Solução integrada para 802.1x em rede cablada

Gonçalo, Rui[1]; Ferreira, Paulo[2]; Pedrosa, Tiago[3]

[1] a35937@alunos.ipb.pt, Instituto Politécnico de Bragança, Portugal
[2] a34960@alunos.ipb.pt, Instituto Politécnico de Bragança, Portugal
[3] pedrosa@ipb.pt, Instituto Politécnico de Bragança, Portugal

Resumo

Em muitas organizações não existe suporte de monitorização e autenticação dos utilizadores em ligações à rede cablada. O objetivo foi encontrar as melhores alternativas para a autenticação de ligações à rede cablada e também a monitorização dessas ligações, podendo assim facilitar a monitorização e prevenção de possíveis problemas que possam afetar a organização em ligações de rede cablada.

A solução encontrada pode ser dividida em três partes. Primeiro uma máquina com pfSense para a gestão da rede e serviços, que também tem envia logs para servidores remotos, entre os quais logs de traduções NAT e de sistema. A parte seguinte consiste na utilização do protocolo 802.1x que permite dotar a rede com um mecanismo de autenticação e autorização de acesso de utilizadores, que requer que qualquer equipamento ligado a uma porta do switch necessite de ser autenticado em um servidor RADIUS(a correr no pfSense) usando um servidor de LDAP remoto com a informação das contas de utilizador, prevenindo assim o acesso a qualquer pessoa externa à organização. A última parte consiste na implementação de uma solução de gestão de logs, usando o Graylog para visualizar e filtrar os logs recebidos do pfSense, podendo assim através da sua API realizar consultas personalizadas, principalmente uma criada por nós, que para dado timestamp, IP externo e uma porta identifica o utilizador.

Esta solução permite que organizações controlem quem acede à rede, e quando é detetado um incidente seja possível identificar o dono do equipamento problemático.

Palavras-Chave: 802.11x; infosec; cybersecurity; aaa; logs;

Integrated solution for 802.1x in wired network

Gonçalo, Rui[1]; Ferreira, Paulo[2]; Pedrosa, Tiago[3]

[1] a35937@alunos.ipb.pt, Instituto Politécnico de Bragança, Portugal
[2] a34960@alunos.ipb.pt, Instituto Politécnico de Bragança, Portugal
[3] pedrosa@ipb.pt, Instituto Politécnico de Bragança, Portugal

Abstract

Most organizations don't have mechanisms to enable user monitoring and authentication over wired networks. The goal was to analyze alternatives to implement authentication and monitoring connections to enable to detect and prevent some threats and problems on user computers that can impact the normal operation of the organization.

The proposed solution was divided in three components. First a machine running pfSense for network routing and services that also enabled to sent NAT translating info to remote system logs. Then followed the use of 802.11x protocol, to authenticate and authorize users, forcing any device connected to the switch to authenticate. This request is made to a RADIUS server (running on the pfSense) using remote LDAP server with the user account information. Without proper credentials equipment can't access the network. The final component was the implementation of a log event manager, using Graylog that makes easier to visualize and filter the information, enabling the use of an API to custom query, especially one created by us, which for a given timestamp and external IP and port identify the user.

This solution allows organizations to control who can access the network and when detecting incident enabled to identify the owner of the problematic equipment.

Keywords: 802.11x; infosec; cybersecurity; aaa; logs;