HebeSec Technologies Intern Training Program

Note : (R) – Requires Documentation

(N) – Requires Note taking

Prerequisite:

-- Kali or Parrot OS either by Virtual Machine , Dual boot or Full install

-- Internet Connectivity

-- Virtual box and Vmware player (For running Kali or Parrot and also for Attack boxes)

-- Libreoffice (Linux based office suite for Documentation)

-- Cherrytree or Joplin (Note Taking Apps)

-- (THM) means = Tryhackme website

-- (HTB) means = Hackthebox website

-- (Web) means = Requires self research or indicates a website

-- (t) means = tool present by default or need to be installed

-- Vulnhub is a site where you can get attact boxes for practicing

How does a Full Cyber security document look like:

Begining with Cyber security – Needed books for Networking, linux and Programming and easy scripts?

https://github.com/HRSecurity

Learning Topics

Day 1 = OS, Windows , Linux, Terminal and Command Prompt (N)

-- Pentesting Fundamentals (THM)

-- Linux Fundamentals 1,2,3 (THM)

-- Windows Fundamentals 1,2,3 (THM)

-- OpenVPN

Day 2 = Network (N)

- -- OSI and TCP/IP Protocol (Web)
- -- What is Networking (THM)
- -- Network Classes and Ports (Web)
- -- Introductory Networking (THM)
- -- Intro to LAN (THM)
- -- Networking (THM)

Day 3 - 5 = Information Gathering (N)

- -- netdiscover (t)
- -- Angryip scanner (t)
- -- Passive reconnaissance (THM)
- -- Active reconnaissance (THM)
- -- Google Dorking (THM)
- -- Red Team Recon (THM)
- -- Whois domain tools (Web)
- -- ViewDNS.info (Web)
- -- Virus total (Web)
- -- The Harvester (t) (Web)
- -- Recon-ng (t) (Web)
- -- Wayback Machines (Web)
- -- OSINT Framework (Web)
- -- Nmap (t) (THM)

Day 6-8 = Enumeration (N)

- -- vulnerabilities 101 (THM)
- -- Basic Services (FTP, HTTP/HTTPS, SMB, SSH, SMTP, Telnet and more)
- -- Service Enumiration (https://www.youtube.com/watch?v=WvSEkPU1n0I)
- -- Service Based Enumeration
  - > Starting Point (Tier 0, Tier 1, Tier 2) = (HTB)
- -- CC : Pentest (THM)
- -- Vulnhub box to Practice:
  - > kioptrix 1,2,3,4,5 ((R) only for kioptrix 1,2,3)

> Metasploitable 2

> DVWA

> Basic Pentesting 1

> Mr Robot 1

> Basic Pentest (R) (THM)

Day 9-11 Valnerability Assessment Automated

-- Nessus ((R) on Basic kioptrix 1,2,3 IP)

-- Nikto ((R) on Kioptrix 2 IP)

Day 12 – 16 Metasploit

-- Metasploit Unleashed (Web)

-- Metasploit (THM)

-- Vulnhub = Metasploit 1,2

Day 17-26 Attack Process

-- What the shell? (THM)

-- Linux Privialge Esc (THM)

-- Windows Privilage Esc (THM)

-- Post Exploitation Basics (THM)

-- Blue (THM) (R)

-- ICE (THM) (R)

-- Kioptrix 4,5 (R)

Day 27-36

-- How web page works (Web)

-- Client Server Communication (Web)

-- Burp suite : the Basics (THM)

-- OWASP top 10 (THM)

-- DVWA (THM (R)) (Vulnhub)

-- Juiceshop (THM (R)) (Vulnhub)

-- OWASP Zap (THM)

Day 37-40 Documentation

-- Pentest Document { Content and Procedures }

Extras :

Wifi Hacking 101 (THM)

Programming : Bash script & python

Note :

-- Avoid using Walkthroughs

-- Try Googling

-- Ask within the whatsapp group

-- Try at your Max Level

-- if solutions not found then Go for walkthrough

-- Finally if the walkthrough is clear but you didn’t understand the concept – ping me in the whatsapp group

-- Contact me only through whatsapp and No calls will be taken.

Fin

** Hebesec Technologies is not promoting TryhackMe , Hackthebox or Vulnhub **

** Free Resources are shared for Beginners **

** For Educational Purpose only **

** #Happy Hacking **