

CYBER SECURITY

Lezione 06 – Il monitoraggio

IL MONITORAGGIO : LE CONNESSIONI



- Controllare lo stato delle connessioni con la console

```
Prompt dei comandi
C:\>ipconfig /all

Configurazione IP di Windows

Nome host . . . . . : CDSW-PC
Suffisso DNS primario . . . . . :
Tipo nodo . . . . . : Ibrido
Routing IP abilitato. . . . . : No
Proxy WINS abilitato . . . . . : No

Scheda Ethernet Ethernet:

Stato supporto. . . . . : Supporto
Suffisso DNS specifico per connessione:
Descrizione . . . . . : Intel(R)
Indirizzo fisico. . . . . : 50-EB-F
DHCP abilitato. . . . . : No
Configurazione automatica abilitata : Si

Scheda LAN wireless Connessione alla rete locale (LAN)* 9:

Stato supporto. . . . . : Supporto disconnesso
Suffisso DNS specifico per connessione:
Descrizione . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
Indirizzo fisico. . . . . : 56-EF-33-FC-24-34
DHCP abilitato. . . . . : Si
Configurazione automatica abilitata : Si

Scheda LAN wireless Connessione alla rete locale (LAN)* 10:
```

IL MONITORAGGIO : LE CONNESSIONI



- Controllare lo stato delle connessioni con la console
- Verificare con whois e dnslookup chi sono gli indirizzi presenti in lista
- Salvare i dati a 'macchina pulita'
- In caso di attacco confrontare i dati correnti con quelli salvati

```
Prompt dei comandi - netstat x + v
C:\>netstat

Connessioni attive

Proto  Indirizzo locale      Indirizzo esterno      Stato
TCP    127.0.0.1:53524        CDSW-PCF-01:65001     ESTABLISHED
TCP    127.0.0.1:53525        CDSW-PCF-01:53558     ESTABLISHED
TCP    127.0.0.1:53525        CDSW-PCF-01:54098     FIN_WAIT_2
TCP    127.0.0.1:53558        CDSW-PCF-01:53525     ESTABLISHED
TCP    127.0.0.1:54098        CDSW-PCF-01:53525     CLOSE_WAIT
TCP    127.0.0.1:65001        CDSW-PCF-01:53524     ESTABLISHED
TCP    192.168.2.9:53373      20.54.37.73:https     ESTABLISHED
TCP    192.168.2.9:53382      20.54.37.64:https     ESTABLISHED
TCP    192.168.2.9:53752      fritz:microsoft-ds    ESTABLISHED
TCP    192.168.2.9:53916      52.111.231.2:https    ESTABLISHED
TCP    192.168.2.9:54075      a-0001:https          TIME_WAIT
TCP    192.168.2.9:54081      152.199.21.118:https  ESTABLISHED
```

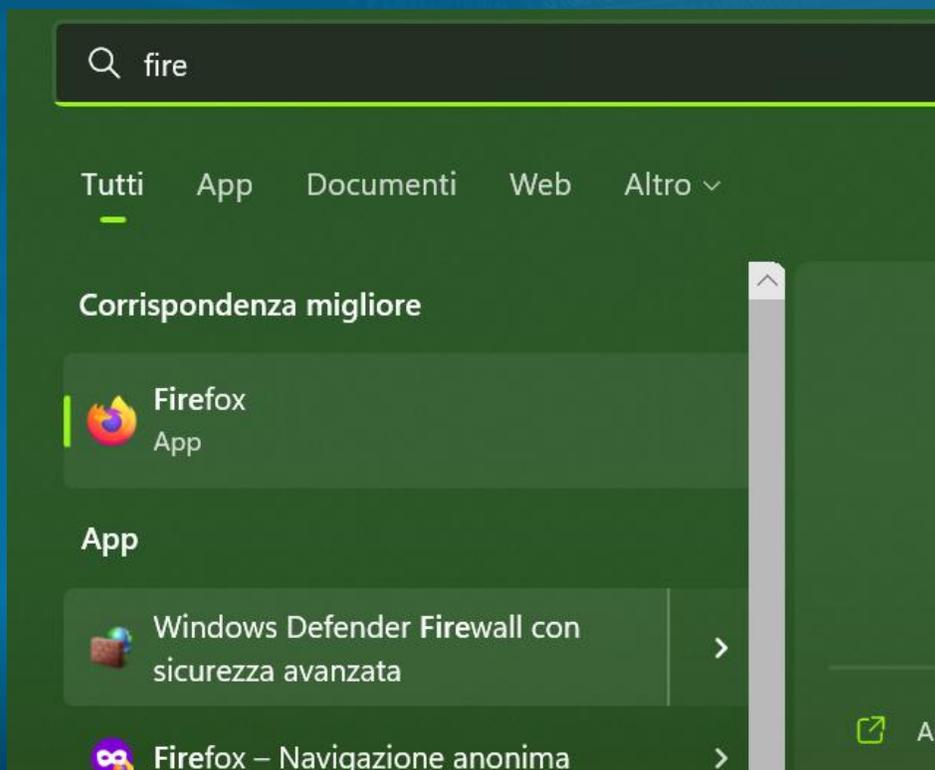
```
Prompt dei comandi - netstat x +
C:\>netstat

Connessioni attive
```

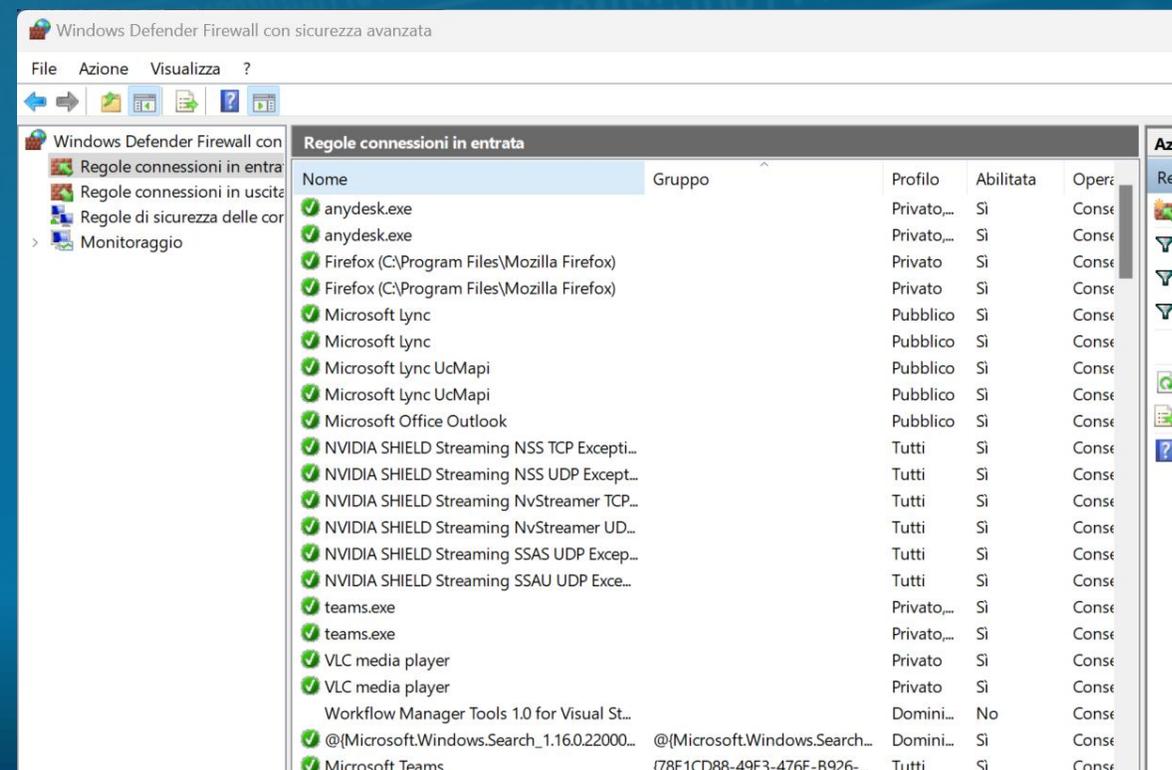
IL MONITORAGGIO : IL FIREWALL



- Aprire il firewall in modalita' Avanzata



- Rimuovere tutte le regole superflue (Ripristino per reset)



IL MONITORAGGIO : I SERVIZI E I PROCESSI



- Creare un'immagine dello stato iniziale e pulito del dispositivo per confrontarla in caso di sospetto

The screenshot shows the Windows Task Manager 'Processi' (Processes) tab. The left sidebar contains navigation options: Processi, Prestazioni, Cronologia applicazioni, App di avvio, Utenti, Dettagli, Servizi, and Impostazioni. The main area displays a list of processes under 'Applicazioni (7)' and 'Processi in background (78)'. A yellow box highlights the system resource usage summary at the top right of the process list:

Nome	Stato	CPU	Memoria	Disco	Rete
		1%	25%	0%	0%
		CPU	Memoria	Disco	Rete
Applicazioni (7)					
> Account di Posta e Calendario		0%	3,0 MB	0 MB/s	0 Mbps
> Esplora risorse		0,1%	156,8 MB	0 MB/s	0 Mbps
> Gestione attività		0,1%	59,3 MB	0 MB/s	0 Mbps
> Microsoft Management Console		0%	6,4 MB	0 MB/s	0 Mbps
> Microsoft PowerPoint (2)		0%	287,8 MB	0 MB/s	0 Mbps
> Strumento di cattura (2)		0,1%	36,5 MB	0 MB/s	0 Mbps
> Terminale (3)		0%	30,4 MB	0 MB/s	0 Mbps
Processi in background (78)					
> Adobe Acrobat Update Service (32 bit)		0%	0,9 MB	0 MB/s	0 Mbps
> Advanced SystemCare (32 bit)		0,1%	265,4 MB	0 MB/s	0 Mbps
> Advanced SystemCare Service (32 bit)		0%	0,9 MB	0 MB/s	0 Mbps

IL MONITORAGGIO : I SERVIZI E I PROCESSI



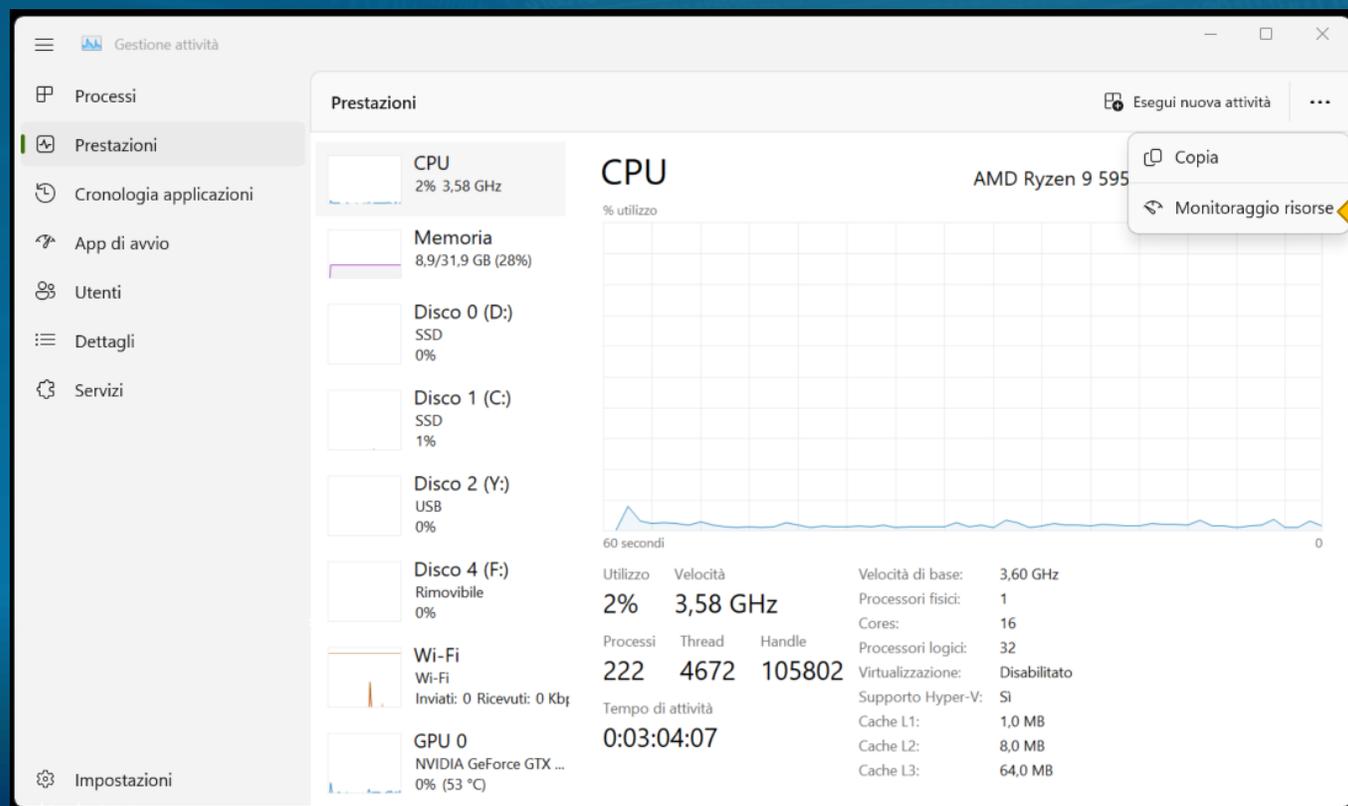
- Creare un'immagine dello stato iniziale e pulito del dispositivo per confrontarla in caso di sospetto

Nome	PID	Descrizione	Stato	Gruppo
XboxGipSvc		Xbox Accessory Management Service	Arrestato	netsvcs
LanmanWorkstation	4772	Workstation	In esecuzione	NetworkService
wuauclnt		Windows Update	Arrestato	netsvcs
WSearch	3704	Windows Search	In esecuzione	
IpOverUsbSvc	5068	Windows Phone IP over USB Transport (IpOverUsbSvc)	In esecuzione	
msiserver		Windows Installer	Arrestato	
mpssvc	3168	Windows Defender Firewall	In esecuzione	LocalServiceN
wcncsvc	19052	Windows Connect Now - Registro configurazioni	In esecuzione	LocalServiceA
SDRSVC	3960	Windows Backup	In esecuzione	SDRSVC
WebClient	21208	WebClient	In esecuzione	LocalService
WarpJITSvc		Warp JIT Service	Arrestato	LocalServiceN
WalletService		WalletService	Arrestato	appmodel
WaaSMedicSvc		WaaSMedicSvc	Arrestato	wusvcs
DispBrokerDesktopSvc	2892	Visualizza servizio criteri	In esecuzione	LocalService
VSStandardCollectorServi...		Visual Studio Standard Collector Service 150	Arrestato	
svsvc		Verifica spot	Arrestato	LocalSystemN
Schedule	1348	Utilità di pianificazione	In esecuzione	netsvcs

IL MONITORAGGIO : LE PRESTAZIONI



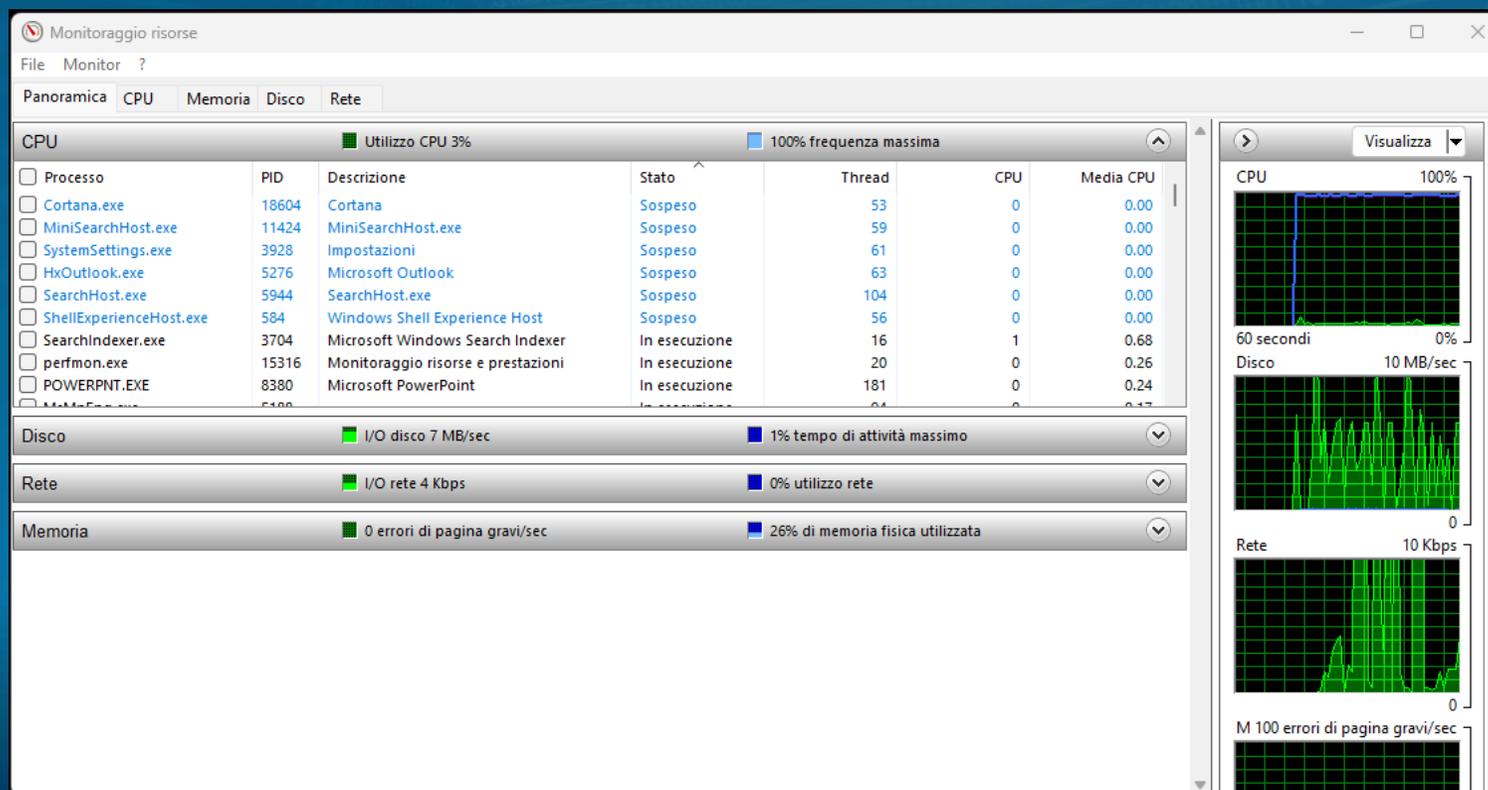
- Creare un'immagine dello stato iniziale e pulito del dispositivo per confrontarla in caso di sospetto



IL MONITORAGGIO : LE PRESTAZIONI



- Creare un'immagine dello stato iniziale e pulito del dispositivo per confrontarla in caso di sospetto



IL MONITORAGGIO : GLI UTENTI ATTIVI



- Osservare se ci sono utenti indesiderati

Utenti

Utente	Stato	2% CPU	25% Memoria	0% Disco	0% Rete
> DanieleCELOTTI (92)		1,3%	1.243,1 MB	0,1 MB/s	0 Mbps

IL MONITORAGGIO : VISUALIZZARE GLI EVENTI



- Creare un'immagine dello stato iniziale e pulito del dispositivo per confrontarla in caso di sospetto

The screenshot shows the Windows Event Viewer interface. The main pane displays a list of security events under the 'Sicurezza' category. The table below represents the data shown in the main pane:

Parole chiave	Data e ora	Origine	ID evento	Categoria attività
Controllo riuscito	10/11/2022 08:04:11	Microsoft Windo...	5379	User Account Ma...
Controllo riuscito	10/11/2022 08:04:11	Microsoft Windo...	5379	User Account Ma...
Controllo riuscito	10/11/2022 08:04:11	Microsoft Windo...	5379	User Account Ma...
Controllo riuscito	10/11/2022 08:04:11	Microsoft Windo...	5379	User Account Ma...
Controllo riuscito	10/11/2022 08:04:11	Microsoft Windo...	5379	User Account Ma...
Controllo riuscito	10/11/2022 08:04:11	Microsoft Windo...	5379	User Account Ma...
Controllo riuscito	10/11/2022 08:04:11	Microsoft Windo...	5379	User Account Ma...
Controllo riuscito	10/11/2022 08:04:11	Microsoft Windo...	4672	Special Logon
Controllo riuscito	10/11/2022 08:04:11	Microsoft Windo...	4672	Special Logon
Controllo riuscito	10/11/2022 07:58:43	Microsoft Windo...	4624	Logon
Controllo riuscito	10/11/2022 07:58:16	Microsoft Windo...	5061	System Integrity
Controllo riuscito	10/11/2022 07:51:39	Microsoft Windo...	5382	User Account Ma...
Controllo riuscito	10/11/2022 07:51:38	Microsoft Windo...	4672	Special Logon
Controllo riuscito	10/11/2022 07:51:38	Microsoft Windo...	4624	Logon
Controllo riuscito	10/11/2022 07:51:02	Microsoft Windo...	5379	User Account Ma...
Controllo riuscito	10/11/2022 07:51:02	Microsoft Windo...	5379	User Account Ma...
Controllo riuscito	10/11/2022 07:51:02	Microsoft Windo...	5379	User Account Ma...
Controllo riuscito	10/11/2022 07:51:02	Microsoft Windo...	5379	User Account Ma...
Controllo riuscito	10/11/2022 07:51:02	Microsoft Windo...	5379	User Account Ma...
Controllo riuscito	10/11/2022 07:51:02	Microsoft Windo...	5379	User Account Ma...
Controllo riuscito	10/11/2022 07:51:02	Microsoft Windo...	5379	User Account Ma...

The details pane for event 5379 shows the following information:

Le credenziali di Gestione credenziali sono state lette.

Nome registro: Sicurezza

Origine: Microsoft Windows security Registrato: 10/11/2022 08:04:11

ID evento: 5379 Categoria attività: User Account Management

Livello: Informazioni Parole chiave: Controllo riuscito

Utente: N/D Computer: CDSW-PCF-01

GLI EVENTI DI SISTEMA



Analisi degli eventi per scoprire le intrusioni

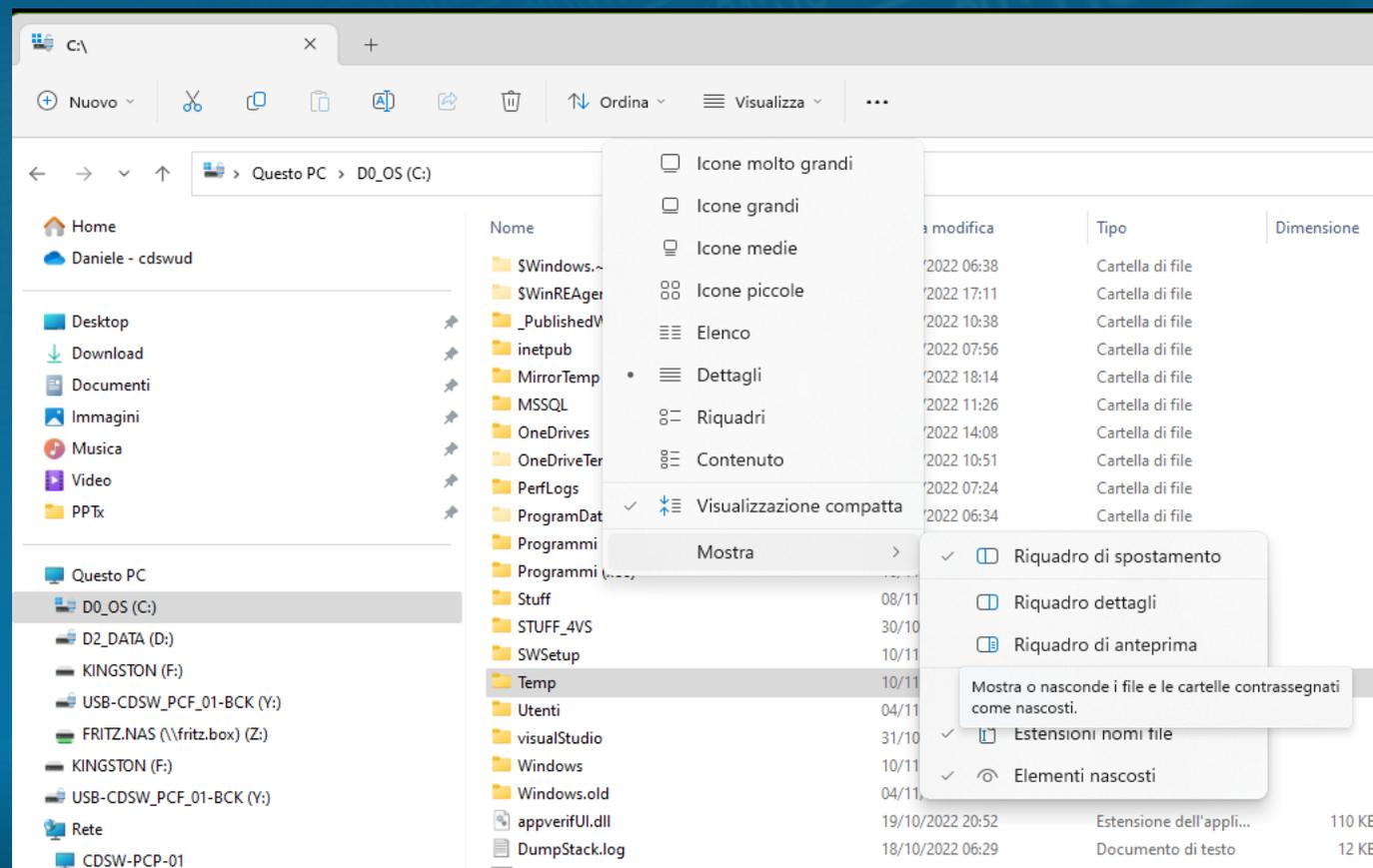
The screenshot displays the Windows Event Viewer interface. The left pane shows the navigation tree with 'Security' selected under 'Windows Logs'. The main pane shows a list of events in the Security log, with one 'Audit Failure' event highlighted. A large red arrow points from this event to the details pane. The details pane shows the following information:

Field	Value
Log Name:	Security
Source:	Microsoft Windows security
Event ID:	5061
Level:	Information
User:	N/A
OpCode:	Info
Subject:	Cryptographic operation.
Security ID:	NT SERVICE\MSSQLSERVER
Account Name:	MSSQLSERVER
Logged:	4/10/2024 6:25:02 AM
Task Category:	System Integrity
Keywords:	Audit Failure
Computer:	

IL MONITORAGGIO : LE CARTELLE NASCOSTE



- Analizzare le cartelle nascoste o sospette per rilevare intrusioni ed attività' indesiderate



IL MONITORAGGIO : LE CARTELLE NASCOSTE



- Analizzare le cartelle nascoste o sospette per rilevare intrusioni ed attività indesiderate

```
Prompt dei comandi
C:\>dir C: /a:h /b /s
C:\$Recycle.Bin
C:\$Windows.~WS
C:\$WinREAgent
C:\Documents and Settings
C:\DumpStack.log.tmp
C:\hiberfil.sys
C:\OneDriveTemp
C:\pagefile.sys
C:\ProgramData
C:\Programmi
C:\Recovery
C:\swapfile.sys
C:\SYSTAG.BIN
C:\System Volume Information
C:\$Recycle.Bin\S-1-5-18
C:\Program Files\desktop.ini
C:\Program Files\File comuni
C:\Program Files\Uninstall Information
C:\Program Files\Windows Sidebar
C:\Program Files\WindowsApps
C:\Program Files\Microsoft Office\root\vfs\Common AppData\Microsoft Help\MS.DATABASECOMPARE.16.1040.hxn
C:\Program Files\Microsoft Office\root\vfs\Common AppData\Microsoft Help\MS.EXCEL.16.1040.hxn
C:\Program Files\Microsoft Office\root\vfs\Common AppData\Microsoft Help\MS.GRAPH.16.1040.hxn
C:\Program Files\Microsoft Office\root\vfs\Common AppData\Microsoft Help\MS.LVNC.16.1040.hxn
```

```
Prompt dei comandi
C:\>dir C: /a:h /b /s
C:\$Recycle.Bin
C:\$Windows.~WS
```

[How to Show Hidden Files Windows 10 \(CMD + 4 Ways\)](https://www.minitool.com)
(minitool.com)

CARTELLE CONDIVISE



- Premere Windows+R quindi digitare \\localhost
- Windows+R, cmd poi net share

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Versione 10.0.14393]
(c) 2016 Microsoft Corporation. Tutti i diritti sono riservati.

C:\Users\Michele>net share

Nome cond.  Risorsa                Nota
-----
C$          C:\                   Condivisione predefinita
D$          D:\                   Condivisione predefinita
print$     C:\Windows\system32\spool\drivers
          Driver della stampante
IPC$       IPC remoto
ADMIN$     C:\WINDOWS           Amministrazione remota
Documents  C:\Users\Michele\Documents
Users      C:\Users
Esecuzione comando riuscita.

C:\Users\Michele>
```

CARTELLE CONDIVISE



- Premere Windows+R quindi digitare \\localhost
- Windows+R, cmd poi net share
- Gestione computer

The screenshot shows the 'Gestione computer' window in Windows. The left sidebar is expanded to 'Cartelle condivise', which is further expanded to show a list of shared folders. The main pane displays a table of these shared folders with their names, paths, types, and the number of client connections.

Nome condivisione	Percorso cartella	Tipo	Numero di connessioni client
ADMINS	C:\WINDOWS	Windows	0
CS	C:\	Windows	0
DS	D:\	Windows	0
Documents	C:\Users\Michele\...	Windows	1
IPCS		Windows	0
print\$	C:\Windows\system...	Windows	0
Users	C:\Users	Windows	0

E NATURALMENTE...



▪ **Controllo Sistemi di Sicurezza**

- Sicurezza Fisica
- Antivirus ed Antispyware attivo, funzionante ed aggiornato
- Servizio di aggiornamento del Sistema Operativo acceso e funzionante
- Intrusion Detection System (per chi ce l'ha)
- Restore da Backup
- Firewall non compromesso
- Regole delle password e dei gruppi

IN SINTESI...



- **Backup dei dati**

- Eseguire backup regolari di tutti i file di dati.
- **Testare** il ripristino dei file di dati del client per garantire che i file di backup funzionino.
- Assicurati che almeno una copia dei dati sia archiviata in un luogo sicuro fuori sede.
- Rivedi periodicamente i tuoi requisiti di backup.

IN SINTESI...



Sicurezza fisica

- Assicurati che i tuoi computer si trovino in aree non facilmente accessibili agli estranei.
- Assicurati che tu e il tuo personale siate responsabili della chiusura di porte e finestre.
- Verifica se i tuoi computer desktop e laptop sono dotati di dispositivi antifurto.
- Verifica se i tuoi server di rete sono fisicamente protetti in un'area separata.
- Assicurati di avere un inventario accurato di tutte le apparecchiature informatiche e dei software archiviati fuori sede.
- Implementa una politica di "svuotamento scrivania" per garantire che il tuo personale protegga i file sensibili e riservati quando non ci sta lavorando.

IN SINTESI...



Protezione dai virus

- Controlla se il software antivirus è installato su tutti i tuoi computer.
- Verificare se il software antivirus è stato configurato per verificare la presenza di virus su tutti i supporti (e-mail, siti Web, file scaricati).
- Verificare se è in atto una procedura per l'aggiornamento automatico del software antivirus.
- Verifica se gli utenti sanno cosa fare quando vengono infettati da un virus informatico.
- Assicurati che tu e il tuo staff apriate solo gli allegati che si aspettano.

IN SINTESI...



Ripristino di emergenza

- Avere un piano di continuità scritto in atto in caso di un grave disastro (come un incendio).
- Controlla per quanto tempo la tua pratica potrebbe funzionare senza computer, server o accesso alla rete.
- Verifica se la tua sede centrale fornisce assistenza per il ripristino di emergenza.
- Assicurati di avere almeno una copia dei dati del client e del software applicativo archiviata in un luogo sicuro fuori sede.
- Assicurati di avere un inventario aggiornato delle apparecchiature informatiche, del software e dei file client critici.

IN SINTESI...



Firewall

- Controlla se su tutti i tuoi computer è installato un software firewall.
- Assicurati che il software firewall sia stato configurato per proteggere le informazioni richieste sui tuoi computer.
- Verifica se nella tua rete è installato un firewall hardware.
- Controlla se hai firewall installati in ogni punto in cui i tuoi sistemi informatici sono collegati ad altre reti.

IN SINTESI...



Gestione delle password

- Richiedi password per l'accesso a tutti i computer.
- Scegli password "forti".
- Cambia le password regolarmente.
- Assicurati che le password non siano scritte o condivise.
- Impedisci agli utenti di scegliere password che sono state utilizzate solo poco tempo fa.
- Disattivare gli account per i dipendenti licenziati in modo tempestivo.

IN SINTESI...



Varie

- Non archiviare informazioni sensibili su unità USB
- Cancella frequentemente i dati privati dai browser Web.
- Assicurati che il tuo sistema operativo sia aggiornato.
- Utilizzare uno screen saver protetto da password o "bloccare" lo schermo.