Cannot enter system mode after logging in S75E via Telnet

Switches 孟普 2020-08-21 Published

Network Topology

Null

Problem Description

A customer reported that after logging in S75E via Telnet, the user obtained the highest per mission, but could not enter the system mode after logging in the device.

Process analysis

1. Log in S75E via Telnet, and find that the reboot command can be input normally, which m eans that the logged role has indeed obtained the highest privilege, and the debug informat ion of 7506E can also be seen that the role has obtained the highest privilege, as follows:

```
*Aug 17 15:08:57:425 2017 XYKZC-KS-CORE-7506E-01 RADIUS/7/PACKET: -MDC=1;
   Service-Type=Callback-Administrative
   Session-Timeout=86400
   Login-Service=Telnet
H3c-Exec-Privilege=15
```

The authentication server is IMC, and role levels can also be seen on IMC:

```
CODE = 1.
ID = 71.
ATTRIBUTES:
      User-Name(1) = "test@hxks".
      Password(2) = "$$$".
      Service-Type(6) = 1.
      NAS-Identifier(32) = "XYKZC-KS-CORE-7506E-01".
      Framed-IP-Address(8) = 1781483207.
      NAS-IP-Address(4) = 1781530371.

%% 2017-08-17 13:01:53.499 ; [LDBG] ; [3932] ; radDispatcher ; prsRawPkt: chk-sum 3465568
905.
%% 2017-08-17 13:01:53.499 ; [LDBG] ; [3932] ; LAN ; prsMixedUsr: in [test@hxks], out [test
@hxks].
%% 2017-08-17 13:01:53.499 ; [LDBG] ; [3932] ; radEnt ; setPxyType: Needn&#39;t proxy. do
mainname=hxks, Code=1.
%% 2017-08-17 13:01:53.499 ; [LDBG] ; [3932] ; LAN ; getIpMacFromItem: no attribute of Call
ing-Station-Id.
%% 2017-08-17 13:01:53.530 ; [LDBG] ; [2264] ; MNG ; Send message attribut list:
Code = 2
ID = 71
ATTRIBUTES:
Service_Type(6) = 1
Session-Timeout(27) = 86400
Login_Service(15) = 0
hw_Exec_Privilege(29) = 15
```

No command entered into the system view was found when entering the question mark, whi ch is suspected to be a command line authorization problem.

2. Check the authentication, authorization, accounting, etc. of different applications in the D omain:

```
<XYKZC-KS-CORE-7506E-01>display domain
Total 2 domain(s)

Domain:system
 State: Active
 default Authentication Scheme:  local
 default Authorization  Scheme:  local
 default Accounting     Scheme:  local
```

Authorization attributes :
Idle-cut : Disable

Domain:hxks
State: Active
login Authentication Scheme: radius: hxks, local
login Authorization Scheme: radius: hxks, local
login Accounting Scheme: radius: hxks, none
default Authentication Scheme: local
default Authorization Scheme: local
default Accounting Scheme: local
Authorization attributes :
Under Domain HXKS, everything is local except for login authentication, authorization, billing, and radius HXKS.

3. Once again display the information of the local server. Through debug, it can be found that there will be printing authorization failure and log that the user does not exist:
<XYKZC-KS-CORE-7506E-01>debugging local-server all
<XYKZC-KS-CORE-7506E-01>t m
The current terminal is enabled to display logs.
<XYKZC-KS-CORE-7506E-01>t d
The current terminal is enabled to display debugging logs.
<XYKZC-KS-CORE-7506E-01>*Aug 18 14:29:14:043 2017 XYKZC-KS-CORE-7506E-01 LOCALSER/7/EVENT: -MDC=1;
Received authorization request message.
*Aug 18 14:29:14:043 2017 XYKZC-KS-CORE-7506E-01 LOCALSER/7/EVENT: -MDC=1;
Authorization failed, user "hxks" doesn't exist.

Telnet logins are all authenticated with remote 3A. Generally, there is no need to configure the user name locally, because the command line authorization is also implemented through HwTACacs, and there is no need for local authorization.

4. Check the configuration under VTY and find that command authorization does exist:
line vty 0 4
authentication-mode scheme
user-role network-operator
command authorization
command accounting

Combined with point 2, command line authorization is the default mode, namely local authorization, because the local user name does not exist, so the command line authorization cannot be completed, resulting in the failure of command line authorization.

Solution

Since the RADIUS server is used as the 3A authentication server, it is not recommended to configure command line authorization; simply delete command line authorization.Of course, the on-site problem could be to add a user name to the device and reconfigure the user name with a role that would make command line authorization safe, but that would be unnecessary.