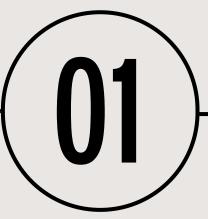


TCP VS UDP

1ER PASO EN HACKING







TCP

Transmission Control Protocol es un protocolo orientado a conexión. Cada paquete tiene que ser confirmado por el receptor. Si se pierde algo, se reenvía

¿Dónde se usa?

- HTTP/S
- FTP
- SSH

- Telnet
- Email (SMTP, IMAP POP3)





02

¿CÓMO LO USAN LOS HACKERS? • Bruteforce el

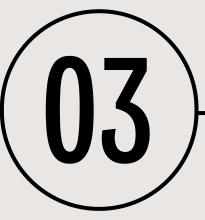
Tips:

- No expongas servicios TCP innecesarios a internet.
- Usá versiones cifradas (SFTP en vez de FTP, HTTPS en vez de HTTP).
- Monitoreá conexiones repetidas o inusuales

- Bruteforce en servicios como FTP, SSH o Telnet, aprovechando respuestas del servidor.
- Sniffing de datos
 sensibles si no hay cifrado
 (como contraseñas en
 Telnet o HTTP).
- Port scanning con ACK o SYN para identificar servicios expuestos.









User Datagram Protocol es más liviano. No hay verificación de entrega ni retransmisión. Se manda y ahí queda

¿Dónde se usa?

- Streaming (video/audio)
- Juegos online
- DNS

- SNMP
- VolP





04

¿CÓMO LO USAN LOS HACKERS?

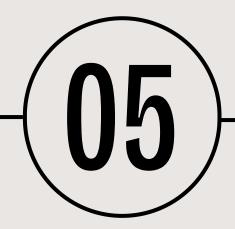
Tips:

- DDoS por amplificación, como con DNS o NTP.
- Scanning sin conexión
 (UDP scan), más sigiloso
 que TCP.
- DNS tunneling para evadir firewalls.

- No dejes puertos UDP abiertos sin necesidad.
- Filtrá tráfico UDP saliente raro o fuera de horario.
- Usá reglas específicas en el firewall (por IP y puerto).







	ТСР	UDP
¿Conexión previa?	Sí	No
¿Fiabilidad?	Alta	Baja
¿Velocidad?	Más lento	Más rápido
¿Dónde se usa?	Web, Email, SSH	Juegos, DNS, Streaming
¿Cómo lo abusan?	Bruteforce, sniffing	DDoS, tunneling







SEGUINOS Y UNITE AL DISCORD PARA SEGUIR APRENDIENDO





