Security Operation: azioni preventive

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)
3. Abilitare il Firewall sulla macchina Windows XP
4. Effettuate una seconda scansione con nmap, utilizzando ancora una volta lo switch –sV.

Che differenze notate? E quale può essere la causa del risultato diverso?

Riferimenti teorici

La **sicurezza di un ambiente informatico** viene parametrata sulla base di «principi fondamentali». Uno dei principi cardine e più importanti per valutare lo stato della sicurezza delle informazioni di un dato ambiente è il «**CIA principle**», dove:

- C, sta per Confidentiality, ovvero la riservatezza del dato;
- I, sta per Integrity, ovvero l'integrità del dato;
- A, sta per Availability, ovvero la disponibilità del dato.

Generalmente, i controlli di sicurezza sono valutati in base al loro impatto sulle componenti del «CIA principle» (detto anche CIA triade).

RISERVATEZZA DEL DATO -> l'accesso al dato, che deve essere garantito solamente agli utenti autorizzati:
cifratura e le tecniche di controllo degli accessi.

INTEGRITA' DEL DATO -> proteggere l'affidabilità e la correttezza del dato e prevenire modifiche non autorizzate al dato:
meccanismi di controllo accessi ed autenticazione oltre a meccanismi di verifica degli hash, o checksum.
L'integrità del dato dipende dalla riservatezza del dato.

LA DISPONIBILITA' DEL DATO -> deve essere garantita in ogni momento e per i soli utenti autorizzati ad accedere alla risorsa in oggetto:
meccanismi di anti-denial of service, backup, ridondanza dell'infrastruttura, e tutte quelle altre misure di sicurezza che garantiscono la disponibilità dei servizi/dati in situazioni di criticità.

Riduzione del rischio: introducendo delle «security **remediation** action», ovvero delle azioni di rimedio per ridurre/eliminare il rischio.
Accettazione del rischio: accettando il rischio residuo.
Rimozione del rischio: rimuovendo l'asset (laddove non critica) soggetta al rischio.

Come la «Security operation» interviene sugli asset per la riduzione del rischio

Il **Security Operation Center (SOC)** è un sotto-dipartimento all'interno del dipartimento di Sicurezza che eroga servizi finalizzati alla protezione dei sistemi informatici, quali:

- **Servizi di gestione e manutenzione dell'infrastruttura IT** delle compagnie, come ad esempio, la manutenzione dei server, degli switch di rete, degli applicativi.
- **Servizi di monitoraggio e risposta** con lo scopo di individuare tempestivamente eventuali «minacce» (anche chiamate «**security threats**») ed in caso di attacco andato a buon fine, ha il compito di rispondere prontamente per limitare i danni. Al fine di settare gli strumenti e le configurazioni, è importante capire da quali tipi di minacce bisogna difendersi. Questa fase prende il nome di «**threat identification**». Minacce «avversarie»; Minacce «strutturali o infrastrutturali»; Minacce «ambientali»; Minacce «accidentali».
- **Rafforzamento della protezione dell'infrastruttura IT** con servizi proattivi come i Vulnerability Assessment o i Penetration test.

Un «**incidente di sicurezza**» si riferisce ad un evento che ha un impatto negativo sulla riservatezza, integrità o disponibilità di una data risorsa, come risultato di un attacco esterno oppure di un azione volutamente dannosa proveniente dall'interno e si includono anche gli eventi ambientali e accidentali (incidente). Ci sono **Azioni preventive** o **Azioni correttive e di risposta** agli incidenti.

Le minacce Cyber

Botnets: sono reti di computer dove un'entità centrale, che prende il nome di control-and-command server (CC server), invia istruzioni a una rete distribuita di computer, che prendono il nome di Zombie, precedentemente infettati tramite virus/malware. Lo scopo di una botnet è effettuare attacchi simultanei contro target in maniera centralizzata, causando impatti negativi sulla disponibilità dei servizi.
Denial-of-service (DoS): gli attacchi DoS hanno lo scopo di mettere fuori uso un servizio in esecuzione su un sistema, come potrebbe essere un'applicazione web o un sito web. Una delle forme più comune di attacco DoS è la trasmissione di un numero ingente di pacchetti ad un server al fine di saturare la CPU, dove si intende che la CPU è al 100% di utilizzo e non può di conseguenza processare altre richieste. La forma più comune di DoS è il **Distributed DoS (DDos)**, ovvero un attacco di tipo denial-of-service che viene inviato contemporaneamente verso un target da sorgenti multiple.
Zero-day Exploit: gli attacchi 0-day si riferiscono a tutti quegli attacchi che sfruttano per la prima volta una vulnerabilità ancora sconosciuta ad altri, ovvero una vulnerabilità non ancora nota. Gli exploit 0-day sono motivo ed oggetto di ricerca da parte di un numero elevato di ricercatori di sicurezza / penetration tester, che appunto testano un sistema per

scovare le vulnerabilità ancora non note prima che esse vengano sfruttate da malintenzionati.
Man-in-the-Middle: due tipi di attacchi MITM ->
1)lo sniffing, dove un attaccante riesce ad intercettare il traffico su un canale e ne legge il contenuto;
2) store-and-forward proxy, dove un attaccante riesce a posizionarsi nel mezzo di una comunicazione, ricevere il traffico dal mittente per poi spedirlo al destinatario. Il traffico viene processato dalla macchina dell'attaccante durante l'attacco.

Le azioni preventive

Le azioni preventive possono essere viste come l'insieme dei controlli di sicurezza che vengono adottati da una compagnia per aumentare il livello di **protezione perimetrale ed interna** al fine di ridurre il rischio di potenziali attacchi.

CONTROLLI NETWORK
NAC: network access control.
Firewall: Packet filtering firewall, Stateful inspection firewall, Next Generation Firewall (NGFW), Web Application Firewall.
Segmentazione di rete: DMZ, ovvero l'area della rete che espone i servizi accessibili da internet, Internal Network, ovvero l'area delle rete che ospita i server che erogano i servizi accessibili dall'interno.
IPS / IDS: i sistemi di prevenzione e rilevamento intrusioni servono ad individuare preventivamente potenziali attacchi alle reti ed alle macchine.

CONTROLLI SUGLI END-POINT (quali laptop, personal computer, smartphone o server)
Hardening dei sistemi e delle configurazioni: indica l'insieme delle azioni di configurazione di un sistema e dei suoi componenti che hanno lo scopo di migliorare la sicurezza complessiva. Tra queste attività ricadono attività come la disabilitazione di eventuali porte non utilizzate, la rimozione di utenti non necessari sui sistemi operativi, la riduzione dei privilegi degli utenti laddove non necessari. Un modo di rafforzare la sicurezza di un sistema mediante la sua **corretta configurazione.**
Patching dei sistemi: la «patch» indica un frammento di codice scritto per aggiornare o migliorare la sicurezza di un programma (rilasciata generalmente dal vendor). Il processo di implementazione della patch e di monitoraggio successivo viene detto «patch management».
Group policy: Le GPO (group policy object) infatti, permettono di applicare centralmente configurazioni standard per tutti i PC che sono all'interno di uno stesso workgroup, dominio, oppure di differenziare le configurazioni di sicurezza in base al ruolo della macchina.
Penetration testing: cicli e sessioni di PT sugli end-point per valutare il loro stato di sicurezza e coprire eventualmente le scoperture implementando le azioni di rimedio.

CONTROLLI SUL SOFTWARE (il software fa parte dell'asset della compagnia)
Code analysis: statica o dinamica.

Reverse engineering: «l'ingegneria inversa» è quell'insieme di tecniche e procedure che permettono di «risalire» al codice sorgente di un determinato software, utilizzando dei tool in base al linguaggio di programmazione utilizzato per scrivere il software stesso.

LOGGING E MONITORING
È quell'insieme di procedure e tecniche che permettono di tracciare tutte le azioni su un determinato sistema da parte degli utenti, come ad esempio il login, il logout, la modifica delle impostazioni ed altri eventi significativi.
Logging: le applicazioni, i servizi, i sistemi e gli altri asset infrastrutturali generano «log» di default, o hanno la possibilità di farlo se correttamente configurati. I «log» sono dei file contenenti gli eventi e le attività che si verificano su un dato sistema, che includono altri dati quali: la data e l'ora in cui l'evento si è verificato, l'utente che ha eseguito l'azione ed il sistema sul quale si è verificato l'evento. Log di sicurezza; Log di sistema; Log applicativi; Log dei Firewall -> spesso vengono inviati ad un sistema centralizzato chiamato **SIEM – Security information event management** («log collector»), che ha il compito di correlare le informazioni provenienti da diverse sorgenti ed automatizzare il monitoraggio.
Monitoring: si introduce il concetto di «accountability», ovvero di «responsabilità». Per aumentare i livelli di automatismo, spesso si implementano delle policy di sicurezza che in presenza di determinati eventi anomali fanno scattare degli «alert di sicurezza».

I **SIEM** sono generalmente costituiti da un'architettura Client-Server, dove la parte client è svolta da un «agent», ovvero un programma installabile su un end-point che permette la comunicazione e l'invio dei log dall'end-point al server centrale (SIEM). Hanno:
-la capacità di ricevere in ingresso i log da diverse sorgenti, estendendo la visibilità del SIEM su tutti gli asset aziendali
-la capacità di correlazione dei dati tra diverse fonti
-la capacità di monitoraggio real-time su tutti gli asset aziendali
-la possibilità di definire preventivamente degli alert configurabili

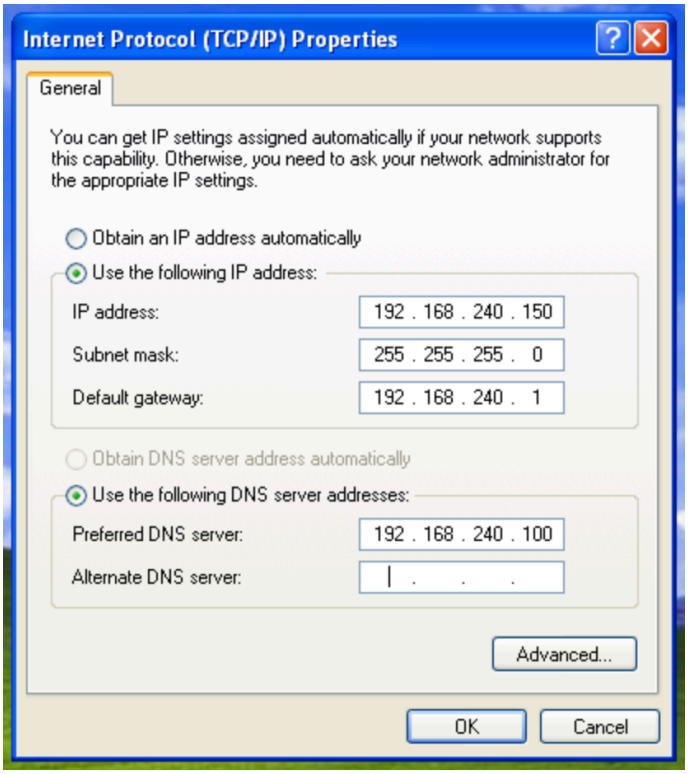
SOAR (Security orchestration, automation and response) può essere visto come un complemento ad un sistema SIEM. Mentre il SIEM si focalizza sul salvataggio ed il monitoraggio degli eventi di sicurezza, il SOAR aggiunge delle funzionalità di risposta automatica a determinati eventi, aggiungendo «workflow» (flussi di lavoro) complessi ed automatizzati. È composto da: gestore delle vulnerabilità e delle minacce, gestore delle risposte agli incidenti e gestore dell'automazione delle Security Operations.

PROCEDIMENTO

Per capire come ridurre la possibilità di attacchi provenienti dall'esterno, analizziamo la configurazione di un Firewall (attivo o disattivato). In questo caso utilizziamo la macchina Kali Linux, per la scansione delle porte e dei servizi, e la macchina Windows XP, per la configurazione del Firewall.

Requisiti:
-Configurate l'indirizzo di **Windows XP** come di seguito: **192.168.240.150**

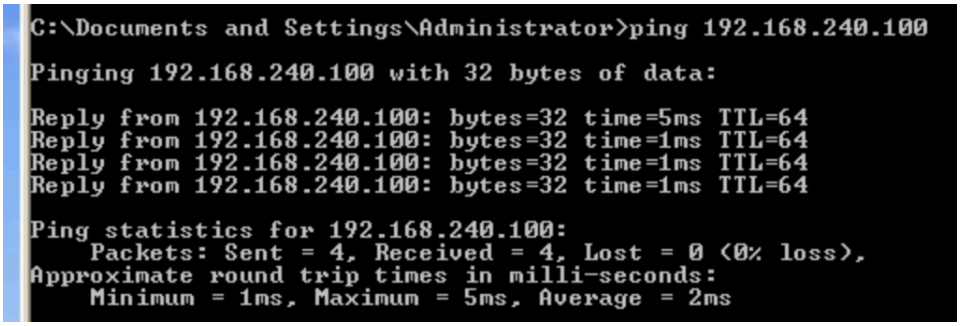
Start —> Control Panel —> Network and Internet Connections —> Network Connections —> tasto destro su "Local Area Connection" —> Properties —> Internet Protocol (TCP/IP) -> Properties -> modifica la configurazione e conferma con "OK"

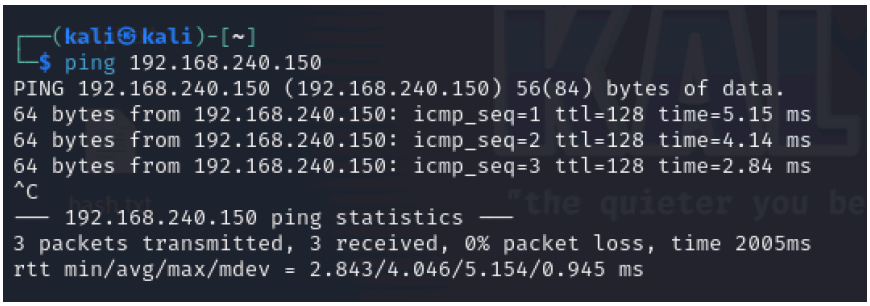


-Configurate l'indirizzo della macchina **Kali** come di seguito: **192.168.240.100**

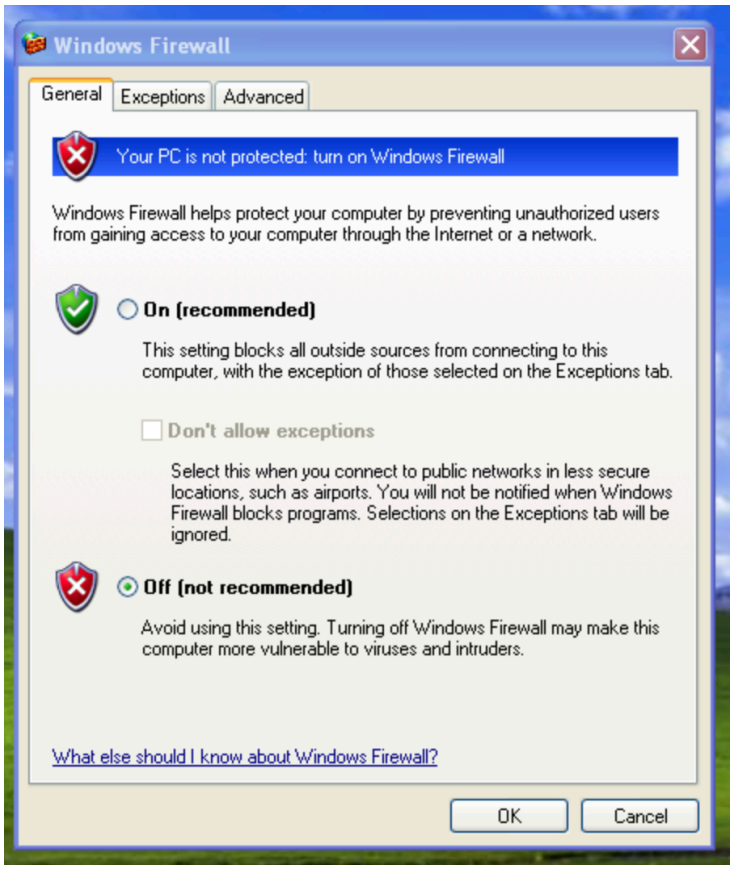
```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.240.100  netmask 255.255.255.0  broadcast 192.168.240.255
        inet6 fe80::a068:d8ff:feb3:868f  prefixlen 64  scopeid 0×20<link>
        ether a2:68:d8:b3:86:8f  txqueuelen 1000  (Ethernet)
        RX packets 6  bytes 728 (728.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 14  bytes 2286 (2.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Testiamo la connettività di rete fra le due macchine con il comando “**ping**” seguito dall’indirizzo **IP.**
Se il ping avviene con successo e quindi le macchine possono comunicare, procediamo.





-Windows Firewall DISATTIVATO: il Firewall è disattivato sulla macchina Windows XP



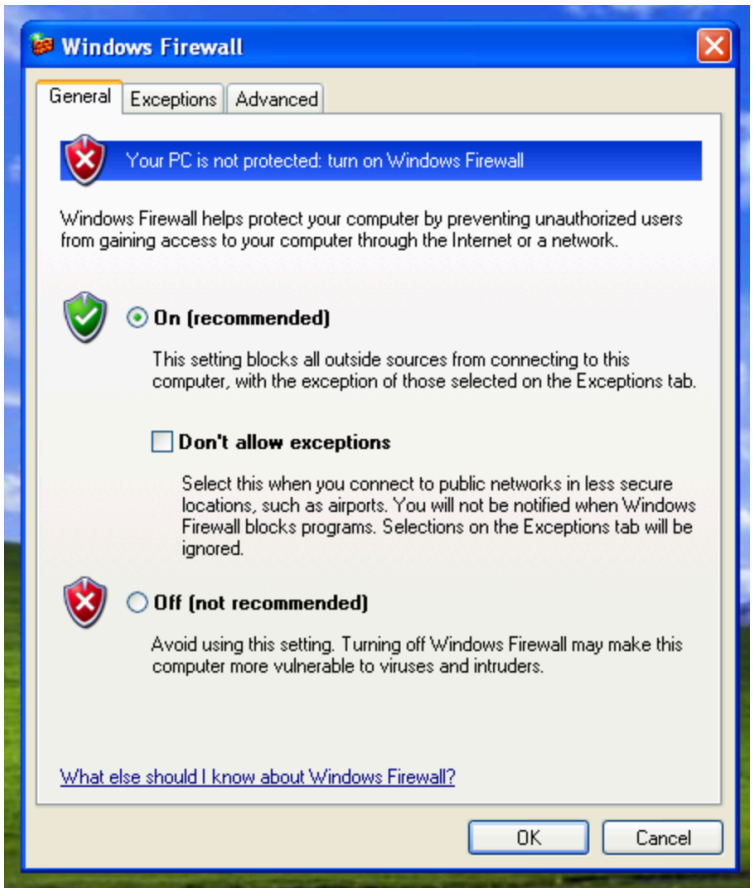
Scansione con nmap sulla macchina target (utilizzo lo switch –sV, per la service detection)

Nmap effettua una scansione delle porte sul dispositivo Windows XP, all'indirizzo IP 192.168.240.150, con individuazione dei servizi in esecuzione sulle porte e le rispettive versioni (-sV).

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-29 13:31 EST
Nmap scan report for 192.168.240.150
Host is up (0.0016s 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 7.44 seconds
```

Questa prima scansione ha rivelato che sono presenti **servizi attivi/in ascolto sulle porte 135, 139, 445**: tutte porte che utilizzano il protocollo TCP e utilizzano servizi di Microsoft. Sono in ascolto, rispettivamente, i servizi Microsoft Windows RPC, Microsoft Windows netbios-ssn e Microsoft Windows XP microsoft-ds (Directory Service) e sono presenti i sistemi operativi Windows e Windows XP.

Abilito il Firewall sulla macchina Windows XP



In che modo l'attivazione del Firewall impatta il risultato di una scansione dei servizi dall'esterno?

Effettuo una seconda scansione con nmap (utilizzo lo switch –sV)

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-29 13:45 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 3.09 seconds
```

Notiamo che la macchina o non è accesa oppure sta bloccando l'host discovery di nmap. L'output della scansione di Windows XP, all'IP 192.168.240.150, non restituisce più lo stato delle porte e i servizi ad esse associati in quanto l'**host sembra essere inattivo sulla rete.** In breve, si disabilita l'utility **ping** e questo significa che il firewall impedisce la risposta ai pacchetti di tipo ICMP Echo Request. **Il Firewall sta quindi bloccando il traffico in entrata con protocollo ICMP** (ping). È importante nascondere e disabilitare la risposta ai ping per la sicurezza o per la protezione ad esempio contro attacchi di ping flood.
Vediamo che il ping non ha più successo:

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.11.115
PING 192.168.11.115 (192.168.11.115) 56(84) bytes of data.
From 192.168.240.100 icmp_seq=1 Destination Host Unreachable
From 192.168.240.100 icmp_seq=2 Destination Host Unreachable
From 192.168.240.100 icmp_seq=3 Destination Host Unreachable
^C
── 192.168.11.115 ping statistics ──
6 packets transmitted, 0 received, +3 errors, 100% packet loss, time 5107ms
pipe 4
```

Ci consiglia quindi di provare con il parametro **–Pn.** Utilizzando questo switch, ignoriamo il ping e forziamo la scansione, passeremo direttamente alla scansione dei servizi (service discovery).
Con il comando "**nmap -Pn -sV 192-168.240.150**" si effettua quindi una scansione ipotizzando che Windows XP sia attivo.

```
┌──(kali㉿kali)-[~]
└─$ nmap -Pn -sV 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-29 13:50 EST
Nmap scan report for 192.168.240.150
Host is up.
All 1000 scanned ports on 192.168.240.150 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 201.80 seconds
```

L’output della scansione indica infatti che l'host è “up" (attivo) ma tutte le 1000 porte scansionate sono in uno stato “ignorato”, e vengono indicate come “filtered" e “no-response”.
Quindi nonostante l'host risponda ai sondaggi di ping, **il firewall impedisce la scansione e l’accesso alle porte, filtrandole**. **Una porta risulta filtrata quando lo scanner non riceve nessun segnale e nessuna risposta alle richieste** quindi in generale non si può dire con certezza se una porta filtrata sia aperta o chiusa.
Questa seconda scansione quindi non è andata a buon fine perchè **il Firewall di Windows XP ha una regola che blocca questo tipo di scansione da un Host non autorizzato.** In sostanza, l’host è attivo sulla rete ma è reso irraggiungibile dall’impostazione del Firewall che lo “blinda”. In questo modo un attaccante non avrà modo di individuare porte e servizi aperti da sfruttare per attaccare il bersaglio.

Conclusioni

L’abilitazione del Firewall di Windows XP blocca la scansione dei servizi attivi sulla macchina Windows XP dall’esterno. I servizi possono essere vulnerabili e in questo modo riusciamo a fare prevenzione riducendo i rischi di attacchi, in particolare nascondendo i servizi sulle porte 135,139,445 TCP.
Nmap tenta di effettuare l’host discovery, cioè inviare pacchetti con l’utility ping ma Windows XP non risponde ai pacchetti inviati e quindi nmap non può concludere la scansione delle porte e dei servizi. La prima differenza che si nota attivando il firewall da XP è quindi che viene bloccata la comunicazione del comando ping. Successivamente, Nmap lancia la scansione con -Pn e notiamo che l’host di destinazione è attivo ma che le porte scansionate hanno uno status che non è possibile identificare in quanto filtrate dal Firewall.
Con l’attivazione del Firewall abbiamo quindi eseguito un azione preventiva che ha bloccato la possibilità di effettuare la scansione dall’esterno. E quindi buona pratica attivare sempre un firewall per proteggersi.