Ferramenta de Proteção Contra Ataques de IP e MAC Spoofing em Redes Sem Fio 802.1X

Gabriele B. Vieira, Jéssica A. Gonçalves, Camilla A. M. Silva, Vinicius S. Faria, Dalbert M. Mascarenhas

***Resumo*— Os ataques de falsificação de IP e falsificação de endereços MAC, conhecidos como IP *spoofing* e MAC *spoofing*, respectivamente, têm aumentado a dificuldade de detecção e contenção de ações de usuários maliciosos dentro de redes sem fio. Este trabalho apresenta uma ferramenta para detecção e bloqueio de ataques de IP *spoofing* e MAC *spoofing* em uma rede sem fio utilizando o protocolo IEEE 802.1X. Para isto é utilizada uma combinação de informações obtidas na análise de logs e dados do banco de usuários do servidor Radius. Estas informações são também analisadas em conjunto com as informações de tabela ARP e logs de TCPdump dos roteadores.**

***Palavras-Chave*— 802.1X, MAC spoofing, IP spoofing, IPS.**

***Abstract*— IP address spoofing and MAC address spoofing attacks, known as IP spoofing and MAC spoofing, respectively, have increased the difficulty of detecting and containing malicious actions from users within wireless networks. This paper presents a tool for detecting and blocking IP spoofing and MAC spoofing attacks on a wireless network using the IEEE 802.1X protocol. For this purpose, our tool uses a combination of information obtained in the analysis of logs and learning of the Radius server user database. This information is also analyzed in conjunction with information from the ARP table and TCPdump logs of the routers.**

***Keywords*— 802.1X, MAC spoofing, IP spoofing, IPS.**

I. Introdução

A utilização de redes sem fio em redes locais nos últimos anos tem proporcionado um aumento na utilização de dispositivos móveis [1]. Estas redes possuem características como a flexibilidade de implantação e mobilidade, estes fatores contribuem para a adesão cada vez maior de usuários de ambientes domésticos e ambientes corporativos [2]. Devido à natureza física deste tipo de rede, que utiliza difusão de mensagens em um meio compartilhado, a segurança da rede e os dados que nela trafegam podem estar vulneráveis. Portanto, a proteção dos dados trafegados e dos recursos da rede precisa ser cuidadosamente analisada. Esta proteção pode ocorrer em diferentes níveis, incluindo a identificação, a autenticação e a autorização de acesso à rede que comporta esses recursos.

O IEEE 802.1X é um protocolo de estrutura cliente-servidor de controle e autenticação. Este protocolo pode ser utilizado em uma rede sem fio utilizando dispositivos de acesso e dispositivos de controle de acesso [3]. Nas redes que utilizam o protocolo 802.1X, o dispositivo de controle de acesso pode estabelecer um túnel de autenticação com o dispositivo de acesso, neste caso o dispositivo cliente. Nesta estrutura, todo pedido de conexão de um usuário à rede é encaminhado para o dispositivo de controle de acesso. Este dispositivo realiza a autenticação do usuário na rede. O usuário pode ter o pedido de conexão concedido ou negado pelo dispositivo de controle de acesso.

Engenharia de Computação, CEFET/RJ campus Petrópolis/RJ, {jalcantara,vfaria,gbritto,calves}@e-computacao.com.br, dalbert.mascarenhas@cefet-rj.br

Atuando como um dispositivo de controle de acesso em uma rede 802.1X, o servidor Radius (Remote Authentication Dial In User Service) provê autenticação, autorização e contabilização de acessos. No processo de autenticação ocorre a verificação da validade de usuário e senha. Na autorização as permissões que o usuário possui no sistema são verificadas, com o objetivo de identificar o que o usuário pode acessar. A contabilização consiste no monitoramento das atividades do usuário relativas a utilização dos serviços da rede.

Nas redes sem fio, a difusão de mensagens em meio compartilhado pode propiciar ataques que utilizam informações coletadas na área de cobertura da rede. Desta forma, um atacante pode capturar dados transmitidos na rede e obter informações relativas às identidades de usuários válidos, como endereços IP e MAC. De posse dessas informações, o atacante pode forjar a sua própria identificação dentro da rede, fazendo-se passar por um usuário legítimo ou até mesmo por servidores e nós de gerência e controle.

A utilização do 802.1X em conjunto com o Radius possibilita maior controle do acesso à rede sem fio, contudo, a combinação não elimina as ameaças advindas da falsificação de endereços IP e MAC. Desta forma, atacantes podem forjar endereços IPs ou MACs e realizar ataques dentro de uma rede 802.1X. Ataques de MAC e IP *spoofing* fundamentam-se justamente em forjar endereços MAC e IP de origem dos pacotes, com o objetivo de mascarar a sua verdadeira origem e realizar ações maliciosas na rede. Os endereços forjados podem ser considerados válidos na rede, o que pode causar danos ainda maiores por medidas de contenção de ataques. Este aumento de danos se torna crítico quando ferramentas de proteção, como sistemas de prevenção de intrusos, que promovem um isolamento de máquinas suspeitas e consequentemente impedem a comunicação de máquinas que tiveram seus endereços copiados e usados em ataques.

Dentre os ataques que podem ser usados combinados ao endereço MAC e endereço IP há o ataque de negação de serviço DoS (*Denial of Service*). Os ataques de DoS têm como propósito causar a interrupção de um serviço ou recurso disponibilizado na rede [4]. Este ataque é comumente executado sobre dois modos: através do esgotamento de recursos de sua vítima e através da exploração de vulnerabilidades. O DoS é responsável por grande parte das ameaças à segurança de sistemas na atualidade e parte dos ataques de DoS são feitos juntamente com a utilização de MAC ou IP *spoofing* [5].

Este trabalho apresenta uma ferramenta capaz de interceptar e bloquear ataques de IP e MAC *spoofing* em uma rede sem fio 802.1X. A proposta tem como objetivo detectar e neutralizar um IP *spoofing* ou MAC *spoofing* antes que o atacante seja capaz de realizar um ataque de negação de serviço contra serviços ou dispositivos da rede. A ferramenta proposta utiliza medidas de contenção diretamente no *login* do usuário malicioso. Desta forma, espera-se evitar bloqueios indevidos de usuários válidos que tiveram seus endereços IP ou MAC forjados por um atacante na rede. A detecção de cada tipo de ataque abordado ocorre sobre dois modos:

- A identificação de um ataque de IP *spoofing* através da análise da quantidade de endereços IP associados a um mesmo endereço MAC;

- A detecção da ocorrência de um MAC *spoofing* quando existe mais de um login associado a um mesmo endereço MAC;

A ferramenta proposta atua em conjunto com um servidor Radius para prover autenticação e a contabilização de acessos à rede 802.1X. A ferramenta promove a colaboração entre os roteadores da rede e o servidor Controlador. O servidor Controlador é a máquina que contém o módulo da ferramenta de análise de informações do Radius e também hospeda o servidor Radius. O outro módulo da ferramenta atua nos roteadores, possibilitando a detecção de um ataque o mais próximo de sua origem e consequentemente tornando o processo de contenção do ataque mais rápido.

A organização do trabalho é descrita a seguir. A seção II apresenta um resumo sobre o IEEE 802.1X descrevendo seu funcionamento. Os trabalhos relacionados que abordam a detecção de MAC ou IP *spoofing* em redes sem fio utilizando 802.1X são apresentados na seção III. A seção IV descreve a ferramenta proposta. Os resultados dos experimentos são descritos na seção V e posteriormente a conclusão é apresentada na seção VI.

II. IEEE 802.1X

O padrão para redes sem fio IEEE 802.11, apresenta vulnerabilidades de segurança que tornam difícil o rastreamento das ações dos usuários na rede, principalmente quando estes utilizam técnicas de disfarce de endereços. O padrão IEEE 802.1X é uma opção para controle de acesso, autenticação e gerenciamento de chaves em uma rede sem fio.

O 802.1X provê a autenticação dos usuários baseado em portas. O padrão conta com diversos métodos de autenticação. O método abordado neste trabalho é o que utiliza um servidor de autenticação. A sua estrutura consiste nos componentes de dispositivo de acesso, denominado autenticador, e dispositivo de controle de acesso, o servidor de autenticação. Este padrão utiliza como base o protocolo EAP - *Extensible Authentication Protocol*, um framework de autenticação. A principal funcionalidade do 802.1X é a troca de mensagens EAP entre o dispositivo cliente, comumente denominado suplicante, o autenticador e o servidor de autenticação.

O suplicante solicita acesso à rede por meio do autenticador, que pode ser um AP (*Access Point*). Inicialmente, o estado da porta utilizada na conexão é configurado como "não autorizado". Neste estado, somente pacotes do tipo 802.1X são permitidos. O autenticador envia ao suplicante um pacote *EAP-request*, que por sua vez responde com um pacote *EAP-response*. O autenticador encaminha a mensagem recebida ao servidor de autenticação, como o servidor Radius. Este tem a função de validar as credenciais de acesso do suplicante. Após a verificação, o servidor Radius envia ao AP a confirmação ou negação de acesso do suplicante. Em caso de confirmação, o estado da porta no AP é modificado para "autorizado". Após esta etapa, o cliente tem acesso aos recursos disponibilizados na rede.

III. Trabalhos Relacionados

Parte dos trabalhos sobre detecção de MAC *spoofing* utilizam a análise de características específicas da transmissão de sinal de cada placa de rede [6], [7], [8], [9]. No entanto a detecção baseada em características de sinal apresenta um alto número de falsos positivos em função da característica instável do meio. Lackner *et al.* argumentam que soluções baseadas em características de sinal necessitam de hardware específico. Este argumento também é mencionado por Banakh *et al.* [10]. Hwang *et al.* realizam um estudo das vulnerabilidade de redes 802.1X e propõem um framework para esta análise [11]. No entanto, diferentemente do que está sendo proposto neste trabalho os autores de [11] se concentram em ataques de falsificação de Access Point. Diferentemente dos trabalhos apresentados, a proposta neste trabalho detecta e bloqueia IP *spoffing* e MAC *spoofing* sem a necessidade de análise de força de sinal ou características relacionadas à placas de redes específicas. A ferramenta proposta utiliza informações da base de dados do Radius vinculada a coletas de informações de tabelas ARP e *logs* de TCPdump para a detecção de usuários maliciosos. Portanto, a proposta não precisa de investimento em hardwares específicos para a detecção dos dois tipos de ataque abordados.

IV. Proposta

O trabalho apresenta uma ferramenta capaz de detectar e bloquear ataques de IP *spoofing* e MAC *spoofing*. Após a detecção de um comportamento suspeito caracterizado como um dos ataques mencionados, a ferramenta inicia ações preventivas para contenção do tráfego malicioso. O objetivo principal da solução é identificar corretamente um atacante, ainda que este utilize endereços IP ou MAC forjados para disparar ataques na rede. Reconhecer a verdadeira origem de um ataque implica em uma menor incidência de falso positivos, cenário em que um usuário legítimo é erroneamente identificado como um atacante. A correta categorização de um usuário suspeito viabiliza políticas de contenção mais justas, onde um usuário legítimo não é afetado por bloqueios indevidos e outras medidas restritivas.

A ferramenta proposta é dividida em dois módulos: o módulo que atua nos roteadores e o módulo que atua no servidor que hospeda o Radius, chamado aqui de módulo Controlador. Os roteadores são o ponto de acesso para conexão do usuário à rede. Todas as requisições de conexão recebidas pelos roteadores são encaminhadas ao servidor de autenticação

Radius. O Radius analisa cada solicitação com base no login e senha do usuário. Após a verificação, o servidor pode autorizar o pedido de conexão do cliente, confirmando a solicitação ao roteador que a encaminhou. Com sua solicitação aceita, o cliente passa a ter acesso aos recursos da rede de acordo com o que lhe é permitido, tendo como base os seus níveis de acesso previamente configurados.

A ferramenta proposta atua de forma distribuída sobre os roteadores e o servidor Radius. A ferramenta utiliza módulos que atuam nos roteadores e no servidor que hospeda o Radius para a detecção de ataques de IP/MAC *spoofing*. Os *logs* e dados de tráfego são analisados para possibilitar a detecção de comportamentos anômalos. O módulo executado nos roteadores envia alertas de possíveis ataques para os módulos executados nos outros roteadores e para o Controlador. O módulo do Controlador é responsável por detectar ataques e também por aceitar alertas de ataques e iniciar os procedimentos de bloqueio. Este comportamento da ferramenta possibilita a identificação de anomalias e a pronta ação de prevenção mais próximo da origem do ataque de IP ou MAC *spoofing*.

A ação de detecção de um IP *spoofing*, que é executada dentro dos roteadores, utiliza a análise da tabela ARP e dados de tráfego para detectar o ataque. Já a detecção de um ataque de MAC *spoofing* é realizada sobre os *logs* de conexão do servidor Radius.

A detecção e consecutiva tratativa dos ataques citados se dá sob dois diferentes modos, que são descritos a seguir.

A. Detecção de IP spoofing

A Figura 1 mostra o funcionamento do ataque de IP *spoofing*. Este ataque é detectado pela ferramenta através de duas formas: uma utilizando a tabela ARP e outra através de logs do TCPDump. Utilizando a análise da tabela ARP buscase a relação dos endereços IPs associados aos endereços MACs de cada dispositivo conectado à rede. Para a detecção deste tipo de ataque, o roteador varre a sua tabela ARP em busca de endereços MACs associados a mais de um endereço IP, caracterizando esse comportamento como suspeito.

Outra forma de identificação é a análise de registros de tráfegos obtidos usando o TCPDump. O TCPDump permite gerar uma lista de *logs* de pacotes que entram e saem das interfaces do roteador. A ferramenta analisa estes *logs* e procura por mais de um IP associado a um mesmo MAC.

As duas formas de detecção ampliam o escopo de identificação de ataques de IP *spoofing*. A detecção baseada na tabela ARP atua de forma mais rápida em tipos de ataques que utilizam interfaces adicionais para realizar ataques direcionados à vulnerabilidade de servidores de aplicação. Parte destes ataques precisam manter uma conexão com o servidor alvo, como o Slowloris [12]. Outros tipos de ataques podem utilizar o IP *spoffing* apenas falsificando o IP de origem no pacote, sem a necessidade de uma conexão com o servidor alvo, como os ataques de DoS do Ethercap. Neste caso são utilizados os logs colhidos periodicamente com o TCPDump para verificar se existe mais de um IP associado à um mesmo MAC.

Uma vez identificado o ataque, o roteador bloqueia o endereço MAC e em seguida cria uma lista chamada de *Blacklist*

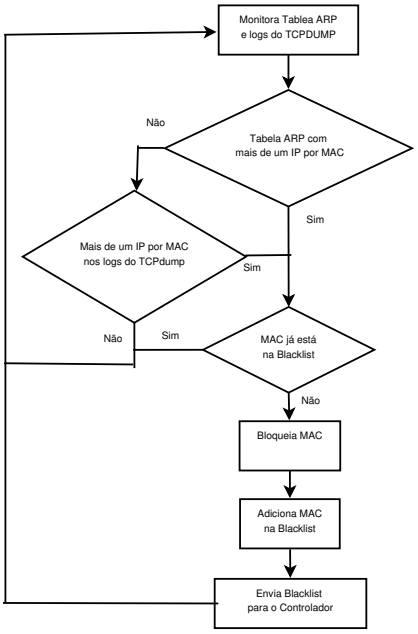

Fig. 1. Módulo de detecção de IPspoffing nos roteadores

.

contendo o MAC ou os MACs que foram encontrados em pelo menos uma das formas de detecção. Em seguida, a *Blacklist* é enviada para o servidor Controlador.

Dentro do servidor Controlador, que hospeda o servidor Radius, estará o outro módulo do programa que recebe essa *Blacklist*. A Figura 2 apresenta o funcionamento deste módulo que analisa o histórico dos *logs* do servidor Radius para encontrar MACs que foram identificados como pertencentes à usuários maliciosos. Uma vez encontrados o MAC ou os MACs dos atacantes na análise de *logs* do Radius, a ferramenta inicia o processo de bloqueio do *login* do atacante. Este bloqueio é realizado excluindo o *login* da base de dados do Radius e em seguida enviando um pedido de desconexão para o MAC apontado. Após o bloqueio do *login* e desconexão do MAC, uma nova lista é enviada aos roteadores indicando que já podem remover o MAC da *Blacklist*. O motivo desta remoção se deve ao fato de que com o login desabilitado o atacante não poderá mais efetuar ataques nesta rede e consequentemente não é necessário manter uma lista com MACs de usuários que já não fazem mais parte da rede.

B. Detecção de MAC spoofing

Para a detecção de um ataque de MAC *spoofing*, a análise é realizada exclusivamente no servidor Controlador. A ferramenta realiza continuamente uma busca nos *logs* de dispositivos conectados do Radius. O objetivo é identificar o cenário em que um mesmo MAC aparece conectado sob múltiplos logins ao mesmo tempo. Uma vez encontrada a anomalia, a ferramenta analisa o histórico de uso do *login* e MAC. O objetivo desta análise de histórico é verificar a qual login o MAC tem se conectado ao longo do tempo. Com base na análise deste histórico a ferramenta toma a decisão de classificar como atacante o login que apresenta o menor histórico de utilização do MAC identificado.

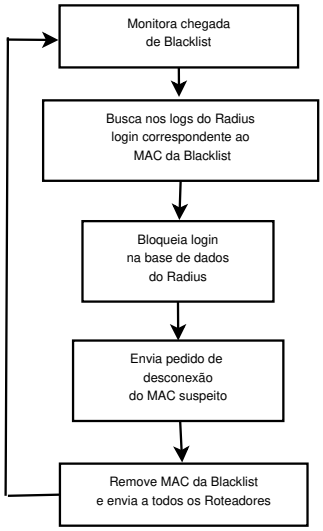

Fig. 2. Módulo de detecção de IP *spoffing* no Controlador

.

Fig. 3. Módulo de detecção de ARP *spoofing* no Controlador

.

Supõe-se que o usuário legítimo se conectou primeiro à rede, considerando o caso em que o atacante aguardou pela conexão da vítima a fim de obter o seu endereço MAC por meio de ferramentas de *sniffing*. Este tipo de ferramenta possibilita ao atacante analisar os pacotes que trafegam na rede e obter informações como o endereço MAC de seu alvo. Desta forma, ao identificar o último login utilizado para conexão de um dispositivo, este *login* é categorizado como suspeito e a ferramenta bloqueia o *login* na base de dados do Radius e em seguida envia um pedido de desconexão para o MAC em questão.

Cabe ressaltar que neste caso quando o pedido de desconexão de MAC for realizado no Radius, tanto a vítima como o atacante serão desconectados. No entanto, a vítima fica desconectada por um curto espaço de tempo já que o próprio protocolo 802.1X tenta reconectar imediatamente. Em contrapartida, o atacante fica impossibilitado de reconectar à rede pois seu login já está bloqueado.

V. Resultados

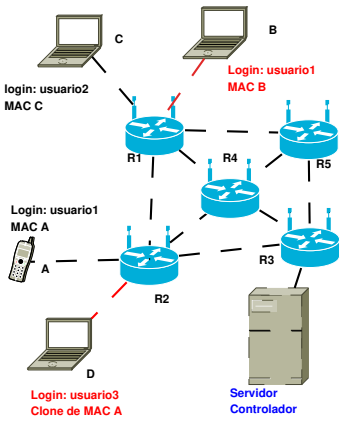

Fig. 4. Cenário do Teste 1

.

A Figura 4 apresenta o cenário de testes usado em laboratório. Os hardwares utilizados foram: 5 Roteadores sem-fio TEW-632BRP, um *Desktop* I5-4590 8 GB , três notebooks AMD A8-4500M com 8 GB, 1 Smartfone. O *Desktop* e os notebooks utilizam Ubuntu 18. Os roteadores tiveram seus *firmwares* substituídos pelo Open-WRT. Esta substituição ocorreu para permitir a instalação dos módulos da ferramenta nos roteadores. Os experimentos foram divididos em um experimento para ataque de IP *spoofing* e outro para MAC *spoofing*.

A. Experimento com IP Spoofing

O primeiro experimento utiliza ataque de IP *spoofing*. Para isto, a máquina B após se conectar à rede executa uma ferramenta de falsificação de IPs com o objetivo de causar um DoS no Servidor Web utilizando o Ettercap [13]. Assim que a máquina B começa a transferir pacotes falsificando seu IP de origem, o módulo de detecção de IP *spoofing* detecta nos *logs* do TCPdump um mesmo MAC sendo atribuído a mais de um IP e consequentemente bloqueia o MAC no próprio roteador (R1). Após isso, a ferramenta adiciona o MAC B na *Blacklist* e envia para o Controlador. O Controlador compara o MAC B com os *logs* de MACs do servidor Radius e descobre o login utilizado: *usuario2*. A próxima etapa é bloquear o *usuario2* na base de dados do Radius e enviar o comando de desconexão 802.1X passando como parâmetro o MAC B. Em seguida o Controlador retira o MAC B da *Blacklist* e a envia aos roteadores.

O atacante B é bloqueado no momento em que o módulo que atua no roteador bloqueia seu MAC. Após a desconexão no Controlador e bloqueio do MAC o roteador recebe a nova *Blacklist* do controlador sem o MAC B. Após o bloqueio e desconexão do login, o atacante B não consegue mais ter acesso à rede. Desta forma, o roteador não precisa continuar bloqueando localmente o MAC B.

O experimento foi realizado 10 vezes, e os seus resultados estão apresentados na Tabela I. Esta tabela apresenta o

momento de início do ataque, o momento em que o *login* é bloqueado e o tempo total entre o início do ataque e o bloqueio do *login* do atacante. A média do tempo de bloqueio de *login* foi de 3.044s, no entanto vale ressaltar que o bloqueio do MAC atacante no roteador aconteceu antes mesmo do roteador enviar a *Blacklist*.

O tempo de detecção de um ataque é crucial em relação ao impacto causado na rede. Quanto antes detectado, menores são as chances do atacante obter sucesso nas ações contra recursos e usuários da rede. A média de tempo obtida durante o experimento aliada à característica do bloqueio do MAC do atacante no roteador, possibilitou a contenção do tráfego malicioso antes que os recursos do Servidor Web fossem comprometidos, impedindo assim o sucesso do ataque.

TABELA I
TESTE 1: TEMPO DE INÍCIO E FIM DO ATAQUE, TEMPO TOTAL PARA BLOQUEIO DE LOGIN

Início	Fim	Tempo
38.410s	40.144s	1.734s
29.430s	31.749s	2.319s
33.740s	37.730s	3.990s
53.15s	57.151s	4.001s
21.527s	23.715s	2.188s
47.724s	50.253s	2.529s
21.260s	26.140s	4.880s
51.540s	53.350s	1.810s
10.382s	14.501s	4.118s
12.051s	14.924s	2.873s

B. Experimento com MAC Spoofing

No segundo experimento, um usuário malicioso situado na máquina B ouve a rede com uma ferramenta de *sniffing* e detecta o MAC de A comunicando com a rede. Após isso, o atacante D clona o MAC de A e realiza o login na rede. Neste caso, o módulo de MAC *spoofing* que está no Controlador detecta em sua análise de *logs* do Radius que houveram dois logins diferentes (*usuario1* e *usuario3*) com o mesmo MAC A. A ferramenta analisa o histórico e verifica que o *usuario1* tem um histórico de utilização do MAC A maior que o do *usuario3*. Neste caso a ferramenta classifica o usuario3 como malicioso e em seguida bloqueia seu login na base de autorização do Radius e em seguida envia um pedido de desconexão para o MAC A. Neste caso tanto o *usuario1* como o *usuario3* vão ser desconectados. No entanto, o usuario1 tenta reconexão automática e tem sucesso. Já o *usuario3* fica impedido de acessar a rede. O tempo de bloqueio neste experimento é menor que o do anterior pois o ataque de falsificação de MAC é detectado no próprio controlador e consequentemente é bloqueado assim que o usuário malicioso inicia a conexão. Este bloqueio não depende do envio da *Blacklist* dos roteadores. Neste experimento o atacante fica impedido de iniciar um ataque de DoS com as ferramentas Ettercap e Slowloris. Este impedimento se deve ao atacante ser desconectado e bloqueado antes mesmo de iniciar o ataque.

VI. CONCLUSÕES

O trabalho propõe uma ferramenta de detecção e bloqueio de usuários que realizam ataques de IP *spoofing* e MAC *spoofing* em uma rede sem fio utilizando o protocolo IEEE 802.1X. A presente proposta utiliza uma combinação de informações obtidas de análise de *logs* e do banco de usuários do servidor Radius. Estas informações são analisadas em conjunto com as informações de tabela ARP dos roteadores e *logs* de TCPdump. Durante os testes, os ataques de IP *spoofing* foram bloqueados inicialmente nos próprios roteadores e posteriormente realizando o bloqueio do login do usuário malicioso, neste caso em um tempo médio de 3 segundos para bloqueio de login. Para o ataque de MAC *spoofing* a contenção do ataque e consequente bloqueio do login do atacante é mais rápida devido a ação do módulo da ferramenta que atua diretamente na máquina que hospeda o servidor Radius. Para trabalhos futuros pretende-se utilizar a ferramenta em uma rede maior e utilizar técnicas de aprendizado de máquina para detectar padrões de utilização de logins e MACs dos usuários.

REFERÊNCIAS

[1] Y. Ma and H. Ning, "The improvement of wireless lan security authentication mechanism based on kerberos," in *2018 International Conference on Electronics Technology (ICET)*. IEEE, 2018, pp. 392–397.

[2] C. Benzaid, K. Lounis, A. Al-Nemrat, N. Badache, and M. Alazab, "Fast authentication in wireless sensor networks," *Future Generation Computer Systems*, vol. 55, pp. 362–375, 2016.

[3] B. Dey, S. Vishnu, and O. S. Swarnkar, "An efficient dynamic key based eap authentication framework for future ieee 802.1 x wireless lans," in *Proceedings of the 2nd International Conference on Digital Signal Processing*. ACM, 2018, pp. 125–131.

[4] C. A. M. da Silva, J. A. Gonçalves, V. da Silva Faria, G. de Britto Vieira, and D. M. Mascarenhas, "Iremac: Um ips para ataques internos," *XXXIV Simpósio Brasileiro de Telecomunicações e Processamento de Sinais*, 2016.

[5] H. Zhang, Y. Qi, J. Wu, L. Fu, and L. He, "Dos attack energy management against remote state estimation," *IEEE Transactions on Control of Network Systems*, vol. 5, no. 1, pp. 383–394, 2018.

[6] G. Lackner, U. Payer, and P. Teufl, "Combating wireless lan mac-layer address spoofing with fingerprinting methods." *IJ Network Security*, vol. 9, no. 2, pp. 164–172, 2009.

[7] Y.-G. Yu, K.-R. Park, and D.-H. Kim, "Study on port based on user authentication system using ieee 802.1 x." *Journal of Theoretical & Applied Information Technology*, vol. 96, no. 6, 2018.

[8] Q. Li and W. Trappe, "Light-weight detection of spoofing attacks in wireless networks," in *2006 IEEE International Conference on Mobile Ad Hoc and Sensor Systems*. IEEE, 2006, pp. 845–851.

[9] R. Xiao, H. Zhu, C. Song, X. Liu, J. Dong, and H. Li, "Attacking network isolation in software-defined networks: New attacks and countermeasures," in *2018 27th International Conference on Computer Communication and Networks (ICCCN)*. IEEE, 2018, pp. 1–9.

[10] R. Banakh, A. Piskozub, and I. Opirskyy, "Detection of mac spoofing attacks in ieee 802.11 networks using signal strength from attackers' devices," in *International Conference on Computer Science, Engineering and Education Applications*. Springer, 2018, pp. 468–477.

[11] H. Hwang, G. Jung, K. Sohn, and S. Park, "A study on mitm (man in the middle) vulnerability in wireless network using 802.1 x and eap," in *2008 International Conference on Information Science and Security (ICISS 2008)*. IEEE, 2008, pp. 164–170.

[12] E. Cambiaso, G. Papaleo, G. Chiola, and M. Aiello, "Slow dos attacks: definition and categorisation," *International Journal of Trust Management in Computing and Communications*, vol. 1, no. 3-4, pp. 300–319, 2013.

[13] J. A. Goncalves, V. S. Faria, G. B. Vieira, C. A. Silva, and D. M. Mascarenhas, "Widip: Wireless distributed ips for ddos attacks," in *2017 1st Cyber Security in Networking Conference (CSNet)*. IEEE, 2017, pp. 1–3.