

# PRIMO HOMEWORK: UNA SEMPLICE BOTNET

Elaborato di Reti di Calcolatori 1 – A.A. 2022/23

Alessio Botta

Nel seguito sono riportate le istruzioni per la creazione dell'elaborato (o homework) di Reti di Calcolatori 1 per il corso di Laurea in Informatica. Gli studenti interessati alla preparazione di questo elaborato devono seguire tutte le indicazioni riportate sotto. Per tutto quanto non riportato, gli studenti devono decidere in autonomia come procedere.

## Indicazioni (dovete seguirle)

- L'elaborato si fa in gruppi di massimo 4 studenti.
- L'elaborato si fa in linguaggio python.
- L'elaborato consiste in un applicazione client/server
  - Che usa le socket.
  - Che è in grado di lavorare su macchine diverse.
  - In cui uno dei due componenti (il bot) raccoglie informazioni sulla macchina su cui è eseguito e invia tali informazioni all'altro componente (il bot master).
  - Il bot non deve modificare niente sulla macchina su cui è eseguito ma deve raccogliere informazioni sulla stessa.
  - Le informazioni che il bot deve raccogliere possono includere, ad esempio, la CPU, la memoria, il sistema operativo (tipo, versione, patch level, etc.) e i file presenti sul file system.
- Il bot dovrà essere eseguito su una macchina che metterà a disposizione il docente e dovrà scoprire quante più cose possibile su questa macchina. Dovrà quindi comunicare al master queste informazioni attraverso la rete.
- Gli studenti avranno la possibilità di provare i loro programmi in una prima sessione (di prova) sulla macchina del docente. Durante la prova, il docente eseguirà i bot sulla sua macchina e gli studenti dovranno comunicare con questi usando i loro bot master.
- In seguito, dopo una settimana almeno, ci sarà la sessione finale in cui gli studenti dovranno eseguire la prova finale. La macchina sarà la stessa durante le due sessioni (stesso hardware e sistema operativo) ma sarà ripulita. Alcune informazioni della macchina potrebbero cambiare (cioè dovete raccoglierle nella seconda sessione). La sessione avrà una durata limitata e il bot potrà essere lanciato una sola volta dal docente sulla macchina. Nella macchina ci potranno essere delle informazioni nascoste di particolare interesse (es. file contenenti codici, password, etc.).
- Al termine della seconda sessione gli studenti dovranno preparare un breve report (massimo 2 pagine) in cui dovranno descrivere quanto fatto: le scelte fatte, le prove effettuate, quanto scoperto sulla macchina del docente.
- Il report potrà includere, a discrezione degli studenti, una pagina aggiuntiva che gli studenti devono utilizzare per illustrare il comportamento sulla rete delle applicazioni durante la prova finale. La pagina aggiuntiva dovrà contenere delle immagini che mostrano il traffico scambiato tra il bot e il master catturato con wireshark e una spiegazione dei pacchetti catturati. L'inclusione della pagina aggiuntiva darà diritto ad un bonus sulla valutazione finale.

## Suggerimenti (potete seguirli)

- Il bot può raccogliere informazioni una tantum e poi inviarle al master quando si collega a questo, oppure raccoglierle solo quando collegato a questo.
- Il bot può fare da server o da client. In caso faccia da client, il bot dovrà cercare periodicamente di collegarsi al master (il server) che potrà esserci o meno.

- E' opportuno fare tante prove, auspicabilmente su macchine diverse, prima di quella messa a disposizione dal docente.

Scadenze (dovete rispettarle: il non rispetto di una sola scadenza, comporta il fallimento della prova)

- 30-10-2022
  - Compilazione del form messo a disposizione dal docente con le indicazioni circa il nome e la composizione del gruppo
- 11-11-2022
  - Invio del prototipo delle applicazioni, avendo curato in primo luogo la parte di raccolta delle informazioni
- Un giorno da fissare tra il 14 e il 28 novembre 2022
  - Prima prova delle applicazioni sulla macchina del docente
- 11-12-2022
  - Invio della versione completa delle applicazioni da usare durante la prova finale
- Un giorno da fissare tra il 12 e il 16 dicembre
  - Prova finale delle applicazioni sulla macchina del docente
- 18-12-2022
  - Invio della relazione al docente

#### DISCLAIMER IMPORTANTE

Le botnet sono spesso utilizzate per scopi illegali (es. compromissione di infrastrutture critiche, furti, ricatti, diffusione di materiali pedopornografici, etc.). L'elaborato non vuole in nessun modo incentivare gli studenti a violare la legge. Lo scopo dell'elaborato è invece quello di ottenere maggiore conoscenza e consapevolezza di come funzionano queste applicazioni che rappresentano una grave minaccia alla sicurezza informatica e di rete. Gli studenti sono e restano i soli responsabili della loro condotta.