Traccia:

Durante la lezione teorica, abbiamo studiato le azioni preventive per ridurre la possibilità di attacchi provenienti dall'esterno. Abbiamo visto che a livello di rete, possiamo attivare / configurare Firewall e regole per fare in modo che un determinato traffico, potenzialmente dannoso, venga bloccato.

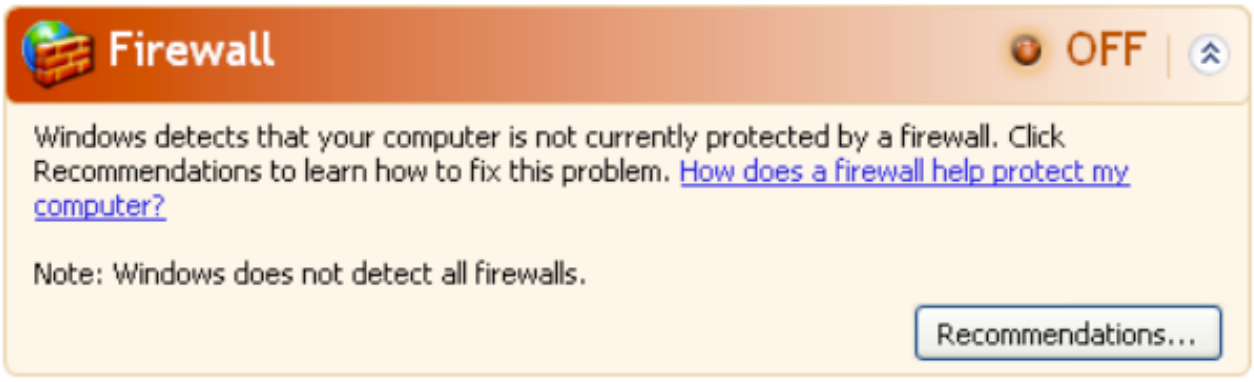
La macchina Windows XP in formato OVA che abbiamo utilizzato nella Unit 2 ha di default il Firewall disabilitato.

L'esercizio di oggi è verificare in che modo l'attivazione del Firewall impatta il risultato di una scansione dei servizi dall'esterno. Per questo motivo:

1. Assicuratevi che il Firewall sia disattivato sulla macchina Windows XP
2. Effettuate una scansione con nmap sulla macchina target (utilizzate lo switch –sV, per la service detection e -o nomefilereport per salvare in un file l'output)
3. Abilitare il Firewall sulla macchina Windows XP
4. Effettuate una seconda scansione con nmap, utilizzando ancora una volta lo switch –sV.

Svolgimento:

Firewall disabilitato sulla macchina Windows XP

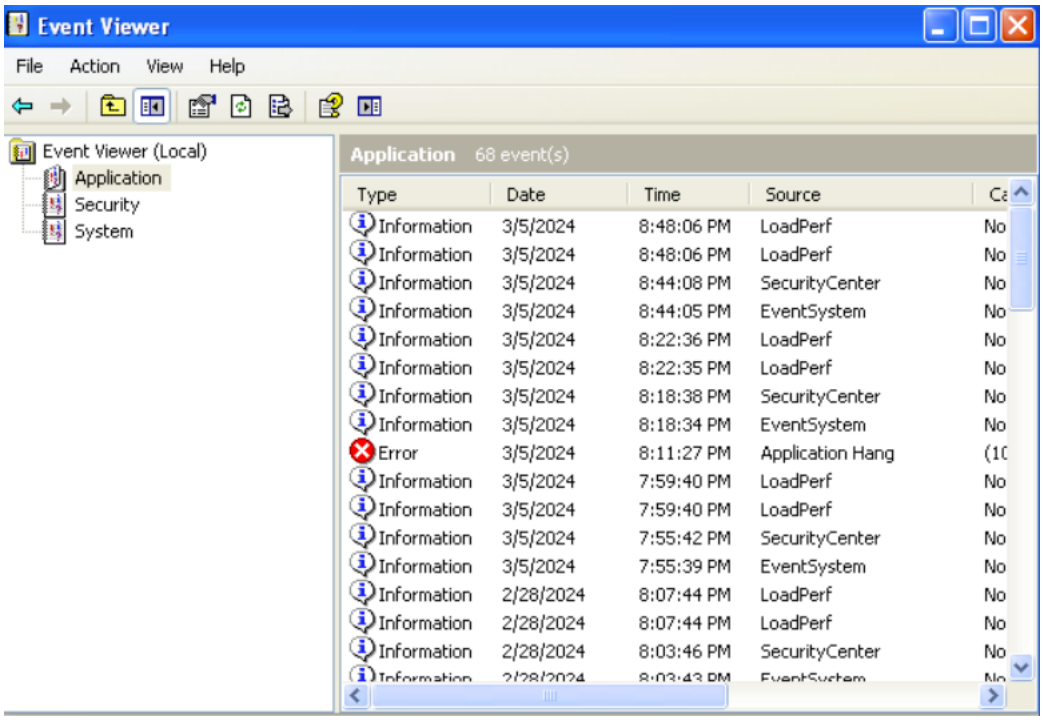


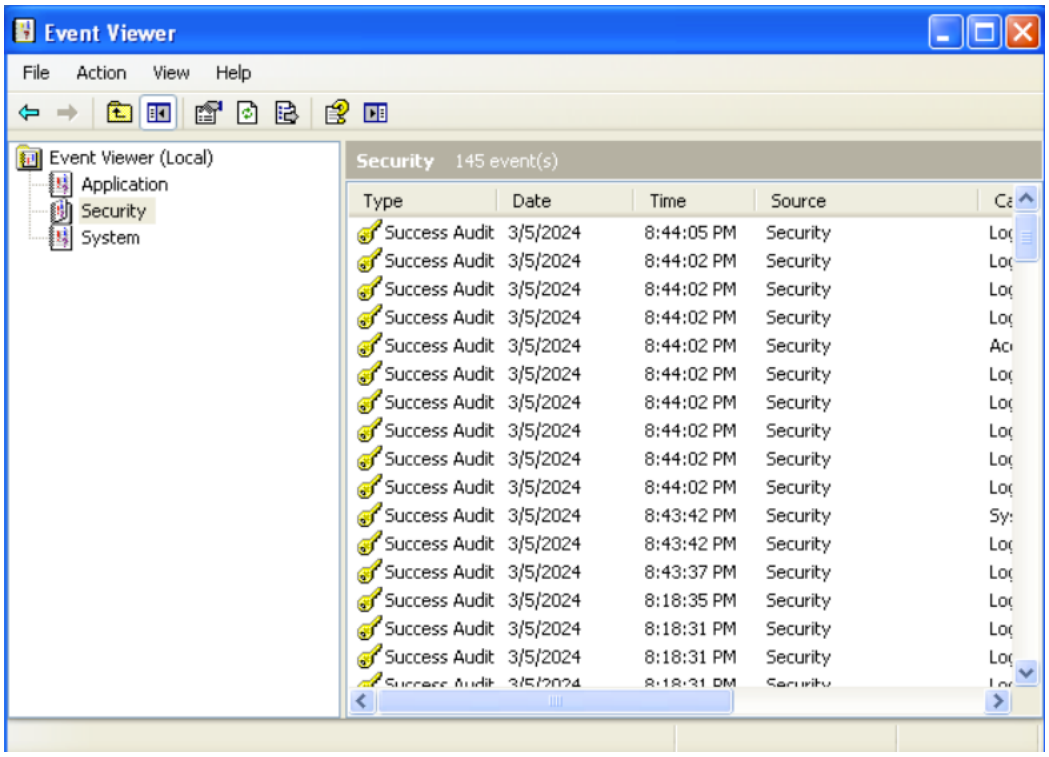
Scansione nmap con switch -sV sulla macchina target Windows XP

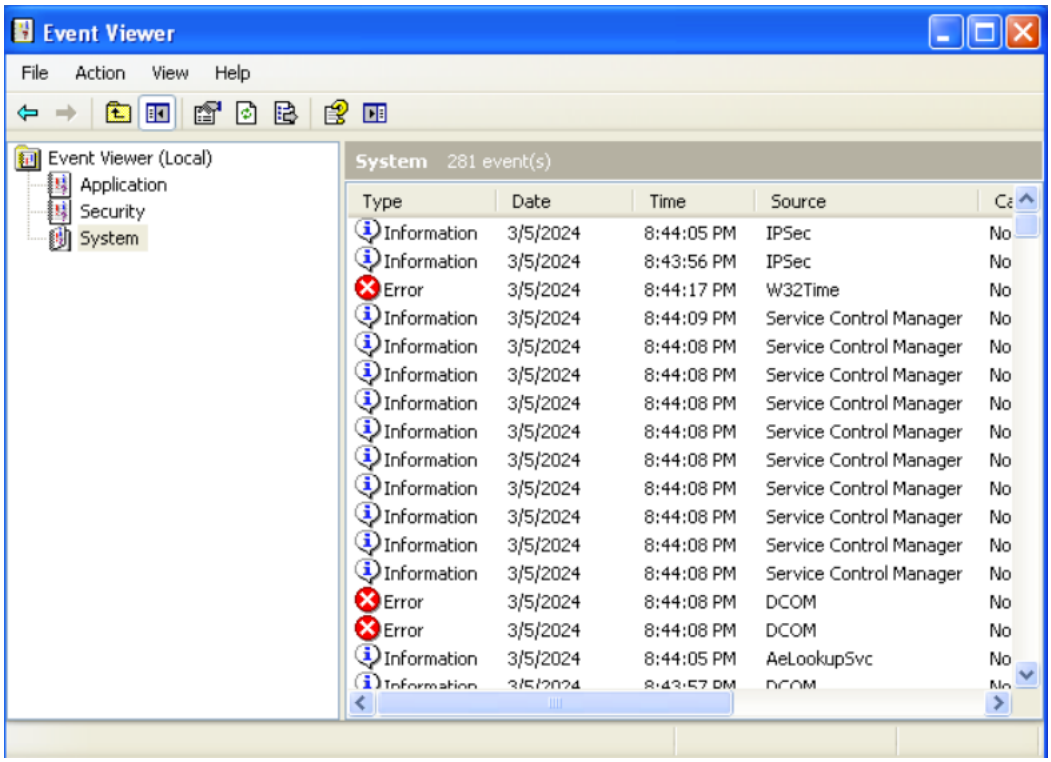
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.11.119
Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-05 14:30 EST
Nmap scan report for 192.168.11.119
Host is up (0.0012s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT     STATE SERVICE      VERSION
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds Microsoft Windows Vista Embedded microsoft-ds (workgroup: WORKGROUP)
1026/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: WINDOWSXP; OS: Windows; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_vista

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 68.23 seconds
```

Cattura dei log con il tool messo a disposizione dal sistema operativo. Operazione andata a buom fine solo con firewall attivo




Event Viewer
File Action View Help
Event Viewer (Local)
Application
Security
System
Security 145 event(s)
Type Date Time Source Ca
Success Audit 3/5/2024 8:44:05 PM Security Log
Success Audit 3/5/2024 8:44:02 PM Security Log
Success Audit 3/5/2024 8:44:02 PM Security Log
Success Audit 3/5/2024 8:44:02 PM Security Log
Success Audit 3/5/2024 8:44:02 PM Security Ac
Success Audit 3/5/2024 8:44:02 PM Security Log
Success Audit 3/5/2024 8:44:02 PM Security Log
Success Audit 3/5/2024 8:44:02 PM Security Log
Success Audit 3/5/2024 8:44:02 PM Security Log
Success Audit 3/5/2024 8:44:02 PM Security Log
Success Audit 3/5/2024 8:43:42 PM Security Sy
Success Audit 3/5/2024 8:43:42 PM Security Log
Success Audit 3/5/2024 8:43:37 PM Security Log
Success Audit 3/5/2024 8:18:35 PM Security Log
Success Audit 3/5/2024 8:18:31 PM Security Log
Success Audit 3/5/2024 8:18:31 PM Security Log


Event Viewer
File Action View Help
Event Viewer (Local)
Application
Security
System
System 281 event(s)
Type Date Time Source Ca
Information 3/5/2024 8:44:05 PM IPSec No
Information 3/5/2024 8:43:56 PM IPSec No
Error 3/5/2024 8:44:17 PM W32Time No
Information 3/5/2024 8:44:09 PM Service Control Manager No
Information 3/5/2024 8:44:08 PM Service Control Manager No
Information 3/5/2024 8:44:08 PM Service Control Manager No
Information 3/5/2024 8:44:08 PM Service Control Manager No
Information 3/5/2024 8:44:08 PM Service Control Manager No
Information 3/5/2024 8:44:08 PM Service Control Manager No
Information 3/5/2024 8:44:08 PM Service Control Manager No
Information 3/5/2024 8:44:08 PM Service Control Manager No
Information 3/5/2024 8:44:08 PM Service Control Manager No
Information 3/5/2024 8:44:08 PM Service Control Manager No
Information 3/5/2024 8:44:08 PM Service Control Manager No
Error 3/5/2024 8:44:08 PM DCOM No
Error 3/5/2024 8:44:08 PM DCOM No
Information 3/5/2024 8:44:05 PM AeLookupSvc No