باسمه تعالی

حملات DDoS با سوءاستفاده از پروتکل NTP

تقویت ترافیک پروتکل NTP نوعی از حمله DDoS است که در آن فرد حمله‌کننده با سوءاستفاده از سرویس‌دهنده‌های NTP در دسترس عموم، فرد قربانی را هدف بسته‌های UDP قرار می‌دهد.

پروتکل NTP یکی از قدیمی‌ترین پروتکل‌های شبکه است که برای همگام‌سازی ساعت بین سیستم‌ها از طریق شبکه استفاده می‌شود. این پروتکل معمولاً به صورت کلاینت-سرور مدل می‌شود ولی در عین حال می‌تواند به صورت peer-to-peer نیز مدل شود. در پیاده‌سازی این پروتکل، ارسال بسته‌های برچسب زمانی با استفاده از پروتکل UDP و شماره پورت ۱۲۳ انجام می‌شود.

علاوه بر همگام‌سازی ساعت، نسخه‌های قدیمی NTP از یک سرویس پایش (مانیتورینگ) نیز پشتیبانی می‌کنند. با استفاده از این سرویس، مدیر شبکه می‌تواند به یک سرور NTP درخواستی مبنی بر پایش ترافیک ارسال کند. این کار با استفاده از دستور monlist انجام می‌شود. با ارسال این دستور به سرور لیستی از ۶۰۰ سیستم متصل به سرور مورد نظر به درخواست کننده بازگردانده می‌شود.

در بسیاری از حملات تقویت ترافیک با استفاده از NTP، حمله کننده به صورت متوالی دستور get monlist را با جعل آدرس IP قربانی به یک سرور NTP ارسال می‌کند. سرور نیز لیست ذکر شده را به سمت فرد قربانی ارسال می‌کند. این پاسخ بزرگتر از درخواست اولیه می‌باشد و باعث تقویت ترافیک می‌شود. در این روش، ضریب تقویت ترافیک مابین ۲۰ الی ۲۰۰ می‌باشد.

برای بررسی آسیب‌پذیر بودن یک سرور نسبت به این مورد می‌توان از دستور زیر استفاده کرد:

```
ntpdc -n -c monlist [Time Server IP]
```

در صورتی‌که سرویس‌دهنده NTP به پرسش فوق مطابق شکل زیر جواب دهد، آن سرویس‌دهنده مستعد استفاده شدن در حمله DDoS خواهد بود و بایستی با پیکربندی مناسب ذکر شده در ادامه مستند، مانع ارسال پاسخ فوق شد (البته لازم به ذکر است که از نسخه 4.2.7 به بعد قابلیت monlist از NTP حذف شده است).

```
freya:ntp_caps tuna$ ntpdc -n -c monlist 10.1.10.33
remote address          port local address      count m ver rstr avgint  lstint
===============================================================================
1.7.111.187             3291 127.0.0.1             1 5 4      0    349     349
241.140.62.63           3290 127.0.0.1             1 2 1      0    349     349
66.251.229.148          3288 127.0.0.1             1 5 4      0    350     350
2.67.10.67              3287 127.0.0.1             1 2 1      0    350     350
52.3.14.215             3285 127.0.0.1             1 5 4      0    350     350
138.248.122.13          3282 127.0.0.1             1 5 4      0    350     350
44.22.112.238           3281 127.0.0.1             1 2 1      0    350     350
44.93.70.190            3279 127.0.0.1             1 5 4      0    350     350
152.177.91.144          3278 127.0.0.1             1 2 1      0    351     351
121.69.181.186          3275 127.0.0.1             1 2 1      0    351     351
241.7.121.66            3273 127.0.0.1             1 5 4      0    351     351
78.144.191.1            3272 127.0.0.1             1 2 1      0    351     351
183.236.162.96          3269 127.0.0.1             1 2 1      0    351     351
87.137.188.3            3267 127.0.0.1             1 5 4      0    352     352
91.34.29.191            3263 127.0.0.1             1 2 1      0    352     352
249.177.179.29          3261 127.0.0.1             1 5 4      0    352     352
162.14.11.89            3260 127.0.0.1             1 2 1      0    352     352
82.186.176.145          3258 127.0.0.1             1 5 4      0    353     353
29.1.237.203            3257 127.0.0.1             1 2 1      0    353     353
144.122.181.119         3254 127.0.0.1             1 2 1      0    353     353
55.51.24.1              3252 127.0.0.1             1 5 4      0    353     353
183.155.39.120          3251 127.0.0.1             1 2 1      0    353     353
129.75.39.215           3249 127.0.0.1             1 5 4      0    353     353
103.245.79.131          3248 127.0.0.1             1 2 1      0    354     354
245.47.25.63            3246 127.0.0.1             1 5 4      0    354     354
66.2.70.239             3245 127.0.0.1             1 2 1      0    354     354
203.207.21.161          3243 127.0.0.1             1 5 4      0    354     354
26.102.33.1             3240 127.0.0.1             1 5 4      0    354     354
1.162.80.111            3239 127.0.0.1             1 2 1      0    354     354
91.148.121.140          3237 127.0.0.1             1 5 4      0    355     355
186.231.245.137         3234 127.0.0.1             1 5 4      0    355     355
47.154.10.215           3233 127.0.0.1             1 2 1      0    355     355
190.235.127.188         3231 127.0.0.1             1 5 4      0    355     355
167.236.63.215          3230 127.0.0.1             1 2 1      0    355     355
59.235.254.190          3228 127.0.0.1             1 5 4      0    356     356
0.244.206.111           3227 127.0.0.1             1 2 1      0    356     356
```

در نوع دیگری از حمله با سوءاستفاده از پروتکل NTP، دستور readvar به کار گرفته می‌شود که برای خواندن نسخه NTP است. البته در این حالت ترافیک مانند استفاده از دستور monlist تقویت نمی‌شود. ضریب تقویت این حالت حدوداً برابر ۳۰ می‌باشد.

برای بررسی آسیب‌پذیر بودن یک سرور نسبت به readvar می‌توان از دستور زیر استفاده کرد:

ntpq -c rv [Time Server IP]

روش امن‌سازی

پیش‌گیری از وقوع حمله DDoS ناشی از تقویت ترافیک NTP بسیار دشوار است زیرا پاسخ‌های دریافتی قانونی بوده و همچنین از سوی سرویس‌دهنده‌های قانونی NTP دریافت شده است. با این حال رعایت موارد زیر می‌توانند تا حدودی مفید واقع شوند:

- با توجه به برطرف شدن قابلیت monlist در نسخه‌های 4.2.7 به بعد، اکیداً توصیه می‌گردد که سرویس‌دهنده NTP به‌روزرسانی گردد.

- در حالتی که سرویس‌دهنده NTP قدیمی بوده و امکان به‌روزرسانی آن وجود ندارد، بایستی قابلیت monlist غیرفعال گردد. بدین منظور بایستی در فایل ntp.conf به خط restrict default مقدار noquery افزوده شود:

```
restrict default kod nomodify notrap nopeer noquery
restrict -6 default kod nomodify notrap nopeer noquery
```

- استفاده از لیست کنترل دسترسی (ACL): می‌توان با محدودسازی ترافیک UDP/123 تا حدودی جلوی گسترش حمله به داخل شبکه را گرفت. البته در صورت اشباع لینک‌های اصلی ارتباطی، این روش کارآمد نیست. در خصوص تجهیزات سیسکو، در اغلب موارد می‌توان از دستورات زیر استفاده نمود:

```
! Core NTP configuration
ntp update-calendar        ! update hardware clock (certain hardware only, i.e. 6509s)
ntp server 192.0.2.1       ! a time server you sync with
ntp peer   192.0.2.2       ! a time server you sync with and allow to sync to you
ntp source Loopback0       ! we recommend using a loopback interface for sending NTP messages if possible
!
! NTP access control
ntp access-group query-only 1       ! deny all NTP control queries
ntp access-group serve 1            ! deny all NTP time and control queries by default
ntp access-group peer 10            ! permit time sync to configured peer(s)/server(s) only
ntp access-group serve-only 20      ! permit NTP time sync requests from a select set of clients
!
! access control lists (ACLs)
access-list 1 remark utility ACL to block everything
access-list 1 deny any
!
access-list 10 remark NTP peers/servers we sync to/with
access-list 10 permit 192.0.2.1
access-list 10 permit 192.0.2.2
access-list 10 deny any
!
access-list 20 remark Hosts/Networks we allow to get time from us
access-list 20 permit 192.0.2.0 0.0.0.255
access-list 20 deny any
```

برای تجهیزات ژونیپر نیز می‌توان از مجموعه دستورات زیر استفاده نمود:

```
system {
   ntp {
      authentication-key [key-id] type md5 value "[pass-phrase]";
      trusted-key [key-id];
      /* Allow NTP to sync if server clock is significantly different than local clock */
      boot-server 192.0.2.1;
      /* NTP server to sync to */
      server 192.0.2.1;
      server 192.0.2.2 key [key-id] prefer;
   }
}

from {
   source-address {
      0.0.0.0/0;
      /* NTP server to get time from */
      192.0.2.1/32 except;
   }
   protocol udp;
   port ntp;
}
then {
   discard;
}

from {
   source-address {
      /* NTP server to get time from */
      192.0.2.1/32;
   }
   protocol udp;
   port ntp;
}
then {
   accept;
}
```