ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
«АЛМАТЫ ЭНЕРГЕТИКА ЖӘНЕ БАЙЛАНЫС УНИВЕРСИТЕТІ»
коммерциялық емес акционерлік қоғамы
«Ақпараттық қауіпсіздік жүйелері» кафедрасы

«ҚОРҒАУҒА ЖІБЕРІЛДІ»
Кафедра меңгерушісі с.ғ.к., доцент Бердібаев Р. Ш.
_____ «_____» _____ 2019 ж.
(қолы)

ДИПЛОМДЫҚ ЖОБА

Тақырыбы: «Honeypot бағдарламалық жасақтама көмегімен рұқсатсыз қолжеткізуді зерттеу»
Мамандығы: 5В100200 – «Ақпараттық қауіпсіздік жүйелері»
Орындаған: Бағидолла Азиз Тобы: СИБк-15-1
Ғылыми жетекші: д.т.н, профессор Ахметов Б. С.

Кеңесшілер:
Экономикалық бөлім бойынша:
э.ғ.к., профессор Ергебаева Т.С.
(ғылыми дәрежесі, атағы, аты-жөні)
(қолы) «11» 06 2019 ж.

Тіршілік қауіпсіздігі бөлімі бойынша:
аға оқытушы Торгаев Э.Э
(ғылыми дәрежесі, атағы, аты-жөні)
(қолы) «29» 05 2019 ж.

Есептеу техникасын қолдану бойынша:
проф. Ахметов Б.С.
(ғылыми дәрежесі, атағы, аты-жөні)
(қолы) «07» 06 2019 ж.

Мелшер бақылаушы:
аға оқытушы Искакова Н.Б
(ғылыми дәрежесі, атағы, аты-жөні)
(қолы) «8» маусым 2019 ж.

Пікір беруші:
(ғылыми дәрежесі, атағы, аты-жөні)
(қолы) «_____» 201 ж.

Алматы 2019

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
«АЛМАТЫ ЭНЕРГЕТИКА ЖӘНЕ БАЙЛАНЫС УНИВЕРСИТЕТІ»
коммерциялық емес акционерлік қоғамы

Басқару және ақпараттық технологиялар институты
Ақпараттық қауіпсіздік жүйелері кафедрасы
5В100200 – «Ақпараттық қауіпсіздік жүйелері» мамандығы

Дипломдық жобаны орындауға берілген

ТАПСЫРМА

Студент: Бағдолла Азиз
(аты-жөні)

Жобаның тақырыбы: Honeypot бағдарламалық жасақтама көмегімен рұқсатсыз қатынауды зерттеу

2018 ж. «26» 10 № 124 университет бұйрығымен бекітілді.

Аяқталған жұмысты тапсыру мерзімі: «12» 06 2019 ж.

Жобаға алғашқы деректер (талап етілетін зерттеу (жоба) нәтижелерінің параметрлері және зерттеу нысанының алғашқы деректері): Рұқсатсыз қатынауды зерттеу үшін бұл Honeypot бағдарламалық жасақтамасы Интернеттегі кейбір зиянды әрекеттер туралы құнды ақпаратты жинауға арналған. Бұл бағдарламалық жасақтаманы пайдалану ұйымдарға және зерттеушілерге бұзғыш пайдаланушыларды және әртүрлі желілерді уақытылы және тиімді түрде анықтауға мүмкіндік береді.

Диплом жобасындағы әзірленуі тиіс мәселелер тізімі немесе диплом жобасының қысқаша мазмұны: Honeypot көмегімен тіркелген шабуылдарды зерттеу; Шабуыл сканерлерінің қызметін бағалау; Модульдердің қызметі. MHN Honeypot – мыңдаған орталықта бейін деу таралған аудандарда сұрауға және ішкі honeypot конфигурацияларын қолдайтын еркін ашық бастапқы бағдарламалық жасақтама.

Графикалық материалдардың (міндетті түрде дайындалатын сызбаларды көрсету) тізімі:

1. Dashboard модульдер статистикасы;
2. Админ-ға орнату сызбасы;
3. Модульдер тартпасы.

Негізгі ұсынылатын әдебиеттер:

1. Гради Буч, Роберт А. Максимчук, Майкл У. Энгл, Бобби Дж. Янг, А. Хьюстон. Объектно-ориентированный анализ и проектирование с примерами приложений. – М.: Вильямс, 2010.
2. Бошнева А.И. Методические указания к выполнению экономической части дипломных работ для бакалавров специальности 5В0703 – Информационные системы. – Алматы: АУЭС, 2013. – 24 с.
3. Вербецкий А.А. Основы компьютерных технологий и современные ПК. – М.: Алекс, 2002. – 264 с.

Жоба бойынша жобаның бөлімдеріне қатысты белгіленген кеңесшілер

Бөлімдері	Кеңесшілері	Мерзімі	Қолы
Негізгі бөлім			
Өміртіршілік қауіпсіздігі бөлімі	Торгаев Э.Э.	11.03-29.05	[signature]
Экономика бөлімі	Арепбаева Ж.Г.	04.03-11.06.19	[signature]

Диплом жобасын дайындау
КЕСТЕСІ

Бөлімдердің атауы, әзірленетін мәселелердің тізімі	Ғылыми жетекшіге ұсыну мерзімдері	Ескерту
Кіріспе	25.01.2019	
Honeypot бағдарл-ң мақсаттық сипаты ақпараттық қауіпсіздігін талдау	05.02.2019	
Modern Network Honeypot бағдарламасының мақсаттылығы анықтау	22.02.2019	
Honey RJ-ды іске қосу және инициализациялау	07.03.2019	
Шабуылдар қорғаушы қызметін талдау	20.03.2019	
Жүйелестердің саны анықтау	28.03.2019	
Атын қорғаны MHN Honeypot-қа біріктіру	02.04.2019	
Ұсыну, тірлеу модульдерінің Honeypot-тағы қызметін талдау	10.04.2019	
Shellcode анализаторының пайдаланылуы	21.04.2019	
Деректердің қауіпсіздігі бойынша талдау	30.04.2019	
Техникалық-экономикалық негіздеме	05.05.2019	
Қорытынды	18.05.2019	

Тапсырманың берілген уақыты «28» қазан 2018 ж.

Кафедра меңгерушісі ____________ (________________________)
(қолы) (аты-жөні)

Жобаның
ғылыми жетекшісі ____________ (Ахметов Б.С.)
(қолы) (аты-жөні)

Орындалатын тапсырманы
қабылдаған студент ____________ (Бағдаулет А.М.)
(қолы) (аты-жөні)

АҢДАТПА

Бұл құжат екі бөліктен тұрады: honeypot технологиясын шолу және Java-де іске асырылған төмен деңгейлі қақпандарды сипаттайтын мысалдар. Зерттеуде мақалалардың тұжырымдамалары мен егжей-тегжейлі жұмысқа сілтемелер туралы қысқаша шолу берілген. Іс жүзінде іске асыру мысалында, төменгі өзара әрекеттесетін қақпанды жобалау мен енгізу кезінде көптеген шешімдер қажет деп есептеледі.

АННОТАЦИЯ

Этот документ состоит из двух частей: обзор технологии honeypot и тематическое исследование, описывающее honeypot с низким уровнем взаимодействия, реализованный в Java. В обзоре представлен краткий обзор концепций honeypot и ссылки на более подробные работы. В практическом примере реализации рассматриваются многие решения, необходимые при разработке и реализации honeypot с низким уровнем взаимодействия.

ANNOTATION

This document is divided into two parts: technology for catching technology and thematic research, high-level interaction such as honeypot, Java implementation. For an illustrative example, look carefully at the honeypot and references. In the practical example of many realizations, many solutions address the problem of neutralization and honeypot realizations with low-level interactions.

Мазмұны

58

Кіріспе

Бұл бөлімде біз желілік басып кірудің анықтау жүйелерін, желілік қауіпсіздіктің дәстүрлі амалын сипаттадық. Содан кейін біз honeypot-тың қысқаша тарихын ұсынамыз. Бөлім алдамшының жалпы артықшылықтары мен кемшіліктерін талқылаумен аяқталады. Зиянды бағдарламалардың таралуы бүгінгі күні Интернеттегі негізгі қауіптің бірі болып табылады. Құрттар мен боттар әлем бойынша әлсіз машиналарды үнемі сканерлеп отырады. Бұдан кейін бұзылған құрылғы ірі ботнеттерді қалыптастыру үшін пайдаланылады, мысалы, қызметтік шабуылдардың бөлінуінен бас тарту үшін немесе электрондық пошта спамының массасын жібереді. Алдамшылардың көмегімен біз мұндай зиянды бағдарламаны жылдам әрі жеңіл жолмен басып аламыз. Әсіресе, шабуылдаушымен өзара әрекеттесу болмаған жағдайда, өзара әрекеттесу деңгейі төмен, құзыретті ТЛЕ қауіпсіздіктің осы саласына өте пайдалы. Honeypot сияқты серверлерге негізделген төлемдер зиянкестерді шатастырып, нақты зиянды екілік файлды ұстап алу үшін пайдалану кодын талдауға арналған көптеген қызметтерді ұсынады. Төмен деңгейдегі алдамшылар бастапқы зондтар туралы ақпаратты жинаудың төменгі тәуекелдік әдісін қамтамасыз етеді, себебі шабуылдаушымен толық өзара әрекеттесу жоқ. Осылайша, бұл алдамшыларды сақтау оңай және ақпарат автоматты жиналады. Бұл қасиет анықтау жүйелеріне (IDS) басып кіруді төмен деңгейлі алдамшылармен әрекеттесеуін қамтамасыз етеді. Кейбір HoneyPot шешімдері бұрын істелді. Бұл бөлімде біз Amun сияқты бірдей көзқарасты ұстанатын үш түрлі нұсқаны енгіземіз. Төменгі әрекетті алдамшының бірі – Honeyd. Бұл фонды режимде жұмыс істейтін бағдарлама Linuxтің кішігірім нұсқасы, желіде виртуалды хостты құрастырады және еркін осал қызметтерді ұсынады. Бұл виртуалды «dual» хосттар Microsoft Windows сияқты белгілі бір операциялық жүйемен әрекет ету үшін конфигурациялануы мүмкін. Honeypot-та жеңіл кеңейту үшін плагин жүйесі бар және жеңіл кеңейтуге арналған жүйелер сияқты кейбір пайдалы құралдармен басып алынған деректерді табуды автоматты түрде түсіретін пайдалы құралдармен жабдықталған.

1 Интернет-ресурстары осалдылыққа тексеретін сканерлер

1.1 Жұмыс өзектілігі

Қауіпсіздік мамандары шешуге тиіс ең маңызды міндеттердің бірі – шабуылдарды анықтауға, олардың қалай әрекет ететінін түсінуге және неге себепкер болатын ақпаратты жинау. Бұған дейін киберқауіптерді анықтауға тырысты, тек қана ену үшін қолданылған бағдарламаларды талдау, оқиға орын алғаннан кейін сарапшылардың тек қана хакерлік жүйеде қалған ақпараттар екендігі. Өкінішке орай, бұл өте аз және тұтастай алғанда қауіп туралы аз айтуға болады. Шабуылдарды табу, соның ішінде Honeypot желілерінің негізінде, шабуыл мен шабуылшы туралы ақпаратты айтарлықтай кеңейтеді. Әрбір елде Honeypot дамуының ерекшелігі бар. Honeypot серверлерін бөлу және олардың әртүрлі мәртебесін мемлекет пен қорғау объектісі айқындайды. Қауіпсіздік мамандарының аз саны Honeypot қашықтан басқаруымен өтеледі. Индонезияның географиялық тұрғыдан ерекшелігі бар. Индонезия – 2700-ден астам аралдар бар архипелагтағы шағын дамушы ел. Технология, әсіресе, үкімет үшін ақпараттың қауіпсіздігі дамудың ынталандырушы факторы болып табылады. Бұл тезис Honeynet желісін жобалау мен дамытуды автоматтандыру мәселелеріне қатысты.

Honeypot – ресурстың рұқсатсыз немесе заңсыз пайдаланылуын анықтау мақсаты болып табылатын жүйенің ақпараттық ресурсы. Honeynet – желілерді модельдеу және тіркелген, маргиналды және рұқсатсыз кіруді бақылау мүмкіндігі бар Honeypot байланысының жоғары деңгейлі желісі. Honeynet жобасы 9 қауіпті жағдайды бақылауды жақсартуға арналған. Зерттеушілер командасы бүкіл компьютерлік желі құрды және оны датчиктермен толтырды. Содан кейін бұл желі интернетте орналастырылып, тиісті атау беріп, тиісті мазмұнмен толтырылып, содан кейін осы желіде болған барлық оқиғаларды жаза бастады.

Нақты IP-мекен-жайы жарияланбайды және үнемі өзгереді. Хакерлердің іс-әрекеттері, әдетте, орындалған кезде жазылады, яғни. Интриграция әрекеттері сәтті болғанда және табысты бұзудан кейін жасалған әрекеттерде жазылады. «Honeynet\f» жобасы басқа тәсілдерді ұсынады: жүйеге хакерлерді «лас» деп аударады және олардың әрекетін ең басынан талдайды. Бұл әдіс танымал интрузияны анықтау және алдын-алу технологиясын тиімді толықтырады.

Осы саладағы жетістіктерге қарамастан, Honeynet деректерін жобалау, конфигурациялау және өңдеу процесі әлі де күрделі және жеткіліксіз автоматтандырылған тапсырма болып табылады. Қауіпсіздік мамандары шешуге тиіс ең маңызды міндеттердің бірі – шабуылдарды анықтауға, олардың қалай әрекет ететінін түсінуге және неге себепкер болатын ақпаратты жинау. Бұған дейін киберқауіптерді анықтауға тырысты, тек қана ену үшін қолданылған бағдарламаларды талдау, оқиға орын алғаннан кейін сарапшылардың тек қана хакерлік жүйеде қалған ақпараттар екендігі.

Өкінішке орай, бұл өте аз және тұтастай алғанда қауіп туралы аз айтуға болады. Шабуылдарды табу, соның ішінде Honeypot желілерінің негізінде, шабуыл мен шабуылшы туралы ақпаратты айтарлықтай кеңейтеді. Әрбір елде Honeypot дамуының ерекшелігі бар. Honeypot серверлерін бөлу және олардың әртүрлі мәртебесін мемлекет пен қорғау объектісі айқындайды. Қауіпсіздік мамандарының аз саны Honeypot қашықтан басқаруымен өтеледі. Индонезияның географиялық тұрғыдан ерекшелігі бар. Индонезия 2700-ден астам аралдар бар архипелагтағы шағын дамушы ел. Технология, әсіресе, үкімет үшін ақпараттың қауіпсіздігі дамудың ынталандырушы факторы болып табылады. Бұл тезис Honeynet желісін жобалау мен дамытуды автоматтандыру мәселелеріне қатысты. Honeypot – ресурстың рұқсатсыз немесе заңсыз пайдаланылуын анықтау мақсаты болып табылатын жүйенің ақпараттық ресурсы. Honeynet – желілерді модельдеу және тіркелген, маргиналды және рұқсатсыз кіруді бақылау мүмкіндігі бар Honeypot байланысының жоғары деңгейлі желісі. Honeynet жобасы 9 қауіпті жағдайды бақылауды жақсартуға арналған. Зерттеушілер командасы бүкіл компьютерлік желі құрды және оны датчиктермен толтырды. Содан кейін бұл желі интернетте орналастырылып, тиісті атау беріп, тиісті мазмұнмен толтырылып, содан кейін осы желіде болған барлық оқиғаларды жаза бастады. Нақты IP-мекен-жайы жарияланбайды және үнемі өзгереді. Хакерлердің іс-әрекеттері, әдетте, орындалған кезде жазылады, яғни. Интриграция әрекеттері сәтті болғанда және табысты бұзудан кейін жасалған әрекеттерде жазылады. «Honeyne\f» жобасы басқа тәсілдерді ұсынады: жүйеге хакерлерді «лас» деп аударады және олардың әрекетін ең басынан талдайды. Бұл әдіс танымал интрузияны анықтау және алдын-алу технологиясын тиімді толықтырады.

Осы саладағы жетістіктерге қарамастан, Honeynet деректерін жобалау, конфигурациялау және өңдеу процесі әлі де күрделі және жеткіліксіз автоматтандырылған тапсырма болып табылады.

1.2 Интернет ресурстарының ақпараттық қауіпсіздігіне қатер көздері

Интернет-ресурстардың ақпараттық қауіпсіздігіне қатердің негізгі көзі сыртқы бұзушылар болып табылады. Сыртқы құқық бұзушы - әдетте коммерциялық қызығушылық танытқан адам тергеудің ақпараттық жүйесі туралы білімі жоқ интернет желісіне қол жеткізе алады, желілік қауіпсіздік мәселелері бойынша жоғары біліктілікке ие және ақпараттық жүйелердің әртүрлі түрлеріне желілік шабуылды жүзеге асыруда жеткілікті тәжірибесі бар.

Интернет ресурстарына шабуыл түрлері:

Мақсатты шабуылдар – бұл бір ғана белгіпен біріктірілген бір интернет ресурсына немесе олардың тобына бағытталған шабуылдар. Мұндай шабуылдарды кінәлаушылар, әдетте, интернет-ресурстардың қауіпсіздігі саласында жоғары білікті мамандар болып табылады. Мұндай шабуылдардың

мақсаты – жасырын ақпарат алу, ол ақысыз бәсекелестер немесе қылмыскерлердің пайда табу үшін пайдалануы мүмкін.

Мақсатты емес шабуылдар шабуылдар, кездейсоқ интернет-ресурс танымалдыққа, бизнестің өлшеміне, географиясына немесе саласына қарамастан, құрбан болып қалады. Интернеттегі ресурсқа рұқсатсыз шабуыл жасау – шабуылдаушы белгілі бір ресурсты бұзуға бағытталған емес, бірақ кейбір критерий бойынша таңдалған жүздеген немесе мыңдаған адамға шабуыл жасайтын интернет-ресурсына рұқсатсыз кіруге әрекет жасау.

Интернет-ресурстардың осалдығы – бұл қателердің салдарынан оларды бұзу мүмкіндігі, басқару жүйесінің (CMS) дұрыс емес параметрлері және веб-сервердің операциялық жүйесі. Жыл сайын компания өз веб-жобаларында осалдықтарды табу және түзету үшін үлкен ақша жұмсайды. Интернет-қордың коды әрдайым осалдықтарға ие. Қазіргі уақытта интернет-ресурстың көптеген осалдықтары жіктеледі және бұл анықталған 0 күндік осалдықтарды санамайды. Зияндылық – жүйеде зиянды болуы мүмкін кез-келген белгілі әлсіздік бағдарламалар немесе хакерлер [1].

Интернет ресурстарының осалдықтарының негізгі түрлері:

1) SQL инжекциясы – инъекциялық шабуылдың түрі болып табылады. Инъекциялық шабуылдар шабуыл жасаған зиянды енгізілген деректерді ұсынып, өтінішті күтпеген әрекетті орындауға әкеледі. SQL дерекқорларының әрқайсысының себебінен SQL инъекциясы интернеттегі шабуылдардың ең көп таралған түрлерінің бірі болып табылады.

2) Кросс-сайтты сценарийлер. Егер сіздің сайтыңызға пайдаланушыларға мазмұн қосуға рұқсат берсеңіз, шабуылдаушылар зиянды JavaScript-ды енгізе алмайтындығына сенімді болуыңыз керек. Бұл әрекетті орындаудың бір жолы «кросс-сайтты сценарийлер» деп аталады.

3) Командалық орындау. Көптеген веб-бағдарламалар пәрмен жолы арқылы операциялық жүйе процестерін шақырады. Егер сіздің қолданбаңыз ОЖ-ға қоңырау шалса, командалық жолдар сенімді түрде салынғанына сенімді болуыңыз керек.

4) Батырма басылуы шабуылдары веб-пайдаланушыларды ойламаған әрекетті орындауға мәжбүрлейді, әдетте пайдаланушы көрінген әрекеттің үстіне көрінбейтін бет элементін көрсету арқылы.

5) Тораптағы сұранысты жасыру – осалдығы сіздің сайтыңыздағы қажетсіз әрекетті орындау үшін пайдаланушының браузерлерін ұрлау үшін пайдаланылуы мүмкін.

6) Анықтамалық тізбектегі – осалдықтар шабуылдаушыларға сіздің жүйеңіздегі еркін файлдарға қол жеткізуге мүмкіндік береді. Олар әдетте ескірген технологиялық стектерде пайда болады, олар URL мекенжайларын дискідегі каталогтарға тым толықтай аударады.

7) Кросс сценарий сценарийлері – хакерлердің веб-сайттарға шабуыл жасайтын ең көп таралған әдісі. Осалдықтары зиянкес пайдаланушыға басқа пайдаланушылар сіздің торабыңызға кірген кезде JavaScript-тың ерікті бөліктерін орындауға мүмкіндік береді.

8) Файлдарды кері жүктеу зиянкесі – зиянды кодты қолданбаңызға жеңілдетеді. Жүктеп салынған файлдар толығымен қамтамасыз етілгенге дейін сақталуы керек, немесе сіз өзіңіздің жүйелеріңізге қауіп төндіретін оңай жолды жасау қаупін тудырасыз.

9) Қолжетімді кіруді бақылауды қамтамасыз ету – дұрыс қолдана отырып қол жеткізуді бақылау ережелері деректеріңіздің қауіпсіздігін қамтамасыз етудің кілті болып табылады. Деректердің барлығына дерлік құпия деректер мен операцияларды қорғау қажет, сондықтан жүйені жобалау кезінде қатынауды шектеудің маңыздылығын ескеру керек.

10) Зиянды бағыттауды болдырмау – егер торабыңыз ашық қайта бағыттауға рұқсат берсе, сіз білмейсіз, шабуылдаушыларға өзіңіздің пайдаланушы базаңызды пайдалануға көмектеседі.

11) Шифрланбаған байланыс – шифрлау шабуылдаушы сіз және сіздің пайдаланушыларыңыз арасында жіберілетін трафикті ұстап қалуына жол бермейді. Бұл арзан әрі оңай іске асады, ал құпия деректерді беру кезінде абсолютті қажеттілік.

12) Пайдаланушыны тіркеуден аулақ болу – егер шабуылдаушы сіздің сайтыңызды пайдаланушы аты бар-жоғын тексеру үшін тексеруі мүмкін болса, ол сіздің пайдаланушыларыңыздың есептік жазбаларын бұзуға тырысады.

13) Ақпараттың ағуы – жүйелік ақпараттардың ашылуы сіздің қарсыласыңызды сайт туралы білуге және шабуыл жоспарын қалыптастыруға көмектеседі. Пайдаланушыларыңыз білуі үшін қажет болғандықтан, технологиялық стек пен архитектураны мүмкіндігінше аз көріңіз.

14) Құпиясөзді дұрыс басқармау – қауіпсіз түпнұсқалық растама сіздің пайдаланушыларыңызды қауіпсіз сақтау үшін маңызды. Бұл құпия сөздермен қауіпсіз түрде жұмыс істеуді білдіреді.

15) Артықшылықтардың өсуін болдырмау – артықшылығын арттыру осалдығы зиянкестерге басқа пайдаланушыларды имплементациялауға немесе оларға ие болмайтын рұқсаттарды алуға мүмкіндік береді. Бұл осалдықтар сенімсіз кірістердің артқы жағында қол жетімділік шешімдерін қабылдаған кезде пайда болады.

16) Сеансты түзету – осалдығы сіздің пайдаланушыларыңыздың өз сеанстарын ұрлауы үшін жауапты ете алады. Сіздің сайтыңыздағы сеанстардың қауіпсіз орындалуы - сіздің пайдаланушыларыңызды қорғаудың кілті.

17) Әлсіз сеанс идентификаторлары – зиянсыз сеанс идентификаторлары пайдаланушыларыңызды сеанстың ұрлануына әкелуі мүмкін. Егер сеанс идентификаторлары шағын мәндер ауқымынан таңдалса, шабуылдаушы сәйкестікті тапқанға дейін кездейсоқ таңдалған сеанс идентификаторларын тексеруі керек.

18) XML бомбасы – жүктеуді қабылдайтын болса, шабуылдаушы серверге қарсы бас тарту шабуылын жасаудың оңай жолы.

19) XML сыртқы нысандар – кепілсіз талдаушылары шабуылдаушыға құпия ақпарат үшін файл жүйесін тексеруге рұқсат бере алады. Егер сіздің сайт кез келген түрде қабылдайтын болса, парсерін дұрыс конфигурациялау керек.

Қызмет көрсетуден бас тартудан қорғану қызметтік шабуылдарды бас тартуға шабуыл жасайды(DOS) – интернеттің қалай құрастырылғандығының ең жақсы және ең нашар аспектісі – кез-келген веб-сайттың интернетке қосылған кез келген адамға қол жетімділігі. Бұл сіздің веб-сайтыңызға ықтимал үлкен аудиторияны білдіреді, бірақ сонымен қатар зиянды трафикпен күресу керек дегенді білдіреді. Егер шабуылдаушы сізге ресурстардың серверін ашу үшін жеткілікті трафик жасай алса, олар заңды пайдаланушыларды қызметтен бас тарта алады. Егер хакер жүйеге кіре алмаса, қызмет көрсету шабуылының сәтсіздікке ұшырауын әрдайым таңдау мүмкіндігі бар. Саяси мақсаттар немесе интернетте жұмыс істейтін компания, әдетте, шабуылдың бұл түріне ұшырайды және осал болады. Ақаулықты жоюдың көптеген жолдары бар – service шабуылынан бастап, негізгі маршрутизаторды трафикті бомбалаудан белгілі белгілі бір пайда табу үшін бағдарламадағы қателік және қызметті қол жетімді етпеуі және сондықтан сервердің істен шығуы. Бұл мәселені қорғау қиын, бірақ егер соңғы бағдарлама жаңартуларын тәуекел төмендетілген [2].

Электрондық поштадағы спуфинг – жалған «мекен» мекенжайы бар электрондық пошта хабарларын жіберу. Шабуылданған электрондық пошта мекенжайын пайдалану – олардың құрбандарының сеніміне ие болу үшін әдеттегі тактикалық электрондық пошта алаяқтары. Веб-сайтыңыз мен ұйым жіберетін электрондық хаттардың түпнұсқалы деп белгіленгеніне көз жеткізіңіз.

Малверинг – (зиянды бағдарламаларды немесе жарнамалық желілер арқылы алдамшы жарнамаларды жеткізу). Интернеттегі ең жылдам өсіп келе жатқан қауіпсіздік қатерлерінің бірі болып табылады. Сайт авторы ретінде сіз кез келген хабарландырулар сіздің пайдаланушыларыңызға зиян тигізбейтініне сенімді болуыңыз керек.

Лакс қауіпсіздік параметрлері – қауіпсіздіктің дұрыс емес конфигурациясы технологиялық стек үшін ең жиі кездесетін қауіптердің бірі болып табылады. Серверлеріңізден шықпаған болсаңыз, қорғалмаған хакерлер қарапайым Google іздестіруі арқылы осал кіру нүктелерін таба алады.

Уытты тәуелділік – даму топтары бөгде тәуелділіктер бойынша кодтамалық шолуларды сирек орындап отырады, бірақ біз қолданатын кітапханалар мен құралдар жиі бағдарламалық жасақтаманың осалдығы болып табылады. Ресурс иесі ретінде, сіз басқа адамдардың жазған кодын қамтамасыз етуіңіз қажет, бұл сіздің жүйеңізді қатерсіз етпейді.

1.3 Интернеттегі ресурсқа негізделген ақпарат көздері.

Осалдықтарды анықтайтын және түзетін бірнеше бағдарламалық құрал бар. Мұндай міндеттер осалдылық сканерлері тексеріледі, зиянкестер

тарапынан пайдаланылуы мүмкін осалдықтар жүйесінде түрлі қосымшаларды тексеруге мүмкіндік береді. Порт сканері сияқты төмен деңгейлі құралдар, жүйеде жұмыс істейтін ықтимал бағдарламаларды және хаттамаларды анықтау және талдау үшін пайдаланылуы мүмкін. Төменде оннан астам үздік осалдық сканерлерінің көрсетілімі ұсынылған:

1) nessus: UNIX үшін осалдығын бағалау;

2) GFI LANguard: Windows үшін коммерциялық желі осалдығын қарап шығу құралы;

3) retina: осалдықты бағалау үшін коммерциялық сканер;

4) негізгі әсер: жүйеге рұқсатсыз кіруді сынау үшін автоматтандырылған өнім;

5) ISS Internet Scanner: Қолдану деңгейінде осалдықтарды бағалау;

6) X-scan: Желілік осалдықтарды зерттеуге арналған сканер;

7) сара: Қауіпсіздік аудиторының ғылыми қызметкері;

8) qualysGuard: осалдығы сканері (веб-қызметі);

9) SAINT: Қауіпсіздік әкімшісінің біріктірілген желілік құралы;

10) MBSA: Microsoft Baseline Security Analyzer.

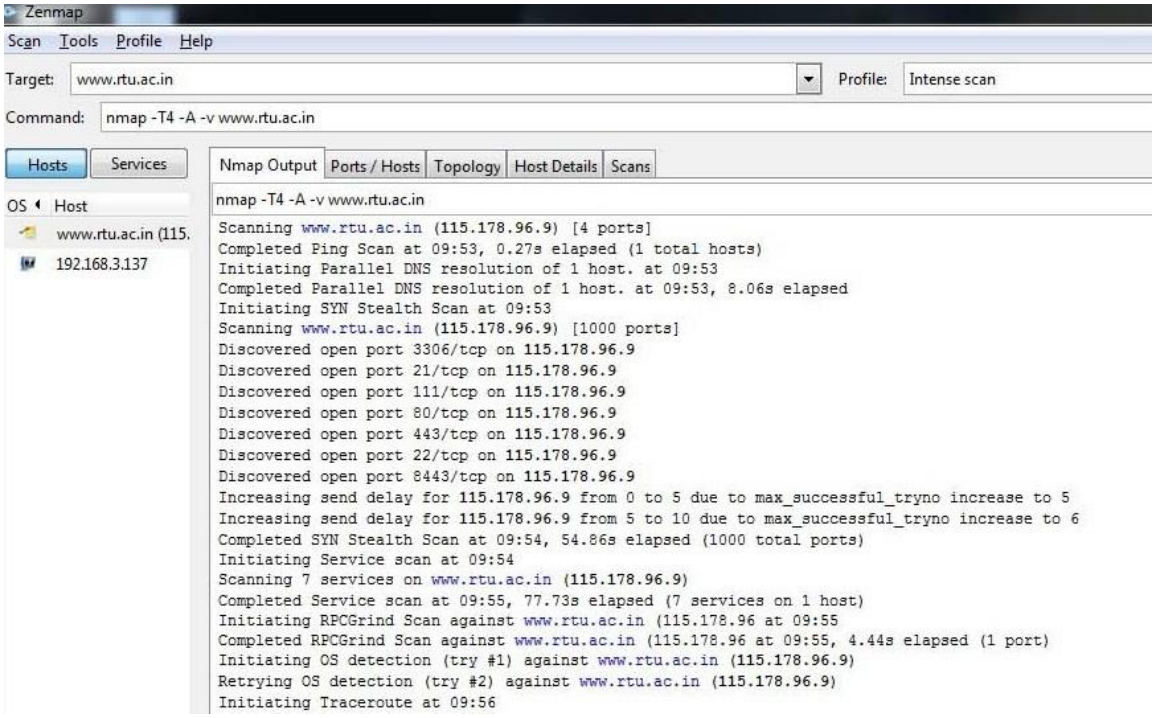
Басқа осалдық сканерлер:

- XSpider;
- OpenVAS;
- ERPScan сканер безопасности SAP;
- SurfPatrol.

Айта кету керек, барлық осалдықтарды толығымен жоятын әмбебап бағдарламалық жасақтама, интернет-ресурсты бұзу туралы ескертуімен жоқ. Зияндылықты бағалау жүйеде осалдықтарды анықтауды білдіреді, олар кез-келген желіге зиян келтіретін жаман ниетті адаммен қолданыла алады. Бұл осалдылық анықталған біреу білмес бұрын және қарастырылатын белсенді көзқарас бұл туралы тиісті түрде айтылуы тиіс. Брандмауэрді қорғауға көбірек көңіл бөлінді, бірақ ішкі функциялары маңызды. Зияндылықты бағалау тек белгілі бір бағдарламада орындалмайды, бірақ тіпті қолданба іске қосылған платформаға, ортақ бағдарламаға, операциялық жүйеге және т.б. қолданылады. Осылайша, осалдық сканерлері желілік жүйені және бағдарламалық жасақтаманы сканерлеу үшін пайдаланылады.

Nmap – порттарды сканерлеу үшін пайдаланылатын порт сканері. Егер IP-адресі берілсе, онда ол оған тиесілі хостты табады. Сондай-ақ, ол белгілі бір хостта жұмыс істейтін порттардың саны, ашылған порттар саны, жабық порттардың саны, осы порттар ұсынатын қызметтер, мысалы, қызметтер TCP-бағдарлы ма немесе FTP-бағдарлы ма екендігін табады. Ол тіпті осы хостта қолданылатын операциялық жүйенің түрін болжайды. Хосттың сканерленетін топологиясы жергілікті құрылғы осы нақты қашықтағы торапқа кіретін түрлі шлюздерді көрсететін графикалық форматта жазылады. Ашылған порттарды ескере отырып, шабуыл хостқа рұқсатсыз және заңды түрде кіруге арналған болуы мүмкіндікті таныту. Сонымен қатар, егер ашық порттар TCP-бағдарланған немесе қызмет көрсететін болса FTP-бағытталған, хостқа кіру

оңай болады. Nmap көмегімен түрлі сайттар сканерленді. Төмендегі суретте RTU сайтын сканерлегеннен кейін алынған нәтижелер көрсетіледі. 1.1-суретте РТА сайтының негізгі бөлшектері, соның ішінде IP мекенжайы, қол жетімді порттардың саны, ашық порттардың саны көрсетіледі порттар, ашық, RPCGrind сканерлеу және көптеген басқа да егжей-тегжейлі мәліметтер.



Сурет 1.1 – RTU веб-сайтының Nmap басты шығарылымы

Nessus қашықтағы хостта орналасқан түрлі осалдықтарды тізімдейтін осалдық сканер. Бұл ішкі және сыртқы сканерлеуді қамтамасыз етеді. Ішкі сканерлеу белгілі бір маршрутизатордағы түйіндермен байланысты. Сыртқы сканерлеу белгілі бір маршрутизатордың (қашықтағы хост) тыс түйіндерді қамтиды. Веб-қосымша сынағы сканерде орындалады. Сканерлеуді бірінші кезекте жасауға болады, көрсетілетін немесе үлгіні белгілі бір хост үшін жасау мүмкін, содан кейін ол осы хостқа сканерлеуді іске қосуға болады. Хосттарды бірнеше сканерлеу дереу жасалуы мүмкін. Nessus тапқан осалдылық төрт түрлі дәрежеде қарастырады – жоғары, орташа, төмен және ұйымдастырылмаған. Нәтижелер белгілі бір хосттың сканерлеуі аяқталғаннан кейін сақталады. Нәтижелер екі түрлі жолмен ұсынылған – хосттың плагиндері мен осалдықтарын пайдаланатын осалдықтар. Алғашқы санат бірінші сыныпта табылған барлық осалдықтарды сканерлеп жіктейді, содан кейін осы осалдықтардан зардап шеккен хосттарды көрсетеді. Жасалған есептерді пайдалану арқылы проблемаларды анықтау және оңай анықтау мүмкін. Соңғы санат сканерлеу кезінде және табылған осалдықтарда табылған барлық түйіндерді анықтайды. Бұл есепте сенімді хосттармен, PCI сканерлеуімен, кейінгі аудиттермен және мақсатты жарналармен байланысты түрлі мәселелер қарастырылады. Нақты уақыттағы PVS сканерлеу Nessus

белсенді сканерлеуді аяқтайды, үздіксіз желіні бағалауды қамтамасыз етеді және ұшыру арасындағы қауіпсіздік кемшіліктерін артырады. Нәтижелер кез келген пішімде экспортталуы мүмкін (мысалы, PDF, HTML, CSS және т.б.).

Acunetix WVS веб-қауіпсіздік тексерулерін орындау үшін талдау құралын қолдану болып табылады. Acunetix WVS жұмыс істейтін критерийлерге мақсатты ерекшелігі, сканерлеу және құрылымды бейнелеу және сызбаға талдау жасау кіреді:

1) Идентификацияның мақсаты. WVS белсенді веб-сервері бар мақсатты тексереді, сондықтан хост кез келген веб-бағдарлама. Қолданылатын веб-технологиялар, веб-сервердің түрі және тиісті сүзу сынақтарын жүргізу үшін жауаптылық туралы ақпаратты жинау.

2) Сеансты және дисплей құрылымын сканерлеу. Веб-қосымшаға арналған индекс файлы жүктеледі. Біріншіден, URL анықталды (мысалы, http://192.168.1.128:80/ негізгі index.html жүктейді). Алынған жауаптар сілтемелерді, пішіндерді, параметрлерді, енгізу өрістерін және құрылатын клиенттік сценарийлерді алу үшін өңделеді веб-бағдарламадағы каталогтар мен файлдардың тізімі.

3) Талдау үлгісі веб-қосымшада орындалады.

Nikto – нақты ресурсты сканерлеу үшін пайдаланылатын командалық құрал. Бұл функцияны осы тілге негізделгендіктен жүйеде орнатылған Perl тілінің болуын талап етеді. Ол қауіпті CGI файлдарына/серверлердегі ақауларға қарсы қауіпсіздік тексерулерін орындайды. Шабуылшылар қауіпті WordPress іске асырудан бастап, Apache серверлеріне дейінгі барлық мүмкіндіктерге қол жеткізу үшін веб-сервердің осалдығын іздейді.

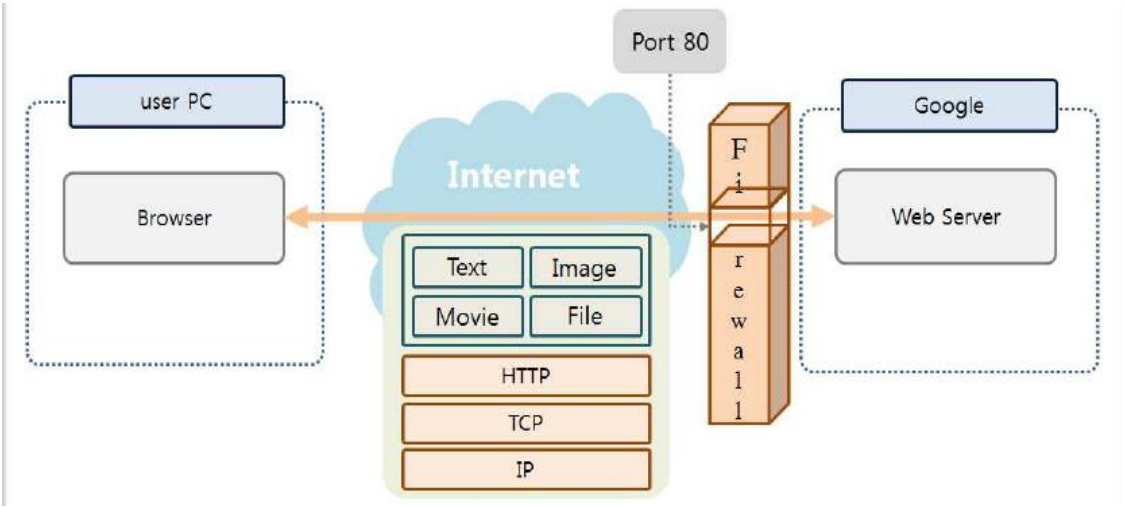
Nikto – бұл АТ қауіпсіздік мамандары мүмкін, сондықтан тегін және ашық бастапқы коды бар веб-сервер қауіпсіздігі сканері сервердің кәсіпорындарға қауіпсіздігін жақсы түсініп, қорғау бағытында оңтайлы қадамдар жасап, Есептеу техникасы мен жүйелерді жаңғыртуға арналған халықаралық журналды қолданады. Құрал кәсіпорын жасамаған және осалдықтарды анықтайтын Scamp серверлерін таба алады. Сондай-ақ, ол 65 000-нан астам қауіпті CGI файлдарын бұрынғы серверлерде тексеруге болады.

Burpsuite – проксиге негізделген құралдар жиынтығы. Ол түрлі функционалдық ерекшеліктерден тұрады. Burp-мен жұмыс істеуді бастау үшін, браузердегі проксиді қалай қолданатынына қарай конфигурациялау бірінші талап болып табылады. Прокси-сервер браузерде орнатылғаннан кейін, burp іске қосуға дайын. Прокси-сервер қойындысы прокси-серверді конфигурациялау және оны конфигурациялау үшін қолданылады. Xampp сервері қолданбаларды сынау идеясымен жасақталған Mutillidae сервері бар жүйеде орнатылған. Осының арқасында, пайдаланушы атын және құпия сөзін белгілі бір пайдаланушыға анықтауға болады, бұл кезде қиылысу қойындысы ажыратылған сіз оны Mutillidae-дан қол жеткізуге тырысады. Негізгі аспект – бұл осалдықтардың қамтуын түсіну. Қамту осалдықтардың санын салыстырады, осалдықтардың жалпы санына қатысты анықталды. Әлбетте, біздің жағдайымызда сканерлердің қандай да бір осалдыққа ұшырамағанын

білу мүмкін емес (біз бастапқы кодқа қол жеткізе алмаймыз). Осылайша, қамтуды есептеу мүмкін емес. Алайда, аз болса да, салыстырмалы салыстыруды жасауға болады қол жетімді деректер. Іс жүзінде анықталған осалдықтардың жалпы санын білеміз (анықталған осалдықтарды шоғырландыруға сәйкес келеді жалған позитивтерді жойғаннан кейін төрт сканерді пайдалану) және әрбір жеке сканер анықталған осалдықтардың саны. Осы ақпараттың негізінде оптимистік көрсеткішке қол жеткізуге болады қамту (әрбір сканер үшін) (яғни нақты қамту төменірек болады ұсынылған біреудің құны). Әлбетте, бұл тек SQL инъекциясының осалдығына қатысты болады, себебі бұл барлық сканерлер арқылы анықталған жалғыз түрі. Байқауымызға мүмкіндік бергенге дейін ұсынылған кейбір қызықты аспектілер. Бірінші байқау – бұл әр түрлі сканерлер әр түрлі ақауларды анықтады. Зияндылық сканерлері зертханалық желіні іске қосты. Сол желіде жүйеге кіру үшін пайдаланылатын қауіпсіздік тесіктерін білу үшін ену тесті өткізілді. Зиянды сканерлердің және осалдықтардың нәтижелерін салыстыру және ену тесті барысында анықталған осалдықтар салыстырмалы сканерлерге қаншалықты сенуге болатындығын көрсетеді. Нәтижелер сканерлердің өткізіп жібермейтінін көрсетеді. Бұл осалдықтар қол жетімділік үшін пайдаланылған болса да, елеулі осалдықтарды немесе олардың төмен басымдықтарын желідегі адамға беруге мүмкіндік береді. Зияндылық сканерлері жақсы ниетпен жұмыс істейді, бірақ сенімсіздікке ие тәуелсіз қауіпсіздік құралы.

1.4 Веб-хакерлікке шолу

Сіз қолданатын қызметтердің көпшілігі интернет арқылы жұмыс істейді. Атап айтқанда, HTTP протоколы арқылы тасымалданған веб-бет қызмет көрсету орталығында болуы мүмкін Интернет (1.2-сурет). ДК және смартфон үшін пайдаланылатын басты бет жеке веб-қызметтің бір түрі. Көптеген компаниялар, негізінен, барлық сервистік порттарды блоктайды қауіпсіздік, бірақ порт 80 веб-қызметтер үшін ашық қалады. Google, яғни күнделікті байланыста болатын әдеттегі портал торабы, сондай-ақ портты 80 пайдаланады. Веб-қызметтер порттың артында басқа портты көрсетпесеңіз, 80 портын пайдаланатыныңызды біледі. 80 порты арқылы веб-сервер әртүрлі деректерді сіздің компьютеріңізге жібереді мәтін, суреттер, файлдар, бейне. 80 порты арқылы пайдаланушы сонымен бірге жібере алады Веб-сервердегі үлкен файлға мәтіннен түрлі деректер [3].



Сурет 1.2 – Интернеттің концептуалды схемасы

Порт 80 әртүрлі формаларда қолданыла алады. Дегенмен, брандмауэр орындалмайды, бұл қауіпсіздік осалдығын шешу үшін, веб-желіаралық қалқан жүзеге асырылуы мүмкін. Алайда, барлық шабуылдардан қорғау мүмкін емес, олар күн сайын дамиды. Қазіргі уақытта хакерлердің осалдығы веб-қызметтері және өлім шабуылын жүргізуге тырысады. OWASP (Open Web Application Security) осалдығын шығарады. Интернеттегі қауіпсіздік жыл сайын. OWASP Top-10 және толық мәліметтерді жариялайды [3].

A1 инъекция. Хакерлер трансляция кезінде жарамсыз деректерді пайдаланып, шабуылды деректер базасына нұсқау жібереді, операциялық жүйелер, LDAP. Хакерлер команданы басқарады операциялық жүйеге қол жеткізу үшін инъекциялық шабуылдар арқылы рұқсатсыз деректер.

A2 сынған аутентификация және сессияны басқару. Программистер түпнұсқаландыруды және сеансты басқаруды өзі дамыту функциясы және тәжірибелі бағдарламашылар функциясын қауіпсіз түрде жасай алады. Тақырыптар кем емес, тәжірибесіз бағдарламашылар осал болып табылатын функцияларды дамытады бұзу үшін. Хакерлер парольдерді осы осалдықтарды пайдаланып ұрлайды немесе тіпті түпнұсқалық растама айналымы.

A3 Cross-Site сценарийі (XSS). XSS осалдығы бағдарлама деректерді жіберген кезде орын алады, дұрыс тексерусіз веб-браузер. Маңызды Жәбірленуші енгізген компьютер туралы ақпарат XSS сценарийі кейін хакерге жіберіледі.

A4 қорғалмаған тікелей нысан сілтемелері. Қауіпсіздікті қамтамасыз ету жөніндегі тиісті шаралар қолданылған жағдайда, пайдаланушы бұлай істемейді. Ішкі нысандарға, осындай файлдарға, каталогтар мен дерекқор кілттеріне URL арқылы кіруге болады. Қосалқы құралдар арқылы ғана ішкі мүмкіндіктерге қол жеткізу мүмкіндігі бар объектілер. Егер ішкі нысан тікелей пайдаланушыға әсер етсе, қатынасу әдісі жұмыс істеген кезде рұқсатсыз деректерге қол жеткізу.

A5 қауіпсіздігі дұрыс емес. Қолданбалар, рамкалар, бағдарлама серверлері, веб-серверлер, дерекқор серверлері және платформаға түрлі қауіпсіздік технологиялары енгізілді. Әкімші мүмкін қоршаған орта файлын өзгерту арқылы қауіпсіздік деңгейін өзгертіңіз. Технология орнатылған қауіпсіздік, жаңа шабуылға ұшырауы мүмкін уақыт. Жүйенің қауіпсіздігін қамтамасыз ету үшін әкімші болуы керек үнемі қоршаған ортаны тексеріп, бағдарламалық жасақтаманың қамтамасыз етілуін қамтамасыз етуі керек бұл ереже қазіргі заманға сай.

A6 сезімтал деректер әсері. Веб-бағдарламалар маңызды деректердің әртүрлі нысандарын пайдаланады, соның ішінде құпия ақпарат және аутентификация туралы ақпарат. Бағдарламашы керек деректерді шифрлау, сақтау немесе беру сияқты қорғаныс шаралары құпия деректер.

A7 жетпейтін функция қол жеткізуді басқару деңгейі. Қауіпсіздік мақсатында сізден рұқсаттарды тексеру керек веб-қосымшалары сервер жағында. Кейде әзірлеушілер жасайды рұқсатты сценариймен клиент жағынан тексеру үшін қате. Web Scroller – веб-сервердің URL-мекен-жайын табады және HTML қоңырауын талдайды. Сценарий арқылы өңделетін рұқсаттар веб-шиыршықты бейтараптандыру арқылы тексерілуі мүмкін.

A8 кросс-сайт сұранысын жасыру (CSRF). Хакер белгілі бір сайтқа шабуыл жасау функцияларын қамтитын сценарий жасайды, оны Интернетте жариялайды. Жәбірленуші веб-бетті қай жерден қотарған болса CSRF сценарийі салынған, сценарий басқа сайттарға білмей-ақ шабуыл жасайды пайдаланушы.

A9 Белгілі осалдығы бар компоненттерді пайдалану. Серверде артықшылықтармен жұмыс істейтін құрамдастар бар superuser. Егер кез-келген хакер осындай компоненттерге қол жеткізе алатын болса, бұл үлкен салдарға әкелуі мүмкін. Сондықтан компоненттер үшін тіркелген қауіпсіздік осал тұстарына қатысты тиісті шаралар қабылдау өте маңызды.

A10 Түпкілікті қайта бағыттау және форвардтар. Кейбір сценарийлер пайдаланушы қарайтын беттерді мәжбүрлеп жылжытуы мүмкін. Жаңа бетке қашан, қалай және қайда бару керектігін шешкен кезде сенімді деректерді пайдалану керек.

Көптеген хакерлік шабуылдар брандмауэр, IDS, IPS немесе брандмауэр веб-қосымшалары арқылы бұғатталуы мүмкін. Дегенмен, веб-хакерлерді бұғаттау қиын, себебі ол тұрақты веб-қызметті және ашық портты 80 пайдаланады. Шындығында, веб-хакинг – хакерлік техниканы жүзеге асырудың қарапайым жолы. Ол кез келген басқа хакерлік әдістерден әлдеқайда күшті. SQL инъекциясы, парольдерді бұзу үшін, веб-қабық шабуылдары OWASP Top 10 тізімінің жоғарғы жағында.

1.5 Honeypot-ты енгізу мысалы

Honeypot – шабуылдаушылармен байланысу үшін желіге орналастырылған арнайы жүйе. Жүйеге қосылулар әдетте рұқсат етілмеген және желілік қорғаушыға егжей-тегжейлі тіркеу арқылы қаскүнемдерді анықтауға

мүмкіндік береді. Тіркеу қосылыс туралы ақпаратты ғана емес, сонымен қатар, сеанстар туралы ақпаратты шабуылдаушы қолданатын әдістерді, тактикаларды және процедураларды (TTP) көрсетеді. Cowrie Honeypot – бұл SSH және Telnet қосылымдарын, сондай-ақ сеанс ақпаратының хост жазбасын басып шығаратын жүйе. Бұл Honeypot-тың түрлері Интернет желісіне кілтсөзді орнатуға тырысқан шабуылдаушылар пайдаланатын құралдарды, сценарийлерді және хосттарды қадағалау үшін жиі қосылады. Honeypot қосымшасы төмен деңгейде жүзеге асырылады. Жоғарыда анықталғандай, төменгі өзара әрекеттесетін Honeypot аулауға түсетін трафиктің көзін алу үшін шектеулі функционалдығы бар бірқатар хаттамаларға қызмет етеді. Honeypot кез-келген заңды қызмет үшін емес, тек honeypot мақсаттары үшін пайдаланылатын IP-адресте орналасады; кез келген бағдарламалық жасақтама қосылымдары зиянды деп саналады және кейінірек шолу үшін жазылады.

Honeypot-тар өте қарапайым болып және оңай кеңею үшін жасалған. Жоба шешімдері зиянкестердің әрекеттерін тіркеуге арналған тұжырымдаманы көрсететін бағдарламаны жасауды қалайды. Сондай-ақ, зерттеулер ақпараттық қауіпсіздік саласындағы техникалық дағдыларды қажет етсе, қажетті хаттамаларды қосу үшін қосымшаны кеңейту керек. Қазіргі уақытта этикалық бұзудың зерттеушілері ішкі және сыртқы желілер қауіпсіз емес дейді. Сондықтан желі деңгейінде әр түрлі қауіпсіздік саясаттары енгізіледі. Бұл саясаттар жақсы қауіпсіздік шараларын алу үшін әлі күнге дейін жаңа бейімделуді қажет етеді. Әртүрлі компаниялар желілік қауіпсіздік үшін желілік брандмауэрлерді, IDS, IPS және honeypots-тарды пайдаланады. Қазіргі уақытта көптеген компаниялар өздерінің қауіпсіздігіне Honeypots-тарды енгізеді. Honeypot – шабуылдаушыларға арналған тұзақтардың желісін қорғау. Honeypots хакерлерді қорғауға және желідегі зиянды әрекеттерді анықтауға арналған. Көптеген компаниялар пайдаланатын көптеген танымал Honeypotstap бар. Халықаралық киберқауіпсіздік институтының этикалық хакерлік зерттеушісінің айтуынша, honeypot шабуылдарды бақылаудың тамаша құралы болып табылады және зиянды бағдарламаларды талдау үшін өте пайдалы.

1.6 Басып енуді анықтау амалдары

Біз әртүрлі шешім алдамшыларын қарастырдық. Барлық өзара әрекеттесуі төмен. Әртүрлі сервистер мен операциялық жүйелерді эмуляциялау арқылы жұмыс істейді. OpenSource шешімдері бар және олар Specter-ға қарағанда әлдеқайда күшті және икемді болып есептеледі, бірақ оны пайдалану да қиын. Specter, коммерциялық қолдау көрсететін шешім, Windows жүйесінде жұмыс істейтіндіктен оңай. Осы тарауда біз бір сәтке қадам жасап, honeypot технологиясының мәнін талқылаймыз.

Бұл дипломдық жобада жалпы қауіпсіздік стратегиясын анықтаудың рөлі қарастырылады. Содан кейін біз кейбір дәстүрлі анықтау әдістерін, сондай-ақ осы тәсілдерге тән кейбір мәселелерді талқылаймыз. Осыдан кейін honeypots осы проблемаларды тиімді шеше

отыруын, стратегияның қауіпсіздікті анықтау компонентін жақсартуын көрсетеді [4]. Тиімді анықтаудың артықшылықтары екі талай. Біріншіден, рұқсат етілмеген әрекеттерді жылдам анықтау арқылы сіз шабуылды алдын ала тоқтата аласыз. Мысалы, ашық файлдық ресурстарға арналған ішкі желіде сканерлеу кезінде бейбіреуді анықтасаңыз, сіз бұл әрекетті оларға қатынай алмайтын файлдарды таппас бұрын анықтап және тоқтата аласыз. Екіншіден, уақтылы анықтау арқылы табысты шабуылды жеңілдетуге болады. Жүйе немесе ресурсты қауіпті деп тез анықтасаңыз, жүйені оқшаулап, қалпына келтіре аласыз. Дегенмен, егер шабуылдаушы сіздің пошта серверіңізге шабуыл жасап анықталмаса және олар 1 ай ішінде байланысыңызды бақылаған кезде елеулі зақым келтіруі мүмкін. Рұқсат етілмеген іс-әрекеттерді анықтау және ескерту оңай деп ойлауға болады. Өкінішке орай, бұл туралы көбісі білетіндей бола бермейді. Дәстүрлі түрде анықтау технологияларының ең көп тараған түрі желіге кіруді анықтау жүйесін (NIDS) қамтиды. Бұл жүйелер күдікті немесе рұқсат етілмеген қызмет үшін желілік трафикті пассивті түрде бақылайды. Мұндай жүйелер осындай әрекетті анықтаған кезде міндетті түрде ескертулер жасайды. НИП-пен күресу – күдікті немесе рұқсат етілмеген әрекеттерді қалай бақылайтынын анықтау. Мұны істеудің көптеген жолдары бар. Дегенмен, екі айрықша таралған тәсілдер ережелер мен ауытқуларға негізделген. Ережеге сүйене отырып, NIDS бірқатар модельдер мен қолтаңбаларға негізделеді. Арнайы ереже FTP серверіне шабуылдарды ұстауға арналған. Ол «5057 440A 2F69» деген портқа баратын пакеттерді іздейді. Бұл мазмұн он алтылық санмен беріледі. Бұл мазмұнды алғанда тиісті ескерту жасалады.

tcp $ EXTERNAL_NET any -> $ HOME_NET 21 (хабарлама: «FTP EXPLOIT») толып кету "; flow: to_server, орнатылған; құрамы:" | 5057 440A 2F69 | "; ClassType: пәрмен-администратор; с.и.д.: 340;)

Біреу файлды файл серверіне суретке түсіргенде, кескіннің бөлігі мазмұнға сәйкес келуі мүмкін, бірақ трафик заңды болып табылады, жалған ескертулер жасайды. Ережеге негізделген NIDS-ті қолданған кезде, ұйым бірнеше аптада ережелерді негіздеу үшін ұйымды қабылдауы мүмкін, ол ережелерді жалған ескертулерді іске қосуды анықтайды. Жалған іске қосылуларды азайту өте сынды болып келеді. Егер қосылулар тым көп жасалса, ұйымдар оларды табу механизмдерін елемейді, себебі көптеген адамдар автокөлік сигналдары өшіп қалғанда елемейді. Жалған қосылулар NIDS-дің проблемасы болғанымен, мәселе жаңартуларда болуы мүмкін. Жаңа шабуылдар анықталғандықтан, дерекқорға жаңа ережелерді қосу керек немесе NIDS жаңа шабуылдарды анықтай алмайды. Бұл ережені жаңарту процесі ешқашан аяқталмайды, өйткені жаңа шабуылдың өңделуі ешқашан аяқталмайды. Аномалияға тәуелді NIDS-ті ерекшеленеді. Ол ережелер бойынша жұмыс істемейді; Керісінше, ауытқуларға негізделген технологиялар орнына әдеттегі желінің тәртібі қандай екенін білуге тырысады, содан кейін ғана шабуылды бастау үшін дұрыс емес болып саналатын ескертуді іске қосады. Аномалияларды анықтау мәселесі қалыпты жағдайды анықтау болып

табылады. Егер желі ұзақ уақыт бойы өзгермейтін болса, онда оны анықтау оңайырақ болады. Дегенмен, жаңа қосымшалар мен технологиялар желіге үнемі қосылып отырады, сондықтан жиі өзгереді. Әңгімелесу бағдарламалары, біррангты байланыс желілері, қолданыстағы хаттамалардың жаңа енгізулері, IP байланысының динамикалық сипаты, бұл қалыпты желі мен мінез-құлықты орнату қиындық тудыратын метриканы белгілеуді өте қиын екенін көрсетеді [5].

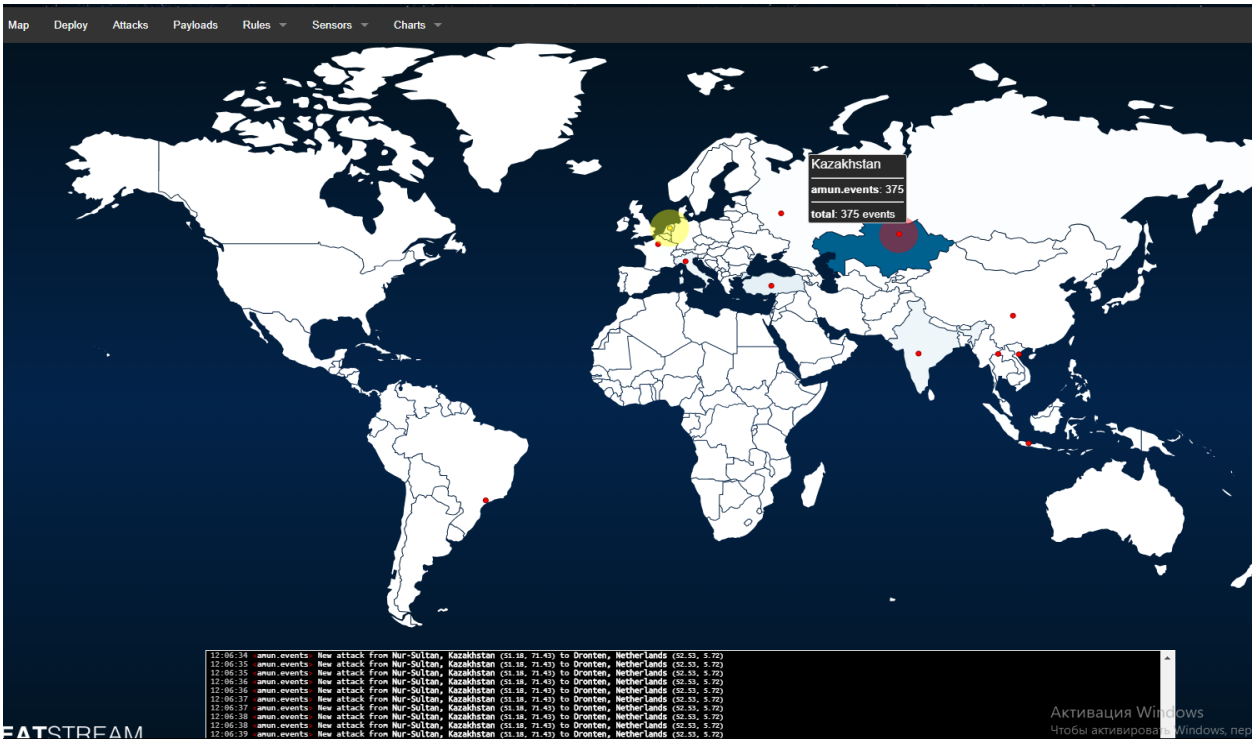
Олар жылдам орналастырылуы мүмкін және көптеген жүйелерді бақылау өте қиын. Барлық жүйелерді пассивті қадағалау арқылы барлық желілік белсенділікті күдікті қызмет үшін талдауға болады. Дегенмен, көптеген NIDS-тер осы мәселелермен кездеседі.

2 Modern Network Honeypot

2.1 HoneyRJ-ды іске қосу және инициализациялау

Біздің супер көңілді шабуыл карточкасы 24 сағат бойы Cowrie Honeypot-қа қосылып тұрған бірегей ASN-ды көрсетеді. Сары түспен белгіленгені SSH байланыстарын көрсетсе, қызыл түсті белгі Telnet қосылымдарын көрсетеді (2.1-сурет). Мұндай шабуыл карталарының көпшілігінде болғандай, мұндай визуализацияның тактикалық құндылығы жоғары қауіпсіздік құралдары мен ресурстарын алу үшін осы әдіс пайдаланушыларды жиі таңдандырады. Дегенмен, ол 24 сағат ішінде біздің хостымызға шабуыл көздерінің нақты географиялық және ұйымдық таратуды көрсететін белгілі бір құндылықты береді. Анимацияланған графикте әрбір дереккөзден қосылымдардың көлемі туралы ешқандай түсінік жоқ.

Қауіп-қатерлер картасы кибершабуылдардың қауіпсіздігінің көрінісі болып табылады, әдетте анимацияланған және өте көрнекі болып келеді. Бұл Nors корпорациясы қолданған өніміңізді сатуға арналған сәнді тәсілі. Компания визуальды шабуыл картасын көрсеткенімен танымал болды, бірақ карталар құндылығы аз болыпжәне фрагменттік деректер сияқты көрінді. Leafletjs көмегімен жасалған. NOC проекторына арналған шабуыл картасын жасауды қалайтындар үшін: мұны Flyer Migration Layer Plugin және Maxmind GeoIP Sprinkler құрылғысымен біріктіріңіз.



Сурет 2.1 – Қазіргі уақыттағы шабуылдар картасы

Көптеген көздер бірнеше рет қосылуға тырысты. Бұл шабуылдау сценарийлерінде тіркелгі деректерінің тізімі болады және қосылым үшін бірнеше комбинациядан өтуі күтіледі. Cowrie Honeypot тек белгілі бір пайдаланушы аты мен құпия сөз тіркесін қабылдауға теңшелген. Бұл user.db файлында дәлденген.

Maxmind Geolocation деректерін пайдаланып, мен әр елдегі қосылыстардың санын белгіледім. Бразилия мен Қытай елдері таңқалдырмайды, себебі олар көбінесе сканерлеу шуы жоғары елдер болып табылады.

Шабуылдау жүйелеріндегі ашық порттар (Shodan.io деректері). Әрі Shodan арқылы IP-адрестердің бастапқы тізімінің орындалуы ашық портты жүйелерді анықтады. Елге және ұйымға қатысты ашық порттардың шоғырлануы. Бұл ұқсас жүйелердің үлкен блоктарын бұзуы мүмкін, бірақ кішігірім үлгіде Қытайда ашық порты 500-ке көп қосылымдарды қоспағанда, шынымен ештеңе шықпайды [6].

Бразилиядағы көптеген жүйелердің қызықты қорытындысы – олар Censys пен Shodan-да жазылған 22, 23 немесе басқа порттары жоқ болуы. Олардың барлығы да интернетке қосылған тұтынушы болып келген.

Маңызды жүйелерден зиянды трафикті таратуға, сыни жүйелердің соққылары алдында ағымдағы шабуылды алдын-ала ескертуге және зиянкестер мен олардың әдістеріне қатысты ақпаратты жинауға тырысатын көптеген қосымшалар бар. Егер honeypot нақты деректерді қамтымаса және мұқият бақыланатын болса, шабуылдаушының (TTP) құралдарын, тактикасын

және процедураларын білуге және бүкіл желіге қауіп төндірмей заңды және заңдық дәлелдерді жинауға болады.

Алдамшы жұмыс істеуі үшін жүйе заңды түрде көрінуі керек. Өндірістік жүйе жүргізетін процестерді іске қосу керек және көрінетін файлдар болуы керек. Алдамшы болып сызықты кез-келген жүйе болуы мүмкін, ол сниффинг және тіркеу мүмкіндігімен бапталған. Сондай-ақ honeypot-ты корпоративті брандмауэрдің қасына орнату жақсы идеясы болып табылады – себебі бұл маңызды тіркеу мен ескерту мүмкіндіктерін ғана емес, сонымен қатар, бұзылған honeypot апаратын басқа ішкі ресурстарға ауысуға болмайтындай шығатын трафикті блоктауға мүмкіндік береді.

Мақсаты бойынша, алдамшылардың екі түрі бар: зерттеу және өндіру алдамшылары. Зерттеулерде шабуылдар туралы ақпарат жиналады және табиғатта зиянды әрекеттерді зерттеу үшін арнайы қолданылады. Сіздің қоршаған ортаңызды және бүкіл әлемді ескере отырып, олар шабуылдаушылар үрдістеріне, зиянкестер мен зиянкестердің белсенді түрде қолданатын осалдықтарына қатысты ақпаратты жинайды. Бұл сіздің профилактикалық қорғауыңызды, басымдықты және болашақ инвестицияларыңызды хабардар етуі мүмкін.

Басқа жағынан, өндіріс алдамшылары сіздің ішкі желідегі белсенді сатылымдарды анықтауға және зиянкестерді алдауға бағытталған. Ақпарат жинау бұрынғыдай басым мәселе болып табылады, себебі, honeypot сізге қосымша бақылау мүмкіндіктерін қамтамасыз етеді және желілік сканерлеу кезінде және бүйірлік қозғалыста ортақ анықталған кемшіліктерді жояды. Өндірісті алдамшылар басқа өндіріс серверлерімен жұмыс істеуге және сіздің ортаңызда жұмыс істейтін қызметтерді бастауға мүмкіндік береді. Зерттеулер, әдетте, күрделірек және өндірістен гөрі көп деректер түрлерін қамтиды.

Honeypot қиындығының өзгермелері:

Өндірістік және ғылыми-зерттеу алдамшылары шеңберінде сіздің ұйымыңыз қажет ететін күрделілік дәрежесіне қарай әртүрлі деңгейлер бар:

1) Таза алдамшы. Бұл әртүрлі серверлерде жұмыс істейтін кең ауқымды, толық имитациялық жүйе. Ол «құпия» деректерді және пайдаланушы туралы ақпаратты, сондай-ақ сенсорлармен толыққанды. Алдамшылар қиын және қолдануда күрделі болса да, одан алған ақпарат өте құнды.

2) Жоғары деңгейдегі қарым-қатынасы бар Honeypot. Ол соншалықты күрделі емес және көп деректер жоқ болғаннан қызметтерді жүзеге асыратын мағынада таза honeypot-қа ұқсайды. Жоғары деңгейлі honeypot-тар толыққанды өндірістік жүйені имитациялауға арналмаған, бірақ олар өндіріс жүйесінде, соның ішінде тиісті операциялық жүйеде жұмыс істейтін барлық қызметтерді іске қосады. Бұл түрдегі алдамшылар шабуылдаушы операциясының мінез-құлқы мен әдістерін көруге мүмкіндік береді. Жоғары деңгейдегі өзара әрекеттесу үшін үлкен қорлар мен техникалық қызмет көрсету талап етеді.

3) Өзара әрекеттесуі орташа Honeypot-тар. Олар қолданбалы қабаттың аспектілерін жасайды, бірақ өздерінің операциялық жүйелері жоқ. Олар

шабуылға қалай әрекет ету керектігін анықтау үшін ұйымдарға көп уақыт жұмсайтын зиянкестерді тоқтатуға немесе шатастыруға тырысады.

4) Өзара әрекеттесуі төмен деңгейлі Honeypot-тар. Бұл honeypot түрі өндірісте кең таралған. Өзара әрекеттесуі нашар honeypot-тар бірнеше қызметтерді ұсынады және әлемдегі алдын алуды ерте анықтау механизмі ретінде қызмет етеді. Оларды орналастыру және қолдану көптеген қауіпсіздік желілердің әртүрлі сегменттерінде бірнеше honeypot таратқаннан оңай [7].

Алдамшы технологиясының әртүрлі түрлері. Бірнеше қолданылатын honeypot технологиялары мыналарды қамтиды:

1) Зиянды бағдарламалар. Олар зиянды бағдарламаларды анықтау үшін белгілі векторларды пайдаланады. Мысалы, honeypots (мысалы, Ghost) USB-диск ретінде эмуляция үшін жасалған. Егер құрылғы USB арқылы зиянды бағдарламалық жасақтамамен жұқтырылған болса, honeypot зиянды бағдарламалық жасақтаманы эмуляцияланған құрылғыны жұқтыруға түртеді.

2) Спам бағанасы. Ашық пошта релелерін және ашық прокси-серверлерді эмуляциялауға арналған. Спаммерлер ашық пошта транспондерін алдымен электрондық поштаны жіберу арқылы тексереді. Егер олар сәтті аяқталса, олар үлкен көлемді спамдарды жібереді. Бұл honeypot түрі осы сынақты тауып, тануға және кейінгі көлемді спамдарды сәтті жояды.

3) Деректер базасының алдамшысы. SQL инжекциясы сияқты іс-әрекеттер жиі брандмауэрлер арқылы байқалмайды, сондықтан кейбір ұйымдар жасанды дерекқорларды жасау үшін бағындыруды қамтамасыз ететін дерекқордың брандмауэрін пайдаланады.

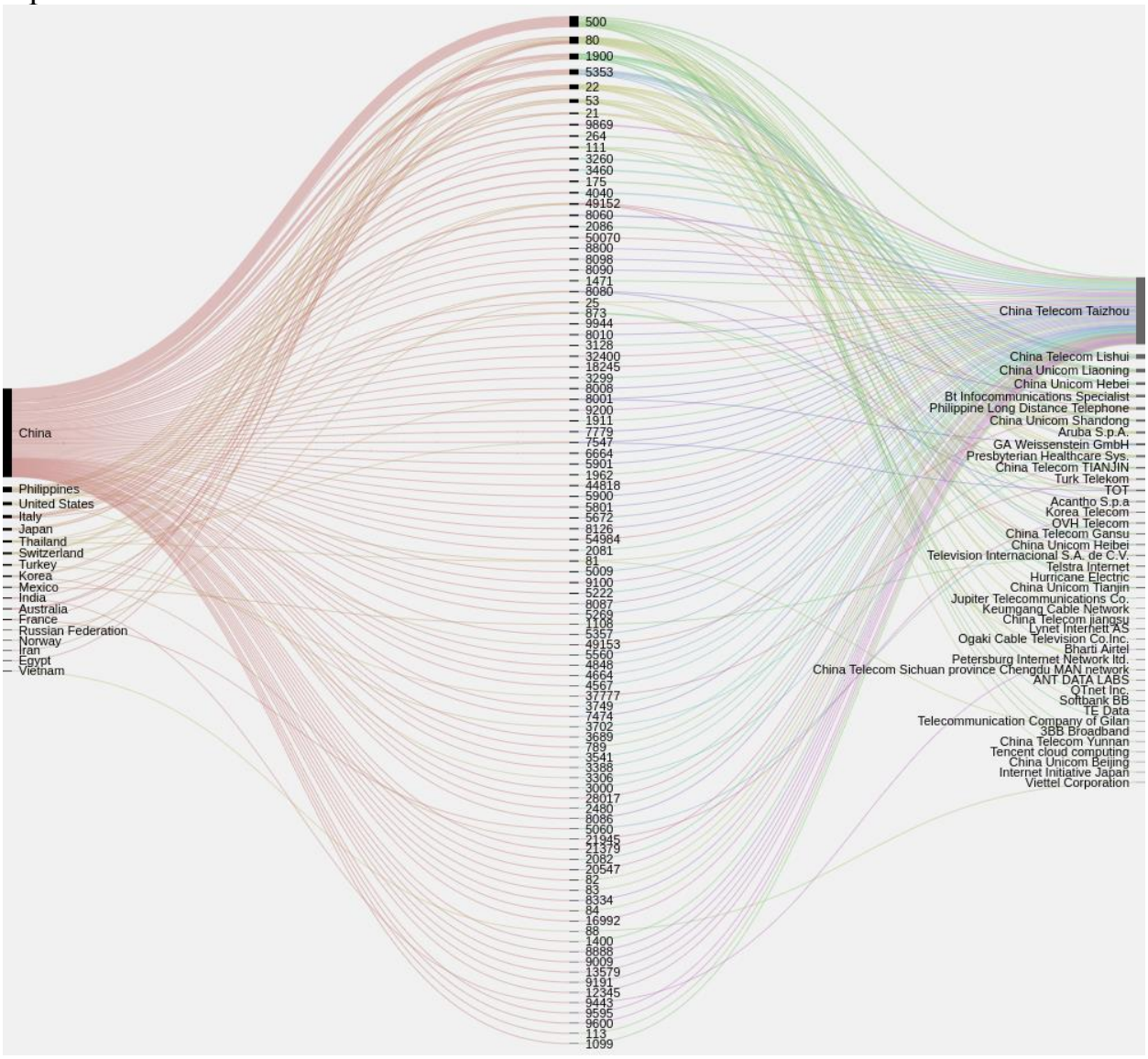
4) Клиенттің төлемі. Көптеген алдамшылар – қосылыстарды тыңдайтын серверлер. Клиенттік honeypot-тар клиентке шабуыл жасайтын зиянды серверлерді белсенді түрде іздейді, бұл олардың күдікті және күтпеген өзгерістерін бақылайды. Бұл жүйелер, әдетте, виртуалдандыру технологиясында жұмыс істейді және зерттеу тобына қауіп-қатерді барынша азайту үшін қорғаныс стратегиясына ие.

Honeypots-тар оны жүзеге асыруға шешім қабылдаған ұйымдарға көптеген артықшылықтар ұсынады. Олар шабуылдаушының өлім тізбегін бұзып, шабуылдаушы әрекетін бәсеңдетеді. Шабуылдаушылар сіздің ортаңызда жүргенде, олар желіңізді сканерлейді, тексереді және дұрыс конфигурацияланбаған, осал құрылғыларды іздейді. Бұл сатыда олар сіздің зиянкесінің қолжетімділігін тексеру және шектеу қажеттілігі туралы ескерте отырып сіздің алдамшыңызды өшіре алады. Бұл шабуылдаушы сіздің ортаңыздан деректерді сәтті жоюға дейін жауап беруге мүмкіндік береді. Шабуылшылар нақты деректер бар аумақтарды іздеудің орнына, жыртқышпен жұмыс істеуге тырысатын уақытты айтарлықтай жұмсай алады. Шабуылдарды пайдасыз жүйеге қайта бағыттау циклдарға жұмсалады және шабуылдың ілгерілеуін алдын-ала ескертеді.

Қазіргі заманғы honeypots-тар – жүктеу және орнатуда ғана оңай емес, сонымен қатар қауіпті қате конфигурациялар мен зиянкестер туралы нақты ескертулер бере алады. Кейбір жағдайларда, сіздің командаңыз, егер біреу сіздің ішкі желіңізге кіре бастағанға дейін, honeypot қолданылғанын ұмытып

кетуі мүмкін. Интрузияны анықтау жүйелерінен айырмашылығы, honeypot шабуылдардың нашар беделі немесе жаңа қауіп туралы ақпараты қажет емес.

Honeypot-тар қауіпсіздікті жақсартуға көмектеседі, себебі олар қауіпсіздік қызметі күтпеген әрекетті анықтаса, не істеу керектігін біледі. Қауіпсіздік тобы ескертуді зерттеп, тиісті шаралар қабылдауы мүмкін бе? Honeypots сіздің қауіп-қатерді анықтайтын стратегияңыз болуға тиіс емес, бірақ олар шабуылды ерте анықтауға көмектесетін қауіпсіздіктің тағы бір деңгейін білдіреді. Олар зиянды мінез-құлықты зерттеу және ішкі желідегі ымыраға келуді анықтау үшін қауіпсіздіктің мамандарына қол жетімді бірнеше әдістердің бірі. Зиянкестер мүмкін болатын саны 2.2-суретте көрсетілген.



Сурет 2.2 – Зиянкестердің саны

Censys деректер жиынтығын 22-портта және 23-портта тексеру мені таңқалдырды. Мен осы сканерліктердің көпшілігі мен парольді қолдана отырып, шабуылдардың өздігінен көшірілетін сценарийлер (боттар) көмегімен

жасалуы туралы болжамнан бастадым. Сценарий ашық порттарды іздеу және парольдерді іздеу арқылы таратылады, ол қабыстан кейін оны көшіреді және бірдей әдісті қолданады. Дегенмен, мұнда telnet сканерлейтін Интернетке ашылған 23 порты бірнеше бірегей хосттарды көруге болады. Бұл жүйенің басқа әдіспен бұзылуын немесе сценарийлерді қолмен орындағаны бар зиянкесерлерді білдіреді.

2.2 Honeypot көмегімен тіркелген шабуылдарды зерттеу

MHN Honeypot – мыңдаған оқиғаларға дейін кең және таралған ауқымда сыртқы және ішкі honeypot қондырғыларын қолдайтын еркін ашық бастапқы бағдарламалық жасақтама.

Бұл Honeypot бағдарламалық жасақтамасы Интернеттегі кейбір заңсыз әрекеттер туралы құнды ақпаратты жинауға арналған. Бұл бағдарламалық жасақтаманы пайдалану ұйымдарды және зерттеушілерді бұзушы пайдаланушыларды және әртүрлі желілерді уақтылы және тиімді түрде анықтауға мүмкіндік береді.

MHN Honeypot корпоративтік деңгейдегі тиімділік пен қауіпсіздікті қамтамасыз ету үшін стандартты HPFeeds және төмен өзара әрекеттесетін honeypots-ты пайдаланады. MHN толыққанды REST API-ны ұсынады және SIEM коммерциялық Optic платформасы арқылы интеграциялау үшін CEF және STIX қолдауымен қол жетімді. Optic өз кезегінде барлау және талдау үшін бағдарламалық жасақтама болып табылады. Жоғарыда аталған құралдарды Anomali (авторлық құқық (C) 2019 - Anomali, Inc. қол жетімді) компаниясы әзірледі [8].

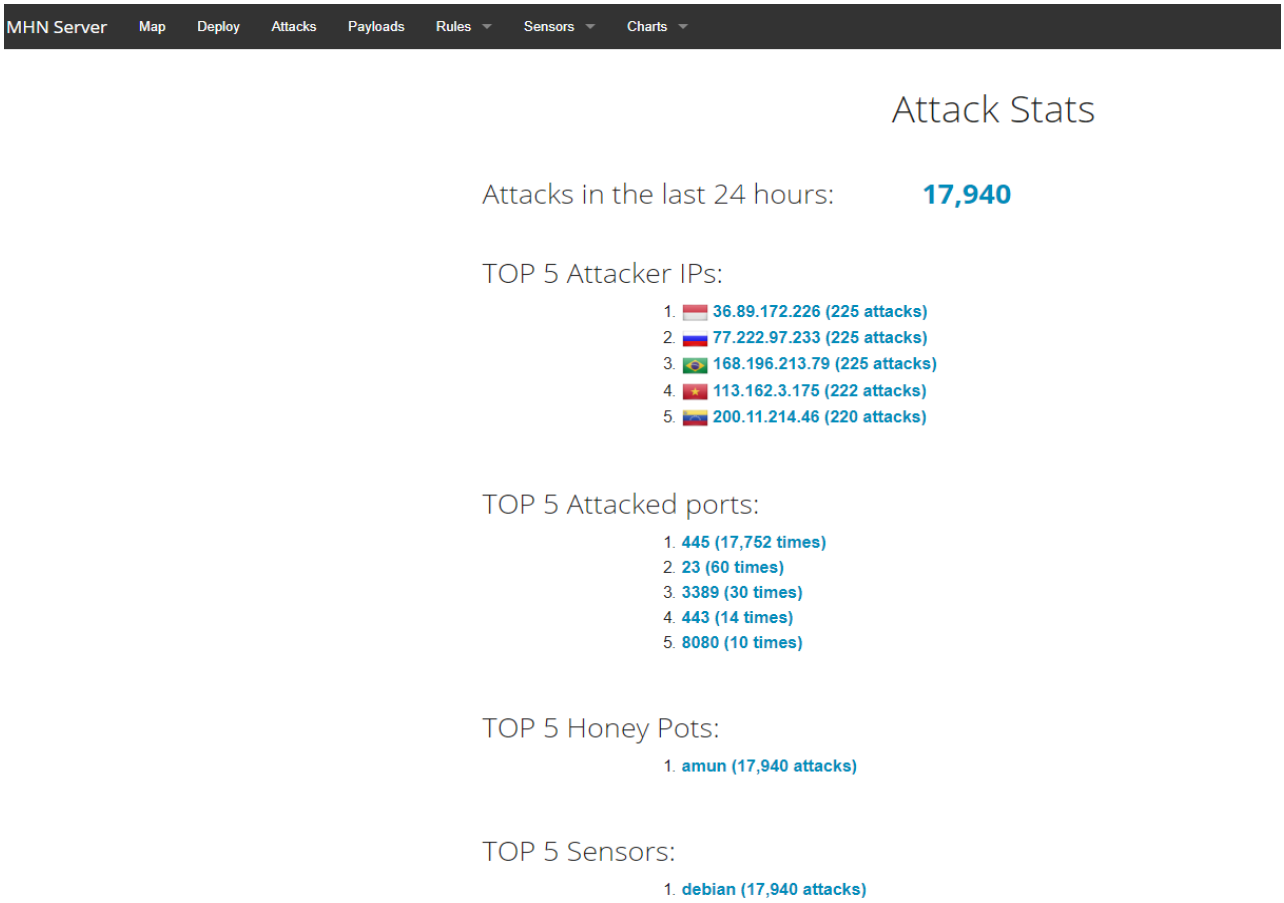
Anomali – бұл АҚШ-тың ақпараттық қауіпсіздікті талдау платформасы белгілі АҚШ кибер-қауіпсіздік компаниясы. Сонымен қатар, Anomali Black Hat Conference компьютерлік қауіпсіздік конференциясының негізгі ұйымдастырушыларының бірі. MHN honeypot бағдарламалық жасақтамасы өте танымал болғанымен, пайдаланылған кезде жоғары сапалы қауіпті талдау жүргізуге мүмкіндік береді, ол ешқашан кең таралған емес. Менің ойымша, honeypot-тар орналасуы тым күрделі және басқару үшін ауқымды болғаннан танымал емес. Бұл MHN Honeypot мүмкіндіктері әртүрлі типтегі тұзақтарды енгізуді, инфрақұрылымның белгілі бір жүйелерін клондау мүмкіндігін, сондай-ақ шабуыл картасымен (2.4-сурет) графикалық интерфейспен ыңғайлы панельді қамтиды. Қолданыстағы honeypottар (сенсорлар):

- Snort;
- Suricata;
- Dionaea;
- HTTP арқылы Dionaea;
- Conpot;
- Drupot;
- Kippo;
- Amun;
- Glastopf;

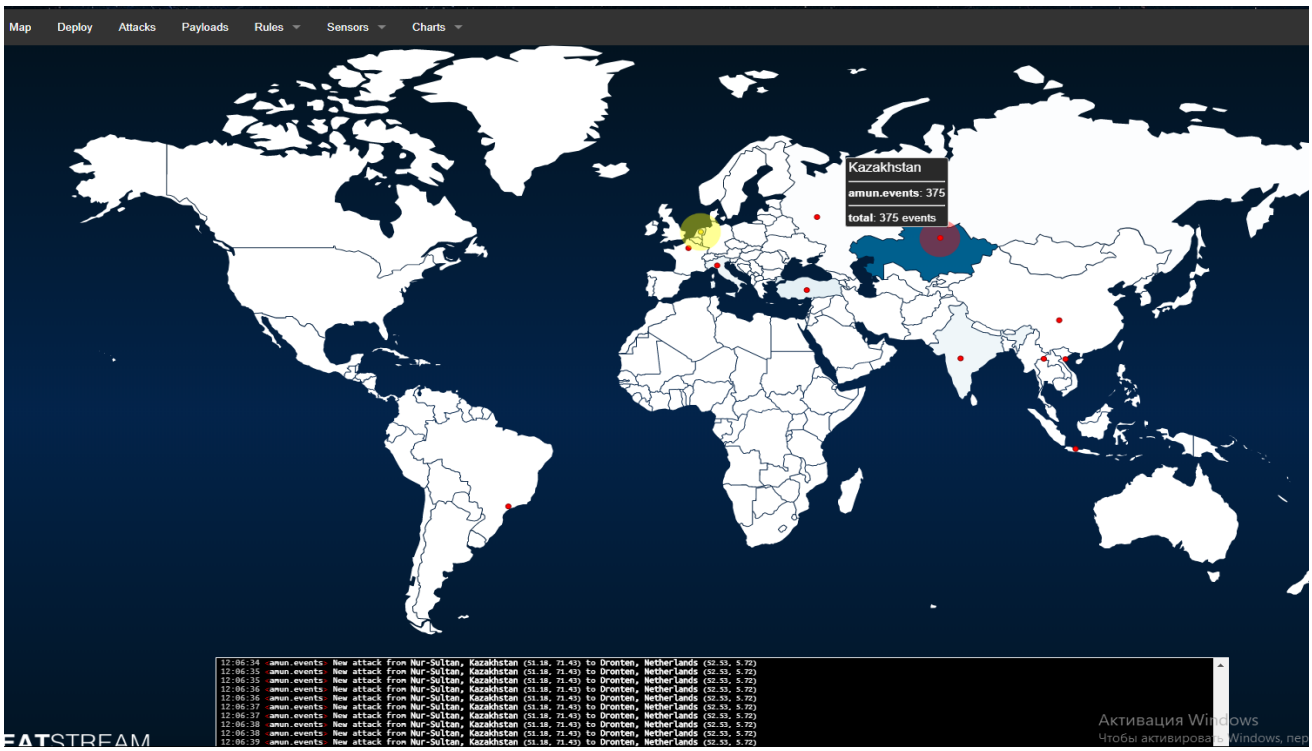
- Wordpot;
- ShockPot;
- p0f;
- Elastichoney.

Техникалық мүмкіндіктері:

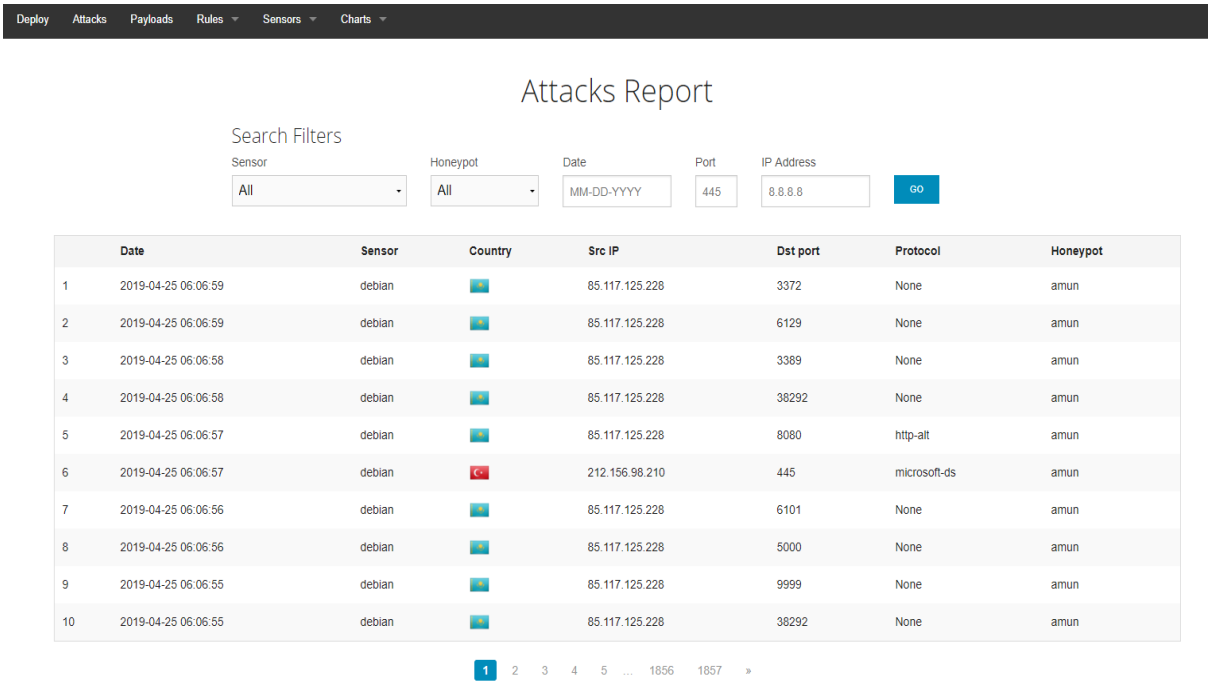
- өзінің арсеналында тұзақтардың 15 түрі бар (алдамшылар);
- жаңа honeypot-тарды қосу мүмкіндігі бар;
- шабуылды анықтайтын қолтаңбаларды конфигурациялау;
- тиісті сенсорлардың ережелерін конфигурациялау;
- шабуылдың көздері мен мақсаттарының нақты уақытында жаңартылған картасы бар. Шабуылдар статистикасы және шабуылдар есептемесі сәйкесінше 2.3 және 2.5-суреттерде келтірілген.



Сурет 2.3 – Dashboard шабуылдар статистикасы.



Сурет 2.4 – Нақты уақыттағы шабуылдар картасы

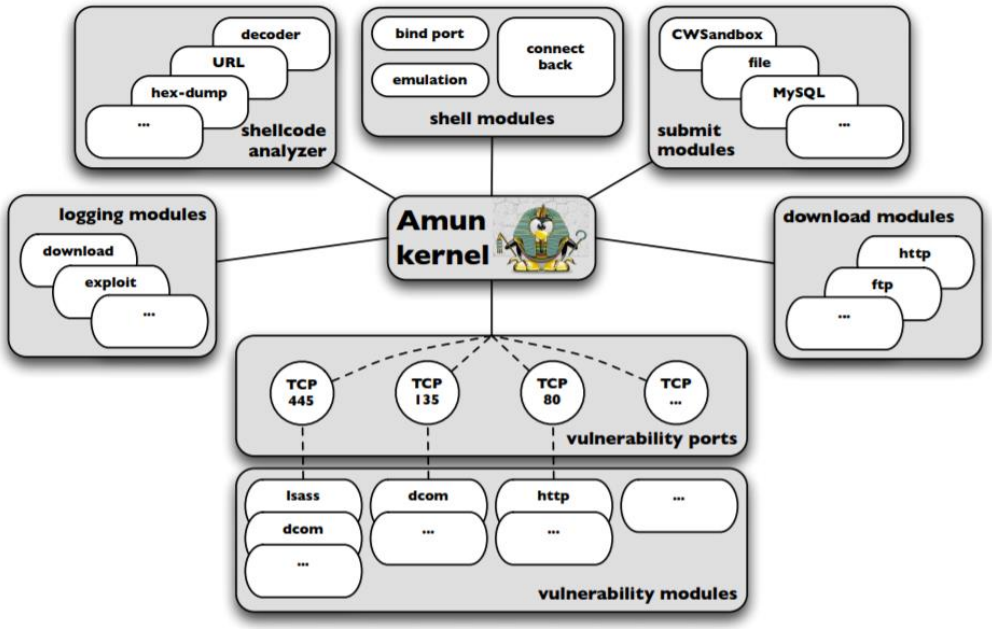


Сурет 2.5 – Шабуылдар есептемесі

2.3 Amun қақпаны (сенсор). MHN Honeypot-қа біріктіру

Келесі бөлімдерде біз Amun honeypot бағдарламалық жасақтамасының енгізілуін және конфигурациясын суреттейміз. Біріншіден, біз жүйенің кең шолуын ұсынамыз, содан кейін, honeypot жұмыс істегенде қатысатын түрлі бөліктердің толық сипаттамасын қарастырамыз. Amun Python-да жазылған,

қарапайым сценарий тілі. Honeypot осы бөлікте толығырақ сипатталатын түрлі компоненттерден тұрады [9].



Сурет 2.6 – Amun-ды орнату сызбасы.

2.6-суретте Amun және әрбір бағдарламалық жасақтаманың ядросымен өзара әрекеттесуі көрсетілген. Жоғарыдағы компоненттердің әрқайсысы келесі бөлімдердегі мәліметтерде бейнеленген.

2.3.1 Amun ядросы

Amun ядросы – бұл honeypot-тың негізгі компоненті болып табылады. Бұл бөлім іске қосу және орнату процедураларын, сондай-ақ негізгі бағдарламалық жасақтама рәсімдерін қамтиды. Amun – бұл бір ретті қолданылатын бағдарлама, оны таңдау схемасы арқылы қайталау үшін қолданылатын нұсқасы. Розетка операцияларынан басқа, Amun жүктейді, конфигурацияны қайта жүктейді, қабықты кеңейтеді және оқиғаларды негізгі циклде тіркейді.

Іске қосу кезеңінде Amun ядросы шелл-кодын сәйкестендіру үшін пайдаланылатын қалыпты өрнектерді инициализациялайды, негізгі конфигурация файлын оқиды, ішкі тіркеу модульдерін жасайды және барлық сыртқы модульдерді жүктейді. Сыртқы модульдер – жеке осалдықтарды эмуляциялауға жауапты осалдық модульдері, мысалы, дерекқорлар сияқты басқа қызметтердегі шабуылдар туралы ақпаратты жазатын модульдерді тіркеу және екілік файлдарды қатты дискіге жазуға болатын презентация модульдері. Әрбір жүктелген осалдық модулінде Amun ядросы байланысқан порттардың тізімін шығарады және осал модулін порт арқылы перне ретінде алапта сақтайды.

Array

([139] => Array
([0] => vuln-netdde
[1] => vuln-ms06040)
[445] => Array
([0] => vuln-ms08067
[1] => vuln-ms06040
[3] => vuln-ms06070))

Келесі қадамда осалдық модулі тіркелген әр порт үшін, яғни жиіліктер пернелері, TCP сервері іске қосылады. Сондай-ақ, Amun UDP-ге негізделген қызметтерді қолдайды, бірақ бұл мүмкіндік қазір пайдаланылмайды және конфигурация арқылы файлдар қол жетімді емес. Барлық бастапқы модульдерді жүктеп, тиісті TCP серверлерін іске қосқаннан кейін, Amun ядросы негізгі циклге кіреді. Осы цикл барысында ол барлық қосылатын розеткалар арқылы жылжиды, жүктеме оқиғаларын бастайды, ақпаратты нақты модульдерге аударады және өзгертулер үшін негізгі конфигурация файлын қайта оқиды. Негізгі конфигурация файлын қайта орындау белгілі бір параметрлерді жұмыс уақытында өзгертуге мүмкіндік береді, яғни Amun тоқтатуды және қайта іске қосуды қажет етпейді. Amun honeypot-ты іске қосу үшін қажетті барлық параметрлерді конфигурациялау үшін бір конфигурациялық файлды пайдаланады. Бұл бөлімде біз параметрлердің әрқайсысын, олардың ықтимал мәндерін және бұл адреске қалай әсер ететінін қысқаша сипаттаймыз. Amun-нің негізгі конфигурация каталогында орналасқан конфигурациялық файлы amun.conf деп аталады. Негізгі параметрлердің бірі - IP. Ол Аммун жұмыс уақытында тыңдайтын IP-мекен-жайын анықтайды. Хост-жүйеге тағайындалған барлық мекен-жайларды және интерфейстерді тыңдау үшін сізде бір IP-адрес параметр немесе әмбебап IP-адрес 0.0.0.0 болуы керек. Сондай-ақ, интерфейс атауын (мысалы, eth0), IP мекенжайының ауқымдарын (192.168.0.1-192.168.0.5), желілер үшін CIDR белгілеуін (192.168.0.0/24) немесе үтірлермен бөлінген IP мекенжайларын көрсете аласыз. Өтінеміз, назар аударыңыз, бұл соңғы параметрлері ауқымды IP мекенжайлар жақсы, өйткені операциялық жүйе саны шектеулі. Егер сізге жүзден астам IP-мекен-жайды тағайындау қажет болса, сіз қойылмалы мекен-жайды пайдалануыңыз керек. Honeypot IP-адресінен басқа, Amun-ның артықшылықтарын шектейтін пайдаланушы және топ анықталуы мүмкін. Қосылғаннан кейін, Amun осы жерде анықталған пайдаланушыға және топқа ауысады. Алайда, кейбір жағдайларда, эксплуатациялар 1024-ден төмен порттарды ашуды талап етеді, бұл тек түбірлік артықшылықтармен жасалуы мүмкін. Егер Amun түбір билігі болмаса, бұл сұрауды өңдеу мүмкін емес. Төменде Amun байланыстары, ашық порттар және жүктеу сұраулары үшін күту уақытының әдісін теңшейтін кейбір уақытша күту параметрлері берілген. Кейбір шабуылдар дұрыс жұмыс істемеуі мүмкін болғандықтан, мысалы, шабуылдаушылар сұралған портқа қосылмайды, сондықтан Amun белгілі бір уақыт өткеннен кейін осы портты жабуы керек. Опциялар: қосылымды күту

уақыты, бинпорт уақытының үзілуі және ftp уақытша күту уақыты деп бөлінеді. Көрсетілген мән Amun қосылымды аяқтағанша күтуге болатын секундтардың санын білдіреді. Сондай-ақ, Amun кейбір шабуылдаушы хосттарды белгілі бір оқиғалар жағдайында қайта қосудан бас тартуға мүмкіндік береді. Бұдан келесі оқиғалар: зиянды бағдарламаны қотарудан бас тартылды, жүктеу уақыты тайм-аутқа байланысты аяқталмады, екілік файл сәтті түрде жүктелді және хост адресатты сәтті қолданды. Осы оқиғалардың әрқайсысы үшін конфигурация файлы сізге блоктың мәнін орнатуға және сонымен қатар, хосттың қанша уақыт бойы блокталуы керектігін анықтайтын уақытша мәнді (секундтармен) орнатуға мүмкіндік береді [10].

[...] ### block refused IPs, timeouts, successfull downloads, ### or successfull exploits for x seconds ### (can be changed while running) refused_blocktime: 1200 timeout_blocktime: 1200 sucdown_blocktime: 1200 sucexpl_blocktime: 1200 ### block ips which refuse a connection, throw a ### timeout, or from which we already have a ### successfull download or exploit ### (can be changed while running) block_refused: 0 block_timeout: 0 block_sucdown: 0 block_sucexpl: 0 [...]

```
### block refused IPs, timeouts, successfull downloads,
### or successfull exploits for x seconds
### (can be changed while running)
refused_blocktime: 1200
timeout_blocktime: 1200
sucdown_blocktime: 1200
sucexpl_blocktime: 1200
### block ips which refuse a connection, throw a
### timeout, or from which we already have a
### successfull download or exploit
### (can be changed while running)
block_refused: 0
block_timeout: 0
block_sucdown: 0
block_sucexpl: 0
```

Amun ену сенсоры ретінде пайдаланылса бұл параметрлер әсіресе қызықты болып келеді. Көптеген жұқтырған хосттар бал аузына бірден бірнеше рет шабуылдайды, әсіресе, егер адреске бірден көп IP-мекен-жайы берілсе. Жасалатын журнал хабарларының санын азайту үшін осындай хостты нақты уақытқа тыйым салуға болады. Біз екілік файлды сәтті жүктеп алған хосттарды құлыптауға мүмкіндік берудің себебі, көбінесе бір хост белгілі бір уақытта бір ғана екілік файлды таратады. Бірдей хосттан сол файлды қайта-қайта жүктеу үшін ресурстардың қалдықтары болады. Сондықтан, осы хосттардан кез-келген қосымша байланыстарды белгілі бір уақыт кезеңінде қабылдамауға болады. Amun TFTP жүктеу модуліне арналған қосымша үш

параметрді ұсынады, олар трансфессиялық tftp, максималды ретрансляция tftp және толық емес tftp үнемдеу деп өзгертілуі мүмкін. TFTP UDP протоколын пайдаланғандықтан пакеттер жоғалуы мүмкін. Осы себепті, Amun сізге беруден бұрын қайта беру санын белгілеуге мүмкіндік береді. Бірінші параметр TFTP сұрауын қайта жібергенше қанша секунд күтетінін анықтайды, ал екінші параметр Amun жалпы алғанда қанша рет қайта жіберуді анықтайтынын анықтайды. Соңғы нұсқасы Amun-ның толық емес TFTP жүктеулерін сақтау керек екенін анықтайды, яғни файл ішінара жүктеледі. Толық емес tftp сақтауға ұқсас опция, http файлының өлшемін тексеру мүмкіндігі. Көптеген зиянкес бағдарламаларды HTTP протоколы ретінде HTTP протоколы пайдаланады және HTTP серверінің функцияларының бірі HTTP жауап тақырыбындағы файл өлшемін сақтау болып табылады. Егер http файл өлшемін тексеру қосылса, Amun жүктелген екілік файлдың өлшемін HTTP тақырыбында алынған мәнмен салыстырады. Егер сәйкес келмейтін болса, жүктелген файл жойылады. Тағы бір маңызды ерекшелігі – жергілікті параметрді ауыстыру. Shellcode Analyzer жүктелетін пайдалы жүктемесінен жүктеу URL-мекен-жайын алған кезде, кез-келген IP-мекен-жайы жергілікті IP-мекенжайлар тізіміне қарсы тексеріледі (мысалы, 192.168.0.0/24). Егер жергілікті IP-адресті ауыстыру әдісі қосылса, Amun осы IP-мекен-жайларының барлығын эксплоит жіберген шабуылдаушылардың бірімен алмастырады. Шелл кодтағы жергілікті IP-мекен-жайлар желілік мекен-жайларды аудару (NAT) серверінің артында хост қабылданған кезде пайда болады, себебі көптеген зиянды бағдарламалар хост конфигурациясынан IP-мекен-жайды алады. Дегенмен, IP мекенжайларын ауыстыру, сонымен қатар, honeypot-ты анықтауды жеңілдетеді. Егер, мысалы, шабуылдаушы жергілікті IP мекенжайлары бар жүктеу URL-мекенжайларымен эксплоиттер жіберсе және эксплуатацияланған хост шабуылдаушының хостынан файлды жүктеуге тырысса, шабуылшы IP-мекен-жайын эксплуатациядан ауыстыру керек екенін біледі, сондықтан шабуылдаушы honeypot болып табылады. Сондықтан, жергілікті ір ауыстыру әдепкі бойынша ажыратылған. Одан кейін, Amun іске қосылуы керек модульдерді баптауға мүмкіндік береді. Жіберуші модульдер тізімі кез келген жүктелген екілік файлды өңдейтін модульдерді қамтиды. Әдепкі түрде жүктелетін модуль - submitmd5 модулі, ол кез-келген жүктелген файлды қатты дискіге сақтайды. Бірегейлік MD5 файлының хеші арқылы анықталады. Осы типтегі қосымша модульдер екілік файлдарды CWSandbox сияқты сыртқы қызметтерге тасымалдауға мүмкіндік береді. Журнал модульдері арнайы журнал жүргізу функцияларын орындайтын модульдер болып табылады. Көптеген жағдайларда бұл модульдер сыртқы интрузияны анықтау жүйелеріне ақпаратты жібереді. Вулвер модульдер тізімі Amun басталған кезде жүктелетін барлық осалдық модульдерін қамтиды. Төменде конфигурация файлының бөлігі көрсетіледі, ол қайсы осалдық модульдерін жүктеу керектігін және қандай модуль модульдердің әрқайсысына байланысты екенін көрсетеді.

```
[...]
### define the vulnerability modules to load
### (can be changed while running)
vuln_modules:
vuln-ms08067,
vuln-netdde,
vuln-ms06040,
vuln-ms06070,
[...]
vuln-helix,
vuln-hpopenview
### define ports for vulnerability modules
### (can be changed while running)
vuln-ms08067: 445
vuln-netdde: 139
vuln-ms06040: 139,445
vuln-ms06070: 445
[...]
```

Ақырында, конфигурация файлы бірнеше параметрлерді қамтиды, олар сирек конфигурациялануы керек, атап айтқанда: honeypot pingable, жаңа vulns тексеру, шығу curr сокеты, жергілікті жүктеулерді тіркеу және егжей-тегжейлі журнал. Бірінші параметр барлық келіп түсетін пинг сұрауларын блоктайтын iptables ережесін баптауға мүмкіндік береді. Бұл параметрдің мақсаты – Microsoft Windows жүйесін орнату кезінде, мысалы, әдетте, ICMP эхо-сұрауларын бұғаттайды. Екінші параметр Amun кез-келген өзгерістерге конфигурация файлын қайта қарап шықпас бұрын өтетін секундтар санын көрсетеді. Үшінші нұсқа - тек ретке келтіру мақсаттары. Amun орнатылса конфигурация файлын оқыған сайын Amun түбірлік каталогындағы файлға барлық қосылған хосттардың тізімін жазады. Төртінші параметр жергілікті IP мекенжайларын қамтитын жүктеу URL мекенжайларын тіркеуге мүмкіндік береді, ал соңғы параметр honeypot барлық бөліктері үшін егжей-тегжейлі журнал жүргізуді қамтамасыз етеді. Әдетте бұл опцияларды ретке келтіру үшін қажет, сондықтан олар әдепкі бойынша ажыратылған [11].

2.3.2 Тапсырыс берушіге сұрау

Сұрау өңдегіші барлық кіріс және шығыс желілік honeypot трафигіне жауап береді. Amun ядросына жететін әр қосылым сұрауы үшін, байланыс жабылғанға дейін өңделетін сұрауды өңдеуші жасалады. Сұрау өңдегіші жүктелген осалдық модульдерінің тізімін сақтайды және ағымдағы портқа тіркелген модульдерге кіріс трафигін жібереді. 445 порты арқылы келетін қосылысты қарастырыңыз, егер бұл жаңа қосылым сұрау процессорымен өңделсе 445 порты бойынша осалдықтардың жиілігін тексеру үшін 445 портына арналған барлық осалдық модульдерін жүктейді. Әлсіз модульдердің әрқайсысы кіретін трафик эмуляцияланған қызметке сәйкестігін тексереді және қосылымды қабылдаса немесе қабылдамаса қайтаратын болады. Нәтижесінде, әрбір кіретін шабуылдаушының өтінішіне қосылуға арналған эмуляцияланған осалдықтардың тізімі азаяды. Нашар жағдайда, тіркелген модульдердің ешқайсысы шабуыл үлгісіне сәйкес келмейді және байланыс жабық. Әйтпесе, шабуылдаушы жасаған барлық қажетті әрекеттерді сәтті эмуляциялайтын және зиянды бағдарламаның жүктелуі туралы ақпаратты қамтитын соңғы жүктемеге ие модуль қалады. Кіретін желілік пакеттер барлық тіркелген осалдық модульдеріне таратылуына назар аударыңыз, бірақ тек бір жауап жіберілуі мүмкін. Ең жақсы жағдайда, бірінші пакетті алғаннан кейін жауап үшін тек бір модуль қалуы керек, алайда көп болса, тізімдегі бірінші модульдің жауабы таңдалады [12].

2.3.3 Осалдық модульдері

Зиянды модульдер зиянды бағдарламалардың дербес бөлінуіне әсер ететін эмуляция қызметтері болып табылады. Әрбір модуль FTP сервері сияқты жеке қызметті білдіреді. Қызметтер белгілі бір эксплуатацияны іске қосу үшін қажетті деңгейде ғана эмуляцияланады. Бұл эмуляцияланған қызметтерді үнемі пайдаланыла алмайды дегенді білдіреді, яғни олар түпнұсқалық қызметтің толық функционалдығын ұсынбайды. Зияндылық ақырғы автомат ретінде жүзеге асырылады. Әдетте олар бірнеше кезеңнен тұрады, олар эмуляцияланған қызмет арқылы өтеді. «Эксплуатация» деген сөзге сәйкес келетін соңғы мемлекеттік аппарат үлгісі көрсетілген. Бұл әрбір келушіге кіретін желілік пакет мемлекеттік аппараттың келесі күйіне салыстырылады. Егер ол сәйкес келсе, осалдық модулінің күйі келесі кезеңге ауысады, әйтпесе осалдық модулі кіріс сұрауды қабылдамайды. Осылайша, Amun тек эмуляцияланған қызметті пайдалануға әкелетін сұранымдар ғана қабылданады. Белгісіз күйге әкелетін барлық деректер сұрау өңдегіші арқылы жазылады. Бұл ақпаратпен эксплуат әдістеріндегі өзгерістерді анықтауға, жаңа қадамдар жасауға немесе жаңа осалдық модульдерін жасауға болады. Жаңа осалдық модульдерін жазу үрдісін жеңілдету үшін, Amun модульді сипаттау үшін XML-ді қолдайды. Бұл XML файлы кейіннен Amun Python кодын түрлендіреді және одан кейін осалдық модулі ретінде пайдаланылуы мүмкін. Бұл қарапайым осалдық модульдерінде Python кодын жазудың қажеті жоқ дегенді білдіреді. 6-суретте Plug and Play осалдығын (PNP) жасау үшін

қажетті параметрлерді білдіретін XML құжатынан мысал көрсетілген. Ол эксплоитты іске қосу үшін талап етілетін сатылардың санын және әр кезеңде байттардың тиісті сценарийімен () байттың күтілетін санын () көрсетеді. Алтыншы кезеңнен кейін модуль қабық кодын жинау сатысына енеді, яғни, осы кезеңде эксплуат болуы керек, ал шабуылшы қабық кодын жібереді. Қабық кодын жинау сатысында жиналған барлық деректер сұрау өңдегішке, содан кейін қабық кодын талдаушыға жіберіледі. XML файлын қажет ететін Python кодын айналдыру үшін, vuln creator.py деп аталатын шағын сценарий бар. Пайдалану келесідей: python vuln creator.py -f filename.xml. Сайып келгенде бұл атаумен екі жаңа файл жасайды: файлдың аты modul.py және shellcodes.py файл атауы. Бірінші файл әртүрлі қадамдар мен жауаптармен нақты эмуляцияланған қызметті қамтиды. Екінші файл қосымша болып табылады және 6-суретте көрсетілген үлгі XML файлының бірінші кезеңінде анықталған сұрау сияқты жаңа кезеңге өтуге қажетті белгілі бір сұрауды қамтуы мүмкін. Соңғы Python модулі осалдығы коды бірнеше түрлі функциялардан тұрады. Бірінші функция модульді инициализациялауға арналған, осында осалдықтың атауы, бастапқы кезең және сәлемдесу хабары анықталған. Құттықтау хабары, мысалы, шабуылдаушы қосылған кезде аттың және нұсқаның атауы баннеры бар. Осалдық модулінің негізгі функциясы кіріс деп аталады. Бұл функция желі бумасын, осы буманың байттар саны, шабуылдаушының IP-мекен-жайы, тіркеу модулі, бұрын құрылған кездейсоқ жауап және адрес IP-мекен-жайын алады. 8-суретте бұрын сипатталған XML файлын пайдалану арқылы жасалған осалдылық модуліне кіретін функцияның бөліктері көрсетілген. Кіріс функциясының бірінші бөлігінде жаңа жауап көрсетілген [13].

```
<Vulnerability>
<Init>
<Name>PNP</Name>
<Stages>6</Stages>
<WelcomeMess></WelcomeMess>
<Ports>
<Port>445</Port>
</Ports>
<DefaultReply>random</DefaultReply>
</Init>
<Stages>
<Stage stage="1">
<ReadBytes>137</ReadBytes>
<Reply position="9">\x00</Reply>
<Request>\x00\x00\x00\x85\xFF\x53\x4D\x42
\x72\x00\x00\x00\x00\x18\x53\xC8
\x00\x00\x00\x00\x00\x00\x00\x00
\x00\x00\x00\x00\x00\x00\xFF\xFE
```

\x00\x00\x00\x00\x00\x62\x00\x02
\x50\x43\x20\x4E\x45\x54\x57\x4F
\x52\x4B\x20\x50\x52\x4F\x47\x52
\x41\x4D\x20\x31\x2E\x30\x00\x02
\x4C\x41\x4E\x4D\x41\x4E\x31\x2E
\x30\x00\x02\x57\x69\x6E\x64\x6F
\x77\x73\x20\x66\x6F\x72\x20\x57
\x6F\x72\x6B\x67\x72\x6F\x75\x70
\x73\x20\x33\x2E\x31\x61\x00\x02
\x4C\x4D\x31\x2E\x32\x58\x30\x30
\x32\x00\x02\x4C\x41\x4E\x4D\x41
\x4E\x32\x2E\x31\x00\x02\x4E\x54
\x20\x4C\x4D\x20\x30\x2E\x31\x32
\x00</Request>
</Stage>
<Stage stage="2">
<ReadBytes>168</ReadBytes>
<Reply position="9">\x00</Reply>
<Request> [...] </Request>
</Stage>
<Stage stage="3">
<ReadBytes>222</ReadBytes>
<Reply position="9">\x00</Reply>
<Request> [...] </Request>
</Stage>
[...]
<Stage stage="5">
<ReadBytes>106</ReadBytes>
<Reply position="9">\x00</Reply>
<Request> [...] </Request>
</Stage>
<Stage stage="6">
<ReadBytes>160</ReadBytes>
<Reply position="9">\x00</Reply>
<Request> [...] </Request>
</Stage>
</Stages>
</Vulnerability>

2.3.4 Shellcode анализаторы

Егер осалдық модулі зиянкестер эксплуат кодын жібермес бұрын қызметті сәтті шығарса, барлық кіріс деректері жазылып, соңында Shellcode Analyzer-ге ауысады. Shellcode Analyzer - бұл Amun негізі, себебі ол қабық кодын тану және декодтау үшін жауап береді. Shellcode қабықтың белгілі

бөліктеріне сәйкес келетін бірнеше тұрақты өрнектерді пайдалану арқылы танылады. Көптеген жағдайларда бұл декодердің бөлігі, ол түпнұсқаға қайтарылған қабық кодын декодталған кішкентай цикл. 9-сурет нақты снарядтың декодтау бөлігіне сәйкес келетін тұрақты өрнек үлгісін көрсетеді. Шығарылған төрт бөлек байт пайдалы жүктемені декодтау үшін пайдаланылатын кілтті құрайды.

Айқын мәтінді және кодталған (қапталған) қабық кодын ажырата аласыз. Shell кодын бұзу көбінесе бір байтты (қарапайым XOR) немесе төрт байтты (көпбір XOR) немесе алфавиттік-сандық кодтауды пайдалану арқылы XOR операторы арқылы қол жеткізіледі. Shellcode-тің ашық мәтіні оның мазмұнын жасырудың ешқандай әдісін ұсынбайды, сондықтан ол жай ғана http://192.168.0.1/x.exe сияқты URL мекенжайын қамтиды. Сондықтан, Shellcode Analyzer бағдарламасының алғашқы қадамдарының бірі шабуылдаушы біздің эмулирленген осалдықтарымызға қосылған пайдалы жүктеме ішіндегі шифрланбаған URL-мекен-жайларын тексеру болып табылады. Қарапайым XOR кодтауы қабықтың бір байтты пайдаланып кодталғанын білдіреді. Нақты шелл-коды жәбірленушінің хостында орындалмас бұрын декодталған болуы керек, сондықтан бұл қабықшаның бірінші түрі декодер бөлігі деп аталады. Декодер бөлімі пайдалы жүктеменің қалған бөлігіне қатысты тиісті байтпен XOR операциясын орындайтын цикл. Shellcode Analyzer-де декодердің осы бөліктеріне сәйкес келетін және қажетті XOR байтын шығаратын бірнеше тұрақты өрнектер бар. Келесі қадамда, қабық коды декодталған және сығындылары шығарылады. Нұсқаулар нақты жүктеу портының адресін ашуға немесе шабуылға кері байланыс орнатуға және қабықшаны жасауға арналған қарапайым жүктеу URL немесе пәрмендері болуы мүмкін. XOR-тің көп деңгейлі нұсқасы өте ұқсас, бірақ қабық-кодты кодтау үшін бірнеше байтты пайдаланады. 10-суретте декоратордың көп бөліктен тұратын XOR кодталған қабықшасы үшін бөліктері көрсетілген. Ассемблердің бұл бөлімі қабықтың қалған бөлігіне дейін орындалады және біріншіден орындалады. XOR кілті - 0x9432bf80.

```
[...]
000001F9 EB19 jmp short 0x214
000001FB 5E pop esi
000001FC 31C9 xor ecx,ecx
000001FE 81E989FFFFFF sub ecx,0xffffff89
00000204 813680BF3294 xor dword [esi],0x9432bf80
0000020A 81EEFCFFFFFF sub esi,0xfffffffc
00000210 E2F2 loop 0x204
[...]
```

Shellcode-тің алфавитті-сандық кодтауы сәл өзгеше, себебі оның мақсаты тек презентация үшін әріптік-сандық таңбаларды пайдалану болып табылады. Мұндай дайындалған сандық кодты қолданудың себебі көптеген жаңа қосымшалар мен интрузияны анықтау тетіктері ерекше таңбаларды

сүзгілеуі болып табылады, сондықтан 0-9 және АЖ сияқты таңбаларды ғана қолданып, табуды айтарлықтай азайтады және табысқа ықтималдығын арттырады. Талдаған пайдалы жүктеме кез келген тұрақты өрнектермен танылмаса, деректерді қамтитын файл қатты дискіге жазылады. Қабық кодын табу үшін жаңа тұрақты өрнектерді біріктіру үшін оны қолмен талдауға болады [14].

```
cmd /c
net stop SharedAccess &
echo open 192.168.1.3 60810 >> tj &
echo user d3m0n3 d4rk3v1l >> tj &
echo get sr.exe >> tj &
echo bye >> tj &
ftp -n -v -s:tj &
del tj &
sr.exe &
net start SharedAccess
```

2.3.5 Тіркеу модульдері

Журнал жүргізу модульдері эксплуатация орын алған кезде әртүрлі хабарландыруларды жасаудың жеңіл әдісін ұсынады. Қазіргі уақытта Amun бес модульді ұсынады: log-syslog, log-mail, log-mysql, log-surfnet және log-blastomat. Соңғы тіркеу модулі RWTH Aachen Blasto-Mat атымен әзірленген интрузияны анықтау жүйесіне (IDS) қатысты болып келеді. IDS желілік шабуылдарды анықтау үшін honeypots-тарды интрузивті сенсорлар ретінде пайдаланады. Log-syslog модулі кіріс шабуылдар туралы барлық ақпаратты жергілікті Syslog қызметіне жібереді. Сонымен, шабуыл туралы қашықтағы машиналарға, мысалы, орталық тіркеу серверіне жіберуге болады. Тағы бір тәсілі – пайдаланушылық ақпаратты алдын ала анықталған электрондық пошта мекенжайына жіберетін лог-пошта модулін пайдалану. Шабуылдардың санына байланысты, пошта серверін жүктеу үшін көптеген электрондық пошта хабарлары жасалуы мүмкін екенін ескеріңіз. Бұны болдырмау үшін конфигурация файлын бұғаттау параметрлерін конфигурация бөлімінде сипатталғандай пайдалануға болады. Log-mysql модулі MySQL дерекқорындағы шабуылдар туралы ақпаратты жазуға мүмкіндік береді. Дерекқордың орналасуы Amun конфигурация каталогында сақталады. Алайда бұл модуль әлі күнге дейін өңделуде. Log-surfnet модулі Amun-ге SURFids деп аталатын серфингге арналған IDS жүйесіне қосылу мүмкіндігін береді. SURFids-honeypots секілді пассивті сенсорларға негізделген ашық көзден бөлінген кіруді анықтау жүйесі. SURFids PostgreSQL-ты негізгі дерекқор ретінде пайдаланады. Тіркеу модульдері оқиғаларды тіркеу үшін үш негізгі функцияларды қолдайды: initialConnection, incoming және successfullSubmission. Алғашқы функция хосттың honeypots-қа қосылуын сұраған кезде басталады. Бұл сұрау қазіргі уақытта зиянды болмауы керек.

Екінші функция эксплуатация анықталғаннан кейін және кейбір жүктеу әдісі ұсынылғаннан кейін шақырылады. Соңғы функция бинарлық файл сәтті жүктелген кезде аталады, сондықтан бұл функция бұрын сипатталған презентация модулінің кіріс функциясы сияқты бірдей параметрді қабылдайды.

```
import psyco ; psyco.full()
from psyco.classes import *
import time
import amun_logging
import amun_config_parser
import psycopg2
class log:
def __init__(self):
try:
self.log_name = "Log MODUL"
conffile = "conf/log-MODUL.conf"
config = amun_cfg_parser.ConfigParser(conffile)
self.sensorIP = config.getSingleValue("sensorIP")
[...]
except KeyboardInterrupt:
raise
def initialConnection(self, attackIP, attackPort, \
victimIP, victimPort, identifier, \
initialConnectionsDict, loLogger):
[...]
def incoming(self, attackIP, attackPort, victimIP, \
victimPort, vulnName, timestamp, \
downloadMethod, loLogger, attackerID, \
shellcodeName):
[...]
def successfullSubmission(self, attIP, attaPort, \
victimIP, downloadURL, md5hash, data, \
filelength, downMethod, loLogger, \
vulnName, fexists):
[...]
```

2.3.6 Шектеулер

Қарапайым өзара әрекеттесу серверлеріне арналған төлемдер заманауи интрузияны анықтау механизміне қосымша болып табылады, бірақ оларда кейбір шектеулер де бар. Жалпы өзара әрекеттесудің төмен деңгейі бар алдамшылар үшін ең айқын шектеу-нөлдік күн шабуылдардың жетіспеушілігінің болмауы. Мұның себебі – біз өзіміз білетін осалдықтарды ғана көре аламыз, сондықтан бұл тәсіл әрқашан артта қалды. Сол шектеу қабық-кодты пайдалану үшін қолданылады. Одан кейін, осал қызметтер әр

функциямен толықтай имитацияланбайды, бірақ тек эксплуатацияны іске қосу үшін қажет бөліктермен ғана. Нәтижесінде, төменгі өзара әрекеттесуші төлемдер кез келген зиянкесін алдай алмайды, бірақ бірінші кезекте қызметтің функционалдығын тексермейтін зиянды бағдарламаларды ғана таратады. Мұндай чектерді оңай қосуға болатынына қарамастан, қазіргі кездегі зиянды бағдарламалық жасақтама өте нашар жазылған. Сервердің жауабы тіпті тексерілмеген және зиянды бағдарлама қызмет көрсетудің әлсіз болғанына қарамастан, оның қабықшасын жіберді [15].

3 Техникалық-экономикалық бөлім

3.1 Honeypot бағдарламалық жасақтамасын қорғауды жобалаудың күрделілігін анықтау

Honeypot бағдарламалық жасақтамасын қорғауды жобалаудың күрделілігін дәл анықтау үшін бүкіл тапсырманы қарапайым кезеңдерге бөлу қажет. БӨ талдаудың күрделілігін үлестіру үлгісі 3.1-кестеде келтірілген.

Кесте 3.1 – Honeypot бағдарламалық жасақтамасын қорғауды жобалау кезеңдері

Жоба кезеңдері	Жұмыс түрі	Еңбек қарқындылығы, адам сағ.
1 кезең	Жабдықты таңдау	24
2 кезең	Ықтимал шабуылдарды талдау	15
3 кезең	Сыртқы трафик бойынша талдау	8
4 кезең	Жергілікті есептеу желісінің трафигінің инфрақұрылымы жобасын әзірлеу	30
5 кезең	Сыртқы трафикті басқару жобасын әзірлеу	10
6 кезең	HoneyPot-ты конфигурациялау және орнату	30
7 кезең	Тестілеу	20
8 кезең	Деректерді жинау	35
9 кезең	Жақсарту	24
Қорытынды: дипломдық жобаны орындаудың еңбек қарқындылығы		186

Жұмыс күнінің ұзақтығы - 8 сағат. Нәтижесінде бағдарламалық өнімді іске асыру үшін 23 жұмыс күні қажет.

3.2 Honeypot бағдарламалық жасақтаманы қорғауды жобалау шығынын есептеу

Honeypot бағдарламалық жасақтаманы қорғауды жобалау шығынын есептеу төмендегі элементтерді қамтитын смета негізінде жүргізіледі:

- материалдық шығындар;
- еңбекақы шығындары;
- әлеуметтік салық;

- негізгі фондтар амортизациясы;
- басқа шығындар.

Кесте 3.2 – Материалдық ресурстарға шығындар

Материал атауы	Марка	Өлшем бірлігі	Саны	Дана бағасы теңгемен	Сомасы теңгемен
Кеңсе қағазы	SvetoCopy	Қаптама	1	1 500,00	1 500,00
Дәптер (96 бет)	Abdi	Дана	5	100,00	500,00
Блокнот	Abdi	Дана	1	1000,00	1000,00
Қаламдар	Abdi	Дана	2	50,00	500,00
Қорытынды					3 500,00

Материалдық шығындар адам тұлғасының белгілері бойынша аутентификация құрылымын жобалау үшін қажетті негізгі және қосалқы материалдарға, энергияға және басқа да шығындарға бөлінеді. Материалдық шығындарды есептеу 3.2-кестеде берілген форма бойынша жүргізіледі.

Honeypot бағдарламалық жасақтамасын қорғауды жобалау үшін SuperChassis 731D-300B CSE-731D-300B сервері қолданылады, сервердің қуаты қойылған міндеттерді орындау үшін жеткілікті. Сервер үшін операциялық жүйені және бағдарламалық жасақтаманы орнату қажет.

Материалдық құралдарға қажетті жалпы соманы мынадай (3.1) формула бойынша есептеуге болады:

$$З_м = \sum P_i * Ц_i, \quad (3.1)$$

мұндағы - материалдық ресурстың і-нші түрінің шығысы, заттай бірліктер;

$Ц_i$ - материалдық ресурстың і-нші түрінің бірлігі үшін баға, тг;

і - материалдық ресурстың түрі;

n - материалдық ресурс түрлерінің саны.

Қажетті жабдықтар мен бағдарламалық қамтамасыз ету шығындарын есептеу 3.3-кестеде келтірілген форма бойынша жүргізіледі.

Кесте 3.3 – Жобаға қажетті жабдықтар мен бағдарламалық жасақтама шығындарын есептеу

Материал атауы	Марка	Өлшем бірлігі	Саны	Дана бағасы теңгемен	Сомасы теңгемен
Сервер	Едендік сервер HP ML30 Gen9/1	Дана	1	342 027,00	342 027,00
Коммутатор	Басқарылмайтын D-link DES-1016D/H1A	Дана	1	11 788,00	11 788,00
Операциялық жүйе	Microsoft Windows Server 2016 R2	Лицензия	1	25 000,00	25 000,00
Honeypot бағдарлама-лық жасақтама	Windows HoneyPot Defender	Лицензия	1	17 600,00	17 600,00
Қорытынды:					396 415,00

$$З_м = 3\ 500 + 396\ 415{,}00 = 399\ 915{,}00 \text{ (тг)}$$

Бет белгілері бойынша аутентификация құрылымын жобалауды жүзеге асыру үшін 399 915,00 теңге сомаға материалдар қажет.

3.3 Электр энергиясына шығындарды есептеу

Honeypot бағдарламалық жасақтамасын қорғауды жобалауды электр энергиясын тұтынусыз жасай алу мүмкін емес болғандықтан, электр қуатының құнын есептеу керек.

3.1-кестеге сәйкес Honeypot бағдарламалық жасақтамасын қорғауды жобалау үшін 318 сағатқа жуық уақыт қажет, енді 318 сағат ішінде жұмсалатын электр энергиясының құнын (3.2) формуламен есептеу қажет.:

$$Э = З_{эл.эн.обор.} + З_{доп.нужды.}, \quad (3.2)$$

мұндағы $З_{эл.эн.жабд.}$– жабдықтың электр энергиясына шығындар;

$З_{қос.қажет.}$ – қосымша қажеттіліктерге электр энергиясының шығындары.

Жабдық үшін қажетті электр энергиясын есептеу (3.3) формула бойынша анықталады:

$$З_{эл.эн.обор.} = \sum W * К_{исц} * S * T, \quad (3.3)$$

мұндағы W – тұтынылатын қуат, Вт;

$К_{пайда}$ – пайдалану коэффициенті (= 0,7 - 0,9);

Т – жұмыс уақыты;

S – тариф (1кВт/сағ. = 23,85тг – «АлматыЭнергоСбыт» ЖШС-тің заңды тұлғаларға арналған тарифі, 01.01.19).

Электр энергиясының құнын есептеу бойынша қорытынды 3.4-кестеде көрсетілген.

Кесте 3.4 – Электр энергиясына шығындар

Құралдар атауы	Паспорттық қуаты, кВт	Қуат коэффициенті	Жабдықтың жұмыс уақыты, сағ	ЭЭ бағасы тг/кВтсағ	Сомма, тг.
Сервер	0,75	0,9	186	23,85	2994,36
Honeypot бағдарламалық жасақтамасы	0,45	0,9	186	23,85	1796,62
Коммутатор	0,320	0,7	186	23,85	993,68
Жарықтандыру	0,2	0,7	186	23,85	621,05
Қорытынды:					6405,71

$$З_{эл.эн.обор.} = 6405,71(\text{тенге})$$

Қосымша қажеттіліктерге шығыстар электр энергиясына шығыстардың 5% көлемінде жоғары көрсеткіш негізінде есептеледі:

$$З_{доп.нужды} = 5\% * З_{эл.эн.обор.} \quad (3.4)$$

Қосымша қажеттіліктерге шығыстар электр энергиясына шығыстарды мына (3.4) формулаға сәйкес анытаймыз

$$З_{доп.нужды} = 0.05 * 6405,71 = 320,28 \text{ (тенге)}$$

Барлық есептеулерге сүйене отырып, электр энергиясына толық шығындар құрайды:

$$Э = 320,28 + 6405,71 = 6725,99 \text{ (тенге)}$$

3.4 Еңбекақы шығындарын есептеу

Honeypot бағдарламалық жасақтамасын қорғауды жобалау үшін үш қызметкер қажет:

- жоба жетекшісі – жұмыс уақытын басқару, жұмыс процестерін түзету, үйлестіру, пәндік облысты зерттеу;
- желілік әкімші-желілік трафиктің қол жетімділігін және оның өзгермейтіндігін қамтамасыз ету;
- БҚ әкімшісі – белгілі бір пайдалану уақытында бағдарламалық қамтамасыз етудің дұрыс жұмысына жауапты адам. Кейінгі есептерді анықтау және қателерді әдейі іздеу.

Еңбекақы төлеу шығындарының сомасын келесі (3.5) формула бойынша есептеуге болады:

$$З_{тр} = \sum ЧС_i * T_i \quad (3.5)$$

мұндағы, $ЧС_i$ – і-ші қызметкердің сағаттық мөлшерлемесі, тг;

T_i – модельді әзірлеудің еңбек сыйымдылығы, адам.×сағ;

і – қызметкердің санаты;

n – БӨ әзірлеумен айналысатын қызметкерлердің саны.

Жобаны іске асыру кезінде қатысушылардың жұмыс уақыты біркелкі емес, сондықтан әр қызметкердің сағаттық мөлшерлемесін және жалпы жалақыны белгілеу маңызды.

Қызметкердің сағаттық мөлшерлемесі келесі формула бойынша есептеледі:

$$ЧС_i = \frac{ЗП_i}{ФРВ_i} \quad (3.6)$$

мұнда, $ЗП_i$ – і қызметкердің айлық жалақысы, тг;

$ФРВ_i$ – і қызметкердің айлық жұмыс уақытының қоры, сағ.

Жетекшінің айлық жалақысы 200 000 теңгеге тең және желілік администратордікі 170 000 теңгеге тең, ал инженер администратор 150 000 теңгеге жалақы алады. Әрбір қызметкердің сағаттық мөлшерлемесін (3.6) формулаға сәйкес есептейміз:

$$ЧС_{руководитель} = \frac{200\,000}{22 * 8} = 1136 \text{ тг/сағ}$$

$$ЧС_{инж.адм} = \frac{150\,000}{22 * 8} = 852 \text{ тг/сағ}$$

$$ЧС_{сет.админ} = \frac{170\,000}{22 * 8} = 965 \text{ тг/сағ}$$

Жоба жетекшісінің сағаттық мөлшерлемесі 1136 (тг/сағ) құрайды, әзірлеудің еңбек сыйымдылығы 100 сағатқа тең. Серверлік әкімшінің сағаттық ставкасы 852 (тг/сағ) құрайды, жобалаудың және іске асырудың еңбек сыйымдылығы 200 сағатқа тең. Желілік әкімшінің сағаттық мөлшерлемесі тең 965 (тг/сағ). (3.5) формулаға сәйкес қызметкерлердің еңбекақысына кететін шығындар сомасын есептеуге болады:

$$З_{ең} = 1136 * 170 + 852 * 186 + 965 * 186 = 531\ 082{,}00 \text{ (тенге)}$$

Еңбекақы төлеуге кететін шығындарды есептеу 3.5-кестеде көрсетілген.

Кесте 3.5 – Еңбекақы шығындарын есептеу

Қызметкердің санаты	Біліктілік	БӨ әзірлеудің еңбек сыйымдылығы, сағ.	Сағат мөлшерлемесі, тг/сағ.	Сомма, тг.
Жетекші	Жоба жетекшісі	170	1136	193 120,00
Инженер әкімші	Ақпараттық технологиялар бойынша сертификат	186	852	158 472,00
Желілік әкімші	Cisco сертификациясы	186	965	179 490,00
Қорытынды:				531 082,00

3.5 Әлеуметтік салық бойынша шығындарды есептеу

Қазақстан Республикасының Салық кодексіне сәйкес әлеуметтік салық еңбекақы төлеу қорының 9,5%-ын құрайды. Әлеуметтік салықты келесі (3.7) формула бойынша есептеуге болады:

$$С_н = (ФОТ - ПО) * 0{,}095 \qquad (3.7)$$

мұнда, ПО – зейнетақы қорына аударымдар, олар ФОТ 10% құрайды.

$$ПО = 531\ 08200 * 0{,}1 = 531\ 08{,}00 \text{ тенге}$$

$$С_н = (531\ 082{,}00 - 531\ 08{,}00\ ) * 0{,}095 = 45\ 407{,}53 \text{ тенге}$$

Есептеу нәтижелері 3.6-кестеде көрсетілген.

Кесте 3.6 – Әлеуметтік салықты есептеу

Қызметкердің санаты	Саны	Жалақы, тг	Зейнетақы аударымы, тг	Әлеуметтік салық, тг
Жетекші	1	193 120,00	193 12,00	16 511,76
Желілік әкімші	1	158 472,00	158 47,20	13 549,35
Honeypot бағдарламалық жасақтамасы-ның әкімшісі	1	179 490,00	179 49,00	15 346,39
Қорытынды:				45 407,50

3.6 Негізгі қорлардың амортизациясы және өзге де шығындар

НҚ-дың амортизациясы нормаларын ҚР салық кодексіне сәйкес анықтау керек. НҚ-дың амортизациясы келесі формуламен анықталады:

$$A_{\text{г}} = \frac{\text{С}_{\text{об}} * \text{Н}_{\text{а}}}{100} \quad (3.8)$$

мұнда, $\text{С}_{\text{об}}$ – жабдықтың құны;

$\text{Н}_{\text{а}}$ – амортизация нормасы (амортизация нормасы = 25);

3.8-формула сервер үшін бір жыл ішінде амортизациялық аударымдар үшін қажетті соманы есептеуге мүмкіндік береді:

$$A_{\text{г}} = \frac{396\,415{,}00 * 25}{100} = 99\,103{,}75 \text{ тенге}$$

Енді жобалау кезеңінде амортизация нормасын есептеу қажет:

$$A_{\text{г}} = \frac{99\,103{,}75 * 23}{365} = 6\,244{,}89 \text{ теңге}$$

Осылайша, барлық жабдық үшін амортизация нормасын есептеу қажет. Есептеу нәтижелері 3.7-кестеде келтірілген.

Кесте 3.7 – НҚ амортизациясы

Жабдық пен БЖ атауы	Жабдық пен БЖ бағасы, тг	Жылдық амортизация нормасы,%	Жылдық амортизация сомасы, тг	Әзірлеу уақытындағы амортизация сомасы, тг
Сервер	342 027,00	25	85 506,75	21 552,38
Коммутатор	11 788,00	20	2357,60	742,80

3.7-кестенің жалғасы

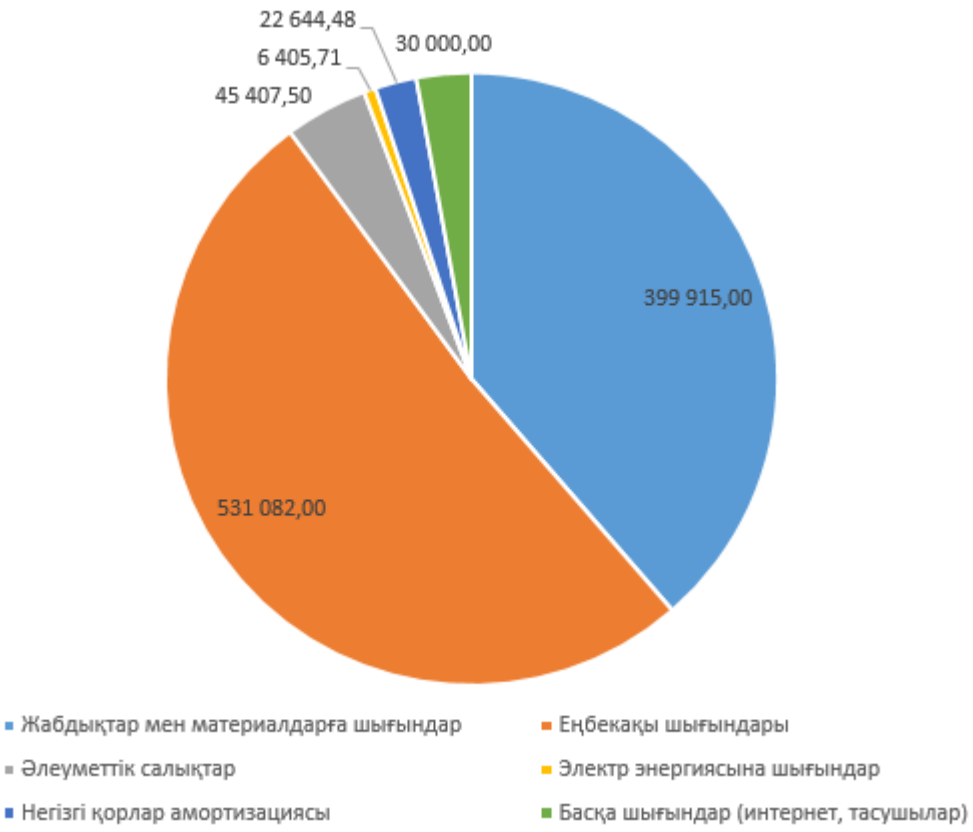
Операциялық жүйе	25 000,00	15	3 750,00	349,30
Honeypot БЖ	17 600,00	20	3520,00	1109,04
Қортынды:				22644,48

Адамның бет белгілері бойынша аутентификация құрылымын жобалауға арналған шығындар сметасы.

Барлық ұсынылған есептеулер негізінде 3.8-кестеде келтірілген формаға сәйкес адамның бет белгілері бойынша аутентификация құрылымын жобалауға арналған шығындар сметасын ресімдеу қажет. 3.1-суретте жұмыс шығындарының диаграммасы көрсетілген.

Кесте 3.8 – БӨ әзірлеуге шығындар сметасы

Шығындар	Сомма, тг
Жабдықтар мен материалдарға шығындар	399 915,00
Еңбекақы шығындары	531 082,00
Әлеуметтік салықтар	45 407,50
Электр энергиясына шығындар	6 405,71
Негізгі қорлар амортизациясы	22 644,48
Басқа шығындар (интернет, тасушылар)	30 000,00
Смета бойынша қортынды:	1 005 454,69



Сурет 3.1 – Шығындар диаграммасы

3.7 Жобалаудың ықтимал бағасын анықтау

Бағдарламалық жасақтаманың құны әзірленген өнімнің сапасы, оны әзірлеу мерзімі және өнімнің өнімділігі негізінде анықталады. Бағдарламалық жасақтаманың құнын келесі (3.9) формула бойынша есептеуге болады:

$$Ц_Д = З_{нир}\left(1 + \frac{P}{100}\right), \quad (3.9)$$

мұндағы – бағдарламалық жасақтаманы әзірлеуге шығындар, тг;

Р – БЖ рентабельділігінің орташа деңгейі (%). Бұл параметр 25% деп алынған.

$$Ц_Д = 1\,005\,454{,}69\left(1 + \frac{25}{100}\right) = 1\,256\,818{,}36 \text{ тенге}$$

Бұдан әрі ҚҚС есебімен сату құнын анықтау қажет, ҚҚС ставкасы ҚР заңнамасымен белгіленеді. 2019 жылға ҚҚС ставкасы 12% құрайды. Іске асыру құны ҚҚС-ты ескере отырып мынадай (3.10) формула бойынша есептеуге болады:

$$Ц_р = Ц_д + Ц_д * НДС, \quad (3.10)$$

Осылайша, ҚҚС есебімен сатудың шартты бағасы 1 407 636,56 теңгеге тең. Бағдарламалық өнімнің құны 1 256 818,36 теңгеге тең. Пайда теңгеге тең.

4 Өмір тіршілік қауіпсіздігі

4.1 Еңбек жағдайларын талдау

Дипломдық жұмыста мен Honeypot бағдарламалық жасақтамасы арқылы зерттеу жүргіземін.Бас директордың, бухгалтерлік есептің, сату жөніндегі менеджерлердің кеңсесін дұрыс жабдықтау қаншалықты маңызды? Ең жақсы еңбек жағдайлары қызметкерлердің жоғары нәтижелілігінің кілті болып табылады және нәтижесінде компания үшін жоғары пайда болады. Әрине, табыстылыққа ықпал ететін факторлар әлдеқайда көп, бірақ компанияның ең құнды ресурсы, ақпаратының негізгі кастодианы - аппараттық бөлме, бұл серверлік бөлме. Мемлекеттік ұйымдар мен өндірістік компаниялардың әзірлеген қолданыстағы нормативтік базасына сүйене отырып, мынадай талаптар (ұсынымдар) жасалды. Ғимарат бөлмелерін таңдау, бөлме аумағының көлемі және оның жабдықтары өте маңызды. Компанияның жинақталған ақпаратын «багажды» бұзу қаупі дәрежесі жабдықтың барлық нұсқаулықтары мен стандарттарына қаншалықты дұрыс жауап беретініне байланысты. Үшінші тұлғалардың шағын ағуы немесе араласуы қалпына келтірілмейтін зақым келтіруі мүмкін және сіздің бизнесіңіздің тиімділігін қалпына келтіру үшін күтпеген шығындарға әкелуі мүмкін.

Жабдық - ғимаратта қолданатын телекоммуникация немесе серверлік жабдықпен қамтылған бөлме. Көбінесе аппараттық құрал - бұл арнайы бөлме. Жабдықтар магистральдармен байланысады және әдетте ғимаратқа қызмет көрсету құралдары ретінде қарастырылады.

Бөлмедегі жабдық:

- жабдық бөлмелерінің ең аз рұқсат етілген көлемі - 14 м²;
- жабдық бөлмесінің өлшемдері онда орналасқан жабдыққа қойылатын талаптарға сәйкес болуы керек немесе (деректер болмаған кезде) қызмет көрсетілетін әрбір 10 м² жұмыс орны үшін 0,07 м² болуы тиіс;
- жұмыс орындарының тығыздығы төмен ғимараттарда жабдықтың ауданы кемінде 37 км² - 400 жұмыс орнынан кем емес, кемінде 74 м² - 800-ден көп емес және кемінде 111 м² - 1200-ден астам жұмыс орны болмауы тиіс;
- аппараттың ең төменгі төбенің биіктігі 2,44 м болуы тиіс;
- жабдықтар бөлмесіндегі едендер, 45.120-2000 РР 45.202-тармағына сәйкес, біркелкі болуы тиіс және 106 Ом кедергісі бар антистатикалық жабынға ие, бұл статикалық электр тогының ағымын және ағынын қамтамасыз етеді. Едендер отқа төзімді негізде жүзеге асырылады. Қаптау шаңсорғыш пен дымқыл тазалауға мүмкіндік береді.

4.2 Электромагниттік сәулелердің адамға әсері

Электромагниттік сәулелердің адам ағзасына неге зиянды екенін анықтайық. Адам ағзасы да электрлік импульстерді шығарады. Олардың көмегімен ми мен жұлынға жүйке үштары арқылы сигналдар келіп түседі, қаңқа бұлшықеті мен жүрек бұлшықеттері азаяды. Жүйке үштары арқылы

секундына мыңдаған сигналдар беріледі, сондықтан компьютерден қандай зиян келетінін оңай түсінуге болады, сәулелер электрлік импульс жіберудің қиын жүйесіне әсер етіп, олардың өзара байланысына бөгет келтіруі мүмкін. Оның әсері бір сәтте сезілмейді,ол ағзада жинақталып, мүшелер мен жүйелердің жұмысын біртіндеп нашарлатады.

Екі маңызды жүйе ең осал болып табылады:

- жүйке жүйесі;
- жүрек – қан тамырлар жүйесі.

Бұның әсерінен ми сигналдары патологиялық түрде өзгеруі мүмкін. Бұл мидың және жүрек-тамыр жүйесі органдарының бұзылуына себеп болады. Жүрек-қантамыр жүйесінің қалыпты жұмыс істеуі импульстердің когеренттігіне және беріктігіне байланысты. Үйдегі бір немесе одан да көп құрылғылар жүрек жұмысын елеулі бұзылуға алып келмейді, бірақ үнемі сәулелену аритмия мен жүрек-тамыр қабілетінің бұзылуына әкелуі мүмкін. Ұзақ уақыт бойы әсер етуі бас ауруы, мигреньдер, иммунитеттің төмендеуі, депрессия, гормоналды теңгерімсіздік және ұйқының бұзылуына әкелуі мүмкін. Компьютерде көп жұмыс істеу Альцгеймер ауруы, Паркинсон ауруы, қатерлі ісік ауруы және ұрпақты болу жүйесінің бұзылу қаупін арттырады. Сонымен қатар миокард және перикард ауруларына, ағзаның жалпы гормональды фонының бұзылуына, су-тұз алмасуының нашарлауына, гомеостаздың бұзылуына алып келуі мүмкін.

Үй компьютері, ноутбук немесе смартфон зиянды сәуле көзі болып табылады. Компьютерден қанша сәуле алатынымыз түрлі факторларға байланысты: құралдың түрі, пайдалану уақыты, орналасуы.

Кондиционер, егер жұмысшы біреудің бөлмесіне ие болса, онда қызметкердің жақсы микроклиматының бір жылын ұстап тұру керек еді, ол жұмыс уақытының барлық ауыртпалығы кезінде жұмыс үшін қажетті бөлмені оңтайлы күйде орналастырады. Үш адам бөлмені шаңнан шығаруды қажет етеді екі зиянды заттарды білдіретін басқа файл. Шабуылдарды орындау үшін бұл аз мөлшерде, үшеуі өте таза, біреуі таза бөлмеде жүргізіледі. Мұның бәрі, қоспағанда, ластаушы ауа арқылы бөлме шабуылының ауырсынуын болдырмауға мүмкіндік береді. Жабдықта болса да, бұл функциялар әуе файлын бөлу туралы ереже бойынша жекелендірілген болса да назарға алынады. Үш қызметкердің бөлмесінде жұмыс істейтін ең төменгі ауа температурасы кемінде 18°С кем емес.

Оңтайлы жағдайлардың кодтарын қалыптастыру үшін бірқатар жұмысшылардың еңбек нормалары осы өндіріс микроклиматының барлық нормалары ретінде анықталады. Дербес компьютердің шабуыл шотымен жұмыс жасағанда, SanPin 2.2.2 / 2.4.1340-03:

Жоғарыда суық мезгілде:

- 22-24 ° С температура файлын қалыпқа келтірді;
- рұқсат етілген ядролар - 18-26 ° С;
- ауаның салыстырмалы ылғалдылығы 40-60%;
- рұқсат етілген желі 75%.

Жылы кезеңде:

- температура 23-25 ° С-ге дейін қалыпты;
- рұқсат етілген дос 20-30 ° С;
- ауаның салыстырмалы ылғалдылығы 40-60%;
- қабырғалардың рұқсат етілген ылғалдылығы 55% құрайды.

Олардың кэшті орналасуы қарастырылған (5.1 суретте) сипаттамалары:

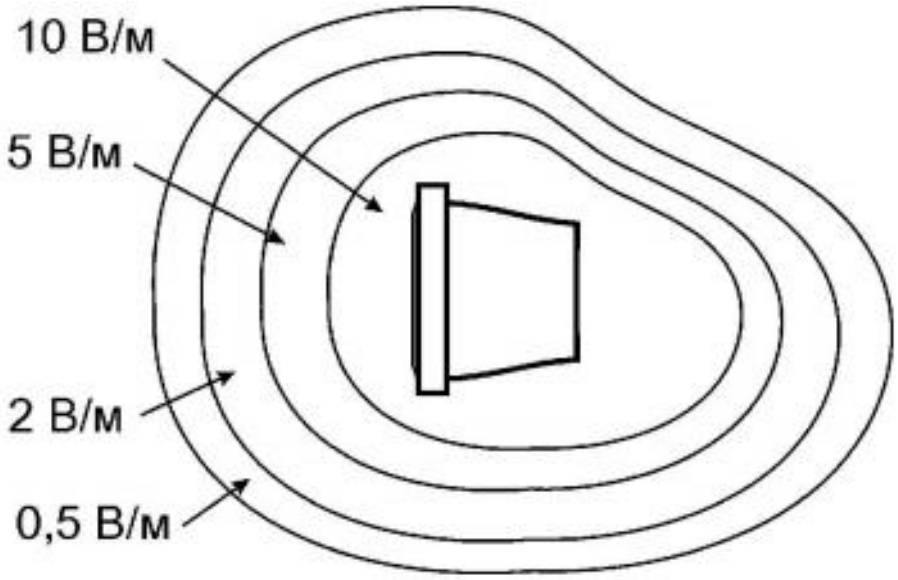
- екі қабатты ғимараттың бірінші қабатында орналасқан;
- бір қызметкердің көлемі бір бөлме: ядро ұзындығы 4 м, ені 3 м, биіктігі 3 м;
- жасанды жарықтандыру - шамдар: әрқайсысында 2 шам;
- әрқайсысының 2 люминесцентті лампасы (PVLM - 1 × 40);
- визуалды жағдайларға ауыр жұмыстардың ауырлығы жоғары IV санатына жатқызу, ең кішкентай нысан нысанды 1-ден 5 мм-ге дейін бөлетіндіктен;
- жұмыс орындарының саны.

4.3 Электромагниттік сәулеленуден қорғау тәсілдері

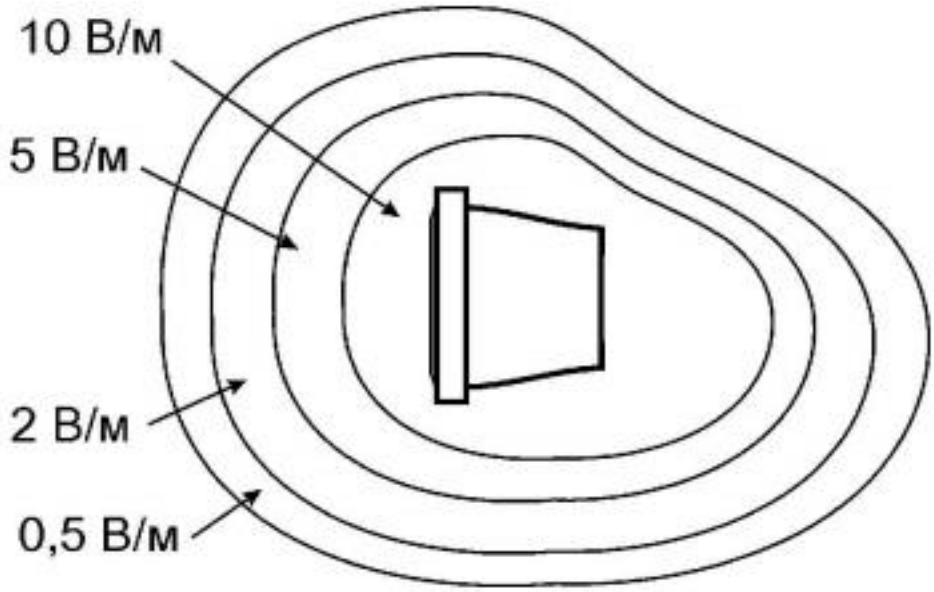
Электромагниттік сәулеленудің жағымсыз әсерінен қорғаудың ең тиімді тәсілдерінің бірі арнайы құралдарды қолдану болып табылады, ол осы сәулеленуді бейтараптандыруға және оның адам ағзасына теріс әсерін барынша азайтуға мүмкіндік береді. Бұл құралдардың жұмыс істеу принципі адам ағзасына жағымсыз электромагниттік сәулеленудің жағымсыз әсерін төмендетуге ықпал ететін қарсы ЭДС-ға негізделген.

Электромагнитті сәулеленудің әсер ету аймағында болу уақытын барынша қысқарту ағзаны электромагнитті сәулеленудің жағымсыз әсерінен қорғаудың ең тиімді тәсілдерінің бірі болып табылады. Бұл мәселе электрмагниттік сәулелену деңгейі ең жоғары электр энергетикалық кәсіпорындардың қызметкерлері үшін ерекше өзекті.

Мысалы, жоғары вольтты тарату қосалқы станциясына қызмет көрсететін персонал. Тарату құрылғыларында, ашық және жабық типті электромагниттік сәулелену деңгейі өте үлкен. 110кВ және одан жоғары электр қондырғыларында электромагниттік сәулелену деңгейі адам ағзасына теріс әсер етуі өте күшті болып табылады. Магниттік өрістің күш сызықтары мен электромагниттік өріс пен дисплей арасындағы күш сызықтарының көріністері сәйкесінше 4.1 және 4.2-суреттерде көрсетілген.



Сурет 4.1 – Магниттік өрістің күш сызықтары



Сурет 4.2 – Электромагниттік өріс пен дисплей арасындағы күш сызықтарының көріністері.

Алғашқы белгілер бірден пайда болады: бас ауруы, әлсіздік, тітіркену, тежелу. Мұндай жағдайларда адамның арнайы қорғаныш жинақтарын (экрандаушы құрылғыларды) пайдаланбай электромагниттік сәулеленудің әрекет ету аймағында болуына жол берілмейді. Қызмет көрсететін персонал жоғары вольтты жабдықтан алыста болған кезде, мысалы, жалпы станциялы басқару пунктінде электромагниттік сәулелену деңгейі әлдеқайда аз, бірақ оның мәні рұқсат етілген мәндерден жүздеген есе асып түседі. Бұл бөлмеде көптеген электромагниттік сәулелену көздері бар: компьютерлік техника,

қорғаныс құрылғылары және жабдықтың автоматикасы, төменвольтті тарату қалқандары және т. б. Мұндай жағдайда, мүмкін болған жағдайда үзіліс жасап, үй-жайдан шығып, сол арқылы электромагниттік сәулелену аймағында болу уақытын қысқартқан жөн.

4.4. Шудың әсері. Акустикалық шуды есептеу

Есептеуде қолданылатын физикалық шамалар:

Дыбыс қысымының деңгейі (4.1) формуламен есептеледі.

$$L = 20 \lg \frac{p}{p_0} \tag{4.1}$$

бұл жерде, p_0 - қысымы $2 \cdot 10^{-5}$ Па тең дыбыс қысымының нөлдік деңгейі;

p – өлшенетін дыбыс қысымы (Па).

Жылдам дыбыс қарқындылығы. Бұл бағытта перпендикуляр беті арқылы белгілі бір бағытта энергияның лездік ағынына тең мән (4.2) формуламен анықталады:

$$\mathrm{I(t)} = \mathrm{pu} \tag{4.2}$$

мұндағы, p – жылдам дыбыстық қысым, Па;

u – бөлшектер нүктесінің жылдамдығы.

Дыбыс қарқындылығы. Уақыт бойынша орташа дыбыс қарқындылығын есептеу (1.3) формулада көрсетілген.

$$\boldsymbol{I} = \lim_{T \to \infty} \frac{1}{T} \int_0^T \boldsymbol{I}(t) dt \tag{4.3}$$

Дыбыс қуаттылығы.Көзден шығарылатын жалпы дыбыс қуаты (4.4) формуламен есептеледі.

$$P = \sum_{i=1}^{N} \boldsymbol{I}_n S_i \tag{4.4}$$

мұндағы, N – өлшеу бетінің сегменттерінің саны;

S_i –i сегмент ауданы.

Дыбыс қуатының деңгейі. Көзі шығаратын дыбыс қуатының логарифмдік өлшемі (1.5) формула негізінде:

$$L_w = 10 \lg P / P_0 \tag{4.5}$$

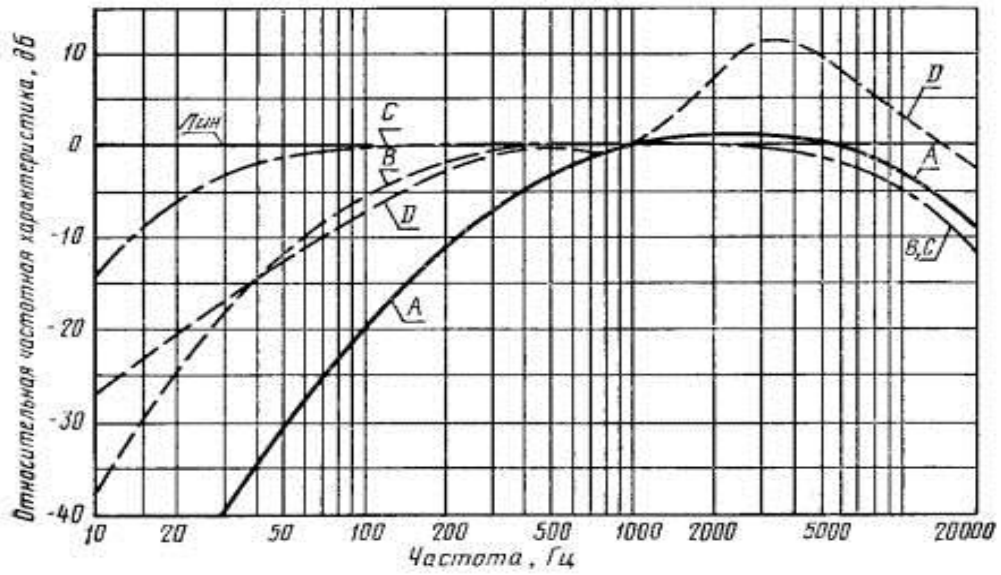
мұндағы, P_0 – қуат шегі 10^{-12} Вт.

Дыбыс қысымының деңгейін кейде аудару үшін (p/p_0), сіз 4.1-кестені пайдалана аласыз.

Дыбыс қысымының түзетілген деңгейлері (дыбыс деңгейлері). А, В, С, Д дыбыс деңгейін өлшеуіштердің 4 халықаралық жиіліктік сипаттамалары (халықаралық жиіліктік түзету сипаттамалары) бар. Шуөлшеуіштің жиілілік характеристикалары 4.1-суретте көрсетілген.

Кесте 4.1 – Қысымға байланысты УЗД өзгерту.

l, дБ	p/p_0	l, дБ	p/p_0
1	1,122	20	10
3	1,413	40	100
6	1,995	60	1000
8	2,512	80	10000
10	3,162	100	100000



Сурет 4.1 – Шуөлшеуіштің жиілілік характеристикалары (ГОСТ 17187-2010. Шу өлшеуіш.Техникалық талаптар)

Шуды қорғаудың тиімділігі ΔL УДЗ-да ультрадыбыстық ультрадыбыспен (L) және одан кейін (L_0) шудан қорғауды қолданудан айырмашылығы ретінде (4.6) формуламен анықталады.

$$\Delta L = L_0 - L_{\text{ш}} \tag{4.6}$$

Бірнеше дереккөзден жобалау нүктесінде (RT) ультрадыбысты (қарқындылықты) қосу (4.7) формуламен жүреді:

$$L_\Sigma = 10 \lg \sum_{i=1}^{N} 10^{L_i/10} \tag{4.7}$$

мұндағы, L_Σ – жалпы дыбыс қысымының деңгейі, дБ, егер олардың әрқайсысы ультрадыбыстық L бар N бірдей көздері бар болса, онда ол (4.8) формулаға түрленеді:

$$L_\Sigma = L + 10 \lg N \tag{4.8}$$

Екі түрлі УЗД қосқанда, жалпы деңгей үлкен мерзімге қоспа ретінде ыңғайлы болуы мүмкін. Ол (4.9) формулада:

$$L_\Sigma = L_{\max} + \Delta \tag{4.9}$$

Қоспаның мәнін арнайы кестеде немесе кесте түрінде табуға болады. Қоспалардың кейбір мәндері 4.2-кестеде келтірілген. Қосылған деңгейлер арасындағы айырмашылық 20 дБ-ден артық болғанда, жалпы ультрадыбыс болады.

Кесте 4.2 – Ультрадыбыстық Δl айырмашылығына байланысты ультрадыбыстық Δ қосудың маңызы.

Δl, дБ	Δ, дБ	Δl, дБ	Δ, дБ
0	3	7	0,8
1	2,5	8	0,6
2	2	9	0,5
3	1,8	10	0,4
4	1,5	15	0,2

Акустикалық есептеу үшін бастапқы деректер:

- технологиялық жабдық пен ТТ орналасатын бөлменің жоспары мен бөлімі;

- бөлмедегі қоршау құрылымдары туралы ақпарат (материал, қалыңдығы, тығыздығы);

- шу сипаттамалары (техникалық құжаттамада көрсетілген L_w дыбыс деңгейінің дыбыс деңгейі), шу көздерінің геометриялық өлшемдері.

Акустикалық есептеу келесі тәртіпте жүргізіледі.

Шу көздерінің салыстырмалы орналасу схемасын және дизайн нүктелерін және бөлмелік акустикалық сипаттамаларын пайдалана отырып, АТ шу көздерінің L_w дыбыс қуатының белгілі деңгейлерінде РТ-де ультрадыбыстық дыбыстарды анықтау.

L_dop шу көрсеткіштерінің стандартты мәндерін пайдалана отырып, жұмыс нүктесінде ΔL_tr қажетті төмендету деңгейін анықтау.

Шу деңгейін азайту қажет болса, шуды қорғау шаралары таңдалады және шуды қажетті мәнге дейін азайту үшін (4.10) формуламен есептеледі.

$$B = \frac{A}{1-\alpha_{\text{ср}}} \tag{4.10}$$

мұндағы, A – формула бойынша анықталған балама дыбыс сіңіру алаңы, м^2 (4.11-формула).

$$A = \sum_{i=1}^{n} \alpha_i S_i + \sum_{j=1}^{m} A_j n_j \tag{4.11}$$

мұндағы, α_i – і-ші бетінің дыбыс сіңіру коэффициенті;

S_i – і-ші бетінің ауданы;

A_i – дыбыс жұтқыштың балама дыбыс жұту аймағы;

n_j - саны, $\alpha_{\text{ср}}$ – орташа дыбыс сіңіру коэффициенті $\alpha_{\text{ср}} = A/S$, мында S – қоршау беттерінің жалпы ауданы, м^2.

Бөлмедегі акустикалық тұрақты және кеңістіктік сәулелену бұрышын негізге ала отырып, r_gr, m (тікелей дыбыстың энергия тығыздығы шағылыстырылған дыбыстың энергия тығыздығына тең) шекара радиусы (4.12) формула бойынша анықталады.

$$r_{\text{гр}} = \sqrt{\frac{B}{4\Omega}} \tag{4.12}$$

Кесте 4.3 – Қашықтықтың r қатынасына және көздің максималды геометриялық өлшеміне байланысты жақын өріс коэффициентінің мәндері.

r/l_{max}	x	10lgx, дБ
0,6	3	5
0,8	2,5	4
1,0	2	3
1,2	1,6	2
1,5	1,25	1
2	1	0

Таңдалған октавалық жолағы үшін, fcp = 500 Гц, таңдалған α ср-ге тең келетін орташа дыбыс сіңіру коэффициенті бар өлшемді бөлмеде, көрсетілген октавада бір қондырғының (техникалық құжаттамаға сәйкес) корпусы шығаратын дыбыс қуатымен бірдей үш қондырғы бар. Lw диапазоны, дБ және максималды желілік өлшемі lmax, жабдықты N схемасына сәйкес орнатады. R1, r2, r3, m аралығындағы схемаға сәйкес RT есептік нүктесінде ультрадыбыстық қозғауды тиісті орнатудан анықтаңыз [17].

Кесте 4.4 – Айнымалылар мәндері

$a \times b \times c$	$\alpha_{\text{ср}}$	L_{w}	l_{max}	N	r_1	r_2	r_3
6×5×3	0,1	62	0,69	1	3	2	3

Формулаға сәйкес (4.11) дыбыс жұтылудың балама ауданын анықтаймыз.

$$A = \sum_{i=1}^{n} \alpha_i S_i + \sum_{j=1}^{m} A_j n_j = \alpha_{\text{ср}} S = 0{,}1 \cdot 2 \cdot (6 \cdot 5 + 3 \cdot 5 + 3 \cdot 6) = 12{,}6 \text{ м}^2$$

Формула бойынша (4.10) акустикалық тұрақты бөлме В.

$$B = \frac{A}{1-\alpha_{\text{ср}}} = \frac{12,6}{1-0,1} = 14 \text{ м}^2$$

Барлық үш көздер еденде болатынын қарастырайық (Ω = 2π), шекаралық радиус.

$$r_{\text{гр}} = \sqrt{\frac{B}{4\Omega}} = \sqrt{\frac{14}{8\pi}} \approx 0,75$$

Тиісінше, RT L_RT-де ультрадыбыстық сканерлеу ф = 1, Ω = 2π, x = 1 (кесте 3.3), k = 1 (3.5 кесте) немесе (3)

$$L_{\text{РТ}} = 10 \lg\left(\sum_{i=1}^{n} \frac{10^{0,1L_{wi}}\,\chi_i \Phi_i}{\Omega_i r_i^2} + \frac{4}{kB}\sum_{i=1}^{m} 10^{0,1L_{wi}}\right) =$$

$$= 10 \lg\left(10^{0,1\cdot 62}\left(\frac{1}{2\pi}\left(\frac{1}{2^2} + 2\cdot\frac{1}{3^2}\right) + \frac{4}{14}\cdot 3\right)\right) = 58,9 \text{ дБ}$$

Кесте бойынша шу деңгейі SNiP 23.003-2003 қозғалтқыш бөлмесінде 500 Гц - 78 дБ жиілікте тұрақты жұмыс орнына арналған, яғни есептелген ультрадыбыстық қалыпты болып табылады.

Қорытынды

Жүйеге зиянкестердің сеанстарын 24 сағат бойы қарап шыққаннан кейін, шабуылдардың шоғырлануы ұйымға, елге немесе тіпті операциялық жүйеге байланысты емес екені анық болады. Шабуыл көздерінің кең таралуы сканерлеу шуының тұрақты екенін көрсетеді және белгілі бір көздер үшін сәйкестендіру мүмкін емес. Интернетке қосылған кез-келген операциялық жүйе осы жүйелерде бірнеше деңгейдегі қауіпсіздікті қамтамасыз етуі тиіс. Жалпы және тиімді SSH шешімі шабуылдаған қызметті кездейсоқ жоғары портқа жылжытады. Бұл мықты парольді қорғауды және мониторингті қажет етпейді, бірақ сіздің мониторингіңіз үздіксіз сканерлеуден зардап шекпеуді қамтамасыз етеді. Біз осалдықтарды эмуляциялауға жауапты бағдарламалық жасақтаманың толық сипаттамасын ұсындық. Біз осалдықты эмуляциялау, тіркеу, қабықша кодтауды талдау және жіберу үшін бөлек модульдерді көрсеттік. Әр түрлі модульдер арасында үйлестіруді Amun-ның негізгі бөлігі болып табылатын Amun ядросы жүзеге асырады. Amun-ның басты мақсаты - құрттар немесе боттар сияқты зиянды бағдарламаларды жинауға арналған қарапайым платформа. Осы мақсатта Amun қарапайым Python сценарий тілін және жаңа осалдылық модульдерін қарапайым құруды қолдау үшін XML негізіндегі осалдық модульдерін жасау процесін қолданады. Осылайша, зиянды бағдарлама сарапшылары жабайы табиғатта қолданыстағы зиянды бағдарламаларды жинай алады және бағдарламалық жасақтама білімдерінсіз бағдарламалық жасақтаманы кеңейте алады. Нашар шабуылдарды анықтауға қатысты төменгі өзара әрекеттесетін аулаудың кейбір шектеулері болса да, олар бүгінгі желілік қауіпсіздік жүйелеріне тамаша қосымша болып табылады. Желіде жақсы орналастырылған астауды ескере отырып. Бұл пассивті датчиктер кез-келген сканерлеу машинасын анықтап, орталық IDS-ге ешқандай жалған позитивтерсіз хабарлауы мүмкін. Бұл дегеніміз, сигнализация эмуляцияланған осалдығын пайдаланған кезде ғана пайда болады. Ақыр соңында, honeypots зиянкестер мен олардың рәсімдерін зерттеу және зерттеуде маңызды құрал болып табылады.

Сіздің жоғары сапалы қызметіңізге қосылулар, сізді қызықтыруы мүмкін, мақсатты және шабуылға ұшырауы мүмкін. Жиі ашық Telnet порттары маршрутизаторларда немесе жоғары портқа оңай ауыстырылмайтын басқа құрылғыларда орналасқан. Ұйымыңыздың шабуыл бетінде сіздің ашық порттарыңызды түсіну - бұл қызметтердің брандмауэр арқылы қорғалғанына немесе мүлде ажыратылғанына кепілдік берудің жалғыз жолы. Егер Telnet қолданылса, бұғатталса, оны бақылап, күшті құпия сөздерді қолданатын болса, Telnet мүмкіндігінше шифрланған емес. Мен жазылған зиянкестердің журналдар мен сеанстардың үлкен саны бар келесі мақаланы орындаймын. Құқық бұзушылар әрекеттерін біле отырып, прогрессивті қорғаумен бір қадам алға тұруға болады. Осы бағдарламалық жасақтаманы зерттеу нәтижелері мен honeypot-тің зерттелу нәтижелері бойынша, осы

өнімді зиянкестердің сыни қауіп-қатерлерін және әрекеттерін анықтау және басымдықтау үшін пайдалануға болады деп есептеймін.

Әдебиеттер тізімі

1 Джеимс К.Ф. Принятие решений на основе нечетких моделей. Примеры использования. -Рига: Зинантне, 1990. -184 с.

2 Заде Л. Понятие лингвистической переменной и его применение к принятию приближенных решений. -М.: Мир, 1976. -166 с.

3 Непомнящий Е.Г. Экономическая оценка инвестиции: Учебник пособие. -Таганрог: Издательство ТРТУ, 2009. -262 с.

4 Каид Вадиа Ахмед Абдо, Многовариантный нечеткий выбор//III Всероссийская научная конференция молодых ученых, аспирантов и студентов. Т. 1. -Геленджик: Изд-во ЮФУ, 2014. - С. 105-106.

5 Кангро М.В. Методы оценки инвестиционных проектов: Учебное пособие. -Ульяновск: УлГТУ, 2011. -131 с.

6 Финаев В.И. Моделирование систем: Учебное пособие. -Таганрог: Изд-во ЮФУ, 2013. - 181 с.

7 Аверкин А.Н., Батыршин И.З., Блиншун А.Ф., Силаев Б.В., Тарасов Б.Н. Нечеткие множества в моделях управления и искусственного интеллекта -М.: Наука, 1986. - 312 с.

8 А. А. Муханова, А. М. Федотов. Классификация уязвимостей информационной безопасности в корпоративных системах, №1 (17), 2014.

9 Муханова А.А., Ревнивых А.В., Федотов А.М. Классификация угроз и уязвимостей информационной безопасности в корпоративных системах.// Вестник НГУ. -Сер.: Информационные технологии, 2013. - С. 55-72.

10 Конышев В.Н. Американский неореализм о природе войны: эволюция политической теории. URL: http://all-politologija.ru (кіру уақыты 15.05.2019)

11 Заде Л.А. Размытые множества и их применение в распознавании образов и кластер анализе. -М.: Мир, 1980 - С. 208-247

12 Бенджамин Пирс. Типы в языках программирования. -М.:Добросвет, 2012. - 680 с.

13 Иан Грэхем. Объектно-ориентированные методы. Принципы и практика. -М.: Вильямс, 2009. - С. 880

14 Антони Синтес. Освой самостоятельно объектно-ориентированное программирование за 21 день -М.: Вильямс, 2008. - С. 672

15 Гради Буч, Роберт А. Максимчук, Майкл У. Энгл, Бобби Дж. Янг, Джим Коналлен, Келли А. Хьюстон. Объектно-ориентированный анализ и проектирование с примерами приложений. -М.: Вильямс, 2010

16 Бекишева А.И. Методические указания к выполнению экономической части диломной работы для бакалавров специальности 5В0703 - Ифнормамционные системы - Алматы: АУЭС, 2013. -24 с.

17 Вербецовский А.А. Основы компьютерных технологий и современные ПК. -М.: АЛЕКС, 2002. -264 с.