

# [TOOL] Windows TCP/IP Stack Hardening Tool

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-08/0059.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 08/14/05

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 14 Aug 2005 17:40:41 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

-----

Windows TCP/IP Stack Hardening Tool

---

## SUMMARY

## DETAILS

The following tool was designed to harden the Windows TCP/IP stack against different types of DoS attacks. The tool also provides a simple to use GUI. The tool has been tested to work under all versions of Windows XP and Windows 2000.

You can download the tool's source code from:

<<http://www.securitywireless.info/download/sourceHard.txt>>

<http://www.securitywireless.info/download/sourceHard.txt>

Tool Source:

```
Private Sub cmdRetrive_Click()
```

```
DefVal(0).Text =
```

```
GetDWORDValue("HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",  
"EnableICMPRedirect")
```

```
If DefVal(0).Text = "Error" Then DefVal(0).Text = "NP"
```

```
DefVal(1).Text =
```

```
GetDWORDValue("HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",
```

## Securiteam: [TOOL] Windows TCP/IP Stack Hardening Tool

"SynAttackProtect")

If DefVal(1).Text = "Error" Then DefVal(1).Text = "NP"

DefVal(2).Text =

GetDWORDValue("HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",  
"TCPMaxConnectResponseRetransmissions")

If DefVal(2).Text = "Error" Then DefVal(2).Text = "NP"

DefVal(3).Text =

GetDWORDValue("HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",  
"TcpMaxHalfOpen")

If DefVal(3).Text = "Error" Then DefVal(3).Text = "NP"

DefVal(4).Text =

GetDWORDValue("HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",  
"TCPMaxHalfOpenRetired")

If DefVal(4).Text = "Error" Then DefVal(4).Text = "NP"

DefVal(5).Text =

GetDWORDValue("HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",  
"TCPMaxPortsExhausted")

If DefVal(5).Text = "Error" Then DefVal(5).Text = "NP"

DefVal(6).Text =

GetDWORDValue("HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",  
"TCPMaxDataRetransmissions")

If DefVal(6).Text = "Error" Then DefVal(6).Text = "NP"

DefVal(7).Text =

GetDWORDValue("HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",  
"EnableDeadGwDetect")

If DefVal(7).Text = "Error" Then DefVal(7).Text = "NP"

DefVal(8).Text =

GetDWORDValue("HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",  
"EnablePmtuDiscovery")

If DefVal(8).Text = "Error" Then DefVal(8).Text = "NP"

DefVal(9).Text =

GetDWORDValue("HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",  
"DisableIPSourceRouting")

If DefVal(9).Text = "Error" Then DefVal(9).Text = "NP"

DefVal(10).Text =

GetDWORDValue("HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",  
"NonameReleaseOnDemand")

If DefVal(10).Text = "Error" Then DefVal(10).Text = "NP"

DefVal(11).Text =

GetDWORDValue("HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",  
"PerformRouterDiscovery")

## Securiteam: [TOOL] Windows TCP/IP Stack Hardening Tool

```
If DefVal(11).Text = "Error" Then DefVal(11).Text = "NP"
```

```
DefVal(12).Text =
```

```
GetDWORDValue("HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",  
"KeepAliveTime ")
```

```
If DefVal(12).Text = "Error" Then DefVal(12).Text = "NP"
```

```
End Sub
```

```
Private Sub cmdHARDreg_Click()
```

```
SetDWORDValue
```

```
"HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\AFD\Parameters",  
"EnableICMPRedirect", DefVal(25).Text
```

```
DefVal(0).Text =
```

```
GetDWORDValue("HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",  
"EnableICMPRedirect")
```

```
If DefVal(0).Text = "Error" Then DefVal(0).Text = "NP"
```

```
SetDWORDValue
```

```
"HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\AFD\Parameters",  
"SynAttackProtect", DefVal(24).Text
```

```
DefVal(1).Text =
```

```
GetDWORDValue("HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",  
"SynAttackProtect")
```

```
If DefVal(1).Text = "Error" Then DefVal(1).Text = "NP"
```

```
SetDWORDValue
```

```
"HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\AFD\Parameters",  
"TCPMaxConnectResponseRetransmissions", DefVal(23).Text
```

```
DefVal(2).Text =
```

```
GetDWORDValue("HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",  
"TCPMaxConnectResponseRetransmissions")
```

```
If DefVal(2).Text = "Error" Then DefVal(2).Text = "NP"
```

```
SetDWORDValue
```

```
"HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\AFD\Parameters",  
"TcpMaxHalfOpen", DefVal(22).Text
```

```
DefVal(3).Text =
```

```
GetDWORDValue("HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",  
"TcpMaxHalfOpen")
```

```
If DefVal(3).Text = "Error" Then DefVal(3).Text = "NP"
```

```
SetDWORDValue
```

```
"HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\AFD\Parameters",  
"TCPMaxHalfOpenRetired", DefVal(21).Text
```

```
DefVal(4).Text =
```

```
GetDWORDValue("HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",  
"TCPMaxHalfOpenRetired")
```

```
If DefVal(4).Text = "Error" Then DefVal(4).Text = "NP"
```

## Securiteam: [TOOL] Windows TCP/IP Stack Hardening Tool

```
SetDWORDValue  
"HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\AFD\Parameters",  
"TCPMaxPortsExhausted", DefVal(20).Text  
DefVal(5).Text =  
GetDWORDValue("HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",  
"TCPMaxPortsExhausted")  
If DefVal(5).Text = "Error" Then DefVal(5).Text = "NP"
```

```
SetDWORDValue  
"HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\AFD\Parameters",  
"TCPMaxDataRetransmissions", DefVal(19).Text  
DefVal(6).Text =  
GetDWORDValue("HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",  
"TCPMaxDataRetransmissions")  
If DefVal(6).Text = "Error" Then DefVal(6).Text = "NP"
```

```
SetDWORDValue  
"HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\AFD\Parameters",  
"EnableDeadGwDetect", DefVal(18).Text  
DefVal(7).Text =  
GetDWORDValue("HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",  
"EnableDeadGwDetect")  
If DefVal(7).Text = "Error" Then DefVal(7).Text = "NP"
```

```
SetDWORDValue  
"HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\AFD\Parameters",  
"EnablePmtuDiscovery", DefVal(17).Text  
DefVal(8).Text =  
GetDWORDValue("HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",  
"EnablePmtuDiscovery")  
If DefVal(8).Text = "Error" Then DefVal(8).Text = "NP"
```

```
SetDWORDValue  
"HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\AFD\Parameters",  
"DisableIPSourceRouting", DefVal(16).Text  
DefVal(9).Text =  
GetDWORDValue("HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",  
"DisableIPSourceRouting")  
If DefVal(9).Text = "Error" Then DefVal(9).Text = "NP"
```

```
SetDWORDValue  
"HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\AFD\Parameters",  
"NonameReleaseOnDemand", DefVal(15).Text  
DefVal(10).Text =  
GetDWORDValue("HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",  
"NonameReleaseOnDemand")  
If DefVal(10).Text = "Error" Then DefVal(10).Text = "NP"
```

```
SetDWORDValue  
"HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\AFD\Parameters",  
"PerformRouterDiscovery", DefVal(14).Text
```

## Securiteam: [TOOL] Windows TCP/IP Stack Hardening Tool

```
DefVal(11).Text =
GetDWORDValue("HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",
"PerformRouterDiscovery")
If DefVal(11).Text = "Error" Then DefVal(11).Text = "NP"

SetDWORDValue
"HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\AFD\Parameters",
"KeepAliveTime", DefVal(13).Text
DefVal(12).Text =
GetDWORDValue("HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",
"KeepAliveTime ")
If DefVal(12).Text = "Error" Then DefVal(12).Text = "NP"
End Sub

Private Sub Command3_Click()
Check1(0).Value = 1
Check1(1).Value = 1
Check1(2).Value = 1
Check1(3).Value = 1
Check1(4).Value = 1
Check1(5).Value = 1
Check1(6).Value = 1
Check1(7).Value = 1
Check1(8).Value = 1
Check1(9).Value = 1
Check1(10).Value = 1
Check1(11).Value = 1
Check1(12).Value = 1

End Sub

Private Sub Autore_Click()
Frame3.Visible = True

End Sub

Private Sub Command1_Click(Index As Integer)
On Error GoTo GestoreErrori
Dim msg As String

msg = msg & "Are you Sure?"

If MsgBox(msg, vbQuestion + vbYesNo, "ATTENTION!") = vbYes Then

If Check1(0).Value = vbChecked Then

SetDWORDValue
"HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",
"EnableICMPRedirect", DefVal(25).Text
DefVal(0).Text =
GetDWORDValue("HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",
```

Securiteam: [TOOL] Windows TCP/IP Stack Hardening Tool

"EnableICMPRedirect")

If DefVal(0).Text = "Error" Then DefVal(0).Text = "NP"

End If

If Check1(1).Value = vbChecked Then

SetDWORDValue

"HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",

"SynAttackProtect", DefVal(24).Text

DefVal(1).Text =

GetDWORDValue("HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",

"SynAttackProtect")

If DefVal(1).Text = "Error" Then DefVal(1).Text = "NP"

End If

If Check1(2).Value = vbChecked Then

SetDWORDValue

"HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",

"TCPMaxConnectResponseRetransmissions", DefVal(23).Text

DefVal(2).Text =

GetDWORDValue("HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",

"TCPMaxConnectResponseRetransmissions")

If DefVal(2).Text = "Error" Then DefVal(2).Text = "NP"

End If

If Check1(3).Value = vbChecked Then

SetDWORDValue

"HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",

"TcpMaxHalfOpen", DefVal(22).Text

DefVal(3).Text =

GetDWORDValue("HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",

"TcpMaxHalfOpen")

If DefVal(3).Text = "Error" Then DefVal(3).Text = "NP"

End If

If Check1(4).Value = vbChecked Then

SetDWORDValue

"HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",

"TCPMaxHalfOpenRetired", DefVal(21).Text

DefVal(4).Text =

GetDWORDValue("HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",

"TCPMaxHalfOpenRetired")

If DefVal(4).Text = "Error" Then DefVal(4).Text = "NP"

End If

If Check1(5).Value = vbChecked Then

SetDWORDValue

## Securiteam: [TOOL] Windows TCP/IP Stack Hardening Tool

```
"HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",
"TCPMaxPortsExhausted", DefVal(20).Text
DefVal(5).Text =
GetDWORDValue("HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",
"TCPMaxPortsExhausted")
If DefVal(5).Text = "Error" Then DefVal(5).Text = "NP"

End If
If Check1(6).Value = vbChecked Then

SetDWORDValue
"HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\AFD\Parameters",
"TCPMaxDataRetransmissions", DefVal(19).Text
DefVal(6).Text =
GetDWORDValue("HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",
"TCPMaxDataRetransmissions")
If DefVal(6).Text = "Error" Then DefVal(6).Text = "NP"

End If
If Check1(7).Value = vbChecked Then

SetDWORDValue
"HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",
"EnableDeadGwDetect", DefVal(18).Text
DefVal(7).Text =
GetDWORDValue("HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",
"EnableDeadGwDetect")
If DefVal(7).Text = "Error" Then DefVal(7).Text = "NP"

End If
If Check1(8).Value = vbChecked Then

SetDWORDValue
"HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",
"EnablePmtuDiscovery", DefVal(17).Text
DefVal(8).Text =
GetDWORDValue("HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",
"EnablePmtuDiscovery")
If DefVal(8).Text = "Error" Then DefVal(8).Text = "NP"

End If
If Check1(9).Value = vbChecked Then
SetDWORDValue
"HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",
"DisableIPSourceRouting", DefVal(16).Text
DefVal(9).Text =
GetDWORDValue("HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",
"DisableIPSourceRouting")
If DefVal(9).Text = "Error" Then DefVal(9).Text = "NP"
```

## Securiteam: [TOOL] Windows TCP/IP Stack Hardening Tool

```
End If
If Check1(10).Value = vbChecked Then

SetDWORDValue
"HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",
"NonameReleaseOnDemand", DefVal(15).Text
DefVal(10).Text =
GetDWORDValue("HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",
"NonameReleaseOnDemand")
If DefVal(10).Text = "Error" Then DefVal(10).Text = "NP"

End If
If Check1(11).Value = vbChecked Then
SetDWORDValue
"HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",
"PerformRouterDiscovery", DefVal(14).Text
DefVal(11).Text =
GetDWORDValue("HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",
"PerformRouterDiscovery")
If DefVal(11).Text = "Error" Then DefVal(11).Text = "NP"

End If

If Check1(12).Value = vbChecked Then

SetDWORDValue
"HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",
"KeepAliveTime", DefVal(13).Text
DefVal(12).Text =
GetDWORDValue("HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",
"KeepAliveTime")
If DefVal(12).Text = "Error" Then DefVal(12).Text = "NP"

End If

GestoreErrori:

If Err.Number = 13 Then

MsgBox "Wrong Value!", vbCritical, "ERRORE"
End If
End If

End Sub

Private Sub Command2_Click()
Frame3.Visible = False

End Sub
```

Securiteam: [TOOL] Windows TCP/IP Stack Hardening Tool

```
Private Sub Command4_Click()
```

```
Check1(0).Value = 0  
Check1(1).Value = 0  
Check1(2).Value = 0  
Check1(3).Value = 0  
Check1(4).Value = 0  
Check1(5).Value = 0  
Check1(6).Value = 0  
Check1(7).Value = 0  
Check1(8).Value = 0  
Check1(9).Value = 0  
Check1(10).Value = 0  
Check1(11).Value = 0  
Check1(12).Value = 0
```

```
End Sub
```

```
Private Sub Command5_Click()
```

```
Check2(0).Value = 1  
Check2(1).Value = 1  
Check2(2).Value = 1  
Check2(3).Value = 1
```

```
End Sub
```

```
Private Sub Command6_Click()
```

```
Check2(0).Value = 0  
Check2(1).Value = 0  
Check2(2).Value = 0  
Check2(3).Value = 0
```

```
End Sub
```

```
Private Sub Form_Load()
```

```
DefVal(0).Text =
```

```
GetDWORDValue("HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",  
"EnableICMPRedirect")
```

```
If DefVal(0).Text = "Error" Then DefVal(0).Text = "NP"
```

```
DefVal(1).Text =
```

```
GetDWORDValue("HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",  
"SynAttackProtect")
```

```
If DefVal(1).Text = "Error" Then DefVal(1).Text = "NP"
```

```
DefVal(2).Text =
```

```
GetDWORDValue("HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",  
"TCPMaxConnectResponseRetransmissions")
```

```
If DefVal(2).Text = "Error" Then DefVal(2).Text = "NP"
```

## Securiteam: [TOOL] Windows TCP/IP Stack Hardening Tool

```
DefVal(3).Text =  
GetDWORDValue("HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",  
"TcpMaxHalfOpen")  
If DefVal(3).Text = "Error" Then DefVal(3).Text = "NP"
```

```
DefVal(4).Text =  
GetDWORDValue("HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",  
"TCPMaxHalfOpenRetired")  
If DefVal(4).Text = "Error" Then DefVal(4).Text = "NP"
```

```
DefVal(5).Text =  
GetDWORDValue("HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",  
"TCPMaxPortsExhausted")  
If DefVal(5).Text = "Error" Then DefVal(5).Text = "NP"
```

```
DefVal(6).Text =  
GetDWORDValue("HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",  
"TCPMaxDataRetransmissions")  
If DefVal(6).Text = "Error" Then DefVal(6).Text = "NP"
```

```
DefVal(7).Text =  
GetDWORDValue("HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",  
"EnableDeadGwDetect")  
If DefVal(7).Text = "Error" Then DefVal(7).Text = "NP"
```

```
DefVal(8).Text =  
GetDWORDValue("HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",  
"EnablePmtuDiscovery")  
If DefVal(8).Text = "Error" Then DefVal(8).Text = "NP"
```

```
DefVal(9).Text =  
GetDWORDValue("HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",  
"DisableIPSourceRouting")  
If DefVal(9).Text = "Error" Then DefVal(9).Text = "NP"
```

```
DefVal(10).Text =  
GetDWORDValue("HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",  
"NonameReleaseOnDemand")  
If DefVal(10).Text = "Error" Then DefVal(10).Text = "NP"
```

```
DefVal(11).Text =  
GetDWORDValue("HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",  
"PerformRouterDiscovery")  
If DefVal(11).Text = "Error" Then DefVal(11).Text = "NP"
```

```
DefVal(12).Text =  
GetDWORDValue("HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters",  
"KeepAliveTime")  
If DefVal(12).Text = "Error" Then DefVal(12).Text = "NP"
```

## Securiteam: [TOOL] Windows TCP/IP Stack Hardening Tool

```
DeflValW(0).Text =  
GetDWORDValue("HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\AFD\Parameters",  
"EnableDynamicBacklog")  
If DeflValW(0).Text = "Error" Then DeflValW(0).Text = "NP"
```

```
DeflValW(1).Text =  
GetDWORDValue("HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\AFD\Parameters",  
"MinimumDynamicBacklog")  
If DeflValW(1).Text = "Error" Then DeflValW(1).Text = "NP"
```

```
DeflValW(2).Text =  
GetDWORDValue("HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\AFD\Parameters",  
"MaximumDynamicBacklog")  
If DeflValW(2).Text = "Error" Then DeflValW(2).Text = "NP"
```

```
DeflValW(3).Text =  
GetDWORDValue("HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\AFD\Parameters",  
"DynamicBacklogGrowthDelta")  
If DeflValW(3).Text = "Error" Then DeflValW(3).Text = "NP"
```

End Sub

```
Private Sub Label1_Click()  
MsgBox "EnableICMPRedirect When ICMP redirects are disabled (by setting  
the value to 0), attackers cannot carry out attacks that require a host to  
redirect the ICMP-based attack to a third party.", , "Help"
```

End Sub

```
Private Sub Label10_Click()  
MsgBox "DisableIPSourceRouting Determines whether a computer allows  
clients to predetermine the route that packets take to their destination.  
When this value is set to 2, the computer will disable source routing for  
IP packets.", , "Help"  
End Sub
```

```
Private Sub Label11_Click()  
MsgBox "NoNameReleaseOnDemand Determines whether the computer will  
release its NetBIOS name if requested by another computer or a malicious  
packet attempting to hijack the computer's NetBIOS name.", , "Help"  
End Sub
```

```
Private Sub Label12_Click()  
MsgBox "PerformRouterDiscovery Determines whether the computer performs  
router discovery on this interface. Router discovery solicits router  
information from the network and adds the information retrieved to the  
route table. Setting this value to 0 will prevent the interface from  
performing router discovery.", , "Help"  
End Sub
```

## Securiteam: [TOOL] Windows TCP/IP Stack Hardening Tool

Private Sub Label13\_Click()

MsgBox "Keep Alive settings control how Windows manages connection keep alive transmissions. Including the timeout before keepalives are sent and the interval between keepalive transmissions.", , "Help"

End Sub

Private Sub Label14\_Click()

MsgBox "EnableDynamicBacklog Switches between using a static backlog and a dynamic backlog. By default, this parameter is set to 0, which enables the static backlog. You should enable the dynamic backlog for better security on Winsock.", , "Help"

End Sub

Private Sub Label15\_Click()

MsgBox "MinimumDynamicBacklog Controls the minimum number of free connections allowed on a listening Winsock endpoint. If the number of free connections drops below this value, a thread is queued to create additional free connections. Making this value too large (setting it to a number greater than 100) will degrade the performance of the computer.", , "Help"

End Sub

Private Sub Label16\_Click()

MsgBox "MaximumDynamicBacklog Controls the maximum number of half-open and free connections to Winsock endpoints. If this value is reached, no additional free connections will be made.", , "Help"

End Sub

Private Sub Label17\_Click()

MsgBox "DynamicBacklogGrowthDelta Controls the number of Winsock endpoints in each allocation pool requested by the computer. Setting this value too high can cause system resources to be unnecessarily occupied.", , "Help"

End Sub

Private Sub Label2\_Click()

MsgBox "SynAttackProtect Enables SYN flood protection in Windows 2000 and Windows XP. You can set this value to 0, 1, or 2. The default setting, 0, provides no protection. Setting the value to 1 will activate SYN/ACK protection contained in the TCPMaxPortsExhausted, TCPMaxHalfOpen, and TCPMaxHalfOpenRetried values. Setting the value to 2 will protect against SYN/ACK attacks by more aggressively timing out open and half-open connections.", , "Help"

End Sub

Private Sub Label3\_Click()

MsgBox "TCPMaxConnectResponseRetransmissions Determines how many times TCP retransmits an unanswered SYN/ACK message. TCP retransmits

## Securiteam: [TOOL] Windows TCP/IP Stack Hardening Tool

acknowledgments until the number of retransmissions specified by this value is reached.", , "Help"

End Sub

Private Sub Label4\_Click()

MsgBox "TcpMaxHalfOpen parameter controls the number of connections in the SYN-RCVD state allowed before SYN-ATTACK protection begins to operate.", , "Help"

End Sub

Private Sub Label5\_Click()

MsgBox "TCPMaxHalfOpenRetired Determines how many connections the server can maintain in the half-open state even after a connection request has been retransmitted. If the number of connections exceeds the value of this entry, TCP/IP initiates SYN flooding attack protection. This entry is used only when SYN flooding attack protection is enabled on this server that is, when the value of the SynAttackProtect entry is 1 and the value of the TCPMaxConnectResponseRetransmissions entry is at least 2.", , "Help"

End Sub

Private Sub Label6\_Click()

MsgBox "TCPMaxPortsExhausted Determines how many connection requests the system can refuse before TCP/IP initiates SYN flooding attack protection. The system must refuse all connection requests when its reserve of open connection ports runs out. This entry is used only when SYN flooding attack protection is enabled on this server that is, when the value of the SynAttackProtect entry is 1, and the value of the TCPMaxConnectResponseRetransmissions entry is at least 2.", , "Help"

End Sub

Private Sub Label7\_Click()

MsgBox "TCPMaxDataRetransmissions Determines how many times TCP retransmits an unacknowledged data segment on an existing connection. TCP retransmits data segments until they are acknowledged or until the number of retransmissions specified by this value is reached.", , "Help"

End Sub

Private Sub Label8\_Click()

MsgBox "EnableDeadGWDetect Determines whether the computer will attempt to detect dead gateways. When dead gateway detection is enabled (by setting this value to 1), TCP might ask IP to change to a backup gateway if a number of connections are experiencing difficulty. Backup gateways are defined in the TCP/IP configuration dialog box in Network Control Panel for each adapter. When you leave this setting enabled, it is possible for an attacker to redirect the server to a gateway of his choosing.", , "Help"

End Sub

Private Sub Label9\_Click()

MsgBox "EnablePMTUDiscovery Determines whether path MTU discovery is

## Securiteam: [TOOL] Windows TCP/IP Stack Hardening Tool

enabled (1), in which TCP attempts to discover the largest packet size over the path to a remote host. When path MTU discovery is disabled (0), the path MTU for all TCP connections will be fixed at 576 bytes.", ,

"Help"

End Sub

Private Sub Web\_Click()

Unload Me

End Sub

Private Sub winsok\_Click(Index As Integer)

On Error GoTo GestoreErrori

Dim msg As String

msg = msg & "Are you Sure?"

If MsgBox(msg, vbQuestion + vbYesNo, "ATTENTION!") = vbYes Then

If Check2(0).Value = vbChecked Then

SetDWORDValue

"HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\AFD\Parameters",

"EnableDynamicBacklog", DeflValW(7).Text

DeflValW(0).Text =

GetDWORDValue("HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\AFD\Parameters",

"EnableDynamicBacklog")

If DeflValW(0).Text = "Error" Then DeflValW(0).Text = "NP"

End If

If Check2(1).Value = vbChecked Then

SetDWORDValue

"HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\AFD\Parameters",

"MinimumDynamicBacklog", DeflValW(6).Text

DeflValW(1).Text =

GetDWORDValue("HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\AFD\Parameters",

"MinimumDynamicBacklog")

If DeflValW(1).Text = "Error" Then DeflValW(1).Text = "NP"

End If

If Check2(2).Value = vbChecked Then

SetDWORDValue

"HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\AFD\Parameters",

"MaximumDynamicBacklog", DeflValW(5).Text

DeflValW(2).Text =

GetDWORDValue("HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\AFD\Parameters",

"MaximumDynamicBacklog")

If DeflValW(2).Text = "Error" Then DeflValW(2).Text = "NP"

Securiteam: [TOOL] Windows TCP/IP Stack Hardening Tool

End If

If Check2(3).Value = vbChecked Then

SetDWORDValue

"HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\AFD\Parameters",

"DynamicBacklogGrowthDelta", DeflValW(4).Text

DeflValW(3).Text =

GetDWORDValue("HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\AFD\Parameters",

"DynamicBacklogGrowthDelta")

If DeflValW(3).Text = "Error" Then DeflValW(3).Text = "NP"

End If

GestoreErrori:

If Err.Number = 13 Then

MsgBox "Wrong Value!", vbCritical, "ERRORE"

End If

End If

End Sub

' EoF

ADDITIONAL INFORMATION

The information has been provided by <mailto:admin@securitywireless.info>

D'Amato Luigi.

To keep updated with the tool visit the project's homepage at:

<<http://www.securitywireless.info/>> <http://www.securitywireless.info/>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.