

Is the server running on host "localhost" (:::1) and accepting
TCP/IP connections on port 5432?
could not connect to server: Connection refused
Is the server running on host "localhost" (127.0.0.1) and accepting
TCP/IP connections on port 5432?

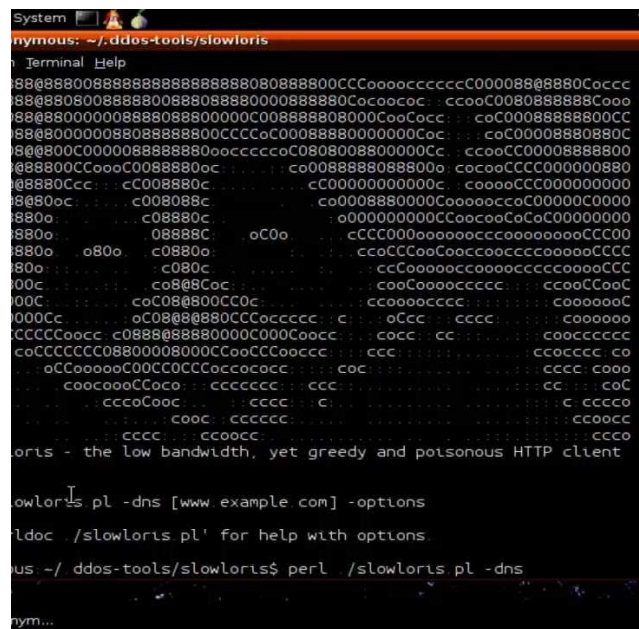
CYBERSECURITY: ATTACCHI INFORMATICI E COME PREVENIRLI

In questa presentazione tratteremo il
rischio degli attacchi informatici e di
vari metodi utilizzati possono aiutarci
a prevenirli

```
+ -- --=[ exploits - 1019 auxiliary - 310 post ]  
+ -- --=[ 538 payloads - 41 encoders - 10 nops ]  
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
```

msf >

COSA SONO GLI ATTACCHI INFORMATICI:

A screenshot of a terminal window titled 'System'. The prompt is 'nymous: ~/ddos-tools/slowloris'. The terminal shows a series of commands and their outputs. The first command is 'perl /slowloris.pl -dns [www.example.com] -options'. The output is 'ldoc /slowloris.pl' for help with options. The second command is 'perl /slowloris.pl -dns'. The output is 'loris - the low bandwidth, yet greedy and poisonous HTTP client'. The terminal also shows a list of options for the slowloris tool, including '-dns', '-url', '-port', '-delay', '-count', and '-help'.

Gli attacchi informatici possono essere spiegati brevemente come dei tentativi di accesso, furto e danneggiamento di dati. Questi tipi di attacchi possono essere svolti da una sola persona o anche da più persone, tra quelli che tratteremo oggi ci sono ---->

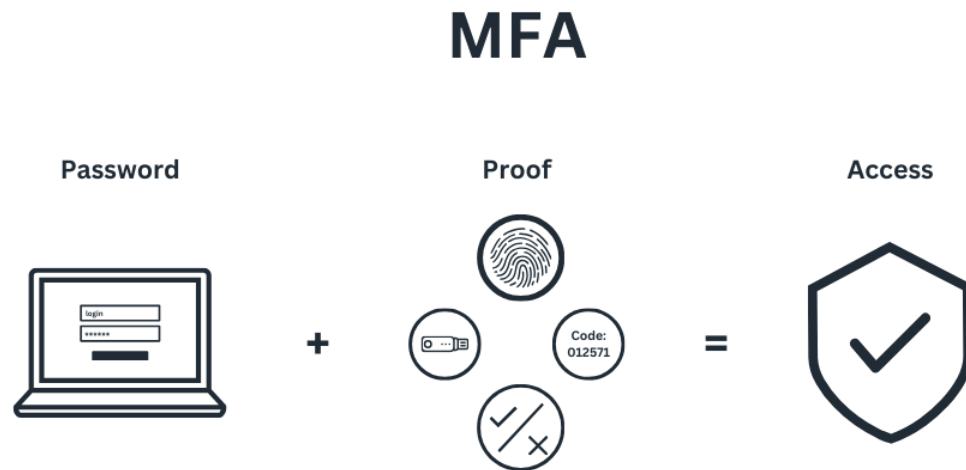
Man-In-The-Middle : Un attacco in cui l'aggressore intercetta la comunicazione tra due host per spiarla o manipolarla.

Sniffing: Quando un aggressore intercetta e registra il traffico di rete che transita, per esempio una rete Wi-Fi non protetta, ciò permettere di catturare informazioni sensibili come password, dati di login o altre comunicazioni.

Phising: Un tentativo fraudolento di ottenere dati sensibili come ad esempio una password, tramite ad esempio un link fingendosi enti affidabili.

Dos: è Un attacco volto a rendere un servizio online non disponibile tramite un sovraccaricamento del traffico con per esempio dei pacchetti.

BASTANO SEMPLICI AZIONI PER PREVENIRE QUESTI TIPI DI ATTACCHI, COME:



Usare Password forti e sicure .

Crittografare il traffico di rete sensibile: Utilizza protocolli sicuri come HTTPS per il traffico web e VPN per connessioni remote per proteggere i dati in transito.

Mantenere software e firmware aggiornati: Aggiorna regolarmente il sistema operativo, i software applicativi e il firmware dei dispositivi di rete (router, switch, firewall). Le patch spesso correggono vulnerabilità di sicurezza che potrebbero essere sfruttate.

Implementare l'autenticazione multi-fattore (MFA): Ove possibile, abilita l'MFA per aggiungere un ulteriore livello di sicurezza. Questo richiede una seconda forma di verifica oltre alla password (ad esempio, un codice inviato al telefono).

STANDARD DI SICUREZZA RETE:



- WEP (Wired Equivalent Privacy): Il primo standard di sicurezza Wi-Fi. Insicuro e obsoleto.
- WPA (Wi-Fi Protected Access): Introdotta come miglioramento temporaneo a WEP. Più sicuro di WEP, ma anch'esso considerato obsoleto.
- WPA2 (Wi-Fi Protected Access 2): Standard più sicuro che ha utilizzato per anni l'AES (L'algoritmo di crittografia vero e proprio, che "mescola" i dati per renderli incomprensibili senza la chiave) con CCMP (È un protocollo che *usa* l'AES, ma aggiunge delle funzionalità extra). Sono state scoperte vulnerabilità.
- WPA3 (Wi-Fi Protected Access 3): Lo standard più recente e sicuro, offre una crittografia più robusta e nuove funzionalità di protezione. Raccomandato per le nuove configurazioni.

CONCLUSIONI:

La presenza di tutto questo ci fa capire l'importanza che dobbiamo dare alla sicurezza dei nostri dati personali e dei dispositivi. Pertanto bisogna agire con azioni di prevenzione come lezioni a studenti ecc. , combinate con uso di misure tecniche.

