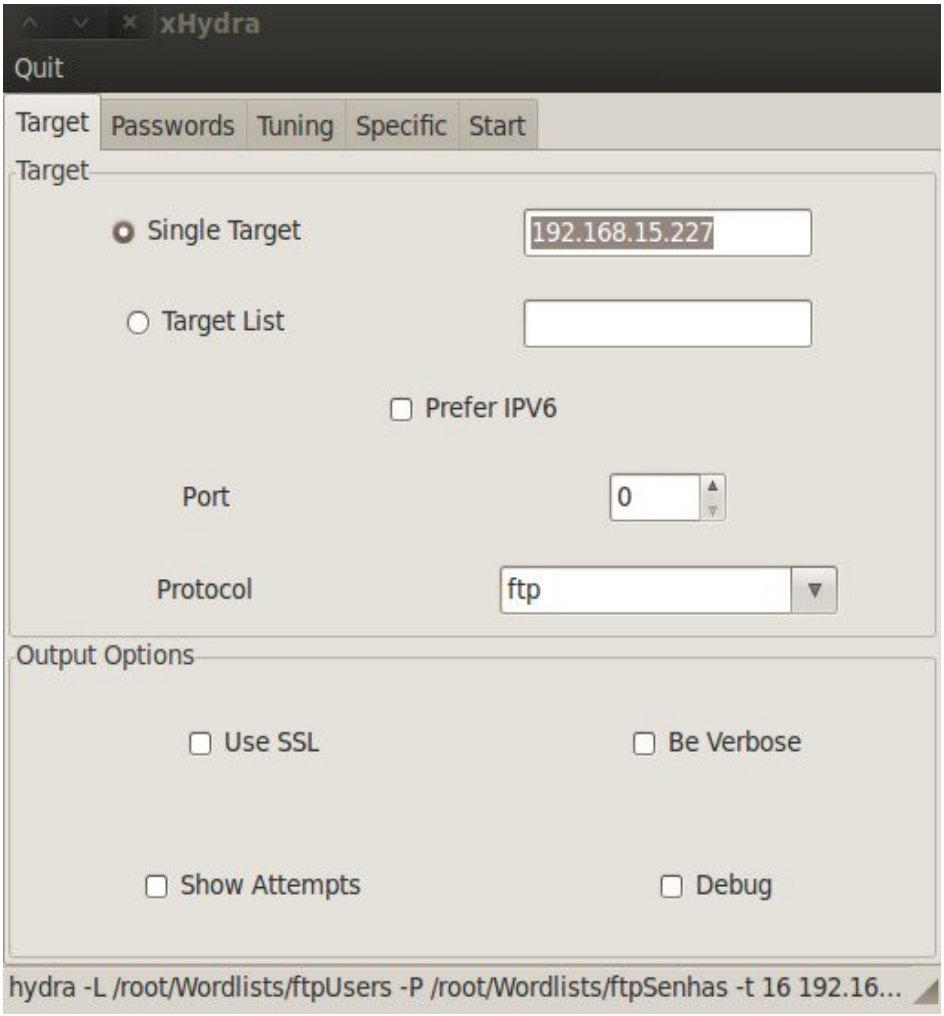

Figura 22 – Especificação de endereço IP utilizando-se a ferramenta xHydra.

Conforme exibido anteriormente na Figura 22 é selecionada a caixa de marcação "*Single Target*" e especificado o endereço IP "192.168.15.227". O próximo passo então é a definição da lista de usuários e senhas na guia "*Passwords*", conforme exibido na figura seguinte.

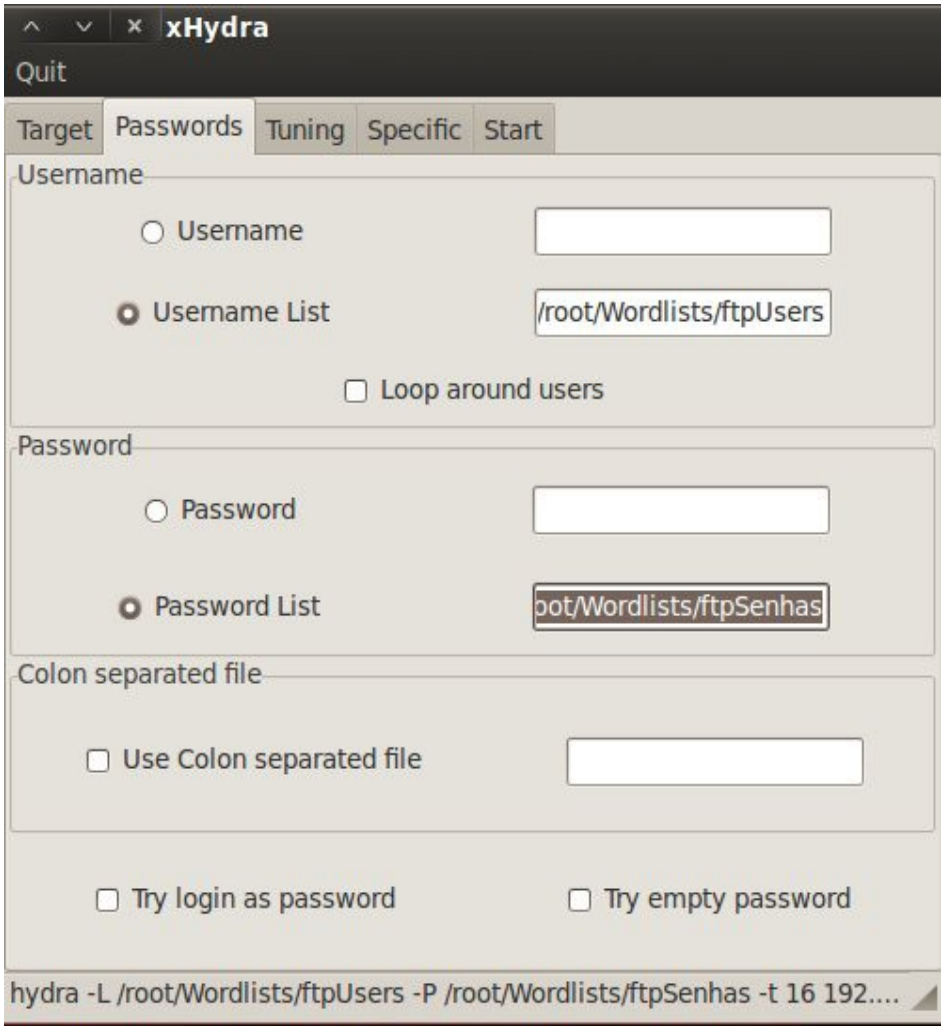

Figura 23 – Definição de Wordlists de usuários e senhas utilizando-se a ferramenta xHydra.

Uma vez definidas as *Wordlists* de usuários e senhas o último passo então é o início da obtenção de acesso ao clicar sobre o botão “Start”.

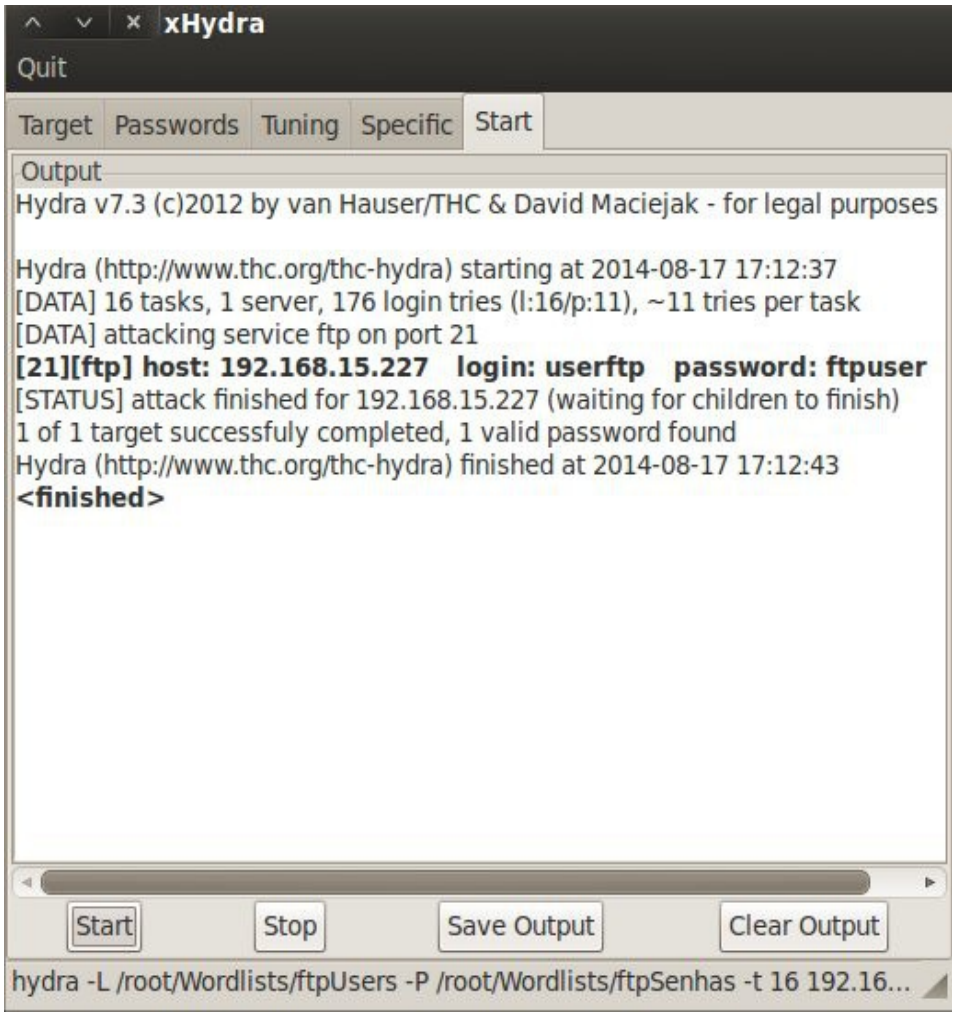

Figura 24 - Conclusão de obtenção de acesso utilizando-se a ferramenta xHydra.

Uma vez que o botão "*Start*" é selecionado dentro de alguns segundos já é possível obter-se o usuário "userftp" e a senha "ftpuser". É importante ressaltar que esta quebra de senha pode ocorrer de um modo muito mais demorado, uma vez que todo este processo depende do nível de complexidade de senhas e do tamanho das *Wordlists* e do processamento da máquina. Neste exemplo foram utilizadas *Wordlists* de baixa complexidade, o que resultou em uma instantânea quebra de senha.

5.5. MEDUSA

A ferramenta Medusa também possui a finalidade de quebrar senhas no modo de força bruta, assim como a ferramenta xHydra. Conforme GIAVAROTO et al. (2013) informa, sua sintaxe de funcionamento ocorre por meio do terminal de comandos, na seguinte forma:

"Medusa [-h host |-H arquivo de hosts] [-u nome de usuário |-U arquivo de usuários] [-p senha|-P arquivo de senhas] [-C arquivo] -M module [Opção]"

GIAVAROTO et al. (2013) informa ainda que os parâmetros “-h” e “-H” significam respectivamente um endereço de Host ou arquivo de Hosts, assim como “-u” e “-U” significam um nome de usuário ou um arquivo de usuários. A mesma sequência é válida para os parâmetros “-p” e “-P” que equivalem respectivamente a senha e arquivos de senhas.

O parâmetro “-C” corresponde a uma especificação composta do tipo “host:usuario:senha”, sendo que se um dos parâmetros faltar o mesmo deve ser especificado conforme mostrado anteriormente. Por fim o parâmetro “-M” corresponde ao módulo a ser especificado no comando, como por exemplo ftp, ssh http etc.

No exemplo a seguir, assim como no exemplo utilizado na ferramenta xHydra, é demonstrado como efetuar a obtenção de acesso a um servidor ftp, que se encontra vulnerável com a porta 21 (ftp) aberta.

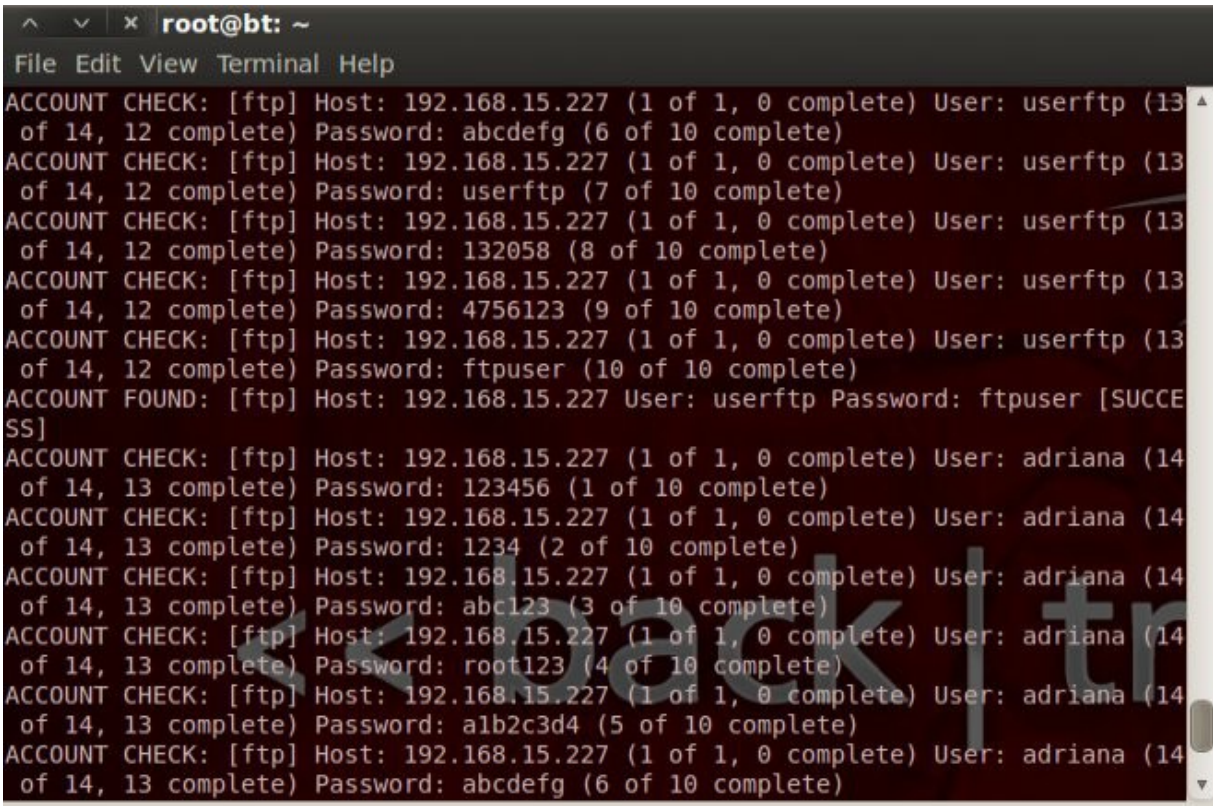

Figura 25 – Obtenção de acesso ao servidor ftp de um alvo utilizando-se a ferramenta Medusa.

O comando utilizado no exemplo anterior da Figura 25 é “medusa -h 192.168.15.227 -n 21 -U /root/Wordlists/ftpUsers -P /root/Wordlists/ftpSenhas -M ftp”. Observa-se que logo é possível descobrir o usuário “userftp” e a senha “ftpuser”.

No final deste capítulo vale ressaltar a importância de sempre utilizar um sistema operacional seguro, e que esteja sempre atualizado. Qualquer tipo de vulnerabilidade ativa no sistema em questão, seja por falha do sistema operacional ou algum software em execução, ou até mesmo uma simples porta aberta conforme mostrado no exemplo anterior, caracteriza a abertura de muitas possibilidades de algum acesso indesejado.

6 – METASPLOIT FRAMEWORK

6.1. INTRODUÇÃO

Em sequência ao quinto capítulo sobre Vulnerabilidades, este capítulo tem como propósito abordar a ferramenta Metasploit Framework, exemplificando o uso da mesma em um processo de obtenção de acesso a uma máquina com vulnerabilidades presentes. Conceitos básicos para um melhor entendimento do Metasploit Framework como Exploit, Payload e Shellcode são definidos.

6.2. DEFINIÇÃO

Metasploit Framework é uma ferramenta de grande utilidade quando o assunto em questão é obtenção de acesso a um determinado sistema e é bastante utilizada por profissionais de segurança. Conforme GIAVAROTO et al. (2013) informa, a ferramenta foi desenvolvida por HD Moore, especialista em segurança, teve sua primeira versão escrita em Perl e foi lançada em Outubro de 2003, tendo em Abril de 2004 uma nova versão 2.0, totalmente reescrita em Ruby, contando com 19 exploits e alguns payloads. Já em 2009 a empresa Rapid7 adquiriu o projeto Metasploit e a ferramenta ganhou força da comunidade envolvida em segurança da informação, estando atualmente na versão 4.

Para um bom entendimento da ferramenta Metasploit Framework, conforme GIAVAROTO et al. (2013) informa é importante ter ciência sobre os conceitos de Exploit, Payload e Shellcode.

• Exploit: é um código de programação com o objetivo de explorar vulnerabilidades existentes em um determinado sistema operacional ou programa em execução. São desenvolvidos habitualmente por hackers e pesquisadores da área de segurança.

• Payload: é a implementação do conceito do código no sistema alvo definido. Uma vez que o código seja executado no sistema alvo será possível a abertura de um canal de comunicação com o atacante.

• Shellcode: é um código executado após a falha explorada pelo exploit, que retornará um payload.

6.3 MSFCONSOLE

Msfconsole ou Metasploit é a ferramenta Metasploit Framework no modo texto. De acordo com PRITCHETT et al. 2012, Msfconsole além de desempenhar sua função principal de lançar exploits contra um alvo definido, é utilizado primariamente para gerenciar a base de dados do Metasploit, gerenciar sessões, configurar e lançar módulos de Metasploit novos. O acesso ao Msfconsole pode ser realizado por meio do menu Applications > BackTrack> Exploitation Tools > Network Exploitation Tools > Metasploit Framework > armitage, ou por meio do comando "./pentest/exploits/framework/msfconsole" a ser executado no terminal do Backtrack 5 R3. Informações sobre o Msfconsole podem ser obtidas também ao informar o comando "msfconsole -h" no terminal do Barcktrack 5 R3.

6.4 ARMITAGE

Armitage conforme GIAVAROTO et al. (2013) declara em seu livro é uma interface gráfica da ferramenta Metasploit Framework, que disponibiliza também um console para a execução de códigos no modo texto. Sua interface é bastante amigável, o que permite ao atacante ter uma visão mais simplificada das opções que o Metasploit Framework pode oferecer. O acesso ao Armitage pode ser feito por meio do menu Applications > BackTrack > Exploitation Tools > Network Exploitation Tools > Metasploit Framework > armitage, ou por meio do comando "./pentest/exploits/framework/armitage" a ser executado no terminal do Backtrack 5 R3. Informações adicionais podem ser obtidas ao digitar o comando "*help*" no

Console da interface gráfica do Armitage, ou ao clicar sobre o menu Help > Tutorial na interface gráfica do Armitage.

Ao acessar a ferramenta Armitage, caso o servidor RPC do Metasploit Framework não esteja em execução, poderá haver uma solicitação de execução do mesmo. Caso isto ocorra basta aceitar a solicitação ao clicar sobre o botão "*Yes*" conforme é exibido na figura seguinte.

Figura 26 – Solicitação de execução do servidor Metasploit Framework.

Em seguida haverá uma solicitação de conexão, e basta deixar as opções padrão como estão e aceitar a conexão ao clicar sobre o botão *"Connect",* conforme exibido na figura abaixo:

Figura 27 – Solicitação de conexão ao Servidor RPC do Metasploit Framework.

Uma vez aceita a conexão, o Armitage irá se conectar ao Servidor RPC do Metasploit

Framework e então entrará em execução.

No exemplo seguinte é demonstrada a obtenção de acesso a máquina virtual Linux Metasploitation 2, que possui várias falhas e vulnerabilidades servindo como objeto de estudo para profissionais da área de segurança. Esta máquina virtual pode ser encontrada para download no seguinte link:

"http://sourceforge.net/projects/metasploitable/files/Metasploitable2/metasploitable-linux-2.0.0.zip/download"

Para a instalação da mesma é necessário o download do software de virtualização "Oracle VM Virtual Box" que pode ser encontrado para download no link "https://www.virtualbox.org/wiki/Downloads". Para realizar o download basta escolher a versão correspondente ao sistema operacional em execução.

Em seguida considerando que o software de virtualização Oracle esteja configurado, e a máquina virtual da distribuição Linux Metasploitation 2 esteja criada e configurada na mesma rede em que a distribuição Linux Backtrack 5 R3 estiver em execução, o próximo passo é acessar o Armitage seguindo os passos anteriores de execução da ferramenta.

Uma vez que o Armitage esteja em execução é necessário que a ferramenta identifique a máquina a ser invadida. Para isto basta adicionar o endereço IP correspondente a máquina manualmente por meio do menu "*Hosts*" > "*Add Host*", ou utilizar-se de uma outra opção, que é a verificação de *Hosts* ativos, através do Nmap por meio do menu Hosts > Nmap Scan e bastando selecionar o tipo de escaneamento desejado. Na figura a seguir é exibida a ferramenta Armitage com os *Hosts* Ativos identificados.

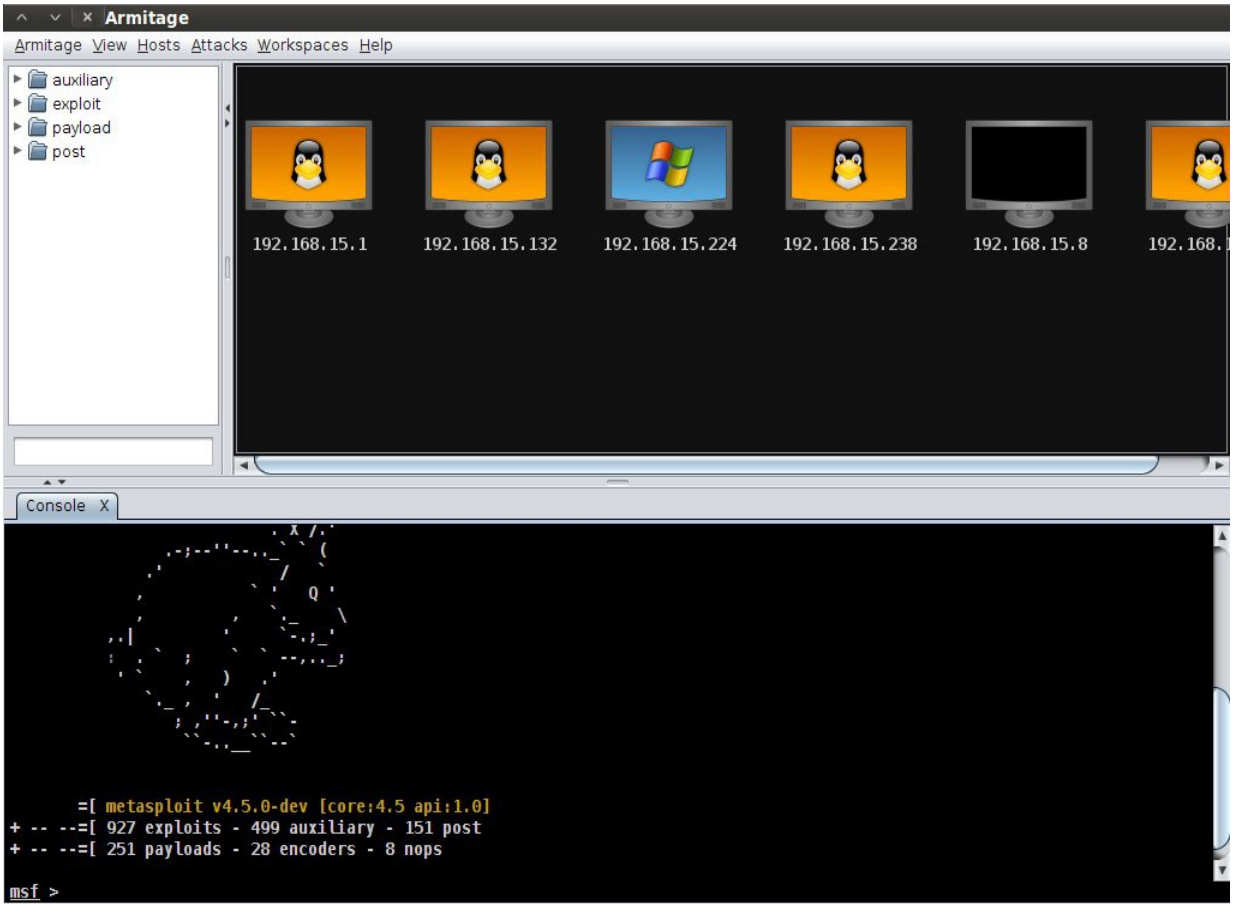

Figura 28 – Identificação de *Hosts* ativos pela ferramenta Armitage.

Observa-se que na Figura 28 exibida acima são identificados os *Hosts* ativos da sequência de endereços IP's “192.168.15.*”. O alvo a se obter acesso em questão possui o endereço IP “192.168.15.238”. Para dar início ao processo de invasão é necessário clicar sobre o menu do *Armitage Attacks* > *Find Attacks*, e então são identificados possíveis ataques a serem realizados em cada um dos *Hosts* ativos.

Identificados possíveis ataques ao alvo de endereço IP “192.168.15.238” o próximo passo é selecionar o tipo de ataque adequado, ao clicar com o botão direito do mouse sobre o computador correspondente ao endereço “192.168.15.238” e selecionar a opção *Attack* > *Samba* > *usermap_script*, conforme exibido na figura seguinte.

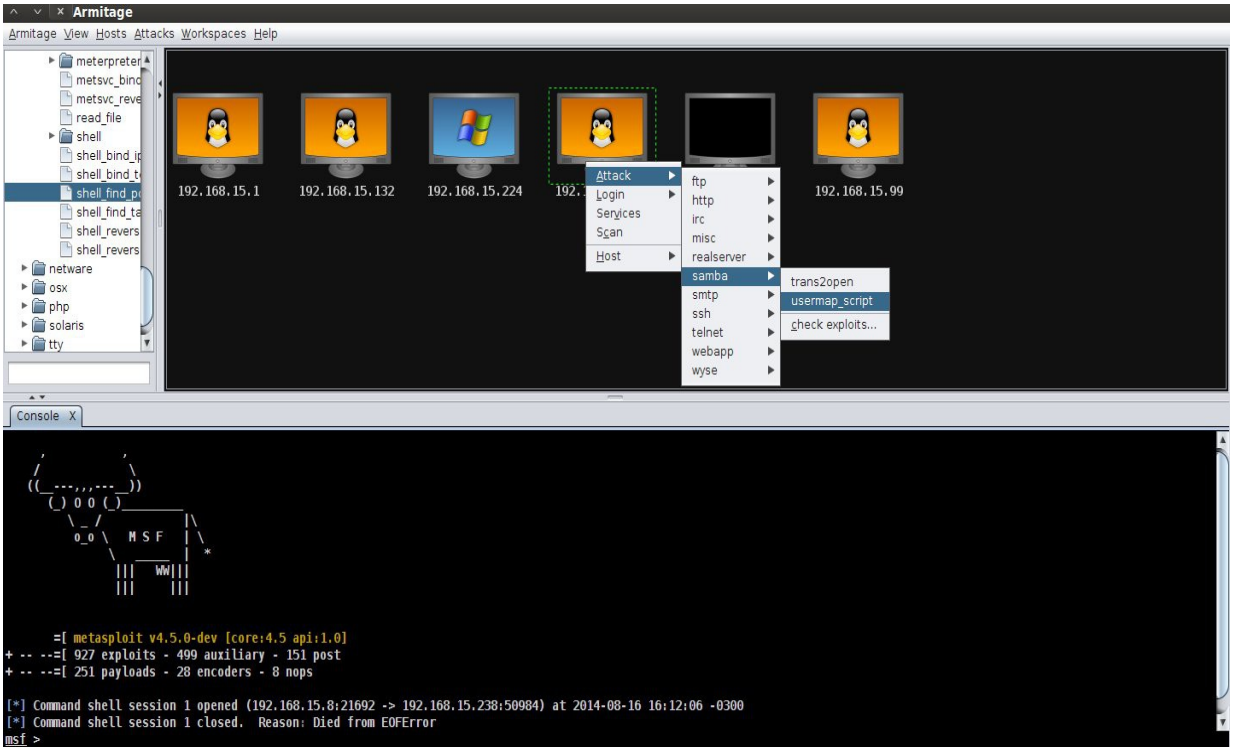

Figura 29 – Seleção de ataque ao alvo 192.168.15.238 utilizando-se a ferramenta Armitage.

O ataque *usermap_script* explora uma vulnerabilidade no processo de autenticação de usuários do servidor de arquivos Samba na versão 3.0.20. Uma vez selecionado o ataque *usermap_script*, é necessário marcar a caixa de seleção "*Use a reverse connection*" e então clicar sobre o botão "*Launch"* conforme exibido na figura seguinte para dar início ao processo de ataque.

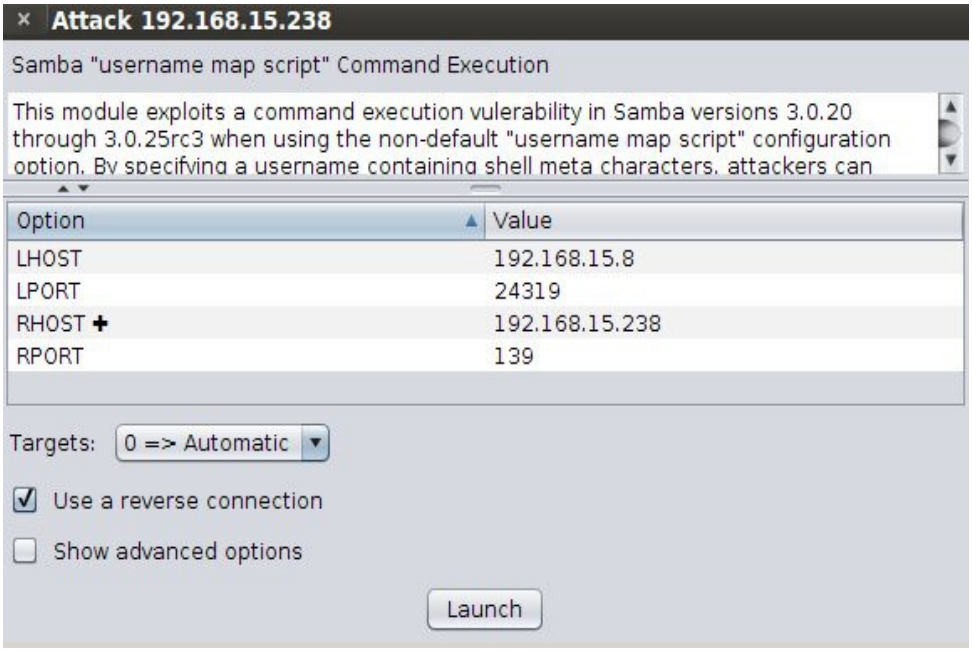

Figura 30 – Lançamento do ataque “username map script” utilizando-se a ferramenta Armitage.

Uma vez executado o último procedimento, o processo de ataque estará concluído, restando ao atacante apenas escolher o que fazer diante das opções da vulnerabilidade “*username map script*”. Uma boa opção oferecida por esta vulnerabilidade é a possibilidade de execução do terminal de comandos da máquina alvo. Para isto basta clicar sobre o botão direito sobre o computador correspondente ao endereço “192.168.15.238” e selecionar a opção *Attacks* > *Shell 1*. Em seguida é exibido o terminal de comandos do alvo selecionado, conforme exibido na figura a seguir.

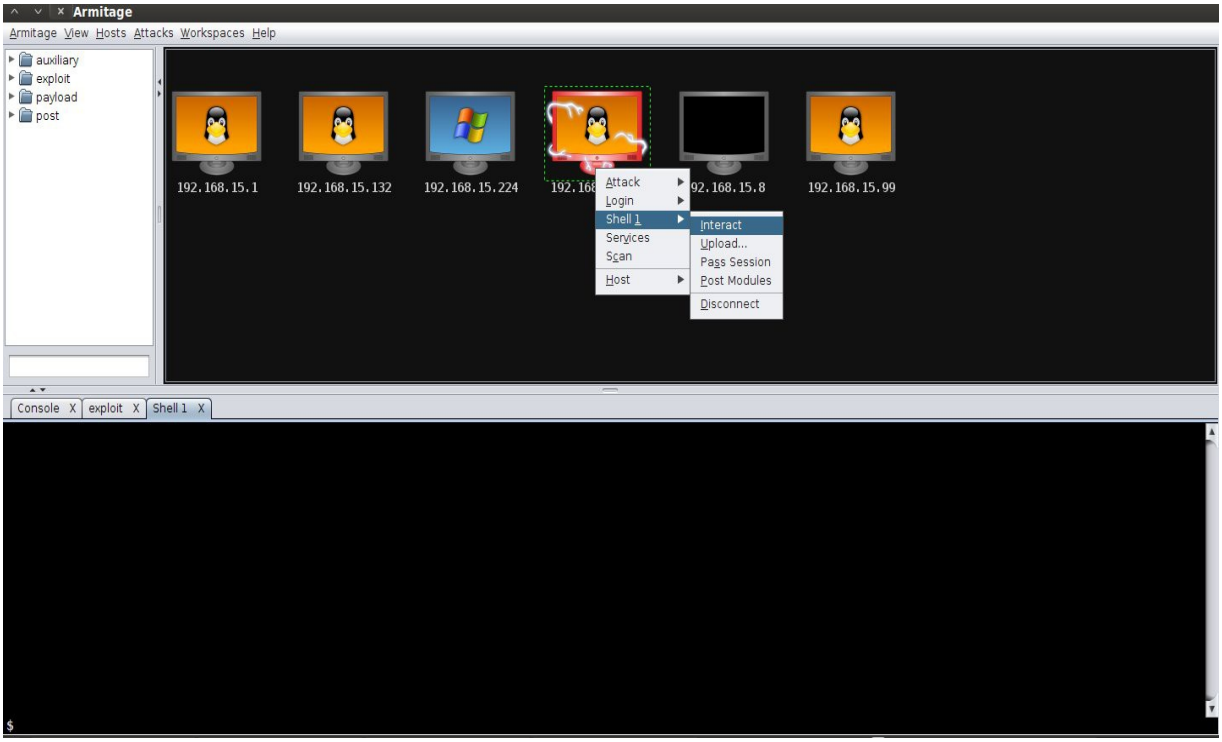

Figura 31 – Abertura do terminal de comandos do alvo 192.168.15.238 utilizando-se o Armitage.

Com o terminal de comandos *Shell* 1 aberto pela ferramenta Armitage é possível ter controle sobre a máquina alvo “192.168.15.238”. Observa-se que neste tipo de ataque ainda existem outras opções como por exemplo a de *upload* de arquivos da máquina alvo.

Uma opção interessante e prática de se utilizar da ferramenta Armitage é o ataque “Hail Mary”. Este tipo de ataque procura *exploits* relevantes aos *Hosts* ativos no Armitage automaticamente. Para executá-lo é necessário apenas navegar ao menu “*Attacks”* e selecionar a opção “*Hail Mary”*, e a busca por *exploits* relevantes a cada Host é iniciada automaticamente.

Ao final deste penúltimo capítulo é importante ressaltar o enorme potencial e o grande número de possibilidades que a ferramenta Metasploit Framework possibilita. Deve-se levar em conta que os tipos e formas de ataque não se resumem apenas nos demonstrados neste capítulo.

7– CONCLUSÃO

Diante do exposto neste trabalho é possível ao leitor obter uma boa noção sobre a aplicabilidade e o funcionamento de algumas das inúmeras ferramentas contidas na distribuição Linux Backtrack 5 R3, e também sobre como profissionais da área de segurança e analistas de rede desempenham seu trabalho de modo geral. É possível perceber também como é importante a utilização de um sistema operacional seguro, que esteja sempre atualizado, a fim de evitar ao máximo a presença de vulnerabilidades ativas no sistema em questão.

É perceptível também a importância de estar sempre com servidores DNS bem configurados de modo a evitar transferências de zona, a fim de evitar a divulgação de informações importantes e relevantes sobre o servidor em questão. Utilizando-se senhas de alta complexidade com uma ampla variedade de caracteres e de grande tamanho, é possível perceber como isto dificulta e aumenta consideravelmente o tempo de espera no processo de quebra de senhas.

Ao utilizar-se a ferramenta Metasploit Framework é notável como a detecção de vulnerabilidades presentes em um sistema alvo combinadas com a ação de *exploits* desenvolvidos especificamente para exploração das mesmas, representa uma maior precisão na efetivação de ataques que utilizam-se destas vulnerabilidades.

A distribuição Linux Backtrack 5 R3 é riquíssima em utilidades, dispondo de ferramentas de amplas finalidades, podendo desempenhar várias funções. É possível ao usuário ter o respaldo de arquivos de ajuda da própria ferramenta e de vários materiais que podem ser encontrados na Internet de modo geral, principalmente em fóruns sobre a área de segurança onde são discutidos assuntos do gênero. Cita-se como exemplo o *site* do Backtrack Linux “http://www.backtrack-linux.org/” que possui tutorias sobre várias ferramentas e um fórum de discussão.

As referências deste trabalho expõem um material mais avançado, com mais ferramentas que o Bracktrack 5 R3 possui. O exposto neste trabalho permite a realização de trabalhos futuros com um maior aprofundamento no uso das ferramentas apresentadas aqui, bem como a apresentação de novas ferramentas do mesmo gênero. É importante ressaltar que a distribuição Backtrack 5 R3 Linux foi descontinuada, sendo substituída por sua sucessora chamada Kali Linux, que apresenta um upgrade geral do Backtrack 5 R3 e suas ferramentas.

REFERÊNCIAS

BEGOSSO, Raíssa Helena. “Computação Forense”, Fundação Educacional do Município de Assis -FEMA, TCC – 2010

DRAVET, J. “Cracking Passwords Version 1.1 ”. Disponível em: <http://www.backtrack-linux.org/forums/showthread.php?t=68>. Acesso em: 23 jul. 2014

GIAVAROTO, Sílvio César Roxo; SANTOS, Gerson Raimundo dos. “Backtrack Linux – Auditoria e Teste de Invasão em Redes de Computadores”. Rio de Janeiro: Editora Ciência Moderna Ltda., 2013

GUETTA , Riccardo; TOLEDO, Juan. EtherApe. Disponível em: <http://etherape.sourceforge.net/>. Acesso em: 08 ago. 2014

MELLO, Rodrigo. Administração de Redes Linux - Módulo 4 - DNS (Domain Naming System) . Disponível em: <http://www.youtube.com/watch?v=800XyiRIAf8>. Acesso em: 15 set. 2014

PAES, Thiago. Como criar uma wordlist com crunch para usar em redes wireless WPA utilizando o Back Track Linux. Disponível em: <http://www.youtube.com/watch?v=VusErwFM5w0>. Acesso em: 15 set 2014

PRITCHETT, Willie; SMET, David de. Backtrack 5 Cookbook. Birmingham, B3 2PB, UK : Packt Publishing Ltd. , 2012

SALVATORE, Sanfilippo. Hping. Disponível em: <http://www.hping.org/>. Acesso em: 17 mar. 2014

SHAKEEL, Ali; HERIYANTO, Tedi. BackTrack 4: Assuring Security by Penetration Testing. Birmingham, B27 6PA, UK: Packt Publishing Ltd. , 2011

VIEIRA, Luiz. Rainbow Crack e Rainbow Tables. Viva o Linux. Disponível em: <http://www.vivaolinux.com.br/artigo/Rainbow-Crack-e-Rainbow-Tables>. Acesso em: 16 jul. 2014