International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 10 Issue: 05 | May 2023 www.irjet.net p-ISSN: 2395-0072

A REVIEW ON NMAP AND ITS FEATURES

YASHVANT MAHADEV HANGE

Department of Mechanical Engineering, DIEMS College of Engineering, Aurangabad, Maharashtra, India.

Abstract - Network assaults have been common, resulting in the theft of private data. Information gathering is the first step that hackers do before launching an attack. Nmap is one of the most often used scanning programs at this point to gather data from the target host. To help with the ensuing attack, the acquired data can be further examined. Hence, a reliable method of identifying Nmap scanning behavior must be developed. In Nmap we can scan all the 65535 ports in one go with the packet customizable option, The intrusion detection system (IDS) frequently employs the ET OPEN rule set to safeguard hosts against nefarious intrusion. With ET OPEN restrictions in place, the Nmap detection rate is 58.3%; however, when IDS evasion is present, it drops to 8.3%. We suggest the Comprehensive Nmap Detection Rules because of the low detection rate of ET OPEN (CNDR). Nmap scanning habits can be precisely and effectively detected by CNDR. The customizable fields in Nmap are gone, and rules for operating system scanning are added in the CNDR. With our specified dataset, CNDR achieves 100% detection rate of regular Nmap scanning and 91.7% detection accuracy of Nmap with IDS evasion. The outcome demonstrates that CNDR is more resistant to customized scanning and is superior to ET OPEN.

Key Words: A Review of Nmap and its features, Network Mapper, Nmap tool, scanning the network, and Computer Networks

1. INTRODUCTION

Nowadays, everybody is connected to the world by the means of the Internet, the Internet has penetrated most of the world, and for connecting through the Internet we need to have devices that are capable of sending and receiving data packets. The devices are connected to each other by different types of topologies.

Every device which is connected to the internet has its own IP and MAC address. Computer Networking is the practice of exchanging data between nodes in a shared medium. This type of data of computers is sensitive in nature as hackers might clone the data and sniff to the target system.

There are several protocols available for the networks, and computers for the smooth functioning of the services. On a normal computer system, there are a total of 65535 ports, from which 1-1024 are dedicated and others are dynamic ports, so it is difficult for system administrators to track all the ports, which might result in possible vulnerability in the network, which can be exploited by hackers for extracting the data.

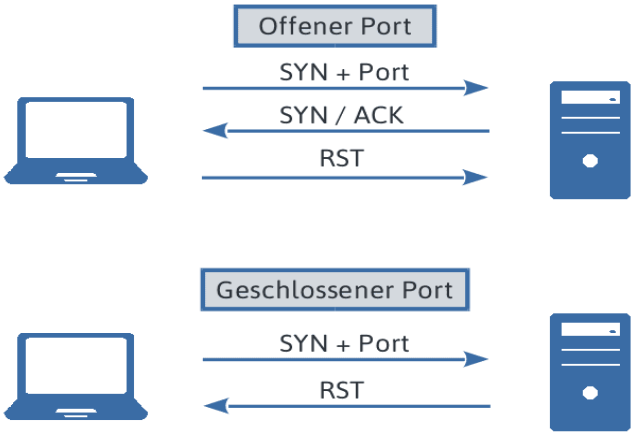
Computer Network security is mainly concerned about the computers that are connected to the internet, from the Network mapping tools we can gather information about the OS, open ports, versions of the system, and its vulnerabilities, The Nmap gives us a lot of features like gathering information about OS, ports, etc.

Nmap is open-source platform, Nmap, which stands for Network Mapper, is a free and open source program used for port scanning, vulnerability analysis, and, obviously, network mapping. Nmap was developed in 1997, yet it continues to serve as the benchmark for all other comparable programs, whether they are open-source or commercial.

2. SCANNING TECHNIQUES

2.1 SYN scanning - This is how nmap operates by default. Sending SYN packets to the intended system and watching for a response are involved. On the target machine, open ports are found using this method.

Each genuine connection attempt begins with this phase of the TCP three-way handshake. Scan me completes the second phase by sending a response with the SYN and ACK flags since the target port is open. On a typical connection, Ereet's machine, krad, would send an ACK packet to acknowledge the SYN/ACK and finish the three-way handshake. The SYN/ACK answer has informed Nmap that the port is open, hence it is unnecessary for it to perform this action.

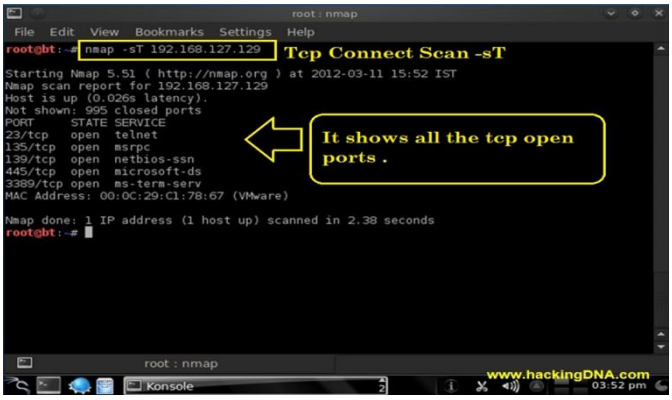


3. CONCLUSIONS

2.2 TCP Stealth Scanning –

To prevent port scans, TCP Stealth is a proposed change to the Transmission Control Protocol (TCP) that would conceal open ports for certain TCP services from the public. It resembles the port-knocking method in certain ways.

What about the failed TCP Packets, though? Unable to inform the sender whether the port is "Open" or "Closed" for business, a "Stealth" port merely "drops" all incoming packets.



2.3 Idle Scanning: By delivering forged packets to the target system, this method operates. An inactive system, sometimes known as a "zombie," receives a SYN packet from Nmap. The destination machine may have an open port at that IP address if the packet is acknowledged and a reply is sent.

2.4 Fragment Scanning:

Fragment scanning is a computer security method that includes evaluating an application's code to find and patch vulnerabilities. This scanning procedure entails breaking down the application's code into smaller, more manageable chunks, scanning each fragment for potential vulnerabilities, and then evaluating the results to establish the application's overall security posture. Fragment scanning can assist firms in identifying and correcting security problems early in the development process, hence avoiding costly and harmful security breaches later. It is a critical component of any complete security testing methodology.

2.5 UDP Scanning:

The technique of discovering open UDP ports on a target machine is known as UDP scanning. It is one of the most extensively used methods for network reconnaissance, and attackers frequently utilize it to uncover flaws in a target's network defenses. UDP, unlike TCP, is connectionless and lacks a handshake procedure, making it more difficult to detect available ports.

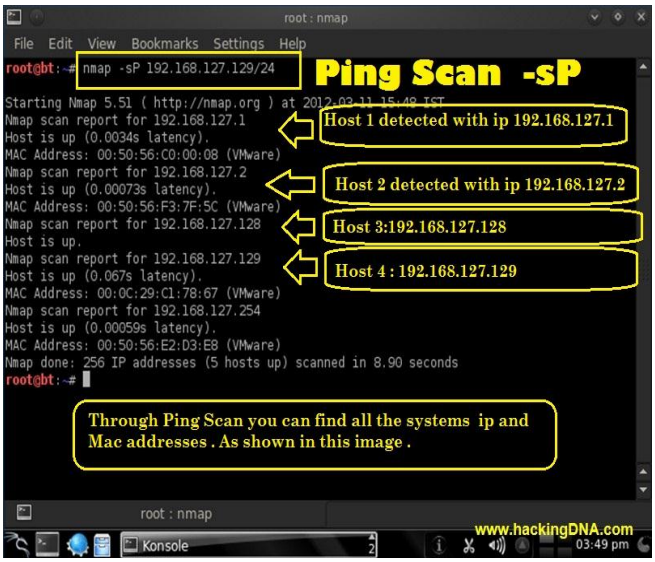
UDP scanning may be done using a variety of programs, including Nmap and hping. These programs send UDP packets to various ports to determine which are open and which are closed. Nevertheless, as compared to TCP scanning, UDP scanning has disadvantages since it does not provide stable connectivity and may not get answers from the target system, resulting in false positives and false negatives. Moreover, UDP scanning may set off network alarms and intrusion detection systems, notifying system administrators and even banning the scanning source.

Generally, UDP scanning can give useful information on a target system's weaknesses and strengths, but it should be handled with caution and consideration for potential consequences.

3. FEATURES:

System administrators, security experts, and ethical hackers frequently utilize Nmap, a well-known network scanner, for tasks including network inventory, vulnerability scanning, and more. With the purpose of learning more about the target network, it employs several scanning techniques. Here are some of the methods that Nmap employs:

3.1 Ping Scanning: To determine if the target IP addresses are up or not, Nmap sends ICMP Echo Queries to them. The term "ping sweep" is another name for this method.



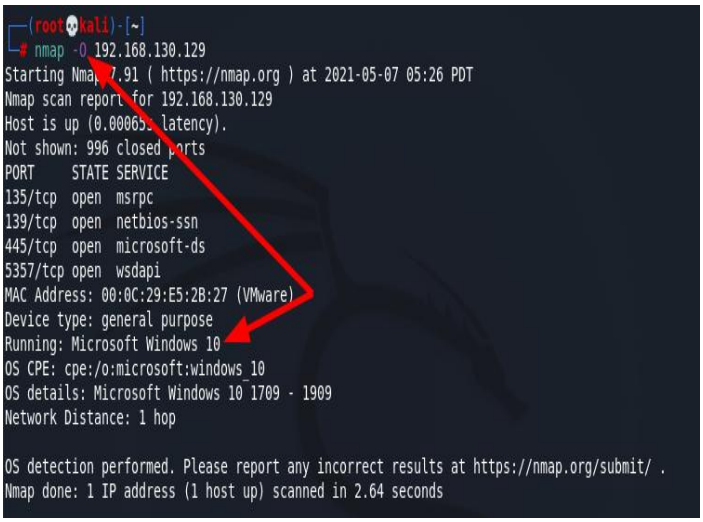
3.2 Port Scanning:

To find out which ports are open and which are closed, Nmap sends packets to the target IP addresses and

examines their responses. To accomplish this, it makes use of many types of scans, including TCP SYN scans, TCP Connect scans, and UDP scans.

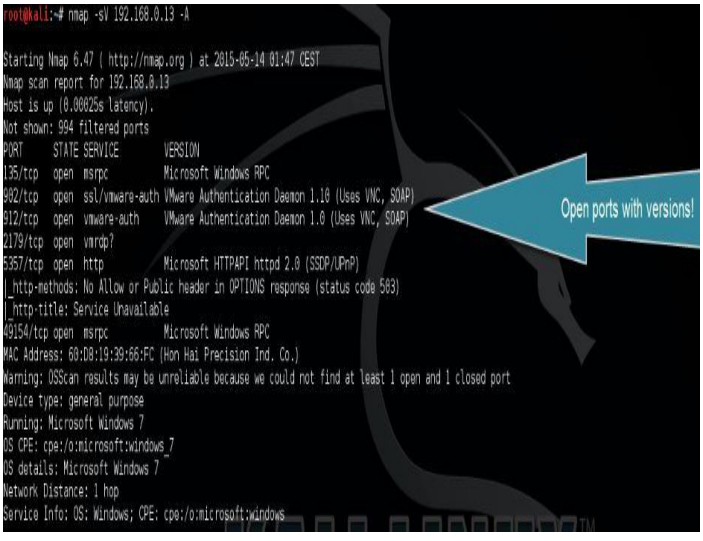
3.3 OS Detection:

By examining the replies to certain probes, Nmap may determine the operating system of the target computer.



3.4 Version Detection:

By examining the responses to specific probes, Nmap can ascertain the version of the services that are active on the target machine.

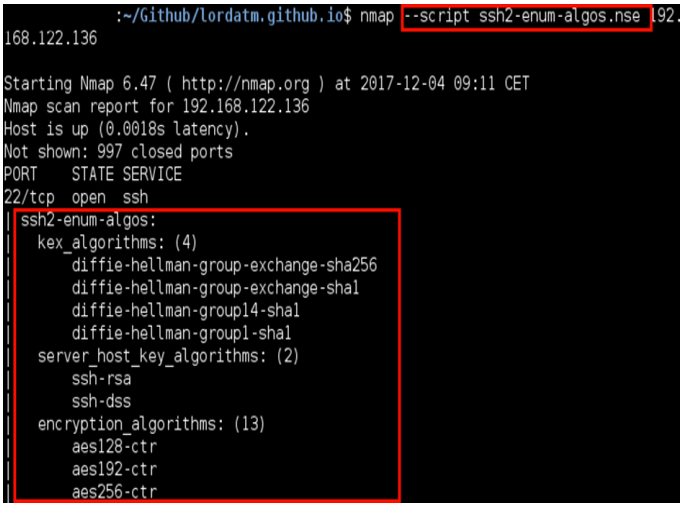


3.5 Script Execution:

Nmap offers a scripting engine that enables users to create original scripts to carry out various activities, like learning more about the target computer and finding vulnerabilities. Users of Nmap may execute both custom and pre-made scripts that can be downloaded from the Nmap Scripting Engine (NSE) database using the script execution feature. These scripts may be used to carry out a number of operations, including network mapping, version detection, and vulnerability screening.

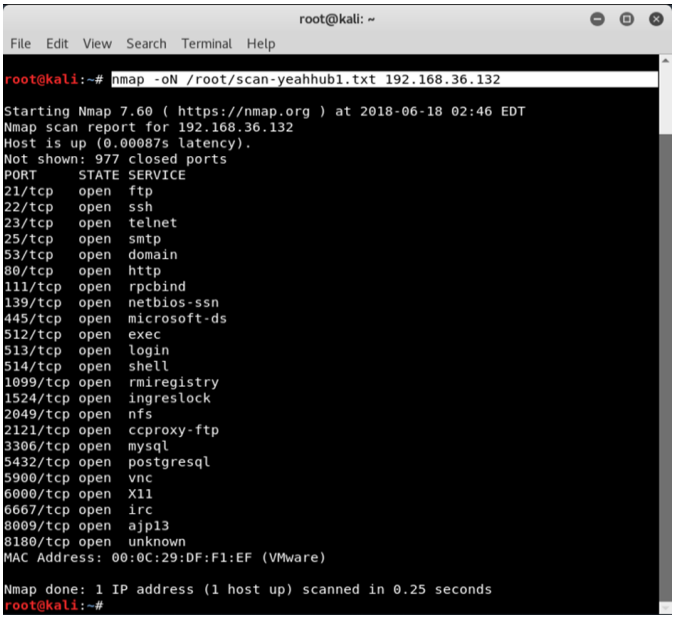
Users of Nmap may execute both custom and pre-made scripts that can be downloaded from the Nmap Scripting Engine (NSE) database using the script execution feature. These scripts may be used to carry out a number of operations, including network mapping, version detection, and vulnerability screening.

The vulnerability detection script and version detection scan will both be run by this command. Any known vulnerabilities will be looked for by the script, which will then notify the user.



3.6 Flexible output formats:

Nmap supports a variety of output formats, including XML, JSON, and GREP.



3.7 Vulnerability assessment:

Nmap is a flexible tool for vulnerability assessment that may be used to find possible vulnerabilities in target hosts and systems. It is vital to stress, however, that vulnerability assessment should be done ethically and with the approval of the target system owner.

Nmap-vulners, Vulcan, and vuln are the common and most popular CVE detection scripts in the Nmap search engine. These scripts allow you to discover important information about system security flaws.

3.8 NSE scripts:

A sophisticated feature of Nmap called NSE (Nmap Scripting Engine) enables the creation and execution of unique scripts during a scan. NSE scripts can automate processes that would otherwise require manual intervention and offer new capabilities to Nmap scans.

Advantages:

1. Automating tasks: Automating manual processes like banner capturing, service enumeration, and vulnerability assessment is possible with NSE scripts.

2. Increased accuracy: By using vulnerabilities and finding hidden services, NSE scripts can produce more precise findings than a regular scan.

3. Customization: NSE scripts provide users the ability to modify scans by adding certain parameters and flags.

4. Ease of use: NSE scripts are easy to use and require minimal input from the user.

3.9 Stealth Scanning:

Nmap has a stealth scanning feature that makes scanning more concealable and challenging to find. By blocking reverse DNS lookups and using idle scanning methods, it can evade discovery. Network administrators and security experts employ the method of stealth scanning to examine a network covertly. Because it is intended to evade detection by the security mechanisms of the target system, it is known as "stealth."

A number of settings for stealth scanning are available in the well-known network mapping program Nmap. Stealth scanning is often used to obtain data on a target system without the owner of the system being aware of the scan.

```
kali@kali:~$ sudo nmap -sT -P0 10.0.2.15
[sudo] password for kali:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-30 05:25 EDT
Nmap scan report for 10.0.2.15
Host is up (0.00018s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
kali@kali:~$
```

4. NSE (Nmap Scripting Engine)

NSE (Nmap Scripting Engine) is a sophisticated Nmap tool feature that allows users to build and run custom scripts to automate a range of network-related operations. NSE scripts are written in the Lua programming language and are supplied by default with the Nmap installation. Below is some information on NSE scripts.

NSE scripts are used to interact with network hosts in a more thorough and dynamic manner than typical network scanning tools allow. The scripts may be adjusted to match unique requirements, and the output generated by NSE scripts can be used to uncover security weaknesses and potential attack routes that typical scanning methods may not find.

NSE also integrates well with other tools like Metasploit, allowing users to expedite their security testing process and quickly detect and address vulnerabilities. In addition, the Nmap community routinely adds new NSE scripts, ensuring that the tool remains relevant and up to date in today's ever-changing cybersecurity scenario.

4.1 Purpose:

NSE's major goal is to automate network-related processes such as network scanning, host finding, vulnerability detection, and exploit testing. NSE scripts can be adjusted to fulfill specific needs, and users can also design their own scripts.

NSE offers a framework for users to develop and run custom Lua scripts to automate processes and enhance the capabilities of the Nmap utility.

4.2 Pre-installed scripts:

Nmap has many pre-installed scripts that may be used to automate a variety of network-related operations. These scripts are classified based on their usefulness, making it simple for users to choose the best script for a certain task. Below are some of the pre-installed script categories in Nmap:

1. Discovery scripts: These scripts are used to identify network hosts and determine which services are active on each host.

2. Host scripts: These scripts are used to collect information on a given host, such as its operating system, open ports, and services that are running.

3. Vulnerability detection scripts: These scripts are used to identify potential vulnerabilities on a host or network, such as weak passwords, open shares, or outdated software versions.

4. Exploit scripts: These scripts are used to test known exploits against specific hosts or services to determine if they are vulnerable to attack.

5. Intrusive scripts: These scripts are used to do more aggressive scans, which may disrupt services or network traffic. These scripts should be used with caution and only with the necessary permissions.

6. Brute force scripts: These programs are used to automate brute force assaults and password guessing.

7. Web scripts:

These scripts interact with web servers and web applications to perform tasks such as vulnerability scanning, web server fingerprinting, and testing for common web application vulnerabilities.

8. Misc scripts:

These scripts carry out several tasks, including checking for default credentials, searching for open proxies, and identifying SQL injection vulnerabilities.

You can use these pre-installed scripts in Nmap as-is or you can modify them to suit your needs. To further expand Nmap's capabilities, users can also create their own unique scripts using the Lua programming language.

4.3 Custom scripts:

NSE scripts can be written by users themselves using the Lua programming language. Any task that can be automated through Nmap can be carried out using these scripts. Users with a fundamental understanding of programming can use Lua because it is a lightweight, user-friendly programming language.

Here are the steps to create a custom script in Nmap:

1. Choose a task: Identifying the precise network-related task you want to automate is the first step in writing a custom script. For instance, you might want to run a more sophisticated network scan, gather more information about a particular host, or scan for a specific vulnerability.

2. Write the script: Once you have determined the task, you can use the Lua programming language to create the script. A lightweight, adaptable language made specifically for scripting, Lua. For the scripting engine, Nmap offers thorough documentation as well as a ton of starter examples.

3. Test the script: Once the script is written, you can run Nmap to test it out. To accomplish this, save the script to a file with the. nse extension and add it to your Nmap installation's scripts directory. The script can then be executed by either specifying its name on the command line or by using the --script option and the script's name.

4. Share the script: If you have written a helpful custom script, you can contribute it to the official Nmap Scripting Engine repository and make it available to the Nmap community. This gives the chance for feedback and collaboration, as well as allowing other Nmap users to profit from your work.

Nmap's custom scripts offer a potent method for automating particular network-related tasks and enhancing the program's functionality. You can build unique scripts that assist you in better comprehending and securing your network with a basic understanding of Lua programming and a little imagination.

4.4 Script execution:

The Nmap Scripting Engine (NSE) in Nmap can be used to run scripts. NSE offers a framework for executing scripts in a number of categories, such as web application scanning, vulnerability detection, and service enumeration. The steps to run scripts in Nmap are as follows:

1. Choose a script: Selecting a script that satisfies your unique requirements is the first step. Nmap comes with a sizable library of pre-installed scripts that are categorized according to their functionality. The Lua programming language can also be used to write unique scripts.

2. Specify the script: Once you have identified the script you want to execute, you can specify it on the command line using the --script option followed by the name of the script. For example, to run the "http-title" script, you would use the following command:

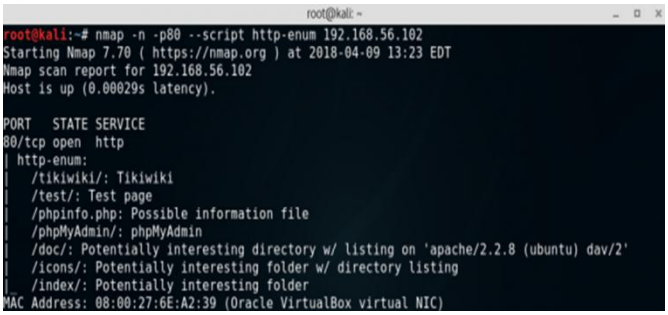
“ nmap -p 80 --script http-title <target>”.

3. Specify the script: Some scripts need extra arguments to function properly. These arguments can be specified by using the --script-args option and a list of key-value pairs. For instance, you would use the following command to specify the user-agent string for the http-title script:

“ nmap -p 80 --script http-title --script-args http.useragent="Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537.3" <target>. ”

4. Run the scan: Once you have specified the script and any required arguments, you can run the scan by specifying the target host or network.

5. View the results: Nmap will show the results of the script execution after the scan is finished. Details like open ports, active services, operating system information, and potential vulnerabilities might be included in the output. Using the -oN option and a filename, you can also save the results to a file for later analysis.



4.5 Integration with other tools:

Nmap can work together with other programs like Metasploit to automate the exploitation of vulnerabilities that it has identified. Users can streamline their security testing procedures and quickly find and fix vulnerabilities thanks to this integration.

4.6 Script output:

NSE scripts generate thorough output that can be used to examine a network scan's outcomes. Information like open ports, active services, and discovered vulnerabilities are included in the output. By using this data, remediation efforts can be prioritized and overall network security can be increased.

4.7 Community contributions:

The Nmap community regularly contributes new NSE scripts, which are open-source. Because of the community-driven approach, the Nmap tool is always current and useful in the rapidly changing cybersecurity environment of today.

In conclusion, the Nmap tool's NSE feature is a strong feature that enables users to automate a variety of network-related tasks. The tool includes a sizable library of pre-installed scripts, and the scripts can be altered to meet requirements. The comprehensive output generated by NSE scripts can be used to enhance overall network security, and Nmap can be integrated with other tools like Metasploit.

5. Conclusion:

Nmap is a versatile network exploration, administration, and security auditing tool. It includes functions such as host finding, port scanning, version detection, operating system identification, and vulnerability assessment. Nmap is adaptable and versatile, thanks to its command-line interface and extensive scripting features. Its user community is constantly building new modules and plugins. While it has significant limitations, such as the possibility of network interruption, system compatibility, and detection by intrusion detection systems, it is nevertheless an important tool for network administrators and security experts. Overall, Nmap is an effective and dependable tool for assessing network security and administration for both novice and professional users.

REFERENCES

1. Fyodor. (n.d.). About Nmap. Retrieved from https://nmap.org/book/man-about-nmap.html

Moore, D., & Beale, J. (2006). Nmap in the Enterprise: Your Guide to Network Scanning. United States: Syngress Publishing.

Smith, R. Parkinson, S. (2017). Nmap: Network Exploration and Security Auditing Cookbook. United States: Packet Publishing