Ethical Hacking Day6

Penetration Testing

- Web
https://academy.hackthebox.eu/modules
https://portswigger.net/web-security/all-materials

- Ibrahem Hegazy Course – Youtube
https://www.youtube.com/playlist?list=PLv7cogHXoVhXvHPzIl1dWtBiYUAL8baHj

eLearn Security → eWAPT - eWAPTx
Offensive Security → OSWE

- Mobile [Android – iOS]
Static Analysis
Dynamic Analysis

- Internal / External
Offensive Security : OSCP
eLearn Security:
Active Directory + Windows attacks
Pentester Academy: CRTP
Pentester Academy: CRTE
Linux machines

https://www.vulnhub.com/
https://app.hackthebox.eu/machines
Active Machines → For free
Retired Machines → Subscription

OSCP Preparation
https://docs.google.com/spreadsheets/d/1dwSMIAPIam0PuRBkCiDI88pU3yzrqqHkDtBngUHNCw8/edit#gid=1839402159

- Wireless
captive portal

- Network
  - Configuration Review

Forensics

Reverse Engineering

- Assembly
- OS

Exploit developer

SOC

- SIEM Solution

Incident Response

Secure Code Review

→ Secure Code Warrior

https://owasp.org/www-pdf-archive/OWASP_Code_Review_Guide_v2.pdf

https://elearnsecurity.com/product/ewdp-certification/

Offensive Security – OSWE

Secure SDLC →

https://www.isc2.org/Certifications/CSSLP

Threat Intelligence

Info Sec

- GRC
- PCI DSS
- HIPAA
- Policies & Procedures

MetaSploit

https://www.javatpoint.com/metasploit-commands

https://www.offensive-security.com/metasploit-unleashed/msfconsole-commands/

Positions

Tools

- Burp Suite
- Nikto
- Nessus
- Dirbuster
- Dirb
- Wfuzz
- Sublist3r
- Nmap
- SQLmap

- Web Penetration Testing
+++++++
- Bug Hunting + CTFs
- iOS Penetration Testing
- Secure Code Review

securecodewarrior.com

- Android Penetration Testing
- Internal Penetration Testing

    Active Directory → CRTP / CRTE

Bug Bounty – Bug Hunting

Bug Bounty Program →

- Hall of Fame (HoF)
- Bounty

Triage Team

Proof of Concept (PoC)

Steps to reproduce

List of Tools

- netdiscover → to find out the machine's IP
- nmap → to find out the open ports
- nikto → to scan the web application

- wpscan →
    - to scan the wordpress
    - to enumerate the users

netcat [nc]→

www-data → apache user

Cyber Security Certificates:

- Offensive Security: OSCP, OSWE
- eLearnSecurity: PTS – PTP – WAPT – WAPTx – MAPT
- Penetester Academy: CRTP – CRTE

HackTheBox

Vulnhub

- IppSec

https://www.youtube.com/channel/UCa6eh7gCkpPo5XXUDfygQQA

OSCP-Like Machines
https://docs.google.com/spreadsheets/d/1dwSMIAPIam0PuRBkCiDI88pU3yzrqqHkDtBngUHNCw8/edit#gid=0

https://academy.hackthebox.eu/modules

Links:

https://www.youtube.com/c/GeneralEG/videos

The Web Application Hacker's Handbook: Discovering and Exploiting Security Flaws

https://raw.githubusercontent.com/briskinfosec/Books/master/Web%20App%20Pentest/the-web-application-hackers-handbook.pdf

Penetration Testing References

- eLearn Security - eWAPT course
- eLearn Security - eWAPTx course

- Ibrahem Hegazy Course – Youtube

https://www.youtube.com/playlist?list=PLv7cogHXoVhXvHPzIl1dWtBiYUAL8baHj

- eLearnSecurity – eJPT (PTS) course [Entry Level]

- Offensive Security - OSCP course
- eLearn Security – PTP course

- Ippsec – Youtube

https://docs.google.com/spreadsheets/d/1dwSMIAPIam0PuRBkCiDI88pU3yzrqqHkDtBngUHNCw8/edit#gid=1839402159

Active Directory Penetration Testing

- Pentester Academy - CRTP course
- Pentester Academy - CRTE course

VulnHub: https://www.vulnhub.com/

HackTheBox: https://www.hackthebox.eu/

- LiveOverFlow – Youtube

- Intro to Bug Bounty Hunting and Web Application Hacking:

https://www.udemy.com/course/intro-to-bug-bounty-by-nahamsec/

OWASP Top 10

https://owasp.org/www-pdf-archive/OWASP_Top_10-2017_%28en%29.pdf.pdf

Web Application Hackers Handbook

https://github.com/briskinfosec/Books/blob/master/Web%20App%20Pentest/the-web-application-hackers-handbook.pdf

Training

Attack & Defense – Pentester Academy
https://attackdefense.com/

Pentester Lab
https://www.pentesterlab.com/exercises?only=free

Web Penetration Testing

XVWA : https://mega.nz/#!4bJ2XRLT!zOa_IZaBz-doqVZz77Rs1tbhXuR8EVBLOHktBGp11Q8

DVWA: https://dvwa.co.uk/

bWAPP: https://www.vulnhub.com/entry/bwapp-bee-box-v16,53/
http://www.itsecgames.com/

WebGoat: https://owasp.org/www-project-webgoat/#:~:text=WebGoat%20is%20a%20deliberately%20insecure,and%20popular%20open%20source%20components.

OverTheWire: https://overthewire.org/wargames/