OSPF路由项欺骗攻击与防御策略

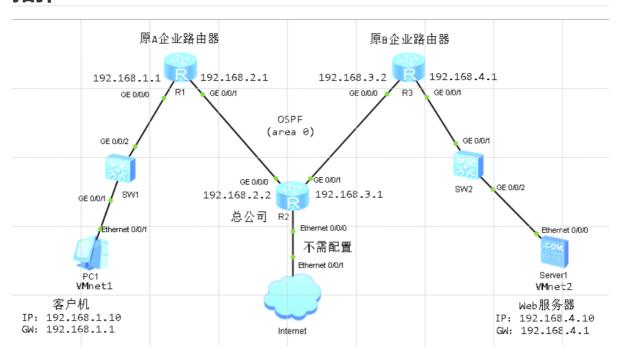
任务目的

掌握OSPF路由项欺骗攻击和OSPF源端鉴别的配置方法。

任务设备、设施

Win 华为ENSP Vmare

拓扑



基本配置

路由器配置

R1

```
1
    <Huawei>sys
    Enter system view, return user view with Ctrl+Z.
 2
 3
    [Huawei]sys R1
 4
    [R1]undo info en
 5
    Info: Information center is disabled.
 6
    [R1] int g0/0/0
    [R1-GigabitEthernet0/0/0]ip add 192.168.1.1 24
 7
 8
    [R1-GigabitEthernet0/0/0]q
 9
    [R1] int g0/0/1
10
    [R1-GigabitEthernet0/0/1]ip add 192.168.2.1 24
11
    [R1-GigabitEthernet0/0/1]q
    [R1]ospf 1
12
13
    [R1-ospf-1]area 0
14
    [R1-ospf-1-area-0.0.0.0]network 192.168.1.0 0.0.0.255
    [R1-ospf-1-area-0.0.0.0]network 192.168.2.0 0.0.0.255
15
    [R1-ospf-1-area-0.0.0.0]q
16
17
    [R1-ospf-1]q
```

R2

```
<Huawei>sys
 1
 2
    Enter system view, return user view with Ctrl+Z.
 3
    [Huawei]sys R2
    [R2]undo info en
 5
    Info: Information center is disabled.
    [R2] int g0/0/0
 7
    [R2-GigabitEthernet0/0/0]ip add 192.168.2.2 24
 8
    [R2-GigabitEthernet0/0/0]q
 9
    [R2] int g0/0/1
10
    [R2-GigabitEthernet0/0/1]ip add 192.168.3.1 24
11
    [R2-GigabitEthernet0/0/1]q
12
    [R2]ospf 1
13
    [R2-ospf-1]area 0
14
    [R2-ospf-1-area-0.0.0.0]network 192.168.2.0 0.0.0.255
15
    [R2-ospf-1-area-0.0.0.0]network 192.168.3.0 0.0.0.255
16
    [R2-ospf-1-area-0.0.0.0]q
17
    [R2-ospf-1]q
18
    [R2]
```

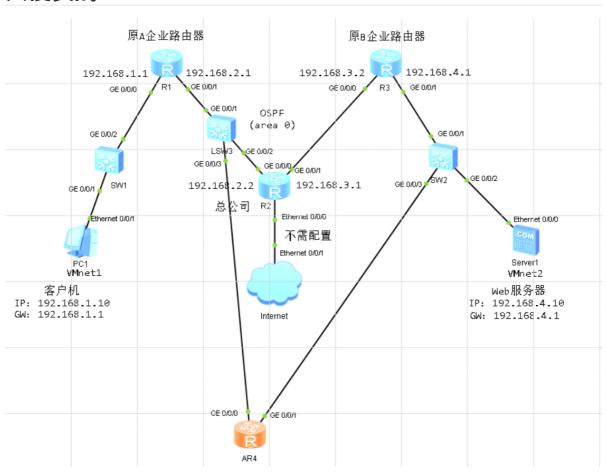
R3

```
<Huawei>sys
 1
    Enter system view, return user view with Ctrl+Z.
    [Huawei]sys R3
 3
 4
    [R3]undo info en
    Info: Information center is disabled.
 5
    [R3] int g0/0/0
 6
    [R3-GigabitEthernet0/0/0]ip add 192.168.3.2 24
 7
 8
    [R3-GigabitEthernet0/0/0]q
 9
    [R3] int g0/0/1
    [R3-GigabitEthernet0/0/1]ip add 192.168.4.1 24
10
    [R3-GigabitEthernet0/0/1]q
11
12
    [R3]ospf 1
13
    [R3-ospf-1]area 0
14
    [R3-ospf-1-area-0.0.0.0]network 192.168.3.0 0.0.0.255
    [R3-ospf-1-area-0.0.0.0] network 192.168.4.0 0.0.0.255
15
    [R3-ospf-1-area-0.0.0.0]q
16
17
    [R3-ospf-1]q
18
    [R3]
```

查看路由器R1路由器表

€ R1						X			
R1 R2	R3								
Routing Tables: Public									
Destinations : 12			Routes : 12						
estination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface			
127.0.0.0/8	Direct	9	9	D	127.0.0.1	InLoopBack0			
127.0.0.1/32	Direct	0	9	D	127.0.0.1	InLoopBack0			
127.255.255.255/32	Direct	Θ	0	D	127.0.0.1	InLoopBack0			
192.168.1.0/24	Direct	0	9	D	192.168.1.1	GigabitEthernet			
9/0/0									
192.168.1.1/32	Direct	0	0	D	127.0.0.1	GigabitEthernet			
9/0/0									
192.168.1.255/32	Direct	0	0	D	127.0.0.1	GigabitEthernet			
9/0/0									
192.168.2.0/24	Direct	0	0	D	192.168.2.1	GigabitEthernet			
9/9/1									
192.168.2.1/32	Direct	0	0	D	127.0.0.1	GigabitEthernet			
9/0/1									
192.168.2.255/32	Direct	0	0	D	127.0.0.1	GigabitEthernet			
9/9/1									
192.168.3.0/24	OSPF	10	2	D	192.168.2.2	GigabitEthernet			
9/0/1									
192.168.4.0/24 9/0/1	OSPF	10	3	D	192.168.2.2	GigabitEthernet			
255.255.255.255/32	Direct	0	0	D	127.0.0.1	InLoopBack0			
[R1]									

入侵实战



R4伪造OSPF路由表

```
1
    <Huawei>
 2
    <Huawei>sys
 3
    Enter system view, return user view with Ctrl+Z.
 4
    [Huawei]sys R4
    [R4]undo info en
 5
    Info: Information center is disabled.
 6
 7
    [R4]int q0/0/0
    [R4-GigabitEthernet0/0/0]ip add 192.168.2.3 24
 8
 9
    [R4-GigabitEthernet0/0/0]q
    [R4] int g0/0/1
10
    [R4-GigabitEthernet0/0/1]ip add 192.168.4.2 24
11
    [R4-GigabitEthernet0/0/1]q
12
13
    [R4]ospf 1
14
    [R4-ospf-1]area 0
    [R4-ospf-1-area-0.0.0.0]network 192.168.2.0 0.0.0.255
15
16
    [R4-ospf-1-area-0.0.0.0] network 192.168.4.0 0.0.0.255
17
    [R4-ospf-1-area-0.0.0.0]q
    [R4-ospf-1]
18
```

路由表信息

R1路由表

```
[R1]disp ip routing-table
Route Flags: R - relay, D - download to fib
Routing Tables: Public
        Destinations : 12
                                Routes : 12
Destination/Mask
                   Proto
                           Pre Cost Flags NextHop
                                                               Interface
     127.0.0.0/8
                   Direct 0
                                Θ
                                                127.0.0.1
                                                               InLoopBack0
     127.0.0.1/32 Direct 0
                                Θ
                                                127.0.0.1
                                                               InLoopBack@
127.255.255.255/32 Direct
                                Θ
                           Θ
                                                127.0.0.1
                                                               InLoopBack0
   192.168.1.0/24 Direct
                           Θ
                                Θ
                                                192.168.1.1
                                                               GigabitEthernet
0/0/0
   192.168.1.1/32 Direct
                                                127.0.0.1
                                                               GigabitEthernet
                           Θ
                                Θ
0/0/0
 192.168.1.255/32 Direct
                                                127.0.0.1
                                                               GigabitEthernet
                           Θ
                                Θ
0/0/0
   192.168.2.0/24 Direct
                                Θ
                                                192.168.2.1
                                                               GigabitEthernet
                           Θ
0/0/1
   192.168.2.1/32 Direct
                                Θ
                                                127.0.0.1
                                                               GigabitEthernet
0/0/1
 192.168.2.255/32 Direct
                           Θ
                                0
                                                127.0.0.1
                                                               GigabitEthernet
0/0/1
   192.168.3.0/24 OSPF
                                                               GigabitEthernet
                           10
                                                192.168.2.2
   192.168.4.0/24 OSPF
                                                               GigabitEthernet
                           10
                                2
                                                192.168.2.3
0/0/1
255.255.255.255/32 Direct 0
                                Θ
                                                127.0.0.1
                                                               InLoopBack@
```

R2路由表

<pre>[R2]disp ip routing-table Route Flags: R - relay, D - download to fib</pre>										
Routing Tables: Public Destinations : 12			Routes : 13							
Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface				
127.0.0.0/8	Direct	0	0	D	127.0.0.1	InLoopBack0				
127.0.0.1/32	Direct	0	9	D	127.0.0.1	InLoopBack0				
127.255.255.255/32	Direct	0	0	D	127.0.0.1	InLoopBack0				
192.168.1.0/24	OSPF	10	2	D	192.168.2.1	GigabitEthernet				
0/0/0										
192.168.2.0/24	Direct	0	0	D	192.168.2.2	GigabitEthernet				
0/0/0										
192.168.2.2/32	Direct	0	0	D	127.0.0.1	GigabitEthernet				
0/0/0										
192.168.2.255/32	Direct	0	0	D	127.0.0.1	GigabitEthernet				
0/0/0										
192.168.3.0/24	Direct	0	0	D	192.168.3.1	GigabitEthernet				
0/0/1										
192.168.3.1/32	Direct	0	0	D	127.0.0.1	GigabitEthernet				
0/0/1										
192.168.3.255/32	Direct	0	0	D	127.0.0.1	GigabitEthernet				
0/0/1										
192.168.4.0/24	OSPF	10	2	D	192.168.3.2	GigabitEthernet				
0/0/1										
	OSPF	10	2	D	192.168.2.3	GigabitEthernet				
0/0/0 255.255.255.255/32	Direct	9	9	D	127.0.0.1	InLoopBack0				

防御策略

路由器R1接口开启OSPF路由项源鉴别功能

```
1    [R1]int g0/0/1
2    [R1-GigabitEthernet0/0/1]ospf authentication-mode hmac-md5 1 cipher huawei
3    [R1-GigabitEthernet0/0/1]q
4    [R1]
```

路由器R2接口开启OSPF路由项源鉴别功能

验证

R1路由表

```
📆 R1
                                                                                                          _ _ X
   R1
Routing Tables: Public
Destinations : 12
                                                  Flags NextHop
127.8.0.9/8 Direct 0
127.0.9.1/32 Direct 0
127.255.255.255/32 Direct 0
192.168.1.9/24 Direct 0
                                                         127.0.0.1
                                                         127.0.0.1
                                                                             InLoopBack0
                                                                            InLoopBack0
GigabitEthernet
0/0/0
0/0/0
    192.168.2.0/24 Direct 0
                                                          192.168.2.1
    192.168.2.1/32 Direct 0
                                                         127.0.0.1
                                                                            GigabitEthernet
0/0/1
    192.168.3.0/24 OSPF
                                                         192.168.2.3
                                 10
255.255.255.255/32 Direct 0
                                                         127.0.0.1
                                                                             InLoopBack0
```

PC1 ping web服务结果

```
_ 🗆 X
F PC1
                             UDP发包工具
            命令行 组播
 Welcome to use PC Simulator!
PC>ping 192.168.4.10
Ping 192.168.4.10: 32 data bytes, Press Ctrl_C to break
Request timeout!
From 192.168.4.10: bytes=32 seq=2 ttl=252 time=94 ms
From 192.168.4.10: bytes=32 seq=3 ttl=252 time=78 ms
From 192.168.4.10: bytes=32 seq=4 ttl=252 time=94 ms
 From 192.168.4.10: bytes=32 seq=5 ttl=252 time=109 ms
  -- 192.168.4.10 ping statistics ---
  5 packet(s) transmitted
4 packet(s) received
  20.00% packet loss
   round-trip min/avg/max = 0/93/109 ms
PC>
```

任务总结

- 1.在配置OSPF路由项源端鉴别时,相邻路由器之间接口必须采用相同得鉴别方式(如Hmac-md5)、相同得鉴别密码(密钥存储方式可以不同,如cipher或者plain)和相同得密钥标识符,否则不能建立邻居关系
- 2.对于交换机SW2而言, 去往目的IP地址192.168.4.1时,可能通过GE0/0/1接口(客户机与Web服务器通信时去跟回走不同路径),也可能通过GE0/0/3接口(客户机与Web服务器通信时去跟回走相同路径),由SW2端口映射表更新状态决定,无法人为指定.