Parâmetros da assinatura de IDS do controlador do Wireless LAN

Índice

Introdução

Este documento descreve como configurar assinaturas do Intrusion Detection System (IDS) em um Controlador de LAN Wireless (WLAN) da Cisco (release de software 3.2 ou posteriores).

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

A informação neste documento é baseada no Software Release 3.2 e Mais Recente do controlador de WLAN.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

Você pode transferir arquivos pela rede o arquivo de assinatura de IDS para a assinatura edita (ou para a revisão de documentação). Escolha **comandos > arquivo > arquivo de assinatura da**

transferência de arquivo pela rede. A fim transferir um arquivo de assinatura de IDS alterado, escolha **comandos > arquivo > arquivo de assinatura da transferência**. Depois que você transfere um arquivo de assinatura ao controlador, todos os Access point (AP) que estão conectados ao controlador estão refrescados no tempo real com os parâmetros recentemente editados da assinatura.

Este indicador mostra como transferir o arquivo de assinatura:

Os parâmetros dos documentos nove do arquivo de texto da assinatura de IDS para cada assinatura de IDS. Você pode alterar estes parâmetros da assinatura e escrever assinaturas feitas sob encomenda novas. Veja o formato que a seção dos parâmetros IDS de controlador deste documento fornece.

Parâmetros IDS de controlador

Todas as assinaturas *devem* ter este formato:

```
Name = <str>, Ver = <int>, Preced = <int>, FrmType = <frmType-type>, Pattern =
<pattern-format>, Freq = <int>, Interval = <int>, Quiet = <int>, Action = <action-val>,
Desc = <str>
```

O comprimento máximo da linha é 1000 caráteres. As linhas que são mais longas de 1000 não são analisadas gramaticalmente corretamente.

Todas as linhas que comece com `# no` arquivo de texto IDS são consideradas comentários e saltadas. Igualmente são saltadas todas as linhas em branco, que são linhas com apenas whitespace ou newline. O primeiro noncomment, linha do nonblank *deve* ter a revisão de palavra-chave. Se o arquivo é um arquivo de assinatura Cisco-fornecido, você não deve mudar o valor da `revisão`. Cisco usa este valor para controlar liberações do arquivo de assinatura. Se o arquivo contém as assinaturas que estiveram criadas pelo utilizador final, o valor da `revisão` *deve* ser `feito sob encomenda` (`revisão = costume`).

Os nove parâmetros da assinatura de IDS que você pode alterar são:

- Nome da assinatura do **`name=`**. Esta é uma série exclusiva que identifique a assinatura. O comprimento máximo do nome é 20 caráteres.
- **`Preced`** = precedência de assinatura. Este é um ID exclusivo que indique a precedência da assinatura entre todas as assinaturas que são definidas no arquivo de assinatura. *Deve* haver um `Token precedente por assinatura`.
- **`FrmType`** = tipo de frame. Este parâmetro pode tomar valores da lista do `<frmType-val>`. *Deve* haver um token por assinatura de `FrmType`. `O <frmType-val>` pode ser uma destas duas palavras-chaves somente:`mgmtdadosO <frmType-val>` indica se esta assinatura detecta quadros dos dados ou do Gerenciamento.
- **`Teste padrão`** = teste padrão da assinatura. O valor simbólico é usado para detectar os pacotes que combinam a assinatura. *Deve* haver pelo menos um token por assinatura do `teste padrão`. Pode haver até cinco tais tokens por assinatura. Se a assinatura tem mais de um tal token, um pacote deve combinar os valores de todos os tokens para que o pacote combine a assinatura.Quando o AP recebe um pacote, o AP toma o fluxo de byte que começa no `<offset>`, ANDs ele com o `<mask>`, e compara o resultado com o `<pattern>`. Se o AP encontra um fósforo, o AP considera o pacote um fósforo com a assinatura. `O <pattern-format>` pode ser precedido pelo operador de negação “`!`”. Nesse caso, todos os pacotes que

FALHAM a operação do fósforo que esta seção descreve são considerados um fósforo com a assinatura.

- **`Freq`** = frequência de compatibilidade de pacote em uns pacotes/intervalo. O valor deste token indica quantos pacotes pelo intervalo de medida devem combinar esta assinatura antes que a ação de assinatura esteja executada. Um valor de 0 indica que a ação de assinatura está tomada todas as vezes que um pacote combina a assinatura. O valor máximo para este token é 65,535. *Deve* haver um `Token de frequência por assinatura`.
- **`Intervalo`** = intervalo de medida nos segundos. O valor deste token indica o período de tempo que o ponto inicial (isto é, o `Freq`) especifica. O valor padrão para este token é 1 segundo. O valor máximo para este token é 3600.
- **`Silêncio`** = tempo quieto nos segundos. O valor deste token indica a quantidade de tempo que deve passar durante qual o AP não recebe os pacotes que combinam a assinatura antes que o AP determine que o ataque que a assinatura indica se abrandou. Se o valor do `Token de frequência` é 0, este token está ignorado. *Deve* haver um token por assinatura `quieto`.
- **`Ação`** = ação de assinatura. Isto indica o que o AP deve fazer se um pacote combina a assinatura. Este parâmetro pode tomar valores da lista do `<action-val>`. *Deve* haver um `Token de ação por assinatura`. O `<action-val>` pode ser uma destas duas palavras-chaves somente:`nenhuns` = não fazem nada.`relatório` = relatório o fósforo ao interruptor.
- **`Desc`** = descrição de assinatura. Esta é uma corda que descreva a finalidade da assinatura. Quando um fósforo da assinatura é relatado em uma armadilha de Protocolo de Gerenciamento de Rede Simples (SNMP), esta corda está fornecida à armadilha. O comprimento máximo da descrição é 100 caráteres. *Deve* haver um `Desc token por assinatura`.

Assinaturas padrão de IDS de controlador

Estas assinaturas de IDS enviam com o controlador como “assinaturas de IDS padrão”. Você pode alterar todos estes parâmetros da assinatura, porque a seção dos parâmetros IDS de controlador descreve.

```
Revision = 1.000
Name = "Bcast deauth", Ver = 0, Preced= 1, FrmType = mgmt, Pattern = 0:0x00C0:0x03FF,
Pattern = 4:0x01:0x01, Freq=30, Quiet = 300, Action = report, Desc="Broadcast
Deauthentication Frame"

Name = "NULL probe resp 1", Ver = 0, Preced = 2, FrmType = mgmt, Pattern =
0:0x0050:0x03FF, Pattern = 36:0x0000:0xFFFF, Freq=1, Quiet = 300, Action = report, Desc =
"NULL Probe Response - Zero length SSID element"

Name = "NULL probe resp 2", Ver = 0, Preced = 3, FrmType = mgmt, Pattern =
0:0x0050:0x03FF, Pattern = !36:0x00:0xFF, Freq=1, Quiet = 300, Action = report, Desc =
"NULL Probe Response - No SSID element"

Name = "Assoc flood", Ver = 0, Preced= 4, FrmType = mgmt, Pattern = 0:0x0000:0x03FF,
Freq=50, Quiet = 600, Action = report, Desc="Association Request flood"

Name = "Auth Flood", Ver = 0, Preced= 5, FrmType = mgmt, Pattern = 0: 0x00b0: 0x03FF,
Freq=50, Quiet = 600, Action = report, Desc="Authentication Request flood"

Name = "Reassoc flood", Ver = 0, Preced= 5, FrmType = mgmt, Pattern = 0:0x0020:0x03FF,
Freq=50, Quiet = 600, Action = report, Desc="Reassociation Request flood"

Name = "Broadcast Probe flood", Ver = 0, Preced= 6, FrmType = mgmt, Pattern =
```

```
0:0x0040:0x03FF, Pattern = 4:0x01:0x01, Pattern = 24:0x0000:0xFFFF, Freq=50, Quiet = 600,
Action = report, Desc="Broadcast Probe Request flood"

Name = "Disassoc flood", Ver = 0, Preced= 7, FrmType = mgmt, Pattern = 0:0x00A0:0x03FF,
Freq=50, Quiet = 600, Action = report, Desc="Disassociation flood"

Name = "Deauth flood", Ver = 0, Preced= 8, FrmType = mgmt, Pattern = 0:0x00C0:0x03FF,
Freq=50, Quiet = 600, Action = report, Desc="Deauthentication flood"

Name = "Res mgmt 6 & 7", Ver = 0, Preced= 9, FrmType = mgmt, Pattern = 0:0x0060:0x03EF,
Freq=5, Quiet = 600, Action = report, Desc="Reserved management sub-types 6 and 7"

Name = "Res mgmt D", Ver = 0, Preced= 10, FrmType = mgmt, Pattern = 0:0x00D0:0x03FF,
Freq=5, Quiet = 600, Action = report, Desc="Reserved management sub-type D"

Name = "Res mgmt E & F", Ver = 0, Preced= 11, FrmType = mgmt, Pattern = 0:0x00E0:0x03EF,
Freq=5, Quiet = 600, Action = report, Desc="Reserved management sub-types E and F"

Name = "EAPOL flood", Ver = 0, Preced= 12, FrmType = data, Pattern = 0:0x0108:0x03FF,
Pattern = 30:0x888E:0xFFFF, Freq=50, Quiet = 300, Action = report, Desc="EAPOL Flood
Attack"

Name = "NetStumbler 3.2.0", Ver = 0, Preced= 13, FrmType = data, Pattern =
0:0x0108:0x03FF, Pattern = 27:0x00601d:0xFFFFFF, Pattern = 30:0x0001:0xFFFF, Pattern =
36:0x466c7572:0xFFFFFFFF, Freq = 1, Quiet = 300, Action = report, Desc="NetStumbler 3.2.0"

Name = "NetStumbler 3.2.3", Ver = 0, Preced= 14, FrmType = data, Pattern =
0:0x0108:0x03FF, Pattern = 27:0x00601d:0xFFFFFF, Pattern = 30:0x0001:0xFFFF, Pattern =
36:0x416C6C20:0xFFFFFFFF, Freq = 1, Quiet = 600, Action = report, Desc="NetStumbler 3.2.3"

Name = "NetStumbler 3.3.0", Ver = 0, Preced= 15, FrmType = data, Pattern =
0:0x0108:0x03FF, Pattern = 27:0x00601d:0xFFFFFF, Pattern = 30:0x0001:0xFFFF, Pattern =
36:0x20202020:0xFFFFFFFF, Freq = 1, Quiet = 600, Action = report, Desc="NetStumbler 3.3.0"

Name = "NetStumbler generic", Ver = 0, Preced= 16, FrmType = data, Pattern =
0:0x0108:0x03FF, Pattern = 27:0x00601d:0xFFFFFF, Pattern = 30:0x0001:0xFFFF, Freq = 1,
Quiet = 600, Action = report, Desc="NetStumbler"

Name = "Wellenreiter", Ver = 0, Preced= 17, FrmType = mgmt, Pattern = 0:0x0040:0x03FF,
Pattern = 24:0x001d746869735f69735f757365645f666f725f77656c6c656e726569:
0xffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff, Freq = 1, Quiet = 600,
Action = report, Desc="Wellenreiter"
```

Mensagens IDS

Com versão 4.0 do controlador do Wireless LAN, você pôde receber esta mensagem IDS.

```
Big NAV Dos attack from AP with Base Radio MAC 00:0f:23:xx:xx:xx,
Slot ID 0 and Source MAC 00:00:00:00:00:00
```

Esta mensagem IDS indica que o campo do vetor da atribuição da rede do 802.11 (NAV) no quadro wireless do 802.11 é demasiado grande e a rede Wireless pôde estar sob um ataque DOS (ou há um cliente se portando mal).

Depois que você recebe esta mensagem IDS, a próxima etapa é seguir para baixo o cliente de ofensa. Você deve encontrar o cliente baseado em sua intensidade de sinal com um sniffer wireless na área em torno do Access point ou usar o server do lugar para localizar sua posição.

O campo de NAV é o mecanismo virtual do carrier sense usado para abrandar hidden colisões entre terminais (clientes Wireless que o cliente Wireless atual não pode detectar quando transmite) em transmissões do 802.11. Hidden os terminais criam problemas porque o Access point pôde receber pacotes de dois clientes que podem transmitir ao Access point mas não

recebe transmissões de cada um. Quando estes clientes transmitem ao mesmo tempo, seus pacotes colidem no Access point e este conduz ao Access point que não recebe nenhum pacote claramente.

Sempre que um cliente Wireless quer enviar um pacote de dados ao Access point, transmite realmente uma sequência do quatro-pacote chamada a sequência do pacote RTS-CTS-DATA-ACK. Cada um dos quatro quadros do 802.11 leva um campo de NAV que indique o número de microssegundos que o canal é reservado para por um cliente Wireless. Durante o aperto de mão RTS/CTS entre o cliente Wireless e o Access point, o cliente Wireless envia um quadro pequeno RTS que inclua um intervalo de NAV grande bastante para terminar a sequência inteira. Isto inclui o quadro CTS, o frame de dados, e o quadro subsequente do reconhecimento do Access point.

Quando o cliente Wireless transmite seu pacote RTS com NAV ajustado, o valor transmitido está usado para ajustar os temporizadores de NAV em todos clientes Wireless restantes associados ao Access point. O Access point responde ao pacote RTS do cliente com um pacote CTS que contenha um valor novo de NAV actualizado para esclarecer o tempo já decorra durante a sequência do pacote. Depois que o pacote CTS é enviado, cada cliente Wireless que pode receber do Access point atualizou seu temporizador de NAV e adia todas as transmissões até que seu temporizador de NAV alcance 0. Isto mantém o canal livre para que o cliente Wireless termine o processo de transmitir um pacote ao Access point.

Um atacante pôde explorar este mecanismo virtual do carrier sense afirmando uma grande estadia no campo de NAV. Isto impede outros clientes dos pacotes de transmissão. O valor máximo para NAV é 32767, ou aproximadamente 32 milissegundos nas redes 802.11b. Assim na teoria um atacante precisa somente de transmitir aproximadamente 30 pacotes um o segundo para bloquear todo o acesso ao canal.

Informações Relacionadas

- Cisco 4400 Series Wireless LAN Controllers
- Cisco 4100 Series Wireless LAN Controllers
- Cisco 2000 Series Wireless LAN Controllers
- Versão 3.1 dos Engine de assinatura do Sistema de Detecção de Intrusão da Cisco
- Suporte Técnico e Documentação - Cisco Systems