# ESERCIZIO W17D1 PARTE 2

La seconda parte di pratica consiste nel trovare le remediation action adeguate per affrontare la vulnerabilità MS08-067. La traccia da seguire riporta questi punti:

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?

## 1. Aggiornamento Windows XP

Sicuramente il modo migliore per contrastare la vulnerabilità, ed impedire l'esecuzione di codice nel servizio Server, è apportare l'aggiornamento dedicato a tutti i sistemi Windows XP. L'aggiornamento risolve la vulnerabilità correggendo il modo in cui il server gestisce le richieste RPC.

Effort: Basso - Medio. Dipende dalla dimensione dell'ambiente e dalla disponibilità di risorse per l'aggiornamentp

## 2. Mitigazione singola delle vulnerabilità

Disabilitazione dei servizi server o browser: Come rimedio immediato, nel caso non si possa fare subito l'aggiornamento, una pratica utile sarebbe quella di disattivare i servizi passando da Strumenti di amministrazione > Servizi.

Impatto mitigazione: Annullando il browser, tutti i servizi collegati a quest'ultimo andranno in errore. Invece, se si spegne il server, verrà interrotta le condivisione di file e risorse delle stampanti.

Blocco delle porte TCP 139 e 445 nel firewall: Un tappa buchi efficiente potrebbe essere quello di bloccare le comunicazioni in ingresso sulle porte aperte dai demoni di servizio. In questo modo si stronca un probabile attacco.

Impatto mitigazione: Bloccare le porte pone fuori commissione i servizi collegati ad esse, ad esempio:

- Applicazione che usano SMB (Server message Block)
- Server di condivisione file e stampa
- File system distribuito (DFS)
- Accesso rete
- Licenze del server terminal
- Servizio di indicizzazione
- E altro

Blocco traffico non richiesto mediante Firewall: Semplicemente blocchiamo i pacchetti che potrebbero andare a toccare i vari servizi interessati. RPC, SMB, SMBV1 etc

Impatto mitigazione: Niente pacchetti, niente comunicazione da parte di altri client, nemmeno per questioni legittime.

### 3. Cosa fare se l’attaccante ha guadagnato l’accesso al sistema?

In questo caso è opportuno aver seguito le best practice di sicurezza per ridurre i danni. Ad esempio, possiamo limitare i privilegi degli utenti, disabilitare le funzioni non necessarie, aggiornare i software inerenti oppure monitorare l’attività di rete.