Ethical Hacking – Day #2

- Dark Web [tor]
- Deep Web
- Surface Web → Facebook, google, twitter, youtube, instagram, …..

- Cyber Security Teams:

- Red Team → Offensive
- Blue Team → Defensive
- Purple Team →

Penetration Testing
→ Scope

Information Gathering
Social Engineering
Phishing

employee@blabla.com

- Hackers Types:

- White-Hat Hacker
- Black-Hat Hacker
- Gray-Hat Hacker

Hacker Classes

- Black Hats
- White Hats
- Gray Hats
- Suicide Hackers
- Script Kiddies

- Cyber Terrorists
- State Sponsored Hackers
- Hacktivist

Google Project Zero
Zero-day Initiative – Trend Micro

- Info Sec Position

Policies & Procedures

- PCI DSS (Payment Card Industry Data Security Standard)
https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf?agreement=true&time=1629620564760

Card Holder Data
- Card Number 12233XXXXXXX1111 → 1223324242423211111
- Card Holder Name
- Expiry Date
- CVV

Payment Gateway
Stripe

- HIPAA (Health Insurance Portability and Accountability Act)
- Patient Data
- Patient History

GRC → Governance, Risk, Compliance

FinTech → Financial Technology

Ransomware →

API → JSON – XML

Web Application

Request → Processing → Response

HTTP Methods
POST – GET – PUT – DELETE – OPTIONS – HEAD

Request Component
- Method
- Endpoint [domain+filename]
- Headers
- Body

GET → send parameters into the URL
POST → Send parameters into the body

Response
- Status Code
    - 200s → Success
    - 300s → Redirect
    - 400s → Error
        - 400 → Bad Request
        - 401 → Unauthorized
        - 403 → Forbidden
        - 404 → Not Found
    - 500s → Server Errors
        - 500 → internal server error
- Response Headers
- Response Body

HTTP vs HTTPs
SSL/TLS Certificate

Vulnerability:
- Missing SSL Certificate
- SSL Certificate Misconfiguration

- Server Fingerprint
- Debug mode is enabled
    Sensitive Data Exposure
    Security Mis-configuration

- 5 Pillars of Information Security - CIA Triad

- Confidentiality →
- Integrity →
- Availability →
- Authenticity →
- Non-repudiation →

Monitoring – Logging

Authentication → Who you are ?

Something I Know → Username & Password
Something I have → 2-FA
Something I am → Fingerprint

Authorization → What can you do ?

Ransomware →

WannaCry

DoS → Denial of Service
DdoS → Distributed Denial of Service

Honeypots
→ Zombies

DdoS DynDNS

DNS → Domain Name Service/Server/System

google.com → 8.8.8.8

IoT devices →

114.21.23.11

- malware
- worm

Antivirus
- List of signatures

Man-in-The-Middle attack (MiTM)
https://www.first.org/cvss/calculator/3.0#

Companies:
- Integrators
    - Big Four (Deloitte – PwC – EY – KPMG)
    - Secure Misr (CySiv)
    - Security Meter
    - Zinad
    - Fixed Solution
    - CyShield
    - Cyber Castle

- Vendors
    - Kaspersky
    - Avast
    - TrendMicro
    - Cisco
    - Palo Alto

- Customers [Info Sec]
    - Vodafone
    - Etisalat
    - Orange
    - WE
    - AXA
    - Allianz
    - Fawry
    - PayMob
    - PaySky

- Banks

Bug Hunting

Bug Bounty Programs
- Hackerone
- BugCrowd
- Synack
- Intigriti