Linux Day 2014 - 22 ottobre - Mix Art

Honey Pot Hack

Giuseppe Augiero

Di cosa parliamo?

- L’**honey pot** è un componente hardware o software utilizzato in ambito della sicurezza informatica come esca.

- Ottima soluzione per analizzare le tecniche e i comportamenti di un attaccante.

- “Erogatore di informazioni”:
    - Natura degli attacchi.
    - Frequenza degli attacchi.

Complemento

- L’honey pot è un ottimo complemento al firewall e all’ids.

- Non viene analizzato tutto il traffico di rete ma solo quello “effettivamente malevolo”.

- E’ possibile installare più honeypot sia all’interno della propria rete che all’esterno.

- E’ possibile studiare i vari “trend di attacco”.

Sicurezza

- Gli honey pot possono essere stessi un pericolo alla sicurezza?

- Vanno “maneggiati” con cura”.

- Potrebbero diventare il punto di ingresso alla nostra rete.

- La scelta di un honeypot deve essere molto oculata.

- Occorre chiedersi se occorre realmente.

Iterazione

- Gli Honeypot si classificano per il loro grado di iterazione:
  - bassa interazione: emulano sistemi operativi e servizi.
  - alta interazione: non emulano ma sono veri computer o applicazioni o servizi.

Vantaggi/Svantaggi

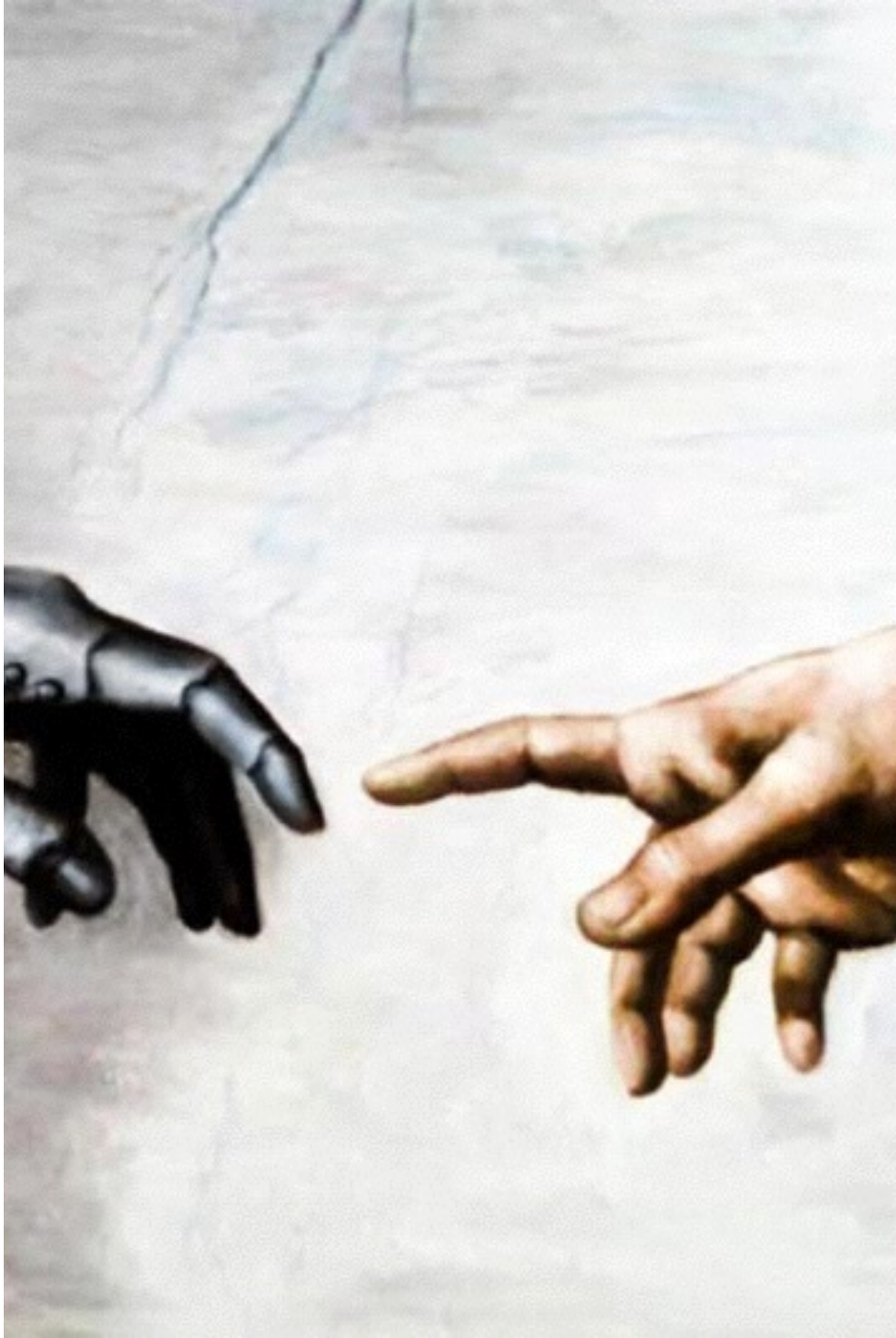
- Gli honeypot a bassa interazione emulando i servizi analizzati sono più sicuri ma per la loro architettura offriranno meno informazioni sugli attacchi avvenuti.

- Quelli ad alta interazione, essendo vere e proprie macchine adibite a questa attività, forniranno maggiori informazioni ma saranno altamente più insicure delle prime.

- I primi sono più semplici da installare.

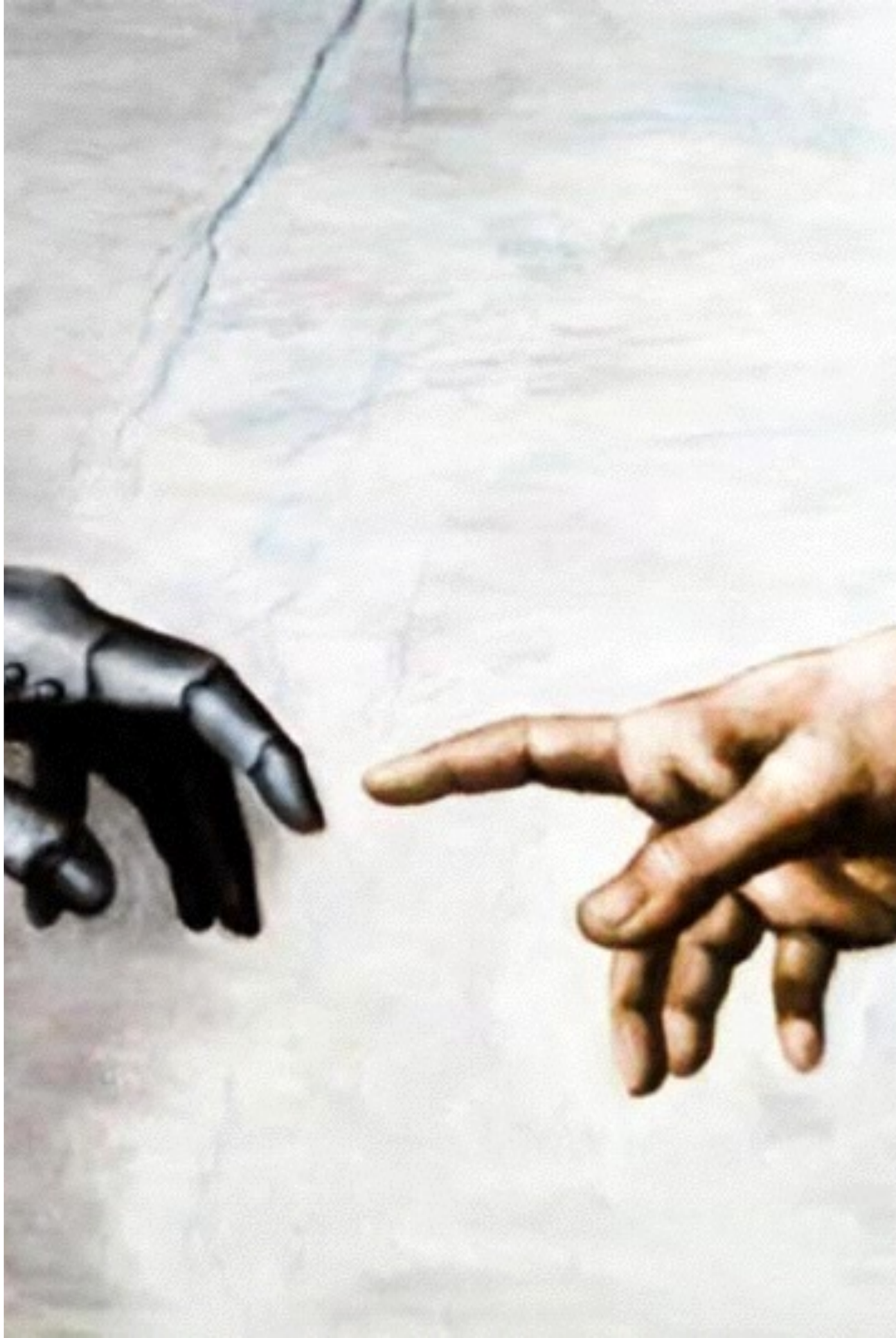
Bassa interazione

- Buoni quasi solo per attacchi automatici (bot,worm,…).
- Richiedono molte meno cure.
- Più resistenti ad exploit sbagliati (niente crash/riavvi se l’attaccante sbagli un offset).
- Computazionalmente meno esigenti.
- Indubbiamente piu’ sicuri per la nostra rete.



Alta interazione

- Difficili o quasi impossibili da rilevare come honeypot.
- Libertà dell’attaccante completa o quasi.
- Difficile trovare un buon compromesso tra sicurezza e libertà dell’attaccante.
- Computazionalmente più esigenti.



Utile?

- Possiamo determinare l'efficienza di un Honeypot?
- Di fatto non può di rilevare o impedire attacchi verso macchine reali
- La sua efficienza dipende da dove viene collocato.
- Il numero di falsi positivi in alcuni casi è praticamente nulla.

L’attaccante

- L’attaccante, fino a quando non si accorgerà di essere in trappola, perderà tempo per attaccare ed impadronirsi del nostro honey pot.

- La regola del gioco è “tenere occupato l’attaccante”.

Kippo

- Kippo emula un servizio ssh protetto da password debole.
- Prevalentemente raccoglie informazioni sugli attacchi a forzabruta edizionario contro ssh.
- Permette di loggare ogni input della sessione dell’attaccante.
- Pacchettizzato per debian.

Cosa offre

- Lista delle password da non utilizzare.
- Lista degli ip da banner .
- Possibilità di studiare il comportamento di chi ci vuole attaccare.
- Avere copia del software utilizzato dagli attaccanti.

Kippo Runtime

- Vediamo un esempio in funzione.

EMAIL: TALK@AUGIERO.IT

TWITTER: @GIUSEPPEAUGIERO

WWW.AUGIERO.IT

Linux Day 2014 - 22 ottobre - Mix Art

Honey Pot Hack

Giuseppe Augiero