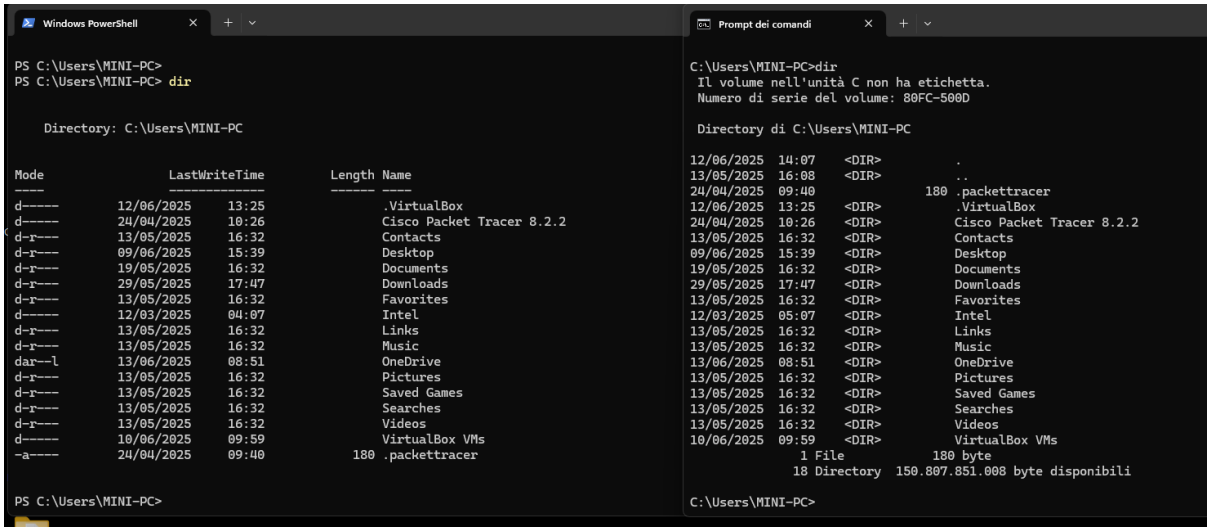
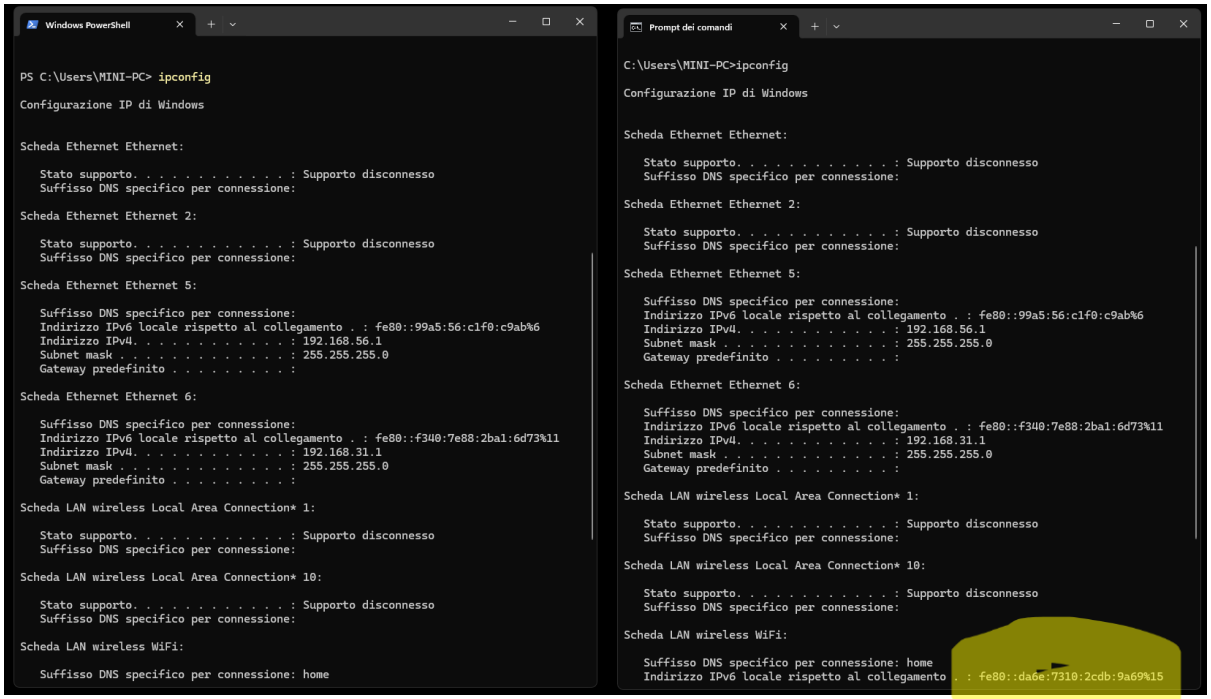
ESERCIZIO 1

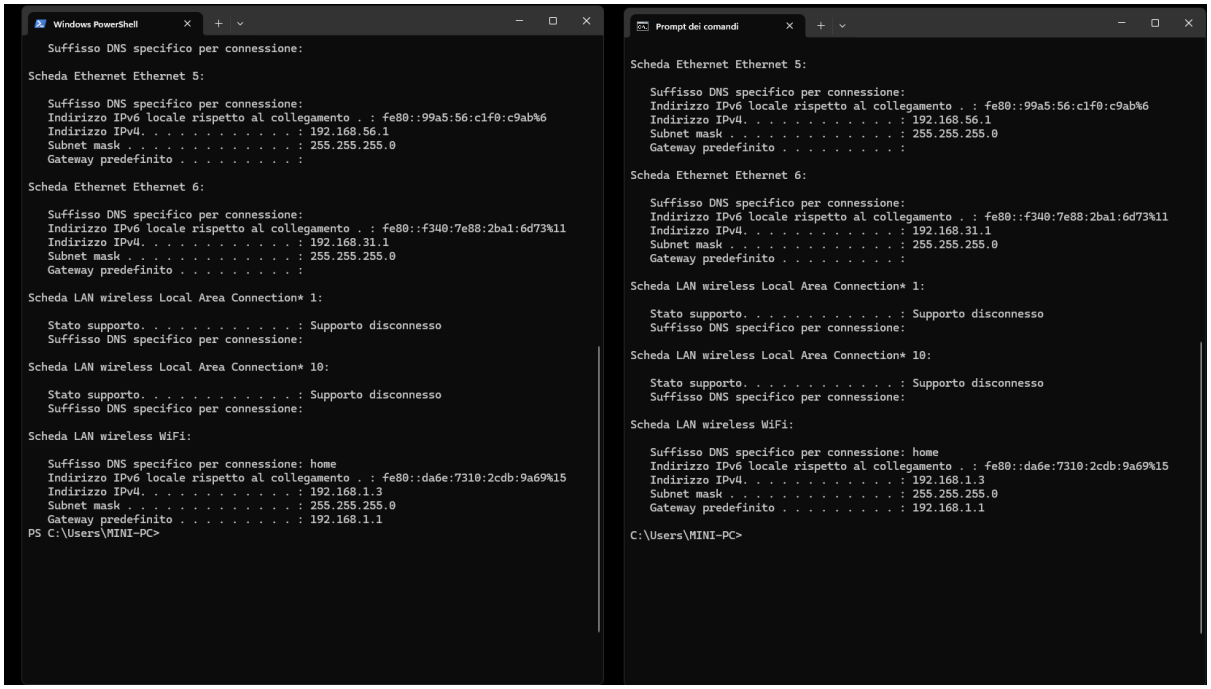
Quali sono gli output del comando dir?



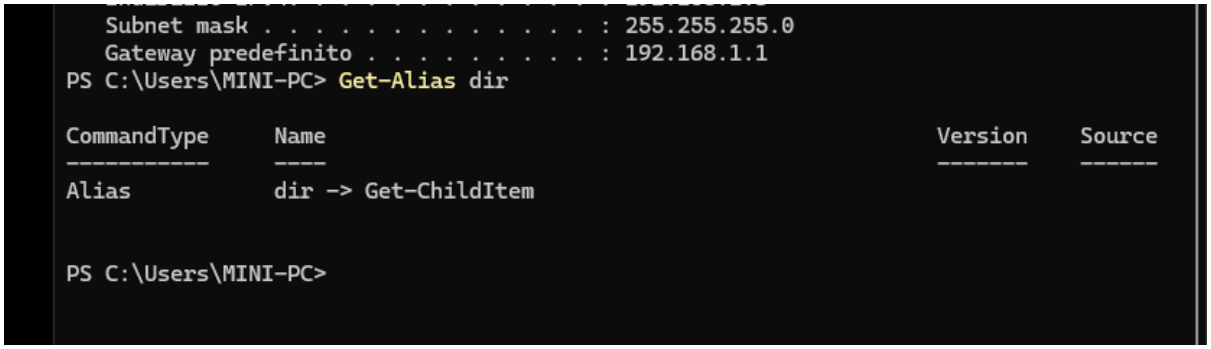
Riprovo con ipconfig

Quali sono i risultati?

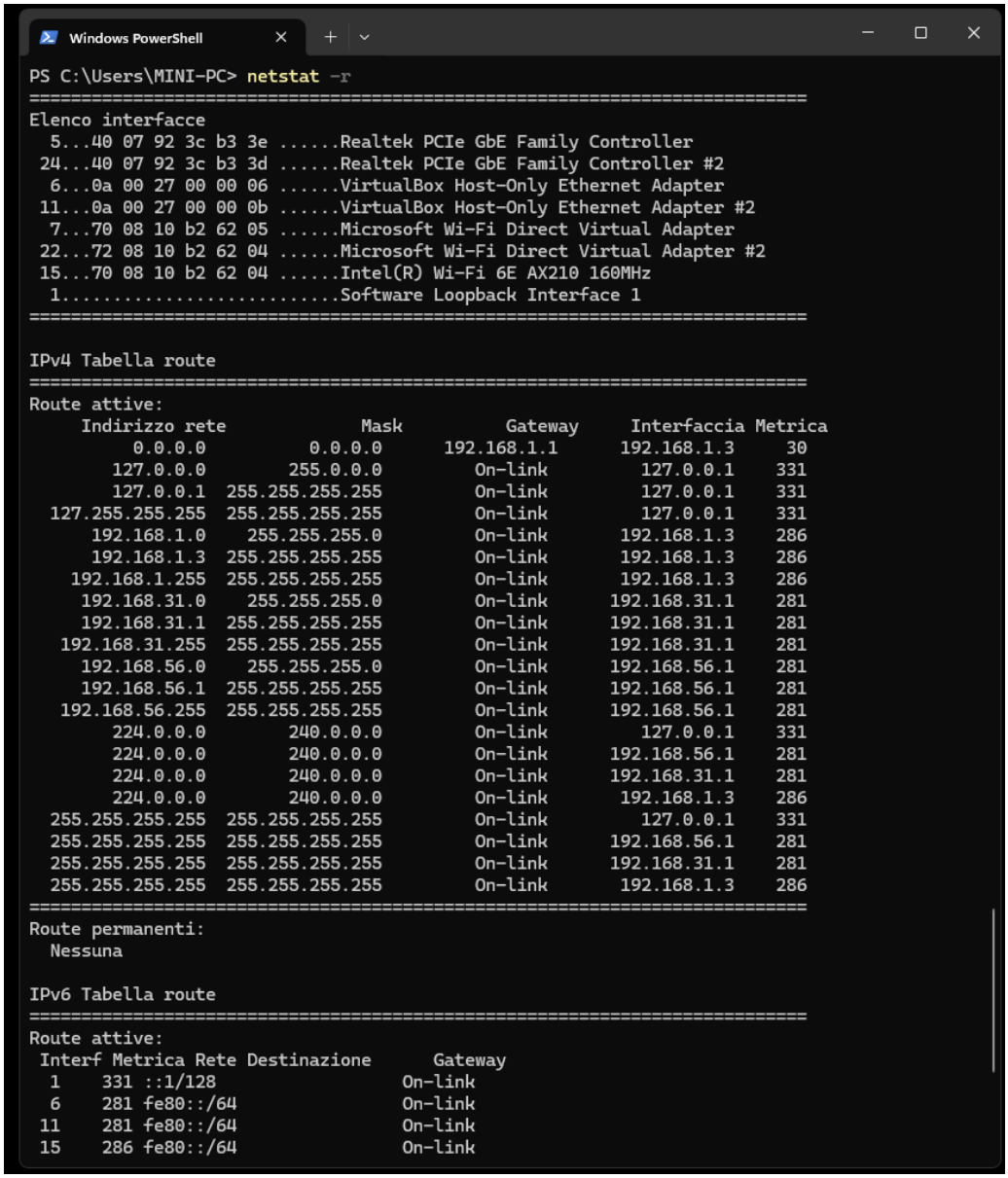


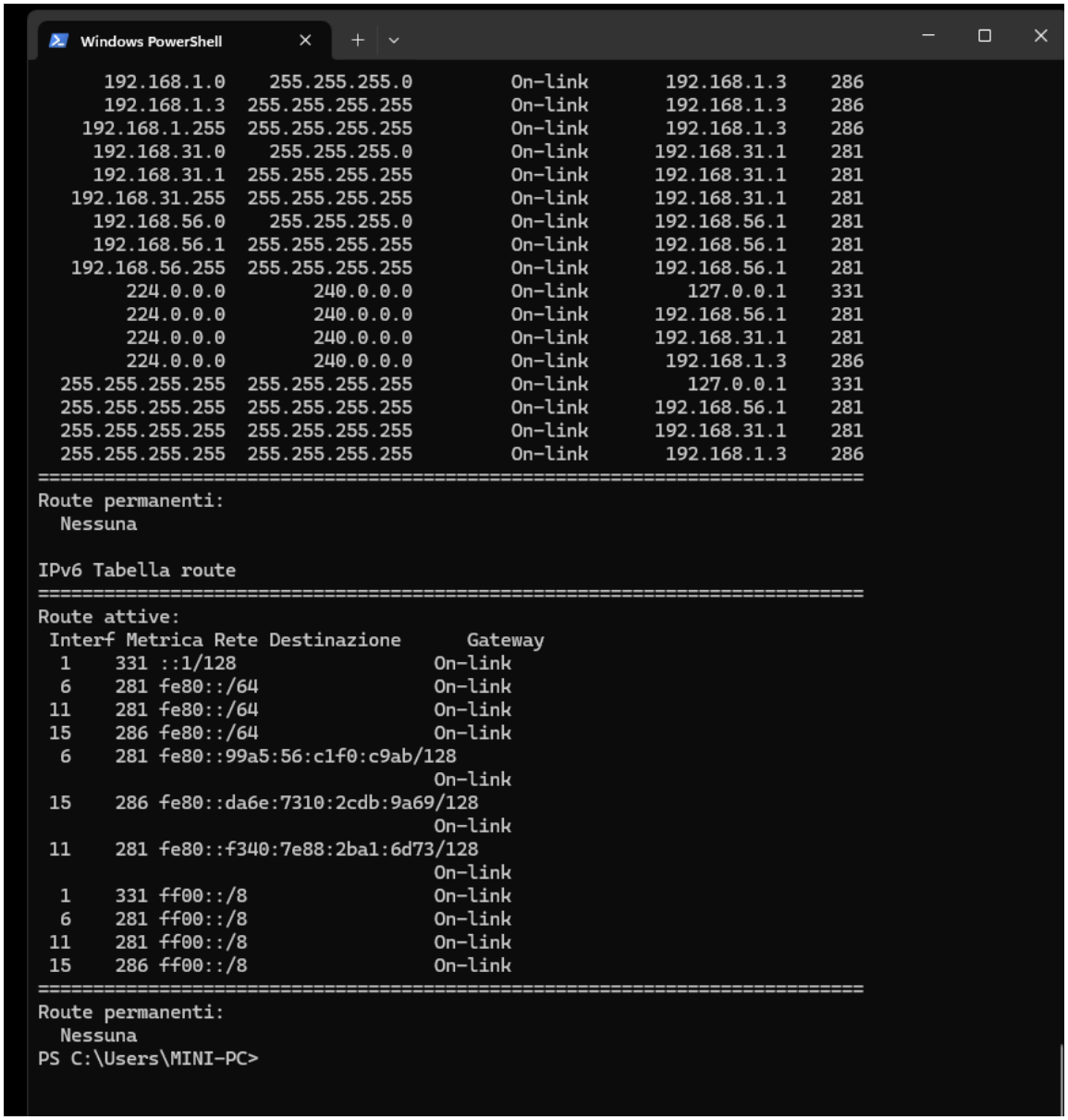


Qual è il comando PowerShell per dir? Get-ChildItem

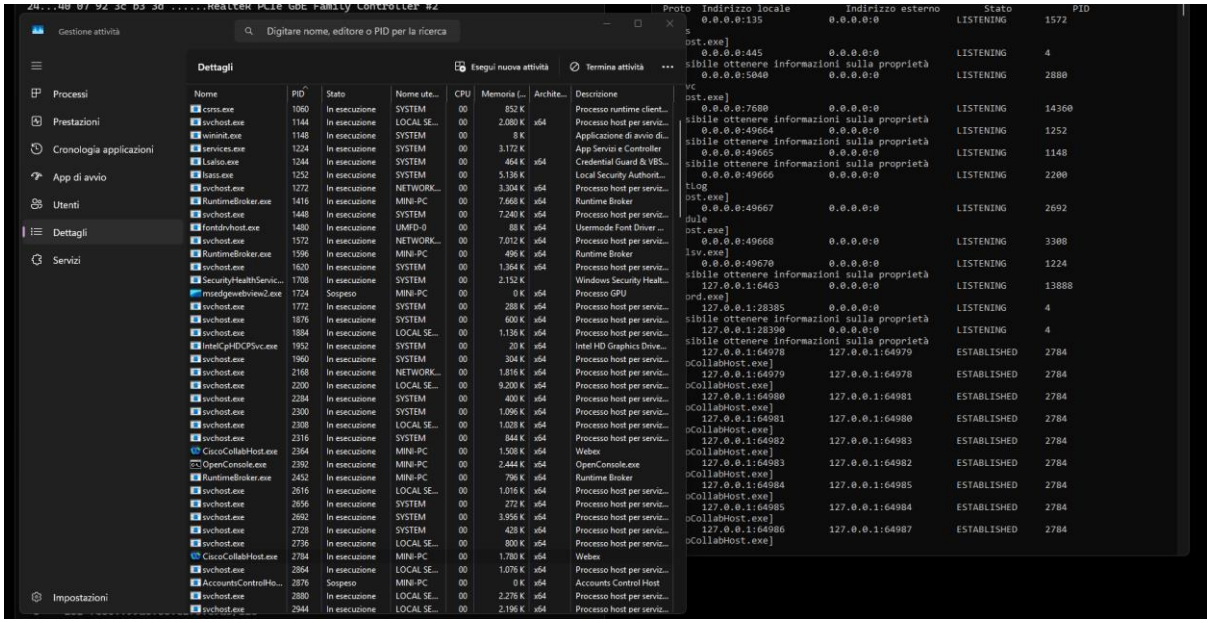


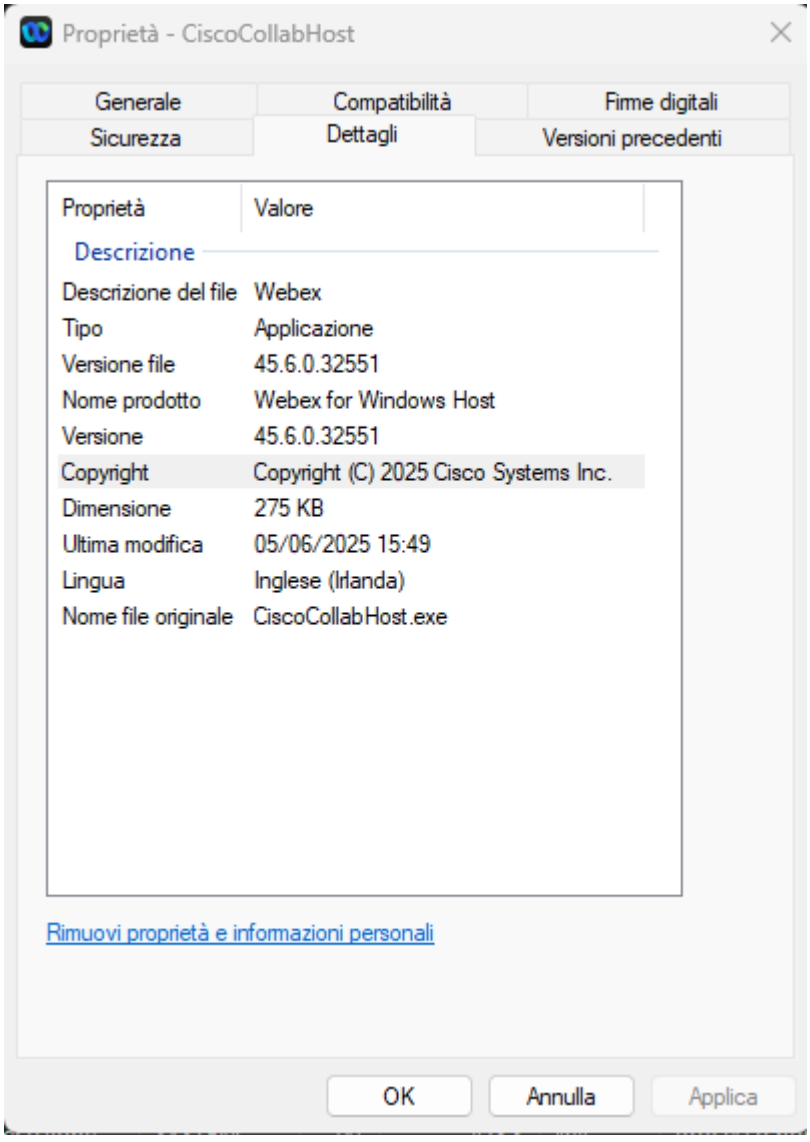
Qual è il gateway IPv4? 192.168.1.1

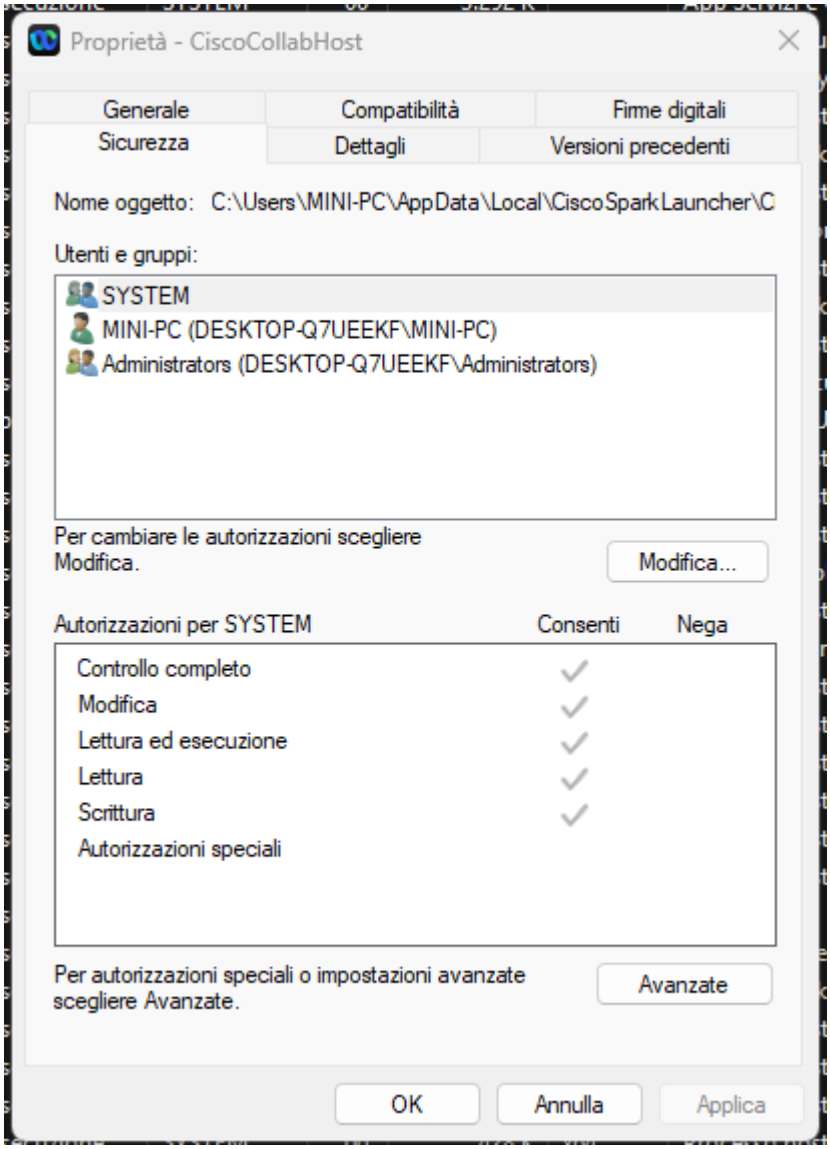

Windows PowerShell
PS C:\Users\MINI-PC> netstat -r
===
Elenco interfacce
  5...40 07 92 3c b3 3e ......Realtek PCIe GbE Family Controller
 24...40 07 92 3c b3 3d ......Realtek PCIe GbE Family Controller #2
  6...0a 00 27 00 00 06 ......VirtualBox Host-Only Ethernet Adapter
 11...0a 00 27 00 00 0b ......VirtualBox Host-Only Ethernet Adapter #2
  7...70 08 10 b2 62 05 ......Microsoft Wi-Fi Direct Virtual Adapter
 22...72 08 10 b2 62 04 ......Microsoft Wi-Fi Direct Virtual Adapter #2
 15...70 08 10 b2 62 04 ......Intel(R) Wi-Fi 6E AX210 160MHz
  1...........................Software Loopback Interface 1
===
IPv4 Tabella route
===
Route attive:
     Indirizzo rete   Mask   Gateway   Interfaccia Metrica
          0.0.0.0   0.0.0.0   192.168.1.1   192.168.1.3   30
        127.0.0.0   255.0.0.0   On-link   127.0.0.1   331
        127.0.0.1 255.255.255.255   On-link   127.0.0.1   331
  127.255.255.255 255.255.255.255   On-link   127.0.0.1   331
      192.168.1.0   255.255.255.0   On-link   192.168.1.3   286
      192.168.1.3 255.255.255.255   On-link   192.168.1.3   286
    192.168.1.255 255.255.255.255   On-link   192.168.1.3   286
     192.168.31.0   255.255.255.0   On-link   192.168.31.1   281
     192.168.31.1 255.255.255.255   On-link   192.168.31.1   281
   192.168.31.255 255.255.255.255   On-link   192.168.31.1   281
     192.168.56.0   255.255.255.0   On-link   192.168.56.1   281
     192.168.56.1 255.255.255.255   On-link   192.168.56.1   281
   192.168.56.255 255.255.255.255   On-link   192.168.56.1   281
        224.0.0.0   240.0.0.0   On-link   127.0.0.1   331
        224.0.0.0   240.0.0.0   On-link   192.168.56.1   281
        224.0.0.0   240.0.0.0   On-link   192.168.31.1   281
        224.0.0.0   240.0.0.0   On-link   192.168.1.3   286
  255.255.255.255 255.255.255.255   On-link   127.0.0.1   331
  255.255.255.255 255.255.255.255   On-link   192.168.56.1   281
  255.255.255.255 255.255.255.255   On-link   192.168.31.1   281
  255.255.255.255 255.255.255.255   On-link   192.168.1.3   286
===
Route permanenti:
  Nessuna
IPv6 Tabella route
===
Route attive:
 Interf Metrica Rete Destinazione   Gateway
  1   331 ::1/128   On-link
  6   281 fe80::/64   On-link
 11   281 fe80::/64   On-link
 15   286 fe80::/64   On-link

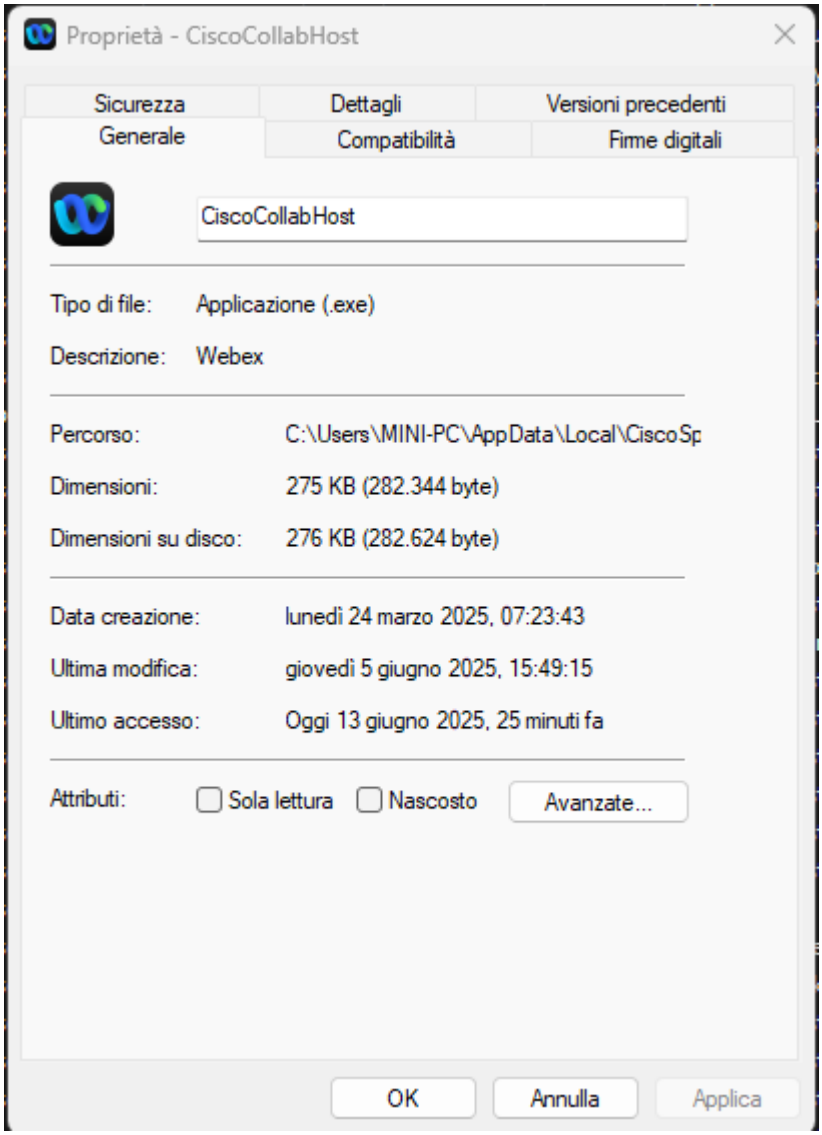


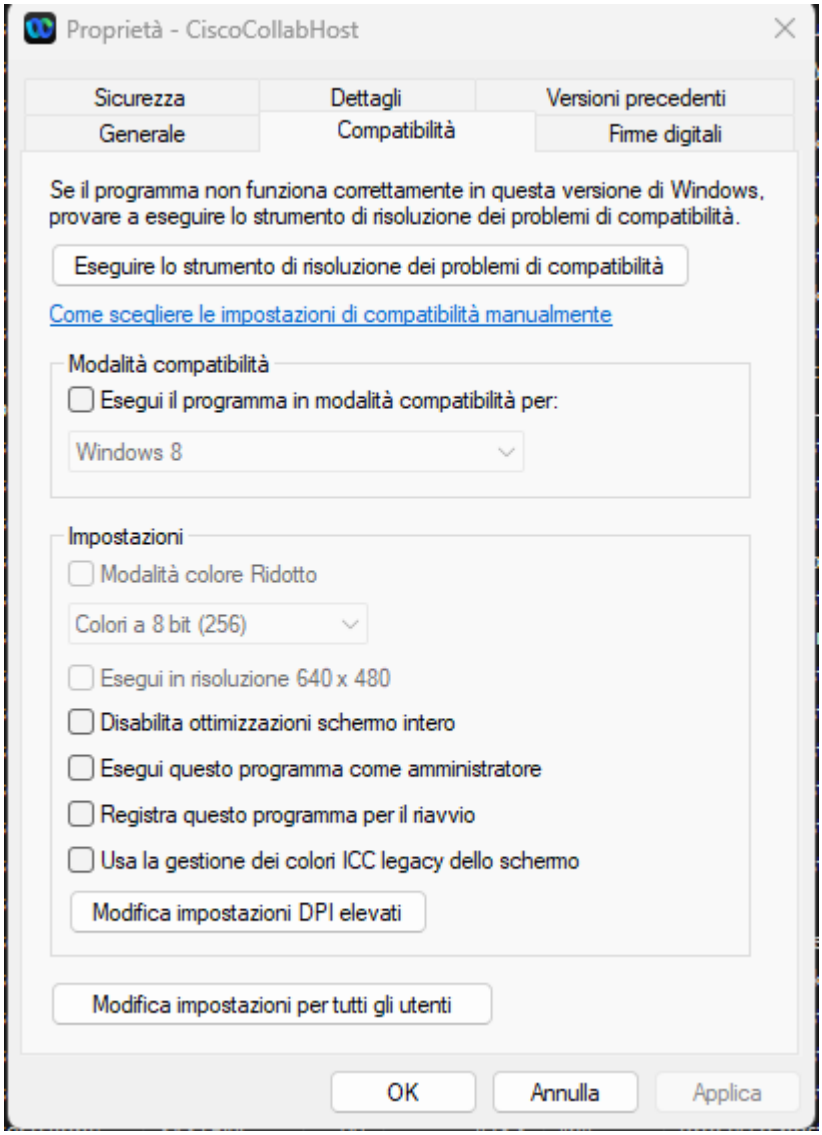
Quali informazioni puoi ottenere dalla scheda Dettagli e dalla finestra di dialogo Proprietà per il PID selezionato? Scelgo il PID 2784

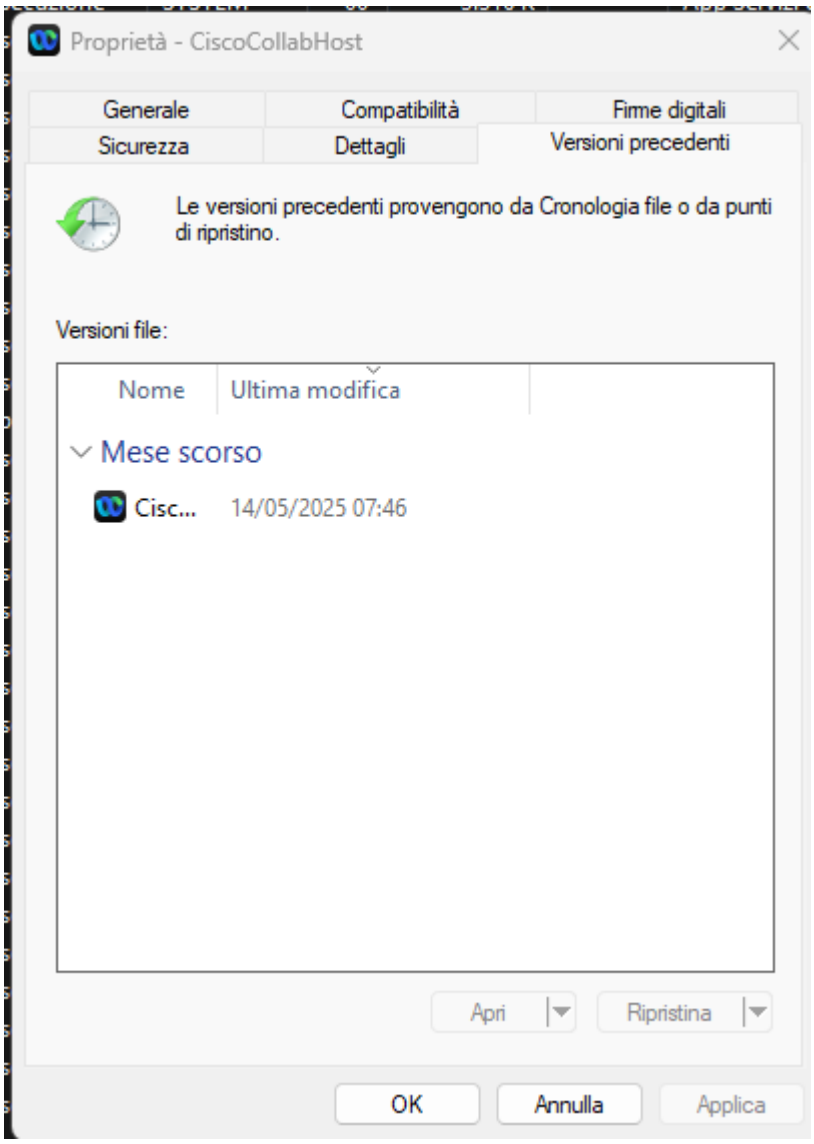

Gestione attività
Digitare nome, editore o PID per la ricerca
Dettagli
Esegui nuova attività
Termina attività
Processi
Prestazioni
Cronologia applicazioni
App di avvio
Utenti
Dettagli
Servizi
Impostazioni
Nome
PID
Stato
Nome ute...
CPU
Memoria (...
Archite...
Descrizione
Proto
Indirizzo locale
Indirizzo esterno
Stato
PID

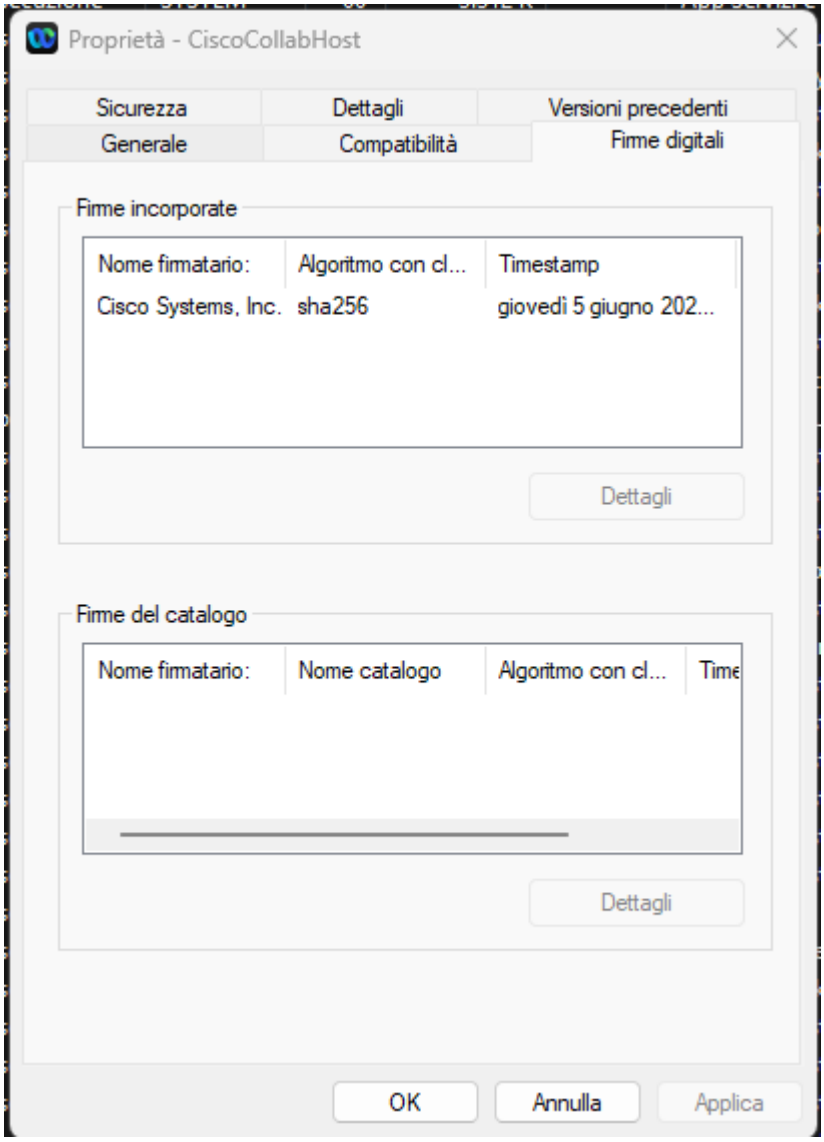

Proprietà - CiscoCollabHost
Generale
Compatibilità
Firme digitali
Sicurezza
Dettagli
Versioni precedenti
Proprietà
Valore
Descrizione
Descrizione del file
Webex
Tipo
Applicazione
Versione file
45.6.0.32551
Nome prodotto
Webex for Windows Host
Versione
45.6.0.32551
Copyright
Copyright (C) 2025 Cisco Systems Inc.
Dimensione
275 KB
Ultima modifica
05/06/2025 15:49
Lingua
Inglese (Irlanda)
Nome file originale
CiscoCollabHost.exe
Rimuovi proprietà e informazioni personali
OK
Annulla
Applica


Proprietà - CiscoCollabHost
Generale
Compatibilità
Firme digitali
Sicurezza
Dettagli
Versioni precedenti
Nome oggetto: C:\Users\MINI-PC\AppData\Local\CiscoSparkLauncher\C
Utenti e gruppi:
SYSTEM
MINI-PC (DESKTOP-Q7UEEKF\MINI-PC)
Administrators (DESKTOP-Q7UEEKF\Administrators)
Per cambiare le autorizzazioni scegliere Modifica.
Modifica...
Autorizzazioni per SYSTEM
Consenti
Nega
Controllo completo
Modifica
Lettura ed esecuzione
Lettura
Scrittura
Autorizzazioni speciali
Per autorizzazioni speciali o impostazioni avanzate scegliere Avanzate.
Avanzate
OK
Annulla
Applica


Proprietà - CiscoCollabHost
Sicurezza
Dettagli
Versioni precedenti
Generale
Compatibilità
Firme digitali
CiscoCollabHost
Tipo di file: Applicazione (.exe)
Descrizione: Webex
Percorso: C:\Users\MINI-PC\AppData\Local\CiscoSp
Dimensioni: 275 KB (282.344 byte)
Dimensioni su disco: 276 KB (282.624 byte)
Data creazione: lunedì 24 marzo 2025, 07:23:43
Ultima modifica: giovedì 5 giugno 2025, 15:49:15
Ultimo accesso: Oggi 13 giugno 2025, 25 minuti fa
Attributi: Sola lettura Nascosto Avanzate...
OK
Annulla
Applica


Proprietà - CiscoCollabHost
Sicurezza
Dettagli
Versioni precedenti
Generale
Compatibilità
Firme digitali
Se il programma non funziona correttamente in questa versione di Windows, provare a eseguire lo strumento di risoluzione dei problemi di compatibilità.
Eseguire lo strumento di risoluzione dei problemi di compatibilità
Come scegliere le impostazioni di compatibilità manualmente
Modalità compatibilità
Esegui il programma in modalità compatibilità per:
Windows 8
Impostazioni
Modalità colore Ridotto
Colori a 8 bit (256)
Esegui in risoluzione 640 x 480
Disabilita ottimizzazioni schermo intero
Esegui questo programma come amministratore
Registra questo programma per il riavvio
Usa la gestione dei colori ICC legacy dello schermo
Modifica impostazioni DPI elevati
Modifica impostazioni per tutti gli utenti
OK
Annulla
Applica


Proprietà - CiscoCollabHost
Generale
Compatibilità
Firme digitali
Sicurezza
Dettagli
Versioni precedenti
Le versioni precedenti provengono da Cronologia file o da punti di ripristino.
Versioni file:
Nome
Ultima modifica
Mese scorso
Cisc...
14/05/2025 07:46
Apri
Ripristina
OK
Annulla
Applica



1. Informazioni Generali sul File

- Nome file: CiscoCollabHost.exe
- Tipo: Applicazione (EXE) legata a Webex for Windows Host.
- Versione: 45.6.0.32551 (rilasciata da Cisco Systems Inc.).
- Percorso:
- Dimensioni: 275 KB.
- Ultima modifica: 5 giugno 2025.
- Ultimo accesso: 13 giugno 2025 (25 minuti prima dello screenshot).

2. Contesto del Processo

- Funzione: Parte dell'infrastruttura di Cisco Webex (probabilmente un componente di background per avviare/gestire Webex).
- Autorizzazioni:
    - Eseguito con privilegi per SYSTEM e Administrators (DESKTOP-Q7UEEKF\MINI-PC).
    - Ha autorizzazioni complete (lettura, scrittura, esecuzione).

3. Possibili Problemi/Configurazioni

- Compatibilità:
    - Le immagini mostrano opzioni per impostare la modalità compatibilità (es. Windows 8) o eseguire come amministratore, suggerendo che potrebbero esserci problemi su versioni recenti di Windows.
- Versioni precedenti:
    - È presente una versione precedente del file (14 maggio 2025), utile per ripristini in caso di malfunzionamenti.

4. Ipotesi sul PID 2784

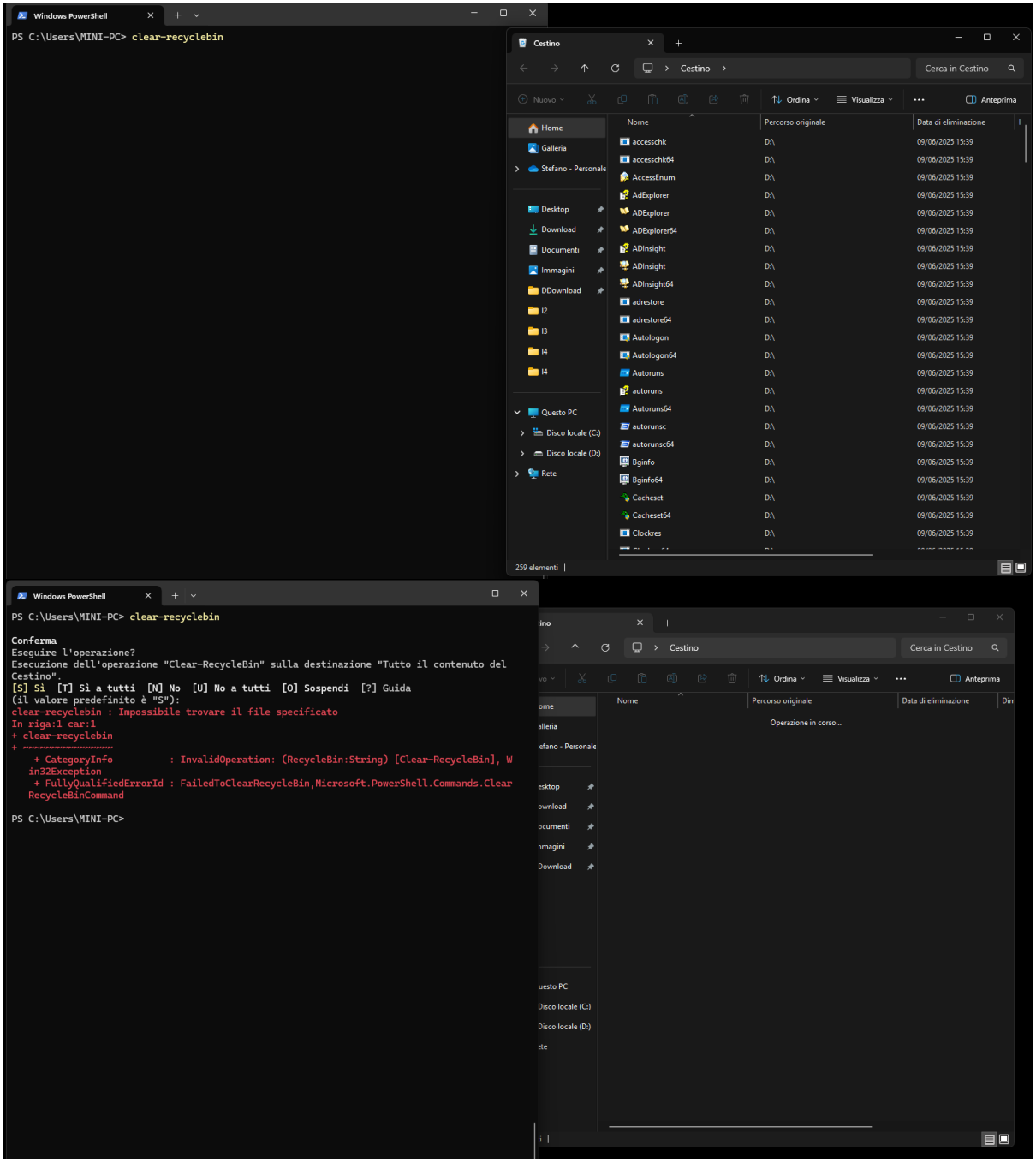
Se il PID 2784 è associato a CiscoCollabHost.exe, potresti verificare:

- Utilizzo risorse: Apri il Task Manager (Ctrl+Shift+Esc) e cerca il PID 2784 per vedere CPU, memoria, ecc.
- Connessioni di rete: Usa netstat -ano | findstr 2784 per controllare se il processo sta comunicando con server Webex.
- Log: Controlla i log di Webex o il Visualizzatore eventi di Windows sotto Applicazioni e Servizi > Cisco.

5. Possibili Azioni

- Se il processo è sospetto:
    - Verificare la firma digitale (già confermata nelle immagini: "Cisco Systems, Inc. sha256").
    - Confrontare l'hash del file con quello ufficiale di Cisco.
- Se consuma troppe risorse:
    - Provare a riavviare il servizio Webex o reinstallare il software.

Cosa è successo ai file nel Cestino? cancellati



Domanda di Riflessione PowerShell è stato sviluppato per l'automazione delle attività e la gestione della configurazione. Usando internet, ricerca comandi che potresti usare per semplificare i tuoi compiti come analista di sicurezza. Registra le tue scoperte.

Categoria	Comandi / Combinazioni salienti
Triage base	`Get-Service`, `Get-Process`, `Stop-Process`

Log & forensics	`Get-WinEvent`, `Select-String`, wrapping con CSV/JSON
Network & DNS	`Get-NetIPConfiguration`, `Resolve-DnsName`
Session recording	`Start/Stop-Transcript`
Security logging	ScriptBlockLogging, AMSI
SOC/API	`Get-ADUser`, PSFalcon, Azure cmdlet
Threat hunting	Rilevamento encoded, obfuscation, path anomali

ESERCIZIO 2

 1. Cobalt Strike (a.exe)

Tipo di minaccia: toolkit di penetration testing abusato (C2)

Osservazioni rilevanti da AnyRun:

- Il file a.exe è stato marcato con comportamento maligno: rilevato da YARA come *Cobalt Strike* .
- Durante l'esecuzione, il processo ha letto impostazioni di sicurezza Internet Explorer e informazioni sul proxy, oltre al nome del computer—tipiche operazioni di tecnologia di attacco (TTP) .
- Il comportamento comprende iniezione di processi, elevate attività in memoria e rete (possibile comunicazione con C2), elevazione privilegi (Integrity), persistenza e drop di eseguibili .
- Connessioni di rete verso un IP remoto (13.41.55.79:443, Amazon Cloud), non riconosciuto come whitelist .

Impatto tipico:

Cobalt Strike consente controllo remoto, esecuzione di payload secondari (es. ransomware), movimento laterale in rete e furto dati. È largamente usato da gruppi APT.

2. . Stealer “Stealc”

Tipo di minaccia: stealer (malware per furto dati)

Osservazioni da un report di AnyRun:

- Identificato come eseguibile Windows con comandi HTTP POST verso C2 .
- Il malware è dotato di persistence, fingerprinting dell’host, offuscamento stringhe e pannello di controllo in remoto .
- Classeggiato come “stealer”: focalizzato su dati sensibili estratti da browser, app di messaggistica, ecc. .

Impatto tipico:

È usato per rubare credenziali, cookie, chiavi, documenti. Può avviare attacchi mirati o vendita di dati.

3. Altri trojan e tendenze rilevate

Secondo il Malware Trends Tracker di AnyRun, alcune delle famiglie più rilevanti del 2025 includono :

- RedLine, NjRAT, Agent Tesla – stealer/RAT largamente impiegati per furto info, keylogging, controllo remoto.
- BlackMoon (KrBanker) – trojan bancario con tecniche MitB e furto credenziali.
- Ramnit, Raspberry Robin – malware diversificati: da worm a loader che sfruttano USB o TOR per download secondari.

Tali trojan vengono usati in campagne phishing, loader e distribuiti in pacchetti malevoli.

4. Indicatori di compromissione (IOCs)

Tipo	Dettagli/Rilevamenti
Processi sospetti	a.exe, slui.exe (iniezione in processi di sistema)
Connessioni C2	13.41.55.79:443 (Amazon AS) ; HTTP POST dai stealer
Comportamenti	Proxy/SEC sett, fingerprinting, recovery credenziali, persistence
Famiglie note	Cobalt Strike, Stealc; menzionati RedLine, Agent Tesla, BlackMoon, ecc.

5. Raccomandazioni operative

1. Monitoraggio processi e rete: registrare lancia di powershell.exe, explorer.exe, slui.exe segnalati, controllare C2 e URL sospetti (es. IP Amazon).
2. Threat hunting: integrare regole YARA per Cobalt Strike e stealer comuni, abilitare lo ScriptBlockLogging per rilevare comandi encoded o offuscati.
3. Blocco/rilevazione: aggiornare AV/EDR con indicatori (hash, IP) e campagne phishing note.
4. AZIONE di mitigazione: isolamento host compromessi, analisi forense, pulizia della persistence (servizi, scheduled tasks), rotazione credenziali exfiltrate.

Conclusione

L'indagine mostra evidenze di attacco strutturato con strumenti sofisticati: un C2 basato su Cobalt Strike e malware specializzato nel furto dati (Stealc). Entrambi condividono componenti avanzate come iniezione, persistence e comunicazione cifrata. È quindi essenziale attuare misure proattive per rilevare e bloccare simili minacce.

BONUS 1

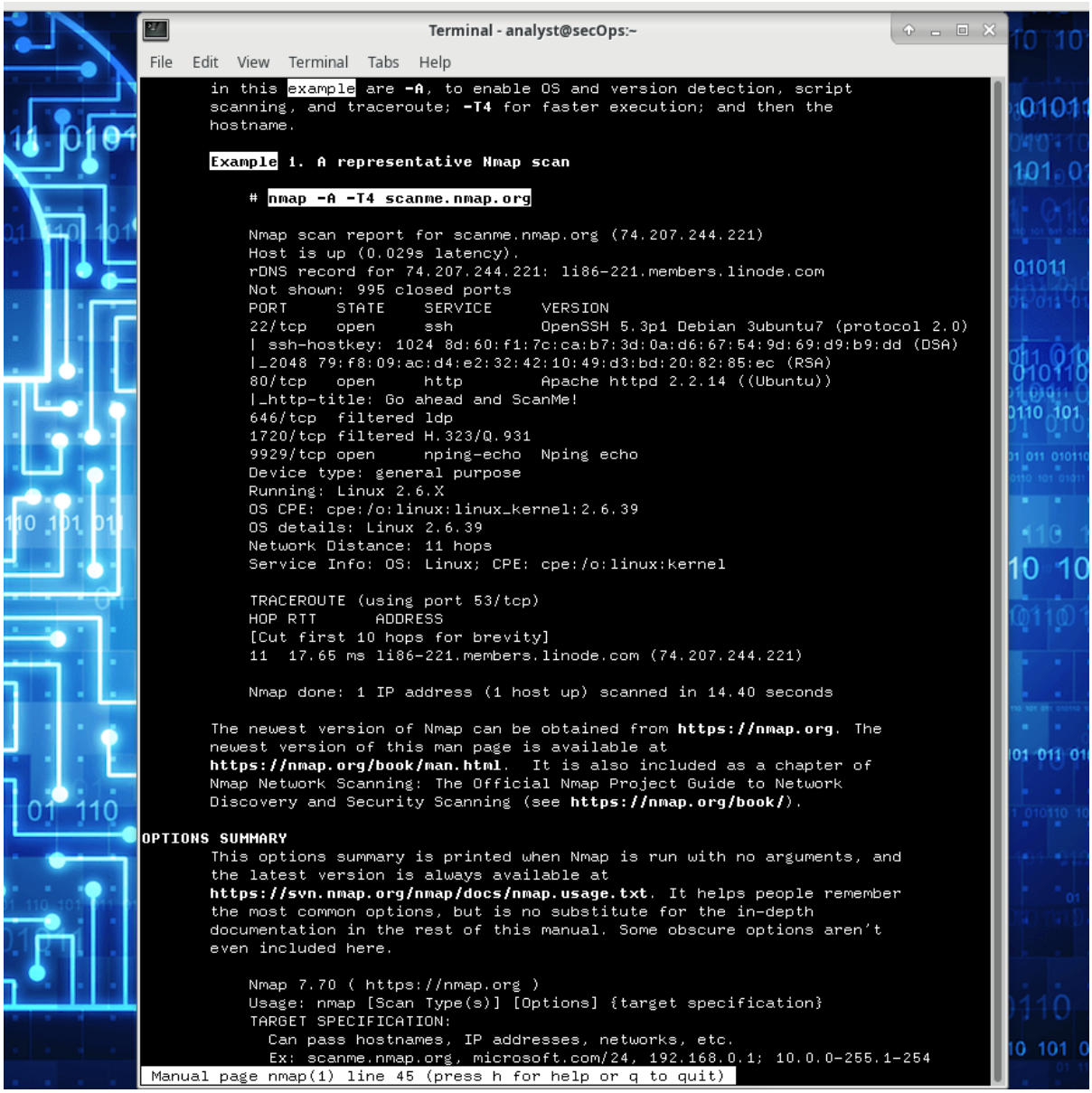
Cos'è Nmap? Per cosa viene usato nmap?

Nmap è uno strumento open source utilizzato per eseguire la scansione e l'analisi di reti informatiche. Il suo nome deriva da "Network Mapper" e viene ampiamente impiegato da amministratori di sistema, analisti di sicurezza e penetration tester per raccogliere informazioni su host e dispositivi presenti in una rete.

Il suo scopo principale è identificare quali dispositivi sono attivi su una rete, quali porte risultano aperte su ciascun host, quali servizi stanno girando su quelle porte e, in molti casi, anche quale sistema operativo è in uso. Nmap può essere usato per valutare il livello di esposizione di un sistema, verificare la configurazione di firewall e router, cercare vulnerabilità note tramite uno specifico motore di scripting integrato (NSE), e mappare reti complesse in modo efficiente.

Grazie alla sua versatilità, Nmap è considerato uno degli strumenti fondamentali per la sicurezza informatica, ma il suo utilizzo deve sempre essere autorizzato: analizzare reti senza permesso può rappresentare un reato.

Qual è il comando nmap usato?
nmap -A -T4 scanme.nmap.org



Cosa fa l'opzione -A?

```
  --no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
  -6: Enable IPv6 scanning
  -A: Enable OS detection, version detection, script scanning, and traceroute
  --datadir <dirname>: Specify custom Nmap data file location
  --send-eth/--send-ip: Send using raw ethernet frames or IP packets
  --privileged: Assume that the user is fully privileged
```

Quando utilizziamo l'opzione -A in Nmap, attiviamo una serie di funzionalità avanzate che ci permettono di ottenere informazioni dettagliate su un host. Con questo comando, Nmap esegue il rilevamento del sistema operativo, identifica i servizi attivi sulle porte aperte specificando nome, versione e tipo di software, analizza la presenza di firewall o sistemi di filtraggio, e avvia alcuni script del motore NSE per individuare eventuali vulnerabilità o comportamenti sospetti. In pratica, otteniamo una

panoramica completa e approfondita della macchina che stiamo analizzando, molto utile soprattutto nei contesti di sicurezza informatica e penetration testing.

Cosa fa l'opzione -T4?

```
   TIMING AND PERFORMANCE:
     Options which take <time> are in seconds, or append 'ms' (milliseconds),
     's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).
     -T<0-5>: Set timing template (higher is faster)
     --min-hostgroup/max-hostgroup <size>: Parallel host scan group sizes
     --min-parallelism/max-parallelism <numprobes>: Probe parallelization
     --min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>: Specifies
```

L'opzione -T4, invece, ci consente di regolare la velocità della scansione. Nmap ci offre diversi livelli di rapidità, dalle modalità lente e silenziose a quelle più aggressive e veloci. Con -T4 scegliamo un livello piuttosto veloce ma ancora stabile, adatto a situazioni in cui non è necessario passare inosservati, come nei test di laboratorio o nelle reti interne.

Quando lanciamo una scansione con `nmap -A -T4`, chiediamo quindi a Nmap di eseguire un'analisi dettagliata e completa, ottenendo molte informazioni utili in un tempo relativamente breve.

Quali porte e servizi sono aperti?

```
Terminal - analyst@secOps:~
File  Edit  View  Terminal  Tabs  Help
[analyst@secOps ~]$ man nmap

[analyst@secOps ~]$ man nmap
[analyst@secOps ~]$ nmap -A -T4 localhost
Starting Nmap 7.70 ( https://nmap.org ) at 2025-06-13 05:35 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000024s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0        0               0 Mar 26  2018 ftp_test
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 127.0.0.1
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 2
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh     OpenSSH 7.7 (protocol 2.0)
| ssh-hostkey:
|   2048 b4:91:f9:f9:d6:79:25:86:44:c7:9e:f8:e0:e7:5b:bb (RSA)
|   256 06:12:75:fe:b3:89:29:4f:8d:f3:9e:9a:d7:c6:03:52 (ECDSA)
|_  256 34:5d:f2:d3:5b:9f:b4:b6:08:96:a7:30:52:8c:96:06 (ED25519)
Service Info: Host: Welcome

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.96 seconds
[analyst@secOps ~]$
```

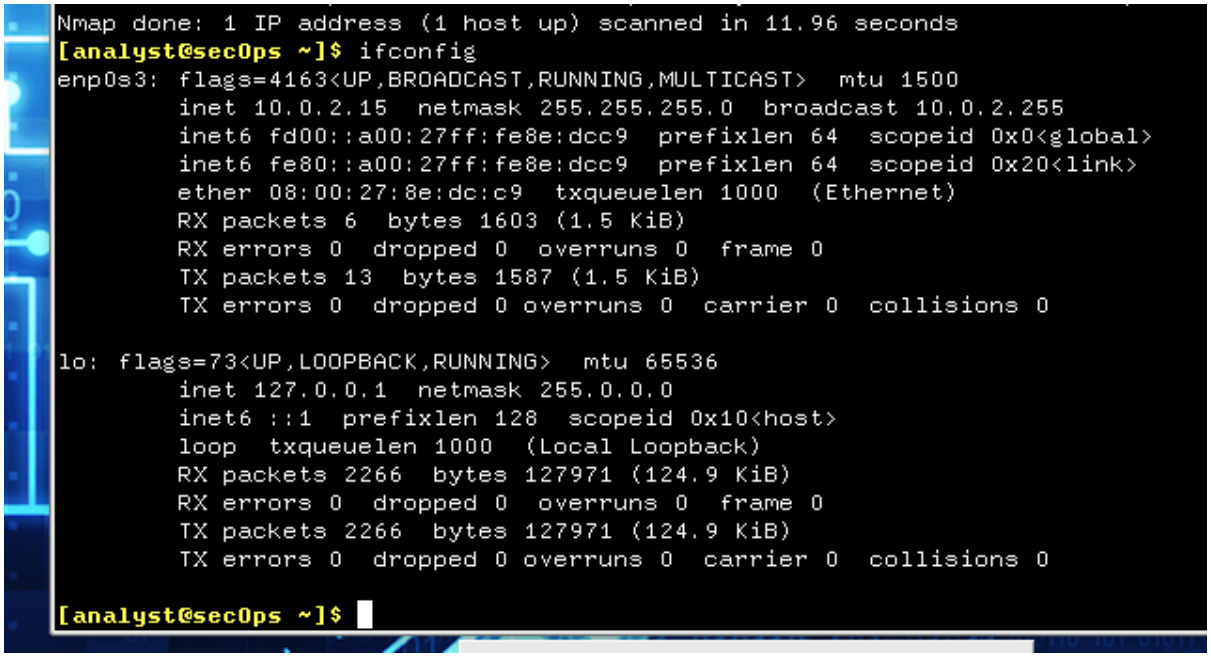
Nella scansione Nmap eseguita sull'indirizzo **localhost (127.0.0.1)**, sono state rilevate due porte aperte con i relativi servizi attivi.

La **porta 21/tcp** è aperta e offre il servizio **FTP**, gestito dal software **vsftpd** nella versione **3.0.3**. Questo servizio permette l'accesso anonimo (senza credenziali), come indicato dal messaggio "Anonymous FTP login allowed". Il server FTP è configurato per trasferimenti in modalità ASCII e non impone limiti di banda, mantenendo le connessioni in testo semplice (senza cifratura). Un file di test, chiamato **ftp_test**, è presente nella directory FTP, ma risulta vuoto (0 byte) e risale al 26 marzo 2018.

La **porta 22/tcp** è aperta e ospita il servizio **SSH**, fornito da **OpenSSH 7.7** (utilizzando il protocollo 2.0). Sono stati registrati tre host key: una chiave RSA a 2048 bit, una ECDSA a 256 bit e una ED25519 a 256 bit. Queste chiavi sono utilizzate per autenticare il server e garantire connessioni sicure. L'hostname del server è identificato come "Welcome".

Entrambi i servizi (FTP e SSH) sono esposti localmente, ma la configurazione dell'FTP anonimo e l'uso di connessioni non cifrate per il trasferimento dei dati potrebbero rappresentare un rischio di sicurezza se accessibili da reti esterne. La presenza di OpenSSH, invece, indica un metodo più sicuro per l'accesso remoto, purché configurato con credenziali robuste e aggiornato per prevenire vulnerabilità note.

A quale rete appartiene la tua VM?



La tua macchina virtuale (VM) è collegata a una rete privata configurata con NAT (Network Address Translation), una tipologia comune negli ambienti virtualizzati come VirtualBox o VMware.

L'interfaccia di rete principale, denominata `enp0s3`, mostra un indirizzo IPv4 assegnato alla VM: **10.0.2.15**, con una subnet mask **255.255.255.0** e un indirizzo di broadcast **10.0.2.255**. Questa configurazione indica che la VM fa parte della subnet **10.0.2.0/24**, un range di indirizzi riservato proprio alle reti NAT di VirtualBox. In questa modalità, la VM condivide l'accesso a Internet attraverso l'host fisico ma rimane isolata dalla rete locale fisica, rendendola non direttamente raggiungibile dall'esterno senza configurazioni aggiuntive come il port forwarding.

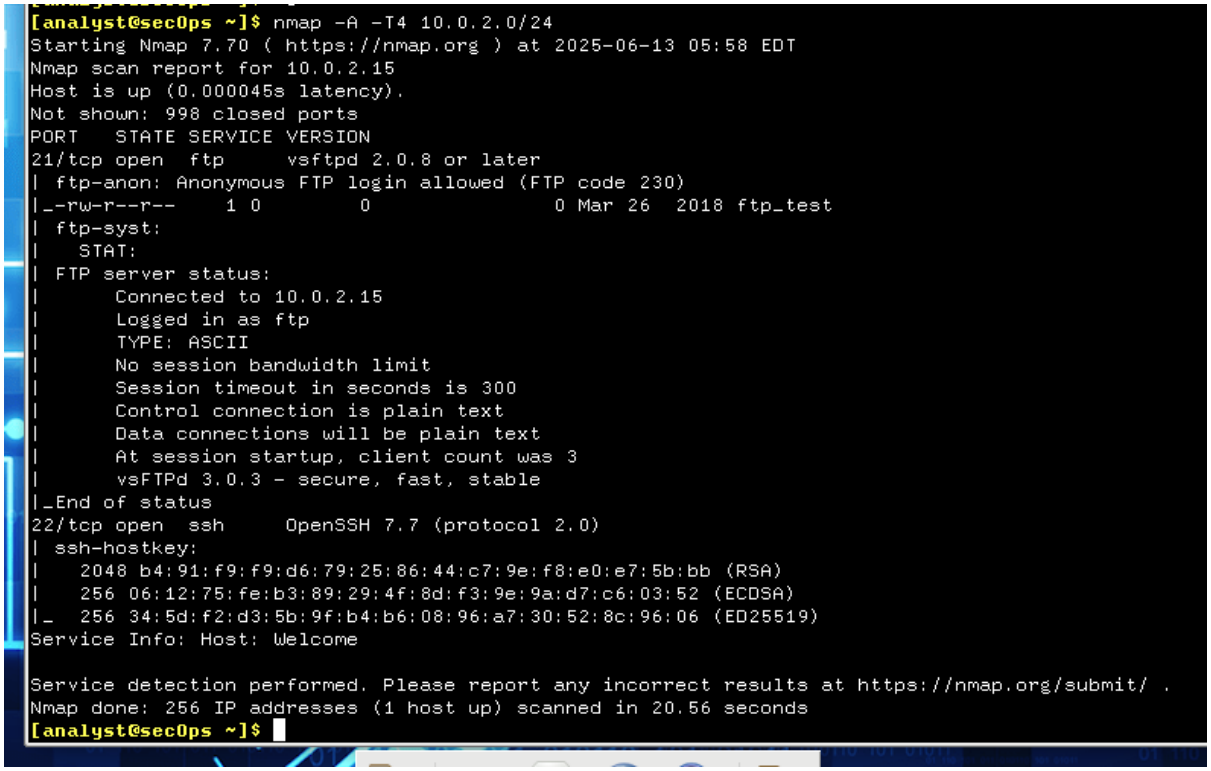
L'indirizzo MAC associato all'interfaccia, **08:00:27:8e:dc:e9**, inizia con il prefisso **08:00:27**, che identifica VirtualBox come vendor, confermando l'ambiente virtualizzato. L'MTU (Maximum Transmission Unit) è impostato al valore standard di 1500 byte, tipico per le connessioni Ethernet.

L'interfaccia di loopback (`lo`) è configurata con gli indirizzi locali classici: **127.0.0.1** per IPv4 e **::1** per IPv6, utilizzati per le comunicazioni interne alla VM stessa.

Per modificare il comportamento di rete della VM, ad esempio per renderla visibile ad altri dispositivi nella tua LAN, potresti cambiare la modalità della scheda di rete da **NAT** a **Bridged** (ponte) o **Host-only**, a seconda delle tue esigenze. La modalità Bridged assegnerebbe alla VM un indirizzo IP nella stessa rete del tuo host fisico, mentre la modalità Host-only creerebbe una rete isolata tra l'host e le VM.

In sintesi, la tua VM attualmente opera in una rete NAT privata (10.0.2.0/24), ideale per test isolati o sviluppo, ma con limitazioni nell'accessibilità esterna senza ulteriori configurazioni.

Quanti host sono attivi?



Dall'analisi della scansione Nmap eseguita sulla rete 10.0.2.0/24, emerge che nella sottorete è attivo un solo host. L'indirizzo IP rilevato è 10.0.2.15, che corrisponde alla tua macchina virtuale. Questo host presenta due servizi attivi: un server FTP sulla porta 21 e un server SSH sulla porta 22.

Il servizio FTP risulta essere gestito da vsftpd nella versione 3.0.3 e permette l'accesso anonimo, come dimostrato dalla presenza del file ftp_test e dalla configurazione che consente login senza credenziali. Il server SSH, invece, utilizza OpenSSH 7.7 ed è configurato con diverse chiavi crittografiche per garantire connessioni sicure.

La scansione ha coperto l'intero range di indirizzi della subnet, da 10.0.2.0 a 10.0.2.255, ma nessun altro dispositivo ha risposto ai probe di Nmap. Questo conferma che la rete NAT è attualmente isolata e contiene soltanto la tua macchina virtuale. L'assenza di altri host potrebbe dipendere dalla configurazione di rete scelta per la VM, che in questo caso è la modalità NAT predefinita di VirtualBox, oppure dalla presenza di firewall o filtri di rete che impediscono la comunicazione con altri eventuali dispositivi.

Dai risultati di Nmap, elenca gli indirizzi IP degli host che si trovano sulla stessa LAN della tua VM. Elenca alcuni dei servizi disponibili sugli host rilevati.

La scansione attuale mostra solo la tua VM (10.0.2.15) con servizi FTP e SSH attivi, suggerendo che la rete 10.0.2.0/24 sia dedicata esclusivamente a questo host virtuale. Per rilevare altri dispositivi nella tua LAN reale, sarebbe necessario modificare le

impostazioni di rete della VM ed eseguire una nuova scansione su un range IP appropriato.

Qual è lo scopo di questo sito?

Il sito **scanme.nmap.org** è un servizio pubblico e ufficiale offerto dal team di **Nmap** (in particolare dalla società **Insecure.org**, che sviluppa Nmap). Il suo **scopo principale** è fornire **un bersaglio legittimo e autorizzato su cui testare Nmap** e imparare a usarlo senza violare la legge o scansionare sistemi senza permesso.

Quando si impara a usare Nmap o altri strumenti di scansione di rete, è importante avere un sistema reale da analizzare. Tuttavia, scansionare dispositivi su Internet senza il consenso del proprietario può essere illegale o considerato un attacco. Per questo motivo, il team di Nmap ha messo a disposizione **scanme.nmap.org**, che chiunque può scansionare liberamente **per scopi didattici e di test**, a patto di non esagerare.

In breve:

- scanme.nmap.org è un server messo online appositamente per essere scansionato.
- È utile per esercitarsi con Nmap in modo legale e sicuro.
- È autorizzato solo per test leggeri, quindi non bisogna sovraccaricarlo o lanciare attacchi aggressivi (come brute force o DoS).

Se vuoi, posso aiutarti a fare una scansione base o avanzata di questo host per vedere cosa si scopre.

Quali porte e servizi sono aperti?

Quali porte e servizi sono filtrati?

Qual è l'indirizzo IP del server?

Qual è il sistema operativo?

Porte e servizi aperti:

Sul server **scanme.nmap.org (45.33.32.156)** sono state rilevate quattro porte aperte:

- **22/tcp**: Servizio SSH (OpenSSH 6.6.1) su Ubuntu, con supporto per chiavi crittografiche DSA, RSA, ECDSA e ED25519.
- **80/tcp**: Server HTTP (Apache 2.4.7) sempre su Ubuntu, che ospita una pagina web con il titolo "Go ahead and ScanMe!".
- **9929/tcp**: Servizio "nping-echo", utilizzato per test di connettività.
- **31337/tcp**: Porta aperta ma con servizio "tcpwrapped", indicando che è protetta da un firewall o non offre servizi accessibili.

Porte filtrate:

996 porte sono risultate **filtrate**, il che significa che Nmap non ha ricevuto risposta, probabilmente a causa di regole firewall che bloccano le richieste.

Indirizzo IP del server:

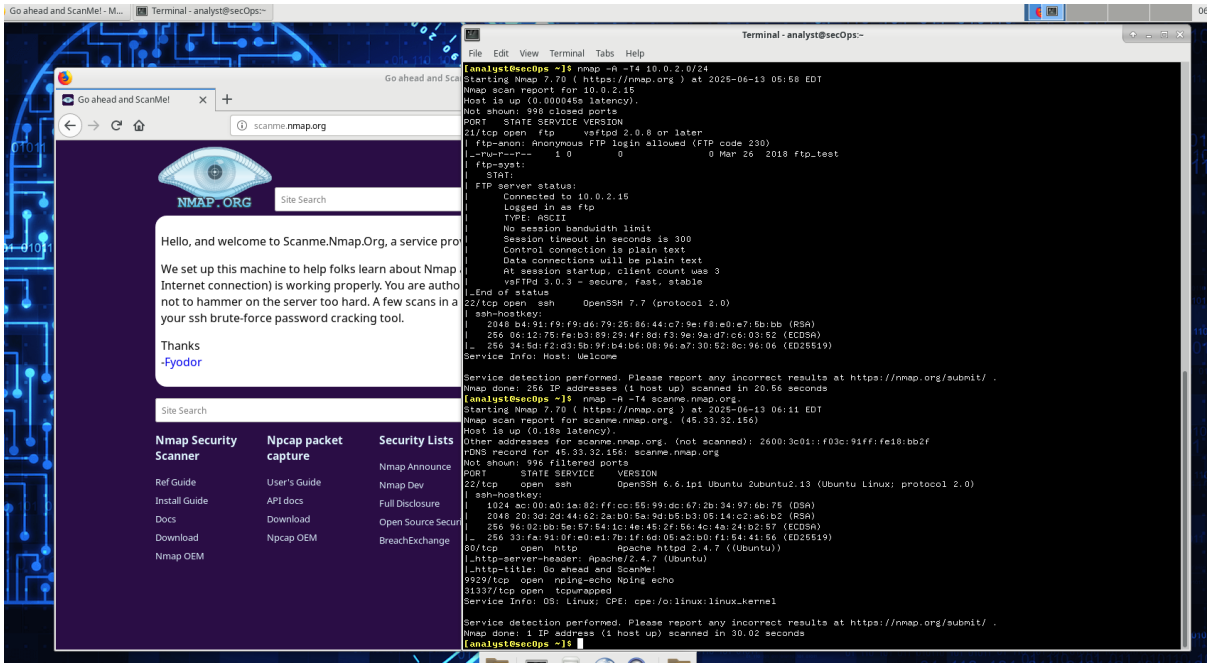
L'IP pubblico del server è **45.33.32.156** (scanme.nmap.org), con un indirizzo IPv6 associato non analizzato (2600:3c01::f03c:91ff:fe18:bb2f).

Sistema operativo:

Il server utilizza **Ubuntu Linux**, come indicato dalle versioni di OpenSSH e Apache, confermato anche dal campo "Service Info" che riporta l'OS Linux e il CPE (cpe:/o:linux:linux_kernel).

Sintesi:

Il server, gestito da Nmap per scopi dimostrativi, espone servizi SSH e HTTP su Ubuntu, con due porte aggiuntive (9929 e 31337) a scopo tecnico/didattico. La maggior parte delle porte è filtrata, tipico di un sistema configurato per minimizzare l'esposizione a scansioni esterne.



Nmap è uno strumento estremamente utile per la sicurezza della rete perché consente di identificare rapidamente quali dispositivi sono attivi su una rete, quali porte sono aperte e quali servizi sono in esecuzione. Queste informazioni permettono agli amministratori di sistema di avere una visione chiara e aggiornata dell'infrastruttura, individuando potenziali punti deboli, come porte inutilmente aperte o servizi obsoleti. Inoltre, grazie al suo motore di scripting, è possibile automatizzare la ricerca di vulnerabilità note, semplificando le attività di auditing e conformità. Nmap aiuta anche nella rilevazione di sistemi non autorizzati, nella verifica di configurazioni firewall e nella valutazione del livello di esposizione verso l'esterno, tutti aspetti fondamentali per costruire e mantenere una rete sicura.

Tuttavia, la stessa potenza che rende Nmap uno strumento prezioso per la difesa può essere sfruttata anche in modo malevolo. Un attaccante, per esempio, può usarlo come primo passo in una fase di ricognizione, per raccogliere informazioni dettagliate sugli host di una rete target. Sapendo quali servizi sono in esecuzione, quali porte sono aperte e quali sistemi operativi sono presenti, un attore malevolo può pianificare attacchi mirati, sfruttando vulnerabilità note o eseguendo exploit specifici. Inoltre, utilizzando tecniche di scansione stealth, può tentare di evitare i sistemi di rilevamento e aggirare le difese. Nmap, se usato senza autorizzazione, diventa quindi uno strumento potenzialmente pericoloso, capace di trasformare un'attività lecita di analisi in una minaccia concreta per la sicurezza informatica.