Sistema de detecção e controle para dispositivos de rede sem fios não autorizados

Henrique de Vasconcellos Rippel[1], **Eduardo Maroñas Monks**[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,emmonks}@gmail.com

Resumo. *A facilidade de uso 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. Neste artigo é apresentada uma ferramenta capaz de identificar dispositivos ativos não autorizados de forma centralizada em um cenário de rede de grande porte.*

Abstract. *The ease of use of wireless devices without authorization can easily compromise information security and cause instability in the local network, significantly impairing the functioning of an organization. In this paper a tool to identify active unauthorized devices centrally in a scenario of a large network is presented.*

1. Introdução

Os benefícios oriundos da rede sem fios são incontestáveis pela facilidade de acesso, mobilidade, praticidade e alcance, pois conforme a tecnologia investida no equipamento, a qualidade e a eficiência tornam-se satisfatórias. A utilização não adequada de dispositivos de rede sem fios traz sérios problemas de segurança, comprometendo desse modo usuários e, principalmente, as informações sigilosas de uma organização.

O baixo custo de aquisição destes *access points* 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 com 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 artigo foi desenvolvido na Universidade Federal de Pelotas (UFPel) para controlar a enorme incidência de dispositivos não autorizados na rede. Por possuir 5 campi e diversos outros prédios espalhados pelas cidades de Pelotas e Capão do Leão, há grande dificuldade de controlar a inserção destes equipamentos, visto que o parque de *switches* da instituição não é padronizado, tornando-se, assim, complexo no âmbito gerencial.

Frente ao exposto, o intuito deste artigo será apresentar um módulo de detecção de dispositivos suspeitos na rede local, por meio de características básicas encontradas nos próprios dispositivos, abordando uma simples metodologia de buscas na rede. Cabe salientar que este sistema faz parte de um projeto experimental adaptado às necessidades de controle com base nas peculiaridades encontradas diariamente na UFPel.

2. Riscos iminentes

Todo e qualquer projeto de rede 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 na rede, 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), disseminar vírus e explorar vulnerabilidades computacionais utilizando a infraestrutura lógica da própria organização.

Por utilizar o ar como meio de transmissão, a rede sem fios desempenha o mesmo papel funcional de um *hub*, 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 não havendo criptografia nos dados, qualquer usuário poderia coletar estas informações.

O número de usuários conectados influencia diretamente no desempenho 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) 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); (b) a 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); (c) e a 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 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*.

2.1. *Rogue Access Points* (*Rogue APs*)

O termo *Rogue Access Points* [Leslie 2004] 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.

3. Formas de detecção e controle

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

Para diminuir a incidência de instalações destes *Rogue APs*, 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 de violação, 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 privadas transferidas na rede local. Segundo [Nakamura and Lima 2003], "um dos principais mecanismos de proteção contra o ataque que envolve Rogue APs é o IEEE 802.1X, que possibilita que os usuários realizem a autenticação dos pontos de acesso aos quais se associam, evitando assim que se associem a pontos de acesso piratas".

3.1. Metodologia

Foi desenvolvido um *script* na linguagem de programação Python automatizando as etapas de abordagem para detecção de sub-redes não autorizadas, em dois estágios: (a) ao executar o *script* em um *gateway* de rede, é acionada a ferramenta Nmap para coletar dados relevantes sobre cada *host* conectado à rede local. Estes dados são tratados e armazenados em banco de dados a fim de serem listados na forma de dispositivos suspeitos. Com a opção "*fingerprint*" encapsulada nas pesquisas, a assinatura digital de grande quantidade de *hosts* de rede é exibida e armazenada, diminuindo os alertas de falsos positivos. Isto quer dizer que no caso de equipamentos estarem configurados em modo roteamento (NAT), estes *access points* são identificados na rede pelo mesmo método de assinatura digital do fabricante da interface de rede; (b) a segunda técnica utilizada no módulo de rede é utilizando o uso do mecanismo de *site survey*, disponível nos *access points* credenciados no projeto de rede sem fios institucional. Desta forma, é feito triangulação entre *access points*, comprovando a existência e a localização aproximada de um dispositivo não autorizado na rede. Esta técnica auxilia na busca por dispositivos que estejam configurados em modo *bridge*, uma vez que servem apenas para repassar o tráfego de rede entre os clientes conectados a ele.

A lógica de funcionamento deste módulo de buscas baseia-se na probabilidade de um dispositivo estar ofertando serviços de rede, como resolução de nomes (DNS),

distribuição de endereços IP (DHCP), páginas Web (HTTP) e demais serviços que não caracterizem o comportamento real de um *host* convencional em uma rede administrativa/acadêmica. Para casos excepcionais, como projetos de pesquisa e similares, as varreduras nos endereços cadastrados para este fim são desconsiderados. Cada curso ou unidade predial da UFPel é representado por uma faixa exclusiva de endereços IP. Em cada um dos *gateways* de rede da instituição é executado periodicamente o módulo de buscas de dispositivos, a fim de capturar informações pertinentes a incidências de ativos não autorizados.

Para iniciar a rotina de buscas, faz-se necessário (a) cadastrar na base de dados os *switches* que farão parte da estrutura de pesquisas; (b) cadastrar as faixas de endereços IP das unidades prediais ou cursos a serem escaneados; (c) e criar a lista de exceções (faixas de endereços IP e *switches*). Ao cadastrar um novo *switch* no parque, define-se que ele será cascata de outro, ou não. Com esta premissa, a lógica de funcionamento encadeará a rotina de comandos do *script*, fazendo com que, caso seja encontrado um endereço *MAC* (*Media Access Control* ou *mac address*) em uma porta de cascata de rede, seja acessado este outro *switch* à procura deste *mac address*.

3.2. Testes realizados

O cenário de testes foi composto por dois *switches* gerenciáveis da marca Extreme Networks, modelo Summit200, os quais foram cadastrados no sistema de detecção e interligados entre si, juntamente com outros dois *access points* (TP-LINK e Allied Telesis), simulando a inserção destes, de forma não permitida, na rede local. Ao serem cadastrados, definiu-se um dos *switches* como o de núcleo da rede, chamado "**teste**", e o outro como acesso, chamado "**Extreme24t**", para fins de hierarquia. A Figura 1 ilustra o cenário de testes.

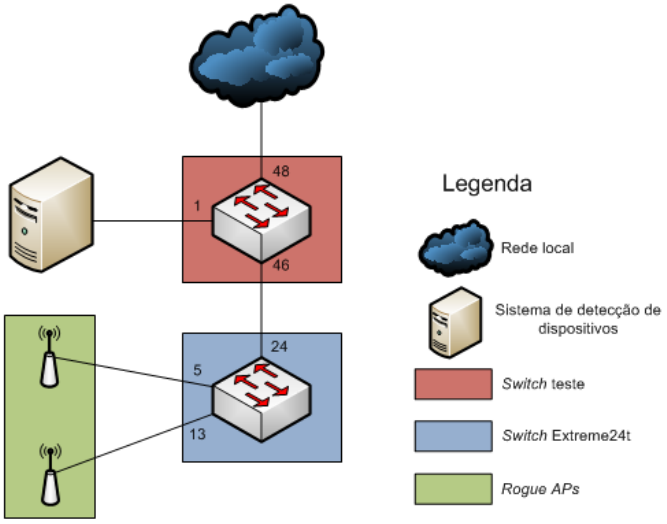

Figura 1. Cenário de testes

Seguindo a lógica da seção anterior, dois *access points* foram inseridos na rede local. Após o escaneamento da rede à procura por dispositivos suspeitos, foi analisada a tabela de endereços *MAC* do *switch* "teste". Caso o *mac address* de um dispositivo suspeito esteja vinculado a uma porta referenciada como cascata, é, então, analisada a tabela

do *switch* “Extreme24t”. 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”, e foi possível reconhecer pelo menos um deles apenas pelo fabricante do dispositivo, relacionado com o *Organizationally Unique Identifier* (OUI) da interface de rede, conforme mostra a Figura 2.

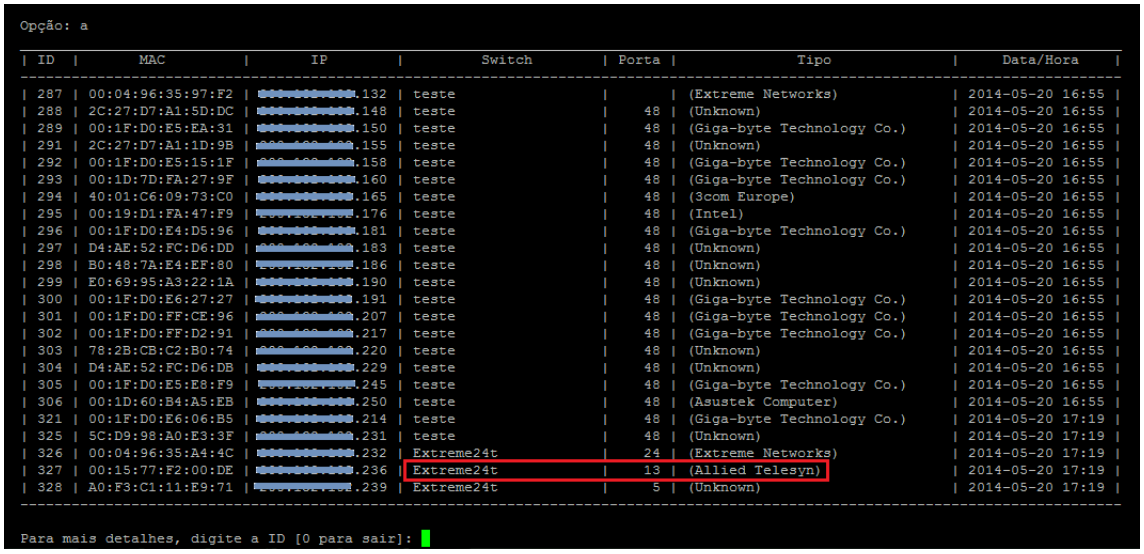

Figura 2. Dispositivos suspeitos

Um segundo teste foi realizado em ambientes reais da UFPel, executado em *access points* credenciados da rede sem fios institucional (WUFPel), coletando dados por 3 semanas, em amostras de 15 em 15 minutos e armazenando dados como SSID, canal, nível e qualidade do sinal e *mac address* dos dispositivos não credenciados, em uma base de dados. A Tabela 1 contém o resultado das coletas armazenadas, apresentando a quantidade de *access points* únicos encontrados nas varreduras, listados pela qualidade de sinal maior do que -60 dBm. Para estas coletas foram consideradas como AP não autorizado todos aqueles que não possuíssem o prefixo “WUFPEL” na SSID. Outras validações podem ser feitas, tais como a relação entre o fabricante do AP legítimo e o nome WUFPEL. Entretanto, na Tabela 1, foram levadas em consideração a relação do fabricante com o SSID.

Tabela 1. Resultados das coletas de redes sem fios não autorizadas por campi da UFPEL

Local	Quantidade de SSIDs não autorizados
Centro	8
Capão do Leão	68
Anglo	57
Cotada	6

Fonte: Universidade Federal de Pelotas

4. Conclusões

É notável os benefícios adquiridos pela utilização da rede sem fios por sua praticidade, baixo custo e alcance. Embora apresente inúmeras vantagens, os dispositivos não autorizados ocasionarão diversos problemas na rede local, comprometendo a disponibilidade dos serviços, além de permitir o compartilhamento de informações privadas sem o consentimento dos responsáveis.

Este artigo apresentou uma ferramenta de rede que utilizou 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 deste módulo de detecção possui uma grande vantagem por ter um controle centralizado dos dispositivos conectados na rede, permitindo que estes sejam bloqueados remotamente se necessário.

4.1. Dificuldades encontradas

A maior dificuldade encontrada durante o desenvolvimento desta ferramenta foi no período em que os testes haviam sido realizados com um *switch* da marca Extreme Networks e o outro, do fabricante D-Link. Por serem de marcas diferentes, já era esperado que não houvesse o mesmo padrão nas pesquisas por dispostivos na rede. Isto fez com que fosse utilizado um outro *switch* Extreme Networks para a realização de testes.

E por fim, a segunda dificuldade encontrada fora a aplicação de um mecanismo de bloqueio por *mac address* em um dos *switches*. Este método não foi possível devido a OID (*Object identifier*) do agente SNMP no *switch* ter somente funções de leitura.

4.2. Projetos futuros

Para dar andamento a este sistema de detecção de dispositivos suspeitos, faz-se necessário destacar as futuras funcionalidades, como (a) o bloqueio de *mac address*; (b) criação de *templates* de *switches*; (c) automatização de ações para casos reincidentes; (d) um módulo para gerar relatórios, estatísticas e notificações; (e) e o desenvolvimento de um painel administrativo via Web.

Referências

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.

Leslie, D. (2004). Rogue Wireless Access Point Detection and Remediation. Disponível em: <http://www.giac.org/paper/gsec/4060/rogue-wireless-access-point-detection-remediation/106460>. Acesso em: maio 2014.

Nakamura, E. T. and Lima, M. B. (2003). Rogue access point, um grande risco para wlan. Disponível em: <http://www.las.ic.unicamp.br/srac/imagens/SSI2003-RogueAP.pdf>. Acesso em: maio 2014.