Gebruik NBAR en ACL's om het "Code Red"-woord te blokkeren

Inhoud

Inleiding

Dit document biedt een methode om de "Code Red"-worm te blokkeren op netwerkingspunten door Network-Based Application Recognition (NBAR) en Access Control Lists (ACL's) binnen Cisco IOS®-software op Cisco-routers. Deze oplossing dient te worden gebruikt in combinatie met de aanbevolen patches voor IIS-servers van Microsoft.

Opmerking: deze methode werkt niet op Cisco 1600 Series routers.

Opmerking: Sommige P2P-verkeer kan niet volledig geblokkeerd zijn vanwege de aard van het P2P-protocol. Deze P2P-protocollen veranderen dynamisch hun handtekeningen om elke DPI-motor te omzeilen, die hun verkeer volledig probeert te blokkeren. Daarom wordt aanbevolen de bandbreedte te beperken in plaats van ze volledig te blokkeren. Schroef de bandbreedte voor dit verkeer. Geef veel minder bandbreedte; laat de verbinding echter doorgaan .

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- QoS-servicebeleid (Quality of Service) met behulp van de opdrachten van de modulaire QoS-opdrachtregel (CLI).
- NBAR
- ACL's
- Op beleid gebaseerde routing

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies. De configuratie in dit document is getest op Cisco 3640 dat Cisco IOS-versie 12.2(24a) draait

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Het "rode code"-woord blokkeren

Het eerste wat u moet doen om "Code Red" te bestrijden, is de pleister die beschikbaar is bij Microsoft aanbrengen (zie de koppelingen in sectie Methode A: Gebruik hieronder een ACL). Dit beschermt kwetsbare systemen en verwijdert de worm van een besmet systeem. Als het patch alleen op uw servers wordt toegepast, voorkomt dit echter dat de worm de servers infecteert, maar dat houdt niet in dat de HTTP GET verzoeken de servers raken. De server kan nog steeds gebombardeerd worden met een overvloed aan besmettingspogingen.

De oplossing die in dit advies wordt beschreven is ontworpen om in combinatie met het Microsoft-stopcontact te werken om de "Code Red" HTTP verzoeken te blokkeren bij een netwerkingpunt.

Deze oplossing probeert de infectie te blokkeren, maar zal geen problemen genezen veroorzaakt door de opbouw van grote aantallen cache items, nabijheid en NAT/PAT-items, omdat de enige manier om de inhoud van HTTP GET aanvraag te analyseren, is het volgen van een TCP-verbinding. De volgende procedure helpt niet tegen een scan van het netwerk te beschermen. Het zal een locatie echter beschermen tegen besmetting door een extern netwerk of het aantal infectiepogingen verminderen dat een machine moet bedienen. In combinatie met inkomende filtering voorkomt uitgaande filtering dat geïnfecteerde klanten de "Code Red"-worm naar het wereldwijde internet kunnen verspreiden.

Ondersteunde platforms

De oplossing die in dit document wordt beschreven, vereist de op klasse gebaseerde markering binnen Cisco IOS-software. In het bijzonder, de mogelijkheid om op elk deel van een HTTP URL aan te passen gebruikt de HTTP sub-port classificatie optie binnen NBAR. De ondersteunde platforms en de minimale Cisco IOS-softwarevereisten worden hieronder samengevat:

platform	Minimale Cisco IOS-software
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

Opmerking: U moet Cisco Express Forwarding (CEF) activeren om NBAR te kunnen gebruiken.

Op klasse gebaseerde markering en Distributed NBAR (DNBAR) zijn ook beschikbaar op de volgende platforms:

platform	Minimale Cisco IOS-software
7500	12.1(6)E
FlexWAN	12.1(6)E

Detecteert de infectiepoging in de IOS-weblogs

De eerste infectie poging stuurt een groot HTTP GET verzoek naar de doel-IS server. De oorspronkelijke voetafdruk "Code Red" wordt hieronder weergegeven:

```
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
```

De voetafdruk "Code Red" II is als volgt:

```
2001-08-04 15:57:35 10.7.35.92 - 10.1.1.75 80 GET /default.ida XXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX%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 -
```

Let op dat het GET verzoek altijd op zoek is naar een bestand met een .ida-extensie. Dit is een algemeen string in alle infectiepogingen en kan daarom gebruikt worden als matrixcriteria met class-based markering in IOS. De rest van het TARGET-verzoek zal niet noodzakelijk consistent zijn, aangezien het slechts probeert een bufferoverloop te creëren. Dit is te zien door de bovenstaande twee vermeldingen te vergelijken.

Er wordt nu gemeld dat het verschil tussen deze twee handtekeningen het gevolg is van een nieuwe stam van de "Code Red" worm, die CodeRed.v3 of CodeRed.C wordt genoemd. De oorspronkelijke "Code Red" stam bevat de "NNNNNNNNNNN"-string in het GET verzoek, terwijl

de nieuwe stam "XXXXXXXX" bevat. Raadpleeg het Symantec Advisory voor meer informatie.

Om 18:24 uur EDT, 6 aug. 2001, registreerden we een nieuwe voetafdruk. Sindsdien hebben we geleerd dat dit de voetafdruk is die nog achterblijft bij de eEye kwetsbaarheidsscanner .

```
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 -
```

De techniek voor het blokkeren van de "Code Red" in dit advies kan deze scanpogingen ook blokkeren door de definitie van de class map zoals in het volgende vak getoond, simpelweg aan te scherpen.

Merk inkomende "Code Rode" Hacks met IOS-klasse-gebaseerde markering

Gebruik een van de drie onderstaande methoden om de "Code Red"-worm te blokkeren. Alle drie methoden classificeren kwaadaardig verkeer met behulp van de Cisco IOS MQC optie. Dit verkeer wordt vervolgens laten vallen zoals hieronder wordt beschreven.

Methode A: Gebruik ACL

Deze methode gebruikt ACL op de uitvoerinterface om de gemarkeerde "Code Rood"-pakketten te laten vallen. Gebruik het volgende netwerkdiagram om de stappen in deze methode te illustreren:

Hier volgen de stappen om deze methode te configureren:

1. Classificeer inkomende "Code Rode" hacks met de class-Based Marking optie in Cisco IOS-software, zoals hieronder getoond:
   ```
   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*"
   ```

   De bovenstaande class map ziet binnen HTTP URL's en correspondeert met een van de opgegeven strings. Merk op dat we andere bestandsnamen hebben toegevoegd dan de default.ida van "Code Red". U kunt deze techniek gebruiken om soortgelijke hack pogingen te blokkeren, zoals het Sadrow-virus, dat in de volgende documenten wordt uitgelegd:http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS00-078.asphttp://www.sophos.com/virusinfo/analyses/unixsadmind.html
2. Creëer een beleid en gebruik de **set** opdracht om inkomende "Code Rode" hacks met een beleidskaart te markeren. Dit document gebruikt een DSCP-waarde van 1 (in decimale volgorde) omdat het onwaarschijnlijk is dat een ander netwerkverkeer deze waarde

draagt.Hier markeren we binnenkomende "Code Red" hacks met een beleidskaart genaamd "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. Pas het beleid op de inkomende interface toe om "Code Red"-pakketten aan te sluiten.

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

4. Configureer een ACL die overeenkomt met de DSCP-waarde van 1, zoals ingesteld door het servicebeleid.

```
Router(config)#access-list 105 deny ip any any dscp 1
Router(config)#access-list 105 permit ip any any
```

Opmerking: Cisco IOS-softwarereleases 12.2(11) en 12.2(11)T introduceren ondersteuning voor het **logtrefwoord** op de ACL bij het definiëren van klassenkaarten voor gebruik met NBAR (CSCdv48172). Als u een eerdere release gebruikt, gebruikt u het **logtrefwoord** niet op de ACL. Door dit te doen worden alle pakketten proces-geschakeld in plaats van CEF-geschakeld, en NBAR zal niet werken aangezien het CEF vereist.

5. Pas de ACL-uitgang op de uitvoerinterface toe die op de doelwebservers is aangesloten.

```
Router(config)#interface ethernet 0/1
Router(config-if)#ip access-group 105 out
```

6. Controleer of de oplossing werkt zoals verwacht. Voer de opdracht **toegang-lijst tonen uit** en zorg ervoor dat de "lucifers"waarde voor het ontkennen van statement toeneemt.

```
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)
```

In de configuratiestap, kunt u ook het verzenden van IP onbereikbare berichten met de **geen ip onbereikbare** interface-level opdracht verhinderen om de router te vermijden om excessieve middelen uit te geven.Deze methode wordt niet aanbevolen als u het DSCP=1 verkeer naar Nul 0 kunt leiden, zoals beschreven in Methode B sectie.

Methode B: Gebruik op beleid gebaseerde routing (PBR)

Deze methode gebruikt op beleid gebaseerde routing om gemarkeerde "Code Red" pakketten te blokkeren. U hoeft de opdrachten in deze methode niet toe te passen, indien de methoden A of C al zijn ingesteld.

Hier volgen de stappen om deze methode toe te passen:

1. Classificeer het verkeer en merk het. Gebruik de opdrachten **class-map** en **policy-map** die in methode A zijn afgebeeld.

2. Gebruik de opdracht **service-beleid** om het beleid als een inkomende beleid op de invoerinterface toe te passen om "Code Red"-pakketten te markeren. Zie methode A.
3. Maak een uitgebreide IP ACL-toegangscontrolelijst die overeenkomt met de markering "Rood"-pakketten.

```
Router(config)#access-list 106 permit ip any any dscp 1
```

4. Gebruik de **route-kaart** opdracht om een routebeleid te bouwen.

```
Router(config)#route-map null_policy_route 10
Router(config-route-map)#match ip address 106
Router(config-route-map)#set interface Null0
```

5. Pas de route-map toe op de invoerinterface.

```
Router(config)#interface serial 0/0
Router(config-if)#ip policy route-map null_policy_route
```

6. Controleer of de oplossing werkt zoals verwacht met de opdracht **toegangslijst tonen**. Als u ACL's (uitgevoerd) gebruikt en ACL's gebruikt heeft, kunt u ook de opdrachten **voor** het **weblog** gebruiken, zoals hieronder wordt getoond:

```
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
```

We kunnen de afgedankte beslissing maken op de ingangsinterface van de router in plaats van op elke uitgang ACL-interface. Opnieuw, raden we aan om het verzenden van IP onbereikbare berichten met de opdracht **geen ip onbereikbaar** opdracht uit te schakelen.

Methode C: Op klasse gebaseerde controle gebruiken

Deze methode is over het algemeen het meest schaalbaar aangezien het niet van PBR of uitvoer ACLs afhangt.

1. Classificeer het verkeer met de **class-map** opdrachten die in methode A worden getoond.
2. Bouw een beleid dat de **politiek-kaart** opdracht gebruikt en gebruik de **politie** opdracht om een vervolgactie voor dit verkeer te specificeren.

```
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. Gebruik de opdracht **Service-beleid** om het beleid als een inkomende beleid op de invoerinterface toe te passen om de "Code Red" pakketten te laten vallen.

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

4. Controleer dat uw oplossing werkt zoals verwacht met de **show beleid-map** opdracht. Zorg ervoor dat u stijgende waarden voor de klasse en de individuele verbindingscriteria ziet.

```
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
```

NBAR-beperkingen

Wanneer NBAR wordt gebruikt met de methoden in dit document, let er dan op dat de volgende functies niet door NBAR worden ondersteund:

- Meer dan 24 gelijktijdige URL's, HOST's of MIME-type overeenkomsten
- Overeenkomend met meer dan de eerste 400 bytes in een URL
- Niet-IP-verkeer
- Multicast en andere niet-CEF-switchmodi
- Gefragmenteerde pakketten
- Aanhoudende HTTP-verzoeken in de leidingen
- URL/HOST/MIME/classificatie met beveiligd HTTP
- Asymmetrische stromen met stateful protocols
- Packets die afkomstig zijn van of bestemd zijn voor de router die NBAR gebruikt

U kunt NBAR niet op de volgende logische interfaces configureren:

- Fast EtherChannel
- Interfaces die tunneling of encryptie gebruiken
- VLAN's
- Kiezerinterfaces
- Multilink PPP

Opmerking: NBAR is Configureerbaar op VLAN's vanaf Cisco IOS release 12.1(13)E, maar alleen ondersteund in het software-switching pad.

Aangezien NBAR niet kan worden gebruikt om uitvoerverkeer op een WAN-link te classificeren waar een tunneling of encryptie wordt gebruikt, past u het in plaats daarvan op andere interfaces op de router, zoals de LAN-interface, toe om invoerclassificatie uit te voeren voordat het verkeer naar de WAN-link is geschakeld voor uitvoer.

Zie de koppelingen in de Gerelateerde informatie voor meer NBAR - informatie