

SKPortScan

ActiveX Control

Port Scanner ActiveX Control for Microsoft® Windows™

Copyright ©2001-2002 by Magneto Software, Inc.

All rights reserved

1 SkPortScan Overview	3
1.1 Introduction	3
1.2 Usage	3
1.3 Property Summary	4
1.4 Event Summary	4
1.5 Method Summary	4
1.6 Error codes	5
2 Properties	6
2.1 optConnectTimeout	6
2.2 optPortMin	7
2.3 optPortMax	8
2.4 optPromptUser	9
2.5 optScanMaxTcpOpenSockets	10
2.6 optScanMaxUdpLoad	11
2.7 optScanMaxUdpRetry	12
2.8 optScanMaxUdpTimeout	13
2.9 optScanMode	14
2.10 optScanProtocols	15
2.11 optScanTimeout	16
2.12 optStatusUpdateInterval	17
3 Events	18
3.1 PortScanCompleted	18
3.2 PortScanFoundPort	19
3.3 PortScanQueryCompleted	20
3.4 PortScanStatusUpdate	21
4 Methods	22
4.1 AboutBox	22
4.2 GetPortsTableEntryInfo	23
4.3 GetPortsTableSize	24
4.4 GetServByPort	25
4.5 PortScanRemoteHost	26
4.6 PortScanReset	27
4.7 ResetPortScanSettings	28

1 SkPortScan Overview

1.1 Introduction

SkPortScan ActiveX Control is a lightweight and powerful port scanner control. It allows developers to integrate port-scanning capabilities into their applications.

SkPortScan can be used for network exploration or security auditing. SkPortScan can determine what services (ports) are open (offered) by remote hosts.

It is capable of scanning multiple hosts simultaneously.

SkPortScan can scan TCP only, UDP only, or TCP and UDP ports simultaneously.

It can operate in 3 different scan modes:

- Scan range of ports.

- Scan authorized ports only port numbers are divided into three ranges: the Well Known Ports, the Registered Ports, and the Dynamic and/or Private Ports. Well Known Ports are those from 0 through 1023, Registered Ports are those from 1024 through 49151, and the Dynamic and/or Private Ports are those from 49152 through 65535. The Well Known Ports are assigned by the IANA (Internet Assigned Numbers Authority) and on most systems can only be used by system (root level) processes or by programs executed by privileged users).

- Scan hostile ports only (ports, that are mostly used for backdoors or trojan programs.

Hackers/crackers that break into systems often start processes running on one of the following ports and then use them to either regain entry or launch attacks against other sites.

SkPortScan ActiveX Control has one of the most complete ports databases available today built in, and, provides comprehensive APIs for accessing it.

It can be used from any 32-bit Windows development environment, including Visual Basic, Visual C++, and Delphi.

SkPortScan ActiveX Control comes with all documentation, sample code, and working demo program.

Additional information about protocol numbers can be found at this location:

[RFC 1700 - ASSIGNED NUMBERS](#)

1.2 Usage

SkPortScan ActiveX Control can perform multiple TCP, or UDP, or TCP and UDP ports scans simultaneously while providing information from the ports usage database.

1.3 Property Summary

[optConnectTimeout](#)

Specify timeout value in milliseconds to wait for replies.

[optPortMin](#)

Specify starting port number value for the range scan mode.

[optPortMax](#)

Specify ending port number value for the range scan mode.

[optPromptUser](#)

Specify whether to prompt before performing a scanning on remote host.

[optScanMaxTcpOpenSockets](#)

Limits number of simultaneously open TCP sockets.

[optScanMaxUdpLoad](#)

Limits number of UDP packets sent per second.

[optScanMaxUdpRetry](#)

Limits number of UDP retransmissions on the detected open UDP ports.

[optScanMaxUdpTimeout](#)

Specify timeout value in milliseconds to wait for ICMP replies (during UDP ports scanning).

[optScanMode](#)

Specify scan mode (“Authorized ports”, or “Hostile ports”, or “Range of ports”).

[optScanProtocols](#)

Specify scan mode (TCP, or UDP, or TCP and UDP).

[optScanTimeout](#)

Specify timeout value in milliseconds to limit a port scanning process.

[optStatusUpdateInterval](#)

Specify timeout value in milliseconds between status update notifications.

1.4 Event Summary

[PortScanCompleted](#)

Indicate that SkPortScan ActiveX Control has stopped processing port scan requests.

[PortScanFoundPort](#)

Indicate that SkPortScan ActiveX Control found open (offered) port on the remote host.

[PortScanQueryCompleted](#)

Indicate that SkPortScan ActiveX Control has stopped processing a single scan request.

[PortScanStatusUpdate](#)

Status update notification.

1.5 Method Summary

[AboutBox](#)

Display a dialog box with SkPortScan ActiveX Control license and version information.

[GetPortsTableEntryInfo](#)

Get a ports table entry

[GetPortsTableSize](#)

Get a ports table size

[GetServByPort](#)

Retrieve service information corresponding to a port and protocol

[PortScanRemoteHost](#)

Start scanning.

[PortScanReset](#)

Stop scanning.

[ResetPortScanSettings](#)

Reset all SkPortScan settings back to default values.

1.6 Error codes

The following provides a complete listing of error codes returned by SkPortScan ActiveX Control.

ERROR_SUCCESS (0)	No errors.
ERROR_CANCELLED (1223)	User canceled the operation.
ERROR_TIMEOUT (1460)	This operation returned because the timeout period expired.
WSAEFAULT (10014)	The <i>name</i> or the <i>namelen</i> parameter is not a valid part of the user address space, the <i>namelen</i> parameter is too small, or the <i>name</i> parameter contains incorrect address format for the associated address family.
WSAEINVAL (10022)	An invalid argument was supplied.
WSAEPFNOSUPPORT (10046)	The protocol family has not been configured into the system or no implementation for it exists.
WSAEADDRNOTAVAIL (10049)	The remote address is not a valid address (such as ADDR_ANY).
WSAENETDOWN (10050)	The network subsystem has failed.
WSAENETUNREACH (10051)	The network cannot be reached from this host at this time.
WSAENOBUFS (10055)	No buffer space is available. The socket cannot be connected.
WSAENOTCONN (10057)	The socket is not connected.
WSAETIMEDOUT (10060)	Attempt to connect timed out without establishing a connection.
WSAECONNREFUSED (10061)	The attempt to connect was forcefully rejected.

2 Properties

2.1 *optConnectTimeout*

Summary

Specify timeout value in milliseconds to wait for replies.

Description

This property specifies the timeout value in milliseconds that is used to wait for a reply when a request packet is sent. By default this value is set to 3000 milliseconds (3 seconds).

This property is of type long.

VB Example

```
Dim IConTimeout As Long  
IConTimeout = 3000  
SKPORTSCAN.optConnectTimeout = IConTimeout
```

2.2 optPortMin

Summary

Specify starting port number value for the “Range of Ports” scan mode.

Description

This property specifies the starting port value the “Range of Ports” scan mode

The default value is 1.

The maximum possible value is 65535 (0xffff).

This property is of type long.

VB Example

```
Dim lPortMin As Long
```

```
lPortMin = 1
```

```
SKPORTSCAN.optPortMin = lPortMin
```

2.3 optPortMax

Summary

Specify ending port number value for the “Range of Ports” scan mode.

Description

This property specifies the ending port value the “Range of Ports” scan mode

The default value is 5000.

The maximum possible value is 65535 (0xffff).

This property is of type long.

VB Example

```
Dim lPortMax As Long
```

```
lPortMax = 5000
```

```
SKPORTSCAN.optPortMax = lPortMax
```

2.4 optPromptUser

Summary

Specify whether to prompt before performing a scanning on remote host.

Description

This property specifies if user needs to be prompted every time before performing a port scan on remote host.

The default value is 1 (True).

This property is of type integer.

VB Example

```
Dim nPrompt As Integer  
nPrompt = 1  
SKPORTSCAN.optPromptUser = nPrompt
```

2.5 optScanMaxTcpOpenSockets

Summary

Limits number of simultaneously open TCP sockets.

Description

This property specifies the maximum number of simultaneously open TCP sockets.

The default value is 64.

This property is of type short.

VB Example

```
Dim nMaxTcpSockets As Integer
```

```
nMaxTcpSockets = 64
```

```
SKPORTSCAN.optScanMaxTcpOpenSockets = nMaxTcpSockets
```

2.6 optScanMaxUdpLoad

Summary

Limits number of UDP packets sent per second.

Description

This property specifies the maximum number of UDP packets sent per second

The default value is 64.

This property is of type short.

VB Example

```
Dim nMaxUdpLoad As Integer
```

```
nMaxUdpLoad = 64
```

```
SKPORTSCAN. optScanMaxUdpLoad = nMaxUdpLoad
```

2.7 optScanMaxUdpRetry

Summary

Limits number of UDP retransmissions on the detected open UDP ports.

Description

This property specifies the maximum number of retransmissions used in UDP scan

The default value is 2.

This property is of type long.

VB Example

```
Dim nMaxUdpRetry As Integer
```

```
nMaxUdpRetry = 2
```

```
SKPORTSCAN. optScanMaxUdpRetry = nMaxUdpRetry
```

2.8 optScanMaxUdpTimeout

Summary

Specify timeout value in milliseconds to wait for ICMP replies (during UDP ports scanning).

Description

This property specifies the timeout value in milliseconds that is used to wait for ICMP reply (destination unreachable) when a request packet is sent.

By default this value is set to 3000 milliseconds (3 seconds).

This property is of type long.

VB Example

```
Dim lScanMaxUdpTimeout As Long
```

```
lScanMaxUdpTimeout = 4000
```

```
SKPORTSCAN. optScanMaxUdpTimeout = lScanMaxUdpTimeout
```

2.9 optScanMode

Summary

Specify scan mode (“Authorized ports”, or “Hostile ports”, or “Range of ports”).

Description

This property specifies the scan mode.

SkPortScan ActiveX Control can operate in 3 different scan modes:

- Scan range of ports.

- Scan authorized ports only port numbers are divided into three ranges: the Well Known Ports, the Registered Ports, and the Dynamic and/or Private Ports. Well Known Ports are those from 0 through 1023, Registered Ports are those from 1024 through 49151, and the Dynamic and/or Private Ports are those from 49152 through 65535. The Well Known Ports are assigned by the IANA (Internet Assigned Numbers Authority) and on most systems can only be used by system (root level) processes or by programs executed by privileged users).

- Scan hostile ports only (ports, that are mostly used for backdoors or trojan programs.

Hackers/crackers that break into systems often start processes running on one of the following ports and then use them to either regain entry or launch attacks against other sites.

Scan Modes Values:

0 – Range of Ports

1 – Authorized Ports

2 – Hostile Ports

This property is of type short.

The default value is 2 (Scan hostile ports)

VB Example

```
Dim nScanMode As Integer
```

```
nScanMode = 1 'Scan authorized ports
```

```
SKPORTSCAN.optScanMode = nScanMode
```

2.10 optScanProtocols

Summary

Specify scan mode (TCP, or UDP, or TCP and UDP).

Description

This property specifies the protocols to scan.

Scan Protocols Values:

1 – TCP

2 – UDP

3 – TCP and UDP

This property is of type short.

The default value is 2 (Scan TCP and UDP ports)

VB Example

```
Dim nScanProtocols As Integer
```

```
nScanProtocols = 3 ' Scan TCP and UDP ports
```

```
SKPORTSCAN.optScanProtocols = nScanProtocols
```

2.11 optScanTimeout

Summary

Specify timeout value in milliseconds to limit a port scanning process.

Description

This property specifies the timeout value in milliseconds that is used to limit a port scanning process.

By default this value is set to 300000 milliseconds (300 sec, or 5 min).

This property is of type long.

VB Example

```
Dim lScanTimeout As Long
```

```
lScanTimeout = 300000
```

```
SKPORTSCAN.optScanTimeout = lScanTimeout
```

2.12 optStatusUpdateInterval

Summary

Specify timeout value in milliseconds between status update notifications.

Description

This property specifies the timeout value in milliseconds between status update notifications.

By default this value is set to 3000 milliseconds (3 seconds).

To disable update notifications completely, the value needs to be set to 0.

This property is of type long.

VB Example

```
Dim lStatusUpdateInterval As Long
```

```
lStatusUpdateInterval = 3000
```

```
SKPORTSCAN.optStatusUpdateInterval = lStatusUpdateInterval
```

3 Events

3.1 PortScanCompleted

Summary

Indicate that SkPortScan ActiveX Control has stopped processing port scan requests.

Syntax

PortScanCompleted(void);

Description

Indicate that SKPORTSCAN.OCX has stopped processing WHOIS requests.

Parameters

None.

3.2 PortScanFoundPort

Summary

Indicate that SkPortScan ActiveX Control found open (offered) port on the remote host.

Syntax

```
PortScanFoundPort(BSTR bstrRemoteHostName, short nProtocol, long IPortNumber, BSTR  
                  bstrPortKeyWord, short nUsage, BSTR bstrAuthorizedUsageDescription, BSTR  
                  bstrHostileUsageDescription);
```

Description

Indicate that SkPortScan ActiveX Control found open (offered) port on the remote host.

Parameters

bstrRemoteHostName is the name of the remote host that is queried,

nProtocol is open port's protocol (Possible values: 1 – TCP, 2 – UDP).

IPortNumber is port for a service, in host byte order.

bstrPortKeyWord is service keyword (See [RFC 1700 - ASSIGNED NUMBERS](#) for more details)

nUsage indicates usage of the open port (Possible values: 0 – Authorized, or Legitimate usage, no information about trojans is available; 1 – Dual usage, there are common trojans that might use this port number; 2 – Hostile usage, there is no information in SkPortScan ports database regarding legitimate use of this port.

bstrAuthorizedUsageDescription is authorized usage description (from SkPortScan ports usage database)

bstrHostileUsageDescription is hostile usage description (from SkPortScan ports usage database). In case of multiple programs known to use the same port number, multiple values will be separated by semicolon.

3.3 PortScanQueryCompleted

Summary

Indicate that SkPortScan ActiveX Control has stopped processing a single scan request.

Syntax

```
PortScanQueryCompleted(BSTR bstrRemoteHostName, short nProtocols, long lStatus, long lTcpPortMin,  
                        long lTcpPortMax, long lTcpPortCount, long lUdpPortMin, long lUdpPortMax,  
                        long lUdpPortCount, long lElapsedTime);
```

Description

Indicate that SkPortScan ActiveX Control has stopped processing a single scan request.

Parameters

bstrRemoteHostName is the name of the remote host that was queried,

nProtocols is protocols used (See section [2.10 optScanProtocols](#) for the complete list of possible values.

lStatus is the return status of each individual reply. See section [1.6 Error Codes](#) for the complete list of supported error codes,

lTcpPortMin is starting scanned TCP port.

lTcpPortMax is ending scanned TCP port.

lTcpPortCount is total number of scanned TCP ports.

lUdpPortMin is starting scanned UDP port.

lUdpPortMax is ending scanned UDP port.

lUdpPortCount is total number of scanned UDP ports.

lElapsedTime is elapsed time in milliseconds

3.4 PortScanStatusUpdate

Summary

Status update notification.

Syntax

```
PortScanStatusUpdate(BSTR strRemoteHostName, short nProtocols, long dwElapsedTime, long  
                    lCountTcpPortsScanned, long lCountTcpPortsTotal, long  
                    lCountUdpPortsScanned, long lCountUdpPortsTotal);
```

Description

Status update notification while performing port scans. The interval between notifications is defined by property [optStatusUpdateInterval](#). To disable notification completely, set optStatusUpdateInterval to 0.

Parameters

bstrRemoteHostName is the name of the remote host that is queried,

nProtocols is protocols used (See section [2.10 optScanProtocols](#) for the complete list of possible values.

lElapsedTime is elapsed time in milliseconds

lCountTcpPortsScanned is total scanned TCP ports.

lCountTcpPortsTotal is total TCP ports to scanned in this scan query.

lCountUdpPortsScanned is total scanned UDP ports.

lCountUdpPortsTotal is total UDP ports to scanned in this scan query.

4 Methods

4.1 AboutBox

Summary

Display a dialog box with SkPortScan ActiveX Control license and version information.

Syntax

```
void AboutBox();
```

Description

This method could be used to display version license information or to register SKPORTSCAN.OCX control.

Parameters

None.

4.2 *GetPortsTableEntryInfo*

Summary

Get a ports table entry

Syntax

```
long GetPortsTableEntryInfo(short nProtocol, short nTableType, long lEntryIndex, long*  
    plMinPortNumber, long* plMaxPortNumber, BSTR* pbstrPortKeyWord, short*  
    pnUsage, BSTR* pbstrAuthorizedUsageDescription, BSTR*  
    pbstrHostileUsageDescription);
```

Description

The *GetPortsTableEntryInfo* method retrieves an entry from the ports database.

It returns a long, which is set to 0 (ERROR_SUCCESS) if the method is successfully executed, otherwise it will be set to the error code from section [1.6 Error Codes](#).

Parameters

nProtocol is the protocol to use (Possible values: 1 – TCP; 2 – UDP).

nTableType is the table type (Possible values: 0 – Authorized ports table; 1 - Hostile Ports table).

lEntryIndex is an ordinal entry index in the table (starting from 0). Table size can be retrieved by calling method [GetPortsTableSize\(\)](#).

If method returns successfully, the following parameters will be filled:

plMinPortNumber will contain a minimum port number value

plMaxPortNumber will contain a maximum port number value.

If plMaxPortNumber is not equal to plMinPortNumber, it means that retrieved information is for the range, rather than for the single port. Vast majority of the entries in the SkPortScan database define a single port, not a range of ports.

pbstrPortKeyWord will contain a port key word, if available.

pnUsage will contain a port usage (Authorized, Dual or Hostile). See section [3.2 PortScanFoundPort](#) for more details.

pbstrAuthorizedUsageDescription will contain an authorized usage description, if available.

pbstrHostileUsageDescription will contain a hostile usage description, if available.

4.3 GetPortsTableSize

Summary

Get a ports table size

Syntax

```
long GetPortsTableSize(short nProtocol, short nTableType);
```

Description

The GetPortsTableSize method retrieves an table size from the ports database.

If successful, it returns a non-zero value.

Parameters

nProtocol is protocol to use (Possible values: 1 – TCP; 2 – UDP).

nTableType is the table type (Possible values: 0 – Authorized ports table; 1 - Hostile Ports table).

4.4 GetServByPort

Summary

Retrieve service information corresponding to a port and protocol

Syntax

```
long GetServByPort(long lPortNumber, short nProtocol, BSTR* pbstrPortKeyWord, short* pnUsage,  
                  BSTR* pbstrAuthorizedUsageDescription, BSTR* pbstrHostileUsageDescription);
```

Description

Retrieve service information corresponding to a port and protocol

It returns a long, which is set to 0 (ERROR_SUCCESS) if the method is successfully executed, otherwise it will be set to the error code 1168 (ERROR_NOT_FOUND).

Parameters

lPortNumber is the protocol number.

nProtocol is the protocol to use (Possible values: 1 – TCP; 2 – UDP).

If method returns successfully, the following parameters will be filled:

pbstrPortKeyWord will contain a port key word, if available.

pnUsage will contain a port usage (Authorized, Dual or Hostile). See section [3.2 PortScanFoundPort](#) for more details.

pbstrAuthorizedUsageDescription will contain an authorized usage description, if available.

pbstrHostileUsageDescription will contain a hostile usage description, if available.

4.5 PortScanRemoteHost

Summary

Start scanning.

Syntax

```
long PortScanRemoteHost(BSTR bstrRemoteHostName);
```

Description

Start scanning.

Parameters

bstrRemoteHostName is the name of the remote host that will be scanned,

4.6 PortScanReset

Summary

Stop scanning.

Syntax

void PortScanIsReset (void)

Description

The PortScanReset method terminates any pending scan requests.

Parameters

None.

4.7 ResetPortScanSettings

Summary

Reset all SkPortScan settings back to default values.

Syntax

```
void ResetPortScanSettings(void)
```

Description

Reset all SkPortScan settings back to default values.

Parameters

None.