GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Symantec pcAnywhere 10.5

Daniel S. Moreira

October 25, 2002

SANS GSEC Practical Assignment v. 1.4b

Abstract:

The need to have remote access to applications and database of computers and central networks from remote locals began in the 60s, when the first time-sharing and multi-user systems appeared.

In today's virtual world, IT professionals must manage servers and networks in companies, in addition to offering technical support to companies' remote employees throughout the world, within the shortest period of time and using the least resources possible. In order to do that, it is necessary to have a reliable and secure remote control solution, that enables administrators connect, install, configure and solve problems of any connection.[8]

Introduction

In this document we will cover the installation methods of pcAnywhere and its main features that are:

-pcAnywhere Packager
  -Serialization
  -Authentication
-Administration Console
-Remote Access Perimeter Scanner
-Host Assessment tool
-Cryptography
-Enhanced Logging

Concept

How does pcAnywhere work ?

In order to establish a connection between two computers it is necessary that one of these computers has been initialized as the Host and the other as the Remote.

What is the host and what is the remote?

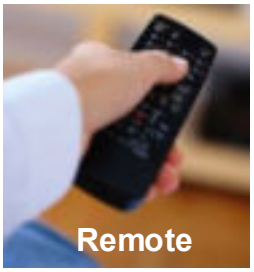


The remote connects and takes control of the host

The Host receives the call

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

On the one hand, the machine where pcAnywhere was installed or initialized as the host can be considered as a server, which will be controlled by the remote.
On the other hand, the machine where the pcAnywhere was installed or initialized as the Remote can be considered as a client that will make the access to the Host computer, therefore, being able to view through its screen the screen of the host computer. It also brings the possibility of access to applications and files of that computer.



A good way to remember this is to think of a T.V. and remote control. The remote controls the T.V. in the same way that the pcA Remote controls the pcA Host machine



How to create a connection through pcAnywhere ?:

pcAnywhere 10.5 supports the following connection methods:

- Modem
- Network
- Serial cable
- Parallel cable

Those connections are classified in pcAnywhere as follows: [1]

-Modem

In this connection method, both the Host and the Remote should have a modem, in which one of the modems installed will call the other, therefore establishing the speed for the connection and the protocol for data transfer.

Note: in corporate environments, the very existence of modems in workstations may constitute a violation of security policies, because it may be an insecure port for exploration of vulnerabilities.

-Network

The following network communication protocols may be used in the Network connection: TCP/IP and IPX/SPX used through network card in the Ethernet and Fast Ethernet standard, and they may be connected through: Hubs, Switches, Routers, Bridges or even through a cross over cable.
In this case the remote user should indicate to the product either the IP address or the access name.

© SANS Institute 2000 - 2002, Author retains full rights.

-Direct

The Direct connection uses connection methods through serials and LPT using null-modems cables or, in if the Operational System supports, it may be used a connection through a bi-directional parallel cable.

Once the connection method used has been determined, the administrator should click twice the connection icon. The Host will automatically initiate the Host service and will wait for a connection.

The remote service should be initialized through another machine by using the same connection method enabled for the Host.

By default, according to the 10.5 version, in order to have access it will be necessary at least one user and one access password. Once the requested information is entered, the user of the computer in which the Pcanywhere is configured as Remote will view the workstation of the Host machine, and, consequently will have access to files and applications.

In order to cancel the connection established, the user of the remote machine will have a button called "Finish Section" in its online toolbars. Once this button is clicked, the connection is canceled.

Problem :

Recently was discovered a security problem with pcAnywhere that permits Denial of Service.

To fix this kind of problem, Symantec released an update that can be downloaded by LiveUpdate or via WebSite

More information about this issue or how to install the patch, can be founded through the link bellow:

http://service2.symantec.com/SUPPORT/pca.nsf/docid/2001030512551712

Ports used by pcAnywhere [6]

The pcAnywhere 10.5 uses by default ports 5631 TCP and 5632 UDP
With this information, the IT administrator can configure the firewall to accept the connection via Internet. If he needs, there is also a possibility of altering the default ports of the product for any other that is not currently in use.
It is important to bear in mind that both the host and the remote should have the same ports configured, or else, the connection will not be established.

The data that traffics through the pcAnywhere via Internet can also traffic through a VPN

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Operating System Required:

-Windows 95/98/NT 4
-Windows Millennium Edition
-Windows 2000
-Windows XP Home Edition/Professional

Installation Methods:

When inserting the installation CD of pcAnywhere in the computer, the following installation options will appear¨

-pcAnywhere for the Professional

In this option pcAnywhere will be installed with all components, that is: Host, Remote and Packager (utilility that compiles a customized installation)
Only administrators usually use this installation because they are the people responsible to implement the most different products in a network its means, they are responsible by the policies and the procedures in a company and through this method of installation they can configure the product according with yours concerns.

-pcAnywhere for the individual

In this option you will be able to make connections to another machine and consequently gain access into the System, sending and receiving files, open application, print files remotely and also wait a connections to left be accessed.

-Remote Only

This installation has the same functionality that above however, will be not possible give access to remote machines

-Host Only

This method of installation provides connectivity with a remote computer allowing be managed.
Normally this option is used in workstation to provide helpdesk support to end user through long distance.

-LAN Host

This installation has the same functionally that above however it only supports LAN connections.

-Customized Installation Package

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

This option describes information on how to create a customized package to install pcAnywhere



Pcanywhere Installation Screen

In addition to the installation methods available in the graphic interface of the installation cd, there are other installation methods, that is:

- Login Script
- Shared Folders
- Page via Web

pcAnywhere Packager

On previous versions, 10.5 , in order to use pcAnywhere it was necessary to carry out a default installation of the product and customize it after installation.

Another problem was that after its installation it was possible to initialize a Host section, without even requesting an authentication method and any user could alter the configurations of the product.

Now, with the pcAnywhere packager resource, it is possible to customize the product before distributing to the stations.
In order to carry out such customization, there are the following features included in the Packager:

-Components

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

With this option, the administrator will be able to configure the components that will be installed in the product that is, establish whether there will be the Host and Remote resources or if it will support all communication protocols and if it will allow to be installed in all Operational Systems supported.

-Objects

The tab Objects shows the connection items that will be able to be initialized as Host (Modem, Direct or Network), and also the authentication method that, besides its own authentications and of Windows NT Domain Authentication, Symantec pcAnywhere also includes 12 authentication methods to validate users that connect to one of its hosts. The administrators can also create lists of centralized passwords and users' names, without having to keep a separate list of users for authentication in Symantec pcAnywhere.

- Active Directory Services (ADS)
- Novell® Directory Services (NDS)
- Novell LDAP
- Microsoft® LDAP
- Netscape® LDAP
- Windows Authentication
- Authentication of NT Domain
- FTP
- HTTP
- HTTPS
- Novell Bindery
- pcAnywhere user's password and name

-Policy

The tab Policy will enable the administrator to remove the product's administration screens, therefore avoiding access to customization interface to the user.

-Security

In the tab Security there are two customization methods

-Serialization

The serialization Resource in the packager was developed with a second protection layer for those cases in which a password is cracked. That means that during this installation packager customization it will be given a serial number to this product.

In order to establish connection between two computers, the remote user will need to have not only a user and an access password, but he/she will need to have in his/her remote the same serial existing in the Host computer as well, otherwise the connection will be aborted.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Problems:

I discovered a problem using this security option. Like I said, the Host and Remote machine will need to have the same serial number to establish a connection.

And how a hacker can break in?

Very easy, He or She just needs to install a full Symantec version and create a remote package, insert into it a lot of serials combinations that are permitted by product without any limit.
So, when the hacker discover the user and password using a sniffing like as Dsniff, he or she will not have problem to gain access because in your Remote will be a lot of combinations that will be checked during the authentication. [11]

How to protect against these attacks?

Bellow some recommendations, which you can implement to obtain more security:

-Use the Public Key Encryption
-Use a limitation IP address to give access for specifics remotes.
-Ensure that the news passwords contains alpha, numbers and signs characters,
-Change the passwords every 60 days
-Limit 3 logins Attempts per connection.
-Prompt to confirm connection
-Use different passwords between pcAnywhere and the Operating System [10]

-Lock

The lock Resource will lock up customizations done by the administrator, that is, the user will be able to view the software customization interfaces, however, he/she won't be able to alter anything.

After enabling the lock resource, pcAnywhere will also enable Integrity Check, which will periodically carry out its own analysis aiming at detecting configuration alterations. In case this happens, it will not allow any of the product services to be used, and in order to restore its functionalities it will be necessary to reinstall the software.

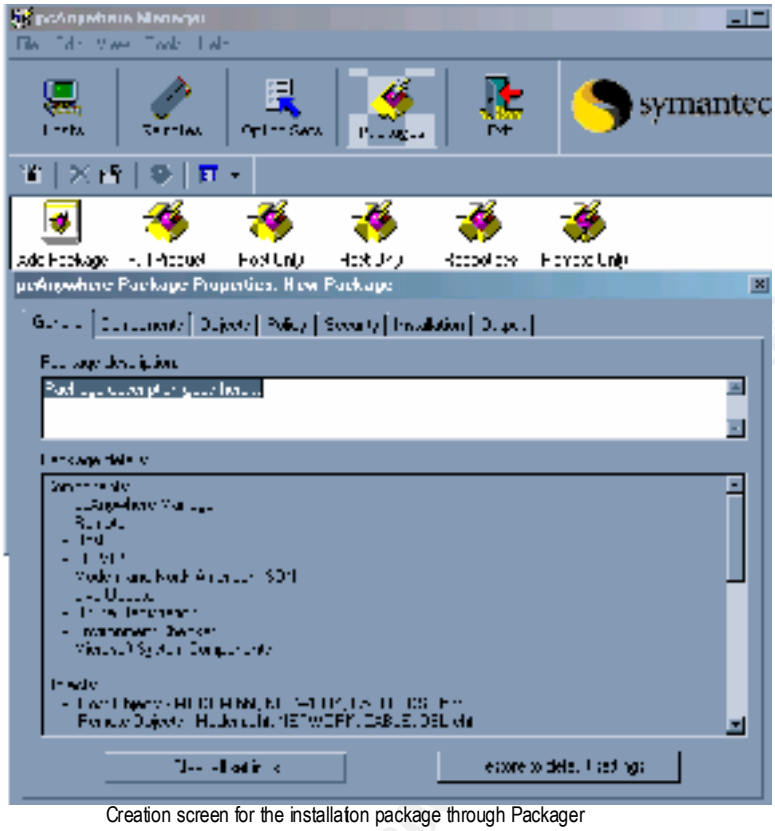
-Installation

In the tab Installation, the administrator will be able to remove the product installation screens, being also able to conduct a totally silent installation.

-Output

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

In the tab Output, the administrator can select MSI or .EXE to compile the customized installation package.



Creation screen for the installaton package through Packager

Are there packages should never be installed?

Symantec pcAnywhere has some packages customized that you can build and deploy in you network

Problem:

This packages was not configured according with your network, once installed can result risk for you environment because are not implemented with your security concerns. Always configure your specifics packages

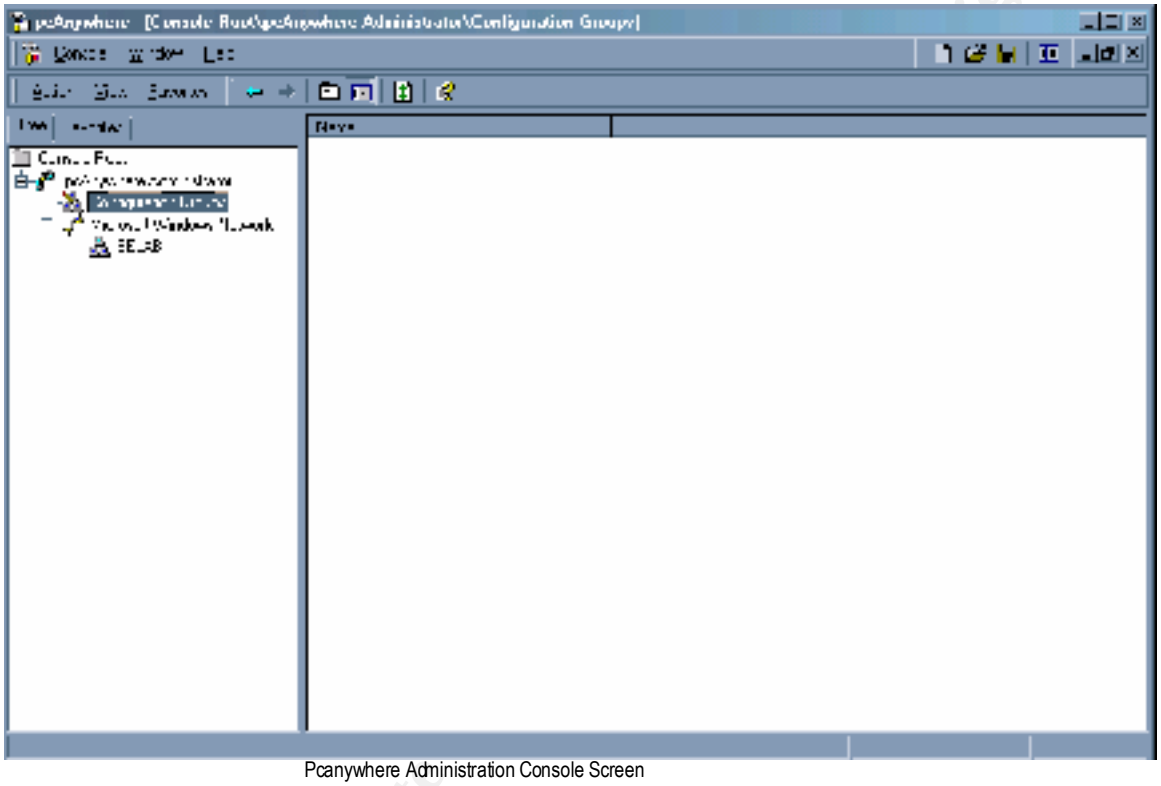
Administration Console

pcAnywhere administration can be done through a management console MMC (Microsoft Management Console). With this console it is possible to obtain information from the machine in which Pcanywhere was installed, as well as initialize and disable the host service in the stations, that is, on previous versions, 10.5, the stations which had pcAnywhere installed had to leave the service host pcAnywhere constantly enabled in

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

order to establish connection or leave the task of initializing the service to the user, who, usually, did not have the skills to handle the solution.

In addition to that, it is possible to choose which connection method will be initialized by the Host, such as modem , network and direct



Pcanywhere Administration Console Screen

Remote Access Perimeter Scanner [4]

Remote Access Perimeter Scanner is a utility included in the pcAnywhere installation CD to scan for Insecure Hosts in a network. With this, it is possible to analyze each computer to verify not only pcanywhere versions with vulnerabilities. This analysis can be done only in one IP or in a subnet.

Which others remote access software RAPS can scan?

The RAPS can scan the following products:

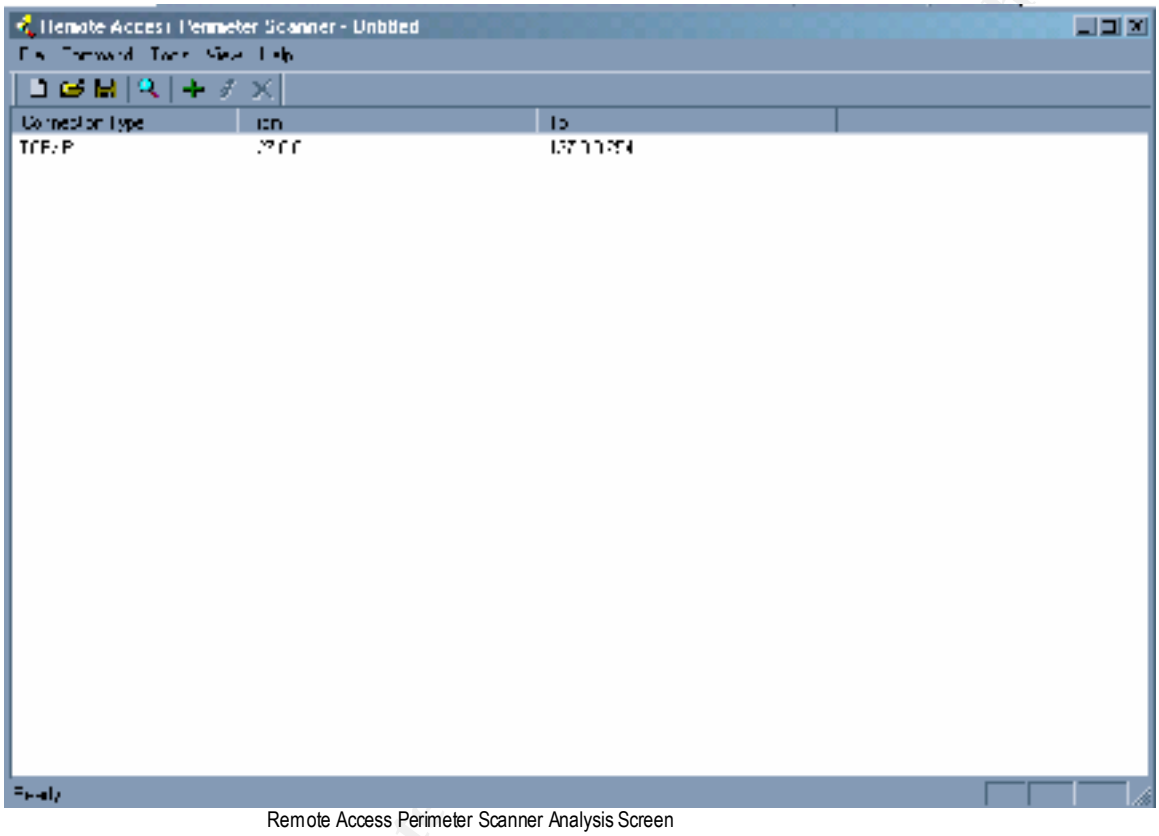
-LapLink
-Carbon Copy
-NetMeeting
-VNC
-ReachOut

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Problem:

RAPS is unable to detect whether a logon is required for Carbon Copy. [9]

Comments : There is not solution for this problem.

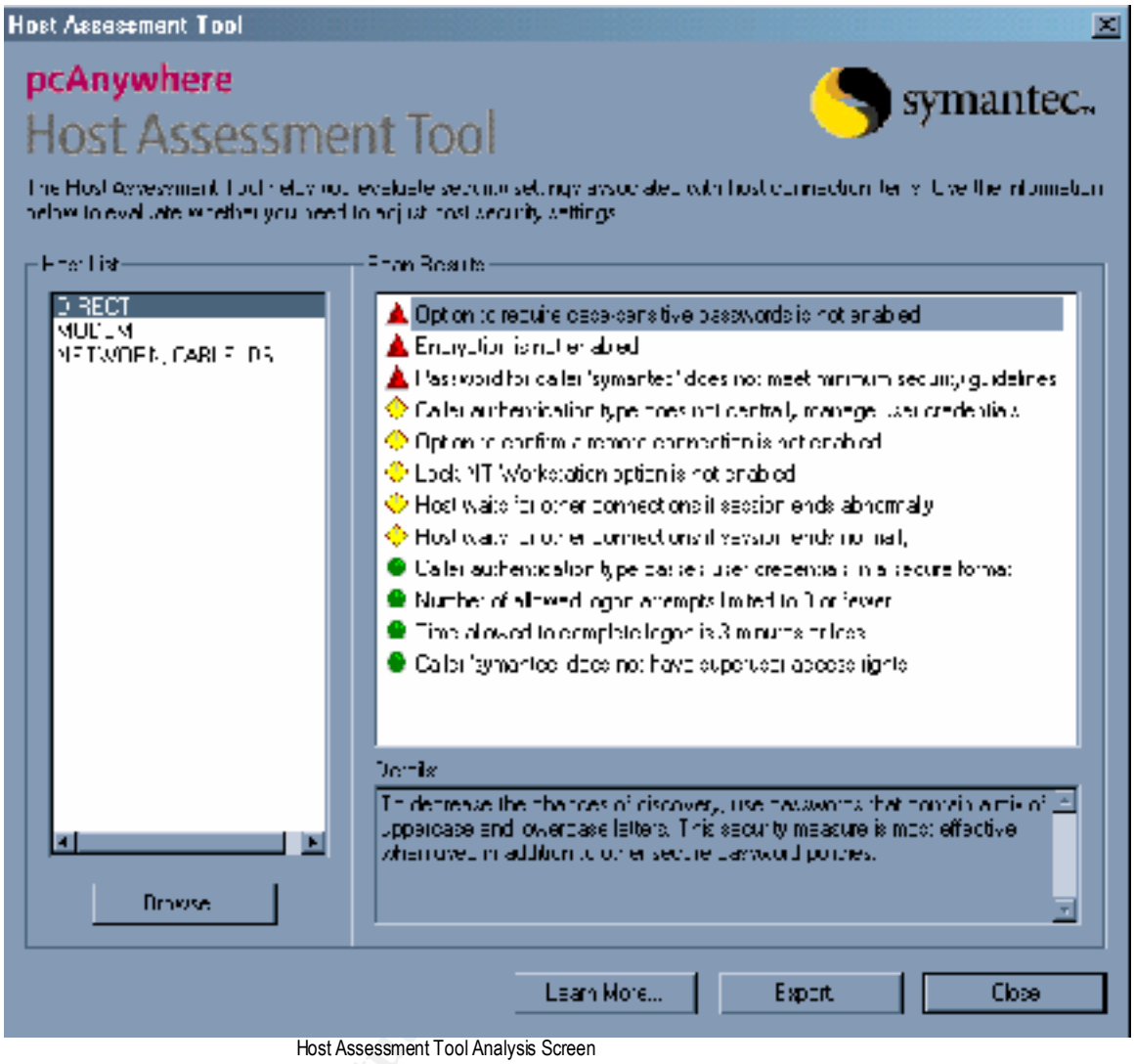


Remote Access Perimeter Scanner Analysis Screen

Host Assessment Tool

Host Assessment tool is a tool that help us evaluate the security configurations of a host and establish the chances of risk.
By means of a scan carried out in the Host, this utility shows - as colors – the risks found and tell us how to solve the problems.
This is a very important tool since it provides means for a greater analysis of the customizations carried out even before putting the solution in the product.
The administrator can run the tool without having to enable any of the product services to obtain Host analysis.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.



Host Assessment Tool Analysis Screen

Type of cryptography [7]

pcAnywhere has 3 cryptography levels to protect data between a Host and a Remote.

The cryptography levels are:

-Pcanywhere Encryption

In this method data are sent in non-clear-text-format. This is the most insecure level of cryptography included, however the only method to support old pcAnywhere versions connections

-Symmetric Encryption

In Symmetric Encryption the same cryptography key encrypt and decrypt data. It's means to realize a connection between two computers; they must be having

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

the same Key. One computer will be using this key to encrypt the data and another computer will use to decrypt it.

-Public key Encryption

The Public key Encryption encrypts and decrypts data using key pairs. This is the strongest method support by pcAnywhere.
In this case will be used two keys, one called Public and another called Private. The public will used to initialize the transmissions. After the data is encrypt and pass using public key from destination computer that will receive and decrypt using your private key.

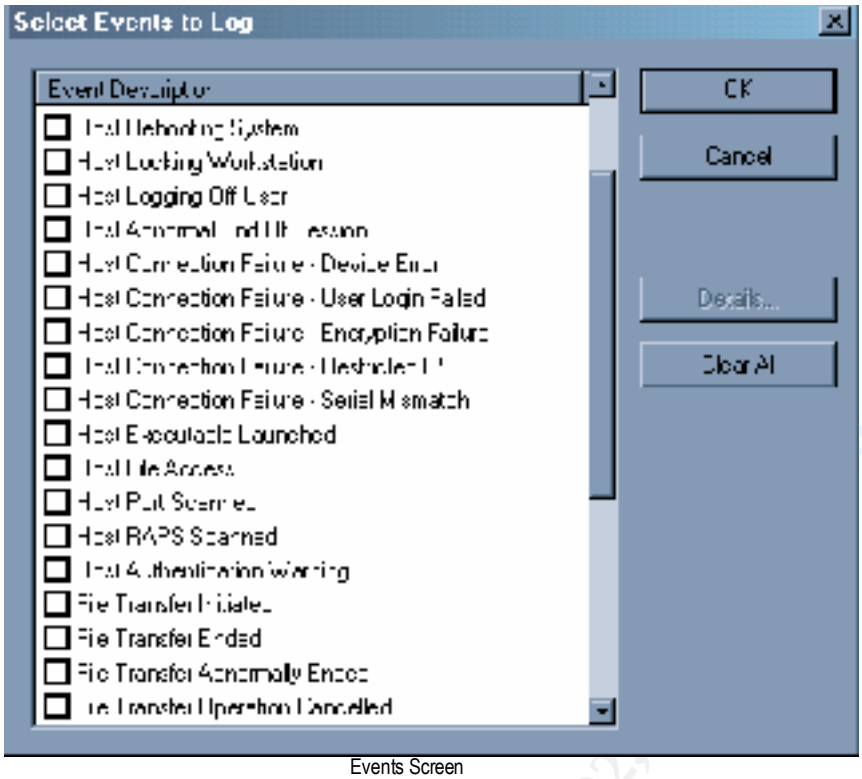
Public Key uses certification for security communication; it's means they need to confirm who holds the public key.

Enhanced Log

The pcanywhere can be configured to record logs and send these logs to a central server. Logs will bring the most diversified events, such as:
-User Login failed
-Host end Session
-Host Locking Workstation
-Host Rebooting System
-File Transfer Initiated and etc.

The pcAnywhere can send logs through SNMP traps, record the logs in the local Event Viewer or in another computer and record the logs in proprietary format of the local product with another computer.
With this feature the administrators will be able to view the end of a section.

© SANS Institute 2000 - 2002, Author retains full rights.



Events Screen

Conclusion:

Today, Pcanywhere, a remote access software, provides its users a remote access and file transfer solution, whose features enable them to balance performance and security, offering to the solution users flexibility in its customization, from its implementation up to the access and authentication levels.

Reference

[1] Document ID: 2001041212035112 Title: 'How to make a pcAnywhere 10.x connection'
Web URL: http://service1.symantec.com/SUPPORT/pca.nsf/docid/2001041212035112

[2] Document ID: 2001031315093512 Title: 'How to install pcAnywhere 10.x'
Web URL: http://service1.symantec.com/SUPPORT/pca.nsf/docid/2001031315093512

[3] Symantec pcAnywhere 10.5 Administration Guide

ftp://ftp.symantec.com/public/english_us_canada/products/pcanywhere/pcanywhere32/ver10.5/manuals/pca_105_admin.pdf

[4] Symantec pcAnywhere 10.5 User Guide

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

ftp://ftp.symantec.com/public/english_us_canada/products/pcanywhere/pcanywhere32/ver10.5/manuals/pca_105_user.pdf

[5] How to create an installation package for pcAnywhere 10x.

Web URL: http://service5.symantec.com/SUPPORT/pca.nsf/docid/2001011510414112

[6] Document ID: 1998122810210812 Title: 'pcAnywhere IP port usage'
Web URL: http://service1.symantec.com/SUPPORT/pca.nsf/docid/1998122810210812

[7] Document ID: 2001060508510012 Title: 'Types of encryption in pcAnywhere'
Web URL: http://service1.symantec.com/SUPPORT/pca.nsf/docid/2001060508510012

[8] Security Remote Control for IT Support Organization

http://score2.symantec.com/salecomm/tools/pca/pca10_secure_remote_control_wp.pdf

[9] Document ID: 2002030416013412 Title: 'pcAnywhere 10.5.1 - Readme.txt'
Web URL: http://service1.symantec.com/SUPPORT/pca.nsf/docid/2002030416013412

[10] 2002-06-18 heavy brute-force password guessing attacks
http://www.infosec.rochester.edu/alerts/2002-06-18-vuln-brute.html

[11] Dsniff and Switched Network Sniffing
http://www.giac.org/practical/Brad_Bowers.doc

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.