UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
COORDENAÇÃO DO CURSO SUPERIOR DE
TECNOLOGIA EM SISTEMAS PARA INTERNET

HENRIQUE OLIVEIRA

ANÁLISE DA INTEGRAÇÃO ENTRE O KERBEROS E O OPENLDAP

TRABALHO DE CONCLUSÃO DE CURSO

CAMPO MOURÃO
2013

HENRIQUE OLIVEIRA

ANÁLISE DA INTEGRAÇÃO ENTRE O KERBEROS E O OPENLDAP

Trabalho de Conclusão de Curso de Graduação, apresentado à disciplina de Trabalho de Conclusão de Curso, do Curso Superior de Tecnologia em Sistemas para Internet da Coordenação do Curso Superior de Tecnologia em Sistemas para Internet da Universidade Tecnológica Federal do Paraná – UTFPR, como requisito para aprovação na disciplina.

Orientador: Prof. Me. Rodrigo Campiolo

CAMPO MOURÃO

2013

ATA DA DEFESA DO TABALHO DE CONCLUSÃO DE CURSO

Às **dezenove horas** do dia **três de maio de dois mil e treze** foi realizada no Mini-auditório do EAD da UTFPR-CM a sessão pública da defesa do Trabalho de Conclusão do Curso Superior de Tecnologia em Sistemas para Internet do acadêmico **Henrique Oliveira** com o título **ANÁLISE DA INTEGRAÇÃO ENTRE O KERBEROS E O OPENLDAP**. Estavam presentes, além do acadêmico, os membros da banca examinadora composta pelo professor **Me. Rodrigo Campiolo** (Orientador-Presidente), pelo professor **Me. Alessandro Kraemer** e pelo professor **Me. Rodrigo Hübner**. Inicialmente, o aluno fez a apresentação do seu trabalho, sendo, em seguida, arguido pela banca examinadora. Após as arguições, sem a presença do acadêmico, a banca examinadora o considerou **APROVADO** na disciplina de Trabalho de Conclusão de Curso e atribuiu, em consenso, a nota ____ (_____). Este resultado foi comunicado ao acadêmico e aos presentes na sessão pública. A banca examinadora também comunicou ao acadêmico que este resultado fica condicionado à entrega da versão final dentro dos padrões e da documentação exigida pela UTFPR ao professor Responsável do TCC no prazo de **onze dias**. Em seguida foi encerrada a sessão e, para constar, foi lavrada a presente Ata que segue assinada pelos membros da banca examinadora, após lida e considerada conforme.

Observações:

_____

_____

_____

_____

_____

Campo Mourão, 03 de maio de 2013.

_____	_____	_____
Prof. Me. Alessandro Kraemer Membro	Prof. Me. Rodrigo Hübner Membro	Prof. Me. Rodrigo Campiolo Orientador

Dedico este trabalho aos meus pais, amigos, colegas de trabalho e a todas as pessoas que me apoiaram e acreditaram em mim, sem eles não chegaria onde estou.

AGRADECIMENTOS

Primeiramente gostaria de agradecer a Deus, o centro e o fundamento de tudo em minha vida, por renovar cada momento a minha força e disposição e pelo discernimento concedido ao longo desta jornada. Agradeço aos meus pais Maria L. L. Oliveira e Miguel J. Oliveira pelo apoio e incentivo em todos os momentos, ao meu colega de trabalho Rafael M. Borges pela ajuda nos momentos que mais precisei.

Agradeço ao professor Rodrigo Campiolo por toda a orientação que foi dada durante o desenvolvimento deste trabalho, sou grato também por todos os professores que fazem parte da Coordenação de Informática. E, também, a todos que direto ou indiretamente fizeram parte da minha formação, o meu muito obrigado.

RESUMO

OLIVEIRA, Henrique. Análise da Integração do Kerberos com o OpenLDAP. 2013. 60 f. Trabalho de Conclusão de Curso – Tecnologia em Sistemas para Internet, Universidade Tecnológica Federal do Paraná. Campo Mourão, 2013.

Devido a dificuldade de gerenciar usuários em diferentes serviços de rede de computadores, hoje existe a tendência de centralizar dados por meio de LDAP (*Lightweight Directory Access Protocol*). Entretanto, as redes de computadores não são totalmente seguras, logo necessita-se à integração de algum serviço ou protocolo que provê segurança a rede. O tráfego de autenticação de usuários e autorização de serviços deve ser confidencial, uma vez que se essas informações forem roubadas poderá acarretar em uma quebra de segurança. O protocolo Kerberos provê uma camada extra de segurança. Neste trabalho é apresentado o Kerberos integrado ao LDAP, visando avaliar os impactos no tráfego ao adicionar um alto nível de segurança à rede. A avaliação foi realizada por meio de quatro estudos de caso: autenticação somente com SSH, autenticação com SSH e OpenLDAP, autenticação do SSH com Kerberos e por fim autenticação do SSH com OpenLDAP e Kerberos, e por meio da análise do tráfego e pacote. Em um ambiente virtualizado foram realizadas medidas de tráfego antes e depois da implantação do Kerberos com LDAP. Após a captura de pacotes referentes a um acesso SSH utilizando o Kerberos como autenticação, observou-se que a integração não afeta significativamente o tráfego da rede.

Palavras-chaves: LDAP; Kerberos; Autenticação;

ABSTRACT

OLIVEIRA, Henrique. Analysis of Integration of Kerberos with OpenLDAP. 2013. 60 f. Trabalho de Conclusão de Curso – Tecnologia em Sistemas para Internet, Universidade Tecnológica Federal do Paraná. Campo Mourão, 2013.

Due to the difficulty of managing users in different services of computer network, today there is a tendency to centralize data via LDAP (Lightweight Directory Access Protocol). However, computer networks are not secure, then the need to integrate some service or protocol that secures the network. The traffic of user authentication and authorization services should be confidential, since that information is stolen may result in a security breach. The Kerberos protocol provides an extra layer of security. This work presents the Kerberos integrated with LDAP, to evaluate the impacts on traffic to add a high level of network security. The evaluation was performed through four case studies: only authentication with SSH, SSH authentication and OpenLDAP, Kerberos authentication with SSH and finally SSH authentication with OpenLDAP and Kerberos, and through traffic analysis and packet. In a virtualized environment, we performed measurements of traffic before and after the implementation of Kerberos with LDAP. After capturing packets regarding SSH access using Kerberos as authentication, it was observed that the integration does not significantly affect network traffic.

Keywords: LDAP; Kerberos; Authentication;

LISTA DE SIGLAS

AS	*Authentication Server* (Servidor de Autenticação)
DAP	*Directory Access Protocol* (Protocolo de Acesso a Diretório)
DES	*Data Encryption Standard* (Padrão de Criptografia de Dados)
DNS	*Domain Name System* (Servidor de Nomes de Domínio)
FQDN	*Fully Qualified Domain Name* (Nome de Domínio Completamente Expressado)
IETF	*Internet Engineering Task Force* (Força Tarefa da Engenharia da Internet)
IP	*Internet Protocol* (Protocolo de Internet)
KDC	*Key Distribution Center* (Centro Distribuição de Chaves)
LDAP	*Lightweight Directory Access Protocol* (Protocolo Leve de Acesso a Diretórios)
LDIF	*LDAP Data Interchange Format* (Formato de Troca de Dados LDAP)
MIT	*Massachusetts Institute of Technology* (Instituto de Tecnologia de Massachusetts)
NTP	*Network Time Protocol* (Protocolo de Tempo)
OSI	*Open System Interface* (Interface de Sistema Aberto)
TGS	*Ticket Granting Server* (Servidor Concessão de Ingressos)
TGT	*Ticket Granting Ticket* (Permissão de Concessão)
USA	*United States of America* (Estados Unidos da América)

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE GRÁFICOS

SUMÁRIO

1. INTRODUÇÃO

Muitos sistemas computacionais fazem uso de uma autenticação baseada em uma palavra secreta, geralmente uma senha conhecida somente pelo usuário. Em muitas situações essa autenticação é feita sem nenhum tipo de criptografia, sendo assim, fácil de ser interceptada e usada por usuários maliciosos.

A fim de evitar ataques virtuais às informações pessoais ou corporativas por meio de ataques internos ou externos (GERMAN, 2003), tem-se que investir em segurança para evitar a violação desses dados. Por isso, o uso de um protocolo de autenticação de serviços em uma rede, evita que mensagens, senhas entre outros sejam interceptados por usuários maliciosos.

O protocolo Kerberos surgiu para eliminar o tráfego de senhas descriptografadas pela rede, e para evitar alguns tipos de ataques, tais como o de reenvio, personificação e criptoanálise, aumentando o nível de segurança durante a autenticação. Um mecanismo para organizar dados dos usuários, senhas e acesso a serviços em uma rede é o protocolo LDAP. Tal protocolo centraliza e agiliza as questões de autenticação e autorização em um sistema.

Os protocolos Kerberos e LDAP podem trabalhar em conjunto, pois o Kerberos precisa acessar as senhas de um usuário para realizar a autenticação, enquanto o LDAP armazena de forma eficiente e organizada informações de autorização e autenticação.

Objetiva-se neste trabalho a análise de impacto no tráfego de rede ao integrar o Kerberos ao LDAP, visando que maioria dos trabalhos relacionados à integração do Kerberos com LDAP foca somente sobre o funcionamento e aplicação da integração.

Os objetivos específicos foram a fim de se obter melhores resultados foi realizada uma análise mais detalhada, gerando e monitorando o tráfego dos pacotes em um ambiente virtualizado, avaliando assim a situação da rede. Isso permitirá analisar de uma forma mais precisa as vantagens e desvantagens em realizar essa integração.

A avaliação da integração foi realizada em um ambiente virtualizado. Usando um analisador de pacotes para um serviço de acesso remoto, foram realizadas medidas de tráfego antes e depois da implantação do Kerberos com LDAP.

Como resultado, é provida uma análise do tráfego e dificuldades da implantação Kerberos e OpenLDAP, o que permitirá um administrador de redes decidir sobre adicionar ou não essa estrutura a rede.

A monografia está dividida em 6 capítulos. O capítulo 2 apresenta todo o referencial teórico estudado para a realização desta monografia, já o capítulo 3 apresenta os materiais e métodos utilizados. O capítulo 4 apresenta a integração dos serviços com o Kerberos e o OpenLDAP, o capítulo 5 apresenta os testes as análises e as discussões sobre a integração dos serviços com o Kerberos e o OpenLDAP, por fim o capítulo 6 apresenta as conclusões obtidas.

2. REFERENCIAL TEÓRICO

Neste capítulo são apresentados os conceitos e tecnologias utilizadas para a elaboração desta monografia: Kerberos e LDAP. Na seção 2.1 é detalhado sobre o protocolo Kerberos, sua origem e funcionamento. Na seção 2.2 é apresentado o funcionamento do protocolo LDAP e sua origem. Na seção 2.3 são apresentados os trabalhos relacionados.

2.1. O PROTOCOLO KERBEROS

A palavra Kerberos tem origem da mitologia grega de Cerberus, que era o guardião da entrada de Hades, o submundo dos mortos. Os gregos acreditavam que o objetivo de Cerberus era deixar as almas entrarem, mais jamais saírem, pois despedaçava os mortais que tentassem atravessar. Na maioria das literaturas, Cerberus era um monstruoso cão de três cabeças e cobras ao redor de seu corpo, além de uma serpente como calda (GARMAN, 2003). O nome Kerberos não foi mera coincidência, é uma alusão ao nome Cerberus, pois a grafia correta de Cerberus em grego é Kerberos.

O Kerberos foi desenvolvido pelo MIT, a princípio para suprir as necessidades do projeto Athena (MIHALIK, 1999). Suas primeiras versões foram somente para testes e continham limitações significativas. Foram úteis para analisar novas ideias para implementar outras versões do Kerberos.

Até então o Kerberos era utilizado somente pelo MIT para uso interno, porém em 24 de janeiro de 1989 o protocolo foi lançado publicamente já com uma versão mais estável e funcional, a versão 4. Porém existia um impasse que não permitia que o Kerberos fosse utilizado fora dos Estados Unidos, pois existia uma restrição na exportação de softwares de criptografia. Como o Kerberos utilizava o DES – um algoritmo de criptografia – organizações fora dos EUA não poderiam legalmente realizar o *download*. A fim de solucionar este problema o MIT retirou toda a parte do código de criptografia para criar uma versão somente para exportação, assim podendo ser utilizada em qualquer lugar do mundo (GARMAN, 2003). Os algoritmos

de chave simétrica correspondem a uma classe de algoritmos para criptografia, esta classe utiliza chaves criptográficas relacionadas para operações de cifragem e decifragem, o algoritmo funciona com uma única chave entre as operações, são usadas para manter um canal confidencial de informações (ALECRIM, 2010).

A versão mais recente do Kerberos é a 5. Essa versão foi aprimorada para corrigir alguns erros da versão 4 e adicionar algumas funcionalidades, destacando a mudança do algoritmo de criptografia, onde na versão 4 era implementado o DES e a versão atual tem a implementação da criptografia em módulo independente, pois assim pode se adaptar o tipo de criptografia desejada.

2.1.1. *Visão geral*

Kerberos é um protocolo para autenticação de serviços de redes que possui um módulo de criptografia de chave simétrica para realizar as autenticações entre cliente/servidor, eliminando assim o risco do tráfego de senhas pela rede.

Baseia-se em um ambiente distribuído onde os usuários podem ter acesso a serviços da rede. A principal ideia do protocolo é oferecer algumas características como: segurança, confiabilidade, transparência e escalabilidade. Seu funcionamento básico consiste em autorizar um usuário a executar um determinado serviço da rede. Para isso, o Kerberos utiliza um *ticket* (também chamado de ingresso) e um autenticador para verificar a autenticidade do *ticket*.

É usado tipicamente quando um usuário tenta acessar algum recurso da rede, e este recurso deseja assegurar que o usuário em questão é realmente quem diz ser. Para isso, o usuário possuí um *ticket*, ele é apresentado ao recurso em questão para realizar a autenticação, assim que o *ticket* for analisado e for verificada a autenticidade do usuário, o recurso é liberado para o usuário (BERGAMASCHI, 2011).

2.1.2. Terminologia

O protocolo Kerberos possui uma nomenclatura própria. Segue os principais termos usados (GERMAN, 2003):

- **Domínio (*Realm*):** refere-se ao sistema que confia no protocolo Kerberos para fazer autenticação. Normalmente utiliza o mesmo nome do domínio de rede, porém convertido para letras maiúsculas.
- **Principal *(Principal)*:** é uma nomenclatura associada a cada usuário a ser autenticado no Kerberos. Segue um padrão com o nome do usuário, seguido pelo símbolo @ (arroba) e o nome do domínio.
- **Ingressos (*Tickets*):** corresponde ao conjunto de informações que revela a identidade do usuário (*principal*). É único e exclusivo para cada serviço da rede.
- **Chave de sessão:** uma chave secreta gerada aleatoriamente. Essa chave é enviada para o cliente que requisitou o serviço e utilizada para proteger os autenticadores e a comunicação com os servidores.

2.1.3. *Funcionamento*

O Kerberos é responsável em prover um maior nível de segurança nas redes de computador onde é implantado, pois faz a autenticação de serviços/servidores de maneira que, mesmo quando os pacotes que trafegam durante uma autenticação, não possam ser interpretados por usuários maliciosos. O Kerberos funciona por um ou mais servidores *Key Distribution Center* (KDC) onde o KDC é responsável pela distribuição de chaves aos usuários e/ou serviços da rede. O KDC é divido em três principais componentes: *Authentication Server* (AS), *Ticket Granting Server* (TGS) e a Base de Dados, conforme é apresentado na Figura 01.

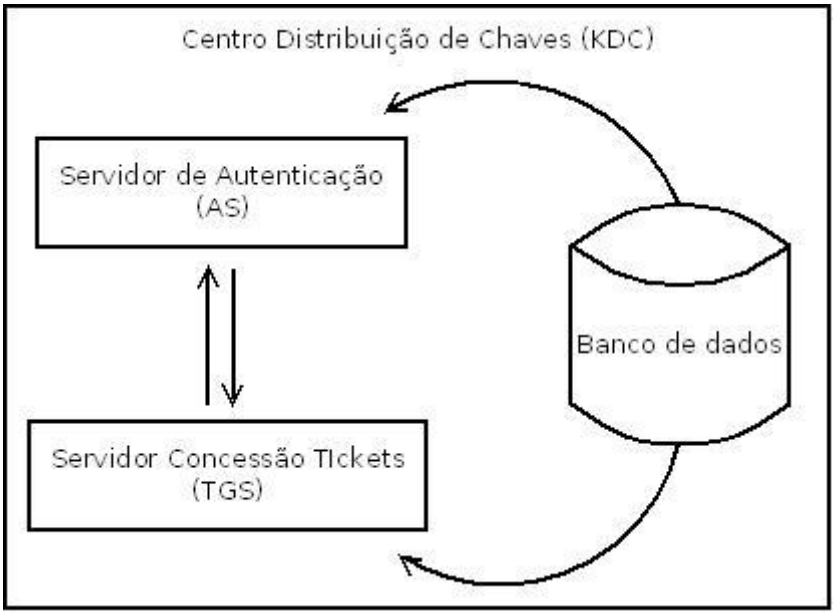

Figura 1 - Componentes do KDC

Observa-se na Figura 01 que cada componente é responsável por uma tarefa.

- O AS recebe o pedido de autenticação de um usuário e verifica a autenticidade deste usuário.
- Após confirmar, o AS emite um TGT, este *ticket* será fornecido a outro componente do KDC, o TGS.
- O TGT é uma credencial concedida ao usuário pelo AS, o usuário precisa deste TGT para fazer suas requisições. Quando o serviço acessado pelo usuário faz uma requisição de um *ticket* para o servidor Kerberos, este solicitará seu usuário e senha.
- O servidor TGS responde à requisição do ticket enviando o TGT. Desta forma, somente este usuário é capaz de descriptografar o TGT. O TGS é responsável por fornecer *tickets* para serviços que o usuário requisitou.
- Após receber o TGT, que foi fornecido pelo AS, o TGS cria um novo *ticket* para ser usado pelos serviços requeridos pelo usuário. No banco de dados ficam registrados todos os usuários e senhas da rede. O banco de dados é utilizado pelo Kerberos para realizar a busca de informações sobre os usuários.

A Figura 02 apresenta a troca de mensagens entre cliente e servidor quando

o protocolo de Kerberos está atuando como autenticador.

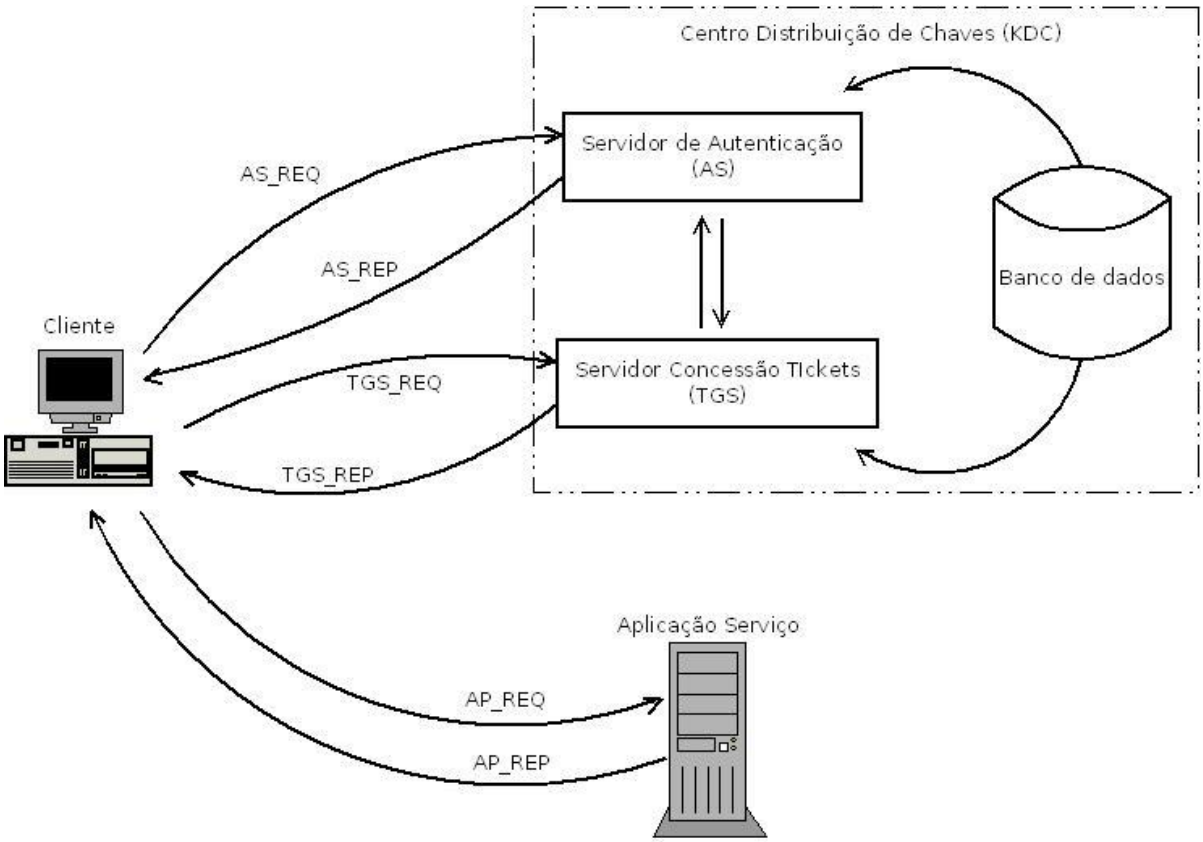

Figura 2 - Troca de mensagens do Kerberos
Fonte: Adaptado de (RICCIARDI, 2007)

A sequência de mensagens é descrita na ordem que ocorrem (RICCIARDI, 2007; GERMAN, 2003):

- **AS_REQ:** é a primeira comunicação do cliente com o Kerberos. A requisição do serviço. Esta mensagem é destinada ao KDC;
- **AS_REP:** é a resposta do servidor AS à solicitação anterior. Contém o TGT em seu contexto;
- **TGS_REQ:** o cliente está repassando o TGT, para ser gerado um novo *ticket* específico para o serviço que está sendo requisitado;
- **TGS_REP:** após receber o TGT, o novo *ticket* é gerado e repassado para o cliente;
- **AP_REQ:** agora o usuário está solicitando permissão para utilizar o

serviço, esta permissão é a resposta que o TGS enviou ao cliente;

- **AP_REP:** o serviço está respondendo ao usuário que realmente é o serviço que ele gostaria de acessar e está lhe dando permissão para acesso.

Mais detalhes sobre a troca de mensagens do Kerberos podem ser vistas em (RICCIARDI, 2007).

2.2. O PROTOCOLO LDAP

Originalmente o LDAP foi desenvolvido por Tim Howes, Wengyik Yeong e Steve Kille em 1993. Em 1997 com ajuda da IETF foi publicada a versão 3 do LDAP (LDAPv3) (JUNIOR, 2011). O LDAP surgiu como uma alternativa ao serviço de diretórios X.500, este serviço de diretório era originalmente acessado através do DAP, tal protocolo realizava a comunicação entre cliente e servidor utilizando o padrão OSI . O X.500 é considerado um protocolo “pesado”, pois operava sobre o protocolo OSI, o qual necessita uma grande quantidade de recursos computacionais, já o LDAP é considerado um protocolo “leve”, pois não precisa operar sobre as camadas do protocolo OSI, pois foi projetado para operar sobre o TCP/IP (TRIGO, 2007).

2.2.1. *Visão geral*

Lightweight Directory Access Protocol - “LDAP, ou Protocolo Leve de Acesso a Diretórios, é um conjunto de regras que controla a comunicação entre serviços de diretórios e seus clientes." (TRIGO, 2007).

A maioria das empresas possui uma rede de computadores devido ao fato de terem aplicações distribuídas para controlarem os diversos níveis organizacionais. Considerando o uso de um mesmo serviço por diversos usuários, torna-se necessário fazer a centralização e organização destes dados, para tornar o

gerenciamento mais fácil.

A partir dessa necessidade de organizar dados que são utilizados frequentemente, foi necessária a criação de um protocolo chamado LDAP. Tal protocolo define métodos de busca e atualização de informações mais eficazes. Mais sobre o protocolo por ser visto em (MACHADO; JUNIOR, 2006).

O LDAP organiza sua estrutura em uma árvore de diretórios, onde o diretório representa um repositório que contém um conjunto de informação. O repositório segue um critério que facilita a busca das informações. Um exemplo é comparar a um diretório a uma lista telefônica, onde podemos facilmente buscar uma informação baseado em um critério que facilita esta busca, ou seja, as informações são separadas em ordem alfabética (MACHADO; JUNIOR, 2006).

2.2.2. Funcionamento

O serviço de diretórios LDAP funciona como uma estrutura organizada em árvore. Como toda estrutura em árvore existe os elementos: raiz, ramos e folhas. Cada elemento é representado por algo, neste caso, a raiz e os ramos são os diretórios, que por sua vez pode conter outros diretórios ou entradas que são chamados de elementos, estes possuem um ou mais valores, todos estes de acordo com um tipo de dado já definido (TRIGO, 2007).

Cada vez que o usuário deseja obter alguma informação desta árvore uma série de mensagens é trocada entre usuário e servidor. A Figura 03 mostra a troca completa de mensagens quando um cliente faz uma requisição ao servidor LDAP.

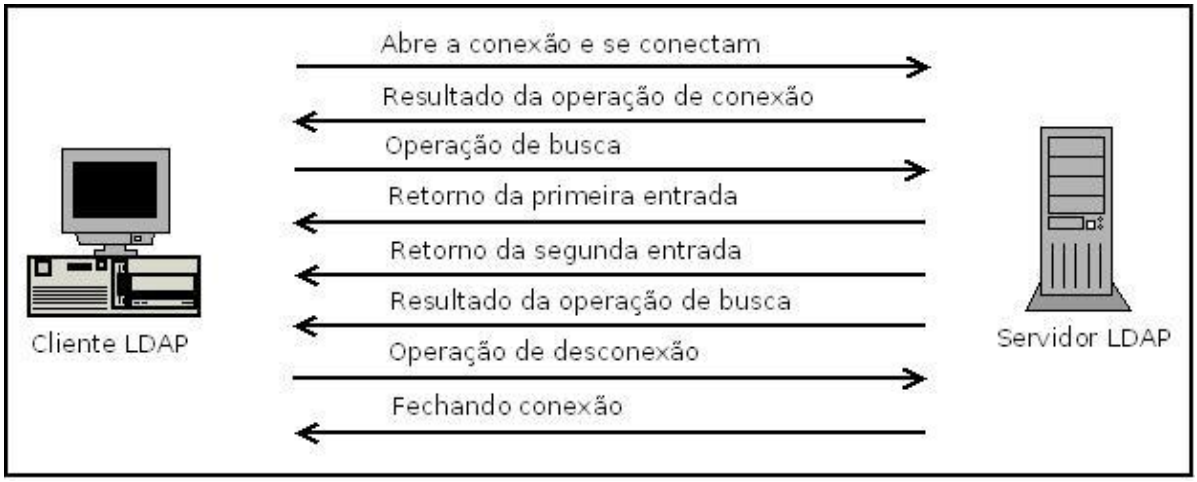

Figura 3 - Troca de mensagens do LDAP
Fonte - Adaptado de (HOWES; SMITH; GOOD; 2003)

Primeiramente o cliente abre uma conexão TCP/IP com o servidor LDAP e envia uma operação de *bind*, esta operação inclui o que ele deseja se autenticar seguido de suas credencias – usuário e senha. Após conferir as credencias do usuário, o servidor retorna uma mensagem de sucesso para o cliente. Uma vez autenticado o usuário envia uma operação de busca (*search*) – essa busca pode ser qualquer informação que consta na base do LDAP – e o servidor realiza a busca e retorna o resultado ao cliente. Após receber o resultado o cliente envia ao servidor um pedido de *unbind*, desejando se desconectar do servidor e o servidor por sua vez realiza a operação e desconecta o cliente do servidor (HOWES; SMITH; GOOD; 2003).

2.2.3. OpenLDAP

OpenLDAP é uma implementação do LDAP, ou seja, é um pacote do LDAP que contém recursos e softwares que o tornam funcional, prático e seguro. O projeto do OpenLDAP foi iniciado na Universidade de *Michigan* no ano de 1998. Seu projeto é OpenSource e está distribuído sobre a licença *Public License* e pode ser executado em vários sistemas operacionais como: Linux, Windows, MAC OS, entre outros.

As informações gerenciáveis e configurações do OpenLDAP são armazenadas em um estrutura de diretórios. Os arquivos LDIF permitem importar e

exportar informações da base do OpenLDAP. Esse arquivo é utilizado para adicionar, remover ou alterar entradas no diretório LDAP, por sua vez, cada entrada tem pelo menos uma classe de objeto definida. Este atributo de classe de objeto especifica um conjunto de atributos obrigatórios e opcionais para a entrada do diretório. A completa descrição do OpenLDAP vai além do escopo deste trabalho. Mais sobre esta implementação pode ser vista em (KURODA, 2011).

2.3. TRABALHOS RELACIONADOS

Analisando algumas monografias que tem um foco semelhante a este trabalho, nota-se que o foco principal delas é apresentar como o Kerberos e o LDAP podem ser integrados. A instalação de ambos são detalhadas pelos autores, como também suas configurações básicas. Uma restrição foi a instalação e configuração em um ambiente de rede simples, sem mostrar a interação com algum tipo de serviço. Dessa forma, não é possível analisar se o Kerberos e o LDAP apresentam resultados positivos para um ambiente de rede.

Em BERGAMASHI (2001), realizou a integração do Kerberos com o Active Directory da Microsoft, onde o Kerberos foi instalado em sistema operacional Linux quanto o Active Direcotory em um sistema operacional Windows Server, o objetivo principal era mostrar que é possível realizar a interoperabilidade entre os serviços, porém não verificou se implantar o Kerberos na rede é viável.

Em JUNIOR (2011), foi realizado a integração do Kerberos com o OpenLDAP, a integração ocorreu em um ambiente virtualizado, porém, somente foi abordado sobre o funcionamento e aplicação em uma rede, não abordando o impacto e vantagens na integração.

O diferencial desta monografia está em realizar uma análise mais detalhada, gerando e monitorando tráfego dos pacotes na rede, avaliando a situação da rede somente com Kerberos, somente com LDAP e depois com a solução integrada, viabiliza uma análise mais precisa das vantagens e desvantagens em realizar essa integração.

3. MATERIAIS E MÉTODOS

Neste capítulo são apresentados os materiais, cenários e procedimentos para a integração e análise do Kerberos com o OpenLDAP.

3.1. CENÁRIO

Os testes realizados nesta monografia foram feitos em um ambiente virtualizado, a Figura 04 mostra o cenário utilizado.

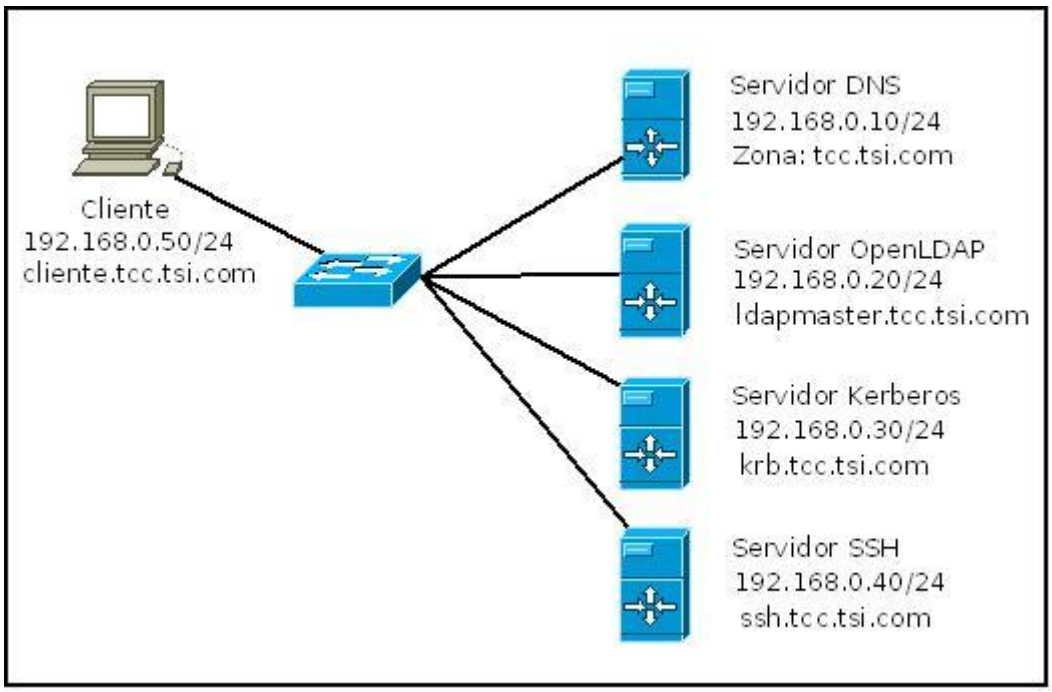

Figura 4 - Cenário para testes.

Foi utilizado um único computador para realizar os teste, neste computador foram instaladas as máquinas virtuais para a realização dos testes. Todas as máquinas virtuais estão utilizando como sistema operacional o Linux, a distribuição utilizada foi o Debian 6.0 “squeeze”. A Tabela 1 mostra a configuração do computador utilizado para rodar as máquinas virtuais.

	Real
Processador	Intel Core 2 Duo
Memória	2 GB

Tabela 1 - Configuração computador utilizado para rodas VMs.

Para as configurações foi necessária a instalação de um servidor DNS, cujo domínio era: **tcc.tsi.com**. A Tabela 02 mostra os *alias* que foram criados no DNS e a quais serviços eles pertencem, também foi necessário criar o mapeamento reverso.

Alias	Serviço
krb.tcc.tsi.com	Kerberos
ldapmaster.tcc.tsi.com	OpenLDAP
ssh.tcc.tsi.com	SSH
cliente.tcc.tsi.com	Cliente

Tabela 2 - Alias criados no servidor DNS.

3.2. MATERIAIS

A Tabela 03 mostra os softwares utilizados para a realização dos experimentos, assim como as versões utilizadas:

Programa	Versão
Debian	6
Virtual Box	4.1.2 r73507
OpenLDAP	2.4.23
Kerberos	5
SSH	2
Tcpdump	4.2.1
Wireshark	1.8.5
Bind	
NTP	

Tabela 3 - Softwares/Versões utilizadas

Como a infraestrutura da rede é virtualizada foi usada apenas uma máquina para realizar os experimentos. Os softwares utilizados são de código aberto.

3.3. MÉTODOS

Nesta seção é apresentado os métodos empregados para a configuração, instalação e análise dos resultados.

Foi realizada a instalação e configuração de um servidor OpenLDAP, tal servidor foi preparado para atender as necessidades do Kerberos, para tal, o *schema* do Kerberos foi adicionado ao serviço de diretórios.

Já com o servidor LDAP configurado e pronto, foi realizada a instalação e configuração do servidor Kerberos. Por padrão, o Kerberos utiliza uma base de dados local para armazenamento das informações, foi necessário a configuração para que o Kerberos utilize o OpenLDAP como *backend* para guardar as informações. O Anexo 1 documenta o arquivo de configuração.

A fim de testar os serviços foi necessário à instalação de um serviço remoto do Linux, o SSH. Por padrão o SSH vem com a opção de autenticação via Kerberos desativada, para que funcione utilizando o Kerberos como autenticador, foi preciso realizar algumas alterações em seu arquivo de configuração. O Anexo 7 mostra o arquivo de configuração completo do SSH.

Para um melhor resultado sobre a integração do OpenLDAP com o Kerberos, foi feito a captura de pacotes em quatro cenários diferentes, são eles:

- Autenticação de um usuário via SSH, sem utilização do Kerberos e OpenLDAP;
- Autenticação de um usuário via SSH, utilizando somente o OpenLDAP;
- Autenticação de um usuário via SSH, utilizando somente o Kerberos;
- Autenticação de um usuário via SSH, com o Kerberos e o OpenLDAP.

Para a realização dos testes foram utilizadas duas ferramentas: uma para realizar a captura de pacotes, o **tcpdump** e outra para analisar os resultados obtidos com o **tcpdump** chamada **Wireshark**.

Para cada etapa foram executados 30 testes, dos quais foram analisadas a quantidade de pacotes transmitidos e a quantidade de bytes, após reunir as informações foi gerado a média e o desvio padrão para cada etapa.

Os capítulos 4 e 5 apresentam os experimentos e análises da integração de um serviço de acesso remoto, SSH, com os protocolos Kerberos e OpenLDAP.

4. INTEGRAÇÃO DOS SERVIÇOS COM KERBEROS E OPENLDAP

Neste capítulo é abordado a integração de um serviço de acesso remoto, SSH, com os protocolos Kerberos e OpenLDAP. A integração de ambos aumenta o nível de segurança e otimiza o gerenciamento de usuários.

A integração consiste em manter o LDAP como *backend* para o Kerberos, para que ele possa realizar as consultas e verificar a autenticidade dos usuários.

Os comandos usados para instalação e configuração são padrões nas distribuições Linux Debian. A instalação e configuração dos procedimentos foram baseados nos tutoriais disponibilizados por OCELIC (2007, 2008).

Existem alguns pré-requisitos que devem ser atendidos antes da integração dos serviços, que são a utilização de um servidor DNS e um servidor NTP. Todas as máquinas envolvidas na integração devem possuir *Fully Qualified Domain Names* (FQDNs) únicos e definidos. Já a instalação de um servidor para sincronização dos relógios, se dá pelo fato que os *tickets* utilizados pelo Kerberos possuem um tempo de expiração, sendo assim se faz necessário que todas as máquinas envolvidas estejam com os relógios sincronizados (JUNIOR, 2011).

4.1. INSTALANDO E CONFIGURANDO O OPENLDAP

A instalação do servidor OpenLDAP requer dois pacotes: *slapd* e *ldap-utils*, respectivamente são: o servidor OpenLDAP e um conjunto de programas que auxiliam na configuração do servidor. O comando utilizado para a instalação destes pacotes é ilustrado na Figura 05:

```
~# apt-get install slapd ldap-utils
```

Figura 5 - Comando para instalação do OpenLDAP..

Durante a instalação do OpenLDAP são solicitadas informações essenciais para a configuração do servidor. A Tabela 04 mostra as informações que são pedidas e as respectivas informações informadas:

Pergunta	Resposta
Omitir a configuração do servidor OpenLDAP ?	Não
Nome do domínio DNS:	tcc.tsi.com
Nome da organização:	tcc.tsi.com
Senha de administrados:	ciscoldap
Confirmar senha:	ciscoldap
Banco de dados usado para Backend:	HDB
Voce quer que o banco de dados é removido quando o slapd for removido ?	Não
Permitir protocolo LDAPv2 ?	Não

Tabela 4 - Informações solicitadas no momento da instalação do OpenLDAP.

Após a instalação do OpenLDAP no servidor Debian, é necessário fazer a configuração do mesmo. O primeiro arquivo que é preciso ser configurado é o **ldap.conf**, fica localizado no diretório: **/etc/ldap/**. Neste arquivo foi informada a base do LDAP e a URI do servidor.

```
...
BASE dc=tcc,dc=tsi,dc=com
URI  ldap://ldapmaster.tcc.tsi.com
SASL_MECH GSSAPI
...
```

Figura 6 - Configuração arquivo ldap.conf.

Logo após configurar o arquivo **ldap.conf**, verifica-se a existência do arquivo **slapd.conf**. O arquivo pode ser encontrado no diretório **/etc/ldap**, caso não esteja neste diretório, pode ser encontrado no diretório **/usr/share/slapd**. Se for este o caso, será preciso copiar o arquivo do diretório **/usr/share/slapd** para o diretório **/etc/ldap.**

Com a configuração do **ldap.conf** feita, servidor OpenLDAP está pronto para ser utilizado. No entanto, para que ele seja capaz de armazenar as chaves de *principals*, alguns ajustes adicionais são necessários. A instalação padrão do OpenLDAP não possui o *schema* que contêm o modelo de dados do Kerberos, desta forma, faz-se necessária a instalação de um pacote que contém o *schema* do Kerberos, a Figura 08 mostra o comando responsável por instalar o pacote que contém este *schema*:

```
~# apt-get install krb5-kdc-ldap
```

Figura 7 - Instalação do pacote para obter *schemas* do Kerberos.

Após a instalação do pacote, foi necessário executar alguns comandos que converte o arquivo de *schema* do Kerberos para um arquivo LDIF. Os comandos são apresentados na Figura 08.

```
~# gunzip -c /usr/share/doc/krb5-kdc-ldap/kerberos.schema
~# echo "include /etc/ldap/schema/kerberos.schema" \
~/converte_schema.conf
~# mkdir ~/LDIF
~# slapcat -f ~/converte_schema.conf -F ~/LDIF -s \
"cn=kerberos,cn=schema,cn=config"
~# cp ~/LDIF/cn\=config/cn\=schema/cn\=\{0\}kerberos.ldif \
~/kerberos.ldif
```

Figura 8 - Comandos para converter *schema* para arquivo LDIF.

Em seguida é necessário alterar o arquivo que foi convertido para LDIF, neste caso o arquivo: **~/kerberos.ldif**. A primeira alteração é nas primeiras linhas do arquivo (Figura 09):

```
dn: cn=kerberos,cn=schema,cn=config
objectClass: olcSchemaConfig
cn: kerberos
...
```

Figura 9 - Primeira edição do arquivo ~/kerberos.ldif.

Continuando com a edição do arquivo **~/kerberos.ldif**, é necessário remover alguns atributos no final do arquivo (Figura 10):

```
structuralObjectClass: olcSchemaConfig
entryUUID: 881712a-7dd3-104e-9910-22041e820f8810
creatorsName: cn=config
createTimestamp: 201304141519Z
entryCSN: 201304141519.176097Z#000000#000#000000
modifiersName: cn=config
modifyTimestamp: 201304141519Z
```

Figura 10 - Segunda edição do arquivo ~/kerberos.ldif, atributos a serem removidos.

Feitas estas configuração foi adicionado o *schema* do Kerberos a *cn=config*, para isso foi utilizado o seguinte comando (Figura 11):

```
~# ldapadd -QY EXTERNAL -H ldapi:/// -f ~/kerberos.ldif
```

Figura 11- Adicionando o *schema* do Kerberos a cn=config.

Com o *schema* do Kerberos já adicionado no OpenLDAP, é necessária a criação de alguns usuários e grupos que posteriormente serão utilizados na configuração do Kerberos, para tal, foi criado um arquivo: **~/krb5.ldif** como seguinte conteúdo:

```
dn: ou=krb5,dc=tcc,dc=tsi,dc=com
ou: krb5
objectClass: organizationalUnit

dn: cn=kdc-srv,ou=krb5,dc=tcc,dc=tsi,dc=com
cn: kdc-srv
objectClass: simpleSecurityObject
objectClass: organizationalRole
description: Utilizado no servidor KDC Kerberos
userPassword: kdckdc

dn: cn=adm-srv,ou=krb5,dc=tcc,dc=tsi,dc=com
cn: adm-srv
objectClass: simpleSecurity
objectClass: organizationalRole
description: Utilizado no servidor AS Kerberos
userPassword admadm
```

Figura 12 - Arquivo com usuários e grupos para configuração do Kerberos.

Após criação do arquivo é necessário adicionar o mesmo ao OpenLDAP, para tal é utilizado o seguinte comando:

```
~# ldapadd -xWD cn=admin,dc=tcc,dc=tsi,dc=com -f ~/krb5.ldif
```

Figura 13 - Adicionando o arquivo krb5.ldif ao servidor OpenLDAP.

É necessária a criação de mais dois grupos (*pessoas* e *grupos*), estes serão responsáveis por guardar os usuários utilizados pelo Kerberos, para tal foi criado o

arquivo **usuarios-grupos.ldif**, segue seu conteúdo:

```
dn: ou=usuarios,dc=tcc,dc=tsi,dc=com
objectClass: organizationalUnit
ou: usuarios

dn: ou=grupos,dc=tcc,dc=tsi,dc=com
objectClass: organizationalUnit
ou: grupos
```

Figura 14 - Conteúdo do arquivo usuários-grupos.ldif.

Após criação do arquivo é necessário adicionar o mesmo ao OpenLDAP, para tal é utilizado o seguinte comando:

```
~# ldapadd -xWD cn=admin,dc=tcc,dc=tsi,dc=com -f \
~/pessoas-grupos.ldif
```

Figura 15 - Adicionando o arquivo pessoas-grupos.ldif ao servidor OpenLDAP.

Enfim, com todas estas mudanças que foram feitas na configuração do OpenLDAP, o *deamon* responsável pelo serviço deve ser reiniciado para que as novas configurações entrem em vigor, para tal utiliza-se o comando:

```
~# /etc/init.d/slapd restart
```

Figura 16 - Comando para reiniciar o serviço OpenLDAP.

4.2. INSTALANDO E CONFIGURANDO O KERBEROS

Para instalação do Kerberos são necessários os pacotes: *krb5-admin-server* e *krb5-kdc*. Durante a instalação padrão no Debian, serão perguntadas algumas informações, a Tabela 05 mostra as perguntas e as respectivas informações concedidas:

Pergunta	Resposta
Reino padrão do Kerberos: (Geralmente nome do domínio em maiúsculo)	TCC.TSI.COM
Servidor Kerberos para o reino:	krb.tcc.tsi.com
Servidor administrativo para o reino:	krb.tcc.tsi.com

Tabela 5 - Informações solicitadas no momento da instalação do Kerberos.

O servidor Kerberos só trabalha com nomes de domínio, caso seja informado no momento da configuração um endereço IP o mesmo não funcionará. Foi utilizado o endereço **krb.tcc.tsi.com** que é um *alias* para o servidor do Kerberos.

Após terminar a instalação foi necessário criar o reino, uma vez que já foi informado o nome que deseja para o reino no momento da instalação, o próximo passo é utilizar o comando para a criação do reino:

```
~# kdb5_ldap_util –D cn=admin,dc=tcc,dc=tsi,dc=com \
–H ldap://ldapmaster.tcc.tsi.com –r TCC.TSI.COM -s
```

Figura 17 - Comando para criação do reino no Kerberos.

Com o reino criado, o próximo passo é fazer as alterações no arquivo responsável pela configuração do Kerberos, o **krb5.conf**, o arquivo fica localizado no diretório: ***/*etc**. O arquivo é dividido em algumas partes:

Sessão	Descrição
[libdefaults]	Configuração das bibliotecas do Kerberos.
[realms]	Configuração das informações para contato com reino.
[domain_realm]	Mapeamento do reino.
[logging]	Configuração de arquivos de *log*.
[dbdefaults]	Configuração padrão da base de dados.
[dbmodules]	Definições para a base de dados.

Tabela 6 - Divisões no arquivo de configuração do Kerberos, krb5.conf.

Durante a instalação do Kerberos foram informados alguns dados, estes dados estão no arquivo de configuração do Kerberos, porém ainda é necessário algumas alterações. Foram acrescentadas algumas informações nas sessões: *[realms], [domain_realm]*, *[logging], [dbdefaults]* e *[dbmodules]*:

```
[realms]
      TCC.TSI.COM = {
            kdc = krb.tcc.tsi.com
```

```
            admin_server = krb.tcc.tsi.com
            database_modules = openldap_ldapconf
      }

[domain_realm]
      tcc.tsi.com = TCC.TSI.COM
      .tcc.tsi.com = TCC.TSI.COM

[dbdefaults]
      ldap_kerberos_container_dn = ou=krb5,dc=tcc,dc=tsi,dc=com

[dbmodules]
      openldap_ldapconf = {
            db_library = kldap
            ldap_kdc_dn = cn=kdc-srv,ou=krb5,dc=tcc,dc=tsi,dc=com
            ldap_kadmind_dn = cn=adm-srv,ou=krb5,dc=tcc,dc=tsi,dc=com
            ldap_service_password_file = /etc/krb5kdc/service.keyfile
            ldap_servers = ldap://ldapmaster.tcc.tsi.com
            ldap_conns_per_server = 5
      }

[logging]
            kdc = FILE:/var/log/kerberos/krb5kdc.log
            admin_server = FILE:/var/log/kerberos/kadmin.log
            default = FILE:/var/log/kerberos/krb5lib.log
```

Figura 18 - Alterações no arquivo de configurações do Kerberos, krb5.conf.

Com as alterações feitas, foi criado um diretório: **kerberos**, no seguinte diretório: **/var/log**, este diretório será responsável por guardar os arquivos de *log* gerado pelo servidor Kerberos. Outro detalhe é conceder ao usuário **admin** todos os privilégios. O arquivo responsável por esta configuração é o **kadmin5.acl**, localizado no seguinte diretório **/etc/krb5kdc**. Foi retirado o caractere # da linha que contém a expressão: ***/admin /**.

Com as configurações realizadas, precisa-se reiniciar os serviços para que as configurações entrem em vigor, para tal foi utilizado os comandos:

```
~# invoke-rc.d krb5-admin-server restart
~# invoke-rc.d krb5-kdc restart
```

Figura 19 - Comandos para reiniciar serviços do Kerberos.

Com os serviços reiniciados, a próxima etapa foi a criação de um usuário administrador para o Kerberos, para tal foi utilizado alguns comandos, como mostra Figura 20:

```
~# kadmin.local
kadmin.local:  addprinc root/admin

WARNING: no policy specified for root/admin@TCC.TSI.COM; de-
faulting to no policy
Enter password for principal "root/admin@TCC.TSI.COM": PASS
Re-enter password for principal "root/admin@TCC.TSI.COM": PASS
Principal "root/admin@TCC.TSI.COM" created.

kadmin.local:  quit
```

Figura 20 - Comando para adicionar usuários root/admin.

O Kerberos utiliza um arquivo chamado **service.keyfile** para armazenar as senhas de duas entradas no LDAP que serão utilizados por ele, são elas:

- **cn=kdc-srv,ou=krb5,dc=tcc,dc=tsi,dc=com;**
- **cn=adm-srv,ou=krb5,dc=tcc,dc=tsi,dc=com.**

A criação deste arquivo é feita utilizando o comando:

```
~# kdb5_ldap_util -D cn=admin,dc=tcc,dc=tsi,dc=com stashsrvpw
-f /etc/krb5kdc/service.keyfile cn=kdc-
srv,ou=krb5,dc=tcc,dc=tsi,dc=com
```

Figura 21 - Comando para criar entrada da cn=kdc-srv no arquivo service.keyfile.

```
~# kdb5_ldap_util -D cn=admin,dc=tcc,dc=tsi,dc=com stashsrvpw
-f /etc/krb5kdc/service.keyfile cn=adm-
srv,ou=krb5,dc=tcc,dc=tsi,dc=com
```

Figura 22 - Comando para criar entrada da cn=adm-srv no arquivo service.keyfile.

Com estas configurações o servidor Kerberos já está apto a cadastrar novos usuários e/ou serviços utilizando um banco de dados do OpenLDAP como *backend*.

4.3. INSTALANDO E CONFIGURANDO SERVIÇOS

O serviço de acesso remoto SSH foi selecionado para avaliar a integração entre o Kerberos e o LDAP. Para a integração do SSH com o Kerberos foi preciso instalar alguns pacotes, são eles: *openssh-server*, *krb5-config*, *krb5-clients*, *krb5-user* e *openldap-clients*. A configuração dos arquivos referente ao Kerberos e ao LDAP são semelhantes às configurações já apresentadas anteriormente.

Para que o SSH faça sua autenticação utilizando o Kerberos é preciso fazer algumas alterações em seu arquivo de configuração, o: **sshd_config**, o mesmo fica localizado no diretório: **/etc/ssh**. A Figura 23 mostra os parâmetros que devem ser alterados no arquivo:

```
KerberosAuthentication yes
KerberosTicketCleanup yes
GSSAPIAuthentication yes
GSSAPICleanupCredentials Yes
PasswordAuthentication no
UserDNS yes
```

Figura 23 - Alterações no arqiuvo de configuração do SSH.

Após realizar estas configurações o próximo passo é adicionar o serviço no servidor do Kerberos, para tal é utilizado o seguinte comando:

```
~# kadmin.local
kadmin.local: addprinc –randkey host/ssh.tcc.tsi.com
kadmin.local: ktadd host/ssh.tcc.tsi.com
```

Figura 24 - Adicionando serviço SSH ao servidor Kerberos.

Com essas alterações o SSH já está apto a fazer sua autenticação no servidor Kerberos.

5. TESTES, ANÁLISE E DISCUSSÃO

Neste capítulo são apresentados os testes e análises feitos para se chegar aos objetivos deste trabalho.

Visando avaliar os impactos no tráfego em uma rede onde existe a integração do Kerberos com OpenLDAP foi realizada a captura dos pacotes de rede utilizando o **tcpdump**. A Figura 25 apresenta o comando utilizado para realizar as capturas.

```
~# tcpdump –i eth0 –s 65535 –w captura.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), cap-
ture size 65535 bytes
```

Figura 25 - Captura de pacotes.

O comando captura todo o tráfego de rede, a partir disto foram executados alguns comandos na máquina do cliente.

As capturas de pacotes foram realizadas em quatro etapas, sendo elas:

- **1ª Etapa:** tráfego de acesso direto ao serviço SSH, sem o Kerberos e sem o OpenLDAP;
- **2ª Etapa:** tráfego de acesso ao serviço SSH, utilizando somente o OpenLDAP, sem o Kerberos;
- **3ª Etapa:** tráfego de acesso ao serviço SSH, utilizando somente o Kerberos, sem o OpenLDAP;
- **4ª Etapa:** tráfego de acesso ao serviço SSH, utilizando o Kerberos e OpenLDAP.

A Figura 26 mostra o comando utilizado para testar a primeira e a segunda etapa, o acesso direto ao serviço SSH:

```
~# ssh henrique@ssh.tcc.tsi.com
Password for henrique@ssh: PASS
```

Figura 26 - Comandos para conectar diretamente ao serviço SSH.

A Figura 27 mostra o comando utilizado para testar a terceira e a quarta etapa, o comando **kinit** seguido do nome do usuário, realiza uma busca na base de dados do Kerberos (OpenLDAP), após realizar a busca é solicitado para o usuário que digite sua senha, após confirmar a senha, o Kerberos emite um *ticket* que será usado pelo usuário para realizar a autenticação nos serviços que estão "kerberizados", neste caso o SSH.

```
~# kinit henrique
Password for henrique@TCC.TSI.COM: PASS
~# ssh henrique@ssh.tcc.tsi.com
henrique@ssh:~# exit
logout
Connection to ssh.tcc.tsi.com closed.
```

Figura 27 - Comando para conectar ao serviço SSH.

Após executar estes comandos, foi interrompido o comando **tcpdump** que já estava sendo executado.

Foram realizados 30 testes para cada etapa, as Tabelas 7, 8, e 9 mostram algumas informações estatísticas referentes aos testes efetuados:

	MÉDIA		
	BYTES	**PACOTES**	**BYTES/SEG**
ETAPA 1	10237	63	427,986
ETAPA 2	13259	101	523,581
ETAPA 3	10928	71	1113,295
ETAPA 4	36147	182	3316,567

Tabela 7 - Média de Bytes, Pacotes e Bytes/Seg capturados.

	DESVIO PADRÃO		
	BYTES	PACOTES	BYTES/SEG
ETAPA 1	437,45	2,69	18,29
ETAPA 2	455,02	3,46	17,97
ETAPA 3	487,94	3,16	49,71
ETAPA 4	466,85	2,35	42,83

Tabela 8 - Desvio padrão das Etapas.

	Tempo médio entre primeiro e último pacote (segundos)
ETAPA 1	5,375
ETAPA 2	8,454
ETAPA 3	6,725
ETAPA 4	10,857

Tabela 9 - Tempo médio (segundos) entre primeiro e último pacote.

O Gráfico 01 apresenta a média de pacotes por cada protocolo:

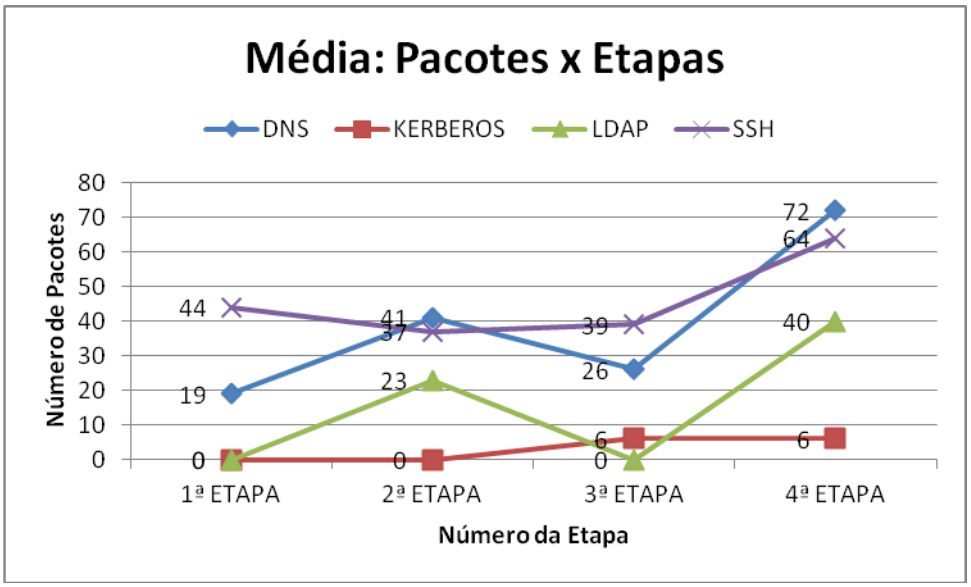

Gráfico 1 - Média de pacotes: Etapa x Protocolo.

Observando o Gráfico 01, verifica-se um aumento expressivo de pacotes DNS. Isso se deve ao fato de que são realizadas muitas consultas ao servidor DNS, pois todas as máquinas envolvidas no processo devem possuir FQDNs definidos,

porém não interfere, pois as consultas são locais, uma solução para eliminar o tráfego de DNS na rede é a utilização do arquivo *hosts*, onde pode ser feito o mapeamento de nomes sem a utilização de um servidor DNS.

Os Gráficos 02 e 03 apresentam a porcentagem de pacotes e bytes com e sem DNS, de uma única amostra dos testes realizados.

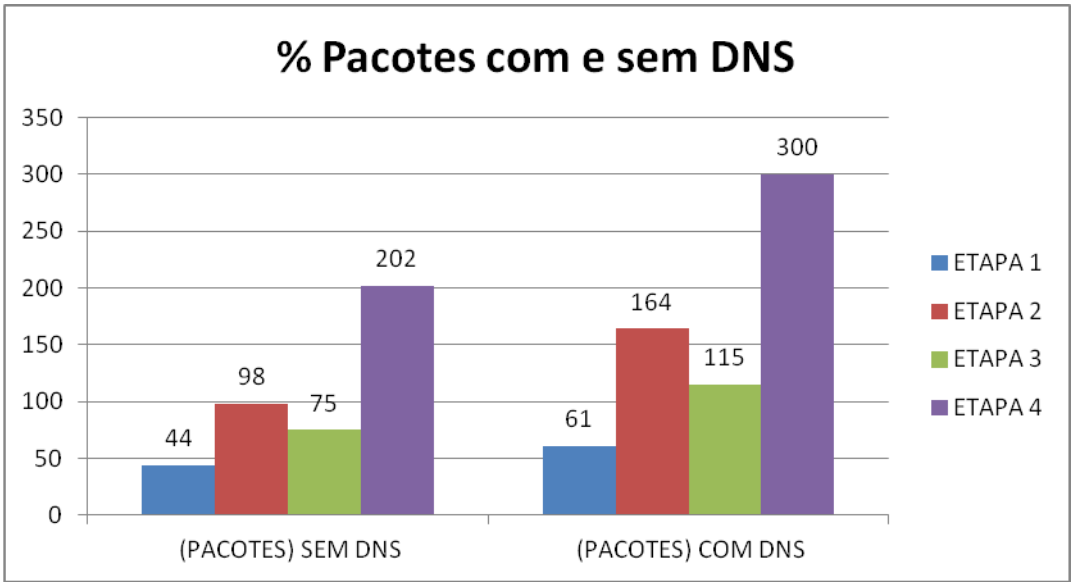

Gráfico 2 - % de Pacotes com e sem DNS.

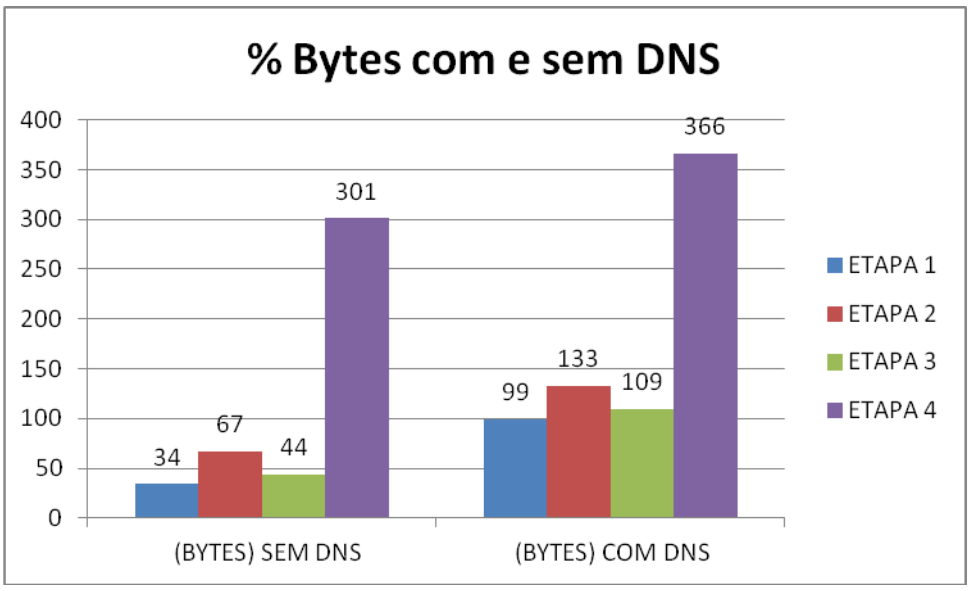

Gráfico 3 - % Bytes com e sem DNS.

O Gráfico 04, apresenta o número de pacotes capturado em cada teste, para melhor visualização dos dados veja os Anexos 08, 09, 10 e 11.

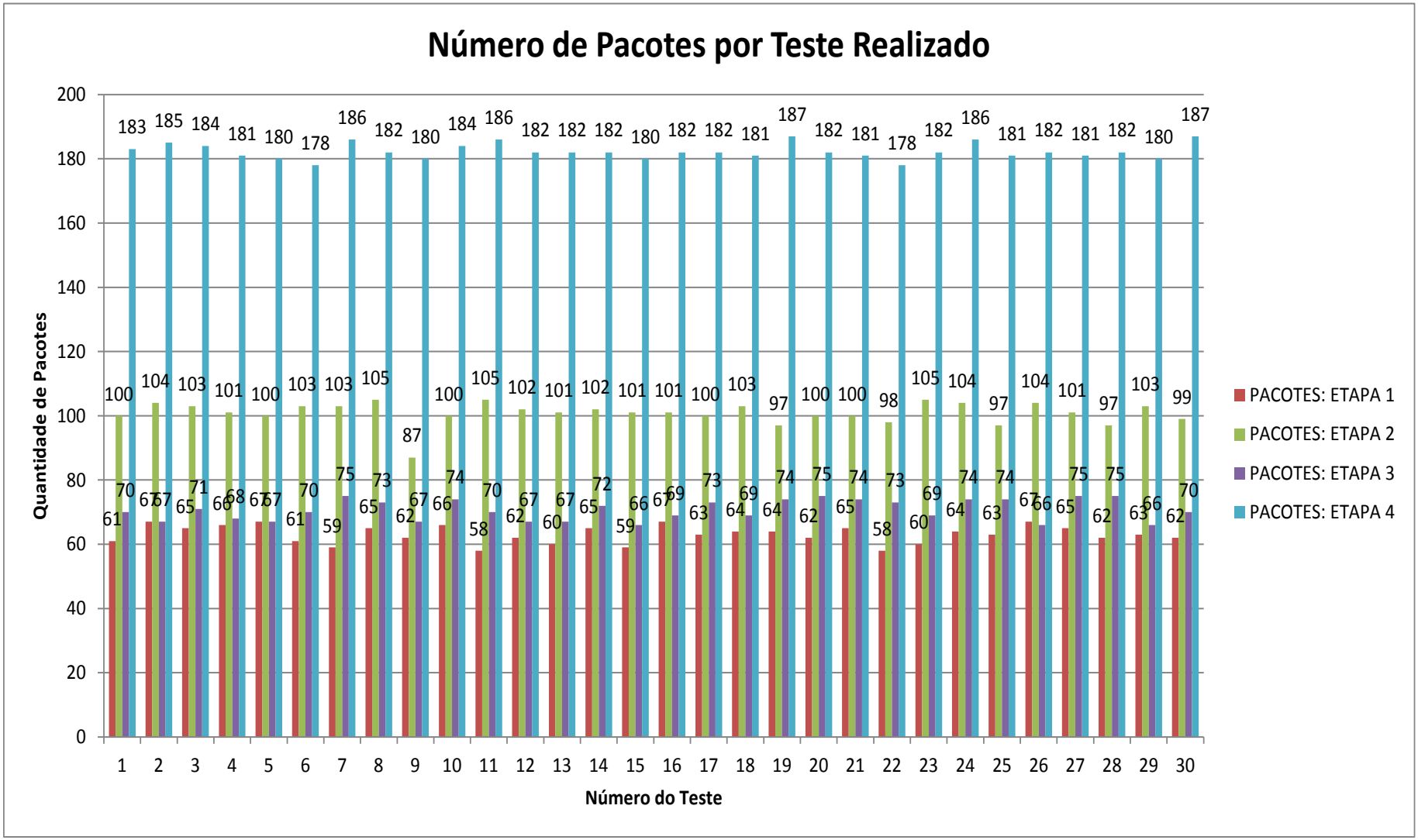

Gráfico 4 - Número de pacotes por teste realizado.

	MÉDIA				
	BYTES	**PACOTES**	**BYTES/SEG**	**% AUMENTO (BYTES)**	**% AUMENTO (PACOTES)**
ETAPA 1	10237	63	427,986		
ETAPA 2	13259	101	523,581	130%	160%
ETAPA 3	10928	71	1113,295	107%	112%
ETAPA 4	36147	182	3316,567	353%	289%

Tabela 10 - % de aumento dos Bytes e Pacotes, considerando pacotes DNS.

Já na Tabela 10 pode-se observar que a integração do Kerberos e OpenLDAP afeta de forma significativa o tráfego de pacotes na rede, pois o aumento de pacotes passa de 300% e o aumento de Bytes fica em aproximadamente 350%. Tal análise foi realizada considerando os pacotes DNS, se desconsiderados os pacotes DNS podemos chegar à conclusão de que o Kerberos com OpenLDAP não afeta o tráfego da rede, pois os pacotes DNS não interferem na rede pois suas consultas são locais.

5.1. VANTAGENS DA INTEGRAÇÃO

Existem diversas vantagens com a integração dos serviços. Tanto o OpenLDAP quanto o Kerberos tendem a centralização, seja ela por autenticação e/ou autorização, a rapidez pelo qual o LDAP faz as consultas de seus dados e a forma que o LDAP faz a organização dos dados, somam pontos para sua integração com o Kerberos.

5.2. DESVANTAGENS DA INTEGRAÇÃO

A utilização do Kerberos tende a eliminar diversas brechas na segurança, porém uma desvantagem é referente ao tempo de vida dos *tickets*, uma vez que é configurado com um tempo muito grande o mesmo está sujeito a ser interceptado e assim dando chance a um invasor de comprometer a rede, caso o tempo seja muito curto, irá levar ao usuário ficar redigitando sua senha com mais frequência.

6. CONCLUSÃO

A instalação, configuração e integração de um serviço de acesso remoto SSH ao Kerberos e ao OpenLDAP apresentou-se como uma tarefa complexa, pois ambos os serviços possuem uma configuração um tanto quanto complexa. Foi verificado que o tráfego na rede foi aumentado em mais de 300% quando se fez a integração, devido a um aumento significativo do tráfego do DNS, o que não ocasiona um problema, pois as consultas são locais, uma solução para eliminar o tráfego de DNS na rede é a utilização do arquivo *hosts.*

Verificou-se que a integração aumenta a segurança e não afeta significativamente os serviços e o tráfego de rede. Quanto a segurança que o Kerberos provê à rede, não fica dúvidas que sua aplicação é extremamente necessária quando se pretende prover um nível a mais de segurança a uma rede. Uma das vantagens da utilização do Kerberos é que a senha nunca é enviada pela rede durante a autenticação e a utilização do OpenLDAP se dá pelo fato de que um diretório é otimizado para consultas, tornando as respostas muito mais rápidas.

A instalação e configuração do Kerberos juntamente com o OpenLDAP foram explorados de maneira superficial, embora suas configurações sejam complexas a integração destes serviços é extremamente viável, uma vez que provê mais segurança a rede tornando os serviços "kerberizados" mais seguros e confiáveis.

O foco principal deste trabalho foi a análise da integração dos serviços e seu impacto numa rede, utilizando somente um serviço integrado ao Kerberos com OpenLDAP. Um cenário interessante para testes seriam vários servidores Kerberos atuando em uma rede com diversos serviços sendo "kerberizados", também a realização de testes com o Kerberos e o Active Directory da Microsoft Estes podem ser utilizados como trabalhos futuros.

REFERÊNCIAS

BERGAMASHI, Rafael J. P. **Interoperabilidade com Kerberos + Samba + LDAP + Active Directory.** 2011. Monografia (Especialista em Administração em Redes Linux) – Universidade Federal de Lavras, Lavras, 2011.

CARTER, Gerald. **LDAP - Administração de Sistemas.** São Paulo: Alta Books, 2009. 280 p. ISBN 9788576083139

COULOURIS, George; DOLLIMORE, Jean; KINDBERG, Tim; **Sistemas Distribuídos: Conceitos e Projeto.** São Paulo: Bookman, 2007. 784 p. ISBN 9788560031498

GERMAN, Jason. **Kerberos: The Definitive Guide.** Cambridge: O'Reilly Media, 2003. 272 p. ISBN 0596004036

JORDÃO, Leonardo de. B. **Uso do Protocolo de Autenticação Kerberos em Redes Linux.** 2005. Monografia (Especialista em Administração em Redes Linux) – Universidade Federal de Lavras, Lavras, 2005.

KURODA, Rodrigo Takashi. **Identificação dos Recursos de Software que Causam Impacto no Desempenho de Perfil Móvel em LDAP.** 2011. Monografia (Tecnólogo em Sistemas para Internet) – Universidade Tecnológica Federal do Paraná, Campo Mourão, 2011.

JUNIOR, Wagner A. de. **Kerberos com Backend LDAP: Análise e Implantação.** 2011. Monografia (Especialista em Administração em Redes Linux) – Universidade Federal de Lavras, Lavras, 2011.

MACHADO, Erich S.; JUNIOR, Flavio de. S. M. **Autenticação Integrada Baseada em Serviços de Diretório LDAP.** 2006. TCC – Instituto de Matemática e Estatística, 2006.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY - MIT MUSEUM**,** Kerberos: The Network Authentication Protocol. Disponível em: <http://web.mit.edu/kerberos> Acesso em 08 out. 2011.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY - MIT MUSEUM**,** Project Athena. Disponível em: <http://museum.mit.edu/150/26> Acesso em 08 out. 2011.

MIHALIK, Aeron D. Projetct Athena. Cambridge, Massachusetts, 1999. Disponível em: <http://tech.mit.edu/V119/N19/history_of_athe.19f.html> . Acesso em: 09 out. 2011.

PAES, Lucas M. J. A.; ALBUQUERQUE, Priscila P. B. Kerberos: Um breve resumo. Jan. 2007. Disponível em: <http://www.gta.ufrj.br/grad/07_1/kerberos/index.html>. Acesso em: 14 nov. 2011.

RICCIARDI, Fulvio. Kerberos protocol tutorial, Lecce, Italy. nov. 2007. Disponível em: <http://www.kerberos.org/software/tutorial.html>. Acesso em: 09 out. 2011.

STALLINGS, William. **Criptografia e segurança de redes: Princípios e práticas.** New Jersey: Prentice Hall, 2008. 512 p. ISBN 9788576051190

TANENBAUM, Andrew S. **Redes de Computadores.** São Paulo: Editora Campus, 2003. 968 p. ISBN 8535211853

TRIGO, C. H. **OpenLDAP - Uma Abordagem Integrada**. 1. ed. São Paulo: Novatec, 2007.

HOWES, Tim; SMITH, Mark; GOOD, Gordon S. **Understanding and Deploying LDAP Directory Services**, 2. ed, Ed. Addison Wesley, 2003. 899 p. ISBN 9780672323164

OCELIC, Davor. OpenLDAP installation on Debian, mar. 2008. Disponível em: <http://www.debian-administration.org/article/OpenLDAP_installation_on_Debian>. Acesso em: 05 mar. 2013.

OCELIC, Davor. MIT Kerberos installation on Debian, dez. 2007. Disponível em: <http://www.debian-administration.org/articles/570>. Acesso em: 05 mar. 2013.

Integrated Kerberos-OpenLDAP provider on Debian squeeze, ago. 2012. Disponível em: <http://www.rjsystems.nl/en/2100-d6-kerberos-openldap-provider.php>. Acesso em: 06 mar. 2013.

ANEXO 01

Arquivo **krb5.conf** completo, referente a configuração do Kerberos.

```
[libdefaults]
    default_realm = TCC.TSI.COM

# The following krb5.conf variables are only for MIT Kerberos.
    krb4_config = /etc/krb.conf
    krb4_realms = /etc/krb.realms
    kdc_timesync = 1
    ccache_type = 4
    forwardable = true
    proxiable = true

# The following encryption type specification will be used by MIT Kerberos
# if uncommented.  In general, the defaults in the MIT Kerberos code are
# correct and overriding these specifications only serves to disable new
# encryption types as they are added, creating interoperability problems.
#
# Thie only time when you might need to uncomment these lines and change
# the enctypes is if you have local software that will break on ticket
# caches containing ticket encryption types it doesn't know about (such as
# old versions of Sun Java).

#   default_tgs_enctypes = des3-hmac-sha1
#   default_tkt_enctypes = des3-hmac-sha1
#   permitted_enctypes = des3-hmac-sha1

# The following libdefaults parameters are only for Heimdal Kerberos.
    v4_instance_resolve = false
    v4_name_convert = {
        host = {
            rcmd = host
            ftp = ftp
        }
        plain = {
            something = something-else
        }
    }
    fcc-mit-ticketflags = true

[realms]
    TCC.TSI.COM = {
        kdc = krb.tcc.tsi.com
        admin_server = krb.tcc.tsi.com
        database_module = openldap_ldapconf
    }

[domain_realm]
    .tcc.tsi.com = TCC.TSI.COM
    tcc.tsi.com = TCC.TSI.COM

[dbdefaults]
    ldap_kerberos_container_dn = ou=krb5,dc=tcc,dc=tsi,dc=com

[dbmodules]
    openldap_ldapconf = {
```

```
        db_library = kldap
        ldap_kdc_dn = cn=kdc-srv,ou=krb5,dc=tcc,dc=tsi,dc=com
        ldap_kadmind_dn = cn=adm-srv,ou=krb5,dc=tcc,dc=tsi,dc=com
        ldap_service_password_file = /etc/krb5kdc/service.keyfile
        ldap_servers = ldap://ldapmaster.tcc.tsi.com
        ldap_conns_per_server = 5
    }

[login]
    krb4_convert = true
    krb4_get_tickets = false

[logging]
    kdc = FILE:/var/log/kerberos/krb5kdc.log
    admin_server = FILE:/var/log/kerberos/kadmin.log
    default = FILE:/var/log/kerberos/krb5lib.log
```

ANEXO 02

Arquivo **kdc.conf** completo, referente a configuração do Kerberos.

```
[kdcdefaults]
    kdc_ports = 750,88

[realms]
    TCC.TSI.COM = {
        database_name = /var/lib/krb5kdc/principal
        admin_keytab = FILE:/etc/krb5kdc/kadm5.keytab
        acl_file = /etc/krb5kdc/kadm5.acl
        key_stash_file = /etc/krb5kdc/stash
        kdc_ports = 750,88
        max_life = 1d 0h 0m 0s
        max_renewable_life = 90d 0h 0m 0s
        master_key_type = des3-hmac-sha1
        supported_enctypes = aes256-cts:normal arcfour-hmac:normal des3-
hmac-sha1:normal des-cbc-crc:normal des:normal des:v4 des:norealm
des:onlyrealm des:afs3
        default_principal_flags = +preauth
    }
```

ANEXO 03

Arquivo **kadmin.acl** completo, referente a configuração do Kerberos.

```
# This file Is the access control list for krb5 administration.
# When this file is edited run /etc/init.d/krb5-admin-server restart to ac-
tivate
# One common way to set up Kerberos administration is to allow any princi-
pal
# ending in /admin  is given full administrative rights.
# To enable this, uncomment the following line:
*/admin *
```

ANEXO 04

Arquivo **service.keyfile** completo, referente a configuração do Kerberos.

```
cn=kdc-srv,ou=krb5,dc=tcc,dc=tsi,dc=com#{HEX}636973636f6c646170
cn=adm-srv,ou=krb5,dc=tcc,dc=tsi,dc=com#{HEX}636973636f6c646170
cn=admin,dc=tcc,dc=tsi,dc=com#{HEX}636973636f6c646170
```

ANEXO 05

Arquivo **ldap.conf** completo, referente a configuração do OpenLDAP.

```
#
# LDAP Defaults
#

# See ldap.conf(5) for details
# This file should be world readable but not world writable.

BASE        dc=tcc,dc=tsi,dc=com
URI         ldap://localhost
SASL_MECH   GSSAPI

#SIZELIMIT  12
#TIMELIMIT  15
#DEREF      never
```

ANEXO 06

Arquivo **sldap.conf** completo, referente a configuração do OpenLDAP.

```
# This is the main slapd configuration file. See slapd.conf(5) for more
# info on the configuration options.

########################################################################
# Global Directives:

# Features to permit
#allow bind_v2

# Schema and objectClass definitions
include         /etc/ldap/schema/core.schema
include         /etc/ldap/schema/cosine.schema
include         /etc/ldap/schema/nis.schema
include         /etc/ldap/schema/inetorgperson.schema
include         /etc/ldap/schema/kerberos.schema

# Where the pid file is put. The init.d script
# will not stop the server if you change this.
pidfile         /var/run/slapd/slapd.pid

# List of arguments that were passed to the server
argsfile        /var/run/slapd/slapd.args

# Read slapd.conf(5) for possible values
loglevel        256

# Where the dynamically loaded modules are stored
modulepath  /usr/lib/ldap
moduleload  back_@BACKEND@

# The maximum number of entries that is returned for a search operation
sizelimit 500

# The tool-threads parameter sets the actual amount of cpu's that is used
# for indexing.
tool-threads 1

########################################################################
# Specific Backend Directives for @BACKEND@:
# Backend specific directives apply to this backend until another
# 'backend' directive occurs
backend     @BACKEND@

########################################################################
# Specific Backend Directives for 'other':
# Backend specific directives apply to this backend until another
# 'backend' directive occurs
#backend        <other>

########################################################################
# Specific Directives for database #1, of type @BACKEND@:
# Database specific directives apply to this databasse until another
# 'database' directive occurs
database        @BACKEND@
```

```
# The base of your directory in database #1
suffix          "@SUFFIX@"

# rootdn directive for specifying a superuser on the database. This is nee-
ded
# for syncrepl.
# rootdn          "cn=admin,@SUFFIX@"

# Where the database file are physically stored for database #1
directory       "/var/lib/ldap"

# The dbconfig settings are used to generate a DB_CONFIG file the first
# time slapd starts.  They do NOT override existing an existing DB_CONFIG
# file.  You should therefore change these settings in DB_CONFIG directly
# or remove DB_CONFIG and restart slapd for changes to take effect.

# For the Debian package we use 2MB as default but be sure to update this
# value if you have plenty of RAM
dbconfig set_cachesize 0 2097152 0

# Sven Hartge reported that he had to set this value incredibly high
# to get slapd running at all. See http://bugs.debian.org/303057 for more
# information.

# Number of objects that can be locked at the same time.
dbconfig set_lk_max_objects 1500
# Number of locks (both requested and granted)
dbconfig set_lk_max_locks 1500
# Number of lockers
dbconfig set_lk_max_lockers 1500

# Indexing options for database #1
index           objectClass eq
index           uid eq

# Save the time that the entry gets modified, for database #1
lastmod         on

# Checkpoint the BerkeleyDB database periodically in case of system
# failure and to speed slapd shutdown.
checkpoint      512 30

# The userPassword by default can be changed
# by the entry owning it if they are authenticated.
# Others should not be able to see it, except the
# admin entry below
# These access lines apply to database #1 only
access to attrs=userPassword,shadowLastChange
        by dn="@ADMIN@" write
        by anonymous auth
        by self write
        by * none

# Ensure read access to the base for things like
# supportedSASLMechanisms.  Without this you may
# have problems with SASL not knowing what
# mechanisms are available and the like.
# Note that this is covered by the 'access to *'
# ACL below too but if you change that as people
# are wont to do you'll still need this if you
```

```
# want SASL (and possible other things) to work
# happily.
access to dn.base="" by * read

# The admin dn has full write access, everyone else
# can read everything.
access to *
        by dn="@ADMIN@" write
        by * read

# For Netscape Roaming support, each user gets a roaming
# profile for which they have write access to
#access to dn=".*,ou=Roaming,o=morsnet"
#        by dn="@ADMIN@" write
#        by dnattr=owner write

#######################################################################
# Specific Directives for database #2, of type 'other' (can be @BACKEND@
too):
# Database specific directives apply to this databasse until another
# 'database' directive occurs
#database        <other>

# The base of your directory for database #2
#suffix     "dc=debian,dc=org"
export  KRB5_KTNAME=/etc/krb5.keytab
```

ANEXO 07

Arquivo **sshd_config** completo, referente a configuração do SSH.

```
# Package generated configuration file
# See the sshd_config(5) manpage for details

# What ports, IPs and protocols we listen for
Port 22
# Use these options to restrict which interfaces/protocols sshd will bind
to
#ListenAddress ::
#ListenAddress 0.0.0.0
Protocol 2
# HostKeys for protocol version 2
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
#Privilege Separation is turned on for security
UsePrivilegeSeparation yes

# Lifetime and size of ephemeral version 1 server key
KeyRegenerationInterval 3600
ServerKeyBits 768

# Logging
SyslogFacility AUTH
LogLevel INFO

# Authentication:
LoginGraceTime 120
PermitRootLogin yes
StrictModes yes

RSAAuthentication yes
PubkeyAuthentication yes
#AuthorizedKeysFile %h/.ssh/authorized_keys

# Don't read the user's ~/.rhosts and ~/.shosts files
IgnoreRhosts yes
# For this to work you will also need host keys in /etc/ssh_known_hosts
RhostsRSAAuthentication no
# similar for protocol version 2
HostbasedAuthentication no
# Uncomment if you don't trust ~/.ssh/known_hosts for RhostsRSAAuthentica-
tion
#IgnoreUserKnownHosts yes

# To enable empty passwords, change to yes (NOT RECOMMENDED)
PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
ChallengeResponseAuthentication no

# Change to no to disable tunnelled clear text passwords
#PasswordAuthentication yes

# Kerberos options
```

```
KerberosAuthentication yes
#KerberosGetAFSToken no
KerberosOrLocalPasswd yes
KerberosTicketCleanup yes

# GSSAPI options
GSSAPIAuthentication yes
GSSAPICleanupCredentials yes

X11Forwarding yes
X11DisplayOffset 10
PrintMotd no
PrintLastLog yes
TCPKeepAlive yes
#UseLogin no

#MaxStartups 10:30:60
#Banner /etc/issue.net

# Allow client to pass locale environment variables
AcceptEnv LANG LC_*

Subsystem sftp /usr/lib/openssh/sftp-server

# Set this to 'yes' to enable PAM authentication, account processing,
# and session processing. If this is enabled, PAM authentication will
# be allowed through the ChallengeResponseAuthentication and
# PasswordAuthentication.  Depending on your PAM configuration,
# PAM authentication via ChallengeResponseAuthentication may bypass
# the setting of "PermitRootLogin without-password".
# If you just want the PAM account and session checks to run without
# PAM authentication, then enable this but set PasswordAuthentication
# and ChallengeResponseAuthentication to 'no'.
UsePAM yes
UseDNS yes

# GSSAPI key exchange (added by ssh-krb5 transitional package)
GSSAPIKeyExchange yes
```

ANEXO 08

Dados capturados na primeira etapa: autenticação utilizando somente SSH.

ETAPA 01				
TESTE	**BYTES**	**PACOTES**	**BYTES/SEG**	**MEDIA 1 E ULTIMO**
1	9902	61	413,961	5,199
2	10876	67	454,678	5,710
3	10551	65	441,106	5,540
4	10714	66	447,892	5,625
5	10876	67	454,678	5,710
6	9902	61	413,961	5,199
7	9577	59	400,389	5,029
8	10551	65	441,106	5,540
9	10064	62	420,747	5,284
10	10714	66	447,892	5,625
11	9415	58	393,602	4,943
12	10064	62	420,747	5,284
13	9740	60	407,175	5,114
14	10551	65	441,106	5,540
15	9577	59	400,389	5,029
16	10876	67	454,678	5,710
17	10227	63	427,533	5,369
18	10389	64	434,320	5,455
19	10389	64	434,320	5,455
20	10064	62	420,747	5,284
21	10551	65	441,106	5,540
22	9415	58	393,602	4,943
23	9740	60	407,175	5,114
24	10389	64	434,320	5,455
25	10227	63	427,533	5,369
26	10876	67	454,678	5,710
27	10551	65	441,106	5,540
28	10064	62	420,747	5,284
29	10227	63	427,533	5,369
30	10064	62	420,747	5,284
MÉDIA	10237	63	427,986	5,375
D. PAD	437,45	2,69	18,29	0,23

ANEXO 09

Dados capturados na segunda etapa: autenticação utilizando SSH com OpenLDAP.

ETAPA 02				
TESTE	**BYTES**	**PACOTES**	**BYTES/SEG**	**MEDIA 1 E ULTIMO**
1	13145	100	519,082	8,381
2	13671	104	539,845	8,716
3	13539	103	534,654	8,632
4	13276	101	524,273	8,465
5	13145	100	519,082	8,381
6	13539	103	534,654	8,632
7	13539	103	534,654	8,632
8	13802	105	545,036	8,800
9	11436	87	451,601	7,291
10	13145	100	519,082	8,381
11	13802	105	545,036	8,800
12	13408	102	529,464	8,549
13	13276	101	524,273	8,465
14	13408	102	529,464	8,549
15	13276	101	524,273	8,465
16	13276	101	524,273	8,465
17	13145	100	519,082	8,381
18	13539	103	534,654	8,632
19	12751	97	503,510	8,130
20	13145	100	519,082	8,381
21	13145	100	519,082	8,381
22	12882	98	508,700	8,213
23	13802	105	545,036	8,800
24	13671	104	539,845	8,716
25	12751	97	503,510	8,130
26	13671	104	539,845	8,716
27	13276	101	524,273	8,465
28	12751	97	503,510	8,130
29	13539	103	534,654	8,632
30	13014	99	513,891	8,297
MÉDIA	13259	101	523,581	8,454
D. PAD	455,02	3,46	17,97	0,29

ANEXO 10

Dados capturados na terceira etapa: autenticação utilizando SSH com Kerberos.

ETAPA 03				
TESTE	**BYTES**	**PACOTES**	**BYTES/SEG**	**MEDIA 1 E ULTIMO**
1	10825	70	1102,792	6,662
2	10361	67	1055,529	6,376
3	10980	71	1118,546	6,757
4	10516	68	1071,284	6,472
5	10361	67	1055,529	6,376
6	10825	70	1102,792	6,662
7	11598	75	1181,563	7,138
8	11289	73	1150,055	6,948
9	10361	67	1055,529	6,376
10	11444	74	1165,809	7,043
11	10825	70	1102,792	6,662
12	10361	67	1055,529	6,376
13	10361	67	1055,529	6,376
14	11134	72	1134,300	6,852
15	10206	66	1039,775	6,281
16	10670	69	1087,038	6,567
17	11289	73	1150,055	6,948
18	10670	69	1087,038	6,567
19	11444	74	1165,809	7,043
20	11598	75	1181,563	7,138
21	11444	74	1165,809	7,043
22	11289	73	1150,055	6,948
23	10670	69	1087,038	6,567
24	11444	74	1165,809	7,043
25	11444	74	1165,809	7,043
26	10206	66	1039,775	6,281
27	11598	75	1181,563	7,138
28	11598	75	1181,563	7,138
29	10206	66	1039,775	6,281
30	10825	70	1102,792	6,662
MÉDIA	10928	71	1113,295	6,725
D. PAD	487,94	3,16	49,71	0,30

ANEXO 11

Dados capturados na quarta etapa: autenticação utilizando SSH, Kerberos e OpenLDAP

ETAPA 04				
TESTE	**BYTES**	**PACOTES**	**BYTES/SEG**	**MEDIA 1 E ULTIMO**
1	36286	183	3329,302	10,899
2	36683	185	3365,688	11,018
3	36484	184	3347,495	10,959
4	35889	181	3292,916	10,780
5	35691	180	3274,723	10,720
6	35295	178	3238,337	10,601
7	36881	186	3383,881	11,078
8	36088	182	3311,109	10,839
9	35691	180	3274,723	10,720
10	36484	184	3347,495	10,959
11	36881	186	3383,881	11,078
12	36088	182	3311,109	10,839
13	36088	182	3311,109	10,839
14	36088	182	3311,109	10,839
15	35691	180	3274,723	10,720
16	36088	182	3311,109	10,839
17	36088	182	3311,109	10,839
18	35889	181	3292,916	10,780
19	37079	187	3402,074	11,137
20	36088	182	3311,109	10,839
21	35889	181	3292,916	10,780
22	35295	178	3238,337	10,601
23	36088	182	3311,109	10,839
24	36881	186	3383,881	11,078
25	35889	181	3292,916	10,780
26	36088	182	3311,109	10,839
27	35889	181	3292,916	10,780
28	36088	182	3311,109	10,839
29	35691	180	3274,723	10,720
30	37079	187	3402,074	11,137
MÉDIA	36147	182	3316,567	10,857
D. PAD	466,85	2,35	42,83	0,14

.