МРНТИ 10.77.51 https://doi.org/10.58805/kazutb.v.1.22-308

METASPLOIT FRAMEWORK АРҚЫЛЫ ЖЕЛІ МЕН СЕРВЕРДЕГІ ОСАЛДЫҚТАРДЫ СКАНЕРЛЕУ ЖӘНЕ ОПЕРАЦИЯЛЫҚ ЖҮЙЕЛЕРГЕ ҚАШЫҚТАН ҚОЛ ЖЕТКІЗУ

Ж. Бидахмет[1], А. Уайда[1*], А.Д. Майлыбаева[2], Д.К. Даркенбаев[1], С. Бекназаров[1], Д. Бағдаулет[1]

[1]әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан,

[2]Халел Досмұхамедов атындағы Атырау университеті, Атырау, Қазақстан,

e-mail: uaida_a@mail.ru

Берілген мақалада ақпараттық қауіпсіздік аудитінің бір мысалы, желі мен сервердегі осалдықтарды Metasploit Framework құралымен сканерлеу және осы құрылғы көмегімен басқа операциялық жүйеге қалай қашықтан қол жеткізуді жүзеге асыруға болатындығы қарастырылып, толықтай сипатталған. Жұмыс практикалық түрде қосымшаларды пайдалана отырып жасалынды. Аудит құралдары үшін негізгі назар Kali Linux операциялық жүйесі және олардың қазіргі ақпараттық қоғамда желілік қауіпсіздікті қамтамасыз етудегі маңызды рөлін зерттеу қарастырылды. Сонымен қатар, мақалада зерттеу мақсаттарын анықтаудан бастап нәтижелерді талдауға және ұсыныстарды тұжырымдауға дейінгі ақпараттық қауіпсіздік аудитінің негізгі кезеңдеріне шолу жасалды. Сондай-ақ, аудит процесінде қолданылатын негізгі құралдар мен технологиялар қарастырылады, бұл киберқауіпсіздік саласындағы білімді кеңейтуге және аудит жүргізу сапасын арттыруға ықпал етеді. Мақалада зерттеу жұмыстары бойынша ақпараттық қауіпсіздік саласына қызығушылар үшін тиімді мысалмен қосымша сипатталып көрсетілген.

Түйін сөздер. Metasploit Framework, Meterpreter, аудит, ақпараттық қауіпсіздік, сканерлеу, шабуыл.

СКАНИРОВАНИЕ УЯЗВИМОСТЕЙ СЕТИ И СЕРВЕРА С ПОМОЩЬЮ METASPLOIT FRAMEWORK И УДАЛЕННЫЙ ДОСТУП К ОПЕРАЦИОННЫМ СИСТЕМАМ

Ж.Бидахмет[1], А. Уайда[1*], А.Д. Майлыбаева[2], Д.К.Даркенбаев[1], С. Бекназаров[1], Д. Бағдаулет[1]

[1]Казахский национальный университет имени аль-Фараби, Алматы, Казахстан,

[2]Атырауский университет имени Х. Досмухамедова, Атырау, Казахстан,

e-mail: uaida_a@mail.ru

В данной статье рассмотрен и подробно описан пример аудита информационной безопасности. Работа выполнена на практике с использованием приложений. Основное внимание для инструментов аудита уделялось операционной системе Kali Linux и изучению их важной роли в обеспечении сетевой безопасности в современном информационном обществе. Кроме того, статья предоставляет обзор ключевых этапов аудита информационной безопасности, начиная от определения целей исследования до анализа результатов и формулирования рекомендаций. Также рассматриваются основные инструменты и технологии, применяемые в процессе аудита, что способствует расширению знаний в области кибербезопасности и повышению качества проведения аудита. В статье дополнительно описан эффективный пример для тех, кто интересуется областью информационной безопасности по исследовательской работе.

Ключевые слова. Metasploit Framework, Meterpreter, аудит, информационная безопасность, сканирование, атака.

NETWORK AND SERVER VULNERABILITY SCANNING WITH METASPLOIT FRAMEWORK AND REMOTE ACCESS TO OPERATING SYSTEMS

Zh. Bidakhmet[1], A.Uaida[1*], A.D.Mailybayeva[2], D.K.Darkenbayev[1], S. Beknazarov[1], D.Bagdaulet[1]

[1]Al-Farabi Kazakh National University, Almaty, Kazakhstan,

[2]Khalel Dosmukhamedov Atyrau University, Atyrau, Kazakhstan,

e-mail: uaida_a@mail.ru

This article discusses and describes in detail one example of an information security audit. The work was done in practice using applications. The main focus for audit tools was on the Kali Linux operating system and the study of their important role in ensuring network security in the modern information society. In addition, the article provides an overview of the key stages of an information security audit, starting from defining the goals of the study to analyzing the results and formulating recommendations. The main tools and technologies used in the audit process are also considered, which contributes to expanding knowledge in the field of cybersecurity and improving the quality of audit. The article additionally describes an effective example for those who are interested in the field of information security for research work.

Keywords. Metasploit Framework, Meterpreter, audit, information security, scanning, attack.

Кіріспе. Ақпараттық-коммуникациялық технологиялар уақыт өткен сайын біздің өмірімізде барынша қолжетімді болып келеді. Бүгінгі таңда технологиялар өздерінің дамуы тұрғысынан емес, оларды қоғамның әр саласында пайдалану мүмкіндігімен бағаланады.

Компьютерлік желілерде қол жеткізуді басқаруды ұйымдастыру және пайдаланушының артықшылықтарын бөлу кезінде көбінесе желілік операциялық жүйелердің кіріктірілген құралдарын пайдаланады. Сонымен бірге, мұндай қауіпсіздікті басқару жүйесінде әлсіз тұстар бар: қол жеткізу деңгейі және жүйеге кіру мүмкіндігі парольмен анықталады. Құпия сөзді теріп алуға болатындығы құпия емес [1].

Ақпараттық қауіпсіздік аудиті - ақпараттық қауіпсіздік жүйесінің ағымдағы жағдайын тәуелсіз бағалау, оның белгілі бір критерийлерге сәйкестік деңгейін белгілеу және ұсынымдар түрінде нәтижелерді беру. Ақпараттық қауіпсіздік аудиті ақпараттық қауіпсіздіктің барынша толық және объективті бағасын алуға, бар туындаған мәселелерді жоюға және ұйымның ақпараттық қауіпсіздік жүйесін құрудың тиімді бағдарламасын әзірлеуге мүмкіндік береді [2].

Ақпараттық қауіпсіздік аудитіне жалпылама тоқталатын болсақ, әрбір кәсіпорындар мен жеке компаниялар, жоғары оқу орындарындағы ақпараттардың қаншалықты қорғалғандығын анықтау, деңгейін білу болып табылады. Ақпараттық қауіпсіздік аудиторы ұйымның ақпараттық қауіпсіздігін бақылау құралдарын, саясаттары мен процедураларын бағалауға жауап береді. Олардың рөлі ұйымның ақпараттық активтерін дұрыс қорғауды қамтамасыз етуге және оларды салалық стандарттарға, ережелерге және озық тәжірибелерге сәйкестендіруге бағытталған. Ақпараттық қауіпсіздік аудиторлары ұйымның қауіпсіздік жүйесіндегі осалдықтарды, олқылықтар мен әлсіздіктерді анықтау және жақсарту бойынша ұсыныстар әзірлеу мақсатында кешенді тексерулер жүргізеді [3-4].

Аудитор мамандар тәуекелдерді бағалайды, қауіпсіздік саясаты мен процедураларын талдайды және ұйымның техникалық инфрақұрылымын, жүйелері мен желілерін терең зерттейді. Олар кіруді бақылау, шифрлау, оқиғаларға жауап беру процедуралары және Апатты қалпына келтіру жоспарлары сияқты қауіпсіздік шараларының тиімділігін бағалайды. Ақпараттық қауіпсіздік аудиторлары, сонымен қатар, заңды және реттеуші тәуекелдерді орындау және азайту үшін ұйымның тиісті заңдарға, ережелерге және салалық стандарттарға сәйкестігін бағалайды. Олар егжей-тегжейлі аудиторлық есептерді ұсынады, нәтижелерді басшылықтың назарына жеткізеді және түзету шараларын жүзеге асыру және ұйымның жалпы қауіпсіздігін арттыру үшін мүдделі тараптармен ынтымақтасады [5-6].

Материалдар мен әдістер. Практика жүзінде осалдықты сканерлеу құралы ретінде - Metasploit Framework қолданылады. Ол - бұл хакерлер, ену мамандары және киберқылмыскерлер желідегі және сервердегі осалдықтарды зерттеу үшін пайдалана алатын қуатты құрал. Бұл платформа ашық бастапқы код болып табылады, сондықтан оны әртүрлі операциялық жүйелерде оңай бейімдеуге және пайдалануға болады. Көптеген негізгі себептерге байланысты Metasploit Framework кеңінен танылған және киберқауіпсіздік саласында қолданылады.

1. Бастапқы кодтың ашықтығы: Metasploit, ашық

бастапқы жоба, киберқауіпсіздік мамандарына оны нақты талаптарға сәйкес өзгертуге және бейімдеуге мүмкіндік береді. Бұл элемент құралды жақсартуға және оның мүмкіндіктерін кеңейтуге көмектесетін белсенді әзірлеушілер мен зерттеушілер тобын құруға ықпал етеді.

2. Модульдік Архитектура: Metasploit құрылымы эксплуатациялар, пайдалы жүктемелер және көмекші модульдер сияқты әртүрлі бөліктерді біріктіруге мүмкіндік беретіндей етіп ұйымдастырылған. Бұл Metasploit бағдарламасын ену сынақтарын өткізуге арналған қуатты және икемді құралға айналдырады.

3. Халықаралық зерттеушілер қауымдастығы: Metasploit киберқауіпсіздік зерттеушілерінің, әзірлеушілерінің, мамандарының әртүрлі және белсенді халықаралық қауымдастығынан тұрады. Бұл осы құралдың үздіксіз дамуы үшін маңызды болып табылатын ақпарат, тәжірибе және жаңа эксплуатациялармен алмасуды қамтамасыз етеді.

4. Протоколдар мен осалдықтардың кең ауқымын қолдау: Metasploit веб-қосымшалар, желілік құрылғылар және операциялық жүйенің қауіпсіздігін тексеру құралдары сияқты әртүрлі нысандармен жұмыс істейді.

5. Пайдалану мүмкіндігі: Metasploit құралдар жинағы консольді де, графикалық пайдаланушы интерфейстерін де қамтиды, бұл оны тәжірибелі мамандар үшін де, киберқауіпсіздікке жаңадан келгендер үшін де оңай етеді.

Осылайша, Metasploit Framework өзінің кәсіби міндеттерін орындау үшін киберқауіпсіздік мамандары үшін ең қолайлы құралдардың бірі ретінде өзінің беделін сақтайды, өйткені ол әмбебап және тиімді құрал болып табылады. Егер біз сипаттамаларды қарастыратын болсақ:

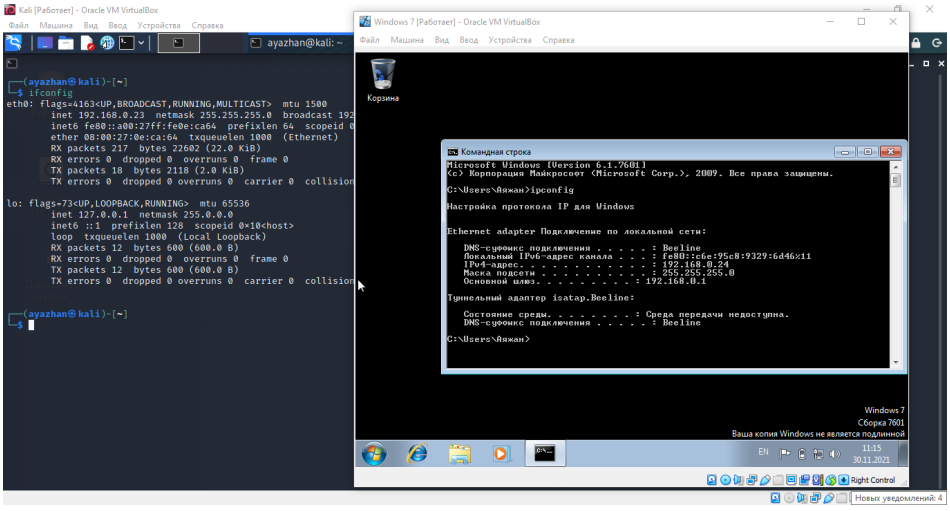
- Модуль архитектурасы: Metasploit көптеген модульдерден тұрады, соның ішінде эксплуатациялар, пейлоадалар, осалдық сканерлері және т.б.
- Эксплуатациялар мен пейлоадалар: бұл құралдар анықталған осалдықтарды пайдалануға мүмкіндік береді. Пейлоадалар жүйеде белгілі бір функцияларды орындайды, ал эксплуатациялар қол жетімділікті қамтамасыз етеді.
- +Әртүрлі операциялық жүйелерді қолдау: Metasploit Windows, Linux, macOS және басқаларға негізделген жүйелердегі осалдықтарды анықтай алады.
- Интерфейстердің әртүрлілігі: пайдаланушыларға графикалық интерфейсті (мысалы, Armitage) және консоль интерфейсін (msfconsole) ұсынады.

Пайдаланылған машиналар:
Шабуылдаушы: Kali Linux (2020)
Құрбаны: Windows 7 x 64

Біздің жүйедегі IP мекенжайлары келесідей:

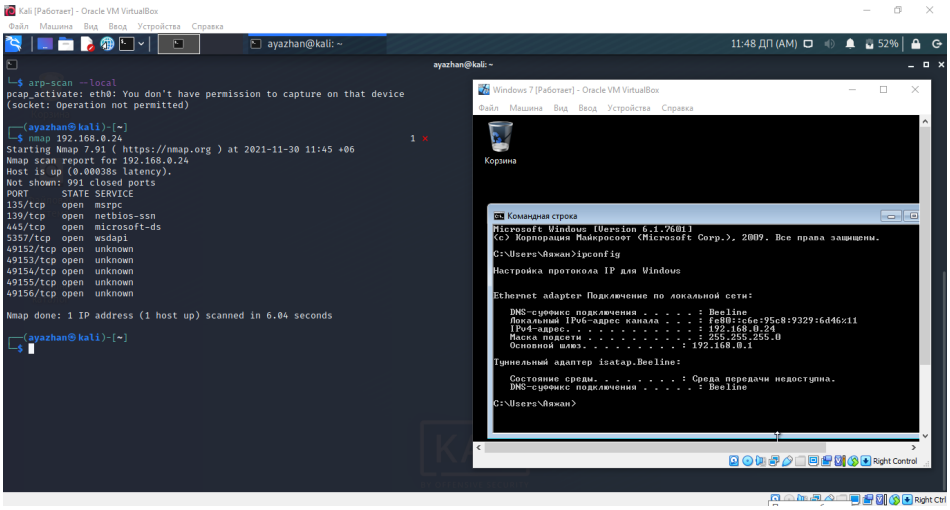
Kali Linux: 192.168.0.23
Windows 7: 192.168.0.24

Нәтижелер және талқылау. Алдымен екі операциялық жүйеде де IP мекенжайларын Kali-де ifconfig, Windows-та ipconfig пәрменімен төмендегі суретте көрсетілгендей тексеріп аламыз (1-сурет).



1-сурет - IP-мекенжай тексеру

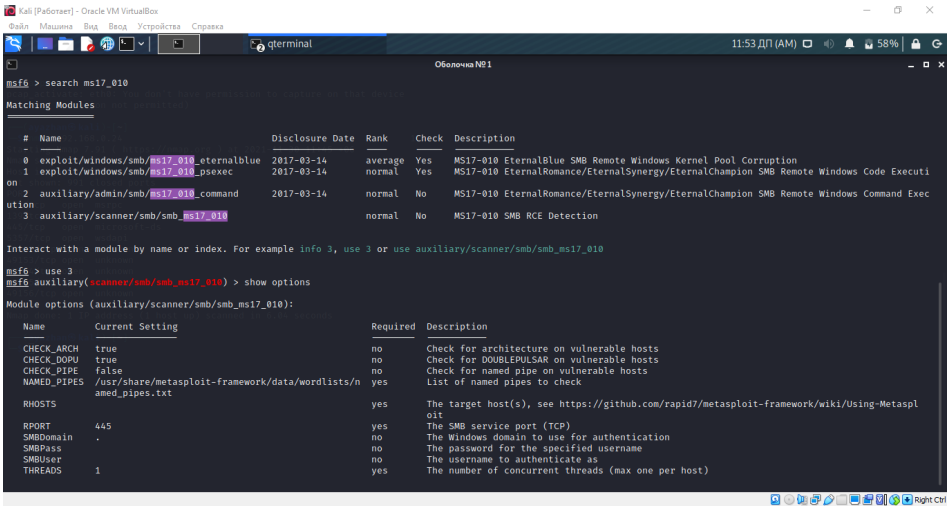
Келесі nmap құрылғысы арқылы Kali Linux операциялық жүйесінде ашық порттарды қараймыз. #nmap 192.168.0.24



2-сурет- Nmap арқылы сканерлеу

Metasploit Framework қосымшасына қосылып, meterpreter-ге қосыламыз (3-сурет).

```
#msfconsole
> search ms17_010
> use auxiliary/scanner/smb/smb_ms17_010
> show options
```

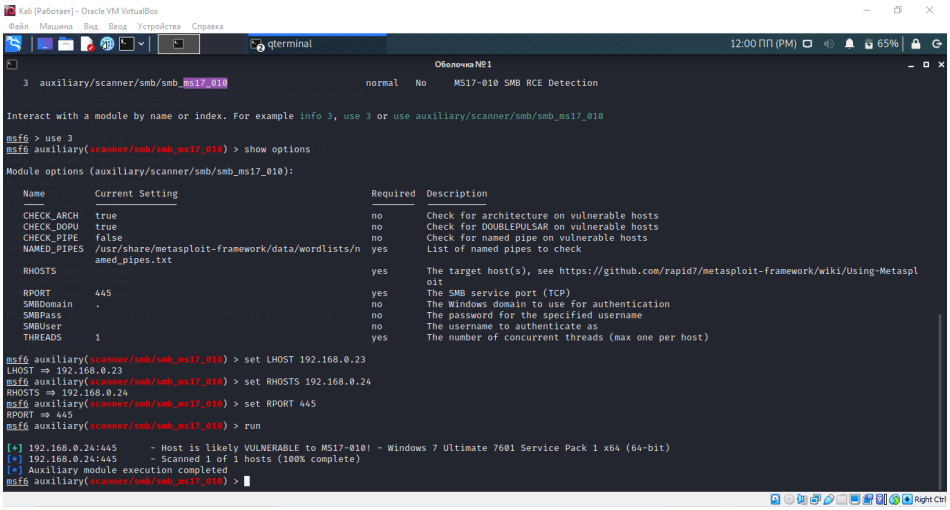


3-сурет - Meterpreter-ге қосылу

Осында қажетті IP мекенжай, порттарды 4-суреттегідей етіп қоямыз.

```
> set LHOST 192.168.0.23
```

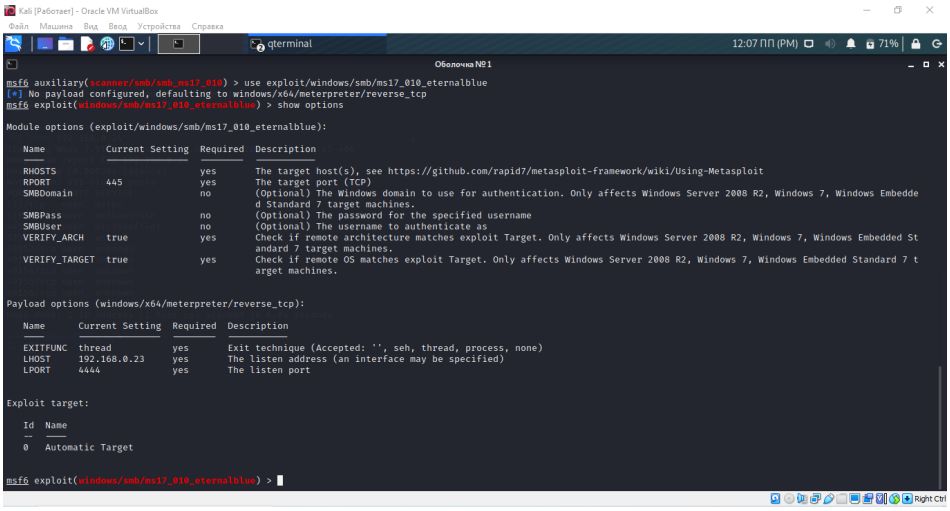
```
> set RHOSTS 192.168.0.24
> set RPORT 445
> run
```



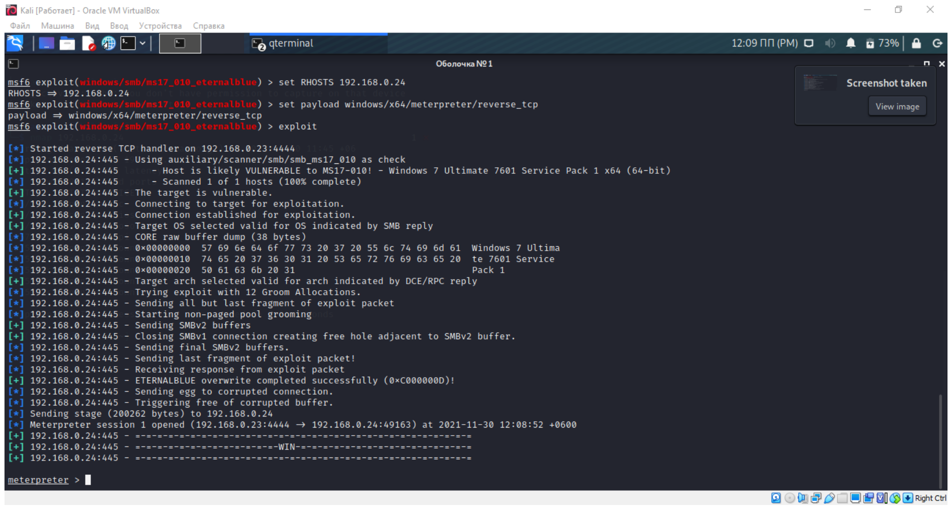
4-сурет - IP мекенжай, порттарды қою

Енді біз Windows 7 жүйесінде шабуылды орындауға көшеміз (5-6-суреттер).

```
> use exploit/windows/smb/ms17_010_eternalblue
> show options
> set RHOSTS 192.168.0.24
> set payload windows/x64/meterpreter/reverse_tcp
> exploit
```

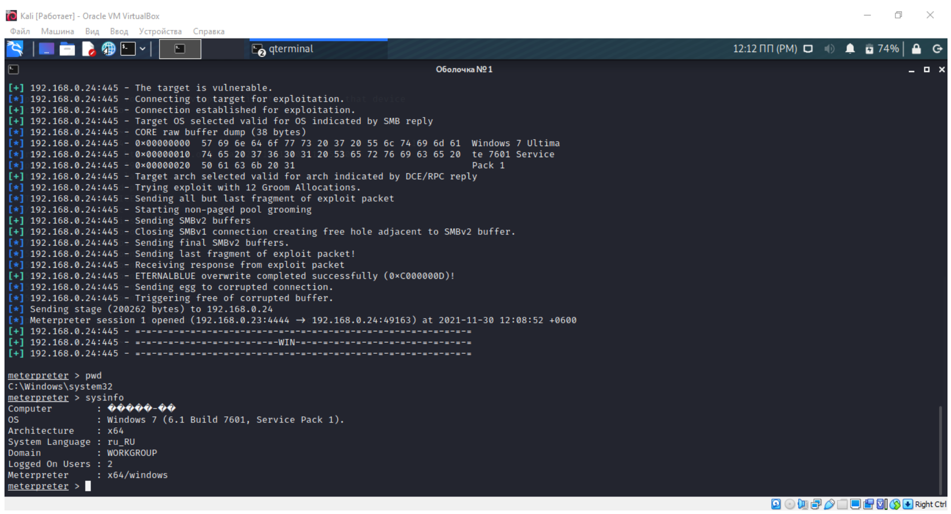


5-сурет - Windows 7 жүйесінде шабуылды орындау



6-сурет - Windows 7 жүйесінде шабуылды жалғастыру

Бізде *meterpreter* іске қосылғанын 7-суреттен байқауға болады.



7-сурет - Windows 7 жүйесінде шабуылды аяқтау

Windows 7 meterpreter сеансын алдық!

Егер meterpreter-ге screenshare пәрменін теретін болсақ, онда ол бізге Windows 7 ОЖ-дегі командалық қатарды көрсетеді (8-сурет).

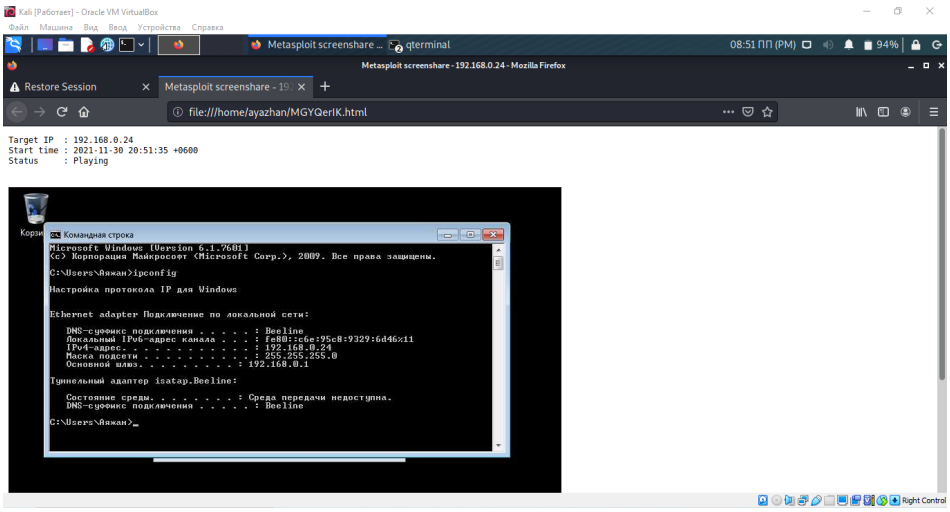
Нәтижесінде, біз meterpreter арқылы Windows операциялық жүйесіне қашықтан қол жеткізе алдық.

Metasploit Framework-киберқауіпсіздік маманы үшін қол жетімді ең қуатты және икемді құралдардың бірі. Оны пайдалану үшін қажет бірнеше негізгі кезеңдердің әр адамға қол жетімді емес белгілі бір білім мен дағдыларды қажет етеді.

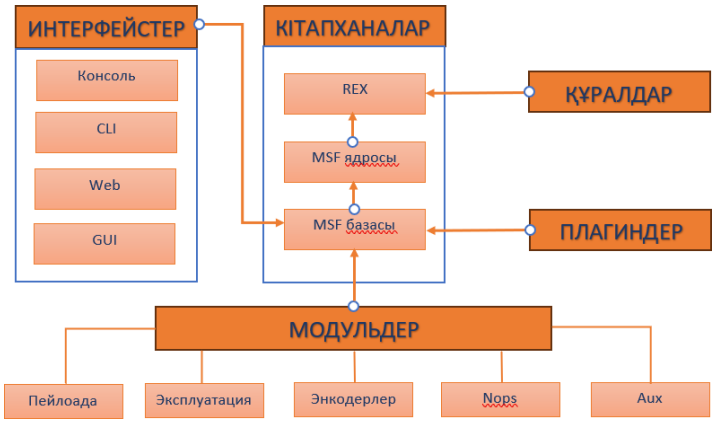
Модульдік болып табылатын Metasploit архитектурасы жаңа эксплуатациялар мен модульдерді біріктіруді, сондай-ақ, өзіңізді жасауды жеңілдетеді. Бұл MSF-ке үнемі өзгеріп отыратын және динамикалық кибершабуылдар ортасына бейімделуге көмектеседі. Сонымен қатар, Metasploit екі түрлі интерфейс - графикалық және консольдік типтерге ие, бұл оны көптеген пайдаланушылар үшін қол жетімді етеді.

Барлық қауіпсіздік талдаушылары немесе енуді

тестілеу мамандары осы платформаға кіруі керек. Бұл әртүрлі құралдар мен утилиталарды қолдана отырып, жасырын осалдықтарды табудың маңызды құралы. Пайдаланушылар Metasploit көмегімен хакерлік әрекеттерді желілер мен серверлерді зерттеу және ену үшін ұқсас әдістерді қолдана отырып бақылай алады. Metasploit архитектурасының схемасы төменде сипатталған (9-сурет).



8-сурет - Screenshare пәрменін теру



9-сурет - Metasploit архитектурасының схемасы

1. Metasploit қолдануға дайындық. Metasploit-ті бастамас бұрын мұқият дайындық қажет:

Мақсаттарды бағалау: тестілеу мақсаттарын анықтау және іс-әрекеттер заңды және этикалық стандарттарға сәйкес келетініне сену.

Ортаны орнату: Metasploit-ті үйлесімді операциялық жүйеге, әдетте Linux немесе Windows-қа орнату [7].

2. Эксплуатацияны таңдау және теңшеу. Metasploit пен жұмыс істеудің негізгі аспектілерінің бірі дұрыс эксплуатацияны таңдау:

Эксплуатациялық базаны зерттеу: Metasploit әртүрлі эксплуатациялары бар кең дерекқорды ұсынады. Эксплуатацияны таңдау мақсатты жүйенің нақты осалдығына байланысты.

Параметрлерді теңшеу: әрбір эксплуатация мақсатты жүйенің IP мекенжайы, порт және басқа параметрлер сияқты белгілі бір параметрлерді конфигурациялауды талап етеді [8].

Біз/windows/smb/ms17_010_eternalblue эксплуатациясын қолдандық. Соңғы жылдары Metasploit Framework-те exploit/windows/smb/ms17_010_eternal blue эксплуатациясы ең көп талқыланған және сұранысқа ие болды. Ол Windows-тың кейбір нұсқаларында анықталуы мүмкін Microsoft SMB протоколының осалдығына бағытталған.

3. Пейлоаданы таңдау және теңшеу. Эксплуатацияны таңдағаннан кейін пейлоада туралы шешім қабылдау керек:

Пейлоадалардың түрлері: Metasploit-те қарапайым командалардан күрделі сценарийлерге дейін көптеген пейлоадалар бар. Пейлоада конфигурациясы: тест мақсаттары мен мақсатты жүйенің сипаттамаларына сәйкес пейлоаданы теңшеу. Біз Meterpreter пейлоадын қолдандық. Ол осалдықты сәтті пайдаланғаннан кейін мақсатты жүйенің жадына жүктелетін қуатты пайдалану құралы болып табылады. Meterpreter түсірілген жүйені терең бақылауды қамтамасыз етеді және әрі қарай зерттеу мен басқарудың көптеген мүмкіндіктерін ұсынады.

4. Шабуылды бастау және нәтижелерді талдау

Эксплуатацияны орындау: эксплуатация мен пейлоаданы орнатқаннан кейін оларды мақсатты жүйені сынау үшін іске қосуға болады.

Нәтижелерді талдау: шабуылдың нәтижесін түсіну қанаудың сәтті болғанын және одан әрі қандай әрекеттер жасау керектігін анықтауға көмектеседі.

5. Жүйе сәтті жұмыс істеген жағдайда, жүйені одан әрі талдау үшін post-exploitation модульдерін пайдалануға болады.

Деректерді жинау: пайдаланушының тіркелгі деректері сияқты маңызды ақпаратты алу.

Терең талдау: жүйені басқа осалдықтарға зерттеу.

Қорытынды. Қорытындылай келе, ақпараттық жүйелердің қауіпсіздік аудиті әдетте автоматтандырылған жүйенің кешенді ақпараттық технологиялары аудитінің кезеңдеріне сәйкес келетін бірнеше дәйекті кезеңдерден тұрады, соның ішінде:

- аудиттің басталуы;
- аудит үшін ақпарат жинау;
- аудит деректерін талдау;
- ұсыныс;
- аудиторлық есепті дайындау.

Практикалық қолдану кезінде Metasploit Framework meterpreter шабуылы арқылы осалдықтарды сканерлеуді орындау үшін қолданылады. Бұл құрылғы бізге басқа амалдық жүйеге шабуыл жасауға және қашықтан қол жеткізуге мүмкіндік береді. Мұндай шабуылдардың алдын алу олардың қайталануын болдырмау үшін өте маңызды. Осылайша:

1. Тұтынушы немесе ұйым тап болатын ең өзекті тәуекелдерге назар аударыңыз. Metasploit модуль жасай алатындығына немесе барлық тиісті қауіптерді жаба алатындығына көз жеткізу үшін қосымша құралдарды қолдану қажет.

2. Imperva брандмауэрінің Веб-қосымшалары кодтың эксплуатациясы мен инъекциясын болдырмайды; мысалы, WAF зиянды трафикті ұстап, Metasploit құрылғыларын тексеру кезінде оны нақты уақыт режимінде бұғаттай алады.

3. Сонымен қатар, Imperva Runtime Application Self-Protection (RASP) нақты уақыт режимінде қолданбаның күту режиміндегі шабуылдарды анықтауға және алдын алуға мүмкіндік береді. RASP аяқталмаған осалдықтарды азайтып, инъекциялар мен сыртқы шабуылдарды тоқтата алады.

4. API қорғау. API-ді автоматты түрде қорғау API-дің соңғы нүктелерін олар жарияланған кезде қорғайды, бұл клиенттік қосымшалардың қолданылуына жол бермейді.

5. Боттардан күшті қорғаныс. Веб-сайттар, мобильді құрылғылар мен API қосымшалары бизнес логикасына қарсы кибершабуылдардан қорғалуы керек. Шотты немесе бәсекеге қабілетті бағаны алу арқылы интернеттегі алаяқтықтың алдын алу үшін Сіз боттар трафигін толығымен көріп, бақылауыңыз керек.

Ғылыми мақала киберқауіпсіздікті талдау және нығайту үшін Metasploit Framework пайдалануды сипаттайтын ақпараттық жүйелерді қорғауда айтарлықтай ілгерілеушілікті көрсетеді. Ол жаңа әдістер мен тактикаларды ұсына отырып, заманауи киберқауіпсіздікте білім беру мен этикалық тәжірибенің маңыздылығын көрсетеді. Осылайша, бұл мақала ақпараттық технологиялардың қауіпсіздігін қамтамасыз ету тәжірибесіне де, ғылыми қоғамдастыққа да айтарлықтай әсер етеді.

Әдебиеттер

1.Сесин Е.М., Белов В.М. Системы идентификации, основанные на интеграции нескольких биометрических характеристик человека / отчеты TUSUR.-2012. -№1(25). - Ч. 2. - стр. 175-179.

2.Скрабцов Н. Аудит безопасности информационных систем.-2017.- стр.1-20. ISBN- 978-5-4461-0662-2

3.Web application security analysis using the Kali Linux operating system, 2016.

https://elibrary.ru/download/elibrary_25736411_98758218.pdf - Дата обращения -22.09.2023.

4.Утилиты для поиска Web-уязвимостей, не имеющих сигнатур, 2020.

https://elibrary.ru/download/elibrary_45557857_26768929.pdf - Дата обращения -16.10.2023.

5.Аверченков В.И., Рытов М.Ю., Кувыклин А.В., Рудановский М.В. Аудит информационной безопасности органов исполнительной власти: учеб. Пособие.-5-е изд., стереотип.-М.: ФЛИНТА.-2021.-100 с.

6.Аверченков В.И. Аудит информационной безопасности: учеб. пособие для вузов, - 2-е изд., стереотип. -М.: ФЛИНТА.-2021.- 269 с.

7.Metasploit как проект компьютерной безопасности, 2022.-

https://cyberleninka.ru/article/n/metasploit-kak-proekt-kompyuternoy-bezopasnosti/viewer - Дата обращения - 16.10.2023.

8.Гибилинда Р.В., Коллеров А.С., Синадский Н.И., Хорьков Д.А.,
Фартушный А.В. Аудит информационной безопасности компьютерных систем. Учебное пособие для вузов.- 2023.- 126 с.

References

1. Sesin E.M., Belov V.M. Identification systems based on the integration of several biometric characteristics of a person / TUSUR reports,

2. 2012.- No. 1(25). -Part 2. -pp. 175-179. (in Russ) Skrabtsov N. Information systems security audit, 2017. - pp. 1-20. ISBN- 978-5-4461-0662-2 [in Russian].

3.Web application security analysis using the Kali Linux operating system,2016.

https://elibrary.ru/download/elibrary_25736411_98758218.pdf- Date ofaddress - 22.09.2023.

[in Eng].

4.Utilities for finding Web vulnerabilities without signatures, 2020.

https://elibrary.ru/download/elibrary_45557857_26768929.pdf- Date of address- 16.10.2023.[in Russian].

5.Averchenkov V.I., Rytov M.Yu., Kuvyklin A.V., Rudanovsky M.V. Audit of information security of executive authorities: textbook, - 5th ed., stereotype.-M.: FLINTA.- 2021.-100 p. [in Russian].

6.Averchenkov V.I. Audit of information security: textbook for universities, - 2nd edition, stereotype. -M.: FLINTA, 2021.- 269 p. [in Russian].

7.Metasploit as a computer security project, 2022.

https://cyberleninka.ru/article/n/metasploit-kak-proekt-kompyuternoy-bezopasnosti/viewer - Date of address - 16.10.2023. [in Russian].

8.Ghibilinda R.V., Kollerov A.S., Sinadsky N.I., Khorkov D.A., Fartushny A.V. Audit of information security of computer systems. Textbook for universities, 2023. -126 p. [in Russian].

Авторлар туралы мәліметтер

Бидахмет Ж. - PhD, әл-Фараби атындағы Қазақ ұлттық университетінің доцент м.а., Алматы, Қазақстан, e-mail: bidakhmetzhanar@gmail.com;

Уайда А.Н. - әл-Фараби атындағы Қазақ ұлттық университетінің магистранты, Алматы, Қазақстан, e-mail: uaida_a@mail.ru;

Майлыбаева А.Д. - физика математика ғылымдарының кандидаты, Халел Досмұхамедов атындағы Атырау университеті, Атырау, Қазақстан, e-mail: mjkka@mail.ru;

Даркенбаев Д.К. - PhD, әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан, e-mail:

dauren.kadyrovich@gmail.com;

Бекназаров С.И. - әл-Фараби атындағы Қазақ ұлттық университетінің магистранты, Алматы, Қазақстан,e-mail: sundetnet105@gmail.com;

Бағдаулет Д.С.- әл-Фараби атындағы Қазақ ұлттық университетінің магистранты, Алматы, Қазақстан, e-mail: dasik-007@mail.ru

Information about the authors

Bidakhmet Zh.- PhD, acting Associate professor Al-Farabi Kazakh National University**,** Almaty, Kazakhstan, e-mail: bidakhmetzhanar@gmail.com;

Uaida A.-graduate student at Al-Farabi Kazakh National University, Almaty, Kazakhstan, e-mail: uaida_a@mail.ru;

Mailybayeva A. - candidate of physical and mathematical sciences,associate professor, Khalel Dosmukhamedov Atyrau University, Atyrau, e-mail: Kazakhstanmjkka@mail.ru

Darkenbayev D.- PhD, Al-Farabi Kazakh National University, Almaty, Kazakhstan, e-mail:

dauren.kadyrovich@gmail.com

Beknazarov S. - graduate student at Al-Farabi Kazakh National University, Almaty, Kazakhstan, e-mail:

sundetnet105@gmail.com

Bagdaulet D.- graduate student at Al-Farabi Kazakh National University, Almaty, Kazakhstan, e-mail: dasik-007@mail.ru