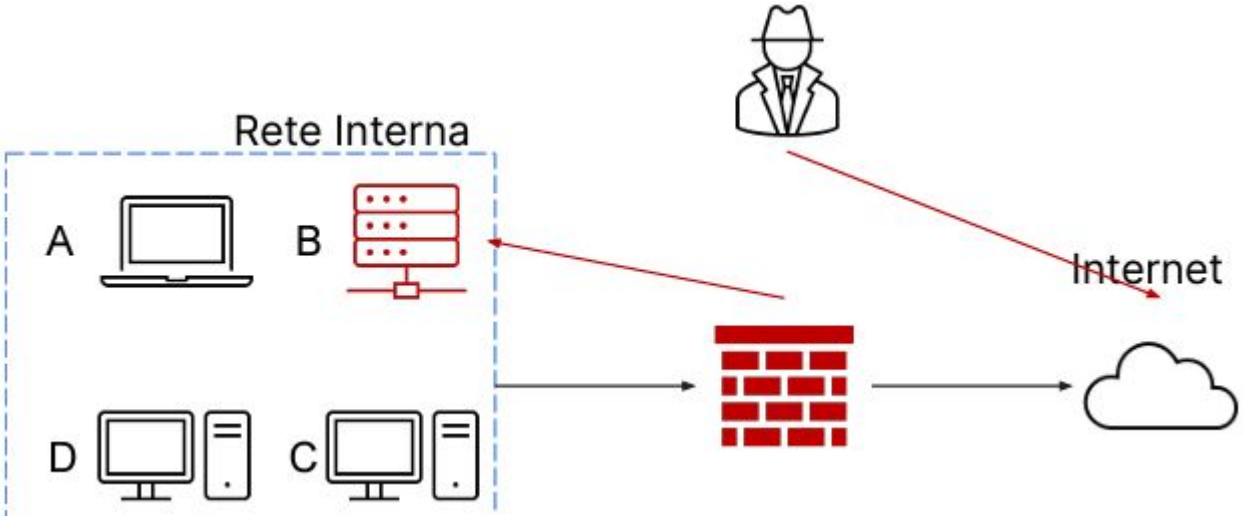
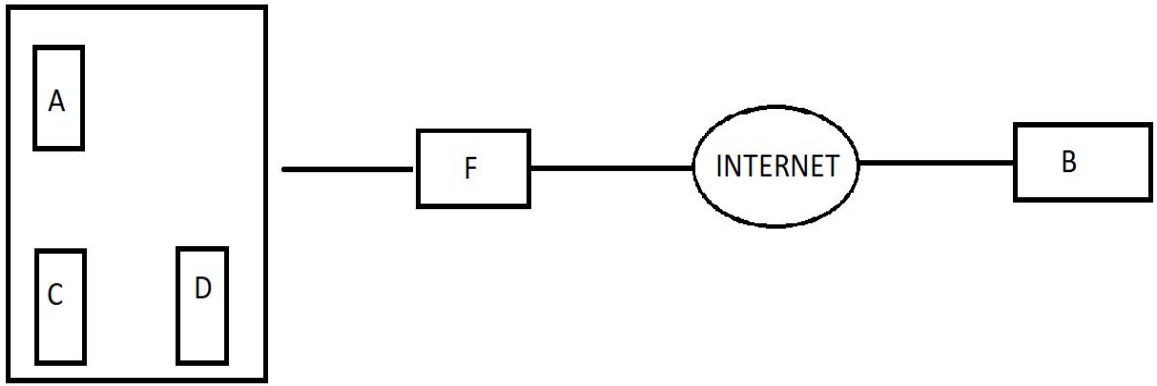


Il sistema B (un database con diversi dischi per lo storage) è stato compromesso interamente da un attaccante che è riuscito a bucare la rete ed accedere al sistema tramite internet. L'attacco è attualmente in corso e siete parte del team di CSIRT. Rispondere ai seguenti quesiti. Mostrate le tecniche di:

I) Isolamento

II) Rimozione del sistema B infetto

III) Spiegate la differenza tra Purge e Destroy per l'eliminazione delle informazioni sensibili prima di procedere allo smaltimento dei dischi compromessi


A
C
D
F
INTERNET
B

Nell’ immagine precedente ho ipotizzato di dover procedere, come richiesto dall’ esercizio, con **l’ isolamento** del computer B in quanto vittima di un Malware. Il problema della prima slide è che tutti e quattro i computer si trovavano all’ interno della stessa rete, per cui se il malware avesse avuto la capacità di replicare sè stesso avrebbe potuto infettare gli altri computer presenti. Con l’ isolamento (possibile grazie alla segmentazione della rete tramite subnetting o VLAN), questo rischio viene annullato in quanto trovandosi all’ interno di una sotto rete dove non sono presenti altre macchine, non c’è il pericolo che il virus possa diffondersi su altri sistemi ma viene contenuto sul computer B. Tuttavia ha ancora accesso ad Internet, per cui rimane il rischio che chi abbia attaccato il sistema possa collegarsi al computer dalla rete.

Per questo motivo, alcune volte è consigliabile procedere con la **rimozione** di una macchina anzichè con il suo isolamento.Questo è possibile scollegamento fisicamente il computer dalla rete, in modo che non solo non sia all’ interno di una rete locale ma non sia proprio più raggiungibile in nessun modo dall’ esterno non avendo più possibilità di connessione ad internet. Questo esclude sia la possibilità che un Malware infetti altri computer, sia che un criminale informatico possa continuare ad avere accesso al computer B nonostante questo sia stato messo in isolamento.

Purge e **Destroy** sono due tecniche di eliminazione di dati sensibili all' interno di un disco rigido o comunque di un sistema di storage compromesso.

Purge: consiste nella sovrascrittura, più e più volte, dei file originari all' interno del disco rigido con altri file meno importanti. Questo per rendere più complicato risalire ai file originariamente presenti all' interno del disco. In alternativa si utilizza un potente magnete che disturba il campo magnetico del disco al fine di rendere illegibili i file al suo interno.

Destroy: è la procedura più sicura, e consiste nella totale distruzione **fisica** dello storage in questione utilizzando specifiche tecniche. Questo rende totalmente inaccessibili e illegibili i file all' interno del disco, ma rende ovviamente anche inutilizzabile il disco stesso.