

IsaServer.it – FTP Brute Force

Autore :

Giulio Martino
IT Security, Network and Voice Manager



Technical Writer e Supporter di ISAserver.it

www.isaserver.it
giulio.martino@isaserver.it

Creatore e Fondatore di VoipExperts.it

www.voipexperts.it
<mailto:giulio.martino@voipexperts.it>

[Appendice A]

Alcuni dettagli sul programma KillTcpConn.exe

Il programma si appoggia alle API per enumerare e “killare” una sessione. Le API interessate sono due :

GetTcpTable

SetTcpEntry

E fanno parte della libreria iphlapi.dll e si appoggiano alla struttura MIB_TCPROW.

Definizioni per VB6 :

```
Public Type MIB_TCPROW
```

```
dwState As Long
```

```
dwLocalAddr As Long
```

```
dwLocalPort As Long
```

```
dwRemoteAddr As Long
```

```
dwRemotePort As Long
```

```
End Type
```

```
Public Declare Function SetTcpEntry Lib "iphlpapi.dll" (pTcpTableEx As MIB_TCPROW) As Long
```

```
Public Declare Function GetTcpTable Lib "iphlpapi.dll" (ByRef pTcpTable As Any, ByRef pdwSize As Long, ByVal bOrder As Long) As Long
```

Definizioni per .NET

```
Public Class MIB_TCPROW
```

```
Public dwState As Integer
```

```
Public dwLocalAddr As Integer
```

```
Public dwLocalPort As Integer
```

```
Public dwRemoteAddr As Integer
```

```
Public dwRemotePort As Integer
```

```
End Class
```

```
Public Declare Function SetTcpEntry Lib "iphlpapi.dll" (ByVal pTcpTableEx As MIB_TCPROW) As Long
```

```
Public Declare Function GetTcpTable Lib "iphlpapi" (ByVal pTcpTable As IntPtr, ByRef pdwSize As Integer, ByVal bOrder As Boolean) As Integer
```

Definizione Costanti per la struttura TCPROW (dwstate) valide sia per VB6 che .NET

IsaServer.it – FTP Brute Force

```
Public Const MIB_TCP_STATE_CLOSED = 1
Public Const MIB_TCP_STATE_LISTEN = 2
Public Const MIB_TCP_STATE_SYN_SENT = 3
Public Const MIB_TCP_STATE_SYN_RCVD = 4
Public Const MIB_TCP_STATE_ESTAB = 5
Public Const MIB_TCP_STATE_FIN_WAIT1 = 6
Public Const MIB_TCP_STATE_FIN_WAIT2 = 7
Public Const MIB_TCP_STATE_CLOSE_WAIT = 8
Public Const MIB_TCP_STATE_CLOSING = 9
Public Const MIB_TCP_STATE_LAST_ACK = 10
Public Const MIB_TCP_STATE_TIME_WAIT = 11
Public Const MIB_TCP_STATE_DELETE_TCB = 12
```

Riferimenti

Mib_TcpRow

[http://msdn2.microsoft.com/en-us/library/aa366909\(VS.85\).aspx](http://msdn2.microsoft.com/en-us/library/aa366909(VS.85).aspx)

GetTcpTable

[http://msdn2.microsoft.com/en-us/library/aa366026\(VS.85\).aspx](http://msdn2.microsoft.com/en-us/library/aa366026(VS.85).aspx)

SetTcpEntry

[http://msdn2.microsoft.com/en-us/library/aa366378\(VS.85\).aspx](http://msdn2.microsoft.com/en-us/library/aa366378(VS.85).aspx)

[Appendice B]

FTP Status Code

1xx – Risposta preliminare positiva

110 Risposta dell'indicatore di riavvio
120 Servizio pronto tra nnn minuti
125 Connessione dati già aperta. Inizio del trasferimento in corso
150 Stato del file corretto. Apertura della connessione dati in corso

2xx – Risposta di completamento positiva

200 Comando corretto
202 Comando non implementato. Superfluo in questo sito
211 Stato del sistema o risposta della Guida di sistema
212 Stato della directory
213 Stato del file
214 Messaggio della Guida in linea
215 Tipo di sistema NAME
220 Servizio pronto per un nuovo utente
221 Chiusura della connessione di controllo da parte del servizio
225 Connessione dati aperta. Nessun trasferimento in corso
226 Chiusura della connessione dati. Azione di file richiesta riuscita
227 Inizio modalità passiva
230 Utente connesso. Continuare
250 Azione di file richiesta corretta. Completata
257 Creato "PATHNAME"

3xx – Risposta intermedia positiva

331 Nome utente corretto. Richiesta password

IsaServer.it – FTP Brute Force

332 Richiesto account per l'accesso
350 Azione di file richiesta in attesa di ulteriori informazioni
4xx – Risposta di completamento negativa temporanea
421 Servizio non disponibile. Chiusura della connessione di controllo
425 Impossibile aprire la connessione dati
426 Connessione chiusa. Trasferimento interrotto
450 Azione di file richiesta non eseguita. Il file non è disponibile
451 Azione richiesta interrotta. Errore locale durante l'elaborazione
452 Azione richiesta non eseguita. Spazio di archiviazione insufficiente nel sistema
5xx – Risposta di completamento negativa permanente
500 Errore di sintassi. Comando sconosciuto
501 Errore di sintassi in parametri o argomenti
502 Comando non implementato
503 Sequenza di comandi errata
504 Comando non implementato per il parametro specificato
530 Non connesso
532 Richiesto account per l'archiviazione dei file
550 Azione richiesta non eseguita. Il file non è disponibile
551 Azione richiesta interrotta: Tipo di pagina sconosciuto
552 Azione di file richiesta interrotta
553 Azione richiesta non eseguita. Nome file non consentito

Win32Status (Estratto del file WinError.h)

```
//  
// MessageId: ERROR_LOGON_FAILURE  
//  
// MessageText:  
//  
// Logon failure: unknown user name or bad password.  
//  
#define ERROR_LOGON_FAILURE          1326L
```

Abbiamo riportato un estratto dei valori assegnati ai campi StatusCodes e Win32Status utili per poter effettuare verticalizzazioni e/o implementazioni future.

Riferimenti

Codici di stato IIS

<http://support.microsoft.com/?id=318380>

I codici di stato del campo Win32Status sono riportati dal SDK di windows nel file WinError.h

<http://msdn2.microsoft.com/en-us/library/ms819773.aspx>

IsaServer.it – FTP Brute Force

Risorse

[IIS/FTP]

<http://technet2.microsoft.com/windowsserver/en/library/46e15c9a-fd7c-4c1e-aaa6-0767ccd6fdd11033.msp?mfr=true>

<http://www.isaserver.it/articoli/20061128-GM04.htm>

[SQL Server]

[http://msdn2.microsoft.com/it-it/express/bb410792\(en-us\).aspx](http://msdn2.microsoft.com/it-it/express/bb410792(en-us).aspx)

<http://msdn2.microsoft.com/it-it/library/ms165636.aspx>

<http://msdn2.microsoft.com/en-us/library/ms189799.aspx>

[ISA Server]

www.isaserver.it/articoli

www.isaserver.it/forum

www.isaserver.it/download

www.isaserver.it/blog

<http://www.isascripts.org/>

[Discussioni]

E' stata aperta su www.isaserver.it una sezione sul forum chiamata "Caffè con gli Autori", dove è possibile discutere sugli articoli pubblicati. Per qualsiasi dubbio, domanda e/o errori, potete usare questo link :

http://www.isaserver.it/forum/forum.asp?FORUM_ID=22