Report Esercizio

W17-D3

Redatto da Andrea Sciattella

16/06/2024

TRACCIA

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

SVOLGIMENTO ESERCIZIO

Questo report descrive l'attacco condotto sulla macchina Windows XP del precedente esercizio utilizzando Meterpreter di Metasploit Framework. L'obiettivo è valutare la vulnerabilità sfruttata, le capacità dell'attaccante una volta ottenuto l'accesso e proporre soluzioni per mitigare o eliminare le problematiche riscontrate.

-L'attacco colpisce Windows XP, possiamo risolvere in qualche modo? Se sì, con quale effort?

Windows XP è un sistema operativo ormai obsoleto, non più supportato ufficialmente da Microsoft dal 8 aprile 2014. Questo indica che non riceve più aggiornamenti di sicurezza, rendendolo quindi un OS vulnerabile a vari tipi di attacchi.

La soluzione più efficace sarebbe aggiornare il sistema operativo a una versione più recente e supportata, come Windows 10 o Windows 11. Questo aggiornamento include migliorie in termini di sicurezza e funzionalità, riducendo drasticamente il rischio di exploit noti.

Effort:

- **Tempo**: Il tempo necessario per aggiornare dipende dal numero di macchine coinvolte e dalla complessità della migrazione. Per una singola macchina, potrebbe richiedere diverse ore.
- **Costo**: Potenzialmente elevato, considerando i costi delle licenze e dell'hardware compatibile, oltre al tempo di inattività durante la migrazione.
- **Risorse**: Personale IT per la pianificazione e l'esecuzione della migrazione, hardware e software per supportare il nuovo sistema operativo.

-L'attacco colpisce una particolare vulnerabilità, possiamo risolvere solo la vulnerabilità?

L'attacco è stato condotto utilizzando la vulnerabilità ms08_067_netapi, una vulnerabilità critica di esecuzione di codice remoto in Windows. Per risolvere la criticità possiamo applicare la patch di sicurezza specifica rilasciata da Microsoft (MS08-067).

Tuttavia, è importante capire che risolvere una sola vulnerabilità non rende il sistema sicuro, poiché Windows XP ha molte altre vulnerabilità note e non corregibili.

Effort:

- **Tempo**: Applicare una singola patch è relativamente veloce, richiedendo pochi minuti per macchina.
- **Costo**: Basso, considerando che la patch è disponibile gratuitamente. Tuttavia, il costo della manodopera per applicarla su tutte le macchine può variare.
- **Risorse**: Amministratori di sistema per distribuire e verificare l'applicazione della patch.

- Una volta dentro, l'attaccante può accedere a webcam e/o tastiera, possiamo risolvere queste problematiche?

Una volta ottenuto l'accesso a una macchina tramite il modulo Meterpreter, l'attaccante può accedere alla webcam e registrare le sequenze di tasti (tramite i comandi di keylogging).

Soluzioni:

1. **Aggiornamento del Sistema Operativo**: Come menzionato precedentemente, l'aggiornamento a un sistema operativo più recente riduce notevolmente il rischio di exploit.
2. **Software Anti-Malware**: Installare e mantenere aggiornato un software antivirus/anti-malware che può rilevare e bloccare comportamenti sospetti come l'accesso non autorizzato alla webcam o al keylogger.
3. **Configurazione della Sicurezza**:
    - **Disabilitare la Webcam**: Se non è necessaria, disabilitare la webcam tramite il BIOS/UEFI o le impostazioni di sistema.
    - **Monitoraggio delle Attività**: Implementare soluzioni di monitoraggio delle attività che possono rilevare e avvisare su comportamenti anomali.
4. **Hardening del Sistema**: Seguire le best practice per la sicurezza, inclusa la disabilitazione dei servizi non necessari, l'uso di firewall e la restrizione dei privilegi utente.

Effort:

- **Tempo**: Varia a seconda delle soluzioni implementate. L'installazione di software anti-malware e la configurazione delle impostazioni di sicurezza possono essere effettuate rapidamente, mentre l'aggiornamento del sistema operativo richiede più tempo.

- **Costo**: Software anti-malware può avere costi di licenza. Disabilitare la webcam e altre configurazioni di sicurezza hanno un costo minimo in termini di tempo.
- **Risorse**: Personale IT per configurare e monitorare le soluzioni di sicurezza.

Conclusioni

1. **Aggiornamento di Windows XP**: La soluzione più efficace e a lungo termine per mitigare i rischi è l'aggiornamento del sistema operativo. Questo richiede un effort significativo ma offre la migliore protezione contro future vulnerabilità.
2. **Patch Specifica**: Applicare la patch MS08-067 risolve la vulnerabilità specifica sfruttata in questo attacco, ma non risolve le problematiche di sicurezza generali di Windows XP.
3. **Protezione Contro Accessi Illegittimi**: Implementare misure di sicurezza aggiuntive come software anti-malware, disabilitazione della webcam non necessaria e monitoraggio delle attività può ridurre ulteriormente i rischi.

Si raccomanda una combinazione di aggiornamenti del sistema operativo, applicazione di patch e misure di sicurezza per abilitare tutti gli effetti la protezione delle macchine contro attacchi simili.