

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

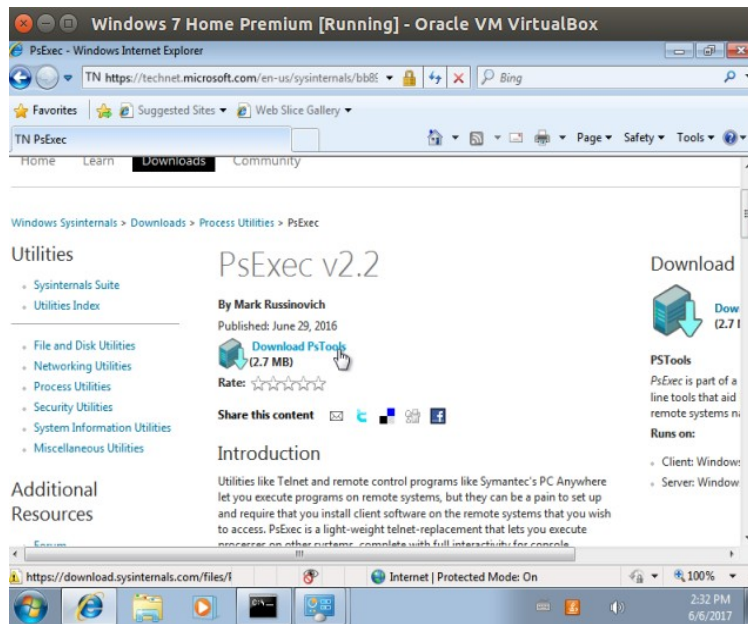
Windows 7 Home Premium

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.

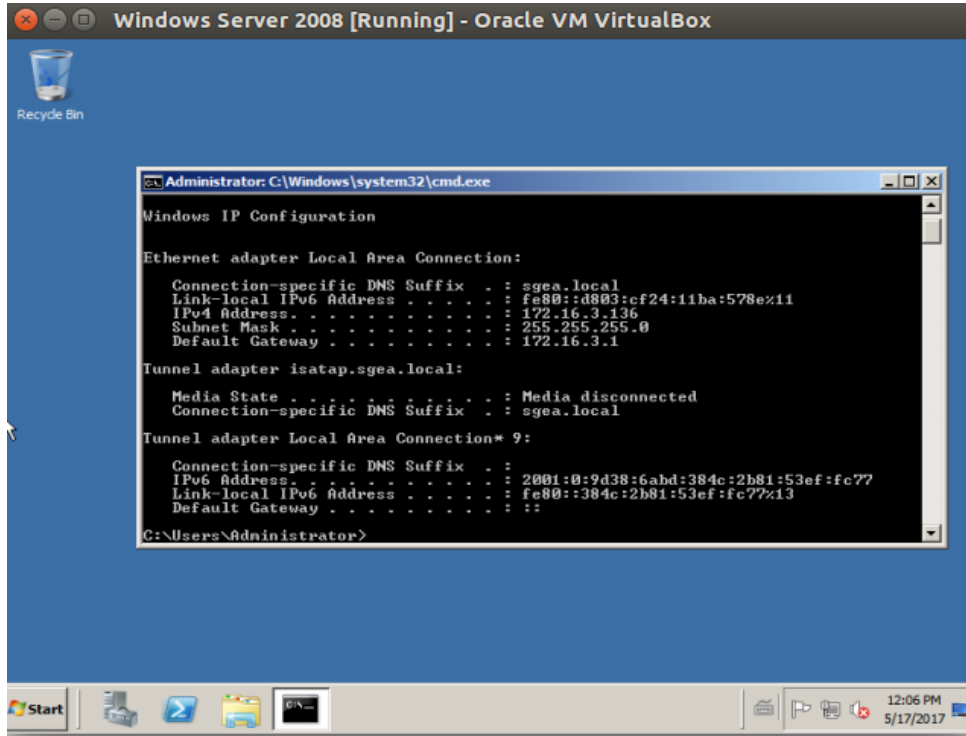
<https://technet.microsoft.com/en-us/sysinternals/bb897553.aspx>



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:

```
\\172.16.3.136: cmd
C:\Users\hefese\Desktop>PsExec.exe -u Administrator -p U.ogretim1992 \\172.16.3.136 cmd
PsExec v2.2 - Execute processes remotely
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

Görüldüğü üzere uzak sistemin komut satırı komut satırımıza gelmiştir.

Windows 7 Home Premium Console

```
> cd C:\Users
> dir
```

Output:

```
\\172.16.3.136: cmd
C:\Users>dir
Volume in drive C has no label.
Volume Serial Number is 40D3-7BC2

Directory of C:\Users

05/16/2017 09:33 AM <DIR> .
05/16/2017 09:33 AM <DIR> ..
05/16/2017 09:31 AM <DIR> Administrator
05/16/2017 09:33 AM <DIR> Classic .NET AppPool
07/13/2009 09:57 PM <DIR> Public
0 File(s) 0 bytes
5 Dir(s) 34,715,820,032 bytes free

C:\Users>
```

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