



HACKTHEBOX

Hack The Box

Μια ολοκληρωμένη λύση cyber readiness και ανάπτυξης δεξιοτήτων cybersecurity ομάδων.



Οι κορυφαίες cybersecurity ομάδες
δεν δημιουργούνται στις αίθουσες διδασκαλίας.
Διαμορφώνονται μέσα από συνεχή ανάπτυξη δεξιοτήτων,
επικυρωμένη από τις απαιτήσεις του κλάδου.


Η **Hack The Box** μετατρέπει τη μάθηση σε βίωμα,
προσελκύοντας τα πιο προηγμένα talέντα στον χώρο,
βοηθώντας τους να αναβαθμίζουν συνεχώς
τις δεξιότητές τους σε κορυφαίο επίπεδο.



Τι Προσφέρουμε



Ανάπτυξη **Δεξιοτήτων**
Κυβερνοασφάλειας



Ανάπτυξη **Εργατικού**
Δυναμικού Κυβερνοασφάλειας



Πιστοποίηση &
Επιχειρησιακή Ετοιμότητα



Εκτεταμένη Κάλυψη Cyber Domains & Ρόλων



AI



Coding



DevSecOps



Red Teaming
/ APTs



ICS /
SCADA



Mobile



Networking



Gaming



Blockchain



Wi-Fi



OSINT



Quantum



Cloud



SOC / DFIR



Hardware



GRC

And
more...

Offensive

- (Web) Penetration Tester
- Red Team Operator
- Cloud Penetration Tester
- AI Red Teamer etc.

Defensive

- SOC/DFIR Analyst
- Malware Analyst
- Detection Engineer
- SIEM Engineer
- Cloud Security Engineer etc.

General IT & Mgmt

- Software Developer
- IT Manager
- NOC/SOC Manager
- GRC Analyst
- CISO / DPO



Cyber Mastery

2.200+

εργαστήρια και
εκπαιδευτικό περιεχόμενο

Νέο
εκπαιδευτικό
υλικό
σε εβδομαδιαία
βάση



9

αναγνωρισμένα
προγράμματα
πιστοποίησης

1

αναγνωρισμένο
certificate program
από US DoD 8140

Community Inspired

4.3M+

μέλη στις πλατφόρμες

19M+

ώρες εξάσκησης / έτος

131

τοπικές
κοινότητες και
συναντήσεις

Enterprise Trusted

1.5K+

οργανισμοί,
συμπεριλαμβανομένων
εταιρειών Fortune 100



EA SPORTS



TOYOTA

SIEMENS

Deloitte.

intel



Πως Το Προσφέρουμε

AI-Augmented Pentesting Foundations

CREATOR: vaulia | LAST UPDATED: 19 Jun 2026

Note: This module is a **bring-your-own-API-key** module. To complete the module, you need access to an LLM, for instance, through an API key from any popular LLM provider.

With the rapid advancement of **Artificial Intelligence (AI)**, penetration testing engagements can benefit greatly from **AI assistance**, increasing efficiency and scalability. AI is a powerful tool that human testers need to learn to use to their advantage.

In this module, we will cover:

- **AI-augmented penetration testing:** Foundations of AI assistance in offensive engagements, including benefits, risks, and integration into traditional workflows.
- **Governance:** Safely using AI in corporate environments.
- **Prompt engineering:** Crafting effective prompts for common penetration testing use cases.
- **Managing the context window:** Dealing with large input data from artifacts such as tool outputs to avoid model performance degradation.
- **AI-augmented analysis:** Using AI for artifact analysis and the importance of manual verification.

This module is broken into sections with accompanying hands-on exercises to practice each of the tactics and techniques we cover. The module ends with a practical hands-on skills assessment to gauge your understanding of the various topic areas.

You can start and stop the module at any time and pick up where you left off.

- 1 Intro to AI-Augmented Penetration Testing
- 2 Governance & Environment Setup
- 3 Prompt Engineering for Penetration Testing
- 4 Managing the Context Window
- 5 AI-Augmented Analysis & Verification Discipline
- 6 Skills Assessment

Your Progress: 100%

Continue Learning

SillyEli

7: 2018 - Hard

PLAY SHERLOCK ABOUT ACTIVITY RECOMMENDATIONS

You are viewing as Admin.

Switch to Member view

Solve the Sherlock Solve It OFFICIAL WRITEUP

Eli, a recent addition to the IT team, is eager to settle into his new role. Due to the company's flexible "Bring Your Own Device" (BYOD) policy, which applies to everyone except IT administrators, Eli receives a newly prepared PC from Metushelah, the senior IT administrator, as part of the IT team's secure device protocol. Eli's first priority is to install essential applications that will enable him to connect seamlessly with the rest of the team. He begins setting up the system and downloading the necessary software. After a few days on the job, Eli starts noticing something unusual: every so often, a PowerShell window flashes on his screen, disappearing almost instantly, too quickly to read any of its contents. Assuming it's just a minor glitch, Eli continues with his work. However, as the unsuspected PowerShell pop-ups persist, Eli decides to confront Metushelah. Metushelah suspects these PowerShell flashes could indicate malicious activity. To ensure there are no security breaches, he conducts a forensic acquisition of Eli's PC and forwards it to the Incident Response team for further analysis. Now, as a member of the IR team, your mission is to investigate Eli's workstation.

allipen1.cip

QUESTION 1

Identify the specific time the malware was downloaded in UTC.

YYYY-MM-DD HH:MM:SS

Solve It

QUESTION 2

Which domain name was the file downloaded from?

.....

Solve It

QUESTION 3

Identify the SHA-1 hash of the malware.



Θεωρία

Εξάσκηση



Πως Το Προσφέρουμε

AI-Augmented Penesting F

MODULE **NEW**

Note: This module is a **bring-your-own-API** key module, you need access to an LLM, for instance, through any popular LLM provider.

With the rapid advancement of **Artificial Intelligence**, testing engagements can benefit greatly from **AI assistance** in terms of efficiency and scalability. AI is a powerful tool that humans can use to their advantage.

In this module, we will cover:

- **AI-augmented penetration testing:** Foundations of offensive engagements, including benefits, risks, and traditional workflows.
- **Governance:** Safely using AI in corporate environments.
- **Prompt engineering:** Crafting effective prompts for testing use cases.
- **Managing the context window:** Dealing with large outputs to avoid model performance degradation.
- **AI-augmented analysis:** Using AI for artifact analysis and manual verification.

This module is broken into sections with accompanying hands-on practice exercises. We will practice each of the tactics and techniques we cover. The practical hands-on skills assessment to gauge your understanding in each topic area.

You can start and stop the module at any time and pick up where you left off.

Job Role Paths

Job Role Paths contain groups of modules each related to a specific cybersecurity job role.

Web Penetration Tester The Web Penetration Tester Job Role Path is for individuals who want to enter the world of web penetration testing with little to no prior... Completed	Penetration Tester The Penetration Tester Job Role Path is for newcomers to information security who aspire to become professional penetration testers... Completed
SOC Analyst The SOC Analyst Job Role Path is for newcomers to information security who aspire to become professional SOC analysts. This path... Completed	Senior Web Penetration Tester The Senior Web Penetration Tester Job Role Path is designed for individuals who aim to develop skills in identifying advanced and harmful... Completed
Active Directory Penetration Tester The Active Directory Penetration Tester Job Role Path is designed for individuals who aim to develop skills in pentesting large Active... Completed	AI Red Teamer The AI Red Teamer Job Role Path, in collaboration with Google, trains cybersecurity professionals to assess, exploit, and secure AI... Hard 18d 4h 12 Modules
Junior Cybersecurity Analyst The Junior Cybersecurity Analyst Job Role Path is the first step to enter and gain practical, hands-on experience in the cybersecurity field... Completed	Wi-Fi Penetration Tester The Wi-Fi Penetration Tester Job Role Path is designed for professionals and aspiring security practitioners who want to build... Completed

OFFICIAL WRITEUP

Due to the company's flexible policy, as part of the IT team's secure device policy, I was granted access to the necessary software. After every so often, a PowerShell window flashes up any of its contents. Assuming it's just a expected PowerShell pop-ups present, I ignored them. However, I noticed that the PowerShell flashes could indicate malicious activity. I performed a forensic acquisition of the PC and now, as a member of the IR team, your

Hard 18d 4h 12 Modules

Completed

Θεωρία

Πλάνα Εκπαίδευσης

Εξάσκηση



Πως Το Προσφέρουμε

Job Role Paths

Job Role Paths contain groups of modules each related to a specific cybersecurity job role.

HACKTHEBOX **ANAB**
ACCREDITED
CYBERSECURITY

CERTIFICATE OF COMPLETION

Defense Operations Analyst

Has successfully completed the requirements of the HTB Defense Operations Analyst certificate program.

DATE EARNED: _____

CERTIFICATE TERM: **3 YEARS**

Charalampos Pylarinos
Charalampos Pylarinos
CEO

Dimitrios Boujoukas
Dimitrios Boujoukas
VP OF TRAINING

Πιστοποίηση

The Junior Cybersecurity Analyst Job Role Path is the first step to enter and gain practical, hands-on experience in the cybersecurity field... **Completed**

The Wi-Fi Penetration Tester Job Role Path is designed for professionals and aspiring security practitioners who want to build... **Completed**

Θεωρία

Πλάνα Εκπαίδευσης

Εξάσκηση



Μετρήστε την απόδοση και την αποτελεσματικότητα των ομάδων σας



Καθορισμός στόχων σε συνεργασία με εξειδικευμένους Customer Success Managers της HTB



Δοκιμάστε στην πράξη τα playbooks σας και επιβεβαιώστε τις γνώσεις που έχουν αποκτηθεί



Πλάνο ανάπτυξης δεξιοτήτων ανθρώπινου δυναμικού



Συνεχής προσαρμογή και ανανέωση του εκπαιδευτικού περιεχομένου



Τακτικές αξιολογήσεις και δράσεις benchmarking



Τι κάνουμε διαφορετικά

Ένα οικοσύστημα προϊόντων



Τι κάνουμε διαφορετικά

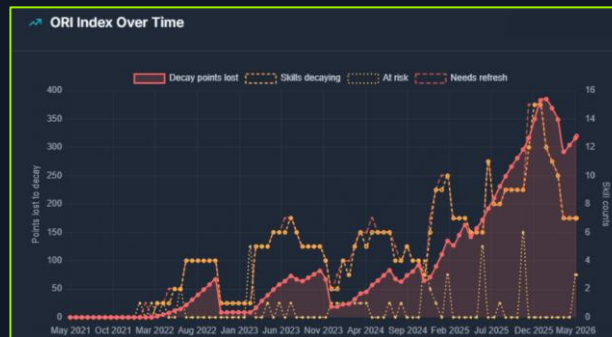
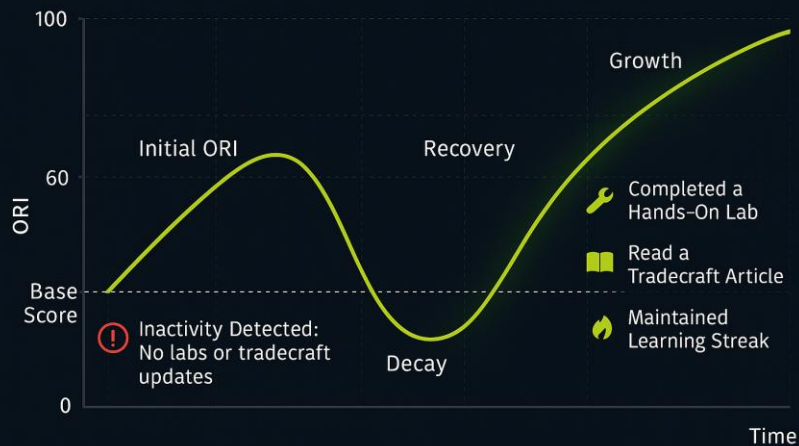
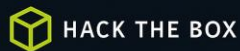
Ρεαλιστικά περιβάλλοντα εκπαίδευσης



Τι κάνουμε διαφορετικά

Δείκτης Επιχειρησιακής Ετοιμότητας

ORI Progression



GenAI & Το μέλλον

Μια νέα επιφάνεια επίθεσης



Άμεση Εισχώρηση Εντολών & Διαρροή System Prompt

Κρυφοί κανόνες, κλειδιά και τα συστήματα στα οποία φτάνει το bot εξάγονται κατευθείαν από το context.



Jailbreaks & Παράκαμψη Guardrail

Roleplay, obfuscation και persona tricks οδηγούν το μοντέλο πέρα από την πολιτική ασφαλείας του, σε μη επιτρεπτή ή επιβλαβή έξοδο.



Διαρροή PII & Ευαίσθητων Δεδομένων

Το bot αναδεικνύει προσωπικά ή ιδιόκτητα δεδομένα από το context, αποθήκες RAG ή μνήμη προηγούμενων γύρων που δεν θα έπρεπε να εκθέσει.



Υπερβολική Χρήση Token

Εχθρικά ή επαναλαμβανόμενα prompts διογκώνουν το κόστος inference και εξαντλούν τα rate limits - η διαθεσιμότητα και ο προϋπολογισμός γίνονται ο στόχος.



Έμμεση Εισχώρηση Εντολών

Οδηγίες κρυμμένες σε σελίδες, έγγραφα, emails ή έξοδο εργαλείων εκτελούνται όταν το μοντέλο τις απορροφά.



Excessive Agency & Κατάχρηση Εργαλείων

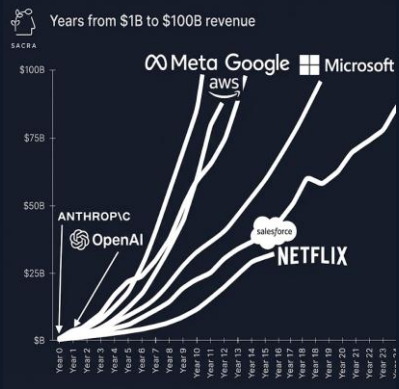
Συνδεδεμένα εργαλεία, βάσεις δεδομένων και APIs μετατρέπουν μία ένεση σε πραγματικές ενέργειες - SSRF, απώλεια δεδομένων, ακούσιες κλήσεις.



GenAI & Το μέλλον

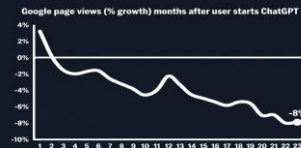
Πιστεύουμε ότι ο κλάδος της κυβερνοασφάλειας βρίσκεται μόλις στην αρχή μιας ταχείας, σαρωτικής επανεφεύρεσης με γνώμονα την AI.

Η GenAI έχει δημιουργήσει τις ταχύτερα αναπτυσσόμενες εταιρείες στην ιστορία...



...ανατρέποντας ολόκληρους κλάδους μέσα σε 2-3 χρόνια.

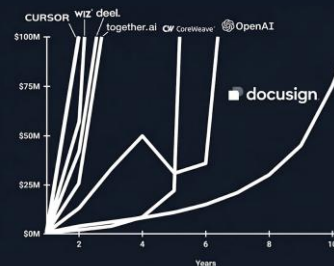
Example 1: Google Search
Declining page views



Example 2: RPA
UiPath declining revenue multiple



Οι προγραμματιστές ήταν οι πρώτοι που την υιοθέτησαν στον επιχειρηματικό χώρο...



Εταιρείες AI όπως οι Cursor και Lovable, φτιαγμένες για παραγωγή κώδικα με AI, φτάνουν σε ορόσημα ετήσιων επαναλαμβανόμενων εσόδων (ARR) 100 εκατ. δολαρίων μέσα σε λίγα χρόνια — και σε χρόνο μόλις 8 μηνών.

...και η κυβερνοασφάλεια είναι η επόμενη.



Οι ρόλοι του αύριο

Τι ποσοστό των σημερινών ρόλων μπορεί να ενισχυθεί με την χρήση AI

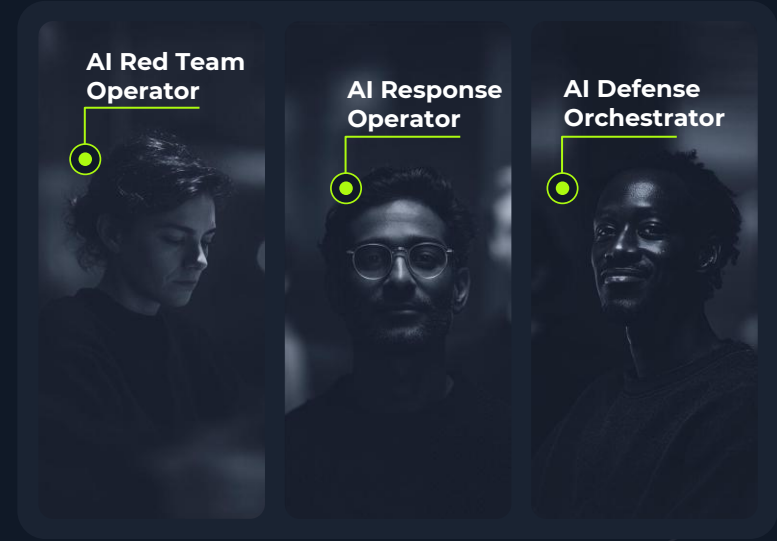


Οι ρόλοι του αύριο

Οι cyber ρολοι **σημερα**



Οι cyber ρολοι **αυριο**



Οι ρόλοι του αύριο



Οι ρόλοι του αύριο

Υπάρχουν τρία ώριμα πεδία. Καθένα μετρά κάτι υπαρκτό — αλλά κανένα δεν μετρά την ικανότητα του χειριστή.



ΑΞΙΟΛΟΓΗΣΗ AGENT

Βαθμολογεί τον agent

Αντιστοίχιση τροχιάς, ακρίβεια χρήσης εργαλείων, process reward.

Πλούσιες, δοκιμασμένες μέθοδοι — αλλά το υποκείμενο είναι το μοντέλο, όχι το άτομο που το χειρίζεται.



ΕΠΙΣΤΗΜΗ ΤΗΣ ΕΜΠΙΣΤΟΣΥΝΗΣ

Βαθμολογεί μεμονωμένες αποφάσεις

Το αν ένας άνθρωπος εμπιστεύτηκε κατάλληλα μία συμβουλή AI.

Στέρη — αλλά μόνο για μεμονωμένες, ναι/όχι κρίσεις. Ποτέ ανά άτομο, ποτέ σε μια ολόκληρη εργασία.



ΨΥΧΟΜΕΤΡΙΑ

Βαθμολογεί την ικανότητα

Το adaptive testing μετατρέπει τη συμπεριφορά σε μια τεκμηριώσιμη βαθμολογία ικανότητας.

Ωριμη — αλλά ποτέ δεν στράφηκε στο ίχνος αλληλεπίδρασης ανθρώπου-AI.

ΤΟ ΚΕΝΟ → AI-AUGMENTED OPERATOR COMPETENCE (AAOC)



Μια βαθμολογία προερχόμενη από τηλεμετρία και επικυρωμένη, για το πόσο καλά ένα άτομο κατευθύνει έναν αυτόνομο agent σε μια ολόκληρη ανάθεση.



Οι ρόλοι του αύριο

Τα KPIs που εξηγούν τον βαθμό ικανότητας του χειριστή.



1

Κόστος ανά Επαληθευμένο Στόχο

\$ / στόχο

Συνδέει τη δαπάνη με πραγματικά, επιβεβαιωμένα αποτελέσματα, όχι με ακατέργαστη δραστηριότητα ή πλήθος token.



2

Κατάλληλη Εμπιστοσύνη

agent / (agent + χειριστής)

Έπιασε τον agent όταν έκανε λάθος, τον άφησε να τρέξει όταν είχε δίκιο - βαθμολογείται βάσει seeded ground truth



3

Ολοκλήρωση Επαληθευμένη με Κατανόηση

δικαιολογημένα / ολοκληρωμένα

Το ποσοστό των ολοκληρωμένων στόχων που ο εκπαιδευόμενος μπορεί πράγματι να δικαιολογήσει - ολοκλήρωση που κατανόησε, όχι απλώς έφτασε. (βασισμένο σε LLM-judge)



Κορυφαίες ομάδες παγκοσμίως εμπιστεύονται την Hack The Box

Δημόσιος τομέας / Κυβερνητικοί οργανισμοί



Χρηματοοικονομικές υπηρεσίες



Τεχνολογία και συμβουλευτικές υπηρεσίες



Άλλοι τομείς



Εκπαίδευση





HACKTHEBOX

Ευχαριστούμε!