Uso di NBAR e ACL per bloccare il worm "Code Red"

Sommario

Introduzione

Questo documento fornisce un metodo per bloccare il worm "Code Red" sui punti di ingresso della rete tramite NBAR (Network-Based Application Recognition) e ACL (Access Control Lists) all'interno del software Cisco IOS® sui router Cisco. Questa soluzione deve essere utilizzata insieme alle patch consigliate per i server IIS di Microsoft.

Nota: questo metodo non funziona sui router Cisco serie 1600.

Nota: alcuni tipi di traffico P2P non possono essere bloccati completamente a causa della natura del protocollo P2P. Questi protocolli P2P modificano in modo dinamico le proprie firme per evitare qualsiasi motore DPI che cerchi di bloccare completamente il traffico. Pertanto, si consiglia di limitare la larghezza di banda invece di bloccarli completamente. Limita la larghezza di banda per il traffico. Assegnare molta meno larghezza di banda; ma lasciate passare la connessione.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Criteri del servizio QoS (Quality of Service) che utilizzano i comandi dell'interfaccia della riga di comando (CLI) di QoS modulare.
- NBAR
- ACL
- Routing basato su policy

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware. La configurazione descritta in questo documento è stata testata su Cisco 3640 con Cisco IOS versione 12.2(24a)

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Come bloccare il worm "Code Red"

La prima cosa da fare per combattere "Code Red" è applicare la patch disponibile presso Microsoft (vedere i collegamenti nella sezione Metodo A: Usare un ACL (qui sotto). Questo protegge i sistemi vulnerabili e rimuove il worm da un sistema infetto. Tuttavia, l'applicazione della patch ai server impedisce solo al worm di infettare i server, non impedisce alle richieste HTTP GET di colpire i server. C'è ancora la possibilità che il server venga bombardato da una marea di tentativi di infezione.

La soluzione descritta in questo advisory è progettata per essere utilizzata insieme alla patch Microsoft per bloccare le richieste HTTP GET "Code Red" in un punto di ingresso di rete.

Questa soluzione tenta di bloccare l'infezione, ma non risolve i problemi causati dall'accumulo di un numero elevato di voci della cache, adiacenze e voci NAT/PAT, poiché l'unico modo per analizzare il contenuto della richiesta HTTP GET è seguire la creazione di una connessione TCP. La procedura seguente non consente di proteggere la rete da un'analisi. Tuttavia, protegge un sito dall'infestazione proveniente da una rete esterna o riduce il numero di tentativi di infezione che una macchina deve servire. In combinazione con il filtro in entrata, il filtro in uscita impedisce ai client infetti di diffondere il worm "Code Red" nell'Internet globale.

Piattaforme supportate

La soluzione descritta in questo documento richiede la funzionalità di contrassegno basato su classi nel software Cisco IOS. In particolare, la capacità di individuare corrispondenze in qualsiasi parte di un URL HTTP utilizza la funzionalità di classificazione delle porte secondarie HTTP in NBAR. Di seguito sono riepilogati le piattaforme supportate e i requisiti minimi del software Cisco IOS:

Piattaforma	Software Cisco IOS minimo
7200	12.1(5)T
7100	12.1(5)T
3745	12.2(8)T
3725	12.2(8)T
3660	12.1(5)T
3640	12.1(5)T
3620	12.1(5)T
2600	12.1(5)T
1700	12.2(2)T

Nota: per utilizzare NBAR, è necessario abilitare Cisco Express Forwarding (CEF).

Il contrassegno basato su classi e DNBAR (Distributed NBAR) sono disponibili anche sulle seguenti piattaforme:

Piattaforma	Software Cisco IOS minimo
7500	12.1(6)E
FlexWAN	12.1(6)E

Rileva il tentativo di infezione nei log Web IIS

Il tentativo iniziale di infezione invia una richiesta HTTP GET di grandi dimensioni al server IIS di destinazione. L'impronta originale "Code Red" è mostrata di seguito:

```
2001-08-04 16:32:23 10.101.17.216 - 10.1.1.75 80 GET /default.ida
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNN%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u
7801%u9090%u9090%u8190%u00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a 403
```

L'impronta "Code Red" II è illustrata di seguito:

```
2001-08-04 15:57:35 10.7.35.92 - 10.1.1.75 80 GET /default.ida XXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX%u9090
%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%
u9090%u8190%u00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a 403 -
```

Si noti che la richiesta GET cerca sempre un file con estensione ida. Si tratta di una stringa comune in tutti i tentativi di infezione e può pertanto essere utilizzata come criterio di corrispondenza con un contrassegno basato su classi in IOS. Il resto della richiesta GET non sarà necessariamente coerente, in quanto sta solo tentando di creare un overflow del buffer. A tale scopo, è possibile confrontare le due voci precedenti.

Si è ora appreso che la differenza tra queste due firme è dovuta a una nuova varietà del verme

"Code Red", soprannominato CodeRed.v3 o CodeRed.C. Il ceppo originale "Code Red" contiene la stringa "NNNNNNN" nella richiesta GET, mentre il nuovo ceppo contiene "XXXXXXXX". Per ulteriori informazioni, fare riferimento a Symantec Advisory .

Il 6 agosto 2001, alle 18:24 EDT, abbiamo registrato un nuovo ingombro. Da allora abbiamo imparato che questa è l'impronta lasciata dallo scanner di vulnerabilità eEye .

```
2001-08-06 22:24:02 10.30.203.202 - 10.1.1.9 80 GET /x.ida AAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=X 403 HTTP/1.1 -
```

La tecnica per bloccare "Code Red" fornita in questo avviso può anche bloccare questi tentativi di scansione semplicemente stringendo la definizione della mappa di classe come mostrato nella sezione successiva.

Contrassegna gli hack "Code Red" in entrata utilizzando la funzionalità di contrassegno basato su classi IOS

Per bloccare il verme "Code Red", utilizzare uno dei tre metodi descritti di seguito. Tutti e tre i metodi classificano il traffico dannoso utilizzando la funzionalità MQC di Cisco IOS. Il traffico viene quindi interrotto come descritto di seguito.

Metodo A: Uso di un ACL

Questo metodo utilizza un ACL sull'interfaccia di output per eliminare i pacchetti contrassegnati come "Code Red". Utilizzare il diagramma di rete seguente per illustrare i passaggi di questo metodo:

Di seguito sono riportati i passaggi per configurare questo metodo:

1. Classificare gli hack "Code Red" in entrata con la funzione di contrassegno basato su classi nel software Cisco IOS, come mostrato di seguito:

   ```
   Router(config)#class-map match-any http-hacks
   Router(config-cmap)#match protocol http url "*default.ida*"
   Router(config-cmap)#match protocol http url "*cmd.exe*"
   Router(config-cmap)#match protocol http url "*root.exe*"
   ```

   La mappa di classe sopra riportata viene eseguita all'interno degli URL HTTP e corrisponde a una delle stringhe specificate. Si noti che sono stati inclusi altri nomi di file oltre a default.ida di "Code Red". È possibile utilizzare questa tecnica per bloccare simili tentativi di hack, come il virus Sadmind, che è spiegato nei seguenti documenti:http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS00-078.asphttp://www.sophos.com/virusinfo/analyses/unixsadmind.html

2. Compilare un criterio e utilizzare il comando **set** per contrassegnare gli hack "Code Red" in ingresso con una mappa dei criteri. Questo documento utilizza un valore DSCP di 1 (in decimale) perché è improbabile che questo valore sia assegnato a qualsiasi altro traffico di rete.In questa sezione vengono contrassegnati gli hack "Code Red" in ingresso con una mappa dei criteri denominata "mark-inbound-http-hacks".
```
Router(config)#policy-map mark-inbound-http-hacks
Router(config-pmap)#class http-hacks
Router(config-pmap-c)#set ip dscp 1
```

3. Applica il criterio come in ingresso nell'interfaccia di input per contrassegnare i pacchetti in arrivo con "rosso codice".
```
Router(config)#interface serial 0/0
Router(config-if)#service-policy input mark-inbound-http-hacks
```

4. Configurare un ACL che corrisponda al valore DSCP di 1, come impostato dai criteri del servizio.
```
Router(config)#access-list 105 deny ip any any dscp 1
Router(config)#access-list 105 permit ip any any
```

   Nota: le versioni software Cisco IOS 12.2(11) e 12.2(11)T introducono il supporto per la parola chiave **log** sull'ACL nella definizione sulle mappe di classe da usare con NBAR (CSCdv48172). Se si usa una versione precedente, non usare la parola chiave **log** sull'ACL. In questo modo tutti i pacchetti vengono commutati in base al processo invece che in base al CEF e NBAR non funzionerà poiché richiede il CEF.
5. Applicare l'ACL in uscita sull'interfaccia di output che si connette ai server Web di destinazione.
```
Router(config)#interface ethernet 0/1
Router(config-if)#ip access-group 105 out
```

6. Verificare che la soluzione funzioni come previsto. Eseguire il comando **show access-list** e verificare che il valore "match" per l'istruzione deny sia in aumento.
```
Router#show access-list 105
Extended IP access list 105
 deny ip any any dscp 1 log (2406 matches)
 permit ip any any (731764 matches)
```
   Nel passaggio della configurazione, è possibile anche disabilitare l'invio dei messaggi IP non raggiungibili con il comando **no ip unreachable** interface-level per evitare che il router investa risorse eccessive.Questo metodo non è consigliato se è possibile instradare il traffico DSCP=1 a Null 0 tramite criteri, come descritto nella sezione Metodo B.

Metodo B: Usa Policy-Based Routing (PBR)

Questo metodo utilizza il routing basato su criteri per bloccare i pacchetti contrassegnati come "Code Red". Non è necessario applicare i comandi di questo metodo se i metodi A o C sono già configurati.

Di seguito sono riportati i passaggi per l'implementazione di questo metodo:

1. Classificare il traffico e contrassegnarlo. Utilizzare i comandi **class-map** e **policy-map** mostrati nel metodo A.
2. Utilizzare il comando **service-policy** per applicare il criterio come criterio in entrata sull'interfaccia di input per contrassegnare i pacchetti in arrivo con "lettura codice". Vedere il metodo A.
3. Creare un ACL IP esteso che corrisponda ai pacchetti contrassegnati con "Code Red".
   ```
   Router(config)#access-list 106 permit ip any any dscp 1
   ```
4. Utilizzare il comando **route-map** per creare un criterio di routing.
   ```
   Router(config)#route-map null_policy_route 10
   Router(config-route-map)#match ip address 106
   Router(config-route-map)#set interface Null0
   ```
5. Applicare la mappa route all'interfaccia di input.
   ```
   Router(config)#interface serial 0/0
   Router(config-if)#ip policy route-map null_policy_route
   ```
6. Verificare che la soluzione funzioni come previsto con il comando **show access-list**. Se si usano gli ACL di output e si è abilitata la registrazione degli ACL, è possibile usare anche i comandi **show log**, come mostrato di seguito:
   ```
   Router#show access-list 106
   Extended IP access list 106
    permit ip any any dscp 1 (1506 matches)

   Router#show log
   Aug 4 13:25:20: %SEC-6-IPACCESSLOGP:
    list 105 denied tcp A.B.C.D.(0) -> 10.1.1.75(0), 6 packets
   Aug 4 13:26:32: %SEC-6-IPACCESSLOGP:
    list 105 denied tcp A.B.C.D.(0) -> 10.1.1.75(0), 6 packets
   ```
   Siamo in grado di prendere la decisione di scartare l'interfaccia in entrata del router, piuttosto che avere bisogno di un ACL di uscita su ciascuna interfaccia in uscita. Anche in questo caso, si consiglia di disabilitare l'invio dei messaggi IP unreachable con il comando **no ip unreachables**.

Metodo C: Usa criteri basati su classi

Questo metodo in genere è il più scalabile in quanto non dipende da PBR o ACL di output.

1. Classificare il traffico utilizzando i comandi **class-map** mostrati nel metodo A.
2. Creare un criterio utilizzando il comando **policy-map** e utilizzare il comando **Police** per specificare un'azione di rilascio per questo traffico.
   ```
   Router(config)#policy-map drop-inbound-http-hacks
   Router(config-pmap)#class http-hacks
   Router(config-pmap-c)#police 1000000 31250 31250
    conform-action drop exceed-action drop violate-action drop
   ```
3. Utilizzare il comando **service-policy** per applicare il criterio come criterio in entrata

sull'interfaccia di input per eliminare i pacchetti "rosso codice".

```
Router(config)#interface serial 0/0
Router(config-if)#service-policy input drop-inbound-http-hacks
```

4. Verificare che la soluzione funzioni come previsto con il comando **show policy-map interface**. Assicurarsi di visualizzare i valori incrementali per la classe e i singoli criteri di corrispondenza.

```
Router#show policy-map interface serial 0/0

Serial0/0

  Service-policy input: drop-inbound-http-hacks

    Class-map: http-hacks (match-any)
      5 packets, 300 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: protocol http url "*default.ida*"
        5 packets, 300 bytes
        5 minute rate 0 bps
      Match: protocol http url "*cmd.exe*"
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: protocol http url "*root.exe*"
        0 packets, 0 bytes
        5 minute rate 0 bps
      police:
        1000000 bps, 31250 limit, 31250 extended limit
        conformed 5 packets, 300 bytes; action: drop
        exceeded 0 packets, 0 bytes; action: drop
        violated 0 packets, 0 bytes; action: drop
        conformed 0 bps, exceed 0 bps, violate 0 bps

    Class-map: class-default (match-any)
      5 packets, 300 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

Restrizioni NBAR

Quando si utilizza NBAR con i metodi di questo documento, si noti che le funzionalità seguenti non sono supportate da NBAR:

- Più di 24 URL simultanei, host o tipi MIME corrispondono
- Corrispondenza oltre i primi 400 byte di un URL
- Traffico non IP
- Multicast e altre modalità di commutazione non CEF
- Pacchetti frammentati
- Richieste HTTP persistenti pipeline
- Classificazione URL/HOST/MIME/ con HTTP protetto
- Flussi asimmetrici con protocolli stateful
- Pacchetti provenienti da o destinati al router che esegue NBAR

Non è possibile configurare NBAR sulle seguenti interfacce logiche:

- Fast EtherChannel
- Interfacce che usano il tunneling o la crittografia

- VLAN
- Interfacce dialer
- Multilink PPP

Nota: NBAR è configurabile sulle VLAN a partire da Cisco IOS versione 12.1(13)E, ma è supportato solo nel percorso di commutazione software.

Poiché NBAR non può essere utilizzato per classificare il traffico di output su un collegamento WAN in cui viene utilizzato il tunneling o la crittografia, applicarlo ad altre interfacce sul router, ad esempio l'interfaccia LAN, per eseguire la classificazione di input prima che il traffico venga trasferito al collegamento WAN per l'output.

Per ulteriori informazioni su NBAR, vedere i collegamenti nella sezione Informazioni correlate