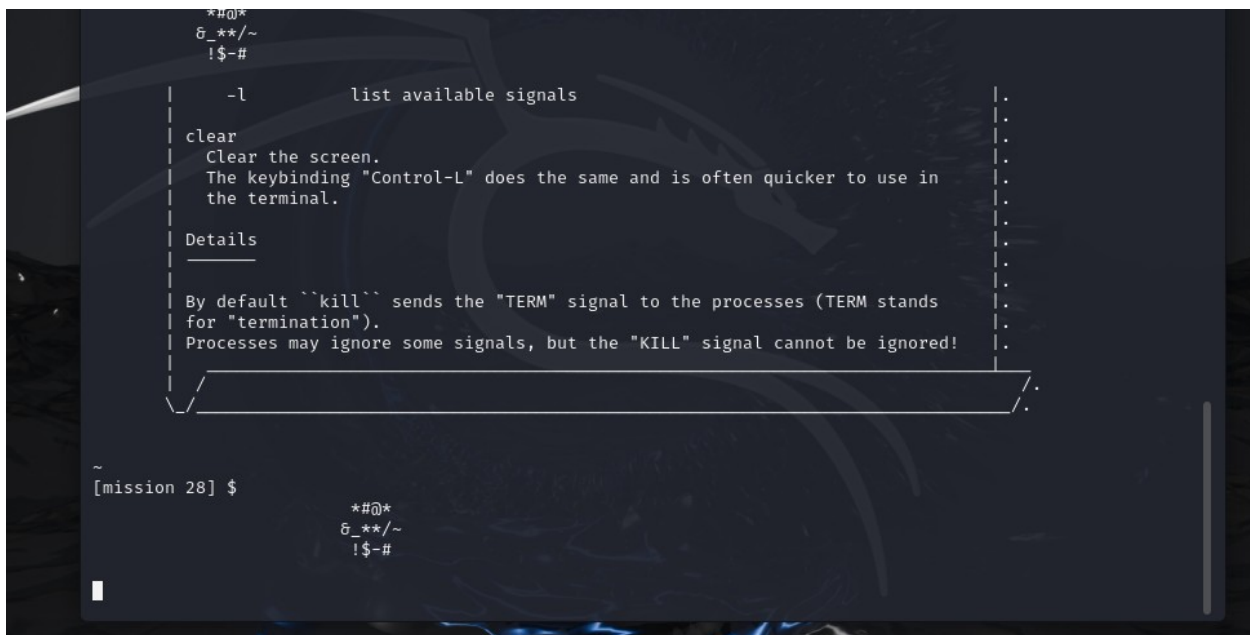


## Benchmark M2 – Daniele Rufo

### Gameshell



```

*#@*
G_**/~
!$-#

-l      list available signals

clear
Clear the screen.
The keybinding "Control-L" does the same and is often quicker to use in
the terminal.

Details
-----

By default ``kill`` sends the "TERM" signal to the processes (TERM stands
for "termination").
Processes may ignore some signals, but the "KILL" signal cannot be ignored!

~
[mission 28] $

*#@*
G_**/~
!$-#
```

Ho completato 27 livelli del gioco, sul 28esimo mi sono incagliato, ma il gioco lo tengo installato prima o poi vincerò.

### Bonus di squadra: Steganografia e linguaggi esoterici

Con steganografia si fa generalmente riferimento all'antica arte di occultare informazioni all'interno di un messaggio o anche di un oggetto. Praticata da millenni si è evoluta nel tempo fino ad arrivare ai giorni nostri dove ha trovato moltissima applicazione anche nel mondo digitale.

Le sue origini risalgono all'antica Grecia: steganografia= "steganos" (nascosto o coperto) e "graphein" (scrittura) e come si può intuire dalla parola stessa veniva usata per celare messaggi, spesso usando intagli nel legno poi ricoperti di cera. La steganografia trovò largo uso anche nell'impero romano, tramite varie forme di inchiostro invisibile che si rivelava esclusivamente in presenza di calore o luce, in Cina, con l'uso della carta da cortecchia, e nel Rinascimento, affinando così negli anni tecnica e flessibilità e rivelandosi ancora utile tutt'oggi in diversi ambiti: quello della cybersecurity è uno di questi.

Indipendentemente dall'ambito usato la steganografia si basa su alcuni concetti chiave sviluppati nel tempo, vediamo quali:

- **Innocuità** - Il messaggio nascosto non deve suscitare sospetti. Il supporto steganografico (come un'immagine, un audio o un video) deve apparire del tutto normale.

- **Capacità** - La capacità è la capienza del messaggio cioè quanto può essere lungo ed articolato. È importante bilanciare la quantità di dati nascosti con la qualità del supporto.
- **Robustezza** - La resistenza del messaggio nascosto a manipolazioni o distorsioni.
- **Segretezza** – La capacità di un messaggio nascosto di non essere rilevabile da terzi.
- **Trasparenza** - La trasparenza si riferisce al grado in cui il supporto steganografico è visivamente o audibilmente indistinguibile dal supporto originale. L'alterazione apportata al supporto per nascondere il messaggio deve essere minima.

Dopo aver fissato questi concetti, che risultano fondamentali per un' applicazione corretta e di successo, possiamo prendere in analisi più da vicino le varie tipologie di steganografia che ad oggi sono utilizzate nel mondo digitale:

### **Testo**

La steganografia di testo prevede che le informazioni siano nascoste all'interno di file di testo. Questo include modificare il formato del testo esistente, cambiare le parole all'interno di un testo, utilizzare grammatiche context-free per generare testi leggibili o generare sequenze di caratteri casuali.

### **Immagini**

Implica che le informazioni vengano nascoste all'interno di file di immagine. Nella steganografia digitale, spesso le immagini vengono utilizzate per nascondere le informazioni perché è presente un numero elevato di elementi (pixel) all'interno della rappresentazione digitale di un'immagine ed esistono diversi modi per nascondere le informazioni all'interno di un'immagine.

### **Audio**

La steganografia audio prevede che i messaggi segreti vengano incorporati in un segnale audio che altera la sequenza binaria del file audio corrispondente. Nascondere messaggi segreti in un suono digitale è un processo che risulta nel complesso più difficile rispetto agli altri.

### **Video**

Avviene quando i dati vengono occultati all'interno di formati video digitali. La steganografia video consente di nascondere grandi quantità di dati all'interno di un flusso in movimento di immagini e suoni. Due tipi di steganografia video sono:

- Incorporare dati in un video non elaborato e non compresso e quindi comprimerlo in un secondo momento
- Incorporare dati direttamente nel flusso di dati compresso

## **Rete**

Detta anche steganografia di protocollo, consiste nella tecnica di incorporare le informazioni all'interno dei protocolli di controllo di rete utilizzati nelle trasmissioni dati quali TCP, UDP, ICMP e così via.

In tempi recenti, la steganografia è stata utilizzata principalmente nei computer assegnando ai dati digitali il ruolo di vettori e alle reti quello di canali di distribuzione ad alta velocità. Gli usi della steganografia ai nostri giorni possono includere metodi per evitare la censura (viene utilizzata per inviare notizie senza che siano censurate e senza il timore che i messaggi siano riconducibili al mittente), oppure la filigrana digitale per creare filigrane invisibili che non distorcono l'immagine riuscendo a tracciare quando viene usata senza autorizzazione.

La steganografia viene inoltre usata dalle forze dell'ordine e dagli organi governativi per inviare informazioni estremamente sensibili ad altre parti senza destare sospetti.

Per lo svolgimento dell'esercizio il gruppo Cypher Squad ha scelto due linguaggi esoterici che spiegheremo brevemente fornendo due esempi di come si possa scrivere una semplice parola come "Hello world".

## **Linguaggio Cow:**

Linguaggio di programmazione esoterico, creato all'inizio del 2003 da Alex van Oostenrijk e Martijn van Beek. utilizza un set di undici istruzioni, composta dalle lettere M e O.

Richiama il verso delle mucche poiché ogni riga di codice è composta solo dalla parola "moo", ma essendo case-sensitive diverse combinazioni sono possibili.

Il linguaggio è strutturato come la macchina di Turing cioè fornisce un vettore di numeri interi e delle istruzioni per spostarsi e modificare i valori contenuti. Inoltre mette a disposizione un registro temporaneo in grado di contenere un numero intero.

Di base funziona grazie all'utilizzo di un puntatore con cui possiamo cambiare il valore nelle celle. Usando i caratteri ASCII dà anche la possibilità di scrivere e celare messaggi nascosti dentro un codice che apparirà come un'infinita serie di muggiti agli occhi dell'osservatore.

Vediamone un esempio che riporta la scritta "Hello World":

```
MoO MoO MoO MoO MoO MoO MoO MoO Moo
MoO MoO MoO Moo
MoO moO MoO MoO Moo
MoO MoO moO MoO Moo
MoO moO Moo
MoO MoO MoO MoO Moo
MoO moO MoO MoO Moo
MoO MoO Moo
```

MoO Moo  
MoO Moo

### **Linguaggio Monicelli:**

Questo linguaggio attinge a piene mani dall'opera cinematografica di Monicelli dal titolo "Amici miei" uscita nel 1975. Nella pellicola ottiene un posto tutto speciale la "supercazzola": "è possibile definire questo neologismo come una sequenza casuale di termini, in alcuni casi inventati, completamente priva di senso. Lo scopo di una supercazzola è quello di ingannare l'interlocutore che fingerà di averla capita perché pronunciata velocemente e composta anche da parole comprensibili o apparentemente tali". Il linguaggio riprende appunto battute celebri del film, così per dichiarare il *main* si scrive "lei ha clacsonato" oppure "vaffanzum <valore>" per la restituzione di un valore. Ecco come risulta il nostro classico esempio "Hello World":

ah però h  
ah però e  
ah però l  
ah però l  
ah però o  
mammamia  
ah però w  
ah però o  
ah però r  
ah però l  
ah però d  
mammamia

Risulta chiaro come l'applicazione più immediata per i linguaggi di programmazione esoterici sia quella di celare messaggi tramite codici difficili da decifrare e da capire perché differenti da qualsiasi altro linguaggio: sono unici e questa è la loro peculiarità principe (in alcuni linguaggi più che in altri).

Vediamo infine come la steganografia può migliorare la protezione dei dati e, più in generale, quali applicazioni trova specificatamente al campo della cybersecurity:

### **Nascondere payload dannosi in file multimediali digitali**

Le immagini digitali possono essere manipolate senza modificare visivamente l'immagine. Anche video, documenti, file audio e addirittura firme e-mail costituiscono potenziali metodi alternativi per utilizzare la steganografia per introdurre payload dannosi.

### **Ransomware ed estrapolazione dei dati**

Anche i criminali dediti al ransomware hanno imparato che usare la steganografia può essere d'aiuto per portare avanti i loro attacchi. La steganografia può essere usata anche

nella fase di estrapolazione dei dati di un attacco informatico. Nascondendo dati sensibili all'interno di comunicazioni legittime, la steganografia fornisce uno strumento per estrarre i dati senza essere rilevati. Considerato che molti attacchi fanno dei dati l'obiettivo principale, gli specialisti della sicurezza affinano sempre più le loro tecniche di implementazione di misure per rilevare quando vengono estratti i dati, spesso monitorando il traffico di rete criptato.

### **Nascondere comandi nelle pagine Web**

Gli autori delle minacce possono nascondere comandi nelle pagine Web con whitespace e all'interno di log di debug pubblicati in forum, caricare di nascosto dati rubati in immagini

### **Malvertising**

Vere e proprie campagne di *malvertising* possono trarre vantaggio dalla steganografia. Possono incorporare codice dannoso all'interno di annunci banner online che, una volta caricati, estraggono un codice dannoso e reindirizzano gli utenti verso una landing page di un kit di exploit.

Grazie. Daniele Rufo