UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
SCUOLA POLITECNICA E DELLE SCIENZE DI BASE
DIPARTIMENTO DI INGEGNERIA ELETTRICA E TECNOLOGIE DELL'INFORMAZIONE

Reti di Calcolatori

Implementazione di una Botnet in Python
Nome Gruppo: Bot Tattici Nucleari

Giorgio Longobardo N86003571
Gianluca Perna N86003172
Giuseppe Francione N86003734
Claudio Simonelli N86003781

Anno Accademico 2022/2023

Docente:
Alessio Botta

Indice

Capitolo 1

Progetto di Reti

1.1 Descrizione del progetto

Bot Tattici Nucleari è un progetto deputato allo sviluppo di una Botnet in linguaggio Python: in particolare, le funzionalità principali sono quelle di reperire informazioni da remoto di un PC (client) e inviarle, mediante una connessione stabilita tramite socket, al PC di controllo (server o master), indipendentemente dal tipo di macchina e dal sistema operativo in uso.

1.2 Cronologia sviluppo del progetto

Il progetto contiene due file eseguibili portanti: il primo, *botmaster.py*, avvia il server con protocollo TCP e IPv4, riceve le informazioni dai client ed esegue i comandi di controllo mentre, il secondo, *botslave.py*, si connette al server creato (con IP e porte specifiche), manda le prime informazioni di sistema ed esegue eventualmente i comandi ricevuti dal botmaster.
Per la realizzazione della funzionalità dell'ottenimento delle informazioni, inizialmente la nostra idea era di utilizzare alcune delle funzioni implementate e disponibili della libreria psutil, ma abbiamo notato che sarebbe stato un lavoro troppo laborioso e prolisso: quindi, dopo aver stabilito la connessione ed aver identificato il sistema operativo in uso, abbiamo implementato in botmaster una send che invia un comando di controllo (cmd se il sistema operativo in uso sia Windows, bash altrimenti) e una recv corrispondente in botslave che utilizza la stringa ricevuta come comando di sistema (utilizzando la libreria subprocess). In questo modo, le informazioni della macchina in uso si possono ottenere con maggiore facilità e con meno righe di codice.
Un'altra funzionalità implementata è la capacità di navigare fra le cartelle e ottenere i file. Per questo motivo il botmaster dispone di altri tre comandi: ls, cd e get che servono, rispettivamente, a visualizzare in quale cartella di navigazione ci si trova, a navigare in un percorso specificato e a ottenere un file scelto. Per la realizzazione di queste funzionalità viene usata la libreria os system.
Questi comandi, insieme alla capacità di inviare i comandi di sistema al botslave, ricoprono la funzionalità di invio delle informazioni.
Una volta implementati questi comandi, ci era sorto il problema della perdita della connessione mentre uno dei due file era in uso. Per ovviare a questo problema, abbiamo inizialmente ideato a implementare due Thread, uno in botmaster e uno in botslave, che utilizzassero una socket e una porta dedicata, e questi si sarebbero dovuti inviare informazioni banali: se uno dei due non avesse ricevuto le informazioni, allora sarebbe stato attivato un flag che ci avrebbe avvisato della perdita della connessione. Un altro problema che abbiamo provato a prevenire era l'avvio di botslave prima dell'avvio di botmaster, poichè, se botslave non avesse trovato il server, si sarebbe spento senza fare altre computazioni. Dunque abbiamo messo in un ciclo il tentativo di connessione che sarebbe terminato una volta stabilita la connessione.
A questo punto abbiamo provato i nostri eseguibili e abbiamo effettuato test diversi su macchine diverse, non riscontrando particolari problemi.

1.3 Prima sessione di prova

Alla prima sessione di prova, abbiamo riscontrato un problema grave relativo all'ottenimento delle informazioni sulla macchina. I due bot si connettevano ma il botmaster non riceveva le informazioni iniziali. Apparentemente il problema sembrava fosse legato esclusivamente alla macchina del docente, poichè il malfunzionamento non si era mai presentato prima. Inizialmente pensavamo fosse un blocco legato al firewall delle nostre macchine ma l'errore persisteva.
Successivamente, abbiamo pensato che il problema fosse il thread di controllo della connessione. Una volta rimosso, continuava a persistere. Grazie all'aiuto del professore, avendo avuto a disposizione un'ulteriore prova, abbiamo individuato il problema nella funzione di attesa della connessione, e, una volta riformulata quella funzionalità, tutto ha ripreso a funzionare correttamente.

1.4 Seconda sessione finale

Nella sessione finale i due bot si sono connessi correttamente, abbiamo utilizzato i comandi implementati e registrato tutto su dei file di log. Entrambe le macchine eseguivano come sistema operativo Linux (Ubuntu), l'user in esecuzione era alessio, la macchina aveva come nome "Ubuntu-20-04-LTS", il processore era basato su x86, aveva come indirizzo IP 127.0.1.1 e disponeva di 3GB di RAM. Sono stati reperite molte altre informazioni, come ad esempio i pacchetti installati, il path dove girava l'eseguibile, il numero di partizioni e relative informaizoni. Per maggiori dettagli si possono consultare i file di log cliccando qui.

1.5 Conclusione

E' stato utilizzato git per lavorare sul progetto, la repository è pubbica ed è accessibile cliccando su questo link.

Giorgio Longobardo
Claudio Simonelli
Gianluca Perna
Giuseppe Francione