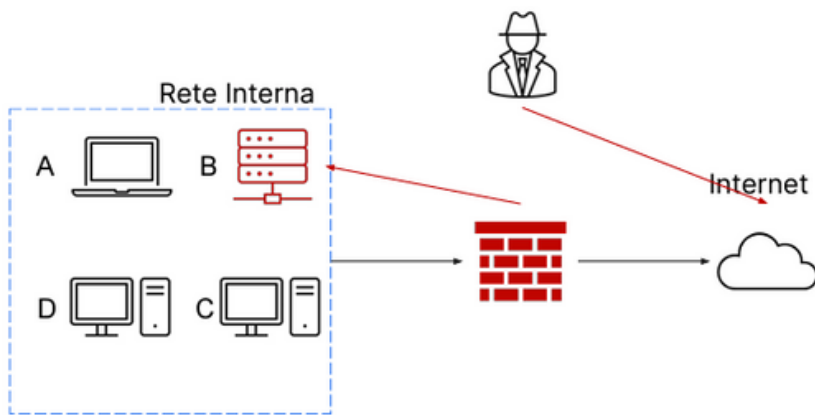


Security Operation: azioni preventive

Traccia:

Con riferimento alla seguente figura, il sistema B (un database con diversi dischi per lo storage) è stato compromesso interamente da un attaccante che è riuscito a bucare la rete ed accedere al sistema tramite internet. L'attacco è attualmente in corso e siete parte del team di CSIRT. Rispondere ai seguenti quesiti. Mostrate le tecniche di: I) Isolamento II) Rimozione del sistema B infetto Spiegate la differenza tra Purge e Destroy per l'eliminazione delle informazioni sensibili prima di procedere allo smaltimento dei dischi compromessi



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Versione 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Epicode_user>ping 192.168.240.100

Esecuzione di Ping 192.168.240.100 con 32 byte di dati:

Risposta da 192.168.240.100: byte=32 durata<1ms TTL=64
Risposta da 192.168.240.100: byte=32 durata<1ms TTL=64
Risposta da 192.168.240.100: byte=32 durata<1ms TTL=64
Risposta da 192.168.240.100: byte=32 durata<1ms TTL=64

Statistiche Ping per 192.168.240.100:
    Pacchetti: Trasmessi = 4, Ricevuti = 4, Persi = 0 (0% persi),
    Tempo approssimativo percorsi andata/ritorno in millisecondi:
        Minimo = 0ms, Massimo = 0ms, Medio = 0ms

C:\Documents and Settings\Epicode_user>_
```

```
kali@kali: ~
File Actions Edit View Help

(kali@kali)-[~]
$ ping 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=0.329 ms
64 bytes from 192.168.240.150: icmp_seq=2 ttl=128 time=0.300 ms
64 bytes from 192.168.240.150: icmp_seq=3 ttl=128 time=0.245 ms
64 bytes from 192.168.240.150: icmp_seq=4 ttl=128 time=0.255 ms
^C
— 192.168.240.150 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3126ms
rtt min/avg/max/mdev = 0.245/0.282/0.329/0.034 ms
```

Con il comando ***nmap -sV 192.168.240.150*** scansiono le porte aperte sulla macchina target e tento di identificare la versione dei servizi in esecuzione (firewall disattivato)

```
(kali@kali)-[~]
$ nmap -sV 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-29 04:32 EST
Nmap scan report for 192.168.240.150
Host is up (0.00017s 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 20.76 seconds
```

Riprovo dopo aver attivato il firewall

```
(kali@kali)-[~]
$ nmap -sV 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-29 04:33 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 3.13 seconds
```

Le analisi dettagliate effettuate tramite l'utilizzo di Nmap, un noto software di scansione di rete, forniscono una chiara dimostrazione dell'impatto significativo che i firewall hanno sulla sicurezza dei sistemi operativi, in questo caso specifico, Windows XP. Quando i firewall sono attivati, si osserva che ogni tentativo di ping verso il sistema viene efficacemente bloccato. Questo fenomeno evidenzia l'efficacia dei firewall come strumento cruciale per la difesa del sistema, agendo da barriera contro gli attacchi esterni e impedendo l'individuazione remota delle attività del sistema.

Al contrario, disattivando i firewall, la situazione cambia drasticamente. Senza questa barriera protettiva, Nmap riesce a eseguire una scansione approfondita delle porte, permettendo così di rilevare quelle aperte e di identificare potenziali vulnerabilità all'interno del sistema. Queste vulnerabilità possono essere sfruttate da attaccanti per infiltrarsi nel sistema, causando potenziali danni o compromettendo dati sensibili. Queste osservazioni sottolineano l'importanza vitale di mantenere sempre attivi i firewall e di adottare un approccio olistico alla sicurezza informatica, che includa l'implementazione di varie misure di sicurezza come software antivirus, aggiornamenti regolari del sistema e pratiche di navigazione sicura. Inoltre, è essenziale per gli amministratori di sistema e per gli utenti finali essere consapevoli delle configurazioni di sicurezza dei loro dispositivi e di comprendere il ruolo fondamentale che le misure preventive giocano nel proteggere i sistemi informatici da attacchi esterni e intrusioni indesiderate. In sintesi, la protezione offerta dai firewall, unita ad altre pratiche di sicurezza, costituisce una difesa essenziale contro le minacce informatiche, salvaguardando l'integrità e la privacy dei dati nei sistemi operativi moderni.