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.

```
[i] Dimostrazione di bruteforce del login di HackerLab
[i] Autore: Filippo Finke
[?] Inserisci una email: filippo.finke@samtrevano.ch
[i] Caricate 501 passwords!
[-] Accesso con     123456      -> FALLITO! (0/501)
[-] Accesso con    password     -> FALLITO! (1/501)
[-] Accesso con    12345678     -> FALLITO! (2/501)
[-] Accesso con      pussy      -> FALLITO! (3/501)
[-] Accesso con      12345      -> FALLITO! (4/501)
[-] Accesso con     dragon      -> FALLITO! (5/501)
[-] Accesso con     qwerty      -> FALLITO! (6/501)
[-] Accesso con     696969      -> FALLITO! (7/501)
[-] Accesso con     mustang     -> FALLITO! (8/501)
[-] Accesso con     letmein     -> FALLITO! (9/501)
[-] Accesso con      1234       -> SUCCESSO!
[!] PASSWORD TROVATA: 1234
[!] CREDENZIALI -> filippo.finke@samtrevano.ch:1234
```

Figura 1 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.

```
[i] Dimostrazione di email checker di HackerLab
[i] Autore: Filippo Finke
[i] Caricate 32 emails!
[-] Email        gerry.lillie@hackerlab.ch         -> INESISTENTE! (0/32)
[-] Email         otha.arzate@hackerlab.ch         -> INESISTENTE! (1/32)
[-] Email     jonathon.wentworth@hackerlab.ch      -> INESISTENTE! (2/32)
[-] Email       victor.hartness@hackerlab.ch       -> INESISTENTE! (3/32)
[-] Email       allen.fenimore@hackerlab.ch        -> INESISTENTE! (4/32)
[-] Email       filippo.finke@samtrevano.ch        -> REGISTRATA! (5/32)
[-] Email       darius.hollaway@hackerlab.ch       -> INESISTENTE! (6/32)
[-] Email        glenn.wallis@hackerlab.ch         -> INESISTENTE! (7/32)
[-] Email      isiah.branstetter@hackerlab.ch      -> INESISTENTE! (8/32)
[-] Email      adalberto.maheux@hackerlab.ch       -> INESISTENTE! (9/32)
[-] Email       tristan.nottage@hackerlab.ch       -> INESISTENTE! (10/32)
[-] Email      derrick.gressett@hackerlab.ch       -> INESISTENTE! (11/32)
[-] Email        julio.cullum@hackerlab.ch         -> INESISTENTE! (12/32)
[-] Email     whitney.schleusner@hackerlab.ch      -> INESISTENTE! (13/32)
```

Figura 2 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.