Settimana 9 Giorno 1

Report

Kali
WinXp

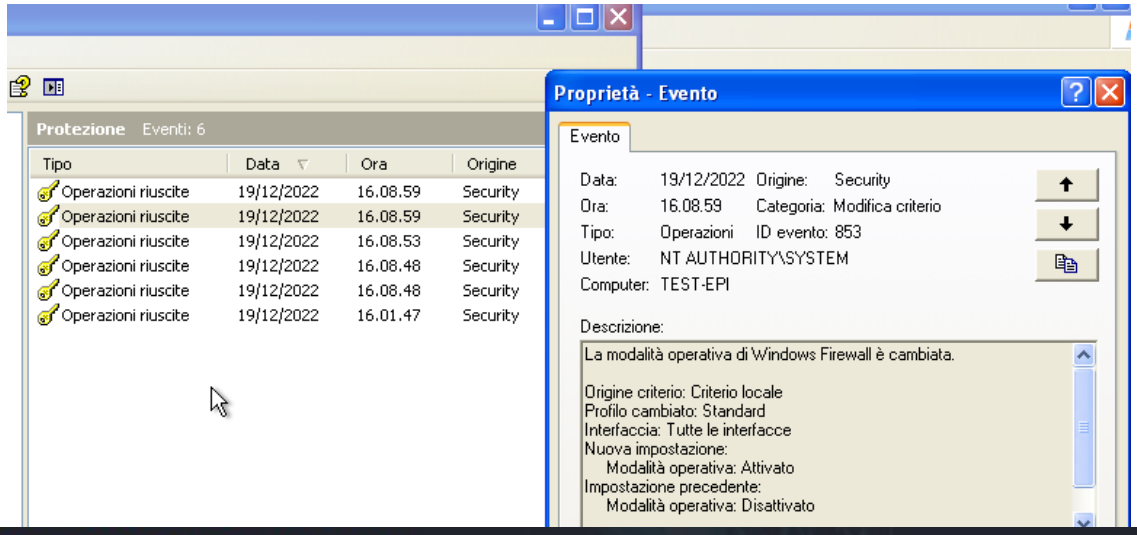
Obbiettivo: Scansionare WinXp con Nmap da Kali con Firewall abilitato e disabilitato, per vedere le differenze; Bonus: monitorare i log di Windows

nota: Ho usato PFSense per velocizzare la scansione per quanto le VM comunicano meglio se in reti diverse.

Nmap, Firewall: OFF

```
┌──(filip㉿KaLinux)-[~/Desktop]
└─$ nmap -sV 192.168.1.150
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-19 10:16 EST
Nmap scan report for 192.168.1.150
Host is up (0.0012s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.40 seconds
```

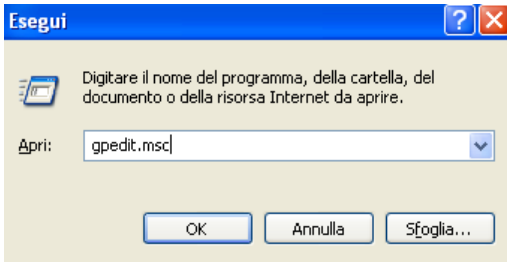
Nmap, Firewall: ON

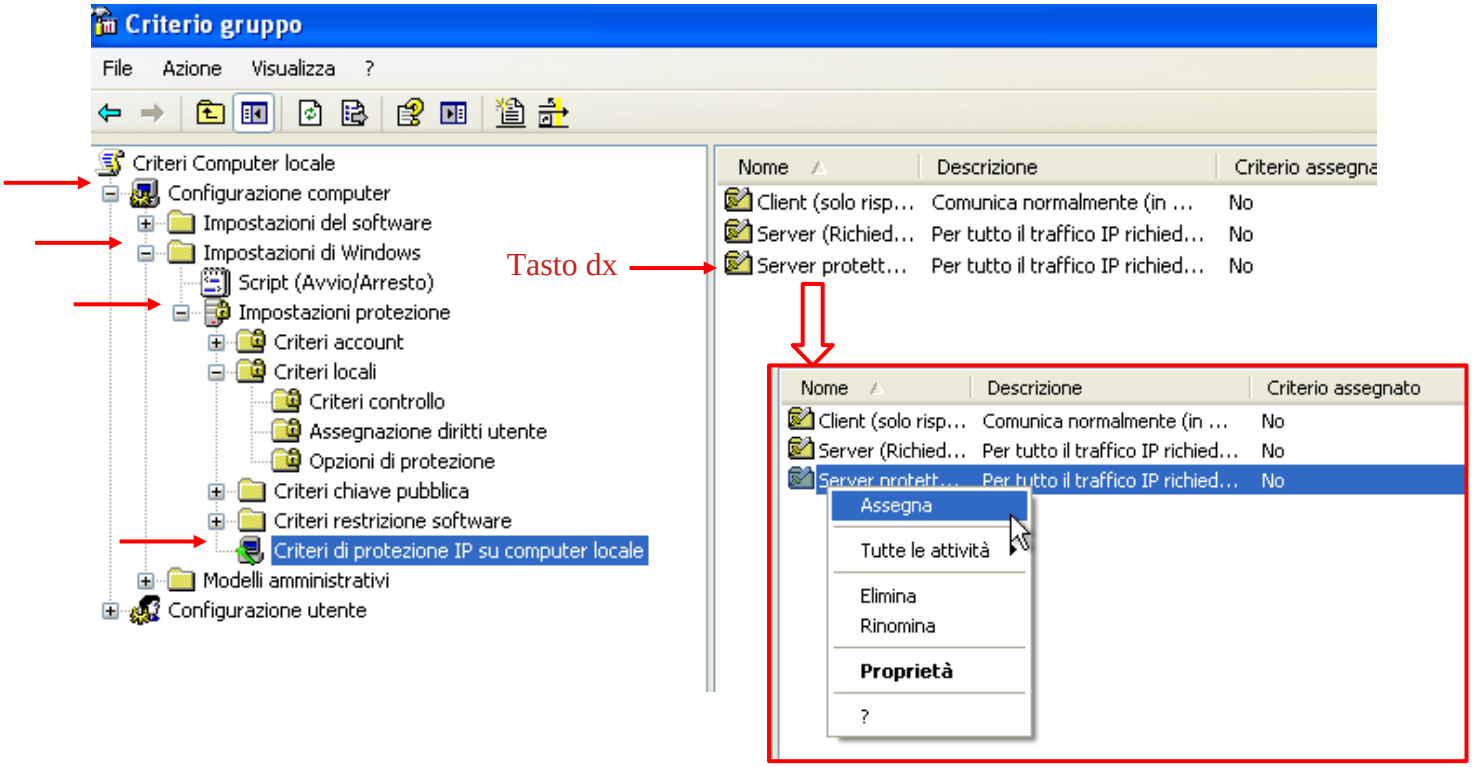



```
┌──(filip㉿KaLinux)-[~/Desktop]
└─$ nmap -sV 192.168.1.150
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-19 10:18 EST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.23 seconds

┌──(filip㉿KaLinux)-[~/Desktop]
└─$
```

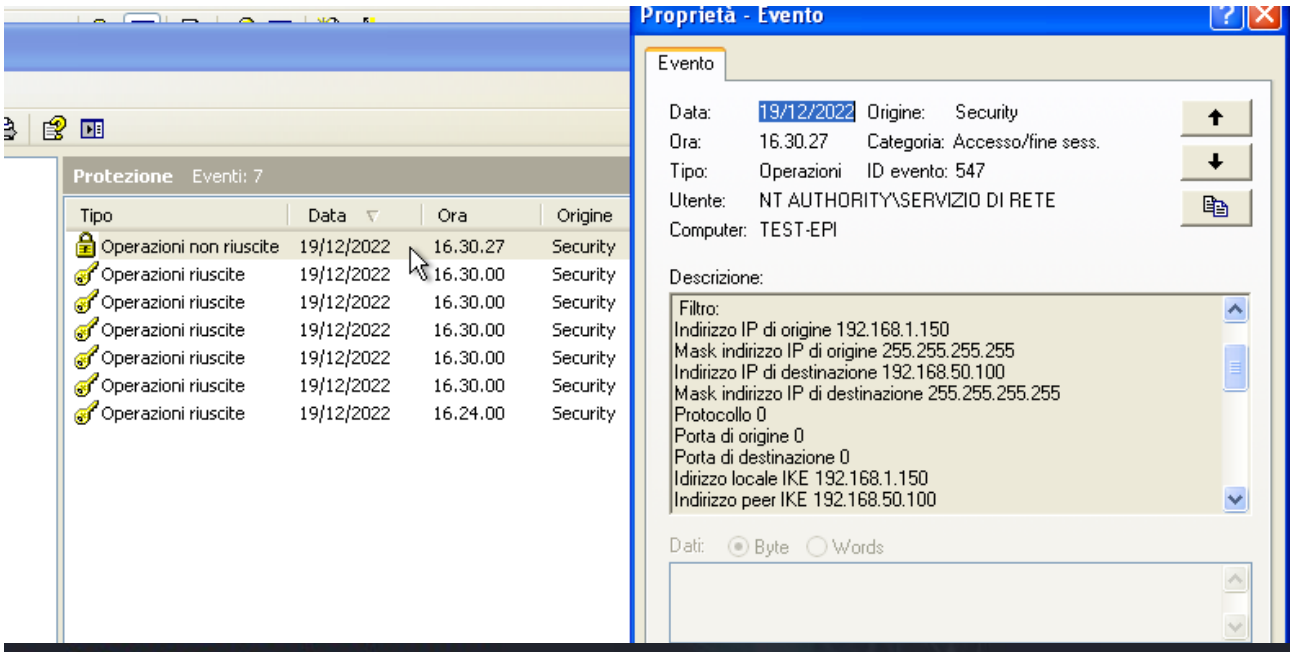
WinXP:

Sulla tastiera premiamo insieme **Win.Key+R** e scriviamo ***gpedit.msc***





Risultato:




```
┌──(filip㉿KaLinux)-[~/Desktop]
└─$ nmap -sV 192.168.1.150
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-19 10:40 EST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.19 seconds

┌──(filip㉿KaLinux)-[~/Desktop]
└─$
```

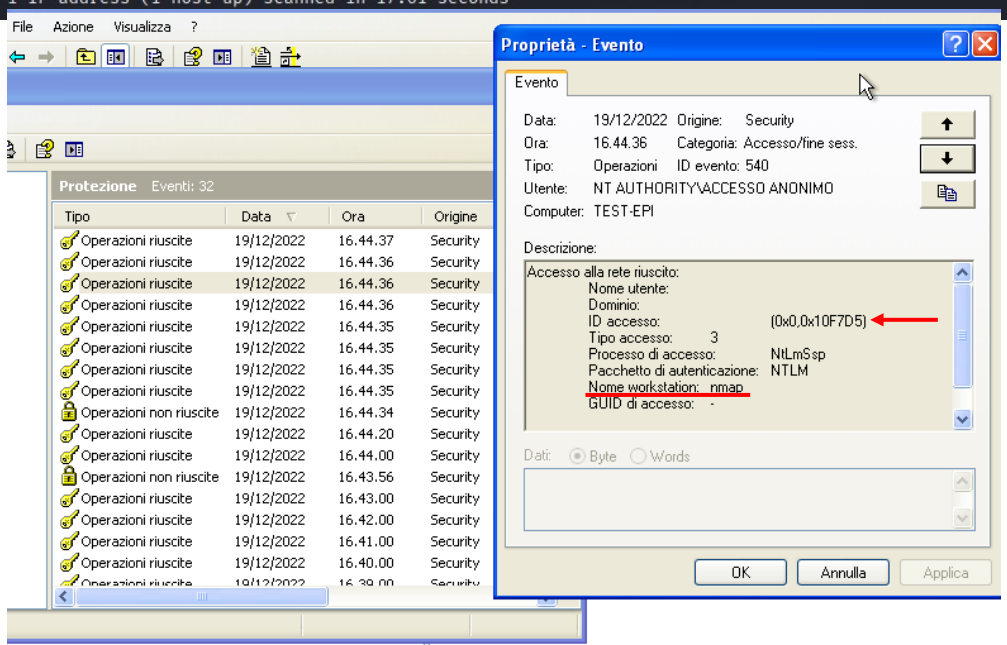
System logs alone are rarely sufficient for detecting port scans. Usually only scan types that establish full TCP connections are logged, while the default Nmap SYN scan sneaks through. Even full TCP connections are only logged if the particular application explicitly does so. Such error messages, when available, are often cryptic. However, a bunch of different services spouting error messages at the same time is a common indicator of scanning activity. Intrusive scans, particularly those using Nmap version detection, can often be detected this way. But only if the administrators actually read the system logs regularly. The vast majority of log messages go forever unread. Log monitoring tools such as Logwatch and Swatch can certainly help, but the reality is that system logs are only marginally effective at detecting Nmap activity.

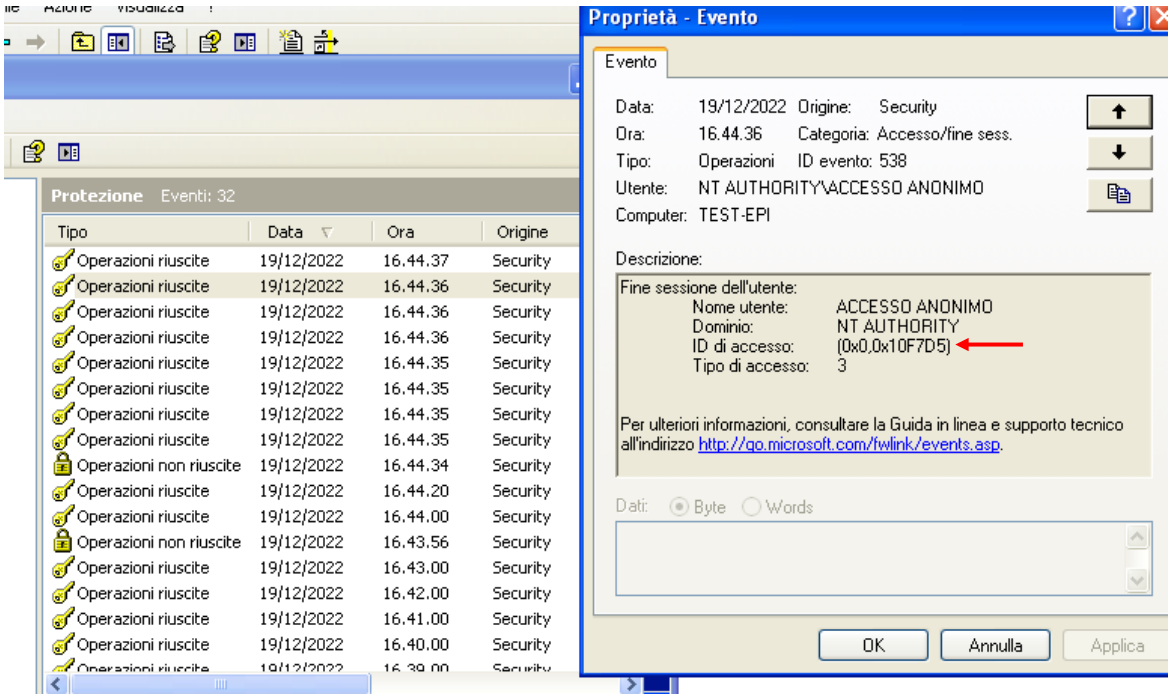
Special purpose port scan detectors are a more effective approach to detecting Nmap activity. Two common examples are PortSentry and Scanlogd. Scanlogd has been around since 1998 and was carefully designed for security. No vulnerabilities have been reported during its lifetime. PortSentry offers similar features, as well as a reactive capability that blocks the source IP of suspected scanners.

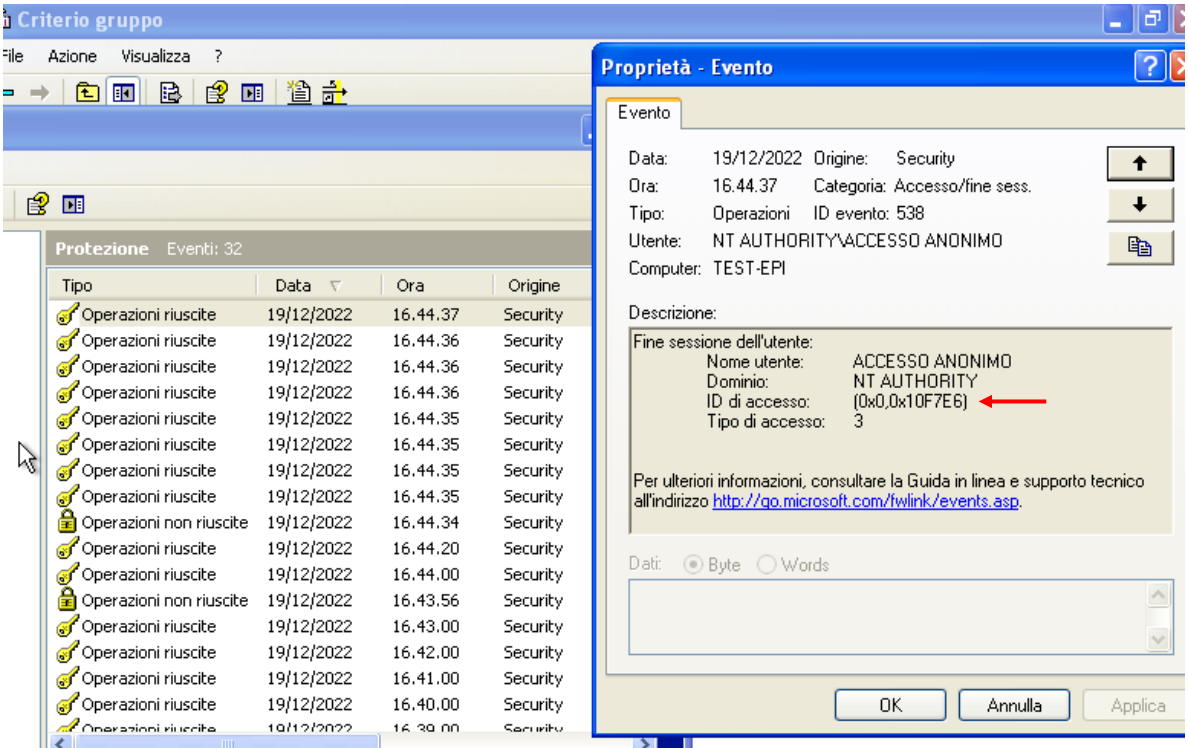
Source: *https://nmap.org/book/nmap-defenses-detection.html*

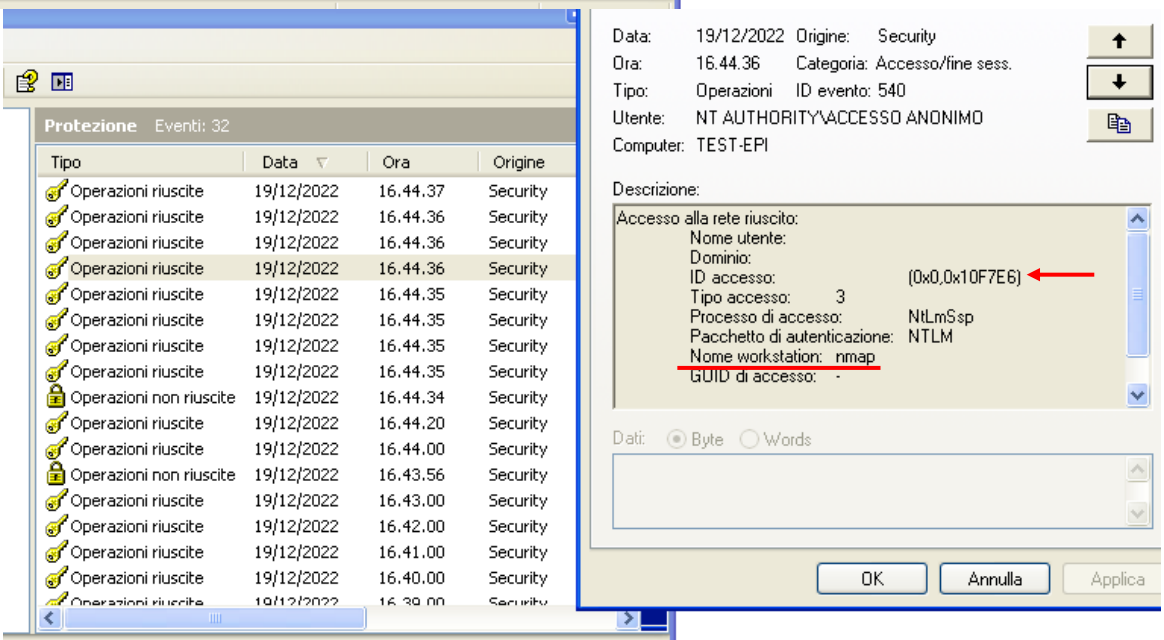
prova

```
┌──(filip㉿KaLinux)-[~/Desktop]
└─$ nmap -A 192.168.1.150
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-19 10:54 EST
Nmap scan report for 192.168.1.150
Host is up (0.0014s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Windows XP microsoft-ds
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Host script results:
|_nbstat: NetBIOS name: TEST-EPI, NetBIOS user: <unknown>, NetBIOS MAC: 08002748a44a (Oracle VirtualBox virtual NIC)
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: test-epi
|   NetBIOS computer name: TEST-EPI\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2022-12-19T16:44:34+01:00
|_clock-skew: mean: -39m33s, deviation: 42m24s, median: -1h09m33s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.61 seconds
```

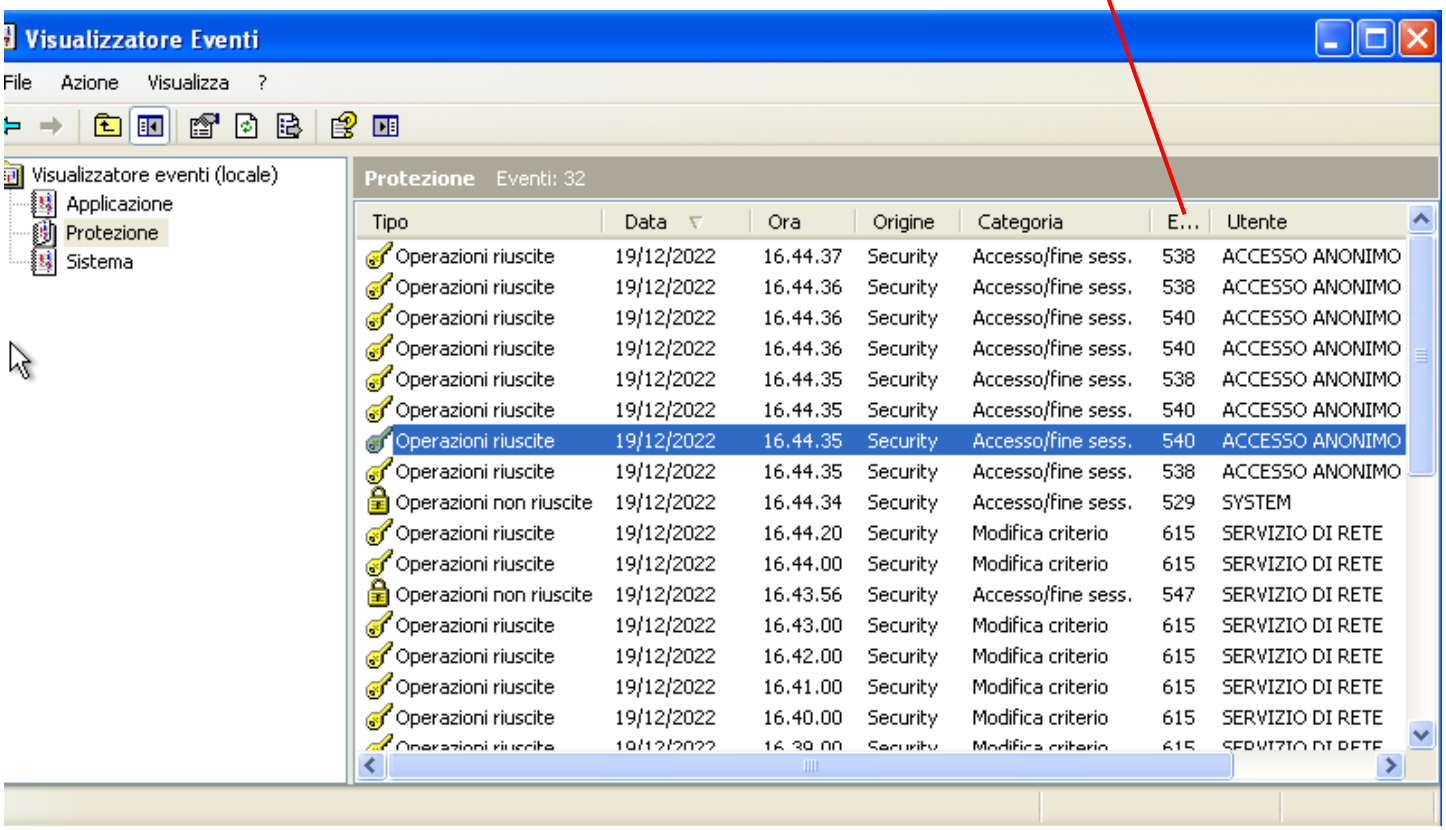



Proprietà - Evento
Evento
Data: 19/12/2022 Origine: Security
Ora: 16.44.36 Categoria: Accesso/fine sess.
Tipo: Operazioni ID evento: 538
Utente: NT AUTHORITY\ACCESSO ANONIMO
Computer: TEST-EPI
Descrizione:
Fine sessione dell'utente:
Nome utente: ACCESSO ANONIMO
Dominio: NT AUTHORITY
ID di accesso: (0x0,0x10F7D5)
Tipo di accesso: 3
Per ulteriori informazioni, consultare la Guida in linea e supporto tecnico all'indirizzo http://go.microsoft.com/fwlink/events.asp.
Dati: Byte Words
OK
Annulla
Applica
Protezione Eventi: 32
Tipo Data Ora Origine
Operazioni riuscite 19/12/2022 16.44.37 Security
Operazioni riuscite 19/12/2022 16.44.36 Security
Operazioni riuscite 19/12/2022 16.44.36 Security
Operazioni riuscite 19/12/2022 16.44.36 Security
Operazioni riuscite 19/12/2022 16.44.35 Security
Operazioni riuscite 19/12/2022 16.44.35 Security
Operazioni riuscite 19/12/2022 16.44.35 Security
Operazioni riuscite 19/12/2022 16.44.35 Security
Operazioni non riuscite 19/12/2022 16.44.34 Security
Operazioni riuscite 19/12/2022 16.44.20 Security
Operazioni riuscite 19/12/2022 16.44.00 Security
Operazioni non riuscite 19/12/2022 16.43.56 Security
Operazioni riuscite 19/12/2022 16.43.00 Security
Operazioni riuscite 19/12/2022 16.42.00 Security
Operazioni riuscite 19/12/2022 16.41.00 Security
Operazioni riuscite 19/12/2022 16.40.00 Security


Criterio gruppo
File Azione Visualizza ?
Proprietà - Evento
Evento
Data: 19/12/2022 Origine: Security
Ora: 16.44.37 Categoria: Accesso/fine sess.
Tipo: Operazioni ID evento: 538
Utente: NT AUTHORITY\ACCESSO ANONIMO
Computer: TEST-EPI
Descrizione:
Fine sessione dell'utente:
Nome utente: ACCESSO ANONIMO
Dominio: NT AUTHORITY
ID di accesso: (0x0,0x10F7E6)
Tipo di accesso: 3
Per ulteriori informazioni, consultare la Guida in linea e supporto tecnico all'indirizzo http://go.microsoft.com/fwlink/events.asp.
Dati: Byte Words
OK
Annulla
Applica
Protezione Eventi: 32
Tipo Data Ora Origine
Operazioni riuscite 19/12/2022 16.44.37 Security
Operazioni riuscite 19/12/2022 16.44.36 Security
Operazioni riuscite 19/12/2022 16.44.36 Security
Operazioni riuscite 19/12/2022 16.44.36 Security
Operazioni riuscite 19/12/2022 16.44.35 Security
Operazioni riuscite 19/12/2022 16.44.35 Security
Operazioni riuscite 19/12/2022 16.44.35 Security
Operazioni riuscite 19/12/2022 16.44.35 Security
Operazioni non riuscite 19/12/2022 16.44.34 Security
Operazioni riuscite 19/12/2022 16.44.20 Security
Operazioni riuscite 19/12/2022 16.44.00 Security
Operazioni non riuscite 19/12/2022 16.43.56 Security
Operazioni riuscite 19/12/2022 16.43.00 Security
Operazioni riuscite 19/12/2022 16.42.00 Security
Operazioni riuscite 19/12/2022 16.41.00 Security
Operazioni riuscite 19/12/2022 16.40.00 Security


Data: 19/12/2022 Origine: Security
Ora: 16.44.36 Categoria: Accesso/fine sess.
Tipo: Operazioni ID evento: 540
Utente: NT AUTHORITY\ACCESSO ANONIMO
Computer: TEST-EPI
Descrizione:
Accesso alla rete riuscito:
Nome utente:
Dominio:
ID accesso: (0x0,0x10F7E6)
Tipo accesso: 3
Processo di accesso: NtLmSsp
Pacchetto di autenticazione: NTLM
Nome workstation: nmap
GUID di accesso: -
Dati: Byte Words
OK
Annulla
Applica
Protezione Eventi: 32
Tipo Data Ora Origine
Operazioni riuscite 19/12/2022 16.44.37 Security
Operazioni riuscite 19/12/2022 16.44.36 Security
Operazioni riuscite 19/12/2022 16.44.36 Security
Operazioni riuscite 19/12/2022 16.44.36 Security
Operazioni riuscite 19/12/2022 16.44.35 Security
Operazioni riuscite 19/12/2022 16.44.35 Security
Operazioni riuscite 19/12/2022 16.44.35 Security
Operazioni riuscite 19/12/2022 16.44.35 Security
Operazioni non riuscite 19/12/2022 16.44.34 Security
Operazioni riuscite 19/12/2022 16.44.20 Security
Operazioni riuscite 19/12/2022 16.44.00 Security
Operazioni non riuscite 19/12/2022 16.43.56 Security
Operazioni riuscite 19/12/2022 16.43.00 Security
Operazioni riuscite 19/12/2022 16.42.00 Security
Operazioni riuscite 19/12/2022 16.41.00 Security
Operazioni riuscite 19/12/2022 16.40.00 Security

EVENTO



Tipo	Data	Ora	Origine	Categoria	E...	Utente
Operazioni riuscite	19/12/2022	16.44.37	Security	Accesso/fine sess.	538	ACCESSO ANONIMO
Operazioni riuscite	19/12/2022	16.44.36	Security	Accesso/fine sess.	538	ACCESSO ANONIMO
Operazioni riuscite	19/12/2022	16.44.36	Security	Accesso/fine sess.	540	ACCESSO ANONIMO
Operazioni riuscite	19/12/2022	16.44.36	Security	Accesso/fine sess.	540	ACCESSO ANONIMO
Operazioni riuscite	19/12/2022	16.44.35	Security	Accesso/fine sess.	538	ACCESSO ANONIMO
Operazioni riuscite	19/12/2022	16.44.35	Security	Accesso/fine sess.	540	ACCESSO ANONIMO
Operazioni riuscite	19/12/2022	16.44.35	Security	Accesso/fine sess.	540	ACCESSO ANONIMO
Operazioni riuscite	19/12/2022	16.44.35	Security	Accesso/fine sess.	538	ACCESSO ANONIMO
Operazioni non riuscite	19/12/2022	16.44.34	Security	Accesso/fine sess.	529	SYSTEM
Operazioni riuscite	19/12/2022	16.44.20	Security	Modifica criterio	615	SERVIZIO DI RETE
Operazioni riuscite	19/12/2022	16.44.00	Security	Modifica criterio	615	SERVIZIO DI RETE
Operazioni non riuscite	19/12/2022	16.43.56	Security	Accesso/fine sess.	547	SERVIZIO DI RETE
Operazioni riuscite	19/12/2022	16.43.00	Security	Modifica criterio	615	SERVIZIO DI RETE
Operazioni riuscite	19/12/2022	16.42.00	Security	Modifica criterio	615	SERVIZIO DI RETE
Operazioni riuscite	19/12/2022	16.41.00	Security	Modifica criterio	615	SERVIZIO DI RETE
Operazioni riuscite	19/12/2022	16.40.00	Security	Modifica criterio	615	SERVIZIO DI RETE
Operazioni riuscite	19/12/2022	16.39.00	Security	Modifica criterio	615	SERVIZIO DI RETE

Filip. S