CCCY221 University of Jeddah

College of Computer Science and Engineering

Department of Cyber-Security

5 TOOLS IN THE CYBERSECURITY WORLD

Made by:

Faisal Al-Malki 2142049

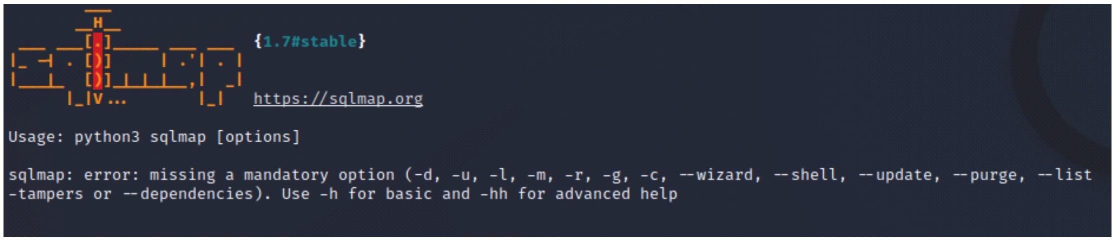
Audai Al-Sulimany 2141825

Abdulrahman Quraish 2142476

5 TOOLS IN THE CYBERSECURITY WORLD

(1) Sqlmap:

The open-source tool sqlmap is used to identify and take advantage of SQL injection vulnerabilities in online applications. A security flaw known as SQL injection enables an attacker to insert malicious code into a SQL statement, potentially giving them access to confidential database information.



```
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.7#stable}
|_ -| . [)]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

Usage: python3 sqlmap [options]

sqlmap: error: missing a mandatory option (-d, -u, -l, -m, -r, -g, -c, --wizard, --shell, --update, --purge, --list
-tampers or --dependencies). Use -h for basic and -hh for advanced help
```

Security experts and ethical hackers can more easily find and test for SQL injection vulnerabilities thanks to sqlmap, which automates the process of discovering and exploiting these flaws. With the use of sqlmap, you can evaluate the security of both your own web apps and those developed by others in order to find any potential vulnerabilities and thwart assaults.

It's crucial to remember that using sqlmap or any other tool for malicious intent is against the law and unethical. utilizing sqlmap should only be used for learning purposes or as part of a legitimate security evaluation.

(2) Exiftool:

Tool designed to read, write and manipulate png images or PDF files

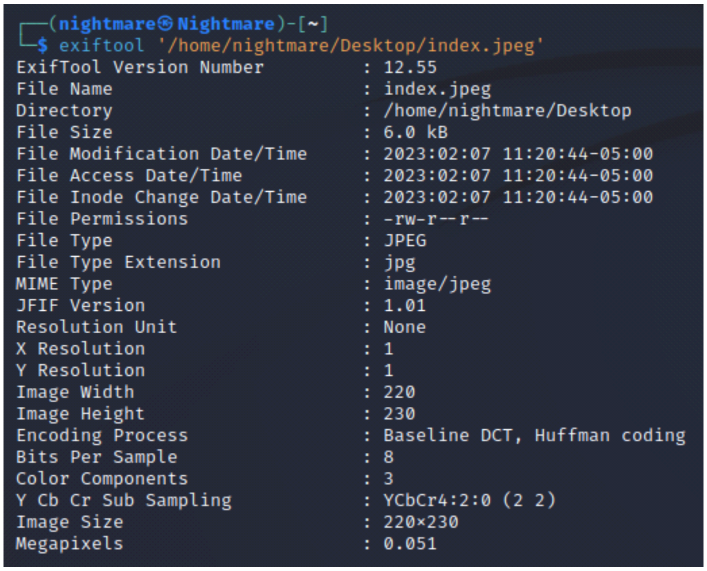
It is mainly used to extract **metadata** of a file, it doesn’t mainly focus on images it could break down videos, audio and PDF files too.

There could be data hiding inside an image that we can look at using the tool.

What is metadata?

Metadata is basically data that gives us information about when was a specific part of data created and why it was created, this makes tracking data and working with it much easier.

So to try it out we found a random image on google and implemented the Exiftool on it...



```
┌──(nightmare㉿Nightmare)-[~]
└─$ exiftool '/home/nightmare/Desktop/index.jpeg'
ExifTool Version Number         : 12.55
File Name                       : index.jpeg
Directory                       : /home/nightmare/Desktop
File Size                       : 6.0 kB
File Modification Date/Time     : 2023:02:07 11:20:44-05:00
File Access Date/Time           : 2023:02:07 11:20:44-05:00
File Inode Change Date/Time     : 2023:02:07 11:20:44-05:00
File Permissions                : -rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : None
X Resolution                    : 1
Y Resolution                    : 1
Image Width                     : 220
Image Height                    : 230
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 220x230
Megapixels                      : 0.051
```

After using it on the image we can see all the information about the image including file size, file modification date and time, the file permissions and type,

We also can see that there is no secret data hiding inside the image file.

(3) Hashcat:

helpful recovery tool that is used for cracking password hashes, it also works with the GPU since GPUs are fast and used in gaming, AI and VR it can also be applied to accelerate the password cracking process.

Hashcat has various attack modes here are some of them:

- Dictionary attack: attack performed by using a wordlist, the better the wordlist the better chances of cracking a code.

- Mask attack: similar to dictionary attack but uses information we already have like the length of the password or some characters included.

- Combinator attack: tries different combinations of words from our existing wordlist.

How to defend against Hashcat:

- The stronger the password the harder to crack, so setting up a powerful password would be recommended.

- Adding salts to hashes, a salt is an additional string added to the already set up password so the hash generated is different from the normal hash.

- we can also make the salts stronger by using dynamic salts instead of static salts, which writes a function that creates a salt value for every string making it extremely hard to crack down a password.

(4) Hydra:

Hydra is a login cracker which performs attacks against numerous protocols including (HTTP, HTTPS, FTP), it is fast and flexible and makes it easier for penetration tester, ethical hackers and security consultant to gain unauthorized access to network service systems remotely.

Hydra vs Hashcat:

Hydra is a penetration tool used to crack passwords while Hashcat is a recovery tool used in security testing.

Pros and Cons:

Pros:

- Open source which means the source code is available for everyone.

- The ability it has to perform HTTP post form and a great number of protocol attacks.

Cons:

- Not a straight forward tool to use it depends on certain installs so it can function.

- Sometimes the tool gives False Positive passwords.

(5) Wireshark:

A tool that is used to record and analyze the routing of every packet being transmitted inside and outside the network which includes wireless, Ethernet, Bluetooth, etc. traffic.

It is also a useful tool for hackers, it allows them to read and write data being transmitted inside an unsecure network, such users of Wireshark may be seeking to sniff confidential information such as money transactions, passwords, private messages etc.

Wireshark is the most common packet sniffer in the world, similar to other sniffers it does the following:

- Packet capture: Wireshark captures entire line stream of traffic in a network, possibly thousands of packets at once.

- Visualization: it allows you to dive into the middle of a network packet while also allows you to visualize entire conversations and stream in a network.

Who uses Wireshark?

Used by government agencies, small businesses, education centers to troubleshoot network issues and can be used as a learning tool for new information security employees to further understand network traffic analysis.

References used in this project

https://www.freecodecamp.org/news/hacking-with-hashcat-a-practical-guide/#:~:text=Hashcat%20is%20a%20powerful%20tool,and%20salts%20before%20hashing%20passwords.

https://whisperlab.org/introduction-to-hacking/notes/wireshark#:~:text=Wireshark%20can%20also%20be%20used,%2C%20financial%20transactions%2C%20and%20more.