堡垒机开局web端口可达但是登录失败

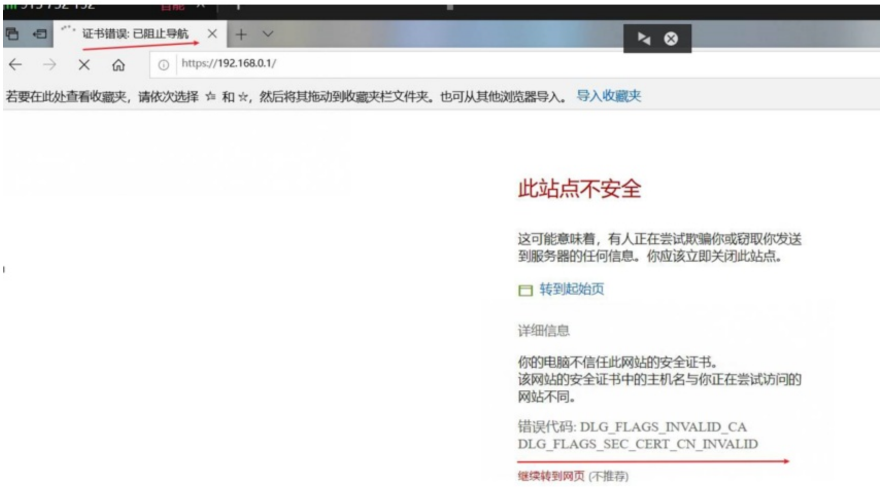
运维审计 吴昊A 2024-01-03 发表

问题描述

开局web打不开，ping和443端口可达

点击如下无反应

换个浏览器，清缓存，换电脑， 重启过，故障依旧



证书错误: 已阻止导航

https://192.168.0.1/

若要在此处查看收藏夹，请依次选择 ☆ 和 ☆，然后将其拖动到收藏夹栏文件夹。也可从其他浏览器导入。 导入收藏夹

此站点不安全

这可能意味着，有人正在尝试欺骗你或窃取你发送到服务器的任何信息。你应该立即关闭此站点。

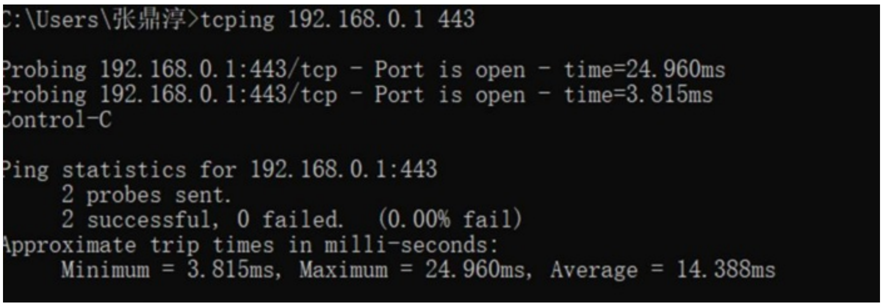
转到起始页

详细信息

你的电脑不信任此网站的安全证书。
该网站的安全证书中的主机名与你正在尝试访问的网站不同。

错误代码: DLG_FLAGS_INVALID_CA
DLG_FLAGS_SEC_CERT_CN_INVALID

继续转到网页 (不推荐)

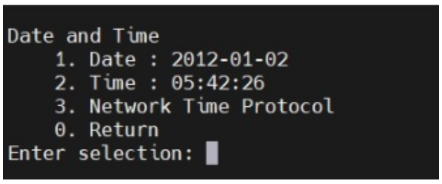


```
C:\Users\张鼎淳>tcping 192.168.0.1 443

Probing 192.168.0.1:443/tcp - Port is open - time=24.960ms
Probing 192.168.0.1:443/tcp - Port is open - time=3.815ms
Control-C

Ping statistics for 192.168.0.1:443
     2 probes sent.
     2 successful, 0 failed.  (0.00% fail)
Approximate trip times in milli-seconds:
     Minimum = 3.815ms, Maximum = 24.960ms, Average = 14.388ms
```

过程分析

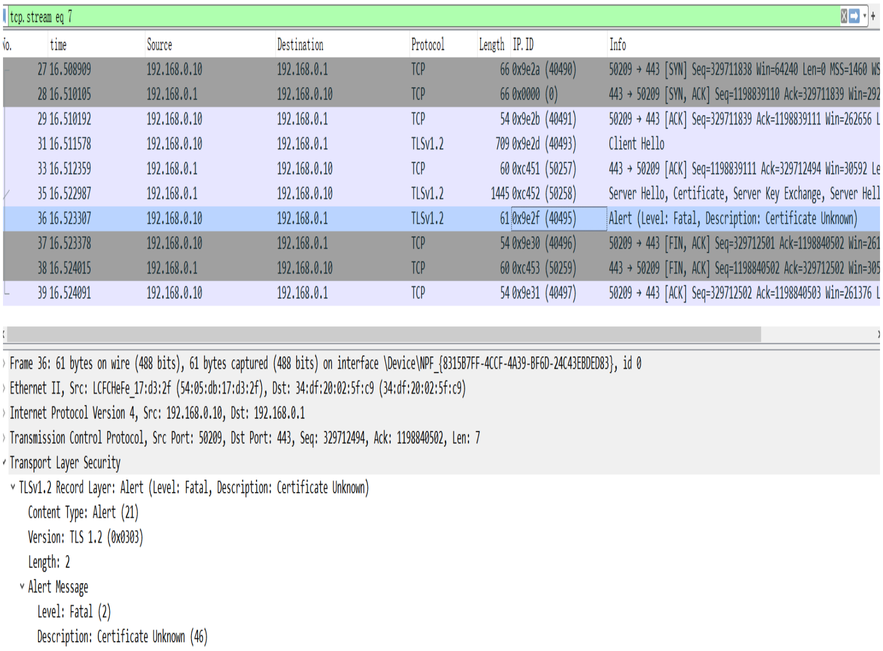
查看浏览器版本符合要求，并且更换电脑清楚缓存依旧;

通过SSH登录设备后发现设备时间不对，

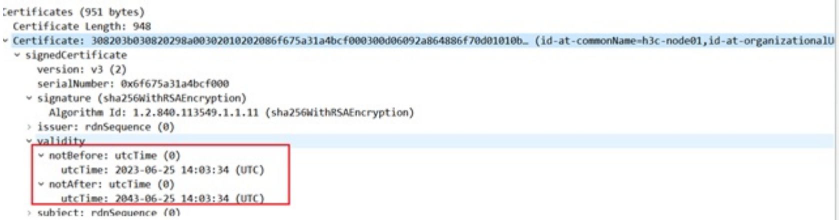


```
Date and Time
    1. Date : 2012-01-02
    2. Time : 05:42:26
    3. Network Time Protocol
    0. Return
Enter selection: 
```

抓包看证书的有效期是2023-2043年，所以导致证书认证交互失败。



```
tcp.stream eq 7
No.   time        Source         Destination    Protocol  Length IP.ID            Info
  27 16.508909   192.168.0.10   192.168.0.1    TCP          66 0x9e2a (40490)  50209 → 443 [SYN] Seq=329711838 Win=64240 Len=0 MSS=1460 WS
  28 16.510105   192.168.0.1    192.168.0.10   TCP          66 0x0000 (0)      443 → 50209 [SYN, ACK] Seq=1198839110 Ack=329711839 Win=292
  29 16.510192   192.168.0.10   192.168.0.1    TCP          54 0x9e2b (40491)  50209 → 443 [ACK] Seq=329711839 Ack=1198839111 Win=262656 L
  31 16.511578   192.168.0.10   192.168.0.1    TLSv1.2     709 0x9e2d (40493)  Client Hello
  33 16.512359   192.168.0.1    192.168.0.10   TCP          60 0xc451 (50257)  443 → 50209 [ACK] Seq=1198839111 Ack=329712494 Win=30592 Le
  35 16.522987   192.168.0.1    192.168.0.10   TLSv1.2    1445 0xc452 (50258)  Server Hello, Certificate, Server Key Exchange, Server Hell
  36 16.523307   192.168.0.10   192.168.0.1    TLSv1.2      61 0x9e2f (40495)  Alert (Level: Fatal, Description: Certificate Unknown)
  37 16.523378   192.168.0.10   192.168.0.1    TCP          54 0x9e30 (40496)  50209 → 443 [FIN, ACK] Seq=329712501 Ack=1198840502 Win=261
  38 16.524015   192.168.0.1    192.168.0.10   TCP          60 0xc453 (50259)  443 → 50209 [FIN, ACK] Seq=1198840502 Ack=329712502 Win=305
  39 16.524091   192.168.0.10   192.168.0.1    TCP          54 0x9e31 (40497)  50209 → 443 [ACK] Seq=329712502 Ack=1198840503 Win=261376 L

> Frame 36: 61 bytes on wire (488 bits), 61 bytes captured (488 bits) on interface \Device\NPF_{8315B7FF-4CCF-4A39-BF6D-24C43EBDED83}, id 0
> Ethernet II, Src: LCFCHeFe_17:d3:2f (54:05:db:17:d3:2f), Dst: 34:df:20:02:5f:c9 (34:df:20:02:5f:c9)
> Internet Protocol Version 4, Src: 192.168.0.10, Dst: 192.168.0.1
> Transmission Control Protocol, Src Port: 50209, Dst Port: 443, Seq: 329712494, Ack: 1198840502, Len: 7
v Transport Layer Security
  v TLSv1.2 Record Layer: Alert (Level: Fatal, Description: Certificate Unknown)
      Content Type: Alert (21)
      Version: TLS 1.2 (0x0303)
      Length: 2
    v Alert Message
        Level: Fatal (2)
        Description: Certificate Unknown (46)
```



```
Certificates (951 bytes)
  Certificate Length: 948
v Certificate: 308203b030820298a00302010202086f675a31a4bcf000300d06092a864886f70d01010b… (id-at-commonName=h3c-node01,id-at-organizationalU
  v signedCertificate
      version: v3 (2)
      serialNumber: 0x6f675a31a4bcf000
    v signature (sha256WithRSAEncryption)
        Algorithm Id: 1.2.840.113549.1.1.11 (sha256WithRSAEncryption)
    > issuer: rdnSequence (0)
    v validity
      v notBefore: utcTime (0)
          utcTime: 2023-06-25 14:03:34 (UTC)
      v notAfter: utcTime (0)
          utcTime: 2043-06-25 14:03:34 (UTC)
    > subject: rdnSequence (0)
```

解决方法

SSH进去后修改设备时间后重启正常登录。