14º SIEPE SALÃO INTERNACIONAL DE ENSINO, PESQUISA E EXTENSÃO
#EDUCAÇÃO + CIÊNCIA INDEPENDÊNCIA
30 nov. a 02 dez. 2022
REALIZAÇÃO: unipampa Universidade Federal do Pampa
APOIO: CNPq CAPES FAPERGS

Segurança e exploração de vulnerabilidades em dispositivos IoT

Matheus de Jesus Marques, discente de Engenharia de Computação, Universidade Federal do Pampa
Itiberê Gonçalves Silva Filho, egresso de Engenharia de Computação, Universidade Federal do Pampa
Leandro Bolzan Béria, servidor vinculado, Universidade Federal do Pampa
Gabriel Kitzmann Haab, Microchip Technology Inc.
Érico Marcelo Hoff do amaral, docente de Engenharia de Computação, Universidade Federal do Pampa

matheusmarques.aluno@unipampa.edu.br

Internet of Things (IoT) ou Internet das Coisas, em tradução livre, como o próprio nome sugere, se trata da união de informações ou dados, provenientes de diferentes objetos, a uma plataforma virtual em alguma infraestrutura da Internet. Conforme esses tipos de objetos se tornam cada vez mais comuns, a segurança destes dispositivos deve ser avaliada de forma pontual, visto que estas plataformas conectam-se a rede e, desta forma, podem ser utilizados como porta de entrada para ataques e invasões, possibilitando para um usuário mal-intencionado a obtenção de informações pessoais, interrupção de sistemas, e, por consequência, afetando a disponibilidade, integridade e confidencialidade da rede. Como medidas preventivas para evitar tais situações, são realizadas varreduras (*scans*) de segurança nas redes, procurando mapear e explorar as vulnerabilidades presentes nos dispositivos identificados. A metodologia utilizada abordou o modelo de pesquisa aplicada, com a finalidade de obter aplicações práticas e precisas para o desenvolvimento de uma solução que visa demonstrar as ferramentas e processos a serem seguidos na realização da verificação e mapeamento dos dispositivos IoT conectados na rede, suas respectivas informações, dados, características e vulnerabilidades. Assim sendo, foi realizado um vasto levantamento bibliográfico sobre o tema Internet das Coisas, dispositivos baseados nesta tecnologia e suas características. Como resultado, foram avaliadas as ferramentas Network Mapper (NMAP), Nessus Vulnerability Scanner e Wireshark, as quais são utilizadas no processo com o intuito de realizar a identificação e o mapeamento dos respectivos dispositivos internos às redes a serem analisados. A análise e mapeamento dos dispositivos podem ser descritos em cinco etapas, sendo a primeira etapa a identificação de todos os aparelhos conectados à rede utilizando a ferramenta NMAP, onde os dispositivos podem ser referenciados por uma faixa de IPs ou algum IP individual especificado, seja ele público ou interno à rede em que os procedimentos são realizados. A segunda etapa envolve a análise das portas de comunicação e identificação de seus respectivos protocolos ativos, sendo isso observado também através da ferramenta NMAP para cada dispositivo identificado na faixa analisada, onde os mesmos recebem uma análise e busca por suas *open ports* (portas abertas) para detectar atividades e interações. Na terceira etapa do processo, o objetivo é a análise de protocolos e monitoramento do fluxo de atividade nas portas identificadas com a ferramenta Wireshark, visando encontrar e gerar

feedbacks sobre seus fluxos de navegação e chamadas na rede. Para a quarta etapa, propõe-se o mapeamento e verificação das vulnerabilidades de cada dispositivo identificado, através do uso da ferramenta para verificação de vulnerabilidades *Nessus*, que é capaz de realizar uma análise de segurança detalhada e explicativa para cada um dos dispositivos presentes na rede, gerando feedbacks e soluções explicativas satisfatórias. Por fim, a quinta etapa, onde o desafio em desenvolvimento atual é a identificação dos dispositivos na rede classificados como IoT, além de filtrar todas as prováveis vulnerabilidades identificadas. Para tal classificação, são consideradas a comparação de endereços físicos (MAC) com repositórios específicos de prefixos de endereçamento disponibilizados por diferentes fabricantes de interfaces de rede, os sistemas operacionais dos dispositivos, suas respectivas capacidades computacionais e a frequência de atuação. De modo a se obter uma proposta de solução, o presente trabalho visa gerar um processo ferramental de análise de segurança e identificação de dispositivos IoT em redes, bem como a exploração das vulnerabilidades presentes nos mesmos. Com o roteiro de execução e análise fundamentado e sólido, conseguimos obter um feedback sobre a faixa de IP selecionada para análise, transmitindo para o usuário a maturidade de segurança em que a rede analisada se encontra. Os resultados obtidos até o momento, com a aplicação do protocolo proposto, permitem ao administrador de um ambiente de redes identificar os dispositivos IoT conectados à rede, suas vulnerabilidades e, desta forma, apontar, de forma detalhada, as possíveis soluções para os problemas identificados. Com o presente trabalho, conseguimos demonstrar o uso das ferramentas NMAP, *Nessus* e *Wireshark* no mapeamento e identificação de dispositivos IoT em redes.

Agradecimentos: UNIPAMPA.

Palavras-chave: *Internet of Things*; Segurança de sistemas; Vulnerabilidades; Dispositivos;