CHAMELEON

FOR OUR SMARTER WORLD

XMAS, FIN, SYN, NULL scan on MOP website

BIPANJEET SINGH SODHI

222093716

INTRODUCTION

What is XMAS scan?

Xmas scan is type of method that is used to check for any weakness in computer system's defenses. This is performed by making use of messages which are sent to the computer. It then analyses the response, and this response helps it to figure out the open ports/ doorways that are vulnerable and open to attacks.

EXAMPLE

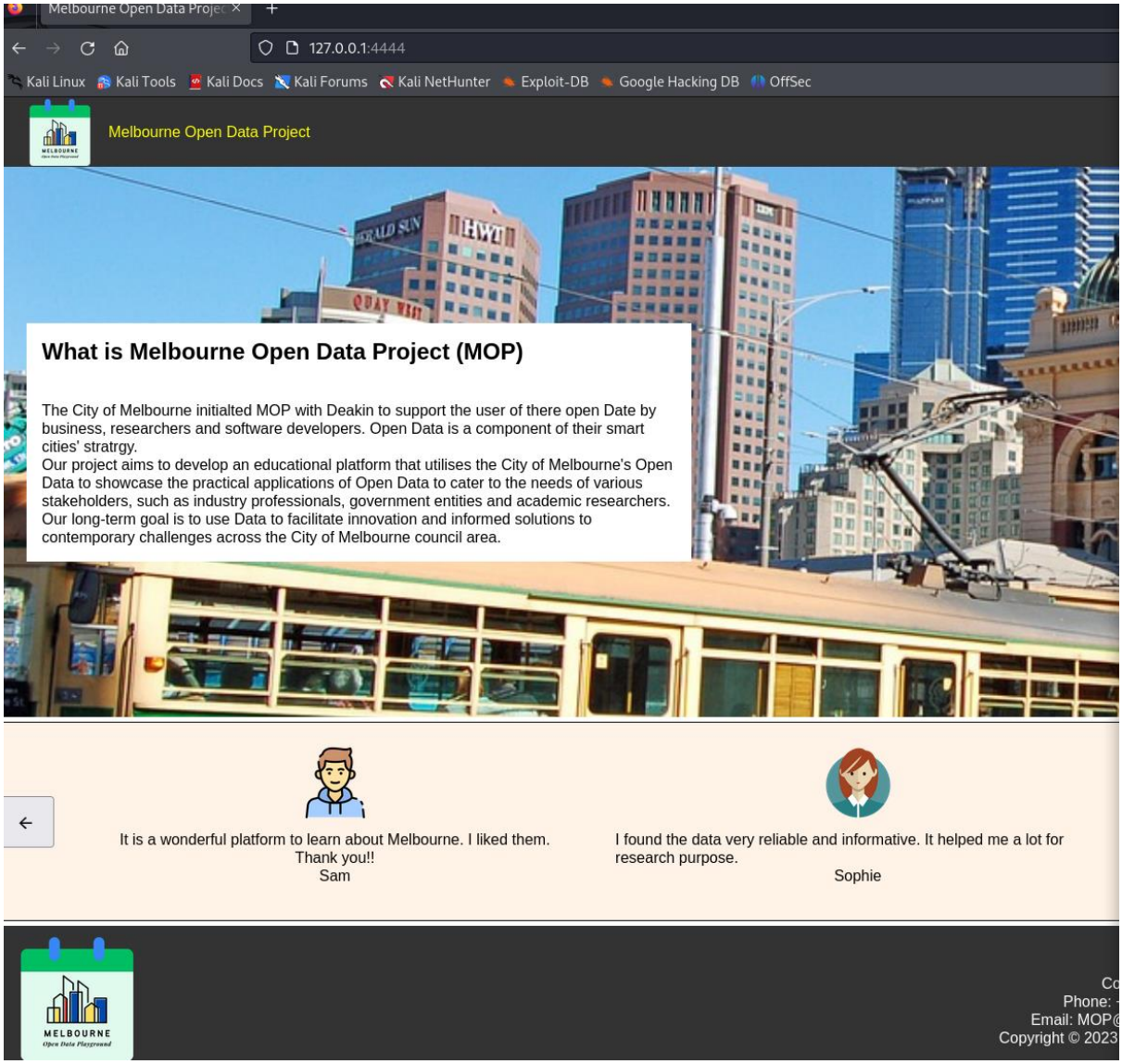
Peeking through the window to check for weaknesses/open ports.

Performing XMAS scan on MOP website

PRE-CHECKS

Making sure that MOP website is up and running

```
┌──(kali㉿kali)-[~/Desktop/MOP-Code-master/webapp]
└─$ python -m gunicorn -b 127.0.0.1:4444 app:app
[2024-03-25 17:31:06 -0400] [179726] [INFO] Starting gunicorn 20.1.0
[2024-03-25 17:31:06 -0400] [179726] [INFO] Listening at: http://127.0.0.1:4444
(179726)
[2024-03-25 17:31:06 -0400] [179726] [INFO] Using worker: sync
[2024-03-25 17:31:06 -0400] [179727] [INFO] Booting worker with pid: 179727
/home/kali/Desktop/MOP-Code-master/webapp/flaskr/controllers/use_cases.py:21: Sy
ntaxWarning: "is" with a literal. Did you mean "=="?
  if name is 'parking-availability':
/home/kali/Desktop/MOP-Code-master/webapp/flaskr/controllers/tools.py:17: Syntax
Warning: "is" with a literal. Did you mean "=="?
  if name is 'parking-availability':
[2024-03-25 17:41:30 -0400] [179726] [CRITICAL] WORKER TIMEOUT (pid:179727)
[2024-03-25 17:41:30 -0400] [179727] [INFO] Worker exiting (pid: 179727)
[2024-03-25 17:41:31 -0400] [179726] [WARNING] Worker with pid 179727 was termin
ated due to signal 9
[2024-03-25 17:41:31 -0400] [184588] [INFO] Booting worker with pid: 184588
[2024-03-30 07:36:51 -0400] [179726] [CRITICAL] WORKER TIMEOUT (pid:184588)
[2024-03-30 07:36:51 -0400] [184588] [INFO] Worker exiting (pid: 184588)
[2024-03-30 07:36:52 -0400] [179726] [WARNING] Worker with pid 184588 was termin
ated due to signal 9
[2024-03-30 07:36:52 -0400] [202150] [INFO] Booting worker with pid: 202150
[2024-03-31 04:20:23 -0400] [179726] [CRITICAL] WORKER TIMEOUT (pid:202150)
[2024-03-31 04:20:23 -0400] [202150] [INFO] Worker exiting (pid: 202150)
[2024-03-31 04:20:24 -0400] [179726] [WARNING] Worker with pid 202150 was termin
ated due to signal 9
[2024-03-31 04:20:24 -0400] [207562] [INFO] Booting worker with pid: 207562
```



Performing XMAS scan using the cmd:

Sudo nmap -sX <IP address of website>

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -sX 127.0.0.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-30 07:43 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000040s latency).
Not shown: 999 closed tcp ports (reset)
PORT     STATE         SERVICE
4444/tcp open|filtered krb524
```

RESULT

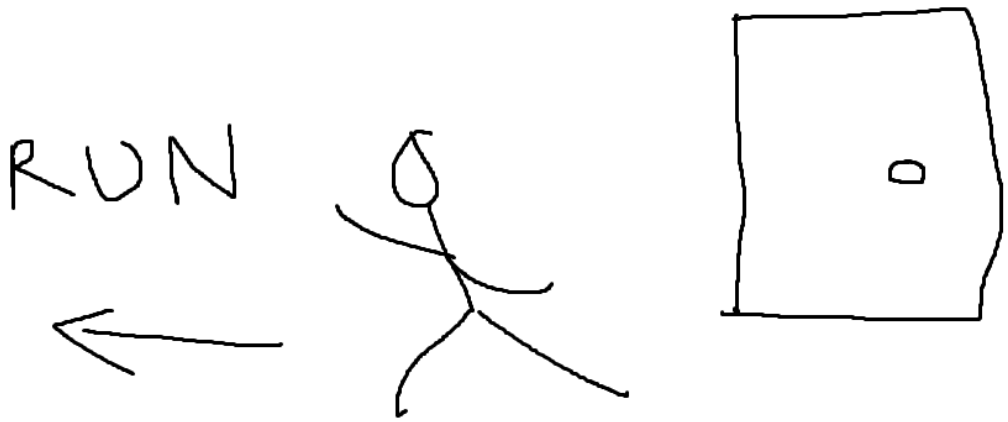
We were expecting a response indicating the open ports. But as we see, the state is filtered. This probably means that the firewall successfully dropped the packet, and the website security is intact.

What is SYN scan?

SYN scan is also used to figure out whether a port on the system is open or closed. It makes use of incomplete TCP handshake process. It is used by attackers to find weaknesses in a system, just like XMAS scan.

EXAMPLE

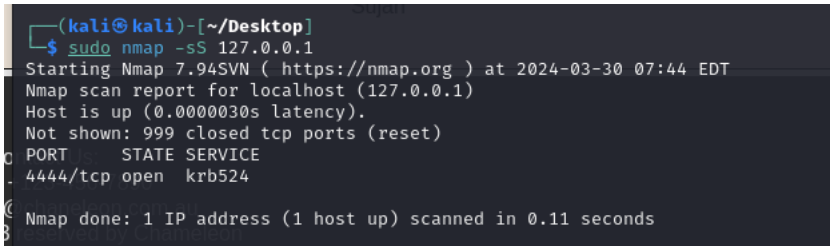
Knocking the door and running away, without waiting for response.



Performing SYN scan

To perform SYN scan, we run the following command.

Sudo nmap -sS <IP address of website>



RESULT

We get a similar response to what we got in XMAS scan. This indicates that the website security is doing well against the SYN scans aswell, and is not revealing any open/closed ports to the attacker.

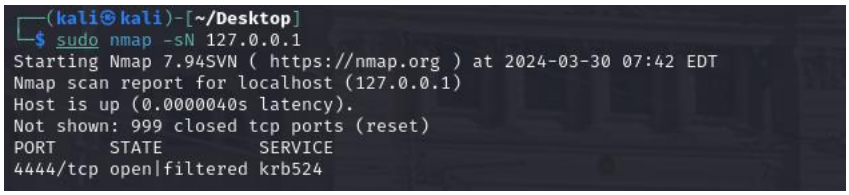
What is NULL scan?

NULL scan makes use of not setting any TCP flags, or in other words, sending an empty message to some port. It then waits to see the response and analyses it. So, in case of an open port, the null packet gets ignored. In other case, which is, if the port is closed, a RST packet is sent to reject the attempt for connection.

Performing NULL scan

We perform NULL scan by using the following command on the MOP website.

Sudo nmap -sN <IP address of website>



RESULT

We get a similar response as the other two scans above.

This indicates that the website does well against the NULL scan as well.

Lastly,

What is FIN scan?

FIN scan is basically same like NULL scan, except for in this case we have the FIN flag for TCP set (FIN= finish). The FIN flag is made use of whenever we need to end the connection/communication between two hosts. So, if a port is open or closed, the port receives the FIN flag from the attacker. In its response, the system sends a reset packet or RST packet which gives indicates no connection. So, it helps the attacker identify the open/closed ports.

Performing FIN scan

To perform FIN scan on the MOP website, we run the following command:

Sudo nmap -sF <IP address of website>

RESULT

This too indicates the MOP website's security/defence against such scans.

In conclusion, We can finally conclude that the MOP website is not vulnerable to XMAS, SYN, NULL and FIN scans. No open/closed port data is revealed to attacker when using these scans via Nmap.

References

1. Nmap Project. (n.d.). SYN scan. In Nmap documentation. Retrieved from https://nmap.org/book/synscan.html
2. Plixer. (n.d.). The null scan: You're being watched. Plixer. Retrieved from https://www.plixer.com/blog/the-null-scan-youre-being-watched/
3. Packt. (n.d.). FIN scans. In Mastering Kali Linux for Advanced Penetration Testing (p. 60). Packt Publishing. Retrieved from https://subscription.packtpub.com/book/security/9781788995177/4/ch04lvl1sec40/fin-scans#:~:text=A%20FIN%20scan%20is%20when,no%20established%20connection%20to%20close.
4. Nmap Project. (n.d.). Scan methods: NULL, FIN, Xmas scan. In Nmap documentation. Retrieved from https://nmap.org/book/scan-methods-null-fin-xmas-scan.html