Personal Tool for Protection on the Net

Yasir mahmood
Department of Computer Science, College of Computer Science and Mathematics, University of Mosul, Mosul, Iraq
yaser.ali@uomosul.edu.iq

Article history : Received Nov 15, 2024 | Revised Des 28, 2024 | Accepted Des 31, 2024

Every time a computer device connects to the Internet it is at risk. Data theft is one of the threats facing computers when they connect to the Internet. For a computer to connect to the Internet, it needs an IP address and a port address to send and receive data. When the data reaches the computer via a port, it needs to reach the process that requested this information, which is linked to that port. A process does all the internet connections by the compute. These processes need an approach to send and receive information, which is the ports themselves. The attacker uses this port to make a connection to the victim's computer to steal information. In such situations, support is crucially needed to prevent these attacks from affecting our system. This work develops a personal tool for helping users to protect themselves from external attacks. The proposed tool monitors the open ports and shows all the information about the processes that are used. The proposed tool can close the open port, kill the process associated with it, and delete the process. When closing this port, the attacker cannot have access to the victim's computer. The findings show that the proposed tool is highly efficient when it comes to computer protection. The experimental results also demonstrate that the features of the tool can be tuned to fit users' interest.

Keywords: Port Scanner, Attack, Protection, Network Security, Personal Protection

1. INTRODUCTION

Network and computer security keeps equipment and data operational and restricts access to the right individuals. Because everyone in an organization could be impacted by a security breach, everyone should prioritize security. A network or computer can be damaged through theft, loss, infiltration into the network, and physical damage, among other methods. Production may suffer if equipment is destroyed or damaged. Equipment replacement and repairs can be expensive and time-consuming for the business. A network's resources can be depleted and private information exposed by unauthorized use. A deliberate assault that impairs a computer's or network's performance can also negatively impact an organization's output.

A firewall has been stated as one of the most effective security mechanisms for protection. Attacks on systems connected to the Internet are becoming more serious and sophisticated than they were in the past. We require all the assistance we can get to prevent these attacks from jeopardizing our system. Port scanning techniques can be used to discover some of the security holes at the victim, which means gathering information. So this technique is used as a preparation before the attackers have done. A port scanner can also be used as a simulation attack to test the same computer itself. So the user can discover the security holes in his computer and find the solution for it.

1.2 Research goal

The goal of this research is to discover the local open ports that the attacker can use to steal data or information. This is accomplished by finding all open ports and processes that used them, then terminating the suspicious or entrusted process and closing its port. Firewalls have their limitations, including the following [6]:

1. Attacks that get around the firewall are not something that the firewall can stop. Dialing out to the outside is a possibility for internal systems.
2. Internal dangers, such as a dissatisfied employee or an employee who unintentionally collaborates with an external attacker, are not covered by the firewall.
3. The transfer of files or programs contaminated with viruses is not something that the firewall can stop.

Because of this limitation, computers need to protect themselves from internal, and external attacks. The proposed tool finds all processes that make connections, terminates the untrusted process, and closes ports that are used by this process, which gives us more security by protecting the host from outer attacks, this tool works as a personal firewall.

1.3 Literature review

Recently, there has been a lot of research done to address problems associated with port scanning. The speed of port scans has been increased by sacrificing the accuracy of port scanning techniques. According to [1], the speed of the Scanrand utility is mostly attributable to its reliability tradeoff, which alters the duration of the timeout of connections to achieve higher scanning speed. One common trend in port scanning research is the application of machine learning to assist in the identification of port scanning assaults. After that [2] suggests a

DOI: 10.33387/ijeeic.v2i1.9105

machine learning technique to identify port scanning threats that take advantage of well-known supervised learning algorithms including Random Forest, AdaBoost, K-nearest neighbors, and Linear SVM. On the other hand, an anomaly detection approach, based on a mathematical model that analyzes captured packets, is proposed by the authors in [3], which is less traditional. The implementation of this mathematical model is done by software that detects ACK scans within 19 seconds on average. Moreover, To combat this particular issue, port scanning detection requires overcoming challenges like false positives and false negatives, [4] suggests battling false positives in the detection process by utilizing a customized fuzzy logic controller in conjunction with Snort. This approach's primary drawback is that its effectiveness over Snort without the fuzzy logic controller hasn't been thoroughly verified. A variety of methods have been suggested for performing port scanning instead of detecting it. Finally, [5] states that compared to other conventional port scanning approaches, its UDP scanning method can operate at a pace of about 190 times faster. Their method necessitates the presence of a network connection without network address translation (NAT) or port address translation (PAT).

1.3 Literature Gap and Contribution

Reviewing the previous literature, we found that all researchers focus only on scanning ports, and no action is taken regarding open ports. Therefore, we proposed a solution to address open ports using a tool that allows the user to discover open ports and the process that uses them, and then the user can stop the process, close the port, and delete the process. The remaining sections of this article describe the security threats and attacks, services, and mechanisms. The second section describes the proposed tool. The third section presents the results obtained and discussions. Finally, the whole work is concluded in Section Four.

1.4 Security threats

Two categories of computer security dangers need to be taken into account to safeguard machines and the network:

1. Physical events or attacks include those that steal from, harm, or destroy servers, switches, and wiring.
2. Data refers to incidents or cyber-attacks that erase, contaminate, restrict, permit, or pilfer information.

Threats to an organization's security can originate from both inside and outside and the possible harm can differ substantially.

There are two types of attackers:

1. Internal: Workers have access to the network, equipment, and data. Employees who intend to cause harm are said to be making malicious threats.
2. External: Users who are not affiliated with a company and who are not permitted to access a network or its resources

For understanding and satisfying network security, three aspects must be taken into account: security attacks, security mechanisms, and security services.

1.5 Attacks, Services, and Mechanisms

The manager in charge of security needs a methodical approach to defining security requirements and categorizing security techniques to assess an organization's security needs, and evaluate, and select different security products and policies. Three information security considerations can be taken into consideration as one method. [7, 8, 9]:

1. Any activity that jeopardizes the security of data that belongs to an organization is considered a security attack.
2. A security mechanism is a device or process intended to identify, stop, or neutralize security breaches.
3. A security service improves the safety of an organization's information exchanges and data processing systems. The services employ several security mechanisms to provide the intended defense against security assaults.

2. METHOD

One of the most widely used methods by attackers to find services they can compromise is port scanning. Many services on both well-known and lesser-known ports are operated by all computers linked to a Local Area Network (LAN) or the Internet. An attacker can determine which ports are open by using a port scan (i.e., what service might be listing to a port). A port scan entails delivering a message to every port individually. The type of response obtained shows whether or not the port is in use, allowing for additional probing for vulnerabilities.

Using the TCP/IP protocols, there are three tiers of addresses used on the internet: the Physical, Logical, and Port addresses. To transfer a significant amount of information from a source to the destination host, both logical and physical addresses are required. Nevertheless, the ultimate goal of data communication across the Internet is not to arrive at the destination host.

Computers these days are devices that can run numerous tasks at once, so a system that only transmits data between them is incomplete. The process of communicating with another process is the ultimate goal of Internet communication. To put it another way, methods—or addresses—are required to identify various operations. A process that has been given a label in TCP/IP architecture is referred to as a port process. To attempt to get access to the computer, the attacker searches for a vulnerability (open port) in the system.

Therefore, the first step in this research is to find all the open ports and the process in which that port. In this step, we implement a port scanner to find all the opening ports, and by using an AlocateAndGetTCPExTable function we can get the connection structure of all the active connections. The second step is to connect the process ID with the processes running on the computer, to isolate the processes that use a port from the another, and this is done by the process identifier PID of the process where each process has its ID and is the only one, and by this identifier, the process is connected with the port, so when the identifier is known we have got the port that is used by this process. The next step is to close the port by killing the process that used it. The last step is to locate the path of the process to delete it from the computer. Fig (1) shows the general steps of the proposed tool.

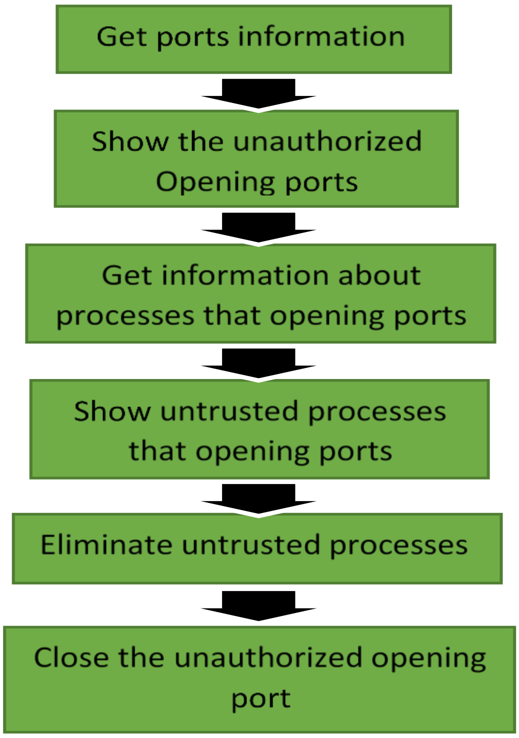

Get ports information
Show the unauthorized Opening ports
Get information about processes that opening ports
Show untrusted processes that opening ports
Eliminate untrusted processes
Close the unauthorized opening port

Figure 1. General steps of the proposed tool

2.1 Algorithm of the proposed tool

1. Call the function AlocateAndGetTCPExTable, this function gets a pointer to the array of the TCP connection structure (reside in the stack) for TCP connection.
2. Call the function AlocateAndGetUDPExTable this function gets a pointer to the array of the UDP connection structure (residing in the stack) for the UDP connection.
3. From steps 1 and 2 get the structure fields information that contains information about each connection, the information is:
   a) Protocols (TCP or UDP).
   b) Local Port.
   c) Remote port.
   d) Local IP.
   e) Remote IP.
   f) Status of connection.
   g) Process id.
4. For each running process in the system
   a) If the current processID = the required processID.
   b) Find the process name and process path.
      1) Select the untrusted process(s).
      2) Terminate the selected process(s).
      3) Close its port.
      4) From its path delete the source file.
      5) End.

3. RESULTS AND DISCUSSION

3.1 Results

Since the open ports could be considered as a weak point in a computer, therefore defending the computer can be done by terminating the untrust processes and closing its ports. Fig (2) shows the program interface with detailed information about each required process. The untrust process is the process that does not belong to the system and it is foreign to the user. Before terminating the untrusted process, the user has to ensure that it does not work again and he wants to know the source of this file (e.g. From a friend, downloaded from the Internet). To do that the user must find the path of each process, the path (the location that the process is stored in) then he will go to this location and remove the process.

There is a lot of information that belongs to each process. These are Process Name, Process ID, Local IP, Remote IP, Local Port, Remote Port, and the status of each port.

Remote IP: The IP of the computer that the process is trying to make a connection with.

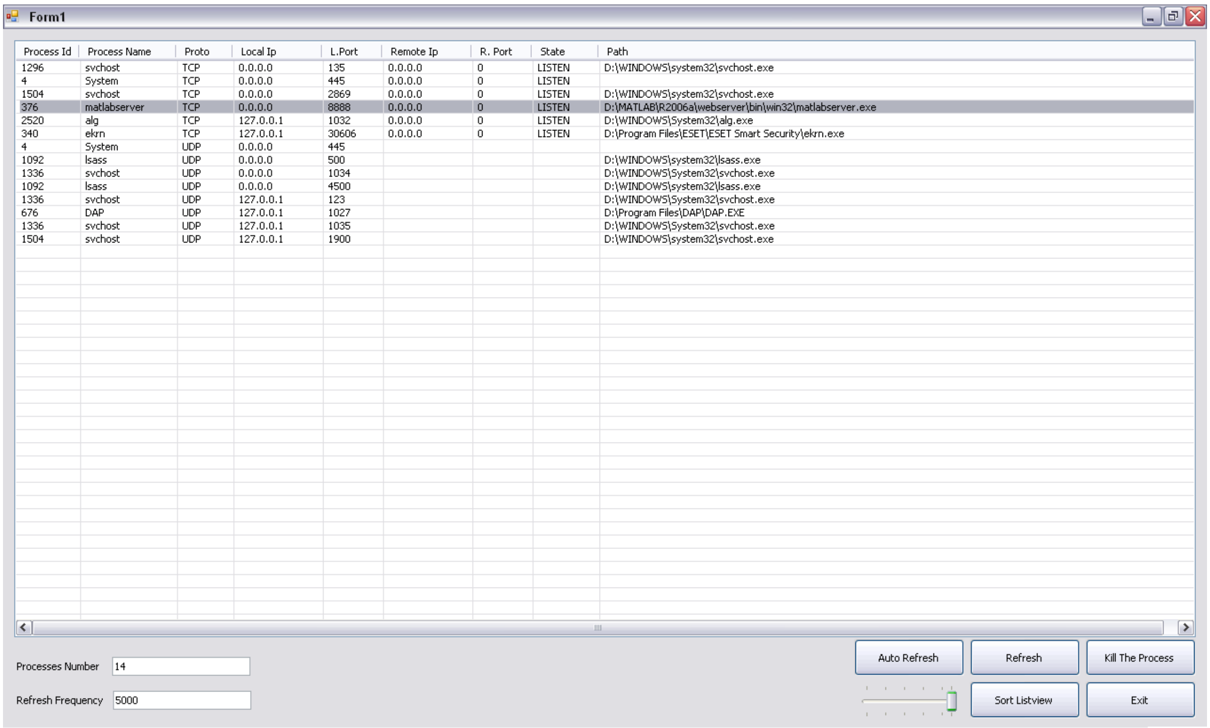
Local IP: the IP of the source computer.

Remote port: the open port number in the remote (destination) computer.

Local port: the port number in the source computer.

Status: the status of each port (listen or not).

The presented results show the performance of the proposed tool. However, other tools in the literature try only to perform port scanning without providing any information about these ports and the processes opened. Therefore, we believe that this work is promising compared to the literature since it outperformed the other similar tools in terms of the knowledge that can provide to users.



Process Id	Process Name	Proto	Local Ip	L.Port	Remote Ip	R. Port	State	Path
1296	svchost	TCP	0.0.0.0	135	0.0.0.0	0	LISTEN	D:\WINDOWS\system32\svchost.exe
4	System	TCP	0.0.0.0	445	0.0.0.0	0	LISTEN	
1504	svchost	TCP	0.0.0.0	2869	0.0.0.0	0	LISTEN	D:\WINDOWS\system32\svchost.exe
376	matlabserver	TCP	0.0.0.0	8888	0.0.0.0	0	LISTEN	D:\MATLAB\R2006a\webserver\bin\win32\matlabserver.exe
2520	alg	TCP	127.0.0.1	1032	0.0.0.0	0	LISTEN	D:\WINDOWS\System32\alg.exe
340	ekrn	TCP	127.0.0.1	30606	0.0.0.0	0	LISTEN	D:\Program Files\ESET\ESET Smart Security\ekrn.exe
4	System	UDP	0.0.0.0	445				
1092	lsass	UDP	0.0.0.0	500				D:\WINDOWS\system32\lsass.exe
1336	svchost	UDP	0.0.0.0	1034				D:\WINDOWS\System32\svchost.exe
1092	lsass	UDP	0.0.0.0	4500				D:\WINDOWS\system32\lsass.exe
1336	svchost	UDP	127.0.0.1	123				D:\WINDOWS\System32\svchost.exe
676	DAP	UDP	127.0.0.1	1027				D:\Program Files\DAP\DAP.EXE
1336	svchost	UDP	127.0.0.1	1035				D:\WINDOWS\System32\svchost.exe
1504	svchost	UDP	127.0.0.1	1900				D:\WINDOWS\system32\svchost.exe

Processes Number 14

Refresh Frequency 5000

Figure 2. Interface of the tool

3.2 Discussion

This research tries to develop a tool for finding open ports and the processes use these ports. The proposed tool detects these ports and provide users with comprehensive information about the ports and the processes. The, the tool enable users to close these ports easily. This kind of tool is crucial for protecting users' computers. It is recommended to use this tool whenever the user online. Furthermore, the tool can be further used to investigate other issues related to the information presented by the tool. This is important for securing the connections that tie the computer to the spider web. It is worth to mention that this tool can be integrated with other security tools aiming at providing more secure environment for computers.

Based on the literature mentioned in the literature review section, a table was created to compare the previous literature with the proposed tool and summarize it in terms of speed, reliability, data quality, and whether it was used as a tool or not. As show in Table 1.

Table 1. Compare proposed tool with literature review

Literature No.	Speed	Reliability	Data quality	Using as tool
[1]	Yes	No	No	No
[2]	No	Yes	Yes	No
[3]	Yes	No	No	No
[4]	No	No	Yes	No
[5]	Yes	No	Yes	No
Proposed tool	Yes	Yes	Yes	Yes

4. CONCLUSION

This tool plays a role in adding a personal protection layer to the personal computer while connecting it via the Internet by showing all open ports as well as showing the processes that use these ports to the user. By relying on the name of the processes as well as the location of these processes that exploits the ports we can identify the malicious process, and close these ports as well as kill the malicious processes that use these ports and remove them from the computer. Additional conclusions can be summarized as follows:

1. Using a port scanner to discover the open ports (in use).
2. There is not a complete security system, but there are many policies and procedures that must be traced by the users to protect their computers.
3. A personal firewall is effective and robust by discovering and controlling the malicious process that has connections that use the open ports.
4. To make the computer more secure, it's preferred to use a network firewall in the server computer besides the personal firewall in each local computer, for all local computers, using a network firewall like network address translation (NAT), can prevent the attacker (to make a scan to the local computer on a network because the attacker can't get the IP of the victim).

As future work, the proposed tool can be integrated with other port scanning tools. The proposed tool can also be extended to include more information that is of interest to users.

ACKNOWLEDGEMENTS

The author would appreciate the support provided by the Computer Science Department/ College of Computer Science and Mathematics/ University of Mosul during the steps of this work.

REFERENCES

[1] [1] Yuan, C., Du, J., Yue, M. and Ma, T. (2020) The design of large-scale IP address and port scanning tool. Sensors (Basel, Switzerland) 20 (16), 1-12.

[2] Algaolahi, A. Q. M., Hasan, A. A., Sallam, A., Sharaf, A. M., Abdu, A. A. and Alqadi, A. A. (2021) Port-Scanning Attack Detection Using Supervised Machine Learning Classifiers. 2021 1st International Conference on Emerging Smart Technologies and Applications (eSmarTA). 10-12 Aug. 2021.

[3] M. Lefoane, I. Ghafir, S. Kabir, and I. Awan, “Machine Learning for Botnet Detection: An Optimized Feature Selection Approach”. International Conference on Future Networks & Distributed Systems. Association for Computing Machinery, New York, NY, USA, 2021.

[4] Ananin, E. V., Nikishova, A. V. and Kozhevnikova, I. S. (2017) Port scanning detection based on anomalies. 2017 Dynamics of Systems, Mechanisms, and Machines (Dynamics). 14-16 Nov. 2017.

[5] I. Ghafir, V. Prenosil, A. Alhejailan and M. Hammoudeh, “Social Engineering Attack Strategies and Defence Approaches.” International Conference on Future Internet of Things and Cloud. Vienna, Austria, pp. 145-149, 2016.

[6] TCP/IP Protocols suite Second edition by Behrouz A. Forouzan with Sophia Chung Fegan

[7] Stallings W., "Network Security Essentials: Application and Standards", Printce-Hall, 2000.

[8] Majeed W., "Study of Computer Networks Protection and Simulation by Firewall", Mosul University, 2004.

[9] Al-Obaedey Y., "Study and Implementation Authentication Using Digital Signature", Computers Sciences, University of Mosul, 2004.

[10] Marni, R., Madgul, U. R., & Koyyala, C. T. (2023). OPEN PORT SCANNER TO IDENTIFY OPEN PORTS USING PYTHON. Journal of Science & Technology (JST), 8(12), 17-22.

[11] R. Marni, U. R. Madgul, and C. T. Koyyala, “OPEN PORT SCANNER TO IDENTIFY OPEN PORTS USING PYTHON”, Journal of Science &amp; Technology (JST), vol. 8, no. 12, pp. 17–22, Dec. 2023.

[12] Jafarian, J. H., Abolfathi, M., & Rahimian, M. (2023). Detecting network scanning through monitoring and manipulation of DNS traffic. IEEE Access, 11, 20267-20283.

[13] Abu Bakar, R., & Kijsirikul, B. (2023). Enhancing Network Visibility and Security with Advanced Port Scanning Techniques. Sensors, 23(17), 7541.

[14] Dhanya, K. A., Vajipayajula, S., Srinivasan, K., Tibrewal, A., Kumar, T. S., & Kumar, T. G. (2023). Detection of network attacks using machine learning and deep learning models. Procedia Computer Science, 218, 57-66.

[15] Mahmood, Y., & Abdulqader, A. (2021). A platform for porting IPv4 applications to IPv6. International Journal of Computing and Digital Systems, 10, 501-508

BIOGRAPHIES OF AUTHORS

Yasir Ali Mahmood, received a Bachelor of Science Degree from the Department of Computer Science from the University of Mosul in 2009 and a Master of Science Degree from the Department of Computer Science from the University of Mosul in 2020. Yasir Ali Mahmood is a lecturer at the Faculty of Computer Science and Mathematics, Mosul University, Mosul, Iraq. Researching about being in network, web scraper, and data mining. he can be contacted at email: yaser.ali@uomosul.edu.iq