WX系列AC入侵检测功能配置举例

攻击检测及防范 **周龙翔** 2013-07-01 发表

WX系列AC入侵检测功能配置举例

一、组网需求：

WX5004、WA2612、WA2620i-AGN

二、组网图

三、特性介绍

802.11网络容易受到各种干扰源、恶意入侵者、非法客户端以及周边无线设施的威胁或影响。WIPS通过分析侦听到的802.11无线报文，来检测针对WLAN网络的无意或者恶意的攻击，并以告警的方式通知网络管理员。目前WIPS支持的攻击检测包括Spoofing检测、Ad hoc网络检测、非法信道检测、DoS攻击检测、Flood攻击检测、自定义攻击检测和针对WIPS系统的攻击检测。

三、配置步骤

```
#
version 5.20, Test 2507P01
#
 sysname AC
#
 domain default enable system
#
 telnet server enable
#
 port-security enable
#
 undo password-recovery enable
#
vlan 1
#
domain system
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
#
dhcp server ip-pool ap
 network 172.16.1.0 mask 255.255.255.0
 gateway-list 172.16.1.1
#
user-group system
 group-attribute allow-guest
#
```

```
local-user admin
 password cipher $c$3$7rnYmeeswoi6xu57uwbf//uweam0Qrjq
 authorization-attribute level 3
 service-type telnet
 service-type web
#
wlan rrm
 dot11a mandatory-rate 6 12 24
 dot11a supported-rate 9 18 36 48 54
 dot11b mandatory-rate 1 2
 dot11b supported-rate 5.5 11
 dot11g mandatory-rate 1 2 5.5 11
 dot11g supported-rate 6 9 12 18 24 36 48 54
 dot11n mandatory maximum-mcs 15
#
wlan ap-group default_group
 ap ap
#
interface NULL0
#
interface LoopBack0
 ip address 10.153.43.200 255.255.255.255
#
interface Vlan-interface1
 ip address 172.16.0.188 255.255.255.0
#
interface GigabitEthernet1/0/1
#
interface GigabitEthernet1/0/2
#
interface GigabitEthernet1/0/3
#
interface GigabitEthernet1/0/4
#
interface Ten-GigabitEthernet1/0/5
#
wlan ap ap model WA2612 id 1
 serial-id 219801A0CJC124002846
 radio 1
  wips detect mode detect-only
  channel 13
  radio enable
#
wlan ips
 wips enable
 signature deauth_flood signature-id 1
 signature broadcast_deauth_flood signature-id 2
 signature disassoc_flood signature-id 3
 signature broadcast_disassoc_flood signature-id 4
 signature eapol_logoff_flood signature-id 5
 signature eap_success_flood signature-id 6
 signature eap_failure_flood signature-id 7
 signature pspoll_flood signature-id 8
 signature cts_flood signature-id 9
 signature rts_flood signature-id 10
  detect-threshold per-signature 50
 signature beacon_flood signature-id 33
  action report event-level 2
  sub-rule frame-type management frame-subtype beacon
 signature probe_request signature-id 34
  action report event-level 2
  sub-rule frame-type management frame-subtype probe-request
 signature deauthentication signature-id 35
  action report event-level 2
```

```
 sub-rule frame-type management frame-subtype deauthentication
signature disassociation signature-id 36
 action report event-level 2
 sub-rule frame-type management frame-subtype disassociation
signature pro_responese signature-id 37
 action report event-level 2
 sub-rule pattern proberesp offset 0 mask ff00 equal 5000
signature-policy default
signature-policy test
 signature signature-id 1 to 10 33 to 37 precedence 1
attack-detect-policy default
attack-detect-policy test
 detect ap-flood
 detect dos-eapol-start
 detect dos-authentication
 detect dos-association
 detect dos-reassociation
virtual-security-domain default
 attack-detect-policy default
 signature-policy default
virtual-security-domain test
 attack-detect-policy test
 signature-policy test
 sensor ap
#
 info-center loghost 172.16.0.9
 info-center loghost 172.16.0.44
 undo info-center enable
 undo info-center logfile enable
#
dhcp enable
#
user-interface con 0
user-interface vty 0 4
 authentication-mode scheme
 user privilege level 3
#
Return
```

四、配置关键点

4.1此功能在目前版本需要license,可以在H3C license管理平台上申请。

```
<H3C>display license wips
No. Activation key                    WIPS Sensor Number   Available Time Left
--------------------------------------------------------------------------------
 1  AdZBL-hhV7q-C$UtX-Wc9at-Kjd3m-AnxQk-nWVnW          12          87
```

4.2 Wlan ips下攻击检测使能，该功能不能和WIDS同时使能，并且检测ap的工作模式必须为普通接入。

[AC-wlan-ips]wips enable

4.3 配置Signature规则

4.3.1 一条Signature规则包含了对一种特征报文的识别方式和对该特征报文所采取的动作，分为内置Signature规则和自定义Signature规则。以上配置举例中1-10为内置Siganature规则，33-37为自定义Siganature规则。

4,3,2 自定义Siganature规则配置方法以第33号为例，设备检测到规则定义的无线攻击时命名为“beacon_flood”，并以level 2级别告警，匹配帧类型为管理帧中的beacon帧。

[AC-wlan-ips]signature beacon_flood signature-id 33
[AC-wlan-ips-sig-beacon_flood]action report event-level 2
[AC-wlan-ips-sig-beacon_flood]sub-rule frame-type management frame-subtype beacon

4.4 创建Signature策略，引用Siganature规则。

[AC-wlan-ips]signature-policy test

[AC-wlan-ips-sigpolicy-test] signature signature-id 1 to 10 33 to 37 precedence 1

4.5 创建攻击检测策略，配置检测检测的攻击项。

[AC-wlan-ips]attack-detect-policy test
[AC-wlan-ips-dctp-test]detect dos-eapol-start
[AC-wlan-ips-dctp-test]detect dos-authentication
[AC-wlan-ips-dctp-test]detect dos-association
[AC-wlan-ips-dctp-test]detect dos-reassociation

4．6 创建虚拟安全域，绑定Siganature规则、攻击检测策略以及sensor（即检测AP）。

[AC-wlan-ips]virtual-security-domain test
[AC-wlan-ips-vsd-test]attack-detect-policy test
[AC-wlan-ips-vsd-test]signature-policy test
[AC-wlan-ips-vsd-test]sensor ap

4.7 使能监视AP的2.4G频段入侵检测功能功能

[AC]wlan ap ap model WA2612
[AC-wlan-ap-ap]serial-id 219801A0CJC124002846
[AC-wlan-ap-ap]radio 1
[AC-wlan-ap-ap-radio-1]wips detect mode detect-only
[AC-wlan-ap-ap-radio-1]channel 13
[AC-wlan-ap-ap-radio-1]radio enable

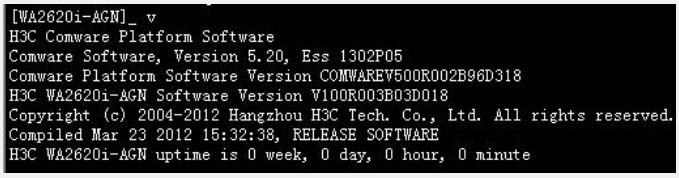
五、结果验证

5.1以上配置支持检测的攻击项如下，均已在实际测试中验证过。

DOS authentication flood、DOS deauthentication flood、DOS De-Auth Broadcast flood、DOS De-Auth flood、DOS probe request flood、DOS beacon flood、DOS probe response flood、DOS Dis-Assoc Broadcast flood、DOS Dis-Assoc flood、DOS RTS flood、DOS Unauthenticated Association。

5.2 攻击源需要专业设备，我司AP WA2620i-AGN通过特殊手段可以模拟部分无线攻击。以flood-deauthen类型为例，操作方法如下：

5.2.1 攻击源为WA2620i-AGN，加载特殊版本。此版本可以从二线或者售前测试部获取。



5.2.2 本地创建一个txt文档，命名为flood-deauth-modified.txt，写入以下内容（加粗部分为sensor AP的bss口mac地址，注意空格），导入攻击源AP的flash中。

c0 00 3a 01 58 66 ba 67 60 80 00 24 01 ed ab 73

58 66 ba 67 60 80 f0 7a 03 00

5.2.3 在攻击源AP上进入隐藏模式，输入以下命令后，攻击源发起无线攻击。

[H3C-hidecmd]ar5 2 tx-packets file flash:/flood-deauth-modified.txt frequency 500

5.3 在AC上查看检测到的无线攻击：