M5-W17D1 - Pratica (2)

DATA

Cybersecurity Analyst

Studente:
Andrea Scarmagnani
Docente:
Federico Daidone

Cyber Security & Ethical Hacking Giorno 3 – Hacking Windows - remediation

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. **L'attacco colpisce Windows XP, possiamo risolvere in qualche modo? Se si, con quale effort?**

-Si procede scollegando la macchina dalla rete locale, cosi da isolarla;
-Eseguire una scansione Malware/Virus approfondita;
-Cercare eventuali falle di sicurezza;
-Chiuderle ed eseguire un controllo se sono ancora aperte;
-Limitare l'accesso a determinate porte di rete, mettendo filtri se la macchina non ha la possibilità di essere aggiornata.

2. **L'attacco colpisce una particolare vulnerabilità, possiamo risolvere solo la vulnerabilità?**

-Si nel caso in cui il problema risale a una vulnerabilità riconosciuta si può verificare nel sito Microsoft (essendo macchina windows) e carcare se è stata rilasciata una patch.

https://learn.microsoft.com/it-it/security-updates/
https://learn.microsoft.com/it-it/security-updates/securitybulletins/securitybulletins

Nel caso della vulnerabilità dell'esercizio precedente, qui sotto una la linea guida da utilizzare per risolverla:

https://learn.microsoft.com/it-it/security-updates/securitybulletins/2008/ms08-067

Microsoft rilascia una dettaglia descrizione su come mitigare il problema.

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

-Si installando una Antivirus/Internet Security, alzando un firewall, che blocchi tutto quello che non è necessario, installando dei dispositivi che analizzano la rete della macchina e cercando di monitorare il più possibile la macchina debole.

Cybersecurity Analyst 2023