Le Cronache di HogTheta:

Diario di un Spezzaincantesimi della Gringott

Classificazione: *Massima Sicurezza Magica (Livello Auror)* **Soggetto dell'Incursione:** La Fortezza Digitale di HogTheta (Target IP: 192.168.50.213) **Redattore:** Datashields, Gruppo Spezzaincantesimi

"La mente non è un libro che si può aprire a piacimento. La verità va cercata tra le righe degli incantesimi più oscuri."

Capitolo 1: Revelio (Reconnaissance & Enumeration)

Il nostro avvicinamento alle mura perimetrali di HogTheta è iniziato con la massima cautela. La fortezza sembrava avvolta in una nebbia protettiva, un potente ***Incanto Fidelius*** che celava la sua struttura.

Per dissipare questa nebbia, abbiamo innalzato le nostre bacchette e lanciato il potente **Incanto Revelio Supremo** (noto ai babbani come una scansione completa di Nmap).

```
$ nmap -p- -A -T4 192.168.50.213
```

L'incantesimo ha colpito le barriere, e la nebbia si è diradata rivelando una struttura complessa e instabile. Oltre al Grande Portone d'Ingresso (Porta 80/HTTP) e a un insolito passaggio di servizio (Porta 2222/SSH), la fortezza presentava altre tre finestre spettrali aperte sui piani alti (porte alte casuali), come se il castello stesso stesse cambiando forma. Un chiaro segno di magia instabile o di un potente incantesimo di distrazione.

Avvicinandoci al Portone Principale (la pagina web sulla porta 80), abbiamo notato delle strane incisioni sul telaio della porta. Non erano caratteri comuni, ma **Rune Antiche** nello stile oscuro di Salazar Serpeverde. Un'analisi più attenta del codice sorgente della pagina ha rivelato che queste rune erano un cifrario ***Brainfuck*.**

Con l’aiuto della Prof. Bathsheda Babblig,di Rune Antiche, abbiamo decifrato alcuni degli indizi, mentre con la Prof. Sibilla Cooman ne abbiamo individuati altri, una sequenza particolare, evocativa.

Capitolo 2: Il Ritratto Parlante e la Parola d'Ordine (Steganography)

Esplorando l'atrio del sito web, la nostra attenzione è stata catturata dallo stemma della scuola: un'immagine apparentemente innocua (theta-logo.jpg). Tuttavia, la mia bacchetta vibrava leggermente in sua presenza: l'immagine era un **Ritratto Parlante** sotto un incantesimo Silente.

Tornando al codice sorgente, abbiamo trovato l'incantesimo per farlo "parlare". Un attributo nascosto recitava: pass="accio".

Abbiamo rivolto quindi la nostra attenzione alla Signora Grassa e pronunciato la parola d'ordine: *"Accio!"*. Utilizzando l'artefatto magico noto come steghide, abbiamo estratto i segreti celati nel dipinto.

```
$ steghide extract -sf theta-logo.jpg
```

Alla richiesta della passphrase, abbiamo inserito: accio

Il ritratto ha "sputato" una pergamena nascosta (poesis.txt). Era una poesia scritta su un certo Luca e la sua amata Milena. Tra le righe sdolcinate, però, si celava un indizio cruciale, una profezia numerica:

"Era il 22, o il 2222?"

La porta 22 era chiusa magicamente. La 2222 era aperta, ma non avevamo le chiavi. La poesia ci ha fornito due nomi di studenti su cui indagare: **Luca** e **Milena**.

Capitolo 3: La Camera dei Segreti (SQL Injection & Cracking)

Seguendo i sussurri dei fantasmi del castello, abbiamo scoperto un'ala abbandonata della struttura: il vecchio sito web, accessibile tramite /oldsite/. Lì, una polverosa pagina di login (/oldsite/login.php) sbarrava il passo alle segrete.

Le protezioni qui erano antiche e fragili, non aggiornate dai tempi dei Fondatori. Ho deciso di evocare il **Basilisco**, un costrutto magico automatizzato capace di insinuarsi nelle crepe delle difese (SQLMap). Ho iniziato a parlargli in *Serpentese*, iniettando comandi malevoli nel campo di input.

```
$ sqlmap -u "http://192.168.50.213/oldsite/login.php" --forms --dbs
```

La porta della Camera dei Segreti si è spalancata. Il database hogtheta è stato rivelato. Abbiamo ordinato al Basilisco di portarci le pergamene contenenti l'elenco degli studenti e i loro segreti.

```
$ sqlmap -u "http://192.168.50.213/oldsite/login.php" --forms -D hogtheta -T users --dump
```

Dalle fauci del Basilisco sono emersi quattro nomi e le loro password criptate (hash bcrypt): *Anna, Luca, Marco, Milena*.

Milena, che la poesia identificava come una delle possibili chiavi, aveva una password protetta da un incantesimo debole. Gli Spezzaincantesimi della Gringott (e un buon dizionario rockyou.txt) hanno spezzato l'incantesimo in pochi secondi.

Le credenziali della "Principessa Mezzosangue" erano nostre:

- Utente: milena
- Password: darkprincess

Capitolo 4: Il Passaggio della Strega Orba (Initial Access)

Con le credenziali di Milena, siamo tornati al passaggio di servizio insolito che avevamo notato all'inizio: la **Porta 2222**. Era come utilizzare il passaggio segreto dietro la statua della Strega Orba per entrare a Hogsmeade, ma Milena non aveva l'accesso.
Abbiamo quindi indossato il mantello dell'invisibilità e, come utenti comuni (user), abbiamo effettuato un attacco a colpi d'incantesimi ripetuti (a dizionario), fino a riuscire a entrare.

```
$ ssh user@192.168.50.213 -p 2222
```

Password: harry

Eravamo dentro. Ci siamo ritrovati in una stanza di servizio limitata (una shell rbash), simile a uno sgabuzzino per le scope da cui era difficile muoversi. Tuttavia, esplorando la stanza (ls -la), abbiamo trovato un artefatto curioso: accendendo la punta della nostra bacchetta (lumos), una parte della stanza (partizione del disco) ci ha fornito un ultimo indizio: il suo mount point ci svelava il valore di "solennemente".

Grazie a una lezione approfondita di Aritmanzia, abbiamo analizzato la sequenza numerica complessa ottenuta dalle rune, dalle divinazioni e da questo indizio: un ritmo magico da battere su porte specifiche per sbloccare l'ingresso principale.

Il Rituale di Apertura: 9220 -> 1700 -> 9991 -> 55677 -> 37789 -> 7282 -> 65511 -> 12000 -> 41002

Capitolo 5: Alohomora! (Port Knocking)

Siamo tornati fuori dalle mura. Era tempo di eseguire il rituale. Con precisione chirurgica, come fossimo davanti al muro per Diagon Alley, abbiamo "bussato" magicamente su ciascuna delle nove porte spettrali nell'ordine esatto prescritto dalla Mappa.

Con questa sequenza magica e l'incantesimo, abbiamo rivelato la mappa.

```
$ knock 192.168.50.213 9220 1700 9991 55677 37789 7282 65511 12000 41002
```

"Giuro solennemente di non avere buone intenzioni."

Un sordo *click* metallico ha echeggiato attraverso la rete. L'incantesimo di blocco sul Grande Portone di Quercia (Porta 22/SSH standard) era stato infranto.

Abbiamo usato nuovamente le credenziali di Milena, questa volta entrando dall'ingresso principale.

```
$ ssh milena@192.168.50.213 -p 22
```

Eravamo ufficialmente dentro il castello. Nella stanza di Milena, abbiamo recuperato il primo frammento di anima digitale: **La User Flag** FLAG{incanto_della_sapienza_123}.

Capitolo 6: La Pozione Polisucco (Lateral Movement)

Vagando per i corridoi del castello, siamo arrivati alla Sala Grande (la directory /home/shared). L'aria era densa di vapori strani. In un angolo, abbandonato come un calderone lasciato a metà cottura, c'era un file temporaneo nascosto: .myLovePotion.swp.

Era chiaro che la studentessa Milena stava tentando di preparare una pozione d'amore illegale (probabilmente mentre usava l'editor vim). Abbiamo analizzato i residui nel calderone (leggendo il file swap con strings).

Tra gli ingredienti corrotti, abbiamo trovato l'essenza stessa di Luca, Milena e Marco: le loro password in chiaro.

Ingredienti Segreti Estratti: Luca - 9iT(0F98!7^-1&h, Marco - ai(q4P7>(Fw9S3P , Milena - darkprincess

Non restava che bere la Pozione Polisucco. Abbiamo assunto le sembianze di Luca.

```
$ su luca
```

Password: 9iT(0F98!7^-1&h

Capitolo 7: I Doni della Morte (Privilege Escalation)

Ora eravamo Luca, un mago con accesso a segreti più profondi. Nella sua stanza privata, abbiamo trovato un oggetto che emanava un'aura di magia oscura: un file di backup chiamato theta-key.jpg.bk.

Era chiaro che questa immagine era un **Horcrux**: un oggetto comune usato per nascondere un frammento di potere immenso. Sapevamo che conteneva qualcosa, ma serviva una chiave per aprirlo.

Ricordando le nostre lezioni di Babbanologia applicata (analisi del browser), abbiamo recuperato un "Biscotto Magico" (un cookie del browser) che avevamo notato in precedenza. Il biscotto si chiamava "wand" (bacchetta) e aveva un sapore strano: c2MqVDFSOVN5ezVi.

Questa era la nostra **Bacchetta di Sambuco**. Abbiamo usato il valore del biscotto come contro-incantesimo per appropriarci dell'Horcrux (l'immagine di backup) e aprirlo.

```
$ steghide extract -sf theta-key.jpg.bk
```

Passphrase: c2MqVDFSOVN5ezVi

L'immagine si è infranta, rivelando al suo interno la **Pietra della Resurrezione**: una Chiave Privata RSA.

Con questo potere supremo, non eravamo più semplici studenti o intrusi. Avevamo il potere del Preside. Abbiamo usato la chiave per smaterializzarci direttamente nell'ufficio del Root.

```
$ chmod 600 id_rsa_root
```

```
$ ssh -i id_rsa_root root@192.168.50.213
```

Siamo apparsi nella torre più alta. Davanti a noi, il simbolo dei Doni della Morte brillava sulla schermata del terminale. Abbiamo aperto lo scrigno finale (flag.txt) e ottenuto l'ultimo frammento.

Accesso Root Ottenuto. Il castello di HogTheta è sotto il nostro controllo.

"Fatto il misfatto."