UNIVERSIDADE FEDERAL DO CEARÁ

CAMPUS DE QUIXADÁ

CURSO DE TECNOLOGIA EM REDES DE COMPUTADORES

AVALIAÇÃO PREVENTIVA DE VULNERABILIDADE NOS SISTEMAS COMPUTACIONAIS DA UNIVERSIDADE FEDERAL DO CEARÁ - CAMPUS QUIXADÁ

EVELYNE FERREIRA AVELINO

QUIXADÁ

Fevereiro 2013

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

TECNOLOGIA EM REDES DE COMPUTADORES

AVALIAÇÃO PREVENTIVA DE VULNERABILIDADE NOS SISTEMAS COMPUTACIONAIS DA UNIVERSIDADE FEDERAL DO CEARÁ - CAMPUS QUIXADÁ

Autora

EVELYNE FERREIRA AVELINO

Orientador

DAVID SENA OLIVEIRA

Trabalho de Conclusão de curso submetido à Coordenação do Curso Superior de Tecnologia em Redes de Computadores da Universidade Federal do Ceará como parte dos requisitos obtidos para obtenção do título de Tecnólogo em Redes de Computadores**.**

QUIXADÁ

Fevereiro 2013

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca do Campus de Quixadá

A967a Avelino, Evelyne Ferreira
Avaliação preventiva de vulnerabilidade nos sistemas computacionais da Universidade Federal do Ceará /Evelyne Ferreira Avelino. – 2013.
69 f. : il. color. ; 30 cm.

Monografia (graduação) – Universidade Federal do Ceará, Campus de Quixadá, Curso de Redes de Computadores, Quixadá, 2013.
Orientação: Prof. Dr. David Sena Oliveira
Área de concentração: Computação

1. Sistemas de computação. 2. Segurança de sistemas. 3. Falhas de sistemas de computação I. Título.

CDD 658.4038

SUMÁRIO

INTRODUÇÃO 8
1 Conceitos essenciais sobre Testes de Penetração 10
1.1 Introdução 10
1.2 Segurança da informação 10
1.3 Termos importantes 12
1.3.1 Vulnerabilidade 13
1.3.2 Ameaça 13
1.3.3 Risco 13
1.4 Ataques 14
1.5 Crescimento dos ataques reportados 15
1.5.1 DoS e DDoS 16
1.6 Categorias Hacker 16
1.7 Teste de penetração 18
1.7.1 Etapas de um Teste de Penetração 18
1.7.2 Teste de caixa preta 20
1.7.3 Teste de caixa branca 21
2 PLANO DE TESTES 22
2.1 Introdução 22
2.2 Escopo 22
2.3 Não escopo 22
2.4 Testes a serem Realizados 23
2.5 Ferramentas utilizadas no teste. 23
2.5.1 Backtrack 23
2.5.2 Nmap 6.0 24
2.5.3 T50 24
2.5.4 Metasploit 25
2.5.5 Nikto 25
2.5.6 Nessus 26
2.5.7 Aircrack-ng 26
2.5.8 Reaver 27
2.5.9 Ataque de dicionário 27
3 PESQUISA E INVESTIGAÇÃO, RECONHECIMENTO E EXPLORAÇÃO 28
3.1 Introdução 28
3.2 Pesquisa e Investigação 28
3.2.1 Resultados obtidos na fase de pesquisa e investigação 32
3.3 Reconhecimento 33
3.3.1 Resultados obtidos na fase de reconhecimento 37
3.4 Exploração 38
3.4.1 Resultados obtidos na fase de exploração 39
3.5 Conclusão 45
4 RELATÓRIO TÉCNICO 46
4.1 Introdução 46
4.2 Apache 46
4.3 CVE 47
4.4 Relação das vulnerabilidades reportadas pelo Apache 48
4.5 Vulnerabilidades e Recomendações reportadas pelo Nikto 51

4.6 Vulnerabilidades Identificadas pelo Scanner Nessus. 54
4.7 Recomendações adicionais 55
1. IDS 55
2. Dicas comuns para evitar ataques DoS 55
Conclusão 57
REFERÊNCIAS 58
Apêndice 1 – Termo de Compromisso 59
Apêndice 3 – Resultado detalhado dos escaneamentos 61

ÍNDICE DE FIGURAS

Figura 1.1– Incidentes Reportados ao CERT.br – Janeiro a Março de 2012. 15
Figura 3.1- Descoberta www.quixada.ufc.br 29
Figura 3.2 - Descoberta www.rc.quixada.ufc.br 30
Figura 3.3 - Descobeta - sistemas.quixada.ufc.br 30
Figura 3.4- Descoberta de Hosts ativos 34
Figura 3.5 - Scanner de Sistema operacional com Nmap. 35
Figura 3.6 - Scanner Nmap www.rc.quixada.ufc.br 36
Figura 3.7 - Resultados Scanner Web Nikto 36
Figura 3.8- Mapa da Topologia da Rede descoberta na fase de Scanner 38
Figura 3.9- Framework Metasploit 40
Figura 3.10- Listagem das redes com airodump 41
Figura 3.11- Reaver em busca da vunerabilidade WPS 41
Figura 3.12 - Identificando WPS em rede 42
Figura 3.13 - Usando Ferramenta T50 43
Figura 3.14– Tráfego medido pelo Nagius no switch dos alunos 44

ÍNDICE DE TABELAS

Tabela 1.1- Procedimentos para realização dos testes 21
Tabela 3.1- Resultados obtidos na fase de reconhecimento. 31
Tabela 4.1 – Vulnerabilidade 1 48
Tabela 4.2 – Vulnerabilidade 2 49
Tabela 4.3 – Vulnerabilidade 3 49
Tabela 4.4 – Vulnerabilidade 4 50
Tabela 4.5 – Vulnerabilidade 5 50

INTRODUÇÃO

No Brasil, a redução dos preços dos computadores e a facilidade de conexão à internet tem causado grande aumento na popularidade dos dispositivos computacionais. Atualmente, 43% da população possui acesso à internet no Brasil (NIC.br, 2010).

O aumento da conectividade, ao mesmo tempo em que é positivo pelo avanço tecnológico, faz com que a segurança da informação seja um assunto cada vez mais reincidente no atual cenário computacional. Entre os anos de 2010 e 2012, os aumentos sofridos e reportados por empresas e instituições brasileiras passam de 200% (CERT.br 2012). Essa evolução de ataques virtuais denota a carência por um modelo eficaz de segurança que assegure a integridade dos recursos, tanto em nível de usuários domésticos como organizacionais.

Novas tecnologias são desenvolvidas a cada momento e incorporadas aos sistemas de comunição em um processo contínuo. Da mesma forma, falhas são descobertas, exploradas e corrigidas enquanto estas tecnologias estão em uso. Isso gera um constante conflito entre a geração de novas funcionalidades e a segurança relacionada ao seu uso (NAKAMURA; GEUS, 2007).

A evolução contínua da segurança e de novas tecnologias traduz-se, na prática, em uma impossibilidade de possuir ou desenvolver um sistema 100% seguro. Como alternativa a essa impossibilidade deve-se buscar vulnerabilidades, estudá-las e explorá-las, limitando-as ou corrigindo-as (FARMER; VENEMA, 1993). Avaliações preventivas nos recursos de rede podem revelar falhas potenciais a serem consideradas e corrigidas antes que um usuário mal intencionado possa explorá-las.

A Universidade Federal do Ceará está presente em Quixadá desde 2007, primeiramente com o curso de Sistemas de Informação. Em 2010, foram criados os cursos Redes de Computadores e Engenharia de Software. A instituição possui uma rede de computadores que abriga serviços essenciais aos cursos e é utilizada por professores, servidores e alunos nas atividades letivas. Essa rede, atualmente, não possui profissional alocado exclusivamente para zelar pela segurança dos sistemas ou com formação específica para isso.

O objetivo principal do presente trabalho é identificar e avaliar as potenciais vulnerabilidades dos sistemas computacionais da UFC, Campus Quixadá, por meio de testes

de penetração em redes, bem como propor soluções caso ameaças sejam encontradas.

As principais etapas realizadas para alcançar esse objetivo foram:

- A criação de um plano de testes condizente com as necessidades da instituição;
- A realização de testes de vulnerabilidades na metodologia de Caixa Preta;
- A exploração de vulnerabilidades
- Geração de um relatório técnico com a relação das vulnerabilidades encontradas, avaliação dos riscos, danos envolvidos e alternativas de segurança para correção das vulnerabilidades encontradas.

Este trabalho está organizado como segue:

O Capítulo 1 apresenta conceitos introdutórios sobre Segurança da Informação e Testes de Penetração. O Capítulo 2 aprensenta o Plano de Testes. O Capítulo 3 apresenta a realização dos testes na fases de pesquisa e investigação, reconhecimento e exploração. O Capítulo 4 apresenta o relatório técnico e em seguida o Capítulo de Conclusão. O Apêndice 1 contém o termo de compromisso para realização dos testes, o Apêndice 2 o acordo de confidencialidade e o Apêndice 3 a saída detalhada de alguns escaneamentos da rede.

1 Conceitos essenciais sobre Testes de Penetração

1.1 Introdução

Neste Capítulo são apresentados conceitos essenciais sobre a área de Segurança da Informação que se refere à execução de testes de penetração.

Testes de penetração são métodos de simulação de ataques que buscam encontrar falhas no projeto e implementação da rede dado que a única maneira de mensurar as vulnerabilidades de um sistema é explorá-lo (WHITAKER; NEWMAN, 2005).

Estes conceitos são de fundamental importância para o entendimento do trabalho.

1.2 Segurança da informação

A Segurança de Informática ou Segurança de Computadores está intimamente relacionada com a Segurança da Informação, incluindo não apenas a segurança dos dados/informação, mas também a dos sistemas em si (ISO/IEC 17799:2005).

O conceito de segurança é definido na norma ISO/IEC 17799:2005. Afirmar que algo é seguro implica em garantir sua integridade, confidencialidade e disponibilidade. Segundo Beal (2005), estas garantia podem ser definidos como:

- A **confidencialidade** é a garantia de que apenas os usuários autorizados terão acesso à informação segurada. Essa limitação do acesso é definida pelo proprietário da informação que informa os níveis de acesso relacionados a cada usuário.

- A **integridade** é a garantia da criação legítima e da consistência da informação ao longo do seu ciclo de vida. Isto inclui prevenção contra criação, alteração ou destruição não autorizada de dados e informações. Nesse contexto, a integridade engloba a garantia de autenticação, que visa validar a identidade de cada usuário.

- A **disponibilidade** é a garantia de que a informação esteja sempre disponível para o uso dos usuários legítimos, que foram autorizados pelo proprietário da informação.

A informação é tudo aquilo que permite a aquisição de conhecimento. Segundo o dicionário Houaiss, a **informação** compreende qualquer conteúdo que possa ser armazenado ou transferido de algum modo, servindo a determinado propósito e sendo utilizado pelo ser

humano.

Armazenar informação é uma preocupação do homem desde tempos remotos como pode-se perceber através das pinturas rupestres encontradas em cavernas. A evolução desse processo passa pela criação do alfabeto, pela escrita em pergaminhos ou papiros, pela invenção da imprensa, etc. Tudo isso contribuiu para tornar mais acessível o armazenamento e a distribuição da informação.

A informação armazenada em formato digital é um passo recente na história da humanidade. Esse passo permitiu formas de manipulação e transmissão até então nunca vistas. A informação tornou-se mutável e dinâmica. Ela pode ser lida, modificada e/ou apagada. Com o advento da Internet, seu alcance quebrou as barreiras geográficas permitindo-a chegar a quaisquer povos e culturas.

Gerenciar o acesso e a manipulação da informação digital tornou-se essencial e deu origem ao que chamamos de Segurança da Informação. Nesse contexto, a informação é um ativo essencial para os negócios de uma organização ou de uma pessoa e consequentemente necessita ser adequadamente protegida. Essa proteção é especialmente importante no ambiente de negócios, cada vez mais interconectado. Como um resultado deste incrível aumento da conectividade, a informação está agora exposta a uma grande variedade de ameaças e vulnerabilidades (ABNT, 2005).

Segundo Nakamura e Geus (2007, p. 56) “A defesa é mais complexa do que o ataque”, pois, para o atacante, basta que ele consiga explorar um ponto de falha da organização. Caso uma determinada técnica não funcione, ele pode tentar explorar outras, até que seus objetivos sejam atingidos. Já para as organizações, a defesa é muito mais complexa, pois exige que todos os pontos de ataque sejam defendidos.

A falta de conhecimento sobre as vulnerabilidades do próprio sistema e os mecanismos apropriados de defesa geram várias falácias relacionadas com a problemática da segurança. Algumas falácias são: “tenho um firewall, então meu sistema está seguro” ou “meu sistema é totalmente seguro”. Na verdade, negligenciar um único ponto de defesa faz com que todos os esforços dispensados na segurança dos outros pontos sejam em vão se este ponto vulnerável for descoberto e explorado.

Profissionais mal qualificados tendem a mal dimensionar ou ignorar as reais fragilidades e supervalorizar os dispositivos de segurança implementados. Com isso, a

organização passa a correr riscos ainda maiores, que são o resultado da negligência dos profissionais responsáveis. Isso acontece, comumente, com os *firewalls* ou antivírus, que podem não proteger a organização contra diversos tipos de ataques. (WHITAKER; NEWMAN, 2005)

Novas tecnologias trazem consigo novas vulnerabilidades e é preciso ter em mente que novas vulnerabilidades surgem diariamente. O aumento da conectividade resulta em novas possibilidades de ataques visto que a facilidade de acesso traz como consequência o aumento de novos curiosos.

Entender a natureza dos ataques é fundamental. Muitos ataques são resultado da exploração de vulnerabilidades que podem ser uma falha no projeto ou na implementação de um protocolo, aplicação, serviço, sistema. Erros de configuração e administração de recursos computacionais e falhas humanas também geram brechas de segurança (NAKAMURA; GEUS, 2007).

Em particular, alguns fatores, como a utilização de serviços remotos e as frequentes atualizações de software fazem com que as redes sejam mais vulneráveis ao passo que ferramentas maliciosas estão tornando-se a cada dia, mais simples e mais acessíveis. (WHITAKER; NEWMAN, 2005).

1.3 Termos importantes

Alguns termos que se referem a ataques a sistemas de informação são constantemente mal interpretado ou confundidos. Uma breve lista com o resumo de termos comuns em Segurança da Informação é apresentada abaixo e foi extraída de (RABÊLO, 2013).

- **Ativo:** qualquer bem pertencente à organização que atribua um valor.
- **Problema:** causa desconhecida de algum incidente ou de um conjunto de incidentes.
- **Evento:** informação gerada ou tentativa de algo que não é comum.
- **Consequência:** resultado de um evento.
- **Probabilidade:** possibilidade de algo ocorrer.
- **Ameaça:** perigo em potencial que pode causar dano ao sistema.
- **Risco**: combinação de probabilidade de um evento e sua consequência.
- **Vulnerabilidade:** falha ou fraqueza que podem ser exploradas por ameaças.

- **Incidente**: evento com consequências negativas resultante de um ataque bem-sucedido

Os 3 termos mais importantes nesse trabalho são melhor detalhados nas próximas seções.

1.3.1 Vulnerabilidade

Segundo a norma (ISO/IEC 27000), uma vulnerabilidade é uma falha ou fraqueza de procedimento, design, implementação, ou controles internos de um sistema que possa ser **acidentalmente** ou **propositalmente** exploradas, resultando em uma brecha de segurança ou violação da política de segurança do sistema.

Uma **falha** de configuração ou gestão de uma rede pode permitir um evento que comprometa a segurança. Essas **vulnerabilidades** fazem com que redes sejam suscetíveis à perda de informações e tempo de inatividade. O sistema se torna, neste caso, suscetível a um **ataque**. "Toda rede e sistema tem algum tipo de vulnerabilidade**"(**DEKKER, 1997).

No contexto do presente trabalho, relatar as vulnerabilidades envolve descrever as falhas e os métodos utilizados por atacantes para explorá-las. O termo *avaliação de vulnerabilidade* será utilizado para testar a infraestrutura interna ou externa.

1.3.2 Ameaça

Segundo a norma ISO/IEC 27000 (ISO, 2005), ameaça é a possibilidade de um agente (ou fonte de ameaça) explorar acidentalmente ou propositalmente uma vulnerabilidade específica; Ação ou evento que se caracteriza como potencial violação dos sistemas e possa comprometer a segurança.

1.3.3 Risco

Segundo Beal (2005), os riscos são as possibilidades das ameaças explorarem as vulnerabilidades ocasionando prejuízos e perdas de dados, o que acaba impactando os princípios da segurança da informação: confidencialidade, integridade e disponibilidade.

1.4 Ataques

Um ataque é uma tentativa deliberada, realizada por indivíduo inteligente que tem por objetivo utilizar de técnicas para burlar os mecanismos de segurança e violar a política de segurança de uma instituição. De acordo a legislação brasileira em vigor, a partir de 2012 foi aprovada a Lei 12.737/12, popularmente conhecida como **Lei Carolina Dieckmann,** que afirma que para ser considerado ataque, é necessário o atacante realizar o ataque para instalar vulnerabilidades ou obter vantagem ilícita. A porção de texto da lei que afirma isso pode ser lida na íntegra no seguinte parágrafo.

> "É crime devassar dispositivo informático alheio, conectado ou não a rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo, instalar vulnerabilidades ou obter vantagem ilícita."

Dessa forma, desastres naturais como terremotos ou maremotos não são considerados ataques, mesmo que ocasionem destruição de dados. Também não são considerados ataques outros eventos de falha técnica como HDs que falham, servidores que queimam, etc. Falhas humanas que gerem danos, mas não tenham sido propositais também não são consideradas ataques.

Os ataques se dividem em passivos e ativos. Ataques passivos são aqueles que violam o sigilo sem alterar recursos do sistema. Um exemplo de ataque passivo é a utilização de softwares de captura do tráfego da rede. Estes softwares são conhecidos por *sniffers* e obtém dados sem interferir no funcionamento do sistema. Por sua natureza de não alterar recursos, alguns tipos de ataques são praticamente impossíveis de serem detectados (STALLINGS, 2006). Um ataque passivo pode comprometer a confidencialidade do sistema.

Os ataques ativos possuem a intenção direta ou indireta de alterar recursos do sistema. Um exemplo de ataque ativo é *web defacement*, ou pixação web, no qual páginas web são alteradas por atacantes maliciosos em atos de vandalismo. Este tipo de ataque normalmente provoca mais danos por ser capaz de alterar ou destruir dados. Por interferir no funcionamento do sistema é mais fácil de ser detectado. Os ataques ativos podem afetar a disponibilidade e a integridade do sistema.

O modo como os ataques ocorrem os diferenciam em duas categorias: Um ataque

quando ativo altera recursos do sistema ou afeta a sua operação, já um ataque passivo obtém informações de um sistema sem a intenção de afetar os seus recursos.

1.5 Crescimento dos ataques reportados

O CERT.br (CERT.br, 2012) é o Grupo de Resposta a Incidentes de Segurança para a Internet brasileira. Ele atua como um ponto central para notificações de incidentes de segurança no Brasil. A Figura 1.1 informa as principais categorias de incidentes de segurança reportados no Brasil.

Figura 1.1– Incidentes Reportados ao CERT.br – Janeiro a Março de 2012.
Fonte: CERT.br (2012)

Os ataques apresentados podem ser definidos como (CERT.br, 2012):

- **Dos** (DoS - *Denial of Service*): o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, computador ou rede.
- **Invasão**: um ataque bem sucedido que resulte no acesso não autorizado a um computador ou rede.
- **Web**: um caso particular de ataque visando especificamente o comprometimento de servidores Web ou desfigurações de páginas na Internet.
- **Scan**: notificações de varreduras em redes de computadores com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles.

- **Fraude**: Esta categoria engloba as notificações de tentativas de fraudes, seja no comércio eletrônico ou para enganar o usuário levando-o a fornecer dados sigilosos.
- **Outros**: notificações de incidentes que não se enquadram nas categorias anteriores.

1.5.1 DoS e DDoS

É importante a diferenciação correta entre DoS e DDoS. O DoS, ou ataque de negação de serviços, tem como objetivo impedir o uso de recursos pelos seus usuários legítimos comprometendo a disponibilidade do sistema. Um exemplo seria a execução de um vírus que paralisasse um sistema operacional de um servidor o que acarretaria na indisponibilidade de todos os serviços. Diferente do DDoS (Negação de Serviço Distribuído), o DoS não obrigatoriamente é um ataque de força bruta com o objetivo de conseguir recursos, mas pode ser qualquer ataque que afete a disponibilidade.

O DDoS necessita de uma Rede de Computadores infectados que possam ser possam ser controladas remotamente pelo atacante. Essa rede de computadores zumbis é utilizada para multiplicar o poder do ataque. Estes computadores recebem remotamente uma ordem e trabalham de forma coordenada para sobrecarregar um serviço com objetivo de gerar indisponibilidade

Devido a arquitetura do ataque e de sua força, não existe uma maneira totalmente eficaz de evitar o ataque DDoS. Dado um equipamento conectado há sempre a possibilidade de receber dados em quantidade acima do limite suportado. Se o atacante possuir tempo e recursos disponíveis, o ataque inevitavelmente será bem-sucedido. A única forma utópica de impedir ataques DDoS seria evitar a formação de redes de computadores zumbis, o que é impossível.

Apesar de não haver uma solução definitiva contra ataques de negação de serviço, existem várias maneiras de se minimizar o risco de ser atacado e os danos caso os ataques ocorram. O Capítulo 4, Relatório Técnico apresenta algumas destas soluções.

1.6 Categorias Hacker

Segundo Nakamura e Geus (2007), denominam-se atacantes as pessoas que atacam um sistema computacional, explorando uma vulnerabilidade, podendo ou não obter êxito. Em

(KIMBERLY, 2010), os agentes relacionados com o processo de descoberta e uso das vulnerabilidades são divididos em papeis conforme seus objetivos específicos. De acordo com os chapéus (*hat*)[1], os hackers podem ser divididos em *Black Hat, White Hat* e *Grey Hat*. Optou-se por manter os nomes originais em inglês porque são mais comuns.

Black Hat

Os *Black Hats* são atacantes mal intencionados (*crackers*), que usam suas habilidades para fins ilegais ou maliciosos. Eles invadem ou violam a integridade dos sistemas. Seu objetivo é obter acesso não autorizado para destruir dados vitais. Como consequência, geram problemas de disponibilidade negando acesso aos usuários legítimos do sistema apenas para causar problemas aos seus alvos.

White Hat

Os *White Hats* são *hackers*[2] éticos que usam suas habilidades tendo como finalidade a defesa. Geralmente são profissionais de segurança com conhecimento de técnicas de invasão que utilizam esse conhecimento para localizar as fraquezas e implementar contramedidas. Eles são contratados pelos proprietários dos dados e autorizados a executarem os testes de penetração nas empresas. Possuem a missão de encontrar e corrigir as vulnerabilidades antes que sejam exploradas pelos atacantes maliciosos. Essa autorização prévia é fundamental, pois diferencia os *White Hats* das demais categorias *hacker*.

Grey Hat

Os *Grey Hats* podem trabalhar ofensivamente ou defensivamente, dependendo da situação. Esta escolha é a linha divisória entre *hackers* e *crackers*, podendo os *Grey Hats* apenas estar interessados em ferramentas de invasão e novas tecnologias sem praticar ações maliciosas. Além disso, se autodenominam *hackers* éticos: Eles podem querer destacar os problemas de segurança de um sistema. Com intuito de educar suas "vítimas" a proteger seus sistemas adequadamente.

[1] Os nomes têm origem nos filmes de faroeste americanos, onde era possível identificar pela cor do chapéu o lado pelo qual lutavam os caubóis.

[2] Profissionais especializados na área de segurança de redes.

1.7 Teste de penetração

O termo *hacker* originou-se no Instituto de Massachusetts de Tecnologia (MIT) em 1960, com o Clube de Via Férrea Modelo Tecnológico (TMRC), quando eles quiserem "*hackear*" os circuitos e modificar o desempenho dos seus modelos de trem. Eventualmente, *hackear* veio a significar “ação para propósitos ofensivos”, como por exemplo a invasão de uma rede de computadores. A ação de *hackear* pode ser executada maliciosamente ou defensivamente. (WHITAKER; NEWMAN, 2005)

Um teste de penetração é um método de avaliação da segurança de um sistema de computadores, que simula um ataque de uma fonte de mal-intencionada. Um provador de penetração é um *hacker* ético que é contratado para tentar comprometer a rede de uma companhia na finalidade de avaliar a segurança de dados. Uma equipe de *hackers* éticos trabalhando para violar uma rede é chamada de equipe de tigre (*tiger team*) (PALMER, 2001). Restrições designam o que um o provador de penetração pode e não pode fazer.

Testes de penetração podem ser divididos em relação à forma de teste ou conhecimento prévio do sistema a ser testado. Os mais comuns são o teste de caixa preta e o teste de caixa branca. O teste de caixa preta é mais realista, porém demanda maior esforço do avaliador. O teste de caixa branca é mais rápido e mais preciso, porém menos realista.

1.7.1 Etapas de um Teste de Penetração

Um teste de penetração pode conter diversas etapas. Na literatura (WHITAKER; NEWMAN, 2005), estas etapas são divididas em:

- Assinatura de um termo de compromisso,
- Elaboração de um plano de testes,
- Pesquisa e investigação,
- Reconhecimento da rede,
- Exploração de vulnerabilidades,
- Limpeza de vestígios,

- Elaboração o relatório final.

A assinatura dos **termos de compromisso** engloba documentos de autorização que especificarão quais testes poderão ser realizados no sistema, bem como um acordo de confidencialidade que visa proteger a instituição contra o vazamento de informações não autorizadas. Tais informações podem ser quaisquer dados ou resultados obtidos durante a realização do serviço e são extremamente importantes, pois do contrário, qualquer ação feita na rede pode ser considerada como sendo mal-intencionada.

Para **elaboração do plano de testes** são recomendadas as práticas do *Open Source Security Testing Methodology Manual,* (OSSTMM). Um documento elaborado pelo *Institute for Security and Open Technologies,* (ISECOM). O ISECOM é uma organização de pesquisa de segurança científica, colaborativa, aberta e sem fins lucrativos registrada na Catalunha, Espanha, e em NY, EUA. O OSSTMM apresenta uma metodologia científica para o planejamento e verificação (relatórios) de testes de segurança em ambientes de TI.

O **plano de testes** contém um cronograma a ser seguido, o escopo do teste e detalhes técnicos como: que tipos de testes serão feitos na rede, quais ferramentas serão utilizadas, a forma de uso da engenharia social, etc.

O **reconhecimento da rede** é a fase inicial de coleta de informações **públicas** sobre a rede a ser testada. Ferramentas de busca e engenharia social são utilizadas para estudar o perfil da organização, os serviços que oferecem, os nomes de domínios, os nomes de servidores, as informações do fornecedor de Internet (ISP), endereços IP envolvidos, etc.

A fase de **pesquisa e investigação** caracteriza-se pelo uso de ferramentas de varredura da rede (*scanning*). O objetivo é a descoberta de dados que revelem eventuais vulnerabilidades e informações específicas sobre o sistema. Exemplos de dados que podem ser obtidos através da varredura: as portas abertas, os serviços em execução, a versão, as correções de atualização, os sistemas operacionais, etc. Exemplos de dados relacionados à topologia da rede que podem ser descobertos: protocolos e rotas de roteamento, posicionamento dos servidores, roteadores, pontos de acesso e mecanismos de defesa.

A **exploração de vulnerabilidades** é realizada de acordo com as vulnerabilidades obtidas na fase anterior. Com o objetivo de mensurar o dano gerado por um possível ataque a cada uma dessas vulnerabilidades, estas são exploradas através de ferramentas específicas

(*exploits*). As vulnerabilidades cuja exploração possam causar danos ao ambiente de produção, normalmente, são realizadas em ambiente simulado.

A fase de **limpar vestígios da pesquisa exploratória** é necessária para limpar qualquer alteração que o teste de penetração tenha realizado no sistema. O processo de exploração altera recursos, cria contas de acesso, gera logs e ativa alarmes. O objetivo do testador nessa fase é restaurar o sistema de forma que ele opere em condições normais. Nesta fase são feitas ações como: remover arquivos de log, alarmes de Sistemas de Detecção de Intrusos ou contas de usuário.

Para elaboração de **relatório de avaliação,** recomenda-se seguir o padrão OSSTMM. O **relatório** a ser elaborado deverá apresentar as vulnerabilidades encontradas relacioanando-as com seus respectivos riscos e danos envolvidos. Algumas s**oluções** podem ser propostas como recomendações para remediar as vulnerabilidades

1.7.2 Teste de caixa preta

Este teste envolve a execução de uma avaliação de segurança sem o prévio conhecimento infraestrutura de rede do sistema a ser testado. O teste simula um ataque de um hacker mal-intencionado que não conheça os sistemas da organização. A principal vantagem deste método é que ele simula com fidedignidade como os atacantes oriundos da internet operam e aplicam seus métodos maliciosos para conseguir resultados.

Ao testador pode ser dado um endereço de site da Web ou endereço de IP. Seu objetivo poderia ser invadir o site da Web como se ele fosse um hacker malicioso. (WHITAKER; NEWMAN, 2005).

O teste de caixa preta contempla os seguintes passos: Criação dos Plano Pesquisa e Investigação; Enumeração; Exploração; Limpeza de Vestígios; Elaboração do Relatório Final.

No contexto do presente trabalho os testes serão feitos considerando um aluno que não tem conhecimento da estrutura da rede a ser testada, portanto um teste de caixa preta. O testador realizará todos os passos de descoberta e enumeração.

1.7.3 Teste de caixa branca

Teste de caixa branca é o termo que designa o teste de penetração que envolve a execução de avaliações de segurança tendo previamente o completo conhecimento da infraestrutura de rede a ser testada. Ao testador poderiam ser dados diagramas de rede, lista de sistemas operacionais e aplicações antes da penetração. Seria uma simulação de um fato incomum, de pior caso, onde o atacante teria acesso a todas as informações da rede antes do ataque.

Este teste é muito mais rápido que os outros métodos, pois o hacker ético pode saltar direito para a fase de ataque, contornando todas as fases de reconhecimento, investigação e coleta de informações. Muitas das auditorias de segurança consistem no teste de caixa branca para evitar despesas e tempo adicionais. (KIMBERLY, 2010, WHITAKER; NEWMAN, 2005).

O teste de caixa preta é mais abrangente que o teste de caixa branca, pois possui passos adicionais a serem realizados. Como não faz sentido realizar os dois testes, desde que um contém o outro, o teste de caixa preta foi escolhido como o teste a ser aplicado no presente trabalho. A Tabela 1.1 apresenta a comparação entre as etapas executadas em cada um dos testes.

Tabela 1.1- Procedimentos para realização dos testes

Etapas dos testes de caixa:	**Preta**	**Branca**
Assinatura de um termo de compromisso,	X	X
Elaboração de um plano de testes,	X	
Reconhecimento da rede,	X	
Pesquisa e investigação,	X	
Exploração de vulnerabilidades,	X	X
Limpeza de vestígios,	X	X
Elaboração do relatório final.	X	X

2 PLANO DE TESTES

2.1 Introdução

Neste Capítulo é apresentado o plano de testes utilizado na avaliação da segurança da UFC-Quixadá. Nele são definidos fatores essenciais ao teste de penetração, tais como o escopo do trabalho, os tipos de testes a serem realizados e as ferramentas utilizadas.

2.2 Escopo

O escopo escolhido para Avaliação de vulnerabilidades compreende:

- Avaliação da rede wireless;
- Avaliação dos serviços;
- Avaliação dos servidores.

2.3 Não escopo

Engenharia social é termo utilizado para descrever um método de ataque, onde alguém faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações.

Não fazem parte do escopo:

- Uso de engenharia social para obter informações ou privilégios;
- Análise das barreiras físicas de acesso aos recursos, tais como, portas, chaves, localização física dos servidores e dispositivos como switch e Access Points, facilidade de acesso físico à sala da Telemática[3].

[3] Na sala da Telemática estão os servidores do Campus, o firewall e os switchs que interligam toda a rede do Campus.

2.4 Testes a serem Realizados

Como dito anteriormente será utilizada a metodologia de teste de caixa preta, a seguir são descritos os tipos de testes realizados em cada uma das etapas do teste de caixa preta.

Na fase de pesquisa e investigação optou-se por se utilizar apenas mecanismos de busca.

A fase de reconhecimento será feita por meio de *scanners* de vulnerabilidades. O objetivo é identificar portas abertas em servidores, serviços, sistemas operacionais, versões, rotas de endereços IP, servidores DNS, topologia da rede, etc.

A fase de exploração será feita por meio de *exploits*[4] específicos para vulnerabilidades encontradas. O teste da rede Wireless será feito por meio de ataques de dicionário e tentativa de descoberta de PIN[5] através da vulnerabilidade de WPS[6]. Na seção 2.5 é apresentada uma descrição de cada uma das ferramentas usadas na avaliação.

2.5 Ferramentas utilizadas no teste.

2.5.1 Backtrack

O Backtrack é um sistema open source baseado em Linux, desenvolvido para auditoria de segurança da informação. Consiste em uma longa lista de mais de 300 ferramentas de segurança prontas para uso, entre os quais numerosos scanners de vulnerabilidades, *exploits*, *sniffers*, ferramentas de análise forense e ferramentas para auditoria wireless.

[4] Um *exploit* é um código específico escrito para explorar uma determinada vulnerabilidade.
[5] O PIN de um roteador que possua segurança WPS. É uma senha de acesso que se descoberta, permite ao atacante desvendar senhas WPA/WPA2 de acesso à rede.
[6] O WPS (Wi-Fi Protected Setup) é um padrão de computação que tinha como objetivo permitir fácil criação de uma rede doméstica sem fio segura.

As diversas ferramentas são estruturadas de acordo com o fluxo de trabalho dos profissionais de segurança. Novas tecnologias e técnicas de teste são incluídas ao Backtrack constantemente para mantê-lo atualizado.

2.5.2 Nmap 6.0

Nmap ("Network Mapper") é uma ferramenta livre e de código aberto para a descoberta de rede e auditoria de segurança. O programa Nmap envia pacotes IP aos hosts e através de requisições e respostas específicas é capaz de determinar: quais hosts estão disponíveis na rede; quais serviços, nomes de aplicações e versões estão sendo executados; quais os sistemas operacionais e versões; que tipo de filtros de pacotes e *firewalls* estão em uso; e várias outras características da rede. Ele foi projetado para escanear rapidamente grandes redes, mas funciona bem contra hosts individuais.

O Nmap, em geral, opera nas camadas de rede e transporte. Em alguns casos também é capaz de manipular dados da camada de enlace, como por exemplo, endereços MAC e requisições ARP. Também é capaz de interpretar dados da camada de aplicação para inferir informações como versões de serviços e sistemas operacionais. Neste trabalho o Nmap foi usado na fase de reconhecimento.

2.5.3 T50

O T50 é um *packet injection* (injeção de pacote). É uma ferramenta livre, criada pelo brasileiro Nelson Brito, capaz de fazer ataques DoS e DDoS usando o conceito de *stress testing*.[7]

Este software pode enviar um numero elevado de pacotes de requisições de forma que o alvo não consiga atender a todas as requisições ou as atenda consumindo recursos como memória e CPU, causando indisponibilidade.

Segundo o site corujadeti.com o T50 é capaz de emitir as seguintes requisições.

[7] Tipo de teste de confiabilidade destinado a avaliar como o sistema responde em condições anormais. O stress no sistema pode abranger cargas de trabalho extremas, memória insuficiente, hardware e serviços indisponíveis ou recursos compartilhados limitados.

- Mais de 1.000.000 (1 milhão) de pacotes por segundo de SYN Flood (+50% do uplink da rede) em uma rede 1000BASE-T (Gigabit Ethernet).
- Mais de 120.000 pacotes por segundo de SYN Flood (+60% do uplink da rede) em uma rede 100BASE-TX (Fast Ethernet).

O T50 ainda pode enviar requisições de pacotes utilizando protocolos ICMP, IGMP, TCP e UDP sequencialmente com diferença de microsegundos. A ferramenta foi utilizada na fase de exploração.

2.5.4 Metasploit

Metasploit é um "*framework*" *open source*, que permite a verificação e auditoria explorando falhas de segurança em softwares. Seu conjunto de ferramentas é atualizado diariamente para incluir recentes falhas de segurança que são identificadas por profissionais do ramo.

Conforme o site metasploit.com, a ferramenta é líder em testes de penetração, e que, além disso, fornece informações sobre vulnerabilidade de segurança em várias plataformas, sistemas operacionais, servidores e assim contribuir para que os desenvolvedores escrevam seus códigos com mais segurança. O Metasploit foi utilizado na fase de exploração.

2.5.5 Nikto

Nikto é um *scanner* de vulnerabilidades para servidores web, de código aberto e estruturado com *plugins* que estendem seus recursos. O Nikto realiza mais de 2000 diferentes solicitações HTTP GET para o servidor web a ser escaneado e através das respostas a estas solicitações ele é capaz de descobrir sobre

1. Configurações incorretas,
2. Arquivos padrão e scripts,
3. Arquivos inseguros e scripts,
4. Software desatualizado,

5. Determinar a versão apache.

O problema no uso do Nikto é que as solicitações criam um grande número de abertura de conexões em servidores web que ficam gravadas em arquivos de log. Esse comportamento é facilmente percebido como sendo de uma ataque disparando alarmes na rede atacada. Tanto sistemas de detecção de intrusão baseada em rede(NIDS) como o baseado em baseado em host (HIDS) devem detectar uma varredura do Nikto. O Nikto foi utilizado na fase de reconhecimento.

2.5.6 Nessus

Nessus é uma ferramenta de auditoria e segurança, para a verificação de falhas e vulnerabilidades. Ele realiza um escaneamento das portas do computador alvo. Esse escaneamento é realizando executando scripts que são específicos para cada porta de destino e abrem conexões com objetivo de descobrir vulnerabilidades. Os scripts são escritos em NASL (Nessus Attack Scripting Language).

O Nessus é capaz de trabalhar em conjunto como o nmap. É possível atualizá-lo a adicionar novas funcionalidade através da atualização ou instalação de *plugins*. No trabalho será utilizada a versão gratuita do Nessus. A ferramenta foi utilizada na fase de reconhecimento.

2.5.7 Aircrack-ng

Aircrack-ng é um conjunto de ferramentas de auditoria para redes sem fio. Consiste em um detector, um *sniffer* , um *cracker*[8]de senhas e uma ferramenta de análise para redes 802.11. Ele funciona com qualquer placa de rede que suporte operar em modo promíscuo[9]. O software foi utilizado na fase de exploração.

[8] O termo cracker aqui refere-se a um software que objetiva descobrir ou "quebrar" uma senha.
[9] Em modo promíscuo a placa recebe todos os pacotes que trafegam na rede e não apenas os endereçados a ela.

2.5.8 Reaver

Reaver é uma ferramenta para exploração de vulnerabilidades WPS em redes sem fio com criptografia WPA/WPA2. Ele foi publicado pela Tactical Network Solutions, possuindo versão open-source gratuita e também uma versão paga com mais funcionalidades.

O WPS é uma método de autenticação que oferece uma forma simples de configuração para redes Wireless. O roteador inclui um PIN de 8 dígitos, geralmente informado em uma etiqueta na parte inferior do dispositivo. Este número é utilizado para criar uma conexão com outros clientes apenas informando o número PIN.

Além do PIN, outros dispositivos exigem que um botão de conexão deva ser pressionado para autorizar a criação da conexão. O WPS foi concebido como um padrão de segurança a ser utilizado em redes domésticas. O WPS utiliza como principal restrição para autenticação o acesso físico ao dispositivo, desde que é possível obter o PIN e acessar o botão de configuração apenas tendo acesso direto ao dispositivo.

Entretanto, mesmo com tamanha facilidade de configuração, foi descoberta uma falha grave no protocolo WPS. Essa falha permite descobrir o PIN de qualquer roteador que venha habilitado com WPS em apenas poucas horas utilizando um ataque específico de força bruta, tornando equipamentos com WPS extremamente inseguros. O software foi utilizado na fase de exploração.

2.5.9 Ataque de dicionário

Um **ataque de dicionário** é um método de descobrimento de senhas que testa palavras de uma base de dados como possíveis senhas do sistema. Muitos usuários utilizam como senha uma palavra do seu idioma ou de seu cotidiano.

Ataques de dicionário são improváveis de sucesso em sistemas que utilizam **senhas fortes**. Uma senha forte possui letras maiúsculas e minúsculas misturadas com números (alfanumérico) e quaisquer outros símbolos. No entanto, para a maioria dos usuários, lembrar de senhas complexas é difícil.

Existem variantes do ataque de dicionário que verificam também algumas substituições típicas (algumas letras com números, a troca de duas letras, abreviaturas) e diferentes combinações de letras maiúsculas e minúsculas. O ataque de dicionário foi aplicado na rede wireless para testar vulnerabilidades de senhas na fase de exploração.

3 PESQUISA E INVESTIGAÇÃO, RECONHECIMENTO E EXPLORAÇÃO

3.1 Introdução

Neste Capítulo é apresentada a metodologia da avaliação de vulnerabilidades e os resultados obtidos em cada um das fases. As fases descritas são: Pesquisa e Investigação, Reconhecimento e Exploração. Os testes foram executados entre Novembro e Dezembro de 2012 e podem não condizer com a atual situação da rede. Este capítulo apresentará algumas imagens correspondentes as saídas dos programas em execução. O objetivo é apenas exemplificar e apresentar as ferramentas. Como a lista de dados obtidos é muito extensa, optou-se por descrever apenas os resultados mais relevantes com o objetivo de preservar a clareza do texto e facilitar a leitura.

3.2 Pesquisa e Investigação

Esta fase é essencial para modelar os ataques e determinar quais seriam os ataques com maior probabilidade de sucesso. O primeiro passo é coletar informações de fontes públicas sobre a rede a ser testada. A coleta é passiva, não exigindo nenhum contato com o sistema. E geralmente, serve como uma avaliação sobre o alvo no quesito exposição de informações.

O objetivo da fase de pesquisa é encontrar

- Informações **públicas** sobre a rede a ser testada.
- Informações sobre serviços que oferecem.
- Nomes de domínios.
- Nomes de servidores.

- Informações do fornecedor de Internet (ISP).
- Endereços IP envolvidos.

A fase de pesquisa e investigação foi feita sem se utilizar de ferramentas de hacking[10]. Através do mecanismo de busca do Google chegou-se ao site http://www.whoishostingthis.com/. Este site retorna para qualquer domínio buscado os seguintes dados: informações sobre o ISP[11], servidor DNS[12] e IP.

A Tabela 3.1 apresenta um resumo dos resultados obtidos por todas as buscas relacionadas aos domínios dos serviços oferecidos pela UFC-Quixadá.

A busca sobre o domínio www.quixada.ufc.br, que é o site oficial da Instituição, retornou o seguinte resultado:

Figura 3.1- Descoberta www.quixada.ufc.br

A busca pelo site do curso de redes www.rc.quixada.ufc.br, é apresentada Figura 3.2.

[10] Ferramentas hackers.
[11] ISP – Provedor que fornece conectividade de Internet a um cliente
[12] DNS – Servidor de nomes que realiza a tradução do nome do site para o endereço IP.

Figura 3.2 - Descoberta www.rc.quixada.ufc.br

A UFC – Quixadá utiliza diversos sistemas de gestão acadêmica de autoria própria ou instalados nos servidores do Campus. Os mais importantes são:

- SIPPA – Controle de Presenças, Planos de Aula.
- SAVI – Sistema de Avaliação Institucional.
- Moodle – Sistema para ativadades de ensino a distância.

A busca pelos endereços dos sistemas internos resultou nos seguintes resultados.

Figura 3.3 - Descobeta - sistemas.quixada.ufc.br

O Registro Br também foi utilizado como mecanismo de busca. Foram obtidos resultados parecidos com os recolhidos de whoishostingthis. A busca pelo site principal retornou:

```
https://registro.br/cgi-bin/whois/#lresp

www.quixada.ufc.br

domínio:       ufc.br
entidade:      UNIVERSIDADE FEDERAL DO CEARA
documento:     007.272.636/0001-31
responsável:   Ladislav Trupl
país:          BR
ID entidade:   LATRU
ID admin:      LATRU
ID técnico:    LATRU
ID cobrança:   FAG
servidor DNS:  taiba.ufc.br 200.19.190.1
status DNS:    18/12/2012 AA
último AA:     18/12/2012
servidor DNS:  cici.npd.ufc.br 200.17.41.36
status DNS:    18/12/2012 AA
último AA:     18/12/2012
servidor DNS:  jeri0.ufc.br 200.19.190.6
status DNS:    18/12/2012 AA
último AA:     18/12/2012
criado:        antes de 01/01/1995
alterado:      25/03/2011
status:        publicado
```

A Tabela 3.1 faz uma síntese da fase de investigação mostrando os resultados obtidos.

Tabela 3.1- Resultados obtidos na fase de reconhecimento.

Domínio	IP	ISP	DNS
www.quixada.ufc.br			taiba.ufc.br cici.npd.ufc.br
www.rc.quixada.ufc.br	201.20.65.197	Baydnet	abilhao.quixada.ufc.br
sistemas.quixada.ufc.br	201.20.65.202	Baydnet	maracana.quixada.ufc.br

3.2.1 Resultados obtidos na fase de pesquisa e investigação

1) O domínio www.quixada.ufc.br não retornou endereço IP ou provedor ISP. Isto significa que existe um mecanismo de segurança que impede a divulgação de informações que comprometam a confidencialidade e facilitem ataques. Provavelmente este domínio deve ser gerenciado pelo STI em Fortaleza, já que o servidor de DNS responsável pelo domínio responde em cici.npd.ufc.br. Assim, conclui-se que o site está hospedado fora dos servidores existentes no campus de Quixadá e ficará fora do escopo de testes.

2) Os sites dos curso de Sistemas de Informação e Engenharia de Software também retornaram o mesmo resultado que o site www.quixada.ufc.br. Conclui-se que ambos estão hospedados também nos servidores do STI.

3) O site do curso de Redes de Computadores aponta para máquina 201.20.65.197 e possui como DNS a máquina abilhao.quixada.ufc.br. Conclui-se, pelo próprio nome da máquina, que esta se localiza no Campus Quixadá. Um posterior escaneamento na rede interna do Campus revelará a existência da máquina abilhão e sua localização dentro da rede interna.

4) O site sistemas.quixada.ufc.br, bem como todos os sites relacionados aos serviços, tais quais:

   a. moodle.quixada.ufc.br,

   b. sistemas.quixada.ufc.br/apps/sippa/,

   c. sistemas.quixada.ufc.br/apps/savi/,

   retornam para o mesmo IP 201.20.65.202. Conclui-se que todos devem estar hospedados no mesmo servidor do Campus. O DNS aponta para a máquina maracana e um escaneamento posterior revelou a localização da máquina dentro da rede interna.

3.3 Reconhecimento

Refere-se à fase antes do ataque em que o atacante varre a rede com informações específicas obtidas durante a fase de reconhecimento. A busca pode ser vista como uma consequência lógica do reconhecimento feito na fase anterior. Atacantes costumam usar ferramentas automatizadas, como os motores de busca para localizar sub-redes, sistemas de equipamentos e tentar descobrir vulnerabilidades.

Qualquer invasor pode obter informações sobre vulnerabilidades ou posicionamento de máquinas e firewalls usando ferramentas simples como o comando traceroute ou nmap.

Objetivos da fase de Reconhecimento.

- Obter hosts ativos.
- Executar uma varredura de portas para detectar portas abertas e os serviços que fornecem.
- Identificar rotas.
- Identificar servidor DNS.
- Mapear a topologia da rede.
- Obter as versões de sistema operacionais existentes em servidores.

Os resultados da fase de Reconhecimento podem ser encontrados na seção 3.3.1. A saída completa dos escaneamentos dos servidores pode ser encontrada no Apêndice 3.

O primeiro passo de uma auditoria de segurança ou projeto de mapeamento de rede é reduzir uma grande faixa de endereços IP a uma lista de endereços de interesse. Este interesse pode variar dependendo do propósito da varredura. Em uma auditoria teste de invasão caixa preta, que corresponde ao caso escolhido neste trabalho, o auditor se interessa por qualquer host que esteja ativo na rede. O zenmap é uma interface gráfica para o nmap e possui a vantagem de separar as informações obtidas pelos escaneamentos em abas, salva resultados e permite comparações de resultados. Foi utilizado para se descobrir hosts ativos dentro da rede e retornou resultado da Figura 3.4.

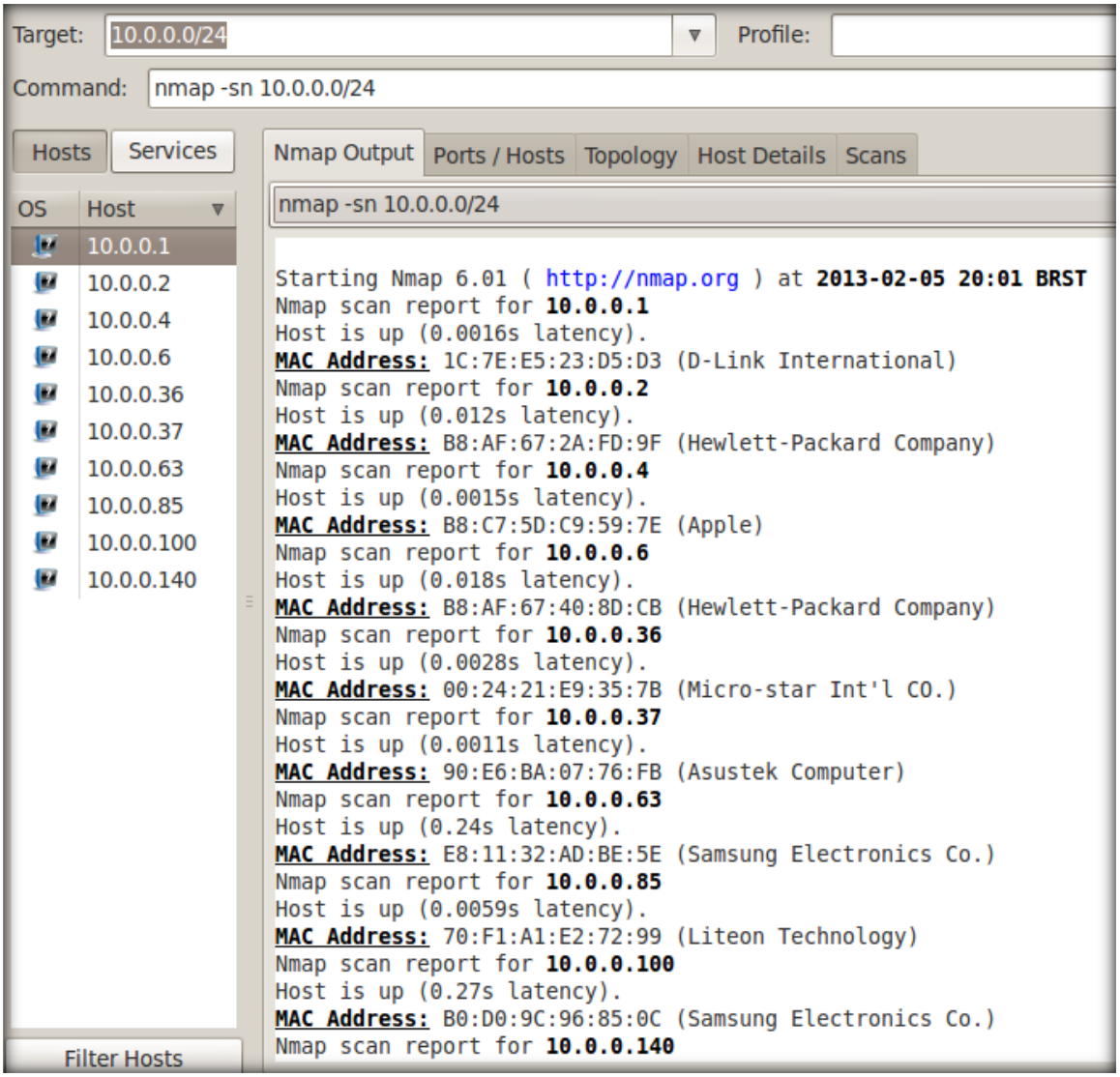

Figura 3.4- Descoberta de Hosts ativos

As vulnerabilidades divulgadas em sites de segurança estão relacionadas a versões específicas de software. Faz-se necessário obter uma leitura mais específica sobre um serviço descoberto, do que somente a porta em que este está sendo executado. Um serviço pode ser executado em qualquer porta. Sendo assim, o nmap fornece uma opção para aferir o serviço e a versão do software provendo este serviço através da opção “sV”. O software tenta, então, através do envio de pacotes construídos com este propósito, descobrir qual serviço está sendo provido de fato e sua versão aproximada.

Assim como servidores possuem serviços que podem ser explorados, falhas em sistemas operacionais também devem ser verificadas. Um ponto essencial no teste é detectar

qual sistema é executado pelos alvos na rede, sua versão e atualizações de segurança. O nmap fornece uma opção para aferir o sistema operacional e sua versão aproximada através da opção “O”.

O nmap foi executado contra os hosts abilhao e maracana para descobrir o sistema operacional, os serviços e portas. A Figura 3.5 exemplifica a saída do zenmap mostrando o resultado do escaneamento do domínio sistemas.quixada.ufc.br na aba que apresenta as descobertas referentes ao sistema operacional.

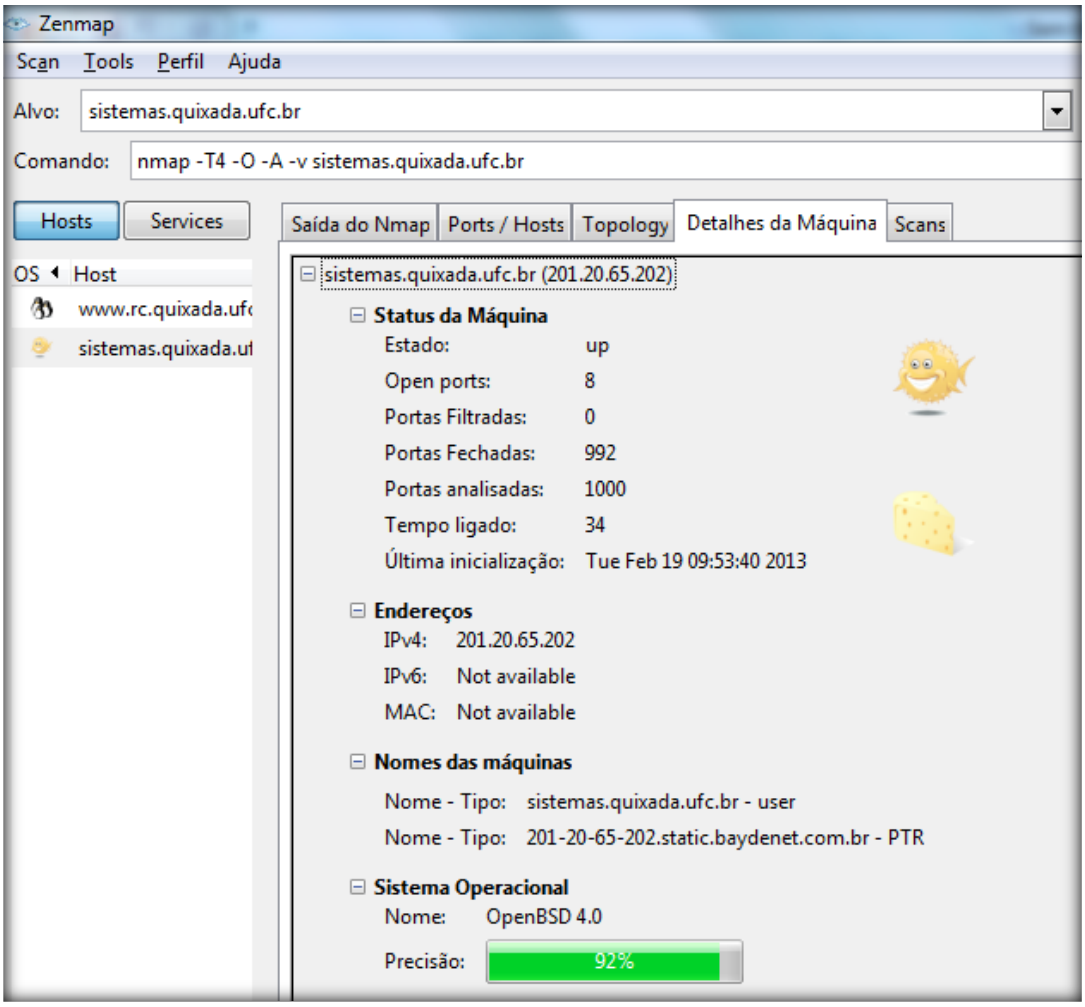

Figura 3.5 - Scanner de Sistema operacional com Nmap.

A Figura 3.6 exemplica a saída do zenmap na aba relacionada a serviços ativos, versões e portas abertas para o escaneamento da máquina abilhao.

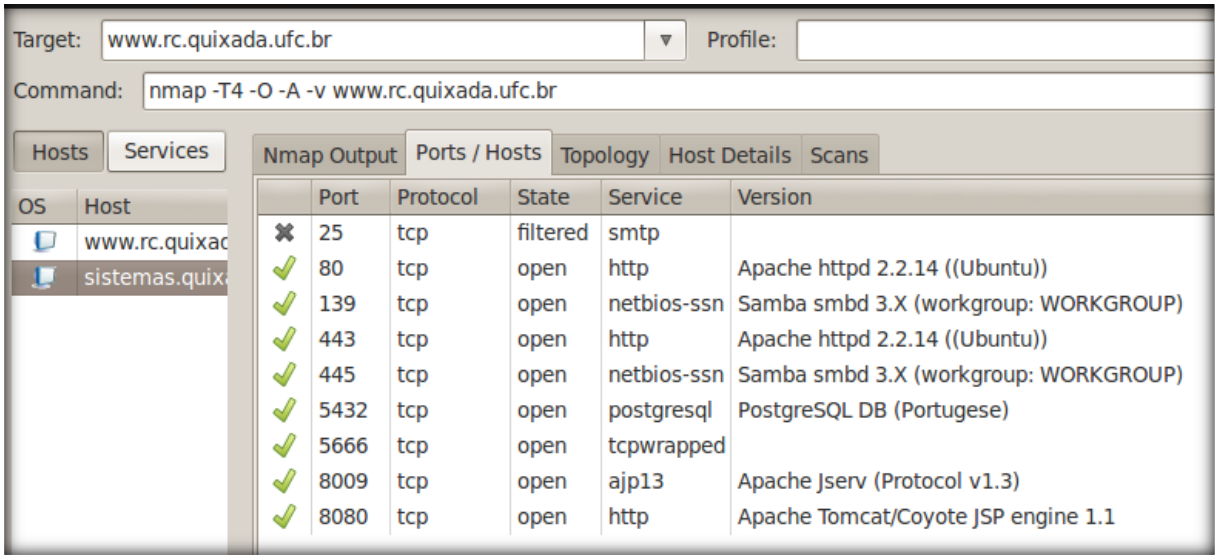

Figura 3.6 - Scanner Nmap www.rc.quixada.ufc.br

Nos dois domínios investigados foi detectada a presença de serviços web, para tanto foi usado Scanner de vulnerabilidades Nikto a fim de se descobrir vulnerabilidades resultantes de falhas de configuração, serviço desatualizado etc. A imagem Figura 3.7 exemplifica a saída do Nikto.

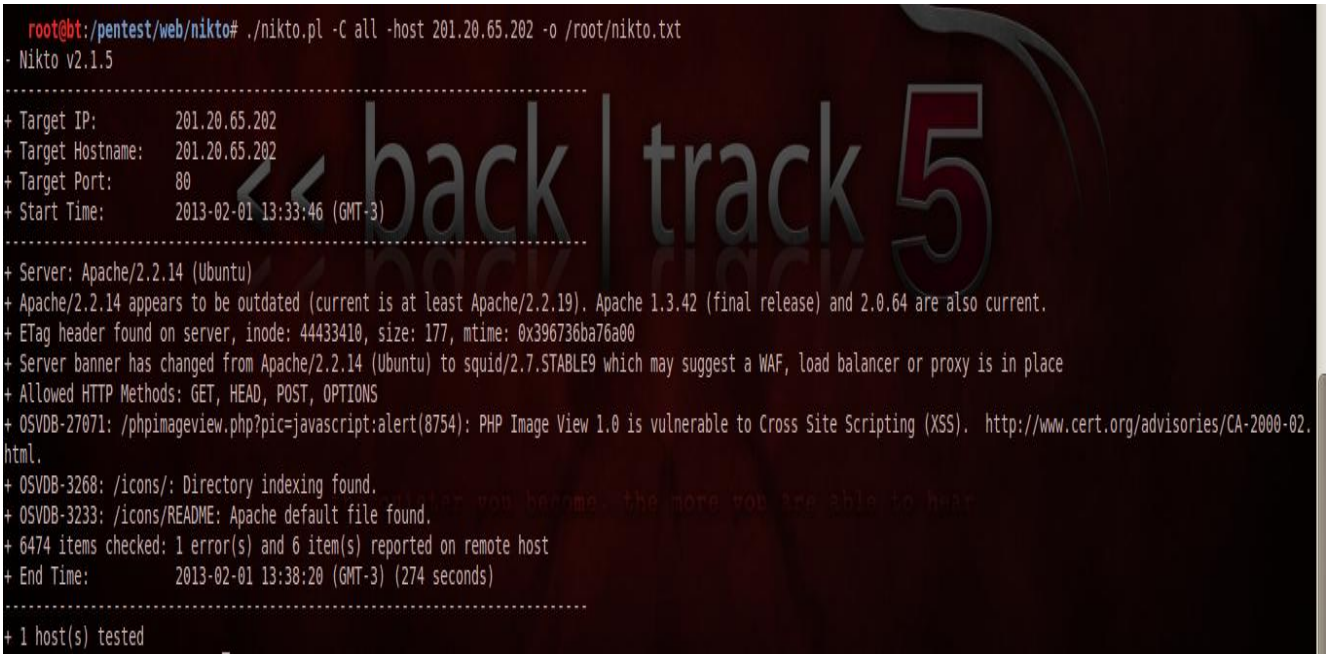

Figura 3.7 - Resultados Scanner Web Nikto

3.3.1 Resultados obtidos na fase de reconhecimento

1. Foi realizado com sucesso o escaneamento da rede interna do campus para obter informações sobre os hosts ativos. A Figura 3.8 apresenta um resumo da topologia da rede. É possível observar que a faixa de rede local é 10.0.0.0/24.
2. As máquinas referentes aos domínios sistemas.quixada.ufc.br (maracana), rc.quixada.ufc.br (abilhao) encontra-se na rede local. Pela figura é possível observar que a resposta do traceroute retorna um tempo inferior a 30 milissegundos para ambas as máquinas evidenciando sua localização a um salto de distância dentro da rede.
3. A máquina de ip 201.20.65.193 corresponde ao gateway situado no provedor ISP Baydenet com distância maior que 100 milissegundos.
4. Nesta fase consegui-se obter o IP do servidor responsável pelo domínio quixada.ufc.br. Tal informação não tinha obtida na fase pesquisa e investigação. É possível observar que ele não se encontra na rede do Campus.
5. A máquina maracana possui sistema operacional OpenBSD versão 4.0 e a maquina abilhao possui sistema operacional Linux versão 2.6.
6. Acessar a internet através da rede dos alunos gera algumas vezes mensagens de bloqueios a páginas. A máquina que responde bloqueando os acessos aparece como a a maracana. Pode se supor que sendo o OpenBSD um sistema com foco em segurança, a máquina maracanã também seja utilizada como gateway e firewall da rede.
7. As vulnerabilidades e informações adicionais obtidas nesta fase podem ser encontradas no capítulo do relatório técnico.
8. Uma séria de serviços foram encontrados seriamente desatualizados. Se estes forem atacados por um hacker com melhor conhecimento técnico ou tempo disponível, os servidores podem vir a sofrer sérios danos. A lista de serviços também se encontra no relatório técnico.

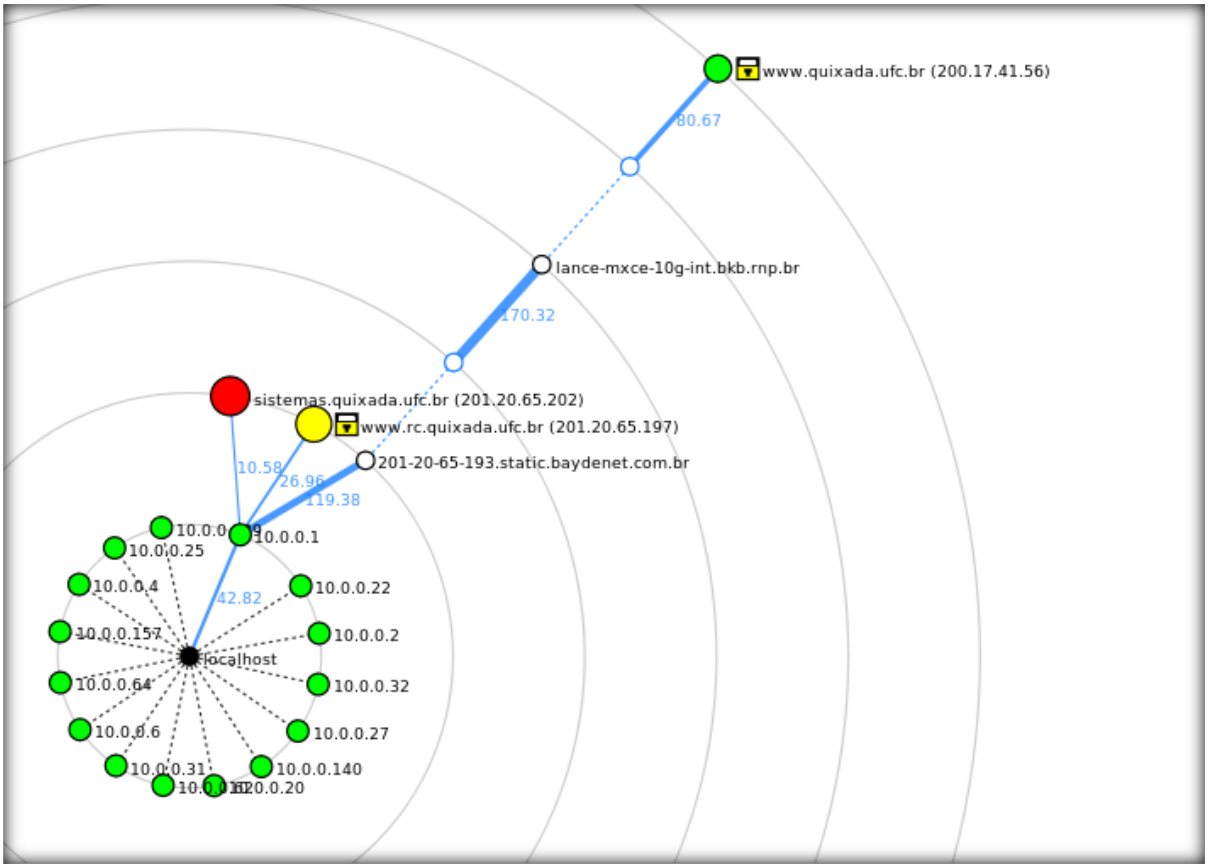

Figura 3.8- Mapa da Topologia da Rede descoberta na fase de Scanner

3.4 Exploração

Após uma cuidadosa análise das vulnerabilidades descobertas, o próximo passo é pesquisar por *exploits* que explorem essas vulnerabilidades.

As principais possibilidades de exploração que surgiram após cuidadosa análise dos resultados das fases anteriores foram:

- Foi encontrada uma versão desatualizada do servidor Apache nas duas máquinas para a qual existia uma vulnerabilidade que permitia DoS por consumo de memória e CPU. O *exploit* encontrado explorava uma vulnerabilidade nos dados do cabeçalho fazendo com que um único pacote fosse interpretado como uma série de requisições. Uma possibilidade de ataque é verificar como os servidores do campus reagiriam a um ataque dessa natureza.

- Teste de vulnerabilidade na rede wireless. O ataque seria tentar descobrir a senha de acesso à alguma das redes administrativas do Campus. Após ser capaz de se autenticar em alguma das redes administrativas, o próximo passo seria escanear a procura de novas informações.
    - Ataque de dicionário a senha da rede administrativa
    - Exploração da vulnerabilidade WPS nos *Access Points*.
    - Ataque por força bruta caso nenhum dos anteriores funcione.
- Pôde ser observado que a velocidade de enlace do Campus disponível para os alunos é de 4 Mpbs. Supõe-se que se este não for o enlace total, deve existir largura de banda reservada para os professores e servidores ou para outros serviços do Campus.
- Realizar-se-á um teste de DoS por inundação utilizando o conceito de *stress testing*. Será realizado um teste partindo de dentro da rede do Campus e outro teste partindo da rede externa.

3.4.1 Resultados obtidos na fase de exploração

Metasploit

A exploração da vulnerabilidade encontrada no servidor Apache exigia que o teste não fosse realizado no ambiente de produção. Tal teste poderia gerar resultados inesperados e o termo de compromisso assinado exigia que não fossem realizados ataques que pudessem comprometer a integridade da rede ou causar danos.

Para explorar essa vulnerabilidade fazia-se necessário simular o ambiente de forma fidedigna. Isso implicaria em obter um hardware igual com os mesmos sistemas, serviços e versões no mínimo. Devido as dificuldade encontradas em se montar tal ambiente, optou-se por não realizar este teste visto que esta falha que pode ser facilmente corrigida com a atualização do software.

O ataque seria efetuado executando-se os seguintes passos:

- Fazer o download do código do exploit no site do metasploit.
- Adicionar o código ao framework do metasploit.
- Executá-lo dentro do framework passando por linha de comando as informações necessárias para o ataque, tal como ip do alvo.

A tela inicial do console do metasploit pode ver vista na Figura 3.9.

Figura 3.9- Framework Metasploit

Testes de vulnerabilidade da rede Wireless

Para o teste de vulnerabilidade na rede Wireless foi utilizado o Reaver, software que identifica vulnerabilidades caso a máquina tenha habilitado o WPS. O Reaver trabalha em conjunto com as ferramentas aircrack-ng. A placa de rede deve suportar modo promíscuo. A Figura 3.11 apresenta a listagem das redes realizada com a ferramenta airodump, que é parte do pacote aircrack-ng.

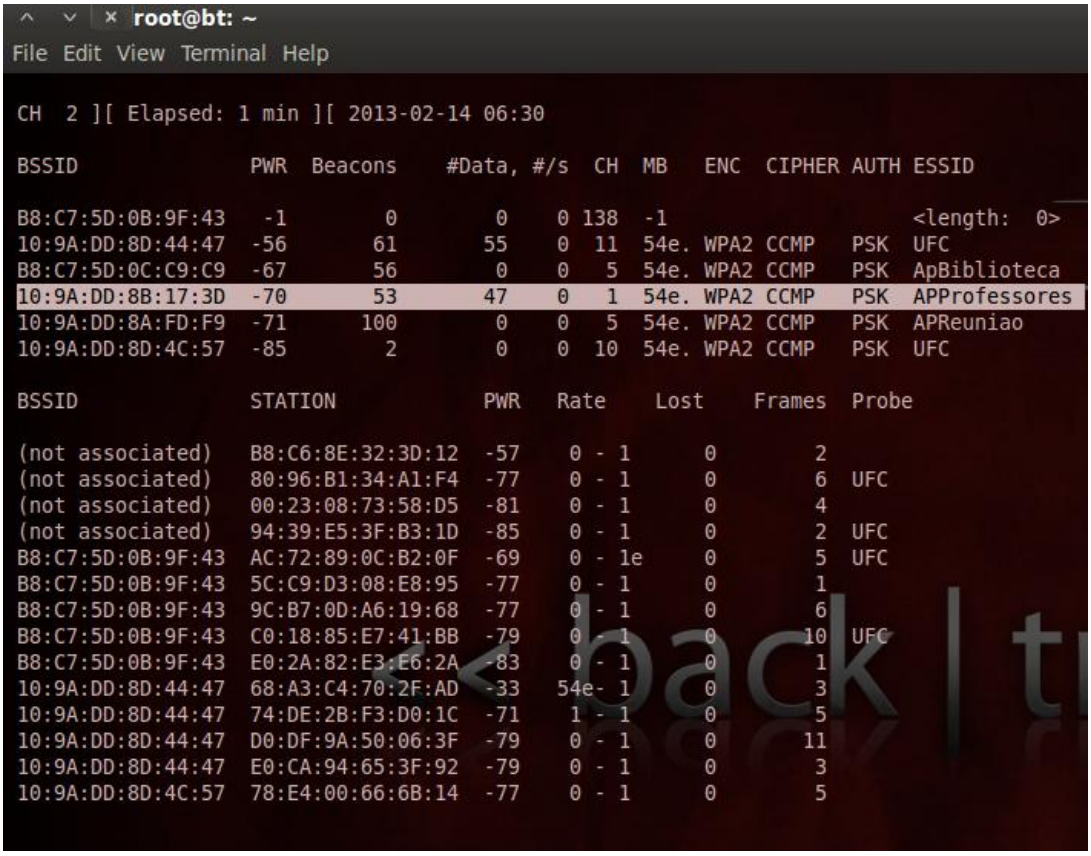

Figura 3.10- Listagem das redes com airodump

Identificada a rede “alvo”, APProfessores com BSSID:10:9A:DD:8D:17:3D, o Reaver é utilizado com objetivo de descoberta do PIN. A Figura 3.11 mostra ferramenta realizando o ataque.

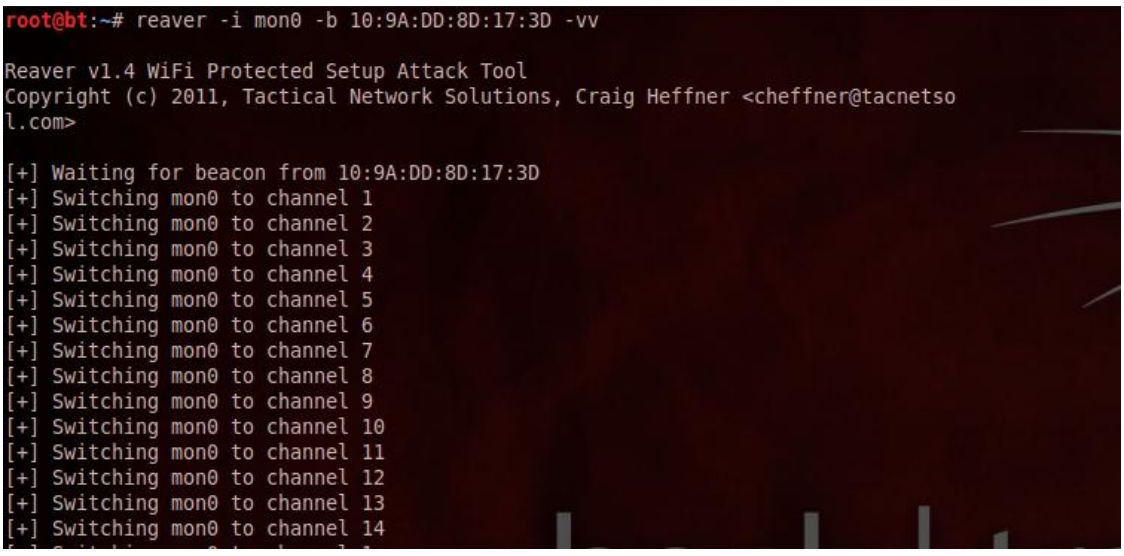

Figura 3.11- Reaver em busca da vunerabilidade WPS

Como resultado obtido o Reaver não conseguiu completar o ataque. Uma busca posterior para descobrir quais dispositivos estavam habilitados com WPS mostrou que nenhum dos *Access Poins* do prédio tinha essa opção habilitada, Figura 3.12. Pode-se concluir que o ataque não daria certo e que nenhum dos equipamentos da rede é suscetível a este tipo de ataque.

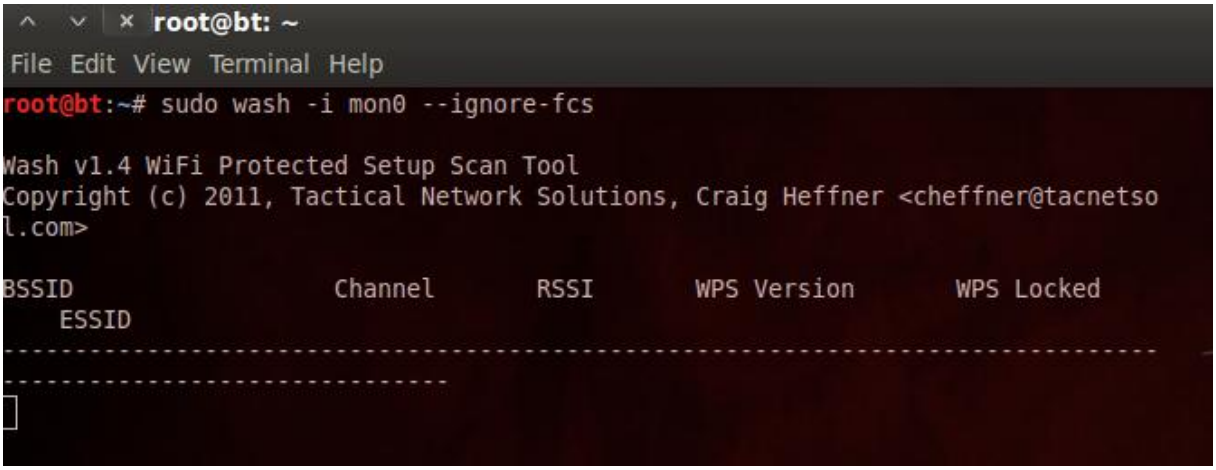

Figura 3.12 - Identificando WPS em rede

Ataque de dicionário

O ataque de dicionário à rede wireless foi realizado utilizando o aircrack-ng. A primeira etapa foi escolher a base de dados que seria utilizada no ataque. Optou-se por procurar uma base que incluísse ou possuísse palavras em língua portuguesa. A base de dados utiliza no teste foi obtida em http://www.outpost9.com/files/WordLists.html. O ataque utilizando esta base de dados não obteve sucesso. Por questões de tempo hábil para executar o teste de penetração, não foram tentados ataques com outras bases de dados ou ataques híbridos que utilizem ataque de dicionário com variações. O que poderia ter levado a um sucesso na detecção dependendo da força da senha que protege a rede.

Ataque de dicionário

Foi executado um ataque de força bruta contra a senha da rede dos professores. O WPA exige uma senha mínima de 8 caracteres. Apenas utilizando letra minúsculas e números para uma senha entre 8 e 10 caracteres existiriam 146805426396928 chaves diferentes. Uma máquina atual é capaz de testar até 1000 senhas por segundos. Se a senha fosse realmente

composta só por letras minúsculas e números testar todas as possibilidades levaria 7000 anos.

Uma máquina foi deixada executando o teste de força bruta por três dias. Após 3 dias de tentativas sem sucesso o ataque foi abortado.

Ataque de força bruta

O ataque de DoS por inundação foi realizado utilizando a ferramenta T50 tanto para rede interna como pela rede externa. A Figura 3.13 mostra as opções utilizadas para realizar o ataque ao host maracana na porta 80 onde se encontra o servidor Apache.

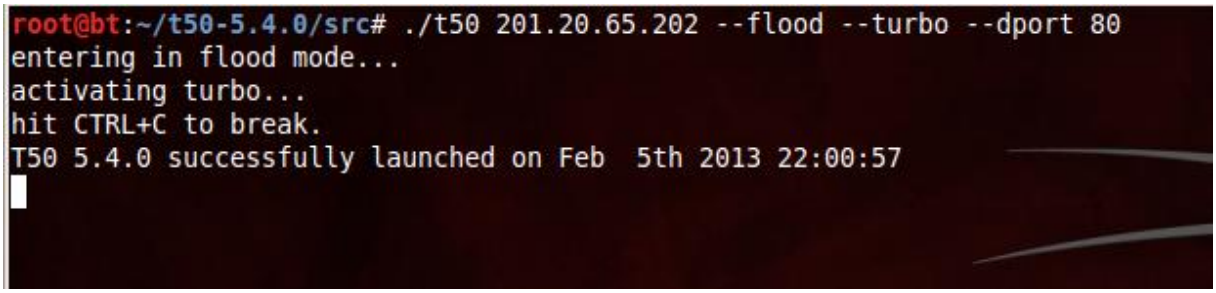

Figura 3.13 - Usando Ferramenta T50

Os teste foram realizados no ambiente de produção desde que estes ataques não geram danos permanentes à rede. Todos os serviços da máquina voltam a funcionar imediatamente após o fim do ataque.

Consequência do ataque originado na rede interna

Ataque ao maracana

O primeiro servidor a ser atacado foi o **maracana**, responsável por hospedar os sistemas acadêmicos e que supõe-se ser o firewall e gateway da rede. Em média, entre 2 a 3 minutos após o início do ataque, utilizando uma única máquina para gerar a inundação:

- a rede interna perdeu a conexão com a internet.
- Acesso a partir da rede interna:
    - não era possível acessar nenhum dos sistemas acadêmicos,
    - não era possível acessar o site do curso de Redes.
- Acesso a partir da rede externa:
    - não era possível ou demorava muito o acesso aos sistemas acadêmicos.

- não era possível ou demorava muito o acesso ao site do curso de Redes.

Pelos resultados podemos supor que:

- a máquina maracana realmente é o Proxy da rede desde que
  - não foi possível alcançar o abilhao a partir da internet enquanto o maracana estava sobrecarregado.
- Como não foi possível acessar o abilhao também pela rede interna, supõe-se que são os mesmos *switchs* que encaminham o tráfego interno a ambos os servidores e que o ataque sobrecarregou também os *switch*.
- O ataque é possível e causa sério problema de negação de serviço na rede.

Existe no campus de Quixadá um serviço interno disponível para alunos e servidores que possibilita a visualização do tráfego na rede para qualquer um dos *switchs* do Campus. Este serviço pode ser encontrado em http://nagios.quixada.ufc.br/mrtg. Foi possível visualizar a vazão no switch dos alunos durante o ataque como pode ser visto na Figura **Erro! Fonte de referência não encontrada.**. A vazão máxima foi de 81 Mpbs.

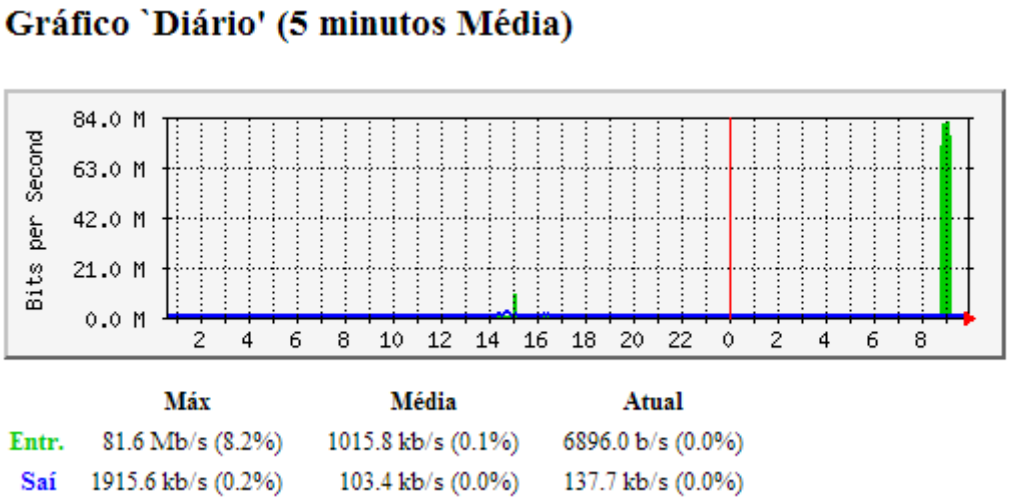

Figura 3.14– Tráfego medido pelo Nagius no switch dos alunos

Ataque ao abilhao

Ao atacar o abilhao a partir da rede interna:

- A rede interna ficou sem conexão com a internet.
- De dentro da rede
  - não era possível acessar o site dos sistemas acadêmicos,

    - não era possível acessar o site do curso de Redes.
- De fora de rede
    - era possível acessar o site dos sistemas,
    - não era possível acessar o site do curso de Redes.

Supõe-se que:

- a impossibilidade de acesso a internet a partir da rede interna foi gerado pela sobrecarga nos *switchs* e
- o acesso a partir da rede externa aos sistemas acadêmicos não é prejudicado.

Consequência do ataque originado na rede externa

Ataques iniciados com a mesma ferramenta, mas a partir da rede externa não foram capazes de gerar negação de serviços. O link utilizado era uma conexão Velox com capacidade nominal de 10 Mega de download e 1 de upload. Além disso, alguns instantes após o início do ataque, o provedor ISP onde estava conectado o atacante encerrava a conexão. Supõe-se que haja um mecanismo de detecção de atividades anômalas no provedor que causava automaticamente o aborto da conexão.

O T50 permite que um atacante que tenha acesso remoto a várias máquinas em redes distintas inicie um ataque coordenado cujo resultado seria a soma da força dos ataques individuais. Por dificuldade de encontrar em Quixadá máquinas e links disponíveis cuja soma dos uploads fosse pelo menos 10 Mega esse ataque não foi realizado, mesmo sendo completamente viável.

3.5 Conclusão

Este Capítulo mostrou as ferramentas e as tentativas de ataque planejadas. As mais viáveis foram realizadas e os resultados foram apresentados. As não realizadas estão justificadas, porem são totalmente viáveis caso o atacante possua tempo e recursos disponíveis.

4 RELATÓRIO TÉCNICO

4.1 Introdução

Para a presente investigação foi escrito um relatório de avaliação técnica. O relatório contém:

- Relação das vulnerabilidades
    - Dano gerado pela possível exploração da vulnerabilidade.
    - Dificuldade de exploração e recursos necessários para tal.
- Recomendações de segurança para correção ou minoração dos riscos.

4.2 Apache

Toda essa seção foi retirada do site apache.org e nenhuma modificação foi realizada no texto aqui apresentado. Ela foi incluída aqui e não como Anexo porque é de fundamental importância para a compreensão das métricas existentes no relatório técnico.

O Apache tem a sua própria pontuação de impacto de cada falha de segurança que afeta o servidor web Apache, utilizando uma escala muito semelhante ás utilizadas por outros grandes fornecedores. Basicamente, o objetivo do sistema de classificação é responder à pergunta: "Como eu deveria estar preocupado sobre essa vulnerabilidade?".

O Apache usa as seguintes descrições para decidir sobre a classificação de impacto para dar a cada vulnerabilidade:

- **Crítico -** A vulnerabilidade é classificada com um impacto crítico é uma que poderia ser explorada por um atacante remoto para obter o Apache para executar código arbitrário (como o usuário que o servidor está sendo executado, ou raiz). Estes são os tipos de vulnerabilidades que podem ser exploradas automaticamente pelos *crackers*.

- **Importante -** Uma vulnerabilidade classificado como impacto importante é aquela que pode resultar na fuga de dados ou disponibilidade do servidor. Para o servidor web Apache isto inclui questões que permitem uma fácil negação de serviço remoto (algo que

está fora de proporção com o ataque ou com uma consequência duradoura), acesso a arquivos arbitrários fora da raiz do documento, ou o acesso a arquivos que devem ser de outra forma impedidos por limites ou autenticação.

- **Moderada -** A vulnerabilidade é avaliada como moderada, se houver possibilidade significativa de problema, mas em gral de dificuldade de exploração mediano. Isso pode ocorrer porque a falha não afeta as configurações possíveis, ou é uma configuração que não é amplamente utilizado, ou onde um usuário remoto deve ser autenticado, a fim de explorar o problema. Falhas que permitem que o Apache para servir listas do diretório em vez de arquivos de índice são incluídas aqui, como são falhas que podem travar um processo

- **Baixo -** Todas as outras falhas de segurança são classificadas como de baixo impacto. Essa classificação é utilizada para problemas que se acredita ser extremamente difícil de explorar, ou onde um exploit apresenta consequências mínimas.

4.3 CVE

Essa seção apresenta um resumo das principais características do CWE, que é um repositório de vulnerabilidades que já foram publicamente reportadas.

A especificação Reconhecimento Fraqueza Comum (CWE) fornece uma linguagem comum de discurso para discutir, encontrar e lidar com as causas de vulnerabilidades de software de segurança e como eles são encontradas na arquitetura de código, design, ou sistema onde cada CWE representa um tipo de vulnerabilidade único.

O CWE é atualmente mantido pelo MITRE[13] Corporation com o apoio da National Cyber Security Division (DHS) [14]contando assim com uma lista de definição pormenorizada de cada CWE individualmente em seu site; O NVD[15] integra CWE na pontuação de vulnerabilidades CVE, fornecendo uma seção transversal da estrutura CWE geral.

As seções seguintes apresentam a relação das vulnerabilidades encontradas e informações com relação ao impacto de confidencialidade, integridade, disponibilidade e grau de dificuldade de exploração.

[13] Organização americana sem fins lucrativos, responsável por gerenciar Centros financiados pelo governo federal, relacionados à Pesquisa Desenvolvimento e segurança digital.
[14] Divisão do Departamento de Segurança Cibernética e Comunicação dos Estados Unidos.
[15] Repositório do governo dos EUA de padrões de gerenciamento de dados baseados em vulnerabilidades.

4.4 Relação das vulnerabilidades reportadas pelo Apache

A contribuição do presente trabalho nessa seção foi a de procurar as vulnerabilidades nos diversos repositórios de vulnerabilidades, agrupá-los, montar as tabelas com as informações obtidas e transcrever os textos que os descrevem. As vulnerabilidades estão ordenadas por grau de criticidade.

Descrição Vulnerabilidade 1: O filtro byterange no Servidor HTTP Apache 1.3.x, 2.0.x através 2.0.64 e 2.2.19 através 2.2.x, permite que atacantes remotos possam causar uma negação de serviço por consumo excessivo de memória e consumo de CPU através de um cabeçalho de intervalo que expressa múltiplos intervalos sobrepostos, como explorado livremente em agosto de 2011, uma vulnerabilidade diferente do CVE-2007-0086.

Tabela 4.1 – Vulnerabilidade 1

Tipos de Vulnerabilidade	- 2011-3192
Pontuação CVSS	7,8
Impacto Confidencialidade	Nenhum – Não há impacto para confidencialidade do sistema
Impacto Integridade	Nenhum – Não há impacto para integridade do Sistema.
Impacto Disponibilidade	Completa – Desligamento Total do recurso afetado.
Complexidade de Acesso	Baixa – Condições de acesso especializado ou de circunstâncias atenuantes não existem. Muito pouco conhecimento ou habilidade é necessário para explorar.
Autenticação	Não exigida – Não é necessária autenticação para explorar a vulnerabilidade.
Tipo de Vulnerabilidade	Negação de Serviço
CWE ID	399

Descrição Vulnerabilidade 2 - Envars no Apache HTTP Server 2.4.2 lugares antes de um nome de diretório de comprimento zero no LD_LIBRARY_PATH, que permite que os usuários locais para obter privilégios por meio de um cavalo de Tróia DSO no diretório atual de trabalho durante a execução de apachectl

Tabela 4.2 – Vulnerabilidade 2

Tipos de Vulnerabilidade	- CVE-2012-0883
Pontuação CVSS	6.9
Impacto Confidencialidade	Completa- Não é a divulgação de informação total, resultando em todos os arquivos de sistema que está sendo revelado.
Impacto Integridade	Conclui - Existe um compromisso total de integridade do sistema. Existe uma perda completa de proteção do sistema, o que resulta em todo o sistema a ser comprometida.
Impacto Disponibilidade	Completa – Desligamento Total do recurso afetado.
Complexidade de Acesso	Médio - As condições de acesso são um pouco especializados. Algumas condições devem ser satisfeitas exploração
Autenticação	Não exigida – Não é necessária autenticação para explorar a vulnerabilidade.
Tipo de Vulnerabilidade	Obter privilégios
CWE ID	264

Descrição Vulnerabilidade 3: A função ap_proxy_ajp_request em mod_proxy_ajp.c em mod_proxy_ajp no Servidor HTTP Apache 2.2.x antes de 2.2.15 não lidar correctamente com certas situações em que um cliente envia nenhum corpo solicitação, que permite que atacantes remotos possam causar uma negação de serviço (falha no servidor de back-end) por meio de um pedido trabalhado, relacionado com a utilização de um código de erro 500, em vez do código de erro apropriado 400.

Tabela 4.3 – Vulnerabilidade 3

Tipos de Vulnerabilidade	- CVE-2010-0408
Pontuação Impacto CVSS	2.9
Pontuação Exploração CVSS	10
Impacto Confidencialidade	Completa- Divulgação total de informação, resultando em todos os arquivos de sistema que está sendo revelado.
Impacto Integridade	Conclui - Existe um compromisso total de integridade do sistema. Existe uma perda completa de proteção do sistema, o que resulta em todo o sistema a ser comprometida.
Impacto Disponibilidade	Completa – Desligamento Total do recurso afetado.
Complexidade de Acesso	Baixa -
Autenticação	Não exigida – Não é necessária autenticação para explorar a vulnerabilidade.
Tipo de Vulnerabilidade	Negação de Serviço
CWE ID	703

Descrição Vulnerabilidade 4: O módulo mod_proxy no Servidor HTTP Apache 1.3.x através de 1.3.42, 2.0.64 através 2.0.x, 2.2.x e através de 2.2.21, quando a Revisão 1179239 patch está

no lugar, não interage adequadamente com uso de (1) RewriteRule e (2) as combinações do padrão ProxyPassMatch para a configuração de um proxy reverso, que permite que atacantes remotos para enviar solicitações a servidores da intranet através de um URI malformado contendo um @ (arroba) e um personagem: (dois pontos) de caracteres em posições inválidas. NOTA: esta vulnerabilidade existe devido a uma correção incompleta para CVE-2011-3368.

Tabela 4.4 – Vulnerabilidade 4

Tipos de Vulnerabilidade	**- CVE-2011-4317**
Impacto CVSS	2,9
Exploração CVSS	8,6
Impacto Confidencialidade	Completa- Não é a divulgação de informação total, resultando em todos os arquivos de sistema que está sendo revelado.
Impacto Integridade	Conclui - Existe um compromisso total de integridade do sistema. Existe uma perda completa de proteção do sistema, o que resulta em todo o sistema a ser comprometida.
Impacto Disponibilidade	Completa – Desligamento Total do recurso afetado.
Complexidade de Acesso	Medio -
Autenticação	Não exigida – Não é necessária autenticação para explorar a vulnerabilidade.
Tipo de Vulnerabilidade	Permite a modificação não autorizada
CWE ID	264

Descrição Vulnerabilidade 5: protocol.c no Apache HTTP Server 2.2.x através 2.2.21 não restringe adequadamente as informações de cabeçalho durante a construção de Bad Request (**(**400) em relatórios de erro, o que permite que atacantes remotos para obter os valores dos cookies HttpOnly através de vetores envolvendo um (1) de comprimento ou (2) cabeçalho mal formado em conjunto com o script web criado.

Tabela 4.5 – Vulnerabilidade 5

Tipos de Vulnerabilidade	**- CVE-2012-0053**
Pontuação Impacto CVSS	2.9
Pontuação Exploração CVSS	8,6
Impacto Confidencialidade	Completa- Não é a divulgação de informação total, resultando em todos os arquivos de sistema que está sendo revelado.
Impacto Integridade	Conclui - Existe um compromisso total de integridade do sistema. Existe uma perda completa de proteção do sistema, o que resulta em todo o sistema a ser comprometida.
Impacto Disponibilidade	Nenhuma.
Complexidade de Acesso	Baixa -
Autenticação	Não exigida – Não é necessária autenticação para explorar a vulnerabilidade.

Tipo de Vulnerabilidade	Permite a divulgação não autorizada de informação
CWE ID	264

Recomendação

Todas essas vulnerabilidades no servidor web podem ser corrigidas com a atualização do Apache para versão 2.2.20.

4.5 Vulnerabilidades e Recomendações reportadas pelo Nikto

A contrubuição desse trabalho nessa seção foi de encontrar as vulnerabilidades nos repositórios da OSVDB e transcrevê-las aqui.

O Nikto usa como parâmetro as vulnerabilidades da OSVDB, um repositório de vulnerabilidade, independente e aberto baseado na web criado para a comunidade de segurança. O objetivo do OSVDB é fornecer informações precisas e detalhadas, atuais e imparciais sobre vulnerabilidades de segurança.

As vulnerabilidades encontradas com o Scanner Nikto podem ser encontradas nas próximas seções:

Vulnerabilidade 3268 - Diretório de indexação Ativado.

Descrição: Indexação diretório foi encontrado para ser habilitado no servidor web. Embora não exista uma vulnerabilidade conhecida ou explorar associada a este, pode revelar sensível ou "escondidos" arquivos ou diretórios para usuários remotos, ou ajuda em ataques mais focados.

Localização: Remoto / Network Access Tipo de ataque:
Divulgação de Informações
Impacto : Perda de Confidencialidade Exploit : PoC / Exploit Pública de Divulgação :
OSVDB Verificado OSVDB : Web relacionados

Recomendação: Desativar a indexação do diretório de acordo com a documentação do seu servidor web

Vulnerabilidade 27071 - PHPImageView phpimageview.php pic XSS parâmetro

Nota de Perigo - 6.8

Descrição: (descrição fornecida por <a href = "http://cve.mitre.org/cgi-bin/cvename.cgi?name=2002-1724" target = "_blank "> CVE </ a>) </ em>: Cross-site scripting vulnerabilidade (XSS) no phpimageview.php para PHPImageView 1,0 permite que atacantes remotos para executar script arbitrário como outros usuários através do parâmetro pic.

Localização: Remoto / Network Access Tipo de ataque : Entrada de Manipulação Impacto : Perda de Integridade Solução : Upgrade Divulgação : Vendedor Verificado OSVDB : Web relacionados

Recomendação: Upgrade para a versão 2.0 ou superior, como foi relatado para corrigir essa vulnerabilidade. Uma atualização é necessária já que não existem soluções conhecidas.

Vulnerabilidade 6233 - Secure Computing Sidewinder G2 Firewall Proxy RTSP inválido Tráfego DoS.

Nota de Perigo - 5.0

Descrição: Sidewinder G2 Firewall contém uma falha que pode permitir que uma negação de serviço remoto. A falha passível de descoberta quando os erros não especificados dentro do proxy RTSP pode ser explorado para causar falha no processamento de tráfego RTSP mal formado, e irá resultar em perda de disponibilidade para a plataforma. Não há mais detalhes disponíveis.

Localização: Remoto / Network Access Tipo de Ataque : Negação de Serviço Impacto : Perda de Disponibilidade Exploit : Exploit rumores Divulgação : OSVDB Verificado OSVDB : Software de Segurança

Recomendações: Atualmente, não existem soluções conhecidas ou atualizações para corrigir esse problema. No entanto, Secure Computing Corporation lançou um patch para resolver esta
Vulnerabilidade.

Vulnerabilidade 74721 - Apache HTTP Server ByteRange memória do filtro Esgotamento remoto DoS

Descrição: A vulnerabilidade de negação de serviço foi encontrado na forma como os vários intervalos de sobreposição são manipulados pelo servidor Apache HTTPD antes da versão 2.2.20. Uma ferramenta de ataque está circulando na natureza. Uso ativo

desta ferramenta tem sido observado. O ataque pode ser feito remotamente e com um número modesto de solicitações pode causar consumo de memória e CPU do servidor muito elevado. O padrão httpd Apache versão 2,0 instalações antes de 2.0.65 ea versão 2.2.20 2,2 antes são vulneráveis. Apache 2.2.20 faz corrigir este problema, no entanto, com uma série de efeitos colaterais (ver notas de lançamento). Versão 2.2.21 corrige um defeito protocolo em 2.2.20, e também introduz a directiva MaxRanges. Apache 1.3 não é vulnerável. No entanto, como explicado na secção dos antecedentes com mais detalhe - este ataque causar uma carga significativa e possivelmente inesperado. Você é aconselhado a rever a sua configuração.

Localização : Remoto / Network Access

Tipo de Ataque : Negação de Serviço

Impacto : Perda de Disponibilidade

Exploit : PoC / Exploit Pública **de Divulgação** : Divulgação descoordenada

Recomendação: Upgrade para o Apache 2.0.65, ou Apache 2.2.20 ou versão posterior. Consulte o Apache vendedor consultivo na seção de referências para mais detalhes.

Vulnerabilidade: OSVDB-3268: GET /icons/: /icons/: Directory indexing found.

Descrição: Indexação de diretório foi encontrado para ser habilitado no servidor web. Embora não exista uma vulnerabilidade conhecida ou explorar associada a este, pode revelar sensível ou "escondidos" arquivos ou diretórios para usuários remotos, ou ajuda em ataques mais focados.

Recomenação: Desativar a indexação do diretório de acordo com a documentação do servidor web.

Vulnerabilidade OSVDB-3233: GET /icons/README: /icons/README: Apache default file found.

Descrição: Um arquivo padrão de diretório ou programa CGI que instalado por padrão com o servidor web ou o software instalado foi encontrado. Embora não exista uma vulnerabilidade conhecida ou explorar associada a este, arquivos padrão muitas vezes revelar informações sensíveis ou conter vulnerabilidades desconhecidas ou não-revelado. A presença de tais arquivos também pode revelar informações sobre a versão

do servidor web ou sistema operacional.

Recomendações: Remova os arquivos do servidor web ou restrinja o acesso a eles.

4.6 Vulnerabilidades Identificadas pelo Scanner Nessus.

Escaneamento do site rc.quixada.ufc.br

Vulnerabilidade CVE-1999-0505 - É possível logar no sistema remoto.

Descrição: O host remoto está executando um dos sistemas operativos Windows da Microsoft sistemas. Foi possível logar como um usuário convidado usando um conta aleatória.

Solução: Na política de grupo alterar a configuração para "Acesso à rede: compartilhamento e modelo de segurança para contas locais". Os usuários locais são autenticados como convidado' para 'Clássico - usuários locais autenticados como eles próprios ".

Fator de risco: Médio

CVSS pontuação base

5,0 (CVSS2 # AV: N / AC: L / Au: N / C: P / I: N / A: N)

Escaneamento do site dos sistemas acadêmicos

Vulnerabilidade CVE 1999-0505 - É possível logar no sistema remoto

Descrição: O serviço remoto tem uma de duas configurações que são conhecidos por serem necessário para o ataque CRIME O serviço de controle remoto tem uma configuração que pode torná-lo vulnerável ao ataque CRIME.:

- SSL / TLS compressão é ativada.

- TLS anuncia o protocolo SPDY anterior a versão 4.

Recomendação: Desativar a compressão e / ou o serviço SPDY.

Fator de risco: Médio

CVSS pontuação base: 4,3 (CVSS2 # AV: N / AC: M / Au: N / C: P / I: N / A: N)

4.7 Recomendações adicionais

Além das recomendações já expostas para cada vulnerabilidade são apresentadas nessa seção algumas outras recomendações que teriam inviabilizado ou dificultado a maioria dos ataques realizados.

1. IDS

A maioria dos ataques e escaneamentos seriam facilmente detectados se a rede do Campus possuísse algum sistema de detecção de intrusão. A sugestão é a instalação de pelo menos um IDS baseado em Rede (NIDS). O Snort é um IDS que pode funcionar tanto IDS de rede ou de Host protegendo assim ataques direcionados aos servidores e não apenas a rede.

2. Dicas comuns para evitar ataques DoS

Servidores que possam ser alvos de ataques devem sempre possuir programas antivírus instalados e atualizados assim como atualizadas versões de seus sistemas. As portas de comunicação abertas devem se limitar às que proveem serviços essenciais.

O tamanho do enlace disponível na rede deve ser observado. Deve ser estipulado um limite de largura de banda por serviço a fim de impedir que a rede seja usada como amplificadora em ataques.

O tráfego da rede deve ser analisado com cuidado e as solicitações de ping devem ser recusadas, a não ser em casos de real necessidade. Sistemas de detecção de intrusos baseados em Host são recomendados para proteção dos servidores que hospedarem serviços web.

As empresas devem possuir um plano de reação a incidentes.

Ataques DOS por inundação possuem algumas características detectáveis. Alguns tipos de firewall podem ser configurados para minimizar ataques DoS gerando restrições para alguns tipos de tráfego. Alguns parâmetros que podem ser utilizados são:

- Excesso de tráfego: A banda utilizada excede o máximo, ultrapassando o número de acessos esperados ou a assimetria deste.
- A existência de pacotes UDP e ICMP de tamanho acima do normal ou em excesso: Geralmente as sessões UDP utilizam pacotes pequenos de dados dificilmente maiores que 10 bytes (payload). As mensagens ICMP não excedem a faixa entre 64 e 128 bytes.

Pacotes cujo tamanho seja superior a esses números são considerados suspeitos de conter mensagens de controle, destinadas a cada um dos agentes que está participando do ataque. Apesar do conteúdo dos pacotes estar cifrado, o endereço do destino é verdadeiro, desta forma pode-se localizar um dos agentes que estão realizando o ataque baseado no seu fluxo de mensagens.

- Pacotes TCP e UDP que não fazem parte de uma conexão: Alguns tipos de DOS utilizam aleatoriamente vários protocolos (incluindo protocolos orientados a conexão) para enviar dados sobre canais não orientados a conexão. Isto pode ser detectado utilizando-se *firewalls* que mantenham o estado das conexões (*statefull-firewalls*). Outro ponto importante é que estes pacotes costumam destinar-se a portas acima de 1024.

Conclusão

As estatísticas de segurança da informação indicam que muitos dos ataques hackers as empresas vem de usuários internos que possuem informações sobre a rede. Isso torna as intranets especialmente vulneráveis.

O teste de penetração realizado partiu de dentro da rede da UFC, mas levando-se em conta um aluno que não tivesse nenhum conhecimento da rede. Na verdade, um aluno com intuito de executar um ataque conseguiria obter muitas informações através de engenharia social, conversando com professores ou os responsáveis pela rede, facilitando ainda mais o ataque. O acesso físico aos servidores ou outros recursos também seria um problema de difícil resolução, pois o Campus não mecanismos de segurança física eficiente, tais como câmeras, portas reforçadas, etc. Caso o aluno mal intencionado se ofereça como voluntário ou bolsista de TI, teria ainda mais acesso aos recursos e menos monitoramento. Desde que existem tantos casos difíceis de resolver no que tange a segurança da universidade, o mínimo que se deve ter são mecanismos eficientes de backup, firewall, IDS e uma política de Segurança que cubra ao menos a política de senhas.

Os testes realizados mostram a fragilidade da rede em uma grande diversidade de aspectos. Isso reflete a falta de um profissional de administração de redes com competências em Segurança de Redes. Na Universidade este seria o papel de um Analista de TI, cargo técnico administrativo que não existe no Campus da UFC-Quixadá. O atual responsável possui o cargo de Técnico de Laboratório e está alocado para a função de Gerente de TI pela falta de outro profissional mais qualificado.

O presente trabalho propunha a realização de testes de penetração para avaliar a potenciais vulnerabilidades da rede. O plano de testes foi gerado e executado. Todos os testes viáveis foram realizados e os resultados podem ser encontrados nos Capítulos 3 e 4. O relatório Técnico, parte integrante do Teste de Penetração encontra-se no Capítulo 4.

Espera-se com esse trabalho contribuir para melhoria da segurança dos sistemas da UFC, que os problemas reportados sejam corrigidos e que se crie uma cultura de avaliação preventiva em toda a Universidade.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT), NBR 17799:2005. **Código de pratica para a gestão da segurança da Informação.** ABNT, 2005.

BEAL, Adriana. **Segurança da Informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações**. São Paulo: Atlas, 2005. 236

CERT.br (2010). **Cartilha de Segurança para Internet. Núcleo de Informação e Coordenação do Ponto BR**. Disponível em <www.cert.br> Acesso em 22 de jun 2012

DEKKER Mareei, **Kent de Telecomunicações**. New York, A Enciclopédia Froehlich vol 15, 1997

FARMER, Dan; VENEMA, Wietse. **Improving the Security of Your Site By Breaking Into It**. USENET: posting, December 1993. 14

GORDON "Fyodor" Lyon, **Nmap Network Scanning** Insecure.com LCC Publishings. ISBN: 9780979958717

HERZOG, Pete. OSSTMM 3.0 **Open Source Security Testing Methodology Manual.** Isecon: Disponível em: <http://www.isecom.org/osstmm/>. Acesso em: Jun/2012

HOUAISS, Antônio. **Dicionário Houaiss da Língua Portuguesa**. Rio de Janeiro, Ed. Objetiva, 2001.

KIMBERLY Graves, **Ceh Certified Ethical Hacker Study Guide**. USA: Wiley Publishing, 2010. 439p.

NAKAMURA Emílio, GEUS Paulo. **Segurança de redes em ambientes cooperativos**. Br: Novatec, 2007. 489p.

NIC.br (2008). **TIC Domicílios e Usuários - Pesquisa sobre o Uso das Tecnologias da Informação e da Comunicação no Brasil**. Disponível em <http://www.cetic.br/indicadores.htm> Acesso em 22 de jun 2012.

PALMER Charles. **Ethical hacking.** USA: IBM Systems journal, Vol 40 (3): 769, 2011.

RABÊLO, Maicon; **Plano de continuidade aplicado à UFC de Quixadá.** Monografia, 2013.

STALLINGS, W. **Cryptography and network security: principles and practice**. 2. ed. Prentice Hall, 2006. 569 p.

WHITAKER, Andrew, NEWMAN Daniel. **Penetration Testing and Network Defense**. USA: Cisco Press, 2005. 400p.

Apêndice 1 – Termo de Compromisso

Autorizo a aluna Evelyne Ferreira Avelino, CPF: 05029440305, a executar procedimentos de auditoria de Segurança na rede do Campus da UFC Quixadá durante o período letivo de 2012.2. Entretanto todos os procedimentos executados devem ter o único objetivo de avaliar a segurança dos recursos internos, serviços e servidores. É vetada qualquer ação que coloque em risco a integridade permanente dos recursos ou mesmo temporária, desde que não possa ser corrigida pela mesma na sua condição de aluna.

_____
Jeandro de Mesquita Bezerra
Gerente de TI do Campus UFC – Quixadá.

Eu, Evelyne Ferreira Avelino, CPF: 05029440305, me comprometo a executar procedimentos de auditoria de Segurança na rede do Campus da UFC Quixadá apenas durante o período letivo de 2012.2. Afirmo que todos os procedimentos executados terão o único objetivo de avaliar a segurança dos recursos internos, serviços e servidores. Me comprometo a não executar nenhuma ação que coloque em risco a integridade permanente dos recursos ou mesmo temporária, que necessite de intervenção do departamento de TI para normalização do sistema.

_____
Evelyne Ferreira Avelino

Apêndice 2 – Acordo de confidencialidade e

Eu, Evelyne Ferreira Avelino, CPF: 05029440305, afirmo que as informações obtidas através dos procedimentos de auditoria serão utilizadas em fins acadêmicos para elaboração do trabalho de conclusão de curso com Tema: Análise Preventiva de Vulnerabilidades na UFC – Quixadá tendo como orientado o prof Dr. David Sena Oliveira. A monografia gerada utilizando-se dessas informações será publicada somente se obtiver aprovação do Coordenador de TI do Campus UFC – Quixadá. Não sendo aprovada, a mesma será arquivada em situação de sigilo conforme o estatuto da Universidade.

_____

Evelyne Ferreira Avelino.

Apêndice 3 – Resultado detalhado dos escaneamentos

nmap -T4 -O -A -v www.rc.quixada.ufc.br – sV

```
Starting Nmap 6.01 ( http://nmap.org ) at 2012-12-18 19:42 BRST
NSE: Loaded 93 scripts for scanning.
NSE: Script Pre-scanning.
Invalid target host specification: -
Failed to resolve given hostname/IP: sV.  Note that you can't use '/mask'
AND '1-4,7,100-' style IP ranges. If the machine only has an IPv6 address,
add the Nmap -6 flag to scan that.
Initiating Ping Scan at 19:42
Scanning www.rc.quixada.ufc.br (201.20.65.197) [4 ports]
Completed Ping Scan at 19:42, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:42
Completed Parallel DNS resolution of 1 host. at 19:42, 0.22s elapsed
Initiating SYN Stealth Scan at 19:42
Scanning www.rc.quixada.ufc.br (201.20.65.197) [1000 ports]
Discovered open port 53/tcp on 201.20.65.197
Discovered open port 443/tcp on 201.20.65.197
Discovered open port 8080/tcp on 201.20.65.197
Discovered open port 80/tcp on 201.20.65.197
Discovered open port 3690/tcp on 201.20.65.197
Completed SYN Stealth Scan at 19:42, 4.59s elapsed (1000 total ports)
Initiating Service scan at 19:42
Scanning 5 services on www.rc.quixada.ufc.br (201.20.65.197)
Completed Service scan at 19:43, 14.45s elapsed (5 services on 1 host)
Initiating OS detection (try #1) against www.rc.quixada.ufc.br
(201.20.65.197)
Initiating Traceroute at 19:43
Completed Traceroute at 19:43, 0.03s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 19:43
Completed Parallel DNS resolution of 2 hosts. at 19:43, 6.58s elapsed
NSE: Script scanning 201.20.65.197.
Initiating NSE at 19:43
Completed NSE at 19:44, 76.98s elapsed
Nmap scan report for www.rc.quixada.ufc.br (201.20.65.197)
Host is up (0.014s latency).
rDNS record for 201.20.65.197: abilhao.quixada.ufc.br
Not shown: 995 filtered ports
PORT     STATE SERVICE  VERSION
53/tcp   open  domain   ISC BIND 9.7.0-P1
| dns-nsid:
|_  bind.version: 9.7.0-P1
80/tcp   open  http     Apache httpd 2.2.14 ((Ubuntu))
| http-robots.txt: 16 disallowed entries (15 shown)
| /joomla/administrator/ /administrator/ /cache/ /cli/
| /components/ /images/ /includes/ /installation/ /language/
|_/libraries/ /logs/ /media/ /modules/ /plugins/ /templates/
|_http-methods: No Allow or Public header in OPTIONS response (status code
200)
|_http-generator: Joomla! - Open Source Content Management
|_http-title: UFC - Redes de Computadores
|_http-favicon: Unknown favicon MD5: E668F4BD56036E023DE82FFB5E90E998
443/tcp  open  ssl/http Apache httpd 2.2.14 ((Ubuntu))
| ssl-cert: Subject:
commonName=UFC/organizationName=UFC/stateOrProvinceName=CE/countryName=BR
| Issuer:
commonName=UFC/organizationName=UFC/stateOrProvinceName=CE/countryName=BR
```

```
| Public Key type: rsa
| Public Key bits: 1024
| Not valid before: 2012-10-18 19:16:24
| Not valid after:  2013-10-18 19:16:24
| MD5:   20c3 f06a 35b0 11e2 081e 66ca c946 9be4
|_SHA-1: 2112 68ea 8fd7 ea3a 47f1 04c8 e52f 6d95 c464 b394
|_http-title: Redirecionar
|_http-methods: No Allow or Public header in OPTIONS response (status code
200)
3690/tcp open  svnserve Subversion
8080/tcp open  http     Apache Tomcat/Coyote JSP engine 1.1
| http-methods: GET HEAD POST PUT DELETE OPTIONS
| Potentially risky methods: PUT DELETE
|_See http://nmap.org/nsedoc/scripts/http-methods.html
|_http-title: Apache Tomcat
Warning: OSScan results may be unreliable because we could not find at
least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:kernel:2.6
OS details: Linux 2.6.32 - 2.6.33
Uptime guess: 53.655 days (since Fri Oct 26 04:01:14 2012)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=203 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE (using port 443/tcp)
HOP RTT      ADDRESS
1   24.57 ms 10.0.0.1
2   26.96 ms abilhao.quixada.ufc.br (201.20.65.197)

NSE: Script Post-scanning.
Read data files from: /usr/local/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 105.31 seconds
           Raw packets sent: 2054 (92.920KB) | Rcvd: 25 (1.228KB)
```

nmap -sV -T4 -A -v sistemas.quixada.ufc.br

```
Starting Nmap 6.01 ( http://nmap.org ) at 2012-12-18 19:58 BRST
NSE: Loaded 93 scripts for scanning.
NSE: Script Pre-scanning.
Initiating Ping Scan at 19:58
Scanning sistemas.quixada.ufc.br (201.20.65.202) [4 ports]
Completed Ping Scan at 19:58, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:58
Completed Parallel DNS resolution of 1 host. at 19:58, 0.21s elapsed
Initiating SYN Stealth Scan at 19:58
Scanning sistemas.quixada.ufc.br (201.20.65.202) [1000 ports]
Discovered open port 8080/tcp on 201.20.65.202
Discovered open port 139/tcp on 201.20.65.202
Discovered open port 443/tcp on 201.20.65.202
Discovered open port 445/tcp on 201.20.65.202
Discovered open port 5666/tcp on 201.20.6
```

```
Discovered open port 80/tcp on 201.20.65.202
Discovered open port 8009/tcp on 201.20.65.202
Discovered open port 5432/tcp on 201.20.65.202
Completed SYN Stealth Scan at 19:58, 3.10s elapsed (1000 total ports)
Initiating Service scan at 19:58
Scanning 8 services on sistemas.quixada.ufc.br (201.20.65.202)
Completed Service scan at 19:58, 12.22s elapsed (8 services on 1 host)
Initiating OS detection (try #1) against sistemas.quixada.ufc.br
(201.20.65.202)
Retrying OS detection (try #2) against sistemas.quixada.ufc.br
(201.20.65.202)
Retrying OS detection (try #3) against sistemas.quixada.ufc.br
(201.20.65.202)
Retrying OS detection (try #4) against sistemas.quixada.ufc.br
(201.20.65.202)
Retrying OS detection (try #5) against sistemas.quixada.ufc.br
(201.20.65.202)
Initiating Traceroute at 19:59
Completed Traceroute at 19:59, 0.02s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 19:59
Completed Parallel DNS resolution of 2 hosts. at 19:59, 6.51s elapsed
NSE: Script scanning 201.20.65.202.
Initiating NSE at 19:59
Completed NSE at 19:59, 3.94s elapsed
Nmap scan report for sistemas.quixada.ufc.br (201.20.65.202)
Host is up (0.082s latency).
rDNS record for 201.20.65.202: 201-20-65-202.static.baydenet.com.br
Not shown: 992 closed ports
PORT     STATE SERVICE     VERSION
80/tcp   open  http        Apache httpd 2.2.14 ((Ubuntu))
| http-title: 302 Found
|_Did not follow redirect to https://sistemas.quixada.ufc.br/
|_http-methods: No Allow or Public header in OPTIONS response (status code
302)
139/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
443/tcp  open  ssl/http    Apache httpd 2.2.14 ((Ubuntu))
| ssl-cert: Subject: commonName=maracana.quixada.ufc.br
| Issuer: commonName=maracana.quixada.ufc.br
| Public Key type: rsa
| Public Key bits: 1024
| Not valid before: 2002-01-01 01:10:13
| Not valid after:  2011-12-30 01:10:13
| MD5:   4f0c 0d75 073b 4f0a b5f1 9429 db58 f0c0
|_SHA-1: 7583 323b 76ea c8ee 28d6 b0f8 71f8 135e dfd0 2879
| http-methods: GET HEAD POST PUT DELETE OPTIONS
| Potentially risky methods: PUT DELETE
|_See http://nmap.org/nsedoc/scripts/http-methods.html
|_http-title: Apache Tomcat/6.0.24 - Error report
445/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
5432/tcp open  postgresql  PostgreSQL DB (Portugese)
5666/tcp open  tcpwrapped
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
```

```
8080/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
| http-methods: GET HEAD POST PUT DELETE OPTIONS
| Potentially risky methods: PUT DELETE
|_See http://nmap.org/nsedoc/scripts/http-methods.html
|_http-title: Apache Tomcat/6.0.24 - Error report
No exact OS matches for host (If you know what OS is running on it, see
http://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=6.01%E=4%D=12/18%OT=80%CT=1%CU=34505%PV=N%DS=2%DC=T%G=Y%TM=50D0E7
OS:41%P=i686-pc-linux-gnu)SEQ(SP=FB%GCD=1%ISR=100%TI=RD%TS=22)OPS(O1=M5B4NW
OS:7ST11%O2=M578NW7ST11%O3=M280NW7NNT11%O4=M5B4NW7ST11%O5=M218NW7ST11%O6=M1
OS:09ST11)WIN(W1=FECC%W2=FECC%W3=FECC%W4=FECC%W5=FECC%W6=FECC)ECN(R=Y%DF=Y%
OS:T=42%W=FECC%O=M5B4NW7SLL%CC=N%Q=)T1(R=Y%DF=Y%T=42%S=O%A=S+%F=AS%RD=0%Q=)
OS:T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=Y%T=41%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=
OS:N)T7(R=N)U1(R=Y%DF=N%T=41%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=3B5B%RU
OS:D=G)IE(R=N)

Uptime guess: 0.000 days (since Tue Dec 18 19:59:16 2012)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=264 (Good luck!)
IP ID Sequence Generation: Randomized

Host script results:
| nbstat:
|   NetBIOS name: MARACANA, NetBIOS user: <unknown>, NetBIOS MAC: <unknown>
|   Names
|     MARACANA<00>         Flags: <unique><active>
|     MARACANA<03>         Flags: <unique><active>
|     MARACANA<20>         Flags: <unique><active>
|     \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
|     WORKGROUP<1d>        Flags: <unique><active>
|     WORKGROUP<1e>        Flags: <group><active>
|_    WORKGROUP<00>        Flags: <group><active>
| smb-security-mode:
|   Account that was used for smb scripts: guest
|   User-level authentication
|   SMB Security: Challenge/response passwords supported
|_  Message signing disabled (dangerous, but default)
|_smbv2-enabled: Server doesn't support SMBv2 protocol
| smb-os-discovery:
|   OS: Unix (Samba 3.4.7)
|   Computer name: maracana
|   Domain name: quixada.ufc.br
|   FQDN: maracana.quixada.ufc.br
|   NetBIOS computer name:
|_  System time: 2012-12-18 19:59:13 UTC-3

TRACEROUTE (using port 25/tcp)
HOP RTT      ADDRESS
1   8.68 ms  10.0.0.1
2   10.58 ms 201-20-65-202.static.baydenet.com.br (201.20.65.202)
NSE: Script Post-scanning.
```

```
Read data files from: /usr/local/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 48.47 seconds
           Raw packets sent: 1299 (65.540KB) | Rcvd: 1610 (126.291KB)
```