ESERCIZIO W17D1
PRATICA 2

Ecco alcune ipotesi di remediation basate sull'esercizio pratico di hacking:

Risolvere l'attacco su Windows XP:

Effort: La cessazione del supporto esteso per Windows XP è avvenuta nel 2014, il che significa che Microsoft non rilascia più aggiornamenti di sicurezza per questo sistema operativo.

La soluzione migliore sarebbe migrare a una versione più recente di Windows o, preferibilmente, a un sistema operativo supportato e più sicuro, come Windows 10 o una distribuzione Linux.

Tuttavia, la migrazione potrebbe richiedere un notevole sforzo, inclusa la verifica della compatibilità delle applicazioni esistenti e la formazione del personale per l'utilizzo di nuovi sistemi operativi.

Risolvere la vulnerabilità colpita:

Effort: Sebbene MS08-067 sia stata una vulnerabilità critica e ben nota, Microsoft ha rilasciato una patch per questa vulnerabilità molti anni fa.

La remediation più diretta sarebbe applicare la patch di sicurezza appropriata ai sistemi vulnerabili.

Tuttavia, poiché il supporto per Windows XP è terminato, potrebbe essere necessario cercare soluzioni alternative, come l'applicazione di misure di mitigazione come firewalls, monitoraggio dei log e segmentazione di rete per ridurre il rischio di sfruttamento della vulnerabilità.

Limitare l'accesso a webcam e tastiera:

Effort: Per limitare l'accesso a webcam e tastiera una volta che un attaccante ha ottenuto accesso al sistema, possono essere adottate diverse misure di sicurezza.

Ad esempio, disabilitare fisicamente la webcam se non è necessaria, utilizzare coperture per webcam quando non in uso e aggiornare regolarmente i driver e il firmware per correggere le vulnerabilità note.

Per quanto riguarda la sicurezza della tastiera, l'uso di software di rilevamento delle intrusioni (IDS) e di autenticazione a due fattori può aiutare a prevenire l'accesso non autorizzato alla tastiera e al sistema nel complesso.

Queste ipotesi di remediation possono aiutare a mitigare i rischi derivanti dall'exploit della vulnerabilità MS08-067 e dalle conseguenze di un attacco di successo.

Tuttavia, è importante ricordare che la sicurezza informatica è un processo continuo e dinamico, e quindi è consigliabile monitorare costantemente le minacce emergenti e adattare le misure di sicurezza di conseguenza.