Stealth Scans: Introduction and Discussion (August 2021)

Nalongsone Danddank, Chi Dang, Adam Felling, Nathan Lantaigne-Goetsch

***Abstract*- This paper will review stealthy scans and security implications associated with these types of network scans. We will identify how these scans are performed, as well as the reasons behind these scans. The goal of our research is to deliver corroboration on how stealthy scans can be useful, while at the same time being a source of computer security problems. While showing the security issues associated with being scanned stealthily, we will observe how cybersecurity professionals can use stealth scans to improve security by visualization on networks through comparison of various methods of stealth scans.**

***Index Terms*--- Computer Hacking, Computer Security, Data Security, Encryption, Network**

I. INTRODUCTION

In the world of cybersecurity, stealth scans provide much functionality to computer and network protection. Stealth scans are procedures used to perform reconnaissance on a particular network, while remaining undetected[1]. Network administrators use stealth scans to perform penetration testing and to better understand their network. Cybercriminals use it as an important reconnaissance tool to help identify open ports, identify current running services, and identify operating systems. A stealth scan is a maneuver that a malicious hacker can use to establish the state of a communications port without establishing a full connection. In a lot of cases, hackers will devote extra time in reconnaissance to prepare for their exploits[2].

Various techniques can be used to perform stealth scans during reconnaissance periods, such as a method using TCP Connect protocol, utilizing the SYN flag, and alternate scans. Certain scans, or combinations of scans, can be used for better results under differing circumstances. Stealth scans can also provide security to networks if used correctly, and also get more interesting by developing a visualized technique for detecting network safety information by port scanning. Network administrators with a healthy understanding of stealth scans can strengthen their network and be better prepared for attacks from hackers.

II. HOW STEALTH SCAN WORKS

Stealth scan is the common type of port scanning that hackers tend to use to determine the status of communication ports from remote targets without fully establishing a connection [18]. Stealth Scan is TCP half-open port, and sometimes we refer to it as an SYN scan. It can scan more than thousands of ports in a second on a network while remaining undetected. This scanning does not affect by intrusive firewalls [18].

In order to start the process of communication between devices over the internet, an

Manuscript received August 10, 2021.

N. Danddank is a student at Metropolitan State University, St. Paul, MN 55106 USA (e-mail: nalongsone.danddank@my.metrostate.edu).

C. Dang is a student at Metropolitan State University, St. Paul, MN 55106 USA (e-mail: chi.dang@my.metrostate.edu).

A. Felling is a student at Metropolitan State University, St. Paul, MN 55106 USA (e-mail: dx1182nr@go.minnstate.edu).

N. Lantaigne-Goetsch is a student at Metropolitan State University, St. Paul, MN 55106 USA (e-mail: ri1178lw@go.minnstate.edu).

intruder has to initiate a connection to a server. This can be done by implementing a TCP three-way handshake [18]. First, the intruder would send a TCP packet with an SYN flag set to a target to establish a connection. When the port is open, the target will send a response packet with SYN and ACK flags back, which indicates the port is open and is listening [18]. So now, the port is open and ready to communicate between the intruder and the target. The last step will be different from the TCP three-way handshake; instead of sending an ACK to the target, the intruder sends an RST packet. RST means that it will reset and discard the attempted TCP connection [18]. Then, it terminates the connection.

III. IMPORTANCE OF STEALTH SCAN TECHNIQUES

Stealth scans can often be counteractive to defense mechanisms in cybersecurity and may or may not be authorized. They are normally done in order to find out what services are available. System administrators and network security analysts perform stealth scans in order to see what is exposed and vulnerable to attacks. On the other hand, bad faith actors perform stealth scans for the purpose of identifying what is unprotected and open to attacks[3]. For instance, during port scanning, a port scanner inspects IP address blocks for hosts and open ports. It is using Transmission Control Protocol/Internet Protocol (TCP/IP) network protocols. The status of a port will be open, closed, or filtered. Any open ports found pose a security risk, as they provide easy access to attackers.

Network administrators need to perform stealth scanning to monitor and troubleshoot their network. Particularly of importance for administrators is being able to identify which ports are open so they can limit these to some degree. The various types of stealth scan techniques have been developed to try to stay ahead of scan detection technology. Stealth scans help administrators better understand their network system, and in turn, provide better defenses against would-be attackers[3].

Additionally, stealthy bot threats are on the rise, looking to inflict damage on infrastructure or gather sensitive data from networks. Bots are programs to operate over the internet to perform repetitive tasks[4]. Stealthy bots are made to evade network detection often using open ports to gain access[5]. An administrator's job to defend the network against these types of attacks includes complete network monitoring solutions[6]. Thus, stealth scanning can be viewed as vitally important for cybersecurity professionals, with the idea that it helps administrators and cybersecurity analysts be proactive against attackers.

While stealth scans can help cybersecurity professionals better protect their network, hackers and cyber criminals utilize stealth scans to identify which networks to intrude and possibly exploit. Remaining unnoticed is an important advantage for hackers, which lessens the likelihood of getting booted from the network or caught. This is the reasoning behind hackers using stealth scans. Building on this, the hacker would first run a stealth scan, then identify if there is a vulnerability by fingerprinting the services run on machines on the network, determining if there is a service to be attacked, and finally, releasing an exploit targeting a specific service[7]. Once a hacker has access to this information, the outcome may be detrimental to any devices or data on the network.

As stealth scans provide data on how networks operate, bad faith actors exploit vulnerabilities to assist in larger malicious schemes. When hackers are able to identify vulnerabilities, like missing patches, unused services, poor authentication, or poor encryption, they can partake in several operations against the network, data on the network, or devices on the network[8]. When an attacker has infiltrated a network, server, or computer, they are able to gain access to higher level permissions. If the attacker is successful with privilege escalation, they could potentially install and run software on the machine and/or other machines. They also would be able to remove any previous remnants of their trail. This would be problematic, as they might have access to higher privacy files or install malicious software on machines on the network. Furthermore, following successful stealth scans and successful infiltration, hackers may install software to create a backdoor, which allows the attacker to remotely log onto the computer or server without detection[9]. All of this

adds up to attackers being able to maintain access to networks, while staying undetected. This means that sensitive information would be at risk until the attacker becomes detected. Therefore, stealth scans can be a vital piece of an attacker's arsenal, as cybersecurity professionals will likely handle the situation quickly if the intrusion is discovered.

IV. COMPARISON OF STEALTH SCANS

When it comes to ethical hacking there are some different ways for a computer security specialist to perform a stealthy scan of a target network. One of the most common tools used for performing these stealthy scans is known as nmap. Ironically, a solid number of computer security specialists do not have a proper understanding of how to control the binary switches(on/off) that allow for the nmap tool to be used for stealthy scanning of a network. Something that makes stealthy scanning more challenging is that the person attempting to perform the stealth scan must know the computer's system it is operating on. Which, in order to determine that, is typically done through a non stealthy scan. Now this scan can be done without being noticed, but the scan "will largely get picked up by devices on the network such as firewalls, SIEMs and IDS devices"[17]. These are basic security devices that nearly all computer systems have, because there are people who use computers that do not know a single thing about computer security and the threats against their computer.

The stealthy scans that we will be executing are typically targeting two things on the target computer. Which are identifying the ports and services for that computer. The reason for this is that the ports and services monitor any activity that is not considered to be 'normal'. A simple example of this abnormal activity could include an outside person (a random hacker) attempting to scan your computer's WiFi network it is connected to. With the intent on wanting to gather information about your computer's operating system, ip address, and anything else connected to the network. In order to make this happen the hacker must utilize a specific method for scanning the network without being caught. There are a few different ways that a hacker could do this, but each method has a difference compared to the others. These are the following stealthy scans that a hacker would likely use: half-open scan, inverse mapping, slow scan, FIN scan, X-mas tree scan. Now the first stealth scanning technique that a hacker would likely want to use as a go to weapon would be the half-open scan.

The half-open scan (which is also known as a syn-scan) is the most common type of stealth scan on the list. This scan is really similar to another type of stealthy scan, where the hacker would implement a handshake (connecting with another computer) that has a three way communication channel. This is known as a TCP connect() scan, and is more or less a half-open scan. However, the half-open scan is a two way communication channel instead of three. According to nmap's website, "The client sends a SYN packet to the server, then the server responds with a SYN-ACK packet to the client in case the port is open. The server will respond with an RST packet if the port is not open. Instead of the client responding with an ACK to acknowledge receipt of the RST, it sends the server an RST packet"[18]. What this means for a person who is not completely familiar with this kind of terminology. Is that the SYN-ACK packet is a TCP message that attempts to establish connection with the target device. This message from the ACK is to check for if the port is actively monitoring. Seeing how this stealth scan approach works. There are some disadvantages to this method. The firewalls can catch this scan pretty easily, and the scan requires root privileges in order to be executed. A root privilege means that the scan must have access to the superuser of the computer's operating system. After going over how the half-open scan compares to other stealthy scans such as the TCP connect() scan. Let us take a look at a unique stealth scan that tricks the target computer into believing a packet's check has concluded, but really that is something that this next scan will take major advantage of.

A scan that is well known for tricking target computers into accidentally revealing open ports that are being used by the system is known as a FIN scan. This scan's intent is to discover any tcp ports that are being used by the target computer. Now you are probably wondering how this scan performs in a stealthy manner? According to the website on Chapter 5. Port Scanning Techniques and Algorithms, The FIN scan sends packets of information with the FIN flag (which means the end of a communication).

Which then determines what tcp ports are open or closed based on the way each port reacts to the FIN flag packet. If the port is closed, then the computer responds back with an RST flag. However, if the port is open. Then the port's response is to simply ignore the FIN flag [18]. One thing that the FIN scan does an incredible job of compared to other stealth scans is determining what scans are filtered/open. Unlike scans that are similar like the xmas scan. The FIN scan can determine what ports are either open/closed. Which is really helpful for someone that is trying to determine the vulnerabilities of a target computer. However, the one downside of this scan is that it has difficulty determining what ports are filtered or open[18]. This reason is simple, because the FIN scan is designed to mainly determine what ports are either open/closed.

V. STEALTH SCAN AND VISUALIZATION

As network attacks increase in complexity, the ability to quickly analyze security data and mitigate the effect of these attacks becomes a difficult problem. Network security analysts depend only on some network secure products to study large amounts of log information to analyze and cope with network anomalies. With dramatic increase of network data volumes, diversities of attack types and more complexity, the traditional analytical means are no longer effective. How to enable those analysts to quickly figure out network status by advantage of cumbersome high-dimensional data information has become a critical concern in the field of network safety.

Here it develops a visualized technique for detecting network safety information by port scanning. After the analysis of network data packets and the use of information visualization technique, the visualized port scanning and detection system Scan Viewer is designed and developed. The experiment reveals that it can detect slow scan, distributed scan, various TCP stealth scans and so on. With the method, people have gotten out of helpless embarrassment by the weak scan [11]. To enhance security and to probe behavior of determining whether particular services are available on a host or network by observing the responses of connection attempts [12].

For example, using the Hilbert-curve map clearly revealed the strictly ordered reverse-byte incrementing behavior of the progression of the entire scan; without this visualization technique it is not clear that we would have verified this sequence (for all the three observable changing bytes) at all. Animations of the scan over time also exposed the three different phases of the scanning, and juxtaposing the Hilbert maps with a geographic map of bot activity as well as a traffic time-series allowed us to visualize multiple dimensions of the scanning simultaneously. We anticipate this technique will be useful by us and others for analysis of other large-scale Internet probing behavior [13].

As the world's voice communications completes its transition to an all-IP network, the vulnerability of VoIP infrastructure, and the emerging capabilities of botnets to illegitimately commandeer its resources, present a daunting challenge for internet architects, engineers, and policymakers. Analysis of this scan provides an illustrative if ominous indicator of the more sophisticated capabilities to surreptitiously survey and exploit critical infrastructure vulnerabilities on a planetary scale. Our darknet packet capture allowed a detailed analysis of a botnet's comprehensive and covert scanning behavior, and in the process we developed generalizable methods to correlate, visualize, and extrapolate botnet behavior across the global internet [13]. In particular, we use this technique to filter out traffic from sources that have not gained knowledge from the network in question. We evaluate the benefits of our technique on different visualizations of network flows.

The number of attacks against large computer systems is currently growing at a rapid pace. Despite the best efforts of security analysts, large organizations are having trouble keeping on top of the current state of their networks. With the multiplication of attacks on computer networks, system administrators need to monitor the networks carefully. But all the techniques or tools that they use still heavily rely on human detection [14]. A visual interactive network connection system representing traffic activities that reside in network flows and their patterns. In today's digital world, computer network security experts struggle to manage security issues

effectively. Reporting the network data in graphical form helps the expert to make decisions in a more effective and efficient way. Visualizing the network traffic seamlessly is a big challenge but an integrated network traffic visualization approach can resolve such issues effectively [15].

Another interest is the intersection of the fields of network security and data visualization techniques. Its objectives are to study modern approaches to represent data, which may be currently being used in other areas, and apply one of those approaches in the visualization of network traffic and attacks. Assessing the usefulness of the visualizations was also an objective, along with the constitution of a large data set of representations for several traffic classes and classical network attacks [16].

VI. Conclusion

In summary, stealth scans are an important aspect of cybersecurity and aid in maintaining a secure network. In this review paper, we have discussed how both cybersecurity professionals and cybercriminals use stealth scans to gather information about networks. We looked at how stealth scans work, specifically focusing on SYN scans and briefly looking at TCP connect protocol. Other techniques for stealth scans include, but are not limited to; half-open scan, inverse mapping, slow scan, FIN scan, and X-mas tree scan. Bad faith actors use varieties of these scans to perform reconnaissance for future possible attacks. It is imperative for network administrators to routinely run stealth scans to better understand their network and potential vulnerabilities. Thus, tools for scanning networks need to be well understood by computer security specialists. Nmap is a crucial tool that plays a large role in performing stealthy scans and can help administrators with mapping networks. We go on to observe the emerging trends in visualization of network traffic. We see how the representation of this data combined with stealth scans can improve overall security of our networks.

References

[1] Your Dictionary. (Website Accessed 2021, July). Stealth-Scan Meaning. [Online]. Available: https://www.yourdictionary.com/stealth-scan

[2] Said, Younis. (2020, June) Performing Stealth Scans with Nmap. [Online]. Available: https://linuxhint.com/stealth_scans_nma/

[3] Azad, Maulana. (2015, February). Network Forensics: Detection and Analysis of Stealth Port Scanning Attack. International Journal of Computer Networks and Communications. Available Online: https://ijcncs.org/published/volume3/issue2/p2_3-2.pdf

[4] Claypool, Brenden. (2002). Stealth Port Scanning Methods. GIAC Certifications. Available Online: https://www.giac.org/paper/gsec/1985/stealth-port-scanning-methods/103446#:~:text=Stealth%20scanning%20is%20a%20technique,to%20detect%20these%20stealth%20scans.

[5] Bot Definition. (Website Accessed 2021, July). What is a Bot? [Online]. Available: https://www.cloudflare.com/learning/bots/what-is-a-bot/

[6] C.B. Basha, N.S. Ram, P. Rodrigues, and Ranjith. (2010, April). Defending Against Stealthy Botnets. [Online]. Available: https://www.proquest.com/openview/fd0268ab00c471f5b5330e1472ebde23/1?pq-origsite=gscholar&cbl=2030612

[7] S. Venkatesan, M. Albanese, A. Shah, R. Ganesan, and S. Jajodia. (2017, October). Detecting Stealth Botnets in a Resource-Constrained Environment using Reinforcement Learning. [Online]. Available: https://dl.acm.org/doi/pdf/10.1145/3140549.3140552

[8] Manguino, J. (Website Accessed 2021, July). How Snort's Stealth TCP Port Scanning Works. [Online]. Available: http://bucarotechelp.com/networking/security/85092001.asp

[9] Buster, D. (2021, March). The 5 Phases of Hacking: Maintaining Access. [Online]. Available: https://www.globalknowledge.com/us-en/resources/resource-library/articles/the-5-phases-of-hacking-maintaining-access/

[10] Benniestan, A. (2004). NMap Tutorial. [Online]. Available: http://apachepersonal.miun.se/~janjon/oldcourse/dtab80/lab/lab1/Nmap_tutorial_2004-10-10.pdf

[11] X.D. Yu, M.Y. Zhang, M.Q. Zhu, K.H. Xu and Q.C. Xiang. (2014, March). Visualization of Network Security Information Based on Slow and Stealth Scan. [Online]. https://doi.org/10.4028/www.scientific.net/AMM.543-547.3173

[12] G. Shau, X. Chen, X. Yin, and X. Ye. (2016, July). A Fuzzy Detection Approach Toward Different Speed Port Scan Attacks Based on Dempster-Shafer Evidence Theory. [Online]. Available: https://onlinelibrary.wiley.com/doi/epdf/10.1002/sec.1508

[13] A. Dainotti, A. King, and K.C. Claffy. (2012). Analysis of a "/0" Stealth Scan from a Botnet. [Online]. Available: https://www.caida.org/catalog/papers/2015_analysis_slash_zero/analysis_slash_zero_imc.pdf

[14] Z. Jiwan, Y. Peng, L. Liangfu, and C. Lei. NetViewer: A Visualization Tool for Network Security Events. (2009, April). [Online]. Available: https://ieeexplore.ieee.org/document/4908300

[15] A. Bhardwaj and M.. Singh. Network Traffic Threat Detection and Reporting System Validation through UML. (2015). [Online]. Available: https://www.semanticscholar.org/paper/Network-Traffic-Threat-Detection-and-Reporting-UML-Bhardwaj-Singh/e2b766c2ca891d09eb8ac768523ab4feb1a073f3

[16] Pereira, P. Analysis of Network Attacks and Security Events using Modern Data Visualization Techniques. (2015). [Online]. Available: https://www.semanticscholar.org/paper/Analysis-of-Network-Attacks-and-Security-Events-Pereira/a3a76afb274d82d0bc2059f2c214e442ab76333b

[17] Obbayi, L. (2020, December 22). Ethical hacking: Stealthy network recon techniques. Infosec Resources. https://resources.infosecinstitute.com/topic/ethical-hacking-stealthy-network-recon-techniques. Available: https://resources.infosecinstitute.com/topic/ethical-hacking-stealthy-network-recon-techniques

[18] Nmap.org.(Website Accessed 2021, August).TCP SYN (Stealth) Scan (-sS).[Online]. Available: https://nmap.org/book/synscan.html