Remote Installation for Windows

Introduction

- Requirements
  - Remote Installation
  - Scheduling Jobs
  - Silent Installation
- Tools Explored
  - PsExec
  - RemoteExe
  - Winexe

Winexe

- winexe remotely executes commands on Windows systems from GNU/Linux.
- It is run from Linux where as PsExec run from windows
- freely redistributed under the terms of the GNU GPLv3.
- Free utility and light weight
- Support Windows XP and Higher
- Enable interactive command prompt
- Not required to manually install client software.

Winexe : Requirements

- Linux/Unix side
  - Working network
  - Samba
- Windows side
  - Working network
  - Standard Windows installation with enabled remote sharing and administration

Installation

- You can find the pre compiled packages in following repository. https://build.opensuse.org/project/repositories?project=home:ahajda:winexe

- Can download from sourceforce site http://sourceforge.net/projects/winexe/?source=dlp

Winexe : Usage

- winexe started without arguments shows list of options, using "--help" will show their descriptions.
- Most of the tasks can be done using syntax:

  winexe -U [Domain/]User%Password //host command

- *Eg:*

  # winexe -U HOME/Administrator%Pass123 //192.168.0.10 "ipconfig /all"

- To get Interactive command prompt of windows

  # winexe -U HOME/Administrator%Pass123 //192.168.0.10 cmd.exe

How does it works

- winexe connects to IPC$ share of host.
- Next it tries to open winexesvc control named pipe.
- If there is not such pipe, winexe copies winexesvc.exe to ADMIN$ share, creates winexesvc service, starts it and tries to connect to control pipe again
- After successful connection it passes optional parameters (ex. --runas, --system) and the command itself to winexesvc process via the pipe.
- winexe redirects those pipes to Linux console.
- After command exit winexe return its exit code to system.

Installing WinZip

- Here installing Winzip msi package from Ubuntu 12.4 machine to Windows XP machine(192.168.100.130) where firewall traffic is enabled between these machine.
- Msi package(winzip155) and silent installation script(winzip-install) are located at shared location (192.168.100.128).
- Shell script for installing WinZip.

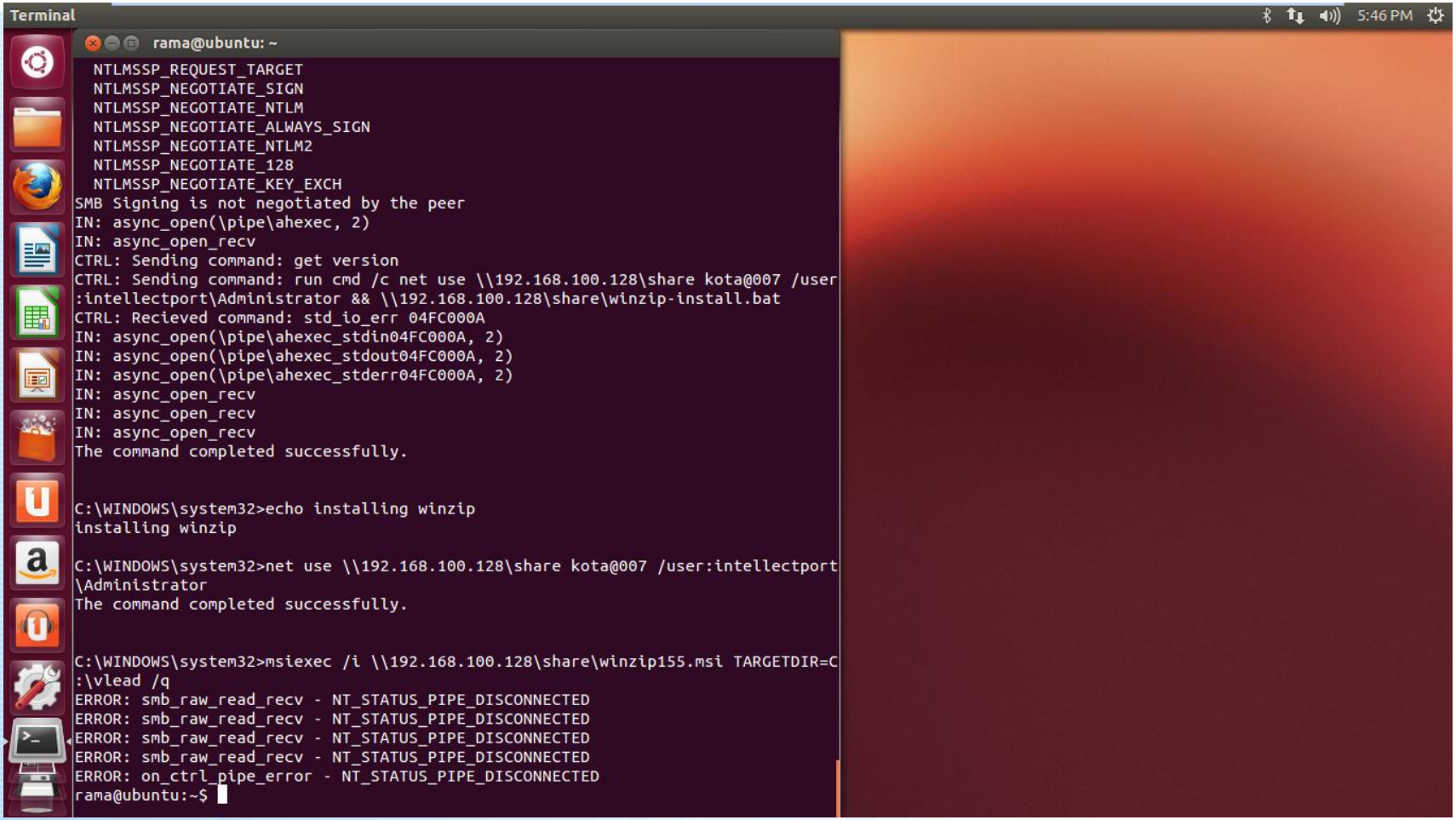
- Wizip.sh

  winexe --user intellectport/Administrator //192.168.100.130 'cmd /c net use \\192.168.100.128\share pass007 /user:intellectport\Administrator && \\192.168.100.128\share\winzip-install.bat' -d 11
- winzip-install.bat

echo installing winzip

net use \\192.168.100.128\share kota@007 /user:intellectport\Administrator

msiexec /i \\192.168.100.128\share\winzip155.msi TARGETDIR=C:\vlead /q


Terminal
5:46 PM
rama@ubuntu: ~
NTLMSSP_REQUEST_TARGET
NTLMSSP_NEGOTIATE_SIGN
NTLMSSP_NEGOTIATE_NTLM
NTLMSSP_NEGOTIATE_ALWAYS_SIGN
NTLMSSP_NEGOTIATE_NTLM2
NTLMSSP_NEGOTIATE_128
NTLMSSP_NEGOTIATE_KEY_EXCH
SMB Signing is not negotiated by the peer
IN: async_open(\pipe\ahexec, 2)
IN: async_open_recv
CTRL: Sending command: get version
CTRL: Sending command: run cmd /c net use \\192.168.100.128\share kota@007 /user
:intellectport\Administrator && \\192.168.100.128\share\winzip-install.bat
CTRL: Recieved command: std_io_err 04FC000A
IN: async_open(\pipe\ahexec_stdin04FC000A, 2)
IN: async_open(\pipe\ahexec_stdout04FC000A, 2)
IN: async_open(\pipe\ahexec_stderr04FC000A, 2)
IN: async_open_recv
IN: async_open_recv
IN: async_open_recv
The command completed successfully.
C:\WINDOWS\system32>echo installing winzip
installing winzip
C:\WINDOWS\system32>net use \\192.168.100.128\share kota@007 /user:intellectport
\Administrator
The command completed successfully.
C:\WINDOWS\system32>msiexec /i \\192.168.100.128\share\winzip155.msi TARGETDIR=C
:\vlead /q
ERROR: smb_raw_read_recv - NT_STATUS_PIPE_DISCONNECTED
ERROR: smb_raw_read_recv - NT_STATUS_PIPE_DISCONNECTED
ERROR: smb_raw_read_recv - NT_STATUS_PIPE_DISCONNECTED
ERROR: smb_raw_read_recv - NT_STATUS_PIPE_DISCONNECTED
ERROR: on_ctrl_pipe_error - NT_STATUS_PIPE_DISCONNECTED
rama@ubuntu:~$

Remarks

- **winexe** is very quiet, if you want to have some (not too much) debug info run with *-d 1* parameter
- No User interface.
- Debug gives lot of other info.
- No in-depth documentation.
- Issues with executing on multiple computers simultaneously.

References

- References
  - http://www.aldeid.com/wiki/Winexe
  - http://opensourceinfo.blogspot.in/2010/01/winexe.html
  - http://en.wikipedia.org/wiki/WinExe
  - http://manpages.ubuntu.com/manpages/intrepid/man1/winexe.1.html

Thank You