Fundação Educacional do Município de Assis
IMESA - Instituto Municipal de Ensino Superior de Assis

VINÍCIUS MARQUESINI TERZI

UM ESTUDO DE SEGURANÇA DA INFORMAÇÃO NO PROJETO REDE CIRANDA

2015

ASSIS – SP

Avenida Getúlio Vargas, 1200 – Vila Nova Santana – Assis – SP – 19807- 634
Fone/Fax: (0XX18) 3302 1055 – homepage: www.fema.edu.br

Fundação Educacional do Município de Assis
IMESA - Instituto Municipal de Ensino Superior de Assis

UM ESTUDO DE SEGURANÇA DA INFORMAÇÃO NO PROJETO REDE CIRANDA

Trabalho de Conclusão de Curso apresentado ao curso de Bacharelado em Ciência da Computação ao Instituto Municipal de Ensino Superior de Assis – IMESA e a Fundação Educacional do Município de Assis – FEMA, como requisito do Curso de Graduação.

ORIENTANDO: VINÍCIUS MARQUESINI TERZI

ORIENTADOR: DR. ALMIR ROGÉRIO CAMOLESI

2015

ASSIS – SP

FICHA CATALOGRÁFICA

TERZI, Vinícius Marquesini
Um estudo de Segurança da Informação no Projeto Rede Ciranda – Fundação Educacional do Município de Assis – FEMA – Assis, 2015.
78 p.

Orientador: Dr. Almir Rogério Camolesi
Trabalho de Conclusão de Curso – Instituto Municipal de Ensino Superior de Assis – IMESA.

1. Segurança da Informação 2. Rede Ciranda 3.Kali Linux 4.Penetration Testing

CDD: 001.6
Biblioteca da FEMA

UM ESTUDO DE SEGURANÇA DA INFORMAÇÃO NO PROJETO REDE CIRANDA

VINÍCIUS MARQUESINI TERZI

Trabalho de Conclusão de Curso apresentado ao Instituto Municipal de Ensino Superior de Assis, como requisito do Curso de Graduação, analisado pela seguinte comissão examinadora:

Orientador: Dr. Almir Rogério Camolesi

Analisador: Me. Fábio Eder Cardoso

ASSIS

2015

DEDICATÓRIA

À minha família, amigos e todos que contribuíram de alguma forma para que eu pudesse realizar meu trabalho.

AGRADECIMENTOS

Agradeço primeiramente pela minha saúde e sabedoria, essenciais para meu desenvolvimento pessoal.

Agradeço também meus pais e meu irmão, por contribuírem me apoiando nos momentos em que mais precisei me dando força para seguir sempre adiante.

Aos meus amigos e namorada que fizeram parecer que todas as dificuldades enfrentadas eram apenas mais uma simples barreira das quais ultrapassei e terei de ultrapassar no decorrer da minha vida.

Ao Projeto Rede Ciranda e sua equipe de TI, que me passaram muito conhecimento e me deram oportunidade e confiança para que eu pudesse realizar este trabalho.

Por fim, agradeço ao meu orientador Dr. Almir Rogério Camolesi, que me mostrou o caminho exato para que meu trabalho fosse realizado com sucesso.

Podemos ir longe, se começarmos de muito perto. Em geral começamos pelo mais distante, o "supremo princípio", "o maior ideal", e ficamos perdidos em algum sonho vago do pensamento imaginativo. Mas quando partimos de muito perto, do mais perto, que é nós, então o mundo inteiro está aberto — pois nós somos o mundo. Temos de começar pelo que é real, pelo que está a acontecer agora, e o agora é sem tempo.

Jiddu Krishnamurti

RESUMO

Em uma era globalizada onde quase tudo é movido por meio das novas tendências tecnológicas, as empresas estão cada vez mais preocupadas com a segurança do seu ambiente computacional e temem que suas valiosas informações sejam expostas, então, investem no mercado de segurança e uma boa parcela adere ao teste de penetração.

A realização dos testes segue um escopo pré-definido e são realizados pelo hacker ético que atua de forma semelhante a intrusos hostis, porém de forma legal e autorizada. Após a realização dos testes, tudo é documentado por meio de relatórios para que depois, as correções julgadas necessárias possam ser executadas.

Este trabalho tem por objetivo realizar um estudo prático e real sobre a aplicação dos conceitos de Segurança da Informação no Projeto Rede Ciranda.

Palavras-chave: Segurança da Informação; Rede Ciranda; Kali Linux; Teste de Penetração.

ABSTRACT

In a globalized era where almost everything is moved by means of new technological trends, companies are increasingly concerned about the security of your computing environment and are concerned that their valuable information is exposed, then invest in the security market and a good portion sticks the penetration test.

The performance of tests following a pre-defined scope and are made by the ethical hacker who acts similarly to hostile intruders, but a legal and authorized manner. After the tests, everything is documented by reports that after the necessary corrections deemed to be executed.

This study aims to realize a practical and real study on the implementation of the Information Security concepts in Projeto Rede Ciranda.

Keywords: Information Security; Rede Ciranda; Kali Linux; Penetration test.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

ABNT - Associação Brasileira de Normas Técnicas

APAE - Associação de Pais e Amigos dos Excepcionais

C|EH - Certified Ethical Hacker

CAPSA - Círculo dos Amigos dos Pobres do Pão de Santo Antônio

CCSC - Commercial Computer Security Center

CMDCA – Conselho Municipal da Criança e do Adolescente

CPD - Centro de Processamento de Dados

HTTP - Hypertext Transfer Protocol

IP – Internet Protocol

ISO – International Standards Organization

JSP - JavaServer Pages

SER - Serviço Especial de Reabilitação

SGBD – Sistema Gerenciador de Banco de Dados

SI – Segurança da Informação

SSH - Secure Shell

TCP - Transmission Control Protocol

TI – Tecnologia da Informação

UDP - User Datagram Protocol

Sumário

1 INTRODUÇÃO

Na época em que as informações eram armazenadas apenas em papel, a segurança era relativamente simples. Bastava trancar os documentos em algum lugar e restringir o acesso físico àquele local. Com as mudanças tecnológicas, a estrutura de segurança ficou um pouco mais sofisticada e com a chegada dos computadores pessoais e das redes que conectam o mundo inteiro, os aspectos de segurança atingiram tamanha complexidade que há a necessidade de desenvolvimento de equipes e de métodos de segurança cada vez mais sofisticados.

Nos dias atuais é comum ouvir falar em ataques, invasões à servidores e sistemas. Quando não são implementadas as medidas básicas de segurança, estes podem apresentar diversas vulnerabilidades.

Segundo a ABNT NBR ISO/IEC 27002 (2007), a informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegida.

A ISO/IEC 17799 (2005), em sua seção introdutória, define segurança da informação como “a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio”. Assim, define-se segurança da informação como a área do conhecimento que visa à proteção da informação das ameaças a sua integridade, disponibilidade e confidencialidade a fim de garantir a continuidade do negócio e minimizar os riscos.

Com o aumento das atividades on-line a segurança precisa se adequar aos novos tempos para fornecer facilidades de uso seguro e assumir o uso mais responsável da tecnologia, comprometendo-se com sua integridade digital. A segurança da informação não é apenas uma atitude, uma pessoa ou um produto, são modelos que, se implementados em conjunto vão garantir a segurança das redes e da informação nas empresas.

As técnicas e os métodos de proteção são variados e mudam de acordo com a evolução das ameaças, mas podemos definir algumas medidas e ferramentas básicas para a segurança de ambientes computacionais, como, manter o sistema operacional atualizado, efetuar *backup* dos arquivos, usar antivírus e implementar um *firewall*. Entretanto, quando se pensa em medidas para proteção dos recursos computacionais, deve haver um compromisso entre a funcionalidade e a segurança.

Muitas empresas estão sujeitas a encarar o extravio de informações, seja por descuido ou outros tipos de ações maléficas. Alguns desses eventos podem ser poupados quando se possui boas normas e medidas para segurança dessas informações.

Desta forma, fica clara a necessidade de analisar vulnerabilidades, criar e adotar normas e processos para obter uma maior segurança dentro de qualquer organização.

1.1 Objetivo geral

Este trabalho visa mostrar o atual valor da informação, a necessidade do uso das tecnologias da informação, a importância com a Segurança da Informação e as principais medidas que devem ser tomadas para se obter uma boa Segurança da Informação dentro de uma empresa, utilizando o Projeto Rede Ciranda como base para a realização dos estudos práticos.

1.2 Objetivos específicos

Para alcançar o objetivo geral serão realizados testes de penetração no servidor do Projeto Rede Ciranda, visando mostrar a importância da Segurança da Informação, os riscos com sua ausência e quais os principais recursos para garantir uma assertiva Segurança da Informação dentro de uma empresa.

Por fim, apresentar propostas para que futuramente, estas sejam implementadas com intuito de tornar a infraestrutura tecnológica do Projeto Rede Ciranda cada vez mais segura em relação às suas informações.

1.3 Justificativa

Hoje, empresas buscam saídas práticas e efetivas para aperfeiçoar suas atividades e garantir segurança nos seus mecanismos de trabalho. Por isso, é necessária para qualquer organização a criação de uma política de segurança formal, clara e objetiva, com foco nas necessidades da empresa.

1.4 Motivação

O assunto em questão é uma necessidade da maioria das empresas, seja ela de pequeno, médio ou grande porte. Portanto, a realização desse estudo é de grande valia porque é uma questão muito procurada por diversas organizações. Uma empresa que não possui políticas de segurança apresenta muitas desvantagens em relação àquelas que possuem.

No Projeto Rede Ciranda, não há nenhum documento ou informações comprovando que foram realizados investimentos em segurança da informação. Por isso, a elaboração desse trabalho se torna extremamente importante para que a infraestrutura tecnológica deste Projeto se torne fisicamente segura em relação às suas informações.

1.5 Perspectivas de contribuição

No Projeto Rede Ciranda há uma constante troca e admissão de novos estagiários para ocuparem os cargos no setor de TI. Então, a elaboração de uma política de

segurança é importante para que esses estagiários a sigam com os devidos cuidados, evitando futuros problemas relacionados às informações.
Esse estudo também tem uma proposta que visa facilitar a implantação de políticas de segurança da informação no Projeto, seguindo todos os passos para que essas medidas correspondam com suas necessidades.

1.6 Metodologia

Com base nos conhecimentos adquiridos nesta área, foi elaborado um documento contendo políticas de segurança da informação para o Projeto Rede Ciranda, com o objetivo de conscientizar os funcionários sobre o assunto e evitar descuidos que possam comprometer os serviços disponibilizados. Posteriormente, foi realizado um estudo para utilizar ferramentas específicas com intenção de testar a vulnerabilidade do servidor Rede Ciranda, sempre buscando respostas para uma melhoria de sua segurança.

1.7 Recursos necessários

Para a realização dos testes de vulnerabilidades do servidor e nos sistemas Rede Ciranda, foi necessário o estudo de algumas ferramentas específicas do Kali Linux[1], para executar esses testes com prudência.

1.8 Estrutura do trabalho

O trabalho está dividido em cinco capítulos, sendo eles:

[1] Kali Linux é uma avançada distribuição Linux especializada em testes de intrusão e auditoria de segurança. Possui mais de trezentas ferramentas e testes de intrusão. Disponível em: https://www.kali.org/

Capítulo 1 – **Introdução.** Neste capítulo é apresentada a contextualização do trabalho, introduzindo os conceitos de informação, segurança da informação, as normas ISO e os recursos que serão utilizados no decorrer da pesquisa e testes.

Capítulo 2 – **Segurança da Informação.** O capítulo trás o conceito de segurança da informação, abrangendo principalmente o uso dela dentro de uma organização. Como implantá-la, estabelecer políticas e medidas.

Capítulo 3 – **Conceitos de teste de penetração e suas ferramentas.** Este capítulo apresenta o conceito e os objetivos dos testes de penetração. A diferença entre ameaças e vulnerabilidades. Os tipos de hackers existentes. Os tipos de testes de penetração existentes. E também, apresenta o Sistema Operacional Kali Linux, que será utilizado para a realização desses testes.

Capítulo 4 – **Estudo de Segurança da Informação no Projeto Rede Ciranda.** Neste capítulo será apresentado o Projeto Rede Ciranda da Criança e Adolescente de Assis, mostrando a importância deste Projeto e qual o seu papel na Rede de Atendimento à Criança e ao Adolescente, sua Infraestrutura de TI e os softwares desenvolvidos pelo Projeto. Também será descrita a situação atual da segurança da informação de sua infraestrutura tecnológica.

Capítulo 5 – **Aplicando os testes de penetração no Projeto Rede Ciranda.** Neste capítulo será descrita a realização da fase prática do trabalho, onde será utilizado todo o conhecimento adquirido sobre políticas de segurança e teste de penetração. Os testes seguem o escopo definido, mostram os resultados e algumas soluções para as vulnerabilidades encontradas.

Capítulo 6 – **Resultados e Conclusão.** Por fim, o capítulo 6, discorre sobre os benefícios que este estudo trará para o Projeto Rede Ciranda, mostrando a importância de se implantar medidas e técnicas de Segurança da Informação e apresenta os resultados obtidos pela pesquisa e testes que foram realizados com intuito de esclarecer e detectar vulnerabilidades, indicando a importância e as vantagens da adoção de medidas de segurança da informação dentro de uma organização.

Referências. Contêm todas as referências de livros, sites, artigos, e outros materiais de pesquisa que serão utilizados ao decorrer da elaboração de todo o trabalho e por fim o cronograma de atividades.

2 SEGURANÇA DA INFORMAÇÃO

Ao longo da história, desde a mais remota antiguidade, o ser humano vem buscando controlar as informações que julga serem importantes. Conforme relaciona Schneier (2001), na antiga China, a própria linguagem escrita era usada como uma forma de criptografia, porque somente as classes superiores podiam aprender a ler e a escrever. Outros povos como os egípcios e os romanos deixaram registrado na história sua preocupação com o trato de certas informações, especialmente as de valor estratégico e comercial. Com a Segunda Guerra Mundial, a questão da segurança ganhou uma nova dimensão na medida em que sistemas automáticos, eletromecânicos foram criados tanto para criptografar como para efetuar a criptoanálise e quebrar a codificação (Schneier, 2001).

Segundo (CARUSO, 1999):

> Tradicionalmente, as organizações dedicam grande atenção para com seus ativos tangíveis físicos e financeiros, mas relativamente pouca atenção aos ativos de informação que possuem. Em anos recentes, contudo, a informação assumiu importância vital para manutenção dos negócios, marcados pela dinamicidade da economia globalizada e permanentemente on-line, de tal forma que, atualmente, não há organização humana que não dependa da tecnologia de informações, em maior ou menor grau, de forma que o comprometimento do sistema de informações por problemas de segurança pode causar grandes prejuízos ou mesmo levar a organização à falência.

Como o uso de computadores vem crescendo rapidamente e muitas pessoas acessam informações, é importante que haja um cuidado para controlar o acesso de pessoas não autorizadas a tais informações. Nenhum sistema é totalmente seguro, e o que se tem para chegar o mais perto de torna-los seguros são várias medidas que se implementadas em conjunto podem diminuir tais problemas.

Visando minimizar esses riscos a ISO *(International Standartization Organization)*, publicou uma norma internacional para garantir a segurança das informações nas empresas.

A ABNT (Associação Brasileira de Normas Técnicas), operando em sintonia com a ISO e atenta tanto com as necessidades nacionais quanto com a segurança da informação, disponibilizou o projeto na versão brasileira da norma ISO para consulta pública. Percebe-se que, antes mesmo da publicação do documento oficial, as empresas brasileiras já se antecipavam no sentido de preparar suas estruturas para implementação dos itens que compõem a norma. Tal procedimento justifica-se na medida em que as empresas estão mudando seu comportamento quanto à questão da segurança da informação, premidas pelo risco crescente de roubos e ataques aos seus sistemas. Por outro lado, compreendem que as normas ISO e ABNT são o resultado de um esforço internacional que consumiu anos de pesquisa e desenvolvimento para obter um modelo de segurança eficiente e universal.

2.1 Surgimento das Normas de Segurança Informação

Os esforços nos quais resultaram a ISO17799 e a Norma ABNT remontam a 1987 quando o departamento de comércio e indústria do Reino Unido (*DTI*) criou um centro de segurança de informações, o CCSC *(Commercial Computer Security Center)* que dentre suas atribuições tinha a tarefa de criar uma norma de segurança das informações para companhias britânicas que comercializavam produtos para segurança de TI (Tecnologia da Informação) através da criação de critérios para avaliação da segurança (SOLMS, 1998).

Outro objetivo do CCSC era a criação de um código de segurança para os usuários das informações. Com base nesse segundo objetivo, em 1989 foi publicada a primeira versão do código se segurança, denominado PD0003 - Código para Gerenciamento da Segurança da Informação. Em 1995 esse código foi revisado e publicado como uma norma britânica (BS), a BS7799:1995. Em 1996, essa norma foi proposta ao ISO para homologação, mas foi rejeitada (HEFFERAN, 2000).

Uma Segunda parte desse documento foi criada posteriormente e publicada em novembro de 1997 para consulta pública e avaliação. Em 1998 esse documento foi publicado como BS7799-2:1998 e, após revisado, foi publicado junto com a primeira parte em abril de 1999 como BS7799:1999. (HEFFERAN, 2000) Em 1998 a lei britânica, denominada “Ato de Proteção de Dados”, recomendou a aplicação da norma na Inglaterra, o que viria a ser efetivado em 1º de março de 2000.

Ao longo de seu desenvolvimento, a norma foi sendo adotada não só pela Inglaterra como também por outros países da Comunidade Britânica, tal como Austrália, África do Sul e Nova Zelândia (SOLMS, 1998).

A parte 1 desse documento foi levada a ISO e proposta para homologação pelo mecanismo de "*Fast Track*" para um trâmite rápido, pois normalmente, uma norma leva até cinco anos para ser avaliada e homologada pela ISO.

Em outubro de 2000, na reunião do comitê da ISO em Tóquio, a norma foi votada e aprovada pela maioria dos representantes. Os representantes dos países do primeiro mundo, excetuando a Inglaterra, foram contrários a homologação, mas, sob votação, venceu a maioria, e a norma foi homologada como ISO/IEC 17799:2000 em 01 de dezembro de 2000.

2.2 Objetivos e Abrangência

A Segurança da Informação tem como objetivo básico proteger os dados que trafegam para assim garantir sua confidencialidade, a sua integridade e a sua disponibilidade.

O objetivo fundamental da norma ISO e da norma brasileira, nela baseada, é assegurar a continuidade e minimizar o dano empresarial prevenindo e minimizando o impacto de incidentes de segurança. (ISO/IEC 17799:2000).

Segurança da Informação é a proteção contra um grande número de ameaças às informações, de forma a assegurar a continuidade do negócio, minimizando danos comerciais e maximizando o retorno de investimentos e oportunidades. A segurança da informação é caracterizada pela preservação dos seguintes atributos básicos:

a) Confidencialidade: segurança de que a informação pode ser acessada apenas por quem tem autorização. Normalmente, isso é implementado a partir de um mecanismo de senhas ou de assinatura digital.

b) Integridade: certeza da precisão e completude da informação. Garantir que a informação chegue ao seu destino sem passar por nenhuma mudança em seu conteúdo em algum período de sua existência.

c) Disponibilidade: garantia de que os usuários autorizados tenham acesso à informação e aos recursos associados, quando necessário.

A preservação desses atributos constitui no paradigma básico da Norma Internacional para Gerenciamento da Segurança da Informação, a ISO e de toda a ciência da Segurança da Informação.

Em contrapartida, a certificação é uma forma bastante clara de mostrar à sociedade que a empresa dá a segurança de suas informações e de seus clientes a importância que merecem, de tal forma que se espera que em poucos anos todas as grandes empresas terão aderido a norma e obtido suas certificações como forma de não só assegurar sua sobrevivência mas também como parte do marketing de suas imagens junto ao público e como fator, mais um diferencial de competitividade no mercado.

2.3 Situação das empresas

Os cenários sociais, tecnológicos, educacionais e econômicos têm sofrido grandes mudanças com o surgimento de novas atividades, e ao mesmo tempo em que outras desaparecem, algumas são profundamente transformadas. As tecnologias de informação e comunicação estão tomando um espaço cada vez maior na sociedade, alterando de forma significativa os meios de produção e disseminação do conhecimento humano.

Antigamente nas décadas de 50 até 70, a segurança das informações e dos sistemas de computação de uma instituição não eram muito preocupantes devido ao limitado acesso que se tinha a esses estes recursos. Em relação aos sistemas, eles eram praticamente confinados ao ambiente interno e estavam protegidos de qualquer

acesso externo. Com a evolução das gerações da informática, o surgimento da microinformática (IBM-PC4), a facilidade na aquisição de computadores pessoais e o advento das redes de computadores, tornou-se possível uma integração das estruturas por meio das redes, um compartilhamento globalizado dos recursos (*networking*) e das informações (*internetworking*). A segurança das informações passou a ser uma área crítica, pois quanto maior a facilidade de acessa-las, maior a probabilidade de usuários externos compartilharem também desse acesso (NORTHCUTT,2001).

Com o crescimento do uso da informática e telecomunicações dentro das corporações, e sua integração com os usuários dessas facilidades, mudou-se o paradigma de segurança. Na época dos *mainframes*, quando ainda não existia a comunicação entre as redes, o objetivo central era a proteção dos dados dentro do CPD (Centro de Processamento de Dados) e a sua utilização em terminais sem capacidade de processamento e armazenamento local; era a época da segurança de dados.

Atualmente os ambientes são heterogêneos, as empresas possuem um parque de informática muito híbrido com equipamentos cujas velocidades, espaços de armazenamento, recursos e periféricos se diferenciam em entre as demais maquinas. Os riscos são diferentes nas diversas arquiteturas de computadores, de redes e ainda por cima com sistemas operacionais diferentes dentro do mesmo local. Existem novas ameaças, e as vulnerabilidades estão sempre aumentando. Dependemos não somente do computador local, mas da informação armazenada em lugares distantes e em várias mídias, desde *Compact Disc* até meios magnéticos, tais como discos rígidos redundantes e fitas com alta capacidade de armazenamento.

Uma pesquisa feita pela PwC[2] em 2014 revelou que, a análise das respostas colhidas com 9.600 executivos de 115 países sugere a utilização de antigos modelos para combater novas ameaças cada vez mais sofisticadas, o que resulta numa proteção pouco efetiva. E apesar de o investimento em segurança ter aumentado, nota-se que as empresas ainda se perdem na hora de definir as melhores práticas, têm dificuldade

[2] http://www.pwc.com.br/pt/publicacoes/servicos/consultoria-negocios/pesquisa-global-seguranca-informacao-14.jhtml

de conduzir analises situacionais e de identificar e priorizar os dados que precisam ser adequadamente resguardados. Poucas estão realmente preparadas para lidar com os riscos crescentes do ciberespaço (PwC, 2014).

Segundo (2014, PwC), “a pesquisa deste ano mostra que os incidentes de segurança detectados aumentaram 25% em relação ao ano anterior, enquanto os custos financeiros médios dos incidentes cresceram 18%”.

Isso nos mostra que as organizações costumam se fiar em estratégias de segurança do passado para travar uma batalha em geral ineficaz contra inimigos altamente qualificados que utilizam as ameaças e as tecnologias do futuro.

Segundo Oliveira (2014, PwC):

> “Não é possível combater as ameaças de hoje com as estratégias de ontem”, diz Viviane Oliveira, diretora da PwC. “É necessário um novo modelo de segurança da informação, que leve em consideração o conhecimento das ameaças do ciberespaço, dos ativos de informação e dos motivos e alvos dos potenciais atacantes.”

2.4 Importância da Segurança da Informação

Com a rápida evolução tecnológica, nenhum ambiente é totalmente seguro, para minimizar os riscos de ataques, diversas tecnologias devem ser empregadas.

O fácil acesso à Internet, tanto na empresa quanto no próprio domicilio, leva as pessoas a exigir uma forma mais segura e adequada para acessar a informação. Os ambientes corporativos estão se tornando extremamente complexos integrando vários sistemas operacionais, o que dificulta ainda mais o planejamento por parte dos administradores de redes. As informações geradas internamente precisam de tratamento muito cuidadoso antes de ser disponibilizadas.

A Segurança da Informação é um fator primordial na tomada de decisões e nos investimentos das empresas, tonando-se parte do próprio negócio. Grande parte das empresas tem orçamento específico para a área de tecnologia da informação e para

a área de segurança. Mas, ainda existem algumas empresas que deixam a segurança em segundo plano, e só dão a devida importância quando são invadidas e suas informações roubadas. Não recebendo a devida importância e sem a definição de uma boa estratégia de segurança, são utilizadas técnicas parciais ou incompletas que podem aumentar a vulnerabilidade da organização (NAKAMURA, 2007).

Os benefícios evidentes são: reduzir os riscos com vazamentos, fraudes, erros, uso indevido, sabotagem, roubo de informações e diversos outros problemas que possam comprometer os princípios básicos que norteiam a segurança de redes citadas acima. Esta política de segurança visa, também, aumentar a produtividade dos usuários em um ambiente mais organizado e com regras.

2.5 Implantação

O primeiro passo na busca de uma solução precisa em relação ao tema é a identificação do que realmente se deve proteger, de quem se está tentando proteger, qual a possibilidade real dessas ameaças, levantamento de dificuldades na implementação de medidas de proteção, nas quais protegerão de maneira efetiva os recursos importantes, e como será feito o processo contínuo de revisão com a finalidade de melhorar cada vez mais, e estar sempre em busca de identificar supostas fraquezas. Existe um velho axioma em segurança que diz: “o custo de se proteger contra uma ameaça deve ser menor que o custo da recuperação se a ameaça o atingir.” (DAVIS, 1997). Neste contexto, custo significa incluir perdas expressadas em moeda corrente real, reputação da empresa, confiança e outras medidas menos óbvias.

Com a integração de todos os serviços e sua disponibilização, a empresa poderá se tornar foco de tentativas de rompimento da segurança interna. Várias portas poderão ficar abertas caso não haja a preocupação constante com a política de proteção a ser implementada. As decisões que o administrador tomará vão determinar a vulnerabilidade na rede. A apresentação dos serviços que serão fornecidos, a facilidade de uso, o custo da segurança versus o risco da perda são os fatores mais importantes.

Uma política de segurança no ambiente corporativo se torna a expressão das regras pelas quais poderá ser fornecido o acesso aos recursos tecnológicos da empresa. O principal propósito será estabelecer tais regras, de que forma serão disseminadas e especificar através de quais mecanismos podem ser alcançadas. Outro propósito será determinar um ponto de referência a partir do qual se possa configurar e auditar os sistemas computacionais e as redes envolvidas, para que sejam adequados aos requisitos de segurança.

Os componentes a serem avaliados são: autenticação, acesso, privacidade, relatórios de violações, procedimentos de *backup* e recuperação, combate a vírus, monitoração e análise de dados, parte física, parte lógica, responsabilidades, manutenção de toda a estrutura de forma a não prejudicar as pessoas envolvidas no ambiente, guias de orientação para compra de tecnologias computacionais que especifiquem os requisitos ou características que os produtos deverão possuir correlacionados com segurança e um meio pelo qual os usuários dessa estrutura poderão relatar problemas e falhas (SCHNEIER,2001).

Empresas que estão preocupadas com a segurança e querem se preparar para implantar tais medidas, devem propor um documento com diretivas de segurança especifica para a organização; contextualizar os princípios de segurança da informação dentro da empresa; enfocar um estudo dentro da empresa sobre:

• confidencialidade — proteção da informação compartilhada contra acessos não autorizados;

• controle das operações individuais de cada usuário através do log;

• autenticidade – garantia que a informação não passe por modificações indesejadas;

• garantia da identidade dos usuários;

• integridade — garantia da veracidade da informação, alterações acidentais ou não autorizadas que podem corrompê-la;

• disponibilidade – garantia de que os usuários autorizados terão acesso à informação desejada com facilidade;

• prevenção de interrupções na operação de todo o sistema (hardware / software), ou seja, uma quebra do sistema não deve impedir o acesso aos dados.

3 CONCEITOS DE TESTE DE PENETRAÇÃO E SUAS FERRAMENTAS

Este capítulo aborda o conceito, os objetivos, as ferramentas e tudo que está relacionado aos testes de penetração e o Sistema Operacional Kali Linux, que será utilizado para a realização dos testes. E apresenta primeiramente os tipos de Hackers existentes.

3.1 Tipos de Hackers

No mundo da segurança computacional, existem alguns termos utilizados pelos especialistas para se referir aos *hackers*.

Segundo o livro Kali Linux – Introdução ao *Penetration Testing* (2015, p. 5):

> *Black Hat* ou *cracker* é um especialista que usa suas habilidades de forma maliciosa e para o mal; alguns exemplos são invasões não autorizadas, furto de informações, negações de serviço etc.
>
> *Gray Hat* é um termo que foi criado para qualificar um tipo de *hacker* que, na maioria das vezes atua dentro da lei, porém alguns de seus atos podem ser qualificados como estando às margens da lei.
>
> O *White Hat* ou *hacker* ético é um profissional com conhecimento na área de segurança computacional que utiliza suas habilidades para o bem, como por exemplo, o teste de penetração. Apesar de o *hacker* ético utilizar as mesmas ferramentas do *black hat*, ele as utiliza de forma ética e somente mediante autorização.

Este último é o tipo de *hacker* que se encaixa neste trabalho, possuindo permissão do superior do departamento de TI do Projeto Rede Ciranda.

3.2 Ameaças e vulnerabilidades

Os riscos associados à segurança da informação podem ser classificados em duas categorias: ameaças e vulnerabilidades. Ameaças são ações tomadas por pessoas que colocam em perigo a informação e infraestrutura da empresa. Vulnerabilidades são deficiências na infraestrutura e organização que expõem os riscos a eventos imprevistos e indesejáveis a empresa.

Ameaças e vulnerabilidades andam em conjunto. As ameaças são ações em potenciais que procuram seguir o caminho de menor resistência, ou seja, o caminho mais vulnerável.

3.2.1 Ameaças

A ameaça de segurança é a intenção da parte de alguém em causar dano a um indivíduo ou uma organização. Podem ser realizadas por pessoas na própria organização como funcionários, fornecedores e visitantes, como por pessoas externas. Os tipos de danos são limitados. Entre eles podem ser: sabotagem de hardware ou software, o roubo de informações, ataques à infraestrutura, entre outros (Oliveira, 2004).

3.2.2 Vulnerabilidades

A vulnerabilidade é qualquer fraqueza em computadores ou redes, em hardware ou software, que deixa uma abertura, facilitando a realização de ataques. Pode ser resultado de uma imperfeição, implantação ou configuração. Entre elas podem ser: má configuração do sistema operacional, o qual permite ao usuário total direito administrativo sobre a máquina, um sistema de banco de dados com defeitos nas prioridades de acesso, uma falha em um programa que permite acesso aos dados do usuário, entre outros (Oliveira, 2004).

3.3 Teste de penetração

Teste de penetração (*Penetration Test*) é um método legal e autorizado pelo contratante, que permite ao profissional testar as fraquezas nos sistemas computacionais e explorá-las. O foco principal é o *hardening* (tornar o sistema seguro) (GIAVAROTO; SANTOS, 2015).

Existem vários tipos de testes de penetração, tais como, *Double Blind*, *Gray Box*, Tandem, Reversal. Os mais comuns são o *White Box* e o *Black Box* (GIAVAROTO; SANTOS, 2015).

No *Black Box* o *pentester* não possui um prévio conhecimento sobre o ambiente, porém um escopo deve ser criado e o alvo deve estar ciente das áreas envolvidas e dos impactos que possam vir a ocorrer (GIAVAROTO; SANTOS, 2015).

Neste trabalho o tipo do teste de penetração será o *White Box*, que é quando o *hacker* ético tem total conhecimento sobre o ambiente a ser explorado, ou seja, mapas de redes, sistemas operacionais, infraestrutura, além de trabalhar diretamente com as equipes de analistas do ambiente-alvo (GIAVAROTO; SANTOS, 2015).

A vantagem do *White Box* é que o teste é realizado de forma mais completa e mais rápida.

Para realizar os testes com qualidade e perfeição é necessária a definição de um escopo, que organiza as fases dos testes.

O objetivo de uma revisão de segurança da aplicação/sistema é o de determinar se ela é vulnerável a um ataque em nível de aplicação feito por um atacante externo. Este nível de prova valida a política de segurança da empresa e as normas de desenvolvimento por meio da tentativa de identificar como o sistema resiste a certos agressores. O produto de uma revisão automatizada do sistema é um relatório que documenta a postura de segurança encontrada, identifica deficiências e vulnerabilidades específicas e provê recomendações para sua remediação.

Os benefícios de um teste de invasão incluem: identificação da exposição da aplicação web a riscos de segurança. Identificação de vulnerabilidades específicas

que afetam o sistema. Validação e verificação dos controles de Segurança existentes, políticas e procedimentos.

3.3.1 Escopo

Para facilitar o andamento e a organização dos testes de penetração, há um escopo a ser seguido. Neste trabalho será utilizada a metodologia definida pelo programa EC-Council C|EH *Certified Ethical Hacker*, baseando-se no livro Kali Linux, Introdução ao *Penetration Testing.* As fases do teste de penetração são divididas em cinco etapas e serão definidas a seguir:

3.3.1.1 Reconhecimento

O reconhecimento é a metodologia utilizada para a obtenção de informações a respeito de determinado alvo. A técnica de reconhecimento advém de táticas militares, nas quais o terreno deve ser estudado de forma estratégica antes que seja atacado. Através do reconhecimento, o invasor poderá munir-se de informações importantes relativas ao alvo, em consequência, minimizar as dúvidas a respeito do alvo e executar um ataque cirúrgico (GIAVAROTO; SANTOS, 2015).

3.3.1.2 Varredura ou *Scanning*

Essa técnica é muito comum e amplamente utilizada para reunir informações a respeito do estado das portas e a descoberta de serviços

Quaisquer máquinas conectadas em uma rede oferecem serviços que usam portas TCP e UDP. Portanto, o rastreamento de portas consiste em enviar uma mensagem por vez para cada uma das portas, explorando as mais comuns e até as menos usadas. Com base na análise de uma varredura pode-se, então, determinar se a porta está sendo ou não utilizada e, caso esteja, o invasor poderá explorá-la de inúmeras

maneiras a fim de encontrar possíveis falhas de segurança (GIAVAROTO; SANTOS, 2015).

Os estados das portas são seis:

OPEN – aberta;

CLOSED – fechada;

FILTERED – filtrada, geralmente protegida por um firewall;

UNFILTERED – não filtrada, está acessível;

OPEN/FILTERED – aberta ou filtrada, a varredura não pode definir se a porta está ativa ou fechada;

CLOSED/FILTERED – fechada ou filtrada, a varredura não pode determinar se a porta está fechada ou (GIAVAROTO; SANTOS, 2015).

Existem três tipos de varreduras:

- de porta – onde são verificados o estado das portas, ou seja, se estão abertas, fechadas ou filtradas;
- de vulnerabilidade – buscam fraquezas presentes em um ambiente computacional;
- de redes – faz a verificação dos equipamentos, geralmente observando o funcionamento e a performance dos mesmos (GIAVAROTO; SANTOS, 2015).

3.3.1.3 Ganho de acesso

Após a execução das tarefas de reconhecimento e varreduras, obtêm-se informações valiosas a respeito do alvo e, então, pode-se iniciar os processos de tomada do sistema, ou seja, o ganho de acesso.

Existem ferramentas utilizadas em quebras de senhas *on-line* e *off-line*; no caso dos serviços de acesso remoto, a tentativa de quebra e ganho de acesso é executada no modo *on-line*.

3.3.1.4 Manutenção do acesso

Após a tomada do sistema, o invasor pode executar a chamada manutenção, ou seja, tática que lhe permitirá plantar *rootkits*[3], cavalos de troia, etc. Isto possibilita um possível retorno e existem invasores que até corrigem vulnerabilidades para garantir que somente ele fará novas incursões.

3.3.1.5 Cobertura de rastros

Após a tentativa ou sucesso do ganho de acesso, o atacante tentará apagar seus rastros e limpar a casa, ou seja, aplicar as técnicas de *housekeeping*[4] excluindo os logs do sistema.

Cada uma das fases do teste de penetração acima é realizada a partir de ferramentas e técnicas específicas, que serão definidas e mostradas adiante.

3.4 Kali Linux

[3] *Rootkit* é um tipo de software, muitas das vezes malicioso, projetado para esconder a existência de certos processos ou programas de métodos normais de detecção e permitir contínuo acesso privilegiado a um computador. Disponível em: https://pt.wikipedia.org/wiki/Rootkit

[4] Housekeeping – Serviço de Limpeza

Para a realização dos testes envolvendo o servidor e os sistemas do Projeto Rede Ciranda, será utilizado o Sistema Operacional Kali Linux, que é uma distribuição Linux própria para realizar testes de vulnerabilidade.

Kali Linux é um arsenal Teste de Invasão baseado no Debian Linux usado por profissionais de segurança (e outros) para realizar avaliações de segurança. Oferece uma variedade de conjuntos de ferramentas personalizadas para identificar e explorar vulnerabilidades em sistemas. Foi uma reconstrução de outra ferramenta da *Offensive Securit*, chamada *Back Track*, que tinha o mesmo objetivo e era uma distribuição com base em Ubuntu e já contava com uma grande quantidade de usuários e seguidores.

Algumas ferramentas do Kali Linux serão estudadas e as que mais se encaixarem no perfil dos estudos e do Projeto serão escolhidas para realizarem os testes necessários na detecção de problemas e vulnerabilidades.

3.5 Ferramentas e técnicas

Em cada fase do teste de penetração, será necessário o uso de ferramentas específicas do Kali Linux e algumas técnicas. A seguir, será apresentado o conceito das que serão utilizadas neste trabalho:

a) Dmitry: para levantar algumas informações iniciais na fase de reconhecimento será utilizada a ferramenta dmitry. Desenvolvida em C, com ela é possível reunir informações a respeito de endereços de e-mail, subdomínios, *uptime*, executar varreduras TCP, *lookups*, etc (GIAVAROTO; SANTOS, 2015).

b) Fingerprint: uma técnica importante que será utilizada na fase de reconhecimento é o *Fingerprint* ou impressão digital, na qual o atacante tenta obter informações a respeito das versões dos serviços.

c) Netcat: conhecido pelos analistas de segurança como canivete suíço, além de permitir conexões reversas, o Netcat também é uma excelente opção na busca de informações a respeito de serviços (GIAVAROTO; SANTOS, 2015).

d) Nmap: Uma das principais ferramentas a serem utilizadas na etapa de varredura é o NMAP. Criada em setembro de 1997 por Gordon Fyodor Lyon, o mapeador de redes é utilizado em grande escala no *pentest*. Suas principais funcionalidades são as varreduras de portas, descoberta de serviços e a detecção de versões (GIAVAROTO; SANTOS, 2015).

e) Nessus: outra ferramenta considerada como um dos melhores e mais potentes scanners de vulnerabilidades é o Nessus. Ele não está presente no Kali Linux, mas, possui uma versão gratuita. Depois de instalado e configurado, é necessário criar uma política antes de iniciar a análise de vulnerabilidade.

f) Joomscan: quando o assunto é descobrir se existe qualquer tipo de vulnerabilidade no Joomla, que é um sistema de gestão de conteúdo para sites, a ferramenta ideal a ser utilizada para este serviço é o Joomscan.

g) xHydra: na fase de ganho de acesso, será utilizada a ferramenta xHydra no modo gráfico, que é uma ferramenta muito boa quando o assunto é a escalação de privilégios através de quebra de senha *on-line*. (GIAVAROTO; SANTOS, 2015).

h) Metasploit: ainda na etapa de ganho de acesso será utilizado o Metasploit, que é uma ferramenta desenvolvida por HD Moore, especialista em segurança, que teve sua primeira versão escrita em Perl e lançada em outubro de 2003. Em 2009 a empresa Rapid7 absorveu o projeto Metasploit e a ferramenta ganhou comunidade envolvida em segurança da informação. Até o momento, o Metasploit encontra-se em sua versão 4.93 com 1.324 *exploits*, 719 auxiliares, 213 posts, 346 *payloads*, 35 *encoders* e 8 *nops*. (GIAVAROTO; SANTOS, 2015).

   Alguns termos básicos que estão embutidos no Metasploit:

   Exploit: Código de programação escrito com o intuito de explorar vulnerabilidades em um sistema computacional.

   Payload: Carga de código aplicada ao sistema alvo, sendo possível a abertura de comunicação entre o atacante e o alvo.

Shellcode: São códigos escritos, na maioria das vezes, em *assembly*, têm como missão explorar vulnerabilidades e causar o chamado buffer overflow.

Auxiliary: Módulos que permitem funcionalidades adicionais, como, por exemplo, varreduras, farejamento, entre outros.

Encoders: São utilizados para ofuscar os módulos e com isto, dificultar a detecção por mecanismos de proteção; por exemplo, *firewalls*.

NOP: *No Operation*, utilizado na estabilização de *payloads*, ou seja, pode remover irregularidades em endereços de memória antes de iniciar o *shellcode*.

POST: Módulos pós-exploração; por exemplo, *hash dump*, *screenshots*, etc. (GIAVAROTO; SANTOS, 2015).

i) Dicionário: outra técnica bastante utilizada é o ataque por dicionário, que é quando o invasor cria um arquivo com dezenas, centenas ou milhares de palavras para usuário ou senha e o software se encarrega de fazer o resto. Além desta, existe o ataque de força bruta, onde o software utiliza um algoritmo de combinação que se encarrega de fazer as tentativas de quebras de senha. Este método é mais difícil e demorado, pois, dependendo da complexidade da senha, torna-se quase impossível.

j) Sqlmap: outra ferramenta a ser utilizada na etapa de ganho de acesso é o sqlmap. O sqlmap é uma ferramenta de código aberto, desenvolvida em Python e amplamente utilizada em testes de penetração quando o assunto está relacionado a falhas envolvendo banco de dados, tais como, *sql injection* (GIAVAROTO; SANTOS, 2015).

   É muito comum que programadores desatentos cometam erros de validação, inclusive quando essas validações envolvam programação relativa à SGBD’s. Caso um desenvolvedor permita que consultas arbitrárias sejam executadas em sua aplicação, estará colocando seu ambiente em perigo de tal forma que os impactos poderão ser desastrosos.

4 ESTUDO DE SEGURANÇA DA INFORMAÇÃO NO PROJETO REDE CIRANDA

Após o conhecimento adquirido sobre Segurança da Informação e sua implantação, é realizado uma análise no Projeto Rede Ciranda para obter uma melhor posição por onde iniciar os estudos práticos de SI dentro do Projeto.

4.1 Projeto Rede Ciranda da Criança e Adolescente de Assis

O Projeto Rede Ciranda da Criança e Adolescente de Assis teve início no ano de 2010 por meio de uma parceria entre a Associação Filantrópica Nosso Lar e a Fundação Telefônica com o objetivo inicial de promover um diagnóstico da realidade da criança e adolescente de Assis.

O Projeto faz a integração das áreas de assistência social, educação, saúde, segurança pública e organizações do terceiro setor. Com essa integração, o Rede Ciranda oferece alguns benefícios às entidades associadas, dentre eles, cursos de capacitação e encontros para que seja potencializado a atuação das entidades e projetos sociais, melhoria da atuação do Poder Público, otimização e soluções e realizar o diagnóstico sobre a realidade da criança e do adolescente de Assis que sustenta e apoia o CMDCA na formulação de políticas públicas. (Xavier, et. al., 2012.

Várias instituições fazem parte do Rede Ciranda, entre elas: Associação de Pais e Amigos dos Excepcionais – APAE, Associação Beneficente de Assis – SIM, Associação Filantrópica Nosso Lar, Unidade de Prestação de Serviço Especial de Reabilitação – SER, Casa da Menina São Francisco de Assis, Casa da Criança Dom Antônio José dos Santos, Associação Amigos de Santa Cecília, Círculo dos Amigos dos Pobres do Pão de Santo Antônio – CAPSA, Projeto Broto Verde, entre outras.

Segundo Xavier et. al. (2012), o objetivo maior do Projeto é garantir os direitos e o desenvolvimento integral das crianças e dos adolescentes. Com isso, o Rede Ciranda fica responsável por algumas ações, sendo elas: oferecer cursos de aprimoramento

aos atores sociais da rede; dar visibilidade ao CMDCA com apoio para divulgação de suas ações, auxílio para organização de eventos, entre outros; promover condições para a realização de estudos sobre os problemas que envolvem a criança e o adolescente; realizar encontros para os gestores e funcionários.

O departamento de Tecnologia da Informação do Projeto Rede Ciranda é responsável pelo desenvolvimento e manutenção dos sites e softwares que auxiliam as instituições citadas acima.

4.2 Infraestrutura

4.2.1 Hardware

Hoje o Projeto conta com um servidor Debian responsável por hospedar os sites e sistemas utilizados pelas instituições e quatro computadores que são utilizados pelos funcionários de TI para realizar todas suas tarefas, como o desenvolvimento e manutenção de *softwares*. Três destas máquinas são da LG, modelo *All In One* com processador Intel i5, 4Gb de memória RAM e 500Gb de HD, rodando com o Sistema Operacional Windows 8. A outra roda com o Sistema Operacional Linux, e possui 2Gb de memória, 500Gb de HD e processador Intel Core 2 Duo.

4.2.2 Software

Dentre os sistemas existentes estão, o Sistema Cursos, que realiza a matricula semestral dos alunos das oficinas de informática oferecidos pelo Nosso Lar em parceria com os Projetos Rede Ciranda e Integra Assis, o Sistema Doações, que recebe doações emitindo boletos para os interessados em ajudar as instituições. O Sistema Eventos, que lista os eventos que serão realizados pelas instituições, faz inscrições e confirmações de participação, o Sistema Financeiro, que tem o objetivo de organizar as finanças das instituições, gerenciando as verbas disponibilizadas, convênios firmados com outras instituições e toda a parte fiscal, e o Sistema Cadastro,

desenvolvido recentemente com o objetivo de cadastrar as crianças e adolescentes frequentadores de todos os projetos citados, mantendo os dados gerais para obter o controle de cada frequentador. Além desses, o servidor também hospeda nove sites pertencentes a algumas instituições das quais o Projeto Rede Ciranda auxilia.

4.3 Segurança atual do Projeto Rede Ciranda

Não há nenhuma informação de superiores ou documento comprovando que o servidor do Projeto passou por uma análise ou bateria de testes para verificar se existem vulnerabilidades que podem comprometer as informações existentes. Como ele é utilizado por várias instituições, precisa estar sempre com sua disponibilidade, integridade e confidencialidade garantida, para que nenhuma informação se perca, seja alterada ou acessada por pessoas indesejadas.

Analisando a situação atual do Projeto antes dos devidos testes de reconhecimento, temos alguns pontos positivos e negativos:

- Possui um servidor que hospeda cinco sistemas e nove sites, que são utilizados por diversas instituições;
- Possui cinco funcionários de TI, sendo um técnico em informática e quatro estagiários que não se fixam por muito tempo no cargo, pois praticamente três são substituídos anualmente. Todos possuem acesso direto ao servidor;
- Não possui um documento para conscientização dos funcionários com o objetivo de manter a organização e segurança, sem colocar nenhum serviço em risco;
- Não há antivírus nos computadores dos funcionários;
- São realizados *backups* uma vez na semana, porém nem sempre são efetuados com sucesso;
- Sistemas possuem controle de acesso, para evitar que pessoas indesejadas tenham acesso a eles;
- A Fonte de Energia Ininterrupta (*Nobreak*) é antiga e não passa segurança em casos de queda de energia;

4.4 Proposta de Segurança

Em princípio, diante das características levantadas, há algumas medidas que podem ser tomadas de imediato, como por exemplo, a conscientização dos funcionários sobre as medidas de segurança que devem ser adotadas e seguidas. Considerando que a maioria dos ataques bem-sucedidos está vinculada ao despreparo das pessoas que, de uma forma inocente ou equivocada, habilitam oportunidades que podem ser usadas com grande potencial, será elaborado um documento contendo as políticas de segurança da informação do Projeto Rede Ciranda.

Ainda antes de iniciar a etapa dos testes de penetração, será implementado um firewall básico, que dará os primeiros passos rumo à segurança das informações do Projeto.

A Fonte de Energia Ininterrupta está como urgência no planejamento do Projeto, para que a troca seja efetuada o mais breve possível.

As demais propostas surgirão no decorrer deste trabalho, diante dos estudos e testes que serão realizados. Alguns problemas serão resolvidos e outros serão deixados como propostas para trabalhos futuros.

Algumas partes desse estudo, como o documento contendo as políticas de segurança, serão baseadas nas Normas ABNT ISO/IEC, para que a implantação de Segurança da Informação no Projeto Rede Ciranda ocorra de maneira organizada e facilite a continuidade desse trabalho futuramente.

5 APLICANDO OS TESTES DE PENETRAÇÃO NO PROJETO REDE CIRANDA

Para aplicar os conhecimentos sobre Segurança da Informação no Projeto Rede Ciranda, inicia-se a fase de teste de penetração. Seguindo o escopo definido anteriormente, obtêm-se resultados melhores e mais organizados.

5.1 Reconhecimento

Esta é a primeira etapa a ser executada na busca de vulnerabilidades.

Neste trabalho, já há conhecimento sobre o alvo, porém será abordado o uso de algumas ferramentas para obtenção de algumas informações relevantes, simulando a dificuldade ou facilidade que um atacante externo teria para obter informações a respeito do Projeto Rede Ciranda.

Utilizando a ferramenta dmitry para varredura de portas TCP:

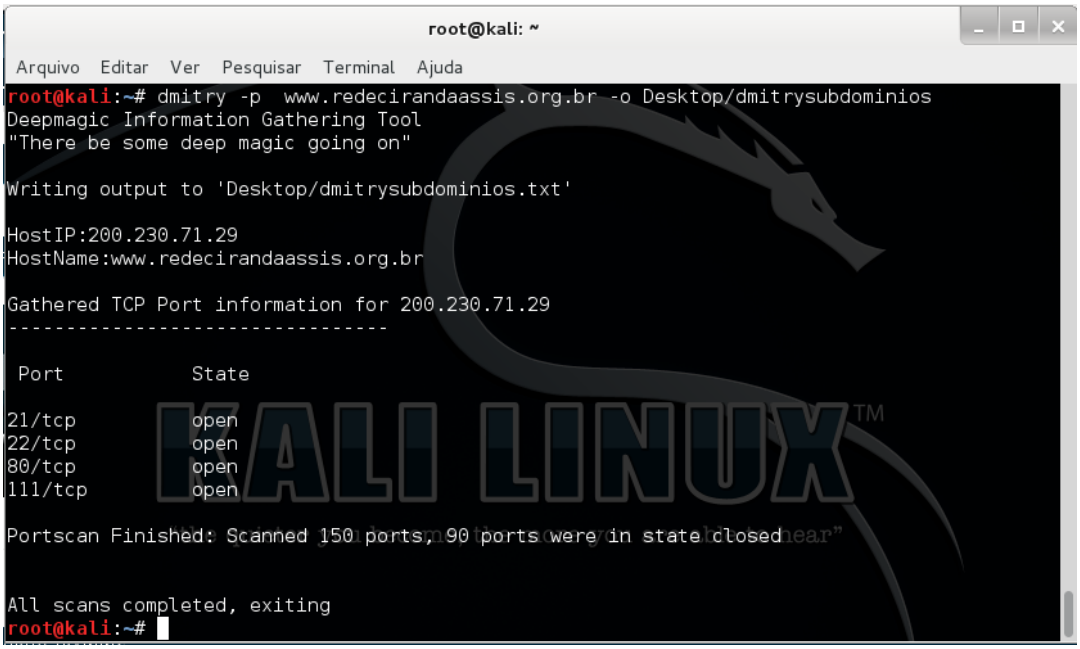


Figura 1 - Varredura de portas TCP

Na Figura 1, percebe-se que quatro portas estão abertas, podendo conter vulnerabilidades. As demais estão fechadas, filtradas ou não foi possível obter informações a respeito.

Com a ferramenta dmitry também foi possível realizar uma pesquisa *whois*[5] através do nome de domínio e obter informações como o dono do servidor, id do dono, nome do responsável, data de criação, etc.

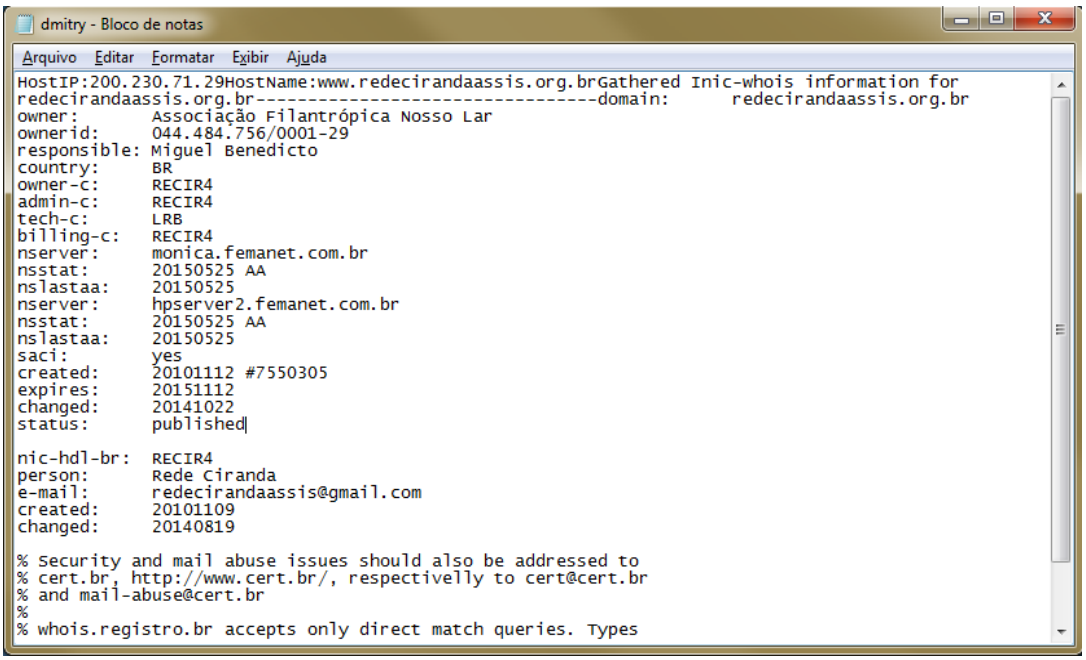


Figura 2 - Pesquisa *whois* através do nome de domínio.

Na Figura 2, obtiveram-se algumas informações a respeito do host do Projeto Rede Ciranda.

No próximo passo, foi utilizada a ferramenta NETCAT para a técnica de *Fingerprint*:

[5] *WHOIS* é um mecanismo que registra domínios, IPs e sistemas autônomos na Internet e que serve para identificar o proprietário de um *site* (Wikipedia).

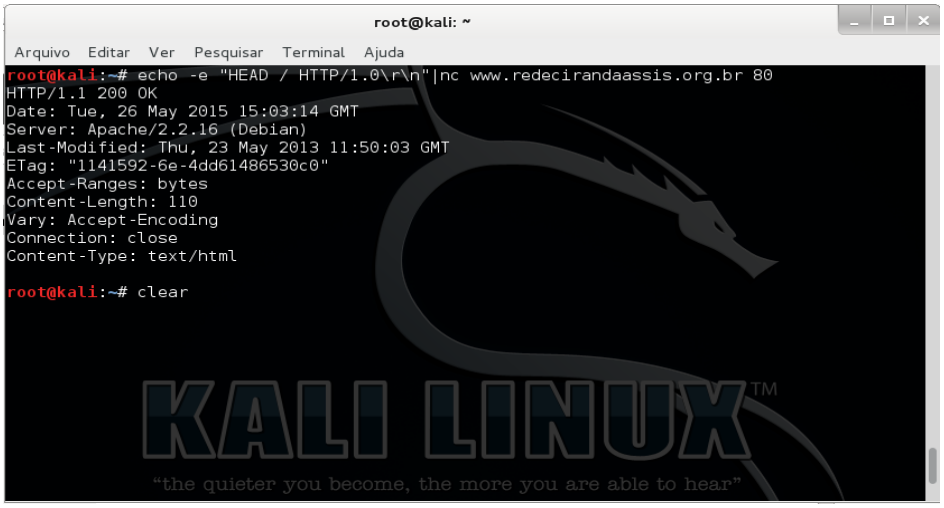


Figura 3 - Buscando informações sobre o serviço http rodando na porta 80

5.2 Varredura (*Scanning*)

Iniciando a etapa de varredura, primeiramente foi realizada uma varredura básica do tipo TCP Connect (-sT) no servidor Rede Ciranda, utilizando a ferramenta nmap. A primeira coluna apresenta as portas e protocolos, a segunda, o estado e a terceira o serviço:

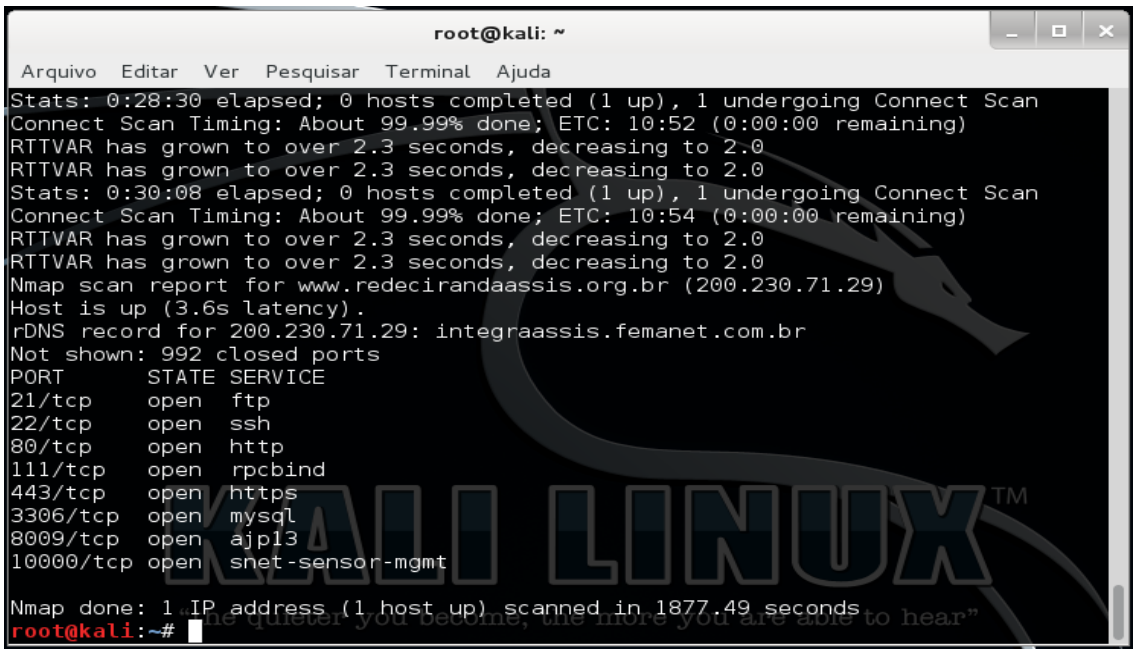


Figura 4 - Varredura básica com nmap

Na figura 4, percebe-se que a varredura básica executada com nmap, trouxe mais portas abertas como resultado do que a varredura feita com a ferramenta dmitry. Isso mostra que o nmap é mais potente.

A seguir foi executada uma detecção de versões no modo agressivo, utilizando o parâmentro –A. nmap –A 200.230.71.29:

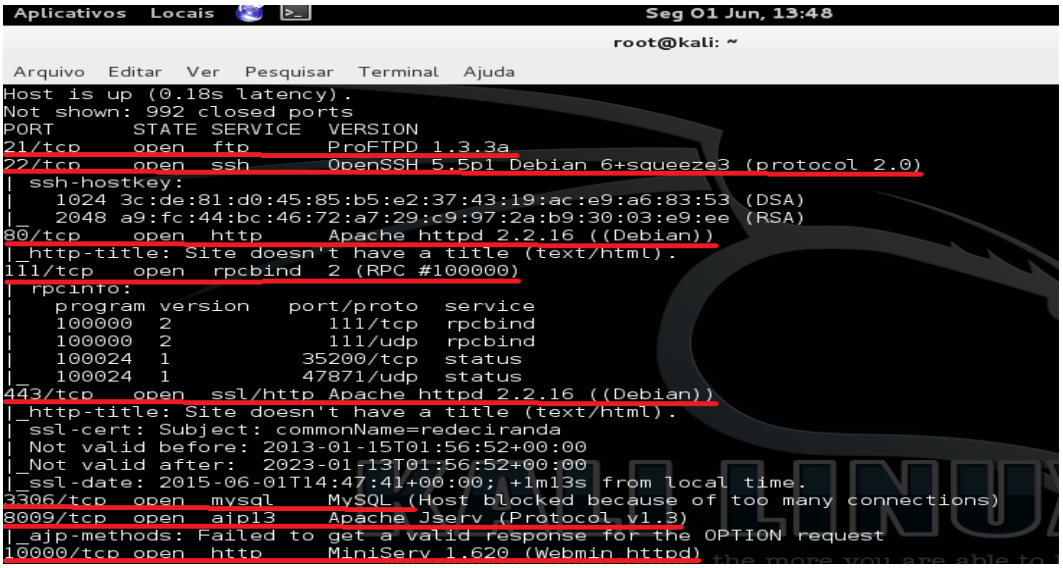


Figura 5 - Detecção de versões no modo agressivo com nmap

Para tentar obter informações a respeito do SGBD MySQL, foi realizado uma varredura do tipo *Syn Connect*[6] –sS, na porta –p 3306, em conjunto com o *script* mysql-info.nse:

[6] É a varredura Syn que examinas as portas de maneira rápida e invisível (GIAVAROTO; SANTOS, 2015).

Figura 6 - Informações a respeito do SGBD MySQL

Após ter conseguido algumas informações sobre o SGBD MySQL, pode-se verificar a existência de contas com senhas em branco. Para isso foi realizada uma varredura juntamente com o *script empty-password*.nse:

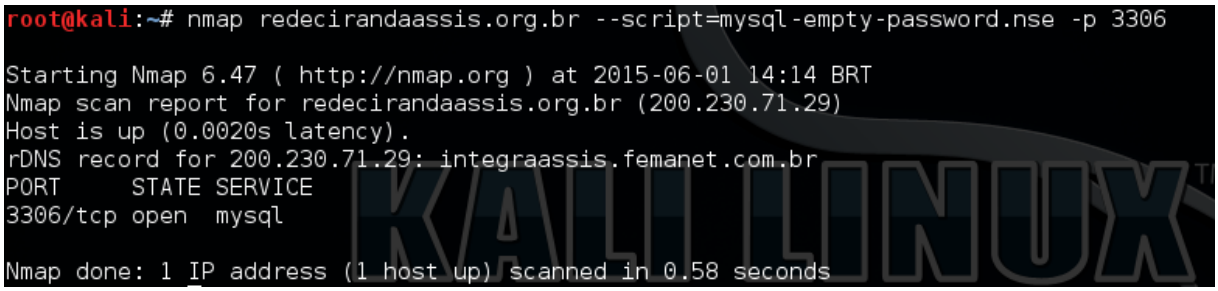


Figura 7 - Verificando a existência de senhas em branco no MySQL

Foi concluído que não há senhas em branco no SGBD MySQL do Projeto Rede Ciranda.

Abaixo foi utilizada a ferramenta Nessus. Depois de criada uma política, inicia-se o escaneamento. Ao final é gerado um relatório prévio das vulnerabilidades:

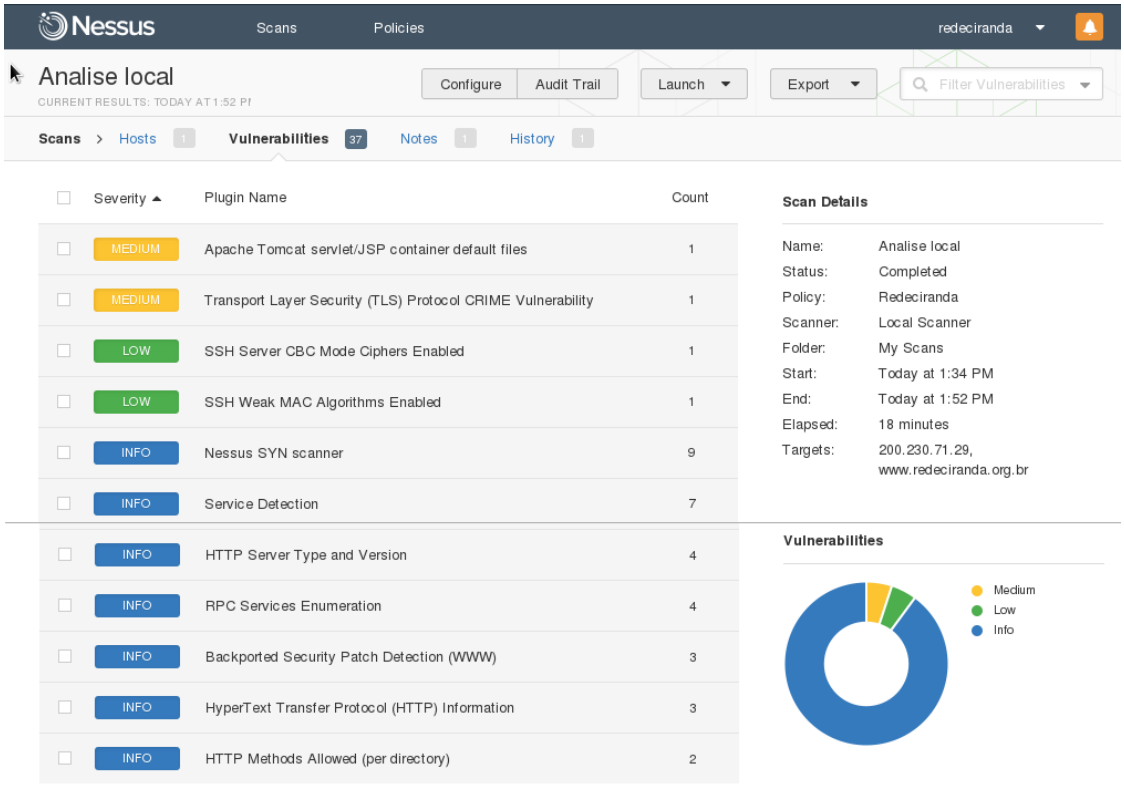


Figura 8 - Relatório Nessus de vulnerabilidades do servidor Rede Ciranda

Foram encontradas 37 vulnerabilidades, como mostra a Figura 8, porém nenhuma possui risco Crítico ou Alto.

Ao acessar cada vulnerabilidade o Nessus apresenta algum tipo de solução. Para a vulnerabilidade encontrada no Apache Tomcat Servlet/JSP o Nessus sugeriu revisar os arquivos contidos e excluir aqueles que não fossem necessários, porque estes arquivos podem conter informações que podem ajudar *hackers*.

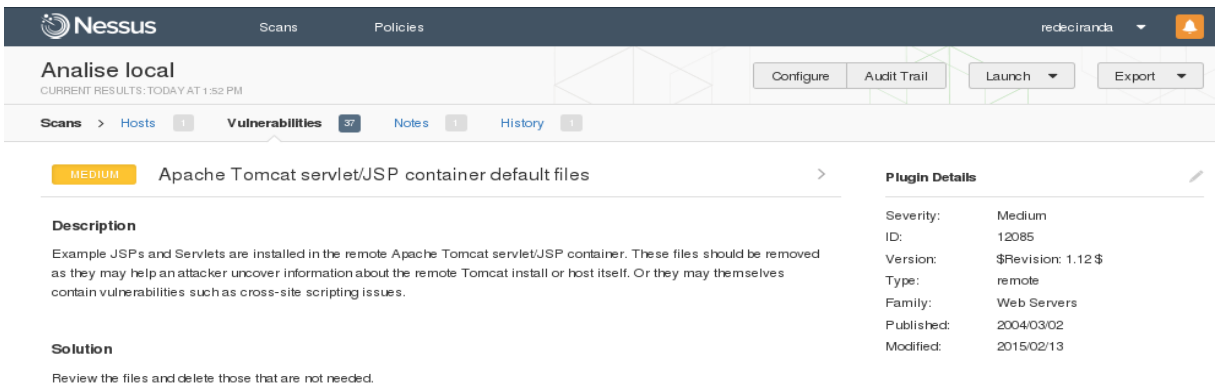


Figura 9 - Descrição e solução para vulnerabilidade

Na próxima varredura, foi utilizada a ferramenta Joomscan para verificar se existem vulnerabilidades no Joomla do Projeto Rede Ciranda.

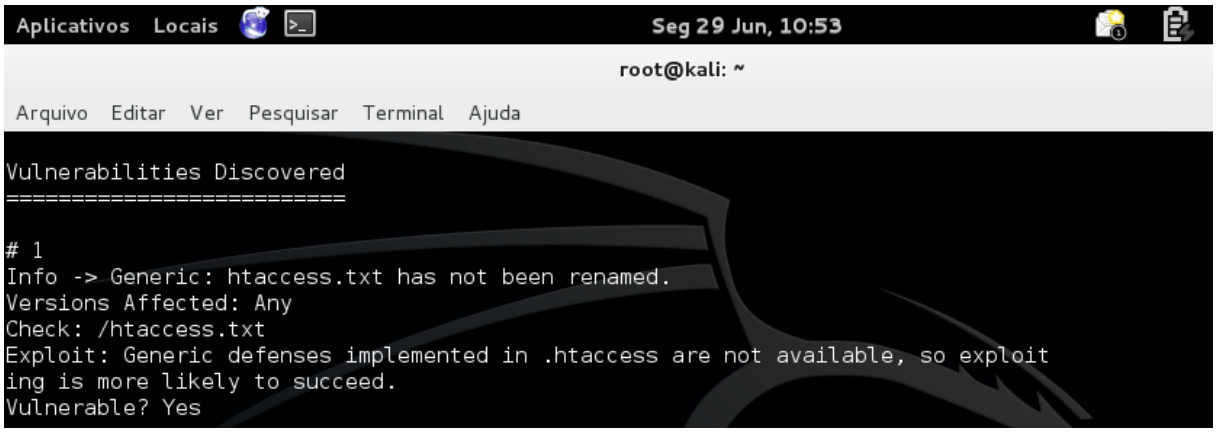


Figura 10 - Vulnerabilidades do Joomla utilizando a ferramenta Joomscan

Foram encontrados 26 resultados de vulnerabilidades a respeito do Joomla, porém apenas o primeiro possui uma falha mais evidente, onde a varredura aponta que as defesas genéricas implementadas no arquivo htacess.txt não estão disponíveis, portanto, é mais provável uma exploração de sucesso.

Para tal vulnerabilidade, a ferramenta Joomla foi atualizada para a versão 3.4, pois a versão utilizada anteriormente era a 2.5.11 de 2013.

5.3 Ganho de Acesso

Para iniciar a etapa de ganho de acesso foi utilizada a ferramenta xHydra. Primeiramente foi criado um arquivo chamado senhas.txt contendo senhas prováveis. Em seguida, a ferramenta xHydra foi configurada para tentar acessar o servidor do Projeto pelo protocolo SSH à partir das senhas contidas no arquivo.

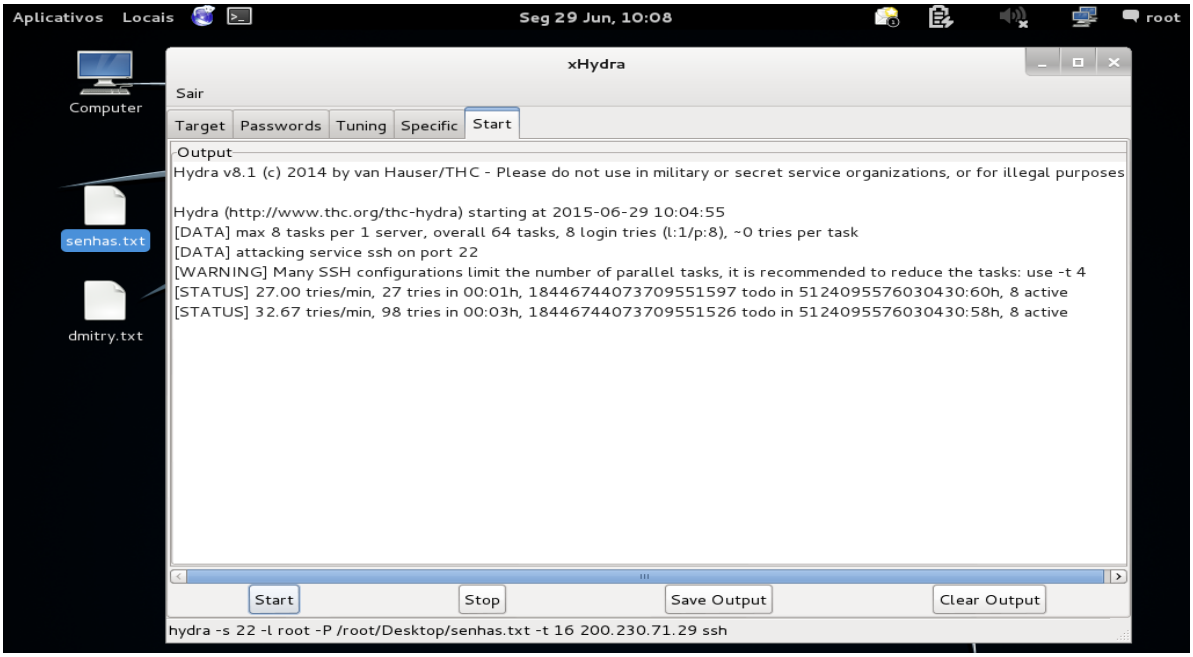


Figura 11 - Tentativa de ganho de acesso ao servidor com a quebra do protocolo SSH

Como a política de senhas do Projeto é bem forte não foi possível acessar o servidor via SSH a partir das senhas consideradas fracas inseridas no arquivo senhas.txt

Para demonstrar um ganho de acesso ao SGBD MySql foi utilizado o MSFCONSOLE, que é uma interface do metasploit que utiliza linhas de comando, juntamente com o módulo auxiliar *mysql_login* e mais dois arquivos contendo usuários e senhas possíveis.

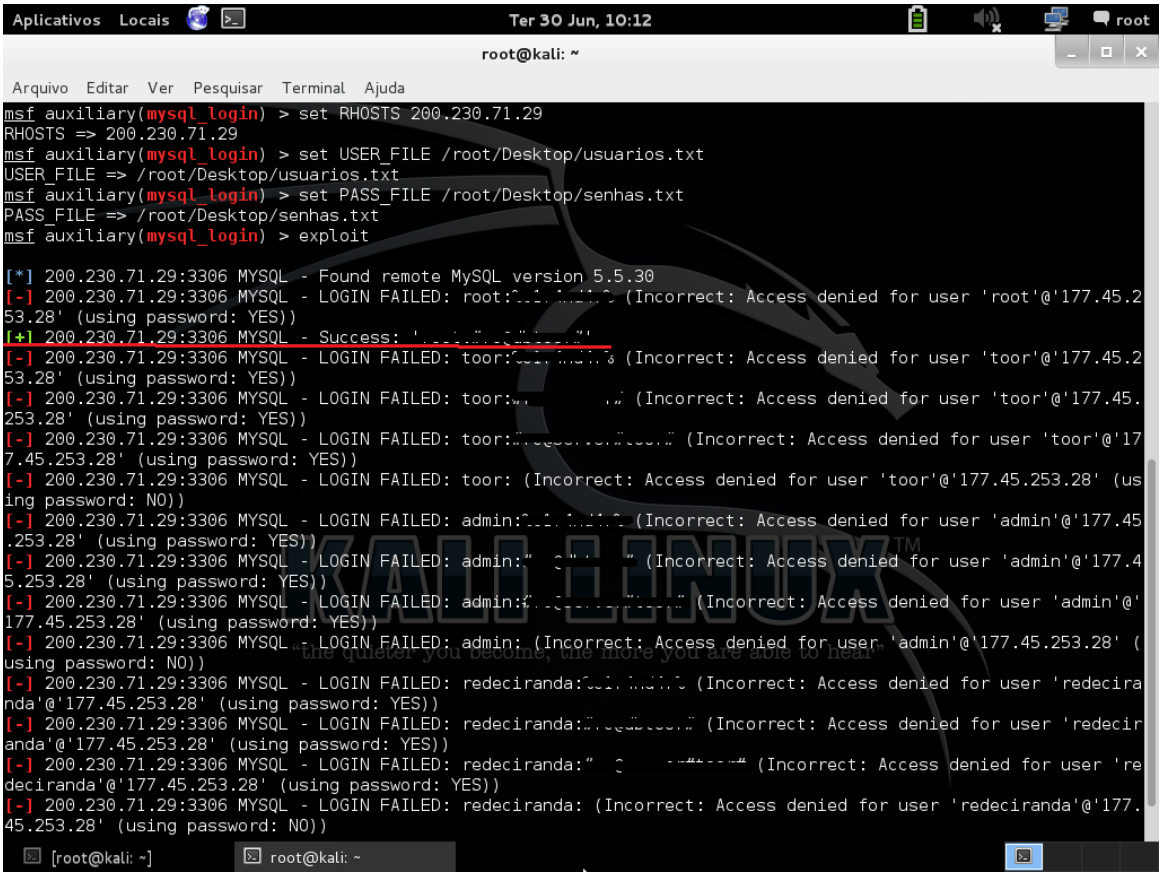


Figura 12 - Ganho de acesso ao SGBD MySql com o Metasploit

Observa-se que na Figura 12, foi encontrado o usuário e a senha do MySql à partir dos dados inseridos nos arquivos usuarios.txt e senhas.txt. Com isso o ganho de acesso está garantido. Porém, somente foi possível obter sucesso neste ataque porque neste trabalho o tipo de *penetration test* é o *White Box*, que, como já dito anteriormente, é quando o *hacker* ético tem total conhecimento sobre o ambiente a ser explorado. Sem esse conhecimento este ganho de acesso seria muito dificultado ou até impossível de ser realizado.

O conhecido servidor de aplicações de tecnologias *JavaServlets* e JSP, Apache Tomcat, não deixa de possuir funções de um servidor Web, inclusive integrado ao Apache *Server*. O Tomcat, quando configurado por administradores displicentes ou sem conhecimentos, pode levar a configurações padrões e, consequentemente, o ganho de acesso se tornará uma tarefa fácil. A seguir será apresentado um ataque de ganho de acesso ao servidor Tomcat do Projeto Rede Ciranda utilizando o Metasploit.

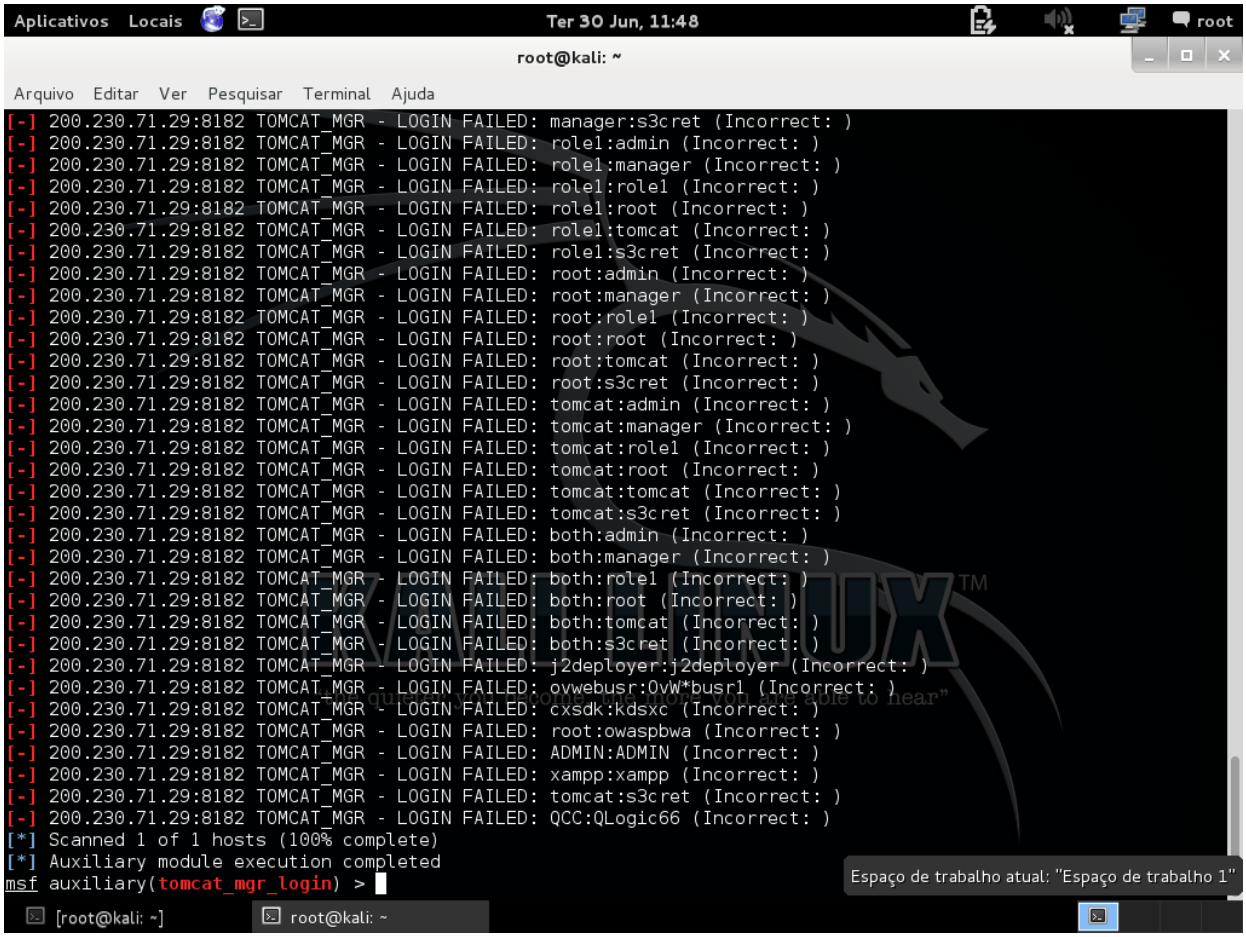


Figura 13 - Tentativa de ganho de acesso ao Tomcat por *word lists* padrão

Neste ataque da figura 13, foi utilizado o *exploit* auxiliar tomcat_mgr_login, setado as word lists padrão para Tomcat, determinado a porta 8182 e aplicado o exploit. Não foi obtido êxito, pois o usuário e a senha não foram encontrados nas *word lists* padrão.

A seguir é apresentado um ataque com êxito, porém novamente foi preciso um bom conhecimento sobre o alvo.

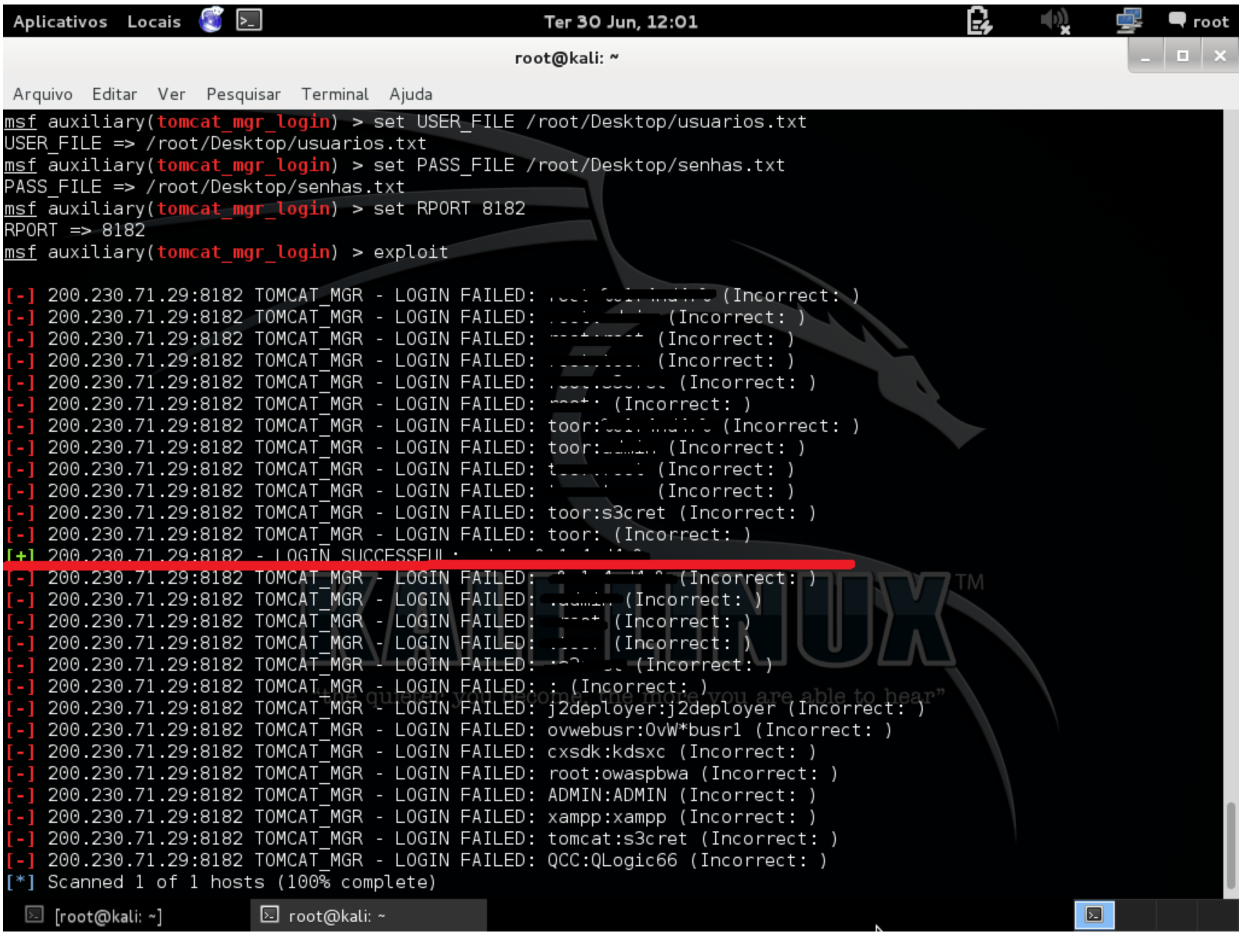


Figura 14 - Ganho de acesso ao Tomcat com Metasploit

Nos ataques das Figuras 12 e 14, foi utilizada a técnica de ataque de dicionário, utilizando arquivos contendo usuários e senhas possíveis.

Para verificar se o Projeto Rede Ciranda possui vulnerabilidades Sql, foi utilizado o Sistema Cadastro para realizar os testes. Desenvolvido pela equipe de TI do Projeto, é um sistema *web* que possui uma tela de *login*, para obter acesso como usuário comum ou administrador:

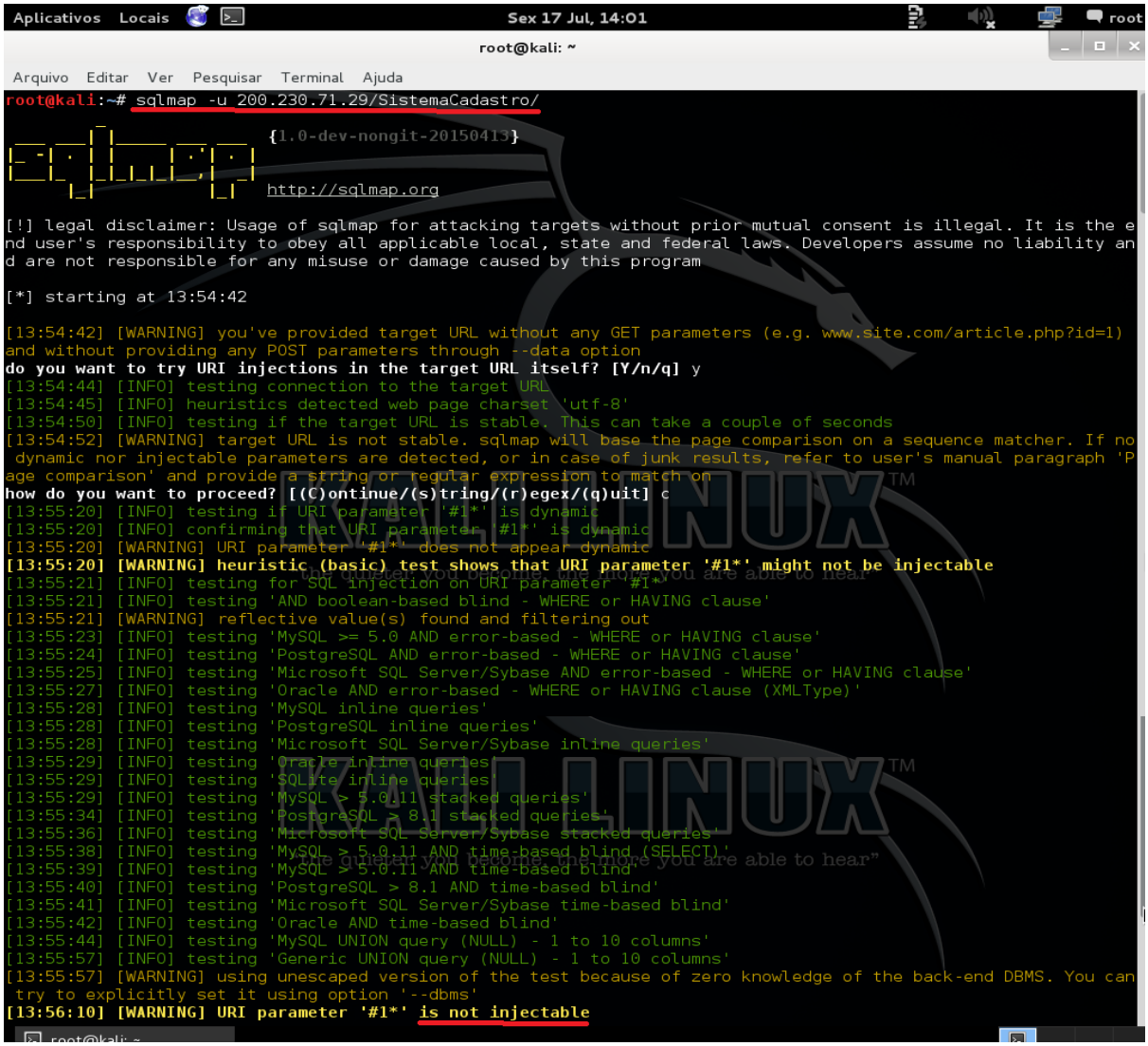


Figura 15 - Teste SQL *Injection* no Sistema Cadastro

Na Figura 15, foi utilizada a ferramenta sqlmap com o parâmetro –u para que pudesse ser oferecido o endereço do alvo, que no caso foi o Sistema Cadastro: sqlmap –u 200.230.71.29/SistemaCadastro. Na última linha da Figura observa-se que não foi obtido sucesso, mostrando que este sistema não pode ser facilmente violado por qualquer atacante.

5.4 Manutenção do acesso

O *hacker* ético não precisa garantir seu retorno, pois após o termino da auditoria, deverá arrumar a casa e deixar tudo como estava. Esta etapa foi citada porque está incluída na metodologia definida pelo programa EC-Council C|EH *Certified Ethical Hacker*, no qual este teste de penetração está baseado, portanto não é necessário executa-la na prática, e sim, apenas saber de sua existência.

5.5 Cobertura de Rastros

A cobertura de rastros se resume na exclusão dos logs que guardam informações sobre o acesso de qualquer usuário ao servidor e seus serviços.

Os logs no ambiente Debian do Projeto Rede Ciranda encontram-se em /var/log:

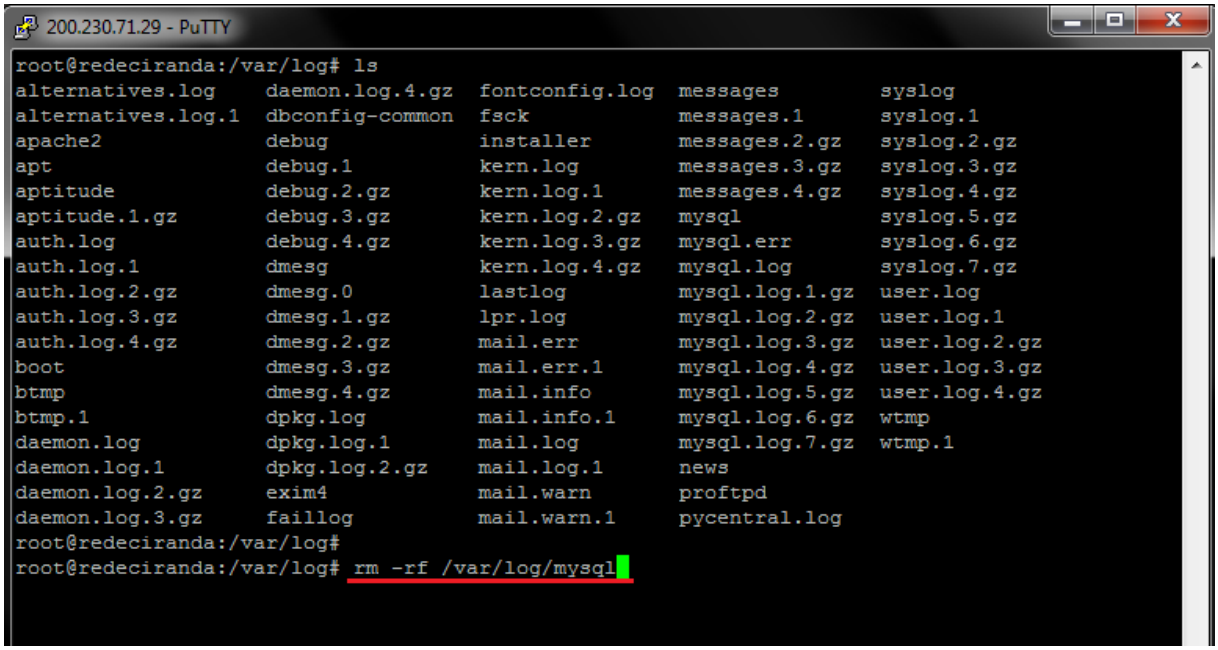


Figura 16 - Logs do Projeto Rede Ciranda

Na Figura 16, foi acessado o servidor como root via ssh e listado todos os arquivos de logs contidos na pasta /var/log. Em seguida há um exemplo de exclusão dos logs de alerta do MySql.

Há métodos mais drásticos para realizar a exclusão dos logs, como por exemplo, o chamado toque da morte, onde o atacante estaria apagando todos os arquivos do sistema com o simples comando rm –rf /*.

Um dos servidores mais utilizados, o Apache, também possui logs. Neste caso, eles possuem todos os registros e erros de acesso aos sites, sistemas e serviços do Projeto Rede Ciranda e podem ser encontrados em /var/log/apache2:

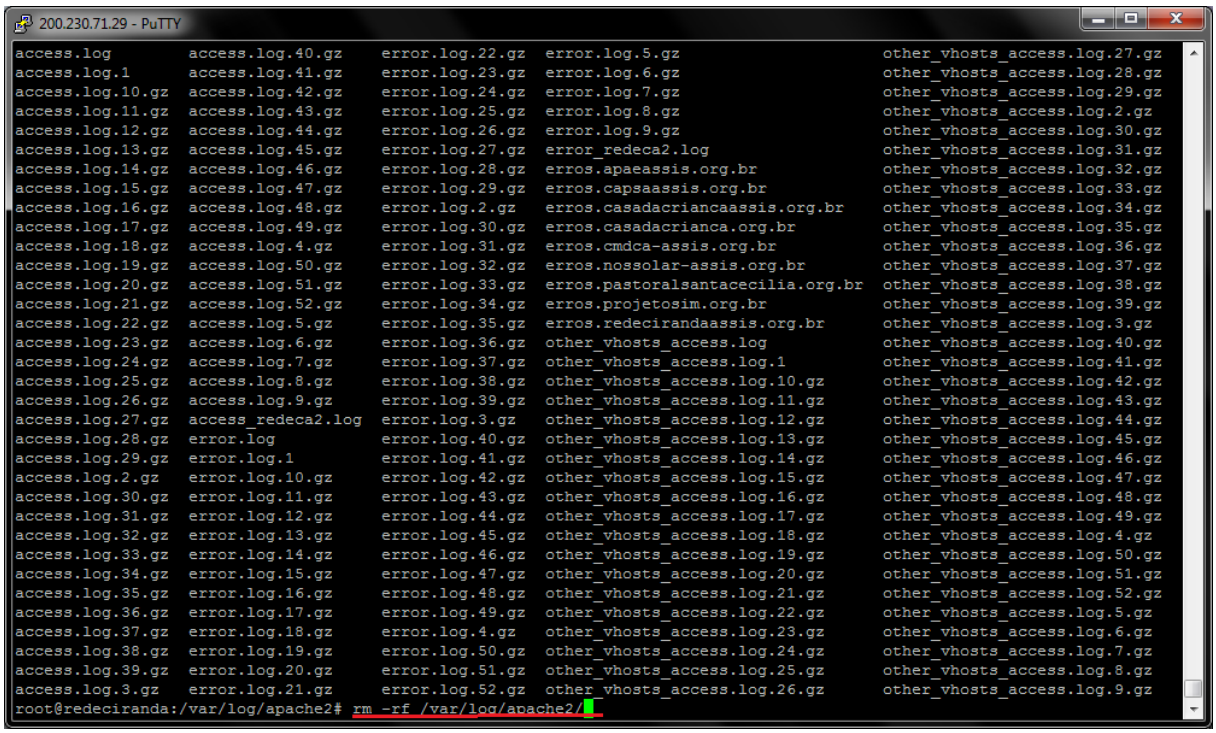


Figura 17 - Logs do servidor Apache Rede Ciranda

Na Figura 17, também foi acessado o servidor como root via ssh e listado todos os logs existentes na pasta /var/log/apache2. Na última linha há um exemplo de exclusão de todos os logs do servidor Apache, que apagaria todos os rastros deixados por qualquer tipo de usuário que tenha passado pelos domínios do servidor.

Como este trabalho é realizado pelo *hacker* ético, foi definido juntamente com o superior do setor de TI, que não seria necessário realizar a exclusão dos logs, portanto, os passos para a exclusão foram apenas demonstrados e não executados.

6 RESULTADOS E CONCLUSÃO

Para iniciar a proteção das informações do Projeto Rede Ciranda, foi elaborado um documento contendo políticas de Segurança da Informação. Este documento (ver Apêndice A) foi totalmente baseado nas necessidades do Projeto, focado em manter uma organização plena, e evitar qualquer descuido que possa comprometer a continuidade e privacidade dos serviços oferecidos.

Este documento também tem o objetivo de melhorar a Engenharia Social do Projeto, que no contexto de segurança da informação, refere-se à manipulação psicológica de pessoas para a execução de ações ou divulgação de informações confidenciais, mesmo que seja de forma inocente. O documento deverá ser repassado e continuado pelos funcionários do setor de TI do Projeto.

A fonte de energia ininterrupta foi trocada por outra em perfeito estado, garantindo manter a disponibilidade dos serviços em caso de queda de energia.

Também foram instalados antivírus gratuitos nos computadores dos funcionários, passando mais de segurança na hora de navegar na internet, acessar e-mails, etc.

Antes de iniciar a parte prática, os testes e correções, foi criada uma regra básica de *firewall* no servidor Rede Ciranda utilizando *iptables*. O *iptables* é uma ferramenta que administra o módulo *netfilter* [7] do sistema operacional. Para usá-lo é necessário possuir direitos administrativos no equipamento.

Foi configurado a *chain*[8] *INPUT* como *DROP* e a *OUTPUT* como *ACCEPT*. Em outras palavras, o servidor poderia sair para qualquer lugar, mas ninguém poderia se conectar nele. Depois foram liberados alguns pacotes dos protocolos icmp, udp e tcp, de acordo com as necessidades do Projeto Rede Ciranda.

[7] O netfilter é um módulo que fornece ao sistema operacional Linux as funções de firewall, NAT e log dos dados que trafegam por rede de computadores. Disponível em: https://pt.wikipedia.org/wiki/Netfilter.

[8] As chains são os locais onde as regras são armazenadas. Disponível em: http://www.vivaolinux.com.br/artigo/Seguranca-com-iptables-1?pagina=2.

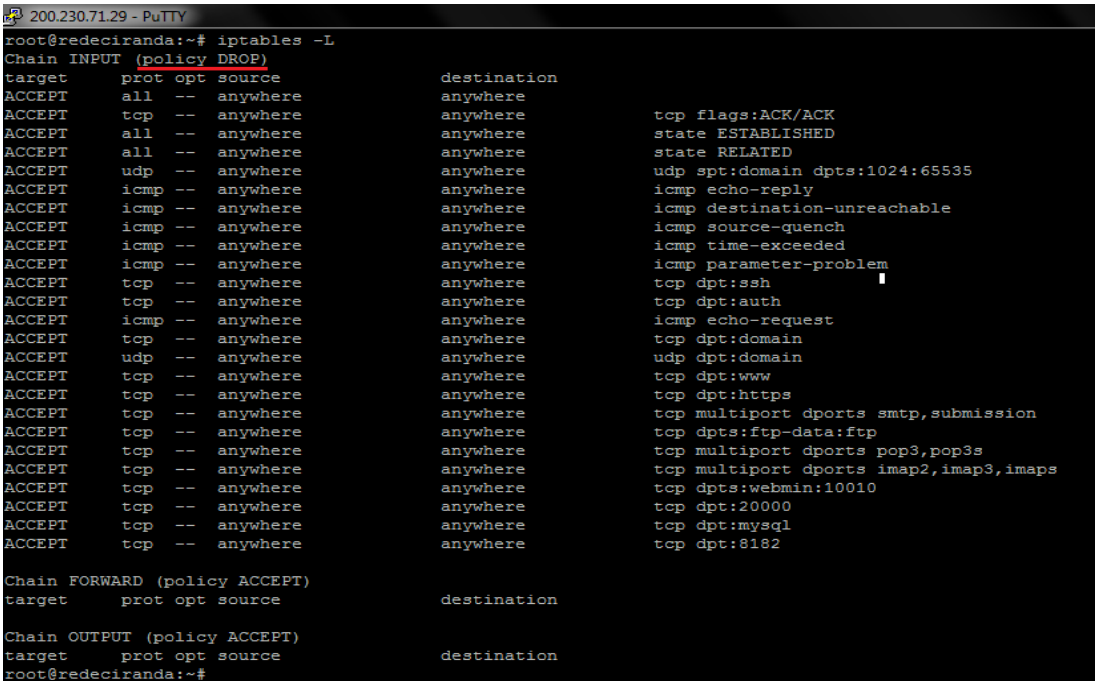


Figura 18 - Regras de *firewall* do servidor Rede Ciranda

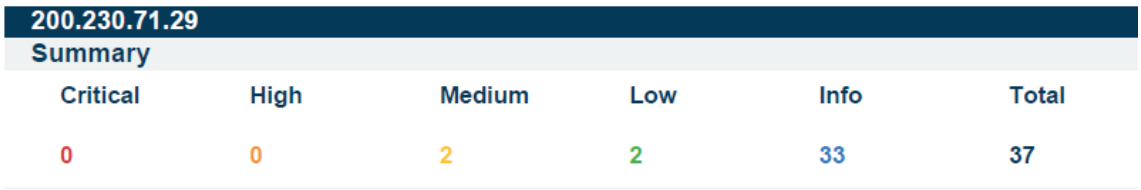
Na fase de reconhecimento e varredura, foi possível levantar pequenas informações a respeito dos serviços do Projeto Rede Ciranda. Obtiveram-se como resultado algumas portas abertas e algumas informações a respeito do host. Estes resultados podem ser considerados como vulnerabilidades, quando não tomadas medidas a respeito.

O *Firewall* implementado se encarrega de manter as demais portas fechadas ou filtradas. A política de senhas fortes, que já era implantada, foi reforçada, então o risco de um ataque bem sucedido é bem pequeno ou até impossível de ser realizado por um atacante externo.

Outra solução para evitar problemas com portas abertas é trocar as senhas padrão de qualquer serviço ou equipamento. Como exemplo, foi feito uma varredura para verificar se há senhas em branco no SGBD MySql, que utilizada a porta 3306 aberta. Para isso foi realizada uma varredura com a ferramenta nmap juntamente com o script empty-password.nse e foi confirmado que não há senhas em branco.

Com a ferramenta Nessus, foram encontradas 4 vulnerabilidades e 33 informações, mas nada preocupante, pois nenhuma possui risco alto ou crítico.

Os resultados de log do *SecurityCenter* do Nessus resultam em “*Info*” (Informação) para êxitos, “*Critical*” (Crítico) para falhas grotescas, “*High*” (Alto) para falhas, “*Medium*” (Médio) para inconclusivos (por exemplo: verificação de permissões para um arquivo que não foi encontrado no sistema) e “*Low*” (Baixo) para riscos muito baixos(Tenable, *Network Security*, 2014).



200.230.71.29

Summary

Critical	High	Medium	Low	Info	Total
0	0	2	2	33	37

Figura 19 - Log Nessus de vulnerabilidades do Projeto Rede Ciranda

No Joomla foram encontradas 26 vulnerabilidades/informações utilizando a ferramenta Joomscan, porém apenas a primeira possui uma falha mais evidente, onde a varredura aponta que as defesas genéricas implementadas no arquivo htacess.txt não estão disponíveis, portanto, é mais provável uma exploração de sucesso. Para resolver esta vulnerabilidade, o Joomla foi atualizado da versão 2.5.11 de 2013 para a versão mais atual 3.4.

Na fase de ganho de acesso, na pele de um atacante externo sem um bom conhecimento sobre o alvo, seria muito difícil ou até impossível obter acesso a qualquer serviço e equipamento do Projeto Rede Ciranda.

Para exemplificar essa dificuldade, a primeira tentativa de invasão foi pela ferramenta xHydra, configurada para tentar acessar o servidor do Projeto pelo protocolo SSH à partir das senhas contidas no arquivo senhas.txt. Neste arquivo foram digitadas senhas padrão e mais conhecidas, consideradas senhas fracas. A tentativa de ganho de acesso foi fracassada.

Para demonstrar um ganho de acesso com êxito, foi utilizado o Metasploit para invadir o SGBD MySql juntamente com o módulo auxiliar *mysql_login* e mais um arquivo contendo usuários e outro contendo senhas possíveis. Porém, somente foi possível obter sucesso neste ataque porque neste trabalho o tipo de *penetration test* é o *White Box*, que é quando o *hacker* ético tem total conhecimento sobre o ambiente a ser

explorado. Como a política de senhas do Projeto Rede Ciranda é muito forte, seria impossível realizar esta invasão.

O Tomcat, quando configurado por administradores displicentes ou sem conhecimentos, pode levar a configurações padrões e, consequentemente, o ganho de acesso se tornará uma tarefa fácil.

Ainda utilizando o Metasploit foi apresentado um ataque de ganho de acesso ao servidor Tomcat do Projeto Rede Ciranda. Neste ataque, foi utilizado o *exploit* auxiliar tomcat_mgr_login, setado as word lists padrão para Tomcat, determinado a porta 8182 e aplicado o exploit. Não foi obtido êxito, pois o usuário e a senha não foram encontrados nas *word lists* padrão, concluindo que este serviço foi configurado corretamente.

Para verificar se o Projeto Rede Ciranda possui vulnerabilidades Sql, foi utilizado o Sistema Cadastro como cobaia. Este é um sistema *web* que possui uma tela de *login*, para obter acesso como usuário comum ou administrador. A ferramenta nmap foi utilizada com o parâmetro –u para que pudesse ser oferecido o endereço do alvo: sqlmap –u 200.230.71.29/SistemaCadastro. Também não foi obtido sucesso, mostrando que este sistema não pode ser facilmente violado por qualquer atacante, sem conhecimentos.

As demonstrações de ganho de acesso acima são impossíveis de serem realizadas somente por atacantes que não possuem conhecimento algum sobre o alvo. A maioria dos ataques bem-sucedidos está vinculada ao despreparo das pessoas que, de uma forma inocente ou equivocada, habilitam oportunidades que podem ser usadas com grande potencial. Para prevenir que isso aconteça com o Projeto Rede Ciranda, foi elaborado um documento contendo políticas de segurança da informação do Projeto Rede Ciranda com o objetivo de melhorar a Engenharia Social do Projeto, que no contexto de segurança da informação, refere-se à manipulação psicológica de pessoas para a execução de ações ou divulgação de informações confidenciais, mesmo que seja de forma inocente. O documento deverá ser repassado e continuado pelos funcionários do setor de TI do Projeto.

Para dar maior durabilidade às medidas de segurança da informação aplicadas ao Projeto Rede Ciranda, existem contramedidas de ganho de acesso que foram utilizadas neste trabalho e devem continuar servindo de base:

- Utilizar senhas fortes que contenham mais de oito caracteres e números, letras maiúsculas, minúsculas e símbolos;
- Manter o antivírus das máquinas de funcionários sempre atualizado;
- Manter um *firewall*;
- Trocar as senhas padrão de qualquer equipamento;
- Manter os sistemas operacionais atualizados e corrigidos;
- Na instalação de qualquer serviço, a atenção deve ser redobrada para que as configurações não estejam padrão.

Depois de finalizada todas as etapas definidas para este trabalho, obtém-se um relatório final com as informações mais relevantes sobre o trabalho e o teste de penetração realizado (ver Apêndice B). Este relatório será passado ao superior do departamento de TI do Projeto Rede Ciranda para continuar mantendo a transparência do trabalho realizado pelo hacker ético.

Testes de invasão devem fazer parte do programa de segurança da informação das empresas. Há diversas formas de se tratar a segurança de uma rede, sistema ou aplicação, e o teste de invasão é apenas uma das possíveis ferramentas, porém é a que apresenta resultados mais concretos, com o mínimo de falsos positivos/negativos. É preciso atentar para a importância de auditorias preventivas, além de compreender a necessidade da percepção exata da exposição dos ativos de TI aos riscos existentes.

Com esses resultados, conclui-se que a segurança eletrônica está cada vez mais ocupando uma das primeiras posições em prioridades de investimento das empresas. Entende-se que um projeto de segurança, além de definir as tecnologias a serem utilizadas, deve contemplar também a definição dos procedimentos para que a solução seja realmente efetiva.

A política de segurança norteará todo o sistema de segurança de acesso à rede. Por se tratar de uma definição “política”, não existe um produto pronto e que seja facilmente encontrado no mercado, tendo de ser desenvolvido em conjunto com a

necessidade da empresa. O resultado desta análise é um produto focado nas características de disponibilidade da informação. As normas e procedimentos refletem as diretrizes das empresas no item segurança, tais como definições de formas de conexões, procedimentos operacionais, escopo de responsabilidade dos usuários e administradores, políticas de utilização de senhas, procedimentos para situações de contingência e os procedimentos de recuperação da rede em caso de violações.

A monitoração da solução de segurança de acesso à rede não têm garantia eterna. Estas soluções são seguras apenas enquanto não são violadas.

Quando já se tem implantada uma norma ou solução de segurança de rede, a realização de testes que simulam a ação de um invasor (interno ou externo) para verificar os pontos vulneráveis eventualmente existentes sempre será necessária. Após os testes, obtém-se um diagnóstico preciso com as indicações de melhorias a serem adotadas.

Poderemos dizer se a segurança da informação no ambiente corporativo estará organizada, quando estas informações somente forem acessadas pelos respectivos interessados, com uma ampla facilidade de consulta, buscando sempre o conforto do cliente, do fornecedor ou de qualquer pessoa que faça parte deste universo, independentemente de onde estiver, e para finalizar, teremos a certeza que imagem da empresa ficará preservada perante o mercado.

REFERÊNCIAS BIBLIOGRÁFICAS

ABNT ISO/IEC 27002 – 1ª Ed. – 2005. Tecnologia da Informação – Técnicas de Segurança – Código de prática para a gestão da segurança da informação. Associação Brasileira de Normas Técnicas – Rio de Janeiro.

CARUSO, Carlos A. A Segurança em Microinformática e em redes locais. São Paulo. Editora: LTC, 1995

Ferramentas Kali Linux – disponível em <http://www.hacks.pt/ferramentas-kali-linux/recolha-de-informacao/analise-dns/nmap/> Acesso em: 17/03/2015

GIAVAROTO, Sílvio César Roxo; SANTOS, Gerson Raimundo dos. Kali Linux – Introdução ao Penetration Testing – Rio de Janeiro: Editora Ciência Moderna Ltda., 2015.

HEFFERAN, Rossylenne; BS 7799 – *Information Security Management*, 2000, disponível em <http://www.istc.org.uk>

ISO 17799. ABNT NBR ISO/IEC 17799:2005 – Tecnologia da Informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação. Associação Brasileira de Normas Técnicas – Rio de Janeiro: ABNT, 2005.

NAKAMURA, Emilio Tissato; GEUS, Paulo Lício de. Segurança de redes em ambientes corporativos. São Paulo: Novatec, 2007.

NORTHCUTT; STEPHEN. Segurança e Prevenção de Redes. Editora: EDITORA BERKELEY, 2001.

OLIVEIRA, Salomão. Vírus: Agentes Digitais do Crime. Evidencia Digital Magazine. Edição 2, 2004.

PWC, Serviços Profissionais Ltda – 2014. Pesquisa Global de Segurança da Informação 2014 - (*The Global State of Information Security*® Survey 2014).

SCHNEIER, Bruce Segurança.com: Segredos e mentiras sobre a proteção na vida digital. São Paulo. Editora: CAMPUS, 2001.

Secretaria de Fiscalização da Informação - 4ª Ed – Brasília, 2012. Boas práticas em segurança da informação/ Tribunal de Contas da União.

SOLMS, Rossouw von; *Information security management* (3): *the Code of Practice for Information Security Management* (BS7799), Information Management & Computer Security, Vol 6 Issue 5, Port Elizabeth, South Africa, 1998.

Tenable, Network Security. Verificações de conformidade do Nessus, Configurações e conteúdo do sistema de auditoria, 14 de janeiro de 2014.

XAVIER, Ana Lúcia Pintar et al.. Rede Ciranda: Desenhando novos caminhos para o trabalho social com crianças e adolescentes. São Carlos: Pedro & João Editores, 2012.

CRONOGRAMA DE ATIVIDADES

Atividades	2014			2015								
	Out	Nov	Dez	Jan	Fev	Mar	Abr	Mai	Jun	Jul	Ago	Set
Leitura e estudos de referências bibliográficas												
Elaboração do pré-projeto												
Entrega do pré-projeto												
Estudos sobre as práticas de SI												
Estudos sobre as ferramentas que serão utilizadas												
Entrega e apresentação da qualificação												
Ajustes finais e otimização estrutural												
Entrega e apresentação do trabalho final												

APÊNDICE A - POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO DO PROJETO REDE CIRANDA 2015

Este documento tem o objetivo nortear a gestão da segurança das informações e evitar futuros transtornos. Deverá ser continuado e divulgado dentro do Projeto Rede Ciranda.

***Hardening*:**

Aplicar procedimento de blindagem dos equipamentos (*hardening*) para prover proteção a esses recursos.

Pentest:

Realizar *PenTest* (teste de penetração) no perímetro interno e externo para identificação de vulnerabilidades pelo menos uma vez ao ano ou após modificações significativas no ambiente.

Acesso aos serviços:

A utilização dos sistemas oferecidos pelo Projeto Rede Ciranda só poderá ser realizada por terceiros por meio de *login* e senha criados pelo responsável pelo setor de TI.

Segregação de funções:

Um critério de segregação de funções baseado em “cargos/ funções/ atividades/ cliente/ operação’, deve estar estabelecido, de forma que o funcionário tenha somente acesso ao indispensável para a execução da atividade para a qual foi contratado.

Gerenciamento de senha do usuário:

A política de senhas ‘forte’ deve ser mantida e passada adiante.

Procedimentos seguros de utilização das máquinas:

Somente pessoas autorizadas devem ter acesso aos computadores do Rede Ciranda.

Navegação internet:

Somente acessos a sites necessários para o desenvolvimento das atividades do funcionário. Caso contrário o Firewall deve ser reforçado.

Ferramenta de Captura Remota:

O acesso remoto a estações de trabalho e servidores pode trazer risco de acessos indevidos, portanto deverão ser aplicados controles para minimizar esses riscos.

Manter a parte tecnológica atualizada:

Manter o Sistema Operacional e softwares atualizados com versões suportadas pelo fabricante.

Registros e proteção de Trilhas de Auditoria:

Devem ser padronizados os registros de logs de auditoria para as atividades de usuários, exceções e outros eventos de rede e sistemas.

Política para o uso de controles criptográficos:

Um conjunto de regras padronizando as técnicas criptográficas e a aplicação adequada das mesmas deve existir.

Mídias em trânsito:

O transporte físico de mídias (externo) aos limites da Organização deve ser efetuado de forma segura.

Controles contra códigos maliciosos:

Softwares maliciosos como vírus de computador, cavalos de Tróia e "*worms*" de rede, devem ser controlados através de software antivírus atualizado em todas as estações de trabalho e servidores, entre outros.

Gestão de mudanças:

Deve haver um processo formalizado para gestão de mudanças.

Separação dos recursos de desenvolvimento, teste e de produção:

Perfis diferentes de acesso de usuários em situação de desenvolvimento, de teste e de produção.

Cópias de segurança das informações:

Prover cópias de segurança das informações conforme periodicidade acordada.

Política de mesa limpa:

Orientar os funcionários, disciplinando cuidados com a política de mesa limpa. Após o expediente é obrigatório.

Política de tela limpa:

Funcionários devem ser orientados sobre a necessidade de desligamento dos computadores pessoais, terminais de computador e impressoras quando não estiverem sendo utilizados.

Responsabilidades e Procedimentos (Incidentes de Segurança da Informação):

Quanto aos incidentes de Segurança da Informação, deve haver planos de respostas para cada um dos incidentes, prevendo falhas, códigos maliciosos, negação de serviço etc.

Recomendações para classificação:

Um procedimento para classificar informações, que defina um conjunto apropriado de níveis de proteção e determine a necessidade de medidas especiais de tratamento para cada um desses níveis deverá existir.

Acordos de confidencialidade:

Deve existir um documento assinado por todos os funcionários do Projeto Rede Ciranda para que estejam cientes das suas responsabilidades de Segurança da Informação.

Conscientização, educação e treinamento em segurança da informação:

Um programa para garantir que os funcionários sejam conscientizados em Segurança da Informação deverá ser aplicado, desde a contratação e em campanhas periódicas.

Remoção de propriedade:

Um fluxo formalizado de retirada e devolução de equipamentos (ex: dispositivos de armazenamento externo), informações ou software deve estar sendo aplicado, contendo a descrição do ativo e motivo da retirada, autorizada pelo responsável do setor.

Controles de entrada física:

Controles de entrada apropriados devem estar implementados para assegurar que somente pessoas autorizadas tenham acesso físico a empresa e áreas restritas (ex: Datacenter e Operação/Atendimento a Clientes).

Continuidade de Negócios:

A prestação do serviço não pode ser interrompida. Quando necessária a interrupção por motivo maior, deve ser informado o tempo que os recursos ficarão indisponíveis aos usuários.

APÊNDICE B - RELATÓRIO PENTEST – REDE CIRANDA 2015

Hacker Ético – Vinícius Marquesini Terzi

Tipo de *Pentest* – *WhiteBox*

Alvo – Projeto Rede Ciranda

Documentação com o objetivo de manter registros de todas as atividades de forma transparente, contendo informações como, escopo do teste de penetração realizado, ferramentas utilizadas, lista de vulnerabilidades identificadas e recomendações para execução de melhorias.

1 ESCOPO

Os testes de penetração aplicados do Projeto Rede Ciranda foram baseados na metodologia definida pelo programa EC-Council C|EH *Certified Ethical Hacker*, baseando-se no livro Kali Linux, Introdução ao *Penetration Testing*. As fases do teste de penetração são divididas em cinco etapas:

1.1 Reconhecimento

O reconhecimento é a metodologia que foi utilizada para a obtenção de informações a respeito do Projeto Rede Ciranda. Apesar de o *hacker* ético já obter muitas informações, foram utilizadas duas ferramentas nesta etapa, com o intuito de verificar a facilidade que qualquer atacante teria em levantar informações a respeito dos serviços do Projeto.

1.2 Varredura ou Scanning

Essa técnica é muito comum e foi utilizada para reunir informações a respeito do estado das portas e a descoberta de serviços do Projeto. O rastreamento de portas consiste em enviar uma mensagem por vez para cada uma das portas, explorando as mais comuns e até as menos usadas. Com base na análise de uma varredura pode-se, então, determinar se a porta está sendo ou não utilizada e, caso esteja, o invasor poderá explorá-la de inúmeras maneiras a fim de encontrar possíveis falhas de segurança.

1.3 Ganho de acesso

Após a execução das tarefas de reconhecimento e varredura, cujos objetivos foram tentar obter informações valiosas a respeito do Projeto Rede Ciranda na visão de um atacante externo, inicia-se os processos de tomada do sistema, ou seja, o ganho de acesso.

Nesta etapa foi utilizada a técnica de ataque de dicionário, que é quando o invasor cria um arquivo com dezenas, centenas ou milhares de palavras para usuário e/ou senha e o se *software* encarrega de fazer o resto. Além deste, existe o ataque de força bruta, onde o *software* utiliza um algoritmo de combinação que se encarrega de fazer as tentativas de quebras de senha, podendo utilizar ou não um dicionário.

1.4 Manutenção do acesso

Após a tomada do sistema, o invasor pode executar a chamada manutenção, ou seja, tática que lhe permitirá plantar, *rootkits*, cavalos de troia, etc. Isto possibilita um possível retorno e existem invasores que até corrigem vulnerabilidades para garantir que somente ele fará novas incursões.

O *pentester* não precisa garantir seu retorno, pois após o termino da auditoria, deverá arrumar a casa e deixar tudo como estava. Portanto não foi necessário executar esta etapa na prática, e sim, apenas saber de sua existência.

1.5 Cobertura de rastros

Após a tentativa ou sucesso do ganho de acesso, o atacante tentará apagar seus rastros e limpar a casa, ou seja, excluir os *logs* do sistema.

Nesta etapa, foi mostrado onde se encontram os principais logs do Projeto Rede Ciranda e algumas maneiras de excluí-los.

Conforme definido juntamente com o superior do setor de TI, não foi necessário realizar a exclusão dos logs, portanto, os passos para a exclusão foram apenas demonstrados e não executados.

2 FERRAMENTAS UTILIZADAS NO PROJETO REDE CIRANDA

2.1 Reconhecimento

Na etapa de reconhecimento foram utilizadas duas ferramentas: Dmitry e NETCAT.

Para levantar algumas informações iniciais foi utilizada a ferramenta dmitry. Com ela foi possível realizar uma varredura de portas TCP, e uma pesquisa whois, que serve para identificar o proprietário de um site através do nome de domínio do Projeto.

O NETCAT, conhecido pelos analistas de segurança como canivete suíço, além de permitir conexões reversas, também é uma excelente opção na busca de informações a respeito de serviços.

2.2 Varredura

Uma das principais ferramentas utilizadas nesta etapa foi o NMAP. Suas principais funcionalidades são as varreduras de portas, descoberta de serviços e a detecção de versões.

Também foi utilizado o Nessus, que é considerado como um dos melhores e mais potentes scanners de vulnerabilidades. Ele não está presente no Kali Linux, mas, possui uma versão gratuita. Depois de instalado e configurado, é necessário criar uma política antes de iniciar a análise de vulnerabilidade. Utilizando esta política inicia-se o escaneamento e, ao final é gerado um relatório prévio das vulnerabilidades.

Como o Projeto Rede Ciranda é responsável por manter os sites de algumas instituições citadas anteriormente. Foi utilizada a ferramenta Joomscan para verificar se existem vulnerabilidades no Joomla, que é o sistema de gestão de conteúdo para sites utilizado pelo Projeto.

2.3 Ganho de acesso

Primeiramente foi utilizada a ferramenta xHydra no modo gráfico, que é muito boa quando o assunto é a escalação de privilégios através de quebra de senha on-line.

Outra ferramenta utilizada nesta etapa foi o Metasploit, que é uma ferramenta muito poderosa quando o assunto é ganho de acesso. Ela possui algumas interfaces, e para este trabalho foi utilizado o MSFCONSOLE, que é uma interface do metasploit que utiliza linhas de comando.

O sqlmap é uma ferramenta de código aberto, desenvolvida em Python e foi utilizada para verificar falhas envolvendo o banco de dados.

2.4 Manutenção de acesso e Cobertura de rastros

Nas duas últimas etapas não foi utilizada nenhuma ferramenta. A fase de manutenção de acesso foi apenas citada, enquanto a de cobertura de rastros foi apenas mostrado onde se encontram os principais logs do Projeto Rede Ciranda e algumas maneiras de excluí-los.

3 VULNERABILIDADES E SOLUÇÕES

Antes de iniciar a parte prática, os testes e correções, foi criada uma regra básica de *firewall* no servidor Rede Ciranda utilizando *iptables*. O *iptables* é uma ferramenta que administra o módulo *netfilter* do sistema operacional. Para usá-lo é necessário possuir direitos administrativos no equipamento.

Na fase de reconhecimento e varredura, foi possível levantar pequenas informações a respeito dos serviços do Projeto Rede Ciranda. Obtiveram-se como resultado algumas portas abertas e algumas informações a respeito do host. Estes resultados podem ser considerados como vulnerabilidades, quando não tomadas medidas a respeito.

O *Firewall* implementado se encarrega de manter as demais portas fechadas ou filtradas. A política de senhas fortes, que já era implantada, foi reforçada, então o risco de um ataque bem sucedido é bem pequeno ou até impossível de ser realizado por um atacante externo.

Outra solução para evitar problemas com portas abertas é trocar as senhas padrão de qualquer serviço ou equipamento. Como exemplo, foi feito uma varredura para verificar se há senhas em branco no SGBD MySql, que utilizada a porta 3306 aberta. Para isso foi realizada uma varredura com a ferramenta nmap juntamente com o script empty-password.nse e foi confirmado que não há senhas em branco.

Com a ferramenta Nessus, foram encontradas 4 vulnerabilidades e 33 informações, mas nada preocupante, pois nenhuma possui risco alto ou crítico.

Os resultados de log do *SecurityCenter* do Nessus resultam em "*Info*" (Informação) para êxitos, "*Critical*" (Crítico) para falhas grotescas, "*High*" (Alto) para falhas, "*Medium*" (Médio) para inconclusivos (por exemplo: verificação de permissões para um arquivo que não foi encontrado no sistema) e "*Low*" (Baixo) para riscos muito baixos(Tenable, *Network Security*, 2014).

No Joomla foram encontradas 26 vulnerabilidades/informações utilizando a ferramenta Joomscan, porém apenas a primeira possui uma falha mais evidente, onde a varredura aponta que as defesas genéricas implementadas no arquivo htacess.txt não estão disponíveis, portanto, é mais provável uma exploração de sucesso. Para resolver esta vulnerabilidade, o Joomla foi atualizado da versão 2.5.11 de 2013 para a versão mais atual 3.4.

Na fase de ganho de acesso, na pele de um atacante externo sem um bom conhecimento sobre o alvo, seria muito difícil ou até impossível obter acesso a qualquer serviço e equipamento do Projeto Rede Ciranda.

Para exemplificar essa dificuldade, a primeira tentativa de invasão foi pela ferramenta xHydra, configurada para tentar acessar o servidor do Projeto pelo protocolo SSH à partir das senhas contidas no arquivo senhas.txt. Neste arquivo foram digitadas senhas padrão e mais conhecidas, consideradas senhas fracas. A tentativa de ganho de acesso foi fracassada.

Para demonstrar um ganho de acesso com êxito, foi utilizado o Metasploit para invadir o SGBD MySql juntamente com o módulo auxiliar *mysql_login* e mais um arquivo contendo usuários e outro contendo senhas possíveis. Porém, somente foi possível obter sucesso neste ataque porque neste trabalho o tipo de *penetration test* é o *White Box*, que é quando o *hacker* ético tem total conhecimento sobre o ambiente a ser explorado. Como a política de senhas do Projeto Rede Ciranda é muito forte, seria impossível realizar esta invasão.

O Tomcat, quando configurado por administradores displicentes ou sem conhecimentos, pode levar a configurações padrões e, consequentemente, o ganho de acesso se tornará uma tarefa fácil.

Ainda utilizando o Metasploit foi apresentado um ataque de ganho de acesso ao servidor Tomcat do Projeto Rede Ciranda. Neste ataque, foi utilizado o *exploit* auxiliar tomcat_mgr_login, setado as word lists padrão para Tomcat, determinado a porta 8182 e aplicado o exploit. Não foi obtido êxito, pois o usuário e a senha não foram encontrados nas *word lists* padrão, concluindo que este serviço foi configurado corretamente.

Para verificar se o Projeto Rede Ciranda possui vulnerabilidades Sql, foi utilizado o Sistema Cadastro como cobaia. Este é um sistema *web* que possui uma tela de *login*, para obter acesso como usuário comum ou administrador. A ferramenta nmap foi utilizada com o parâmetro –u para que pudesse ser oferecido o endereço do alvo: sqlmap –u 200.230.71.29/SistemaCadastro. Também não foi obtido sucesso, mostrando que este sistema não pode ser facilmente violado por qualquer atacante, sem conhecimentos.

As demonstrações de ganho de acesso acima são impossíveis de serem realizadas somente por atacantes que não possuem conhecimento algum sobre o alvo. A maioria dos ataques bem-sucedidos está vinculada ao despreparo das pessoas que, de uma forma inocente ou equivocada, habilitam oportunidades que podem ser usadas com grande potencial. Para prevenir que isso aconteça com o Projeto Rede Ciranda, foi elaborado um documento contendo políticas de segurança da informação do Projeto Rede Ciranda com o objetivo de melhorar a Engenharia Social do Projeto, que no contexto de segurança da informação, refere-se à manipulação psicológica de pessoas para a execução de ações ou divulgação de informações confidenciais, mesmo que seja de forma inocente. O documento deverá ser repassado e continuado pelos funcionários do setor de TI do Projeto.

Para dar maior durabilidade às medidas de segurança da informação aplicadas ao Projeto Rede Ciranda, existem contramedidas de ganho de acesso que foram utilizadas neste trabalho e devem continuar servindo de base:

- Utilizar senhas fortes que contenham mais de oito caracteres e números, letras maiúsculas, minúsculas e símbolos;
- Manter o antivírus das máquinas de funcionários sempre atualizado;
- Manter um *firewall*;

- Trocar as senhas padrão de qualquer equipamento;
- Manter os sistemas operacionais atualizados e corrigidos;
- Na instalação de qualquer serviço, a atenção deve ser redobrada para que as configurações não estejam padrão.