

UNIVERSIDADE FEDERAL DE SANTA CATARINA

**Aspectos Computacionais para um Ambiente de
Processo Ensino-Aprendizagem para Disciplina de
Segurança da Informação e de Redes**

DIOGO VIEIRA CARDOSO
0513846-9

Orientador: Prof. João Bosco Manguiera Sobral

Florianópolis
2012-1

Universidade Federal de Santa Catarina
Departamento de Informática e Estatística
Curso de Bacharelado de Sistemas de Informação

**Aspectos Computacionais para um Ambiente de Processo Ensino-
Aprendizagem para Disciplina de Segurança da Informação e de
Redes**

Diogo Vieira Cardoso

0513846-9

Trabalho de conclusão de curso apresentado
como parte dos requisitos para obtenção do
grau de Bacharel em Sistemas de Informação

Florianópolis

2012-1

Diogo Vieira Cardoso

**Aspectos Computacionais para um Ambiente de Processo Ensino-
Aprendizagem para Disciplina de Segurança da Informação e de
Redes**

Trabalho de conclusão de curso apresentado como parte dos requisitos para
obtenção do grau de Bacharel em Sistemas de Informação.

Orientador: João Bosco Manguiera Sobral
Universidade Federal de Santa Catarina
bosco@inf.ufsc.br

Banca examinadora

Prof.^a Carla Merkle Westphall
Universidade Federal de Santa Catarina
carla@lrg.ufsc.br

Prof. Frank Augusto Siqueira
Universidade Federal de Santa Catarina
frank@inf.ufsc.br

RESUMO

Este trabalho de conclusão de curso surge das experiências na disciplina de segurança do Curso de Graduação em Sistemas da Informação da UFSC. O objetivo é melhorar o processo de ensino-aprendizagem da disciplina, no que tange a ao ensino da disciplina em laboratório.

Pelas características do ensino prático de segurança, existe o problema de se extrapolar o ambiente do laboratório, podendo causar invasões inadequadas fora do ambiente de ensino.

A proposta deste trabalho é a criação de um novo ambiente computacional, onde os testes e experiências das aulas práticas podem ser aplicados sem o comprometimento dos ambientes computacionais utilizados pelos alunos do Centro Tecnológico da UFSC.

Neste novo ambiente, há, também, a preocupação com o conteúdo ministrado nas aulas práticas, demonstrando os problemas propostos pelo professor aos alunos, bem como a resolução deles.

Palavras-chave: Ensino de segurança, segurança da informação, segurança de redes, ambiente para ensino de segurança, práticas de segurança, virtualização, INE5680.

SUMÁRIO

1.	INTRODUÇÃO	1
1.1	Motivação.....	1
1.2	Objetivo Geral	3
1.3	Objetivos Específicos	3
1.4	Organização do Trabalho.....	3
2.	ASPECTOS DIDÁTICOS PARA O ENSINO DA DISCIPLINA EM LABORATÓRIO.....	5
2.1	Esquema de Plano de Aula.....	5
2.2	Assunto.....	5
2.3	Bibliografia Básica.....	6
2.4	Objetivos da Aula	6
2.5	Seleção do Conteúdo	6
2.6	Avaliação do Aprendizado.....	6
3.	O AMBIENTE COMPUTACIONAL.....	8
3.1	Descrição dos Hardwares disponíveis	8
3.2	Funcionalidades dos Hardwares	9
3.3	Preparação do Ambiente Computacional	9
3.3.1	A Virtualização	11
3.3.1.1	Conceito de Virtualização	12
3.3.1.2	Máquina Virtual e Hypervisor	14
3.3.1.3	Tipos de Virtualização.....	15
3.3.1.4	Vantagens da Virtualização	17
3.3.1.5	Características da Virtualização	18
3.3.2	Avaliação dos Principais Softwares de Virtualização	19
3.3.2.1	VMware	19
3.3.2.2	Xen Server	20

3.3.2.3	Oracle VirtualBOX.....	21
3.3.3	Configuração do Servidor.....	22
3.3.4	Configuração das Estações utilizadas pelos Alunos.....	24
3.4	Máquina Virtual Windows 2008 Server.....	26
3.5	Máquina Virtual Ubuntu Server.....	28
3.6	Máquina Virtual Backtrack.....	30
4.	PLANOS DAS AULAS PRÁTICAS.....	31
4.1	Aplicação de Criptografia com Chaves Simétrica e Assimétrica.....	31
4.1.1	Assuntos.....	31
4.1.2	Bibliografia Básica.....	31
4.1.3	Objetivos da Aula.....	32
4.1.4	Seleção do Conteúdo.....	32
4.1.5	Avaliação do Aprendizado.....	35
4.2	Ensino de Segurança da Informação: Aplicação em E-mail.....	36
4.2.1	Assuntos.....	36
4.2.2	Bibliografia Básica.....	36
4.2.3	Objetivos da Aula.....	37
4.2.4	Seleção do Conteúdo.....	37
4.2.5	Avaliação do Aprendizado.....	43
4.3	Ensino de Segurança da Informação: Aplicação WEB.....	44
4.3.1	Assuntos.....	44
4.3.2	Bibliografia Básica.....	44
4.3.3	Objetivos da Aula.....	45
4.3.4	Seleção do Conteúdo.....	45
4.3.5	Avaliação do Aprendizado.....	49
4.4	Ensino de Redes Privadas Virtuais: Estabelecimento de uma VPN.....	50
4.4.1	Assuntos.....	50

4.4.2	Bibliografia Básica.....	50
4.4.3	Objetivos da Aula	51
4.4.4	Seleção do Conteúdo	51
4.4.5	Avaliação do Aprendizado	56
4.5	Análise de vulnerabilidades – NMAP e OpenVAS	57
4.5.1	Assuntos	57
4.5.2	Bibliografia Básica.....	57
4.5.3	Objetivos da Aula	57
4.5.4	Seleção do Conteúdo	58
4.5.5	Avaliação do Aprendizado	63
4.6	Visão Geral de Defesas - Firewall.....	64
4.6.1	Assuntos	64
4.6.2	Bibliografia Básica.....	64
4.6.3	Objetivos da Aula	64
4.6.4	Seleção do Conteúdo	65
4.6.5	Avaliação do Aprendizado	69
4.7	Trabalho Final	71
4.7.1	Assuntos	71
4.7.2	Bibliografia Básica.....	71
4.7.3	Objetivos da Aula	71
4.7.4	Seleção do Conteúdo	72
4.7.5	Avaliação do Aprendizado	72
5.	CONCLUSÃO.....	74
5.1	Trabalhos Futuros.....	75
6.	BIBLIOGRAFIA	76
7.	ANEXOS.....	79
7.1	ANEXO 1 – Plano de Ensino da disciplina	80

7.2	ANEXO 2 – Código da aplicação de Criptografia com Chaves	83
7.3	ANEXO 3 – Questionário de Avaliação 1	87
7.4	ANEXO 4 - Questionário de Avaliação 2	88
7.5	ANEXO 5 - Questionário de Avaliação 3	89
7.6	ANEXO 6 - Questionário de Avaliação 4	90
7.7	ANEXO 7 - Questionário de Avaliação 5	91
7.8	ANEXO 8 - Relatório de Vulnerabilidades OpenVAS.....	92

1. INTRODUÇÃO

O escopo deste trabalho de conclusão de curso é a construção de um ambiente para a prática de laboratório na disciplina de segurança da informação e de redes.

1.1 Motivação

A principal motivação surge das experiências iniciais, desde 2004.1, de docentes da disciplina de segurança, no Curso de Graduação em Sistemas da Informação da UFSC. Uma disciplina de segurança computacional pode ser vista, pelo ensino da base teórica, quando se pode introduzir a base matemática que sustenta, por exemplo, o uso das técnicas de criptografia.

Entretanto, pelas características de um Curso de Graduação em Sistemas de Informação, em que a aplicação de métodos se sobrepõe ao embasamento teórico aprofundado, o processo ensino-aprendizagem para uma disciplina de segurança é revisto por este trabalho, no sentido de melhorar o ensino e a aprendizagem da disciplina de segurança INE 5680 – Segurança da Informação e de Redes.

Desde 2004.1, o Curso de Graduação em Sistemas da Informação da UFSC ofereceu a disciplina INE5630 – Segurança em Computação Distribuída, quando diversas turmas de alunos passaram pela disciplina, com os recursos que o LIICTC – Laboratório de Integração em Informática do Centro Tecnológico da UFSC, disponibilizava. Decorrente desta experiência, uma nova disciplina, INE 5680, começou a ser implantada a partir de 2012.1 (Anexo 1- Plano de Ensino), visando atualizar o nome e a ementa da disciplina, usada desde o projeto inicial do curso em

1999, seus objetivos e, principalmente, melhorar o processo ensino-aprendizagem da disciplina, no que tange a introdução de novos assuntos no programa de ensino da disciplina e a melhoria do ensino, quanto à parte prática.

Como uma característica da disciplina de segurança, em geral, a parte de segurança da informação tem seu ensino baseado na apresentação da criptografia clássica e suas técnicas consequentes, em que a proteção da informação é destacada, não se explorando ou estimulando as atividades de ataques sobre a informação. Relativamente à parte de segurança de redes, evita-se estimular a aprendizagem sobre ataques, optando por demonstrar, de maneira informativa, a defesa de computadores, segmentos de redes, ou a visão de um modelo de segurança em um ambiente cooperativo. Esta foi a orientação da disciplina desde 2004.2 a 2011.2.

A partir de 2012.1, a introdução de nova disciplina, INE 5680, motiva novos assuntos sobre segurança, tais como, ensinar a provar que um protocolo de segurança é seguro, explorar mais o lado da gestão de segurança da informação e explorar a utilização de algumas ferramentas na linha do auto-monitoramento ou ataques numa rede.

Dentro do novo escopo da disciplina INE5680, um novo ambiente computacional é necessário, para um novo processo ensino-aprendizagem mais cooperativo-colaborativo e aberto, em que a parte prática da disciplina possa ser estimulada e explorada. Neste sentido, este trabalho de conclusão de curso se coloca, numa primeira tentativa de melhorar o ensino e a aprendizagem da disciplina de segurança da informação e de redes.

Este trabalho de conclusão de curso representa uma oportunidade de repensar o processo ensino-aprendizagem de uma forma geral, que pode ser utilizado não somente num escopo de ensino de segurança, mas também no ensino de outras disciplinas.

1.2 Objetivo Geral

Reestruturar o ensino de segurança da informação e de redes, no Curso de Graduação de Sistemas da Informação do INE-UFSC, no que tange ao ensino da disciplina em laboratório.

1.3 Objetivos Específicos

Os objetivos específicos que podem ser citados são:

- a) Definição dos aspectos didáticos para o ensino de segurança;
- b) Criação de um ambiente computacional propício para o ensino da disciplina de Segurança da informação e de Redes;
- c) Especificação dos conteúdos das aulas práticas aplicadas.

1.4 Organização do Trabalho

Este trabalho está estruturado da seguinte forma: no Capítulo 2 são apontados os alguns dos aspectos didáticos definidos pelo professor para o ensino da disciplina em laboratório. No Capítulo 3 são descritas as formações e

configurações do ambiente computacional utilizado pela matéria. No Capítulo 4 é apresentado o conteúdo aplicado nas aulas práticas, bem como as ferramentas selecionadas, e suas aplicações. No, Capítulo 5, serão apresentadas a conclusão do trabalho e os trabalhos futuros.

2. ASPECTOS DIDÁTICOS PARA O ENSINO DA DISCIPLINA EM LABORATÓRIO

Este capítulo apresenta os aspectos didáticos definidos pelo professor para traçar os objetivos das aulas em laboratório da disciplina de segurança da informação e de redes.

2.1 Esquema de Plano de Aula

Os esquemas de aula deverão apresentar os seguintes itens:

- Aula de Número → Ordem da aula dentro do plano de ensino;
- Tempo de Aula → Tempo previsto para a aplicação e resolução do conteúdo ministrado na aula;
- Grupo → Imagina-se somente dois alunos por grupo, devido à disponibilidade de computadores.

2.2 Assunto

Descrição do que será abordado na aula prática em laboratório, e as ferramentas utilizadas.

2.3 Bibliografia Básica

Referências bibliográficas devem ser citadas, no sentido de acrescentar para o aluno alguns outros recursos sobre o assunto estudado.

2.4 Objetivos da Aula

Os objetivos da aula deverão complementar os domínios lecionados teoricamente à prática, relacionando-os e apontando as situações em que sua utilização é necessária.

2.5 Seleção do Conteúdo

A seleção do conteúdo das aulas deve ser feita, de acordo com os objetivos traçados. Aqui as aulas são organizadas do ponto de vista da prática de ensino em laboratório, onde o uso da máquina é primordial. O conteúdo é selecionado e organizado, de forma a orientando o aluno sobre os passos a serem seguidos no decorrer da prática do uso de ferramentas de segurança computacional.

2.6 Avaliação do Aprendizado

É proposto que o aluno realize uma auto-avaliação sobre o assunto praticado. Tal avaliação é materializada através de um questionário colocado no roteiro da aula.

Outro formato de avaliação utilizado é a análise dos resultados obtidos em uma prática de aula, bem como os meios utilizados para alcançar estes.

O professor avaliará cada atividade e lançará no sistema Moodle as respectivas avaliações. A prática da atividade garantirá a frequência do aluno. Uma nota de avaliação da aprendizagem do assunto é dada como uma parte do total das tarefas previstas no plano de ensino da disciplina.

3. O AMBIENTE COMPUTACIONAL

O planejamento do ambiente computacional utilizado na disciplina considerou os hardwares disponíveis nos laboratórios LIICT (Laboratório Integrado de Informática do Centro Tecnológico - UFSC), e no DMC-NS (Distributed Mobile Computing and Network Security - UFSC), este último situado na sala 515 do INE. É de suma importância para a disciplina que os hardwares disponíveis suportem as ferramentas de segurança – softwares utilizados na gestão da segurança, e oferecer heterogeneidade de sistemas operacionais, que serão utilizadas pelos alunos nas aulas práticas.

3.1 Descrição dos Hardwares disponíveis

A tabela 1 demonstra os hardwares disponíveis para a disciplina.

Local	Modelo	Unidades	Descrição
Laboratório LIICT – CTC Sala 2	Desktops	17	Desktop HP Processador: AMD Phenom II X4; Memória RAM: 3Gb; Discos: 250Gb, SATA II.
Laboratório DMC – NS	Servidor	1	Servidor DELL, Poweredge 840 Processador: Intel Xeon X3220, 4 núcleos; 2.4GHz; Memória: 4Gb, DDR2 ECC; Discos: 2x 250Gb, SATA II - RAID 1

Tabela 1 – Descrição dos hardwares disponíveis para a disciplina

3.2 Funcionalidades dos Hardwares

Um dos objetivos deste trabalho é disponibilizar o ambiente computacional das aulas práticas da disciplina aos alunos fora do campus. Neste sentido, cada hardware foi configurado para atender a algumas funcionalidades, conforme a tabela 2.

Local	Modelo	Unidades	Funcionalidades
Laboratório LIICT – CTC Sala 2	Desktops	17	<ol style="list-style-type: none">1. Ambiente Computacional completo para resolução dos trabalhos práticos acessível remotamente.2. Disponibilizar na internet as ferramentas utilizadas na disciplina.3. Disponibilizar na internet as imagens das máquinas virtuais, possibilitando aos alunos.
Laboratório DMC – NS	Servidor	1	<ol style="list-style-type: none">1. Ambiente Computacional completo para resolução dos trabalhos práticos, acessível apenas no laboratório.

Tabela 2 – Descrição das funcionalidades dos hardwares disponíveis para a disciplina

3.3 Preparação do Ambiente Computacional

Analisando os hardwares disponíveis para a disciplina, conforme descritos na tabela 2, observou-se que tinham a capacidade de executar as ferramentas de segurança utilizadas no decorrer do semestre, porém, estes softwares são compatíveis com diferentes sistemas operacionais, principalmente em

distribuições Linux e no Microsoft Windows. Como a disciplina utilizará programas compatíveis com ambos os sistemas operacionais, a solução encontrada foi a virtualização de, pelo menos, uma distribuição Linux e uma versão do Windows, bem como a inclusão dos programas necessários no decorrer da disciplina, nas máquinas virtuais.

Neste sentido, foi necessária, também, a virtualização do servidor do laboratório DMC-NS, pois este serviria de base para algumas ferramentas de descoberta de vulnerabilidades, além de hospedar dois Bancos de Dados que seriam disponibilizados para a utilização em algumas tarefas da disciplina.

Outro aspecto que influenciou a decisão de incluir a virtualização na disciplina foi a liberdade que poderia ser dispensada ao aluno, pois disponibiliza-se um ambiente para testes de segurança em redes em um ambiente virtual isolado da rede da UFSC, sem as barreiras de acesso impostas na rede, e sem a preocupação de deixar os computadores dos laboratórios vulneráveis, ou com configuração não correta.

A virtualização, que devido à importância será mais explanada na seção seguinte, possibilitou à disciplina utilizar ferramentas de segurança executadas em ambientes heterogêneos, e simplificar a recuperação de um ambiente danificado, pois basta importar o arquivo imagem do ambiente virtual no software de virtualização, para que este retorne ao estado inicial, ou do seu último backup.

3.3.1 A Virtualização

A virtualização de servidores tem como origem dos seus conceitos às descobertas e pesquisas da IBM e do MIT na década de 60, quando desenvolveu o projeto M44/44X. A partir deste, a IBM desenvolveu vários outros sistemas comerciais compatíveis com a virtualização, dentre eles o OS/370, famoso em sua época (JUNIOR, 2008).

A intenção da IBM era de fornecer um ambiente único e completo para cada usuário, cada um com o seu próprio sistema operacional e aplicações, totalmente desvinculado dos ambientes dos outros usuários.

A virtualização foi perdendo a sua importância com a popularização do hardware do *PC*, na década de 80, pois era mais barato, simples e versátil fornecer um computador completo a cada usuário, que investir em sistemas de grande porte, caros e complexos. Além disso, o hardware do *PC* não tinha o desempenho necessário para dar suporte à virtualização, o que impediu o uso de ambientes virtuais nestas plataformas (JUNIOR, 2008).

A tecnologia de virtualização, nos moldes que se apresenta hoje, vem sendo preparada desde os anos 90, mas só agora, nos últimos cinco anos, que ganhou grande projeção no meio tecnológico. Neste cenário, pode-se destacar a empresa VMware, desenvolvedora do primeiro software de gerenciamento de hardware (hypervisor) para arquitetura x86 na década de 90, como a maior responsável pela popularização da virtualização de servidores (NANDA CHIUEH, 2005).

3.3.1.1 Conceito de Virtualização

A virtualização é, basicamente, a técnica que consiste em criar uma camada entre o hardware e a aplicação. Esta camada intermediária faz com que o ambiente de execução da aplicação seja substituído, transformando-o em um hardware virtual, ou uma máquina virtual.

Para complementar o entendimento sobre virtualização, seguem abaixo os conceitos de outros autores especialistas nesta área.

“A Virtualização é uma técnica que combina ou divide recursos computacionais para prover um ou mais ambientes operacionais de execução” (NANDA CHIUEH, 2005).

“A Virtualização consiste em estender ou substituir um recurso ou uma interface existente por outro de modo a imitar um comportamento. Isso é feito através de uma camada de software responsável por transformar ações de um sistema A em ações equivalentes em um sistema B (isomorfismo).” (CARISSIMI, 2009).

“Na Virtualização ocorre a multiplexação do hardware real, possibilitando assim a criação de diversas máquinas virtuais que podem ser consideradas uma cópia idêntica e isolada do hardware real.” (JUNIOR, 2008)

Dependendo onde essa transformação é feita, é possível classificar os softwares de virtualização em três grandes categorias:

1. **Nível de hardware:** Neste nível de virtualização, é apresentado, para as camadas superiores, um hardware abstrato similar ao original. Este era o

tipo da definição original de máquina virtual dos anos 60, onde máquina virtual é um conceito de sistemas operacionais.

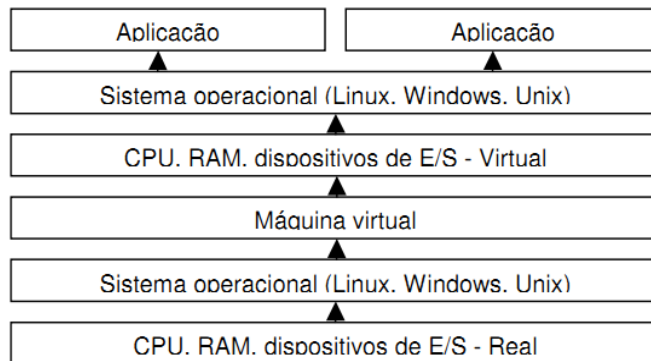


Figura 1. Virtualização nível de Hardware. Fonte: Laureano (2006)

2. **Nível de sistema operacional:** Permite a criação de partições lógicas de maneira que cada partição seja vista como uma máquina isolada, mas que compartilham o mesmo sistema operacional. A camada de virtualização, neste caso, se insere entre o sistema operacional e das aplicações. Desta forma, um software em execução em uma máquina virtual não pode visualizar ou afetar outra máquina virtual execução.

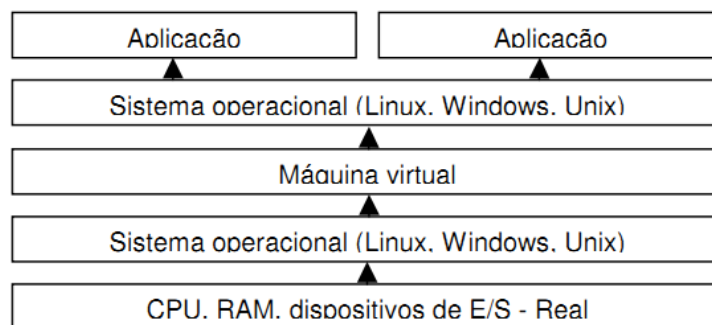


Figura 2. Virtualização nível de Sistema Operacional. Fonte: Laureano (2006)

3. **Nível de linguagens de programação:** a camada de virtualização é um programa de aplicação do sistema operacional. O objetivo é definir uma

máquina abstrata sobre a qual executa uma aplicação desenvolvida em uma linguagem de programação de alto nível específica, como o JAVA.

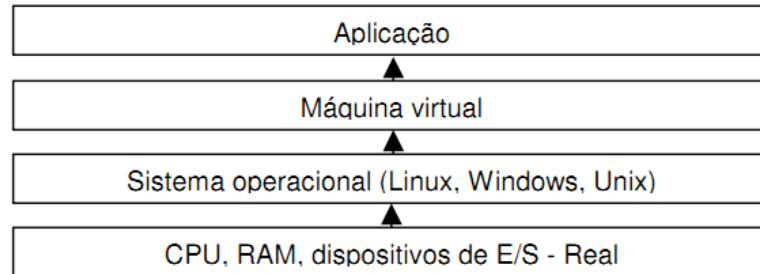


Figura 3. Virtualização nível de Sistema Operacional. Fonte: Laureano (2006)

3.3.1.2 Máquina Virtual e Hypervisor

Máquina Virtual (Virtual Machine – VM) refere-se a uma instância de um hardware virtualizado e um sistema operacional também virtualizado. Pode ser definida, também, como a abstração de uma máquina física real em um software.

“Esta abstração possibilita a divisão de uma única plataforma física de hardware em duas ou mais plataformas virtuais, tendo cada plataforma virtual os seus próprios recursos e dando aos usuários a ilusão de estarem acessando diretamente a máquina física” (JUNIOR, 2008).

“Pode-se dizer que máquina virtual é uma duplicata eficiente e isolada de uma máquina real” (LAUREANO, 2006).

Uma VM pode executar qualquer tipo de software como um servidor, um cliente ou um desktop; podem ser chamadas também de computador virtual, hóspede, convidado e outros. Os recursos das máquinas virtuais (memória,

processador) em execução em determinado computador são virtualizados, dividindo os recursos desse computador em vários ambientes de execução.

Um dos principais conceitos envolvidos no estudo de máquinas virtuais é o Monitor, também conhecido como hypervisor, VMM (*Virtual Machine Monitor*), ou Monitor de Máquina Virtual. Ele é uma camada de software intermediária, inserida entre o sistema visitante e o hardware onde o sistema visitante executa. Essa camada faz uma interface entre os possíveis sistemas visitantes (virtuais, também chamados de *Guest*) e o hardware real que é compartilhado por eles (também chamado de *host*).

“O VMM é o centro da virtualização de servidores, que gera recursos arbitrários de hardware e os múltiplos pedidos dos hóspedes dos sistemas operacionais e das aplicações” (WILLIAMS & GARCIA, 2007).

O *hypervisor* é o responsável por gerenciar todas as estruturas de hardware, como MMU (*Memory Managment Unit*), dispositivos de E/S, controladores DMA, criando o ambiente necessário para uma máquina virtual, oferecendo condições para que os sistemas visitantes possam ser executados.

3.3.1.3 Tipos de Virtualização

I- Emulação de hardware

A Emulação de hardware simula o comportamento de um hardware específico (conjunto de instruções, estado do processador, memórias, ciclos de clock), diferente do hardware real, conforme demonstra a figura 4. Este tipo de

virtualização é utilizado por desenvolvedores de firmware e de hardware, pois podem validar soluções sem a necessidade do hardware real (LAUREANO, 2006)



Figura 4. Emulação de Hardware.

II- Virtualização Completa

A virtualização completa é técnica que realiza uma simulação completa do hardware, de modo que qualquer sistema operacional possa ser executado. Na virtualização completa, toda uma infraestrutura do hardware é virtualizada, assim não há necessidade de modificar o sistema operacional convidado para executar sobre a VM. Como todas as instruções devem ser interpretadas pelo hypervisor, há um comprometimento parcial do desempenho.

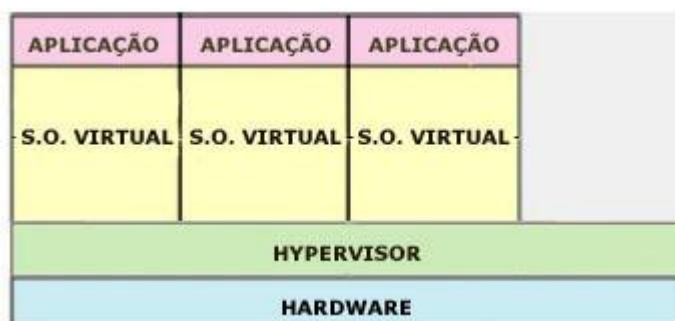


Figura 5. Virtualização Completa.

III- Para-virtualização

Para-virtualização é a técnica que permite que o sistema convidado (*Guest*) acesse diretamente recursos do hardware, com restrições, que são administradas pelo monitor de máquinas virtuais. Nesta técnica há uma otimização do desempenho, já que algumas instruções são passadas diretamente ao hardware real.

A principal limitação da para-virtualização é a necessidade de que o sistema operacional convidado seja previamente adaptado para executar no *hypervisor* de um software de virtualização.

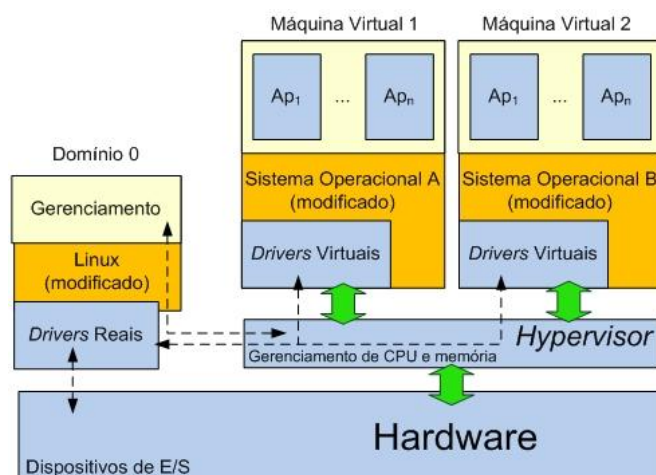


Figura 6. Para-virtualização.

3.3.1.4 Vantagens da Virtualização

O processo de virtualização oferece as seguintes vantagens:

- ✓ Simplificação e flexibilização da Infraestrutura de hardware;
- ✓ Permite a utilização de diferentes sistemas operacionais em único hardware;

- ✓ Capacidade do hardware é alocada dinamicamente, facilitando a recuperação por falhas;
- ✓ Migração de sistemas operacionais e aplicações para outro hardware;
- ✓ Melhor aproveitamento do hardware adquirido;
- ✓ Compatibilidade com sistemas legados;
- ✓ Menor consumo de energia – TI Verde.

3.3.1.5 Características da Virtualização

Algumas características importantes devem ser consideradas como princípios da tecnologia de virtualização:

- a) Particionamento: é a capacidade de partilhar o hardware físico, geralmente executado pelo hypervisor;
- b) Isolamento: Um processo de máquina virtual não pode interferir em outra máquina virtual, nem no hypervisor;
- c) Encapsulamento: Na virtualização, uma máquina virtual é implementada na forma de arquivo, ou conjunto de arquivos, onde constam o hardware virtual, o sistema operacional e as aplicações instaladas. Desta forma, a máquina virtual pode ser movida entre máquinas físicas com dispositivos de armazenamento diferentes (CD, DVD, discos removíveis entre outros). Essa propriedade é uma das responsáveis pela implementação de soluções de recuperação de falhas e continuidade de negócios;
- d) Desempenho: como há uma camada extra de software, deve haver um pequeno comprometimento no desempenho de um Sistema Operacional,

porém este é compensado pelos benefícios adquiridos com o uso da virtualização;

- e) Gerenciabilidade: capacidade de gerenciar uma máquina virtual independente das outras;
- f) Compatibilidade de software: todos os softwares escritos para executar em uma determinada plataforma devem ser capazes de rodar em uma máquina virtual que se propõe a virtualizar esta plataforma;
- g) Eficiência: instruções que não comprometam o hospedeiro podem ser executadas diretamente no hardware;
- h) Inspeccionabilidade: o Monitor da máquina virtual deve ter acesso a todas as informações sobre os processos que estão rodando nas máquinas virtuais, além de ter o controle sobre os mesmos;
- i) Interposição: o *hypervisor* deve ser capaz de inserir instruções de operação de máquinas virtuais.

3.3.2 Avaliação dos Principais Softwares de Virtualização

3.3.2.1 VMware

Os aplicativos de virtualização oferecidos pela empresa VMware Inc. são, provavelmente, os mais conhecidos atualmente. A empresa, pioneira na solução de virtualização para a arquitetura x86, trabalha com a virtualização completa. A VMware, que desenvolve os softwares de mesmo nome, possui uma

vasta linha de ferramentas para virtualização; uma destas é sem custo de licenciamento - porém com limitações; e o restante, comercializáveis, com foco no setor empresarial.

Conforme já mencionado, a VMware trabalha com suítes de softwares com vários produtos, tendo como principais, na linha de virtualização, as famílias: *VMware vCenter* – para aplicações robustas/profissionais, e *VMware vSphere* - para uso doméstico.

O impedimento da utilização do VMWare neste trabalho se dá pelo fato das soluções oferecidas para uso não domésticos serem pagas.

3.3.2.2 Xen Server

O Xen é uma opção de software open-source para virtualização que utiliza o conceito de para-virtualização (seção 3.2.1.3), e tem como base o sistema operacional Linux. Esta ferramenta é focada em soluções para servidores.

As principais características do Xen são:

- Baixo custo na implementação (utiliza softwares open-source);
- Suporte para a tecnologia 64 bits;
- Possui código aberto, proporcionando maior integração com outras tecnologias;
- Possui alto rendimento devido à para-virtualização.

Embora seja uma ferramenta robusta e de bom desempenho, é limitada a ser executada em um sistema operacional Linux, o que, para este trabalho, não é aceitável.

3.3.2.3 Oracle VirtualBOX

VirtualBox é um software de virtualização desenvolvido pela *Sun Microsystems*, posteriormente comprada pela *Oracle*, que utiliza o conceito de virtualização total ou para-virtualização (seção 3.2.1.3). As principais características do *VirtualBox* são:

- Disponibilizado sobre licença GPL;
- Suporte para a tecnologia 64 bits.
- Disponível para os sistemas Linux, Windows, MAC e Solaris;
- Interface gráfica que facilita o gerenciamento das VMs;
- Definições de configuração de máquinas virtuais armazenadas em XML –
Facilita a transferência para outros computadores.

Devido às facilidades de migração e recuperação das máquinas virtuais, a interface gráfica de fácil utilização, ao suporte em diversos sistemas operacionais e por ser um software livre, esta é a ferramenta escolhida para ser utilizada na virtualização dos ambientes computacionais utilizados na disciplina.

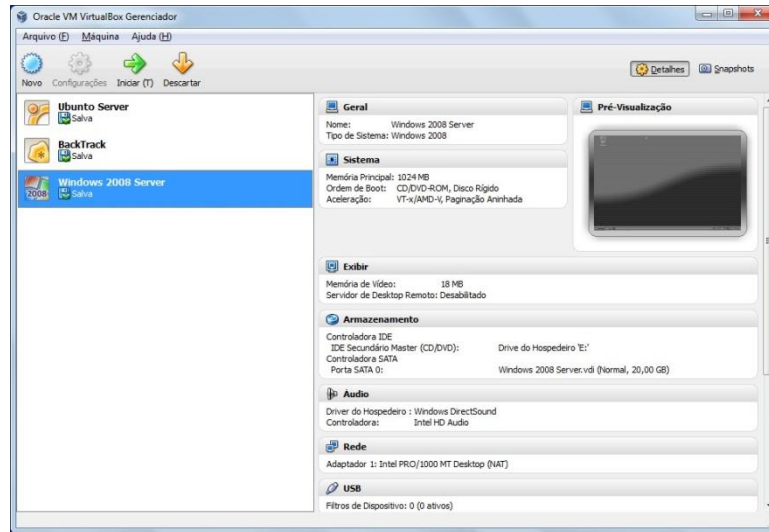


Figura 7. Software de Virtualização Oracle VirtualBox.

3.3.3 Configuração do Servidor

O papel do servidor na disciplina será de apoiar os alunos nos seguintes quesitos:

- Servir de fonte de pesquisa e testes, disponível pela Internet, aos alunos;
- Hospedar os bancos de dados *MySQL* e *SQLServer Express*, para serem utilizados nos trabalhos práticos;
- Disponibilizar os arquivos necessários para os exercícios e trabalhos da disciplina;
- Oferecer ao aluno vivência em sistemas operacionais.
- Oferecer aos alunos da disciplina os arquivos imagens das Máquinas Virtuais para download.

Conforme já mencionado nas seções anteriores, os requisitos apontam a necessidade de virtualizar o servidor, criando ambientes virtuais com sistemas operacionais diferentes, pois, além de algumas ferramentas só funcionarem em ambientes específicos, aproveitar-se-ia melhor o poder de processamento do hardware, já que outras aplicações poderiam ser acrescentadas no futuro, sem a necessidade de paralisação ou exclusão das já em execução.

Para o sistema operacional hospedeiro do servidor, decidiu-se pela instalação da distribuição Linux “*Ubuntu Server 11.10 x64*”. Baseada no *Debian*, esta distribuição tem se demonstrado bastante robusta e confiável. Sobre o SO foi instalado o pacote de interface GNOME - para simplificar algumas operações, e o software de virtualização *Oracle VirtualBOX 4*, pelos motivos já expostos na seção 3.2.2.3. Outras configurações importantes acrescentadas foram: Abertura do SSH para configurações remotas; e a configuração de duas interfaces de rede (uma com IP público, outra com IP interno);

No *VirtualBOX*, software escolhido para a prover a virtualização, foram criados três hardwares virtuais, criando as VMS conforme a tabela 3:

Nome VM	Hardware Virtual	
Máquina Virtual Windows Server	Memória RAM	2 GB
	Disco Virtual	20 GB
Máquina Virtual Ubuntu Server	Memória RAM	512 GB

	Disco Virtual	15 GB
Máquina Virtual Backtrack	Memória RAM	512 GB
	Disco Virtual	8 GB

Tabela 3 – Hardwares virtuais criados no servidor

Os espaços em disco são alocados dinamicamente no hardware real, ou seja, os 20 GB destinados à Máquina Virtual Windows Server, por exemplo, só ocupará o espaço utilizado necessário no disco real, até chegar o limite de 20 Gb. Outro ponto a ser destacado do hardware virtual, é que o mesmo pode ser alterado quando inativo, por exemplo, aumentar ou diminuir o valor de memória RAM disponível.

O nome da máquina virtual, como padrão, já menciona qual será o Sistema Operacional utilizado nela. As características de cada uma, como softwares instalados, configurações e versões, serão mais detalhadas nas seções 3.3, 3.4, 3.5 e 3.6.

3.3.4 Configuração das Estações utilizadas pelos Alunos

As estações utilizadas pelos alunos são os computadores do laboratório do LIICT, sala 02, sendo estes controlados e configurados pelo responsável da rede do CTC (Centro Tecnológico da UFSC). Sendo assim, qualquer modificação no ambiente computacional das estações deveria ser previamente autorizada e liberada por senha pelo administrador da rede.

Após a argumentação das necessidades do ambiente para a disciplina com o administrador da rede do LIICT, obteve-se a autorização do administrador da rede do CTC para a instalação do software de virtualização *Oracle VirtualBOX* nas estações do laboratório, desta forma, bastaria importar as máquinas virtuais necessárias para que o aluno tivesse um ambiente amigoso e preparado para a disciplina.

As máquinas virtuais inseridas nas estações constam na tabela 4.

Nome VM	Hardware Virtual	
Máquina Virtual Windows Server 2008;	Memória RAM	1 GB
	Disco Virtual	20 GB
Máquina Virtual Ubuntu Server	Memória RAM	512 GB
	Disco Virtual	15 GB

Tabela 4 – Hardwares virtuais criados nas estações

Conforme já mencionado na seção anterior, os espaços em disco são alocados dinamicamente no hardware real, e o hardware virtual pode ser alterado quando inativo.

Estas duas VMs, são as mesmas instaladas no servidor, que, por uma praticidade da virtualização, basta importar alguns arquivos para por em operação um sistema operacional diferente. As características de cada uma serão mais detalhadas nas seções seguintes.

3.4 Máquina Virtual Windows 2008 Server

Nesta máquina virtual foi instalado o sistema operacional da Microsoft Windows Server 2008 Standard Edition, versão de 32 bits, oferecido pela Microsoft aos alunos e professores do Curso de Sistemas de Informação, através do convênio com a UFSC, sendo gratuito para fins de aprendizagem.

A configuração do SO ficou com os padrões básicos já estabelecidos pelo desenvolvedor na primeira instalação, apenas foram acrescentados os programas da tabela 5.

Programa	Licença	Finalidade
Microsoft SQL Server 2008 Express	Gratuito, para fins não comerciais	Utilização em trabalhos práticos.
Mozilla Thunderbird	Software Livre	Segurança de e-mails.
Gpg4Win	Software Livre	Para criar e gerenciar chaves.
OpenSSL for Windows	Software Livre	Software para implementação dos protocolos Secure Sockets Layer (SSL v2/v3) e Transport Layer Security (TLS v1)
OpenPGP	Software Livre	Software para criar e gerenciar chaves em cliente de e-mail
NMAP Win	Software Livre	Software para exploração e auditoria de segurança em redes.

Greenbone	Software Livre	Interface gráfica para o software OpenVAS-server, análise de vulnerabilidades.
OpenVPN 2.3	Software Livre	Software para utilização de VPN, tanto cliente quanto Servidor.

Tabela 5 – Softwares instalados na Máquina Virtual Windows 2008 Server

Para o acesso foram criados três usuários: Administrador, Diogo (Pessoal) e de Aluno; todos com perfil de administrador, já que um dos princípios é dar liberdade ao aluno sobre a configuração da máquina local.

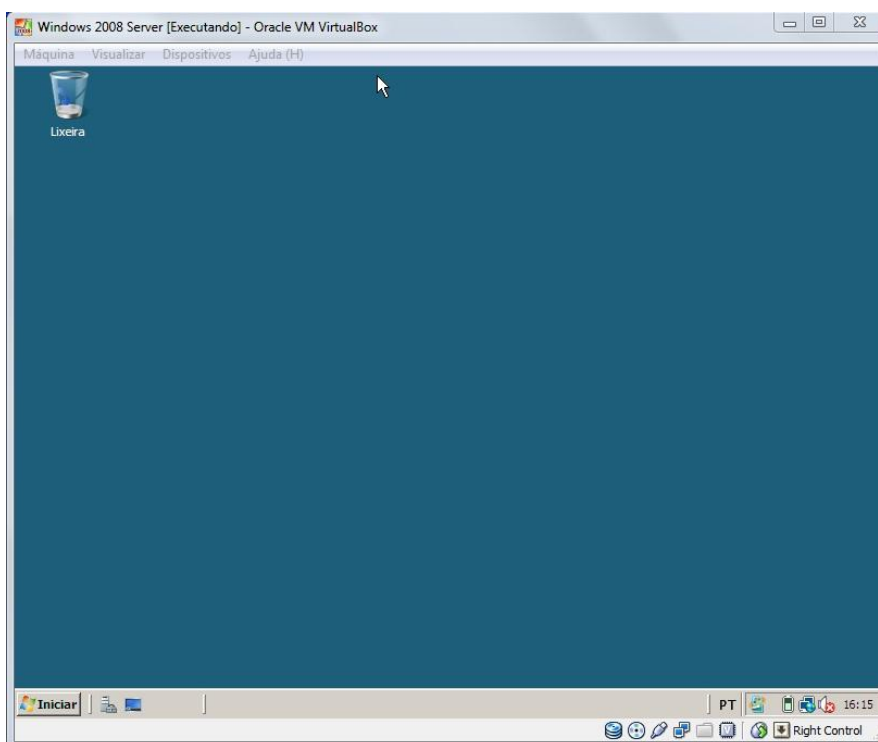


Figura 8. Imagem da tela da Máquina Virtual Windows 2008 Server.

3.5 Máquina Virtual Ubuntu Server

Nesta máquina virtual foi instalado o sistema operacional da distribuição Linux Ubuntu Server 11.10, versão de 32 bits, oferecido gratuitamente através do site <http://www.ubuntu-br.org/>.

A configuração do SO ficou com os padrões básicos já estabelecidos pelo desenvolvedor, sendo estes reconfigurados ao longo das tarefas práticas, incluindo apenas os pacotes Samba, para compatibilidade em redes Microsoft, e o de interface GNOME, para interface gráfica do ambiente. Os programas instalados para uso na disciplina constam na tabela 6.

Programa	Licença	Finalidade
MySQL	Software Livre	Utilização em trabalhos práticos.
GnuPG	Software Livre	Para criar e gerenciar chaves.
Mozilla Thunderbird	Software Livre	Trabalho de segurança de e-mails.
OpenSSL	Software Livre	Segurança em Aplicação WEB.
OpenVPN	Software Livre	Criação de Rede Virtual privada Segura.
Apache	Software Livre	Software de servidor WEB.
OpenSSL	Software Livre	Software para implementação dos protocolos Secure Sockets Layer (SSL v2/v3) e Transport Layer Security (TLS v1).

NMAP	Software Livre	Software para exploração e auditoria de segurança em redes.
OpenVAS	Software Livre	Software para exploração e auditoria de segurança em redes.

Tabela 6 – Softwares instalados na Máquina Virtual Ubuntu Server

Para o acesso foram criados três usuários: root (padrão), diogo (pessoal) e de Aluno; todos alocados no grupo de root, já que um dos princípios é dar liberdade ao aluno sobre a configuração da máquina local.

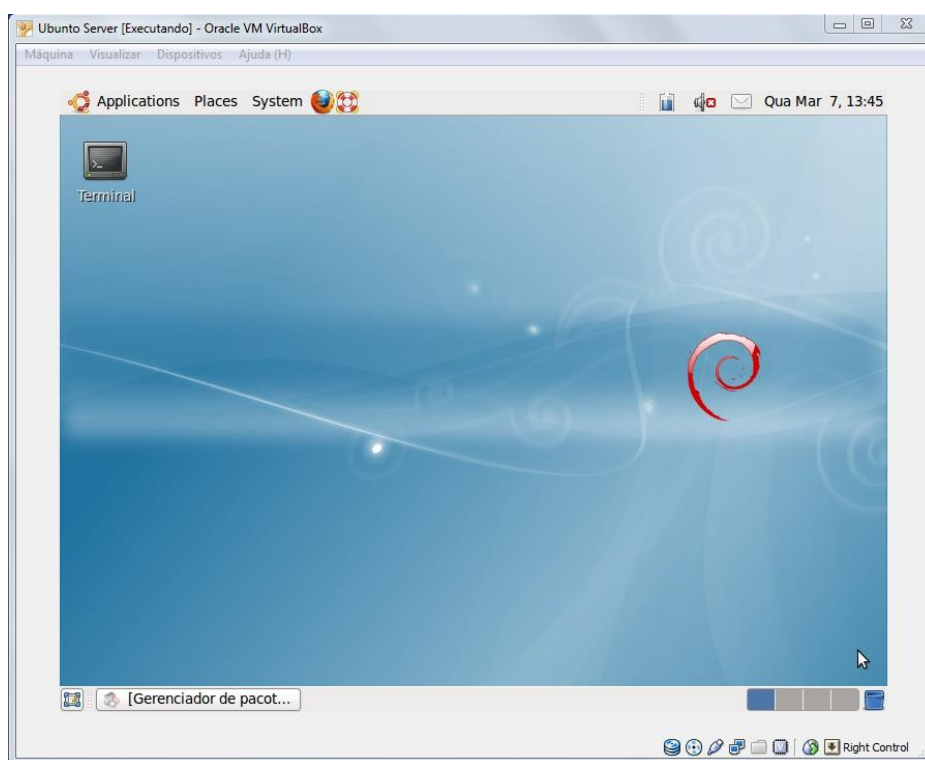


Figura 9. Imagem da tela da Máquina Virtual Ubuntu Server.

3.6 Máquina Virtual Backtrack

O objetivo desta VM é demonstrar aos alunos uma distribuição focada em testes de segurança e de penetração (*pen tests*). Muito utilizada por analistas de segurança, o sistema operacional instalado nesta Máquina Virtual, o Back Track 5, utiliza como base a distribuição Ubuntu, com a adição de ferramentas de segurança, com as funções de Coleta de Informações, Mapeamento de rede, busca de vulnerabilidades, Penetração em redes, Análise de redes móveis, etc.

O Back Track 5 é oferecido gratuitamente através do site <http://www.backtrack-linux.org/downloads/>.

A configuração do SO ficou com os padrões básicos já estabelecidos pelo desenvolvedor.

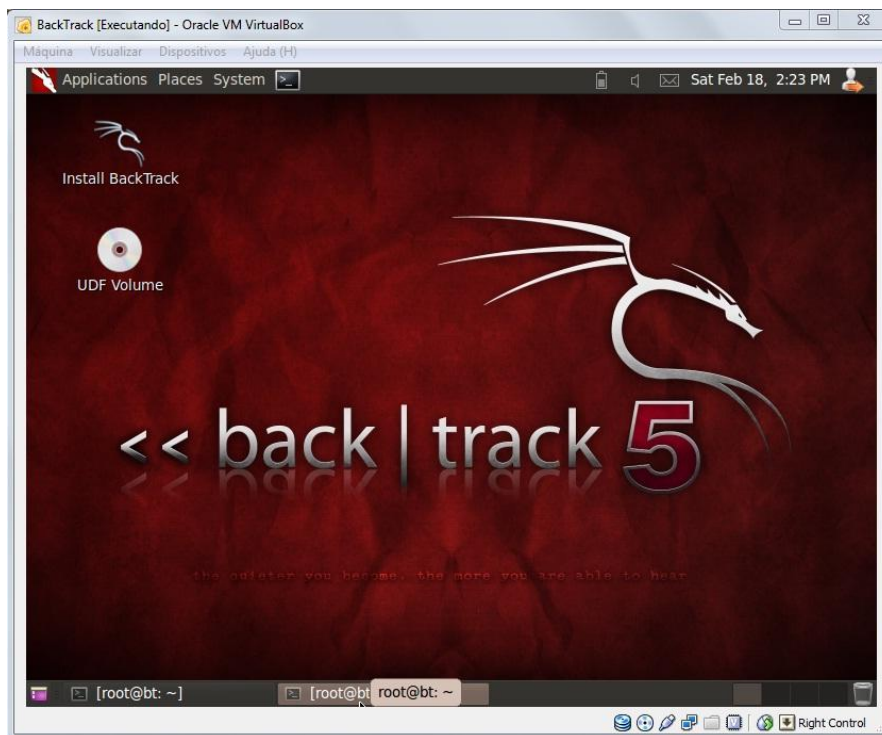


Figura 10. Imagem da tela da Máquina Virtual Back Track.

4. PLANOS DAS AULAS PRÁTICAS

Neste capítulo serão abordadas as aulas práticas - Assuntos, objetivos, seleção dos conteúdos – seguindo os aspectos didáticos definidos pelo professor, já explanados no capítulo 2.

4.1 Aplicação de Criptografia com Chaves Simétrica e Assimétrica

Aula Número: 1

Tempo de Aula: 4 horas-aula

Grupo: 2 Alunos

4.1.1 Assuntos

Criptografia de mensagens com o uso de chaves simétricas e assimétricas, utilizando as linguagens Java ou C#, aproveitando as bibliotecas de segurança disponibilizadas pela linguagem.

Criptografar e descriptografar mensagens com as chaves geradas.

4.1.2 Bibliografia Básica

- Aulas da disciplina, disponibilizadas em:

http://www.inf.ufsc.br/~zancanella/INE_5680/Slides_Aulas/Aula_002%20-%20Criptografia%20Simetrica.ppsx

- Biblioteca JAVAx Crypto, disponível em:
<http://docs.oracle.com/javase/6/docs/technotes/guides/security/crypto/CryptoSpec.html>;
- Biblioteca JAVA Security, disponível em:
<http://docs.oracle.com/javase/6/docs/technotes/guides/security/overview/jsoverview.html>

4.1.3 Objetivos da Aula

Aplicar o uso de criptografia, baseado em chaves simétricas e assimétricas, compreender as funcionalidades e a necessidade de utilização destas.

4.1.4 Seleção do Conteúdo

Uma solução genérica, consistida de um roteiro de aula, visando o uso de criptografia de mensagens com o uso de chaves simétricas e assimétricas, pode ser colocada como:

- Criar par de chaves utilizando as bibliotecas de segurança da linguagem;
- *Escolher um algoritmo para criptografar a mensagem com as chaves criadas;*
- Criptografar uma mensagem com o algoritmo escolhidos, utilizando as chaves geradas;
- Decifrar a mensagem utilizando as chaves geradas.

Para contemplar o conteúdo da aula prática, o aluno deverá seguir os passos, na ordem abaixo, inserindo os comandos no terminal:

1. Verificar nas Bibliotecas JAVA Security e Crypto, os métodos para tratarem a criptografia, descriptografia e geração de par de chaves;
2. Criar par de chaves com o seguinte algoritmo (Quadro 1):

```
private static final int RSAKEYSIZE = 1024; // fora do método  
KeyPairGenerator kpg = KeyPairGenerator.getInstance ("RSA");  
kpg.initialize(new RSAKeyGenParameterSpec(RSAKEYSIZE,  
RSAKeyGenParameterSpec.F4));  
KeyPair kpr=kpg.generateKeyPair ();  
PrivateKey chavePrivada=kpr.getPrivate();  
PublicKey chavePublica=kpr.getPublic();
```

Quadro 1: Algoritmo para criar par de chaves

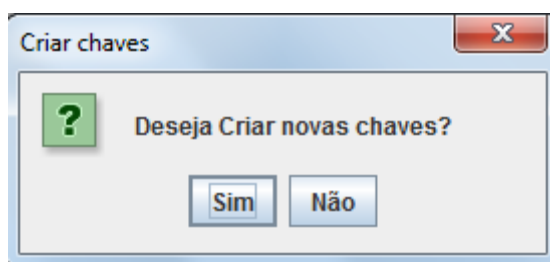


Figura 11. Criando par de chaves.

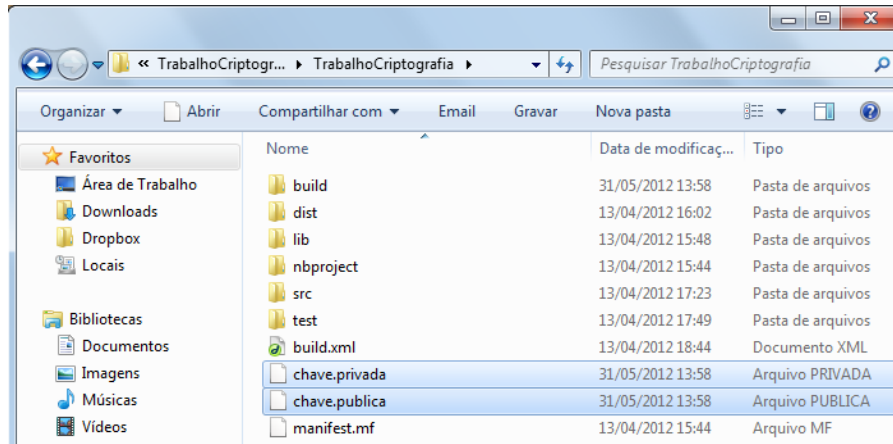


Figura 12. Chaves exportadas para arquivos.

3. *Escolher algoritmo para criptografar a mensagem com as chaves criadas;*
4. *Adicionar meio de inserção de mensagem a ser criptografada;*

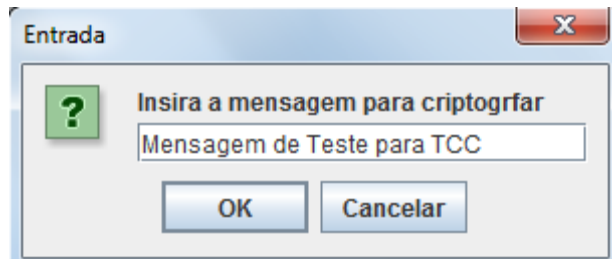


Figura 13. Interface para inserção de mensagem a ser criptografada.

5. *Utilizar o algoritmo escolhido para decifrar a mensagem utilizando o par de chaves;*

```

: Saída - TrabalhoCriptografia (run)
init:
Deleting: C:\Users\Diogo\Documents\FACULDADE\2012-1\Seguranca da Inf e rede\TrabalhoC
deps-jar:
Updating property file: C:\Users\Diogo\Documents\FACULDADE\2012-1\Seguranca da Inf e
compile:
run:
Mensagem criptografada:

0000 - c2 76 85 98 34 93 e4 6d e6 29 db 36 bc eb 3d 0a - .v..4..m..).6..=.
0010 - 06 2e d8 61 41 f4 d6 c2 8a 5e 46 94 da b9 64 ca - ...aA.....^F...d.

0000 - 34 f8 42 33 18 75 19 94 1f 76 58 4b 45 23 78 2b - 4.B3.u...vXKE#x+
0010 - 82 2d 5d 3a 36 19 22 04 89 1b 0a 40 6c 2b da aa - .-]:6."....@1+..
0020 - 39 99 76 23 24 b9 07 d6 96 11 0b 47 4e 06 e1 03 - 9.v#$......GN...
0030 - e3 95 4d cf 1a f1 02 99 d9 62 bb d2 43 89 b6 14 - ..M.....b..C...
0040 - 45 de 87 c8 b5 60 3b 69 64 4e 26 22 7f 39 f3 19 - E.....;idNs".9..
0050 - 64 72 ce c1 8b b6 a4 13 c5 90 9d 2d c1 fa 84 ee - dr.....-.....
0060 - 34 01 3e 5e fa 2e 3d eb 6d 75 6f 4c 7d 5b d0 ca - 4.>^...=..moL}[..
0070 - a2 f6 9e 32 c0 e6 b5 62 97 1c ca e0 cd fa ba f7 - ...2...b.....

A mensagem descriptografada é:

Mensagem de Teste para TCC
CONSTRUÍDO COM SUCESSO (tempo total: 1 minuto 5 segundos)

```

Figura 14. Saída da IDE Netbenas, após execução, demonstrado a mensagem criptografada e descriptografada utilizando o par de chaves gerado.

Para esta resolução, foi criado um programa genérico, utilizando a linguagem JAVA, porém outras soluções podem ser utilizadas, tanto na linguagem JAVA, quanto na C#. O código fonte consta no Anexo 2.

4.1.5 Avaliação do Aprendizado

O professor avaliará os códigos, a execução e os resultados gerados. Uma nota de avaliação é dada como um percentual do total das tarefas previstas no plano de ensino da disciplina.

4.2 Ensino de Segurança da Informação: Aplicação em E-mail

Aula Número: 2

Tempo de Aula: 2 horas-aula

Grupo: 2 Alunos

4.2.1 Assuntos

A prática para a segurança de e-mails. O tópico é estudado através do uso dos softwares GnuPG, OpenPGP e o cliente de e-mail Mozilla Thunderbird, ferramentas apropriadas, softwares livres que proporcionam a segurança de e-mails utilizando a criptografia de chave pública para assinaturas digitais e a criptografia de e-mails.

4.2.2 Bibliografia Básica

- Página do GnuPG, disponível em: <http://www.gnupg.org/>
- Página do OpenPGP, disponível em: <http://www.openpgp.org/>
- Página do Prof. João Eriberto Mota. Universidade Católica de Brasília (UCB), disponível em: <http://eriberto.pro.br/> .

4.2.3 Objetivos da Aula

Compreender como a segurança de e-mail pode ser obtida utilizando um cliente de e-mail, onde são instaladas as condições para aplicar os requisitos de segurança para autenticação de e-mails e confidencialidade de e-mails.

4.2.4 Seleção do Conteúdo

Um conteúdo mínimo, consistindo de um roteiro de aula, com o GnuPG, visando o objetivo acima, pode ser colocado como:

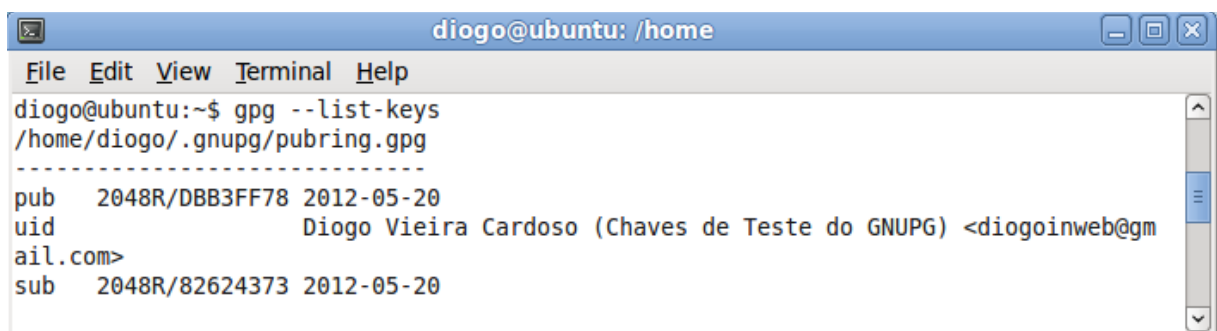
- A criação do chaveiro digital;
- Criação das chaves;
- Exportando e importando chaves localmente;
- Revogação de chaves;
- Servidores de chaves públicas na Internet;
- Relação de confiança;
- Assinatura de uma chave pública alheia;
- Execução da assinatura;
- Envio da chave assinada para o seu dono;
- Inserindo a chave assinada no chaveiro e no servidor público;
- Determinando a confiabilidade das chaves alheias;
- Listar os *fingerprints* em chaves;
- Assinando e criptografando arquivos;
- Uso do GnuPG, ou Open PGP, para assinar e criptografar mensagens de e-mail;

- Mozilla Thunderbird e o GnuPG;
- Registrar chaves públicas alheias em seu cliente de e-mail portando segurança;
- Obter um certificado de correio no sistema ICP-EDU-UFSC;
- Registrar a autoridade certificadora que gerou seu certificado, no seu cliente de e-mail;
- Utilizar o GnuPG para assinatura e criptografia de chave pública;
- Utilizar o GnuPG com o S/MIME, usando certificado obtido.

As ferramentas utilizadas neste tópico, já estão instaladas nas Máquinas Virtuais: Ubuntu Server e Windows Server 2008, cada qual com o software compatível, que constam no Servidor DMC-NS e nas estações da sala 02 do LIICT.

Para contemplar o conteúdo da aula prática, o aluno deverá seguir os passos, na ordem abaixo, inserindo os comandos no terminal:

1. `$ gpg --list-keys` → Criação do chaveiro digital;
2. `$ gpg --gen-key` → Criação das chaves;



```
diogo@ubuntu: /home
File Edit View Terminal Help
diogo@ubuntu:~$ gpg --list-keys
/home/diogo/.gnupg/pubring.gpg
-----
pub   2048R/DBB3FF78 2012-05-20
uid                               Diogo Vieira Cardoso (Chaves de Teste do GNUPG) <diogoinweb@gm
ail.com>
sub   2048R/82624373 2012-05-20
```

Figura 15. Chaves criadas pelo GnuPG.

3. `$ gpg -a --export <nº da chave> > arquivo.asc` → Exportar a chave pública como asc;

4. `$ gpg -a --export-secret-keys <nº da chave> > arquivo.key` → Exportar a chave privada;

5. `$ gpg --import <arquivo com a chave>` → Importar a chave para o chaveiro;

6. `$ gpg --gen-revoke <nº da chave> > <nº da chave>-revcert.asc`
→ Revogar uma chave;

7. Para encontrar servidores públicos de chaves, basta procurar em uma ferramenta de busca na internet, como o Google, por “pgp public servers”. Alguns exemplos disponíveis são: <http://pgp.mit.edu> ; <http://pgp.surfnet.nl> ; <http://pgp.uni-mainz.de> ;

8. `$ gpg --keyserver <subkeys.pgp.net> --send-key <nº da chave>`
→ Enviar a chave para um servidor público por intermédio de um comando (pode ser feito através de página na internet);

9. `$ gpg --sign-key <nº da chave>` → Assinar uma chave pública de outra pessoa (Relação de confiança);

10. `$ gpg --sign-key <nº da chave>` → Especificar a chave que realizará a assinatura, caso possua duas chaves;

11. `$ gpg --keyserver subkeys.pgp.net --recv-key <ID da chave a ser assinada>` → Buscar a chave pública a ser assinada;

12. `$ gpg --fingerprint <ID da chave a ser assinada>` → Conferir dados da chave que será assinada;
13. `$ gpg --sign-key <ID da chave a ser assinada>` → Assinar a chave;
14. `$ gpg -a --export <ID da chave assinada> nomeArquivo.asc` → Exportando a chave em formato ASCII;
15. `$ gpg --import <arquivo que contém a chave>` → importar chave assinada;
16. `$ gpg --keyserver subkeys.pgp.net --send-key <nº da chave>` → enviar a chave assinada para o servidor (Atualização da chave);
17. `$ gpg --fingerprint` → listar as impressões digitais de cada chave (*fingerprint*) – (Figura 16);

```

diogo@ubuntu: /home
File Edit View Terminal Help
7RDMh5IHJLKZgMRUnjkj3/6krVgEWT1nz7TWZ++6zVzdZhoFNA/7CTSpCAzCCTY
Z+//YrH8QNT4e8eGwM9VTXz0/kcVJP5fJsebJ4W5wH/uIpc76bRYyHU6DX0820g
bQChALDE+I6r6ym8GEqxxk0h3teuzcLsRsDh80TMDxpI+dk/Uoc4PV+sfQeSsuHp
SyYUnqmcj7JZIF6ANCDfD2fH9APRjd3Jy3kn0tvkUwknM/u1kteMKP8x9SdA7f
TJXSbGF3h9m10wWdL0AEQEAAYkHwQYAQIACQUCT7LCBgTbDAACRBvupm9Z7P/
eBCNCACRRhHqR7XbTyj4y0Q2uLBdeuInuc03HSIUng0dpy9RJMNSBqzWTRq890
o0802R+JZ3hQ/UdEg37I8EsWjUfYhaAmCvgWEE14UM7s1rWjnmqNMrre59aHTa0
OFQYGVc04meErWx19yALsLQbDwKT8/nRvPzH7MFrZDLUAJcmLubm9kHdA2+X8u6
W+6otZxkX9SAbmLHKg/2H1Ta7/kw8Rh+sH6RZycf6c08JCHOKKSizW771X1JA+/9
U0aULnnatrDW1y8nnbhEB/to35nt7/MydLVUNX0sQ/N+cbFLVDlsZqV3CJE0r1SD
C4vVtNU09QAD+Gk03CAHhQxBPuSs
=aQIK
-----END PGP PUBLIC KEY BLOCK-----
diogo@ubuntu: /home$ gpg --fingerprint
/home/diogo/.gnupg/pubring.gpg
-----
pub 2048R/DBB3FF78 2012-05-20
Impressão digital da chave: 293A 0F5D 2766 2688 4149 9697 6FBA 99BD DBB3 FF7
8
uid Diogo Vieira Cardoso (Chaves de Teste do GnuPG) <diogoinweb@gm
ail.com>
sub 2048R/82624373 2012-05-20
diogo@ubuntu: /home$

```

Figura 16. Impressão digital da Chave criada pelo GnuPG.

18. `$ gpg -a --sign <arquivo>` → Assinando e criptografando arquivos;

19. Uso do GnuPG, ou OpenPGP, para assinar e criptografar mensagens com cliente de e-mail Mozilla Thunderbird;

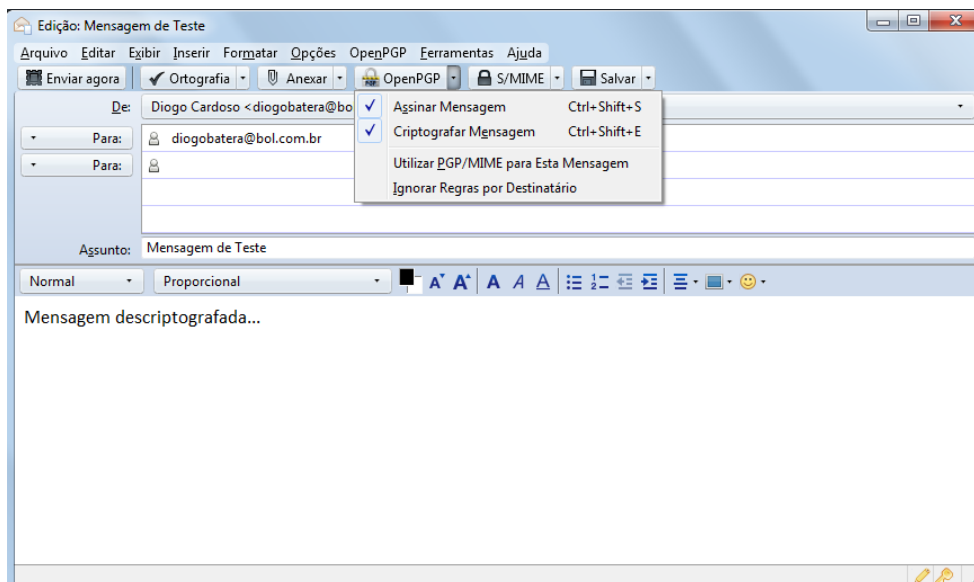


Figura 17. Demonstração de assinatura e criptografia de mensagens no software Mozilla Thunderbird.

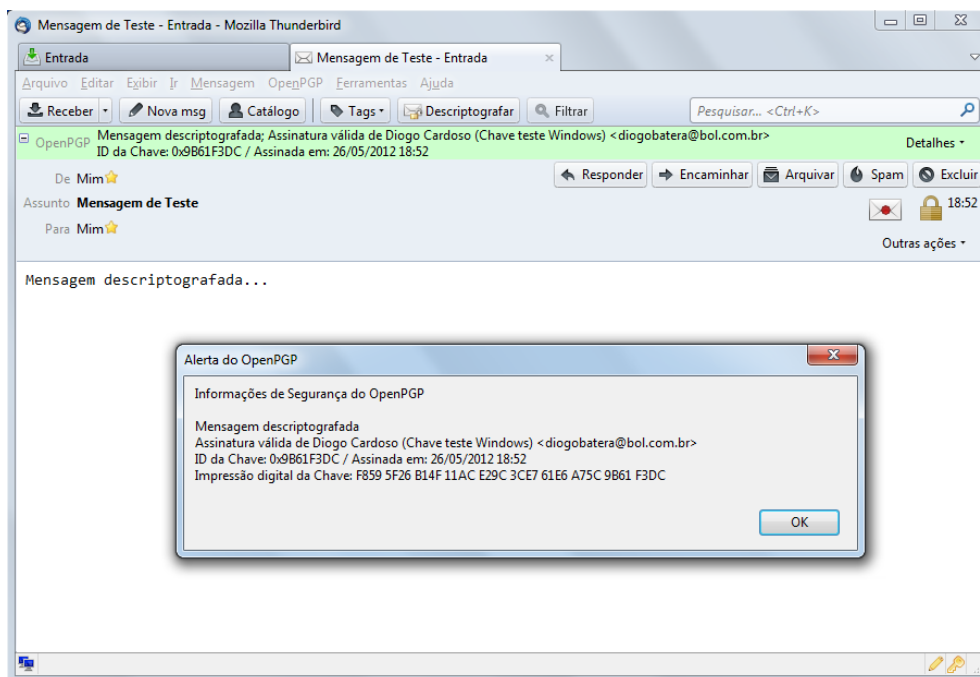


Figura 18. Envio de mensagem assinada e criptografada no software Mozilla Thunderbird.

20. Registrar chaves públicas alheias em seu cliente de e-mail portando segurança;

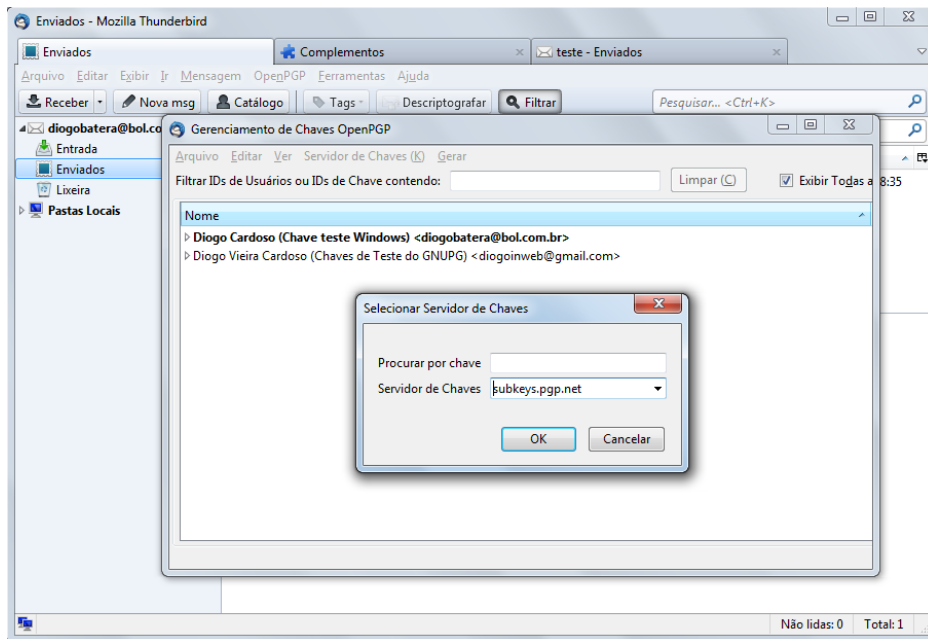


Figura 19. Registrando chaves públicas alheias com o cliente de e-mail Mozilla Thunderbird.

21. Obter um certificado de correio no sistema ICP-EDU-UFSC. – Acessar o endereço: <https://ac-correio.icpedu.ufsc.br>;

22. `$ gpg --sign-key <nº da chave>` → Utilizar o GnuPG para assinatura e criptografia da chave publica criada.

As resoluções apresentadas foram executadas no software GnuPG, instalado no Ubuntu Server 2008. Para o SO Windows Server, pode-se utilizar o GNU-PG for Windows, ou OpenPGP, conforme demonstram as figuras 17, 18 e 19, pois ambos possuem funções similares.

4.2.5 Avaliação do Aprendizado

O professor avaliará as atividades através de um questionário (anexo 3) que será postado no sistema Moodle. Uma nota de avaliação da aprendizagem do assunto é dada como um percentual do total das tarefas previstas no plano de ensino da disciplina.

4.3 Ensino de Segurança da Informação: Aplicação WEB

Aula Número: 3

Tempo de Aula: 2 horas-aula

Grupo: 2 Alunos

4.3.1 Assuntos

Configurar a segurança de um Servidor Web utilizando o software APACHE, com suporte para SSL. Trabalhar com a ferramenta OpenSSL; obter um certificado auto-assinado para servidor; instalar e testar o funcionamento.

4.3.2 Bibliografia Básica

- Página do Apache, disponível em: <http://www.apache.org/>
- Página do OpenSSL, disponível em: <http://www.openssl.org/>
- SANTOS, Leonel Filipe Simões, e JACINTO, Nuno Filipe Pedro. Artigo: Autenticação Web com certificados digitais, 2006, disponível em: http://www.inf.ufsc.br/~bosco/ensino/ine5630/material-cripto-seg/3_Autenticacao_Web_com_certificados_digitais.pdf

4.3.3 Objetivos da Aula

Aplicar o uso de segurança, baseado em certificados auto-assinados em um Servidor Web. Compreender a necessidade e situações que demandam a utilização de páginas seguras.

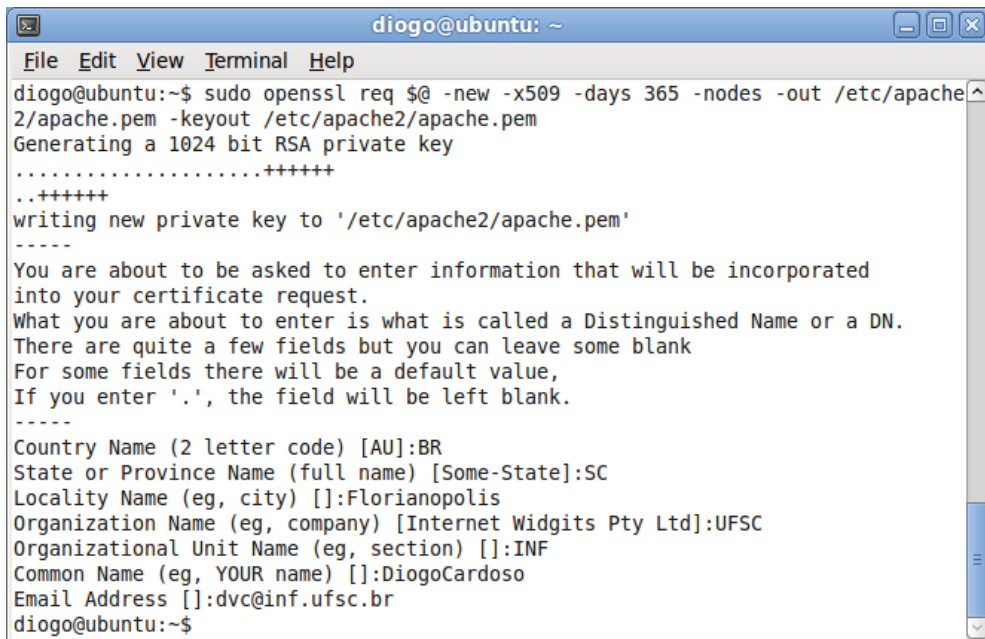
4.3.4 Seleção do Conteúdo

Um conteúdo mínimo, consistindo de um roteiro de aula, com o Apache2 e o OpenSSL, visando o objetivo da aula, pode ser colocada como:

- Criar o Certificado e habilitando-o no Apache para SSL;
- Habilitar o Apache para SSL;
- Testar em um navegador, acessando a página segura em "https://", e verificando o certificado.

Para contemplar o conteúdo da aula prática, o aluno deverá seguir os passos, na ordem abaixo:

1. `$ openssl req @$ -new -x509 -days 365 -nodes -out /etc/apache2/apache.pem -keyout /etc/apache2/apache.pem` → Criando o Certificado e habilitando-o no Apache para SSL



```
diogo@ubuntu:~$ sudo openssl req @$ -new -x509 -days 365 -nodes -out /etc/apache2/apache.pem -keyout /etc/apache2/apache.pem
Generating a 1024 bit RSA private key
.....+++++
..+++++
writing new private key to '/etc/apache2/apache.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:BR
State or Province Name (full name) [Some-State]:SC
Locality Name (eg, city) []:Florianopolis
Organization Name (eg, company) [Internet Widgits Pty Ltd]:UFSC
Organizational Unit Name (eg, section) []:INF
Common Name (eg, YOUR name) []:DiogoCardoso
Email Address []:dvc@inf.ufsc.br
diogo@ubuntu:~$
```

Figura 20. Exemplos de dados para criar o certificado no OpenVPN.

2. `$ chmod 600 /etc/apache2/apache.pem` → Modificar as permissões do arquivo:

3. `$ gedit /etc/apache2/ports.conf` → Modificar o arquivo `ports.conf` para habilitar o Apache para “escutar” a porta 443, conforme o quadro 2.

```
<IfModule mod_ssl.c>
    Listen 443
</IfModule>
```

Quadro 2: Modificação do ifModule no arquivo `ports.conf`

4. `$ a2enmod ssl` → Habilitar o Apache para SSL;

5. `$ gedit /etc/apache2/sites-available/default` – Modificar o arquivo *default* conforme o quadro 3:

```
<VirtualHost *:80>

    ServerAdmin webmaster@localhost

    DocumentRoot /var/www/

    <Directory />

        Options FollowSymLinks

        AllowOverride None

    </Directory>

    <Directory /var/www/>

        Options Indexes FollowSymLinks MultiViews

        AllowOverride None

        Order allow,deny

        allow from all

    </Directory>
</VirtualHost>

<VirtualHost *:443>

    DocumentRoot /var/www-ssl/

    <Directory />

        Options FollowSymLinks

        AllowOverride None

    </Directory>

    <Directory /var/www-ssl/>

        Options Indexes FollowSymLinks MultiViews

        AllowOverride None

        Order allow,deny

        allow from all

    </Directory>

    ErrorLog /var/log/apache2/error.log
```

```
CustomLog /var/log/apache2/access.log combined
SSLEngine on
SSLEngine on
ServerSignature on
SSLCertificateFile /etc/apache2/apache.pem
</VirtualHost>
```

Quadro 3: Modificação no arquivo default

- 6. \$ mkdir /var/www-ssl → Criar diretório para variáveis;
- 7. \$ /etc/init.d/apache2 restart → Reiniciar o Apache;
- 8. Testar em um navegador, inserindo “https://localhost” - para acesso do mesmo computador.

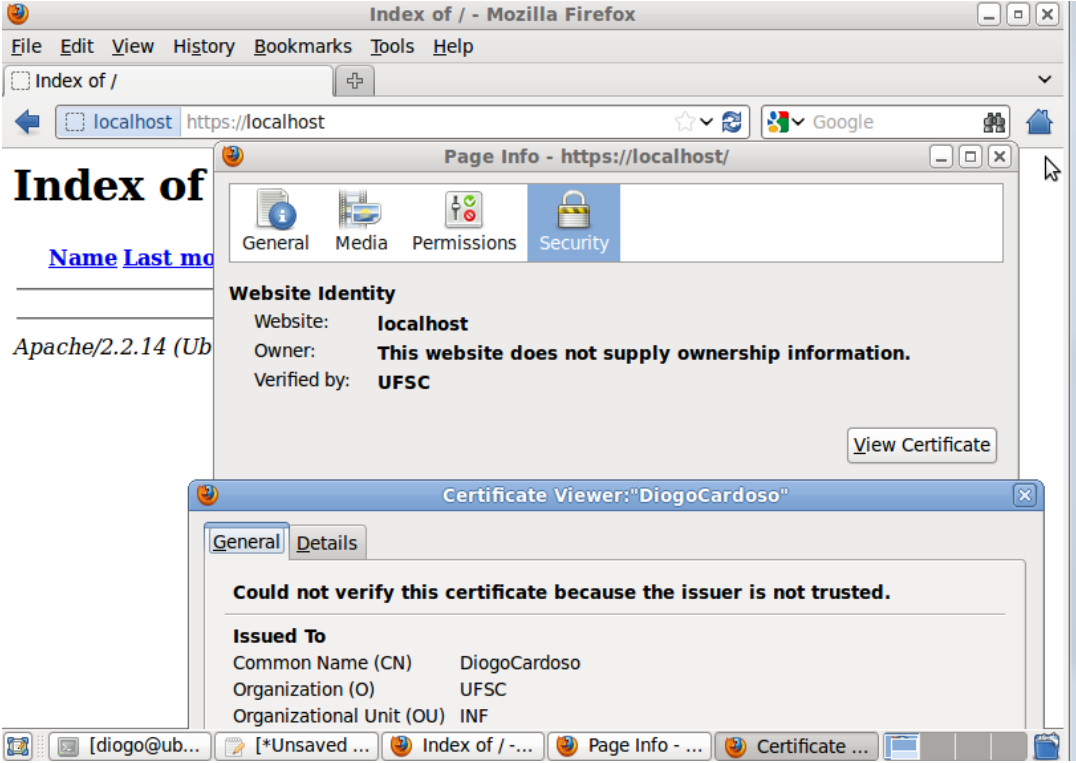


Figura 21. Navegador Mozilla Firefox demonstrando segurança com certificado em pagina https.

4.3.5 Avaliação do Aprendizado

O professor avaliará as atividades através de um questionário (anexo 4) que será postado no sistema Moodle. Uma nota de avaliação da aprendizagem do assunto é dada como um percentual do total das tarefas previstas no plano de ensino da disciplina.

4.4 Ensino de Redes Privadas Virtuais: Estabelecimento de uma VPN

Aula Número: 4

Tempo de Aula: 2 horas-aula

Grupo: 2 Alunos

4.4.1 Assuntos

Prática para se estudar como estabelecer uma VPN básica. O tópico é estudado através do uso do OpenVPN, uma ferramenta apropriada, um software livre que proporciona os meios necessários para estabelecimento de uma VPN, disponível em <http://openvpn.net/>.

A VPN estabelecida deve possuir todos os recursos de segurança para comunicação na Internet, tais como o uso de princípios de Diffie-Hellman, criptografia simétrica ou de chave pública e certificação digital.

4.4.2 Bibliografia Básica

Página do OpenVPN, disponível em: <http://openvpn.net/>;

Página do OpenSSL, disponível em: <http://openssl.org/>;

Página do Prof. João Bosco Sobral, disponível em:

<http://www.inf.ufsc.br/~bosco/ensino/ine5680/>;

4.4.3 Objetivos da Aula

Compreender como a segurança na comunicação de rede pode ser obtida, usando gateways VPNs instalados em ambientes de uma mesma organização, mas separados pela Internet.

Aplicar as condições para alcançar os requisitos de segurança de autenticação e confidencialidade na comunicação.

4.4.4 Seleção do Conteúdo

Um conteúdo mínimo, consistindo de um roteiro de aula, com o OpenVPN, visando o objetivo acima, pode ser colocado como:

- Base de construção de uma VPN.
- Criação de uma Autoridade Certificadora.
- Requisição e emissão de certificados digitais.
- Geração dos parâmetros Diffie-Hellman.
- Instalação e configuração da VPN.
- Execução e teste da VPN.

Para contemplar o conteúdo da aula prática, o aluno deverá seguir os passos, na ordem, inserindo os comandos no terminal:

I. Configuração da VPN na VM Ubuntu Server

1. `$ cd /etc/ssl` → Entrar no diretório etc/ssl

2. `$ vi openssl.cnf` → abrir o arquivo de configuração openssl.cnf e

localizar os parâmetros de [CA_defaults], e alterar as linhas conforme o quadro 4:

```
dir = /etc/ssl/certificados $ Where everything is kept
certificate = $dir/my-ca.crt $ The CA certificate
private_key = $dir/my-ca.key $ The private key
```

Quadro 4: Modificações no arquivo openssl.cnf

3. `$ mkdir certificados` → criar o diretório "certificados"

4. `$ cd certificados` → acessar o diretório certificados

5. `$ touch index.txt` → Criar arquivo de índices;

6. `$ echo '01' > serial` → Criar arquivo serial (pode-se usar o gedit e inserir "01" no arquivo);

7. `$ openssl req -nodes -new -x509 -days 365 -keyout my-ca.key -out my-ca.crt` → Gerar as chaves e certificados da CA - (preencher os dados requeridos, conforme modelo abaixo);

```

File Edit View Terminal Help
diogo@ubuntu:/etc/ssl/certificados$ sudo openssl req -nodes -new -x509 -days 365
-keyout my-ca.key -out my-ca.crt
Generating a 1024 bit RSA private key
.....++++++
.....++++++
writing new private key to 'my-ca.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:BR
State or Province Name (full name) [Some-State]:SC
Locality Name (eg, city) []:Florianopolis
Organization Name (eg, company) [Internet Widgits Pty Ltd]:UFSC
Organizational Unit Name (eg, section) []:INF
Common Name (eg, YOUR name) []:DiogoCardoso
Email Address []:dvc@inf.ufsc.br
diogo@ubuntu:/etc/ssl/certificados$

```

Figura 22. Modelo de dados para a geração de chaves no OpenVPN

8. `$ openssl dhparam -out dh.pem 1024` → Gerar os parâmetros de Diffie-Hellman:
9. `$ cd /etc/ssl/certificados` → Acessar o diretório de certificados;
10. `$ mkdir newcerts` → Criar um novo diretório para os certificados da VPN;
11. `$ openssl req -nodes -new -keyout vpn.key -out vpn.csr` → Criar um novo par de chaves, agora para o certificado da VPN. (Preencher os dados como anteriormente e deixar as senhas em branco)
12. `$ openssl ca -out vpn.crt -in vpn.csr` → Registrar na entidade certificadora do servidor. (Y,Y);
13. `$ cd /etc/openvpn` → Acessar o diretório do OpenVPN (/etc/openvpn)
14. `$ gedit vpn.conf` → Criar o arquivo de configuração da VPN, e inserir os dados do quadro 5.

```
dev tun
ifconfig 10.10.0.1 10.10.0.2
tls-server
dh /etc/ssl/certificados/dh.pem
ca /etc/ssl/certificados/my-ca.crt
cert /etc/ssl/certificados/newcerts/vpn.crt
key /etc/ssl/certificados/newcerts/vpn.key
port 5000
; user nobody
; group nobody
ping 15
verb 3
```

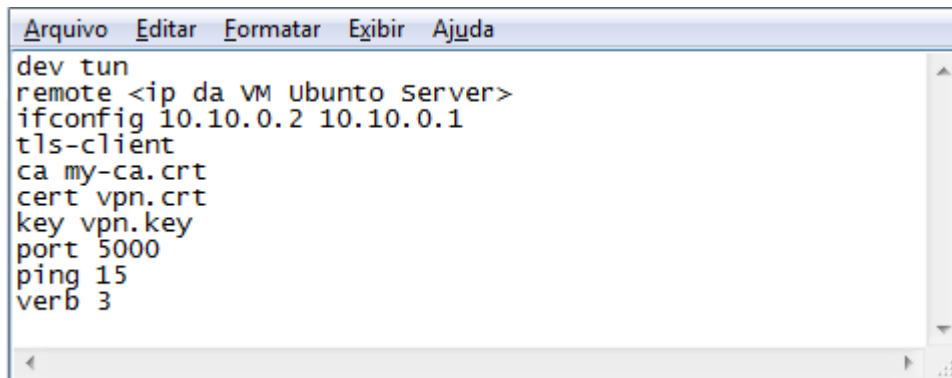
Quadro 5: Modificações no arquivo vpn.conf

15. \$ cd /etc/openvpn
16. \$ openvpn --config vpn.conf → Carregar arquivo de configuração da VPN;
17. \$ openvpn --daemon → Carregar o serviço do OpenVPN;
18. Configurar a placa de rede da VM para modo bridge;

II. Configuração do Cliente VPN na VM Windows Server 2008

19. Copiar os arquivos (my-ca.crt, my-ca.key, vpn.crt, vpn.key, h.pem), criados no diretório /etc/ssl da VM Ubuntu Server, para o diretório c:/arquivos de programas/OpenVPN/config/ na VM Windows Server 2008;

20. Criar, utilizando o notepad, o arquivo de configuração vpn.ovpn, com as configurações abaixo:



```
Arquivo  Editar  Formatar  Exibir  Ajuda
dev tun
remote <ip da VM Ubuntu Server>
ifconfig 10.10.0.2 10.10.0.1
tls-client
ca my-ca.crt
cert vpn.crt
key vpn.key
port 5000
ping 15
verb 3
```

Figura 23. Dados de configuração do arquivo vpn.ovpn

21. Configurar a placa de rede da VM para modo bridge;

22. Executar o OpenVPN-GUI e clicar em “connect” no menu do ícone instalado na bandeja do sistema.

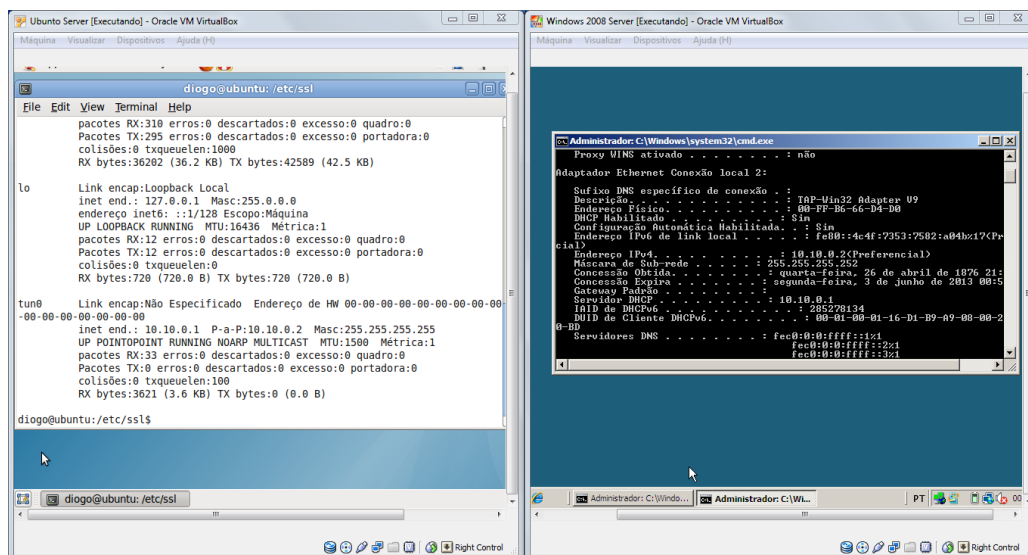


Figura 24. Demonstração da VPN funcionando entre as máquinas virtuais.

O OpenVPN já está instalado nas VMs do Servidor DMC-NS e nas Máquinas Virtuais das estações da sala 02 do LIICT, tanto na Máquina Virtual Ubuntu Server, quanto na Windows Server 2008.

4.4.5 Avaliação do Aprendizado

O professor avaliará as atividades através de um questionário (anexo 5) que será postado no sistema Moodle. Uma nota de avaliação da aprendizagem do assunto é dada como um percentual do total das tarefas previstas no plano de ensino da disciplina.

4.5 Análise de vulnerabilidades – NMAP e OpenVAS

Aula Número: 5

Tempo de Aula: 4 horas-aula

Grupo: 2 Alunos

4.5.1 Assuntos

A prática de “Técnicas de varredura de portas e serviços”. O tópico é estudado através do uso dos softwares NMAP e OpenVAS, ferramentas apropriadas para esta finalidade, softwares livres que apontam as vulnerabilidades de um computador na rede, ou da rede inteira.

4.5.2 Bibliografia Básica

MELO, Sandro. Exploração de Vulnerabilidades em Redes TCP/IP. Editora Alta Books.

Página web do NMAP, disponível em: <http://www.nmap.org>

Página web do OpenVAS, disponível em: <http://openvas.org/>

4.5.3 Objetivos da Aula

Analisar a segurança de uma rede, ou de um computador, utilizar as ferramentas NMAP, para exploração de redes e auditoria de segurança, e OpenVAS para busca de vulnerabilidades, identificar os pontos de vulneráveis, obter informações do *host*, e avaliar os aspectos de segurança dos resultados obtidos.

4.5.4 Seleção do Conteúdo

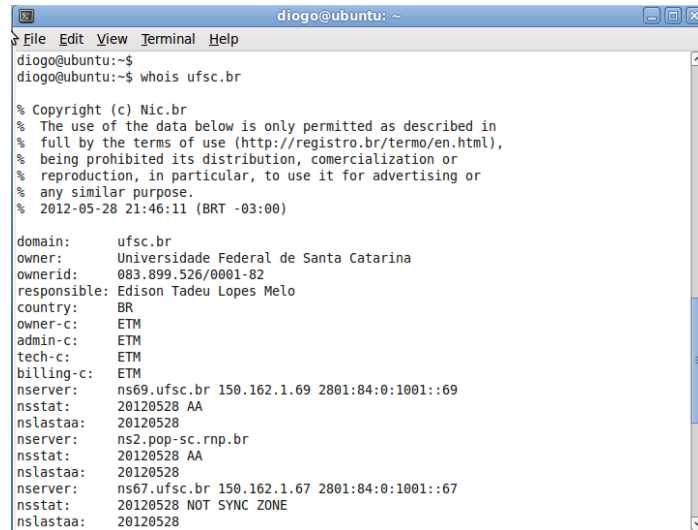
Um conteúdo mínimo, consistindo de um roteiro de aula, com as ferramentas NMAP e OpenVAS, visando os objetivos descritos na seção anterior, pode ser colocado como:

- Busca de informações sobre o domínio;
- Detectar portas abertas de um alvo;
- Detectar portas abertas de computadores de uma rede;
- Explorar vulnerabilidades de um alvo;
- Analisar relatório de vulnerabilidades.

Para contemplar o conteúdo da aula prática, o aluno deverá seguir os passos, na ordem, inserindo os comandos no terminal:

I. Aquisição de informação

1. \$ whois <domínio> → Busca de informações sobre o domínio - Base Whois;



```
diogo@ubuntu: ~  
File Edit View Terminal Help  
diogo@ubuntu:~$  
diogo@ubuntu:~$ whois ufsc.br  
  
% Copyright (c) Nic.br  
% The use of the data below is only permitted as described in  
% full by the terms of use (http://registro.br/termo/en.html),  
% being prohibited its distribution, comercialization or  
% reproduction, in particular, to use it for advertising or  
% any similar purpose.  
% 2012-05-28 21:46:11 (BRT -03:00)  
  
domain:      ufsc.br  
owner:       Universidade Federal de Santa Catarina  
ownerid:     083.899.526/0001-82  
responsible: Edison Tadeu Lopes Melo  
country:    BR  
owner-c:     ETM  
admin-c:    ETM  
tech-c:     ETM  
billing-c:  ETM  
nserver:    ns69.ufsc.br 150.162.1.69 2801:84:0:1001::69  
nsstat:     20120528 AA  
nslastaa:   20120528  
nserver:    ns2.pop-sc.rnp.br  
nsstat:     20120528 AA  
nslastaa:   20120528  
nserver:    ns67.ufsc.br 150.162.1.67 2801:84:0:1001::67  
nsstat:     20120528 NOT SYNC ZONE  
nslastaa:   20120528
```

Figura 25. Resultado do “Whois” para um domínio

2. `$ dig -t ns <domínio>` → Buscando informações sobre o servidor DNS:>

II. Explorando a rede com o escâner de portas NMAP

3. `$ nmap -sS <IP alvo> -p 1-100` → Detectar portas abertas de um alvo. A opção “-p” possibilita definir a faixa de portas a ser explorada. O parâmetro “-sS” - define varredura de portas connect () TCP completa enviando um único pacote SYN.

4. `$ nmap -sT <IP alvo> -p 1-100` → Detectar portas abertas de um alvo. A opção “-p” possibilita definir a faixa de portas a ser explorada. O parâmetro “-sT” define varredura de portas connect () TCP completa.

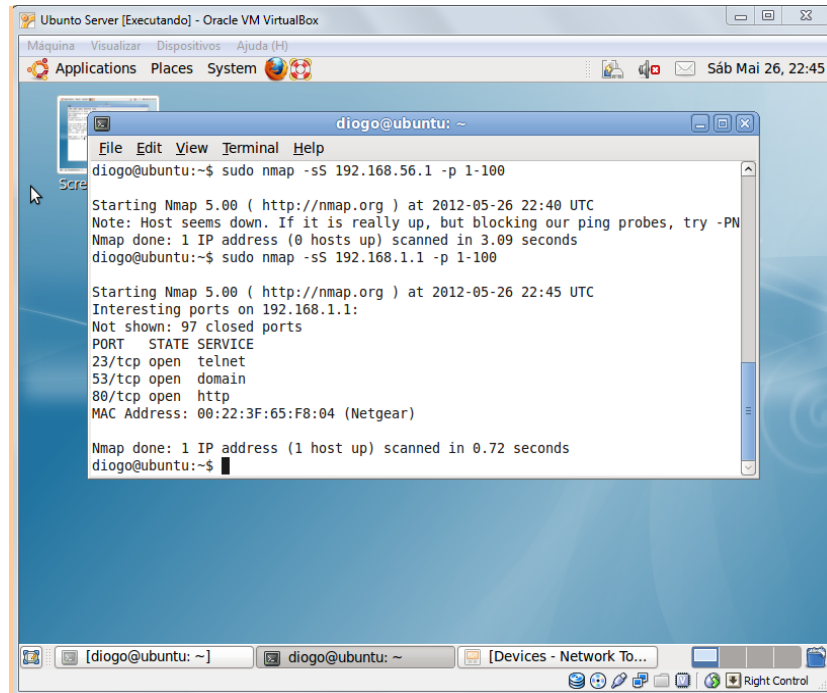


Figura 26 Resultado da pesquisa do NMAP

5. `$ nmap -sS <IP alvo> -O` → Com o parâmetro “-O” é feita uma tentativa de determinar o sistema operacional alvo.

6. `$ nmap -sS <Endereço de rede> -p 1-1000` → Varredura de um endereço de rede para determinar os serviços ativos e as portas abertas, em mais de um host, para identificar falhas de segurança em toda rede interna.

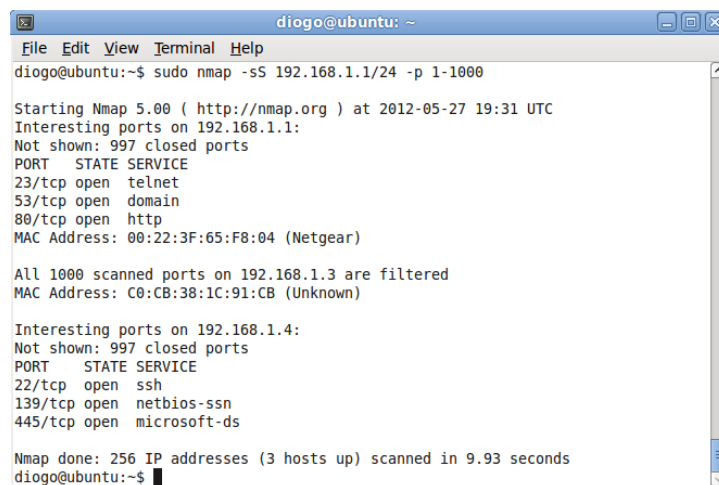


Figura 27. Resultado da pesquisa do NMAP

7. \$ nmap -sS <Endereço de rede> -p 1-1000 → Varredura de um endereço de rede para determinar os serviços ativos em mais de um host, para identificar falhas de segurança em toda rede interna.

III. Busca de Vulnerabilidades com OpenVAS

Utilizando o IP de um computador apontado pelo NMAP com alguma porta aberta, realizar os passos abaixo.

8. \$ /etc/init.d/openvasd start → Inicializar o *Openvas-server*
9. \$ /etc/init.d/openvas-client → inicializar o *Openvas-cliente*.
10. File->New. → Criar um novo projeto
11. File->Scan → *Assistent scan* para configurar um novo *scan*.
12. Preencher o nome do *scan*, escopo e alvo. Ex (*scan-teste, user-host, <IP alvo>*)
13. Inserir usuário e senha (Aluno, 123) → Iniciar escaneamento;

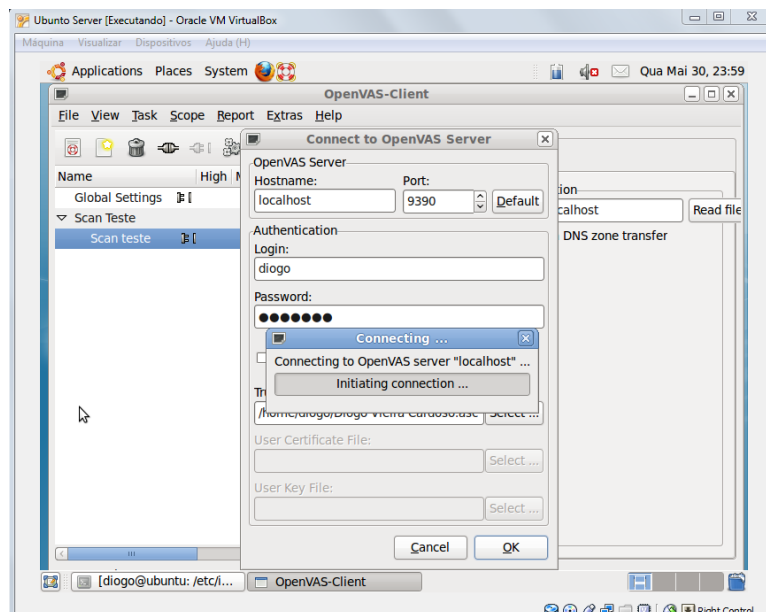


Figura 28. Conectando OpenVAS-client com o OpenVAS-server

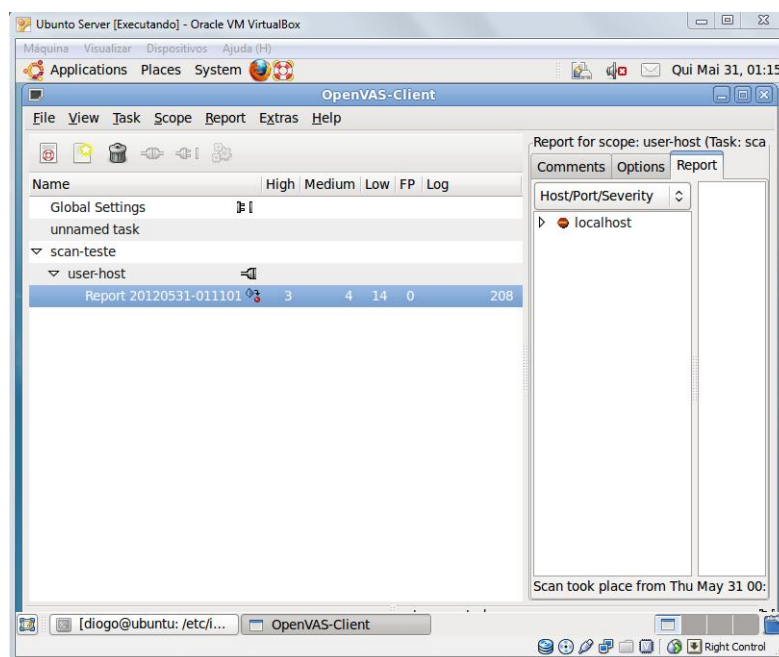


Figura 29. Resultado da pesquisa do OpenVAS

14. Report > Export → Exportar relatório produzido pelo OpenVAS e analisar os resultados (Anexo 8).

As resoluções apresentadas foram executadas no software NMAP e OpenVAS, instalados na VM Ubuntu Server 2008 e BlackTrack. Para a VM Windows Server, pode-se utilizar o NMAP Win; para o OpenVAS, é disponível a interface gráfica Greenbone, porém é necessário conectar a um OpenVAS Server, que só é disponível para Linux.

4.5.5 Avaliação do Aprendizado

O professor avaliará as atividades através de um questionário (anexo 6) que será postado no sistema Moodle. Uma nota de avaliação da aprendizagem do assunto é dada como um percentual do total das tarefas previstas no plano de ensino da disciplina.

4.6 Visão Geral de Defesas - Firewall

Aula Número: 6

Tempo de Aula: 2 horas-aula

Grupo: 2 Alunos

4.6.1 Assuntos

Esta tarefa aborda uma visão geral de defesas para a Máquina virtual Ubuntu Server, configurando algumas das funcionalidades do Firewall Iptables, nativo do Linux.

4.6.2 Bibliografia Básica

Página web do Prof. João Bosco Sobral, disponível em:
<http://www.inf.ufsc.br/~bosco/ensino/ine5630/>

Página web do Ubuntu Brasil, disponível em: <http://wiki.ubuntu-br.org/ConfigurandoFirewall>

4.6.3 Objetivos da Aula

Demonstrar como funciona um firewall, em especial o Iptables - Firewall nativo do Linux, criando uma configuração como técnica de defesa no servidor, visando diminuir os riscos de ataque. Bloquear e liberar conexões feitas com o servidor. Identificar pontos de vulneráveis, e avaliar os aspectos de segurança dos resultados obtidos.

4.6.4 Seleção do Conteúdo


Um conteúdo mínimo, consistindo de um roteiro de aula, com o Iptables, visando o objetivo da seção anterior, pode ser colocada como:

- Ativar firewall;
- Analisar as regras de acesso correntes;
- Liberar tráfego de protocolos e portas;
- Criar regras de acesso;
- Liberar log para o sistema de logs;
- Desativar o firewall.

Para contemplar o conteúdo da aula prática, o aluno deverá seguir os passos, na ordem abaixo, inserindo os comandos no terminal:

I. Habilitando e Configurando o Iptables

1. `$ iptables -L` → Listar as regras correntes no iptables;



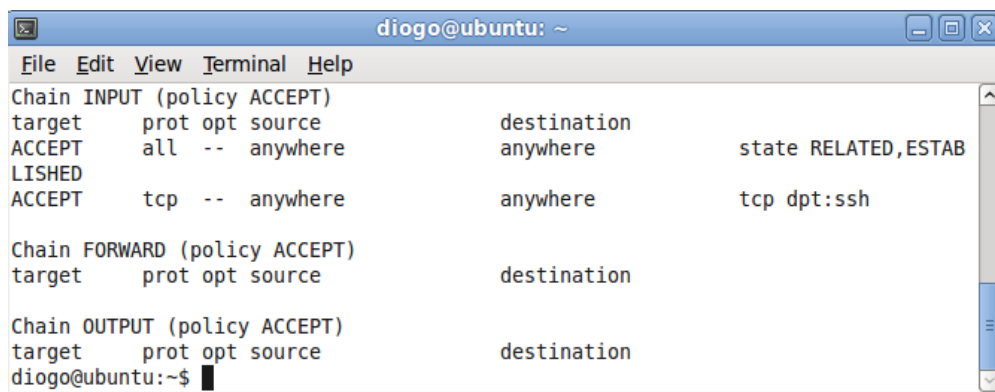
```
diogo@ubuntu: ~  
File Edit View Terminal Help  
diogo@ubuntu:~$ su diogo  
Senha:  
diogo@ubuntu:~$ sudo iptables -L  
[sudo] password for diogo:  
Chain INPUT (policy ACCEPT)  
target    prot opt source                destination  
  
Chain FORWARD (policy ACCEPT)  
target    prot opt source                destination  
  
Chain OUTPUT (policy ACCEPT)  
target    prot opt source                destination  
diogo@ubuntu:~$
```

Figura 30. Lista de acessos do Iptables

2. `$ iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT` → Permitindo sessões estabelecidas para receber tráfego;

3. `$ iptables -A INPUT -p tcp -i eth0 --dport ssh -j ACCEPT` → Permitir tráfego de entrada na porta 22 (tradicionalmente usada pelo SSH), você pode dizer ao iptables para permitir todo tráfego TCP na porta 22 do seu adaptador de rede;

4. `$ iptables -L` → Listar as regras correntes no iptables;

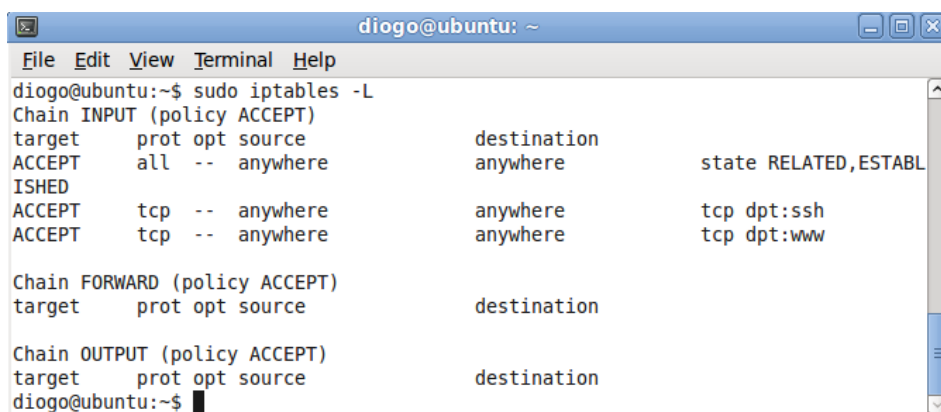


```
diogo@ubuntu: ~  
File Edit View Terminal Help  
Chain INPUT (policy ACCEPT)  
target    prot opt source                destination  
ACCEPT    all  --  anywhere              anywhere  
          state RELATED,ESTAB  
LISHED  
ACCEPT    tcp  --  anywhere              anywhere  
          tcp dpt:ssh  
  
Chain FORWARD (policy ACCEPT)  
target    prot opt source                destination  
  
Chain OUTPUT (policy ACCEPT)  
target    prot opt source                destination  
diogo@ubuntu:~$
```

Figura 31. Lista de acessos do Iptables

5. `$ iptables -A INPUT -p tcp -i eth0 --dport 80 -j ACCEPT` → Permitir todo o tráfego da web

6. `$ iptables -L` → Listar as regras correntes no iptables.

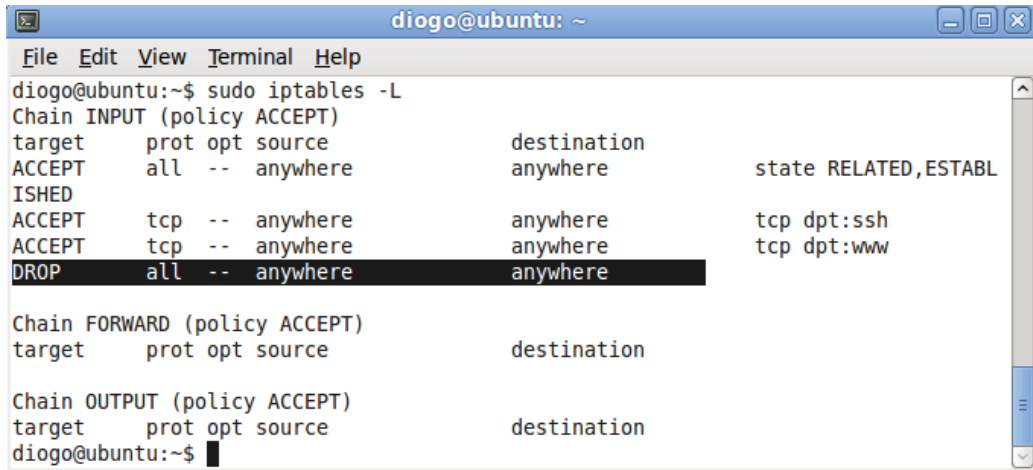


```
diogo@ubuntu: ~  
File Edit View Terminal Help  
diogo@ubuntu:~$ sudo iptables -L  
Chain INPUT (policy ACCEPT)  
target    prot opt source                destination  
ACCEPT    all  --  anywhere              anywhere  
          state RELATED,ESTABLISHED  
ACCEPT    tcp  --  anywhere              anywhere  
          tcp dpt:ssh  
ACCEPT    tcp  --  anywhere              anywhere  
          tcp dpt:www  
  
Chain FORWARD (policy ACCEPT)  
target    prot opt source                destination  
  
Chain OUTPUT (policy ACCEPT)  
target    prot opt source                destination  
diogo@ubuntu:~$
```

Figura 32. Lista de acessos do Iptables

7. `$ iptables -A INPUT -j DROP` → Colocar a regra para bloquear todo o tráfego no fim

8. `$ iptables -L`

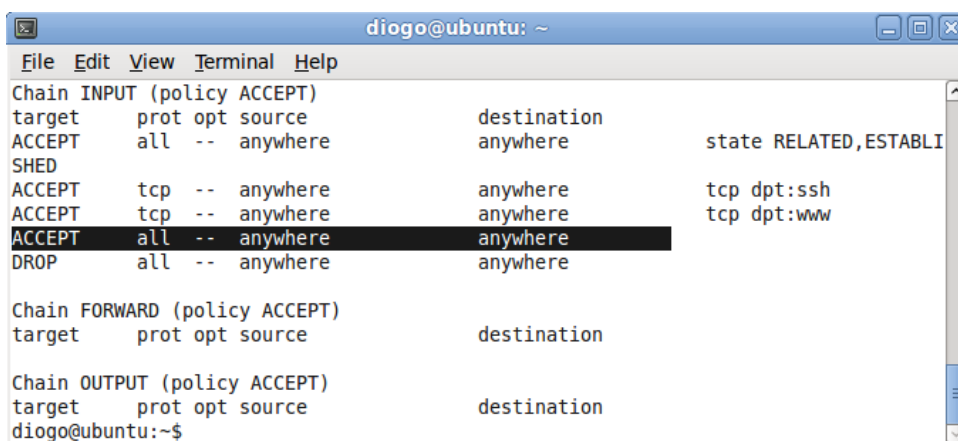


```
diogo@ubuntu: ~  
File Edit View Terminal Help  
diogo@ubuntu:~$ sudo iptables -L  
Chain INPUT (policy ACCEPT)  
target    prot opt source                destination  
ACCEPT    all  --  anywhere              anywhere        state RELATED,ESTABL  
ISHED  
ACCEPT    tcp  --  anywhere              anywhere        tcp dpt:ssh  
ACCEPT    tcp  --  anywhere              anywhere        tcp dpt:www  
DROP      all  --  anywhere              anywhere  
  
Chain FORWARD (policy ACCEPT)  
target    prot opt source                destination  
  
Chain OUTPUT (policy ACCEPT)  
target    prot opt source                destination  
diogo@ubuntu:~$
```

Figura 33. Lista de acessos do Iptables

9. `$ iptables -I INPUT 4 -i lo -j ACCEPT` → Adicionar a regra para o "loopback"

10. `$ iptables -L` → Listar as regras correntes no iptables.



```
diogo@ubuntu: ~  
File Edit View Terminal Help  
Chain INPUT (policy ACCEPT)  
target    prot opt source                destination  
ACCEPT    all  --  anywhere              anywhere        state RELATED,ESTABL  
ISHED  
ACCEPT    tcp  --  anywhere              anywhere        tcp dpt:ssh  
ACCEPT    tcp  --  anywhere              anywhere        tcp dpt:www  
ACCEPT    all  --  anywhere              anywhere  
DROP      all  --  anywhere              anywhere  
  
Chain FORWARD (policy ACCEPT)  
target    prot opt source                destination  
  
Chain OUTPUT (policy ACCEPT)  
target    prot opt source                destination  
diogo@ubuntu:~$
```

Figura 34. Lista de acessos do Iptables

11. `$ iptables -L -v` → Listar as regras correntes no iptables com mais detalhes.

12. `$ iptables -I INPUT 5 -m limit --limit 5/min -j LOG --log-prefix "iptables denied: " --log-level 7` → Logar pacotes liberados ao syslog.

13. `$ cd /etc/` → Acessar a pasta /etc/

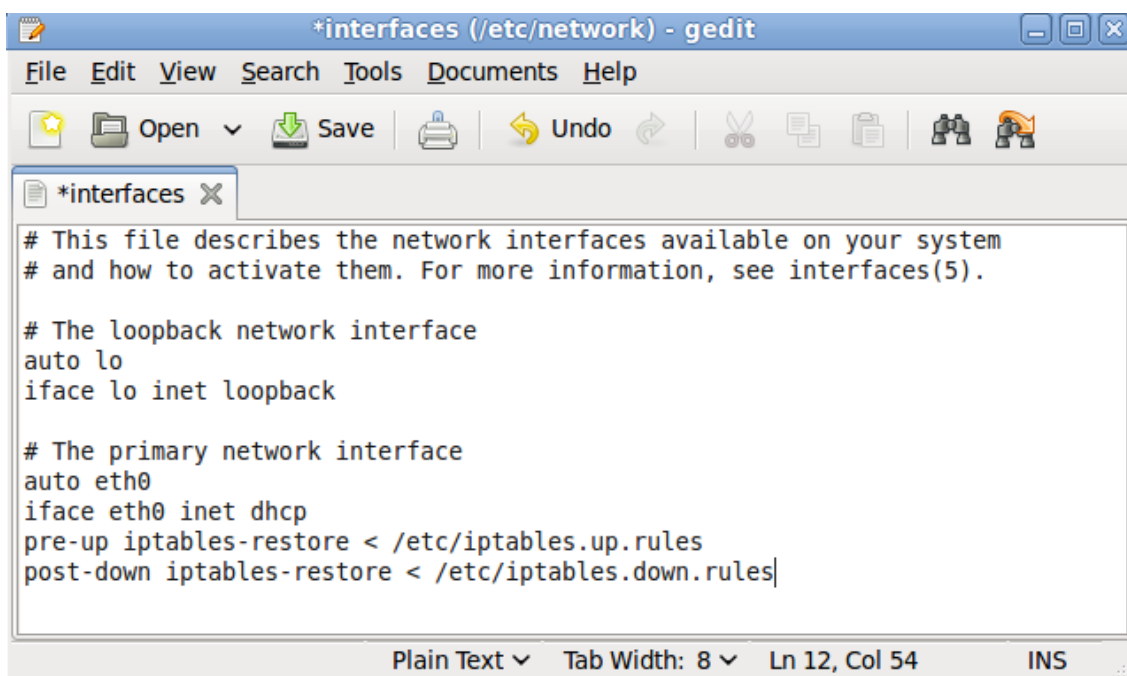
14. `$ gedit iptables.up.rule` → Criar o arquivo de regras do iptable.

Clicar em Salvar ;

15. `$ chmod 777 iptables.up.rules` → Alterar permissões do arquivo

16. `$ iptables-save > /etc/iptables.up.rules` → Salvar as regras do firewall num arquivo

17. `$ gedit /etc/network/interfaces` → Modificar o script, para aplicar as regras ao iniciar e desligar o servidor, inserindo as configurações da imagem abaixo:



```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet dhcp
pre-up iptables-restore < /etc/iptables.up.rules
post-down iptables-restore < /etc/iptables.down.rules
```

Figura 35. Script do arquivo /etc/network/interfaces modificado.

II. Utilizando a Interface Gráfica Firestarter

18. Acessar o firestarter em: *Applications > Internet*.



Figura 36. Interface do Firestartes.

III. Desabilitando o Iptables

19. \$ iptables -F → Desabilitar o firewall.

As resoluções apresentadas foram executadas com a ferramenta Iptables, firewall nativo do Ubuntu Server. Para o SO Windows Server, pode-se utilizar firewall nativo do Windows Server, já que ambos possuem a mesma funcionalidade com funções similares.

4.6.5 Avaliação do Aprendizado

O professor avaliará as atividades através de um questionário (anexo 7) que será postado no sistema Moodle. Uma nota de avaliação da aprendizagem do

assunto é dada como um percentual do total das tarefas previstas no plano de ensino da disciplina.

4.7 Trabalho Final

Aula Número: 7

Tempo de Aula: 6 horas-aula

Grupo: 2 Alunos

4.7.1 Assuntos

O trabalho final da disciplina visa a confecção de um sistema que atenda os conceitos de segurança da informação e de redes abordados na disciplina, garantindo que o sistema gerado é seguro.

4.7.2 Bibliografia Básica

Página web do Prof. João Bosco Sobral, disponível em:
<http://www.inf.ufsc.br/~bosco/ensino/ine5630/>

Página web do Prof. Luiz Carlos Zancanella, disponível em:
<http://www.inf.ufsc.br/~zancanella/>

4.7.3 Objetivos da Aula

Analisar a segurança do sistema proposto, utilizando as técnicas expostas no decorrer da disciplina. Compreender a necessidade de segurança em determinados pontos de um sistema.

4.7.4 Seleção do Conteúdo

O sistema criado pelos alunos deverá ser implementado na linguagem Java ou C#, utilizando o banco de dados MySQL, ou SQL Server Express, já contidos nas Máquinas Virtuais, e seguir as características abaixo

1. O sistema Leitor-Escritor – em banco de dados,
2. Escritores produzem informações sigilosas para leitores específicos.
3. Leitores só tem acesso a informações direcionadas a eles. Ex: Um professor publica as notas da disciplina em base de dados e os alunos consultam suas notas.
4. Sendo seguro, o professor pode conhecer a nota de todos, mas o aluno só tem acesso a sua própria nota.
5. Se necessário, poderá ser utilizado o Apache, ou IIS (Internet Information Services) disponíveis nas máquinas virtuais.

Por se tratar de um sistema livre, sem a definição de um tema específico, não há um modelo de criado, porém, o ambiente necessário para esta tarefa, esta pronto.

4.7.5 Avaliação do Aprendizado

O professor avaliará o trabalho que deverá ser postado no sistema Moodle. Uma nota de avaliação da aprendizagem do assunto é dada como um percentual do total das tarefas previstas no plano de ensino da disciplina.

5. CONCLUSÃO

A Reestruturação da disciplina de Segurança da Informação e de redes - INE5680, do curso de graduação de Sistemas da Informação da UFSC, no que tange o ensino em laboratório, tem como importante passo a adequação do ambiente disponibilizado aos alunos.

A utilização da virtualização nas aulas práticas da disciplina proporciona um ambiente mais adequado ao processo de ensino/aprendizagem. Os benefícios obtidos com a virtualização, além de cumprir os requisitos propostos pelo professor, oferece aos alunos a possibilidade de dispor do ambiente, oferecido no laboratório, fora da estrutura da universidade.

Vantagens como: anular processo de instalação de softwares, independência de restrições da rede INF, acesso total dos recursos do SO, heterogeneidade de Sistemas operacionais, mobilidade do ambiente, fazem da virtualização um fator de reestruturação da disciplina, conforme definido nos objetivos específicos.

As aulas práticas apresentam roteiros superficiais, deixando a cargo da curiosidade do aluno o aprofundamento nas ferramentas, porém demonstrando as funcionalidades básicas e conduzem o aluno pelos procedimentos necessários para chegar aos objetivos propostos em aula.

As especificações das aulas práticas em laboratório abordam os temas lecionados teoricamente, obedecendo às definições dos aspectos didáticos para o ensino, apresentados na seção 2, proporcionadas e aceitas pela instituição de ensino onde a matéria é lecionada.

Por fim, o trabalho posto em prática, certamente contribuirá para otimização do tempo das aulas práticas e a acessibilidade do aluno a esse ambiente, deixando mais proveitosa as aulas práticas de Segurança da informação e de redes.

5.1 Trabalhos Futuros

Como trabalhos futuros, ficam as propostas de:

1. Criar uma Máquina Virtual com o Sistema Operacional OPENBSD;
2. Na aula prática de “Visão Geral de Defesas”, acrescentar a instalação e configuração de um IDS.

6. BIBLIOGRAFIA

CARISSIMI, A.; **Virtualização: Princípios Básicos e Aplicações**, ERAD 2009 - SBC, Caxias do Sul, 2009.

JUNIOR, D. P. Q.; **Virtualização: Conceitos, técnicas aplicadas e um comparativo de desempenho entre as principais ferramentas sem custo de licenciamento**. Instituto Superior Tupy, Joinville, 2008.

LAUREANO, M.; **Máquinas Virtuais e Emuladores - Conceitos, Técnicas e Aplicações**. Novatec Editora, São Paulo, 2006.

LAUREANO, M.; **Uma abordagem para a proteção de detectores de intrusão baseada em máquinas virtuais**. Dissertação de mestrado – PUC/PR, Curitiba, 2004.

NANDA, S.; CHIUEH, T.; **A Survey on Virtualization Technologies**. University at Stony Brook, NY, 2005.

Página web da Ferramenta de Segurança GnuPG, disponível em:
<http://www.gnupg.org/>

Página web da Ferramenta de Segurança OpenPGP, disponível em:
<http://www.openpgp.org/>

Página web da Ferramenta de Segurança OpenVPN, disponível em:
<http://openvpn.net/>

Página web do Prof. João Bosco Sobral, disponível em:
<http://www.inf.ufsc.br/~bosco/ensino/ine5630/>

Página web da ferramenta de Virtualização VirtualBox, disponível em:

<https://www.virtualbox.org/>

Página web da ferramenta de Virtualização XEN, disponível em: <http://xen.org/>

Página web da ferramenta de Virtualização Wmware, disponível em:

<http://www.vmware.com/br/>

Página web do Sistema Operacional Ubuntu, disponível em: <http://www.ubuntu->

[br.org/](http://www.ubuntu-br.org/)

Página web do Sistema Operacional Back Track, disponível em:

<http://www.backtrack-linux.org/>

Página web do Prof. João Eriberto Mota, Universidade Católica de Brasília (UCB),

disponível em: <http://eriberto.pro.br/> .

Página web do Apache, disponível em: <http://www.apache.org/>

Página web da ferramenta de segurança OpenSSL, <http://www.openssl.org/>

Página web da Microsoft, disponível em: [http://technet.microsoft.com/pt-](http://technet.microsoft.com/pt-br/windowsserver)

[br/windowsserver](http://technet.microsoft.com/pt-br/windowsserver)

SANTOS, Leonel Filipe Simões e JACINTO, Nuno Filipe Pedro. **Artigo:**

Autenticação Web com certificados digitais. Disponível em:

<http://www.inf.ufsc.br/~bosco/ensino/ine5630/material-cripto->

[seg/3_Autenticacao_Web_com_certificados_digitais.pdf](http://www.inf.ufsc.br/~bosco/ensino/ine5630/material-cripto-seg/3_Autenticacao_Web_com_certificados_digitais.pdf)

VERAS, M.; **Virtualização - Componente Central do Datacenter**. Editora Brasport,

2011.

WILLIAMS, D.; GARCIA, J.; **Virtualization with Xen: Including XenEnterprise, XenServer and XenExpress**. Editora Syngress, Burlington, 2007.

BANCA EXAMINADORA

Prof. João Bosco M. Sobral (UFSC-orientador, professor responsável),

Prof.^a Carla Merkle Westphall (UFSC)

Prof. Frank Augusto Siqueira (UFSC)

7. ANEXOS

7.1 ANEXO 1 – Plano de Ensino da disciplina



Universidade Federal de Santa Catarina
Centro Tecnológico
Departamento de Informática e Estatística



Plano de Ensino

1) Identificação

Disciplina: INE5680 - Segurança da Informação e de Redes
Turma(s): 08238A, 08238B
Carga horária: 72 horas-aula Teóricas: 40 Práticas: 32
Período: 1º semestre de 2012

2) Cursos

- Sistemas de Informação (238)

3) Requisitos

- INE5625 - Computação Distribuída

4) Ementa

Introdução à Segurança. Conceitos básicos. Técnicas clássicas de criptografia. Criptografia Simétrica. Acordo de chave de Diffie-Hellman. Criptografia de Chave Pública. Gerenciamento de chaves públicas. Funções Hash. Assinaturas Digitais. Certificação Digital. Protocolos de Autenticação. Protocolos Criptográficos. Segurança de aplicações. Redes Privadas Virtuais. Tecnologias disponíveis para defesa. Gestão da Segurança da Informação.

5) Objetivos

Geral: Introduzir a área de segurança computacional, com relação as suas subáreas de: segurança da informação, segurança de redes, segurança de sistemas e segurança de aplicações.

Específicos:

- Conhecer fatos e problemas sobre segurança computacional.
- Compreender conceitos, princípios, mecanismos e métodos para segurança.
- Aplicar algoritmos e protocolos criptográficos.
- Empregar ferramentas que servem de suporte à segurança computacional.
- Conhecer os fundamentos para Gestão de Segurança da Informação.
- Escrever artigo para desenvolver a linguagem escrita.
- Apresentar oralmente trabalho sobre tem escolhido.

6) Conteúdo Programático

- 6.1) Introdução à Segurança Computacional [2 horas-aula]
- 6.2) Conceitos básicos e técnicas clássicas de criptografia [2 horas-aula]
- 6.3) Criptografia Simétrica [4 horas-aula]
- 6.4) Gerenciamento de chaves simétricas [2 horas-aula]
- 6.5) Acordo Diffie-Hellman, Criptografia e Gerenciamento de Chave Pública [6 horas-aula]
- 6.6) Funções Hash, Assinatura Digitais [6 horas-aula]
- 6.7) Infraestrutura de Chaves Públicas e Certificação Digital [6 horas-aula]
- 6.8) Protocolos criptográficos [6 horas-aula]
- 6.9) Segurança de Aplicações [4 horas-aula]
- 6.10) Redes Privadas Virtuais [4 horas-aula]
- 6.11) Vulnerabilidades, Ameaças e Anatomia e Tipos de Ataques [2 horas-aula]
- 6.12) Políticas de Segurança [1 horas-aula]
- 6.13) Protocolos de autenticação, Segurança de acesso remoto [3 horas-aula]
- 6.14) Tecnologias disponíveis para defesa [6 horas-aula]
- 6.15) Conectando-se à Internet com segurança [2 horas-aula]
- 6.16) Modelos de segurança para ambientes cooperativos [2 horas-aula]

- 6.17) Avaliação escrita da aprendizagem [2 horas-aula]
 6.18) Apresentação de tópicos selecionados por grupos [12 horas-aula]
 - Gestão de Segurança da Informação
 - Segurança de Aplicações e Protocolos Criptográficos
 - Ferramentas de segurança
 - Outros tópicos de interesse

7) Metodologia

AT-Aula Teórica, AP-Aula Prática, TT-Tarefa Teórica, TP-Tarefa Prática, APP-Apresentação Prática.

Tarefas teóricas: AT e TT
 Tarefas práticas: AP e TP
 Apresentações Oraís: APP

8) Avaliação

A avaliação da disciplina se dará através de tarefas teóricas (questionários sobre partes da disciplina), tarefas práticas e apresentações orais e duas provas escritas considerando-se os seguintes percentuais máximos para as tarefas:

- Tarefa 1a - Teórica: Questionário introdutório
 Tarefa 1b - Teórica: Ambiente cooperativo
 Tarefa 2a - Teórica: Técnicas clássicas de criptografia (5%)
 Tarefa 2b - Prática: Algoritmo de criptografia simétrica (5%)
 Tarefa 3 - Teórica: Protocolo de autenticação usando criptografia simétrica (5%);
 Tarefa 4 - Prática: Especificar e fazer a validação do protocolo de segurança da questão (3) com a ferramenta Isabelle. (10%)
 Tarefa 5a - Prática: Executar e responder questionário sobre uma ferramenta scanner de portas. (5%)
 Tarefa 5b - Prática: Executar e responder questionário sobre uma ferramenta scanner de vulnerabilidades. (5%)
 Tarefa 6 - Teórica : Criptografia baseada em senha (5%)
 Tarefa 7 - Prática: GnuPG e a segurança de emails (5%);
 Prova 1
 Tarefa 8a - Teórica: Questionário Criptografia de Chave Pública (5%)
 Tarefa 8b - Teórica: Questionário Funções Hash e Assinaturas (5%)
 Tarefa 8c - Teórica: Acordo de Chave Diffie-Hellman (5%)
 Tarefa 9 - Teórica: Funções Criptográficas de Hash, Código de Autenticação de Mensagens Baseado em Hash e Assinatura Digital (5%)
 Tarefa 10 - Prática: Configurar a segurança de servidor web com certificação de cliente e servidor. (10%)
 Tarefa 11 - Prática: Montar uma rede privada virtual (VPN) (5%)
 Prova 2
 Tarefa 12 - Prática: Avaliação de uma ferramenta de segurança escolhida pelo aluno (5%);
 Tarefa 13 - Teórica: Apresentação Oral de Tópicos Selecionados (15%);

Média das Provas MP: $MP = (Prova\ 1 + Prova\ 2)/2$;
 Média das Tarefas (teóricas e práticas) MT:
 $MT = \%T1 + \%T2 + \dots + \%T(n-1) + \%Tn$; varia de 0%=0.00 à 100%=10.00

Média Final MF para aprovação:
 $MF = (MT + MP)/2$; sendo que cada uma das médias deve ser maior ou igual a 6.0. Caso contrário, a média final MF será igual ao valor mais baixo entre a média das tarefas teóricas e práticas e a média das provas.

Conforme parágrafo 2º do artigo 70 da Resolução 17/CUn/97, o aluno com frequência suficiente (FS) e média final no período (MF) entre 3,0 e 5,5 terá direito a uma nova avaliação ao final do semestre (REC), sendo a nota final (NF) calculada conforme parágrafo 3º do artigo 71 desta resolução, ou seja: $NF = (MF + REC) / 2$.

9) Cronograma

- 9/3 Introdução à Segurança Computacional (2), Conceitos básicos e técnicas clássicas de criptografia (2).
 16/3 Vulnerabilidades, Ameaças e Anatomia e Tipos de Ataques (2), Criptografia Simétrica (2).
 30/3 Scanner de Portas (2), Gerenciamento de chaves simétricas (2).
 13/4 Scanner de Vulnerabilidades (2), Acordo Diffie-Hellman (1), Criptografia e Gerenciamento de Chave

Pública (1).
20/4 Protocolos de autenticação (2), Criptografia e Gerenciamento de Chave Pública (2).
27/4 Políticas de Segurança (2), Funções Hash (1), Assinaturas Digitais (1).
4/5 Segurança de emails (GnuPG) (2), Assinaturas Digitais (2).
11/5 Prova 1 (4).
18/5 Firewall, IDS, Conectando-se à Internet, Modelos de segurança para ambientes cooperativos (2),
Infraestrutura de Chaves Públicas e Certificação Digital (2).
25/5 Segurança de servidor (2), Infraestrutura de Chaves Públicas e Certificação Digital (2).
1/6 Redes Privadas Virtuais (2), Protocolos Criptográficos (2)
15/6 Apresentação de Oral de Tópicos (2), Protocolos Criptográficos (2)
22/6 Apresentação de Oral de Tópicos (2), Protocolos Criptográficos (2)
29/6 Apresentação de Oral de Tópicos (2), Prova 2 (2)
06/7 Apresentação de Oral de Tópicos (2).

10) Bibliografia Básica

- Criptografia e Segurança de Redes, William Stallings, 4 Edição, Pearson.
- Segurança de Redes, Emilio T. Nakamura e Paulo L. de Geus, 4 Edição, Futura.
- Segurança de Dados, Routo Terada, 2 Edição, Editora Blucher, 2008.

11) Bibliografia Complementar

- Segurança e Auditoria em Sistemas de Informação, M. R. Lyra, C. Moderna.
- A Nova Escola de Segurança da Informação, A. Shostack et al. Alta Books.
- Redes de Computadores, Tanenbaum e Wetherall, 5 Edição, Pearson.
- Analysing Computer Security, H. Pfleeger e S. Pfleeger, Prent. Hall, 2012.
- Formal Correctness of Security Protocols, G. Bella, Springer, 2010.

7.2 ANEXO 2 – Código da aplicação de Criptografia com Chaves

new 2

quinta-feira, 31 de maio de 2012 13:51

```
package trabalhoCriptografiaAssimetrica;

import java.io.*;
import java.security.*;

public class CarregadorChavePrivada {

    public PrivateKey carregaChavePrivada (File fPvk) throws IOException,
    ClassNotFoundException {
        ObjectInputStream ois = new ObjectInputStream (new FileInputStream (fPvk));
        PrivateKey ret = (PrivateKey) ois.readObject();
        ois.close();
        return ret;
    }
}

package trabalhoCriptografiaAssimetrica;

import java.io.*;
import java.security.*;

public class CarregadorChavePublica {

    public PublicKey carregaChavePublica (File fPub) throws IOException,
    ClassNotFoundException {
        ObjectInputStream ois = new ObjectInputStream (new FileInputStream (fPub));
        PublicKey ret = (PublicKey) ois.readObject();
        ois.close();
        return ret;
    }
}

package trabalhoCriptografiaAssimetrica;

import javax.crypto.*;
import javax.crypto.spec.*;
import java.security.*;

public class Cifrador {

    public byte[][] cifra (PublicKey pub, byte[] textoClaro) throws NoSuchAlgorithmException,
    NoSuchPaddingException, InvalidKeyException, IllegalBlockSizeException,
    BadPaddingException, InvalidAlgorithmParameterException {
        byte[] textoCifrado = null;
        byte[] chaveCifrada = null;

        //-- A) Gerando uma chave simétrica de 128 bits
        KeyGenerator kg = KeyGenerator.getInstance ("AES");
        kg.init (128);
        SecretKey sk = kg.generateKey ();
        byte[] chave = sk.getEncoded();
        //-- B) Cifrando o texto com a chave simétrica gerada
        Cipher aescf = Cipher.getInstance ("AES/CBC/PKCS5Padding");
        IvParameterSpec ivspec = new IvParameterSpec (new byte[16]);
        aescf.init (Cipher.ENCRYPT_MODE, new SecretKeySpec (chave, "AES"), ivspec);
        textoCifrado = aescf.doFinal (textoClaro);
        //-- C) Cifrando a chave com a chave pública
    }
}
```

-1-

```

        Cipher rsacf = Cipher.getInstance ("RSA");
        rsacf.init (Cipher.ENCRYPT_MODE, pub);
        chaveCifrada = rsacf.doFinal (chave);

        return new byte[][] { textoCifrado, chaveCifrada };
    }
}

package trabalhoCriptografiaAssimetrica;

import java.io.*;
import java.security.*;
import javax.swing.JOptionPane;

public class CriptografiaHex {

    public static void printHex(byte[] b) {
        if (b == null) {
            System.out.println ("não encontrado");
        } else {
            for (int i = 0; i < b.length; ++i) {
                if (i % 16 == 0) {
                    System.out.print (Integer.toHexString ((i & 0xFFFF) | 0x10000).substring(1,5)
                        + " - ");
                }
                System.out.print (Integer.toHexString((b[i]&0xFF) | 0x100).substring(1,3) + " ");

                if (i % 16 == 15 || i == b.length - 1)
                {
                    int j;
                    for (j = 16 - i % 16; j > 1; --j)
                        System.out.print (" ");
                    System.out.print (" - ");
                    int start = (i / 16) * 16;
                    int end = (b.length < i + 1) ? b.length : (i + 1);
                    for (j = start; j < end; ++j)
                        if (b[j] >= 32 && b[j] <= 126)
                            System.out.print ((char)b[j]);
                        else
                            System.out.print (".");
                    System.out.println ();
                }
            }
            System.out.println();
        }
    }

    public static void main(String[] args) throws Exception {

        Object[] opcao = { "Sim", "Não" };
        int i = JOptionPane.showOptionDialog(null,
            "Deseja Criar novas chaves?", "Criar chaves",
            JOptionPane.YES_NO_OPTION, JOptionPane.QUESTION_MESSAGE, null,
            opcao, opcao[0]);
        if (i == JOptionPane.YES_OPTION) {
            GeradorDeChaves gpc = new GeradorDeChaves();
            gpc.geraParChaves (new File ("chave.publica"), new File ("chave.privada"));
        }
    }
}

```

```

    }

    System.out.println("Mensagem criptografada:\n");
    //-- Cifrando a mensagem
    byte[] mensagem  JOptionPane.showInputDialog("Insira a mensagem para criptografar").
    getBytes("ISO-8859-1");
    CarregadorChavePublica ccp  new CarregadorChavePublica();
    PublicKey pub  ccp.carregaChavePublica (new File ("chave.publica"));
    Cifrador cf  new Cifrador();
    byte[][] cifrado  cf.cifra (pub, mensagem);
    printHex (cifrado[0]);
    printHex (cifrado[1]);

    //-- Decifrando a mensagem
    CarregadorChavePrivada ccpv  new CarregadorChavePrivada();
    PrivateKey pvk  ccpv.carregaChavePrivada (new File ("chave.privada"));
    Decifrador dcf  new Decifrador();
    System.out.println("A mensagem descriptografada é:\n");
    System.out.println (new String (mensagem, "ISO-8859-1"));
}
}

package trabalhoCriptografiaAssimetrica;

import javax.crypto.*;
import javax.crypto.spec.*;
import java.security.*;

public class Decifrador {

    public byte[] decifra (PrivateKey pvk, byte[] textoCifrado, byte[] chaveCifrada) throws
    NoSuchAlgorithmException,
    NoSuchPaddingException, InvalidKeyException, IllegalBlockSizeException,
    BadPaddingException, InvalidAlgorithmParameterException {
        byte[] textoDecifrado  null;

        //Decifrando a chave simétrica com a chave privada
        Cipher rsacf  Cipher.getInstance ("RSA");
        rsacf.init (Cipher.DECRYPT_MODE, pvk);
        byte[] chaveDecifrada  rsacf.doFinal (chaveCifrada);
        //Decifrando o texto com a chave simétrica decifrada
        Cipher aescf  Cipher.getInstance ("AES/CBC/PKCS5Padding");
        IvParameterSpec ivspec  new IvParameterSpec (new byte[16]);
        aescf.init (Cipher.DECRYPT_MODE, new SecretKeySpec (chaveDecifrada, "AES"), ivspec);
        textoDecifrado  aescf.doFinal (textoCifrado);

        return textoDecifrado;
    }
}

package trabalhoCriptografiaAssimetrica;

import java.io.*;
import java.security.*;
import java.security.spec.*;
import java.security.cert.*;

```

```
public class GeradorDeChaves {

    private static final int RSAKEYSIZE = 1024;

    public void geraParChaves(File arquivoChavePublica, File arquivoChavePrivada) throws
    IOException, NoSuchAlgorithmException,
        InvalidAlgorithmParameterException,
        CertificateException, KeyStoreException {

        KeyPairGenerator kpg = KeyPairGenerator.getInstance ("RSA");
        kpg.initialize (new RSAKeyGenParameterSpec(RSAKEYSIZE, RSAKeyGenParameterSpec.F4));
        KeyPair kpr = kpg.generateKeyPair ();
        PrivateKey chavePrivada = kpr.getPrivate();
        PublicKey chavePublica = kpr.getPublic();
        //-- Gravando chave pública
        ObjectOutputStream oos = new ObjectOutputStream (new FileOutputStream (
        arquivoChavePublica));
        oos.writeObject (chavePublica);
        oos.close();
        //-- Gravando chave privada
        oos = new ObjectOutputStream (new FileOutputStream (arquivoChavePrivada));
        oos.writeObject (chavePrivada);
        oos.close();
    }
}
```

7.3 ANEXO 3 – Questionário de Avaliação 1

Segurança da Informação: Aplicação em E-mail

1. Qual o tamanho de sua chave pública gerada e por que escolheu o tamanho referido?
2. Qual o algoritmo utilizado escolhido para geração de suas chaves? Por que você escolheu este algoritmo?
3. Qual o meio escolhido para você distribuir sua chave pública?
4. Por que a confiabilidade das chaves públicas alheias é importante e como obter essa confiabilidade?
5. O uso do PGP baseia-se em uma relação de confiança. Assim sendo, geralmente, uma chave pública deverá ser assinada pela chave privada de várias pessoas conhecidas. Por que sua chave pública deve ser assinada?
6. Por que *fingerprints* em chaves são importantes?
7. Tente enviar uma mensagem utilizando o GnuPG com o S/MIME, com o certificado obtido.

DEPÓSITO DA TAREFA NO MOODLE

O questionário com as respostas devem ser depositado no prazo previsto pelo professor no sistema MOODLE.

7.4 ANEXO 4 - Questionário de Avaliação 2

Ensino de Segurança da Informação: Aplicação WEB

1. Qual o objetivo de se utilizar criptografia em uma página Web?
2. Um falso remetente envia informação para um destinatário. Este deseja ter certeza de que foi um remetente verdadeiro que enviou a informação. Que **requisito de segurança** precisa ser garantido para que o destinatário tenha plena certeza de quem partiu a informação?
3. Descreva os principais passos configurados nesta tarefa para garantir a publicação de uma página segura.
4. Para que serve, em segurança, o uso das funções hash?
5. Existem alguns algoritmos disponíveis, mais usados, para hash de mensagens: MD5 (128 bits, considerado ótimo) e o SHA-1(160 bits, considerado excelente). Normalmente, os sites que fornecem arquivos longos para serem transferidos, mencionam estes algoritmos e fornecem os cálculos dos hash para esses arquivos. Que outros algoritmos padronizados hash SHA existem para expandir o resultado da função?
6. (Verdade/Falso) No mínimo, a autenticação, garante que uma mensagem provém da origem alegada. Autenticação pode prover proteção contra modificação, atraso, repetição e reordenação.

DEPÓSITO DA TAREFA NO MOODLE

O questionário com as respostas devem ser depositados no prazo previsto pelo professor no sistema MOODLE, no link definido para tal.

7.5 ANEXO 5 - Questionário de Avaliação 3

Redes Privadas Virtuais: Estabelecimento de uma VPN

1. (Verdade/Falso) Uma VPN sempre porta segurança para seus usuários.
2. Se sua resposta é falso, para que serve uma VPN que não porta segurança ?
3. Que forma de certificado, você deve usar na sua experiência de aprendizado sobre VPNs.
4. O que são certificados auto-assinados ?
5. Para que serve a aplicação do método Diffie-Hellman no contexto da criação de uma VPN ?
6. Quando você deve usar uma VPN com criptografia simétrica?
7. Quando você deve usar uma VPN com criptografia assimétrica (chave pública) ?
8. Mostre uma figura que contenha uma outra organização de VPN, mais complexa que seu exemplo.
9. Relacione o uso de uma VPN com a instalação de um firewall. Mostre os casos que uma VPN coexiste com um *firewall*.

DEPÓSITO DA TAREFA NO MOODLE

O questionário com as respostas devem ser depositados no prazo previsto pelo professor no sistema MOODLE, no link definido para tal.

7.6 ANEXO 6 - Questionário de Avaliação 4

Análise de vulnerabilidades – NMAP e OpenVAS

1. Qual é vantagem de ser utilizar a ferramenta NMAP visando a segurança de uma rede?
2. Qual é vantagem de ser utilizar o software OpenVAS visando a segurança de uma rede?
3. Quais é a principal diferença entre as ferramentas OpenVAS e NMAP?
4. Faça uma análise sobre o relatório exibido pelo OpenVAS, sobre o exercício de efetuados em laboratório.
5. NMAP utiliza vários tipos de pesquisa. Cite duas e descreva como funciona.
6. Visando uma rede segura, qual seria o resultado ideal fornecido por estas duas ferramentas.

DEPÓSITO DA TAREFA NO MOODLE

O questionário com as respostas devem ser depositados no prazo previsto pelo professor no sistema MOODLE, no link definido para tal.

7.7 ANEXO 7 - Questionário de Avaliação 5

1. Utilize o IPTables para bloquear todos os acessos, liberando apenas as portas para ssl, e web;
2. Criar regra para carregar as configurações do Iptables automaticamente ao iniciar o sistema Operacional.
3. Desabilitar o Iptables e iniciar um teste de vulnerabilidade com o OpenVAS, utilizando a máquina atual como alvo.
4. Desabilitar o Iptables e iniciar um teste de vulnerabilidade com o NMAP, utilizando a máquina atual como alvo.
5. Utilize as regras dos módulos “state” e “limit” para tentar bloquear varreduras de portas.
6. Configurar o Iptables e iniciar teste com o OpenVAS e NMAP, sendo o computador configurado com o Iptables, o alvo.

DEPÓSITO DA TAREFA NO MOODLE

O questionário com as respostas devem ser depositados no prazo previsto pelo professor no sistema MOODLE, no link definido para tal.

7.8 ANEXO 8 - Relatório de Vulnerabilidades OpenVAS

OpenVAS Scan Report

This report gives details on hosts that were tested and issues that were found. Please follow the recommended steps and procedures to eradicate these threats.

Scan Details

Hosts which were alive and responding during test	1
Number of security holes	3
Number of security warnings	4
Number of security notes	14
Number of false positives	0

Host List

Host(s)	Possible Issue
localhost [return to top]	Security hole(s)

Analysis of Host

Address of Host	Port / Service	Issue regarding Port
localhost	ssh (22/tcp)	Security note(s)
localhost	http (80/tcp)	Security hole(s)
localhost	netbios-ssn (139/tcp)	Security note(s)
localhost	microsoft-ds (445/tcp)	Security hole(s)
localhost	otp (9390/tcp)	Security note(s)
localhost	netbios-ns (137/udp)	No Information
localhost	general/tcp	Security note(s)
localhost	general/IT-Grundschutz	No Information
localhost	general/SMBClient	Security note(s)
localhost	general/IT-Grundschutz-T	No Information
localhost	general/CPE-T	No Information
localhost	general/HOST-T	No Information

Security Issues and Fixes: localhost

Type	Port	Issue and Fix
Informational	ssh (22/tcp)	An ssh server is running on this port OID : 1.3.6.1.4.1.25623.1.0.10330
Vulnerability	http (80/tcp)	<p>Overview: Apache is prone to multiple vulnerabilities.</p> <p>These issues may lead to information disclosure or other attacks.</p> <p>Apache versions prior to 2.2.15-dev are affected.</p> <p>Solution: These issues have been addressed in Apache 2.2.15-dev. Apache 2.2.15 including fixes will become available in the future as well. Please see the references for more information.</p> <p>References: http://www.securityfocus.com/bid/38494 http://httpd.apache.org/security/vulnerabilities_22.html http://httpd.apache.org/ https://issues.apache.org/bugzilla/show_bug.cgi?id=48359 http://svn.apache.org/viewvc?view=revision&revision=917870 </p>

Vulnerability	http (80/tcp)	<p>CVE : CVE-2010-0425, CVE-2010-0434, CVE-2010-0408 BID : 38494, 38491 OID : 1.3.6.1.4.1.25623.1.0.100514</p> <p>Overview: This host is running Apache httpd web server and is prone to denial of service vulnerability.</p> <p>Vulnerability Insight: The flaw is caused the way Apache httpd web server handles certain requests with multiple overlapping ranges, which causes significant memory and CPU usage on the server leading to application crash and system can become unstable.</p> <p>Impact: Successful exploitation will let the remote unauthenticated attackers to cause a denial of service.</p> <p>Impact Level: System/Application</p> <p>Affected Software/OS: Apache 1.3.x, 2.0.x through 2.0.64 and 2.2.x through 2.2.19</p> <p>Fix: Please refer below link for fix and mitigate this issue until full fix, http://mail-archives.apache.org/mod_mbox/httpd-dev/201108.mbox/%3CCAAPSnn2PO-d-C4nQt_TES2RRWzr7urefhTKPWBC1b+K1Dqc7g@mail.gmail.com/%3E http://marc.info/?l=apache-httpd-dev&m=131420013520206&w=2</p> <p>References: http://www.exploit-db.com/exploits/17696 http://packetstormsecurity.org/files/view/104441 http://marc.info/?l=apache-httpd-dev&m=131420013520206&w=2</p>
Warning	http (80/tcp)	<p>CVE : CVE-2011-3192 BID : 49303 OID : 1.3.6.1.4.1.25623.1.0.901203</p> <p>Requesting the URI /server-status gives information about the currently running Apache.</p> <p>Risk factor : Low Solution : If you don't use this feature, comment the appropriate section in your httpd.conf file. If you really need it, limit its access to the administrator's machine. OID : 1.3.6.1.4.1.25623.1.0.10677</p>
Warning	http (80/tcp)	<p>Overview: A weakness has been discovered in Apache web servers that are configured to use the FileETag directive. Due to the way in which Apache generates ETag response headers, it may be possible for an attacker to obtain sensitive information regarding server files. Specifically, ETag header fields returned to a client contain the file's inode number.</p> <p>Exploitation of this issue may provide an attacker with information that may be used to launch further attacks against a target network.</p> <p>OpenBSD has released a patch that addresses this issue. Inode numbers returned from the server are now encoded using a private hash to avoid the release of sensitive information.</p> <p>Solution: OpenBSD has released a patch to address this issue.</p> <p>Novell has released TID10090670 to advise users to apply the available workaround of disabling the directive in the configuration file for</p>

Apache releases on NetWare. Please see the attached Technical Information Document for further details.

References:

<https://www.securityfocus.com/bid/6939>
<http://httpd.apache.org/docs/mod/core.html#fileetag>
<http://www.openbsd.org/errata32.html>
<http://support.novell.com/docs/Tids/Solutions/10090670.html>

Information that was gathered:

Inode: 301097
Size: 177

CVE : [CVE-2003-1418](#)
BID : [6939](#)
OID : [1.3.6.1.4.1.25623.1.0.103122](#)

Warning http (80/tcp)

The /doc directory is browsable.
/doc shows the content of the /usr/doc directory and therefore it shows which programs and - important! - the version of the installed programs.

Solution : Use access restrictions for the /doc directory.
If you use Apache you might use this in your access.conf:

```
<Directory /usr/doc>  
AllowOverride None  
order deny,allow  
deny from all  
allow from localhost  
</Directory>
```

Risk factor : High
CVE : [CVE-1999-0678](#)
BID : [318](#)
OID : [1.3.6.1.4.1.25623.1.0.10056](#)

Informational http (80/tcp)

A web server is running on this port
OID : [1.3.6.1.4.1.25623.1.0.10330](#)

Informational http (80/tcp)

The remote web server type is :
Apache/2.2.14 (Ubuntu)

Solution : You can set the directive 'ServerTokens Prod' to limit the information emanating from the server in its response headers.
OID : [1.3.6.1.4.1.25623.1.0.10107](#)

Informational http (80/tcp)

The following directories were discovered:
/cgi-bin, /doc, /icons, /server-status

While this is not, in and of itself, a bug, you should manually inspect these directories to ensure that they are in compliance with company security standards

Other references : OWASP:OWASP-CM-006
OID : [1.3.6.1.4.1.25623.1.0.11032](#)

Informational netbios-ssn (139/tcp)

An SMB server is running on this port
OID : [1.3.6.1.4.1.25623.1.0.11011](#)

Vulnerability microsoft-ds (445/tcp)

Overview: The host is running SMB/NETBIOS and prone to authentication bypass Vulnerability

Vulnerability Insight:

The flaw is caused due to an SMB share, allows full access to Guest users.
If the Guest account is enabled, anyone can access the computer without a valid user account or password.

Impact:

Successful exploitation could allow attackers to use shares to cause the system to crash.

		<p>Impact Level: System</p> <p>Affected Software/OS: Microsoft Windows 95 Microsoft Windows 98 Microsoft Windows NT</p> <p>Fix: No solution or patch is available as on 11th October, 2011. Information regarding this issue will be updated once the solution details are available. For updates refer, http://sourceforge.net/projects/nfs/files/nfs-utils/</p> <p>workaround: 1. Disable null session login. 2. Remove the share. 3. Enable passwords on the share.</p> <p>References: http://xforce.iss.net/xforce/xfdb/2 http://sedab.cs.ucdavis.edu/projects/testing/vulner/38.html CVE : CVE-1999-0519 OID : 1.3.6.1.4.1.25623.1.0.801991</p> <p>Overview: Samba is prone to multiple remote denial-of-service vulnerabilities.</p> <p>An attacker can exploit these issues to crash the application, denying service to legitimate users.</p> <p>Versions prior to Samba 3.4.8 and 3.5.2 are vulnerable.</p> <p>Solution: Updates are available. Please see the references for more information.</p> <p>References: http://www.securityfocus.com/bid/40097 https://bugzilla.samba.org/show_bug.cgi?id=7254 http://samba.org/samba/history/samba-3.4.8.html http://samba.org/samba/history/samba-3.5.2.html http://www.samba.org CVE : CVE-2010-1635 BID : 40097 OID : 1.3.6.1.4.1.25623.1.0.100644</p>
Warning	microsoft-ds (445/tcp)	
Informational	microsoft-ds (445/tcp)	<p>A CIFS server is running on this port OID : 1.3.6.1.4.1.25623.1.0.11011</p>
Informational	microsoft-ds (445/tcp)	<p>It was possible to log into the remote host using the SMB protocol. OID : 1.3.6.1.4.1.25623.1.0.10394</p>
Informational	microsoft-ds (445/tcp)	<p>Overview: It is possible to extract OS, domain and SMB server information from the Session Setup AndX Response packet which is generated during NTLM authentication. Detected SMB workgroup: WORKGROUP Detected SMB server: Samba 3.4.7 Detected OS: Unix</p> <p>OID : 1.3.6.1.4.1.25623.1.0.102011</p>
Informational	otp (9390/tcp)	<p>Overview: OpenVAS is running at this host.</p> <p>OpenVAS stands for Open Vulnerability Assessment System and is a network security scanner with associated tools like a graphical user front-end. The core component is a server with a set of network vulnerability tests (NVTs) to detect security problems in remote systems and applications. See http://openvas.org for more information.</p>

Risk factor : None
OID : [1.3.6.1.4.1.25623.1.0.100076](#)
Informational general/tcp Here is the route from 127.0.0.1 to 127.0.0.1
127.0.0.1
OID : [1.3.6.1.4.1.25623.1.0.51662](#)
Informational general/SMBClient OS Version = Unix
Domain = WORKGROUP
SMB Serverversion = Samba 3.4.7
OID : [1.3.6.1.4.1.25623.1.0.90011](#)
Informational general/SMBClient OS Version = Unix
Domain = WORKGROUP
SMB Serverversion = SAMBA 3.4.7
OID : [1.3.6.1.4.1.25623.1.0.90011](#)
Informational general/SMBClient OS Version = UNIX
Domain = WORKGROUP
SMB Serverversion = Samba 3.4.7
OID : [1.3.6.1.4.1.25623.1.0.90011](#)
Informational general/SMBClient OS Version = UNIX
Domain = WORKGROUP
SMB Serverversion = SAMBA 3.4.7
OID : [1.3.6.1.4.1.25623.1.0.90011](#)

This file was generated by the [OpenVAS](#) security scanner.