Report di Sicurezza: Rimozione del Malware WannaCry

Introduzione

Ho scoperto che il computer dell'azienda che seguo come consulente di sicurezza, con sistema operativo Windows 7, è stato infettato dal malware WannaCry. Di seguito sono riportati i passaggi eseguiti per mettere in sicurezza il sistema.

Intervento Tempestivo sul Sistema Infetto

Isolamento della Macchina Infetta

1. **Disconnessione dalla Rete:**
    - Ho aperto VirtualBox.
    - Ho selezionato la macchina virtuale infetta (Windows 7).
    - Sono andato su "Impostazioni" > "Rete".
    - Ho deselezionato "Abilitato" per la Scheda di rete 1.
2. **Spegnimento della Macchina Virtuale:**
    - Nella finestra di VirtualBox, ho fatto clic con il tasto destro sulla macchina virtuale.
    - Ho selezionato "Chiudi" > "Spegnimento forzato".
3. **Creazione di una Copia di Backup del Disco Virtuale:**
    - Ho trovato il file VDI sul sistema host.
    - Ho copiato e incollato il file in una posizione sicura.

Messa in Sicurezza del Sistema

Aggiornamento del Sistema Operativo

1. **Controllo e Installazione degli Aggiornamenti:**
    - Ho avviato la macchina virtuale in modalità provvisoria con rete.
    - Ho aperto "Control Panel".
    - Sono andato su "System and Security" > "Windows Update".
    - Ho cliccato su "Check for updates" e poi su "Install Updates".

Disabilitazione del Protocollo SMBv1

1. **Disabilitazione tramite Registro di Sistema:**
    - Ho aperto l'Editor del Registro di Sistema (**regedit**).
    - Sono andato a **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters**.
    - Ho creato un nuovo valore DWORD (32-bit) chiamato **SMB1**.

- Ho impostato il valore su **0**.
- Ho riavviato il sistema.

Scansione del Sistema con Software Anti-Malware

1. **Utilizzo di Avast Free Antivirus:**
    - Ho scaricato e installato Avast Free Antivirus.
    - Ho avviato una scansione completa del sistema.
    - Ho rimosso tutte le minacce rilevate seguendo le istruzioni di Avast.

Modifica delle Password degli Account

1. **Modifica delle Password:**
    - Ho aperto "Control Panel".
    - Sono andato su "User Accounts" > "Manage another account".
    - Ho selezionato gli account utente e ho cambiato le password, impostando password complesse e diverse per ogni account.

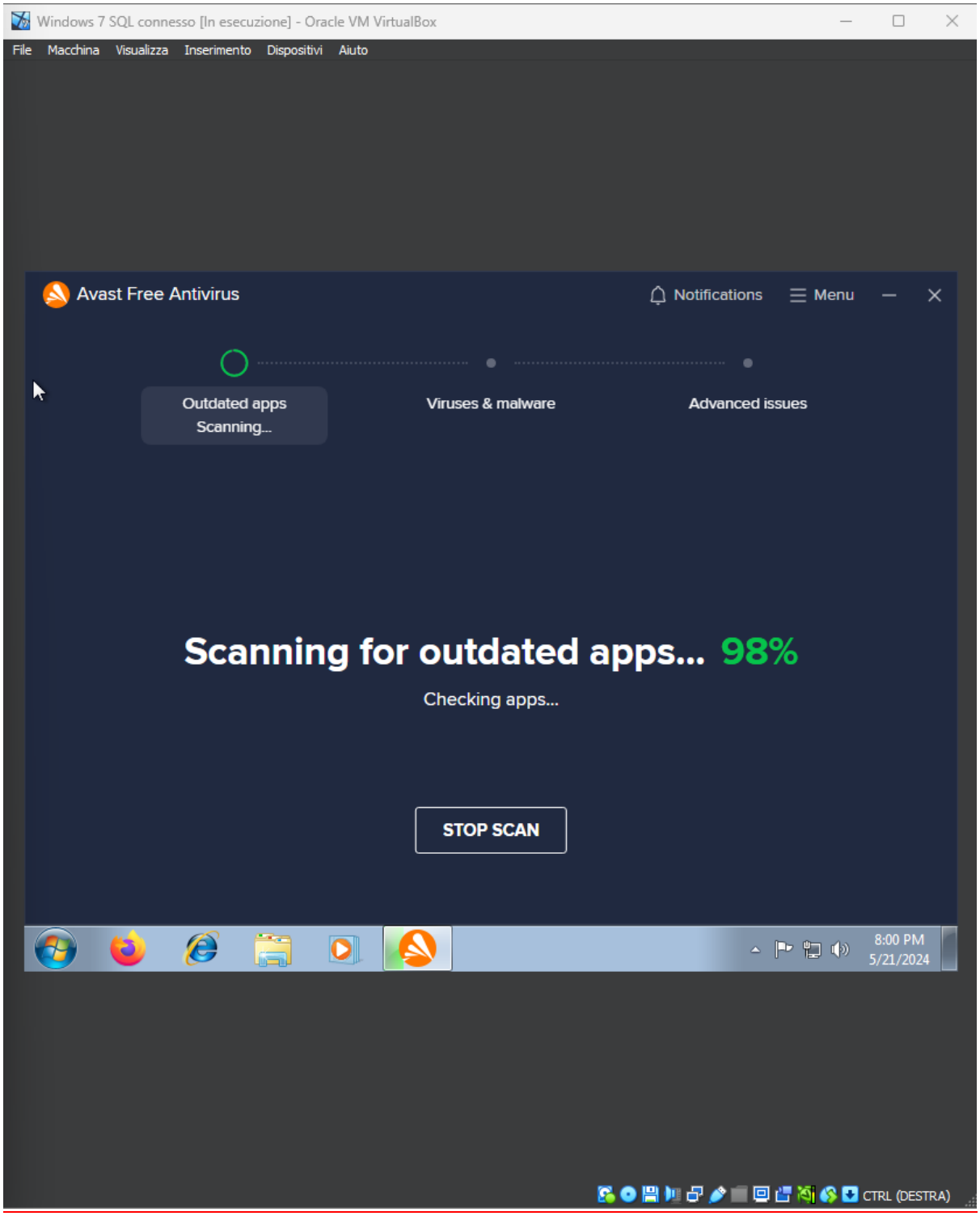
Considerazione dell'Aggiornamento del Sistema Operativo

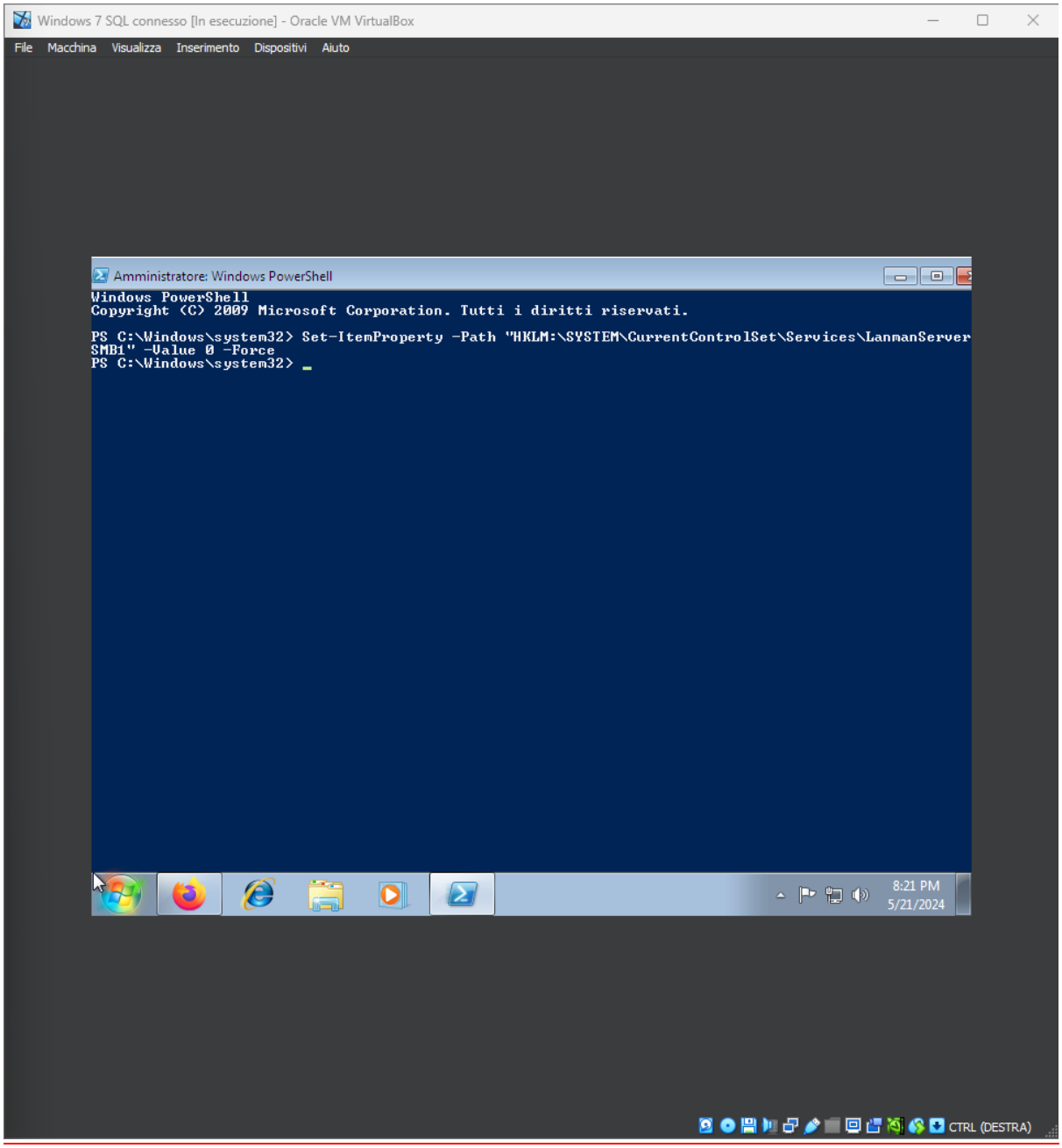
1. **Verifica dei Requisiti di Sistema:**
    - Ho verificato che l'hardware virtuale soddisfacesse i requisiti di sistema per Windows 10.
2. **Backup dei Dati:**
    - Ho eseguito un backup dei dati importanti.
3. **Download e Esecuzione del Media Creation Tool:**
    - Ho scaricato il "Media Creation Tool" dal sito ufficiale di Microsoft.
    - Ho eseguito il tool e seguito le istruzioni per aggiornare il sistema operativo a Windows 10.

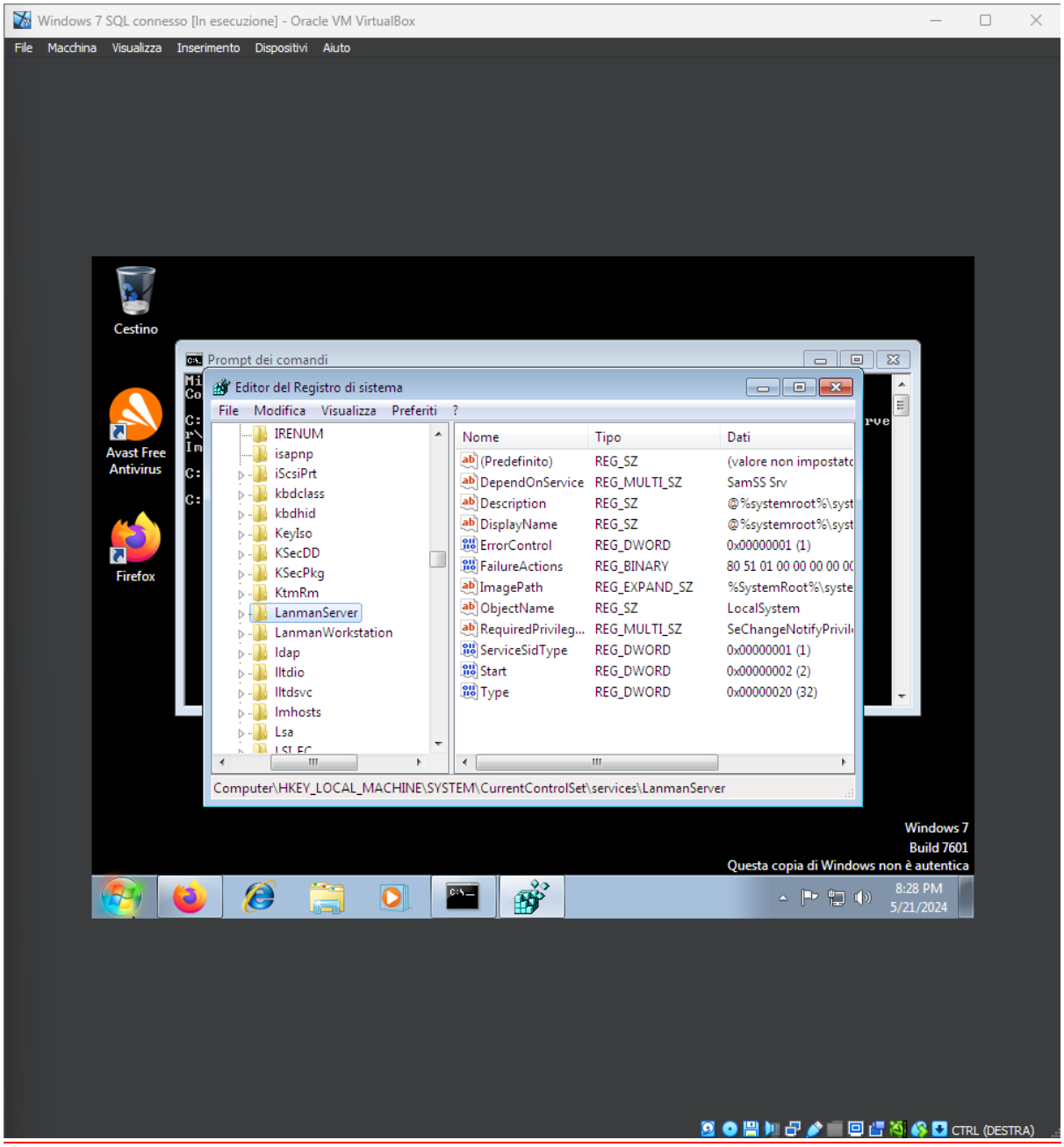
Conclusioni

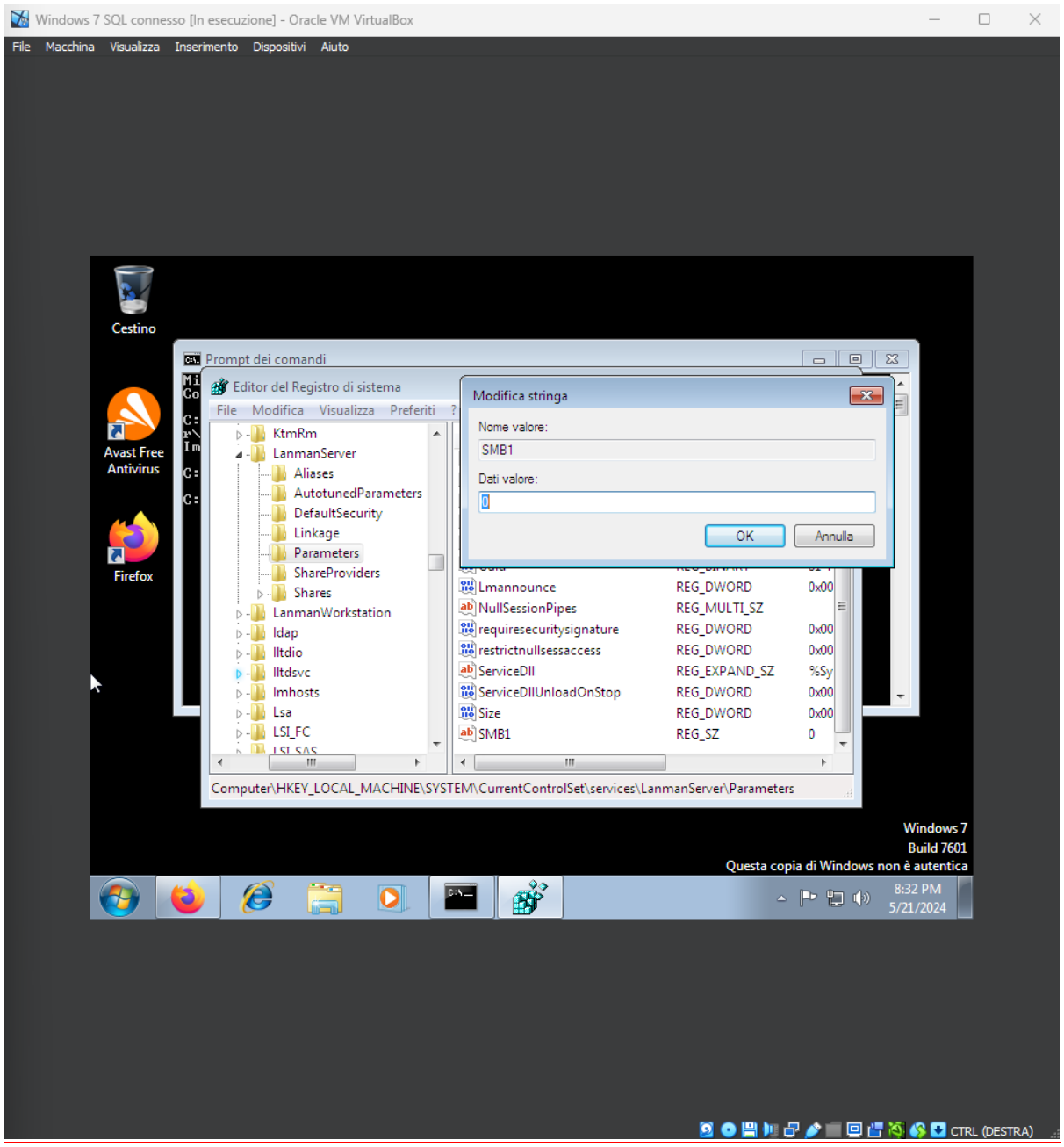
Seguendo questi passaggi, ho messo in sicurezza la macchina virtuale infetta da WannaCry. Ho disabilitato SMBv1, aggiornato il sistema operativo, eseguito una scansione completa con un software anti-malware, e modificato le password degli account utente. Inoltre, ho considerato l'aggiornamento del sistema operativo a Windows 10 per una maggiore sicurezza e supporto a lungo termine.

Screenshot


Windows 7 SQL connesso [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Avast Free Antivirus
Notifications
Menu
Outdated apps
Scanning...
Viruses & malware
Advanced issues
Scanning for outdated apps... 98%
Checking apps...
STOP SCAN
8:00 PM
5/21/2024
CTRL (DESTRA)


Windows 7 SQL connesso [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Amministratore: Windows PowerShell
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. Tutti i diritti riservati.
PS C:\Windows\system32> Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer
SMB1" -Value 0 -Force
PS C:\Windows\system32>
8:21 PM
5/21/2024
CTRL (DESTRA)


Windows 7 SQL connesso [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Cestino
Avast Free Antivirus
Firefox
Prompt dei comandi
Editor del Registro di sistema
File Modifica Visualizza Preferiti ?
IRENUM
isapnp
iScsiPrt
kbdclass
kbdhid
KeyIso
KSecDD
KSecPkg
KtmRm
LanmanServer
LanmanWorkstation
ldap
lltdio
lltdsvc
lmhosts
Lsa
Nome Tipo Dati
(Predefinito) REG_SZ (valore non impostato
DependOnService REG_MULTI_SZ SamSS Srv
Description REG_SZ @%systemroot%\syst
DisplayName REG_SZ @%systemroot%\syst
ErrorControl REG_DWORD 0x00000001 (1)
FailureActions REG_BINARY 80 51 01 00 00 00 00 00
ImagePath REG_EXPAND_SZ %SystemRoot%\syste
ObjectName REG_SZ LocalSystem
RequiredPrivileg... REG_MULTI_SZ SeChangeNotifyPrivil
ServiceSidType REG_DWORD 0x00000001 (1)
Start REG_DWORD 0x00000002 (2)
Type REG_DWORD 0x00000020 (32)
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\LanmanServer
Windows 7
Build 7601
Questa copia di Windows non è autentica
8:28 PM
5/21/2024
CTRL (DESTRA)


Windows 7 SQL connesso [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Cestino
Avast Free Antivirus
Firefox
Prompt dei comandi
Editor del Registro di sistema
File Modifica Visualizza Preferiti
KtmRm
LanmanServer
Aliases
AutotunedParameters
DefaultSecurity
Linkage
Parameters
ShareProviders
Shares
LanmanWorkstation
ldap
lltdio
lltdsvc
lmhosts
Lsa
LSI_FC
Modifica stringa
Nome valore:
SMB1
Dati valore:
OK
Annulla
Lmannounce REG_DWORD
NullSessionPipes REG_MULTI_SZ
requiresecuritysignature REG_DWORD
restrictnullsessaccess REG_DWORD
ServiceDll REG_EXPAND_SZ
ServiceDllUnloadOnStop REG_DWORD
Size REG_DWORD
SMB1 REG_SZ 0
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\LanmanServer\Parameters
Windows 7
Build 7601
Questa copia di Windows non è autentica
8:32 PM
5/21/2024
CTRL (DESTRA)