# Mecanismos de detecção e controle para dispositivos de rede sem fio não autorizados (*Rogue AP's*)

**Henrique de Vasconcellos Rippel**[1]

[1]Faculdade de Tecnologia Senac Pelotas
Rua Gonçalves Chaves, 602 – Pelotas – RS – Brasil – Caixa Postal – 96.015-560
Curso Superior de Tecnologia em Redes de Computadores

hvrippel@gmail.com

***Resumo.*** *A facilidade de implantação de dispositivos de rede sem fios sem autorização pode facilmente comprometer a segurança da informação e causar instabilidade na rede local, prejudicando consideravelmente o funcionamento de uma organização. Este projeto visa o desenvolvimento de uma ferramenta de rede capaz de coletar dados sobre dispositivos ativos na rede local, permitindo aplicar regras para controlá-los.*

***Abstract.*** *The ease of deploying wireless network devices without authorization can easily compromise information security and cause instability in the local network, significantly impairing the functioning of an organization. This project aims to develop a network tool able to collect data of active devices on the local network, allowing to apply rules to control them.*

## 1. Introdução

Os benefícios oriundos da rede sem fios são incontestáveis pela facilidade de acesso, mobilidade, praticidade e alcance, pois dependendo da tecnologia investida no equipamento, a qualidade de uso pode ser bastante interessante. A utilização não adequada de dispositivos de rede sem fios traz sérios problemas de segurança comprometendo usuários e, principalmente, dados e informações sigilosas de uma organização. O baixo custo de aquisição destes equipamentos torna-se um atrativo para a expansão da rede - por parte dos usuários -, sem que o setor técnico competente tenha o devido conhecimento. Por outro lado, a ingenuidade e a falta de informação são fatores que contribuem consideravelmente para a instalação destes dispositivos, expondo o conteúdo privado, além de servir de base à origem de ataques à rede local e às demais redes espalhadas pelo mundo.

O intuito deste projeto será apresentar uma ferramenta de rede capaz de detectar dispositivos suspeitos na rede local, possibilitando aplicar regras restritivas para isolar os pontos de acessos (*access points*) não autorizados. [Kaspersky 2014]

## 2. Rede sem fio

A rede sem fios é um método de interligação entre dispositivos, no qual utiliza o ar como meio de transmissão, por meio de ondas de radiofrequência (*WiFi* [InternetSemFio 2014] e *Bluetooth* [Alecrim 2013]), infravermelho e laser, por exemplo. A rede sem fios é recomendada quando, e somente, existe a necessidade de mobilidade e/ou dificuldade técnica para a implantação de cabeamento estruturado para atender determinado segmento de uma unidade predial. Ela é, também, amplamente utilizada para prover acesso à rede

local e à Internet, utilizando portais de captura (*Hotspots*) [Mitchell 2014b] para registrar a sessão de utilização de um usuário previamente credenciado, atribuindo perfis de acesso de acordo com política de uso adotada. Hospitais, aeroportos, universidades, auditórios, praças, prédios isolados geograficamente, e outros, utilizam este mecanismo por ser inviável tecnicamente a disponibilidade de cabos de rede, uma vez que a utilização de *laptops*, *smartphones* e outros dispositivos possuem apenas antena para conexão sem fio.

### 2.1. Riscos iminentes

Todo e qualquer projeto deve ser muito bem elaborado visando diminuir possíveis riscos e vulnerabilidades que possam comprometer a integridade, disponibilidade e confidencialidade das informações de uma organização. Ao mesmo tempo em que a rede sem fios traz inúmeras vantagens e facilidades de utilização para a rede local, ela pode tornar-se um ponto grave de falha, permitindo que usuários mal-intencionados apropriem-se de informações privadas utilizando-as de forma indevida. Ao deixar a rede aberta, ou seja, sem nenhuma forma de autenticação e criptografia dos dados, estes usuários infiltram-se facilmente, coletando informações sigilosas, como por exemplo, dados bancários, credenciais de acesso a diversos *sites* e sistemas, informações pessoais, além de praticar ataques distribuídos de negação de serviço (DDoS) [Solha et al. 2014], disseminar vírus, explorar vulnerabilidades em serviços e servidores da própria organização, entre outros.

Por utilizar o ar como meio de transmissão, a rede sem fios desempenha o mesmo papel funcional de um *hub* [Morimoto 2014], no qual todo pacote recebido é retransmitido à todos os *hosts* conectados a um *access point*. Dispositivos que possuem interface de rede em modo promíscuo recebem todos os pacotes trafegados nesta rede sem fios, e caso não haja criptografia de dados, qualquer usuário pode coletar as informações sigilosas descritas anteriormente.

O número de usuários conectados influencia diretamente na performance de um dispositivo de acesso sem fio. Embora um aparelho desta categoria seja útil, prático e barato, ele possui limitações de recursos físicos causando instabilidades na rede e, consequentemente, gerando reclamações de mau-funcionamento por parte dos usuários, nele, conectados. A interferência de sinal é outro fator prejudicial a uma rede sem fios. Segundo [Apple 2013], alguns dos efeitos causados pela interfência de sinal são a diminuição do intervalo sem fio entre os dispositivos (*laptops*, *smartphones* e *access points*, neste caso, devem estar muito mais próximos do que o projetado para poderem detectarem-se); diminuição considerável na taxa de transferência de dados (a interferência acaba causando conflito de sinais entre os dispositivos, os quais acabam sendo reenviados até o término de transferência de pacotes); perda parcial ou completa da conexão sem fio (se há muita interferência de sinal, os dispositivos sem fio conectados a um *access point* cancelam a conexão por tempo de resposta excedido).

Um *access point* de baixa qualidade possui outro complicador crucial a uma rede local. Por ser constituído, na maioria das vezes, por peças eletrônicas de segunda linha, estes dispositivos são altamente suscetíveis à falhas de operação devido à oscilações na rede elétrica. Este tipo de ocorrência acarreta travamentos no equipamento, os quais o aparelho para de responder ao gerenciamento e ao serviço ao qual fora atribuído, deixando um setor inteiro, ou parte dele, sem acesso à rede. Além disso, em diversos casos é restaurada a configuração inicial de fábrica ativando o serviço de DHCP [Bugallo et al. 2014]

no *access point*, sendo feito distribuição de endereços IP não-legítimos à rede local. Estes endereços IP são atribuídos aos computadores e dispositivos móveis mais próximos antes que o servidor DHCP autorizado responda aos solicitantes. Com isso, um novo endereçamento IP é misturado aos IPs legítimos, criando rotas alternativas para acesso e compartilhamento de recursos da rede/Internet, podendo causar lentidão na utilização dos serviços locais, por sobrecarga no *access point*.

### 2.2. *Rogue Access Points* (*Rogue AP's*)

O termo *Rogue Access Points* refere-se aos dispositivos de rede sem fios não autorizados, instalados e configurados nas organizações por pessoas não qualificadas ou preparadas tecnicamente para tal finalidade. Na maioria dos casos estas pessoas não fazem a menor ideia do quão prejudicial esta ação torna-se para garantir a segurança e disponibilidade dos serviços de rede.

### 2.3. Formas de detecção e controle

Dependendo do tamanho da rede local administrada, torna-se quase impossível detectar um *Rogue AP* sem que um usuário entre em contato informando problemas de acesso à rede sem fios de seu setor. Para isso, é de fundamental importância a organização e gerenciamento do parque de dispositivos que compõem a rede, projetando soluções que atendam às necessidades da organização, diminuindo, assim, a possibilidade de algum usuário instalar um *access point* de forma não autorizada.

As ferramentas de rede como NetStumbler [NetStumbler 2014] e inSSIDer [inSSIDer 2014] auxiliam na detecção de dispositivos de rede sem fios, coletando informações sobre os canais utilizados, *SSIDs*, tipo de chave criptográfica (se possuir), endereço físico do dispositivo, entre outras. Estas ferramentas são bastante utilizadas para a realização de *site surveys* [Cisco 2008] com a intenção de elaborar projetos para instalação de novos pontos de acesso de fio, permitindo atender locais onde a rede cabeada torna-se inviável.

A padronização de equipamentos e a definição de uma política de uso dos dispositivos de rede garantem um pouco mais de segurança nos dados trocados na rede local. A utilização do protocolo WPA (*Wi-Fi Protected Access*) - especificação de segurança definida em conjunto pelo IEEE (*Institute of Electrical and Electronics Engineers*) e *Wi-Fi Alliance*, para substituir o protocolo WEP (*Wired Equivalent Privacy*) - na sua última versão, WPA2, possui mecanismos de criptografia mais confiáveis e seguros. Porém, mesmo utilizando este método de segurança, é feito apenas autenticação e criptografia de dados entre os dispositivos de rede sem fios, não garantindo que usuários não autorizados utilizem a infraestrutura local. Neste caso, a autenticação de usuários torna-se importantíssima para assegurar que os recursos da rede sejam utilizados por pessoas previamente cadastradas.

A utilização do protocolo RADIUS (*Remote Authentication Dial in User Services*) [GNU 2009], é comumente utilizado para autenticar usuários de rede sem fios, bastando apenas configurar um servidor RADIUS e cadastrar *access points* como clientes deste serviço. Então, cada usuário recebe uma credencial de acesso, configurada em cada *laptop* ou *smartphone*, para poder utilizar a rede sem fios.

## 3. Cenário atual

Este projeto foi aplicado na Universidade Federal de Pelotas (UFPel), o qual possui mais de 404 prédios distribuídos em diversos locais, principalmente no município de Pelotas e município do Capão do Leão [UFPel 2014]. Com o projeto REUNI [MEC 2010], o crescimento e expansão da UFPel obteve-se de forma descontrolada e desorganizada, devido a falta de estrutura física para comportar os novos cursos. Para acompanhar este processo, a universidade obrigou-se a adquirir novos espaços, uma vez que esta alternativa foi a mais rápida e viável para atender de forma temporária os cursos, enquanto não houvessem locais definitivos. A Figura 1 representa os campi e prédios situados no município de Pelotas.

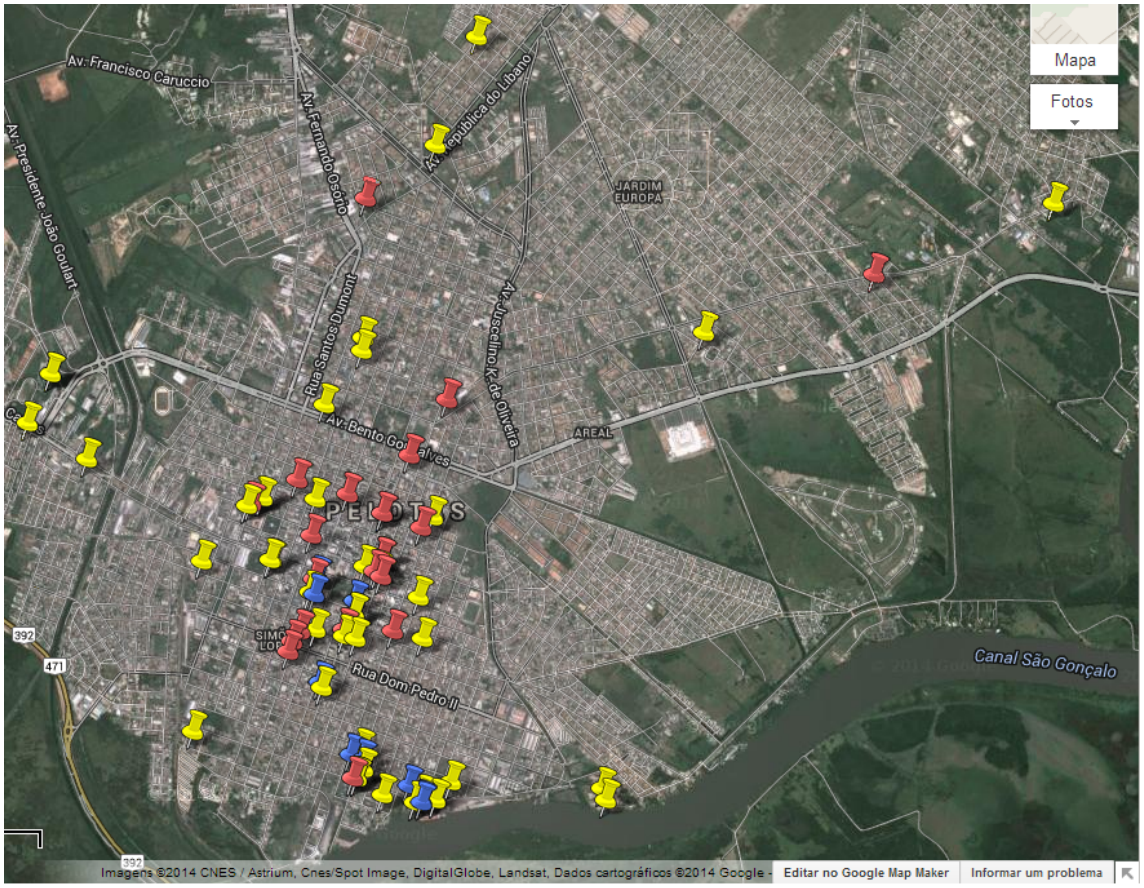


**Figura 1. Campi Pelotas - UFPel**

Com a distribuição de prédios de forma aleatória, houve um aumento considerável na demanda de assuntos relacionados à tecnologia da informação (TI). O quadro técnico de profissionais desta área não acompanhou a evolução crescente do projeto REUNI, possuindo apenas 27 profissionais divididos entre 4 Núcleos e 3 Seções. O Núcleo de Infraestrutura de TI (NITI), responsável por manter o acesso à rede/Internet e aos serviços oferecidos pela instituição em funcionamento, conta com 5 técnicos e 2 analistas de TI para atender os quase 20.000 usuários, conforme Tabela 1, e sua sede fica no Campus Capão do Leão, cerca de 11 quilômetros do centro de Pelotas.

Essa enorme demanda, que gera atrasos nos atendimentos, faz com que os próprios usuários procurem outros meios para solucionarem os problemas de acesso à rede/Internet

**Tabela 1. Recursos Humanos**

| | |
|---|---|
| Discentes de Graduação Presencial | 13.020 matriculados |
| Discentes de Graduação EaD | 2.189 matriculados |
| Discentes de Mestrado Acadêmico | 1.191 |
| Discentes de Mestrado Profissional | 68 |
| Discentes de Doutorado | 626 |
| Servidores Técnico-Administrativos | 1.234 |
| Docentes Permanentes 20h | 16 |
| Docentes Permanentes 40h | 107 |
| Docentes Permanentes 40h DE | 1.054 |
| Docente Substitutos | 8 |
| Docente Temporários | 163 |

Fonte: Universidade Federal de Pelotas

das unidades, aos quais pertencem, criando o atual problema de gerenciamento desordenado. Várias ações já foram tomadas para coibir esta prática, porém a pressa e a urgência para ter acesso aos recursos da Internet fazem com que os usuários pratiquem estes atos sigilosamente. O fator mais agravante baseia-se na dispersão entre as unidades acadêmicas e a distância entre a sede da equipe do NITI. Com esse volume de atendimentos fez-se necessário automatizar diversos serviços para suprir as necessidades diárias, aos quais este projeto também faz parte.

## 4. Sistema GhostBusters

Este projeto teve iniciativa pela forma descontrolada de *Rogue AP's* instalados na UFPel, por não ter uma política de uso de rede estabelecendo as normas e condições para implantação de equipamentos de acesso sem fio. Posto isto, a necessidade de reduzir os prejuízos causados pelos dispositivos não autorizados tornou-se crucial para manter o bom funcionamento da rede como um todo, além de garantir mais controle e segurança das informações trocadas internamente.

Para diminuir a incidência de instalações destes *Rogue AP's*, faz-se necessário projetar adequadamente a rede sem fios, de modo que não seja conveniente para o usuário fazê-lo por sua própria conta. As definições de uma política de uso, bem como sanções nos casos violados, tornam-se fundamentais, e urgentes, para que não seja permitido a utilização de dispositivos de rede sem prévia autorização. Em contrapartida, a equipe responsável pela TI da organização deve conscientizar os usuários de forma educativa, apontando argumentos de que tais práticas podem comprometer seriamente a integridade e segurança das informações pessoais, e privadas, transferidas na rede local.

O sistema GhostBusters - em homenagem ao filme "Os Caça-Fantasmas" [Ghostbusters 2014], é uma ferramenta de rede desenvolvida com a linguagem de programação **Python** [Python 2014], na qual será responsável por analisar a rede local em busca de *access points* não autorizados (*Rogue AP's*). Este *script* [Pereira 2012] é baseado em um conjunto sequencial de linhas de comando que executa rotinas, coletando e tratando as informações conforme a necessidade. Outras aplicações também fizeram-se necessárias para montar a estrutura de coleta, análise e aplicação dos resultados obti-

dos, como **Nmap** [Nmap 2014], **MySQL** [MySQL 2014], **PHP** [PHP 2014] e **SNMP** [Net-SNMP 2013].

A ideia de desenvolvimento do GhostBusters deu-se na intenção de coletar dados sobre todos os dispositivos conectados à rede local que apresentassem portas TCP/UDP [Alecrim 2007] abertas, caracterizando possíveis suspeitos. Partindo do princípio de que os servidores de rede já estariam cadastrados e facilmente conhecidos em endereços IP exclusivos, todos os outros disposivitos de rede que respondessem às rotinas de pesquisa do GhostBusters seriam cadastrados em uma base de dados na forma de "dispositivos suspeitos".

O cenário de testes foi realizado utilizando dois *switches* gerenciáveis Extreme Networks [Networks 2014], os quais foram cadastrados no GhostBusters e interligados entre si, juntamente com outros dois *access points* (TP-LINK e Allied Telesis), simulando a inserção destes, de forma escondida, na rede local. Ao serem cadastrados, definiu-se um dos *switches* como sendo o *master*, chamado "**teste**", e o outro como *slave*, chamado "**Extreme24t**", para fins de hierarquia. Desta forma, ao fazer um escaneamento na rede à procura de dispositivos, o GhostBusters terá um ponto de partida. Este método simularia a estrutura de rede partindo de um *switch* de núcleo, percorrendo as cascatas de rede para os *switches* de distribuição, até que fosse encontrado o *Rogue AP* na extremidade da rede (*switch* de acesso) [Filippetti 2009].

A cada escaneamento de rede, ao encontrar um dispositivo suspeito, o GhostBusters armazena a porta do *switch*, na qual o dispositivo fora encontrado. Seguindo a lógica anterior, é analisada a tabela de endereços físicos (*MAC Address* [Mitchell 2014a]) do *switch master* e caso o *MAC Address* de um dispositivo suspeito esteja vinculado a uma porta referenciada como cascata, o GhostBusters analisará a tabela do *switch slave*. Este ciclo encerra quando o endereço físico do dispositivo procurado é encontrado em uma porta que não seja cascata de outro *switch*. Neste cenário, o *switch* "Extreme24t" estava conectado à porta 46 do *switch* "teste" e o *uplink* de acesso às demais redes estava associado à porta 48. Os *access points* utilizados para testes, foram colocados nas portas 5 e 13 do switch "Extreme24t".

Em termos básicos, é executada uma linha de comando utilizando a ferramenta Nmap, na qual escaneia uma determinada faixa de IPs, armazenando o resultado em uma variável predefinida para uso posterior. Neste escaneamento de rede são coletados dados sobre cada dispositivo, como, *MAC Address*, fabricante da interface de rede, endereço IP e portas TCP/UDP. Depois de feito o escaneamento, o conteúdo é filtrado utilizando expressões regulares [Ramalho 2012], para que os registros, então, sejam armazenados no banco de dados. A partir desta base de conhecimento, o administrador local poderá aplicar a ação mais adequada. No ato de algum bloqueio ou permissão de acesso, é enviado um comando via Net-SNMP, alterando o OID (*Object Identifier*) [IEEE 2014] correspondente à porta do *switch*, no qual fora localizado o dispositivo suspeito. Quando o fabricante de alguma interface de rede não é reconhecido, é posto a identificação "*Unknown*" pelo Nmap, caso do *access point* TP-LINK, que mesmo sendo uma marca conhecida, utilizou, neste modelo, um controlador de rede desconhecido.

A Figura 2 apresenta a tela inicial do *script* ao ser executado via *Command Line Interface* (CLI) [Janssen 2014], mostrando um menu de opções disponíveis. Este menu

foi compactado para facilitar a organização por categorias de ações. Ao escolher a opção "1" (Figura 3), um submenu é apresentado para que seja escolhido o item a ser listado. Dentre eles, a lista de dispositivos suspeitos, *switches* cadastrados (conforme abordagem descrita anteriormente), e usuários cadastrados. Para ter acesso via web a esta ferramenta é necessário ter uma credencial previamente cadastrada no banco de dados. Desta forma, apenas pessoas autorizadas poderão aplicar ações aos casos encontrados.

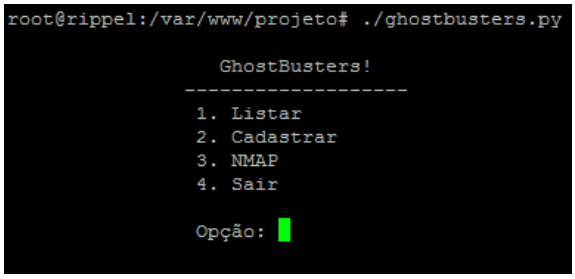


**Figura 2. GhostBusters - Menu principal**

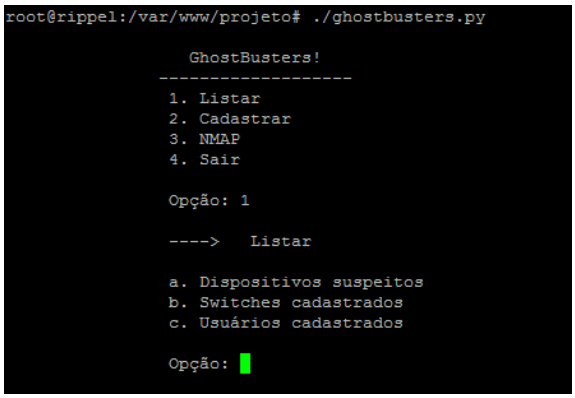


**Figura 3. GhostBusters - Menu Listar**

Selecionando a opção "a", serão apresentados os dispositivos suspeitos cadastrados na base de dados, conforme mostra a Figura 4.

Ao analisar a lista de dispositivos encontrados, é possível ter um bom embasamento visual para diagnosticar um provável suspeito. Supondo que tenha sido identificado um *Rogue AP*, é possível perceber mais detalhes e aplicar uma regra caso seja necessário, bastando selecionar o número de identificação (ID) do dispositivo, conforme mostra a Figura 5.

A segunda opção do menu principal apresenta a parte de cadastro de *switches* e usuários. Estes quesitos são muito importantes para a construção da lógica de buscas do GhostBusters e acesso via Web, respectivamente, conforme a Figura 6. Ao cadastrar um *switch*, serão solicitados o IP, a senha de acesso, a porta caso seja cascata de algum outro *switch* (neste caso, a porta de origem do *switch master*), e a possibilidade de adicionar uma descrição para a localização geográfica deste equipamento. Depois de salvos os dados, o GhostBusters acessa o *switch* e coleta o nome atribuído a ele, via Net-SNMP.

E por fim, a terceira opção do menu principal oferece o escaneamento imediato. Esta opção executa uma função chave do *script*, o qual faz todo o processo de busca por

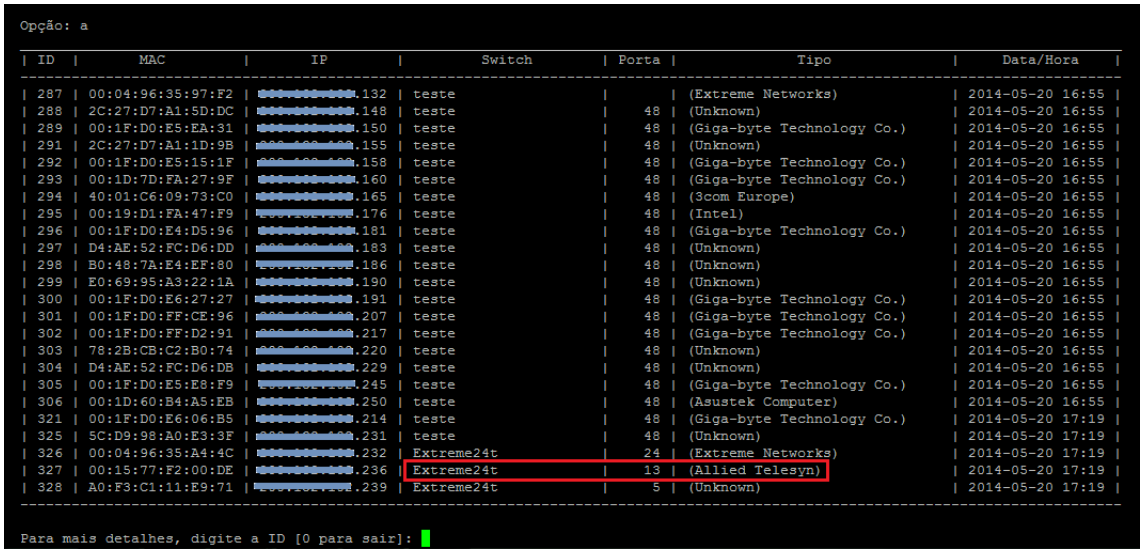


**Figura 4. GhostBusters - Dispositivos suspeitos**

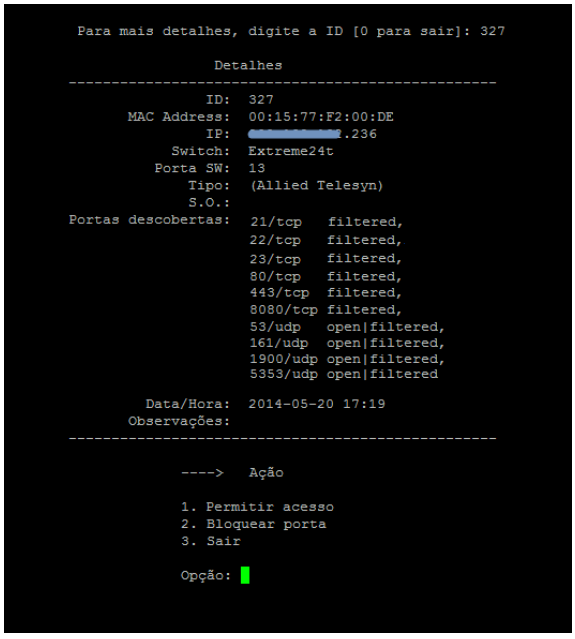


**Figura 5. GhostBusters - Detalhes do dispositivo**

dispositivos suspeitos. A Figura 7 sugere o modo de funcionamento.

Para mostrar de forma mais amigável os resultados obtidos pelo GhostBusters, foi desenvolvido um painel web com basicamente as mesmas opções da ferramenta em modo texto (CLI). A Figura 8 apresenta uma das telas - precisamente a de dispositivos encontrados - para que o admnistrador possa acionar uma regra para cada dispositivo suspeito. Assim como no exemplo anterior, nesta imagem o provável *Rogue AP* encontra-se em destaque.

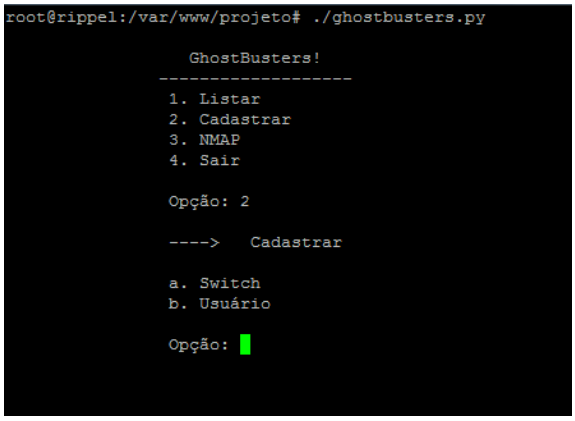


**Figura 6. GhostBusters - Menu Cadastrar**

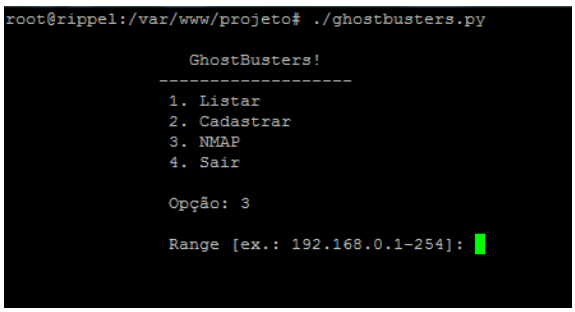


**Figura 7. GhostBusters - Nmap**

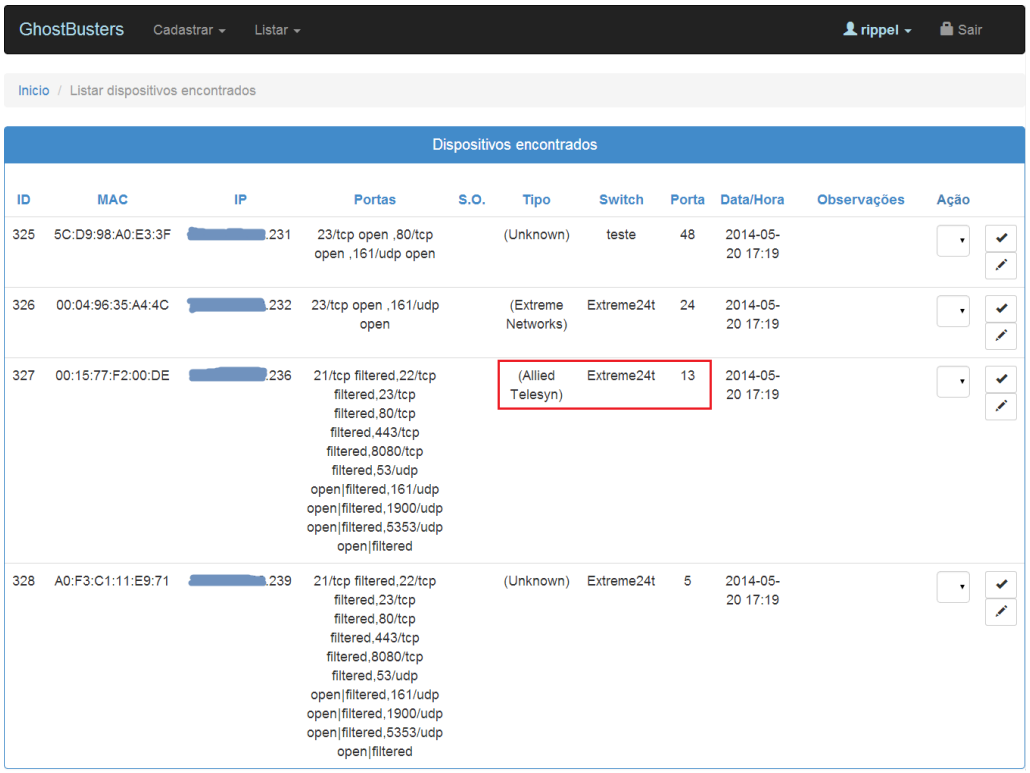


**Figura 8. GhostBusters - Painel Web**

## 5. Conclusões

A utilização inadequada de *access points* traz diversas complicações para a rede local de uma organização. A facilidade de ampliação e alcance de uma rede sem fios estimula o falso entendimento dos usuários de que os problemas diminuirão, pois enxergam a força do sinal como um fator positivo de qualidade de uso. Porém, na maioria dos casos, a quantidade de *access points* instalados é diretamente proporcional aos problemas de instabilidades na rede e aos serviços locais, por questões de interferência de sinal; quantidade exagerada de usuários conectados por ponto de acesso; e ataques oriundos pela falta de segurança nos equipamentos instalados.

A adoção de uma política de uso da rede é de fundamental importância para garantir a estabilidade, integridade e segurança das informações. A elaboração de projetos de rede para atender os segmentos não abrangidos de uma organização torna-se crucial para diminuir a incidência de *Rogue AP's*, uma vez que usuários instalam e configuram estes *access points* de forma ingênua apenas para atender o seu setor, não percebendo que este ato abre uma brecha de segurança, permitindo que terceiros acessem as informações privadas de sua organização.

Este projeto utilizou-se de alguns indícios dos próprios *access points* para que fossem descobertos na rede, sem que houvesse a necessidade de deslocamento de pessoal técnico até as unidades. Desta forma, o desenvolvimento da ferramenta de rede GhostBusters possui uma grande vantagem por ter um controle remoto dos dispositivos conectados na rede local, permitindo que estes sejam bloqueados e localizados nas unidades atendidas pela organização.

### 5.1. Projetos futuros

O projeto inicial contava com diversas ideias para compor este trabalho. Porém, por dificuldades técnicas e tempo hábil, estes tornaram-se projetos futuros. Entre eles pode-se citar (a) o bloqueio de um *MAC Address* em determinada porta de um *switch*, ao invés de bloquear a porta totalmente; (b) o desenvolvimento de um módulo que aceite a criação de modelos (*templates*) de *switches* para que o GhostBusters consiga gerenciar um parque de equipamentos heterogêneos; (c) disponibilizar um mapa da rede por meio de um gráfico de hierarquia entre os switches cadastrados; (d) automatização de ações para casos de reincidência; (e) e desenvolvimento de um módulo para gerar relatórios, estatísticas de incidências e notificações por e-mail.

## Referências


Alecrim, E. (2007). Portas TCP e UDP. Disponível em: <http://www.infowester.com/portastcpudp.php>. Acesso em: maio 2014.

Alecrim, E. (2013). Tecnologia Bluetooth: o que é e como funciona? Disponível em: <http://www.infowester.com/bluetooth.php>. Acesso em: maio 2014.

Apple (2013). Wi-fi e bluetooth: fontes potenciais de interferência sem fio. Disponível em: <http://support.apple.com/kb/ht1365?viewlocale=pt_BR&locale=pt_BR>. Acesso em: maio 2014.

Bugallo, A. M. D., Barros, M. A., and Torres, W. R. (2014). Introdução ao DHCP. Disponível em: <http://www.rnp.br/newsgen/9911/dhcp.html>. Acesso em: maio 2014.

Cisco (2008). Wireless Site Survey FAQ. Disponível em: <http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/68666-wireless-site-survey-faq.html>. Acesso em: maio 2014.

Filippetti, M. A. (2009). *CCNA 4.1*, chapter 2, page 64. Visual Books.

Ghostbusters (2014). Ghostbusters - Official Site. Disponível em: <http://www.ghostbusters.com/>. Acesso em: maio 2014.

GNU (2009). Radius - GNU Project. Disponível em: <http://www.gnu.org/software/radius/radius.html>. Acesso em: maio 2014.

IEEE (2014). What is an Object Identifier (OID)? Disponível em: <https://standards.ieee.org/develop/regauth/tut/oid.pdf>. Acesso em: maio 2014.

inSSIDer (2014). inSSIDer - Discover The Wi-Fi Around You — MetaGeek. Disponível em: <http://www.metageek.net/products/inssider/>. Acesso em: maio 2014.

InternetSemFio (2014). História da Internet sem fio. Disponível em: <http://internet-sem-fio.info/mos/view/História_da_Internet_sem_fio/>. Acesso em: maio 2014.

Janssen, C. (2014). What is a Command Line Interface (CLI)? - Definition from Techopedia. Disponível em: <http://www.techopedia.com/definition/3337/command-line-interface-cli>. Acesso em: maio 2014.

Kaspersky (2014). Segurança redes Sem-Fios :: Kaspersky Lab. Disponível em: <http://www.kaspersky.com/pt/wireless_networks>. Acesso em: maio 2014.

MEC (2010). Reuni - Reestruturação e Expansão das Universidades Federais - REUNI. Disponível em: <http://reuni.mec.gov.br/o-que-e-o-reuni>. Acesso em: maio 2014.

Mitchell, B. (2014a). Mac Addressing - introduction to the MAC Address. Disponível em: <http://compnetworking.about.com/od/networkprotocolsip/l/aa062202a.htm>. Acesso em: maio 2014.

Mitchell, B. (2014b). What Is a Hotspot in Wireless Computer Networking? Disponível em: <http://compnetworking.about.com/cs/wireless/g/bldef_hotspot.htm>. Acesso em: maio 2014.

Morimoto, C. E. (2014). Hub - Definição de Hub. Disponível em: <http://www.hardware.com.br/termos/hub>. Acesso em: maio 2014.

MySQL (2014). MySQL :: The world's most popular open source database. Disponível em: <http://www.mysql.com/>. Acesso em: maio 2014.

Net-SNMP (2013). Net-snmp. Disponível em: <http://www.net-snmp.org/>. Acesso em: maio 2014.

NetStumbler (2014). The award-winning wireless networking tool and the best source for your daily Wi-Fi, WiMAX, 3G and VoIP news. — NetStumbler. Disponível em: <http://www.netstumbler.com/>. Acesso em: maio 2014.

Networks, E. (2014). Network Infrastructure & BYOD Security - Extreme Networks. Disponível em: <http://www.extremenetworks.com/>. Acesso em: maio 2014.

Nmap (2014). Nmap - Free Security Scanner For Network Exploration & Security Audits. Disponível em: <http://nmap.org/>. Acesso em: maio 2014.

Pereira, A. L. (2012). O que é script? - Tecmundo. Disponível em: <http://www.tecmundo.com.br/programacao/1185-o-que-e-script-.htm>. Acesso em: maio 2014.

PHP (2014). PHP: Hypertext Preprocessor. Disponível em: <http://www.php.net/>. Acesso em: maio 2014.

Python (2014). The official home of the Python Programming Language. Disponível em: <https://www.python.org/about/>. Acesso em: maio 2014.

Ramalho, L. (2012). Expressões regulares: introdução - Mini Tutorial RegEx. Disponível em: <http://turing.com.br/material/regex/introducao.html>. Acesso em: maio 2014.

Solha, L. E. V. A., Teixeira, R. C., and Piccolini, J. D. B. (2014). Tudo que você precisa saber sobre os ataques DDoS. Disponível em: <http://www.rnp.br/newsgen/0003/ddos.html>. Acesso em: maio 2014.

UFPel (2014). Institucional - Histórico - UFPel. Disponível em: <http://portal.ufpel.edu.br/historico/>. Acesso em: maio 2014.