Stealth Scans: Something Clever?

By: 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. We will show the security issues associated with being scanned stealthily, how cybersecurity professionals can use stealth scans to improve security on networks and compare 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

Manuscript received August, 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: nathan.lantaigne-goetsch@my.metrostate.edu).

stealth scans to perform penetration testing and to better understand their network. Cyber criminals use it as an important reconnaissance tool to help identify open ports, identify current running services, and to 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 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

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 are 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. Methods of Stealth Scans

V. Comparison of Stealth Scans

VI. 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]. We also developed several animation and visualization techniques to facilitate our own exploration of the phenomena.

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].

VII. Conclusion

 III. References

[1]<https://www.yourdictionary.com/stealth-scan>

[2][https://linuxhint.com/stealth\_scans\_nma/](https://linuxhint.com/stealth_scans_nmap/)

[3]<https://ijcncs.org/published/volume3/issue2/p2_3-2.pdf>

[4][https://www.giac.org/paper/gsec/1985/stealth-port-scanning-methods/103446#:~:text=Stealth%20scanning%20is%20a%20technique,to%20detect%20these%20stealth%20scans](https://www.giac.org/paper/gsec/1985/stealth-port-scanning-methods/103446" \l ":~:text=Stealth scanning is a technique,to detect these stealth scans).

[5]<https://www.cloudflare.com/learning/bots/what-is-a-bot/>

[6]<https://www.proquest.com/openview/fd0268ab00c471f5b5330e1472ebde23/1?pq-origsite=gscholar&cbl=2030612>

[7]<https://dl.acm.org/doi/pdf/10.1145/3140549.3140552>

[8]<http://bucarotechelp.com/networking/security/85092001.asp>

[9]<https://www.globalknowledge.com/us-en/resources/resource-library/articles/the-5-phases-of-hacking-maintaining-access/>

  [10]<http://apachepersonal.miun.se/~janjon/oldcourse/dtab80/lab/lab1/Nmap_tutorial_2004-10-10.pdf>

[11]<https://doi.org/10.4028/www.scientific.net/AMM.543-547.3173>

[12]<https://onlinelibrary.wiley.com/doi/epdf/10.1002/sec.1508>

[13]https://www.caida.org/catalog/papers/2015\_analysis\_slash\_zero/analysis\_slash\_zero\_imc.pdf

[14]<https://ieeexplore.ieee.org/document/4908300>

Z. Jiawan, Y. Peng, L. Liangfu and C. Lei, "NetViewer: A Visualization Tool for Network Security Events," *2009 International Conference on Networks Security, Wireless Communications and Trusted Computing*, 2009, pp. 434-437, doi: 10.1109/NSWCTC.2009.353.

[15]https://www.semanticscholar.org/paper/Network-Traffic-Threat-Detection-and-Reporting-UML-Bhardwaj-Singh/e2b766c2ca891d09eb8ac768523ab4feb1a073f3

[16]https://www.semanticscholar.org/paper/Analysis-of-Network-Attacks-and-Security-Events-Pereira/a3a76afb274d82d0bc2059f2c214e442ab76333b