Diario di lavoro

|  |  |
| --- | --- |
| Luogo | Canobbio |
| Data | 24.10.2019 |

|  |
| --- |
| Lavori svolti |
| 13h15 -14h10  Ho revisionato il codice scritto documentando in un modo migliore la presenza di vulnerabilità all’interno del codice.  14h10 – 14h45 15h00 - 16h20  Ho iniziato a documentare le vulnerabilità “nascoste” di HackerLab. Ho iniziato con lo sviluppo di script di esempio per degli attacchi di tipo bruteforce.  Questo è un esempio di bruteforce del login di HackerLab. Si inserisce un email ed una lista di password, lo script proverà ad accedere con tutte le password inserite nella lista, se riuscirà ad accedere mostrerà la password utilizzata.    Figura Dimostrazione bruteforce login  Questo invece è un esempio di email checker, ovvero uno script che si occupa di verificare se una email è registrata all’interno di HackerLab. Per la creazione di questo programma è stata sfrutta la chiamata del recupero password. Questa chiamata permette di stabilire se un account esiste oppure no.    Figura Dimostrazione bruteforce email  Questi due script con una grande quantità di dati possono essere molto pericolosi in quanto ci sarebbero alte probabilità di trovare account registrati (Sempre se hackerlab fosse online e famoso).  16h20- 16h30  Stesura del diario. |

|  |
| --- |
| Problemi riscontrati e soluzioni adottate |
| Nessun problema riscontrato. |

|  |
| --- |
| Punto della situazione rispetto alla pianificazione |
| Mi trovo molto avanti rispetto alla pianificazione. |

|  |
| --- |
| Programma di massima per la prossima giornata di lavoro |
| Creare le documentazioni docx e pdf delle vulnerabilità nascoste. |