2021 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom)

A Comparative Study of Credentialed Vulnerability Scanning and Non-credentialed Vulnerability Scanning

1st Anjie Chen
School of Computer and Cyber Sciences
Communication University of China
Beijing, China
chen_anjie@cuc.edu.cn

2nd Zhibing Zhang
China Telecommunication Technology Labs
China Academy of Information and Communications Technology
Beijing, China
greatbrian@139.com

***Abstract*—Vulnerability scanning is a common technique to detect security problems in computer systems. The scanning methods are divided into credentialed vulnerability scanning and non-credentialed vulnerability scanning. However, the relation and the difference between the results of two scanning types remain unclear in practice. In this paper, we use Nessus to scan 67 common hosts using the two methods, and perform a comparative analysis of the scan results. Our study shows that the results of the credentialed scans cover the results of the non-credentialed scans in most cases. Also, the difference between the scan results vary accordingly to the hosts' security level, and the variation presents linearity in general.**

Keywords—credentialed vulnerability scanning; non-credentialed vulnerability scanning; Nessus

I. INTRODUCTION

Vulnerability scanning is a common technique for discovering security problems in a computer system. System under test (SUT) is scanned based on a known vulnerability database. It plays an important role in discovering a system's security risks, and evaluating a system's security levels. The vulnerability scanner Nessus is one of the most commonly-used vulnerability scanners on the market. It is a software with a mature architecture and a continuously updated vulnerability database. We use Nessus as the only vulnerability scanner in this study [1].

In the practice of vulnerability scanning, the scanning methods are divided into credentialed vulnerability scanning and non-credentialed vulnerability scanning [2][4]. Non-credentialed vulnerability scans are to scan for vulnerabilities in the remote target system through the network, while credentialed vulnerability scans are to perform vulnerability tests inside the target system through a pre-configured privileged authenticated login. The typical steps of a non-credentialed scan are as follows. After getting the scan configurations, a host discovery is performed first, which aims to find out the hosts responding to the requests sent. Next, find all the listening ports in the hosts. Then, connect to the ports and detect the services or other information. Also, the scan tries to identify the operating system. All the information found in the previous steps contributes to the final vulnerability analysis. For credentialed scans, the operations that can be performed depend on the privileges granted to the pre-configured authentication. The credentialed scans can look through the internal files and processes through the granted authentication, and report insecure configs and other information. In our study, we give all credentialed scans root privileges. Therefore, the credentialed scans can perform any operation that a root user can perform.

In theory, credentialed vulnerability scans can access a system's internal files and processes, so compared with non-credentialed vulnerability scans, they can obtain more detailed system information, therefore can do a more thorough check and provide more comprehensive vulnerability information than non-credentialed vulnerability scans. Also, in related work [2][3][4], it is often mentioned that credentialed vulnerability scanning can gain better results than non-credentialed vulnerability scanning. However, it is not clear that the theory is true or not in practice. Also, there is no data supporting where the specific difference between the scanning results lies, and how much will it affect the quality of vulnerability assessments when we can only do one type of vulnerability scanning in production environments. In particular, even if the assumption is right in the practical sense, how many vulnerabilities and vulnerabilities at what level of risk are often missed out by non-credentialed scans remained unclear. Furthermore, this study can help promote the establishment of the standardized vulnerability scanning practices, providing experts with solid experimental data.

In our study, we performed vulnerability scanning on 67 common hosts applying credentialed vulnerability scanning and non-credentialed vulnerability scanning [1]. All the experiment data are uploaded to GitHub[1]. We perform some analysis on the data, and validate the theory of credentialed scanning being more comprehensive than non-credentialed scanning in most cases. Also, we find some more interesting phenomena regarding the difference between the scan results using credentialed scanning and non-credentialed scanning.

In section 2, we first introduce our practical implementation, and list all the target hosts' operating system and installed services in Appendix A. Next, we perform comparative analysis on the scanning results of the two methods. In section 2.B, we validate that the results of credentialed scans include

[1]https://github.com/Loonyluna12345/scanning-results

978-0-7381-2646-3/21/$31.00 ©2021 IEEE
DOI 10.1109/ISPA-BDCloud-SocialCom-SustainCom52081.2021.00215

the results of non-credentialed scans in most cases. In section 2.C, we find that the difference between the scan vary linearly according to the hosts' security level.

II. Comparative Experiment

A. Practical Implementations

We investigate 67 virtual machines set up on two servers, and each host was assigned an IP address of a local area network. Appendix A summarizes the operating systems and installed services of the 67 targets.

In terms of specific settings for credentialed scans, we configure the authentication information on Nessus' credential page one by one according to the specific services enabled on each host. For example, since most hosts have enabled SSH service on port 22 or remote desktop connection service on port 3389, the login method configured on the Nessus page is SSH or Windows, and more detailed authentication information should be filled in accordingly. Also, we grand all the credentialed scans root privileges.

B. Differences between Credentialed Non-Credentialed Scan Results

Since a credentialed scan is to scan inside the system and can obtain system information that cannot be obtained by a non-credentialed scan through network, the vulnerability information provided by a credentialed scan are more comprehensive and detailed [2][3][4]. For verification, we check whether the credentialed scanning results of the 67 targets include the non- credentialed scanning results.

60 of the 67 targets are consistent with the experience that the credentialed scanning results include non-credentialed scanning results. However, among the non-compliant 7 targets, 4 target's non-credentialed scan results only exceed the credentialed scan results by less than one piece of vulnerability information. To be more precise, these pieces of vulnerability information are also reported in the credentialed scans, but the pairs are not strictly identical. This shows that the scanning experience is basically correct. All the vulnerabilities that the credentialed scans do not discover compared to the non-credentialed scans are in the TCP protocol.

Next, we divide the system types of the target host into Windows and Linux, and count the average number of vulnerabilities of these two systems applying credentialed scanning and non-credentialed scanning. The average number of vulnerabilities in the scanned Windows system is more than that of the Linux system in general, and the number of vulnerabilities discovered in the credentialed scans far exceeds the number of vulnerabilities discovered in the non-credentialed scans. Figure 1 serves as an intuitive overview of the difference between the results.

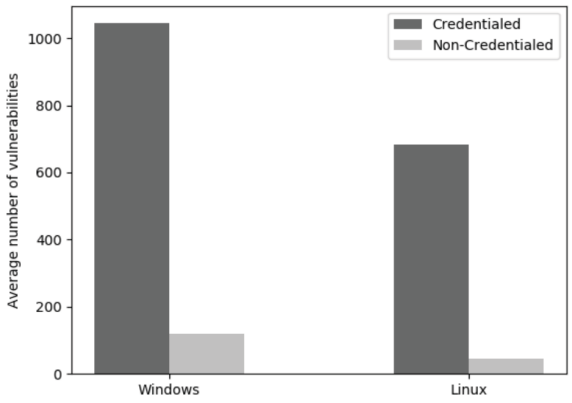
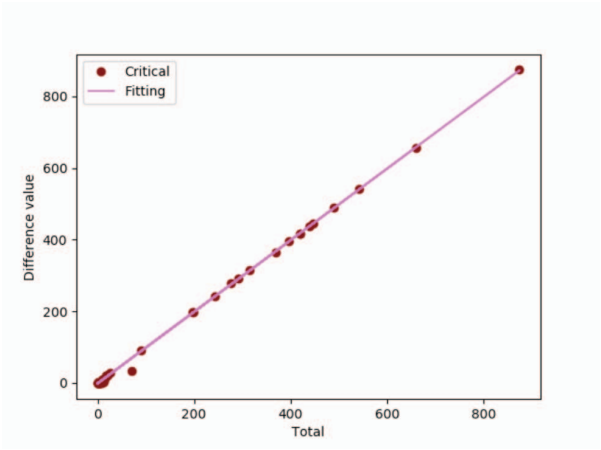


Figure 1. The average number of vulnerabilities of Windows and Linux applying credentialed scanning and non-credentialed scanning.

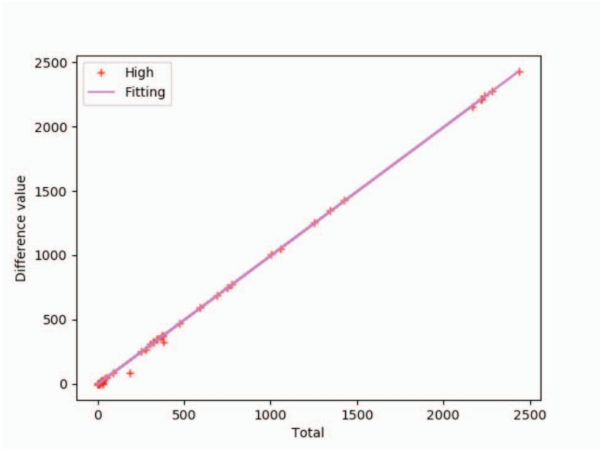
C. The Impact of System Security on the Difference between Credentialed and Non-credentialed Scan Results

Based on reasonable assumptions, the smaller the number of vulnerabilities in a system, the smaller the difference between the credentialed and the non-credentialed scan results; considering the most ideal extreme situation, if the system is very secure with no vulnerability, then the credential scan results will be the same as the non-credentialed scan results, which both report no vulnerability.

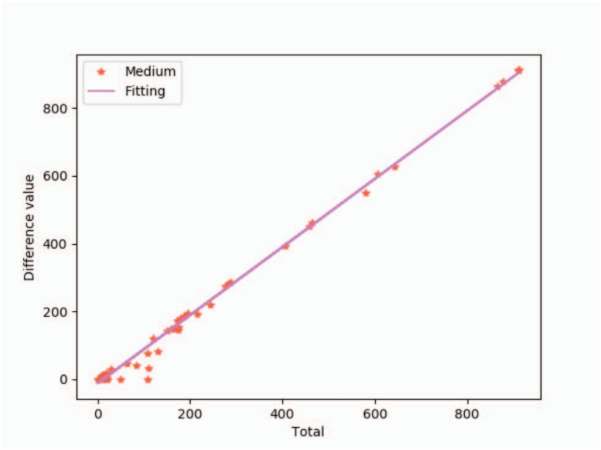
We count the 67 target hosts' credentialed scan results and non-credentialed scan results. According to the analysis in section 2.B, in most cases, the credentialed scan results are more detailed than the non-credentialed scan results, but there are also a few cases where the credentialed scan results do not include the non-credentialed scan result. We regard the total number of vulnerabilities in a system as the measure of the system security, also we view the larger number of vulnerabilities found in the two scans as the total number of vulnerabilities in a system for simplification. Vulnerabilities are categorized into critical, high, medium, and low according to their severity levels. What is more, the difference between the two scan results is measured by the absolute value of the difference in the number of vulnerabilities reported. As shown in Figure 2, according to the two measures mentioned above, we draw the scatter plots and fit polynomial functions based on the points. Whether it is from the number of critical, high, medium, and low vulnerabilities' point of view, or from the total number of vulnerabilities' point of view, the more vulnerabilities there are in the system, the larger is the difference. Furthermore, the relation shows a good linear correlation, and the coefficient of the first power of the fitted first-order polynomial is approximately equal to 1.



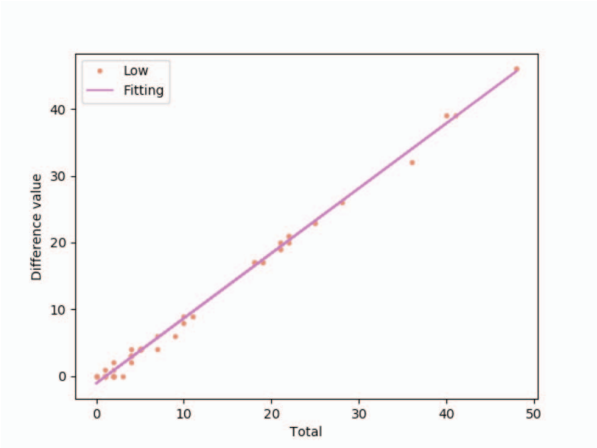
(a) y = x – 1.68



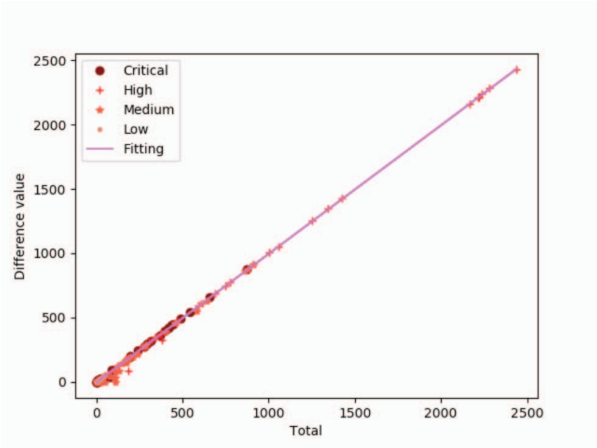
(b) y = x – 5.40



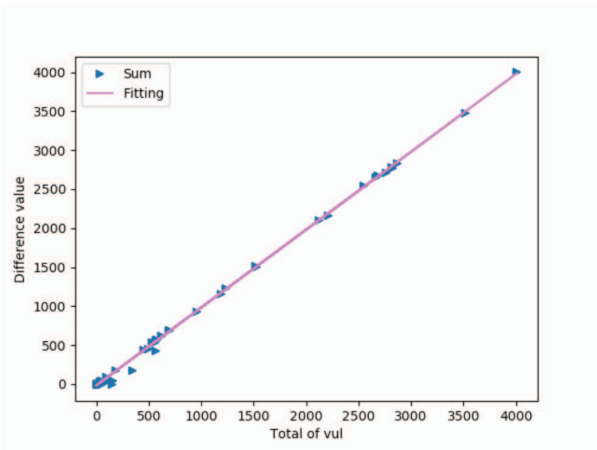
(c) y = 1.10x – 12.2



(d) y = 0.974x – 1.07



(e) y = x – 4.78



(f) y = x – 19.6.

Figure 2. The influence of the total number of vulnerabilities in the system on the difference between the numbers of vulnerabilities reported in the credentialed scans and the non-credentialed scans. The subtitles (a) to (f) list the fitted polynomial functions.

III. CONCLUSION

In this paper, we address the relation and difference between the results of credentialed scans and non-credentialed scans. We use the Nessus vulnerability scanner to scan 67 target hosts applying credentialed scanning and non-credentialed scanning respectively, and compares the scanning results of the two methods. Through comparison, we find that most of the target hosts are basically consistent with the theory of the credentialed scan results are more detailed and comprehensive than the non-credentialed scan results. Also, the less secure the target host is, the greater is the difference between the two scanning results, and the relation shows good linearity. Our work provides solid data and guidance for the choosing of the two types of scanning in practice.

REFERENCES

[1] Nessus 8.10.x User Guide, Tenable, Inc., 2021

[2] Ylätalo, Anssi. "Development of process and tools for vulnerability management." (2019).

[3] Anagandula, Karthik, and Pavol Zavarsky. "An Analysis of Effectiveness of Black-Box Web Application Scanners in Detection of Stored SQL Injection and Stored XSS Vulnerabilities." 2020 3rd International Conference on Data Intelligence and Security (ICDIS). IEEE, 2020.

[4] Aksu, M. Ugur, Enes Altuncu, and Kemal Bicakci. "A first look at the usability of openvas vulnerability scanner." Workshop on Usable Security (USEC) 2019. NDSS, 2019.

APPENDIX A

TABLE I. 67 TARGET HOSTS

No	Operating System	Installed Services
1	Centos7	SSH
2	Centos7	MySQL, SSH
3	Centos7	Tomcat, SSH
4	Centos7	Nginx, SSH
5	Centos7	PostgreSQL, SSH
6	Windows7	Microsoft SQL Server
7	Windows Server 2008	SQL Server 2008
8	Windows Server 2012	SQL Server 2012
9	Windows Server 2016	SQL Server 2016
10	Windows Server 2016	vCenter Server
11	Centos	Hbase, SSH
12	Centos	Kudu, SSH
13	Centos7.3	Mysql5.7, SSH
14	Centos7.6	Tomcat8.5, SSH
15	Centos7	Oracle12c, SSH
16	Redhat8.0	Redhat8, SSH
17	Frdora	Jboss4.3.2GA, SSH
18	Redhat4.8	Oracle11, SSH
19	Rhel	Nginx1.3.9, SSH
20	Ubuntu Kylin	Nginx1.4.6
21	Ubuntu14.04	Nginx1.8.1, SSH
22	Centos	OpenStack, SSH
23	Windows Server 2008	IIS7+PHP5.4.3
24	Ubuntu	MongoDB, SSH
25	Windows Server 2008	PhpMyAdmin
26	Windows7	SNMP
27	Windows7	Tomcat
28	Centos7	Solr, SSH
29	Windows7	Domino
30	Redhat	Oracle, SSH
31	Windows7	PostgreSQL
32	Windows7	SQLServer2012
33	Windows7	VMWare Workstation, DNS bind, MySQL, phpMyAdmin, Nginx, vSphere Client
34	Windows7	Sybase
35	Windows10	Hyper-V
36	Centos7	Xen, SSH
37	Windows Server 2008	Resin
38	Windows7	Squid
39	Centos6.3	TongWeb5.0, SSH
40	Centos	Websphere, AWVS, Wordpress, SSH
41	Centos7	KVM, SSH
42	Windows Server 2008	Wordpress
43	Centos7	Cassandra, Django, Dubbo, Elasticsearch, Wordexpress
44	Centos7	Weblogic, Tomcat, MySQL, Postgres, Redis, MongoDB, DB2, Oracle, SSH
45	Deepin 15.10	SSH
46	Galaxy Kylin Server 4.0	SSH
47	Galaxy Kylin Desktop 4.0.2	SSH
48	NeoKylin Linux ServerV6	SSH
49	NeoKylin Linux Desktop 6.0	SSH
50	Windows10	SQLServer
51	Windows7	DB2
52	NeoKylin Linux ServerV7	SSH
53	Neokylin Linux advanced server distributionsV7.0	SSH
54	NeoKylin Linux Desktop operating system software (megacore version)V7.0 B54	SSH
55	Centos7	Kalka, SSH
56	Centos7	Hadoop, SSH
57	Centos7	Ambari, SSH
58	Centos7	Apache Cassandra, SSH
59	Centos7	Elasticsearch, SSH
60	Centos7	Flume, SSH
61	Centos7	Gearman, SSH
62	Centos7	Oozie, SSH
63	Centos7	Splunk, SSH
64	Centos7	Stomp, SSH
65	Centos7	Hadoop+Hive+Impala+CDH, SSH
66	Centos7	Spark, SSH
67	Centos7	Zookeeper+Storm, SSH