工作任务一

生成树欺骗攻击与防御策略

【工作目的】

掌握交换机生成树选举过程、欺骗原理、攻击过程和防范策略。

【工作背景】

A 企业收购 B 企业，合并后两企业技术部和工程部分布在办公楼 A 栋和 B 栋某楼层，通过接入层交换机 SW1 和 SW2 连接起来，经三层交换机 SW3（根交换机）汇聚后，通过 vlan 40 虚拟接口与企业路由器 R1 相连，接入 Internet 路由器 R2。其中 vlan 10 为技术部，vlan 20 为工程部，vlan 30 为服务器群。

【工作任务】

A 栋楼某员工想获得 B 栋楼工程部主机与外网通信的机密信息，将黑客交换机接入 SW1 和 SW2 中工程部 vlan 20 任一接口（E0/0/11～E0/0/22），并将黑客交换机设置为根交换机，以此劫持 SW2 所有流量，从中分析工程部主机登录的账号和密码。

工程部主机账号屡遭被盗后，管理员发现 SW3 为非根交换机，初步判定为生成树欺骗攻击所致，遂将 SW1 和 SW2 主机接入端口（Access）设为边缘端口，避免重演 SW1 和 SW2 流量劫持事件。

【任务分析】

生成树端口有 Disable、Blocking、Listening、Learning、Forwarding 5 个状态。交换机边缘端口（Portfast）不接收 BPDU，选举时直接从阻塞状态转变为转发状态，不参与生成树选举过程。默认情况下，交换机所有端口均为非边缘端口。为避免生成树欺骗攻击，可将交换机用于主机接入的端口设为边缘端口。

将交换机 E0/0/1 接口配置为边缘端口：

```
[Huawei] interface Ethernet0/0/1
[Huawei-Ethernet0/0/1]stp edged-port enable
```

【设备器材】

接入层交换机（S3700）3 台，汇聚层交换机（S5700）1 台，路由器（AR1220）2 台，主机

4 台,各主机分别承担角色见表 1-1。

表 1-1 主机配置表

角 色	接入方式	网卡设置	IP 地址	操作系统	工 具
技术部主机	Cloud1 接入	VMnet1	192.168.1.10	Win7/10	
工程部主机	Cloud2 接入	VMnet2	192.168.2.10	Win7/10	
内网服务器	eNSP Server 接入		192.168.3.10		
公网 Web 服务器	Cloud3 接入	VMnet3	116.64.100.10/24	Win2008/2012/2016	BBS Web

【环境拓扑】

工作拓扑图如图 1-1 所示。

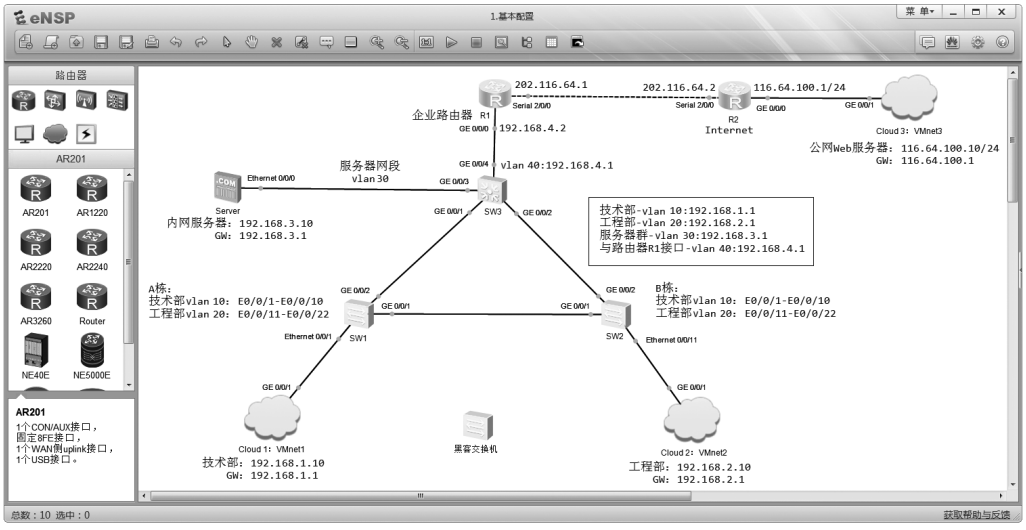

图 1-1 工作拓扑图

【工作过程】

一、基本配置

1. 交换机 vlan 和端口配置

```
<Huawei>system-view
[Huawei]sysname SW1
[SW1]vlan batch 10 20                    //batch:批量
[SW1]stp enable                          //STP 默认开启,本行可不输
[SW1]stp mode rstp
[SW1]port-group 1                        //技术部组
[SW1-port-group-1]group-member Ethernet 0/0/1 to Ethernet 0/0/10
[SW1-port-group-1]port link-type access
[SW1-port-group-1]port default vlan 10
```

```
[SW1-port-group-1]quit
[SW1]port-group 2                          //工程部组
[SW1-port-group-2]group-member Ethernet 0/0/11 to Ethernet 0/0/22
[SW1-port-group-1]port link-type access
[SW1-port-group-1]port default vlan 20
[SW1-port-group-2]quit
[SW1]port-group 3                          //Trunk 组
[SW1-port-group-3]group-member GigabitEthernet 0/0/1 GigabitEthernet 0/0/2
[SW1-port-group-3]port link-type trunk
[SW1-port-group-3]port trunk allow-pass vlan 10 20
[SW1-port-group-2]quit
[SW1]

<Huawei>system-view
[Huawei]sysname SW2
[SW2]vlan batch 10 20
[SW2]stp enable
[SW2]stp mode rstp
[SW2]port-group 1                          //技术部组
[SW2-port-group-1]group-member Ethernet 0/0/1 to Ethernet 0/0/10
[SW2-port-group-1]port link-type access
[SW2-port-group-1]port default vlan 10
[SW2-port-group-1]quit
[SW2]port-group 2                          //工程部组
[SW2-port-group-2]group-member Ethernet 0/0/11 to Ethernet 0/0/22
[SW2-port-group-2]port link-type access
[SW2-port-group-2]port default vlan 20
[SW2-port-group-2]quit
[SW2]port-group 3                          //Trunk 组
[SW2-port-group-3]group-member GigabitEthernet 0/0/1 GigabitEthernet 0/0/2
[SW2-port-group-3]port link-type trunk
[SW2-port-group-3]port trunk allow-pass vlan 10 20
[SW2-port-group-3]quit
[SW2]

<Huawei>system-view
[Huawei]sysname SW3
[SW3]vlan batch 10 20 30 40
[SW3]stp enable
[SW3]stp mode rstp
[SW3]stp root primary                      //设置为主根,优先级为 0(优先级最高)
[SW3]interface GigabitEthernet 0/0/1
[SW3-GigabitEthernet0/0/1]port link-type trunk
[SW3-GigabitEthernet0/0/1]port trunk allow-pass vlan 10 20
//表面上含义是 GE 0/0/1Trunk 口允许 vlan 10 和 vlan 20 通过,相当于把 GE 0/0/1 加入
  vlan 10 和 vlan 20,此时 vlan 10 和 vlan 20 有物理接口,两个 vlan 才能处于 Up 状态。假
  如一个 vlan 没有任何接口,vlan 永远处于 Down 状态
[SW3-GigabitEthernet0/0/1]quit
[SW3]interface GigabitEthernet 0/0/2
```

```
[SW3-GigabitEthernet0/0/2]port link-type trunk
[SW3-GigabitEthernet0/0/2]port trunk allow-pass vlan 10 20
[SW3-GigabitEthernet0/0/2]quit
[SW3]interface GigabitEthernet 0/0/3
[SW3-GigabitEthernet0/0/3]port link-type access
[SW3-GigabitEthernet0/0/3]port default vlan 30
//此时交换机 vlan 30 包含 GE0/0/3，vlan 30 才会处于 Up 状态
[SW3]interface GigabitEthernet 0/0/4
[SW3-GigabitEthernet0/0/4]port link-type trunk
[SW3-GigabitEthernet0/0/4]port trunk allow-pass vlan all
[SW3-GigabitEthernet0/0/4]quit
[SW3]interface Vlanif 10
[SW3-Vlanif10]ip address 192.168.1.1 24
[SW3-Vlanif10]quit
[SW3]interface Vlanif 20
[SW3-Vlanif20]ip address 192.168.2.1 24
[SW3-Vlanif20]quit
[SW3]interface Vlanif 30
[SW3-Vlanif30]ip address 192.168.3.1 24
[SW3-Vlanif30]quit
[SW3]interface Vlanif 40
[SW3-Vlanif40]ip address 192.168.4.1 24
[SW3-Vlanif40]quit
[SW3]interface GigabitEthernet 0/0/4
[SW3-GigabitEthernet0/0/4]port trunk pvid vlan 40
//vlan 40 与 R1 的 GE 0/0/0 接口相连。虽然 vlan 40 包含 GE 0/0/4 接口，但是默认仍属于
  vlan 1，这与思科不同。将端口更改默认 vlan，Access 模式命令为 port default vlan 40，
  Trunk 模式命令为 port trunk pvid vlan 40
[SW3-GigabitEthernet0/0/4]quit
[SW3]
```

2. 接口 IP 与路由协议配置

```
[SW3]ospf 1
[SW3-ospf-1]area 0
[SW3-ospf-1-area-0.0.0.0]network 192.168.1.0 0.0.0.255
[SW3-ospf-1-area-0.0.0.0]network 192.168.2.0 0.0.0.255
[SW3-ospf-1-area-0.0.0.0]network 192.168.3.0 0.0.0.255
[SW3-ospf-1-area-0.0.0.0]network 192.168.4.0 0.0.0.255
[SW3-ospf-1-area-0.0.0.0]quit
[SW3-ospf-1]quit
[SW3]ip route-static 0.0.0.0 0.0.0.0 192.168.4.2
[SW3]

<Huawei>system-view
[Huawei]sysname R1
[R1]interface GigabitEthernet 0/0/0
[R1-GigabitEthernet0/0/0]ip address 192.168.4.2 24
[R1-GigabitEthernet0/0/0]quit
[R1]interface Serial 2/0/0
```

```
[R1-Serial2/0/0]ip address 202.116.64.1 24
[R1-Serial2/0/0]quit
[R1]ospf 1
[R1-ospf-1]area 0
[R1-ospf-1-area-0.0.0.0]network 192.168.4.0 0.0.0.255
[R1-ospf-1-area-0.0.0.0]quit
[R1-ospf-1]quit
[R1]ip route-static 0.0.0.0 0.0.0.0 202.116.64.2
[R1]

<Huawei>system-view
[Huawei]sysname R2
[R2]interface GigabitEthernet 0/0/0
[R2-GigabitEthernet0/0/0]ip address 116.64.100.1 24
[R2-GigabitEthernet0/0/0]quit
[R2]interface Serial 2/0/0
[R2-Serial2/0/0]ip address 202.116.64.2 24
[R2-Serial2/0/0]quit
[R2]
```

3. 路由器 R1 Easy-IP 配置

```
[R1]acl 2000
//基本 ACL: <2000~2999>,只能根据源 IP 地址过滤。高级 ACL: <3000~3999>,基于源 IP、目
  的 IP、协议类型等过滤,类似扩展 ACL
[R1-acl-basic-2000]rule permit source 192.168.0.0 0.0.255.255
[R1-acl-basic-2000]quit
[R1]interface Serial 2/0/0
[R1-Serial2/0/0]nat outbound 2000
//加载 ACL2000 过滤规则与公网接口出栈之间的转换关系,即把内网 IP 经过滤规则匹配后转换
  为公网接口 IP
[R1-Serial2/0/0]quit
[R1]
```

注：Easy-IP 直接使用接口 IP 作为 NAT 转换后地址；NAPT 需指定具体地址池 IP 作为 NAT 转换后的地址。

4. 基本配置验证

(1) 查看 SW3 生成树与端口详细信息。

```
[SW3]display stp
--------[CIST Global Info][Mode RSTP]--------
CIST Bridge         :0    .4c1f-cc32-6eac        //当前网桥优先级和 MAC 地址
Config Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
Active Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC      :0    .4c1f-cc32-6eac / 0     //生成树选举的根网桥优先级和 MAC
                                                    地址,其值与 SW3 网桥相同,从而
                                                    判断 SW3 就是根网桥
CIST RegRoot/IRPC   :0    .4c1f-cc32-6eac / 0
CIST RootPortId     :0.0
BPDU-Protection     :Disabled
```

```
CIST Root Type      :Primary root
TC or TCN received  :216
TC count per hello  :0
STP Converge Mode   :Normal
Time since last TC  :0 days 0h:0m:13s
Number of TC        :89
Last TC occurred    :GigabitEthernet0/0/1
----[Port1(GigabitEthernet0/0/1)][FORWARDING]----     //以下为所有端口详细信息
Port Protocol       :Enabled
Port Role           :Designated Port
Port Priority       :128
Port Cost(Dot1T )   :Config=auto / Active=20000
Designated Bridge/Port   :0.4c1f-cc32-6eac / 128.1
Port Edged          :Config=default / Active=disabled
Point-to-point      :Config=auto / Active=true
Transit Limit       :147 packets/hello-time
  ----More ----       //显示的信息很长,按 Enter 键显示下一行,按 Space 键显示下一
                        页,按 Ctrl+C 组合键或 Tab 键退出显示信息
```

注：CIST(Common and Internal Spanning Tree,公共和内部生成树)是连接一个交换网络内所有设备的单生成树。

(2) 查看 SW3 生成树接口简要信息。

```
[SW3]display stp brief
MSTID  Port                        Role  STP State     Protection
  0    GigabitEthernet0/0/1        DESI  FORWARDING      NONE
  0    GigabitEthernet0/0/2        DESI  FORWARDING      NONE
  0    GigabitEthernet0/0/3        DESI  FORWARDING      NONE
  0    GigabitEthernet0/0/4        DESI  FORWARDING      NONE
```

可以看出,构建生成树的 GE 0/0/1 和 GE 0/0/2 为指定端口,处于转发状态。

(3) 连通性测试。

对技术部主机和工程部主机配置 IP 后,可以连通公网 Web 服务器,TTL 值为 125,如图 1-2 所示。

图 1-2　连通性测试图

二、入侵实战

1.黑客交换机接入与生成树配置

将黑客交换机接入 SW1 和 SW2 中工程部 vlan 20 任一接口(E0/0/11～E0/0/22)，如图 1-3 所示的 E0/0/22。

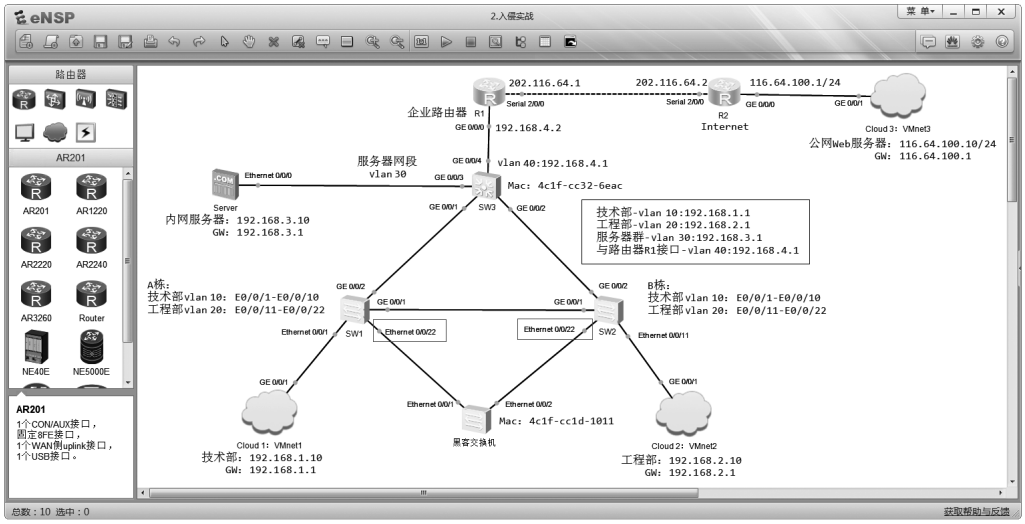

图 1-3　入侵拓扑图

注：如图 1-3 所示，SW3 的 MAC 地址为 4c1f-cc32-6eac，黑客交换机 MAC 地址为 4c1f-cc1d-1011。在相同优先级(priority 0)情况下，为使黑客交换机选举为根交换机，黑客交换机 MAC 地址必须小于 SW3 的 MAC 地址。由于交换机 MAC 地址无法更改和自定义，读者需反复尝试，直到找到适合的交换机作为黑客交换机为止。

黑客交换机生成树配置命令如下：

```
<Huawei>system-view
[Huawei]sysname Hacker
[Hacker]stp enable
[Hacker]stp mode rstp
[Hacker]stp priority 0                          //优先级与 SW3 相同，都为 0
[Hacker]
```

2. 生成树重新选举与验证

(1) 验证黑客交换机选举为根交换机。

由于黑客交换机和 SW3 生成树优先级都设置为 0，则需比较双方 MAC 地址。由于黑客交换机 MAC 地址小(网桥 id＝优先级＋MAC 地址)，从而选举为根网桥。

```
[Hacker]display stp
-------[CIST Global Info][Mode RSTP]-------
CIST Bridge         :0     .4c1f-cc1d-1011       //黑客交换机优先级和 MAC 地址
Config Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
```

```
Active Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC      :0    .4c1f-cc1d-1011 / 0     //生成树选举的根网桥优先级和 MAC
                                                    地址,其值与黑客网桥相同,从而判
                                                    断黑客交换机为根网桥
CIST RegRoot/IRPC   :0    .4c1f-cc1d-1011 / 0
CIST RootPortId     :0.0
BPDU-Protection     :Disabled
TC or TCN received  :17
TC count per hello  :0
STP Converge Mode   :Normal
Time since last TC  :0 days 0h:8m:5s
Number of TC        :9
Last TC occurred    :Ethernet0/0/2
  ----More ----
```

(2) 验证 SW3 交换机为非根交换机。

```
[SW3]display stp
-------[CIST Global Info][Mode RSTP]-------
CIST Bridge         :0    .4c1f-cc32-6eac           //网桥 SW3 优先级和 MAC 地址
Config Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
Active Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC      :0    .4c1f-cc1d-1011 / 220000  //选举黑客交换机为根网桥
CIST RegRoot/IRPC   :0    .4c1f-cc32-6eac / 0
CIST RootPortId     :128.1
BPDU-Protection     :Disabled
CIST Root Type      :Primary root
TC or TCN received  :237
TC count per hello  :0
STP Converge Mode   :Normal
Time since last TC  :0 days 0h:2m:11s
Number of TC        :99
Last TC occurred    :GigabitEthernet0/0/1
  ----More ----
```

(3) 验证 SW3 阻塞端口与备份链路。

根据生成树选举经验,根网桥(黑客交换机)对角线为备份链路。进入交换机 SW3 查看生成树接口简要信息。在 SW3 中,由于没有配置 GE 接口优先级,其优先级默认都为 128(注意:在选举指定端口时,以收到对方接口推送的 PDU 优先级为准,即优先级不是由自身端口优先级决定,而是由所连接的对方接口优先级决定),下一步则比较端口号。由于 GE 0/0/1 端口号小于 GE 0/0/2 端口号,因此 GE 0/0/1 选举为指定端口(DESI),GE 0/0/2 选举为替换端口(ALTE),处于阻塞 DISCARDING 状态,SW3 和 SW2 之间链路为备份链路。

```
[SW3]display stp brief
MSTID  Port                        Role  STP State     Protection
  0    GigabitEthernet0/0/1        ROOT  FORWARDING      NONE
```

```
0    GigabitEthernet0/0/2      ALTE  DISCARDING      NONE
0    GigabitEthernet0/0/3      DESI  FORWARDING      NONE
0    GigabitEthernet0/0/4      DESI  FORWARDING      NONE
```

(4) 验证 SW2 阻塞端口与备份链路。

根据“根网桥对角线为备份链路”准则，SW1 和 SW2 之间链路也应为备份链路，进入交换机 SW2 查看生成树接口简要信息，发现 GE 0/0/1 选举为替换端口，处于阻塞 DISCARDING 状态。

```
[SW2]display stp brief
MSTID  Port                      Role  STP State     Protection
   0   Ethernet0/0/11            DESI  FORWARDING    NONE
   0   Ethernet0/0/22            ROOT  FORWARDING    NONE
   0   GigabitEthernet0/0/1      ALTE  DISCARDING    NONE
   0   GigabitEthernet0/0/2      DESI  FORWARDING    NONE
```

(5) 生成树新拓扑结构。

黑客交换机接入后，生成树重新选举，阻塞备份端口，生成新拓扑如图 1-4 所示。生成树选举过程会导致丢包现象，工程部与外网 Web 服务器连通情况如图 1-5 所示。此时，SW2 流量必须经过黑客交换机转发，从而引发安全事件。

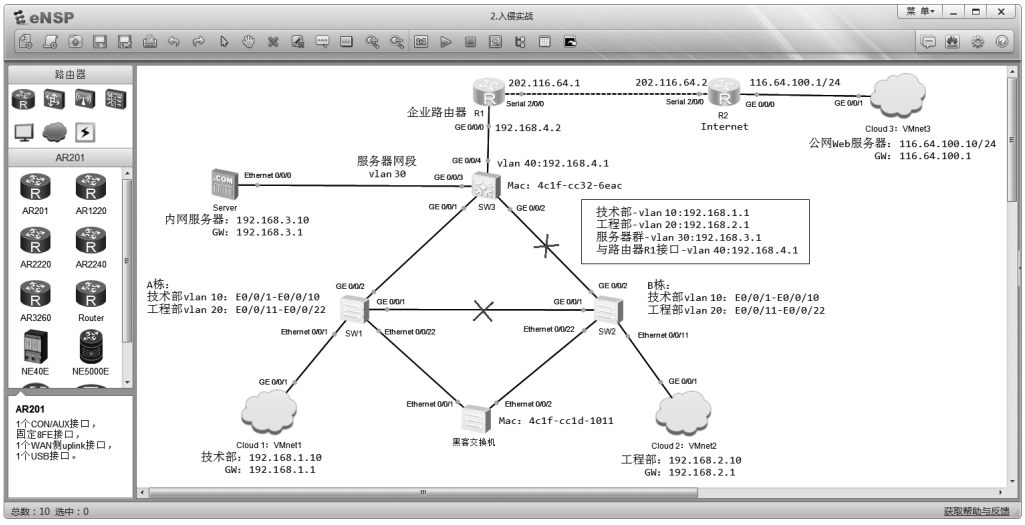

图 1-4　生成树新拓扑结构图

3. 黑客交换机捕获工程部主机账号和密码

(1) 在工程部主机上登录 Web 服务器，注册账号。

在公网 Web 服务器发布 BBS 论坛站点，可通过 Win2008 或 Win2012 或 Win2016 发布，详细步骤请参阅本书附录 2。在工程部主机上的浏览器输入地址 http://116.64.100.10 可以访问公网 Web 服务器站点，并注册账号。如图 1-6 所示在工程部主机上注册的账号名为 gdcp，密码 33732878。注册完后，单击论坛“退出登录”按钮。

图 1-5　工程部主机连通性测试图

图 1-6　通过客户机在服务器上注册账号

(2) 黑客交换机捕捉到账号和密码。

在黑客交换机 E0/0/1 或 E0/0/2 接口启用抓包,如图 1-7 所示。在工程部主机上通过账号 gdcp 和密码 33732878 成功登录公网服务器 Web 站点后停止抓包。在 Wireshar 界面单击“查找下一分组”按钮,输入 33732878;在下拉列表框中单击下拉按钮分别选择“字符串”和“分组详情”选项,可以捕获在工程部主机上登录的账号和密码,如图 1-8 所示。