Emanuele Di Stefano

S9-L4

Esercizio di Incident Response

Scenario

Il sistema B, un database con diversi dischi per lo storage, è stato compromesso da un attaccante che è riuscito a bucare la rete ed accedere al sistema tramite Internet. L'attacco è attualmente in corso e sei parte del team di CSIRT (Computer Security Incident Response Team).

Risposte ai Quesiti

I. Tecniche di Isolamento

Disconnessione dalla rete:

- disconnetti immediatamente il sistema B dalla rete interna e da Internet per interrompere l'accesso dell'attaccante e prevenire ulteriori danni. Questo può essere fatto disabilitando l'interfaccia di rete tramite il sistema operativo o scollegando fisicamente il cavo di rete.

Disabilitare l'interfaccia di rete (esempio per Linux) “sudo ifconfig eth0 down”

Impostazione di firewall:

- configura il firewall per bloccare tutte le comunicazioni in entrata e in uscita dal sistema B.

Blocco di tutto il traffico in entrata e in uscita (esempio per iptables su Linux) “sudo iptables -A INPUT -s 192.168.1.0/24 -j DROP” “sudo iptables -A OUTPUT -d 192.168.1.0/24 -j DROP”

Segmentazione della rete:

- Passo 3: Isola la rete interna in segmenti separati per limitare la propagazione del malware ad altri sistemi. Utilizza VLAN (Virtual Local Area Network) per creare segmenti di rete isolati.

Creazione di un ambiente di contenimento:

- Passo 4: Sposta il sistema B in un ambiente di contenimento sicuro (es. una rete isolata o un segmento di rete separato) dove può essere analizzato senza rischio di ulteriore compromissione della rete.

II. Tecniche di Rimozione del Sistema B Infetto

Backup dei dati:

Passo 1:
Prima di procedere alla rimozione, effettua un backup completo dei dati importanti. Assicurati che il backup sia esente da malware eseguendo scansioni approfondite con un software antivirus aggiornato.

Formattazione del sistema:

Passo 2:
una volta che i dati sono stati messi al sicuro, formatta tutti i dischi del sistema B per rimuovere il malware.

Formattazione di un disco (esempio per Linux) “sudo mkfs.ext4 /dev/sdX”

Reinstallazione del sistema operativo:

Passo 3:
reinstalla il sistema operativo da una fonte pulita e sicura. Assicurati di applicare tutte le patch di sicurezza disponibili durante l'installazione.

Ripristino dei dati:

Passo 4:
dopo aver reinstallato il sistema operativo, ripristina i dati dal backup eseguito precedentemente. Esegui nuovamente una scansione antivirus sui dati prima di reimportarli nel sistema.

III. Differenza tra Purge, Destroy e Clear

Clear (Cancellazione):

la cancellazione è il processo di rimozione dei dati in modo che non possano essere recuperati con mezzi standard. Questo può essere fatto utilizzando software che sovrascrive i dati esistenti con dati casuali.

Comando per cancellare in modo sicuro un file (esempio per Linux) “shred -u filename”

Purge (Epuration):

- l'epurazione è un metodo di rimozione dei dati più robusto rispetto alla cancellazione. Utilizza tecniche di sovrascrittura avanzate e altre misure per garantire che i dati non possano essere recuperati nemmeno con strumenti avanzati di recupero dati.

Comando per epurare un file (esempio per Linux) “wipe filename”

Destroy (Distruzione):

La distruzione è il metodo più sicuro per eliminare i dati. Questo comporta la distruzione fisica dei supporti di memorizzazione, ad esempio triturando i dischi, bruciandoli, o utilizzando dispositivi di smagnetizzazione (degausser) che distruggono i dati a livello fisico.

Esempio di smagnetizzazione

Smagnetizzazione:
usa un degausser per cancellare i dati sui dischi rigidi. Questo processo rende i dati completamente irrecuperabili distruggendo il supporto di memorizzazione a livello fisico.