CC:Crash Course

CC: Pen Testing

CC: Pen Testing

[Task 1] Introduction

The idea behind this room is to provide an introduction to various tools and concepts commonly encountered in penetration testing.

This room assumes that you have basic linux and networking knowledge. This room is also not meant to be a "be all end all" for penetration testing.

The tasks in this room can be completed in any order; however, if you are new to penetration testing, completing the first two sections is recommended before doing anything else.

[#1] No answer needed √

[Task 2] [Section 1 - Network Utilities] - nmap

nmap is one of the most important tools in a pen testers arsenal. It allows a pen tester to see which ports are open, and information about which
services are running on those ports. Ergo this task will focus on showing you nmap's various flags. The beginning questions can be completed by
using the nmap man page; The final questions will require you to deploy the machine :).

[#1] What does nmap stand for?

network mapper √

[#2] How do you specify which ports to scan?

-p

[#3] How do you do a "ping scan"(just tests if the host(s) is up)?

-sn

[#4] What is the flag for a UDP scan?

-sU

[#5] How do you run default scripts?

-sC

[#6] How do you enable "aggressive mode"(Enables OS detection, version detection, script scanning, and traceroute)

-A

[#7] What flag enables OS detection

-O

[#8] How do you get the versions of services running on the target machine

-sV

[#9] Deploy machine

No answer needed

[#10] How many ports are open on the machine?

1

[#11] What service is running on the machine?

Apache

[#12] What version of the service?

2.4.18

[#13] What is the output of the http-title script(included in default scripts)

Apache2 Ubuntu Default Page: It Works

[Task 3] [Section 1 - Network Utilities] - Netcat

**Netcat aka nc is an extremely versatile tool. It allows users to connect to specific ports and send and receive data. It also allows machines
to receive data and connections on specific ports, which makes nc a very popular tool to gain a Reverse Shell.**

**After you connect to a port with nc you will be able to send data, this also has the consequence of the user being able to pipe data through
nc. For example one can do** `echo hello | nc <ip> 1234` **to send the string hello to the service running on port 1234**

Note: **There are multiple versions of nc, so if you are unable to find an answer in your specific man page, try reading the man page for others!**

[#1] How do you listen for connections?

-l

[#2] How do you enable verbose mode(allows you to see who connected to you)?

-v

[#3] How do you specify a port to listen on

-p

[#4] How do you specify which program to execute after you connect to a host(One of the most infamous)?

-e

[#5] How do you connect to udp ports

-u

[Task 4] [Section 2 - Web Enumeration] - gobuster

**One of the main problems of web penetration testing is not knowing where anything is. Basic reconnaissance can tell you
where some files and directories are; however, some of the more hidden stuff is often hidden away from the eyes of users.
This is where gobuster comes in, the idea behind gobuster is that it tries to find valid directories from a wordlist of possible**

directories. gobuster can also be used to valid subdomains using the same method.

The beginning questions of this task use the gobuster man page, while the latter questions will use a virtual machine.

[#1] How do you specify directory/file brute forcing mode?

dir

[#2] How do you specify dns bruteforcing mode?

dns

[#3] What flag sets extensions to be used?

Example: if the php extension is set, and the word is "admin" then gobuster will test admin.php against the webserver

-x

[#4] What flag sets a wordlist to be used?

-w

[#5] How do you set the Username for basic authentication(If the directory requires a username/password)?

-U

[#6] How do you set the password for basic authentication?

-P

[#7] How do you set which status codes gobuster will interpret as valid?

Example: 200,400,404,204

-s

[#8] How do you skip ssl certificate verification?

-k

[#9] How do you specify a User-Agent?

[#10] How do you specify a HTTP header?

-H

[#11] What flag sets the URL to bruteforce?

-u

[#12] dEPLOY THE MACHINE

NO ANSWER NEEDED

[#13] What is the name of the hidden directory

secret

[#14] What is the name of the hidden file with the extension xxa

password

[Task 5] [Section 2 - Web Enumeration] - nikto

**nikto is a popular web scanning tool that allows users to find common web vulnerabilities. It is commonly used to check for
common CVE's such as shellshock, and to get general information about the web server that you're enumerating.**

[#1] How do you specify which host to use?

-h

[#2] What flag disables ssl?

-nossl

[#3] How do you force ssl?

-ssl

[#4] How do you specify authentication(username + pass)?

-id

[#5] How do you select which plugin to use?

-plugins

[#6] Which plugin checks if you can enumerate apache users?

apacheusers

[#7] How do you update the plugin list

-update

[#8] How do you list all possible plugins to use

--list-plugins

[Task 6] [Section 3 - Metasploit]: Intro

**Metasploit is one of the most popular penetration testing frameworks around. It contains a large database of almost every major CVE,
which you can easily use against a machine. The aim of this section is to go through some of the major features of metasploit, and at the
end there will be a machine that you will need to exploit.**

[#1] no answer needed

[Task 7] [Section 3 Metasploit]: Setting Up

**Once you have installed metasploit through either the installer or your distributions repos, you will have many new commands
available to you. This section will primarily focus on the msfconsole command.
Running that command will present you with an "msf5" prompt which will allow you to enter commands. All tasks can be answered
with use of the "help" command.**

[#1] What command allows you to search modules?

search

[#2] How to you select a module?

use

[#3] How do you display information about a specific module?

info

[#4] How do you list options that you can set?

options

[#5] What command lets you view advanced options for a specific module?

advanced

[#6] How do you show options in a specific category

show

[Task 8] [Section 3 - Metasploit]: - Selecting a module

Once you have found the module for the specific machine that you want to exploit, you need to select it and set the proper options.
This task will take you through selecting and setting options for one of the most popular metasploit modules "eternalblue". All basic commands
that could be run before selecting a module can also be done while a module is selected.

[#1] How do you select the eternalblue module?

use exploit/windows/smb/ms17_010_eternalblue

[#2] What option allows you to select the target host(s)?

RHOSTS

[#3] How do you set the target port?

RPORT

[#4] What command allows you to set options?

set

[#5] How would you set SMBPass to "username"?

set SMBPass username

[#6] How would you set the SMBUser to "password"?

set SMBUser password

[#7] What option sets the architecture to be exploited?

arch

[#8] What option sets the payload to be sent to the target machine?

payload

[#9] Once you've finished setting all the required options, how do you run the exploit?

exploit

[#10] What flag do you set if you want the exploit to run in the background?

-j

[#11] How do you list all current sessions?

sessions

[#12] What flag allows you to go into interactive mode with a session("drops you either into a meterpreter or regular shell")

-i

[Task 9] [Section 3 - Metasploit]: meterpreter

**Once you've run the exploit, ideally it will give you one of two things, a regular command shell or a meterpreter shell. Meterpreter is
metasploits own "control center" where you can do various things to interact with the machine. A list of commonmeterpreter
commands and their uses can be found here**

Note: **Regular shells can usually be upgraded to meterpreter shells by using the module** `post/multi/manage/-shell_to_meterpreter`

[#1] What command allows you to download files from the machine?

download

[#2] What command allows you to upload files to the machine?

upload

[#3] How do you list all running processes?

ps

[#4] How do you change processes on the victim host(Ideally it will allow you to change users and gain the perms associated with that user)

migrate

[#5] What command lists files in the current directory on the remote machine?

ls

[#6] How do you execute a command on the remote host?

execute

[#7] What command starts an interactive shell on the remote host?

shell

[#8] How do you find files on the target host(Similar function to the linux command "find")

search

[#9] How do you get the output of a file on the remote host?

cat

[#10] How do you put a meterpreter shell into "background mode"(allows you to run other msf modules while also keeping the meterpreter shell as a session)?

background

[Task 10] [Section 3 - Metasploit]: Final Walkthrough

**It's time to put all the other metasploit tasks together and test them on an example machine. This machine is currently vulnerable
to the metasploit module `exploit/multi/http/nostromo_code_exec`on port 80, and this task will take you through the process
of exploiting it and gaining a shell on the machine.**

[#1] Select the module that needs to be exploited

use exploit/multi/http/nostromo_code_exec

[#2] What variable do you need to set, to select the remote host

RHOSTS

[#3] How do you set the port to 80

set rport 80

[#4] How do you set listening address(Your machine)

LHOST

[#5] Exploit the machine!

no answer needed

[#6] What is the name of the secret directory in the /var/nostromo/htdocs directory?

s3cretd1r

[#7] What are the contents of the file inside of the directory?

Woohoo!

[Task 11] [Section 4 - Hash Cracking]: Intro

**Often times during a pen test, you will gain access to a database. When you investigate the database you will often find a users table,
which contains usernames and often hashed passwords. It is often necessary to know how to crack hashed passwords to gain authentication
to a website(or if you're lucky a hashed password may work for ssh!).**

[#1] No answer needed

[Task 12] [Section 4 - Hash Cracking]: Salting and Formatting

No matter what tool you use, virtually all of them have the exact same format. A file with the hash(s) in it with each hash being separated by a newline.
Example:

<hash 1>
<hash 2>
<hash 3>

Salts are typically appended onto the hash with a colon and the salt. Files with salted hashes still follow the same convention with each hash being separated by a newline.
Example:

<hash1>:<salt>
<hash2>:<salt>
<hash3>:<salt>

Note: **Different hashing algorithms treat salts differently. Some prepend them and some append them. Research what it is you're trying to crack, and make the distinction.**

[#1] **No answer needed**

[Task 13] [Section 4 - Hash Cracking]: hashcat

hashcat is another one of the most popular hash cracking tools. It is renowned for its versatility and speed. Hashcat does not have auto
detection for hashtypes, instead it has modes. For example if you were trying to crack an md5 hash the "mode" would be 0, while if you
were trying to crack a sha1 hash, the mode would be 100.

A full list of all modes can be found here.

[#1] What flag sets the mode?

-m

[#2] What flag sets the “attack mode”?

-a

[#3] What is the attack mode number for Brute-force?

3

[#4] What is the mode number for SHA3-512

17600

[#5] Crack This Hash: 56ab24c15b72a457069c5ea42fcfc640
Type: MD5

happy

[#6] Crack this hash: 4bc9ae2b9236c2ad02d81491dcb51d5f
Type: MD4

nootnoot

[Task 14] [Section 4 - Hash Cracking]: John The Ripper

John The Ripper(jtr) is one of the best hash cracking tools available. It supports numerous formats of hashes and is extremely easy to use, while having a lot of options for customization.

Note: **There are multiple variations of jtr out there. For this task the version that comes pre-installed on kali will be used**
Note 2: **All hashes can be cracked with rockyou.txt**

[#1] What flag let's you specify which wordlist to use?

--wordlist

[#2] What flag lets you specify which hash format(Ex: MD5,SHA1 etc.) to use?

--format

[#3] How do you specify which rule to use?

--rule

[#4] Crack this hash: 5d41402abc4b2a76b9719d911017c592
Type: MD5

hello

[#5] Crack this hash: 5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8
Type: SHA1

password

[Task 15] [Section 5 - SQL Injection]: Intro

SQL injection is the art of modifying a SQL query so you can get access to the target's database. This technique is often
used to get user's data such as passwords, emails etc. SQL injection is one of the most common web vulnerabilities, and
as such, it is highly worth checking for

[#1] No answer needed

[Task 16] [Section 5 - SQL Injection]: sqlmap

Sqlmap is arguably the most popular automated SQL injection tool out there. It checks for various types of injections,
and has plenty of customization options.

[#1] How do you specify which url to check?

-u

[#2] What about which google dork to use?

-g

[#3] How do you select(lol) which parameter to use?(Example: in the url http://ex.com?test=1 the parameter would be test.)

-p

[#4] What flag sets which database is in the target host's backend?(Example: If the flag is set to mysql then sqlmap will only test mysql injections).

--dbms

[#5] How do you select the level of depth sqlmap should use(Higher = more accurate and more tests in general).

--level

[#6] How do you dump the table entries of the database?

--dump

[#7] Which flag sets which db to enumerate? (Case sensitive)

-D

[#8] Which flag sets which table to enumerate? (Case sensitive)

-T

[#9] Which flag sets which column to enumerate? (Case sensitive)

-C

[#10] How do you ask sqlmap to try to get an interactive os-shell?

--os-shell

[#11] What flag dumps all data from every table

--dump-all

[#12] No answer needed

[Task 17] [Section 5 - SQL Injection]: A Note on Manual SQL Injection

Occasionally you will be unable to use sqlmap. This can be for a variety of reasons, such as a the target has set up a firewall or a request limit. In this case it is worth knowing how to do basic manual SQL Injection, if only to confirm that there is SQL Injection.
A list of ways to check for SQL Injection can be found here.

Note: **As there are various ways to check for sql injection, and it would be difficult to properly convey how to test for sqli given each situation, there will be no questions for this task.**

[#1] No answer needed

[Task 18] [Section 6 - SQL Injection]: Vulnerable Web Application

To demonstrate how to use sqlmap to check for vulnerabilities and dump table data, I will be walking you through an example web app. Deploy the machine and let's get started!

Note: **This task will be using sqlmap, however you are welcome to try to exploit it manually. It outputs the full SQL query on every attempt, so you can know what mysql is trying to do!**

[#1] Set the url to the machine ip, and run the command

no answer needed

[#2] How many types of sqli is the site vulnerable too?

3

[#3] Dump the database

no answer needed

[#4] What is the name of the database?

tests

[#5] How many tables are in the database?

2

[#6] What is the value of the flag?

found_me

[Task 19] [Section 6 - Samba]: Intro

Most of the pentesting techniques and tools you've seen so far can be used on both Windows and Linux. However, one of the things you'll find most often when pen testing Windows machines is samba, and it is worth making a section dedicated to enumerating it.

Note: **Samba is cross platform as well, however this section will primarily be focused on Windows enumeration;**

**some of the techniques
you see here still apply to Linux as well.**

[#1] No answer needed

[Task 20] [Section 7 - Samba]: smbmap

**Continuing with the trend of tools having "map" in the name being extremely popular, smbmap is one of the best ways to
enumerate samba. smbmap allows pen-testers to run commands(given proper permissions), download and upload files, and
overall is just incredibly useful for smb enumeration.**

[#1] How do you set the username to authenticate with?

-u

[#2] What about the password?

-p

[#3] How do you set the host?

-H

[#4] What flag runs a command on the server(assuming you have permissions that is)?

-x

[#5] How do you specify the share to enumerate?

-s

[#6] How do you set which domain to enumerate?

-d

[#7] What flag downloads a file?

--download

[#8] What about uploading one?

--upload

[#9] Given the username "admin", the password "password", and the ip "10.10.10.10", how would you run ipconfig on that machine

smbmap -U “admin” -P “password” -h 10.10.10.10 -X ipconfig

[Task 21] [Section 6 - Samba]: smbclient

smbclient allows you to do most of the things you can do with smbmap, and it also offers you and interactive prompt.

[#1] How do you specify which domain(workgroup) to use when connecting to the host?

-w

[#2] How do you specify the ip address of the host?

-i

[#3] How do you run the command "ipconfig" on the target machine?

-c “ipconfig”

[#4] How do you specify the username to authenticate with?

-U

[#5] How do you specify the password to authenticate with?

-P

[#6] What flag is set to tell smbclient to not use a password?

-N

[#7] While in the interactive prompt, how would you download the file test, assuming it was in the current directory?

get test

[#8] In the interactive prompt, how would you upload your /etc/hosts file

put /etc/hosts

[Task 22] [Section 6 - Samba]: A note about impacket

**impacket is a collection of extremely useful windows scripts. It is worth mentioning here, as it has many scripts available that use samba
to enumerate and even gain shell access to windows machines. All scripts can be found here.**

Note: **impacket has scripts that use other protocols and services besides samba.**

[#1] No answer needed

[Task 23] [Miscellaneous]: A note on privilege escalation

**privilege escalation is such a large topic that it would be impossible to do it proper justice in this type of room. However,
it is a necessary topic that must be covered, so rather than making a task with questions, I shall provide you all with some resources.**

General:
https://github.com/swisskyrepo/PayloadsAllTheThings (A bunch of tools and payloads for every stage of pentesting)

Linux:
https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/ (a bit old but still worth looking at)
https://github.com/rebootuser/LinEnum(One of the most popular priv esc scripts)
https://github.com/diego-treitos/linux-smart-enumeration/blob/master/lse.sh (Another popular script)
https://github.com/mzet-/linux-exploit-suggester (A Script that's dedicated to searching for kernel exploits)

https://gtfobins.github.io (I can not overstate the usefulness of this for priv esc, if a common binary has special permissions,
you can use this site to see how to get root perms with it.)

Windows:
https://www.fuzzysecurity.com/tutorials/16.html (Dictates some very useful commands and methods to enumerate the host and gain intel)
https://github.com/PowerShellEmpire/PowerTools/tree/master/PowerUp (A bit old but still an incredibly useful script)
https://github.com/411Hall/JAWS (A general enumeration script)

[Task 24] [Section 7 - Final Exam]: Good Luck :D

Throughout this course, you have learned many tactics and tools to pentesting. This is where it all gets put to the

test,
I have put together a beginner level ctf, that contains 2 flags. Good luck and have fun!

click me	click me
#1	What is the user.txt

supernootnoot

click me	click me
#2	What is the root.txt

congratulations!!!!

scans

NMAP SCAN

```
Nmap scan report for 10.10.142.213
Host is up (0.17s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 12:96:a6:1e:81:73:ae:17:4c:e1:7c:63:78:3c:71:1c (RSA)
|   256 6d:9c:f2:07:11:d2:aa:19:99:90:bb:ec:6b:a1:53:77 (ECDSA)
|_  256 0e:a5:fa:ce:f2:ad:e6:fa:99:f3:92:5f:87:bb:ba:f4 (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

NIKTO SCAN

```
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.142.213
+ Target Hostname:    10.10.142.213
+ Target Port:        80
+ Start Time:         2020-04-28 15:23:26 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.18 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Server may leak inodes via ETags, header found with file /, inode: 2c39, size: 59a2d6bc5ae41, mtime: gzip
 + Allowed HTTP Methods: OPTIONS, GET, HEAD, POST
```

GOBUSTER SCAN

gobuster dir -u 10.10.15.97 -w /usr/share/dirb/wordlists/-

common.txt -x txt

/.htaccess (Status: 403)
/.hta (Status: 403)
/.htpasswd (Status: 403)
/index.html (Status: 200)
/secret (Status: 301)
/server-status (Status: 403)

gobuster dir -u http://10.10.15.97/secret -w /usr/share/dirb/-wordlists/common.txt -x txt

/.hta (Status: 403)
/.hta.txt (Status: 403)
/.htaccess (Status: 403)
/.htaccess.txt (Status: 403)
/.htpasswd (Status: 403)
/.htpasswd.txt (Status: 403)
/index.html (Status: 200)
/secret.txt (Status: 200)

privesc

nyan@ubuntu:~$ cat user.txt

supernootnoot

nyan@ubuntu:~$ sudo -l
Matching Defaults entries for nyan on ubuntu:
env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User nyan may run the following commands on ubuntu:
(root) NOPASSWD: /bin/su

nyan@ubuntu:~$ sudo su
root@ubuntu:/home/nyan# cat root.txt
cat: root.txt: No such file or directory
root@ubuntu:/home/nyan# cd root
bash: cd: root: No such file or directory
root@ubuntu:/home/nyan# cd ~
root@ubuntu:~# cat root.txt

congratulations!!!!

root@ubuntu:~# Connection to 10.10.15.97 closed by remote host.
Connection to 10.10.15.97 closed.

CC: Steganography

CC: Steganography

[Task 1] Intro

Steganography(Stego) is the art of concealing something inside something else, for example: A message inside a jpg file, or a binary inside a png.
Stego has been used since ancient times to deliver messages that they don't want others seeing. In the modern day it's used for the same purpose,
only now we have much more advanced tools. This room is designed to go over those tools and how to use them.

All needed files can be found inside the included zip file

Note: Basic linux knowledge required.

[Task 2] Steghide

Steghide is one of the most famous steganography tools, and for good reason. It's a classic method, hiding a message inside an image, and steghide does it effectively and efficiently. A downside of steghide is that it only works on jpgs; however, that means that if you believe there is a hidden message inside a jpg, then steghide is a probable option.

One of the greatest benefits of stegohide, is that it can encrypt data with a passphrase. Meaning that if they don't have the password then they can't extract any data.

steghide can be installed with the command `sudo apt install steghide`

click me	**click me**
#1	What argument allo into other files?

embed

click me	**click me**
#2	What flag let's you s

-ef

click me	**click me**
#3	What flag allows yo

-cf

click me	**click me**
#4	How do you set the p

-p

click me	**click me**
#5	What argument allo

extract

-sf

click me	click me
#7	Given the passphras message in the included "jpeg1" file.

steghide extract -p password123 -sf jpeg1.jpeg
pinguftw

[Task 3] zsteg

zsteg is to png's what steghide is to jpg's. It supports various techniques to extract any and all data from png files.

Note: zsteg also supports BMP files, but it is primarily used for png's.

zsteg can be installed by using ruby with the command `gem install zsteg`

click me	click me
#1	How do you specify t first

--lsb

click me	click me
#2	What about the mos

--msb

click me	click me
#3	How do you specify v

-v

click me	click me
#4	How do you extract

-E

click me	click me
#5	In the included file

zsteg png1.png -a
nootnoot$

click me	click me
#6	What about the pay

b1,bgr,lsb,xy

[Task 4] Exiftool

Exiftool is a tool that allows you to view and edit image metadata. While this in itself is not a stego tool, I would be remiss not to include at least a footnote on it as one of the most popular forms of image stego is to hide messages in the metadata.

Exiftool can be installed with `sudo apt install exiftool`

click me	**click me**
#1	

Hello :)

[Task 5] Stegoveritas

Personally this is one of my favorite image stego tools. It supports just about every image file, and is able to extract all types of data from it. It is an incredibly useful tool if you don't know exactly what you're looking for, as it has a myriad of built in tests to extract any and all data.

Note: Stegoveritas has other features as well such as color correcting images

Stegoveritas can be installed by running these two commands:

```
 pip3 install stegoveritas
stegoveritas_install_deps
```

click me	**click me**
#1	How do you check the file for metadata?

-meta

click me	**click me**
#2	How do you check fo

steghide

click me	**click me**
#3	What flag allows yo

-extractLSB

click me	**click me**
#4	In the included ima

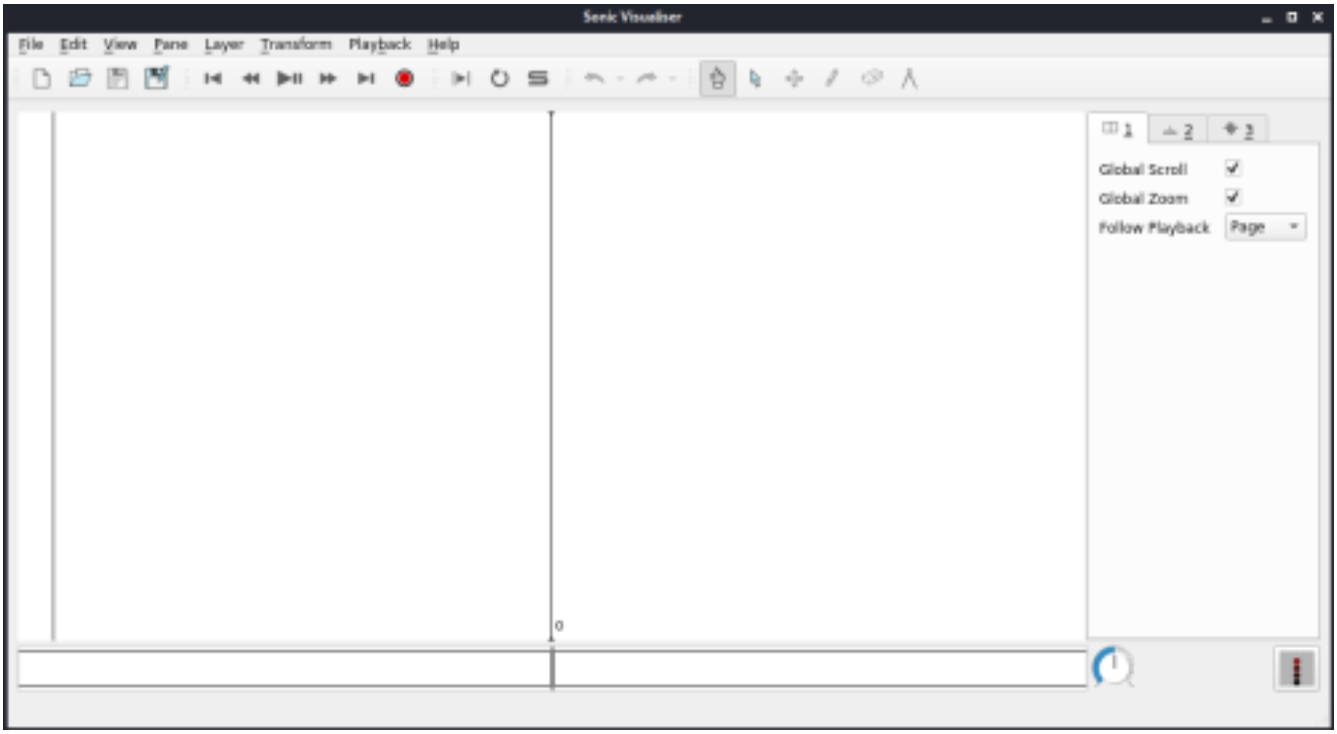
kekekekek

[Task 6] Spectograms

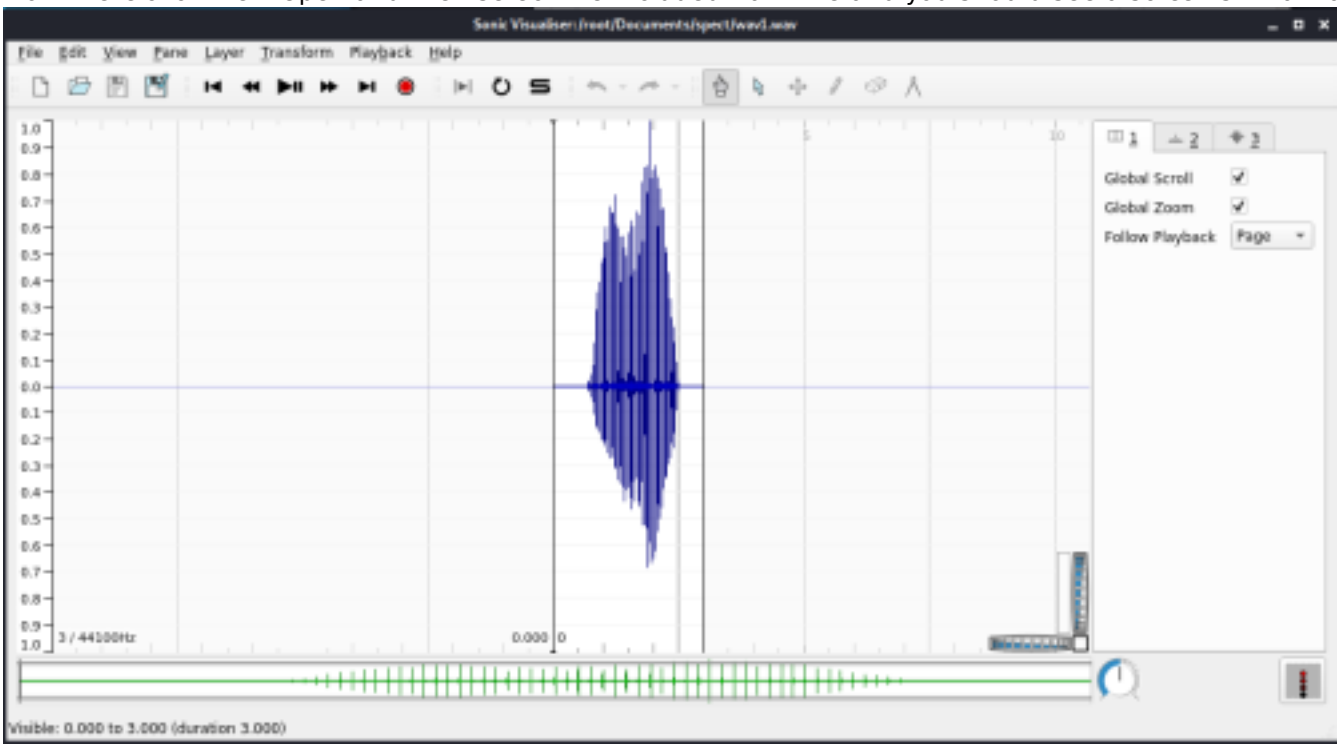
Spectrogram stegonography is the art of hiding hidden an image inside in an audio file's spectogram. Therefore when ever dealing with audio stego it is always worth analyzing the spectrogram of the audio. To do this task we will be using Sonic Visualizer.

Note: This introduction will be done using the included wav1 file.

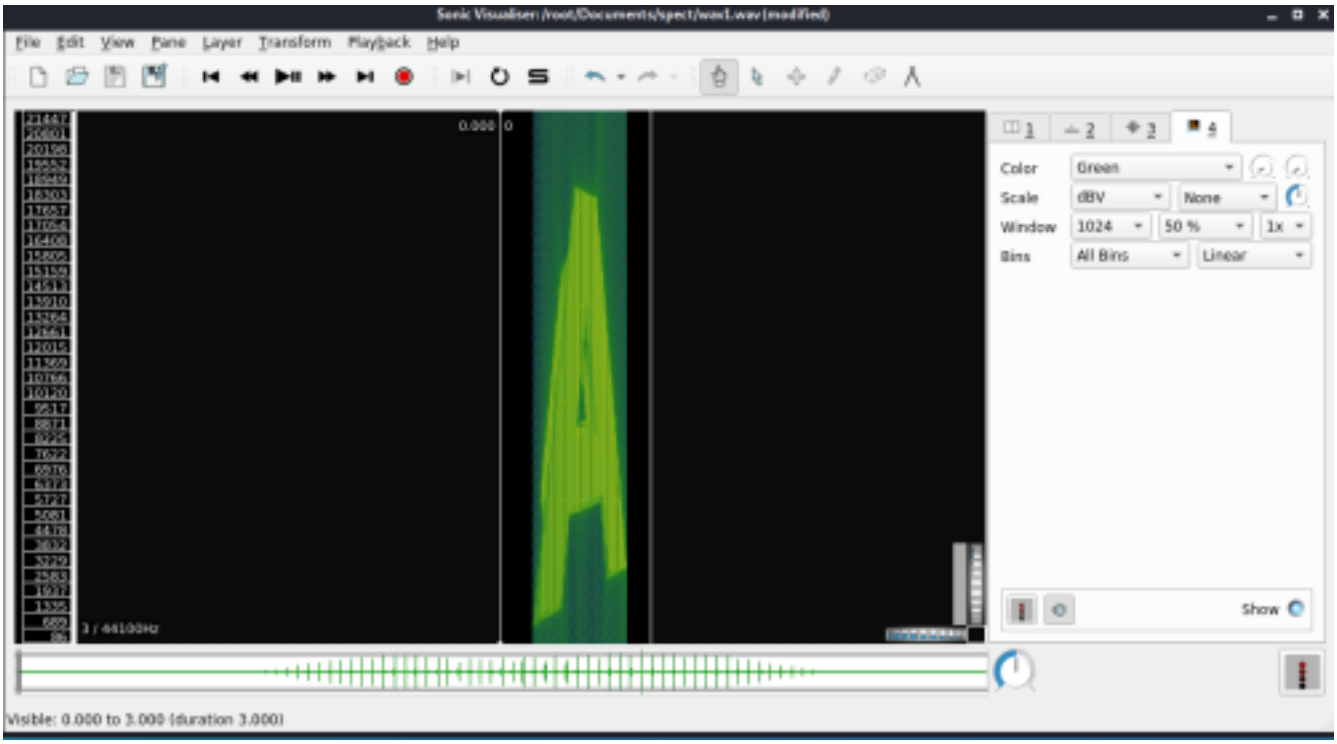
When you open Sonic Visualizer you should see this screen:



From there click File->Open and then select the included wav1 file and you should see a screen similar to this:



From there click layer -> Add Spectogram and you should see this.



click me	click me
#1	What is the hidden text in the included wav2

Google

[Task 7] The Final Exam

Good luck and have fun!

click me	click me
#1	

superkeykey

click me	click me
#2	

https://imgur.com/KTrtNI5

zsteg 2.png

fatality

click me	click me
#3	

QR decoder online tool

killshot