PING

Contact:

mailto:Satanic.hellboy@Yahoo.com
mailto:satanic.hellboy@gmail.com

www.shirazboot.blogfa.com

نویسنده: **satanic.hellboy**

تاریخ: ۱۳۸۶/۶/۱

SATANIC HELLBOY

www.shirazboot.blogfa.com

ابزار ping :

فرمان **ping** یکی ازابتدایی ترین ابزارهای تشخیص وجود نارسایی در شبکه به شمار می رود.این ابزار به سادگی در خواستهایی را در سطح لایه **ICMP** (یکی از پروتکل های لایه شبکه در مدل چهار لایه ای **TCP/IP**) به میزبان ارسال کرده و منتظر پاسخ می ماند.معمولا از این ابزار برای بررسی صحت عملکرد اتصال به شبکه استفاده می شود. اما به زودی همانطور که خواهید دید اهداف دیگری نیز دارد.

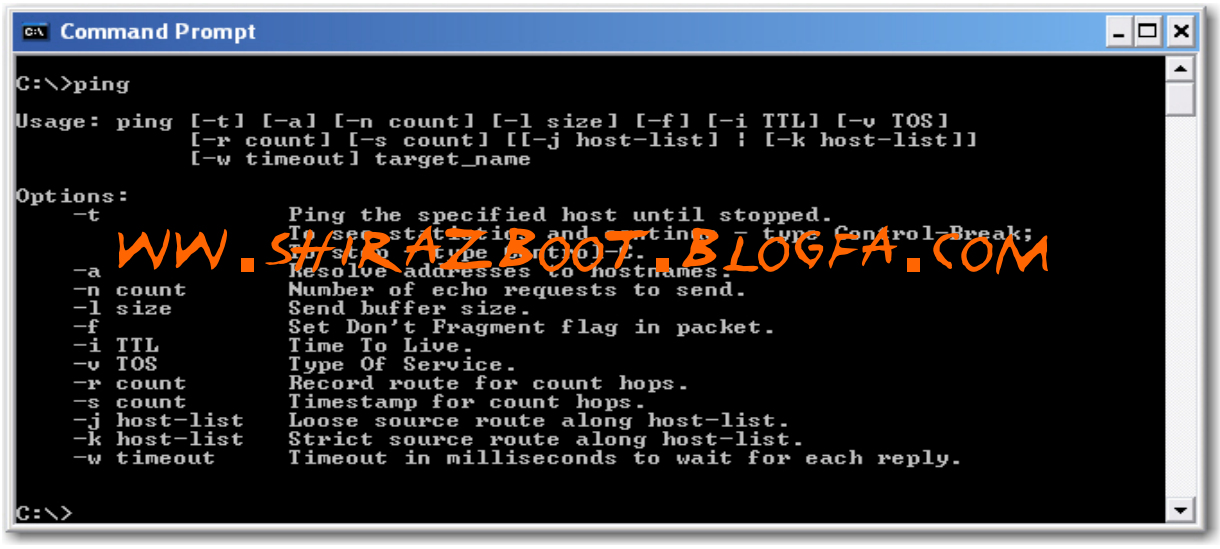
بهره گیری از ابزار ping :

برای اجرای برنامه **ping** از منوی اصلی با انتخاب گزینه های **Start/programs/MS-DOS Prompt** پنجره **DOS** را باز کرده و سپس عبارت **ping system** را تایپ کنید.

نکته:

در فرمان مذکور می توانید به جای کلمه **system** آدرس **IP** یا نام اینترنتی کامپیوتری که با آن در حال تبادل اطلاعات هستید و یا از سویچ ها استفاده کنید.

برای دیدن سویچ های برنامه می توانید دستور **ping** را تنها به کار ببرید مانند نمونه:



گزینه های متداول برنامه Ping :

(یونیکس) -c<count> (ویندوز) -c<count>	تعداد درخواستهای ارسالی
(یونیکس) -f	حالت flood Ping که مشخصه آن ارسال بیشترین درخواست ممکن با آخرین سرعت ممکن است.در این حالت به ازای هر درخواست یک علامت نقطه(.) و به ازای هر پاسخ دریافتی یک علامت backspace (کد ^H) بر روی صفحه چاپ می شود.حالت فوق متدی بصری برای مشاهده بسته های از دست رفته حین فرایند ارسال و دریافت محسوب می شود.همچنین این حالت بسیار روش موثری برای اشغال پهنای باند است.از این رو تنها کاربر اصلی سیستم موسوم به superuser امکان بهره گیری از گزینه را دارد.
(یونیکس) -i <wait>	تنظیم تاخیر مابین ارسال درخواست ها را بر حسب ثانیه مشخص می کند(به طور پیش فرض این تاخیر برابر با یک ثانیه است.
(یونیکس) -m <TTL> (ویندوز) –I <TTL>	تعیین مقدار TTLیا Time-To-live .مقدار این متغیر بیانگر تعداد روترهای موجود در مسیر پیغام pingاز مبدا به مقصد است.
(یونیکس)-n (ویندوز) –a	گزینه n– در سیستم های یونیکس موجب عدم پذیرش آدرس IP به عنوان ورودی برنامه ping می شود.گزینه a– تحت سیستم عامل ویندوز درست عکس این کار را انجام داده و برنامه ping را مجبور به پذیرش آدرسهای ip به عنوان ورودی این برنامه می کند.بنا به پیش فرض نسخه های تحت یونیکس و تحت ویندوز برنامه ping از روشهای متفاوتی برای ترجمه اسامی به آدرسهای ip متناظر بهره می برند.
(یونیکس) –R (ویندوز) -r	فعال سازی گزینه record route در بسته ICMpارسالی.چنانچه روترهای موجود در مسیر بسته نسبت به این گزینه عکس

	العمل نشان دهند.مسیر تعیین شده برای بسته از طریق گزینه های Ip را ثبت می کنند. بدین ترتیب برنامه ping مسیر طی شده توسط بسته را نیز نمایش خواهد داد.اما از آن جا که بیشتر روترها از گزینه های مربوط به مسیر یابی منبع صرف نظر می کنند.گزینه مورد بحث نیز اغلب نادیده گرفته می شود.
–s<size> (یونیکس) –l<size> (ویندوز)	این گزینه امکان تعیین اندازه بسته Icmp ارسالی را در اختیار قرار می دهد.از آن جا که اندازه طول هدر هر بسته ICmp برابر هشت بایت است بنابراین اندازه واقعی هر بسته برابر با 8+<size> خواهد بود. اندازه پیش فرض هر بسته Icmp در سیستم عامل یونیکس برابر ۵۶ بایت و در سیستم عامل ویندوز برابر با ۲۴ بایت است. لذا با احتساب هدر اندازه های فوق به ترتیب برابر با ۶۴ و ۳۲ بایت خواهند بود.
–w<wait> (یونیکس) –w<timeout> (ویندوز)	توقف برنامه ping از ادامه عملیات پس از سپری شدن مدت زمان تعیین شده توسط پارامتر <wait> بر حسب ثانیه.توقف عملیات به اندازه تعیین شده توسط پارامتر <time out> بر حسب میلی ثانیه به ازای هر پاسخ دریافتی.

همانطور که می بینید Ping در سیستم های عامل ویندوز و یونیکس متفاوت است.

در سیستم عامل یونیکس تا زمانی که کلید ctrl+c را فشار ندهید برنامه به کار خود ادامه می دهد ولی در ویندوز به طور پیش فرض برنامه چهار بسته Icmp به سیستم مورد نظر ارسال می کند.و برای تغییر این رفتار در ویندوز از گزینه –t استفاده می شود بدین ترتیب برنامه مذکور تا زمان خاتمه دادن به آن به کار خود ادامه خواهد داد هر چند که گزینه مزبور موجب از دست رفتن گزارش جامع عملیات ping می شود.

به نمونه ای از اجرای برنامه روی سیستم عامل لینوکس توجه کنید:

```
%  ping 192.168.1.102
PING 192.168.1.102  (192.168.1.102)  from  192.168.1.100 :
56(84)  bytes of data.
```

```
64  bytes  from  192.168.1.102:  icmp_seq=0  ttl=128  time=1.9 ms
64  bytes  from  192.168.1.102:  icmp_seq=1  ttl=128  time=0.7 ms
64  bytes  from  192.168.1.102:  icmp_seq=2  ttl=128  time=1.3 ms
64  bytes  from  192.168.1.102:  icmp_seq=3  ttl=128  time=0.7 ms
64  bytes  from  192.168.1.102:  icmp_seq=4  ttl=128  time=1.3 ms
64  bytes  from  192.168.1.102:  icmp_seq=5  ttl=128  time=0.7 ms
64  bytes  from  192.168.1.102:  icmp_seq=6  ttl=128  time=1.3 ms

---  192.168.1.102   ping statistics  ---
7 packets transmitted,  7 packets received,  0% packet lose
Round-trip min/avg/max  =  0.7/1.1/1.9 ms
```


بررسی نمونه: سوءاستفاده مهاجمین از برنامه ping:

نوع اول: ping مرگبار

بدون شک تا به حال چیزهایی در مورد ping مرگبار شنیده اید. Ping مرگبار فرایند کشنده ای است که به واسط ارسال بسته های بزرگتر از ۶۵۵۳۶ حاصل می شود. با وجودی که لایه شبکه قادر به پشتیبانی بسته های بزرگتر از این اندازه نیست! مکانیزمی با عنوان Fragmentation امکان ارسال بسته های بزرگتر از۶۵۵۳۶ بایت را با استفاده از برنامه ping در اختیار قرار می دهد.اما نکته غم انگیز در اینجاست که به محض در یافت تکه های مختلف بسته در مقصد و سر هم شدن آنها عملیات کامپیوتر گیرنده مختل می شود.(از این مورد زمانی استفاده می شود که بخواهیم سیستم میزبان ریستارت بشود بنا به دلایل خاص!!!!.)

دلیل چنین رفتاری را نمی توان عملکرد نامطلوب برنامه **ping** دانست بلکه علت آن را باید در الگوریتمی که لایه **IP** جهت سر هم بندی تکه های مختلف بسته ارسالی اتخاذ می کند، جستجو نمود.!!!!

و اما پیش گیری بهتر از حمله است!!!

بیشتر نسخه های مختلف برنامه **ping** امکان ارسال بسته های بزرگ تر از ۶۵۵۳۶ بایت را از قابلیت های این ابزار حذف کرده اند.با این وجود سیستم عامل ۹۵ و همچنین برخی از نسخه های برنامه **NT** چنین امکانی را در اختیار کاربران قرار می دهند.البته برخی از سیستم های عامل به درستی **Ping** مرگبار را تشخیص داده و به سادگی از دریافت آن سر باز می زنند وبه عبارتی دیگر از پردازش آن جلوگیری به عمل می آورند.در مورد سیستم هایی که دارای چنین مکانیزمی نیستن، تنها را پیش گیری بهره گیری از مکانیزمی برای فیلتر کردن پورت ها یا استفاده از دیواره آتش به منظور بلوکه کردن هر گونه بسته **ICMP** دریافتی یا دست کم بسته هایی است که اندازه آنها از یک حد مشخصی بیشتر باشد.

نوع دوم: حمله دسته جمعی

یکی از حقه هایی که می توانید برای شبکه های محلی خود به کار ببرید این است که آدرس همگانی (یا اصطلاحاً **Broadcost address**) خود را در شبکه **ping** کنید. برای مثال اگر آدرس **Ip** شما **192.168.1.100** و ماسک شبکه ای که از آن استفاده می کنید **255.255.255.0** باشد در این صورت شما بر روی شبکه ای با شاخص **192.168.1.0** واقع بوده و از این رو آدرس همگانی شما عبارت است از **192.168.1.255** خواهد بود.

در چنین وضعیتی چنانچه به **ping**کردن آدرس فوق اقدام کنید به احتملا قوی از تمام سیستم های موجود در آن شبکه پاسخی را دریافت خواهید کرد(در برخی سیستم ها این کار مستلزم استفاده از گزینه **b-** هم چنین بر خورد داری از امتیازات کاربر اصلی یا همان

root می باشد).این یکی از موثرترین و سریع ترین روش ها برای آگاهی از سایر سیستم هایی است که تحت یک شبکه مشغول کار با آنها هستید.

عملیات فوق ممکن است به ظاهر فرایند بسیار ساده ای به نظر برسد اما بد نیست بدانید که استمرار آن خطر تهدید کننده ای برای سرویس های شبکه به شمار می آید.خطر مزبور هنگامی آشکار می شود که کاربران شبکه اقدام به ping کردن یک آدرس همگانی در آن شبکه نمایند.از آنجا که این اقدام آنها ترافیک سهمگینی را بر شبکه تحمیل می کند لذا به خودی خود نوعی حمله به شبکه سازماندهی می شود که معمولاً به عنوان Dos یا Denial-Of-Service شناخته می شود.برای نمونه یک شبکه مقیاس بزرگ(شامل بیش از ۶۵۰۰۰ کامپیوتر) از نوع کلاس B را در نظر بگیرید.اجرای فرایند مورد بحث بر روی یک چنین شبکه ای باعث خواهد شد تا تمامی کامپیوترهای این شبکه پاسخی را در در ازای در خواست ارسالی از جانب یکی از این کامپیوترها به آدرس همگانی به سوی آن کامپیوتر ارسال کنند(چه شود؟!!!)و این بدان معنی است که کامپیوتر مزبور کاملاً از کار بیفتد. به عبارت دیگر این کامپیوتر حکم مرگ خود را امضاء کرده است.از سوی دیگر مهاجمین می توانند از این شرایط کاملاً در جهت اهداف خود سوء استفاده نمایند.چنانچه مهاجمی بتواند به هر روشی آدرس IP کامپیوتر مورد نظر خود را از شبکه بدست آوردقادر خواهد بود تا با استفاده از برنامه ping در خواستی را از طرف آن کامپیوتر به یک آدرس همگانی از شبکه ارسال کند. بدین ترتیب کامپیوتر وی بعد از چند لحضه با خیل انبوهی از از پیغامهای ICMP مواجه شده و از کار باز می ایستد.(شما از این کارها نکنید.!!)در این فرایند مزاحم خراب کار خود هیچ پیغامی دریافت نمی کند.

اما راه مقابله برای چنین اقدامی چیست؟!!!!

اما تنها راه ممکن این است که کلیه سیستم ها باید از پاسخ به درخواست های ارسالی به آدرس های همگانی شبکه اجتناب کنند. می توان روترها و دیواره های آتش را چنان تنظیم تنمود که علاوه بر جلوگیری از قربانی شدن کامپیوترهای شبکه خود نیز از شرکت در این گونه فرایندها پرهیز نمایند.

WWW.shirazboot.blogfa.com