

某局点使用iMC-EIA配合openldap认证失败问题排查

Radius iMC EIA 802.1X LDAP 罗孝晨 2020-06-23 发表

组网及说明

iMC EIA 7.3E0510

问题描述

(1) 用户使用iMC-EIA配合openldap进行peap-mschapv2认证,提示E63032:密码错误

帐号名	登录名	服务名称	认证失败原因	认证失败时间	用户IP地址	用户MAC地址
LDAP_ser			E63032: 密码错误, 密码连续错误次数超过阈值将会加入黑名单。	2020-06-17 20:31:39	0.0.0.0	F4:31:C3:7C:C1:67
LDAP_ser			E63032: 密码错误, 密码连续错误次数超过阈值将会加入黑名单。	2020-06-17 20:31:24	0.0.0.0	F4:31:C3:7C:C1:67
LDAP_ser			E63032: 密码错误, 密码连续错误次数超过阈值将会加入黑名单。	2020-06-17 20:31:13	0.0.0.0	F4:31:C3:7C:C1:67

过程分析

(1) 分析抓包文件,从抓包中可以看到用户密码的加密方式为SSHA加密

The image shows a Wireshark packet capture analysis. The top pane displays a list of packets with a filter set to 'tcp.port==1389'. Packet 3418 is selected, showing an LDAP search response. The bottom pane shows the details of this packet, specifically the 'searchResEntry' section. Under 'attributes', there is a 'PartialAttributeList' for 'userPassword' with a value of 'userPassword'. Under 'vals', there is a single item for 'SSHA' with a value of 'zpcgB+0pyoK3wvYZoTqgNwAh5KLwMzQLpIFA=='. The 'SSHA' value is highlighted with a red box.

(2) 检查现场的接入策略配置中,认证类型为peap-mschapv2认证

The image shows a configuration page for a network device. The '授权信息' (Authorization Information) section is visible. The '首选EAP类型' (Preferred EAP Type) is set to 'EAP-PEAP'. The '子类型' (Subtype) is set to 'EAP-MSCHAPV2'. These two settings are highlighted with a red box.

(3) openldap认证时,密码校验为EIA本地校验。对于微软AD认证,密码校验为AD域控校验。因此当openldap对于用户密码进行加密时,peap-mschapv2认证方式无法进行支持。

解决方法

- (1) 将用户密码加密方式修改为明文
- (2) 或者修改认证类型为PEAP-GTC,因PC自带客户端仅支持PEAP/TLS认证,因此GTC认证类型要求PC客户端必须安装iNode客户端,手机不需要安装客户端