What is Psexec

Psexec is a light-weight telnet replacement. It lets you execute process (e.g. cmd.exe) on remote systems. But psexec executes just command line process on the remote system.

Psexec runs on

client: Windows Vista and higher
server: Windows Server 2008 and higher

Psexec Usage

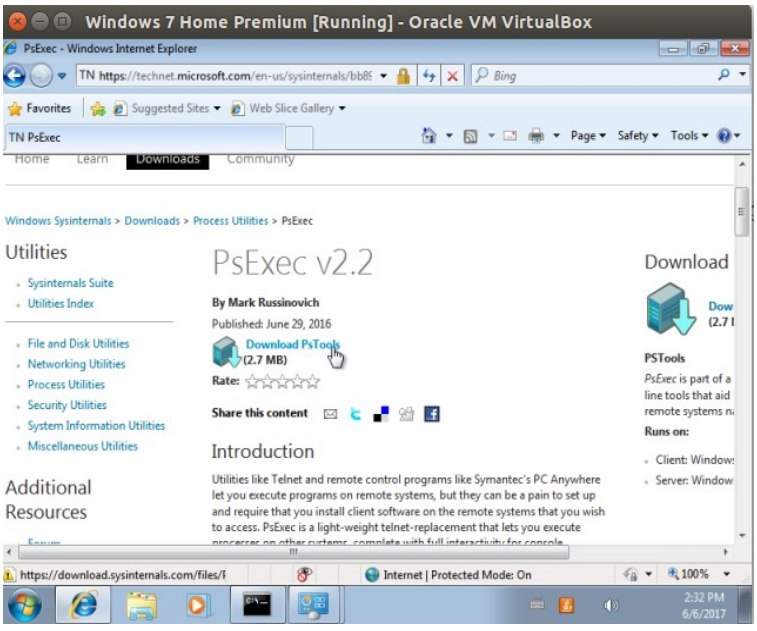
(+) Bu başlık birebir denenmiştir ve başarıyla uygulanmıştır.

Gereksinimler

Windows 7 Home Premium
Windows Server 2008
Psexec Tool

Diyelim ki Windows 7 sanal makinasında Windows Server makinasının komut satırını almak istiyoruz. Bunun için öncelikle Windows 7 sanal makinasına psexec tool'u indirilir.

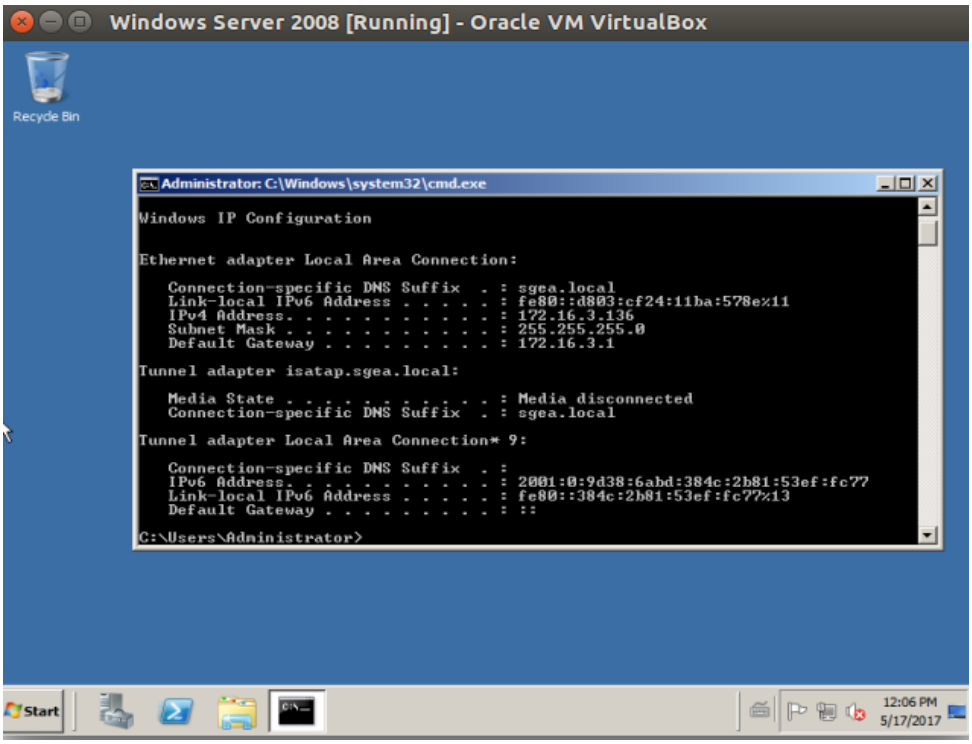
https://technet.microsoft.com/en-us/sysinternals/bb897553.aspx



İnen paket içerisindeki psexec.exe belirlenen bir dizine çıkarılır.

C:\Users\hefese\Desktop\PsExec.exe

Artık Windows 7 makinası hazır durumdadır. Şimdi Windows Server 2008 makinesini başlatalım ve ip'sini öğrenelim.



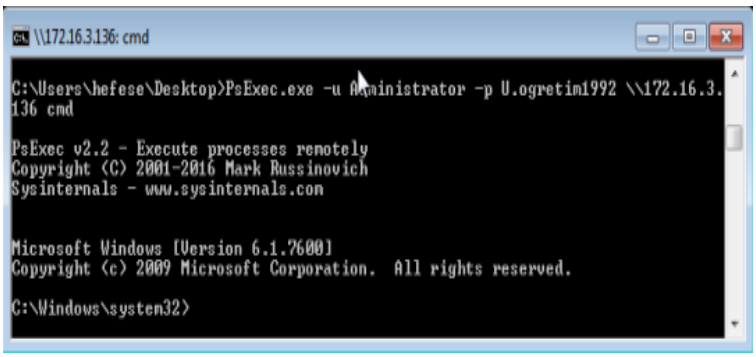
Hedef Windows Server 2008 makinesinin ip'si 172.16.3.136 imiş. Şimdi Windows 7 sanal makinasından hedef Windows Server'a psexec tool'u ile bağlanalım.

Windows 7 Home Premium

> cd C:\Users\hefese\Desktop\
> Psexec.exe -u Administrator -p U.ogretim1992 \\172.16.3.136 cmd

Not: psexec tool'u hedef sistemde cmd process'i başlatır.

Output:

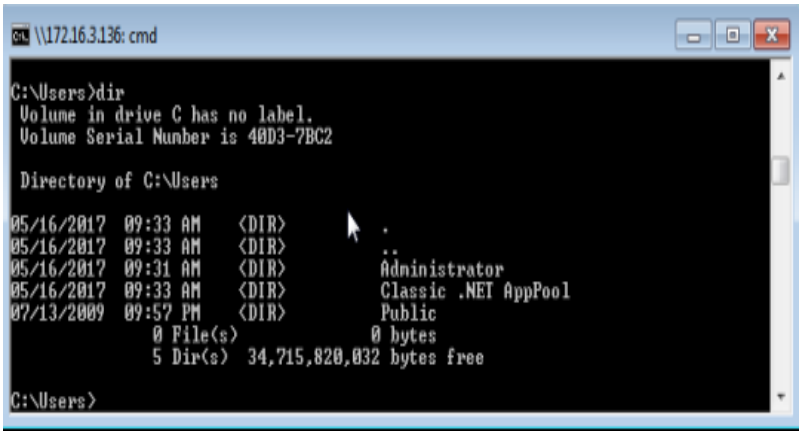


Görüldüğü üzere uzak sistemin komut satırı komut satırımıza gelmiştir.

Windows 7 Home Premium Console

> cd C:\Users
> dir

Output:



Artık uzak windows sunucusunu istediğimiz gibi kontrol edebiliriz.

Kaynak

https://technet.microsoft.com/en-us/sysinternals/bb897553.aspx

https://ss64.com/nt/psexec.html

YTE Eğitimi Defter Notları