Port scanning using Nmap

[1]Mamta Bhavsar, [2]Dr. Priyanka Sharma, [3]Manish Gokani
[1] Student, [2]Head Of Department, [3]CEO, F1 Network Security
[1,2] Department of Cyber Security, Raksha Shakti University, Ahmedabad (Gujarat)
[3]F1 Network Security, Vadodara (Gujarat)

Abstract— Anyone who wants to enter into cyber security domain or hacking world they all started with the port scanning. As we all know that Port is an endpoint of the communication where data enters into and go out from computer it is the first point that attacker or security administrator looking for. Port scanning is one of the most popular exploration techniques attacker used to discover services they can break into. Essentially, a port scan consists of sending a message to each port, one at time. The kind of response received indicates whether the port is open to exploit or not. Nmap is a security scanner used to discover open ports and services running on that port in a computer network.

Index Terms— Nmap, Port Scanning, Network Scanning

I. Introduction

A port scan is a series of messages sent by someone attempting to break into a computer to learn which computer network services associated with that port. Port scanning is a favourite approach of computer cracker, gives the assailant an idea where to probe for weaknesses. Nmap is a free, open source tool that is available under the GNU General Public License as published by the Free Software Foundation. It is most often used by network administrators and IT security professionals or Hackers to scan enterprise networks, looking for live hosts, specific services, or specific operating systems.

II. Six States of Port Determine by Nmap

- **Open**: An application is actively accepting TCP connections, UDP datagrams or SCTP associations on this port. Open port is defined that services running on that port is available for use. Attacker's main target is to find out open ports to exploit the targeted Host while the security provider tries to protect the open port by firewall and make them filtered for the legitimate users.
- **Closed**: Closed port can be reachable but it indicated closed because no application listening on that port. Closed port can be used by various port scanners to determine which OS is running on the targeted Host.
- **Filtered**: When Nmap send any packet to the targeted host and if that packet is blocked by firewall or some defined router rules then it gives error message that indicates Nmap doesn't recognise port is open or not and hence it is called Filtered Port.
- **Unfiltered**: When Nmap does not able to understand whether port is open or not, but it is accessible by the Nmap then it is called Unfiltered Port. Scanning unfiltered port with other scanning method is usefull to determine whether port is open or not.
- **Open Filtered**: Nmap places port in this state when open port gives no response. When Nmap scans the port but unable to determine whether port is open or filtered because of lack of response. It does not recognise packet is drop by the firewall or any response is elicited, then it comes to this category.
- **Closed Filtered**: This is the state when Nmap does not recognise whether port is closed or filtered.

III. Types of Port Scan

There are lots of tools available to determine a system's weaknesses and best method for an attack. Nmap by Fyodor is a best know tool used by system administrators for network exploration. Nmap uses is variety of activity probing techniques to determine live host, operating system, and what services running on that network. Some of the techniques used by Nmap to determine port state describe as below.

- **TCP SYN Scan**: In this scan Nmap sends SYN packet to the TCP port of the targeted Host. If Host replies with SYN-ACK packet it means that port is **open.** If it gets RST in reply that indicates that port is closed on that host. If target host doesn't reply that means our SYN packet is blocked by firewall or drop by some router rules and it indicates port is filtered.
- **UDP Scan:** In this scan Nmap sends UDP packet to the targeted Host. If it replies with UDP port that means port is open. If target port replies with port unreachable error that means port is closed. And if target host doesn't reply that means packet is blocked by firewall or service running on that port is not responding. UDP scan is slow because of it uses ICMP packet.
- **TCP ACK Scan:** This scan is different than the others discussed so far in that it never determines open (or even open|filtered) ports. It is used to map out firewall rulesets, determining whether they are stateful or not and which ports are filtered.

  In this scan Nmap sends packet with ACK flag set to the targeted Host. If it doesn't reply or reply with unreachable error that means packet is blocked by firewall and hence packet is filtered, or if it replies with RST packet Nmap labels them as Unfiltered. By using this scan attacker can get idea about target is easy to attack or not.
- **SCTP INIT Scan:** SCTP is a relatively new alternative to the TCP and UDP protocols, combining most characteristics of TCP and UDP, and also adding new features like multi-homing and multi-streaming..

This technique is often referred to as half-open scanning, because you don't open a full SCTP association. You send an INIT chunk, as if you are going to open a real association and then wait for a response. An INIT-ACK chunk indicates the port is listening (open), while an ABORT chunk is indicative of a non-listener. If no response is received after several retransmissions, the port is marked as filtered. The port is also marked filtered if an ICMP unreachable error (type 3, code 0, 1, 2, 3, 9, 10, or 13) is received.

- **TCP NULL, FIN, and Xmas Scans:** When SYN, RST or ACK bits are not included in packet any combination of other three FIN, PUSH, and URG bits are used by Nmap to determine port state.
- **Null scan (-sN):** set any bits (TCP flag header is 0)
- **FIN scan (-sF):** Sets just the TCP FIN bit.
- **Xmas scan (-sX):** Sets the FIN, PSH, and URG flags, lighting the packet up like a Christmas tree.

  These three scan types are exactly the same in behavior except for the TCP flags set in probe packets. If a RST packet is received, the port is considered closed, while no response means it is open|filtered. The port is marked filtered if an ICMP unreachable error is received.
- **SCTP COOKIE ECHO Scan:** SCTP COOKIE ECHO scan is a more advanced SCTP scan. It takes advantage of the fact that SCTP implementations should silently drop packets containing COOKIE ECHO chunks on open ports, but send an ABORT if the port is closed. The advantage of this scan type is that it is not as obvious a port scan than an INIT scan. Also, there may be non-stateful firewall rulesets blocking INIT chunks, but not COOKIE ECHO chunks. Don't be fooled into thinking that this will make a port scan invisible; a good IDS will be able to detect SCTP COOKIE ECHO scans too. The downside is that SCTP COOKIE ECHO scans cannot differentiate between open and filtered ports, leaving you with the state open|filtered in both cases.

IV. Experimental Platform

For performing port scan by using nmap we can use any platform like Windows, Linux, Mac OS etc. Nmap has come with GUI or command line interface. We can use any of the above to perform port scan. Hardware requirement to install nmap is for linux there is inbuilt tool available in kali linux or other liux OS, For windows OS we should install Nmap first for that intel i3 processor or above,500GB HDD, 2 GB RAM are required.

V. Performing Port Scan Using Nmap

Nmap is a best port scanner, it can do various other things too but are main focus here to scan port.Steps describe here is for linux users.

1. Open terminal or you can directly go to Application -> Information Gathering -> Nmap
2. Type nmap target_ip_address or Domain name
3. Now nmap will scan the most common ports and give result

VI. Conclusion

As we perform port scan using nmap it will give us information about all port state and services running on that port by using various techniques. It will help us to narrow our choice to whether to attack on that host or not. But here we should keep in are mind that it is the first step to hack or protect any network after that there is lot more things remaining to do further. It will just give as an idea about which type of network is there.

VII. References

[1] 2014Tariq Ahamad Ahanger, Port Scan – A Security Concern, International Journal of Engineering and Innovative Technology(IJEIT),ISSN-2277-3754, Volume 3 Issue 10 April.
[2] Nmap Network Scanning Guide – Gordon Lyon.