نوشته شده توسط root
شنبه ، 8 خرداد 1389 ، 18:33 - آخرین بروزرسانی شنبه ، 8 خرداد 1389 ، 19:03

یکی از حمله های که معمولا بر روی Server ها یا سیتم عامل ها انجام می شود حمله ای است به نام DDoS در این نوع حمله فرد Hacker یا cracker به دنبال یک سیستم آلوده یا ضعیف می گردد و سعی می کند آن را آلوده کند و بعد از آلوده کردن آن سیستم . از آن سیستم برای حمله به سایر سیستم ها آستفاده می کند و بعد از مدتی به طور خوشه ای تعداد زیادی سیستم را آلوده می کند که این سیستم های آلوده هر کدام سعی می کنند به دنبال یک سیستم دیگر گشته وآن را آلوده کنند و ممکن است بعد از مدتی یک شبکه ای آلوده به وجود آید که این شبکه آلوده همگی باهم به یک سیستم یا سیستم دیگری حمله می کنند و این حمله باعث از کار انداختن سیستم های فراوانی در طول شبکه می گردد و باعث اشغال شدن شبکه یا بالا رفتن ترافیک شبکه می گردند .

از این نوع حمله به حمله ای عظیم در سال ۲۰۰۶ به server های اصلی خدمات DNS می توان اشاره کرد که در اثر پیدا شدن باگ در Bind خیلی از server های خدمات DNS برای مدتی طولانی از کار افتادند و فلج شدند و ترافیک خطوط آنقدر بالا رفت که باعث از کار افتادن تمام نقل و انتقالات اینترنتی گردید . که این نوع حمله برای همیشه در تاریخچه اینترنت ثبت گردید .

در FreeBSD برای پی بردن به این که در یک شبکه چه سیستم های حمله هایی از نوع DDoS انجام می دهند برنامه ها یا port های متفاوتی وجود دارد که از آن جمله می توان به برنامه یا پورت scan_ddos اشاره کرد . که این برنامه تمام دستگا ها ی موجود در شبکه شما را بررسی می کند و به شما می گوید که ایا این چنین سیستمی وجود دارد یا نه .

برای نصب این برنامه در FreeBSD کافی است در ترمینال دستور های زیر را تایپ کنید

```
# cd /usr/ports/security/ddos_scan
# make install clean
```

بعد از مدتی این برنامه نصب می شود . برای استفاده از این برنامه کافی است در ترمینال دستور زیررا در ترمینال تایپ کنید

```
$ dds 192.168.10.0/24
```

خوب این دستور تمام IP های موجود در شبکه شما را چک می کند و اگر موردی پیدا کرد برای شما گزارش می دهد . اگر این برنامه خروجی به شما نداد : این به این معنی است که هیچ دستگاه آلوده ای وجود ندارد.

شما می توانید IP خاصی را نیز چک کنید .

البته برنامه های دیگری وجود دارد . که می توان به برنامه پر قدرت

find_ddos

ولی متاسفانه من چون از ورژن ۶۴ بیت FreeBSD استفاده می کنم در سیستم من نصب نشد و error داد که فقط بر روی سیستم های 32 بیت نصب می گردد.

find_ddos-4.2_1 is only for i386، while you are running amd64

باید این برنامه را نیز چک کرد .