

# Drone Patrol



**it's time to rethink the security concept!**

A great cyber security and development company

Drone Patrol

# Drone Patrol

## DRONE PATROL

### PERCHÉ UTILIZZARE UN DRONE?

L'utilizzo di un drone consente di raggiungere location non raggiungibili da un umano. Si pensi ad organizzazioni il cui perimetro esterno risulta perfettamente difeso da varchi di accesso impenetrabili. L'attaccante in questo caso, per verificare vulnerabilità presenti su dispositivi utilizzando canali di comunicazione wifi o bluetooth, dovrebbe sfruttare elementi di ingegneria sociale, in modo tale da riuscire ad oltrepassare i varchi di accesso esterni, con tutti i pericoli derivanti (è sufficiente pensare all'esposizione diretta della persona ad eventuali registrazioni video o all'interazione fisica diretta dell'ingegnere sociale con altre persone, eventualità questa solitamente lasciata come extrema ratio da parte dell'attaccante). L'attaccante potrebbe quindi pensare di sfruttare un drone per avvicinarsi il più possibile al perimetro interno.



## ATTIVITÀ

### COSA INTENDIAMO CON IL TERMINE DRONE PATROL?

Si tratta di una ricognizione, effettuata da un pilota di drone abilitato ENAC (*i piloti e operatori che collaborano con SEC4U possiedono certificazione per scenari critici [certificazione CRO] che consente di pianificare missioni in centro abitato. Inoltre le operazioni sono eseguite con i più alti livelli di sicurezza e ogni missione viene valutata tramite piano di volo e valutazione del rischio da personale specializzato*), che fa volare, lungo il perimetro dell'organizzazione, un drone equipaggiato con una sonda basata su hardware Raspberry, con lo scopo di verificare eventuali vulnerabilità nell'ambito dell'infrastruttura wireless e sui dispositivi bluetooth

presenti.



## OBIETTIVI

Con questa attività si vuole simulare il comportamento di un attaccante che si trova di fronte ad una situazione complessa dal punto di vista della buona riuscita dell'attacco. Il drone, fatto volare dal pilota abilitato ENAC, viene controllato remotamente dal personale di SEC4U, attraverso una connessione vpn instaurata con il dispositivo Raspberry (dotato di modem GSM).



Una volta oltrepassato il perimetro esterno aziendale ed avvicinato il drone al perimetro interno, vengono eseguite diverse attività di scanning volte ad identificare la presenza di network wifi e dispositivi bluetooth. Si passa quindi successivamente ad attività di verifica di eventuali accessi non protetti o dispositivi vulnerabili.

## PERSONALE CERTIFICATO

SEC4U esegue le attività di Vulnerability Assessment e di Penetration Test avvalendosi di personale altamente qualificato e certificato CEH (Certified Ethical Hacker) e eCPPT (eLearnSecurity Certified Professional Penetration Tester).

