ESERCITAZIONE W17D1(2)

EPICODE

Esercizio
Hacking Windows XP

Sulla base di quanto visto nell'esercizio pratico di ieri, formulare delle ipotesi di remediation.

Ad esempio:
1. L'attacco colpisce Windows XP, possiamo risolvere in qualche modo? Se si, con quale effort?
2. L'attacco colpisce una particolare vulnerabilità, possiamo risolvere solo la vulnerabilità?
3. Una volta dentro l'attaccante, può accedere a webcam e/o tastiera, possiamo risolvere queste problematiche?

Buon divertimento

1. Risolvere la vulnerabilità MS08-067: La remediation principale sarebbe applicare la patch di sicurezza per la vulnerabilità MS08-067 fornita da Microsoft. Se il sistema operativo è Windows XP, questo potrebbe essere problematico poiché Windows XP non è più supportato da Microsoft. In questo caso, una soluzione alternativa potrebbe essere l'isolamento del sistema dalla rete o l'adozione di soluzioni di sicurezza aggiuntive, come firewall o sistemi di rilevamento delle intrusioni, per monitorare e bloccare eventuali tentativi di sfruttamento della vulnerabilità.

2. Prevenire l'accesso non autorizzato alla webcam e alla tastiera: Per mitigare il rischio di accesso non autorizzato alla webcam e alla tastiera, potrebbe essere utile disattivare queste periferiche quando non sono in uso. Inoltre, l'implementazione di controlli di accesso fisico al dispositivo potrebbe impedire agli attaccanti di fisicamente accedere alla webcam o alla tastiera per scopi dannosi. Tuttavia, se l'attacco avviene tramite software, l'applicazione di patch e aggiornamenti di sicurezza regolari può contribuire a ridurre il rischio di exploit delle vulnerabilità che consentono l'accesso non autorizzato a tali dispositivi.

3. Monitoraggio costante e rilevamento delle attività sospette: Implementare sistemi di monitoraggio e rilevamento delle intrusioni che possono identificare comportamenti anomali o attività sospette sul sistema. Questo potrebbe includere l'uso di strumenti di sicurezza come sistemi di rilevamento delle intrusioni basati su firme o comportamentali, che possono identificare attività inusuali come l'accesso non autorizzato alla webcam o la registrazione della tastiera.

In sintesi, la remediation per un attacco basato sulla vulnerabilità MS08-067 su un sistema Windows XP richiederebbe un approccio multilivello che comprende l'applicazione di patch, la

disattivazione delle periferiche non utilizzate, l'implementazione di controlli di accesso fisico e l'uso di strumenti di monitoraggio e rilevamento delle intrusioni per prevenire e rilevare attività sospette.