Centro Universitário de Brasília
Instituto CEUB de Pesquisa e Desenvolvimento - ICPD

SIDNEY OLIVEIRA CIRQUEIRA

AUDITORIA DE SEGURANÇA UTILIZANDO TESTE DE INVASÃO DE REDES EM AMBIENTES DE TECNOLOGIA DA INFORMAÇÃO

BRASÍLIA
2015

SIDNEY OLIVEIRA CIRQUEIRA

AUDITORIA DE SEGURANÇA UTILIZANDO TESTE DE INVASÃO DE REDES EM AMBIENTES DE TECNOLOGIA DA INFORMAÇÃO

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para obtenção de Certificado de Conclusão de Curso de Pós-graduação em Rede de Computadores com Ênfase em Segurança.

Orientador: Prof. Msc Marco Antônio de Oliveira Araujo.

BRASÍLIA

2015

SIDNEY OLIVEIRA CIRQUEIRA

AUDITORIA DE SEGURANÇA UTILIZANDO TESTE DE INVASÃO DE REDES EM AMBIENTES DE TECNOLOGIA DA INFORMAÇÃO

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para obtenção de Certificado de Conclusão de Curso de Pós-graduação em Rede de Computadores com Ênfase em Segurança.

Orientador: Prof. Msc Marco Antônio de Oliveira Araujo.

Brasília, 06 de Abril de 2015

Banca Examinadora

_____

Prof. Sylas Rodrigues Mendes

_____

Prof.ª Dra Tânia Cristina da Silva Cruz

Dedico este trabalho a minha esposa Samara Rayani Carmo Silva por sua dedicação, atenção e compreensão, sempre permanecendo ao meu lado em todos os momentos.

AGRADECIMENTOS

Agradeço primeiramente a Deus e aos meus pais por terem me dado essa oportunidade. A minha esposa Samara Rayani por sua dedicação, amor e fidelidade. E ao meu amigo Wellington Rodrigues por tudo que ele me ensina todos os dias como pessoa e como profissional da área de Segurança da Informação.

RESUMO

Com o crescimento dos sistemas de informação e das redes de computadores, consequentemente novas ameaças e vulnerabilidades surgem. A interconexão dessas redes ou dispositivos eletrônicos com a internet deixam as organizações expostas a diversos tipos de ataques que podem causar danos irreversíveis a imagem ou aos dados sigilosos nelas armazenados. Para que os sistemas se tornem resistentes e com níveis de segurança aceitáveis, alguns procedimentos de controles são aplicados para aferir se as proteções das redes de computadores estão em conformidade com as principais normas de segurança nacionais e internacionais. O objetivo deste trabalho é identificar a importância de um processo conhecido como Auditoria Teste de Invasão, um método que realiza simulações reais de ataque aos ativos de informação das empresas que solicitam este serviço. Para alcançar esse objetivo, o trabalho buscou nos teóricos que conceituam os fundamentos do tema abordado, juntamente com um estudo de caso que demostrou de forma pratica quais são os procedimentos que giram em torno de um *pentest*. A principal conclusão desse trabalho é que a contratação de serviços de auditoria teste de invasão para a execução de procedimentos que testem os controles aplicados no âmbito da segurança de redes vai além da identificação de potenciais vulnerabilidades, incluindo também uma avaliação do risco real que estas vulnerabilidades representam para a infraestrutura computacional, realizando posteriormente a correção das fragilidades dos ambientes informatizados corporativos.

Palavras-chave: Segurança da Informação. Auditoria. Teste de Invasão. Pentest.

ABSTRACT

With the growth of information systems and computer networks, thus new threats and vulnerabilities emerge. The interconnection of these networks or electronic devices to the internet leave organizations exposed to various types of attacks that can cause irreversible damage to the image or they store sensitive data. For systems become resistant and with acceptable safety levels, some control procedures are applied to assess whether the protections of computer networks are in accordance with the main provisions of national and international security. The objective of this work is to identify the importance of a process known as Audit Penetration Testing, a method that performs actual simulations of attack to information assets of the companies requesting this service. To achieve this goal, the study aimed to conceptualize the theoretical fundamentals of the subject, along with a case study that demonstrated in a practical way what are the procedures that revolve around a pentest. The main conclusion of this study is that hiring audit penetration testing services for the implementation of procedures to test the controls applied in the network security framework goes beyond the identification of potential vulnerabilities, also including an assessment of the real risk that these vulnerabilities pose to the computing infrastructure and subsequently to prepare the correction of weaknesses in corporate computing environments.

.

Key Words: Information Security. Audit. Penetration Testing. Pentest.

SUMÁRIO

INTRODUÇÃO

Devido ao grande volume de dados que são manipulados a cada segundo pelos sistemas de informação, surge a necessidade da proteção dos ativos corporativos com utilização de mecanismos de segurança da informação para que os valores financeiros das diversas empresas permaneçam seguros. A falta de prevenção e a indisponibilidade desses sistemas podem ocasionar uma elevada perda financeira, consequência da interrupção de processos corporativos, e que o vazamento de informações podem levar danos irreversíveis a suas imagens.

Segundo a ABNT. NBR ISO/IEC 27002:2005 (2005, p. 9):

> 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. Isto é especialmente importante no ambiente dos negócios, cada vez mais interconectado. Como um resultado deste incrível aumento da interconectividade, a informação está agora exposta a um crescente número e a grande variedade de ameaças e vulnerabilidades.

A segurança da informação tem como objetivo preservar os três princípios básicos para garantir a implementação desta pratica: Confidencialidade, Integridade e Disponibilidade.

A segurança é obtida a partir de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de hardware e software.

Com o intuito de aprofundar os conhecimentos sobre como implementar e verificar os controles adequados de segurança da informação, é que este trabalho pretende identificar se as técnicas aplicadas para proteção da informação nos ambientes de tecnologia da informação estão em conformidade e resistentes a potenciais invasores.

A verificação da conformidade técnica envolve a análise dos sistemas operacionais para garantir que controles de hardware e software foram corretamente implementados.

Motivação

A proposta deste trabalho é realizar um estudo sobre a importância da pratica da auditoria teste de invasão em redes de computadores.

A confidencialidade, integridade e disponibilidade das estruturas de redes de computadores passam a ser essenciais para o bom andamento das organizações, fazendo com que elas precisem ser protegidas. (NAKAMURA, 2003).

Sobre a visão do autor deste trabalho, a intenção é ampliar o conhecimento pessoal e profissional, proporcionando um melhor desempenho na empresa em que trabalha atualmente e dentro do campo acadêmico na área da segurança da informação. Também tem como principal objetivo se manter atualizado com as novas tecnologias, principais ameaças e vulnerabilidades das redes corporativas no que diz respeito a controles de segurança.

Objetivo Geral

O objetivo geral do trabalho é auditar o ambiente de tecnologia da informação utilizando testes de invasão para verificar se os controles técnicos de segurança foram corretamente implementados.

Objetivos Específicos

O presente estudo tem como objetivos específicos:

1. Identificar a importância da auditoria utilizando teste de invasão em ambientes de tecnologia da informação;
2. Descrever os conceitos de auditoria da segurança da informação, de redes de computadores e testes de invasão;

3. Realizar testes de invasão para verificar vulnerabilidades nos controles de segurança de rede corporativa;
4. Propor recomendações e orientações sobre como sanar as falhas de segurança.

Metodologia

Com o objetivo de analisar a importância da auditoria teste de invasão em ambientes de tecnologia da informação, o trabalho buscou nos teóricos que conceituam segurança da informação, auditoria da segurança da informação e de redes de computadores e testes de invasão.

Além do desenvolvimento da bibliografia com o apoio dos autores referentes no assunto, serão analisadas ferramentas de teste de invasão (*pentest*) para medir a conformidade dos controles de segurança da informação aplicados em determinado ambiente tecnológico.

Para obter informações complementares e ter uma visão pratica deste trabalho, a estratégia será um estudo de caso.

Estrutura da Monografia

O presente trabalho foi estruturado em 3 capítulos:

No primeiro capítulo, apresentam-se os fundamentos teóricos que conceituam o tema abordado neste trabalho no que diz respeito à segurança da informação, auditoria no âmbito da contabilidade e da tecnologia, o segundo capítulo proporciona uma analise mais específica sobre auditoria teste de invasão; no terceiro capítulo, apresentam-se como estudo de caso visando uma demonstração pratica a fim de elucidar a descrição do problema

ocorrido, as atividades realizadas e por fim os resultados alcançados com a contratação da empresa de auditoria de testes de invasão.

1 FUNDAMENTOS TEÓRICOS

1.1 Segurança da Informação

Segurança da informação é 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.

De acordo com Marcos Sêmola (2003), Segurança da informação é definida como uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade.

A segurança de informações visa garantir a integridade, confidencialidade, autenticidade e disponibilidade das informações processadas pela instituição. Boas Praticas em segurança da informação (2012).

Integridade consiste na fidedignidade de informações, sinaliza a conformidade de dados armazenados com relação às inserções, alterações e processamentos autorizados efetuados.

Confidencialidade consiste na garantia de que somente pessoas autorizadas tenham acesso às informações armazenadas ou transmitidas por meio de redes de comunicação.

Autenticidade consiste na garantia da veracidade da fonte das informações. Por meio da autenticação é possível confirmar a identidade da pessoa ou entidade que presta as informações.

Disponibilidade consiste na garantia de que as informações estejam acessíveis às pessoas e aos processos autorizados, a qualquer momento requerido, durante o período acordado entre os gestores da informação e a área de informática.

Segurança da informação é obtida a partir de um conjunto de controles adequados, incluindo politicas, processos, procedimentos, estruturas organizacionais e funções de *hardware* e *software*. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos. (ABNT NBR ISO/IEC 27002:2005).

Para Nakamura e Geus (2007), a confiabilidade, integridade e disponibilidade das redes, passam a ser essenciais para o bom andamento das organizações, fazendo com que elas precisem ser protegidas. A proteção visa a manutenção do acesso às informações que estão sendo disponibilizadas para os usuários. Isso significa que toda informação deve chegar aos usuários de uma forma integra e confiável. A confidencialidade e sigilo também são importantes e, junto com a integridade e a disponibilidade, formam as propriedades mais importantes para a segurança.

A segurança da informação é principal propriedade da empresa para combate aos riscos que a informação fica exposta na internet. Riscos que podem ser ocasionados apenas por um descuido técnico ou humano pode gerar graves problemas para as empresas e negócio, a cada minuto surgem diversas formas de ataque, invasões, vírus entre outros. Portanto, quando se tratam de assuntos relacionados à segurança da informação todas as técnicas, processos e controles aplicados são de extrema importância para proteção dos dados corporativos, prevenção dos riscos e continuidade dos negócios.

1.2 Auditoria

A Auditoria é o ramo da contabilidade que realiza revisões das demonstrações financeiras, sistemas financeiros, registros, transações e operações de uma entidade ou um projeto. A auditoria também indica deficiências no sistema de controle interno e no sistema financeiro gerando, com isso, recomendações e melhorias.

Segundo Attie (2010, p.25), "Auditoria é uma especialização contábil voltada a testar a eficiência e eficácia do controle patrimonial implantado com o objetivo de expressar uma opinião sobre determinado dado".

Ainda segundo o mesmo autor "a contabilidade foi a primeira disciplina desenvolvida para auxiliar e informar ao administrador, sendo ela formadora de uma especialização denominada auditoria, destinada a ser usada como ferramenta de confirmação da própria contabilidade." (2010, p.25).

A partir das definições elencadas acima, é possível entender que o objetivo da auditoria é auxiliar na administração, proporcionando analise e sugestões a respeito das atividades de controles internos, com a finalidade de confirmar as demonstrações financeiras quanto ao patrimonial da empresa.

Existem dois tipos de auditoria: interna e externa. A externa mantém a conformidade com as regulamentações exigidas por leis ou pelo mercado, enquanto a interna é uma preparação para a externa, verificando se os processos da empresa estão prontos para serem auditados por terceiros. (AZEREDO, 2006).

Alguns conceitos básicos relacionados com qualquer tipo de auditoria são campo, âmbito, natureza da auditoria e área de verificação. O campo da auditoria compõe-se de aspectos como objeto a ser fiscalizado, período e natureza da auditoria (operacional, financeira ou de legalidade, por exemplo). O objeto pode ser uma entidade completa

(instituição pública ou privada), uma parte selecionada ou uma função dessa entidade, e o período a ser fiscalizado pode ser de um mês, um ano ou pode até mesmo corresponder ao período completo da gestão de determinado administrador da instituição. (DIAS, 2000).

O mesmo conceito citado acima se aplica nas próximas sessões que descreve sobre auditoria na tecnologia da informação.

1.3 Auditoria de Tecnologia da Informação e Sistemas

Com a crescente demanda na utilização de tecnologia para armazenamento de informações, contábeis, financeiras e operacionais, torna cada dia mais importante o aprimoramento dos processos das organizações para extrair e analisar os dados envolvidos no negócio. Entretanto, o crescimento das vulnerabilidades dos sistemas de informação geraram o aumento na utilização de técnicas e ferramentas para proteção desses sistemas e também a necessidade da auditoria na tecnologia da informação para avaliar a conformidade dos controles implementados.

Para Imoniana (2008), a auditoria em tecnologia da informação não muda a formação exigida para a profissão de auditor, apenas percebe que as informações até então disponíveis em forma de papel agora são guardadas em forma eletrônica e que o enfoque de auditoria teria que mudar para se assegurar de que essas informações em forma eletrônica sejam confiáveis antes de emitir sua opinião. O autor diz também que a filosofia de auditoria em tecnologia da informação está calçada em confiança e em controles internos. Estes visam confirmar se os controles internos foram implementados e se existem; caso afirmativo, se são efetivos.

Segundo Claudia Dias (2000) Auditoria de Tecnologia da Informação é um tipo de auditoria essencialmente operacional, por meio da qual os auditores analisam os sistemas

de informática, o ambiente computacional, a segurança de informações e o controle interno da entidade fiscalizada, identificando seus pontos fortes e/ou deficiências.

A Auditoria de sistemas é o processo que realiza uma revisão e avaliação dos controles, desenvolvimento de sistemas, procedimentos de T.I, infraestrutura e segurança da informação que envolve o processamento de informações criticas.

Portanto, auditoria de tecnologia da informação deve compreender as entradas, processos, controles, arquivos, segurança e extratores de informações. Para o bom funcionamento dos sistemas de informação, a auditoria é de total importância, para avaliar os controles de segurança e tornar os sistemas mais confiáveis. Além disso, deve avaliar também toda a infraestrutura operacional: Equipamentos, Centro de Processamento de Dados e Software.

1.4 Auditoria de Segurança de Informações e de Redes

Claudia Dias (2000) descreve que auditoria de segurança de informações determina a postura da organização em relação à segurança. Avalia a política de segurança e os controles relacionados com aspectos de segurança institucional mais globais. Na verdade, a auditoria de segurança de informações faz parte da auditoria de tecnologia da informação. A autora também descreve que o escopo da auditoria de segurança envolve:

- Avaliação da politica de segurança.
- Controles de acesso lógico.
- Controles de acesso físico.
- Controles ambientais.
- Plano de contingências e continuidade de serviços.

Imoniana (2008) define este tema como auditoria de redes de computadores. Descrevendo que principal objetivo de auditoria de redes é certificar – se da confiabilidade da rede no tocante à:

- Segurança física: que contemple os equipamentos e os periféricos, arquitetura de rede, sua construção e distribuição;
- Segurança lógica: que contemple as customizações dos recursos de softwares, em geral os rendimentos da rede, seu acompanhamento e avaliação de desempenho operacional;
- Segurança de enlace: que segure as linhas e canais de transmissões entre unidades e localidades remotas obedecendo aos limites estabelecidos;
- Segurança de aplicação: disponibilidade da rede – poder confiar e contar com os recursos da rede quando o usuário mais precisa dela.

A Auditoria de segurança de informação tem por objetivo identificar o status de segurança de uma organização, compreender o ponto que se encontra, e dispor de mecanismos que permitam quantificar a sua segurança. Permitindo localizar uma série de problemas de segurança identificados. Seguidos por recomendações e orientações sobre como sanar as falhar verificadas.

2 AUDITORIA DE SEGURANÇA USANDO TESTE DE INVASÃO

2.1 Auditoria Teste de Invasão

Conhecido mundialmente como *Penetration Testing* (teste de penetração) ou apenas *Pentest*, o teste de invasão é um método que realiza testes, analisa e explora todas as possibilidades de vulnerabilidades em uma rede ou sistemas operacionais. Essa auditoria pode ser executada sobre os ativos de informação do cliente. É um processo que avalia detalhadamente o nível de segurança de um sistema ou rede usando a mesma visão de um invasor (*blackhat*), verifica em tempo real o nível de segurança de determinadas infraestruturas corporativas e as informações nelas contidas.

Tem o objetivo de simular ataques de maneira controlada como se fosse alguém mal intencionado na tentativa de invadir um sistema. Obtendo informações do que poderá acontecer se realmente o ambiente for invadido, é extremamente importante à aplicação destes testes, pois através deles serão criados mecanismos de defesa, garantindo assim a possibilidade de prevenção sobre os riscos e impactos associados à exploração das vulnerabilidades.

Teste de invasão é uma técnica que pode ser útil para maioria das organizações que prezem a segurança. Mais para isso é necessário abordar técnicas avançadas utilizadas por *hackers* e especialistas, para obter acesso a um sistema de forma transparente, minimizando os riscos. Há possibilidade dos sistemas serem danificados com o teste de invasão, por isso devem ser realizados por pessoas experientes e capazes, mesmo assim nunca é 100% seguro que a operação tenha sucesso totalmente. (WACK, 2003).

2.2 Motivação para realizar um Teste de Invasão

O principal motivo para medir quais benefícios uma auditoria teste de invasão trará para a empresa, é comparar o custo de uma auditoria ao prejuízo estimado de um ataque concretizado, incluindo também os prejuízos associados a indisponibilidade dos sistemas comerciais, possibilidade de dados sigilosos serem expostos a terceiros e a perda da credibilidade por parte dos clientes em manter vinculo com a organização.

Além disto, Auditorias de segurança utilizando teste de invasão estão cada vez mais exigidos como requisitos para conformidade com as principais normas nacionais e internacionais.

Como exemplos, listam-se abaixo duas principais normas:

A verificação da conformidade também engloba, por exemplo, testes de invasão e avaliações de vulnerabilidades, que podem ser executados por especialistas independentes, contratados especificamente para este fim. Isto pode ser útil na detecção de vulnerabilidades do sistema e na verificação do quanto os controles são eficientes na prevenção de acessos não autorizados devido a estas vulnerabilidades. (ABNT NBR ISO/IEC 27002:2005)

Segundo exigência número 11.3 do PCI DSS (*Payment Card Industry Data Security Standard*) "As vulnerabilidades são continuamente descobertas por *hackers* e pesquisadores e introduzidas por novos *softwares*. Os sistemas, processos e *softwares* customizados devem ser testados frequentemente para garantir que a segurança está sendo mantida ao longo do tempo e através das mudanças nos *softwares*".

2.3 Características do Teste de Invasão

O *Pentest* caracteriza-se como uma auditoria de segurança, pela qual explora de forma abrangente todos os aspectos que envolvem a segurança de um sistema. Uma sequência de processos é aplicada constituindo varias fases do processo de investigação, ou seja, um

levantamento maciço de informações contribuirá com um resultado positivo em cima do alvo. Considerando que todas as informações adquiridas pelo *pentest* serão aplicadas em benefício do sistema investigado e analisado.

Uma das principais características do Teste de invasão, é que ele seja conduzido com total transparência, todo o escopo da auditoria deverá ser definido previamente com cliente e todas as simulações de ataque apresentadas para aprovação. O processo deverá ser documentado para que o cliente possa de maneira simples identificar quais simulações de ataque são oriundas da auditoria contratada. É possível que o cliente queira limitar o teste temendo algum tipo de impacto ao negócio, da mesma maneira que o auditor deverá ter plena consciência dos possíveis efeitos colaterais em cada ativo a ser explorado.

Outro aspecto que deve ser levado em consideração é a posição do auditor e da sua equipe em relação aos ativos da empresa que serão avaliados. O nível de conhecimento da equipe de auditoria é de extrema importância, pois impacta diretamente na maneira de como será realizado o teste e que modalidade de técnica pode ser utilizada.

Por fim, O nível de conhecimento da equipe técnica que cuida desses ativos, influência na quantidade de informações que será repassada à equipe da auditoria.

A divulgação da auditoria pode ser caracterizada de duas maneiras:

Auditoria anunciada: Evita que sejam realizadas mudanças nos ativos contemplados durante a realização da auditoria, influenciando no resultado de algumas simulações de ataque. Mais por outro lado, pode ser recebida pela equipe técnica responsável pelos ativos como uma maneira de verificação do seu trabalho, efetuando propositalmente modificações que forneçam resultados enganosos para os auditores.

Auditoria não anunciada: Permite ao cliente a avaliação da capacidade de detectar e reagir às simulações de ataque por parte da equipe técnica interna.

2.4 As fases do Teste de Invasão

As fases do Teste de Invasão são uma sequência de processos aplicados pelos investigadores (auditores), um levantamento completo de informações é realizado para contribuir com o resultado positivo da empresa auditada, todas as informações adquiridas serão utilizadas em benefício do sistema analisado.

Para Giavaroto e Santos (2013) os procedimentos realizados em um teste de invasão são os mesmos utilizados pelos *blackhats.* Eles são divididos em cinco fases que formam o processo de ataque descrito abaixo:

2.4.1 Informações do Alvo

É a fase onde são coletadas informações essenciais sobre o alvo, para que seja possível modelar o ataque e verificar se o mesmo pode ser explorado. Todo tipo de informação pode ser coletada para garantir uma maior probabilidade de acesso ao sistema auditado. Essa coleta de informações não há necessidade de nenhum contato com o sistema auditado, pois são informações que estão disponíveis em fontes publicas e servirão para avaliação sobre o alvo no que diz respeito à exposição da informação.

Apenas em poucos minutos pode-se conseguir detalhes importantes para sucesso do teste de invasão. Informações relacionadas ao negócio da empresa como servidores, *firewalls*, roteadores, *e-mails*, telefones, *websites* e *intramail*, muitas vezes estão facilmente disponíveis nas maiores ferramentas de busca: *Google*, *Yahoo* e *Bing*.

A engenharia social também pode ser aplicada em alguns funcionários mal informados, com o intuito de obter informações importantes em apenas uma ligação. Outros costumam publicar em redes sociais como *facebook, instagram, google+*, informações que

comprometem toda estrutura organizacional, sem levar em consideração o sigilo e preservação dos dados da empresa.

Estas situações citadas são cada vez mais exploradas pelos *blackhats*, que geralmente se aproveitam destas evidências. Os auditores devem se comportar com o mesmo pensamento, e utilizar técnicas para prevenir e apresentar soluções que evitarão futuramente intrusões inesperadas. O que diferencia um ataque executado por uma pessoa mal intencionada de uma auditoria teste de invasão é a intenção, o escopo e o espaço de tempo disponível para o mesmo.

2.4.2 Varreduras de sistema

É o processo realizado após o levantamento de informações que utiliza algumas técnicas conhecidas como *scanning* ou *port scan,* que é o mapeamento / rastreamento de portas. São utilizados para verificar quais serviços estão vulneráveis em um sistema operacional. Este processo busca identificar os hosts ativos, os serviços que rodam nos servidores de rede, as portas abertas e também identifica quais sistemas operacionais estão rodando por trás dos serviços mapeados.

O mapeamento de portas é executado em maquinas da rede que usam portas TCP e UDP, consiste no envio de mensagens uma de cada vez para cada uma das portas analisadas, verificando se estão sendo utilizadas ou não. Se estiverem, o auditor pode explorar utilizando ferramentas com o intuito de encontrar diversas falhas de segurança no sistema auditado.

O escaneamento é dividido em três tipos: o *scanning* de portas, de vulnerabilidades e de redes. O *scanner* de portas é a verificação das portas e serviços ativos, no *scanner* de vulnerabilidades são verificadas as fraquezas do sistema e no *scanner* de redes são encontrados os hosts ativos na rede.

2.4.2.1 Tipos de testes para varreduras

De acordo com o manual da metodologia OSSTMM 3 (2010) existem vários tipos de testes, mas não estão limitados a um dos seis tipos mais comuns abaixo descritos:

Blind: Um dos mais utilizados procedimentos de varredura, o auditor não possui nenhuma informação sobre o sistema que irá testar. Portanto, ele deverá descobrir quais meios irão possibilitar o êxito no ataque. Neste processo o sistema que será atacado sabe que irá receber algum tipo de invasão externa e possui conhecimento do teste que será realizado.

Double Blind: O auditor não tem nenhuma informação do sistema que irá atacar, mais nesse processo o sistema não sabe que será atacado e nem quais testes serão realizados.

Gray Box: O auditor possui pouco conhecimento do sistema, nesse caso o sistema sabe que será atacado e quais testes serão executados pelo auditor, com a finalidade de obter informações específicas do sistema auditado.

Double Gray Box: O auditor tem pouco conhecimento sobre o sistema que sabe que será atacado, mais não tem conhecimento de quais tipos de testes serão aplicados.

Tandem: Neste tipo de varredura o auditor tem conhecimento sobre o sistema, que também tem conhecimento que será atacado e quais procedimentos serão executados no teste de invasão.

Reversal: O auditor tem conhecimento sobre o sistema, que não sabe que será atacado e nem quais procedimentos serão utilizados durante o teste.

Para Shakeel e Heriyanto (2011), embora existam diferentes tipos de testes de penetração, os dois mais abordados e amplamente aceitos pela indústria são Black-Box e White-Box.

Black Box: um dos procedimentos mais utilizados, no *black box* o auditor não possui conhecimento prévio do sistema que será testado, simula varreduras em cima de conhecimentos do sistema, facilitando na auditoria mais estruturada do sistema, possibilitando a definição de estratégias para aperfeiçoamento do mesmo.

White Box: O auditor possui conhecimento sobre o sistema, com todo tipo de informação possível disponibilizada: diagramas de rede, IPs de rede e tipos de endereçamento. Tem o objetivo de simular os ataques com o sistema alvo em produção, podendo ter acesso a informações cruciais para a empresa auditada, bem como conhecimento de toda estrutura física, roteadores, endereços, senhas de administradores e usuários do sistema.

2.4.3 Ganho de acesso ao sistema

Esta é a fase em que realmente é feita a invasão do sistema ou o ganho de acesso. Após a realização do reconhecimento e varredura, o auditor já tem informações suficientes para que o alvo seja explorado. De acordo com a definição do *pentest* é que se pode ampliar o ataque direcionado. A experiência do auditor lhe permite diferentes ações a serem executadas, depois que o ambiente for invadido pode se realizar um mapeamento de toda infraestrutura do sistema.

Através das vulnerabilidades mapeadas, o auditor utiliza varias técnicas para verificar e obter o acesso não autorizado. Na exploração do ambiente em cada falha encontrada podem ser aplicados diversos tipos de ataques. Por exemplo:

Captura de tráfego: processo que intercepta e examina informações que trafegam pela rede.

Buffer Overflow: quando um buffer de determinado tamanho recebe mais dados do que pode suportar.

Quebra de senha: processo feito através de força bruta, também conhecida como “ataque dicionário” que busca quebrar senhas que consistem em palavras existentes em um dicionário.

Negação de serviço: ataques que submetem a máquina alvo a uma situação de desempenho extremamente baixo ou indisponibilidade, através do esgotamento dos recursos.

Cross-site Script (XSS): ataques que surgem quando dados passados por clientes são utilizados sem validação para gerar alguma pagina de resultados, ou também quando dados passados pelo cliente serem gravados diretamente no servidor, estando publicamente acessíveis, sem nenhuma validação ou limitação.

Injeção de Código: exploram aplicação que não tratam as entradas de um usuário de forma correta. Possibilitando que o atacante “injete” códigos que serão interpretados pelo servidor que está recebendo. Processo que pode ser feito via formulários, *urls*, *cookies*, parâmetros e etc. O caso mais comum é a injeção de consultas SQL (SQL *injection*) que visa alterar as informações contidas no banco de dados utilizado pela aplicação.

2.4.4 Mantendo o acesso no sistema

Após a intrusão do ambiente, o auditor deverá manter o acesso ao sistema para que possa ser explorado em ocasiões futuras. Podendo também fazer correções de vulnerabilidades garantindo que somente ele fará novas tentativas de invasões, implantando *backdoors* e *rootkits* no alvo.

Com a inserção de estruturas maliciosas, é possível realmente contribuir para um *pentest* real, pois a partir desta situação que se verificará que o sistema de defesa e bloqueios ao sistema foram corretamente implantados. As invasões de sistema nem sempre acarretam

em danos ao sistema operacional e aos arquivos de dados, porque na maioria das invasões, os atacantes estão atrás de informações que contribuam com lucros relacionados a crimes.

Portanto, o invasor sempre deixará uma alternativa de acesso que contribua para um retorno posterior e inesperado visando roubo ou obtenção de informações privilegiadas.

2.4.5 Retirando as evidências

O principal objetivo de teste de invasão também é verificar a eficácia da equipe técnica interna, para isto, nesta fase, após o ambiente ser explorado e suas informações acessadas e modificadas, o invasor deverá apagar seus rastros utilizando técnicas conhecidas como "*housekeeping*", ou seja, limpar a casa para que nenhuma evidência seja encontrada. Caso queira deixar um rastro de que o ambiente foi invadido, isso facilitará uma analise posterior por parte da equipe técnica da empresa contratante.

Algumas informações cruciais para a segurança das redes ficam armazenadas em arquivos conhecidos como logs, que guardam todas as tarefas executadas no sistema operacional.

A exclusão desses arquivos facilita que o invasor não seja descoberto e que nenhum rastro do que foi feito durante o ataque seja encontrado. Existem administradores de redes mais experientes que fazem o redirecionamento de logs para outros servidores, assim, mesmo que o invasor apague os logs da maquina invadida, cópias já estão armazenadas em outro ambiente.

2.5 Relatório do teste de invasão

Segundo Dias (2000), o auditor normalmente apresenta seus achados e conclusões na forma de um relatório escrito, o qual inclui fatos sobre a entidade auditada, comprovações, conclusões e, eventualmente, recomendações e/ou determinações.

Relatório do teste invasão é um documento em que são demonstrados todos os resultados parciais das simulações de ataque aplicadas no sistema alvo (cliente), nele contém todos os passos realizados e tudo que foi obtido para que as possíveis falhas encontradas sejam avaliadas e posteriormente corrigidas caso haja alguma potencial vulnerabilidade no sistema auditado. Esse documento deve manter registro de toda ação executada pelo *pentester* com total transparência, informações como: as ferramentas utilizadas, escopo do ataque realizado, data e horário da realização dos testes e uma lista de todas as vulnerabilidades encontradas e exploradas, bem como as recomendações para melhoria da segurança do ambiente.

O que deve conter no relatório:

- Capa: deve conter o nível de confidencialidade do documento, o nome do contratado e do contratante.
- Índice: deve ser o mais detalhado possível.
- Sumário executivo: deve ser demostrado o teste de invasão, horários de realização dos testes, necessidades da realização dos testes e o retorno do investimento que um *pentest* pode trazer para a empresa auditada.
- Definição do escopo: Descrição do tipo e nível do teste realizado, o que foi testado e até aonde, baseado nas permissões recebidas do contratante.

- Ataques realizados: Varias informações devem conter nessas definições, como ferramentas utilizadas, *exploits* executados, comandos utilizados, resultados recebidos e a classificação das vulnerabilidades e informação do risco.
- Solução proposta: Devem ser informadas as possíveis soluções para as vulnerabilidades encontradas no ambiente auditado.

3 ESTUDO DE CASO

3.1 Descrição do problema

Na cidade de Bragança paulista – SP funciona uma empresa especializada em venda de veículos nacionais, denominada 4RODASNAWEB VEÍCULOS. Grande parte da negociação dos veículos é realizada por meio de serviços disponibilizados em seu website (www.4rodasnaweb.com.br) que está online há pouco mais de dois anos. A empresa vende em média dois veículos por semana com valores que variam de R$ 20.000,00 a R$ 25.000,00. Representada por vinte e seis funcionários alocados nas mais diversas funções, das quais a maioria utiliza computador para execução de suas tarefas, esta organização tem como sua maior aliada a tecnologia, que facilita o bom andamento dos seus negócios.

Considerada uma empresa de pequeno porte, a 4RODASNAWEB possui um modesto parque tecnológico composto por: 24 Desktops, 4 Servidores, 2 Switches de 24 portas e um link de internet dedicado. Os três servidores executam as seguintes funções: Hospedagem do site, serviço de DNS, E-mail e armazenamento de arquivos. Para proteção do ambiente de rede existe um Firewall.

Na manhã do dia 01/02/2014, um cliente interessado na compra de um veículo tentou acessar o site da empresa para verificar o modelo do seu interesse, ao abrir a página ele se deparou com a seguinte tela.

Figura 1 – Pagina Hackeada

Fonte: Elaborada pelo autor.

Imediatamente entrou em contato por telefone com a área comercial para informar o ocorrido. O questionamento foi repassado para a área de tecnologia para verificar o que aconteceu que deixou o site indisponível. A resposta do administrador da rede foi simples e categórica. “Nosso site foi invadido”.

Tendo ciência da gravidade do caso, o gerente da rede verificou imediatamente se o servidor sofreu maiores danos. Após várias horas com o serviço de vendas indisponível, foi realizada uma análise nos arquivos, banco de dados, estrutura do site e logs de acesso, o mesmo constatou que o único dano causado pela invasão foi o chamado *defacement* (conhecido pelo ato de modificar a estrutura da aparência do site), e depois da restauração de um Backup recente, o site voltou ao normal, não havendo perda de dados críticos.

Na manhã do dia seguinte, de posse das informações do fato ocorrido o diretor administrativo solicita ao departamento de T.I uma checagem completa das fragilidades possivelmente existentes na rede da sua empresa. Surge então a necessidade da contratação de

uma empresa terceirizada com especialização em teste de invasão em redes corporativas, para verificar se os controles de segurança aplicados pela equipe interna de T.I fornecem a proteção adequada ao seu ambiente.

Após uma reunião com a diretoria e pesquisa de mercado de uma empresa que atendesse as necessidades da 4RODASNAWEB, chegaram ao acordo da escolha da empresa **SAFER PADLOCK**. Os trabalhos se iniciaram uma semana seguinte á invasão.

3.2 Procedimentos Realizados

Primeiramente a empresa contratada juntamente com a contratante reuniu-se para definir o escopo do trabalho que será realizado, onde determinaram quais equipamentos serão alvos do teste de invasão.

O teste inicia-se com a identificação das informações de rede da organização, o procedimento começou com uma busca na internet dos dados públicos referente à 4RODASNAWEB. De posse dessas informações foram encontrados alguns servidores e respectivos endereços IP dos quais foram alvos das varreduras em busca de portas de serviços abertas. Obtendo conhecimento dos serviços disponíveis, foi possível a realização de ataques bem sucedidos a estes servidores, possibilitando exploração de suas vulnerabilidades que pode ocasionar a obtenção de dados sensíveis da empresa e provável indisponibilidade dos serviços.

Detalhes técnicos de todo procedimento realizado pela consultoria SAFER PADLOCK na infraestrutura de redes de computadores da 4RODASNAWEB resultaram em um relatório de auditoria teste de invasão descrito no Anexo A deste trabalho.

3.3 Resultados alcançados

A empresa tem como principal foco a venda online de veículos, onde a indisponibilidade dos servidores que sustenta os serviços e sistemas pode acarretar em enormes prejuízos financeiros.

Com a contratação da consultoria SAFER PADLOCK a 4RODASNAWEB alcançou seu objetivo no que diz respeito a verificação das fragilidades dos servidores disponíveis para acesso de seus clientes. A Consultoria ajudou a contratante na conscientização da gerência administrativa e também da equipe de tecnologia dos princípios referentes a segurança da informação como aliada de seus negócios, para que as tentativas de ataques oriundas da Internet sejam devidamente bloqueadas e prevenidas com o auxilio de técnicas de proteção aplicadas em todo ambiente computacional.

A execução do teste de invasão em ambiente controlado demonstrou de maneira clara para a contratante a quantidade de ferramentas que podem ser utilizadas por *blackhats* para exploração de vulnerabilidades que não são verificadas pela equipe interna de segurança.

A importância da realização de testes periódicos auxiliam na manutenção da conformidade técnica dos controles de segurança implementados, além de reforçar a ideia de que a contratante sempre deverá estar focada na melhoria dos controles e processos para proteção de seu parque tecnológico.

Portanto, a auditoria teste de invasão se tornou uma aliada da instituição na verificação e correção destes controles, proporcionando aos gestores mais confiança e segurança de que seus sistemas estarão sempre acessíveis, garantindo a disponibilidade da informação que consequentemente acarretará na saúde financeira da contratante.

.

CONCLUSÃO

A segurança da informação possui um papel fundamental para as organizações que usufruem dos benefícios da tecnologia, pois impacta diretamente e indiretamente no negócio, provendo a proteção do ambiente tecnológico minimizando os riscos e impactos. A segurança da informação visa à manutenção dos dados particulares da instituição, de forma integra, provendo a confidencialidade, integridade e disponibilidade, eliminando todo tipo de ameaça a estas informações.

Portanto, realizar a proteção ofensiva na infraestrutura destas redes de computadores corporativas, por meio da auditoria teste de invasão é de extrema importância, pois a realização de testes controlados através de tentativas de ataques reais, como se fosse executado por um *blackhat* oriundo da internet, auxilia na identificação de possíveis fragilidades nos sistemas, como a falta de controle técnico e ausência de conformidade com as normas de segurança nacionais e internacionais, e posteriormente na orientação para correção das vulnerabilidades encontradas.

Este trabalho apresentou conceitos de segurança da informação, auditoria contábil, auditoria de tecnologia da informação e teste de invasão para elucidar e conectar as informações que compõem uma auditoria teste de invasão. Apresentou também de maneira pratica através de um estudo de caso fictício em ambiente corporativo, ferramentas que podem realmente comprometer sistemas que disponibilizam serviços, tanto públicos quanto privados, através da invasão de servidores vulneráveis.

A auditoria teste de invasão é um modo de detecção e correção de falhas e vulnerabilidades no sistema de informação da organização contratante deste serviço.

É de grande valia a manutenção da segurança da instituição, realizando auditorias preventivas para que de maneira alguma o negócio seja afetado por conta da indisponibilidade e do vazamento de dados críticos, causando danos e perdas financeiras ao negócio da empresa.

Por fim, com o conhecimento sobre segurança, auditoria e teste de invasão, o leitor tem a possibilidade de perceber com clareza os processos de uma auditoria de segurança da informação e terá a consciência da importância da execução de testes sobre os controles técnicos implementados, para proteção da informação das instituições. O leitor também pode perceber a finalidade deste trabalho proposto pelo autor na pratica, que foi demonstrar através de um estudo de caso os procedimentos realizados pelo teste de invasão com o objetivo de aumentar preventivamente a segurança da informação identificando e corrigindo possíveis falhas de segurança provendo a proteção do ambiente computacional das empresas.

REFERÊNCIAS

ABNT. NBR ISO/IEC 27002:2005: Tecnologia da informação: Técnicas de segurança: Código de pratica para gestão da segurança da informação. Rio de Janeiro, 2005.

Nakamura, Emilio Tissato. **SEGURANÇA DE REDES EM AMBIENTES COOPERATIVOS**. Berkeley 2003

SÊMOLA, Marcos. **GESTÃO DA SEGURANÇA DA INFORMAÇÃO** – Uma Visão Executiva. Rio de Janeiro: Campus, 2003.

NAKAMURA, Emilio Tissato. GEUS, Paulo Lucio. **SEGURANÇA DE REDES EM AMBIENTES COOPERATIVOS**. São Paulo: Novatec, 2007.

ATTIE, William. **AUDITORIA CONCEITOS E APLICAÇÕES**. 5ª Edição Ano 2010, São Paulo – Editora Atlas S.A.

AZEREDO, Patricia. **AUDITORES DE TI BUSCAM ESPAÇO**. 2006. Disponível em: < https://cheila10.files.wordpress.com/2010/03/auditores-de-ti-buscam-espaco.pdf >. Acesso em: 16 jan. 2015

DIAS, Claudia. **SEGURANÇA E AUDITORIA DA TECNOLOGIA DA INFORMAÇÃO**. Rio de Janeiro: 2000.

IMONIANA, Joshua Onome. **AUDITORIA DE SISTEMAS DE INFORMAÇÃO**. 2. ed. São Paulo: Atlas, 2008.

WACK, John; TRACY, Miles; SOUPPAYA, Murugiah. NIST – SP800-42: **GUIDELINE ON NETWORK SECURITY.WASHINGTON**: Nalt, Inst. Stand. Technol. Espec., 2003

PCISECURITYSTANDARDS.ORG. Payment Card Industry (PCI) Data Security Standard. Requiriments and Security Assessment Procedures Version 2.0, 2010. Disponível em: <http://www.pcisecuritystandards.org/documentes/pci_dss_V2.pdf>. Acesso em: 10 fev.2015.

GIAVAROTO, Sílvio César Roxo; DOS SANTOS, Gerson Raimundo. **BACKTRACK LINUX AUDITORIA E TESTE DE INVASÃO EM REDES DE COMPUTADORES**. Rio de Janeiro: Editora Ciência Moderna Ltda, 2013.

HERZOG, Pete. **ISECOM. OSSTMM 3** – The Open Source Security Testing Methodology Manual. December 14, 2014. Disponivel em: < http://www.delmarlearning.com/companions/content/1435486099/osstmm/osstmm_3.0_lite.pdf >. Acesso em: 11/02/2015.

SHAKEEL, Ali; HERIYANTO Tedi. Backtrack 4: **GARANTINDO SEGURANÇA PELO TESTE DE INVASÃO**. Packt Publishing, 2011.

BOAS PRÁTICAS EM SEGURANÇA DA INFORMAÇÃO / TRIBUNAL DE CONTAS DA UNIÃO. – 4.ed. – Brasília: TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2012. Disponível em: <http://portal2.tcu.gov.br/portal/pls/portal/docs/2511466.PDF>. Acesso em: 12 fev.2015.

ANEXO A

CONFIDENCIAL

TESTE DE INTRUSÃO EXTERNO

Relatório de Atividades, Resultados e Recomendações

Cliente: 4RODASNAWEB VEÍCULOS LTDA

Destinatário: Adalberto José da Silva

Remetente: SAFER PADLOCK CONSULTORIA

Contato: Sidney Oliveira Cirqueira

Data: 10 de Fevereiro de 2014

CONFIDENCIAL

Teste de Intrusão Externo

ÍNDICE

CONFIDENCIAL

Teste de Intrusão Externo

---

1. Estrutura do Documento

Este documento inicia-se com o sumário executivo detalhando à diretoria de forma abrangente o relatório, logo depois o escopo das atividades que serão realizadas neste trabalho de teste de intrusão. Posteriormente, existe a descrição das vulnerabilidades encontradas, bem como níveis de criticidade, impacto e as recomendações necessárias para segurança do ambiente.

1.1 Sumário Executivo

O objetivo do trabalho realizado pela SAFER PADLOCK foi alcançado, com a realização da execução dos testes de invasão demonstrados nesse relatório, na qual a empresa 4RODASNAWEB foi submetida a uma auditoria de segurança no dia 10 de fevereiro de 2014 pelo período de 08:00 às 20:00 horas, momento em que o presente trabalho foi concluído.

Os resultados das análises e testes indicaram fragilidades nos controles de segurança dos servidores que disponibilizam os serviços externos, na presença das irregularidades e falhas apontadas no corpo deste relatório.

Percebemos que, nitidamente não houve nenhum tipo de proteção quanto à execução das atividades executadas pela SAFERPADLOCK, que os ataques direcionados ao escopo definido no neste trabalho não foram bloqueados por nenhum tipo de controle.

Nesse contexto, diante do volume de apontamentos negativos no relatório, entendemos ser de fundamental importância o engajamento da área de tecnologia da informação com atuação no processo de segurança da infraestrutura computacional, para que haja um retorno do

investimento realizado com a contratação da auditoria de segurança para identificação e recomendações de melhoria nos controles de proteção à segurança do ambiente tecnológico da 4RODASNAWEB.

2. Definição do Escopo

Realização de diversos testes conhecidos como *BlackBox*, ou seja, sem conhecimento do ambiente a ser testado, sem fornecimento de credenciais de acesso aos sistemas da 4RODASNAWEB para os testes nas partes internas das aplicações em ambiente de produção.

O serviço de segurança proposto para este processo realizou testes de segurança no escopo abaixo definido pela 4RODASNAWEB.

Lista dos servidores que serão testados:

172.20.0.1 / 24 - Endereço IP onde funciona o Servidor DNS01.

172.20.0.3 / 24 - Endereço IP onde funciona o Servidor WEB responsável pela hospedagem da pagina do site da empresa. URL: www.4rodasnaweb.com.br

CONFIDENCIAL

Teste de Intrusão Externo

---

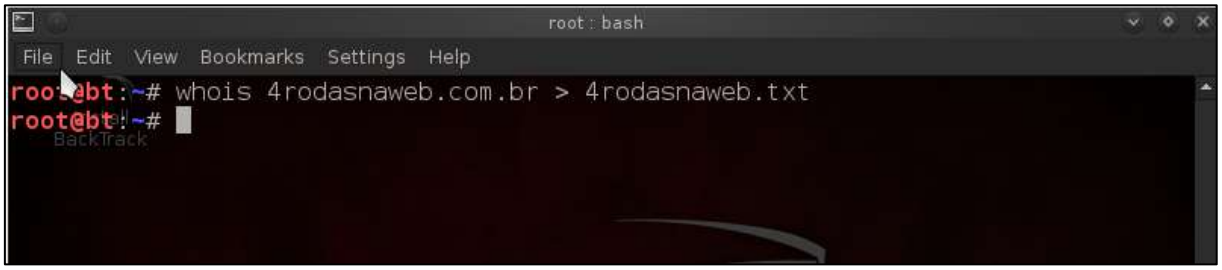
3. Ataques Realizados

3.1. Força Bruta

Um ataque de Força Bruta, ou *Brutal Force*, Consiste em gerar todas as combinações de senha possíveis em sequência para fazer acesso à um sistema. Geralmente são iniciadas com os *logins* padrão, como admin, administrador, root, etc.

Foram realizados tipos de ataques com base nos serviços encontrados em cada endereço IP.

Iniciamos pela realização de um **levantamento de informações** (*footprint*) da empresa alvo. Foi utilizado um comando chamado WHOIS que reúne informações disponíveis na internet sobre determinado domínio.



O resultado obtido no levantamento de informações foi copiado para um documento de texto com todas as informações da 4RODASNAWEB disponíveis na Internet:

CONFIDENCIAL

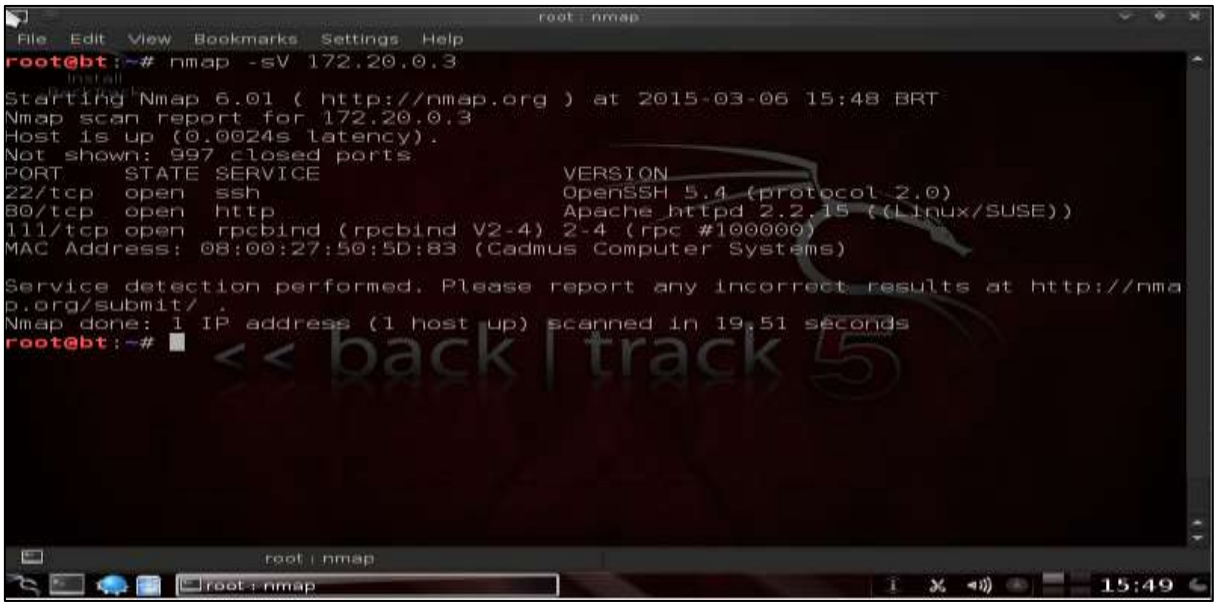
Teste de Intrusão Externo

Com posse das informações importantes e confidenciais, podemos então realizar a **fase de varredura de portas** nos endereços IPs dos servidores encontrados. A primeira varredura foi realizada no servidor que hospeda a pagina web da empresa no endereço IP 172.20.0.3/24.

Utilizamos o comando **nmap –sV 172.20.0.3** com a finalidade de extrair os banners dos serviços que estão rodando no servidor**.**

CONFIDENCIAL

Teste de Intrusão Externo



Após a realização da varredura do servidor, identificamos no sistema operacional OPENSUSE duas portas abertas relacionadas a serviços SSH e HTTP. O próximo passo será a tentativa de ganho de acesso ao sistema / invasão.

Primeiramente realizamos a tentativa de conexão com o serviço SSH.

O SSH é um protocolo de rede desenvolvido para comunicação de dados, *login* remoto por linha de comando e execução remota de comandos de forma criptografada.

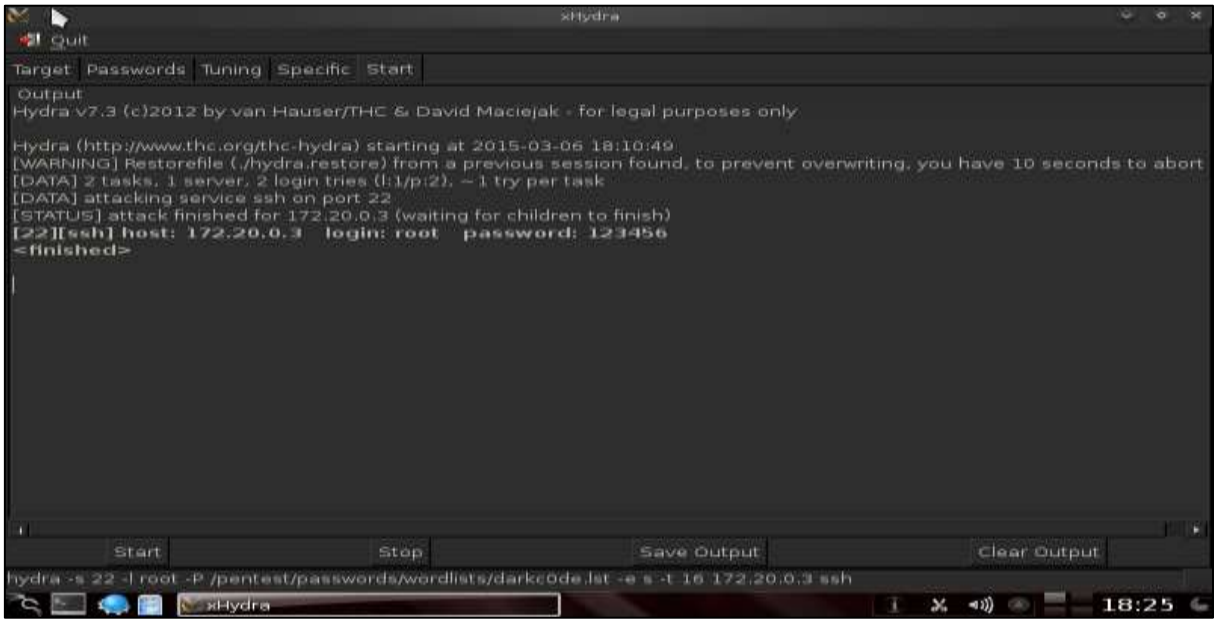
Verificamos então se é possível se conectar ao servidor pela porta do SSH utilizando o comando **ssh 172.20.0.3**.

Perceba que o servidor solicita o *Password* (senha) para conexão.

CONFIDENCIAL

Teste de Intrusão Externo

Por padrão alguns administradores costumam acessar seus servidores como *root*. Então usamos uma ferramenta em interface gráfica chamada xHydra que é muito utilizada para escalação de privilégios através da quebra de senhas para obtermos acesso ao servidor, e depois realizamos a descoberta da senha de *root* utilizando uma *wordlist* (lista de palavras) com senhas mais comuns. Este ataque é conhecido como ataque de dicionário ou força bruta.

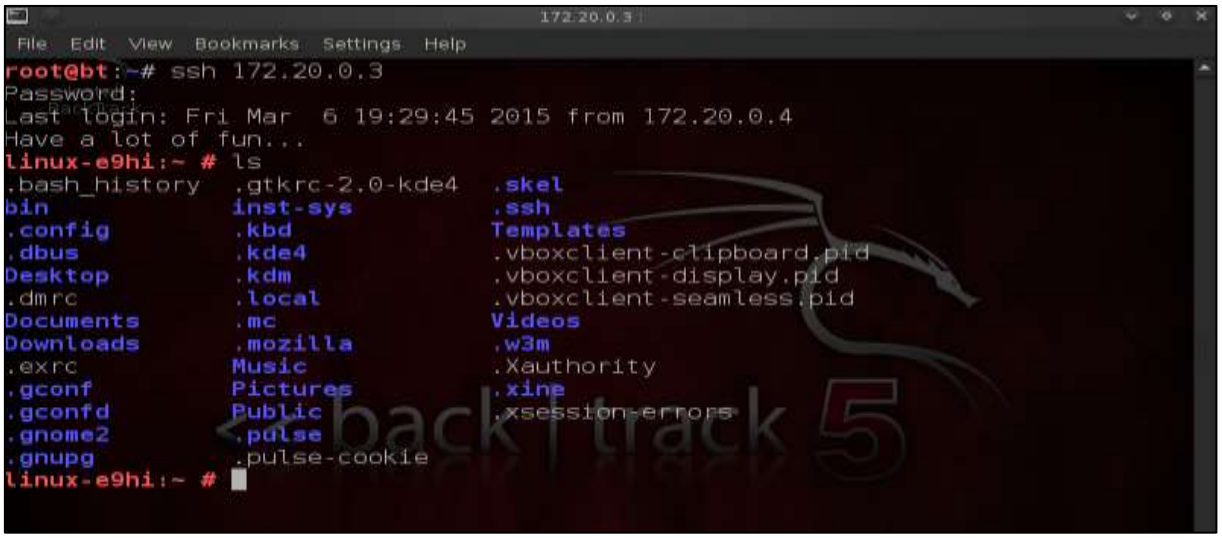


Note que a ferramenta retornou a porta e o serviço atacado, o endereço IP do servidor, o *login* de acesso e a senha do *root*. O próximo passo será a tentativa de invasão com escalação de privilégio.

Novamente utilizamos o comando **ssh 172.20.0.3**, já que o sistema disponibilizava o acesso ao SSH como *root*, foi necessário apenas informar a senha "**123456**" encontrada com a ferramenta xHydra.

CONFIDENCIAL

Teste de Intrusão Externo



Após a inserção da senha, obtemos o ganho de acesso como *root* a todos os principais diretórios do sistema operacional OPENSUSE que hospeda o website da 4RODASNAWEB podendo realizar qualquer tipo de operação com todos os privilégios no sistema auditado.

3.1.1. Impacto

Através da exploração de uma falha humana, deixando um servidor na internet com a porta 22 do serviço de SSH com a configuração de usuário e senha padrão, um atacante tem acesso ao sistema vulnerável, onde pode abusar de credencial administrativa com a qual acessa toda raiz do sistema com o máximo de privilégios, como: Criar contas no sistema, instalar softwares, mudar senhas, realizar downloads e uploads de arquivos, além de extrair e até mesmo excluir dados do servidor.

3.1.2. Criticidade

Alta.

CONFIDENCIAL

Teste de Intrusão Externo

3.1.3. Solução Proposta

Tratar todas as senhas do sistema com configurações de senha forte, que devem ser compostas por letras maiúsculas, símbolos e números, não utilizar palavras contidas em dicionários, não disponibilizar acesso ao SSH diretamente com usuário *root* e alterar a numeração da porta do SSH para outra de preferência do administrador do sistema.

3.2. Negação de Serviço

Um ataque de negação de serviço também é conhecido como **DOS Attack**, consiste na tentativa de tornar os recursos de um sistema indisponível para seus utilizadores. Este tipo de ataque não se trata de uma invasão de sistema, mais sim da sua invalidação por sobrecarga.

Foram realizados tipos de ataques com base nos serviços encontrados no endereço IP do servidor DNS. Novamente realizamos uma varredura com a ferramenta NMAP em cima do endereço IP do servidor DNS, que é responsável pelo sistemas de resolução de nomes da 4RODASNAWEB. O comando utilizado foi **nmap –sV 172.20.0.1**

Perceba que a ferramenta novamente retorna informações importantes a respeito do Servidor que hospeda o serviço de DNS. Varias portas relacionadas a serviços conhecidos encontram – se abertas, a versão do sistema operacional é Windows Server 2003 (sistema que tem o suporte já descontinuado pela microsoft).

Portanto, iremos testar uma vulnerabilidade já conhecida como MS 12-020 em cima do serviço de Desktop remoto conhecido como RDP. O ferramenta **nmap** nomeia este serviço como **ms-wbt-server** porta **3389**.

Utilizamos para realizar o ataque ao servidor DNS uma ferramenta conhecida como metasploit. O metasploit é um framework *open source* que contém programas preparados especificamente para tirarem partido de vulnerabilidades encontradas nos *softwares* e sistemas operativos, permitindo assim a execução de códigos maliciosos e consequentemente a invasão de maquinas.

Com posse do endereço IP do servidor alvo, executamos o metasploit com o comando **msfconsole** para execução dos códigos de ataque ao serviço vulnerável.

O próximo passo foi utilizar um exploit existente no metasploit com os comandos abaixo:

use auxiliary/dos/window/rdp/ms12_020_maxchennelids

set Rhost 172.20.0.1

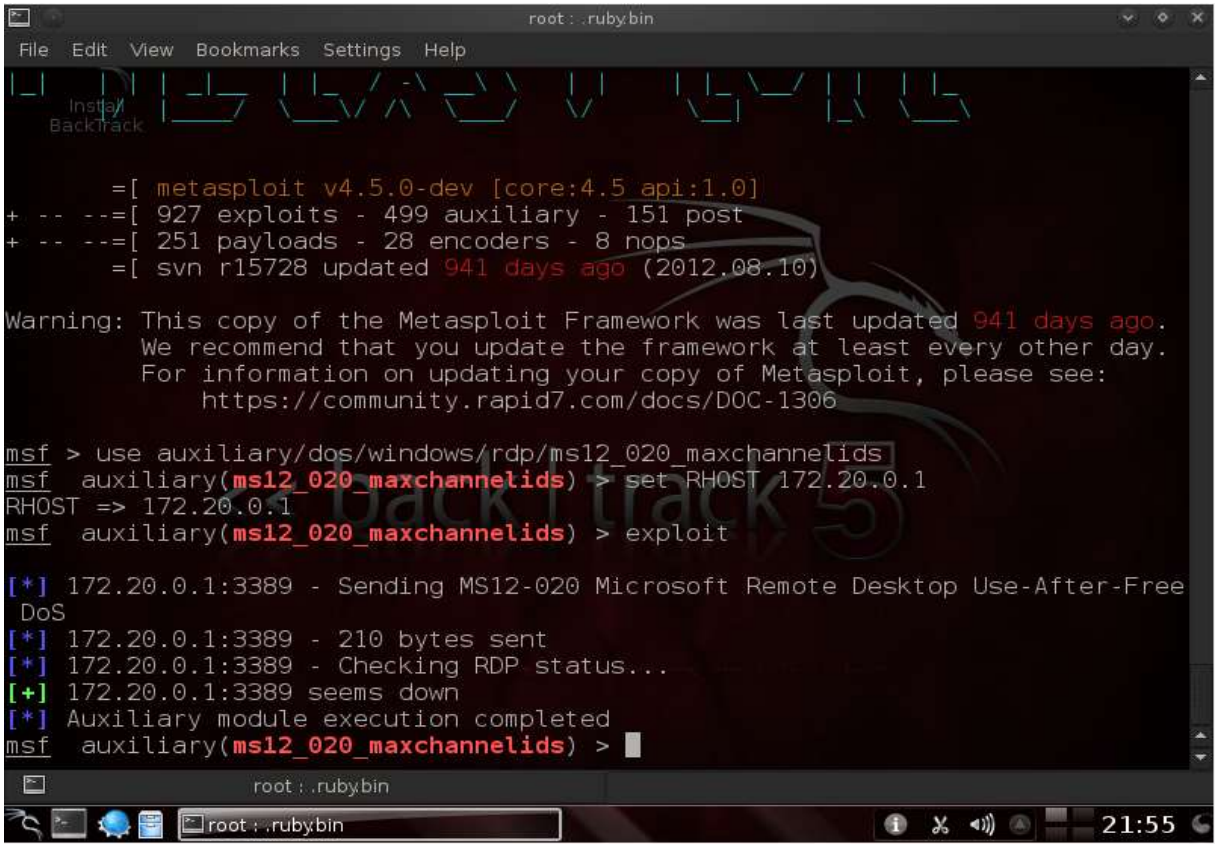
exploit

CONFIDENCIAL

Teste de Intrusão Externo

Servidor abaixo no momento do ataque

Ataque realizado.



Percebam que no momento da execução do comando exploit o servidor atacado fica indisponível imediatamente.

Ataque de negação de serviço realizado com sucesso deixando o sistema de DNS da 4RODASNAWEB indisponível para acesso.

3.2.1. Impacto

Através da exploração de uma falha do protocolo RDP no Windows Server 2003, possibilitando a indisponibilidade do servidor DNS com um ataque de negação de serviço na porta 3389 do serviço RPD, um atacante é capaz de deixar indisponível um serviço de extrema importância para a empresa 4RODASNAWEB, impossibilitando a resolução de nomes internos e externos por parte dos clientes da companhia possibilitando na perda financeira pela falta de acesso dos serviços online.

Teste de Intrusão Externo

3.2.2. Criticidade

Alta.

3.2.3. Solução Proposta

A empresa deve sempre estar alinhada com as principais atualizações de segurança de todos os sistemas operacionais, impedindo que as falhas mais comuns sejam sanadas impossibilitando a exploração das vulnerabilidades pelos *crackers* na Internet. Também é necessário que os sistemas operacionais rodem apenas serviços que estejam ativos no servidor, bloqueando as portas não utilizadas.

4. Conclusão

O teste de intrusão foi bastante elucidativo ao apresentar o nível de exposição a ataques que as aplicações da 4RODASNAWEB estão sujeitas, demonstrando as possibilidades de um ataque.

É importante ressaltar que as tentativas de exploração não foram bloqueadas por algum IPS ou Firewall.

A SAFER PADLOCK CONSULTORIA encontra a disposição para detalhar ainda mais os tipos de ataques realizados e prestar auxilio em definições decorrentes das recomendações de controles que julgamos necessárias descrever neste relatório, incluindo ajuda em definição de escopo e de esforço médio de implantação destes controles de segurança, de acordo com o nosso *expertise* de mercado.