Relazione Esercizio Scannerizzazioni con Nmap con e senza firewall

Traccia Esercizio:

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 che abbiamo utilizzato ha di default il Firewall disabilitato. L'e sercizio di oggi è verificare in che modo l'attivazione del Firewall impatta il risultato di una scansione dei servizi dall'esterno. Per questo motivo:

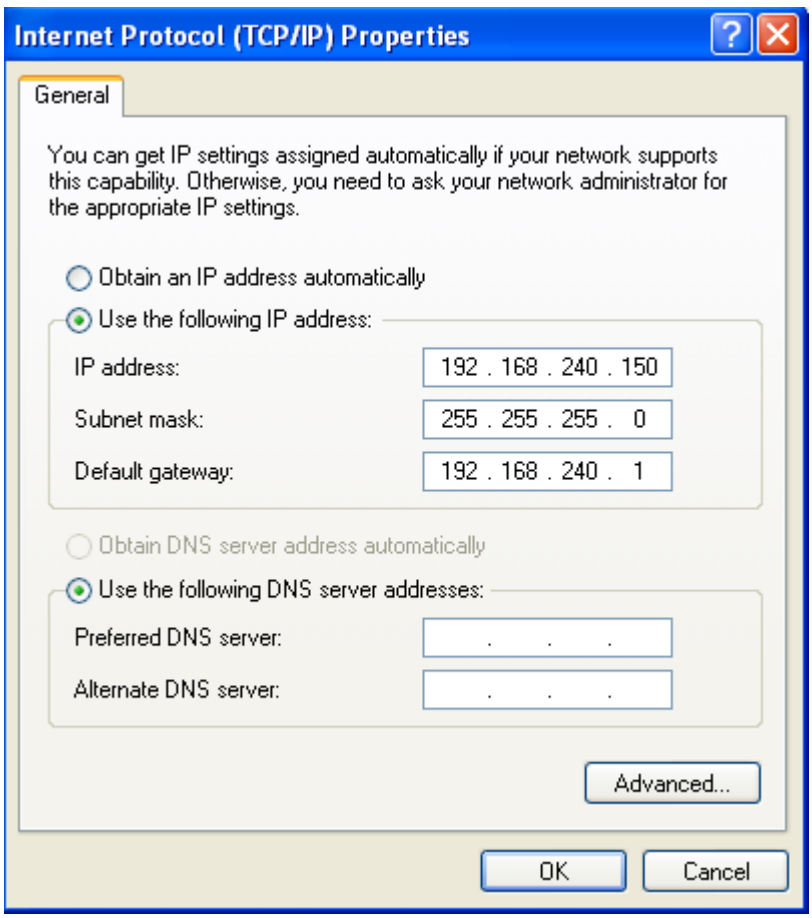
1. Assicuratevi che il Firewall sia disattivato sulla macchina Windows XP
2. Effettuate una scansione con nmap sulla macchina target (utilizzate lo switch–sV, per la service detection e -o nomefilereport per salvare in un file l'output)
3. Abilitare il Firewall sulla macchina Windows XP
4. Effettuate una seconda scansione con nmap, utilizzando ancora una volta lo switch–sV.
5. Provare eventuale scansione differente sempre con il firewall attivo
6. Trovare le eventuali differenze e motivarle.

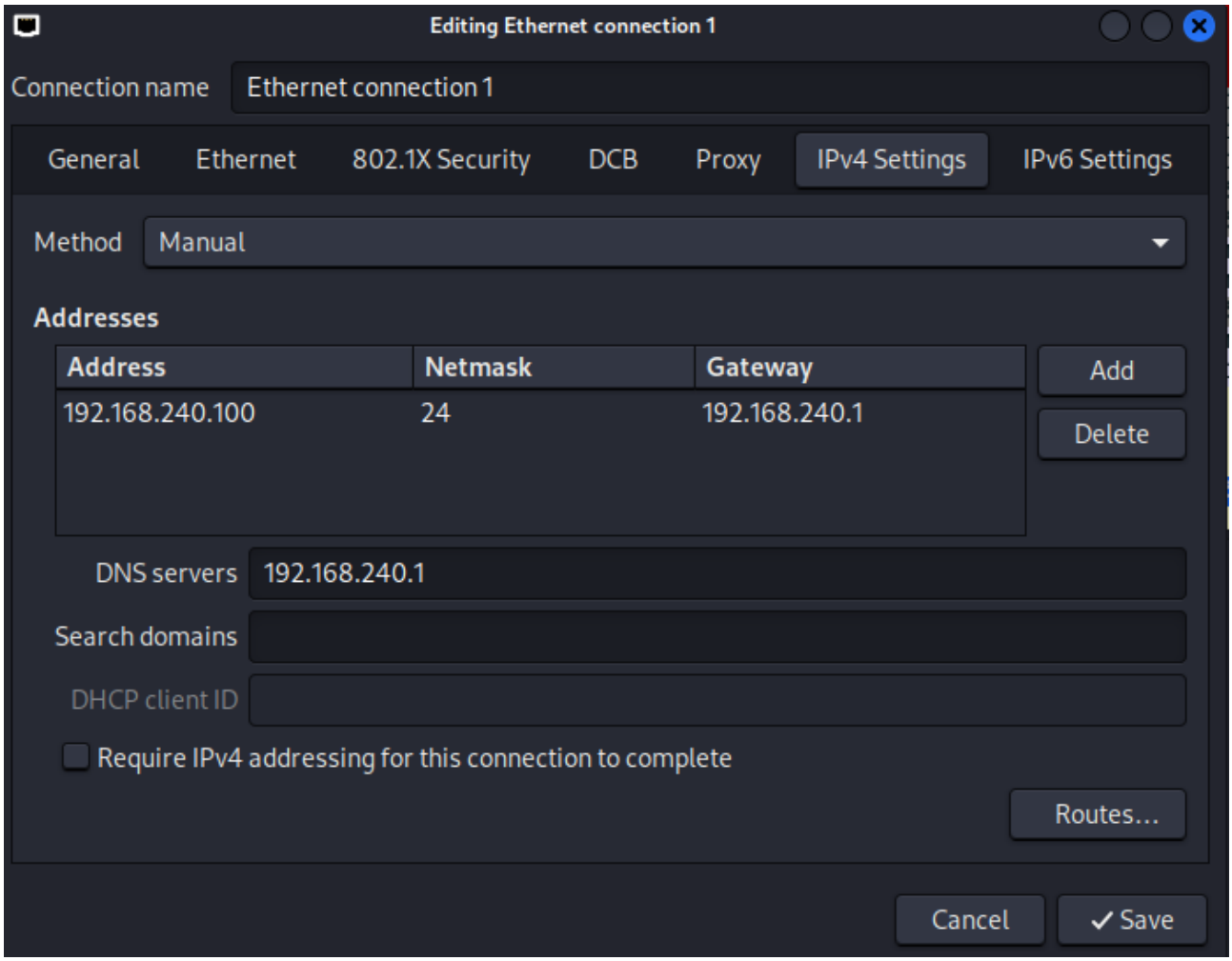
1. Configurazione IP delle Virtual Machine

Per prima cosa ho configurato le due macchine settando gli ip come scritto qui di seguito:

VM Windows XP con indirizzo IP 192.168.240.150.

VM Kali Linux con indirizzo IP 192.168.240.100.





2. Verifica della Comunicazione

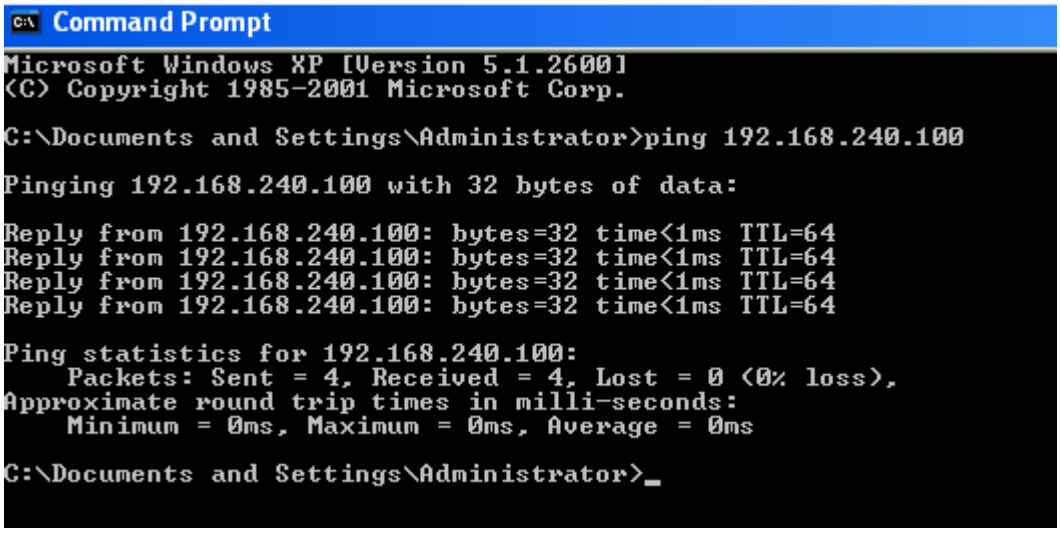
Per assicurarsi che entrambe le macchine potessero comunicare tra loro, è stato eseguito il comando ping dalla VM Kali alla VM Windows, e viceversa, usando:

ping <IPMACCHINABERSAGLIO>

L'esito positivo del ping ha confermato che entrambe le macchine erano correttamente configurate e si trovavano sulla stessa rete.

```
┌──(kali㉿kali)-[~]
└─$ ping -c 4 192.168.240.150
PING 192.168.240.150 (192.168.240.150) 56(84) bytes of data.
64 bytes from 192.168.240.150: icmp_seq=1 ttl=128 time=0.632 ms
64 bytes from 192.168.240.150: icmp_seq=2 ttl=128 time=0.575 ms
64 bytes from 192.168.240.150: icmp_seq=3 ttl=128 time=0.451 ms
64 bytes from 192.168.240.150: icmp_seq=4 ttl=128 time=0.393 ms

── 192.168.240.150 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3080ms
rtt min/avg/max/mdev = 0.393/0.512/0.632/0.095 ms
```



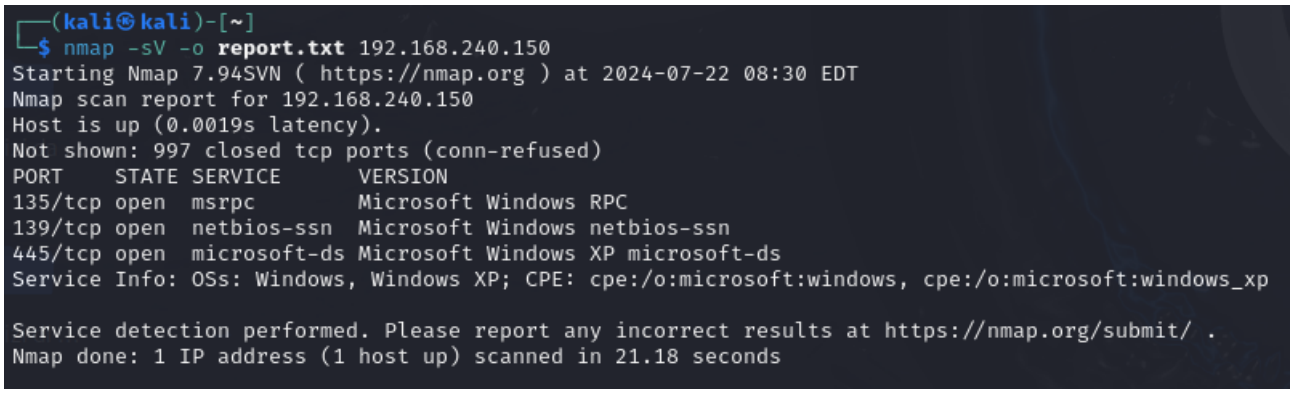
3. Scansione Nmap senza Firewall

La prima parte dell'esercizio consisteva nell'eseguire una scansione di rete con Nmap sulla macchina Windows XP con il firewall disattivato. I comandi utilizzati sono stati:

nmap -sV 192.168.240.150 -o report.txt

Opzione -sV: Effettua il rilevamento delle versioni dei servizi.

Opzione -o report.txt: Salva i risultati della scansione in un file di testo chiamato report.txt.



Da questa scansione abbiamo potuto vedere quali porte erano aperte sulla macchina Windows XP . Per

l'esattezza erano aperte le porte: 135,139 e la 445

4. Prima scansione Nmap con Firewall

Successivamente, il firewall di Windows XP è stato attivato e la scansione è stata ripetuta:

nmap -sV 192.168.240.150 -o report.txt

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -o report.txt 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 08:19 EDT
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 3.55 seconds
```

Da questa scansione non vi erano risultati. Ma grazie al messaggio “If it is really up, but blocking our ping probes, try -Pn” ho riprovato a lanciare la scansione aggiungendo -Pn al comando”

5. Seconda scansione Nmap senza Firewall

Dopo il messaggio precedente ho usato il comando:

nmap -sV -Pn 192.168.240.150 -o report.txt

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -Pn -o report.txt 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 08:34 EDT
Nmap scan report for 192.168.240.150
Host is up (0.00061s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE      VERSION
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 25.07 seconds
```

Da questa scansione si notano 2 porte aperte: la 139 e la 445 non facendo vedere la porta 135

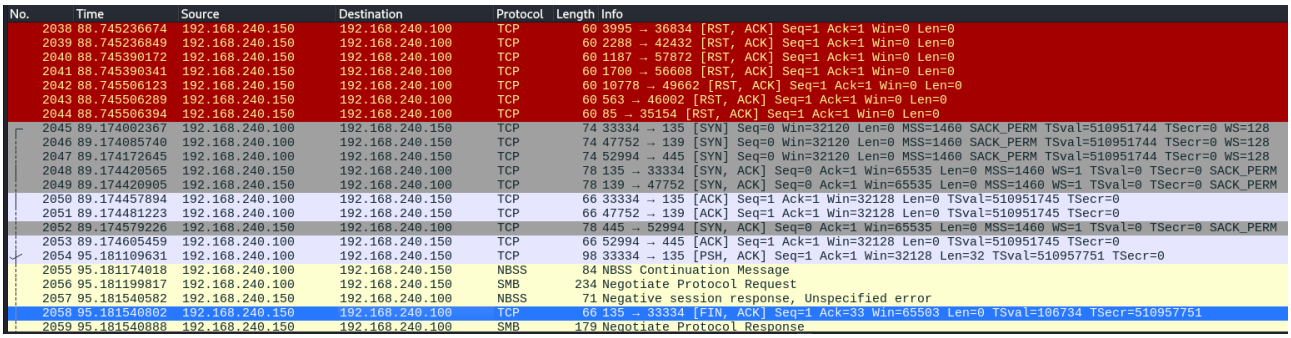
6. Analisi del Traffico con Wireshark

Durante entrambe le scansioni, Wireshark è stato utilizzato per catturare e analizzare il traffico di rete. Questo ha permesso di osservare i pacchetti inviati e ricevuti tra le due macchine, fornendo una visione dettagliata dell'interazione tra Nmap e la macchina Windows XP con e senza firewall.

Wireshark con firewall

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.240.100	192.168.240.150	TCP	74	49764 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=510862570 TSecr=0 WS=128
2	0.000149669	192.168.240.100	192.168.240.150	TCP	74	43172 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=510862570 TSecr=0 WS=128
3	2.009548865	192.168.240.100	192.168.240.150	TCP	74	43180 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=510864580 TSecr=0 WS=128
4	2.009825926	192.168.240.100	192.168.240.150	TCP	74	49780 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=510864580 TSecr=0 WS=128
5	5.090065360	PCSSystemtec_1e:36:…	PCSSystemtec_0f:04:…	ARP	42	Who has 192.168.240.150? Tell 192.168.240.100
6	5.090438117	PCSSystemtec_0f:04:…	PCSSystemtec_1e:36:…	ARP	60	192.168.240.150 is at 08:00:27:0f:04:d5
7	60.694848198	192.168.240.150	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
8	63.692852629	192.168.240.150	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
9	66.691040103	192.168.240.150	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
10	74.517592065	192.168.240.100	192.168.240.150	TCP	74	50638 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=510937088 TSecr=0 WS=128
11	74.517651300	192.168.240.100	192.168.240.150	TCP	74	44478 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=510937088 TSecr=0 WS=128

Wireshark senza firewall



No.	Time	Source	Destination	Protocol	Length	Info
2038	88.745236674	192.168.240.150	192.168.240.100	TCP	60	3995 → 36834 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2039	88.745236849	192.168.240.150	192.168.240.100	TCP	60	2288 → 42432 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2040	88.745390172	192.168.240.150	192.168.240.100	TCP	60	1187 → 57872 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2041	88.745390341	192.168.240.150	192.168.240.100	TCP	60	1700 → 56608 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2042	88.745506123	192.168.240.150	192.168.240.100	TCP	60	10778 → 49662 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2043	88.745506289	192.168.240.150	192.168.240.100	TCP	60	563 → 46002 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2044	88.745506394	192.168.240.150	192.168.240.100	TCP	60	85 → 35154 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2045	89.174002367	192.168.240.100	192.168.240.150	TCP	74	33334 → 135 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=510951744 TSecr=0 WS=128
2046	89.174085740	192.168.240.100	192.168.240.150	TCP	74	47752 → 139 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=510951744 TSecr=0 WS=128
2047	89.174172645	192.168.240.100	192.168.240.150	TCP	74	52994 → 445 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=510951744 TSecr=0 WS=128
2048	89.174420565	192.168.240.150	192.168.240.100	TCP	78	135 → 33334 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=1 TSval=0 TSecr=0 SACK_PERM
2049	89.174420905	192.168.240.150	192.168.240.100	TCP	78	139 → 47752 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=1 TSval=0 TSecr=0 SACK_PERM
2050	89.174457894	192.168.240.100	192.168.240.150	TCP	66	33334 → 135 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=510951745 TSecr=0
2051	89.174481223	192.168.240.100	192.168.240.150	TCP	66	47752 → 139 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=510951745 TSecr=0
2052	89.174579226	192.168.240.150	192.168.240.100	TCP	78	445 → 52994 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=1 TSval=0 TSecr=0 SACK_PERM
2053	89.174605459	192.168.240.100	192.168.240.150	TCP	66	52994 → 445 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=510951745 TSecr=0
2054	95.181109631	192.168.240.100	192.168.240.150	TCP	98	33334 → 135 [PSH, ACK] Seq=1 Ack=1 Win=32128 Len=32 TSval=510957751 TSecr=0
2055	95.181174018	192.168.240.100	192.168.240.150	NBSS	84	NBSS Continuation Message
2056	95.181199817	192.168.240.100	192.168.240.150	SMB	234	Negotiate Protocol Request
2057	95.181540582	192.168.240.150	192.168.240.100	NBSS	71	Negative session response, Unspecified error
2058	95.181540802	192.168.240.150	192.168.240.100	TCP	66	135 → 33334 [FIN, ACK] Seq=1 Ack=33 Win=65503 Len=0 TSval=106734 TSecr=510957751
2059	95.181540888	192.168.240.150	192.168.240.100	SMB	179	Negotiate Protocol Response

7. Conclusioni e Differenze

7.1 Risultati della Scansione Senza Firewall

Visibilità dei Servizi: Senza il firewall attivato, Nmap è stato in grado di rilevare tutti i servizi in esecuzione sulla macchina Windows XP, inclusi i numeri di versione dei servizi.

Risposte dei Pacchetti: I pacchetti di risposta sono stati completi e hanno fornito informazioni dettagliate sui servizi.

7.2 Risultati della Scansione con Firewall

Visibilità dei Servizi: Con il firewall attivato, Nmap ha mostrato una visibilità molto ridotta dei servizi. Molti dei servizi precedentemente visibili erano ora nascosti.

Risposte dei Pacchetti: Molti pacchetti di risposta sono stati bloccati dal firewall, riducendo significativamente la quantità di informazioni ottenute.

7.3 Differenze Osservate

Numero di Porte Aperte: Senza il firewall, 3 porte risultavano aperte. Con il firewall attivo solo 2 usando il comando -Pn altrimenti neanche una.

Informazioni sui Servizi: La quantità e la precisione delle informazioni sui servizi era molto maggiore senza il

Traffico di Rete: Wireshark ha mostrato un aumento significativo dei pacchetti ICMP di tipo "Destination Unreachable" con il firewall attivo, indicando che molte richieste di Nmap venivano bloccate.

8. Motivazioni delle Differenze

Le differenze osservate sono principalmente dovute alla funzione del firewall di filtrare e bloccare il traffico di rete non autorizzato:

Protezione dei Servizi: Il firewall impedisce l'accesso non autorizzato ai servizi in esecuzione sulla macchina, aumentando la sicurezza.

Riduzione della Visibilità: Bloccando le risposte ai pacchetti di scansione, il firewall riduce la quantità di informazioni disponibili agli attaccanti potenziali.

Aumento della Sicurezza: Limitando le informazioni disponibili, il firewall rende più difficile per gli attaccanti identificare e sfruttare le vulnerabilità.