CONFINDUSTRIA
VENETO EST
Area Metropolitana
Venezia Padova Rovigo Treviso

INNOVATION ROADMAP

Webinar tematici: INTELLIGENZA ARTIFICIALE

CYBERSECURITY PER L' AI E LA FABBRICA CONNESSA

Hacking 2.0

Potenziare il Red Teaming con Soluzioni AI

David Tancredi – CISO & Offensive Security Lead (Trevigroup Srl)

16 Giugno 2026

CHI SONO

David Tancredi

Offensive Security Lead

specializzato in sicurezza informatica
e protezione dei dati per Trevigroup Srl

CONFINDUSTRIA
VENETO EST

I Limiti del VAPT Tradizionale

APPROCCIO STATICO E TEMPORALE

- **Fotografia Istantanea:** Un VAPT classico mostra la sicurezza in un solo momento, invecchiando all'istante.
- **Mancata Continuità:** Le modifiche all'infrastruttura avvengono giornalmente, i test sono invece annuali.
- **Scarsa Scalabilità:** Impossibile monitorare superfici d'attacco in costante espansione manuale.

DIPENDENZA DA RISORSE UMANE

- **Costi Elevati:** Elevate tariffe orarie dei penetration tester umani senior per task ripetitivi.
- **Falsi Positivi:** Spreco di tempo prezioso dei team interni nel filtrare report generati da scanner tradizionali.
- **Saturazione del Team:** Gli esperti passano l'80% del tempo sulla noiosa ricognizione iniziale anziché sulla logica d'attacco.

CONFINDUSTRIA
VENETO EST

Automazione dell'intera Kill Chain

1

RECON INTELLIGENTE

Mappatura continua ed autonoma dei target, identificando sub-domain e servizi esposti in real-time senza istruzioni statiche.

2

EXPLOITATION ADATTIVA

Gli agenti decidono quali exploit testare in base al contesto, provando percorsi multipli e correggendo gli errori dinamicamente.

3

REPORTING AUTONOMO

Validazione immediata delle scoperte, rimozione automatica dei falsi positivi e scrittura automatizzata di report strutturati.

CONFINDUSTRIA VENETO EST

La Minaccia: Agenti AI Malevoli

Anche gli Hacker usano soluzioni agentiche

Gli attori di minaccia (Threat Actors) non aspettano. Stanno già implementando l'intelligenza artificiale per l'offensiva.

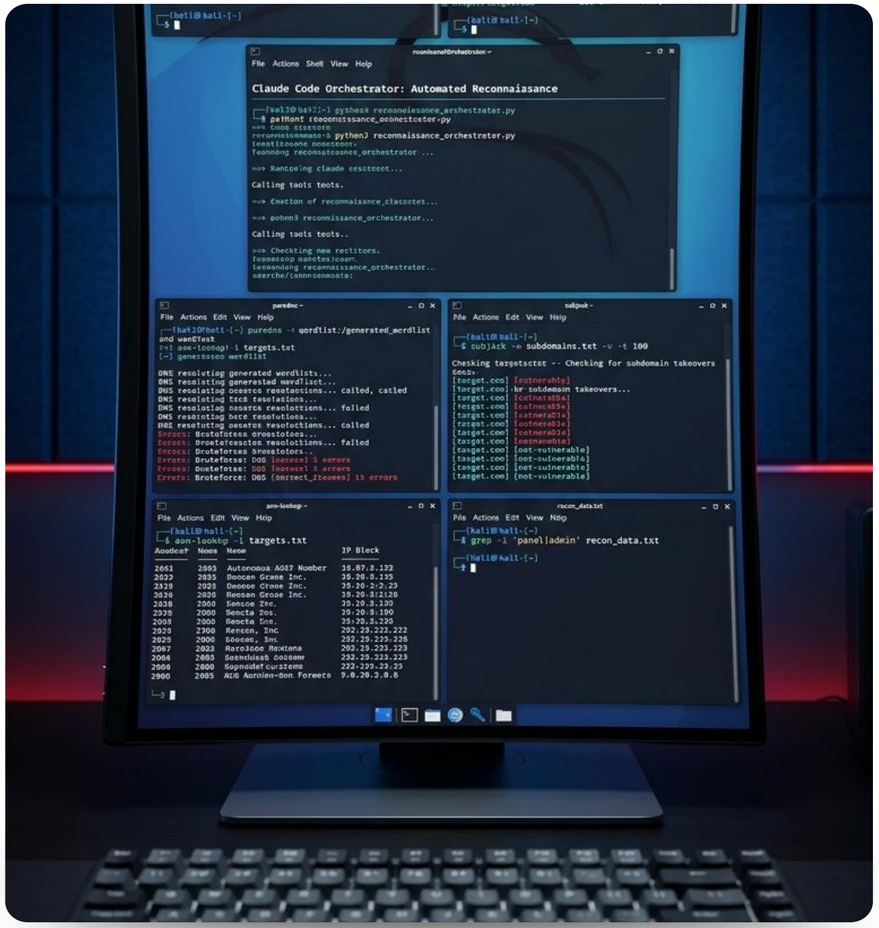
Attacchi Multi-vettore Scalabili: Campagne massive condotte da bot intelligenti.

Recon ultra-veloce: Individuazione istantanea di falle zero-day appena rilasciate.

Adattabilità al Target: Payload mutogeni creati ad-hoc dagli agenti per eludere gli EDR.

CONFINDUSTRIA VENETO EST

Live Demo: Recon con Claude Code



Vedremo come sfruttare in modo pratico l’agente Claude Code per automatizzare completamente la fase iniziale di test di penetrazione in sicurezza.

- Definizione dello scope di un programma reale di Bug Bounty.
- Esecuzione autonoma di strumenti CLI di ricognizione passiva ed attiva.
- Filtro e validazione intelligente dei record scoperti da parte di Claude.
- Identificazione automatica di potenziali vettori di Subdomain Takeover.

CONFINDUSTRIA VENETO EST

kali-linux-2025.4-vmware-amd64 - VMware Workstation Player 25H2

File Virtual Machine Help

1 2 3 4 11:18

✳ Subfinder Tool Availability

Session Actions Edit View Help

(hexstrike-env)root@kali: /home/kali/demo/hexstrike-ai | (hexstrike-env)root@kali: /home/kali/demo/hexstrike-ai | root@kali: /home/kali | ✳ Subfinder Tool Availability

```
  2. hexstrike_mcp.py - Running as PID 105700 on pts/3

  Both processes have been running since around 10:48-10:49 and are active. Let me also check if they're configured in the Claude Code MCP
  settings.

● Searched for 1 pattern (ctrl+o to expand)

● Bash(netstat -tuln | grep LISTEN | grep -E ":(8|9)[0-9]{3}")
  ⎿  Interrupted · What should Claude do instead?

❯ do we have subfinder in this kali installation?

● Searched for 1 pattern (ctrl+o to expand)

● Yes! Subfinder is installed at /usr/bin/subfinder. Let me check the version to confirm it's working.

● Bash(subfinder -version)
  ⎿  Interrupted · What should Claude do instead?

─────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────
❯ leverage subfinder to
─────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────
```

CONFINDUSTRIA VENETO EST

Il Vantaggio dell'Agentic Red Teaming

Costi e Tempi Abbattuti

90%

Vantaggi di Tempo ed Economia rispetto al VAPT Classico

Mentre un VAPT classico richiede settimane di pianificazione, l’approccio agentico esegue la ricognizione e la mappatura iniziale in pochissimi minuti, riducendo drasticamente il costo orario dell’operazione.

Questo permette alle aziende di fare “Continuous Testing” 24/7 anziché limitarsi a una singola scansione annuale, ottimizzando le risorse umane del team Blue & Red Team solo su vulnerabilità ad alto valore.

Per informazioni:
ricercainnovazione@confindustriavenest.it

Grazie per l’attenzione.

CONFINDUSTRIA
VENETO EST