PROJETO EM SEGURANÇA DA INFORMAÇÃO

ANÁLISE CRÍTICA REDE WIFI DA FTSG – FACULDADE DE TECNOLOGIA DA SERRA GAÚCHA

Disciplina: Gestão da Segurança da informação
Semestre /Ano: 2º semestre 2014
Professor: André Gomes
Acadêmicos: Edson Teixeira, Iuri Luis Ghinzelli, Juliano Saraiva, Leandro Borges, Leandro Faccenda, Lucas Duda, Michele Henz, Pedro Nunes, Petter Lopes, Valdo Santos, Viviana Neves, Wilber Bossle.

1. Identificação do alvo

Rede Wifi - Alunos FTSG

2. Lista dos riscos iniciais

- Falta de autenticação;
- Falta controle de banda;
- Falta controle de Aplicação (P2P, UPNP, *Intant Message*);
- Falta restrição de análise de pacotes (*sniffer*);
- Possibilidade de ataque a rede interna.

3. Definir o que atacar

- Será feita uma análise dos pacotes que estão sendo trafegados na rede;
- Testes de *download* utilizando a rede *Wifi;*
- Testes utilizando *softwares* P2P.

4. Definir as ferramentas

Utilizaremos as seguintes ferramentas:

- Wireshark;
- Nmap;
- Ettercap;
- Maltego;
- E - Fing (*Software Mobile*).

5. Elaborar o método

- Wireshark: Para análise e detecção de pacotes;
- Nmap: Para analisar e identificar portas dos dispositivos conectados na rede *wifi;*
- Ettercap: Utilizado para ataques, ARP poisoning, ICMP Redirect, Port Stealing, DHCP spoofing;
- Maltego: Para leitura do ambiente relacionado com engenharia social;
- Fing (*Software Mobile*): Listar IPs da rede e analisar serviços e portas abertas.

6. Cronograma da aplicação

Data	Aula	Atividade
30/10/2014	1ª Aula	Elaboração do plano para: Análise, Identificação, definição de ferramentas.
06/11/2014	2ª Aula	Aplicação das ferramentas e desenvolvimento de relatórios.
13/11/2014	3ª Aula	Finalização de relatórios e apresentação dos dados obtidos.
20/11/2014	4° Aula	Apresentação final do trabalho.

7. Aplicação e resultado

Foram escaneados os seguintes IP's com a ferramenta de intrusão NMAP e com a ferramenta FING:

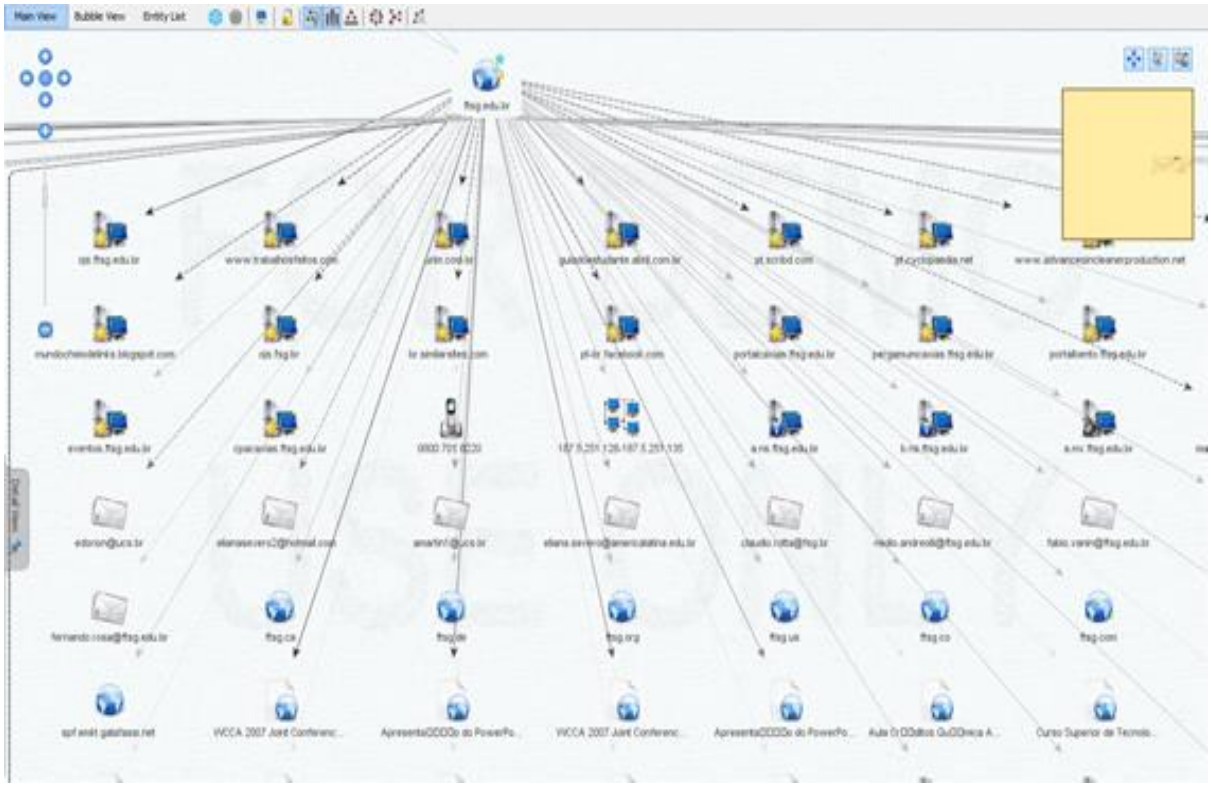
- 10.128.144.0/24 - 144.0.24 (Rede WI-FI);
- 192.168.31.0/24(Rede Cabeada);
- 192.168.0.0/24(Rede Cabeada);
- 192.168.250.0/24(Rede Cabeada).

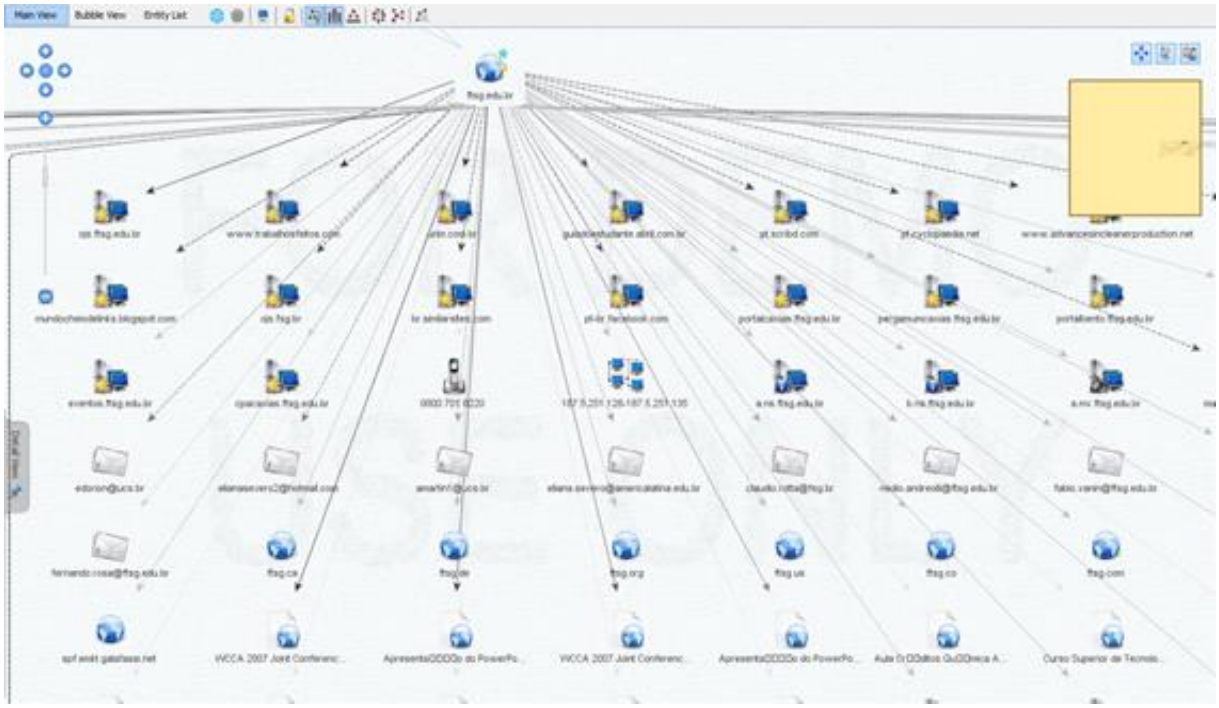
Dentre essas redes foi encontrada uma máquina com compartilhamentos de arquivos abertos, permitindo que qualquer usuário com acesso a rede pudesse excluir, alterar ou até mesmo infectar a máquina com vírus e usá-la para disseminá-lo pela rede.

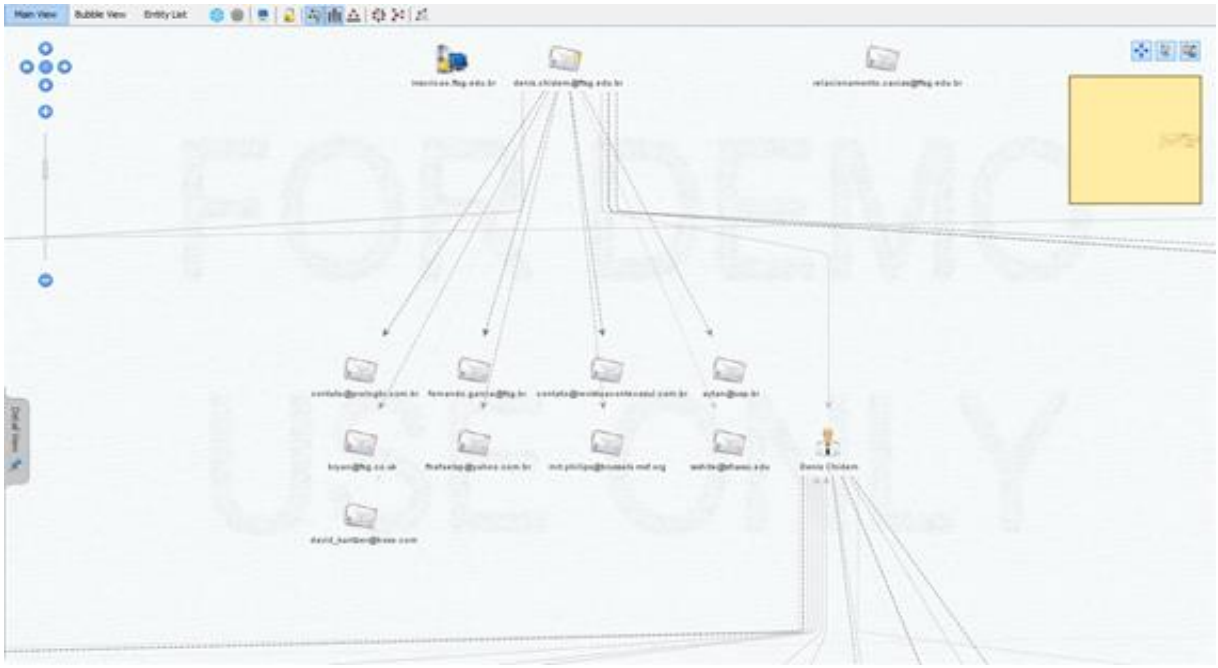
Os domínios abaixo também foram escaneados com NMAP, porém nada foi encontrado com relação a portas comprometedoras. No entanto, através do *scan* com Maltego pelo DNS ftsg.edu.br, foi possível identificar a ligação entre eles, além de exibir alguns dados de redes sociais e contatos de *e-mails* de alguns colaboradores.

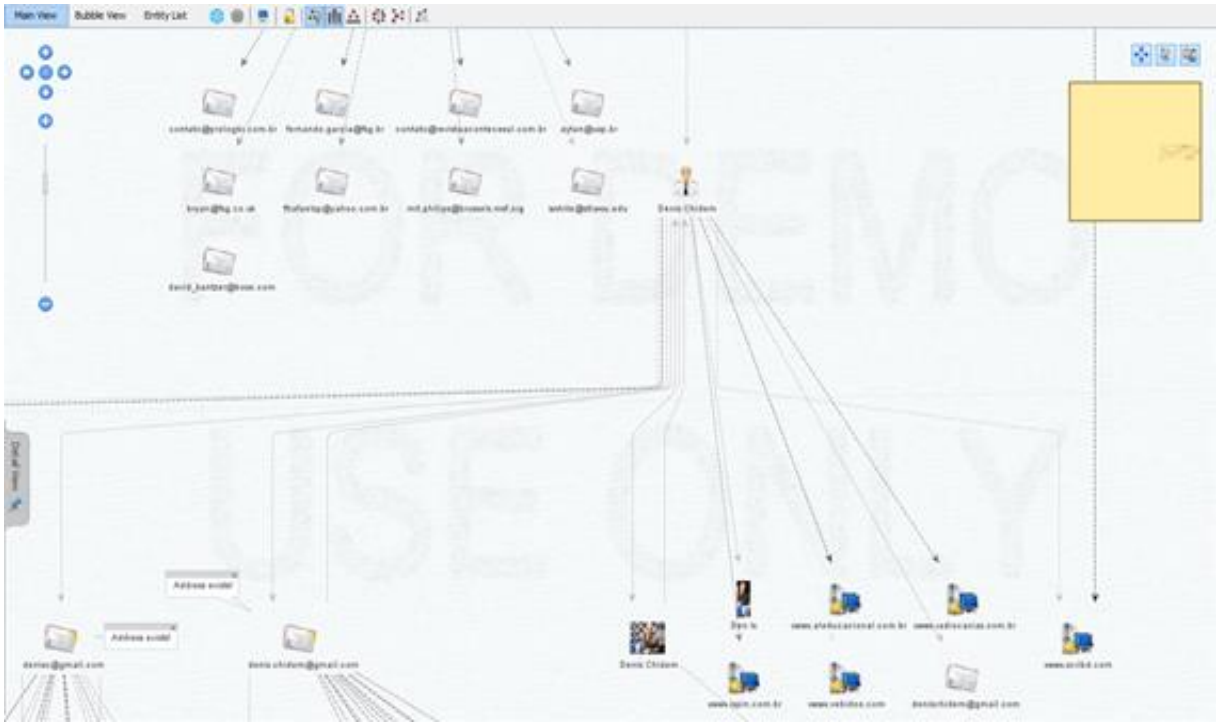
- portalcaxias.ftsg.edu.br;
- a.ns.ftsg.edu.br;
- ojs.ftsg.edu.br;
- eventos.ftsg.edu.br;
- portalbento.ftsg.edu.br.

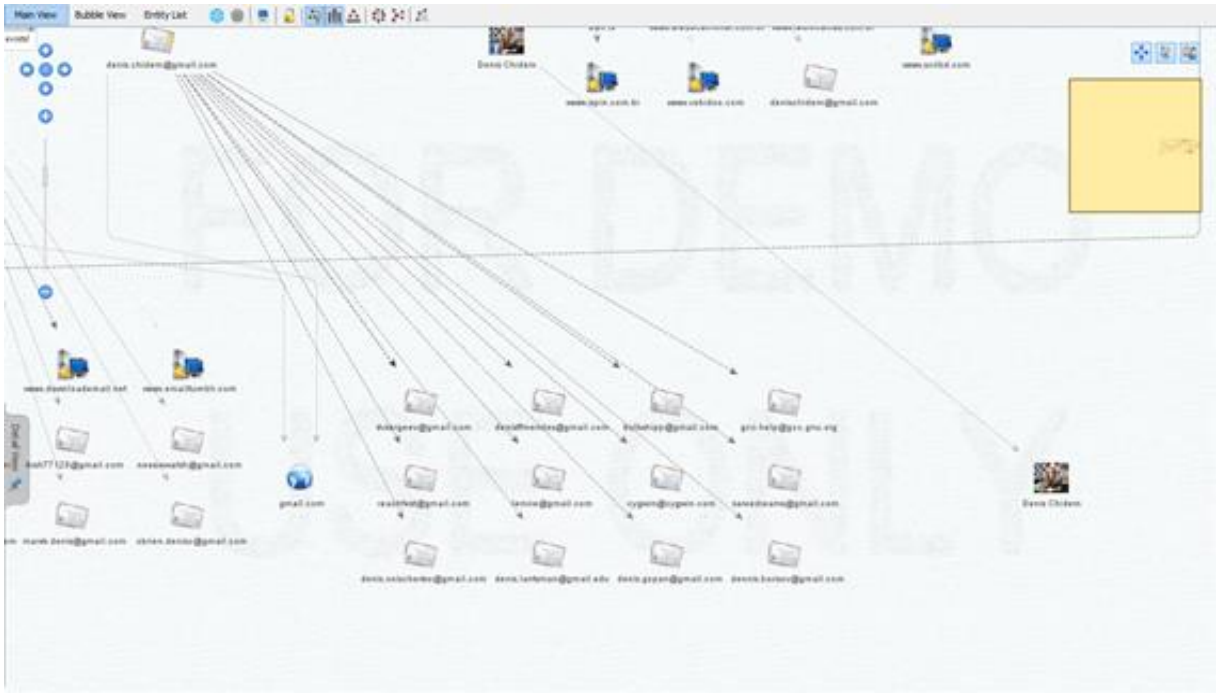
Dados encontrados na busca com o *software* Maltego podem ser analisadas nas imagens abaixo:




Main View
Bubble View
Entity List
ffsg.edu.br


Main View
Bubble View
Entity List





8. ANÁLISE CRÍTICA DO RESULTADO

8.1 DESCRIÇÃO DAS TÉCNICAS UTILIZADAS E MÉTODOS DE PREVENÇÃO

Das técnicas utilizadas as que mais se destacaram foram o ARP Poisoning, Engenharia Social e Sniff.

8.1.1 ARP Poisoning

Utilizado para destacar a possibilidade de atingir a Integridade, Disponibilidade e Confidencialidade da rede WiFi, visto que o uso dessa técnica permite que o atacante possa direcionar usuários para páginas *fake* de *login* dos sistemas da FTSG, afim de capturar usuários e senhas. Também é possível interceptar todo o tráfego da rede e obter outros dados sigilosos dos usuários, bem como acesso a outros sistemas a exemplo de *e-mails* e portais de trabalho. É possível também tornar a rede indisponível gerando um alto tráfego de pacotes aleatórios causando também um resultado de DDOS em servidores que se encontram pelo caminho. A disseminação de *malwares* é facilitada também por esse tipo de ataque.

8.1.2 *Sniffer*

Com essa técnica torna-se possível analisar o tráfego de rede e identificar pacotes sem criptografia com informações sigilosas, é possível também analisar pacotes UDP que normalmente estão abertos e a partir deles identificar o tipo de cliente que está se comunicando, por exemplo, se é um servidor ou máquina de usuário, obtendo versões de Sistema Operacional, nome do Host, ip, *mac address,* origem e destino da comunicação.

8.1.3 Engenharia Social

Através desta técnica foi possível obter dados de alguns usuário e funcionários referentes a redes sociais, *e-mails*, telefones, arquivos, ou seja, tudo o que está disponível na internet sobre os indivíduos.

8.2 TÉCNICAS DE DEFESAS GERAIS

Utilização roteadores com layer3 com a configuração de filtro de pacotes.

Outra questão importante é a autenticação de usuários para evitarmos o acesso de pessoas não autorizadas a rede. Com a implementação de uma rede autenticada.

8.2.1 Defesa contra ARP-Poisoning ou ARP Spofing e sua Detecção

O autor Luiz Vieira, do site *“Viva o Linux”,* explica que a melhor defesa contra o ARP-Poisoning é habilitar o MAC Bridging no *switch*. Esta é uma característica encontrada em *switchs* de qualidade que não permite que os endereços MAC associados com uma porta

sejam alterados depois de configurados. Mudanças legítimas de MAC podem ser realizadas pelo administrador da rede.

Outra defesa é o uso de caminhos estáticos. O cache ARP podem ter entradas estáticas (não alteráveis), assim respostas ARP falsas seriam ignoradas. Essa abordagem não é prática a não ser em pequenas redes caseiras, consequentemente onde não há muitos riscos do ARP Poisoning ocorrer. É importante também saber como se comporta o roteamento estático no Windows. Alguns testes descobriram que o Windows ainda aceita respostas ARP falsas e usa o roteamento dinâmico ao invés do estático, tornando nulo qualquer efeito da utilização do roteamento estático no Windows.

Além desses dois métodos, a única outra defesa disponível é a detecção. Arpwatch é uma das formas de detecção. Arpwatch é uma ferramenta para detectar ataques ARP. Esta ferramenta monitora atividade *ethernet* e mantém uma base de dados dos pareamentos Ethernet/IP. Ela também reporta certas alterações via *e-mail*. Arpwatch utiliza a libcap, uma interface independente que utiliza um método de captura de pacotes no nível de usuário para detecção de ataques ARP. O Arpwatch mantém o administrador informado quando uma nova máquina adquire um endereço da rede. Ele envia por *e-mail* o endereço IP e o MAC da nova máquina na rede. Ele também informa se o endereço MAC mudou de IP. Além de informar se alguém está bagunçando com a configuração da rede e alterando seu IP para o de um *gateway* ou servidor.

A clonagem de MAC pode ser detectada utilizando o RARP (Reverse ARP). O RARP solicita o endereço IP de um endereço MAC conhecido. Enviando uma solicitação RARP para todos os endereços MAC existentes em uma rede, pode determinar se algum computador esta realizando clonagem, e se múltiplas respostas são recebidas por um único endereço MAC.

Muitos métodos existem para detectar máquinas em modo promíscuo. É importante lembrar que sistemas operacionais possuem suas próprias pilhas de TCP/IP e placas *ethernet* possuem seus próprios *drivers*, cada um com seus próprios subterfúgios. Diferentes versões de um mesmo sistema operacional tem variações de comportamento. O Solaris, por exemplo, é único em sua forma de tratar pacotes ARP.

Solaris aceita apenas alterações de ARP após um determinado período de expiração. Para envenenar o cache de um sistema Solaris, um atacante precisaria utilizar um ataque DoS contra uma segunda máquina alvo para evitar uma *"race condition"* após o período de expiração. Este DoS pode ser detectado se a rede possuir um "Sistema de Detecção de Intrusão" (IDS) rodando. A rede pode também estar protegida contra *Spoofing/Poisoning e Sniffing* através de configurações de *firewall* e criptografia de dados ao longo da rede, mas estes dois métodos não são empregados.

9. Lista dos riscos final

Aula 06/11 - Divisão de estudo com base no Marco Civil da Internet. Para embasamento teórico seguem informações abaixo:

- Atentar contra a segurança de serviço de utilidade pública;
- Discriminação de raça ou de cor por meio da internet;
- Divulgação ou utilização de modo indevido, as informações e dados pessoais abrangidos em um sistema informatizado;
- Estelionato eletrônico;
- Falsificação de dados eletrônicos ou documentos públicos;
- Falsificar dados eletrônicos ou documentos particulares;
- Inserir ou propagar código malicioso em um sistema informatizado;
- Inserir ou propagar código malicioso, seguido de danos;
- Interromper ou perturbar serviço telegráfico, telefônico, informático, telemático ou sistema informatizado;
- Inutilizar, destruir ou deteriorar dados eletrônicos de terceiros ou coisas alheias;
- Obter, transferir ou fornecer dados ou informações sem autorização;
- Ter acesso a um sistema informatizado sem autorização.

O que é considerado crime a partir da Lei 12737/2012?

É considerado crime QUALQUER tipo de invasão que tenha como objetivo:

- Obtenção dados;
- Alteração de dados;
- Exclusão de dados;
- Instalação indevida de uma vulnerabilidade para uma vantagem indevida.

Pena: Detenção de 3 (três) meses a 1(um) ano.

- Divulgação, comercialização ou vantagem financeira a cerca de dados obtidos em invasões.

Pena: 6 (seis) meses a 2 (dois) anos.

Referente aos testes realizados, observamos que existem dos direitos e garantias do usuário:

I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;

II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;

III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;

VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;

Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.

9.1 ITENS DE ATENÇÃO IMEDIATA

9.1.1 Falta de autenticação

Atualmente o acesso a rede sem fio da faculdade e feita por meio de uma senha de autenticação criptografada utilizando WPA / WPA2 PSK, ou outros meios mais seguros de autenticação, no entanto essa senha esta disposta em todas as salas de aula e todos os corredores da faculdade.

Isso se torna um problema de segurança, pois o acesso ao prédio da FSTG é aberto ao público em geral, expondo a rede a acessos indevidos.

Como alternativa de solução para esse problema, a faculdade poderia utilizar o já existente cadastro de alunos para acesso ao sistema *Moodle*, para autenticação da rede *wireless,* evitando que pessoas não autorizadas tenham acesso à rede.

9.1.2. Falta controle de banda

Ao acessar a rede, outra grande vulnerabilidade é a falta de um controle de utilização de rede. Isso faz com que quem tenha acesso a rede, possa utilizar toda a largura de banda de internet para uma única aplicação ou usuário, deixando toda rede congestionada e dificultando assim o acesso ao conteúdo de estudo disponibilizado pela faculdade no portal de ensino do aluno.

Para correção desse problema será necessária a implementação de um controle de banda de internet que devera ser gerencia pelo setor de TI que definirá as cotas e as prioridades de cada grupo de utilização.

9.1.3 Falta controle de Aplicação (P2P, UPNP, *Instant Message*)

É possível conectar a qualquer serviço externo com essas portas liberadas. No meio acadêmico não faz sentido a liberação de redes de compartilhamento dos modelos apontados. Esse tipo de liberação causa lentidão da rede, devido e excesso de banda consumida.

9.1.4 Falta restrição de análise de pacotes (*sniffer*)

Como há falta de autenticação fica fácil rodar programas sem controle e identificação de quem esta executando, no entanto, mesmo que haja controle de acessos é de extrema importância saber identificar quem está executando o *sniffer*, para poder aplicar as penalidades conforme estabelecido no contrato do aluno.

9.1.5 Possibilidade de ataque a rede interna

Esse tipo de brecha pode ser explorado facilmente, pois a partir do momento que um computador for registrado na rede e este tem o propósito de atacar com as ferramentas certas, é possível identificar a rede cabeada a partir da rede sem fio.

Por exemplo os IP's:

- 10.128.144.0/24 - 144.0.24 (Rede WI-FI);
- 192.168.31.0/24(Rede Cabeada);
- 192.168.0.0/24(Rede Cabeada);
- 192.168.250.0/24(Rede Cabeada).

Neste momento, contendo essas informações, o ataque pode ser feito por meio de *exploits*, onde, podem ser infectados todos os computadores e dispositivos móveis que possuam alguma falha de segurança.

9.1.6 Possibilidade de ataque tipo *Man In The Middle*

Este ataque é possibilitado por meio das técnicas de ARP Poisoning e DHCP Spoofing, onde todo o tráfego passa a ser controlado pela máquina do atacante. Nos testes realizados utilizando a técnica de ARP Poisoning, foi possível identificar o usuário e senha de autenticação de algumas contas particulares dos usuários, como pode ser observado no exemplo abaixo:

DHCP: [192.168.242.11] ACK: 10.128.144.134 255.255.248.0 GW 10.128.144.1 DNS 192.168.252.21 "academic.lc"

IMAP : 186.202.140.222:143 -> **USER: xxxxxxx@sindmoveis.com.br PASS: "xxxxxxxx".**

(Dados de usuário e senha modificados para segurança do usuário)

Não foi necessário nada além de um *sniff* para capturar essa informação, por meio da ferramenta Ettercap. Como esse ataque efetua o redirecionamento do trafego de rede para a máquina do atacante, e possível criar páginas *fake* de *login* para qualquer tela e capturar usuário e senha dos demais usuários da rede. Isso também e possível por meio da ferramenta Ettercap.

9.1.7 Falta de um IDS (Sistema de Detecçao de Intrusos)

Sem um IDS não há meios mais seguros de detectar e anular ataques a rede.

9.2 – Estrutura Analítica, Ativos de Informação e Método Brasiliano

Análise de Riscos e Auditoria em TI		
FTSG - Faculdade de Tecnologia da Serra Gaúcha		
Tópicos	**Comparativo Tabela Maturidade**	**Proposta de Melhoria**
Documentação de politica de segurança	0	Documentar todos tipos de acessos como exemplo: acesso a estação de trabalho, internet, e-mail, dados da empresa, empréstimo equipamento e dispositivos móveis.
Definição de segurança da informação	0	Criar documento de Definição de Segurança, impondo condições de acessos e liberações de internet, e-mail, sites restritos entre outros para ser implantado no processo de integração de atuais e novos funcionários.
Declaração de compromisso da direção	0	Conscientizar a direção de que existe uma punição para quem burlar a S.I. passando a autonomia para o setor de PSI por punições e demissões por conta destas infrações.

Estrutura de controle	1	Controle de acessos via softwares como FW, AD, Proxy, FS e servidor de e-mail, câmeras, e logs de rastreabilidade.
Conformidade com a legislação	0	Documentar de forma impressa sobre a conformidade da legislação e com os requisitos de contrato, informando as normas da empresa e suas liberações quanto a utilização dos recursos disponibilizados.
Requisitos de conscientização	2	Treinamentos educacionais quanto a uitlização de forma adequada dos recursos disponibilizados como ferramentas de trabalho, e suas respectivas punições quanto ao não cumprimento destas regras.
Gestão da continuidade	2	Criar e documentar políticas de backup diários e mensais para resgate de informações deletadas e/ou modificadas mediante a má fé dos usuários.
Consequências das violações na segurança	0	Acometer os colaboradores que hajam com má conduta a processo disciplinar mediante a assinatura de documento prevenindo um novo acontecimento de mesmo caráter. A partir deste momento, havendo uma reincidência o mesmo deverá ser afastado de seu cargo, perdendo seus privilégios, e dependendo da situação, solicitar a pessoa, a saída imediata da pessoa das dependências da organização, escoltando-a.

Tabela de Maturidade	
0	O benefício não existe
1	Existe, mas é inicial (ad-hoc), sem padrão e o gerenciamento é caso a caso.
2	Existe e é estruturado de forma que os procedimentos possam ser repetidos, porém há forte dependência do conhecimento individual e pouca documentação.
3	Ocorre de forma padronizada, documentado e é comunicado para que cada indivíduo possa percebê-lo, porém não existe certeza de que ele não será desviado (sem controle)
4	Monitorado ao longo do tempo, permitindo verificar sua conformidade com os objetivos do negócio através do uso de ferramentas automatizadas.
5	Otimizado, ocorre de forma automatizada; a preocupação está com as ações de melhorias advindas do controle e análise do comportamento do benefício ao longo do tempo.

ATIVOS DE INFORMAÇÃO						
Nome	**Categoria**	**Responsável**	**Descrição**	**Relevância**	**Ameaças**	**Criticidade**
Desktops	Hardware	Responsável TI	Ferramentas de utilização dos usuários	Média	• Senha Administrador disponível nos laboratórios; • Mau uso dos usuários	Médio
Rede Cabeada	Estrutura Física	Responsável TI	Estrutura de utilização dos usuários	Alta	Falta de controle quando conectado em outras estações não autenticadas a rede	**Alta**
Rede Wifi	Estrutura Lógica	Responsável TI	Liberação de internet local para rede wireless	Alta	• Falta controle de banda; • Falta controle de aplicação (P2P, UPNP, Intant Message); • Falta restrição de analise de pacotes (sniffer)	**Alta**

Classificação dos Ativos de Informação			
Grau de Criticidade	**Ativo de Informação**	**Impacto**	**Cor**
Alto	Data Center, servidores, PABX, recursos criptológicos, cópias de segurança, equipamentos de conectividade ou de armazenamento de informações ou de computação móvel das autoridades de primeiro escalão.	Interrompe a missão do órgão ou provoca grave dano à imagem institucional, à segurança, do estado ou sociedade.	**Vermelho**
Médio	Computadores com dados e informações únicas, de grande relevância, equipamentos de conectividade ou de armazenamento de informações ou de computação móvel das autoridades de segundo escalão.	Degrada o serviço do órgão ou provoca dano à imagem institucional, à segurança do estado ou sociedade.	**Amarelo**
Baixo	Os demais ativos de informação.	Comprometem planos ou provoca danos aos ativos de informação.	**Verde**

MÉTODO BRASILIANO												
Ameaça		**Descrição**	**FR Interno**	**FR Externo**	**FR RH**	**FR Meios Técnico Passivo**	**FR Meios Técnico Ativos**	**FR Meios Organizacionais**	**Fator de Risco**	**Fator de Exposição**	**Grau de Probabilidade**	**Nível de Probabilidade**
1	**Falta de autenticação**	Devido aos produtos terem alto valor de mercado, poderia sofrer muito com o desaquecimento da economia.	2 O que poderia realmente afetar seria o desaquecimento da economia externa.	5 A queda da economia do Brasil poderia levar a queda brusca das vendas.	2 Os efetivos pouco poderiam fazer para evitar este risco.	2 Os meios técnicos físicos não poderiam ajudar a evitar este risco.	2 Os equipamentos e sistemas eletrônicos não poderiam auxiliar neste risco.	2 As normas da empresa só poderiam ajudar a prever, mas não a evitar este risco.	2,5	3	30%	**Média**
2	**Concorrência Desleal**	Empresas concorrentes sempre tentando copiar projetos.	5 Os colaboradores poderiam agir de má fé liberando projetos a concorrentes	2 Os fatores externos não influenciariam muito	5 A equipe de segurança deve estar atenta as políticas de segurança e controle	2 Os meios físicos não influenciam diretamente neste risco	5 Se não tiver boas formas de segurança e controle por meio de sistemas poderá ocorrer desvio de projetos	5 Caso as normas e políticas de segurança não forem bem estruturadas, a empresa abrirá brechas para o desvio de projetos	4	5	80%	**Muita Alta**
3	**Paralização Obra**	Setor responsável pela documentação errar e algum processo.	5 Setor responsável deve estar atento a todo e qualquer documento	5 Setor responsável pela obra deve ficar atento aos colaboradores que possuem riscos	1 A qualificação dos colaboradores não tem muita relevância neste risco.	1 Pela boa estrutura e segurança adotada pela empresa este risco não afeta diretamente.	3 A parte técnica de softwares e sistemas deve auxiliar o setor responsável na parte de documentação diretamente.	4 O fluxo de trabalho e manuais deve estar bem estruturado para que não tenha falhas na parte de documentação.	3,17	5	63%	**Muito Alta**

Escala	Nível de Probabilidade	
1 - 5	Baixa	4% a 20%
5,01 - 10	Média	20,01 a 40%
10,1 - 15	Alta	40,01 a 60%
15,01 - 20	Muito Alta	60,01 a 80%
20,01 - 25	Elevada	80,01 a 100%

10. Documentação de toda atividade

No dia *30/10/2014*, a turma de Gestão da segurança da Informação, recebeu as orientações referente as datas e definições do desenvolvimento do projeto de estudo. O colega Petter Lopes foi eleito como gerente de projeto se encarregando de criar o documento on-line e compartilhar com todos os membros do projeto.

A equipe discutiu e fez apontamentos sobre o estudo a ser desenvolvido, definiu o alvo a ser tratado, o Wifi da FTSG para usuários, foram definidos também as ferramentas, métodos e cronogramas para melhor atender os objetivos principais do projeto.

Lucas Duda ficou encarregado de organizar a parte documental com a análise SWOT (estudos de riscos, ameaças...). Ficou definido também que iremos tratar do Marco Civil da Internet como embasamento para melhorar nossa analise e fundamentação teórica para o estudo.

Foram realizados testes iniciais com as ferramentas escolhidas para ter uma visão melhor do ambiente que estamos estudando. Elaborado a parte documental básica e organizada os próximos encontros. No próximo encontro será estudado os tópicos do Marco Civil da Internet e com embasamento do mesmo realizar os testes.

Ficou como tarefa para o próximo encontro: Estudar as ferramentas para a próxima aula todos possuírem o básico de conhecimento.

Na data de *06/11/14,* estivemos reunidos organizando os testes com as ferramentas elencadas anteriormente no encontro inicial da data de 30/10/14. Foi dividida a turma com os usuários de teste de infraestrutura, acesso a partir de dispositivos móveis a dispositivos com acesso livre. Foi constatado que na rede existem inúmeros e-mails perdidos e que na rede foi possível acessar um notebook com acesso liberado possibilitando criar pastas, colar

arquivos e efetuar testes de precisão. A nota é que em momento algum feriu a integridade das informações do usuário ou ameaças para o mesmo.

Em todas as etapas do processo o gerente do projeto Petter organizou as tarefas e buscou explicar cada uma delas elencando os responsáveis pela realização de cada tarefa com objetivos a cumprir. O colega Valdo ficou responsável por organizar o documento inicial de apresentação (PPT).

Ficou exemplificado cada uma das ferramentas e suas respectivas funções para compreensão e analise. Finalizou-se com as tarefas agendadas pelo Petter e o Valdo. Um organizará a parte dos softwares estudados e o Valdo a apresentação do estudo realizado.

No dia *13/11/2014* a turma se reuniu com 3 pessoas faltantes cada uma com seu motivo pessoal em especifico. Como a nossa internet está lenta demais até conseguirmos a conexão estável com o documento on-line fez-se necessário o download do arquivo para edição off-line.

O gerente do projeto Petter encarregou-se de fazer a divisão das organizar as tarefas finais. Como a disponibilidade de notebooks era pouca dividimos as tarefas em equipes fazendo com que o trabalho fosse concluído.

Pedro e Willber iniciaram a organização da apresentação no Prezi, compartilhando com todos os demais integrantes pudessem editar.

A lista dos riscos ficou completa com a colaboração de todos os colegas deixando o trabalho em fase final. O Petter apresentou para o professor e o mesmo solicitou para que cada um faça uma analise critica do que foi realizado no projeto e que as mesmas sejam descritas abaixo desta ata que se finaliza com o desafio de que surjam mudanças.

11. ANALISE CRITICA

11.1 LEANDRO BORGES

Geralmente disciplinas cursadas na faculdade são em sua maioria teóricas o que por sua vez as torna um tanto monótonas e tediosas. Com esse trabalho de analise de vulnerabilidade da rede conseguimos um grande dinamismo na aula e colocamos em pratica conceitos ate então só estudas. Experiência muito enriquecedora para o currículo escolar.

11.2 IURI GHINZELLI

Acredito que só pelo fato de aplicar o teórico estudado em aula no projeto de estudo de vulnerabilidade, ameaças e pontos a crescer na rede wi-fi da faculdade. Toda e qualquer forma de analise possibilita a criação de novos pensadores e de transformação da realidade

da nossa faculdade. O compartilhamento de ideias e o modo de pensar de cada um dos colegas fez com que todos pudessem compreender de modo simples os problemas do nosso ambiente.

O trabalho desenvolvido nesta disciplina somente terá resultados se os responsáveis utilizem nosso estudo para transformar a realidade em que os estudantes que estão por vir, encontrem um ambiente seguro e tranquilo com velocidade e segurança nas informações. A análise SWOT desenvolvida no 2º semestre de 2013 foi outro dos trabalhos importantes desenvolvidos em aula com apoio e ajuda do professor André Gomes. Se cada um dos professores tivessem uma visão que faça com que consigamos conciliar o teórico com o pratico formaríamos mais pensadores e não repetidores de informações. O estudo realizado tornou claro que, nossa rede está totalmente desprotegida e sem autenticação no acesso faz com que qualquer indivíduo munido da senha da rede sem fio encontre acesso, faça *download* por torrent, videos na rede, facebook e afins nada institucional deixando a rede lenta e repleta de sugadores de informações/rede/velocidade de quem realmente está preocupado em aprender e valoriza seu tempo e dinheiro. Que tal apoiarmos as causas que constroem informações e pensamentos voltados para a construção de um ambiente, uma sociedade e um mundo melhor.

11.3 LEANDRO FACCENDA DA SILVA

Podemos ver neste trabalho como algumas programas utilizados sozinhos ou em conjunto (tornando o furto das informações mais poderoso) já pode possibilitar uma “arma” para o atacante utilizar contra as vitimas (no caso, funcionários e alunos), é claro que após a receptação de algumas informações possivelmente o atacante vai tentar ter um lucro sobre elas, fugindo da esfera da entidade para a vida pessoal da(s) vítimas, então nota-se que a segurança da rede da Faculdade deve ser revista antes que possa acontecer furtos de informações podendo levar a faculdade a ter prejuízo financeiro e de imagem.

11.4 PETTER ANDERSON LOPES

Com a possibilidade de realizar um trabalho prático como este, fica muito melhor a compreensão dos métodos e técnicas que compõe uma análise de vulnerabilidades. O fato de poder reunir uma equipe e todos discutirem os assuntos relativos a segurança bem como expor ideias enriquecedoras para melhorar as implementações de correção e prevenção da segurança na instituição, torna-se muito gratificante, pois sem dúvida aumenta o conhecimento dos integrantes.

É muito importante que trabalhos assim continuem sendo feitos, pois foge da monotonia dos conceitos e torna a aula mais agradável, sem contar que é muito mais fácil memorizar os conceitos e prender o interesse dos envolvidos, além é claro de já estimular a experiência prática, o que por sua vez é muito valioso nas organizações.

11.5 LUCAS CALEGARO DUDA

Faço das palavras do Petter as mesmas da minha, acredito que trabalhos como este proposto pelo Professor André é um dos melhores que tem, pois a interação dos alunos junto aos assuntos e teorias contempladas ao longo do semestre se fazem muito mais efetivas quando há atividades práticas e troca de experiências e informações. A FTSG está muito carente de bons professores e de materiais de bom conteúdo, tendo seu rendimento e imagem bem deteriorada nos meus 3 semestres cursados até o momento.

Talvez seja esta a hora da instituição abrir seus olhos e dar a oportunidade de todo o grupo presente neste projeto junto a FTSG corrigir os problemas apontados, realizando assim um trabalho para a faculdade onde vamos poder aprender mais e ajudar mais ainda, não deixando de divulgar todo este processo, mostrando não só aos alunos presentes mas a toda Caxias e Região que a FTSG é uma instituição que está amadurecendo e que abre portas a novos projetos, novos desafios e está apta a desenvolver melhores profissionais para o futuro, apoiando projetos como os que foram propostos.

Esta atitude poderia mudar e muito a imagem que vem decaindo a cada semestre de má estruturação, aulas precárias, materiais fracos e aulas pouco objetivas, mais uma vez peço para que abram os olhos, pois estão sendo comparados hoje a qualquer tipo de instituição.

11.6 MICHELE NEUJAHR HENZ

Verificamos neste projeto, a importância de implantar os nossos conhecimentos teóricos adquiridos, na análise prática. Usando nossa instituição como modelo do nosso projeto de Segurança de Informação, fez com que tenhamos mais imposição em querer que seja concretizada essa ideia.

Na prática aplicada, verificamos a proporção das vulnerabilidades encontradas e de sua criticidade. Gostaríamos que os itens colocados neste projeto, sejam aprovados pela Alta Administração da instituição, para que a mesma seja referência em tecnologia.

11.7 EDSON TEIXEIRA

Estimular a aprendizagem dos alunos com aulas práticas já se mostrou em muitas vezes muito mais eficaz que aulas onde a teoria predomina. Ao lançar esse desafio nosso orientador e professor André, estimulou nossa criatividade em procurar brechas e resolução dos mesmos. Esse trabalho demostrou na prática a Gestão da Segurança da Informação. Onde por meio dos testes realizados foi possível demostrar o quando vulnerável é a rede sem fio da FTSG. E como muitos alunos em muitas vezes a utilizam sem saber e colocam ali seus *logons* e *passwords*.